THALES

Datacryptor® Ethernet

User Manual

1270A450-005 June 2008

Contents

1 Preface

Trademark Acknowledgements

Datacryptor is a trademark of Thales e-Security.

Microsoft Windows® XP and Windows® 2003 are registered trademarks of Microsoft Corporation.
All other logos and product names are trademarks or registered trademarks of their respective companies.

Revision Status

Revision	Changes	Release Date
1270A450-001	First Issue	March 2006
1270A450-002	Release 1.1	August 2006
1270A450-003	10 Gig Ethernet unit added and Updates for product release 4.00	November 2007
1270A450-004	100 Mb Ethernet unit added	March 2008
1270A450-005	Unsupported features in the 10Gig Ethernet unit: Auto-negotiation; Disabling CTS mode; Fragmentation	June 2008

License Agreement and General Information

THALES e-SECURITY LTD. ("THALES") COMPUTER PROGRAM LICENSE AGREEMENT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT (the "AGREEMENT"). FOR PURPOSES OF THIS AGREEMENT, "SOFTWARE" IS DEFINED TO INCLUDE COMPUTER PROGRAMS INTENDED TO BE RUN ON A WORK STATION, PC, OR SIMILAR MACHINE, AND INCLUDES THE CD-ROM OR OTHER MEDIA ON WHICH THE SOFTWARE IS CONTAINED. "FIRMWARE" IS DEFINED TO INCLUDE COMPUTER PROGRAMS WHICH ARE INTENDED TO BE RUN SOLELY ON OR WITHIN A HARDWARE MACHINE ("MACHINE") PROVIDED BY THALES, INCLUDING, WITHOUT LIMITATION, FPGA BITSTREAMS. THE SOFTWARE AND FIRMWARE AND THE ACCOMPANYING USER DOCUMENTATION (THE "DOCUMENTATION") ARE LICENSED (NOT SOLD) TO YOU BY THALES DIRECTLY OR THROUGH AUTHORIZED RESELLERS OF THALES. OPENING OR INSTALLING ANY OF THE CONTENTS OF THIS CD-ROM OR OTHER PROVIDED MEDIA PACKAGE INDICATES YOUR ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT AGREE WITH THE TERMS AND CONDITIONS, PROMPTLY RETURN THE PACKAGE, THE MACHINE WHICH CONTAINS A COPY OF THE LICENSED FIRMWARE, AND ALL OTHER ENCLOSED ITEMS, IF ANY, TO THE PLACE WHERE YOU OBTAINED THEM, AND YOU WILL RECEIVE A REFUND.

LICENSE GRANT

A. In consideration of the license fee paid to THALES or to an authorized THALES reseller, THALES hereby grants you, and you accept a nonexclusive license to use the Software on a single machine (if a "single license" is purchased) or multiple machines (if an "organizational license" is purchased) owned, leased, or otherwise controlled by you, and to use the Firmware solely on the Machine sold to you by THALES or its dealers, if any, but only to operate or engage those features and/or applications for which a charge appears on your order and invoice under the terms stated in this Agreement. If a software or Firmware enabling key or other similar access device (the "Key") is provided, you agree to use same solely for accessing the Software on a single PC or Firmware on a single Machine. Title and ownership of the Software, Firmware, Documentation and/or Key remain in THALES or its suppliers. If an organizational license is purchased, then you may use the Software or Firmware on multiple Machines in your organization regardless of quantity, provided all Machines are located within a single country. A separate single or organizational license will be required in each country.

B. You may not decompile, reverse engineer, modify, or copy the Software, Firmware, or Documentation for any purpose, except you may copy the Software into machine-readable or printed form for backup purposes in the event the CD-ROM or other provided media is damaged or destroyed. You may combine the Software with other programs. Any portion of the Software merged into or used in conjunction with another program will continue to be the property of THALES and is subject to the terms and conditions of this Agreement.

C. The Software, Firmware, and the Documentation are copyrighted by THALES and/or its suppliers. You agree to respect and not to remove or conceal from view any copyright or trademark notice appearing on the Software, Firmware, or Documentation, and to reproduce any such copyright or trademark notice on all copies of the Software, Firmware, and Documentation or any portion thereof made by you as permitted hereunder and on all portions contained in or merged into other programs and documentation.

D. You may transfer the Software, Firmware, and this license to another party if the other party agrees to accept the terms and conditions of this Agreement. If you transfer the Software and/or Firmware, you must at the same time either transfer all copies whether in printed or machine-readable form, and the Machine, if any, on which the Firmware is licensed for use, to the same party or destroy any copies not transferred; this includes all modifications and portions of the Software and/or contained or merged into other programs.

YOU MAY NOT USE, COPY, MODIFY, OR TRANSFER THE SOFTWARE, FIRMWARE, DOCUMENTATION OR KEY, OR ANY COPY, MODIFICATION OR MERGED PORTION, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED FOR IN THIS LICENSE.

IF YOU TRANSFER POSSESSION OF ANY COPY, MODIFICATION OR MERGED PORTION OF THE SOFTWARE, FIRMWARE, OR DOCUMENTATION OR KEY TO ANOTHER PARTY, EXCEPT AS PROVIDED IN THIS SECTION D, YOUR LICENSE IS AUTOMATICALLY TERMINATED.

TERM

This Agreement is effective upon your acceptance (as set forth above) and shall continue until terminated. You may terminate this license at any time by destroying the Software, Key, and Documentation along with all copies, modifications and merged portions in any form, and return the Machine (including Firmware) to THALES or its authorized resellers. It will also terminate upon conditions set forth elsewhere in this Agreement if you fail to comply with any term or condition of this Agreement. You agree upon such termination to destroy the Software, Documentation, and Key together with all copies, modifications and merged portions in any form, and to return the Machine (including Firmware) to THALES or its authorized resellers.

LIMITED WARRANTY

The following limited warranty applies only to the Software and/or Firmware licensed hereunder. The hardware Machine is warranted pursuant to a separate Warranty set forth in the Machine documentation. The Machine documentation is contained on the CD-ROM, if any.

During the first 90 days after receipt of the Software and/or Firmware by you, as evidenced by a copy of your receipt, invoice or other proof of purchase (the "Warranty Period"), THALES warrants, for your benefit alone, that the Software and Firmware when properly installed, will perform substantially in conformance with the Documentation provided by THALES at the time you obtained the Software and/or Firmware from THALES or its authorized resellers, and that the media on which the Software and/or Firmware is furnished will be free from defects in materials and workmanship under normal use.

EXCEPT AS SPECIFICALLY PROVIDED ABOVE, THE WARRANTIES PROVIDED HEREIN ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. WHEREVER SUCH EXCLUSION IS NOT PERMITTED BY LAW, ALL IMPLIED WARRANTIES, INCLUDING THOSE OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE, SHALL BE LIMITED TO THE WARRANTY PERIOD. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH MAY VARY FROM JURISDICTION TO JURISDICTION.

THALES does not warrant that the functions contained in the Software or Firmware will meet your requirements or that their operation will be uninterrupted or error free.

LIMITATIONS OF REMEDIES

THALES, its authorized resellers', and/or its suppliers' entire liability and your exclusive remedies under this Agreement are as follows:

(1) THALES shall use commercially reasonable efforts to correct any defect in the Software or Firmware which is reported by you during the Warranty Period in writing to THALES, provided such defect can be recreated by THALES in an unmodified version of the Software or Firmware. However, if THALES is unable to correct such defect within a reasonable amount of time, you may terminate this Agreement by returning the Software, Machine including Firmware, Documentation, and Key to the place where you obtained them either for replacement or, if so elected by THALES, a refund of the amount paid by you for the subject item.

(2) THALES shall replace any media not meeting THALES' "Limited Warranty" and which is returned to THALES with a copy of your receipt, invoice or other proof of purchase or, if THALES is unable to deliver replacement media which is free from defects in materials or workmanship, you may terminate this Agreement by returning the Software, Firmware, Documentation, and Key to the place where you obtained them for a refund of the amount paid by you for the subject item.

IN NO EVENT WILL THALES, ITS AUTHORIZED RESELLERS, OR ITS SUPPLIERS BE LIABLE FOR INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES OF ANY KIND OR TYPE, INCLUDING, BUT NOT LIMITED TO LOSS OF PROFITS OR REVENUE, LOSS OF USE OF THE PRODUCT(S) OR ANY ASSOCIATED PRODUCT(S), OR COST OF SUBSTITUTED FACILITIES, PRODUCTS OR SERVICES WHICH ARISE OUT OF THALES' PERFORMANCE OR FAILURE TO PERFORM ANY OBLIGATION CONTAINED WITHIN THIS AGREEMENT OR WITH USE, OR INABILITY TO USE, SOFTWARE AND/OR FIRMWARE, WHETHER THE CLAIM FOR DAMAGES IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE. EXCEPT FOR CLAIMS FOR PERSONAL INJURY OR FOR DAMAGE TO REAL OR TANGIBLE PROPERTY TO THE EXTENT CAUSED BY THALES' FAULT OR NEGLIGENCE, THALES' MAXIMUM LIABILITY FOR ANY CLAIM FOR DAMAGES RELATING TO THALES' PERFORMANCE OR NON-PERFORMANCE UNDER THIS AGREEMENT SHALL BE LIMITED TO THE LESSER OF (a) YOUR ACTUAL DAMAGES OR (b) THE COST OF THE PRODUCT GIVING RISE TO THE LIABILITY.

SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

PURCHASES BY OR FOR THE FEDERAL GOVERNMENT

The government hereby agrees that this software qualifies as "commercial computer software" as that term is used in the acquisition regulation applicable to a purchase order or contract. This software may not be acquired by the government in a contract incorporating clauses prescribed by DFARS Subpart 227.4 (OCT 1988), in which case the government hereby agrees to return the software unused, in exchange for refund of the full purchase price.

The government agrees that it shall be bound by the terms and conditions of this license agreement, to the maximum extent possible under federal law. This license agreement, and the governments assent hereto, supersedes any contrary terms or conditions in other contract documents (such as any statement of work).

EXPORT AUTHORIZATIONS

You shall assume all responsibility for obtaining any required export authorizations necessary to export any Software and/or Firmware and Documentation purchased hereunder. You shall not re-export Software and/or Documentation directly or through others, or the product of such data, to the prescribed countries for which such prohibition exists pursuant to the U.S. or U.K. export regulations unless properly authorized by the appropriate government.

GENERAL

You may not sublicense, assign or transfer this license, Software, Firmware, Documentation or Key, except as expressly provided in this Agreement. Any attempt otherwise to sublicense, assign or transfer any of the rights, duties or obligations hereunder is void.

This Agreement will be governed by the laws of England or the event that the Product was delivered in the United States, Latin America or Canada, the laws of the State of Virginia.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT IT IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN YOU AND THALES WHICH SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING (ORAL OR WRITTEN) BETWEEN US RELATING TO THE SOFTWARE OR FIRMWARE.

NOTWITHSTANDING THE ABOVE, IF YOU PREVIOUSLY SIGNED A SEPARATE AGREEMENT HAVING A SOFTWARE LICENSE PROVISION APPLICABLE TO THIS PROGRAM, WHICH HAS NOT EXPIRED OR BEEN TERMINATED, THE TERMS AND CONDITIONS OF SUCH SEPARATE AGREEMENT AND THE SOFTWARE LICENSE CONTAINED THEREIN SHALL TAKE PRECEDENCE OVER ALL CONFLICTING TERMS AND CONDITIONS, IF ANY, CONTAINED IN THIS LICENSE AGREEMENT. OTHERWISE, ANY ADDITIONAL TERMS AND CONDITIONS SET FORTH IN THIS LICENSE AGREEMENT SHALL SUPPLEMENT AND BE READ IN CONJUNCTION WITH THE SOFTWARE LICENSE CONTAINED IN ANY SUCH SEPARATE AGREEMENT.

Hardware Warranty

The period of warranty for this product starts on the date of sale to the original purchaser and ends 365 days thereafter. Thales e-Security will replace any product that fails within 90 days of the date of sale. For failures which occur more than 90 days after the date of sale, Thales e-Security will repair the product if returned, postage prepaid, to our designated repair center.

Thales e-Security requires a Return Authorization Number (RAN) prior to the return of any equipment under the provisions of this warranty. Please contact your authorized reseller or the nearest Thales e-Security product support center for details.

General Requirements

This equipment should be installed by a qualified Service engineer. Incorrect connection will invalidate warranty and may cause a hazard.

Should any malfunction be suspected in the unit, return the apparatus to your supplier for service and/or repair to ensure continued compliance. The Datacryptor Ethernet unit contains no user serviceable parts.

The unit should be installed in an environment compatible with the maximum operating temperature of the unit.

Installation of the unit in a rack should not reduce airflow so as to compromise safe operation of the unit. Particular attention should be made to make sure that the side ventilation holes on the Datacryptor Ethernet are not obstructed which could reduce the airflow through the unit. Please refer to the Installation chapter, in the section titled "Airflow" for further information on providing appropriate air flow.

When installed in a rack make sure that the unit is securely installed using all the appropriate mechanical fixings so that it will not cause a hazardous condition.

Security Advisory

This unit is being shipped with a Universal Certificate Authority that is to be used for demonstration purposes only. USE OF THE DEVICE, AS INITIALLY CONFIGURED, IN AN OPERATIONAL ENVIRONMENT IS NOT RECOMMENDED. THALES e-SECURITY EXPRESSLY DISCLAIMS ANY AND ALL LIABILITY FOR DAMAGES, INCLUDING BUT NOT LIMITED TO CONSEQUENTIAL DAMAGES, RESULTING FROM USE OF THE UNIVERSAL CERTIFICATE OR ANY OTHER CERTIFICATE SUPPLIED BY THALES e-SECURITY. Prior to use in an operational environment, please change the certificate authority, following the procedure(s) described in the Key Manager section.

Contact Information

SALES OFFICES

Americas

THALES e-Security, INC
2200 North Commerce Parkway
Suite 200
Weston, Florida 33326
U.S.A.
Tel: +1 954 888 6200
Fax: +1 954 888 6211
Toll free within USA:
+1 888 744 4976
e-mail:
sales@thalesesec.com

Europe, Middle East, Africa

THALES e-Security LTD
Meadow View House
Long Crendon
Aylesbury
Buckinghamshire HP18 9EQ
England
Tel: +44 (0)1844 201800
Fax: +44 (0)1844 208550
e-mail:
emea.sales@thales-esecurity.com

Asia Pacific

THALES e-Security (ASIA) LTD
Units 2205-06, 22/F
Vicwood Plaza
199 Des Voeux Road, Central
Hong Kong
Tel: +852 2815 8633
Fax: +852 2815 8141
e-mail:
asia.sales@thales-esecurity.com

PRODUCT SUPPORT CENTERS

Americas

Tel: +1 954 888 6277
Toll free within USA:
+1 800 521 6261
Fax: +1 954 888 6233
e-mail:
support@thalesesec.com

Europe, Middle East, Africa

Tel: +44 (0) 1844 202566
Fax: +44 (0) 1844 208356
e-mail:
emea.support@thales-esecurity.com

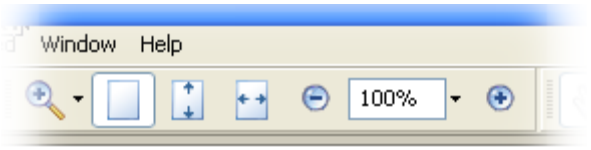
Asia Pacific

Tel: +852 2815 8633
Fax: +852 2815 8141
e-mail:
aisa.support@thales-esecurity.com

2 About This Document

Viewing this document in Adobe Acrobat PDF Viewer

It is recommended that this PDF document is viewed at 100% size with text smoothing adjusted to suit your monitor. The viewing size is easily adjusted by the use of the Zoom toolbar; you may set 100% size, or simply click the *Actual Size* icon:



Viewing at 100% will provide the best appearance of the images in this document.

To change the appearance of the text, select: **Edit** > **Preferences** > **Page Display**. Change the *Smooth Text* option and click **OK**. Use this option to compare the appearance of the text with and without text smoothing, and then select the setting that provides the most comfortable reading experience.

Introduction to this Manual

There are three models in the Datacryptor Ethernet range: 100 Mb Ethernet, 1 Gig Ethernet, and 10 Gig Ethernet. Predominantly, the information in this manual applies equally to all models and as such, the device is referred to simply as the 'Datacryptor Ethernet'. Where there are differences, the unit being described is referred to either as the 100 Mb Ethernet, 1 Gig Ethernet, or 10 Gig Ethernet, as appropriate. The differences between the two models are mainly in the speed of operation and the physical size of the casing.

This manual describes how to install the Thales Datacryptor Ethernet unit and the Element Manager software. It also describes how to use the Element Manager software to configure and manage the Thales Datacryptor Ethernet device.

This document is intended for use by network technicians, managers and security administrators who are familiar with setting up and maintaining network equipment. Some knowledge of network security issues and encryption technologies is assumed.

This document assumes that its readers have an understanding of the following:

- Basic principles of network security issues
- Basic principles of encryption technologies and terminology
- Basic principles of Ethernet technology
- Basic principles of TCP/IP networking, including IP addressing, switching and routing
- Personal computer (PC) operation, common PC terminology, and use of terminal emulation software.

The following conventions are used in the body text of this document:

Bold font: Indicates a command to be issued or selected by the user.

- **`Courier font:`** Indicates information input or output to/from the Control PC.
- *Italic font*: Indicates the name of dialog, parameter, object, etc.

This manual is organized into the following sections:

Overview provides general information on the hardware and software.

Background Information provides a brief introduction to the device and Ethernet Layer 2 technology and terminology.

Installation describes how to install the Datacryptor Ethernet hardware and Element Manager Software.

Connecting to Datacryptor Ethernet Units describes the main methods that can be used to connect the PC to the Datacryptor Ethernet unit.

Element Manager Reference provides an overview of the functions provided by the Element Manager, followed by a detailed description of each in turn.

Appendix A: Device Maintenance describes the periodic maintenance required on your Thales Datacryptor Ethernet unit.

Appendix B: Loading Datacryptor Unit Software describes how to load software into your Thales Datacryptor Ethernet unit. Your Datacryptor will be supplied pre-loaded with software, so you will only require the information in this appendix if a re-load or upgrade is needed.

Appendix C: Product Specifications gives the system specifications.

Appendix D: Environment and Regulatory Information describes the operating conditions and regulatory certifications.

Appendix E: SFP and XFP Interfaces describes the possible transceiver options.

Appendix F: Preventing Electrostatic Discharge describes how to minimize the risk of ESD.

Appendix G: Troubleshooting describes how to diagnose and repair common problems.

Appendix H: SNMP MIB Support describes the SNMP MIBs supported by the device and the location of them.

Appendix I: Log and SNMP Trap Numbers provides a list of all the log and trap numbers together with descriptions of their purpose.

Appendix J: Glossary defines terms used in this document.

3 Overview

The Thales Datacryptor Ethernet is a high speed, high bandwidth, integrated security appliance. The three models provide different transfer speeds; the 100 Mb Ethernet provides 100 Mbps, while the 1 Gig and 10 Gig Ethernet units offer encryption at Gigabit Ethernet Layer 2 transfer rates.

The Datacryptor Ethernet units come in different case styles; the 100 Mb Ethernet and the 1 Gig Ethernet models are housed in a single unit height 19-inch rack case for transmission speeds up to 100 Mbps and 1000 Mbps respectively, while the 10 Gig Ethernet model uses a double height unit for 10,000 Mbps transmission speeds. The 100 Mb Ethernet unit may have its rack mounting brackets removed so that it can be used as a desktop unit.

The 100 Mb Ethernet units have standard RJ45 sockets on the front panel for Host and Network connections, while the 1 Gig and 10 Gig Ethernet units have two Small Form Factor sockets on the front panel; these accept a range of transmit/receive interfaces. The 1 Gig Ethernet unit uses SFP type sockets, and the 10 Gig Ethernet unit uses the XFP type sockets.

The host port is connected to the private network and receives the data for encryption. Encrypted data is then passed through the network port for secure transmission over the public network.

The Datacryptor Ethernet is designed to operate as a Layer 2 (Data Link) encryptor. The advantage of this is it makes the unit fully transparent to higher protocols.

The units are housed in a tamper evident chassis with interlock switches that will cause the key material to be erased if the lid is removed.

Product Images

Figure 3-1: Thales Datacryptor 100 Mb Ethernet Front Panel

Figure 3-2: Datacryptor 100 Mb Ethernet Rear Panel

Figure 3-3: Thales Datacryptor 1 Gig Ethernet Front Panel

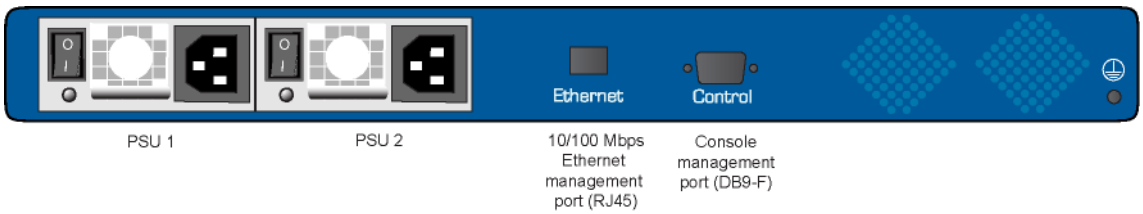


Figure 3-4: Datacryptor 1 Gig Ethernet Rear Panel

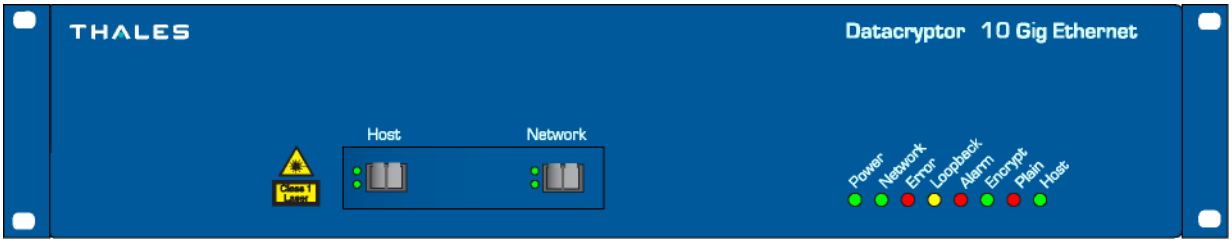


Figure 3-5: Thales Datacryptor 10 Gig Ethernet Front Panel

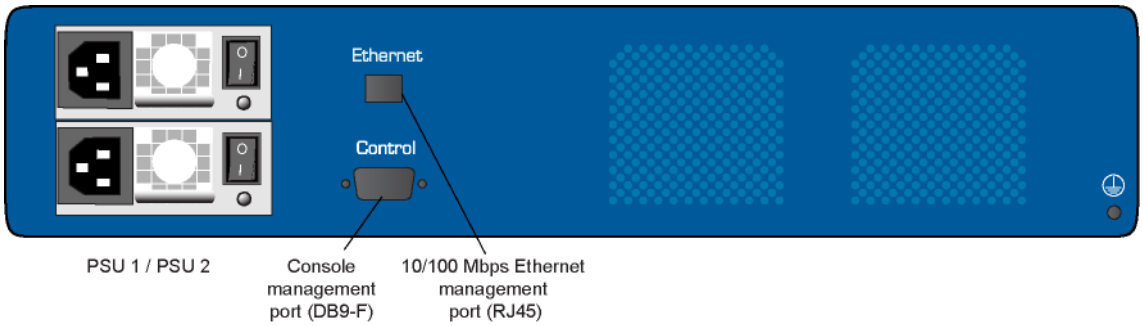


Figure 3-6: Datacryptor 10 Gig Ethernet Rear Panel

Note: See The Front Panel LEDs in the Element Manager Reference section for full information on the LED indicators.

Product Features

Installation

- Mount in any standard 19” rack or on a tabletop

Interfaces

- The 100 Mb Ethernet has two RJ45 sockets for connecting to the Host and Network circuits
- The 1 Gig Ethernet and 10 Gig Ethernet units have two SFP or XFP sockets which accept a range of transceiver modules for the encrypting and decrypting of network traffic
- Device management access through a 10/100 Ethernet port or an RS-232 craft port

Security features

- Designed to FIPS 140-2 Level 3

Hardware-based encryption processing

- Very low latency

Maximum Data Transfer Rate

- 200 Mbps full duplex (100 Mb Ethernet unit), 2 Gbps full duplex (1 Gig Ethernet unit), or 20 Gbps full duplex (10 Gig Ethernet unit)

Network Interfaces

- 10/100BaseT: User selectable between 10 Mbps and 100 Mbps
- 1 Gig Ethernet: 1000 Mbps full duplex
- 10 Gig Ethernet: 10,000 Mbps full duplex
- Auto negotiation (does not apply to the 10 Gig Ethernet)

Key management

- Diffie-Hellman key exchange (groups 1, 2, and 5)

Encryption

- Advanced Encryption Standard (AES):
  FIPS 197 (256 bit keys)

Management integrity

- HMAC-SHA-1-96 (FIPS PUB 180-1): RFC 2104, 2404
- HMAC-MD5-96 : RFC 2104, 2403, 1321

Device management

- Element Manager
- Secure download of software updates
- X.509v1 and X509 v3 digital certificate support

Power

- 100 Mb Ethernet Unit:
  Single fixed AC (universal) or DC (-48 V) power supply:
  15W (51 BTU/hr)
- 1 Gig Ethernet and 10 Gig Ethernet:
  Redundant hot swappable AC (universal) or DC (-48 V) power supplies:
  1 Gig: 120 W (410 BTU/hr)
  10 Gig: 140 (480 BTU/hr)

Element Manager

The Element Manager application provides a secure way to configure, manage, and upgrade the Datacryptor Ethernet. The program runs under various versions of Microsoft Windows operating systems. Please see the Software Requirements for a more detailed description of the environment required.

The PC can connect to a Datacryptor Ethernet unit to manage it using the IP protocol over a standard 10/100 Ethernet connection. The PC can also connect to a Datacryptor Ethernet unit using PPP protocols via a serial connection. Once the PC is connected to the Datacryptor Ethernet unit, a communications session can be established; and all the functions provided by the Element Manager are available.

4 Background Information

Datacryptor Ethernet Unit

The Thales Datacryptor Ethernet units are high performance, integrated security appliances that provide encryption at high line speeds. The 1 Gig and 10 Gig Ethernet units operate at optical line speeds and have the added advantage that they can, over limited distances, use copper media. The device's high-speed processing capabilities eliminate bottlenecks while providing data encryption and integrity.

It is ideal for bandwidth intensive, latency sensitive applications that demand security and speed, such as site-to-site VPNs, and the transfer of imaging over the network. It provides secure transport over private or public networks.

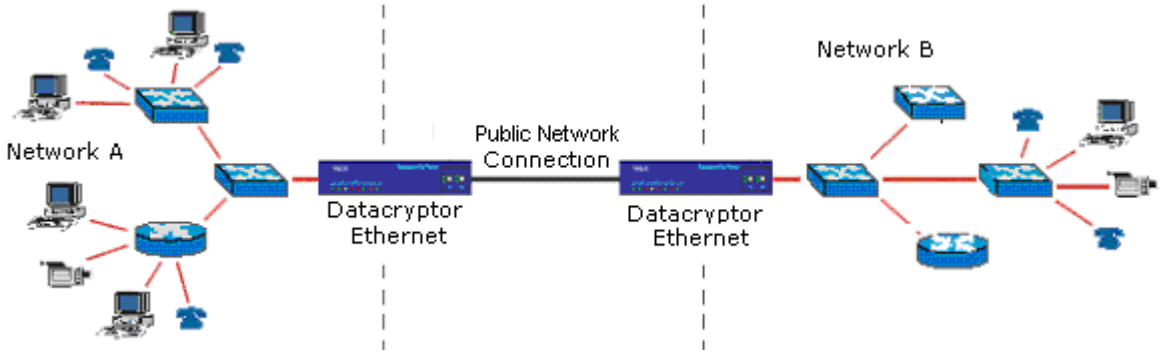


Figure 4-1. An Example of a Site to Site Ethernet Layer 2 connection

A site-to-site VPN application is shown above. The Thales Datacryptor Ethernet is deployed on either side of the connection, securing the data transmitted across the untrusted public network. Data is sent from a web server through to the host network. It is then encrypted by the Datacryptor Ethernet for secure transfer over the public network, where a second Datacryptor Ethernet decrypts the data at its destination.

Gigabit Ethernet Technology Overview

The Gigabit Ethernet technology used by the 1 Gig and 10 Gig Ethernet units is the latest specification in the IEEE 802.3 Ethernet standard series. This standard allows the transmission of data at one or ten Gigabit per second transmission speeds (1 Gbps or 10 Gbps). However the speed is usually designated as 1,000 Mbps or 10,000 Mbps, as appropriate, to comply with the standard method of showing Ethernet network speeds.

Ethernet Layer 2 Services

Ethernet Layer 2 security services include:

Encryption - The Advanced Encryption Standard (***AES***) algorithm is a symmetric block cipher capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. The Datacryptor uses 256 bit keys.

Authenticate Management Data - The Datacryptor Ethernet uses the HMAC keyed hash variant of the SHA-1(Secure Hash Algorithm) to authenticate management data using SNMP v3.

Security Terms

Diffie-Hellman – Diffie-Hellman is a method for key exchange that allows two autonomous systems to exchange a secret key over an untrusted network without prior secrets. Diffie-Hellman groups define the strength supplied to the Diffie-Hellman calculation for the later creation of keys by the peers. Three of the five available groups are generated from modulo function (MODP) calculations and the leveraging of very large prime numbers.

Peer – A peer is a Datacryptor that acts as a tunnel endpoint. A peer encrypts or decrypts data, adding or stripping away headers, respectively.

Other Terms

Layer2 -The Datacryptor Ethernet is designed to work as a Layer two encryptor.

The addressing scheme is physical i.e. the addresses are MAC (Media Access Control) addresses hard coded into a device at the time of manufacture. It is generally a 48-bit address which is usually displayed in hexadecimal format as six two digit parts 01-0B-3B-18-00-CA.

It should be noted that when the unit is operating in the Tunneling mode the peer unit MAC address must be obtained and entered in the box provided on the relevant property tab.

Frame Checksum (FCS) - FCS is an error detection system based on the numerical value of the number of set bits in the Frame (packet). This value is transmitted alongside the message, and the receiving device then applies the same criteria and compares the two values.

Auto-negotiation - Auto-negotiation was devised to address the need for multi-speed devices on a network to operate at the optimum settings. It achieves this by taking control of the connection medium and detecting the various mode options available in the device on the other end, while also advertising its own capabilities. Thus it enables the connection to configure the highest performance mode of interoperation.

Note: The Datacryptor 1 Gig Ethernet only supports I000 Mbps full duplex, and the 10 Gig Ethernet unit only supports I0,000 Mbps full duplex. The 100 Mb Ethernet unit can be set to run at speeds of I0 Mbps and I00 Mbps. The 10 Gig Ethernet unit does not support Auto-negotiation.

Jumbo frames - Jumbo frame is the name given to frames larger than the standard Ethernet MTU of 1500 bytes. The Datacryptor Ethernet encryptor does not have an MTU limit and will therefore allow Jumbo frames. Frame size is only limited if fragmentation is enabled.

Multiprotocol Label Switching – MPLS is a solution to the question of many of the earlier network problems such as speed, scalability and quality of service. This is achieved by the defining of paths across the network by the addition of label information to a packet to aid routing etc. It is referred to as multi-protocol because it supports a number of communication methods such as IP, Frame Relay and ATM. The Datacryptor Ethernet unit is transparent to this operation as long as the equipment is being deployed in a point-to-point environment.

5 Installation

This section will detail the installation of the hardware and software. Hardware installation is discussed first.

Hardware Installation

There are four steps in installing the unit:

- Unpack the Shipping Carton
- Mount the Unit
- Connect the Cables
- Power on the Datacryptor

Unpack the Shipping Carton

Remove all product components from the shipping carton and compare the contents to the packing list. Keep all packaging in case it is necessary to return the appliance. The Datacryptor is packaged with the following items:

- Datacryptor Ethernet, with the Datacryptor firmware and software factory-installed on the appliance.
- 115v, 240v or DC Power Supply cables (as appropriate).
- RS-232 cable.
- Element Manager CD-ROM (includes User Manual).
- Release Notes.
- Quick Start Guide.

Note: Interface transceivers (if ordered) will be shipped separately from the Datacryptor unit (1 Gig and 10 Gig Ethernet units only).

Rack-Mounting Instructions

The Datacryptor can be mounted in a standard 19-inch rack using the front mounting brackets, or simply placed on a rack shelf or solid surface.

Preparation

Before installing the Datacryptor in a 19-inch rack, consider the following rack-mounting guidelines:

Ambient temperature

Install the Datacryptor in an environment compatible with the 105ºF (40ºC) maximum recommended ambient temperature. Extra clearance above or below the unit on the rack is not required; however, be aware that equipment placed in the rack beneath the Datacryptor can add to the heat load. Therefore, avoid installing in an overly congested rack. Air flowing to or from other equipment in the rack might interfere with the normal flow of cooling air through the Datacryptor, increasing the potential for overheating.

Airflow

Make sure that there is sufficient flow of air around the Datacryptor so that safe operation is not compromised. Maintain a clearance of at least 3 inches (7.62 cm) at the sides of the Datacryptor to ensure adequate air intake and exhaust. If installing in an enclosed rack, make sure the rack has adequate ventilation or an exhaust fan. An enclosed rack with a ventilation system that is too powerful can prevent proper cooling by creating negative air pressure around the Datacryptor.

Mechanical Loading

Keep the center of gravity in the rack as low as possible. This ensures that the weight of the Datacryptor will not make the rack unstable. Make sure that the rack is secured and use the proper mounting hardware to secure the Datacryptor to the rack.

Circuit Loading

Consider the connection of the Datacryptor to the supply circuit and the effect that overloading of circuits might have on over current protection and supply wiring. Consult the voltage and amperage ratings on the UL label affixed to the unit's rear panel when addressing this concern. As the 1 Gig and 10 Gig Ethernet units are fitted with two hot swappable power supply units, consideration could be given to these types of Datacryptors using a different supply phase for each of the power supply units.

Disconnection

Power disconnection is achieved by removal of the plugs from the mains outlet sockets. Ensure that the socket-outlets are close to the unit, and can be easily identified and accessed.

Grounding

Maintain reliable grounding of a rack-mounted Datacryptor. Pay particular attention to supply connections other than direct connections to the branch circuit, such as the use of power strips.

Maintenance

Allow at least 19 inches (48.3 cm) of clearance at the front of the rack for maintenance. Use a cable-management system to help keep cables organized, out of the way, and free from kinks or bends that degrade cable performance.

Connect the Cables

Before beginning, make sure the necessary cables are available. See the Cabling Requirements section below for more information.

Cabling Requirements

The following table outlines the cabling requirements for each port on the Datacryptor Ethernet. The connector type listed indicates only what is required to connect to the Datacryptor's port, and may or may not be the same connector type required for the other end of the cable.

Port	Cabling	Supplied By
Network and Host Port	*For the 100 Mb Ethernet unit*: Category 5 or above RJ-45 connector. *For the 1 Gig and 10 Gig Ethernet units*: Dependant on the SFPs or XFPs ordered with the unit. The options are Category 5 or above RJ 45 connector. 850nm Multi-mode fiber. 1310nm or 1550nm Single mode fiber.	Customer
10/100 Ethernet Management Port	Shielded Category 5 straight through cable (STP), RJ-45 connector. Used when connecting through a LAN.	Customer
	Category 5 crossover cable with RJ-45 connector. Required for a direct connection between the management station and the Datacryptor.	Customer
RS-232 Craft Port	Shielded copper serial cable, RS-232 DB9 connector (female to male)	Thales
Power receptacles	Power supply cables	Thales

To meet the requirements of FCC Part 15 and the Directive 89/336/EEEU EMC C, use only shielded cables (DB-9 null modem cables and Category 5 STP cables).

To Cable the Datacryptor

The Host and Network interface transceivers that are used with the 1 Gig and 10 Gig Ethernet units are shipped separately from the Datacryptor unit, and therefore must be inserted before proceeding with the cabling operation.

The connections are the same when using any of the three types of Ethernet unit. The illustration below shows a 1 Gig Ethernet unit – please note that the management ports of the 100 Mb Ethernet unit are on its front panel.

- Either connect the RS-232 craft port directly to a PC or workstation using the supplied DB-9 null modem cable, or
- Connect the 10/100 Ethernet management port for management access:
  - If connecting to a LAN, use a Category 5 STP straight-through cable with an RJ-45 connector.
  - If connecting directly to a PC, use a shielded Category 5 crossover cable and make sure that the PC and management port IP addresses are on the same subnet.

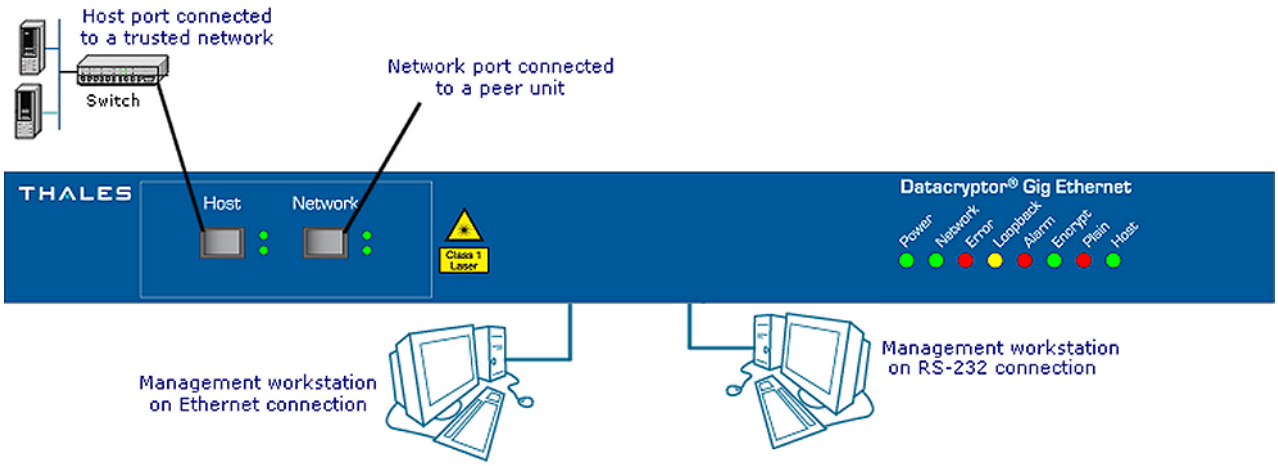


Figure 5-1: Datacryptor Panel Connectors
(The 100 Mb Ethernet unit's management ports are located on the front panel)

	WARNING: (1 Gig and 10 Gig Ethernet units only) Infra-red radiation is emitted from aperture ports of single mode or multi-mode transceivers when no cable is connected. Avoid exposure and do not stare into the open apertures. Apertures should be covered when not in use.

Power on the Datacryptor

The Datacryptor software is factory-installed on the appliance. The bootable image is stored on compact flash. Applying power to the Datacryptor initializes the system, which includes:

- Initializing the components
- Performing hardware diagnostics
- Loading the software
- Diagnostic Boot sequence

To power on the Datacryptor

1. The 1 Gig and 10 Gig Ethernet Datacryptor appliances are supplied with two separate hot swappable power supply units. The 100 Mb Ethernet units have a single fixed power supply unit. The power supply units for all models of Datacryptor can be either AC or DC (-48 V).
2. The AC power supplies are auto-sensing 100 to 240 Volts 50 to 60 Hz.
3. Before applying power to the Datacryptor verify that the voltage shown on the UL label affixed to the unit's back panel is appropriate for your site.

	CAUTION: If the voltage of the Datacryptor is inappropriate for your site, do not apply power to the appliance. Contact Customer Support immediately.

4. On the Datacryptor's rear panel, plug the power cords into the power receptacles. Attach the opposite ends to a power source.

   The power LED illuminates when the unit is powered up. The Diagnostic Boot sequence allows the LEDs to be checked and the unit type to be verified. The sequence follows this pattern:

   - All LEDs on for one second.
   - A pattern which indicates the unit type for one second.
   - All LEDs on for one second.

Unit Type	Network	Error	Loopback	Alarm	Encrypt	Plain	Host
100 Mb Ethernet	_	X	_	_	X	X	_
1 Gig Ethernet	_	X	_	_	X	_	_
10 Gig Ethernet	_	X	_	_	X	_	X

   Where, **X** is LED on, and _ is LED off.

   During the boot process the Datacryptor discards all traffic on its data ports.

If the boot process fails the Error LED illuminates and the Datacryptor generates a **critical Error** trap. If you experience a problem during the system initialization, see the troubleshooting information in Appendix G: Troubleshooting.

Software Installation

There are two software programs, the firmware resident in the Datacryptor Ethernet unit and the Element manager software.

The firmware provides the units functionality and is pre-installed. The unit has the ability to upgrade with new firmware, offering new features, without the requirement of returning the unit to Thales. Instructions on the Firmware Upgrade ability will be provided with any upgrade.

The Element Manager software is provided on the supplied CD-ROM and must be installed as directed below.

Requirements

The PC to be used for running the Element Manager must meet these minimum requirements:

- The PC must be an IBM PC or compatible that meets the minimum requirements for running the following version of Microsoft Windows:
  - Microsoft Windows XP, Service Pack 2 or higher (32 and 64 bit versions).
  - Note: The software may install and run on older Windows platforms, but due to Microsoft's Support Lifecycle policy, we may be unable to support installation and runtime issues on these older platforms. Please refer to the Microsoft Support Lifecycle support web page at: http://support.microsoft.com/gp/lifecycle.

- The PC must have a pointing device (mouse), a CD ROM drive, a free serial port, and at least 228 Mb hard disk space (for the software and data files). If you want to install the Adobe Acrobat reader (included on the CD to view the manuals) this will require a further 10 MB of hard disk space.
- The user should ensure that there is at least 5Mb of memory for each copy of the Front Panel Viewer being run concurrently.
- The PC must be able to reach the Datacryptor on the Ethernet network, or alternatively be connected to the unit via a serial cable to the unit's control port.

Installation Procedure

To install the Element Manager on the PC:

- Insert the CD-ROM containing the Element Manager software into your PC.
- This will auto-start the installation page. Select the "Install the Datacryptor Element Manager Software" link OR run the program 'setup.exe' from the root directory on the CD.
- Follow the instructions displayed by the installation manager.

6 Connecting to Datacryptor Ethernet Units

There are three methods of connecting to the Datacryptor Ethernet units: Element Manager, serial connection to CLI, and SNMP.

The Element Manager GUI application is used to manage and configure the Datacryptor Ethernet device(s). It connects to the Datacryptor via the 10/100 Ethernet Management port.

A serial connection can be made to the Datacryptor Ethernet to interface to a text-based Command Line Interface (CLI). This serial interface can also be used to access the element manager software.

A third-party SNMP Version 1, Version 2c, or Version 3 compliant network management application can collect and display performance monitoring data, but may not alter any system level parameters. The only supported configuration tasks are those associated with SNMPv3 user and view based access control. SNMP traps are issued as Version 3 and authentication and encryption are supported.

Users

The Datacryptor Ethernet will encrypt everything passed to it from the host network and place it onto the public network. Because of this there is no need to create secure users for the Datacryptor Ethernet, as anyone sending information will automatically use the Datacryptor Ethernet unit.

The people who administrate and configure the Datacryptor Ethernet do need to be secure and need to be authenticated using secure methods. Certificates are loaded into the Datacryptor Ethernet units that have keys used to sign messages between the PC used for configuration and the units themselves. The AES keys used to encrypt and decrypt the data being passed between Datacryptor units are automatically generated using Diffie Hellman and the supplied Diffie Hellman parameters.

When first installing the Datacryptor, use the default password. Thales strongly recommends that the Administrator changes the password before the unit is put in service and changes from the Universal CA to their own custom CA to ensure maximum security (see the Change Password dialog section). Passwords are case-sensitive.

IP Parameter Configuration via a Serial Connection

When shipped, a Datacryptor Ethernet device has the following port settings:

Port	IP address	Net Mask
Control	2.2.2.2	255.0.0.0
Ethernet management	255.0.0.0	255.255.255.255
Network	1.n.n.n	255.0.0.0

To change the parameters follow the steps below:

1. Connect the Datacryptor's RS-232 craft port directly to the terminal's serial port using the supplied DB-9 serial cable.

2. Open a terminal session through a VT-100 terminal emulation program such as HyperTerminal. Enter the connection name, the appropriate serial port (usually COM1 or COM2), and the following serial port parameters:

Serial Port Parameter	Value
Baud Speed	115,200
Parity	None
Data Bits	8
Stop Bits	1
Flow Control	None

3. Switch on the Datacryptor unit.
4. As the unit boots the message **CONFIG STARTUP Y/N** will be shown and all the units LEDs will be lit.
5. Press **Y** the unit will respond by displaying a short banner and the prompt IPCONFIG>.
6. At the command prompt, type Help for a list of commands available.

Command	Description
HELP	Display help for a command
HELPKEYS	List of keyboard usage in this command interface
DEFAULT	Return all IP address and net mask settings to defaults.
DISPLAY	Display current IP address and net mask settings
IPFORWARD	Enable or disable IP forwarding
ROUTE	Add, delete, or display IP routing data
SET	Set an IP address and net mask settings
SETTIME	Display or set the unit time (Un-commissioned Datacryptor Ethernet unit)
SHOWLOG	Basic display of log contents
VERSIONS	Display version numbers of application and bootstrap
EXIT	Exit the process and reboot the unit if a parameter has been changed, or just exit if no changes have been made.

Note: Before setting the Management port's parameters, you may want to read the IP Management tab section for some background knowledge on their values.

7. At the IPCONFIG> prompt, type:

   SET <port> <ip address> <subnet mask>

   where: <port> identifies the port to be set and is one of the following:

   - **NETWORK** (public network port),
   - **CONTROL** (serial control port),
   - **ETHERNET** (Ethernet management port).

   <ipaddr> is IP address of a subnet to be added or deleted.

   <netmask value> is netmask of the subnet.

Examples

`Set Control 2.2.2.2 255.255.0.0`	Sets the Control (serial port) IP Address to 2.2.2.2
`Set network 3.4.5.6 255.255.0.0`	Sets the network port IP Address to 3.4.5.6 255.255.0.0

Note: - No two IP addresses should be the same
- IP addresses of 127.x.x.x are not allowed.
- Net masks of 0.0.0.0 and 255.255.255.255 are not allowed.
- Public and Private port addresses must be valid Class A, B or C addresses. For this reason subnet masks must comprise of consecutive 1s from the left hand side when represented in binary, for example 255.255.1.0 is invalid.

To make the unit request an Ethernet Management Port IP address from a DHCP/BOOTP server on the LAN, set its Ethernet Management Port IP address to 255.0.0.0 and net mask to 255.255.255.255 (this is an exception to the rule mentioned in the note above).

To reset the addresses to factory defaults, use the **DEFAULT** command.

The above section details the steps necessary to connect via the Ethernet management port.

Dial Up Networking

It is also possible to connect and run the Element Manager program via the serial Control port using Dial up Networking.

1. Ensure a serial cable is connected between your PC and the Datacryptor Ethernet unit.
2. Use the Networking wizard for your operating system to generate a Dial up connection; the following parameters should be used for the settings:
   - Set up an advanced connection
   - Connect directly to another computer
   - Guest
   - Connection Name
   - Select the Com port to which you have connected the serial cable
   - All users
   - User Name and Password
3. Select the option for Desktop shortcut.
4. Select **Finish**.

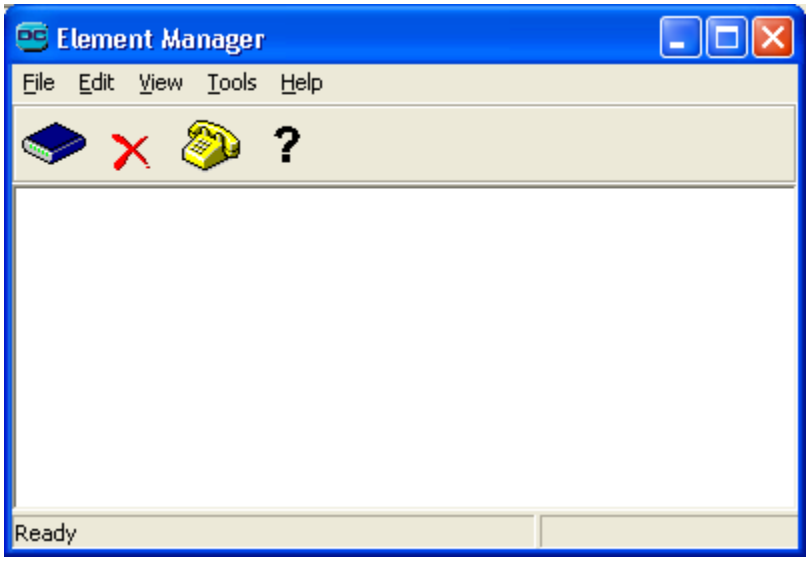
5. Click on the shortcut to launch the connection.
6. Select the **Properties** button.
7. On the *General* tab confirm correct connection.
8. Click **Configure** button and use the menu to set the maximum connection speed of 115200 bps. Set the flow control to none; the Ethernet and SONET do not support flow control.
9. On the Network tab, select TCP/IP and click **Properties** - enter the address 2.2.2.1.
10. Close down the Properties and click **Connect**.
11. A connection with the Datacryptor Ethernet will be made. Ensure the connection is made then disconnect.

Adding a Unit to Element Manager

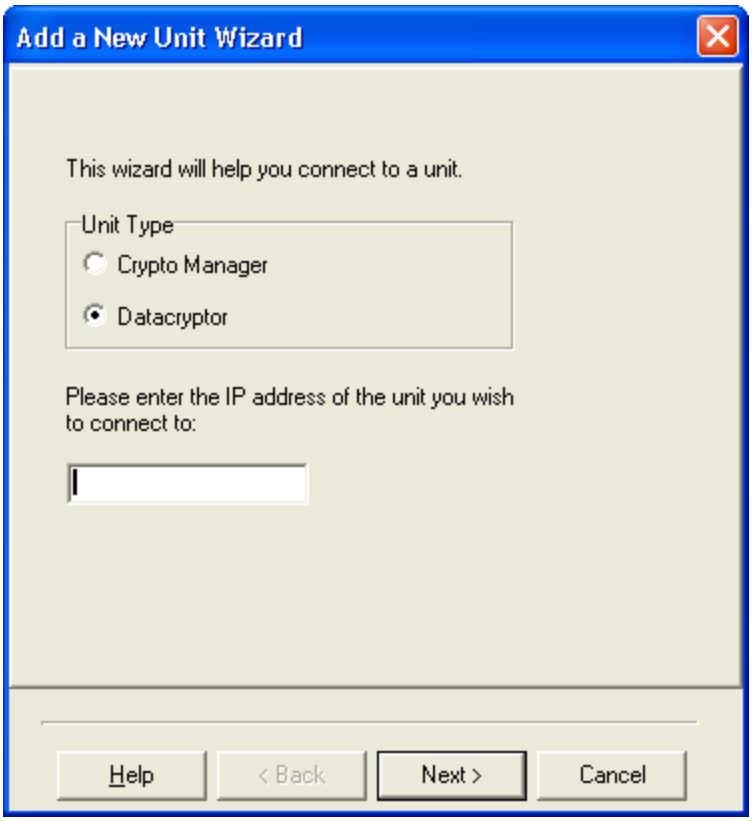
Once the Management or Dial up connection is set up, you can connect to each Datacryptor Ethernet unit by adding an icon in the Element Manager. The Dial Up connection created earlier must be running if a serial connection is to be used.

1. Start the Element Manager, e.g. by double-clicking its icon:

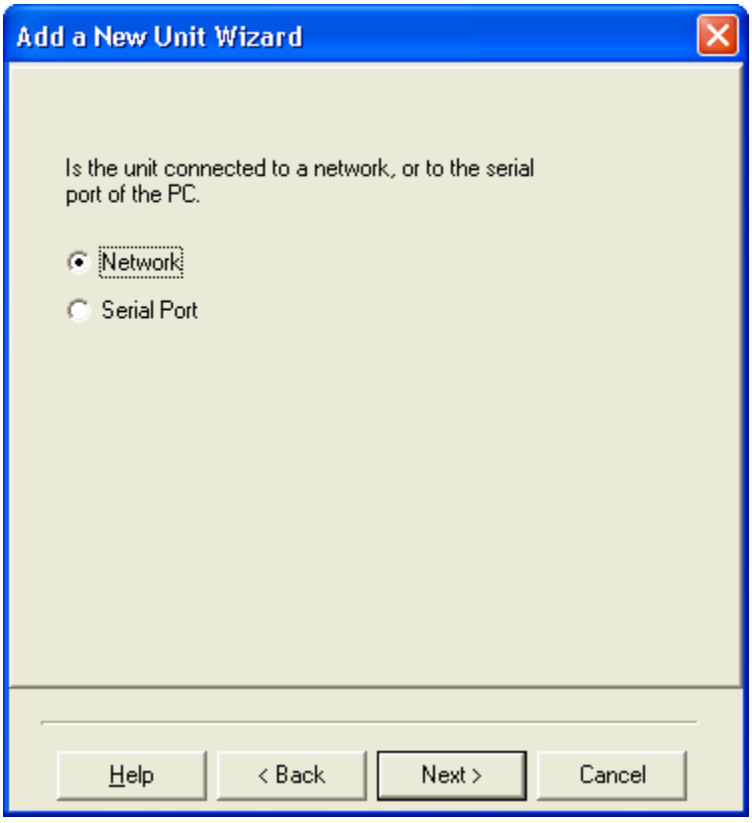
2. The Element Manager Main Window will be displayed:



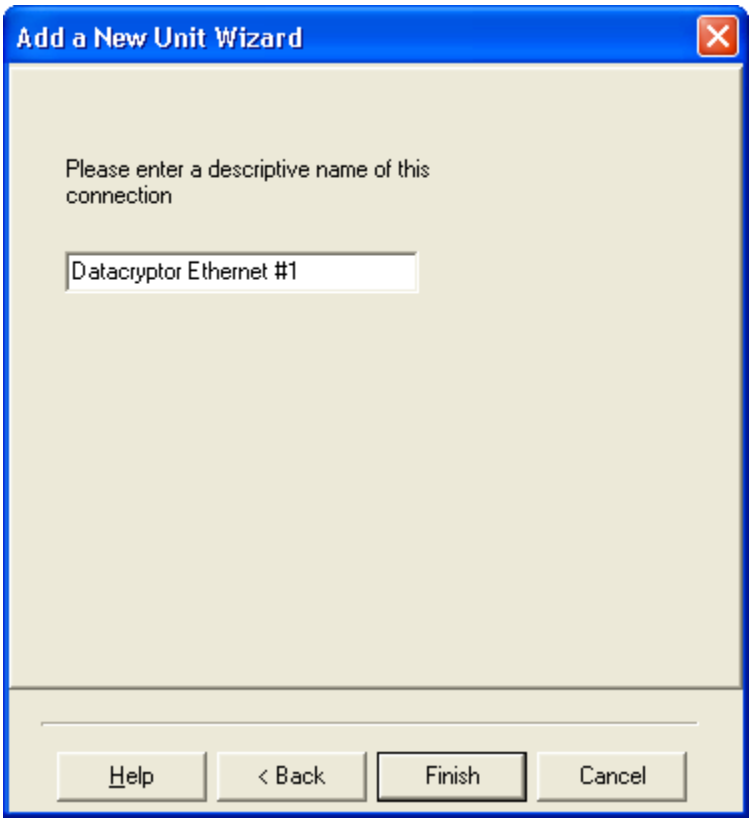
3. Add a new Datacryptor Ethernet unit by clicking on the **New Unit** icon  or selecting the **New Unit** option from the **File** menu. This will launch the **Add a New Unit Wizard**:



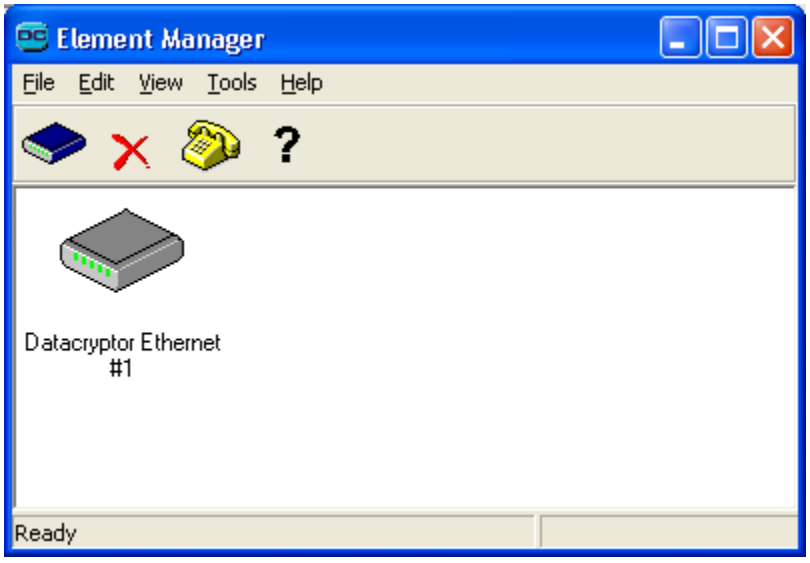
4. Select the unit type as **Datacryptor** and enter the IP address of the Datacryptor Ethernet unit. Press **Enter** or select **Next** to continue.



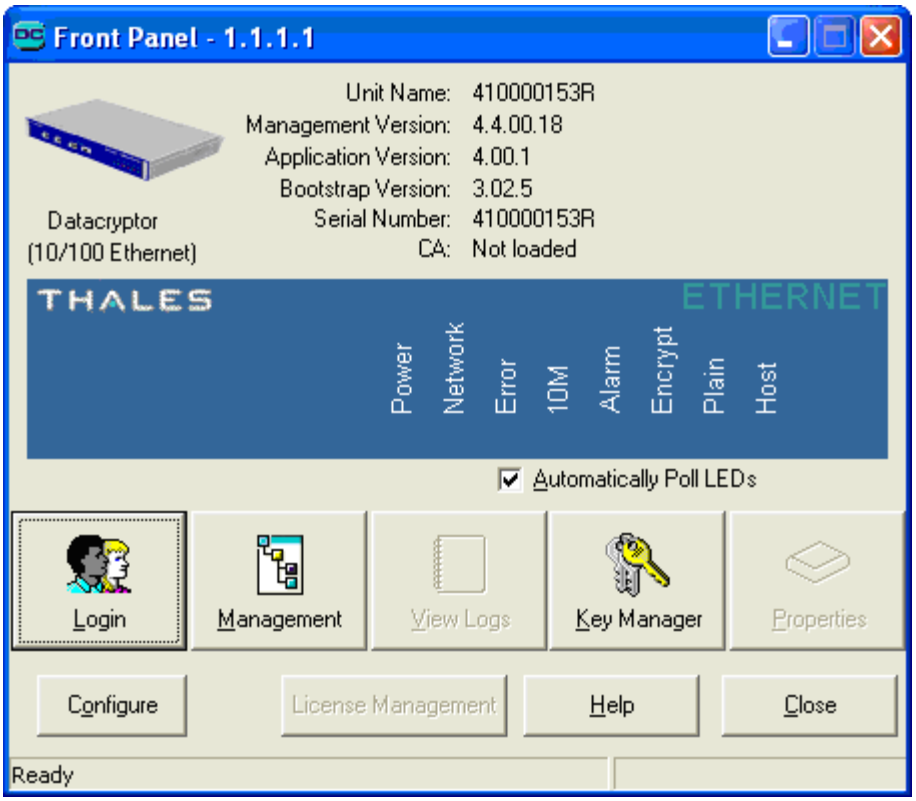
5. Select the connection type for the Datacryptor Ethernet unit; press **Enter** or click on **Next** to continue.



6. The application will attempt to connect to the specified IP address and - if successful - display the unit's Unit Name by way of confirmation, as above. Type a descriptive name for the connection in the edit box (this will be shown in the main window below its icon).
7. Click **Finish** or press **Enter** to finish adding the new connection and Datacryptor icon, which will be displayed as a new icon in the main window like this:



8. Now, double-click on the new Datacryptor icon to connect to it. A splash screen will be displayed whilst connecting to the unit and within a minute this should display the Front Panel Viewer for the unit - an example for the 100 Mb Ethernet Datacryptor is given below. It is possible to abort the connection attempt at the splash screen by pressing its **Cancel** button:



9. You can now check the unit details, at the top of the window, to make sure that the unit is connected correctly, and proceed to configure the unit.

10. You can login to it by using the **Login** button, and **manage** it by using the **View Logs, Properties** and **License Management** buttons. The management facilities are described in Element Manager Reference section below. To configure the unit for your network setup, select the **Properties** button to display the unit's properties, and select the appropriate tabs.

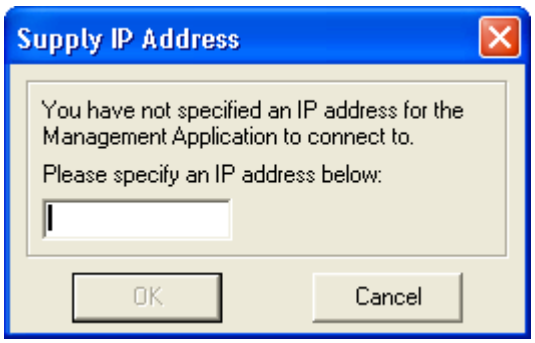
Note: If you are going to add a number of similar Datacryptor Ethernet units, the easiest method is to create a virtual unit and then use this virtual unit to configure them.

Direct Invocation of Front Panel Viewer

It may be advantageous to start the Front Panel Viewer directly from Windows instead of going through the element manager. This may be achieved by:

1. Using Windows Explorer, navigate to the location of the DC2k.exe file, create a shortcut and place on your desktop.

2. Click on the shortcut.
3. The Element Manager Supply IP Address will be displayed.



Enter the IP address of the Datacryptor Ethernet unit and press **Enter** or **OK** to continue. After a few seconds this should display the Front Panel Viewer as shown in Step 8 of the previous section.

Command Line Parameters

The Element Manager's Front Panel Viewer can be invoked from the command line with an IP address as a parameter:

Insert the full path to the exe file, e.g.

```
C:\Program files\Thales e-Security\Element Manager
```

and use:

```
Dc2k.exe 192.168.1.15
```

The parameter is displayed on the title bar at the top of the application's window.

This provides a mechanism for another application (e.g. an SNMP network manager) to invoke the Front Panel Viewer for a specified Datacryptor unit.

If `Dc2k.exe` is invoked without any parameters, it will prompt the user to enter the IP address of the unit to connect to.

To display a short summary of the command line parameters supported, use the command:

```
Dc2k.exe /?
```

7 Element Manager Reference

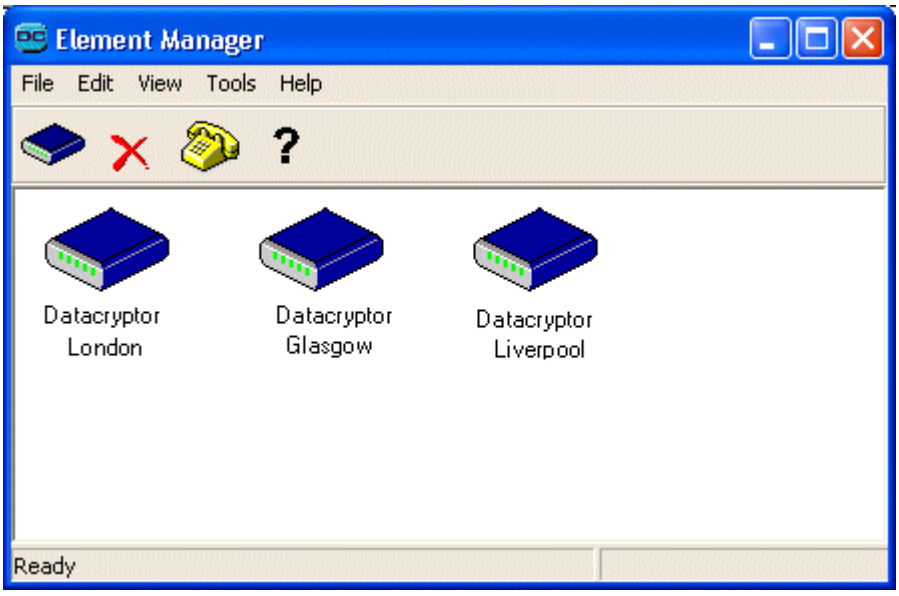
The Element Manager consists of the following components:

- The Main Window
- The Front Panel Viewer
- The Configure dialog
- Key Manager
- The Login dialog
- The Change Password dialog
- The Logs window
- The Properties dialog

Each will now be described in turn.

Remember that you also have access to online help while using the Element Manager via the **F1** (Help) key and the **Help** menu.

Main Window



The main window is displayed when the Element Manager application is launched, providing access to menus, toolbar, and a window containing icons representing each of the Datacryptor units added to the system.

Each of the components of the main window will now be described in more detail.

Main Window Pull-down Menus

The pull-down menus are: File, Edit, View, Tools and Help.

File

The following options are available from the **File** pull-down menu:

Menu Option	Description
New Unit	Add a new Datacryptor unit to the window.
Delete Unit	Delete the selected Datacryptor unit from the window.
Exit	Terminate the application, closing all sessions that may be open.

Edit

The following options are available from the **Edit** pull-down menu:

Menu Option	Description
Undo Delete	Restore the last Datacryptor unit deleted.
Edit Unit	Edit the selected unit's description, IP address or connection method.

View

The following options are available from the **View** pull-down menu:

Menu Option	Description
Toolbar	A toggle controlling the display of the Toolbar and its buttons. Ticked when enabled.
Status bar	A toggle controlling the display of the Status bar, which is used for context-sensitive message and help. Ticked when enabled.
Large icons Small icons List Details	The four different ways that Datacryptor details can be shown, in the main window. The currently selected method has a bullet next to it.
Refresh	Redraw the window, updating all details.

Tools

The following options are available from the **Tools** pull-down menu:

Menu Option	Description
View Audit Log	Display an audit log of all changes made using the Element Manager.
Dial-Up Networking	Launches the operating system's Dial-Up Networking application, to manage dial up connection details or make a connection.
Poll Network Units	Poll all Datacryptor units connected via the network.
Proxy Ping	Ping (test) a specified IP address on a network. Allows the Time To Live (TTL), packet size and Timeout to be selected. This does not apply to Datacryptor Ethernet units and is grayed out.
Options	Displays the **Datacryptor Options** dialog, to control operation of the management application. Options are: **Save changes to Disk** and **Poll all units on startup.**

Help

The following options are available from the **Help** pull-down menu:

Menu Option	Description
Help Topics	The main entry point into the application's on-line Help system.
About…	The application's version information.

Toolbar Icons

The Toolbar displays a number of graphic buttons that provide direct access to key functions:

 - Create New Datacryptor icon (File/New Datacryptor menu option)

 - Delete Selected Datacryptor icon (File/Delete Datacryptor menu option)

 - Dial-Up Networking (Connect/Dial-Up Networking menu option)

 - Help Index (Help/Index menu option)

Visibility of the Toolbar is controlled by the **View** > **Toolbar** menu option.

Datacryptor Icons

Each Datacryptor icon in the main window represents a real or virtual Datacryptor unit:

- **Grey** means a Datacryptor unit that is not connected
- **Blue** means a Datacryptor unit that is connected
- **White** means a virtual Datacryptor, used as a template to add similar units

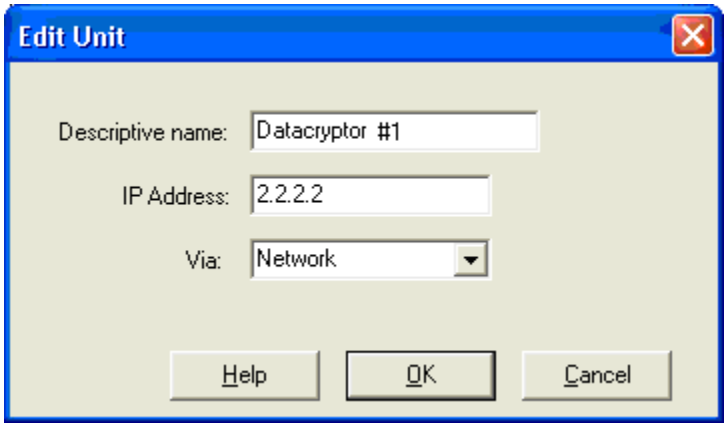
To connect to a Datacryptor unit:

1. Double-click its icon.
2. Once the connection has been made, the Front Panel Viewer will be displayed showing information read from the unit. This dialog provides access to all the Datacryptor unit management facilities described throughout this guide.
3. To disconnect from the Datacryptor unit, click the **Close** button in its Front Panel Viewer.

To delete a Datacryptor unit from the system, select its icon and press **Del**, or select the File/Delete Unit menu option or click on the **Delete** button on the Toolbar. This displays a confirmation dialog first.

To change an icon's description, IP address, or connection method:

1. Select the icon and select the Edit/Edit Unit menu option or press **F2**. This displays the Edit Unit dialog:



2. Edit the name, IP address or connection method and click **OK** or press **Enter**.

Note: The type of unit cannot be changed, if you want to change the unit type it will have to be deleted and re-added.

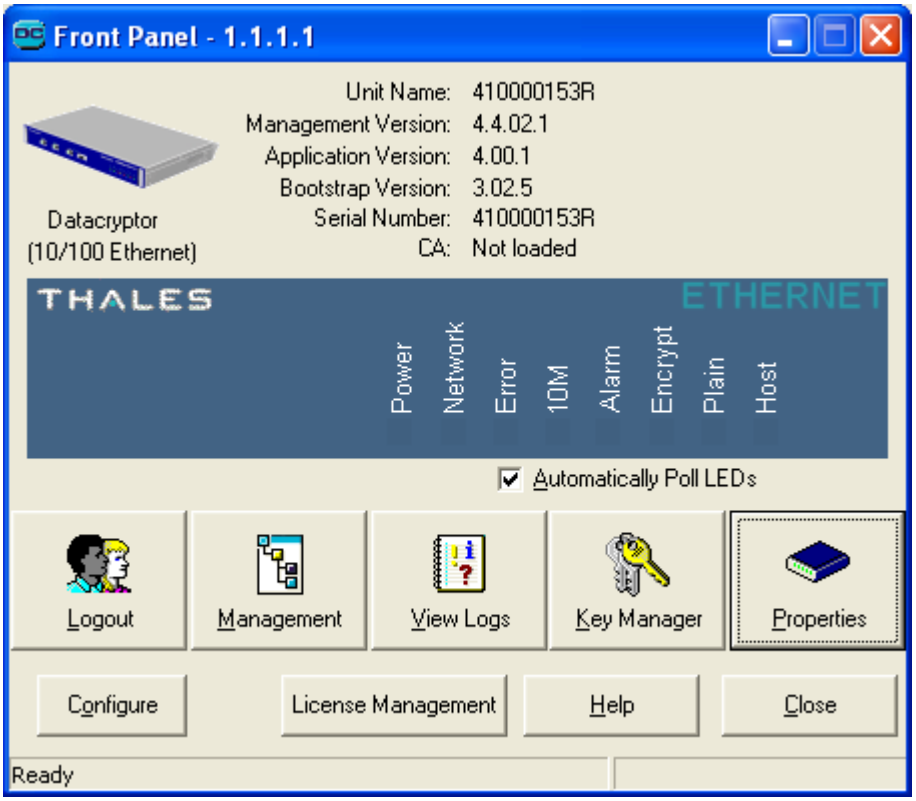
There is also a **pop-up menu** for manipulating Datacryptor icons, displayed by "right-clicking" on the icon. The options are:

- **Open** - opens a session with that unit (like double-clicking on it)
- **Edit** - edit the unit's descriptive name or IP address (like the Edit/Edit Unit menu option)
- **Delete** - deletes the icon from the system (like the File/Delete Unit menu option)

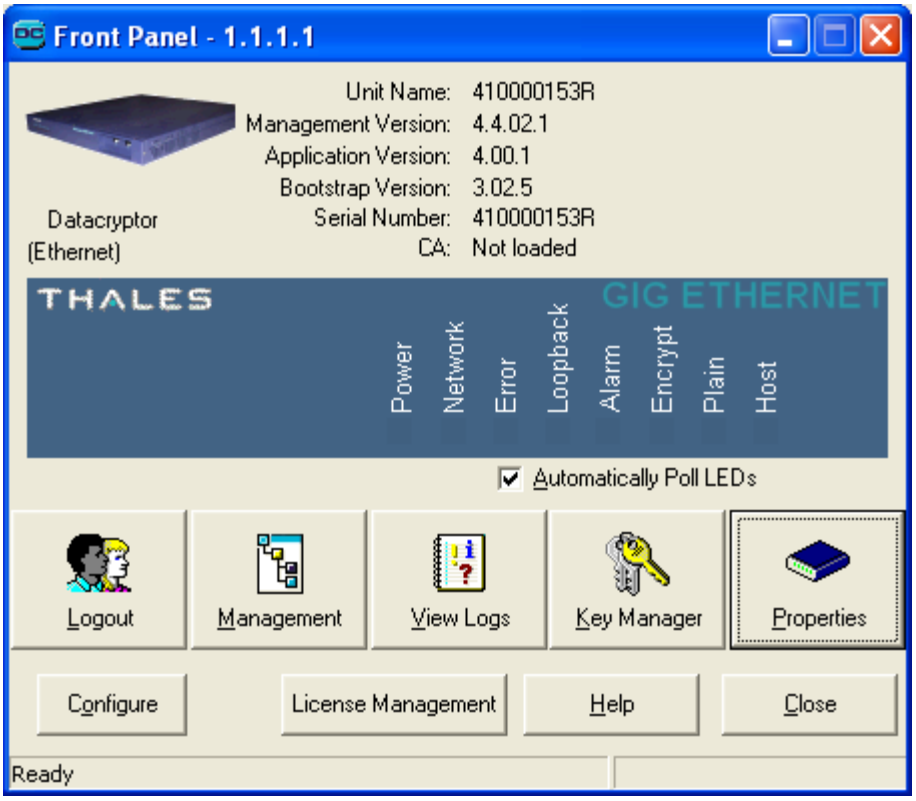
Front Panel Viewer

A splash screen is displayed when you attempt to connect to a Datacryptor Ethernet unit. This process should normally complete within a few seconds but might take up to one minute. You can abort the connection attempt from the splash screen by pressing its **Cancel** button. Note that the text on the splash screen may change from "Identifying unit" to "Fetching unit information" during the connection process.

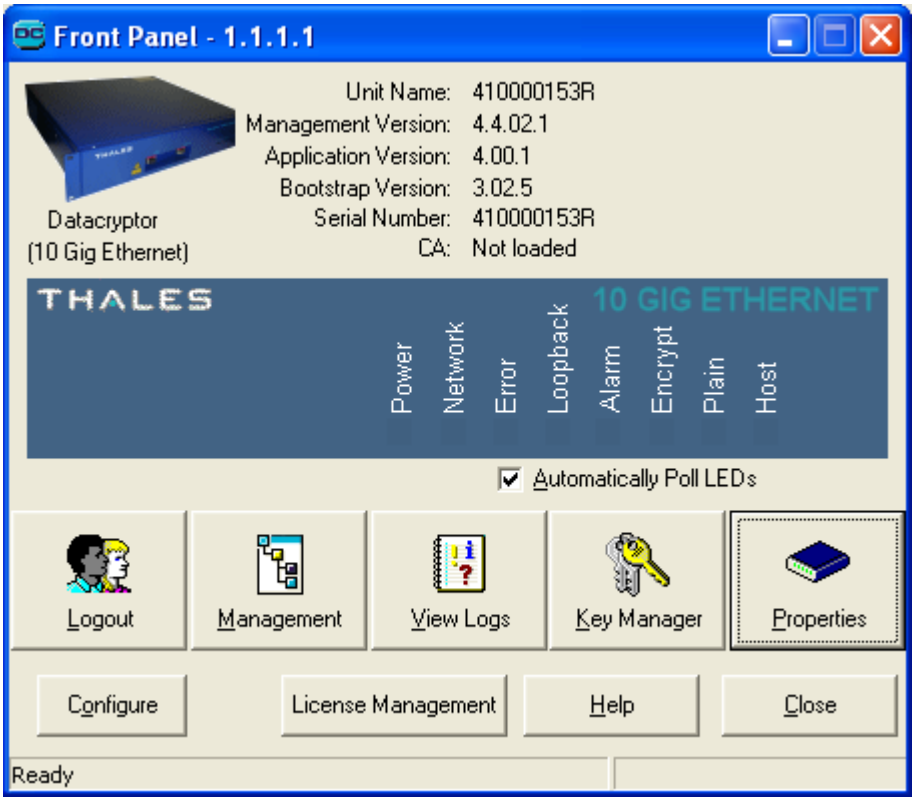
The splash screen closes and the Front Panel Viewer is displayed when you successfully connect to a Datacryptor Ethernet unit, to display its status and provide access to the management facilities. There are some differences between the Front Panel Viewer for the 100 Mb Ethernet, the 1 Gigabit and the 10 Gigabit Ethernet Datacryptors. The three variations are shown below:



100 Mb Ethernet Front Panel Viewer



1 Gig Ethernet Front Panel Viewer



10 Gig Ethernet Front Panel Viewer

The management facilities are provided by the **View Logs** and **Properties** buttons. If **View Logs** or the **Properties** buttons are grayed out, they are inaccessible because you haven't logged in yet - use the **Login** button to do so. Once you have logged in, the **Login** button changes to **Logout**.

The Front Panel Viewer displays the following information:

- The IP address of the unit (management port) in the title bar
- The model description
- **Unit Name**: read from the unit
- **Management Version:** read from the application
- **Application Version**: read from the unit
- **Bootstrap Version**: Firmware number
- **Serial Number:** Unit unique serial number
- In the blue rectangle, a diagram of the unit's front panel shows the state of the LEDs, which can be examined to check the state of the unit (see the Front Panel LEDs section). In addition, if you move the mouse pointer to an LED, after a few seconds a description of its current state will be displayed next to it in a yellow box.
- Beneath the blue rectangle is the **Automatically Poll LEDs** checkbox. Tick this to update the display of the LED status every 10 seconds, or clear it to stop the polling and reduce the network traffic.

- Beneath the front panel diagram are five large buttons that provide direct access to management facilities (see the Front Panel Viewer buttons section below).

Note: Pressing F5 while using the Front Panel Viewer will cause a refresh of all displayed settings from the unit.

User Key Material

Adminv2.usr	User key material (containing public and secret keys of user) protected by a default password of: PASSWORD
Adminv3.usr	Alternative user key material (containing public and secret keys of user) protected by a default password of: 11aaBB!!PASS

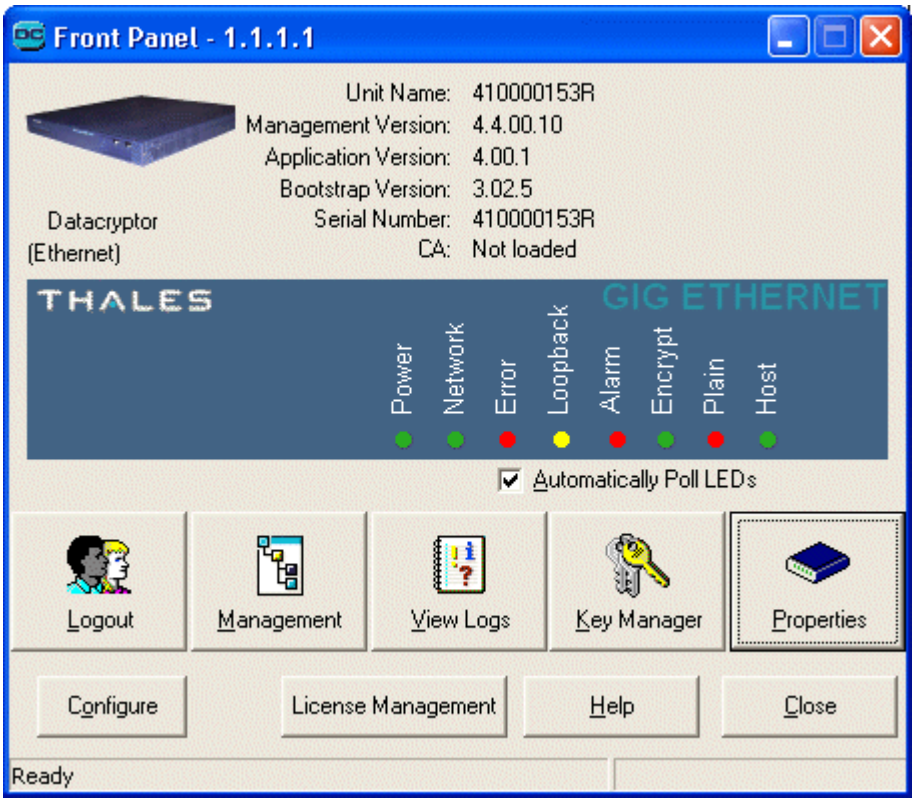
The Front Panel LEDs

The Front Panel LEDs indicate the state of the unit.

Indicator Light	State	Indication
Power (green)	On	Unit is powered on
	Off	No power
Network (green)	On	Normal operation
	Fast Flash	Link Down
	Slow Flash	Not used
	Off	Loss of Signal, Loss of Synchronization
Error (red)	On	Errors have occurred
	Fast Flash	New errors in log
	Off	No errors
10M (100 Mb Ethernet unit only)	Off	100 Mbps operation
	On	10 Mbps operation
Loopback (yellow) (1 Gig and 10 Gig Ethernet units only)	Off	Normal operation - no loopback enabled
	Slow flash	Host loopback enabled
	Fast Flash	Network loopback enabled
	On	Host and Network loopback enabled
Alarm (red)	On	Unit is alarmed - Hardware fault
	Fast flash	Unit is not commissioned
	Off	No Alarm
Encrypt (green)	On	Unit is in Encrypt mode
	Slow flash	Standby
	Off	Unit is not in Encrypt mode
Plain (red)	Fast Flash	Unit is in Plain mode
	Off	Passthrough mode not selected
Host (green)	On	Normal operation

	Fast Flash	Link Down
	Slow Flash	Not used
	Off	Loss of Signal, Loss of Synchronization

The Front Panel Viewer buttons



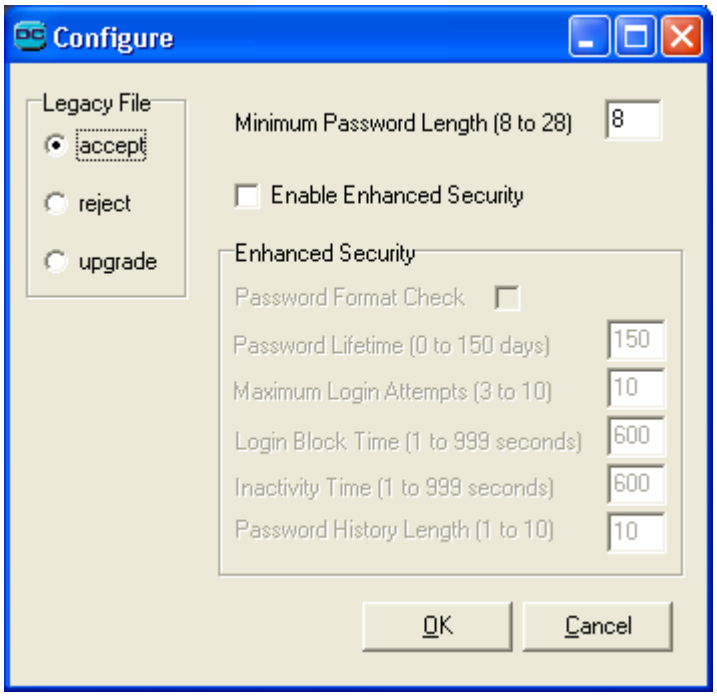
The buttons in the Front Panel Viewer are the same for all models of Ethernet Datacryptor; they provide access to the management facilities, as follows:

- **Login**: This button is only enabled if you have not logged in yet. Click on it to display the Login dialog, supply your password and you will gain access to the full set of management facilities. Once you have logged in, the button changes to Logout.
- **Management**: Click on this button to display the Element Manager main window.
- **View Logs**: This button displays the Logs Window, for you to produce, examine and manage error and other logs from the selected unit.
- **Key Manager**: Displays the Key Manager dialog to manage the units CAs and Certificates.
- **Properties**: This button displays the Properties dialog box for the unit, which allows you to examine and change the unit's properties (configuration).
- **Configure**: This button displays a dialog, which allows you to set properties that control how the Front Panel Viewer manages passwords and session timeout.
- **License Management**: This button is not used in the Datacryptor Ethernet.

- **Help**: The Help button launches the help application displaying the help file for the dialog.
- **Close**: The Close button closes the Front Panel Viewer.

Configure Dialog

This dialog is displayed when you select the **Configure** button from the Front Panel Viewer. It provides configuration of the rules that the Front Panel Viewer will enforce in support of the security policy.



Legacy File

To support the enforcement of security policy the format of the User Key Material file has been extended. The adminv3.usr file is in this extended format.

Any existing files and those generated by the Certificate Manager have not been extended. The adminv2.usr file is in this original format.

The FPV may be configured to reject, accept or upgrade User Key Material files that do not contain the extended fields.

- **accept:** Legacy files will be accepted by the Front Panel Viewer even if enhanced security is turned on. The enhanced checks will not be made when a legacy file is used.
- **reject:** Legacy files will be rejected by the Front Panel Viewer even if enhanced security is turned off. The user will be warned that the file will not be accepted.
- **upgrade:** Legacy files will be automatically upgraded to the extended format when a user attempts to use one. The user will be required to provide the correct password before the file will be upgraded.

Extended files, including those that have been automatically upgraded, should not be used in previous versions of the Front Panel Viewer as that could make them unusable in this current version.

Minimum Password Length

The Front Panel Viewer will require that any new password entered is at least this length. It will also require existing passwords that are shorter than this to be changed before allowing the user to login to gain access to the unit management facilities.

Enable Enhanced Security

Select this box to enable the enhanced security policy enforcing features. If this check box is cleared the Front Panel Viewer will not enforce any of the rules.

Note, however, that the Front Panel Viewer will always keep a record of previous passwords if the user file is in the extended format.

Password Format Check

The basic requirements for passwords are that they must be between 8 to 28 case-sensitive alphanumeric characters. Although certain special characters (see below) are valid for use in passwords, they may cause problems with third party scripting tools. Note also that ampersands, question marks, periods, and commas are not allowed.

Selecting this box will enable password format checks, in addition to the basic password requirements. Those checks require the password to include:

- At least two upper case alpha characters (A-Z).
- At least two lower case alpha characters (a-z).
- At least two numeric characters (0-9).
- At least two special characters from this list:
  ! @ # $ % ^ * ( ) _ + = - [ ] { } \ | ; : < >

Password Lifetime

Enter the required maximum lifetime of a password, in days. The Front Panel Viewer will require the user, when logging into a unit, to change the password if it has not been changed within this many days. A value of zero indicates that the password will not expire.

Maximum Login Attempts

The Front Panel Viewer can block a user from logging into a unit if incorrect passwords are entered. Set this field to the number of wrong attempts that are allowed before the user is blocked.

Once a user has entered the correct password the count of failed attempts is reset.

Login Block Time

As explained in the previous paragraph, the Front Panel Viewer can block a user from logging into a unit if incorrect passwords are entered. Set this field to the time, in seconds, that the user should be blocked for.

The user will be blocked from further attempts for this time. Once the block time has expired the user will again be allowed to attempt to log in.

Inactivity Time

The Front Panel Viewer can automatically log off a user if it has seen no mouse or keyboard activity for a time. Set this field to the maximum inactivity time, in seconds.

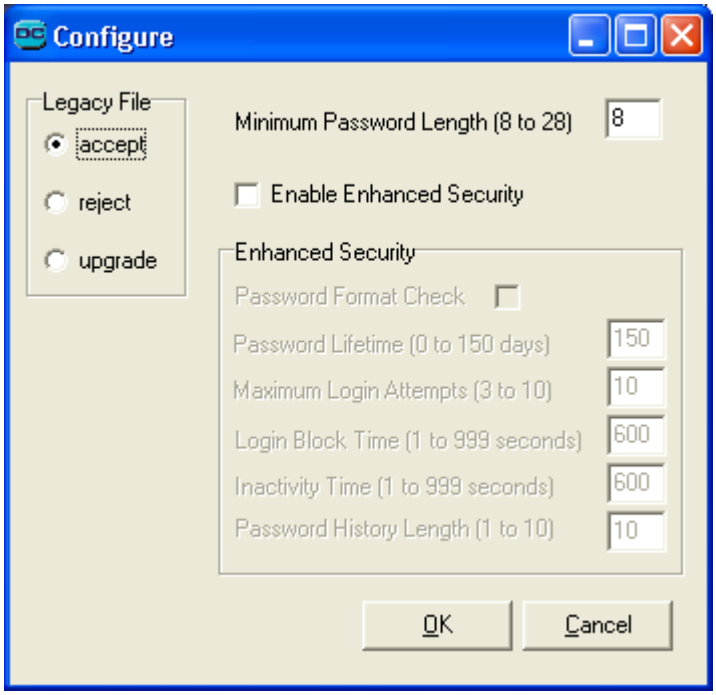
Password History Length

The Front Panel Viewer keeps a record of the last nine passwords for each User Key Material File and will, when changing a password, reject the new password if it has been used before. Set this field to indicate the number of previous passwords that will be included in the check.

Setting this to one indicates that the new password will only be checked against the existing password and not against any of the previous passwords. Setting this to ten indicates that the new password will be checked against the existing password and all nine previous passwords.

Defaults

When the Front Panel Viewer is first installed these fields will default to the values shown here:



These settings permit the Front Panel Viewer to operate identically to the previous version when using legacy files. If the enhanced security enforcement features are not required then legacy User Key Material files, including the universal adminv2.usr file, may be used without upgrade.

Securing the Settings

These settings are stored in a file in the `SecureData` subdirectory. To protect these settings an administrator should configure the Front Panel Viewer as required and then restrict access to the `SecureData` directory and its contents to read-only for users.

When the directory is set to read-only the Front Panel Viewer will disable the Configure button.

Key Manager

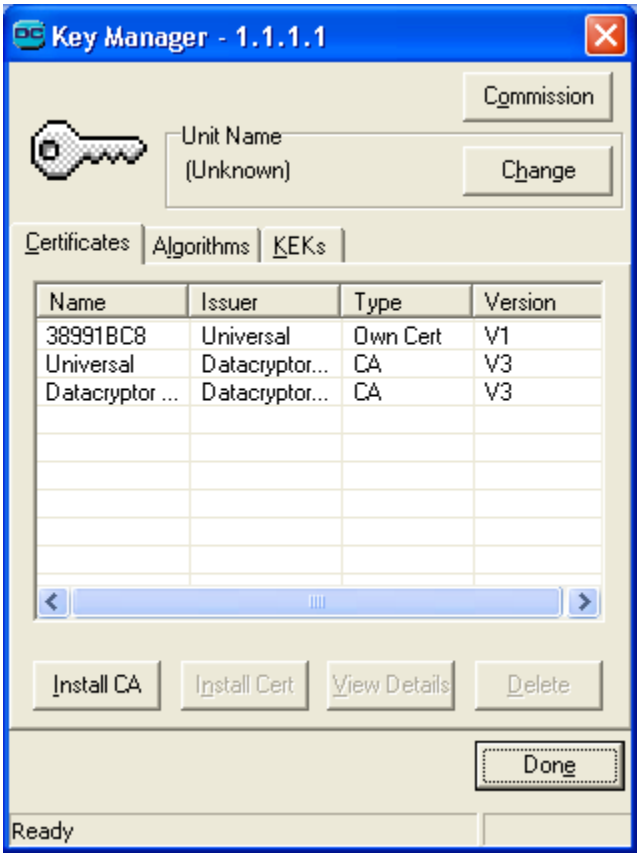
As previously stated when the Datacryptor Ethernet unit is supplied from the Manufacturer, Thales e-Security provides the CA that is loaded. When first commissioned the unit may require testing and the Universal CA provided on the Datacryptor Element Manager CD-ROM can be used. This CA is very insecure, as all owners of Datacryptor units will have a copy, which means that they all have the Admin2.usr file that can be used to log into any unit that has the Universal CA loaded.

It is essential for security to change this Universal CA to a Custom CA as soon as possible. If the unit owner has a copy of 'Certificate Manager' a trusted member of staff can create the Custom CA, if not an external SA can provide one.

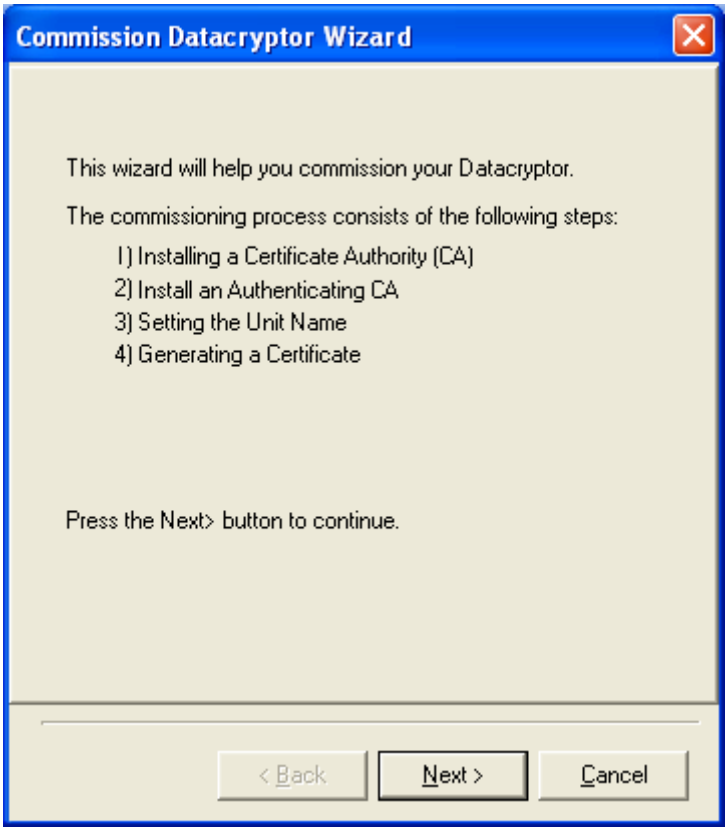
The process of installing the required elements is done via **Commission** button on the *Key Manager* dialog. The Key Manager dialog is opened via the **Key Manager** button on the *Front Panel Viewer*.

To commission a unit with the Commission button

1. Click the **Key Manager** button on the *Front Panel Viewer* – the Key Manager dialog opens:



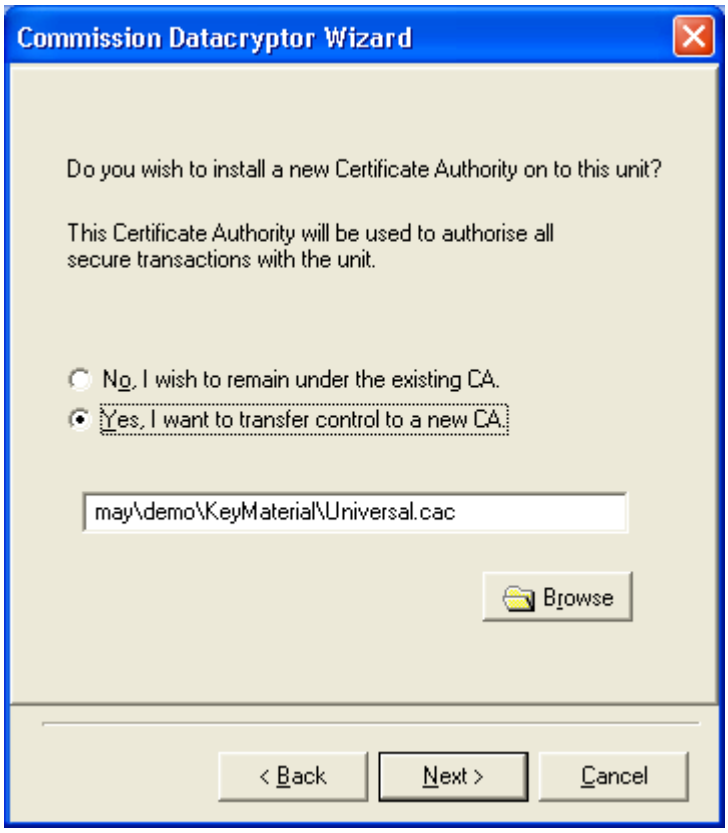
2. Click the **Commission** button at the top of the dialog. This will start the Commissioning Wizard, which begins by displaying an overview of the process as shown below:



The first item in the list will be *Installing a Certificate Authority (CA)* as shown above.

3. Click the **Next** button to proceed to step 1 below. The first page of the wizard asks if a new CA is to be installed in the unit.

Step 1: Installing a new Certificate Authority (CA)



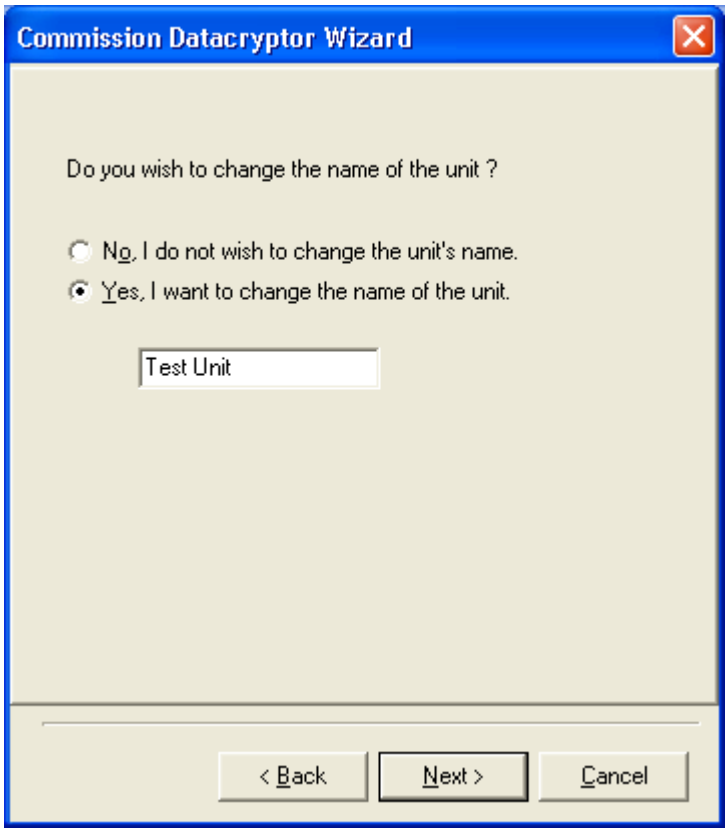
Units are normally delivered under the control of the manufacturer CA (DC2K Manufacturer), with the Universal CA available on disk; this dialog allows you to transfer control to a different custom CA:

1. To stay under the control of the manufacturer CA, select the **No** option and click the **Next** button or press **Enter**. This will take you to step 3.
2. To transfer from the manufacturer CA to a new CA, select the **Yes** option. Insert the diskette containing the new CA's .CAC file and enter the path to the .CAC file (or use the Browse button to find it). Click the **Next** button to proceed to step 2.

Step 2: Installing the authenticating CA:

Insert the diskette containing the authenticating CA's .CA file and enter the path to the .CA file (or use the Browse button to find it). Click the **Next** button to proceed to step 3.

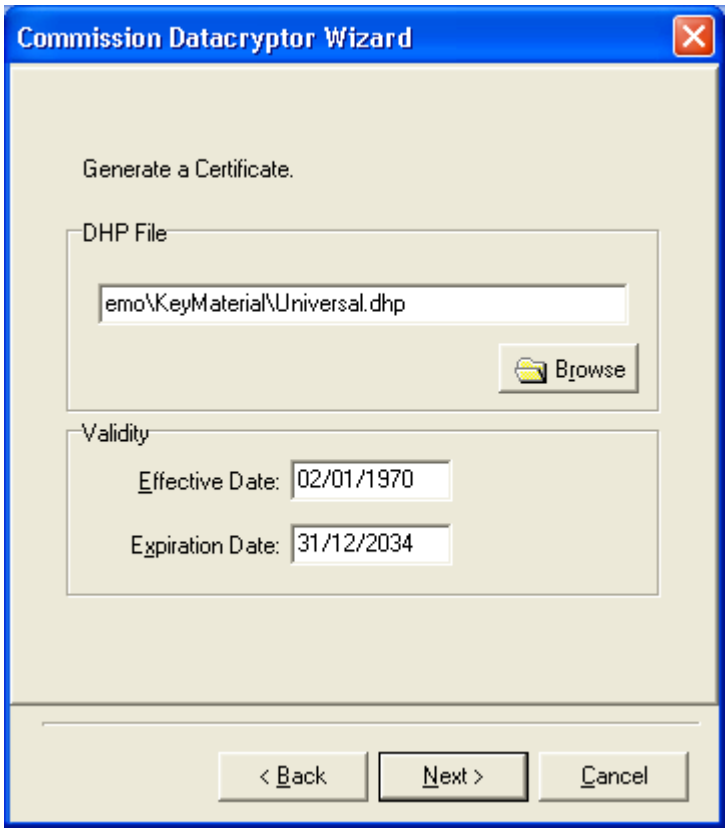
Step 3: Setting the unit name:



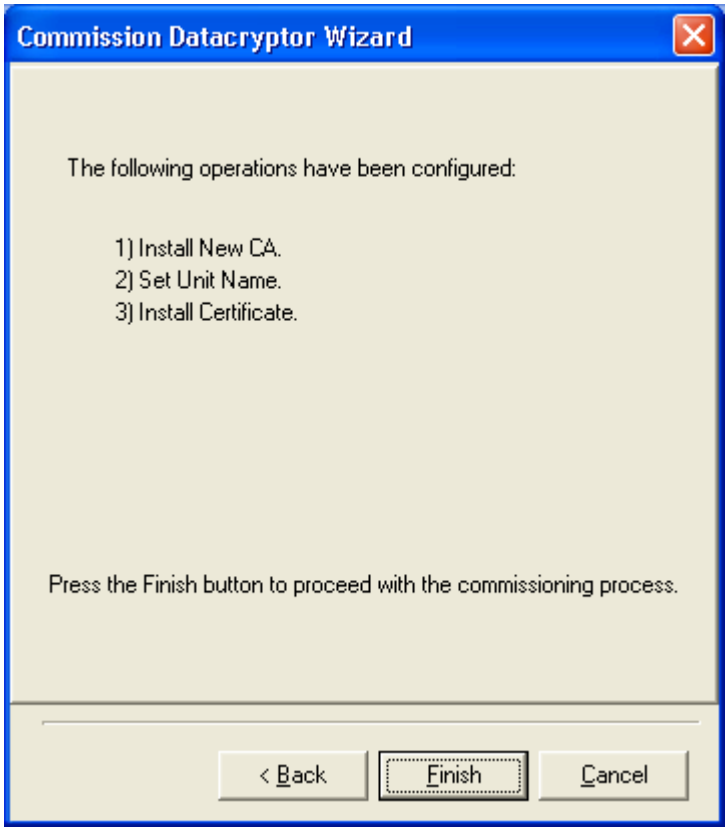
Each Datacryptor Ethernet unit within a User Group must have a different name. You can either leave the unit name as delivered (since units are manufactured with unique names – the same as the serial number) or change it now, according to your security procedures. The edit box displays the unit's current unit name.

1. To keep the displayed unit name, click **Next**.
2. Alternatively, to change the unit's name, click on the **Yes** radio button and edit the name. Then click **Next** to continue.

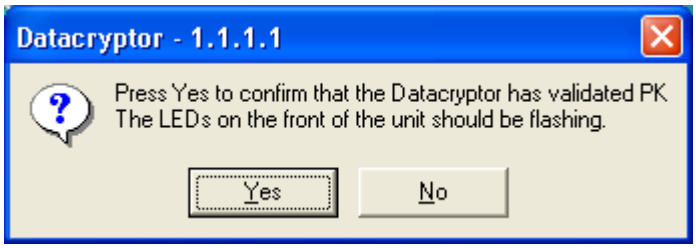
Step 4: Generating a Certificate:



1. Enter the path to the .DHP File (Diffie-Hellman Parameters), or use the **Browse** button to select it.
2. Specify the dates between which the Certificate is valid in the Effective Date (start) and Expiration Date (finish) fields. The Start Time is effectively 00:00 and the End Time is 23:59 (unless the issuing CA is different) on the days selected. The default end date is the last day of the issuing CA
3. Click **Next** to continue and a dialog will list the options you have chosen:



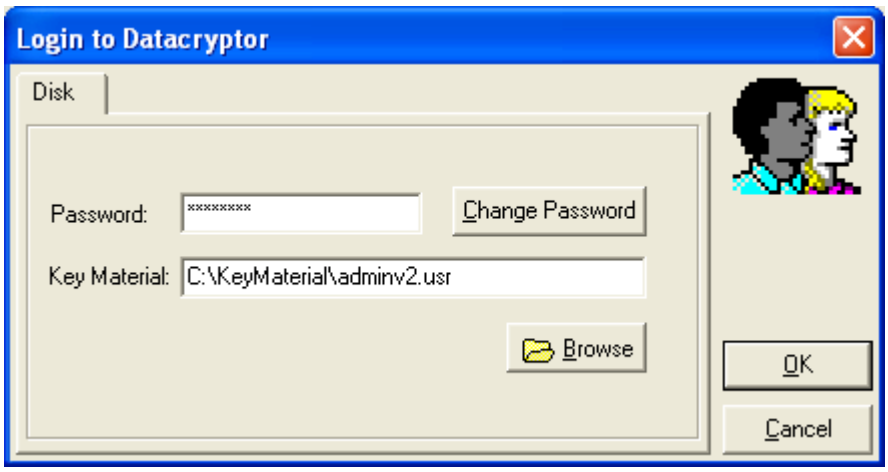
1. Click **Finish** to begin the commissioning process, which will take a few seconds.



2. When commissioning has completed, confirm that the Datacryptor unit's LEDs are flashing (which indicates that the unit has been commissioned successfully). Check the unit's LEDs (or get someone else to do so, if the unit is remote) and click **Yes** if they are flashing.
3. The new CA and certificate can be seen in the Certificates tab of the Key Manager.
4. Once a unit has been commissioned, with the correct CA and Certificate it can be used for the transfer of secure information.

Login Dialog

This dialog is displayed when you select the **Login** button from the Front Panel Viewer, to login to gain access to the unit management facilities.



Enter the password into the login dialog and either click the **OK** button or press **Enter**.

You can also use the **Change Password** button to change your password - providing you know the original password.

Change Password Dialog

This dialog is displayed when you select the **Change Password** button from the Login dialog.

Type the current password in the **Old Password** text box, and enter the new password in the **New Password** and **Re-type New Password** text boxes.

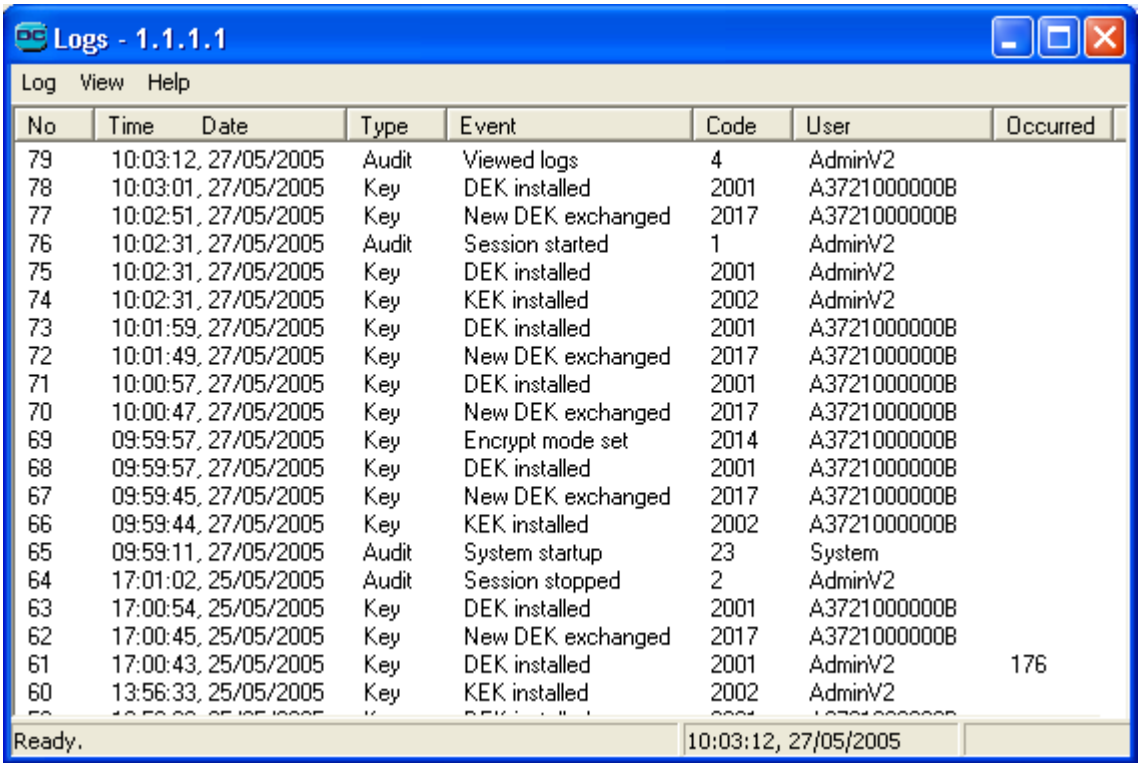
The basic password requirement is that it must be 8 to 28 case-sensitive alphanumeric characters. However, to determine the full requirements that must be met when choosing a password you should refer to the *Password Format Check* section in Configure Dialog.

CAUTION: If the password is lost all Administrator functionality is lost, including the ability to assign a new password. The only means of resetting the password is to the restore the factory settings on the device (please call Customer Service for support). This operation overwrites all previously saved configurations, policies, and keys with factory defaults.

Logs Window

The Datacryptor Ethernet monitors network operations and records information in an audit log about network events or operations specific to a device. The audit log reconstructs an exact sequence of network events or device operations. The audit log configuration determines the types of events that it records.

The Logs Window, which is displayed by clicking on the **View Logs** button in the Front Panel View, allows you to view, search, save or clear the log recorded by the selected unit.



There is only one log, but it contains data of four different types:

- **Audit**: A report of all management operations performed on this unit (using the **Element Manager**).
- **Error:** A report of any faults that have been discovered with unit hardware and keyspace.
- **Key**: A report of all key update and erasure attempts.

- **Trace:** A report of internal software conditions detected by the unit, these are not hardware errors but may help support personnel understand unusual operational conditions. They appear on the display as 'Internal Error' but, when saved to disk as a text file, the text is expanded. When seen, these should be reported to the Support department at Thales e-Security for investigation.

Note: New errors will cause the Error LED to flash. Once they have been read, the Error LED will change to ON and stay on until they have been cleared out of the log.

A list of all the log and SNMP trap numbers with descriptions is provided as an appendix to this guide.

The **Logs** window provides facilities through three pull-down menus.

The **Log** menu provides:

- **Clear Entries** - clear all entries from the currently displayed log(s) - typically after saving them first.
- **Save As** - save the currently displayed log(s) in a named file. You can then keep the file as a backup, print it, or process as appropriate.
- **Close** - close the Logs Window and return to the Front Panel Viewer.

The **View** menu provides:

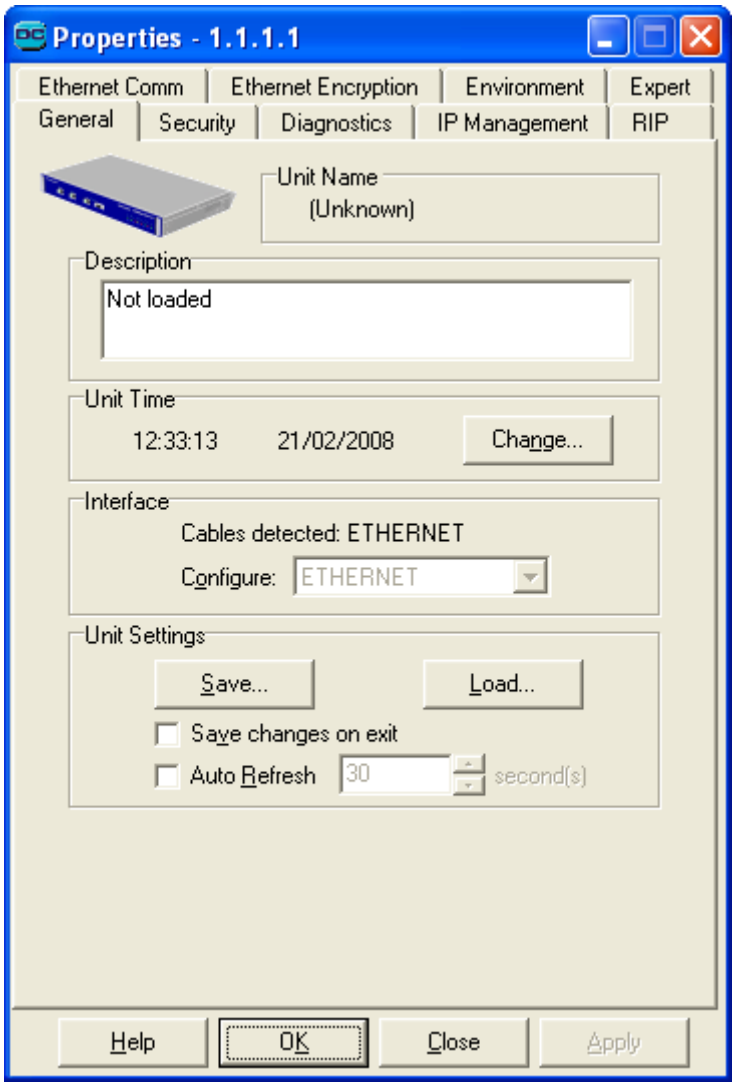
- **Audit**- If this option is ticked the all the Audit entries in the log are shown.
- **Error**- If this option is ticked then all the Error entries in the log are shown.
- **Trace**- If this option is ticked then all the Trace entries in the log are shown.
- **Key Update**- If this is ticked then all the Key Update entries are shown.
- **Newest First**, **Oldest First** - select the order in which entries are displayed by clicking on it. The selected order is indicated.
- **Find** - search through the displayed logs for specified text.
- **Refresh** - update the display by reading the logs from the unit again.
- **Stop Reading** (F6) – halts the process of reading entries from the audit log.

The function key F5 (Refresh) can also be used for the logs window.

The **Help** menu provides access to on-line help

Properties Dialog

The Properties dialog is displayed when you select the **Properties** button in the Front Panel Viewer. The image shown on the dialog will reflect the model of Ethernet Datacryptor that you are using.



You use the dialog to examine and change the properties of the selected unit. These properties are organized into a number of separate tabs. To display a different tab, click on its name or use **Ctrl+Tab** (to display the next tab) or **Ctrl+Shift+Tab** (to display the previous tab).

If you make changes on a tab, they will be written to the unit when you click the **Apply** button, or click the **OK** button to apply the changes and close the dialog.

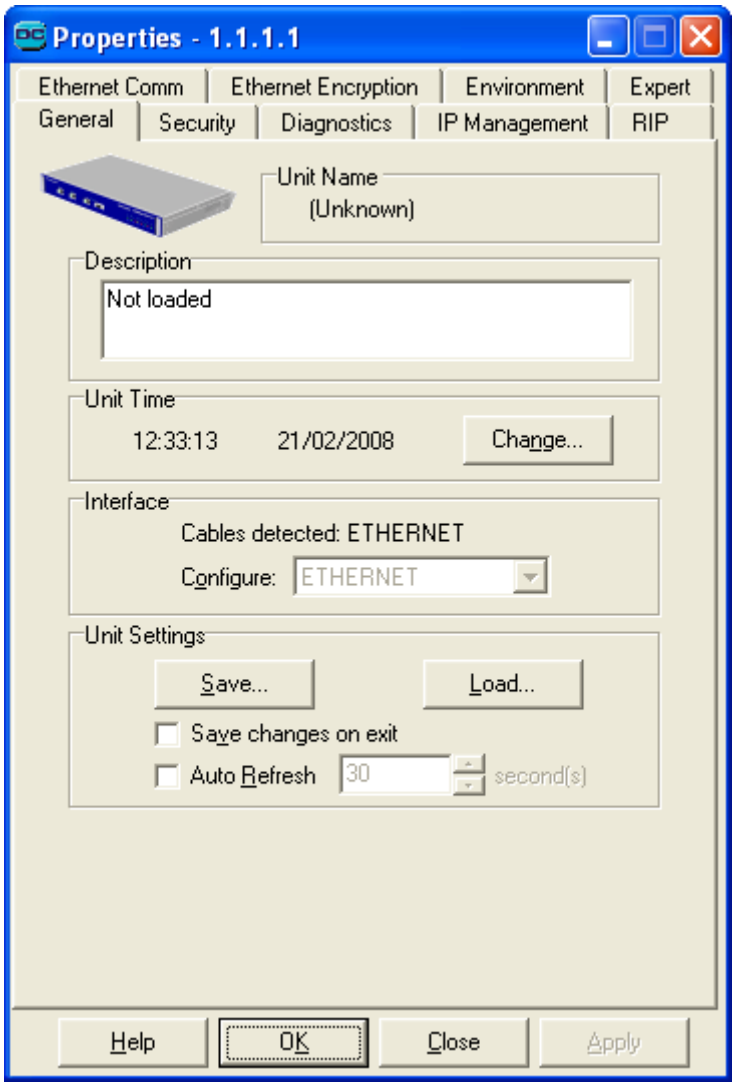
You can also store or retrieve the properties by using the controls in the **Unit Settings** box on the **General** tab - this provides an easy way to backup and restore settings, among other applications.

Note: Press **F5** to refresh the displayed properties or tick auto-refresh on the General tab to refresh automatically.

Each of the tabs will now be described in turn.

The General Tab

The properties on the **General** tab control the general behavior of the unit. The image shown on the General tab will reflect the model of Ethernet Datacryptor that you are using.



Unit Name: read from the unit.

Description: read from the unit.

Change: click this button to set the unit's clock/calendar. (The clock is used to track the time that Keys are created and to track certificate expirations.) The unit operates internally on UTC time and the Element Manager attempts to correct, when setting and when displaying, for the users time zone.

Note: If you set the unit's clock backwards to a date and time in the past, reboot it to avoid filling the log files with error messages about the time setting.

Cable detected: the types of cable connected to the unit.

Save: stores the current properties in a named file, which can then be loaded using the **Load** button (for example, to restore the settings after a unit has been reset to factory defaults).

Load: loads saved properties from a named file. You can then examine, edit or save them, or apply them to the current unit by clicking the **Apply** button.

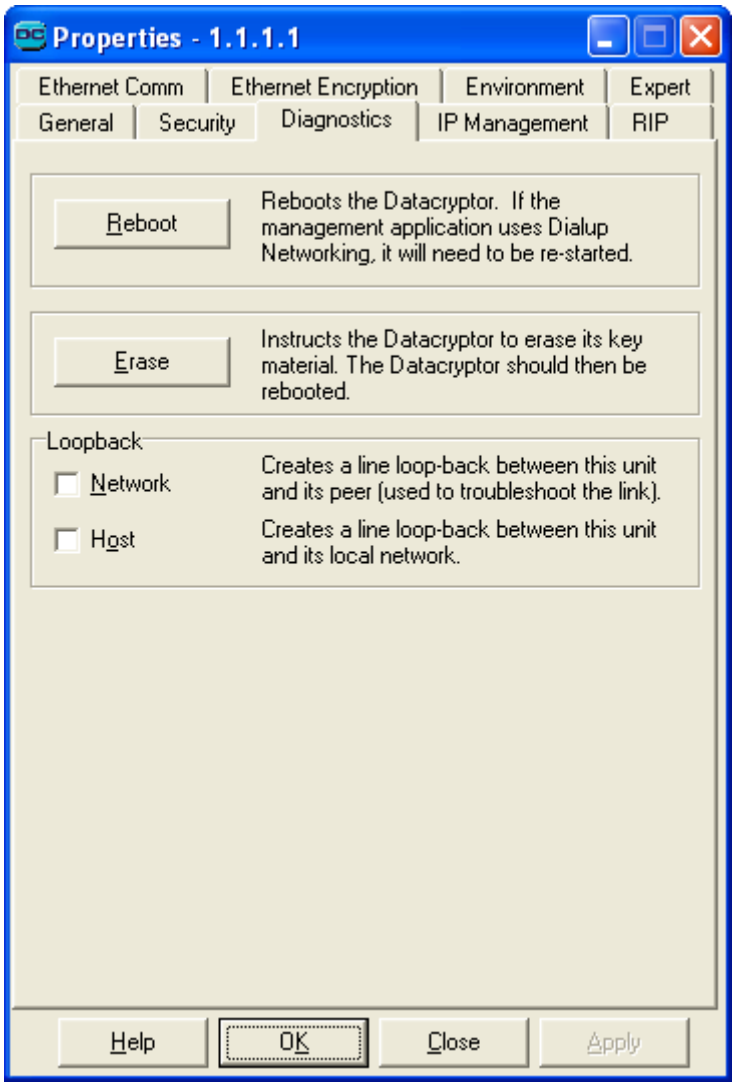
Save changes on exit: tick this box to save the current properties to a named file when you exit the program.

Auto Refresh: tick this box to re-load the current setting from the unit every *n* seconds, where *n* is set by the adjacent control. **Warning:** This may cause large amounts of data to be transferred from the unit under management and may degrade system performance.

The **Save** and **Load** buttons provide a convenient way to set up a number of similar units, as well as a convenient way to keep backups of unit settings.

The Diagnostics Tab

The **Diagnostics** tab will provide a range of diagnostic aids.



Currently, it provides two diagnostic facilities:

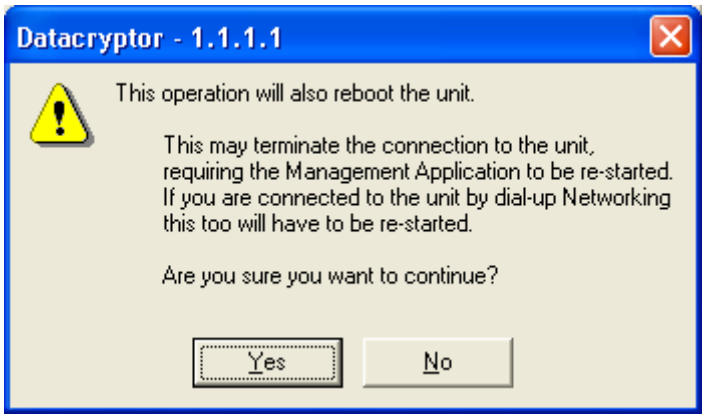
Reboot: click this button to reboot the unit as if it had been turned off and on again. (This operation takes several minutes)

Rebooting halts all operations on the device and starts the boot process in the same manner as when the power is cycled. Save any configuration changes prior to rebooting the unit. Unsaved changes will be lost.

	**CAUTION:** Rebooting the device interrupts the data traffic on the **Host** and **Network** ports.

Erase: click this button to erase the unit's Key material. Basic unit Configuration will not be lost, i.e. the unit can still be managed remotely once the unit has re-booted.

The following confirmation dialog will be shown. Click on **Yes** to continue. The unit will delete the key material and reboot, this will close any management sessions including dial up networking connections



Loopback

The loopback facility is a diagnostics test capability that allows either, or both, of the ports to loop back any signals that are applied.

For example, if the Host port is placed in loopback, then the local signals sent to the Datacryptor for encryption and onward transmission, are in fact simply returned back to the Host port. Likewise, if the Network port is placed in loopback mode, any signals received from a remote unit are looped back out to that remote unit.

An indication of the loopback status of the unit can be obtained from the Loopback LED on the Front panel. See The Front Panel LEDs for the details.

These loopback options allow line diagnostic tests to be performed by external test equipment. The Audit log will record when the host port (Private Loopback) or network port (Public Loopback) has loopback enabled or disabled.

Note: The Datacryptor 100 Mb Ethernet does not support loopback of either the Network or Host interface.

Select one or both of the loopback options:

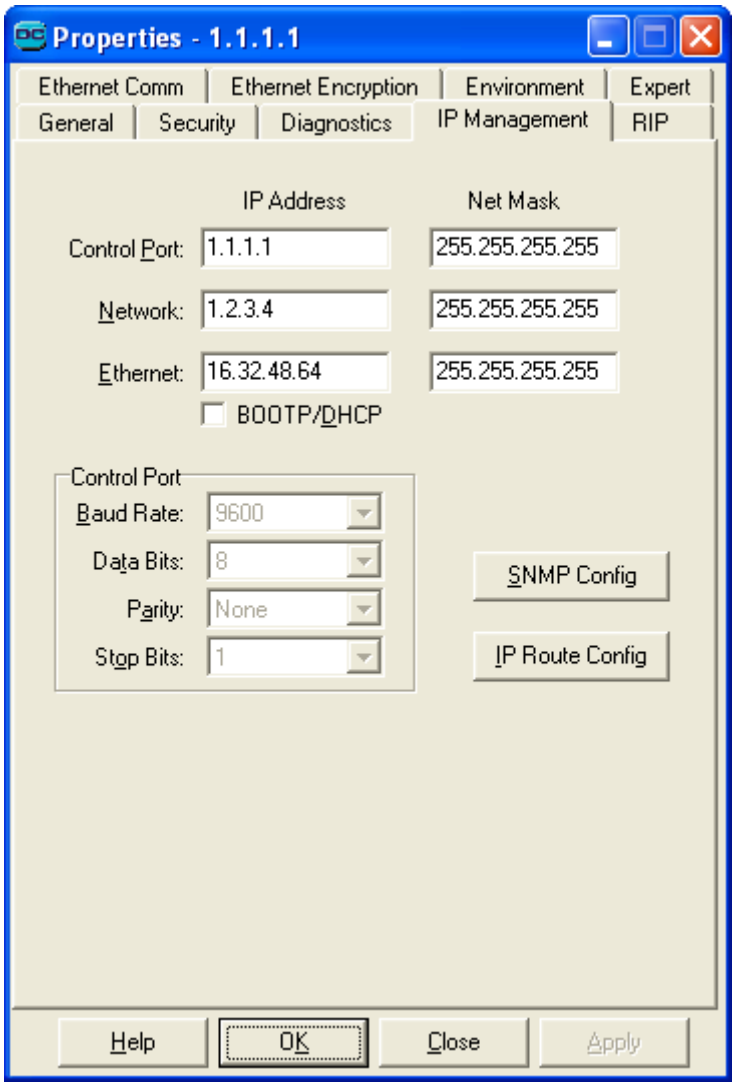
- **Network**: Select the *Network* option to create a loopback between the unit and its peer for troubleshooting purposes.
- **Host**: The *Host* option is used to create a loopback between the unit and its local network.

Loopback functionally is available while the unit is in all encryption modes and all entries and exits will be entered into the units audit log.

Note: The loopback mode is regarded as a transient feature intended purely as an aid to troubleshooting. Therefore when the unit is rebooted the loopback options are set to *Disabled*.

The IP Management Tab

The properties on the **IP Management** tab control the IP addressing of the unit.



They are as follows:

- **Control Port** – the IP address and net mask of the unit's Control Port, this value is only used if the PPP does not negotiate another value
- **Network** - the IP address and net mask of the unit's Network Port.
- **Ethernet** - the IP address and net mask of the unit's Ethernet (management) Port.
- **Control Port** - these fields show the settings for dial up networking.
- **SNMP Config** – click this button to configure the SNMP trapping for this unit.
- **IP Route Config** - click this button to configure the IP Routing table for this unit

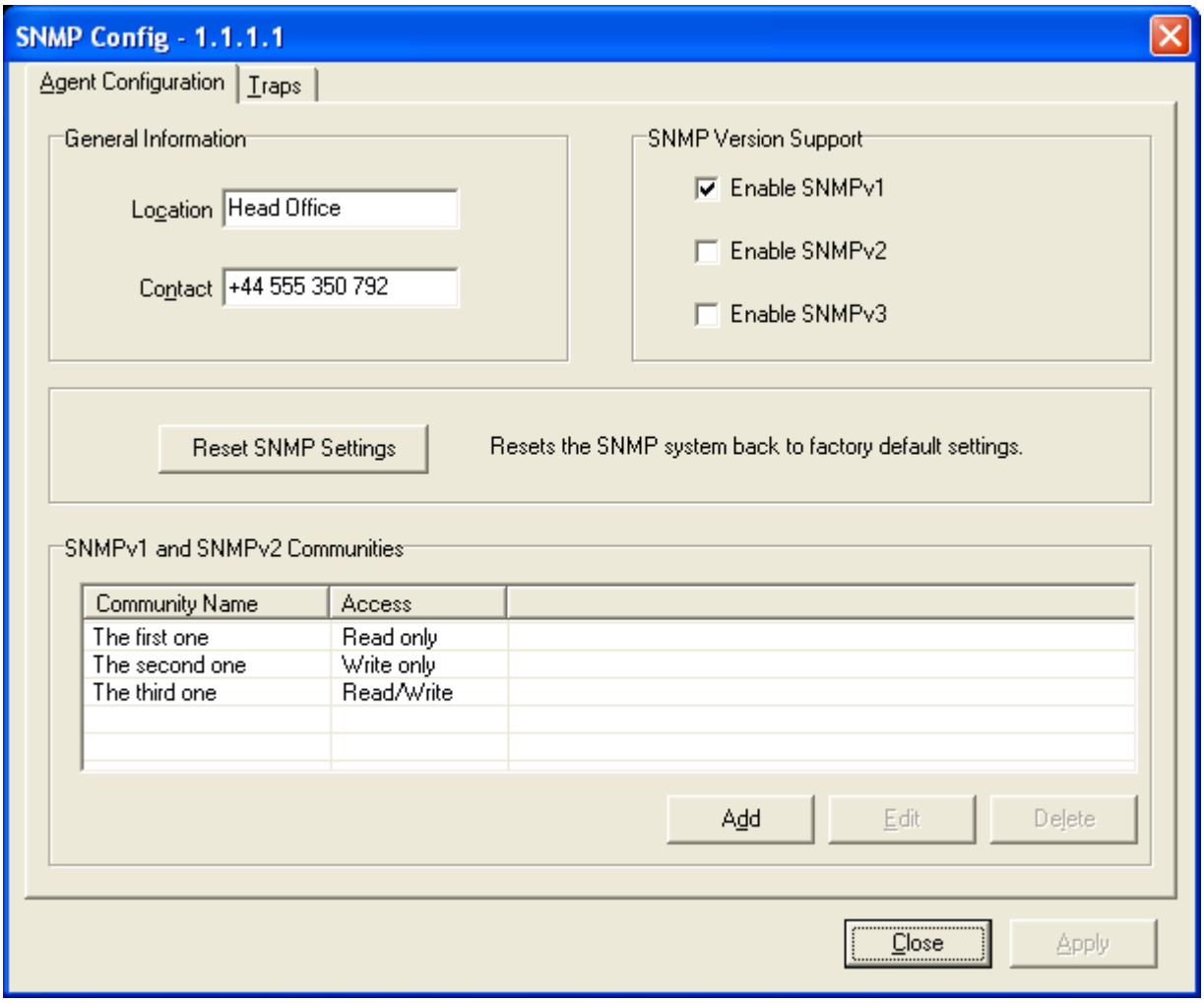
Configuring SNMP

Datacryptor units record all significant management and error events in their logs for later examination, but can also be configured to report them immediately to a central location, by using the SNMP protocol - to help centralize and simplify management. Events are reported as SNMP Traps V1, v2c, or v3 (as selected on the Traps tab – see below), to a central device (typically a PC) called an SNMP Network Manager. This SNMP Network Manager must be compliant with the SNMP agent version support selection on the Agent Configuration tab – see below. A list of the log and SNMP trap numbers with descriptions is provided as an appendix to this guide.

To configure SNMP, click the **SNMP Config** button on the unit's *IP Management* tab to display the *SNMP Config* dialog. This dialog has two tabs – the *Agent Configuration* tab and the *Traps* tab.

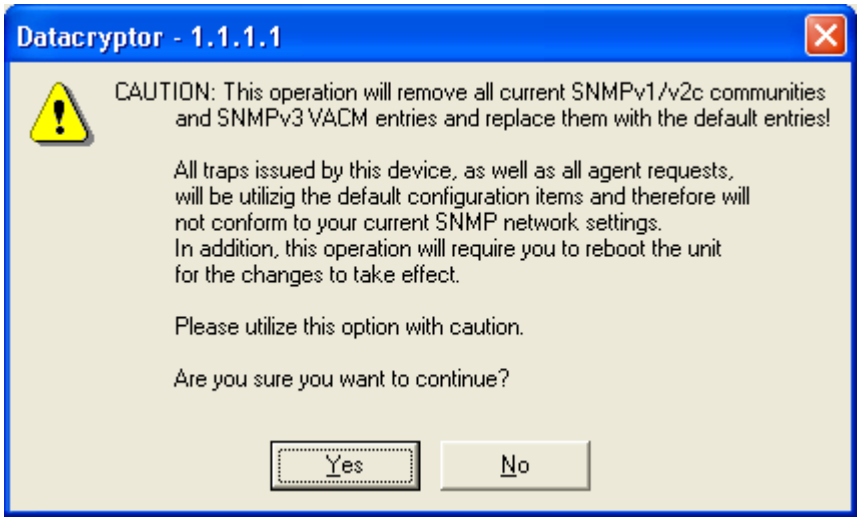
Agent Configuration Tab

The *Agent Configuration* tab lists the SNMP communities defined for this unit, and provides facilities to maintain the list.



- Enter the **Location** and **Contact** information for this unit. Both edit boxes accept spaces and alphanumeric characters. There is a limit of 255 characters for each field.
- Select which versions of SNMP are to be supported using the **Enable SNMP** tick boxes.

Note: Clicking on the Reset SNMP Settings button will result in a caution being shown before the factory defaults are applied – see the following image:



SNMP Communities

SNMP Version 1 and Version 2c support an access control model based upon community names. An SNMP community defines a name and a set of permissions for that community name – each SNMP request received by a Datacryptor unit is labeled with the originator's community name – so the unit can decide whether to permit or deny the request.

These community strings will be utilized by the device to determine whether or not to allow SNMPv1 and SNMPv2c requests. To disable SNMPv1 and SNMPv2c requests, deselect the **Enable SNMP** tick boxes located above the communities list.

To add a new SNMP community:

1. Select the Communities tab.
2. Click the **Add** button – the *Add Community* dialog is shown:

3. Enter the **Name** for this community.
4. Select the type of **Access** for the members of this community: *Read Only*, *Write Only* or *Read/Write*.

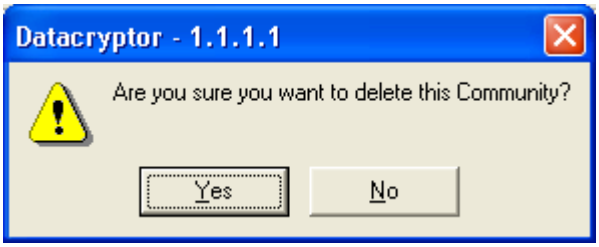
5. Click **OK** to add the community.

To edit an SNMP community:

Select the entry to edit by clicking on it, and then click the **Edit** button.

To delete an SNMP community:

Select the entry to delete by clicking on it, and then click the **Delete** button.



SNMPv3 Users

SNMP Version 3 supports an access control model based upon users and views. Management of these users and views is controlled using native SNMPv3 commands. Please utilize your existing SNMPv3 management tools to manage user and view based access control.

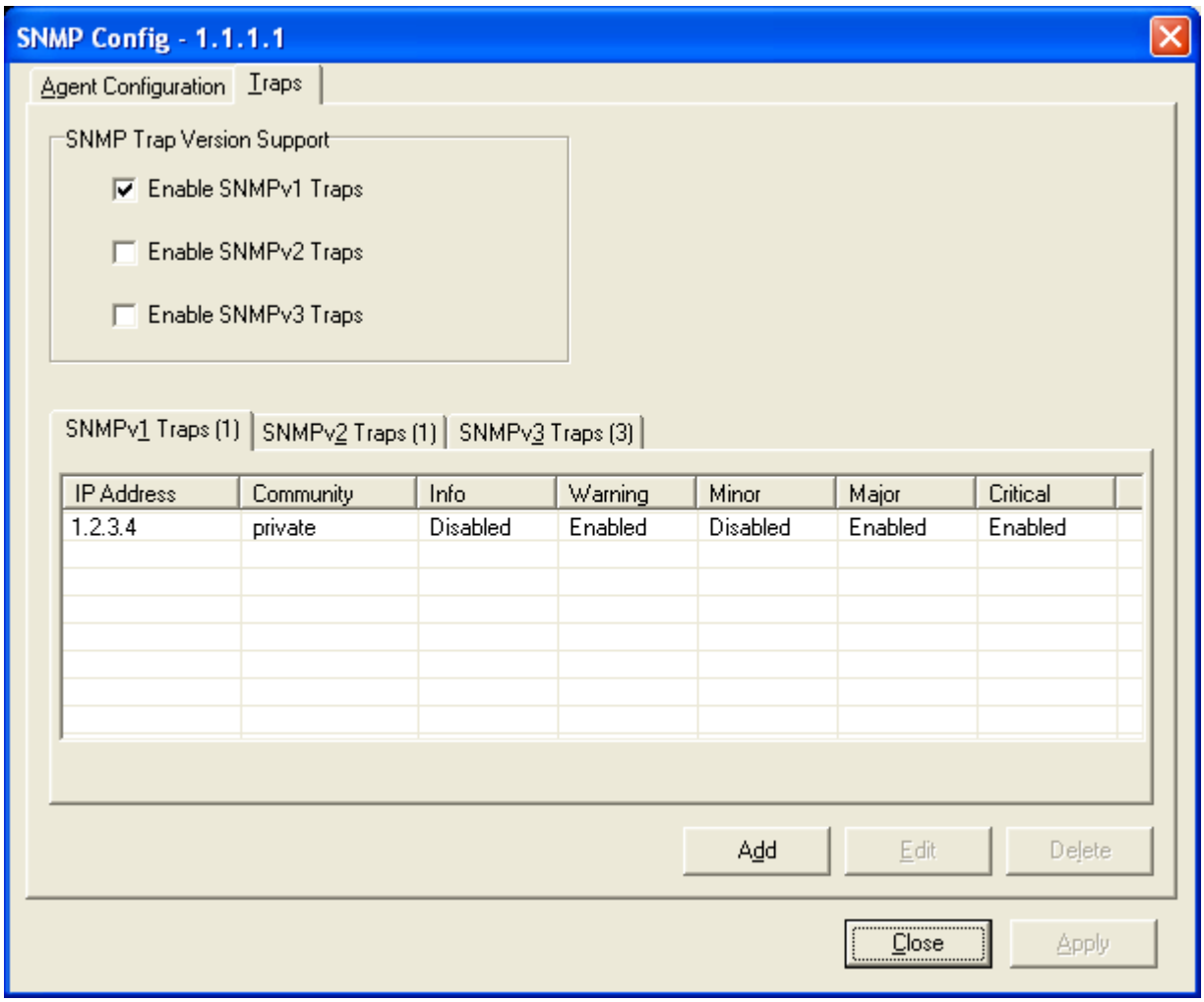
Management of the SNMPv3 users is a time consuming task and you should set your command timeout values to at least 120 seconds per transaction.

Default SNMPv3 user information is displayed in the table below:

Type	Value
User Name	initial
Authentication Password	authentic
Privacy Password	private8

Traps Tab

The *Traps* tab lists the details of each SNMP trap that has been defined for this unit, and provides facilities to maintain the list:

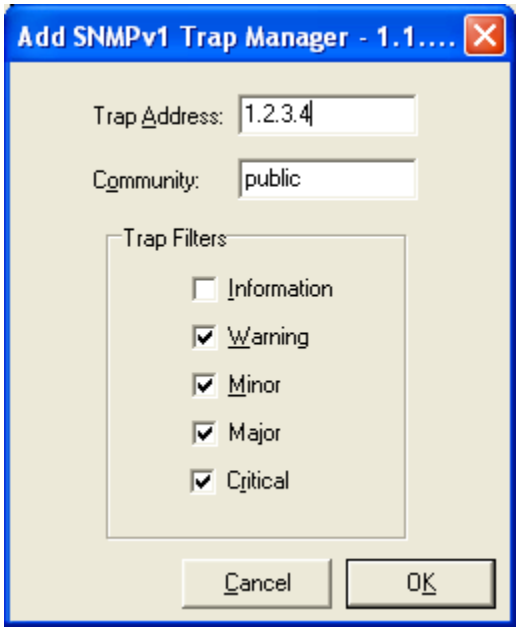


To enable or disable SNMP traps for this unit, use the appropriate **Enable** checkboxes for the each version of SNMP.

When defining an SNMP Trap that is not on a local network connection, the Datacryptor Ethernet must have a route defined for the address in order for the Traps to be delivered to the SNMP Manager.

To add a new SNMP trap manager:

1. Select the **Traps** tab.
2. Select the appropriate SNMP version tab.
3. Click the **Add** button.

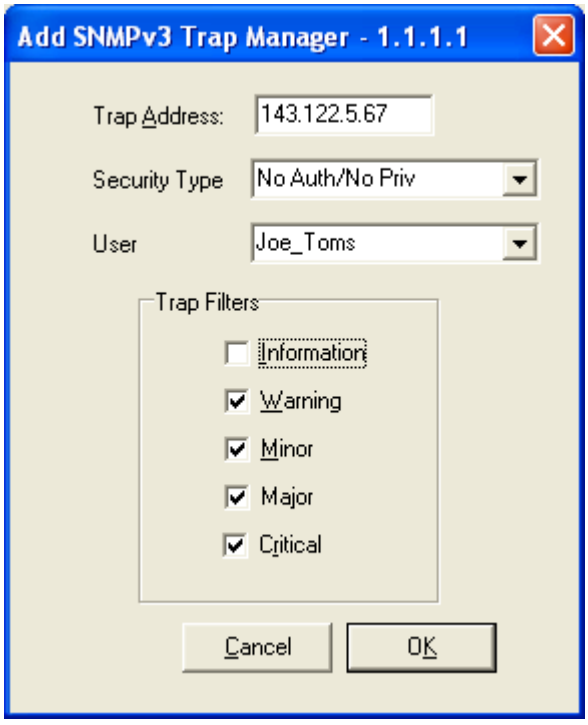


- **Trap Address**: Type the IP address of the SNMP trap manager.
- **Community**: This field is unused because the unit only issues SNMP Version 3 traps. You can set this field to any value without affecting behavior of trap issuance.
- **Trap Filter**: Tick the categories of event to send to this trap manager.

Note: It may take up to 20 seconds to acknowledge the selected action.

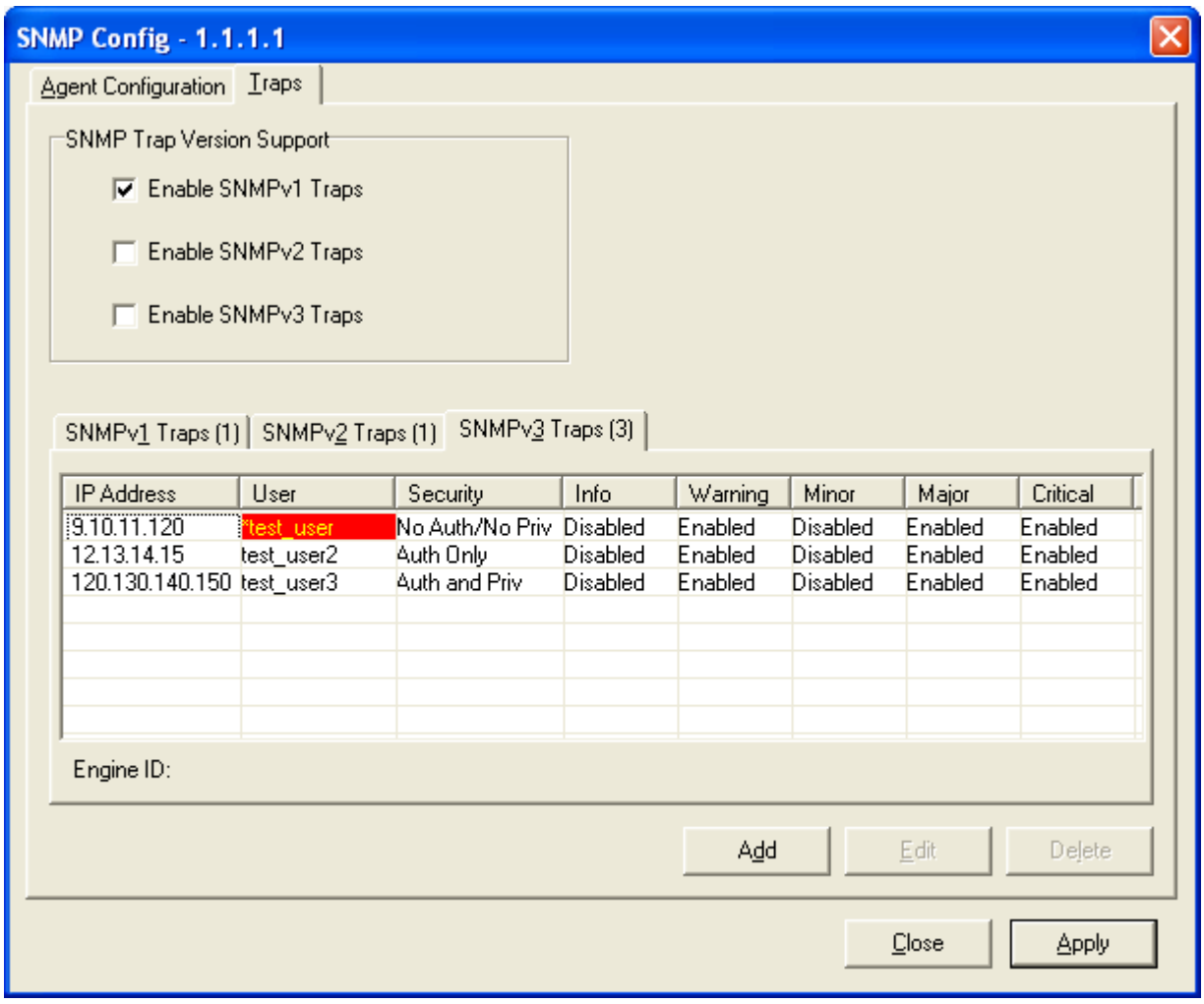
Adding SNMPv3 Trap Managers:

When using SNMPv3 you are able to specify whether the reports will use authentication alone, or authentication and privacy combined, or no security at all.



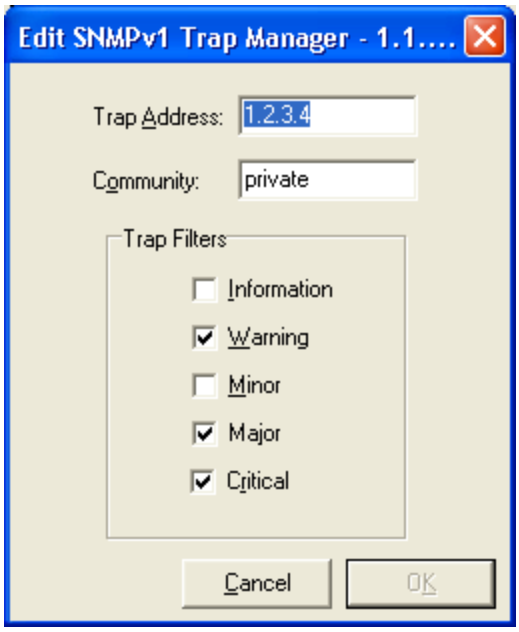
Add Trap Manager dialog for SNMPv3

- **Security Type**: Select the type of security that will be used for the reports from the drop down list. If the security is set to none (*No Auth/No Priv*), then the user name will be highlighted in red on the SNMPv3 tab, as illustrated by the following image:


SNMP Config - 1.1.1.1
Agent Configuration
Traps
SNMP Trap Version Support
Enable SNMPv1 Traps
Enable SNMPv2 Traps
Enable SNMPv3 Traps
SNMPv1 Traps (1)
SNMPv2 Traps (1)
SNMPv3 Traps (3)
IP Address
User
Security
Info
Warning
Minor
Major
Critical
9.10.11.120
*test_user
No Auth/No Priv
Disabled
Enabled
Disabled
Enabled
Enabled
12.13.14.15
test_user2
Auth Only
Disabled
Enabled
Disabled
Enabled
Enabled
120.130.140.150
test_user3
Auth and Priv
Disabled
Enabled
Disabled
Enabled
Enabled
Engine ID:
Add
Edit
Delete
Close
Apply

To edit an SNMP trap manager:

1. Select the entry to edit by clicking on it, and then click the **Edit** button.

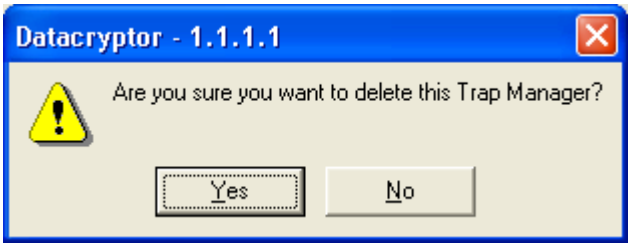


2. Edit the entries in the Edit Trap Manager dialog as required, and then click **OK**.

Note: It may take up to 20 seconds to acknowledge the selected action.

To delete an SNMP trap manager:

1. Select the entry to delete by clicking on it, and then click the **Delete** button.

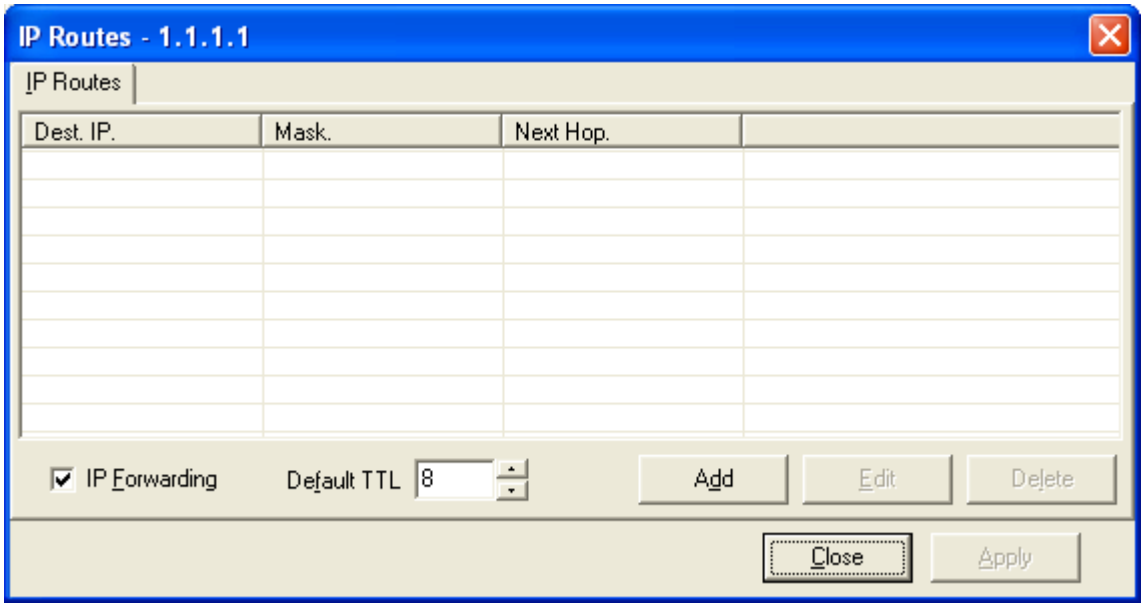


2. Click **Yes** to confirm deletion, or **No** to cancel deletion.

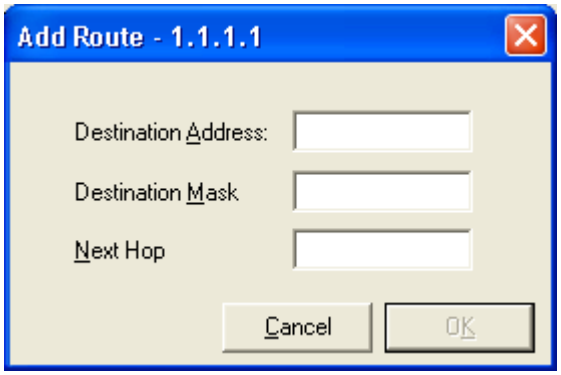
Note: It may take up to 20 seconds to acknowledge the selected action.

IP Route Config

Selecting this button on the Properties - IP Management tab will display the IP routes dialog detailing the IP routes that have been defined for this unit and providing facilities to maintain the IP routes list:

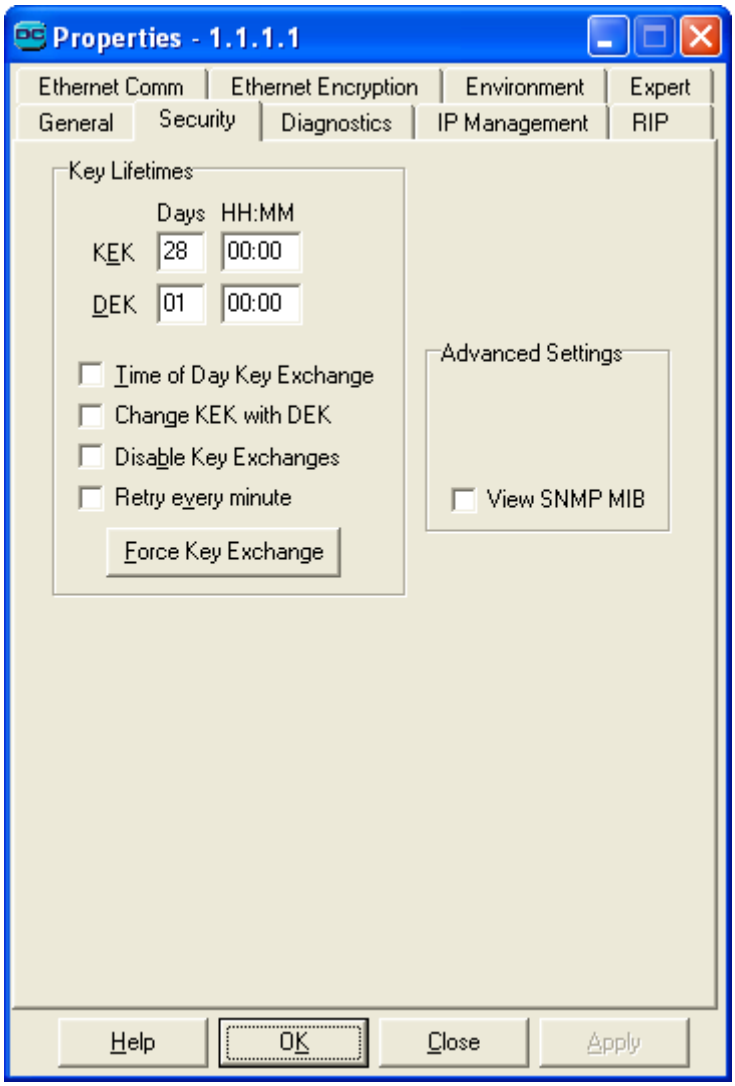


Use the Add, Edit and Delete buttons to manage the required list of IP routes.



The Security Tab

The properties on the **Security** tab control crucial aspects of the security of the Datacryptor unit.



They are as follows:

- **KEK**: the longest time that the unit will use a KEK for, in days, hours, minutes.
- **DEK**: the longest time that the unit will use a DEK for, in days, hours, minutes – or the time at which to perform a daily key exchange (see next control).
- **Time of Day Key Exchange**: check this box to force a regular key exchange at the same time every day (as specified by the DEK field).
- **Change KEK with DEK**: check this box to change the KEK when the DEK changes. When this is checked the KEKs are not stored and will not be visible in the Key Management dialog.

- **Disable Key Exchanges**: check this box to disable all key exchanges other than those required to make a secure connection. (This disables the previous 4 controls until you uncheck it.)
- **Retry every minute** - with this box checked the Datacryptor Ethernet will try to poll for lost peers every minute, this is the default behavior. If the "retry every minute" box is unchecked the Datacryptor Ethernet will gradually increase the time intervals between attempted key exchanges. It will try after one minute, then after a further 2 minutes and then after a further 4 minutes (i.e. the interval is doubled each time). The interval will continue to double up to a maximum interval of 2 hours, it will then continue to poll every 2 hours.
- **Force Key Exchange**: click this button to force an immediate key exchange with the peer unit.

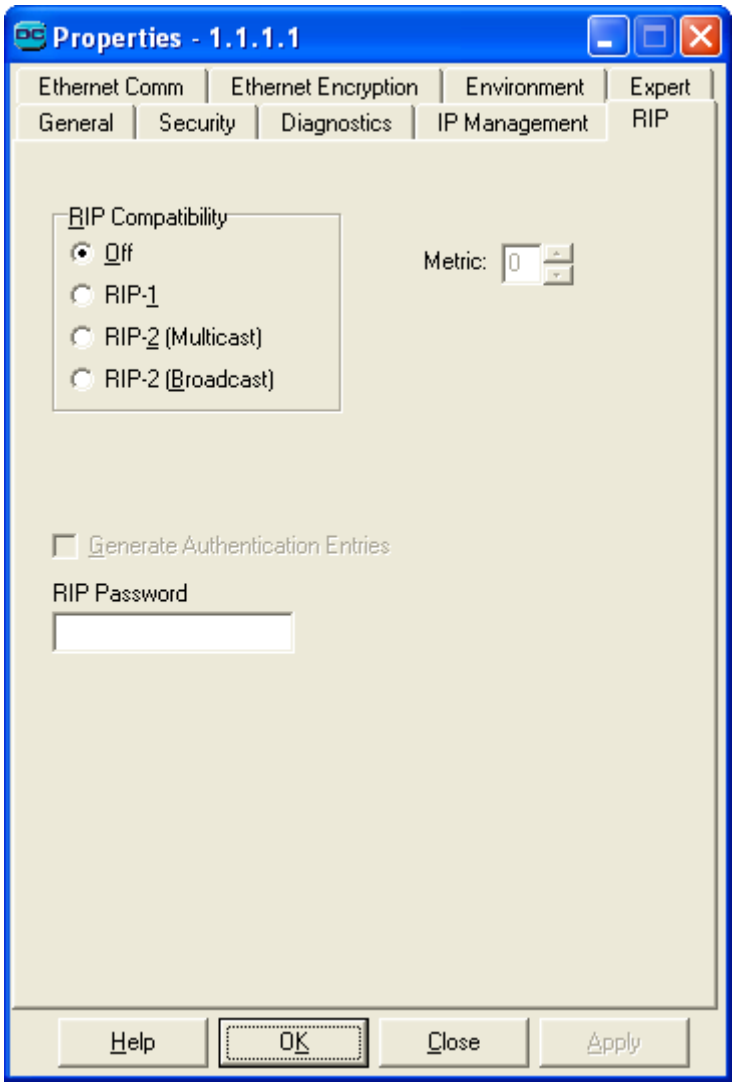
Advanced Setting

- **View SNMP MIB:** If checked the user will be able to use an external SNMP MIB browser to view information regarding network configuration etc.

The RIP Tab

The RIP tab sets up the properties of the Routing Information Protocol (RIP) and configures the way Rip messages are sent to other routers.

The Datacryptor Ethernet supports versions RIP-1 and RIP-2.



RIP Compatibility

This set of radio buttons is used to select which version of RIP that the Datacryptor Ethernet is using:

- **Off** - this switches off compatibility with any version of RIP. No RIP messages transmitted on any port.
- **RIP 1** - select this if you wish the Datacryptor to be compatible with the first version of RIP. This version of RIP only uses broadcasts to pass on information.
- **RIP 2 (multicast)** - this sets the Datacryptor to be compatible with RIP version 2 when used in multicast mode. The multicast mode was implemented with the more versatile RIP 2.

- **RIP 2 (broadcast)** - this sets the Datacryptor to be compatible with RIP version 2 but uses the broadcast mode. Some networks that are using RIP 1 may want to use RIP 2 but not use multicast transmissions. This will ensure that RIP responses are not addressed to multicast address 224.0.0.9.

Note: IGMP is not needed since these are inter-route messages that are not forwarded.

Metric

This sets the metric (or cost) that is associated to each route that is advertised in RIP responses sent out by the Datacryptor unit.

Generate Authentication Entries

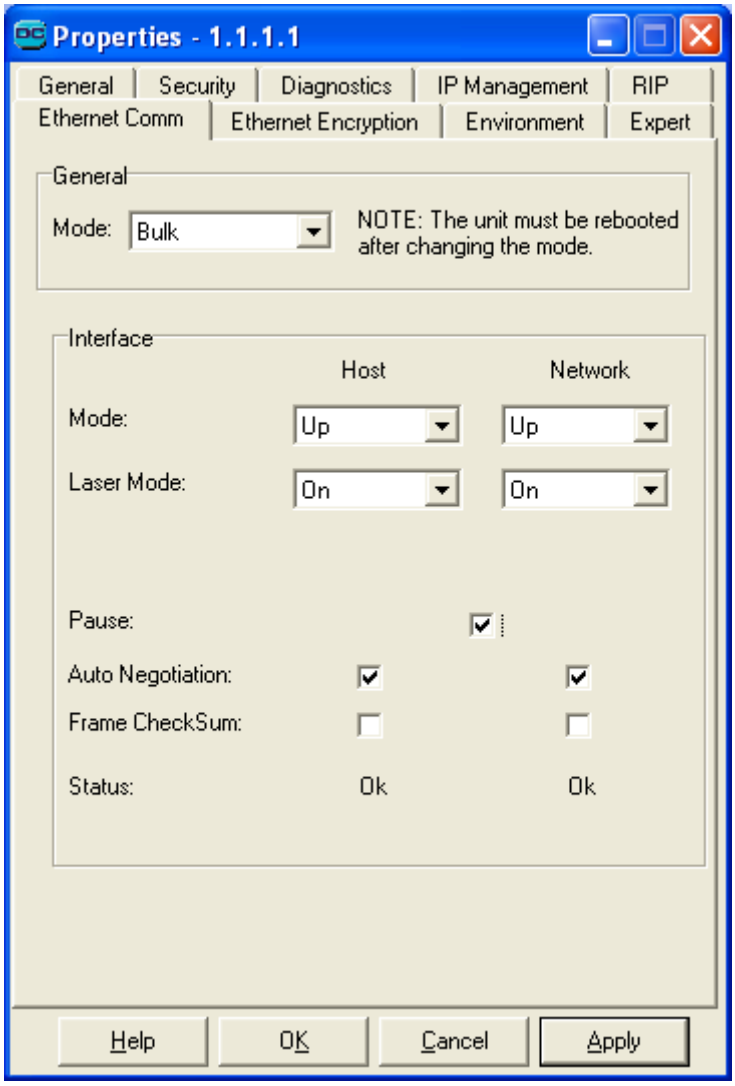
RIP 2 can implement an authentication entry in the first part of its response that contains a password. If a router matches its own RIP password with that of the RIP response authentication entry it will accept the routing information in the RIP response. Tick this check box to enable the inclusion of authentication entries in RIP 2 messages sent from the Datacryptor Ethernet.

Password

This field contains the password to be associated with the authentication entry.

The Ethernet Comm Tab for 1 and 10 Gigabit Datacryptors

The properties on the Ethernet Comm tab control the communications settings of the Datacryptor unit. The Comm tab illustrated in this section applies to the 1 Gig Ethernet unit. Differences between the 1 Gig and 10 Gig units will be stated where relevant.



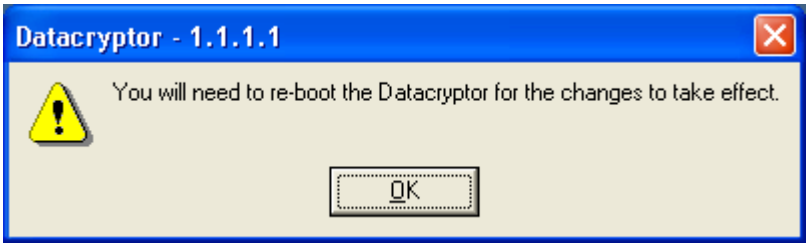
Ethernet Comm Tab for the 1 Gigabit Datacryptor

The properties are as follows:

Mode- Selects one of two options for the transmission mode.

- **Bulk** - Unit encrypts everything including Ethernet header.
- **Tunneling** - Unit encrypts every thing below Ethernet header.

When a mode change is made then the following dialog will be shown advising that the unit must be rebooted.



The unit can be rebooted using the option available on the Diagnostic tab

Interface Mode - Allows the Host and network interfaces to be switched Up/Down.

Laser Mode - Allows the Host and network Lasers to be individually switched On/Off.

Pause - The Pause option is a special Ethernet function that provides flow control between Ethernet devices. If the switch on the public network is told to enable Pause, then a rule has to be configured on the encryption unit to let the Pause frames pass through unencrypted to the switch on the local side. A typical rule is:

Plain public 01:80:c2:00:00:01.

This Multicast address corresponds to address reserved in IEEE 802.3 for the Pause functionality.

Note: The Pause tick box is not displayed for the 10Gig Ethernet unit.
Pause frames can still be used with the 10Gig Ethernet unit but this will not be auto negotiated and would still require the configuration of a rule to pass pause frames in the plain.

Auto Negotiation- allows the unit to automatically negotiate connection without intervention from the user.

Note: The Datacryptor 1 Gig Ethernet only supports I000 Mbps full duplex, and the 10 Gig Ethernet unit only supports I0,000 Mbps full duplex. The 100 Mb unit supports a selection of one 10 Mbps or 100 Mbps. Anything else will cause the auto negotiation (if selected) to fail and report Link Down on the General tab interface status box.
The **Auto Negotiation** tick box is not displayed for the 10Gig Ethernet unit since the 10Gig Ethernet unit does not support auto negotiation.

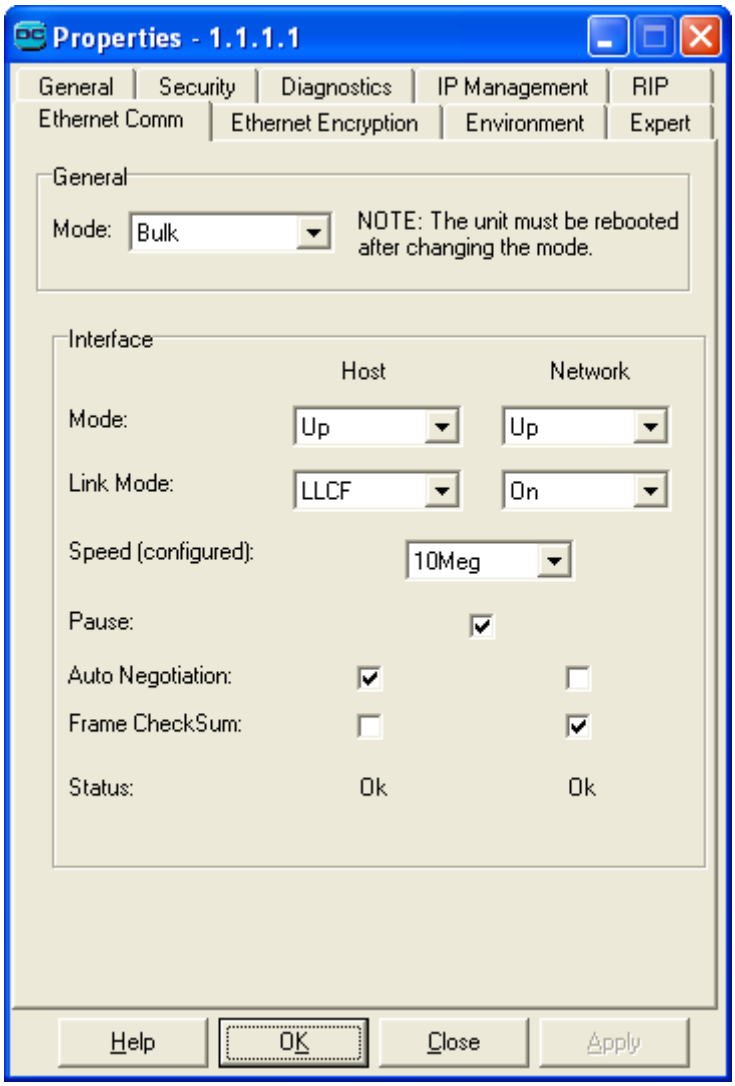
Frame Checksum. If the FCS box is checked then the checksum is stripped off the incoming frame and added again for outgoing frames. When the FCS box is not checked the FCS is treated like normal data will be and encrypted and decrypted like data on the public interface.

The FPV imposes the following defaults when switching modes. When switching from Bulk to Tunneling the Network FCS is checked. When switching from Tunneling to Bulk, the Network FCS is unchecked. It is advised that the user accepts these default settings.

Status- Shows the current status of the Host and network interfaces.

The Ethernet Comm Tab for 100 Mb Datacryptor

The properties on the Ethernet Comm tab control the communications settings of the Datacryptor unit.

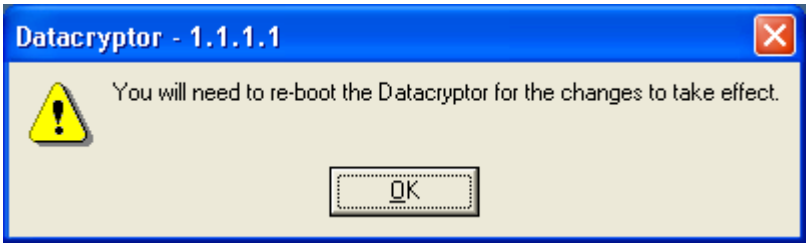


They are as follows:

Mode- Selects one of two options for the transmission mode.

- **Bulk** - Unit encrypts everything including Ethernet header.
- **Tunneling** - Unit encrypts every thing below Ethernet header.

When a mode change is made then the following dialog will be shown advising that the unit must be rebooted.



The unit can be rebooted using the option available on the Diagnostic tab

Interface Mode - Allows the Host and network interfaces to be switched Up/Down.

Link Mode - Allows the Host and network connections to be individually switched On/Off. If the LLCF option is selected, the connection is on with link loss carry forward turned on.

Auto Negotiation - allows the unit to automatically negotiate connection without intervention from the user.

Note: The Datacryptor 100 Mb Ethernet may be set to 100 Mbps or 10 Mbps full duplex. The Host and Network interfaces on encryption units at both ends of the link need to run at the same speed.

Pause - The Pause option is a special Ethernet function that provides flow control between Ethernet devices. If the switch on the public network is told to enable Pause, then a rule has to be configured on the encryption unit to let the Pause frames pass through unencrypted to the switch on the local side. A typical rule is:

Plain public 01:80:c2:00:00:01.

This Multicast address corresponds to address reserved in IEEE 802.3 for the Pause functionality.

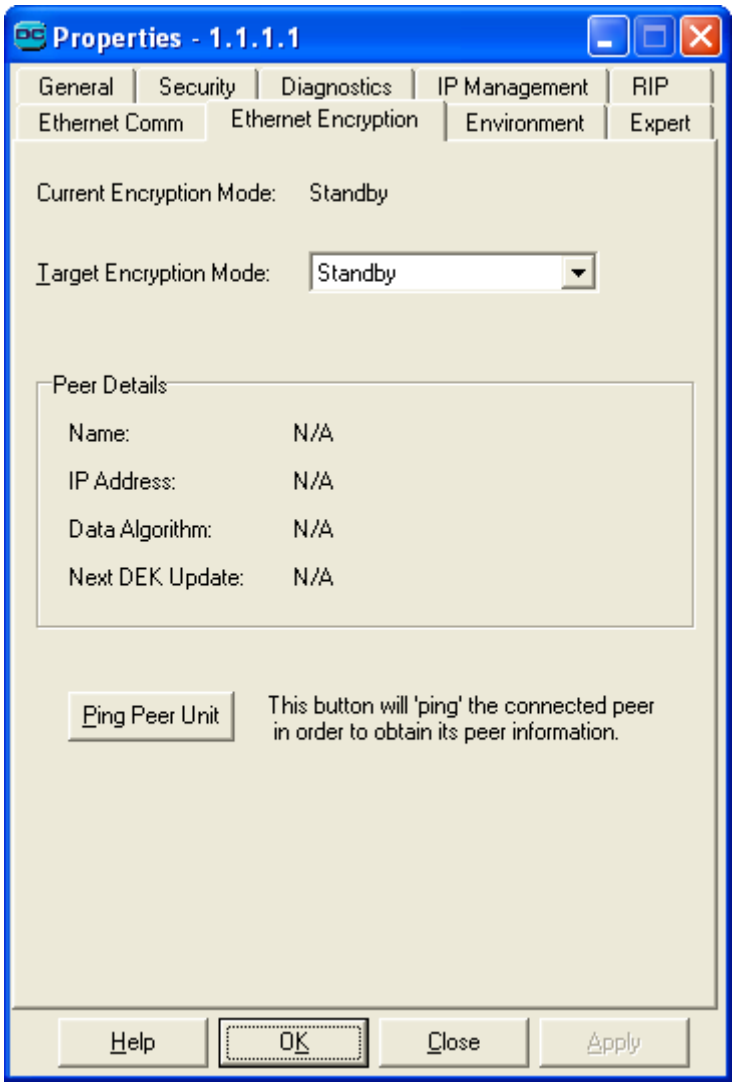
Speed (configured) – Must be set to 10 Meg or 100 Meg as appropriate to the speed of the link. Enabling auto-negotiation only permits the Datacryptor to tell requesting units what speed it is set to, it does not support the auto-negotiation of speed.

Frame Checksum. If the FCS box is checked then the checksum is stripped off the incoming frame and added again for outgoing frames. When the FCS box is not checked the FCS is treated like normal data will be and encrypted and decrypted like data on the public interface.

The FPV imposes the following defaults when switching modes. When switching from Bulk to Tunneling the Network FCS is checked. When switching from Tunneling to Bulk, the Network FCS is unchecked. It is advised that the user accepts these default settings.

Status- Shows the current status of the Host and network interfaces.

The Ethernet Encryption Tab



The Ethernet Encryption tab shows the **Current Encryption mode** in use by the unit.

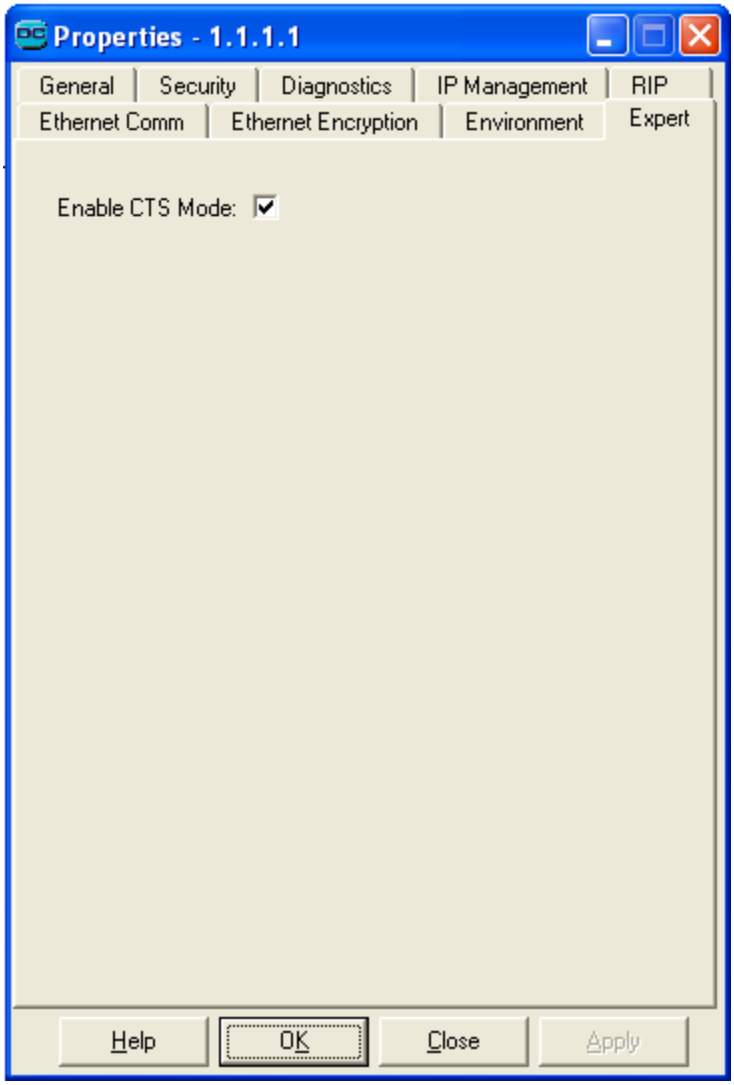
Target Encryption mode: This allows you to select the target or required encryption mode using the drop down menu. The three options are: *Standby*, *Encrypt*, or *Plain*.

Peer Details: The Peer unit's details (Name, IP Address, etc) are shown on the tab.

Ping Peer Unit button: This button may be clicked to shows additional Peer information, if required.

The Expert Tab

The Ethernet Expert tab allows to **Enable CTS Mode**. The Ethernet Expert tab is not shown when using the 10Gig Ethernet unit since CTS mode is always enabled for the 10Gig Ethernet unit.

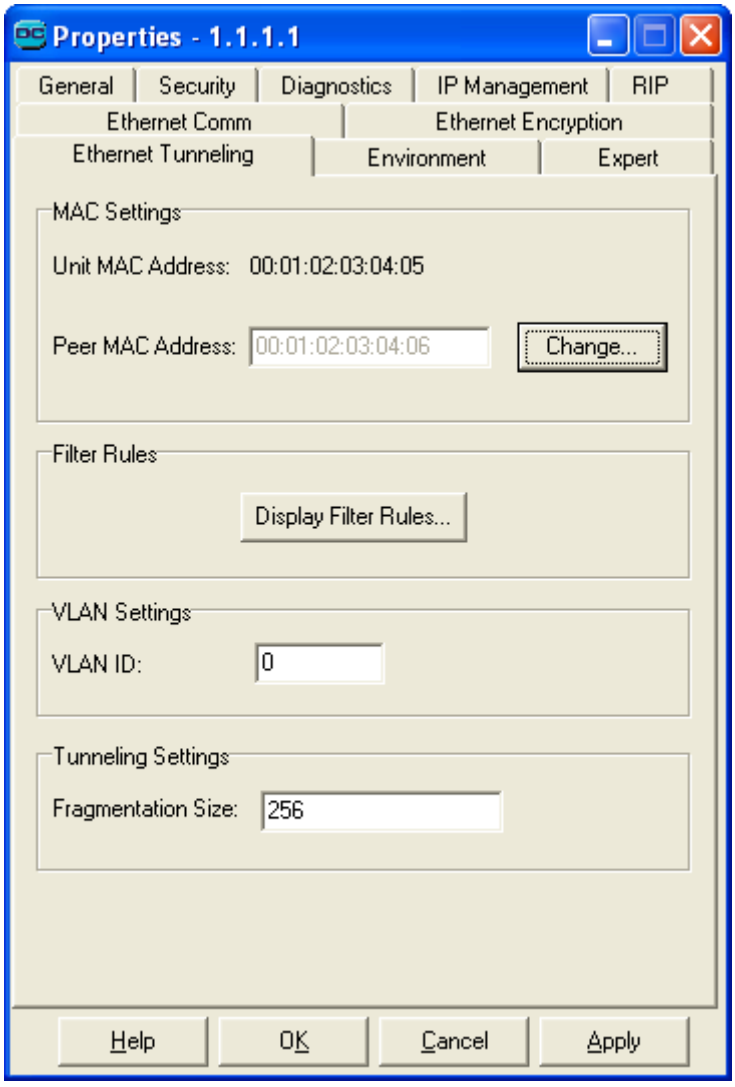


The CipherText Stealing mode minimizes the latency caused by the encryption of the Ethernet packets. By default this mode is enabled, and disabling the mode is only recommended when connecting this unit to a legacy Ethernet Datacryptor which does not support the CTS mode. The **Enable CTS Mode** checkbox is greyed-out when the Current Encryption Mode is Encrypt. The CTS mode may only be changed when in Plain or Standby mode; that includes during the time that Target Encryption Mode is Encrypt but the Current Encryption Mode is still Plain or Standby.

The Ethernet Tunneling Tab

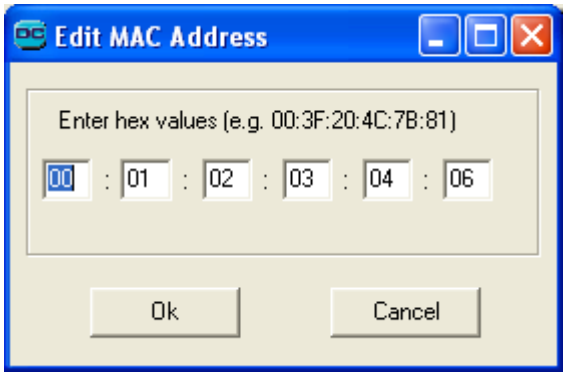
The *Ethernet Tunneling* tab will only be present when **Tunneling** mode is selected on the *Ethernet Comm* tab.

Note: The **Tunneling Settings** section, which includes the **Fragmentation Size** item, is not displayed for the 10Gig Ethernet unit. The 10Gig Ethernet unit does not support fragmentation.



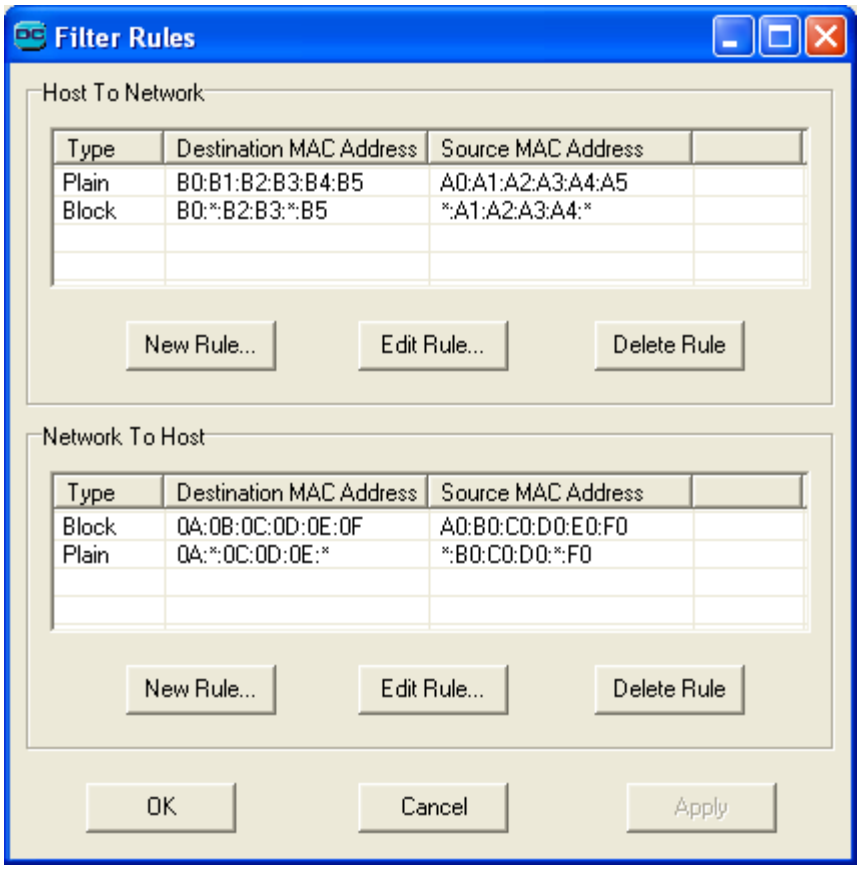
MAC Settings - Operating at the Layer 2 level the in band communications between the units will be controlled by using MAC Addresses. The unit has two addresses assigned for use between the units at either end of an Ethernet Layer 2 link. The Unit MAC Address is displayed. The peer MAC address must be obtained and entered in the box provided.

This is entered by selecting the **Change** button, the following dialog is shown.



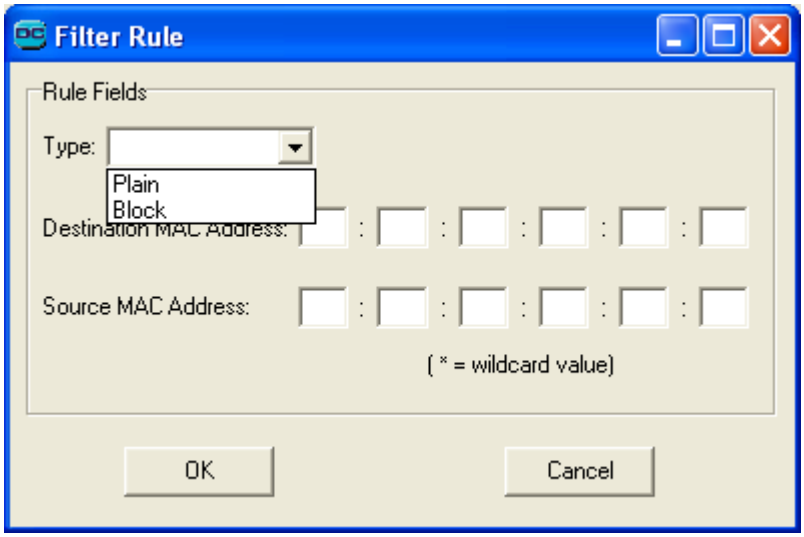
Enter the required address in the boxes shown. Movement between the boxes can be achieved by using the mouse or the tab and shift tab key combinations. The units MAC address must be inserted in the peer unit address box at the other end of the link.

Filter Rules - Clicking the **Display Filter Rules** button will display the following dialog:



This gives the option of setting a maximum of four rules on both the Host to Network and Network to Host ports. Selecting the **New Rule** button will open the *Filter Rule* dialog.

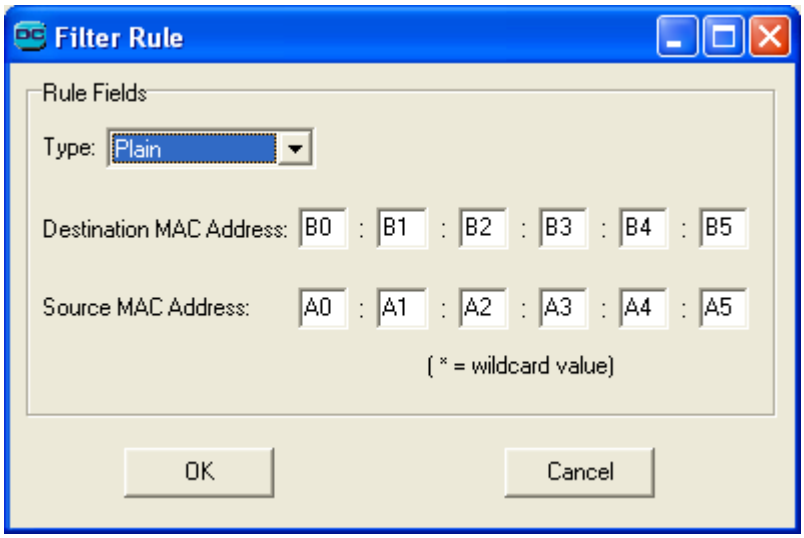
When setting a rule, the first step is to select a rule type:



Rule Type

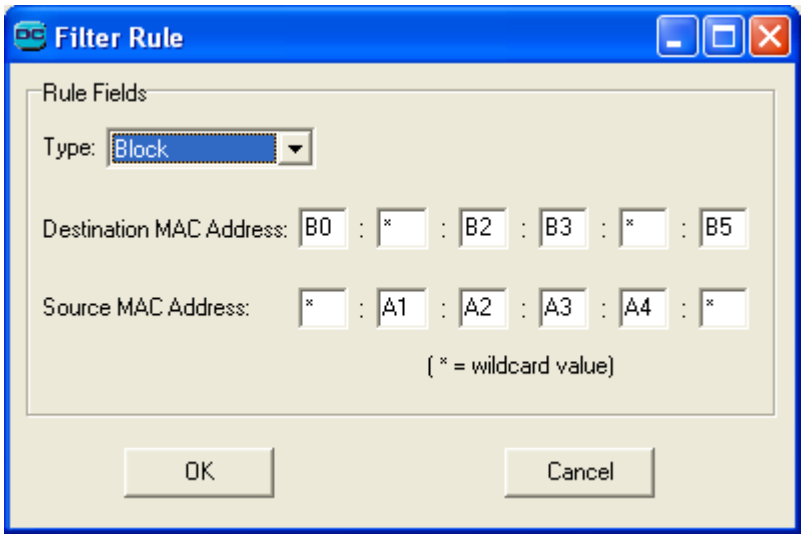
- Plain this allows the Datacryptor unit to pass information from the specified addresses in plain, and is used to allow network specific traffic. To ensure compatibility and operation of equipment within the public network.
- Block this option identifies individual addresses or a range of addresses which are to be denied access by the Datacryptor unit.

The second step is then to set the destination and source MAC addresses:



MAC Address

The destination and source addresses are standard MAC addresses with the added option of using the *wildcard character (see below) to enable a range of addresses to be identified.



When you have set the addresses, select **OK** to add the new rule to the list. The apply button will then become active.

The **Edit** and **Delete** functions requires the user to select a rule prior to clicking the appropriate button. However, if the table contains only one rule and the user presses either the edit or delete button, that rule is automatically selected for the operation.

	**CAUTION:** Care must be exercised when creating filter rules, in order that the intended traffic and only the intended traffic is allowed.

VLAN Settings - Enter the required **VLAN ID** (a number between 1 and 4094). If this is set to zero, then the MAC addresses are used for in band communications.

Tunneling Settings – An optional fragmentation can be enabled with the **Fragmentation Size** field in tunnel mode. Encapsulated frames that become larger than the public networks allow, can be fragmented. The fragmentation works like this:

- Outgoing frames including the tunnel-header smaller or equal to Fragmentation Size will be sent to the WAN without modification.
- Outgoing frames including the tunnel-header larger than Fragmentation Size will be fragmented and sent to the WAN in two parts.
- Incoming frames on the local interface which are already larger than Fragmentation Size will be truncated to Fragmentation Size and therefore discarded on the remote side.

Note: The **Tunneling Settings** section, which includes the **Fragmentation Size** item, is not displayed for the 10Gig Ethernet unit. The 10Gig Ethernet unit does not support **Fragmentation Size** setting and will never fragment.

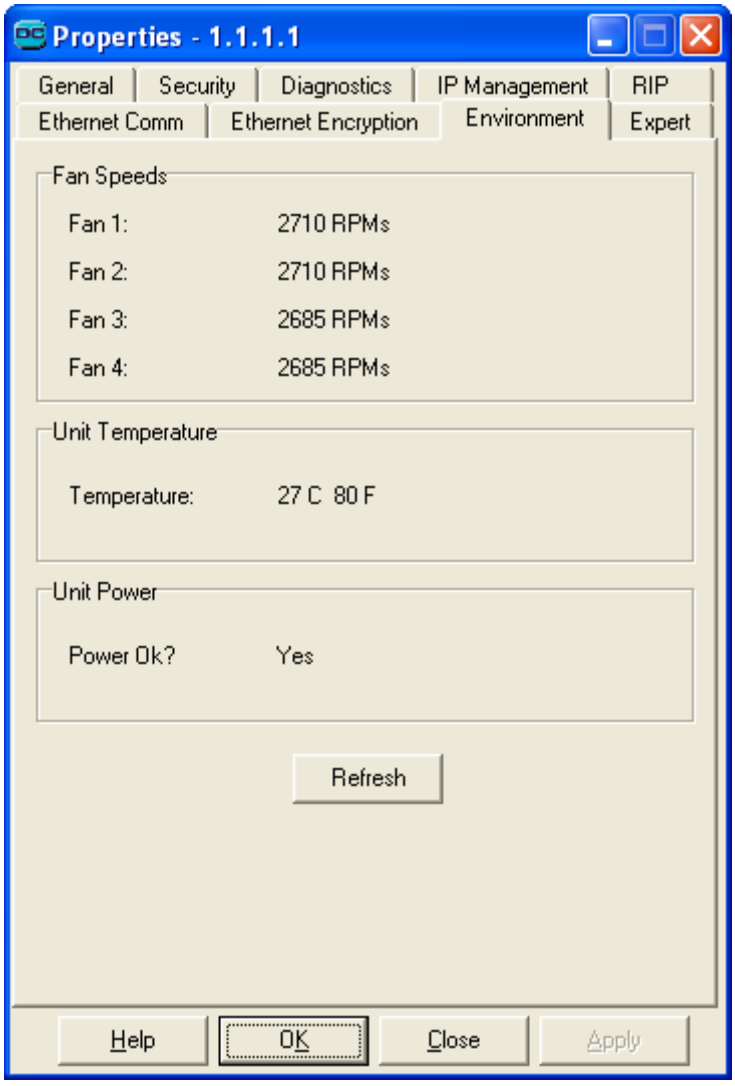
The permissible range for **Fragmentation Size** is:

- *Gigabit Ethernet*: 0 = no fragmentation, 256 ≤ Fragmentation Size ≤ 16300
- *10/100 Mb Ethernet*: 0 = no fragmentation, 256 ≤ Fragmentation Size ≤ 2000.

The Environment Tab

The Environment tab shows the fan speeds along with the unit temperature and power unit condition. These readings may be used to check that the Datacryptor environment is satisfactory for normal operation. It is recommended that you make a note of these readings during normal operation. These readings may be useful for comparison purposes in the event of problems such as overheating.

If the unit temperature becomes excessive, the Alarm LED will be on, and an entry will be made in the Error log – please refer to Fan/Heat Monitor Alarm for more information.



Note: The Datacryptor 100 Mb Ethernet shows only a single fan.

Appendices

Appendix A: Device Maintenance

Periodically perform maintenance on your Datacryptor.

- Keep components free of dust and other particulate matter.
- Check fans for reduced airflow caused by dust build-up and clean as necessary.
- Examine cables and fiber for damage and ensure that airflow requirements have been met.
- Consult the Environment tab on the Front Panel Viewer's Properties dialog for readings of the fan speeds and unit temperature. Make a note of these readings under normal operating conditions – these readings can be used for comparison in the event of a Fan/Heat monitor alarm.

Otherwise, no special maintenance is required.

Physical Inspection

The Datacryptor is housed in a tamper evident chassis. Periodically check the chassis for evidence of tampering. Items to look for include stripped screws and damaged seals.

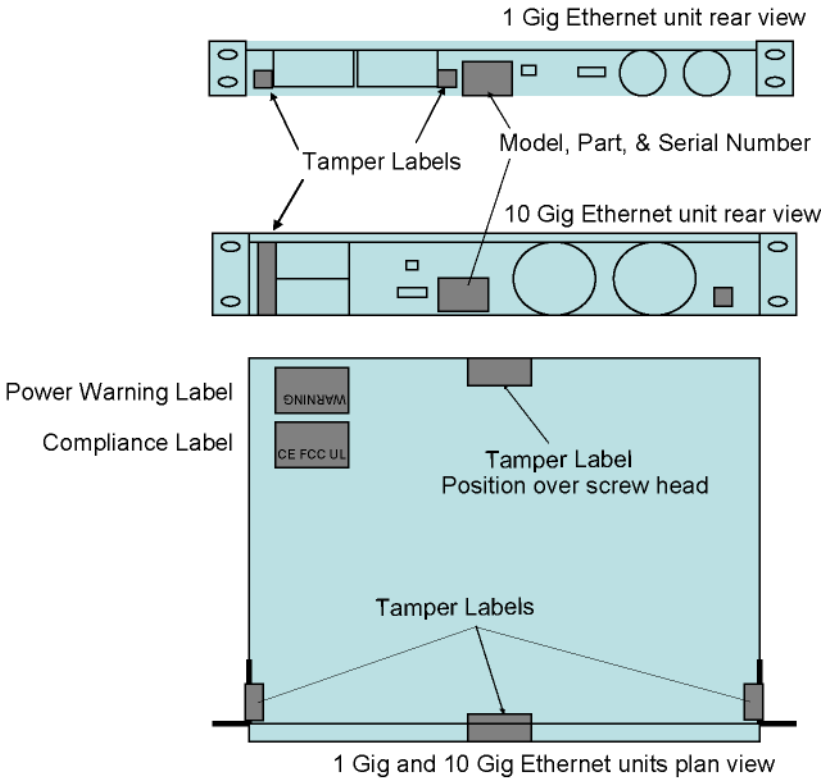


Figure A-1 Location of Tamper Proof and Identification Labels on the units

The frequency of a physical inspection depends on the value of the intellectual property being protected and the security of the environment in which the Datacryptor is located. For example,

a locked equipment closet provides a more secure environment than an open server room. At a minimum, we recommended that the unit's physical integrity be checked monthly.

The units also have interlock switches that will cause the key material to be erased if the lid is removed.

Power Supplies

Failure of one of the power supply units will cause a high-pitched continuous note to sound, allowing a replacement to be planned.

Note: There is only one power supply in the Datacryptor 100 Mb Ethernet and so no audible signal will be generated for power failure in that unit.

Lithium Battery

The Datacryptor contains a lithium battery, which has a typical life expectancy of 10 years, dependant on usage. The Datacryptor must be returned to Thales for battery replacement.

WARNING: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

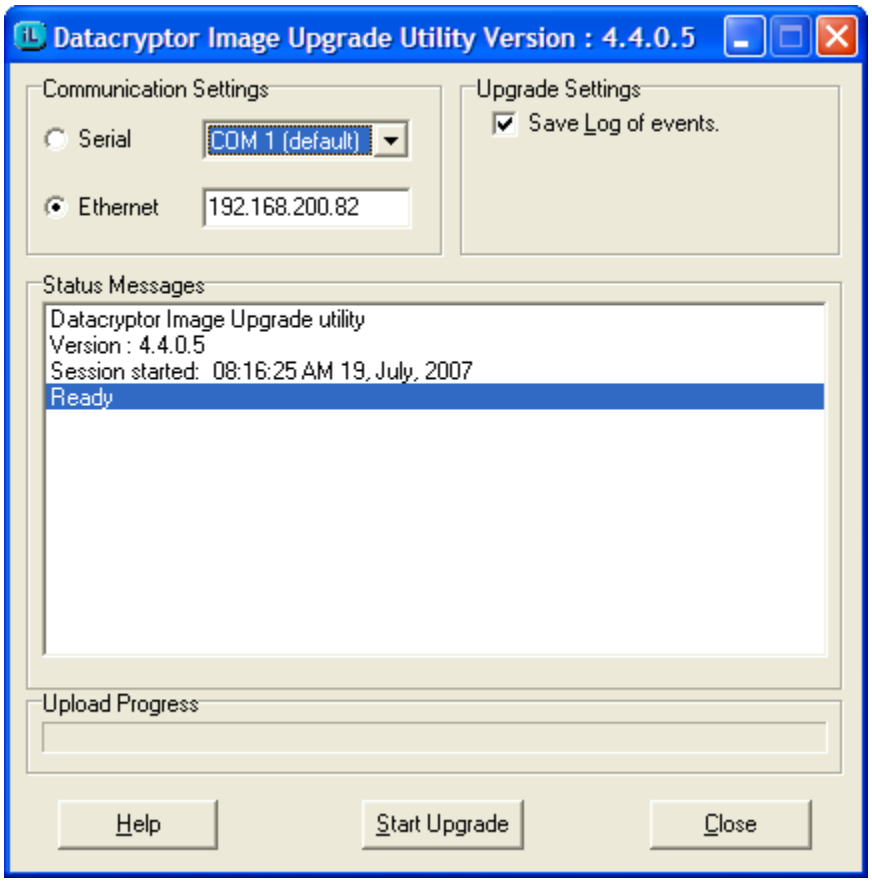
Appendix B: Loading Datacryptor Unit Software

Datacryptors are factory pre-loaded with the required 'application' software and protocol data. However, if a new version of software needs to be loaded into a Datacryptor, the following procedure describes how to carry out the operation using the Image Loader utility, which will be provided with the new version of software.

Note: The process of application upgrade can also be used to upgrade the bootstrap of the unit. If a unit is being upgraded to application software greater then 1.07.04, then the user is advised to upgrade the bootstrap software to the latest version, as this is required for the algorithm retention feature.

	**WARNING:** Do not power the Datacryptor unit down during a bootstrap upgrade; this may cause the unit to enter an unrecoverable state. For this reason, it is recommended that the Datacryptor is connected to an UPS (Uninterruptible Power Supply) during this process.

1. Connect the Datacryptor to the COM port of the PC that has access to the Image Loader utility (`imgload.exe`), and power it on.
2. Start the `imgload.exe` application.



3. Select the COM port that the Datacryptor is connected to, using the pull down menu. This is COM1 by default.
4. If the Datacryptor application is already running, you may choose the **Ethernet** radio button. Enter the IP address in the field next to the Ethernet radio button. Ethernet is faster than Serial for loading code.
5. If the status messages that are generated by the Image Loader utility during the session are not to be saved, clear the check box marked **Save Log of Events**.
6. Ensure that the Datacryptor is connected to the selected COM port, and that the power is on. If the **Ethernet** radio button is selected, use a command window to check that the IP address that you have entered responds to Ping requests.
7. Click the **Start Upgrade** button.

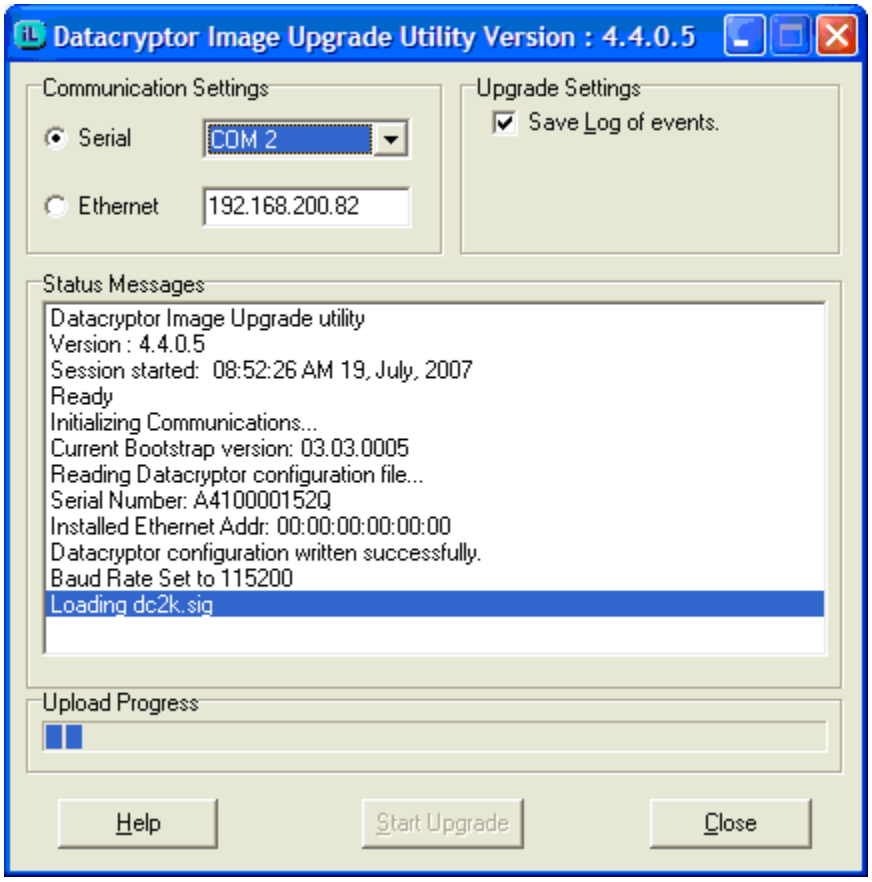
Note: The Image Loader utility will operate differently depending on whether you are using a serial or an Ethernet connection. Please use one of the next two sections, as appropriate to your type of connection.

Operations during Serial Code Loading

If you are using Ethernet loading, please refer to the next section.

1. The Image Loader will try to initialize communications with the Datacryptor. This will take a short time if the Datacryptor has no application loaded; the administrator may be prompted to remove the power and re-power up the Datacryptor. It is best to power down the unit by removing the mains power cable from the Power Supply Unit.
2. The message 'Current Bootstrap version xx.xx.xxxx' will be displayed in the status window when the Image Loader has successfully started talking to the bootstrap program in the Datacryptor.
3. After loading and re-initializing the bootstrap, a prompt will be given to select the Image Loader file (.ilf file) containing the Datacryptor application image (e.g. dc2k.ilf). Select the file and click **OK**. Image Loader files may also contain signed ACE images.

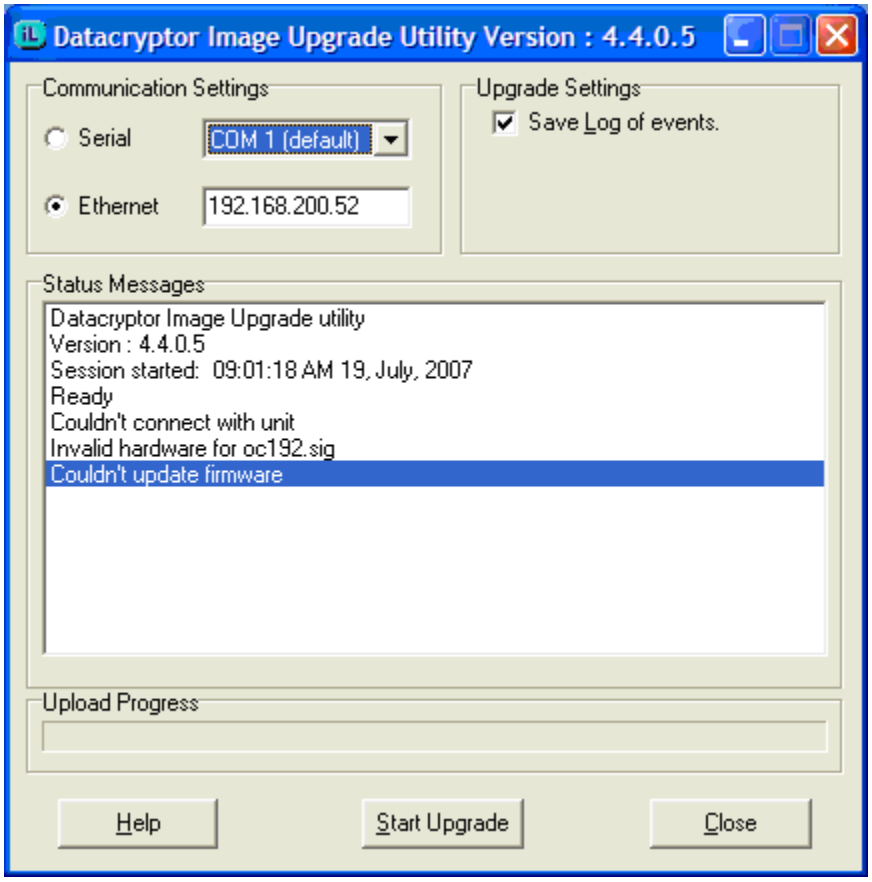
4. The Image Loader may also perform other "housekeeping" tasks such as generation of correct Ethernet address and IP addresses used by later software, if these are missing. If housekeeping tasks are performed, you will be notified in the Status Messages.
5. The baud rate at which the upload will take place is displayed, and the upload of the new application code will begin.



Operations during Ethernet Code Loading

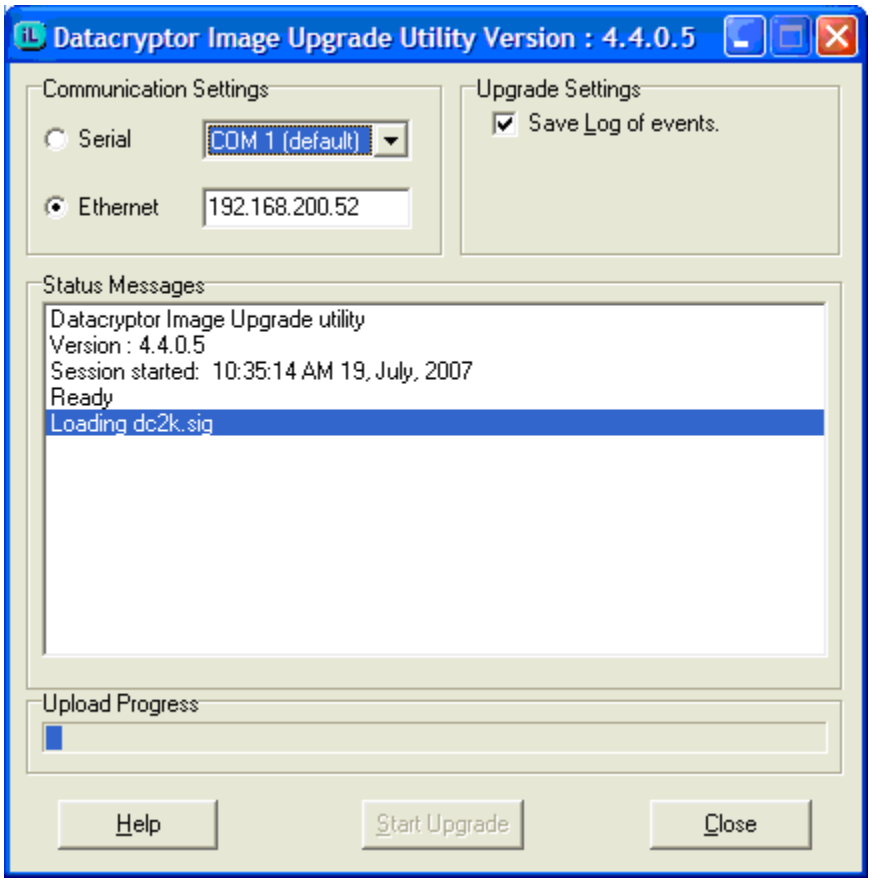
The following operations are only applicable if you are using an Ethernet connection for loading.

1. The Image Loader will try to initialize communications with the Datacryptor.



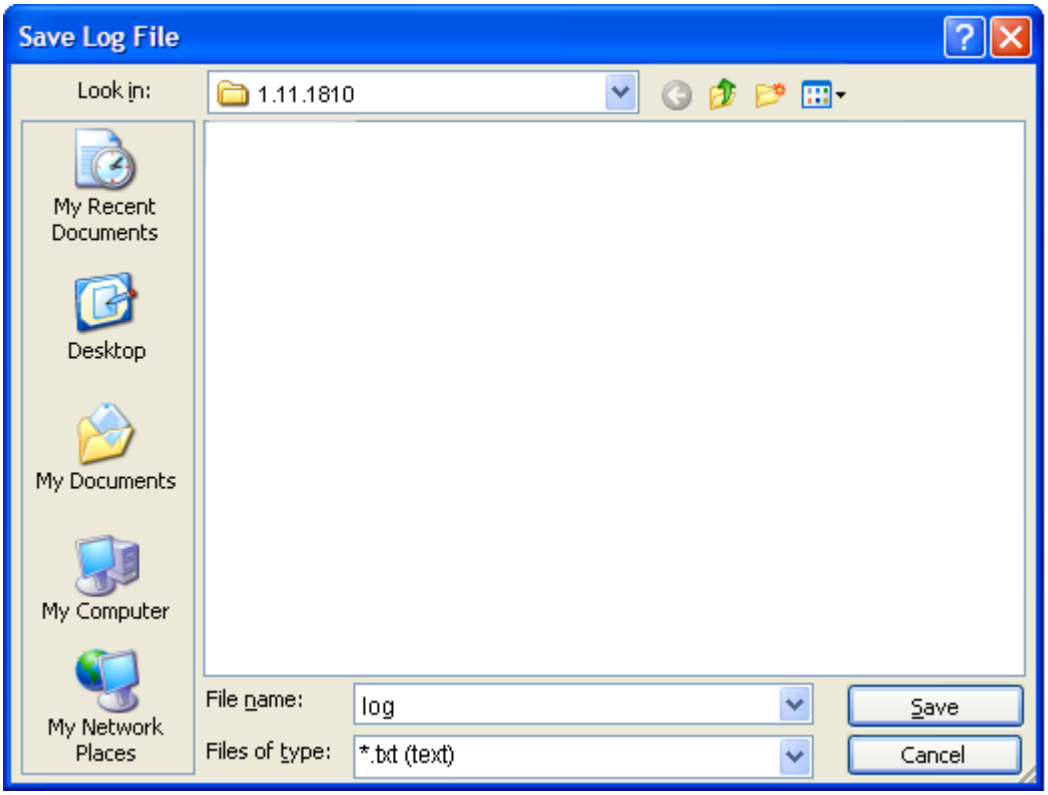
2. Once the hardware has been validated, select the Image Loader file (`.ilf` file) containing the Datacryptor application image (e.g. `dc2k.ilf`). Select the file and click **OK**.

3. Image Loader will begin uploading the code contained in the Image Loader file.



Completing the Upload

1. Progress of the load is shown via the Upload Progress bar and you will be notified when this is finished. If 'Save Log Events' was selected, a dialog will now prompt you for the file name and location for saving the log file.



2. Upload of the application is complete, click **Close** to shut down the application, or connect another Datacryptor for loading.
3. After the application has been loaded and the unit reboots, the algorithm will need to be loaded into the unit. See the section Commissioning for more information.

Note: Some algorithms may have to be loaded at the factory or under secure conditions.

Appendix C: Product Specifications

System Specifications

Interfaces	- Host and network ports (see Appendix E for transceiver details used with the 1 Gig and 10 Gig Ethernet Datacryptors) - 10/100 Mbps auto-sensing LAN port - RS-232C port
Electrical/Mechanical Dimensions	19 inch rack mount design 100-240 VAC, 10A, 50/60 Hz or -48 VDC **100 Mb Ethernet unit**: 100M: 44 mm H x 483 mm W (including mounting brackets) x 240 mm D (including connectors) 3.0 Kg 15 Watts power dissipation (typical) **1 Gig Ethernet unit**: 44 mm H x 483 mm W (including mounting brackets) x 388 mm D (including PSU fixed connector) 8.6 Kg 120 Watts power dissipation (typical) **10 Gig Ethernet unit**: 88 mm H x 483 mm W (including mounting brackets) x 420 mm D (including PSU fixed connector) 10.3 Kg 140 Watts power dissipation (typical)
Environmental	5 to 40 degrees C (40 to 104 degrees F) 10% to 90% at 25°C (77°F) non-condensing, failing to 50% maximum at 40°C (100°F)
Regulatory	See Appendix D
Certifications	Designed to FIPS 140-2 Level 3 compliance.

Appendix D: Environmental & Regulatory

Environmental Specifications

Description	Value
Temperature	5-40 degrees C (40 to 104 degrees F)
Humidity	10% to 90% at 25°C (77°F) non-condensing, failing to 50% maximum at 40°C (100°F)
Altitude	-200 - 10,000 feet AMSL operating altitude

Regulatory

Safety/Emissions/Immunity

IEC 60950, 3rd Edition (1999)	Underwriter Labs Safety
CSA-C22.2 No 60950-00	Canadian Safety
EN 60950	Safety for participating European nations
EN55022: 1998, ANSI C63.4:1992, AS/NZS 3548: 1997 with Amendments 1 and 2, CNS 13438:1997, and CAN/CSA-CISPR 2296	FCC Title 47, Part 15, Subpart B, EMC Directive 89/336/EEC and ICES-003
EN61000-3-2: 1995, EN61000-3-3: 1999	Harmonic Currents

EN61000-4-2: 1995	Electrostatic Discharge
EN61000-4-3: 1995	Radiated Immunity
EN61000-4-4: 1995	Electrical Fast Transient Burst
EN61000-4-5: 1995	Lightning Surge
EN61000-4-6: 1995	Conducted Disturbances
EN61000-4-11: 1995	Voltage Dips, Variations, and Short Interruptions

FCC Information (USA)

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Interference-Causing Equipment Standard Compliance Notice (Canada)

"This Class B digital apparatus meets all requirements of the Canadian-interference causing Regulations."

Cet appareil numérique de la classe B est respecte toutes les exigences du Règlement sur le matériel du Canada.

European Notice

Products with the CE Marking comply with both the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Appendix E: SFP and XFP Interfaces

The Datacryptor 1 Gig Ethernet unit is supplied with Small Form Factor Pluggable (SFP) interfaces (see above), using single-mode fiber or multi-mode fiber (MM SPF), as specified at the time of ordering. The 10 Gig Ethernet unit is supplied with 10 Gigabit Small Form Factor Pluggable (XFP) single-mode fiber laser devices (see below), as specified at the time of ordering.

The following multi-rate devices are supported:

- Copper RJ45

- 1310nm single-mode, short range
- 1310nm single-mode, intermediate range
- 1310nm single-mode, long range

- 1550nm single-mode, intermediate range
- 1550nm single-mode, long range
- 1550nm single-mode, long range, DWDM

Appendix F: Preventing Electrostatic Discharge

	Electrostatic discharge (ESD) can damage electronic components and equipment. ESD occurs when electronic components are improperly handled and can result in complete or intermittent failures. Always follow ESD-prevention procedures when removing and replacing components.

Use the following guidelines to prevent ESD damage:

- Always use an ESD wrist or ankle strap and ensure that it makes skin contact.
- Connect the equipment end of the strap to an unpainted metal chassis surface.
- If no wrist strap is available ground yourself by touching the metal chassis.

Appendix G: Troubleshooting

This appendix is provided to aid you in determining basic problems with your Thales Datacryptor Ethernet unit. If you cannot resolve the problem using this troubleshooting guide, please contact Thales customer support.

Possible Problems and Solutions

The troubleshooting information in this section is grouped into the following categories: logging in, configuration and traffic flow. Within each category you will find a list of symptoms and possible solutions.

Logging In

Symptom	Explanation and Possible Solutions
Boot Process Fails	Contact Thales support for advice
Administrator password is forgotten or lost	Contact Thales for service
Not able to connect to the CLI	Re-boot the unit Log out of the Element Manager application. Check the Baud rate settings are set to: 115200, 8, N, 1
Not able to log in to the Front Panel Viewer	Verify the password

Configuration

Symptom	Explanation and Possible Solutions
Datacryptor does not recognize its new IP address	Verify the IP address using the Element Manager (see The IP Management tab section above). Correct the IP address if necessary, save the configuration, and then reboot the Datacryptor.
The management workstation can't communicate with the Datacryptor	Verify that the network connection to the management port is in place (see the Connect the Cables section above). Check the management interface default gateway configuration. Assign a default gateway if the management workstation is on a different subnet than the Datacryptor's management port.
Datacryptor is not sending SNMP objects to the management workstation	Ensure that SNMP traps are enabled. Verify that the management workstation's IP address is configured as the SNMP trap host address. See the Configuring SNMP section.

Cannot establish a link	Check physical connectivity to ensure proper signal path. If using a 1 Gig or 10 Gig Ethernet Datacryptor, verify that compatible SFPs and fiber type is being used for connectivity. Use the loopback mode to test the connections, see *The Diagnostics Tab* on page 59.

Traffic Flow

Symptom	Explanation and Possible Solutions
Traffic is not being passed	Verify that the Host and Network port transceivers (1 Gig and 10 Gig Ethernet Datacryptors only) and the cables are properly seated. Use the Ping Peer unit on the Ethernet encryption tab to confirm connectivity. Use the loopback mode to test the connections, see *The Diagnostics Tab* on page 59.

Fan/Heat Monitor Alarm

Symptom	Explanation and Possible Solutions
Fan/Heat Monitor Alarm	Consult the Environment tab on the Properties dialog for readings of the fan speeds and unit temperature. Compare these readings to those recorded during normal operation to determine the nature of the problem. Verify that nothing has become inserted in the fan or ventilation holes which could restrict the fan operation or airflow. In a normal working environment i.e. setup in accordance with the rack mounting instructions the unit is able to function correctly with a fan or fans disabled. If the condition persists then it could indicate that the temperature is above the level required for reliable operation and the unit should be returned to Thales for investigation/Repair.

Appendix H: SNMP MIB Support

In order to support organizations who utilize SNMP to monitor network devices and status, the Datacryptor Ethernet product does provide a Simple Network Management Protocol Version 3 (SNMPv3) and Management Information Base II (MIB-II) interface.

The SNMPv3 implementation is based upon RFCs 1157, 1901–1910, 2576, 2578 – 2580, and 3411–3418. The MIB II interface is based upon RFCs 1213, 2011, 2013, 2096, 2665, 2863, and 3417. All MIB files provided with this product are SMIv2 compliant.

Because the Datacryptor Ethernet is a security device, the SNMPv3 implementation in the Datacryptor Ethernet is more restrictive than specified in the standard RFCs listed above. In general, we have disabled most of the SET operations in order to protect critical security parameters, configuration items, and device attributes.

Where the device SNMPv3 implementation has deviated from a RFC specification, we have provided an updated RFC MIB files reflecting those changes.

Supported MIBs are listed in the table below:

MIB Name	Description
DC2K-MIB-R4	SMIv2 compliant MIB file containing Thales e-Security enterprise specific values. This MIB is used as the parent for all other MIB files, except the RFC MIB files. Please see the supplied MIB file for specific details.
DC2K-MIB-ETHERNET	SMIv2 compliant MIB file containing Thales e-Security enterprise specific values for the Ethernet units. Please see the supplied MIB file for specific details.
DC2K-TRAP-ETHERNET	SMIv2 compliant MIB file containing Thales e-Security enterprise specific trap values for the Ethernet units. Please see the supplied MIB file for specific details.
DC2K-MIB-SONET	SMIv2 compliant MIB file containing Thales e-Security enterprise specific values for the SONET units. Please see the supplied MIB file for specific details.
DC2K-TRAP-SONET	SMIv2 compliant MIB file containing Thales e-Security enterprise specific trap values for the SONET units. Please see the supplied MIB file for specific details.

MIB Name	Description
DC2K-MIB-RFC1213	RFC 1213 defines the Management Information Base (MIB-II) for use with network management protocols in TCP/IP-based internets. The Datacryptor supports the majority of read-write attributes in this MIB as read-only in order to preserve the security of sensitive attributes. The Datacryptor does not support TCP communications and EGP operations, and as such, the device will not support any SNMP operations involving the TCP or EGP groups of RFC 1213. Please see the supplied MIB file for specific details.
DC2K-MIB-RFC1317	RFC 1317 defines a portion of the Management Information Base (MIB-II). Specifically, it defines objects for the management of RS-232-like devices. The Datacryptor supports the majority of read-write attributes in this MIB as read-only in order to preserve the security of sensitive attributes. Please see the supplied MIB file for specific details.
DC2K-MIB-RFC1907	RFC 1907 defines a portion of the Management Information Base (MIB-II). Specifically, it defines the new SNMPv2 framework and the associated MIB objects. The Datacryptor supports the majority of read-write attributes in this MIB as read-only in order to preserve the security of sensitive attributes. The Datacryptor does not support the sysOR table entries of this RFC. Please see the supplied MIB file for specific details.
DC2K-MIB-RFC2011	RFC 2011 defines a portion of the Management Information Base (MIB-II). Specifically, it updates various MIB-II objects for use within a SNMPv2 framework. The Datacryptor supports the majority of read-write attributes in this MIB as read-only in order to preserve the security of sensitive attributes. Please see the supplied MIB file for specific details.

MIB Name	Description
DC2K-MIB-RFC2863	RFC 2863 defines a portion of the Management Information Base (MIB-II). Specifically, it defines objects for the management of network interfaces. The Datacryptor supports the majority of read-write attributes in this MIB as read-only in order to preserve the security of sensitive attributes. Please see the supplied MIB file for specific details.
DC2K-MIB-RFC3413	RFC 3413 defines a portion of the Management Information Base (MIB-II). Specifically, it defines five types of Simple Network Management Protocol (SNMP) applications which make use of an SNMP engine as described in STD 62, RFC 3411. SNMP target host tables are neither creatable nor modifiable through the SNMP interface. Modification of these attributes is only supported through the Datacryptor Front Panel Viewer (FPV) application. Please see the supplied MIB file for specific details.
DC2K-MIB-RFC3418	RFC 2863 defines a portion of the Structure of Management Information (SMIv2). The Datacryptor supports the majority of read-write attributes in this MIB as read-only in order to preserve the security of sensitive attributes. Please see the supplied MIB file for specific details.
DC2K-MIB-RFC3584	RFC 3584 defines objects to support compatibility between SNMPv1, v2, and v3. The Datacryptor supports the majority of read-write attributes in this MIB as read-only in order to preserve the security of sensitive attributes. Additionally, we removed references to snmpTargetAddrExtTable and associated objects as they are not supported in the Datacryptor product. Please see the supplied MIB file for specific details.

Appendix I: Log and SNMP Trap Numbers

The following table lists the log messages that may be viewed in the Datacryptor log and the corresponding SNMP trap messages that may be generated.

The log/trap messages are listed in the Log type order Error, Key followed by Audit. The log number is the log number of the message when viewed in the logs by the Front Panel Viewer. The Trap number is the number of the trap reported to SNMP network managers. The message is the actual string seen in the log file. The information is additional background to help understand what has occurred if it is not clear.

There are a large number of messages that are identical, these have different log and trap numbers to help support staff further identify and investigate the actual cause of the log entry.

There are a number of log/trap message numbers, usually failures, that have the same text; this is because the effect the user experiences can be caused by subtly different internal events occurring. Logging these events differently can help Thales e-Security diagnose complex support issues.

Standard Traps

Message	Trap No.	Information
coldStart	0	Issued when the Datacryptor is powered up for the first time or whenever it is power cycled other than by the application.
warmStart	1	Issued when the Datacryptor is restarted by its application.
linkDown	2	Issued when either the host or network interfaces is detected as being down. This might be due to Loss of Signal.
LinkUp	3	Issued when either the host or network interfaces is detected as being up.
authenticationFailure	4	Issued when an attempt is made to access the Datacryptor SNMP interface using an unknown community name or a community name without the correct access level.

The log messages are detailed on the following pages in this order:

Log Trap Errors Hardware

Log Type	Code	Trap No.	Severity	Message	Information
Error (Hardware)	1	120	Critical	Random no. generator fault	
Error (Hardware)	2	120	Critical	Real time clock faulty	
Error (Hardware)	3	120	Critical	RAM faulty	
Error (Hardware)	4	120	Critical	Encrypt Clock Limit Exceeded	Line clock is too fast for the unit
Error (Hardware)	5	120	Critical	Decrypt Clock Limit Exceeded	Line clock is too fast for the unit
Error (Hardware)	6	120	Critical	Encrypt Clock Stopped	
Error (Hardware)	7	120	Critical	Decrypt Clock Stopped	
Error (Hardware)	8	120	Critical	Battery may need replacing	Battery may be more than 10 years old or exhibiting symptoms of low voltage
Error (Hardware)	9	120	Critical	Random Number Generator diagnostics Failed	
Error (Hardware)	10	120	Critical	Continuous Random Number Generator test failed	
Error (Hardware)	11	120	Critical	Real Time Clock not set: set or check battery	
Error (Hardware)	12	120	Critical	Hardware Monitor reports alarm	This can be due to fan, heat or power failure. Note that power failure is reported separately.
Error (Hardware)	13	120	Critical	Power Monitor reports alarm	

Log Type	Code	Trap No.	Severity	Message	Information
Error (Hardware)	14	122	Major	Alarm condition: movement alarm activated	Unit recovered from alarm and noted movement alarm had been activated: it will be necessary to reboot the unit. If alarm persists contact Thales esecurity support
Error (Hardware)	15	122	Major	Alarm condition: temperature alarm activated	Unit recovered from alarm and noted temperature alarm had been activated: it will be necessary to reboot the unit. If alarm persists contact Thales esecurity support
Error (Hardware)	16	122	Major	Alarm condition: erase button activated	Unit recovered from alarm and noted erase button alarm had been activated: it will be necessary to reboot the unit. If alarm persists contact Thales esecurity support
Error (Hardware)	17	122	Major	Alarm condition: battery low	Unit recovered from alarm and noted that the battery low alarm had been activated: it will be necessary to reboot the unit. If alarm persists contact Thales e-security support
Error (Hardware)	18	122	Major	Alarm condition: secure memory was erased	Unit recovered from alarm and noted intrusion detection alarm had been activated: it will be necessary to reboot unit. If alarm persists contact Thales e-security support
Error (Hardware cleared)	1	121	Minor	Random no. gen. fault clear	Random number generator "fault" cleared
Error (Hardware cleared)	2	121	Minor	Real time clock fault clear	Real time clock fault cleared
Error (Hardware cleared)	3	121	Minor	RAM fault cleared	RAM fault cleared
Error (Hardware cleared)	4	121	Minor	Encrypt Clock Now in Range	Encrypt clock fault cleared

Log Type	Code	Trap No.	Severity	Message	Information
Error (Hardware cleared)	5	121	Minor	Decrypt Clock Now in Range	Decrypt clock fault cleared
Error (Hardware cleared)	6	121	Minor	Encrypt Clock Restarted	Encrypt clock fault cleared
Error (Hardware cleared)	7	121	Minor	Decrypt Clock Restarted	Decrypt clock fault cleared
Error (Hardware cleared)	8	121	Minor	Battery state is OK	Battery fault cleared
Error (Hardware cleared)	9	121	Critical	Random Number Generator diagnostics cleared	
Error (Hardware cleared)	10	121	Critical	Continuous Random Number Generator test cleared	
Error (Hardware cleared)	12	121	Critical	Hardware Monitor reports all clear	
Error (Hardware cleared)	13	121	Critical	Power Monitor reports all clear	

Log Trap Errors Software

Log Type	Code	Trap No.	Severity	Message	Information
Error (Software)	1	153	Critical	Trace error	
Error (Software)	2	153	Critical	Exec failure	
Error (Software)	3	153	Critical	System panic	
Error (Software)	4	153	Critical	Internal software error	
Error (Software)	5	153	Critical	Internal software error	
Error (Software)	6	153	Critical	Internal software error	
Error (Software)	7	153	Critical	Internal software error	
Error (Software)	8	153	Critical	Internal software error	

Log Type	Code	Trap No.	Severity	Message	Information
Error (Software)	9	153	Warning	Corrupt Log text entries	
Error (Software)	11	153	Warning	Inconsistent Log error counts	
Error (Software)	12	153	Warning	Inconsistent Log name entries	
Error (Software)	13	153	Warning	Blank name entries in Log	
Error (Software)	19	839	Major	Algorithm version not supported by this application version	User has tried to load incorrect version of algorithm
Error (Software)	20	1849	Major	Destination selector table full	
Error (Software)	21	1850	Major	Source selector table full	
Error (Software)	22	1851	Major	Security Policy table full	
Error (Software)	23	153	Critical	SRAM Corruption has been detected	
Error (Software)	24	153	Critical	SHA-1 Known Answer Test failed	
Error (Software)	25	153	Critical	SHA-1 RNG Known Answer Test failed	
Error (Software)	27	153	Warning	SNMP Agent Error	

Key Errors

Log Type	Code	Trap No.	Severity	Message	Information
Key	0	200	Warning	No response from peer	No response from peer when waiting for Key exchange request - connection may be lost or units may be busy Key
Key	1	201	Major	No common DEK algorithm	Units do not have common symmetric encryption algorithm and so do not continue negotiation
Key	2	202	Warning	DEK exchange unsuccessful	DEK response did not match challenge - Diffie-Hellman parameters may be mismatched
Key	3	203	Minor	DEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	4	204	Minor	DEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	5	205	Minor	DEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	6	206	Minor	DEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	7	207	Minor	DEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	8	208	Minor	DEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	9	209	Minor	DEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	10	210	Minor	DEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy

Log Type	Code	Trap No.	Severity	Message	Information
Key	11	211	Minor	DEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	12	212	Minor	DEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	13	213	Minor	KEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	14	214	Minor	KEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	15	215	Minor	KEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	16	216	Minor	KEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	17	217	Minor	KEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	18	218	Minor	KEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	19	219	Minor	KEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	20	220	Major	No common KEK algorithm	Units do not have common KEK algorithm and so do not continue negotiation
Key	21	221	Minor	KEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	22	222	Minor	KEK exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy

Log Type	Code	Trap No.	Severity	Message	Information
Key	23	223	Minor	Certificate exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	24	224	Minor	Certificate exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	25	225	Minor	Certificate exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	26	226	Minor	Certificate exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	27	227	Major	Peer has no own (unit) certificates installed	Generated by master unit when attempting to perform a Key Exchange with a non-commissioned unit slave unit
Key	28	228	Major	Diffie-Hellman parameters do not match	Generated at Unsuccessful attempt to generate a KEK, due to no matching Diffie- Hellman parameters
Key	29	229	Major	No own (unit) certificate installed	Generated by slave unit when a master unit is attempting to perform a Key Exchange. The slave unit does not contain a valid Key set
Key	30	230	Major	No common certificates	Unit does not contain a "matching" certificate that can be used to authenticate and communicate with remote unit
Key	31	231	Minor	Certificate exchange unsuccessful	Generated by master unit when attempting to perform a Key Exchange with a unit slave which does not contain "matching" certificate that can be used to authenticate and communicate with remote unit

Log Type	Code	Trap No.	Severity	Message	Information
Key	32	232	Minor	Certificate exchange unsuccessful	Generated by master unit when attempting to perform a Key Exchange with a unit slave which is with an invalid certificate
Key	33	233	Minor	Certificate exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	34	234	Minor	Certificate exchange unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	39	235	Warning	Could not delete CA	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	40	236	Warning	Commissioning unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	41	237	Warning	Commissioning unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	42	238	Warning	Commissioning unsuccessful	Unexpected time out in key exchange - connection may be lost or units may be busy
Key	44	239	Informational	Management session already in progress	Unit busy
Key	45	240	Warning	Key exchange already in progress	Key exchange process is busy - the unit must try again later
Key	46	241	Warning	Key exchange already in progress	Key exchange process is busy - the unit must try again later
Key	47	242	Minor	Unknown/missing error	View units logs for more information
Key	49	243	Major	Failed to set peer's mode	
Key	50	244	Major	Failed to set peer's mode	
Key	51	245	Major	DEK installation failed	A key used to encrypt/decrypt manager/unit communications keys failed when loading

Log Type	Code	Trap No.	Severity	Message	Information
Key	52	246	Major	Failed to set line mode	Conditions are not met to enter encryption mode
Key	53	247	Major	Receive and transmit keys are identical	Receive and transmit keys are identical
Key	54	254	Major	No KEK algorithm loaded, or it is operating incorrectly	Failed KEK Known Answer Test
Key	55	255	Major	No DEK algorithm loaded, or it is operating incorrectly	Failed DEK Known Answer Test
Key	56	256	Major	No CA algorithm loaded, or it is operating incorrectly	Failed CA Known Answer Test
Key	57	257	Major	No common Red KEK between this unit and the peer	Load valid key material into the units, check unit date and time.
Key	58	258	Minor	DEK exchange unsuccessful	
Key	59	259	Minor	DEK exchange unsuccessful	
Key	60	260	Minor	DEK exchange unsuccessful	
Key	61	261	Minor	DEK exchange unsuccessful	
Key	62	262	Minor	DEK exchange unsuccessful	
Key	63	263	Minor	DEK exchange unsuccessful	
Key	64	264	Minor	DEK exchange unsuccessful	
Key	65	265	Minor	DEK exchange unsuccessful	
Key	66	266	Minor	Failed to create DEK	
Key	67	267	Minor	Failed to create KEK	
Key	68	268	Minor	Failed to encode private network	
Key	69	269	Minor	Failed to decode peer's private network	
Key	70	270	Major	Failed to store selector	
Key	71	849	Major	Destination selector table full	
Key	72	850	Major	Source selector table full	
Key	73	851	Major	Security Policy table full	
Key	74	271	Major	Key exchange with peer denied due to ACL	
Key	125	810	Major	RIP password does not match password in oncoming RIP message	
Key	126	811	Major	Expecting an authorisation entry in RIP message	

Log Type	Code	Trap No.	Severity	Message	Information
Key	904	895	Informational	Key Material erased	
Key	1000	500	Warning	Peer reported no response from us?	This may indicate an addressing error
Key	1001	501	Warning	Peer reported no common DEK algorithm	
Key	1002	502	Warning	Peer reported DEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1003	503	Warning	Peer reported DEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1004	504	Warning	Peer reported DEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1005	505	Warning	Peer reported DEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1006	506	Warning	Peer reported DEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1007	507	Warning	Peer reported DEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1008	508	Warning	Peer reported DEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1009	509	Warning	Peer reported DEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1010	510	Warning	Peer reported DEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1011	511	Warning	Peer reported DEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy

Log Type	Code	Trap No.	Severity	Message	Information
Key	1012	512	Warning	Peer reported DEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1013	513	Warning	Peer reported KEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1014	514	Warning	Peer reported KEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1015	515	Warning	Peer reported KEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1016	516	Warning	Peer reported KEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1017	517	Warning	Peer reported KEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1018	518	Warning	Peer reported KEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1019	519	Warning	Peer reported KEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1020	520	Warning	Peer reported KEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1021	521	Warning	Peer reported KEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1022	522	Warning	Peer reported KEK exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1023	523	Warning	Peer reported Certificate exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy

Log Type	Code	Trap No.	Severity	Message	Information
Key	1024	524	Warning	Peer reported Certificate exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1025	525	Warning	Peer reported Certificate exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1026	526	Warning	Peer reported Certificate exchange unsuccessful	Unexpected time out in key exchange – connection may be lost or units may be busy
Key	1027	527	Minor	Peer reported we have no own (unit) certificates installed	
Key	1028	528	Major	Peer reported Diffie-Hellman parameters do not match	
Key	1029	529	Minor	Peer reported it has no own (unit) certificate installed	
Key	1030	530	Major	Peer reported no common certificates	
Key	1031	531	Warning	Peer reported Certificate exchange unsuccessful	Unexpected time out in protocol – connection may be lost or units may be busy
Key	1032	532	Warning	Peer reported Certificate exchange unsuccessful	Unexpected time out in protocol – connection may be lost or units may be busy
Key	1033	533	Warning	Peer reported Certificate exchange unsuccessful	Unexpected time out in protocol – connection may be lost or units may be busy
Key	1034	534	Warning	Peer reported Certificate exchange unsuccessful	View units peer logs for more information
Key	1039	539	Warning	Peer reported commissioning unsuccessful	Unexpected time out in protocol – connection may be lost or units may be busy
Key	1040	540	Warning	Peer reported commissioning unsuccessful	Unexpected time out in protocol – connection may be lost or units may be busy
Key	1041	541	Warning	Peer reported commissioning unsuccessful	Unexpected time out in protocol – connection may be lost or units may be busy

Log Type	Code	Trap No.	Severity	Message	Information
Key	1042	542	Warning	Peer reported commissioning unsuccessful	Unexpected time out in protocol – connection may be lost or units may be busy
Key	1044	544	Minor	Management Session already in progress	
Key	1045	545	Major	Peer reported key exchange already in progress	Key exchange process is busy – the unit must try again later
Key	1046	546	Minor	Peer reported key exchange already in progress	Key exchange process is busy – the unit must try again later
Key	1047	547	Major	Peer reported an unknown/missing error	View unit logs for more information
Key	1049	549	Warning	Failed to set peer's mode	
Key	1050	550	Warning	Failed to set peer's mode	
Key	1051	551	Major	PEER DEK installation failed	
Key	1052	552	Major	PEER Failed to set line mode	
Key	1053	553	Major	PEER Receive and transmit keys are identical	
Key	1054	554	Major	Peer has no KEK algorithm loaded, or it is operating incorrectly	PEER Failed KEK Known Answer Test
Key	1055	555	Major	Peer has no DEK algorithm loaded, or it is operating incorrectly	PEER Failed DEK Known Answer Test
Key	1056	556	Major	Peer has no CA algorithm loaded, or it is operating incorrectly	PEER Failed CA Known Answer Test
Key	1057	557	Minor	Peer reported No common Red KEK between this unit and the peer	Load valid key material into the units, check unit date and time.
Key	1058	558	Minor	Peer reported DEK exchange unsuccessful	
Key	1059	559	Minor	Peer reported DEK exchange unsuccessful	
Key	1060	560	Minor	Peer reported DEK exchange unsuccessful	
Key	1061	561	Minor	Peer reported DEK exchange unsuccessful	
Key	1062	562	Minor	Peer reported DEK exchange unsuccessful	

Log Type	Code	Trap No.	Severity	Message	Information
Key	1063	563	Minor	Peer reported DEK exchange unsuccessful	
Key	1064	564	Minor	Peer reported DEK exchange unsuccessful	
Key	1065	565	Minor	Peer reported DEK exchange unsuccessful	
Key	1066	566	Minor	Peer reported failed to create DEK	
Key	1067	567	Minor	Peer reported failed to create KEK	
Key	1068	568	Minor	Peer reported failed to encode private network	
Key	1069	569	Minor	Peer reported failed to decode our private network	
Key	1074	571	Major	Peer reported key exchange with peer denied due to ACL	
Key	2000	600	Informational	Line mode changed	
Key	2001	601	Informational	DEK installed	
Key	2002	602	Informational	KEK installed	
Key	2003	603	Informational	Installed CA certificate	
Key	2004	604	Informational	Expired CA certificate	
Key	2005	605	Informational	Removed CA certificate	
Key	2006	606	Informational	Installed unit certificate	
Key	2007	607	Informational	Expired unit certificate	
Key	2008	608	Informational	Removed unit certificate	
Key	2009	609	Informational	Installed peer certificate	
Key	2010	610	Informational	Expired peer certificate	
Key	2011	611	Informational	Removed peer certificate	
Key	2012	612	Informational	Standby mode set	
Key	2013	613	Informational	Plain mode set	
Key	2014	614	Informational	Encrypt mode set	
Key	2015	615	Informational	Previous unit name	Unit name Changed, Previous unit name
Key	2016	606	Informational	New unit name	Unit name Changed, New unit name
Key	2017	617	Informational	New DEK exchanged	

Log Type	Code	Trap No.	Severity	Message	Information
Key	2018	618	Minor	No Encrypt channel is available	The maximum number of encrypt slots has been reached.
Key	2019	619	Informational	DLCI has become Active (LMI)	
Key	2020	620	Informational	DLCI has become Inactive (LMI)	
Key	2021	621	Informational	Red KEK installed	
Key	2022	622	Informational	Red KEK deleted	
Key	2023	623	Informational	Red Key mode started	
Key	2024	624	Informational	Red Key mode stopped	
Key	2025	625	Informational	CA algorithm loaded	
Key	2026	626	Informational	Key exchange algorithm loaded	
Key	2027	627	Informational	KEK algorithm loaded	
Key	2028	628	Informational	DEK algorithm loaded	
Key	2029	629	Informational	Symmetric algorithm loaded	
Key	2030	630	Informational	CA algorithm load failed	
Key	2031	631	Informational	Key exchange algorithm load failed	
Key	2032	632	Informational	KEK algorithm load failed	
Key	2033	633	Informational	DEK algorithm load failed	
Key	2034	624	Informational	Symmetric algorithm load failed	
Key	2035	635	Informational	All KEKs deleted	
Key	2036	636	Informational	Peer's KEKs deleted	
Key	2037	637	Informational	Single KEK deleted	
Key	2038	638	Informational	Initialised access control password	
Key	2039	639	Minor	Tunnel SA added by Peer	
Key	2040	640	Minor	Transport SA added by peer	
Key	2041	641	Minor	Trunk SA added by Peer	Trunk Mode not supported by Datacryptor AP
Key	2042	642	Minor	SA set to Tunnel by Peer	
Key	2043	643	Minor	SA set to Transport by Peer	

Log Type	Code	Trap No.	Severity	Message	Information
Key	2044	644	Minor	SA set to Trunk by Peer	Trunk Mode not supported by Datacryptor AP
Key	2045	645	Minor	SA mismatch use Tunnel	
Key	2046	646	Minor	SA mismatch use Transport	
Key	2047	647	Minor	SA mismatch use Trunk	Trunk Mode not supported by Datacryptor AP
Key	2048	648	Minor	Tunnel SA deleted by Peer	
Key	2049	649	Minor	Transport SA deleted by Peer	
Key	2050	650	Minor	Trunk SA deleted by Peer	Trunk Mode not supported by Datacryptor AP
Key	2051	651	Minor	Peer deleting non-existent SA	
Key	2052	798	Informational	IP Transport SA with duplicate peer unit name removed	
Key	2053	800	Informational	IP Tunneling SA with duplicate peer unit name removed	
Key	2054	799	Informational	IP Trunk Protocol SA with duplicate peer unit name removed	Trunk Mode not supported by Datacryptor AP
Key	2055	801	Informational	Peers private network information updated	
Key	2056	656	Minor	NUA added by peer	
Key	2057	657	Minor	NUA deleted by peer	
Key	2058	658	Minor	Peer delete Non-existent NUA	
Key	2059	659	Minor	Failed to Delete NUA in Peer Unit	
Key	2060	871	Minor	Failed to add SA to Peer Unit, Peer has Auto-Notify disabled	
Key	2061	872	Minor	Failed to Delete SA from non-Auto-Notify Peer unit	
Key	2062	873	Minor	Peer Failed to Delete SA, Auto-Notify is Disabled	
Key	2063	874	Minor	Peer Failed to Add SA, add bit not set	

Log Type	Code	Trap No.	Severity	Message	Information
Key	2064	875	Minor	Peer Failed to Add SA, Auto-Notify is Disabled	
Key	2065	876	Minor	SA is Offline, Peer Unit has different SA Mode	
Key	2066	877	Minor	SA is Offline, SA is missing from Peer Unit	
Key	2067	878	Minor	Stalled Key Exchange/Installation Abandoned	
Key	2068	879	Minor	Stalled Key Exchange/Installation Abandoned	
Key	2069	880	Minor	Stalled Key Exchange/Installation Abandoned	
Key	2070	888	Informational	Removed peer certificate by ACL	
Key	2071	889	Informational	Peer's KEKs deleted	

Audit Errors

Log Type	Code	Trap No.	Severity	Message	Information
Audit	1	701	Informational	Session started	User has successfully logged into unit
Audit	2	702	Informational	Session stopped	User has logged off
Audit	3	703	Informational	Session stopped - lost contact with host	Session has been terminated, user unable to communicate with unit
Audit	4	704	Informational	Viewed logs	User is viewing the logs
Audit	5	705	Informational	General configuration updated	User has altered either unit Time/Date or interface settings
Audit	6	706	Informational	Security configuration updated	User has altered either KEK lifetime, DEK Lifetime Change DEK with KEK option setting, Movement or Temp alarm status, Erase Button Key requirement
Audit	7	707	Informational	Serial port configuration updated	User has altered one of the control port parameters This could be either Baud Rate, Data Bits, Parity or Stop Bit values
Audit	8	708	Informational	IP management configuration updated	User has altered the IP address
Audit	9	709	Informational	Comms configuration updated	
Audit	10	710	Informational	T1 configuration updated	
Audit	11	711	Informational	E1 configuration updated	
Audit	12	712	Informational	Line test configuration updated	
Audit	13	713	Informational	Date/time before update	Unit time at time of time/date change, with respect to new time
Audit	14	714	Informational	Date/time after update	Unit time at time of time/date change, with respect to old time
Audit	15	715	Informational	Reboot unit	Unit Soft Rebooted
Audit	16	716	Informational	Initiate diagnostic test	
Audit	17	717	Informational	Standby mode configured	
Audit	18	718	Informational	Plain mode configured	

Log Type	Code	Trap No.	Severity	Message	Information
Audit	19	719	Informational	Encrypt mode configured	
Audit	20	720	Informational	Standby mode configured by peer	
Audit	21	721	Informational	Plain mode configured by peer	
Audit	22	722	Informational	Encrypt mode configured by peer	
Audit	23	723	Major	System startup	
Audit	24	724	Informational	Logs cleared	
Audit	25	725	Informational	DLCI configuration updated	
Audit	26	726	Informational	DCLI target configuration updated	
Audit	27	727	Informational	E1 timeslot configuration updated	
Audit	28	728	Informational	T1 timeslot configuration updated	
Audit	29	729	Major	Failed to confirm setting peer encrypt mode	
Audit	30	730	Major	Failed to confirm setting peer plain mode	
Audit	31	731	Major	Failed to confirm setting peer standby mode	
Audit	32	732	Informational	Timeslot to Bundle assignment changed	
Audit	33	816	Minor	Unknown NUA Logged	
Audit	34	817	Minor	X.25 DTE Link Restart	
Audit	35	818	Minor	X.25 DCE Link Restart	
Audit	36	819	Minor	X.25 DTE Link Up	
Audit	37	820	Minor	X.25 DCE Link Up	
Audit	38	821	Minor	X.25 DTE Link Down	
Audit	39	822	Minor	X.25 DCE Link Down	
Audit	40	823	Minor	Peer NUA Added	
Audit	41	824	Informational	Peer NUA Deleted	
Audit	42	825	Informational	Units own NUA Set	
Audit	43	826	Informational	Bar Unknown NUA's	
Audit	44	827	Informational	Accept Unknown NUA's	
Audit	45	828	Informational	Units own NUA learnt	

Log Type	Code	Trap No.	Severity	Message	Information
Audit	46	733	Major	Keylock moved to Transport	
Audit	47	734	Major	Keylock moved from Transport	
Audit	48	735	Major	Keylock moved to Erase	
Audit	49	736	Major	Keylock moved from Erase	
Audit	50	744	Informational	Tunnel SA Added	
Audit	51	745	Informational	Transport SA Added	
Audit	59	746	Informational	Set Private Network	
Audit	60	747	Informational	Set Private Address	
Audit	61	748	Informational	Set Public Address	
Audit	62	749	Informational	Default mode is Discard	
Audit	63	750	Informational	Default mode is Passthrough	
Audit	64	751	Informational	Trunk SA Added	Trunk Mode not supported by Datacryptor AP
Audit	65	752	Informational	Tunnel SA Deleted	
Audit	66	753	Informational	Transport SA Deleted	
Audit	67	754	Informational	Trunk SA Deleted	Trunk Mode not supported by Datacryptor AP
Audit	68	788	Informational	Force Standby on boot cleared	
Audit	69	756	Informational	Key Algorithms stored in backup memory	
Audit	70	757	Informational	Key Algorithms recovered from backup	
Audit	71	758	Critical	Random No. Generator diagnostics FAILED	This may be a "statistical fail, i.e. as it is a random number generator it may fail the tests occasionally, it is normally expected to recover
Audit	72	759	Critical	Random No. Generator diagnostics RECOVERED	
Audit	73	760	Major	Primary mode failure: No response from Private known IP address	Hot standby unit detected possible disconnection from private network
Audit	74	761	Major	Primary Mode Failure: No response from Public known IP address	Hot standby unit detected possible disconnection from public network

Log Type	Code	Trap No.	Severity	Message	Information
Audit	75	762	Critical	Primary mode reboot: KAT test failure	The encryption algorithm failed a "Known Answer Test" (KAT) and has caused the unit to reboot to attempt to recover.
Audit	76	763	Critical	Secondary mode reboot: KAT test failure	The encryption algorithm failed a "Known Answer Test" (KAT) and has caused the unit to reboot to attempt to recover.
Audit	77	764	Major	Hot Standby reboot: FPGA stats mismatch	Hot standby unit has detected a possible problem with the encryption device and has caused the unit to reboot to attempt to recover.
Audit	78	765	Major	Hot Standby reboot: No response from Private CR	Hot standby unit may have detected problem with Host (Private) port Ethernet interface which appears to have stopped responding and has caused the unit to reboot to attempt to recover
Audit	79	766	Major	Hot Standby reboot: No response from Public CR	Hot standby unit may have detected problem with Network (Public) port Ethernet interface which appears to have stopped responding and has caused the unit to reboot to attempt to recover
Audit	80	767	Major	Hot Standby reboot: Failed to change IP address	Hot Standby unit: changing of an IP address appears to have failed and has caused the unit to reboot to attempt to recover
Audit	81	768	Major	Detected Primary failure: No response from Public virtual IP address	Secondary unit has detected Primary unit failure on Network (public) port side
Audit	82	769	Major	Detected primary failure: No response from Private virtual IP address	Secondary unit has detected Primary unit failure on Host (private) port side
Audit	83	770	Major	Primary: Response back from Public virtual IP address	Hot standby: primary unit has detected itself, probable configuration error on public side

Log Type	Code	Trap No.	Severity	Message	Information
Audit	84	771	Major	Primary: Response back from Private virtual IP address	Hot standby: primary unit has detected itself, probable configuration error on private side
Audit	85	772	Major	Primary attempt failed: No response from Private known IP address	Hot standby: Secondary unit attempted to be come primary and failed as no response was received from "known address" on host (private) port.
Audit	86	773	Major	Primary attempt failed: No response from Public known IP address	Hot standby: Secondary unit attempted to be come primary and failed as no response was received from "known address" on network (public) port.
Audit	87	774	Minor	Primary attempt succeeded: Response from Private known IP address	Hot standby: Private side configuration appears to work
Audit	88	775	Minor	Primary attempt succeed: Response from Public known IP address	Hot standby: Public side configuration appears to work
Audit	89	776	Informational	Operating in Secondary mode	Hot standby: unit has become Secondary
Audit	90	777	Informational	Operating in Primary mode	Hot standby: unit has become Primary
Audit	91	778	Major	Primary unprotected: No contact from Secondary unit on host side	Hot standby: Primary unit has detected that the secondary unit does not appear to be responding on the host (private) port
Audit	92	779	Major	Primary unprotected: No contact from Secondary unit on network side	Hot standby: Primary unit has detected that the secondary unit does not appear to be responding on the network (public) port
Audit	93	780	Major	Primary protected: Contact from Secondary unit on host side	Hot standby: Primary unit has detected secondary unit on host (private) port
Audit	94	781	Major	Primary protected: Contact from Secondary unit on network side	Hot standby: Primary unit has detected secondary unit on network (public) port
Audit	95	782	Informational	Hot Standby configuration updated	
Audit	96	783	Informational	DHCP configuration updated	

Log Type	Code	Trap No.	Severity	Message	Information
Audit	97	784	Informational	SNMP configuration updated	
Audit	98	785	Major	Random No. Generator DISCONNECTED	Random number generator has stopped - possible hardware error
Audit	99	786	Major	Random No. Generator RECOVERED	Random number generator has started working again
Audit	100	852	Critical	Standby mode forced	
Audit	101	853	Minor	Standby mode released	
Audit	102	829	Informational	Access control options set	
Audit	103	830	Informational	Disabled access control	
Audit	104	831	Informational	Enabled access control	
Audit	105	832	Informational	Access control password set	
Audit	106	815	Informational	Security configuration updated	
Audit	107	789	Informational	System stopped	The system was powered of at the time this message is logged
Audit	108	790	Informational	IP configuration updated	
Audit	109	791	Informational	Key exchange forced	
Audit	110	792	Informational	Default action set to passthrough	
Audit	111	793	Informational	Default action set to discard	
Audit	112	794	Major	Encrypt clock speed out of range	
Audit	113	795	Major	Decrypt clock speed out of range	
Audit	114	796	Major	Encrypt clock speed within range	
Audit	115	797	Major	Decrypt clock speed within range	
Audit	118	803	Informational	RIP Protocol switched off	
Audit	119	804	Informational	RIP protocol changed to RIP-1	
Audit	120	805	Informational	RIP protocol changed to RIP-2 (broadcast)	
Audit	121	806	Informational	RIP protocol changed to RIP-2 (multi broadcast)	
Audit	122	807	Informational	RIP-2 authentication password changed	

Log Type	Code	Trap No.	Severity	Message	Information
Audit	123	808	Informational	RIP-2 authentication enabled	
Audit	124	809	Informational	RIP-2 authentication disabled	
Audit	127	812	Informational	RIP metric changed	
Audit	128	855	Informational	Subduers length set	
Audit	129	856	Informational	IP settings updated	
Audit	130	857	Informational	Level 2 settings updated	
Audit	131	858	Informational	Level 3 settings updated	
Audit	132	859	Informational	Link settings updated	
Audit	133	860	Informational	NUA in outgoing calls enabled	
Audit	134	861	Informational	NUA in outgoing calls disabled	
Audit	135	862	Informational	NUA in incoming calls enabled	
Audit	136	863	Informational	NUA in incoming calls disabled	
Audit	137	854	Informational	Log text overflow	
Audit	137	864	Informational	Log text overflow	Lack of logging resource will mean that some log entries will not have associated text
Audit	138	836	Informational	Passthrough policy added	
Audit	139	833	Informational	Discard policy added	
Audit	140	837	Informational	Passthrough policy deleted	
Audit	141	834	Informational	Discard policy deleted	
Audit	142	838	Informational	Passthrough policy updated	
Audit	143	835	Informational	Discard policy updated	
Audit	144	813	Informational	LMI monitor active	
Audit	145	814	Informational	LMI monitor inactive	
Audit	146	738	Informational	DHCP gateway interface set	
Audit	148	848	Informational	Auto-notify add SA denied - max SAs reached	
Audit	150	865	Informational	Auto-Notify enabled	
Audit	151	866	Informational	Auto-Notify disabled	
Audit	152	867	Informational	ToS byte passthrough in tunnel mode enabled	

Log Type	Code	Trap No.	Severity	Message	Information
Audit	153	868	Informational	ToS byte passthrough in tunnel mode disabled	
Audit	154	869	Informational	SNMP MIB VIEW enabled	
Audit	155	870	Informational	SNMP MIB VIEW disabled	
Audit	156	881	Informational	RIP broadcast of Ethernet management network information enabled	
Audit	157	882	Informational	RIP broadcast of Ethernet management network information disabled	
Audit	158	883	Informational	Add SA denied - unsupported mode	
Audit	159	884	Informational	Remote Client Relay configuration updated	
Audit	160	885	Informational	Remote Client Relay configuration update failed	
Audit	161	886	Informational	ACL configuration updated	
Audit	162	887	Informational	ACL configuration update failed	
Audit	165	890	Informational	SA Deleted by ACL	
Audit	900	891	Informational	SONET configuration updated	
Audit	901	892	Informational	SONET path hierarchy updated	
Audit	902	893	Informational	SONET path encryption mode updated	
Audit	903	894	Informational	SONET path overhead mode updated	
Audit	905	896	Informational	Ethernet configuration updated	
Audit	906	897	Informational	Ethernet LAN configuration updated	
Audit	907	898	Informational	Ethernet security configuration updated	
Audit	908	899	Informational	License installed	
Audit	909	900	Informational	Reverted to default license	
Audit	910	901	Informational	Private loopback enabled	
Audit	911	902	Informational	Private loopback disabled	
Audit	912	903	Informational	Public loopback enabled	
Audit	913	904	Informational	Public loopback disabled	

Log Type	Code	Trap No.	Severity	Message	Information
Audit	914	905	Critical	Hardware Monitor reports alarm	This can be due to fan, heat, or power failure. Note that power failure is also reported separately. Deprecated, MIB provided for backwards compatibility only.
Audit	915	906	Informational	Hardware Monitor reports all clear	Deprecated, MIB provided for backwards compatibility only.
Audit	916	907	Informational	Power Monitor reports alarm	Deprecated, MIB provided for backwards compatibility only.
Audit	917	908	Informational	Power Monitor reports all clear	Deprecated, MIB provided for backwards compatibility only.
Audit	918	910	Informational	Ethernet extended configuration updated	

Appendix J: Glossary of Terms

Advanced Encryption Standard (AES)	A symmetric algorithm (same key for encryption and decryption) using block encryption of 128 bits in size, supporting key sizes of 128, 192 and 256 bits.
Bits per Sec (bps)	The number of bits passing a point every second; the transmission rate for digital information.
Block cipher	A type of symmetric (secret-key) encryption algorithm that encrypts a fixed length block of plaintext at a time. With a block cipher, the same plaintext block always encrypts to the same ciphertext block, under the same key.
Certificate	A digital document which helps to prevent someone impersonating someone else. Each certificate contains a certified public key and other information such as issuer's name and algorithms used in encryption and decryption.
Certification Authority (CA)	A certificate authority is a trusted organization that accepts certificate applications, authenticates applications, issues certificates, and maintains status information about certificates.
Cipher block chaining (CBC)	A method of using a block cipher in which two identical plaintext blocks encrypt to different ciphertexts.
Ciphertext	An unintelligible form of data that can only be read if specific operations are performed on it using a key and decrypting algorithm.
Ciphertext Stealing (CTS)	CTS mode is a Datacryptor mode of operation that minimizes the latency caused by the encryption of the Ethernet packets passing through the Datacryptor unit.
Command Line Interface (CLI)	The CLI is the text-based user interface to the Datacryptor.
Diffie-Hellman	A protocol which allows two users to agree a secret key over an insecure medium without any prior secret keys.
Digital Signature	A digital signature must be difficult to repudiate, and must protect the integrity of the information being signed. By encrypting a digest of a message with the private key, authentication can later be performed by applying the public key to an encrypted digest (digital signature) and comparing the result to the digest of the message.
Digital Signature Standard (DSS)	A standard for digital signatures using the DSA public key algorithm and the SHA-1 hash algorithm.
DSA	An abbreviation for Digital Signature Algorithm. It is an algorithm used for authentication only.
DSA public parameters	Parameters used to generate and check DSA digital signatures.

Element Manager (EM)	Application used to manage Datacryptor Ethernet devices and is used to launch the Front Panel Viewer (FPV) application.
Encrypted data	Transformed plaintext data to ciphertext.
Encryption	Data encryption scrambles and unscrambles data between two communication endpoints. The encryption process turns an original plaintext message that anyone can read into an encrypted ciphertext message that can be read only by an authorized recipient.
Framing	Method of distinguishing digital channels that have been multiplexed together
Front Panel Viewer (FPV)	Is the application that authenticates the administrator with a Datacryptor Ethernet and allows it to be commissioned and managed.
Hash Function	An algorithm that computes a short digest of a longer message. The digest is usually of a fixed size.
Hash Message Authentication Code (HMAC)	A secret-key authentication algorithm. If only the source and destination know the HMAC key, the algorithm provides data origin authentication and data integrity for packets sent between the two parties. If the HMAC is correct, it proves that it must have been added by the source.
Integrity	Integrity assures that the content of a message has not been altered.
IP	Internet Protocol, this is the protocol that is used to transport data across the Internet.
Key	Secret information used to decrypt or encrypt data
MAC	An abbreviation for Message Authentication Code, a digital signature used to authenticate individual messages.
MAC address	Media Access Control This is the hardware address of an interface card built in during manufacture.
Message Digest #5 (MD-5)	A message-digest algorithm that computes a secure, irreversible, cryptographically strong 128-bit hash value for a document.
Netmask	Used in combination with an IP address to define the network portion of an IP address.
Peer	The Datacryptor device that participates in a connection.
Plaintext	The opposite of encrypted. Plaintext is an intelligible form of data such as the text on this page.
Private Key	See *Public Key*
Public Key	A key that is available to anyone. It is usually the other key to a pair, which consists of a public key and a private key.
Public Key Algorithm	An algorithm that is used in conjunction with a public key set to encrypt and decrypt data.

Public Key Cryptography	In public key cryptography different keys are used for encryption and decryption. The public key is public, but the private key is known only to its owner. Anyone that possesses the public key can encrypt a message so that only a single recipient (the owner of the private key) can decrypt it. The two parties do not need to share any secret information.
Public Key Data	Consists of a public key algorithm, a public key and a private key.
Public Key encryption	The process of encrypting data using public key data.
Public Key Set	A pair of keys: a public key and a private key.
Replay Prevention	Prevents the replaying of a message or part of a message to produce an unauthorized effect, such as the capture and replay a sequence of authentication messages to masquerade as a legitimate user.
Secret Key	The key used in symmetric encryption. Both participants must share the same key, and this key must remain secret to protect the communication.
Secure Hash Algorithm (SHA)	A US standard for a cryptographically strong hash algorithm, designed by the National Security Agency and defined by the National Institute of Standards and Technology (NIST).
SFP	The Small Form-Factor Pluggable device is a compact transceiver used in data communication applications where fiber optic or twisted pair networking cable is to be employed.
SNMP	Simple Network Management Protocol is an Internet standard used to allow monitoring of performance and provide event notifications.
Transform	A transform defines the transformation applied to the data to secure it. This includes the encryption algorithm, security protocols, the key sizes and how they are derived, and the transformation process
X.509	The ITU-T X.509 recommendation defines the formats for X.509 certificates.