THALES

Local HSM Manager v5.1.7

for payShield 9000
User's Guide

>> Revision Status

Document No.	Manual Set	Software Version	Release Date
1270A596-018.2	Issue 18 Revision 2	HSM Manager 5.1.7	June 2015

This manual describes the functionality of the Local HSM Manager for both payShield 9000 and HSM 8000. It replaces the following previous manuals:

- 1270A539 payShield 9000 Local HSM Manager User's Guide
- 1270A536 HSM 8000 Local HSM Manager User's Guide

See the Release Notes for information on compatibility between versions of Local HSM Manager and of HSM 8000/payShield 9000 software.

>> List of Chapters

>> Table of Contents

>> End User License Agreement (EULA)

Please read this Agreement carefully.

THALES E-SECURITY IS WILLING TO LICENSE SOFTWARE TO THE ENTITY THAT HAS PURCHASED A THALES E-SECURITY HARDWARE DEVICE UPON THE CONDITION THAT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT ("AGREEMENT") ARE ACCEPTED AND AGREED. PLEASE READ THIS AGREEMENT CAREFULLY. THE TERMS OF THIS AGREEMENT WILL BE DEEMED TO HAVE BEEN AGREED TO BY THE ENTITY OR END USER CUSTOMER THAT HAS PURCHASED A THALES E-SECURITY HARDWARE DEVICE IF SOFTWARE IS DOWNLOADED OR IF SOFTWARE IS USED OR IF A SECURITY SEAL ON THE MEDIA PACKAGE CONTAINING SOFTWARE IS BROKEN OR IF CONSENT IS MANIFESTED BY CLICKING ON AN ACCEPTANCE KEY.

This document is a legal agreement between Thales e-Security, Inc., ("Thales e-Security"), 900 South Pine Island Road, Suite 710, Plantation, FL 33324 U.S.A. and the end user customer that has purchased a Thales e-Security hardware device, (hereafter referred to as the "End User Customer"). Any person who manifests their agreement to this Agreement represents that they have the requisite and appropriate legal authority to bind the End User Customer.

1. Definitions

(a) "Affiliates" means Thales Transport & Security (Hong Kong) Ltd. and Thales UK Limited.

(b) "Software" means machine readable instructions and all modifications and customizations thereof in binary form and any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Thales e-Security or its corporate Affiliates that direct a computer's processor to perform specific operations.

2. Ownership

Software consists of a combination of proprietary components that are owned by or licensed to Thales e-Security or its Affiliates together with free or open source components ("Free Software Components") that are identified in the text files that are provided with the Software. ONLY THOSE TERMS AND CONDITIONS SPECIFIED FOR, OR APPLICABLE TO, EACH SPECIFIC FREE SOFTWARE COMPONENT PURSUANT TO ITS APPLICABLE GOVERNING LICENSE SHALL BE APPLICABLE TO SUCH FREE SOFTWARE COMPONENT. Each Free Software Component is the copyright of its respective copyright owner. Software is licensed to End User Customer and is not sold. End User Customer has no ownership rights in the Software. Rather, End User Customer is hereby granted a license to use the Software. The Software is copyrighted by Thales e-Security or its Affiliates or its suppliers. End User Customer hereby agrees to respect and not to remove or conceal from view any copyright or trademark notice appearing on the Software or documentation, and to reproduce all copyright or trademark notices on any copy of the Software and documentation or any portion thereof and on all portions contained in or merged into other programs and documentation.

3. License to Use

Subject to the terms and conditions of this Agreement Thales e-Security grants to End User Customer a non-exclusive, limited license to use Software unmodified for the sole purpose of running or operating Software on or with a Thales e-Security hardware device and to copy such Software provided that such copies are made in machine readable form for backup purposes.

4. Restrictions

Software is confidential and copyrighted. Unless enforcement is prohibited by applicable law, End User Customer may not modify, decompile, or reverse engineer Software. End User Customer shall not permit any other person to do any of the same. End User Customer may not rent, lease or sublicense the Software. Any rights not expressly granted by Thales e-Security to End User Customer hereunder are reserved by Thales e-Security and its licensors and all implied licenses are disclaimed. Any other use of the Software by any other entity is strictly forbidden and is a violation of this Agreement. The Software and any accompanying written materials are protected by international

copyright and patent laws and international trade provisions. No right, title or interest is granted under this Agreement in or to any trademark, service mark, logo or trade name of Thales, S.A., Thales e-Security or its licensors or corporate Affiliates. End User Customer may not disassemble the Thales e-Security owned or licensed components of the Software. End User Customer may not create derivative works based on the Software except as may be necessary to permit integration with other technology.

5. Limited Warranty

(a) Thales e-Security warrants that a Thales e-Security hardware device and the accompanying Software will function substantially as detailed in their respective and applicable specifications. The warranty period for a Thales e-Security hardware device is one year from the date of delivery and the warranty period for Software is ninety (90) days from the date of delivery. If either a Thales e-Security hardware device or Software fails to materially conform to their applicable specifications, Thales e-Security or its Affiliates will repair or replace the affected hardware device or Software provided that End User Customer provides Thales e-Security with a written notice of a claim or a defect under this warranty within the warranty period herein described. FOR THE AVOIDANCE OF DOUBT, THALES E-SECURITY NEITHER WARRANTS, NOR CAN BE EXPECTED TO WARRANT THAT A THALES E-SECURITY HARDWARE DEVICE OR SOFTWARE IS WHOLLY FREE FROM DEFECT, OR THAT ANY PARTICULAR DEFECT CAN BE REMEDIED, OR THAT A REMEDY CAN BE PROVIDED IN ANY PARTICULAR TIMEFRAME. THE FOREGOING WARRANTY SHALL NOT APPLY IF THE NONCONFORMITY ISSUE IS CAUSED BY ANY MODIFICATION OR REPAIRS TO A THALES E-SECURITY HARDWARE DEVICE OR SOFTWARE PERFORMED BY ANYONE OTHER THAN THALES E-SECURITY OR TO ANY ASSOCIATED OR COMPLEMENTARY EQUIPMENT OR SOFTWARE NOT FURNISHED BY THALES E-SECURITY OR ITS CORPORATE AFFILIATES, OR BY ANY HARDWARE DEVICE OR SOFTWARE MISUSE OR NEGLECT.

(b) NOTWITHSTANDING THE FOREGOING, TO THE MAXIMUM EXTENT PERMITTED BY LAW, THALES E-SECURITY, ON BEHALF OF ITSELF, ITS AFFILIATES AND ITS THIRD PARTY SUPPLIERS, HEREBY DISCLAIMS ANY AND ALL WARRANTIES OF ANY OTHER KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE. THALES E-SECURITY DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE HARDWARE DEVICE OR SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS THAT END USER CUSTOMER MAY HAVE, OR THAT A THALES E-SECURITY HARDWARE DEVICE OR SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERRUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS WILL BE CORRECTED, OR THAT THE SOFTWARE OR HARDWARE DEVICE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW FOR THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE HARDWARE DEVICE OR SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

6. Intellectual Property Indemnification

Thales e-Security shall defend or, at its option, settle, any claim, action or proceeding brought against End User Customer alleging that a Thales e-Security hardware device or Software infringes upon a trademark, patent, copyright or trade secret or other intellectual property right in a country that is a signatory to the Berne Convention, and shall indemnify End User Customer from and against all damages and costs finally awarded against End User Customer in any such action or proceeding, provided that End User Customer (a) promptly notifies Thales e-Security in writing of the claim, (b) gives Thales e-Security full authority, information and assistance to defend such claim and (c) gives Thales e-Security sole control of the defense of such claim and all negotiations for the compromise or settlement thereof. If a Thales e-Security hardware device or Software or any part thereof becomes, or in the opinion of Thales e-Security is likely to become the subject of a valid claim of infringement or the like under any trademark, patent, copyright or trade secret or other intellectual property right law, Thales e-Security shall have the right, at its option and expense, either to obtain for End User Customer a license permitting the continued use of the Thales hardware device or Software or such part, or to replace or modify it so that it becomes non-infringing. Thales e-Security shall have no liability hereunder for any costs incurred or settlement entered into without its prior written consent.

Thales e-Security shall have no liability hereunder with respect to any claim based upon (i) the combination of a Thales hardware device or Software with other equipment not furnished by Thales e-Security (except if the infringement occurs due to the use of the Thales e-Security hardware device or Software itself as originally provided by Thales e-Security or its Affiliates); (ii) any addition to or modification of a Thales e-Security hardware device or Software by any person or entity other than Thales e-Security or its Affiliates; or (iii) use of a superseded or altered release of the Software. THE FOREGOING STATES THE SOLE AND EXCLUSIVE LIABILITY OF THALES E-SECURITY AND ITS LICENSORS AND THE SOLE AND EXCLUSIVE REMEDY OF END USER CUSTOMER WITH RESPECT TO ANY CLAIM OF PATENT, COPYRIGHT, TRADEMARK, TRADE SECRET OR OTHER INTELLECTUAL PROPERTY RIGHTS INFRINGEMENT BY A THALES E-SECURITY HARDWARE DEVICE OR SOFTWARE, ANY SERVICE, ANY PART THEREOF OR THE USE THEREOF, AND IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED OR ARISING BY CUSTOM OR TRADE USAGE, AND INDEMNITIES WITH RESPECT THERETO. NOTWITHSTANDING THE FOREGOING, ALL OPEN SOURCE SOFTWARE OR FREEWARE INCLUDED WITH THE SOFTWARE IS PROVIDED WITHOUT ANY RIGHTS TO INDEMNIFICATION.

7. Limited Liability

TO THE EXTENT ALLOWED BY LAW, IN NO EVENT WILL THALES E-SECURITY OR ITS CORPORATE AFFILIATES OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF THALES E-SECURITY OR ANY OF ITS CORPORATE AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Thales e-Security or its corporate affiliate's liability, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by End User Customer for the Thales e-Security hardware device or Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose.

8. Export Restrictions.

Thales e-Security hardware devices and Software are subject to the restrictions imposed by the United States Export Administration Regulations and the United Kingdom Export Control Order 2008 and may be subject to export or import regulations in other countries. End User Customer agrees to comply strictly with all such laws and regulations and acknowledges that it has the responsibility to obtain such licenses to export, re-export, or import as may be required.

9. Transfer Rights

End User Customer may transfer a Thales e-Security hardware device together with the Software, and this license to another party if the other party agrees to accept the terms and conditions of this Agreement and notice of such transfer and acceptance is provided to Thales e-Security in writing. FOR THE AVOIDANCE OF DOUBT, IF END USER CUSTOMER TRANSFERS POSSESSION OF ANY COPY OF THE SOFTWARE TO ANOTHER PARTY, EXCEPT AS PROVIDED IN THIS SECTION 9, THE LICENSE GRANT PROVIDED HEREIN IS AUTOMATICALLY REVOKED, CANCELLED AND TERMINATED.

10. Termination

This Agreement is effective until terminated. End User Customer may terminate this Agreement at any time by destroying or erasing all copies of the Software and accompanying written materials in its possession or control. This license will terminate automatically, without notice from Thales e-Security if End User Customer fails to comply with the terms and conditions of this Agreement. Upon such termination, End User Customer shall destroy or erase all copies of the Software (together with all modifications, upgrades and merged portions in any form) and any accompanying written materials in its possession or control.

11. U.S. Government Acquisitions

Software and Documentation acquired by the U.S. Government or on its behalf is furnished with "RESTRICTED RIGHTS," as defined in Federal Acquisition Regulation ("FAR") 52.227-19(b)(2), and DFAR 252.227-7013 to 7019, as applicable. Use, duplication or disclosure of the Software and Documentation by the U.S. Government and parties acting on its behalf is governed by and subject to the restrictions set forth in FAR 52.227-19(b)(1) and (2) or DFAR 252.227-7013 to 7019, as applicable.

12. Governing Law and Dispute Resolution

(a) If an End User Customer is located in Anguilla, Antigua and Barbuda, Argentina, Aruba, Bahamas, Barbados, Belize, Bermuda, Bolivia, Bonaire, Sint Eustatius and Saba, Brazil, British Virgin Islands, Canada, Cayman Islands, Chile, Colombia, Costa Rica, Cuba, Curaçao, Dominica, Dominican Republic, Ecuador, El Salvador, Falkland Islands (Malvinas), French Guiana, Greenland, Grenada, Guadeloupe, Guatemala, Guyana, Haiti, Honduras, Jamaica, Martinique, Mexico, Monserrat, Nicaragua, Panama, Paraguay, Peru, Puerto Rico, Saint-Barthélemy, St. Kitts and Nevis, Saint Lucia, Saint Martin, Saint Vincent and the Grenadines, Saint Pierre and Miquelon, Sint Maarten, Suriname, Trinidad and Tobago, Turks and Caicos Islands, United States, United States Virgin Islands, Uruguay or Venezuela, this End User License Agreement shall be construed, interpreted and governed by the laws of the State of Florida, United States of America without regard to conflicts of laws and all disputes shall be submitted to the State or Federal courts located in Florida.

(c) If an End User Customer is located in Algeria, Angola, Afghanistan, Albania, Andorra, Armenia, Austria, Azerbaijan, Bahrain, Bangladesh, Belarus, Belgium, Benin, Bhutan, Bosnia-Herzegovina, Botswana, Bulgaria, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo, Cote d'Ivoire, Croatia, Cyprus, Czech Republic, Denmark, Democratic Republic of the Congo, Djibouti, Egypt, Equatorial Guinea, Eritrea, Estonia, Ethiopia, Finland, Faroe Islands, France, Gabon, Gambia, Germany, Gibraltar, Georgia, Greece, Ghana, Guerney and Alderney, Guinea, Guinea-Bissau, Hungary, Iceland, India, Iran, Iraq, Ireland, Island of Man, Israel, Italy, Jersey, Jordan, Kazakhstan, Kenya, Kosovo, Kyrgyzstan, Kuwait, Latvia, Lesotho, Liberia, Libya, Liechtenstein, Lithuania, Lebanon, Luxembourg, Macedonia, Madagascar, Malawi, Maldives, Mali, Malta, Mauritania, Mauritius, Moldova, Monaco, Montenegro, Morocco, Mozambique, Namibia, Nepal, Netherlands, Niger, Nigeria, Norway, Oman, Palestine, Pakistan, Poland, Portugal, Qatar, Romania, Russia, Rwanda, San Marino, Sao Tome & Principe, Saudi Arabia, Senegal, Serbia, Seychelles, Sierra Leone Slovakia, Slovenia, Somalia, South Africa, South Sudan, Sudan, Spain, Sri Lanka, Swaziland, Sweden, Svalbard and Jan Mayen Islands, Switzerland, Syria, Tajikistan, Tanzania, Togo, Tunisia, Turkey, Turkmenistan, Uganda, Ukraine, United Arab Emirates, United Kingdom, Uzbekistan, Vatican City State (Holy See), Yemen, Zambia, or Zimbabwe, this End User License Agreement will be governed by the laws of England and Wales and all disputes shall be submitted to the courts of England.

(c) If an End User Customer is located in American Samoa, Australia, Brunei Darussalam, Cambodia, China, Cook Islands, Fiji, Guam, Hong Kong, Indonesia, Japan, Kiribati, Laos, Macao, Malaysia, Marshall Islands, Micronesia, Mongolia, Myanmar (ex-Burma), New Caledonia, New Zealand, Papua New Guinea, Philippines, Samoa, Singapore, Solomon, Islands, South Korea, Taiwan, Thailand, Timor Leste, Tonga, Tuvalu, Vanuatu, Vietnam or Western Samoa, this End User License Agreement will be governed by the Law of the Hong Kong Special Administrative Region of the People's Republic of China and all disputes shall be submitted to arbitration in Hong Kong.

13. Elliptic Curve Cryptography Activation

If End User Customer elects to purchase a Thales e-Security hardware device containing elliptic curve cryptography software (ECC) it agrees that its use of ECC is limited to storing cryptographic keys and the performance of cryptographic operations in a hardware environment together with the management and issuance of digital certificates by a registration authority or certificate authority provided such certificates are either (i) solely for the internal use of the registration authority or (ii) are solely for the internal use of an enterprise that is hosted by a registration authority or certificate authority. No right or license is provided or granted to use ECC as part of a third party service provider for the purpose of acting as a commercial registration authority or certificate authority as part of a commercial service offered by an enterprise, either as a vendor of digital certificates or in the provisioning of certificates for use in a commercial service.

>> Chapter 1 – Introduction

General

The payShield 9000 and HSM 8000 hardware security modules (HSM) provide cryptographic functions to support network and point-to-point data security. Acting as a peripheral to a Host computer, the HSM provides the cryptographic facilities required to implement key management, message authentication and Personal Identification Number (PIN) encryption in real time online environments. The HSM is made physically secure by locks, electronic switches and tamper-detection circuits.

Figure 1 - payShield 9000: Front View

Figure 2 – HSM 8000: Front View

The HSMs supports a number of standard functions and can be customized to perform client-specific cryptographic functions. Standard functions include:

- Verifying and generating Personal Identification Numbers (PINs) such as those used with bank accounts and credit cards.
- Generating encrypted card values such as Card Verification Values (CVVs) for the plastic card industry.
- PIN solicitation, to obtain a new PIN from a card holder (against a reference number).
- Generating keys for use in Electronic Funds Transfer Point of Sale (EFTPOS) systems.
- Key management in non-EFTPOS systems.

> Generating and verifying Message Authorization Codes (MACs) for messages transferred via telecommunications networks.

The HSM is normally online to the Host and does not require operator monitoring or intervention. The HSM performs cryptographic processing in response to commands from the Host. The Host sends command messages, which consist of command codes and other fields that are required by the HSM in order to process the commands. The HSM processes the command messages and generates response messages, which also contain a variable number of fields (depending on the message type). Some commands can be entered from a PC communicating with the HSM over a cross-over Ethernet cable, using the HSM Manager software.

PCI HSM Compliance *(payShield 9000 only)*

See Chapter 10 of the payShield 9000 General Information Manual for information about PCI HSM certification of the payShield 9000.

Physical Description of the HSMs

See Chapter 2 of the payShield 9000 General Information Manual for a description of the payShield 9000.

See Chapter 1 of the HSM 8000 Console Reference Manual for a description of the HSM 8000.

About this Manual

This manual is a reference document containing details of all HSM command functions that can be controlled using the Local HSM Manager. For other HSM information, see the other manuals delivered with the HSM.

The information in this manual applies to both the HSM 8000 and payShield 9000 except where the text indicates that it is appropriate to only one of these HSM types. It replaces the following previous manuals:

- 1270A539 payShield 9000 Local HSM Manager User's Guide
- 1270A536 HSM 8000 Local HSM Manager User's Guide

>> Chapter 2 – Introduction to Local HSM Manager

Overview

The Local HSM Manager is an application that operates within a secure software environment, and provides users with all the functionality that is currently possible using the console interface with standard base software. (*Note: HSM Manager is designed to take advantage of the standard base software functionality. It can be used with customised software developed from an appropriate version of standard base software, but will not be able to provide the functionality of customised Console commands or manage customised Host commands.*)

HSM Manager provides the following features:

- *HSM Configuration* – communication ports settings, security settings, etc.
- *HSM Installation* – generation and installation of LMK from smartcards
- *HSM Key Management* – generation, import, export, etc. of keys
- *HSM Maintenance* – viewing/erasing of audit/error logs, version info, etc.

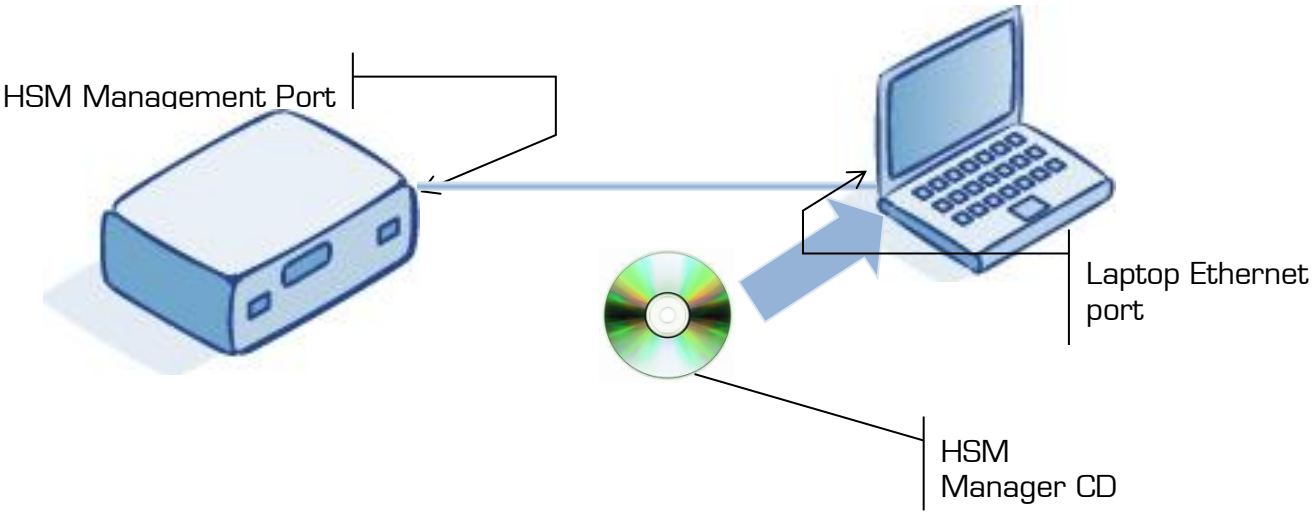
About Local Management

Local HSM Manager operates within a secure software environment by booting the PC using the CD provided. The PC will automatically boot into a functionally-restricted version of Linux, without accessing any data on the PC's internal hard disks.

Note that in order to boot the CD, the PC must be configured to boot from the CD first (BIOS settings may need to be changed). Refer to the PC manufacturer's manual for further details.

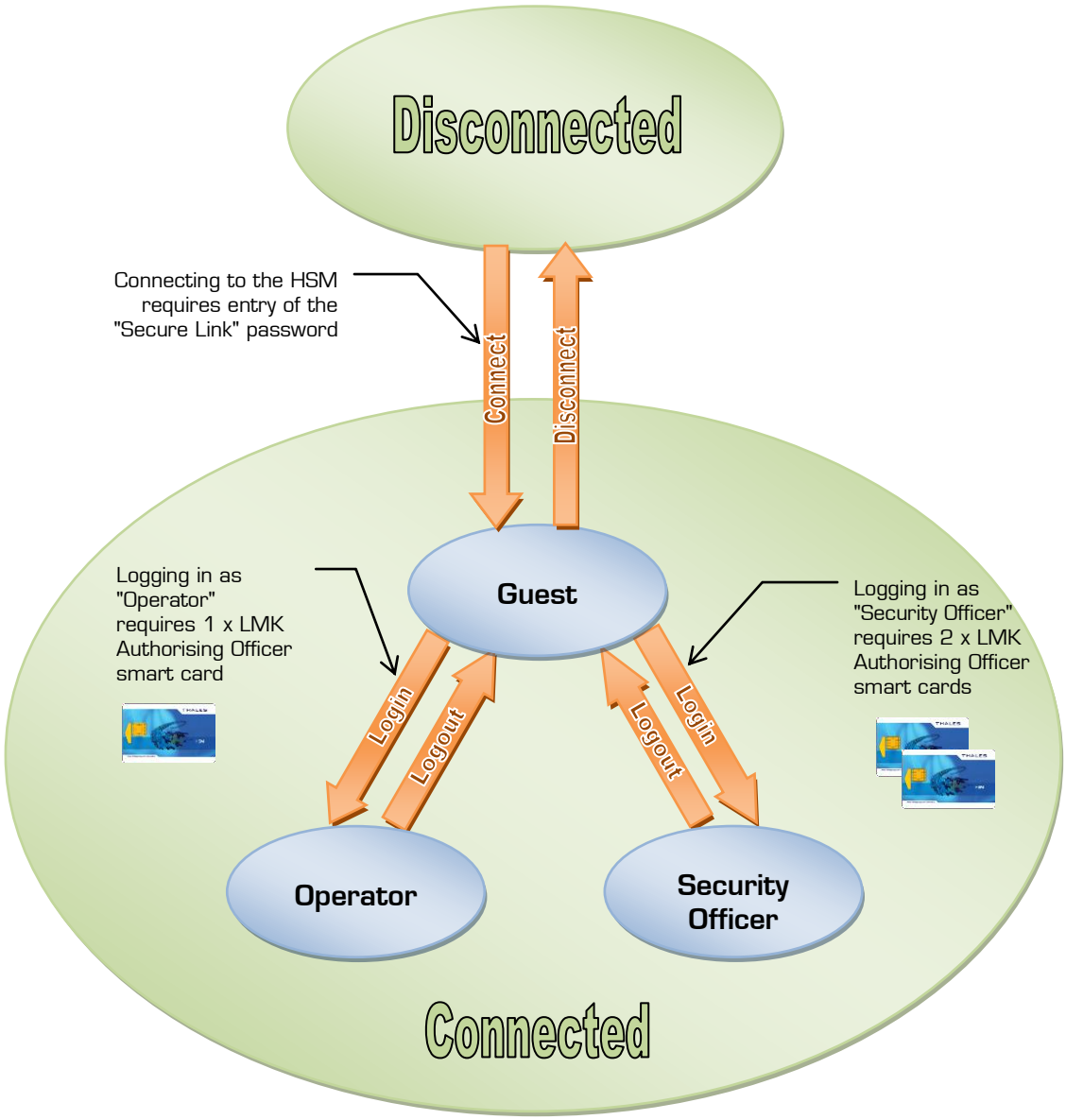
The HSM Manager CD is designed to run on most standard laptop/desktop PCs. However, certain hardware configurations are known to be incompatible with HSM Manager, so in order to minimize the risk of incompatibilities, please ensure that:

- The laptop is not docked into a docking station.
- One (and only one) Ethernet port is available.
- All wireless (Wi-Fi) functionality is disabled.
- All unnecessary peripherals are detached.



HSM Manager State

HSM Manager is always in either one of two states: disconnected, or connected. In the disconnected state, no communication with a HSM is possible. Once connected, the user takes on one of three roles: Guest, Operator, or Security Officer. The diagram below indicates the relationship between the HSM Manager's states and the user's role. The individual roles are described in the next section.



User Roles

Users of the HSM Manager are assigned one of three different roles, depending on the level of authentication provided. Authentication of the user(s) is provided by the HSM verifying the password on the LMK Authorizing Officer (or LMK Component) smart cards inserted into the HSM's smart card reader, and by the user entering the smart card's corresponding PIN via the HSM Manager.

	Without LMK(s) installed	With LMK(s) installed
Guest	In this state, the *Guest* user can perform various fundamental configuration options such as modification of communication port settings, enabling/disabling of commands and PIN block formats, and modification of numerous security settings.	Once LMKs are installed, the *Guest* user can perform a number of "read-only" operations, such as viewing the HSM's configuration, and viewing the error logs.
Operator (1 x Authorizing Officer card)	N/A*	*Operators* inherit the capabilities of *Guests*, but may also perform commonly used key management functions such as key / component generation, smart card formatting, and various diagnostic commands. Note that the LMK used in the subsequent operations will be the LMK identified by the LMK Authorizing Officer card used by the Operator during the login procedure.
Security Officer (2 x Authorizing Officer cards)	N/A*	*Security Officers* inherit the capabilities of *Operators*, but may also perform more sensitive functions that would traditionally require the HSM to be authorized. Note that the LMK used in the subsequent operations will be the LMK identified by the LMK Authorizing Officer cards used by the Security Officer during the login procedure.

* With no LMK(s) installed, the HSM cannot verify the LMK Authorizing Officer smartcards, so the Operator and Security Officer roles are not available.

Note: The specific access rights of the user will also depend on the current HSM state – i.e. Online, Offline or Secure state.

Preparing to use the software

1. Connect the Local HSM Manager PC or laptop to your HSM using a cross-over Ethernet cable.
2. Insert the CD into the CD/DVD drive.
3. Restart the PC, so that it boots from the CD (which may require a BIOS configuration change). If problems are encountered in starting and running HSM Manager, see the information in *Appendix F – Knoppix "Cheat Codes"*.
4. Start the **HSM Manager** application.

Connecting to your HSM

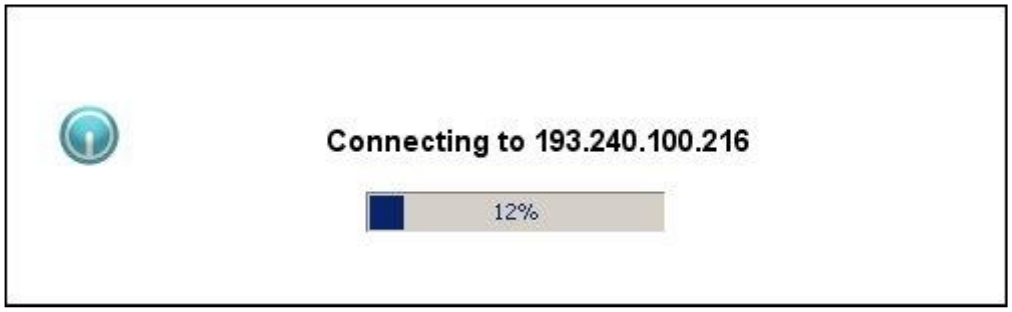
In order to use the Local HSM Manager, you must first connect to your HSM.

Select the **Connect** option from the HSM Manager **File** menu.

The screen similar to that shown below is displayed.

After a few moments, use the drop-down list to select the IP address of the HSM you wish to connect to, and enter that HSM's Secure Link password (configured in the HSM using the CS console command or the HSM Manager **Edit / Initial Settings** option).

When you click **OK**, HSM Manager attempts to connect to the selected HSM.



Once a connection has been made, the HSM Manager main screen is displayed, with your user level set to Guest. For details of the activities available to a Guest user, see *Appendix A - User Roles and Access Rights*.

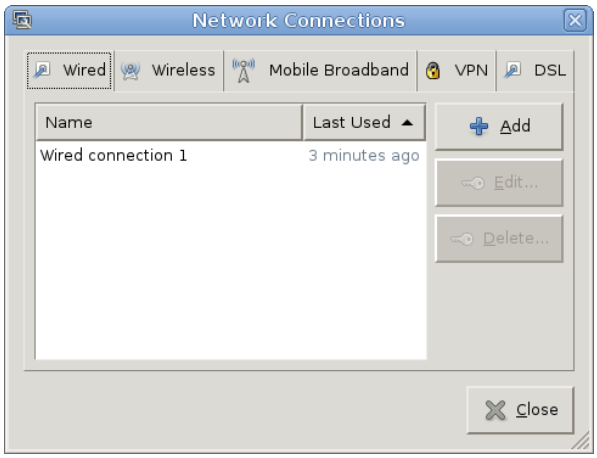
NOTE: the *Set IP Address* icon on the desktop does not need to be used with **Local** HSM Manager, because the PC address is automatically set up based on the HSM addresses detected. *Set IP Address* is only used (where required) for **Remote** HSM Manager.

If Local HSM Manager does not automatically set its IP Address

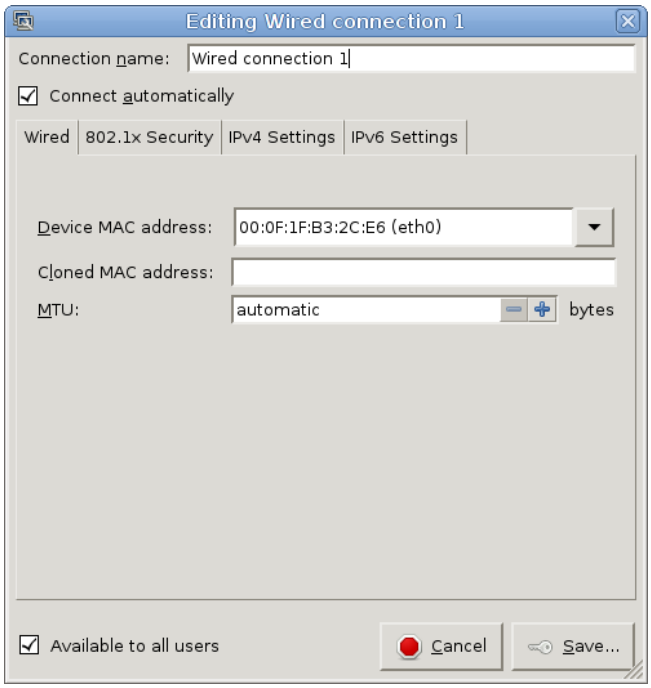
Local HSM Manager will normally set up its IP address automatically to enable it to connect to the payShield 9000. If this is not possible, you will not be able to connect. In this event, you should use the following process.

1. If the Local HSM Manager window is open on the desktop, close it.

2. Click once on the "*Network Connections*" icon on the desktop. This will present the Network Connections dialog box:



3. Double-click on the appropriate "*Wired connection*" line to open the dialog box to let you edit the network connection details:



4. Uncheck the "*Connect automatically*" check box.

5. Click **Save** on the *"Editing ..."* dialog box, and **Close** on the "*Network Connections*" dialog box.

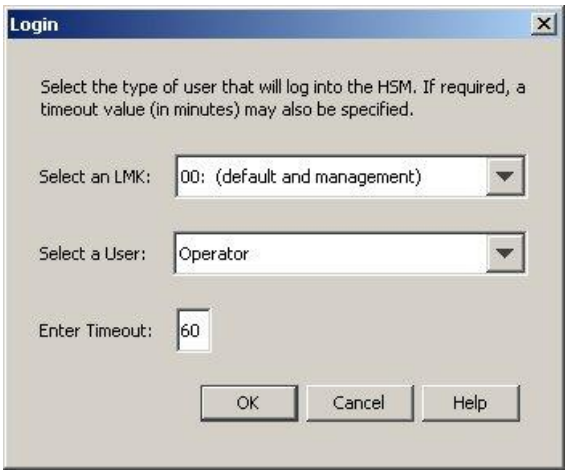
6. Start Local HSM Manager by clicking on the "*HSM Manager*" icon. You will now be able to connect.

Logging in and Setting the User Role

To use HSM Manager functions other than those available to a Guest user, you must login to the system.

Select the **Login** option from the HSM Manager **File** menu. The screen shown below is displayed.

Note: In order to login, you must have an LMK installed.



Complete the fields on this screen as follows.

Select an LMK

Select the LMK you want to log on with. This identifier indicates which LMK Authorizing Officer cards are to be inserted into the HSM and verified during the Login process.

Once successfully logged in, the HSM will only permit operations that involve the selected LMK.

Select a User

There are three types of users:

- Guest: This type of user does not require authentication. Note that if there are no LMKs installed in the HSM then this is the only type of user that can login.
- Operator: This type of user requires that a single LMK Authorizing Officer insert a smartcard for authentication. The user will next be prompted to enter the corresponding smartcard PIN.
- Security Officer: This type of user requires that two (different) LMK Authorizing Officers insert smartcards for authentication in turn. Both users will be separately prompted to enter the corresponding smartcard PIN.

Refer to *Appendix A - User Roles and Access Rights* for details of the access rights of the different user types.

Note: When logging in using the LMK Authorizing Officer smartcards relating to the designated Management LMK, the logged in user will be able to perform certain 'management' functions (e.g. audit trail configuration, enabling/disabling host commands, etc.)

Enter Timeout

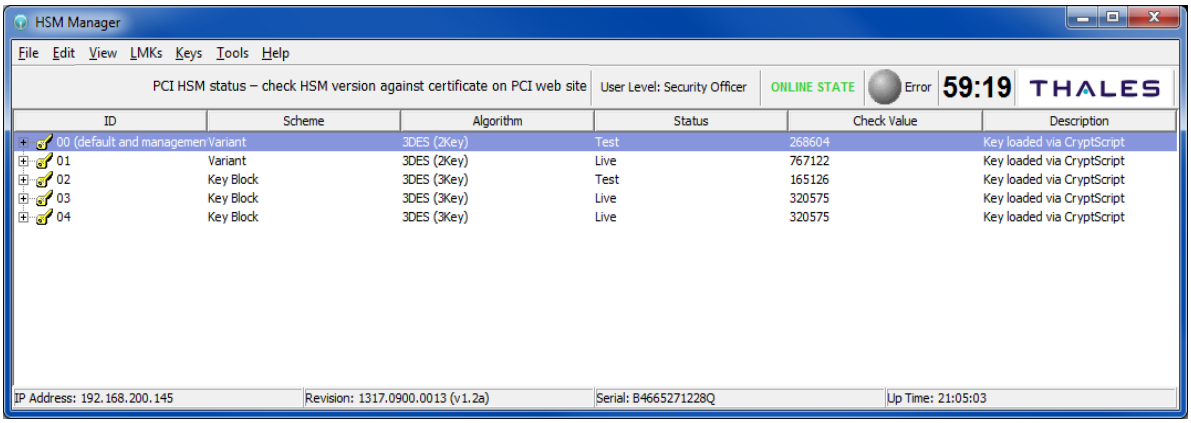
Enter the length of time you want the activity session with this login to be kept open - 1 to 60 minutes.

When you click **OK**, HSM Manager will prompt you to insert the appropriate smartcards into the HSM's smartcard reader, and enter the PIN numbers: PINs must be entered within 60 seconds. Follow the instructions provided on screen.

The login procedure ends with the HSM Manager main screen being updated.

The HSM Manager Main Screen

The HSM Manager main screen is displayed as follows when the HSM Manager application is launched and a user (in this case, a "Security Officer") has logged on.



This screen has the following features:

> Title Bar

The title bar displays the name of the application.

> Menus

The menus provide access to the full range of HSM Manager functions. See later in this section for details.

> Toolbar

The toolbar shows the current user level, the state of the HSM, and the time remaining before HSM Manager times-out. On payShield 9000 (v2.3a onwards), this line also indicates whether the relevant security settings have PCI HSM compliant values:

- "*PCI-HSM status: check HSM version against certificate on PCI web site*" if all of the security settings are in the compliant state.
- "*PCI-HSM status: Security settings are not PCI HSM compliant* " if not all of the security settings are in the compliant state.

- Operational Panel

  The status of installed LMKs is shown in the main window:
  - LMK ID
    - A 2-digit identifier indicating the slot in which this LMK is stored.
  - LMK Scheme
    - Variant or Keyblock.
  - LMK Algorithm
    - 3DES (2Key) for a Variant LMK; 3DES (3Key) for a Keyblock LMK.
  - Status
    - "Test" or "Live" – Determined at time of LMK generation.
  - Check Value
    - A 6-digit check value of the LMK.
  - Description
    - Entered at time of installation.

- Status Bar

  This area contains specific information about the connected HSM:
  - IP address
    - The IP Address of the connected HSM's Ethernet Management Port.
  - Revision
    - The software version number(s) of the connected HSM.
  - Serial Number
    - The serial number of the connected HSM.
  - Up time
    - The number of hours/minutes/seconds that the connected HSM has been running since it was powered on.

HSM Manager Menu Options

The HSM Manager menu options are summarized below and are described in full detail in the rest of this guide.

File Menu

The **File** menu allows users to connect/disconnect and login/logout from HSMs. The following menu items are available:

- **Connect** – establish a connection with an HSM.
- **Disconnect** – terminate an established connection with an HSM.
- **Login** – login using one or two smartcards, to access *Operator* or *Security Officer* functions.
- **Logout** – terminate the current role, and return to *Guest*.
- **Load Settings** – load HSM settings from a previously saved file.
- **Save Settings** – save HSM settings to a selected file.
- **Load Firmware** – download a different version of firmware into the HSM.
- **Load Licence** – download a different licence into the HSM.
- **Exit** – disconnects you from the HSM and closes down the HSM Manager application.

Edit Menu

The **Edit** menu allows authorized users to view/modify the HSM's configuration details. The following menu items are available:

- **General Settings** – to view/modify general HSM settings.
- **Advanced Settings** – to view/modify important system settings.
- **Initial Settings** – to view/modify sensitive security settings.
- **Host Interface** – to view/modify host communications settings.
- **Printer Interface** – to view/modify serial and parallel printer communications settings.
- **Management Interface** – to view/modify management communications settings.
- **Host Commands** – to view/enable/disable individual or groups of host commands.
- **PIN Blocks** – to view/enable/disable individual PIN block formats.
- **Auditing** – to view/modify the list of audited events.
- **HSM Date/Time** – to view/set the HSM's internal clock.
- **Authorize** – to view/set the HSM's authorized state/activities.

View Menu

The **View** menu allows authorized users to view/erase the HSM's internal logs and view the firmware details. The following menu items are available:

- **Logs** – to view/erase the HSM's internal error and audit logs.
- **HSM Information** – to view the HSM information (firmware, licenses, etc.).
- **Remote Details** – to view remote management configuration details.

LMKs Menu

The **LMKs** menu allows authorized users to manage the generation, installation and uninstallation of Local Master Keys (LMKs). The following menu items are available:

- **Generate Keys** – to generate a new LMK onto smart cards.
- **Install LMK** – to load a new LMK from smart cards into the HSM.
- **Install 'Old' LMK** – to load an old LMK from smart cards into the "key change storage" area.
- **Copy LMK Component Card** – to create a copy of an existing LMK component card.
- **Create Authorizing Officer Card** – to create an LMK Authorizing Officer smartcard from an existing LMK Component Card.
- **Uninstall LMK** – to uninstall an LMK from the HSM.

Keys Menu

The **Keys** menu allows authorized users to manage the generation, import, and export of keys and key components. The following menu items are available:

- **Generate Keys** – to generate specific keys under the LMK.
- **Key Import** – to import keys from a different cryptographic zone.
- **Key Export** – to export keys to a different cryptographic zone.
- **Generate Components** – to generate new key components.
- **Encrypt Components** – to encrypt supplied key components using the LMK.
- **Form Key from Components** – to form keys from supplied key components.

Tools Menu

The **Tools** menu allows authorized users to perform smart card management, diagnostic functions and general utility functions. The following menu items are available:

- **Smartcard** – to perform smart card management functions.
- **Diagnostics** – to perform network management diagnostic functions.
- **Utilities** – to perform general utility functions, including:
  - **Calculate Key Check Value**
  - **Encrypt Decimalization Table**

- **Translate Decimalization Table**
- **Generate MAC on Issuer Proprietary Bitmap (for CAP/DPA)**
- **Generate CVV/CVC**
- **Generate VISA PVV**

> **Utilisation and Health Check Data** (*payShield 9000 only*) – to view and manage the HSM's utilization and health check data:

- **Configure Statistics**
- **Health Check Data**
- **HSM Loading Value Host Command Statistics**
- **Reset Statistics**

> **SNMP** (*payShield 9000 only*) – to configure the SNMP interfaces:

- **Display** – show SNMP Communities/Users
- **Add** – add SNMP Communities/Users
- **Delete** – remove SNMP Communities/Users

> **Secure Host Communications** *(payShield 9000 only)*:

- **Generate Certificate Signing Request**
- **Export HSM CA Certificate**
- **Import Signed Certificate**
- **Generate HMK**
- **Recover HMK**
- **Change HMK Passphrase**
- **View Certificates**
- **Delete Certificates**

> **Reset Fraud Detection** – to restore operation after fraud detection.

> **Return to Factory Settings** – to remove all settings that have been made since the HSM was shipped from the factory

Help Menu

The **Help** menu allows all users to view the on-line help system.

Closing your HSM Manager Session and Disconnecting

Once you have finished using HSM Manager, you should log out of the current session, if it has not already timed-out, and then disconnect from the HSM.

Logging out of your HSM Manager session

To close your current HSM Manager session, select the **Logout** option from the **File** menu.

You are asked to confirm that you want to log out. Select **OK** or **Cancel**, as appropriate.

Messages are displayed as you are logged out.

Note: If you do not log out, your session will automatically close at the end of the timeout period specified when you logged in.

Disconnecting from the HSM

To disconnect from your HSM, select the **Disconnect** option from the **File** menu.

You are asked to confirm that you want to disconnect. Select **OK** or **Cancel**, as appropriate.

Messages are displayed as you are disconnected from the HSM.

>> Chapter 3 – General Functions

Overview

This chapter describes the general operational functions, provided by HSM Manager, to perform basic device management operations.

These functions are provided by the HSM Manager **File** menu, and include:

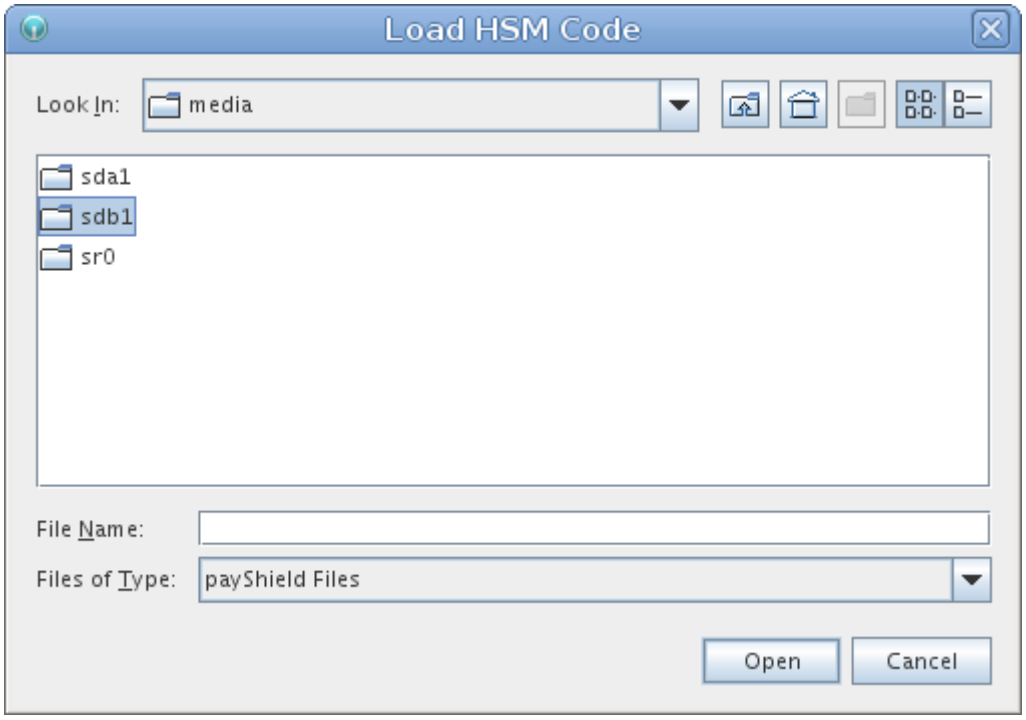
- **Connect** – to initiate a session with an HSM (see page 7).
- **Disconnect** – to terminate a session with an HSM (see page 15).
- **Login** – to login an Operator or Security Officer to an HSM (see page 9).
- **Logout** – to logout an Operator or Security Officer from an HSM (see page 15).
- **Load Settings** – to load previously saved settings into an HSM (see page 57).
- **Save Settings** – to save current HSM settings into a file (see page 55).
- **Load Firmware** – to load a new version of firmware into the HSM.
- **Load Licence** – to load a new licence into the HSM.
- **Exit** – to exit from the Local HSM Manager application.

Load Firmware

The **Load Firmware** option from the **File** menu allows users to update the firmware on the HSM. This function only operates when the HSM is in the Secure state.

Only firmware supplied by Thales can be loaded into the HSM. The firmware files should be stored on a regular Flash memory stick, and inserted into an available USB slot on the laptop/PC.

The first stage in the process is to select the firmware files. The *Load Firmware Wizard* will normally automatically locate the Flash memory stick folder and prompt the user to select the appropriate file.



If, instead, the "Knoppix" folder is offered in the *Look In* field, use the pull-down menu to select "/" and then double-click on "Media" in the main pane.

Note: The process of updating the HSM's firmware involves rebooting the HSM, which causes the Local HSM Manager to become disconnected from the HSM. On-screen prompts will guide the user through this process.

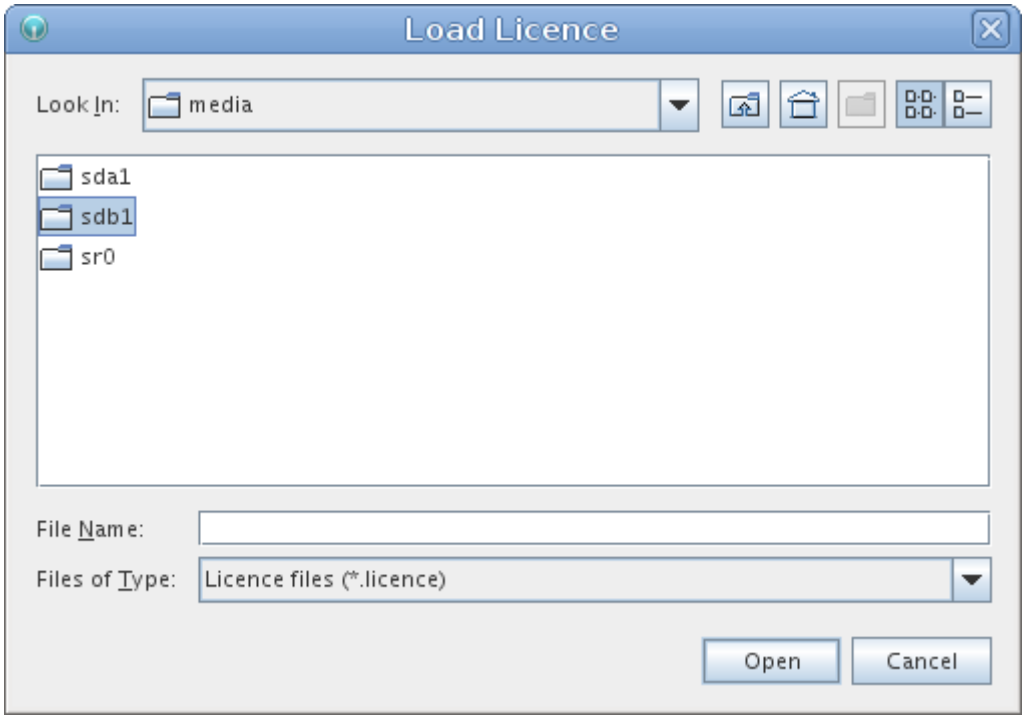
Once the upgrade is in progress, the user will be prompted to re-connect to the HSM (allowing sufficient time for the reboot process to complete – up to 3-4 minutes).

Load Licence

The **Load Licence** option from the **File** menu allows users to update the licence on the HSM. This function only operates when the HSM is in the Secure state.

Only licences supplied by Thales can be loaded into the HSM. The licence file should be stored on a regular Flash memory stick, and inserted into an available USB slot on the laptop/PC.

The first stage in the process is to select the licence file. The *Load Licence Wizard* will normally automatically locate the Flash memory stick folder and prompt the user to select the appropriate file.



If, instead, the "Knoppix" folder is offered in the *Look In* field, use the pull-down menu to select "/" and then double-click on "Media" in the main pane.

Note: The process of updating the HSM's licence involves rebooting the HSM, which causes the Local HSM Manager to become disconnected from the HSM. On-screen prompts will guide the user through this process.

Once the upgrade is in progress, the user will be prompted to re-connect to the HSM (allowing sufficient time for the reboot process to complete – up to 3-4 minutes).

>> Chapter 4 – Configuration Functions

Overview

This chapter describes the configuration functions, provided by HSM Manager for use by authorized users, to configure the HSM to work with the host system. It also includes those commands that provide information to assist with the installation and configuration of the HSM.

These functions are provided by the HSM Manager **Edit** menu, and include:

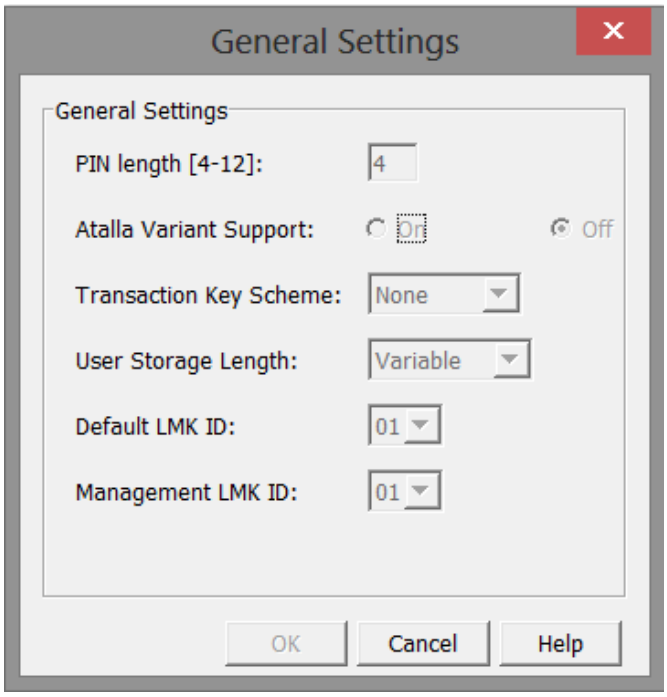
- **General Settings** – to view/modify general HSM settings.
- **Advanced Settings** – to view/modify important system settings.
- **Initial Settings** – to view/modify sensitive security settings.
- **Host Interface** – to view/modify host communications settings.
- **Printer Interface** – to view/modify serial and parallel printer communications settings.
- **Management Interface** – to view/modify management communications settings.
- **Host Commands** – to view/enable/disable individual or groups of host commands.
- **PIN Blocks** – to view/enable/disable individual PIN block formats.
- **Auditing** – to view/modify the list of audited events.
- **HSM Date/Time** – to view/set the HSM's internal clock.
- **Authorize** – to view/set the HSM's authorized state/activities.

Refer to *Appendix A - User Roles and Access Rights* to determine the access requirements for individual functions.

General Settings

The **General Settings** option from the **Edit** menu allows users to configure the HSM's general settings which contain non-critical security parameters.

When you select this menu option, the screen shown below is displayed.



The following parameters can be configured.

PIN Length

This value is used by the HSM to define the length of encrypted PINs, symbolized as "L" in the Host Command manuals in the "Length & Type" column. The value of L is one more than the value entered above for the PIN length.

Cleartext PINs (as entered into the BA host command) must have a length of L: shorter PINs can be entered, but must be padded to the right with hexadecimal F digits.

> For example, if the PIN Length been set to 6 (i.e. L = 7), and the 4-digit PIN "1234" is to be entered into the BA host command, the value that is included in the command is "1234FFF".

All LMK-encrypted PINs will have a length of L.

Where a PIN is generated (e.g. JA host command) and the PIN length specified in the command is less than L, the generated PIN will be padded to the right with hexadecimal F characters to a length of L digits.

When an LMK-encrypted PIN is decrypted using the NG host command, any F-padding used to expand a short PIN is presented in the decrypted PIN and will need to be stripped off to derive the shorter PIN.

The above information applies to the following host commands: BA, BC, BE, BG, BQ, CE, CQ, DE, DG, EE, G2, G4, GA, GU, JA, JC, JE, JG, NG, PE, PG, QC, QK, QW, XK, XM, ZM.**Note:** Once the length is set, it cannot be easily altered. If it has to be changed to accommodate longer PINs, all the existing encrypted PINs will have to be translated. This requires two operations: the old PINs are first translated to encryption under, for example, a ZPK; the HSM is then re-configured for the longer PIN length; the PINs are then translated back from the ZPK to the LMK.

Atalla Variant Support

For interoperation with Atalla systems. This enables the optional Atalla variants within commands. Any HSM Manager command providing key support will prompt for an Atalla variant.

Note: Selection has no effect on host commands - Atalla variants can be supplied with any appropriate command regardless of this setting.

Transaction Key Scheme

Transaction key schemes are techniques whereby data-encrypting keys change with each transaction in a manner that cannot be followed by a third party. The HSM supports three variants of transaction key schemes: Racal, Australian (AS2805) and DUKPT. There are command conflicts between the Racal and Australian scheme so only one can be selected. The use of the DUKPT commands are not affected by this setting.

Notes:

- The default value is now 'None'. In this case, none of the Racal or Australian transaction key scheme commands are available to the host.
- Use of this setting may modify the functionality associated with some Host commands. See Chapter 12 of the *payShield 9000 General information Manual* for further information.

User Storage Length

This is the length of the keys/data stored in user storage; it can be:

- A fixed-length value of single (8 bytes), double (16 bytes) or triple (24 bytes) length. The number of keys that can be stored depends upon this setting. Or
- Variable length.

See Chapter 16 of the *payShield 9000 General Information Manual* for more information on User Storage.

Default LMK ID

Identifies the Default LMK, which the HSM will use if it receives a command that does not explicitly state which LMK is to be used. The use of the Default LMK provides a "backward-compatible" mode, even when multiple LMKs are loaded in the HSM.

Options: 00 up to one less than the number of installed LMKs

Default: 00

Management LMK ID

Identifies the Management LMK, which will be used for authorizing certain management functions (e.g. setting the HSM's date/time), and for encrypting the audit MAC key.

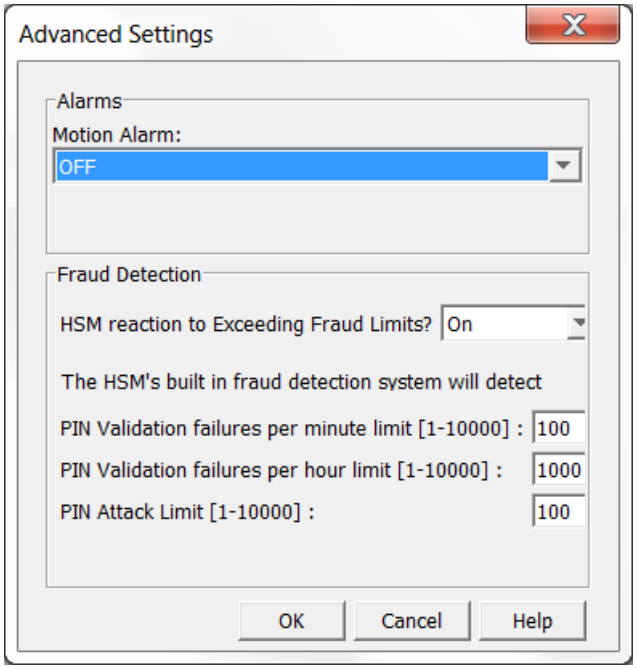
Options: 00 up to one less than the number of installed LMKs

Default: 00

Advanced Settings

The **Advanced Settings** option from the **Edit** menu option allows users to configure the HSM's advanced settings, which contain sensitive security parameters.

When you select this menu option, the screen shown below is displayed.



The following parameters can be configured.

Enable Movement Alarm

Select this checkbox to enable the movement alarm.

Enable Fraud Detection

Select this checkbox to enable internal fraud detection – for more information about the Fraud Detection functionality see Chapter 7 of the payShield 9000 General Information Manual or Appendix J of the HSM 8000 Console Reference Manual. When enabled, the following additional parameters are required:

- Per Hour Limit

  Enter a value between 1 and 10,000. This will be the limit on the number of failed PIN verifications permitted per minute.

- Per Minute Limit

  Enter a value between 1 and 10,000. This will be the limit on the number of failed PIN verifications permitted per hour.

- PIN Attack Limit

  Enter a value between 1 and 100. This will be the limit on the number of PIN attacks detected.

On the payShield 9000, the user can also select how the HSM reacts to the fraud limits being exceeded:

> "Logging Only"

The Health Check data (see Chapter 9) will show how often the limits have been exceeded (if gathering of Health Check statistics is enabled). An entry is also made in the Audit Log when any of the limits is exceeded.

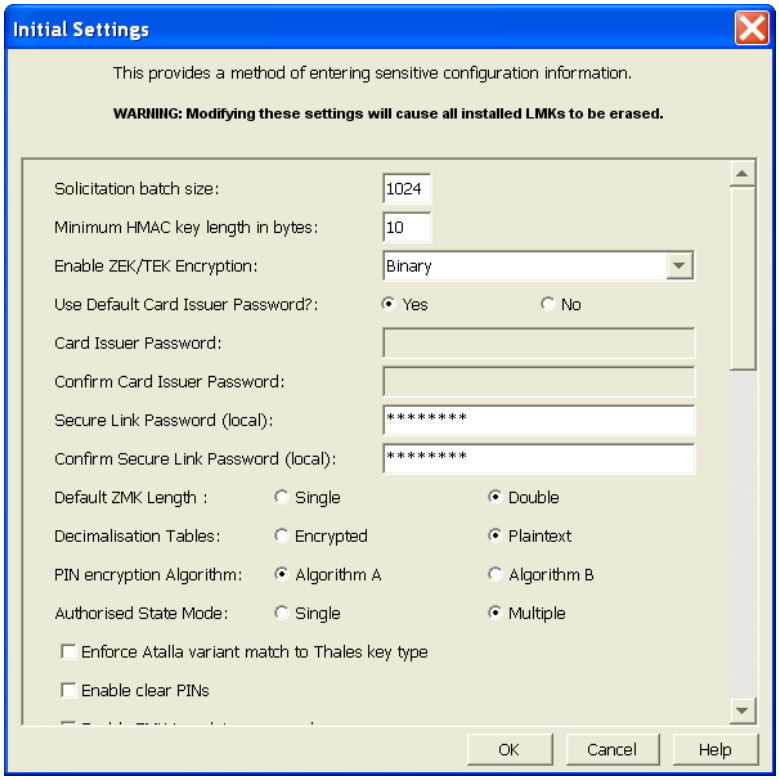
> "On"

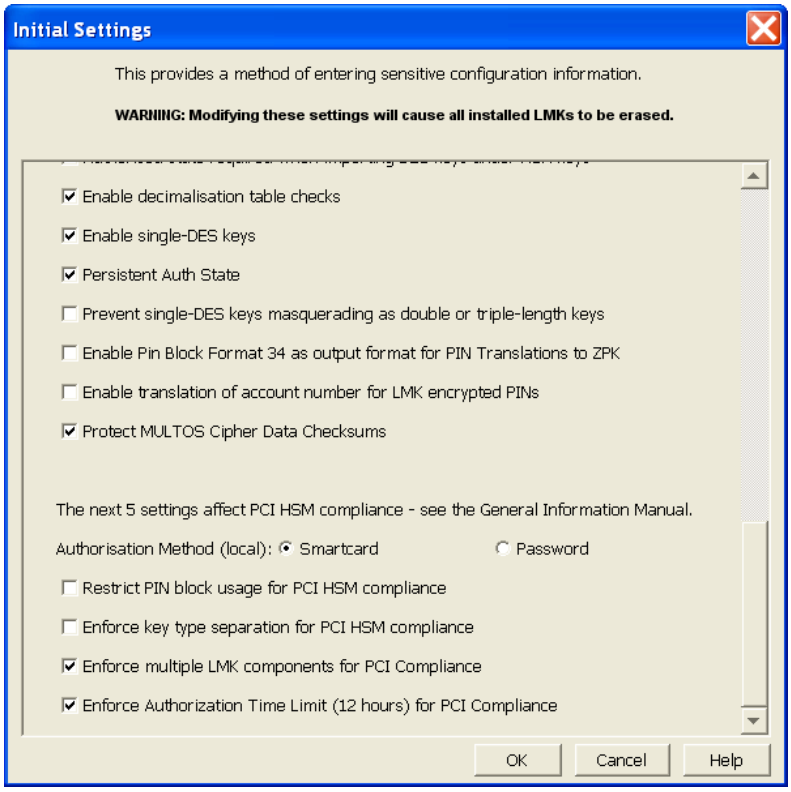
The Health Check data will log the limits being exceeded, but in addition the HSM will start returning error code 39 or delete its LMKs, as described in Chapter 7 of the payShield 9000 General Information Manual. An entry is also made in the Audit Log when any of the limits is exceeded.

Initial Settings

The **Initial Settings** option from the **Edit** menu allows users to configure the HSM's initial settings that are fundamental to the security of the HSM.

When you select this menu option, the screen shown below is displayed.





The following parameters can be configured.

Warning: Changing these parameters requires all LMKs to be erased from the HSM!

Solicitation batch size

A method supported by the HSM to enable customers to self-select their own PINs is to use Solicitation mailers. This is a turnaround form that is sent to the cardholder. The cardholder records the PIN selection on the form and returns it to the issuer. The mailer data consists of the cardholder name and address and a reference number (an encrypted account number). As a security measure, the form returned to the issuer contains only the reference number and the PIN selection. A batch process is used to process these requests when returned.

Options: 1 to 1024

Default: 1024

Minimum HMAC verification length in bytes

This setting determines the minimum lengths of HMAC keys that the HSM can generate. HMAC keys must satisfy the equation L/2 <= key length, where L = is the size of the hash function output. For SHA-1 HMAC keys, L=20, and therefore the key length must be at least 10.

Options: 10 to 99

Default: 10

Enable ZEK/TEK encryption

This setting determines the types of characters that the 'Message Encryption' host commands M0, M2 and M4 can encrypt/decrypt/translate (using a ZEK).

Options:

- ASCII: the plaintext message must contain only ASCII (0x20-0x7F) characters;
- Binary: no restrictions on the contents of the plaintext message;
- None: encryption using a ZEK is not permitted.

Default: None

Use Default Card Issuer Password?

For nearly all users, this setting should be "Yes".

Using the "No" setting is relevant only if customized smartcards are being used. In this case Thales will change the card issuer password for LMK and authorizing officer smartcards: a new password will be advised when new cards are delivered.

Card Issuer Password / Confirm Card Issuer Password

Only available if *Use Default Card Issuer Password* has been set to "No".

Options: 8-digit alphanumeric value

Secure Link Password / Confirm Secure Link Password

This setting allows the user to configure the password which is to be used to protect the HSM Manager/HSM communications.

Options: 8-digit alphanumeric value

Default: password

Default ZMK length

The length of the Zone Master Key: single or double. This is a backwards-compatible mode to enable the switching between 16H and 32H for ZMKs.

Options: Single or Double

Default: Double

Decimalization Tables

This setting determines if the decimalization table will be encrypted or in plain text. The default setting is encrypted, however, to allow for backward compatibility plaintext decimalization tables can be selected. It is recommended that encrypted decimalization tables are used to protect against decimalization table manipulation attacks.

Options: Encrypted or Plaintext

Default: Encrypted

PIN encryption algorithm

This selects the PIN encryption algorithm to be used when encrypted PINs are stored by the card issuer. The Racal algorithm is the best choice for a new installation; it is the stronger of the two methods. The Visa algorithm is offered for compatibility with older HSMs and for customers who already have a database of encrypted PINs.

When the Racal method is used, the output of the encryption is hex characters whereas the Visa method produces numeric digits. Commands that use encrypted PINs describe them as 'LN or LH'.

Options: A (Visa method) or B (Racal method)

Default: A (Visa method)

Authorized State Mode

This setting defines the granularity available when selecting authorized activities. Multiple allows precise selection of authorized activities (including timeout period if required). Single sets the HSM to a global Authorized state only (that is, on or off for all author sable commands).

Options: Single or Multiple

Default: Multiple

Enable clear PINs

This enables the clear PIN support via host commands 'NG' and 'BA'. Authorized state is a requirement for these commands to be processed by a host application.

Note: This is a security risk unless precautions are taken at the host.

Options: Yes/No

Default: No (unchecked)

Enable ZMK translate command

This enables the 'BY' command that allows the translation of Zone Master Keys from under another Zone Master Key. Authorized state is required for this command to process within a host application.

Note: The availability of this command is a significant security risk.

Options: Yes/No

Default: No (unchecked)

Enable X9.17 for import

This enables support for the ANSI X9.17 mechanism for key import. When being imported, each key of double or triple length is encrypted separately using the Electronic Code Book (ECB) mode of encryption. This is a lower security option. It is strongly recommended that the X9 TR-31 keyblock is used instead of X9.17.

Options: Yes/No

Default: No (unchecked)

Enable X9.17 for export

Similar to the previous item, but used when exporting keys.

Options: Yes/No

Default: No (unchecked)

Use HSM clock for date/time validation

If enabled, the HSM uses its integral real-time clock to validate check the start/end date/time optional header blocks of keyblocks (when present).

Options: Yes/No

Default: Yes (checked)

Additional padding to disguise key length

If enabled, the HSM disguises the length of single or double length keys within a keyblock by adding 8 or 16 extra padding bytes, such that single, double and triple length DES keys all appear to be triple length keys.

Options: Yes/No

Default: No (unchecked)

Key import/export in trusted format only

If enabled, the HSM will only import/export keys using a keyblock format. In this case, any export/import process using keys in variant format (including X9.17 format) will be prohibited.

Options: Yes/No

Default: Yes (checked)

Enable variable length PIN offset

If enabled, this will allow the IBM 3624 PIN Offset commands to return an Offset whose length matches the PIN, rather than being restricted to the Check Length parameter.

Options: Yes/No

Default: No (unchecked)

Enable weak PIN checking

If enabled, the HSM's PIN generation/derivation host commands will check to ensure that the PIN does not match one of the entries in the appropriate global 'Excluded PIN Table'. If a match is found in the list, then the command fails, returning error code 86.

Options: Yes/No

Default: No (unchecked)

Restrict Key Check Value to 6 hex chars

This setting determines whether Key Check Values (KCVs) should be restricted to consist of only 6 hex characters. The overall length of the KCV field will remain the same, regardless of this setting. However, when set to 'Yes', only the first 6 characters will contain the KCV: any remaining characters will be ignored (when input to the HSM) or set to '0' (when returned from the HSM).

Options: Yes/No

Default: Yes (checked)

Enable PKCS#11 import and export for HMAC keys

This setting determines whether the host commands LU and LW can import or export HMAC keys in PKCS#11 format.

Options: Yes/No

Default: No (unchecked)

Enable ANSI X9.17 import and export for HMAC keys

This setting determines whether the host commands LU and LW can import or export HMAC keys in ANSI X9.17 format.

Options: Yes/No

Default: No (unchecked)

Authorized state required when importing DES key under RSA Key

This setting determines whether Authorized State is mandatory for the import of DES keys using RSA keys (host command GI). When selected, the GI command always requires Authorized State (and the use of the signature field is optional). When not selected, the GI command does not require Authorized State.

Options: Yes/No

Default: Yes (checked)

Enable decimalization table checks

The values in the decimalization tables, used for deriving and verifying PIN offset values, are normally restricted to provide additional security by rejecting values which are potentially insecure. This can cause problems where existing tables fail the checks, so for backward compatibility this parameter allows the restrictions to be disabled.

Options: Yes/No

Default: Yes (checked)

Enable single-DES

This parameter is only valid if ZMK length is double. If selected, it permits the use of single-length DES keys.

Options: Yes/No

Default: No (unchecked)

Prevent Single-DES keys masquerading as double or triple-length key

When selected, all HSM commands that import double or triple-length DES keys will ensure that the imported key is not simply a single-length key masquerading as a double or triple-length key.

Options: Yes/No

Default: Yes (checked)

Enable PIN Block format 34 as output format for PIN translations to ZPK

If selected, the HSM will permit PIN block format 34 to be used as the output format of PIN translation commands.

Options: Yes/No

Default: No (unchecked)

Protect MULTOS Cipher Data Checksums (payShield 9000 only)

If selected, the HSM will encrypt checksums generated over sensitive data. This is appropriate to MULTOS card data preparation using optional license LIC023.

Options: Yes/No

Default: Yes (checked)

Enforce Atalla variant match to Thales key type

Only available if Atalla Variant Support is enabled. This setting is used to enforce key type matching in the A6 Host Command and IK Console Command during Atalla key import. The default is "No".

The next 5 settings affect PCI HSM Compliance:

Two of these settings apply to both HSM 8000 and payShield 9000, and the remainder applies to payShield 9000 only.

On a payShield 9000 running a software version which has been certified to the PCI HSM standard, the value of these settings affect whether the HSM is compliant with PCI HSM. (For more information about PCI HSM certification, see Chapter 10 of the *payShield 9000 General Information Manual*.)

On a payShield 9000 running a software version which has ***not*** been certified to the PCI HSM standard, the question of PCI HSM compliance is not relevant. However, the functionality provided by these settings may still be required by the user.

On the HSM 8000, no version of software is PCI HSM certified and so the question of PCI HSM compliance is not relevant. However, the functionality provided by the two available settings may still be required by the user.

Authorization Method

This option applies to both HSM 8000 and payShield 9000. It selects the method of authenticating security officers wishing to enter Authorized State or load LMKs at the Console, and also controls the method of authenticating Local HSM Manager users logging in as Operators and Security Officers.

Options: Smartcard or Password

Default: Smartcard

Notes:

- For PCI HSM compliance on the payShield 9000 the "Smartcard" option must be selected.

Restrict PIN block usage for PCI HSM compliance *(payShield 9000 only)*

This setting does not apply to the HSM 8000. It is used to select whether or not to enforce the restrictions on PIN Block format translation and usage required for PCI HSM compliance (see Chapter 10 of the *payShield 9000 General Information Manual*). If this option is not selected, PIN Block translations and usage will be as in earlier versions of payShield 9000 software – but the operation of the HSM will not be PCI HSM compliant.

Options: Yes/No

Default: No (unchecked)

Notes:

- For PCI HSM compliance on the payShield 9000 the "Yes" option must be selected.

Enforce key type separation for PCI HSM compliance

This option applies to both HSM 8000 and payShield 9000. It is used to select whether or not to use the key types required for PCI HSM compliance (see Chapter 10 of the *payShield 9000 General Information Manual*).

Setting this option to "Yes" on a payShield 9000 is a pre-requisite for the payShield 9000 to be PCI HSM compliant.

If this option is set to "No", the key types used in earlier versions of software will be applied – but the operation of the payShield 9000 will not be PCI HSM compliant.

This option is also available on the HSM 8000 (v3.3 or later): the purpose here is to allow the HSM 8000 to inter-operate with payShield 9000s which are PCI HSM compliant.

Options: Yes/No

Default: No (unchecked)

Notes:

- For PCI HSM compliance on the payShield 9000 the "Yes" option must be selected.

Enforce Authorization Time Limit *(payShield 9000 only)*

When this option is set, authorization of Console commands is limited to 12 hours. (Authorization of Host commands is not affected.)

Options: Yes/No

Default: Yes (checked)

Notes:

- For PCI HSM compliance on the payShield 9000 the "Yes" option must be selected.

Enforce Multiple Key Components *(payShield 9000 only)*

When this option is set, at least 2 components must be used when forming working keys and LMKs used for production.

Options: Yes/No

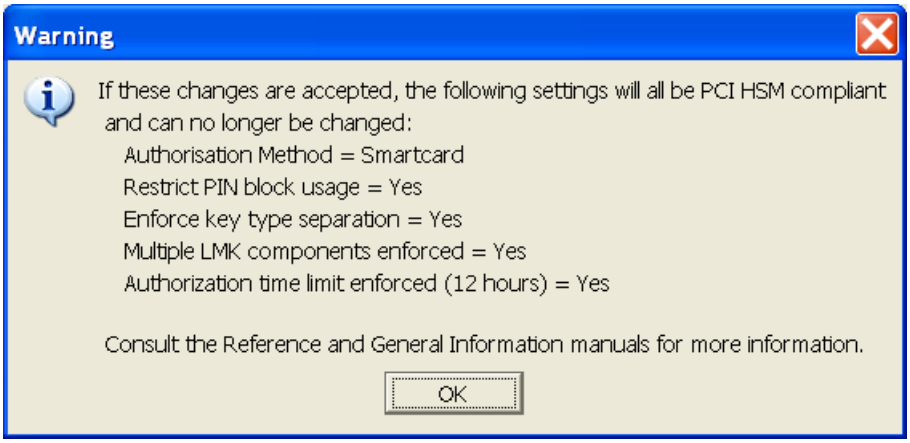
Default: No (checked)

Notes:

- For PCI HSM compliance on the payShield 9000 the "Yes" option must be selected.

On payShield 9000, if any of these settings have a non-compliant value for PCI HSM then the following window is displayed:

On payShield 9000, once all these settings have values which are PCI HSM compliant they cannot be changed. Therefore the user is asked to confirm that they really wish to give the last of these settings a compliant value:



If the user proceeds, these settings then become greyed-out and cannot be changed unless the Return to Factory Settings utility is used.

Host Interface

The HSM Host interface can be configured using the HSM Manager to emulate a number of types of data communications equipment and control equipment

The **Host Interface** option from the **Edit** menu allows users to select the emulation mode and enter the appropriate communications settings.

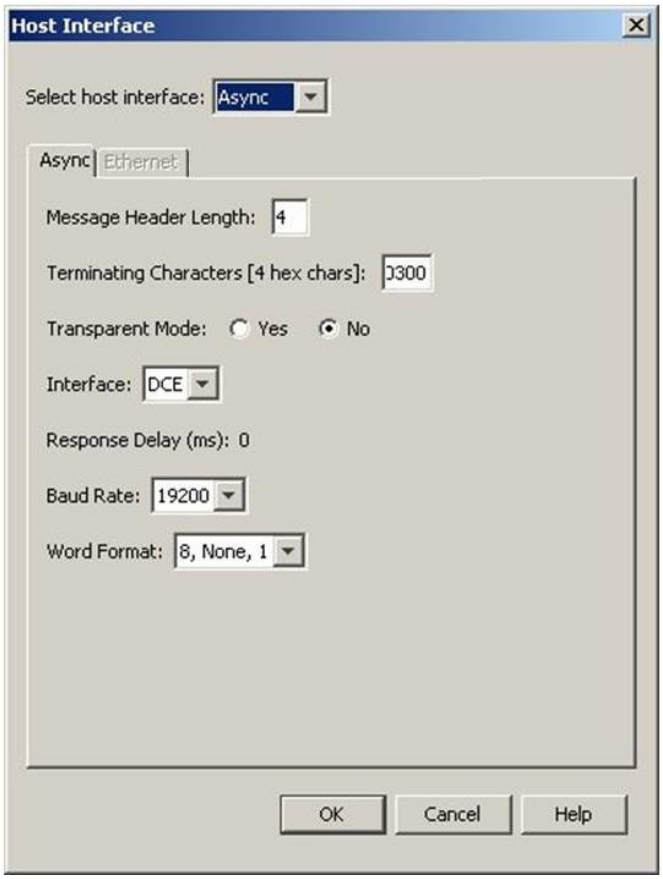
Select the emulation mode you require from the drop-down list at the top of the screen. The following options are available:

- *Asynchronous emulation* (standard or transparent)
- *SNA/SDLC synchronous emulation* (*HSM 8000 only*)
- *Ethernet*
- *ESCON (if available – HSM 8000 only*)
- *FICON* (*if available – payShield 9000 only*)
-

Once you have made a selection, the appropriate tab is displayed, allowing you to enter the required details.

Note: After entering the required parameters, the HSM needs to be restarted for the changes to take effect. You will be offered the option to restart now or to wait until the next time the HSM is restarted manually. Restarting the HSM now may cause your HSM Manager session to terminate.

Async mode



In Asynchronous Emulation the payShield 9000 is viewed by the Host as a DCE (data communications equipment) device, and does not require a modem. The HSM 8000 can be configured to be either a DCE or a DTE (Data Terminal Equipment, which requires a modem or cross-over cable.)

Note: a on the payShield 9000, USB port which has been configured for printer connection cannot be used for Asynchronous Host communications.

The following parameters can be configured.

Message Header Length

Each transaction to the HSM begins with a string of characters (header) which the Host can use to identify the transaction (or for any other purpose). The HSM returns the string unchanged to the Host in the response message. The length of the header can be set to any value between 1 and 255; the default value is 4.

Terminating Characters

The terminating sequence can be either one or two characters. To select the terminating characters four hexadecimal values must be entered. If only one terminating character is required, enter the first two hexadecimal values followed by 00.

If Transparent Mode is enabled, then the terminating characters are fixed at "0300".

Transparent Mode

In the standard asynchronous mode of communication, codes like STX (X'02) and ETX (X'03) have a special meaning, but they can sometimes occur in a stream of binary data, where that special meaning does not apply.

To avoid ambiguity, Transparent Asynchronous Communications mode is used. This has a simplified message format (for details see the Programmers Manual).

The Host port of the HSM must be configured for Transparent Async Communications and 8-bit data transfers.

Interface *(HSM 8000 only)*

Select whether the HSM is to emulate DCE or DTE operation.

Baud Rate

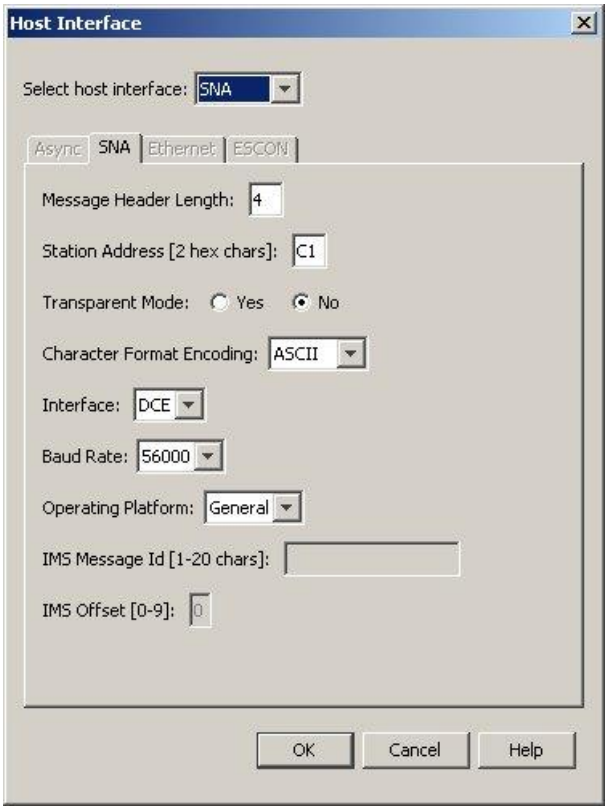
Select the baud rate that matches the host computer.

Word Format

Select the word format (no. of data bits, parity, no. of parity bits) that matches the host computer.

SNA Mode *(HSM 8000 only)*

Note: This dialog is only available when managing an HSM 8000.



The SNA-SDLC interface in the HSM emulates a 3274 Control Unit (CU) with a single device attached. At the SNA level, this control unit appears as two Network Addressable Units (NAU); a Physical Unit (PU) and a Logical Unit (LU). A standard 3274 CU contains 32 such LUs.

Note: IBM SRM users should refer to the relevant manual.

The electrical interface between the Host and the HSM conforms to the RS-232-C standard.

When the SNA-SDLC mode is selected, the standard HSM command/response message, as defined in the Programming Manual, is invalid. In an SDLC environment, the use of the start and end of text characters, STX and ETX, is not relevant, and they are omitted from all messages. Messages therefore start with the Message Header and end with either the last data element or the Message Trailer if it is present.

The following parameters can be configured.

Message Header Length

Each transaction to the HSM begins with a string of characters (header) which the Host can use to identify the transaction (or for any other purpose). The HSM returns the string unchanged to the Host in the response message. The length of the header can be set to any value between 1 and 255; the default value is 4.

Station Address

The station address is the address of the secondary station (in this case the HSM). This address must be the same as defined in the Host system configuration. The default address is X'C1.

Transparent Mode

If the "Normal" (default) setting is selected, the HSM scans each incoming message for any 3270 "Orders". When such an Order is found it is removed from the message and the HSM proceeds to process the message as normal.

If the "Transparent" setting is selected, 3270 Order removal is not carried out, and it is the responsibility of the Host system to ensure that 3270 Orders do not appear in the data sent to the HSM. Hence, in transparent data mode, the messages sent to the HSM can contain binary data.

Interface

Select whether the HSM is to emulate DCE or DTE operation.

Baud Rate

Select the baud rate that matches the host computer.

Not required if the Operating Platform is CICS.

Operating Platform

The HSM can be made compatible with an IBM Host running applications under the following modes:

- **IMS**

  In IMS applications, the HSM requires the entry of one or more test strings (the **IMS Message Identifier**) to enable it to distinguish between valid transactions and system error and status messages. When the Host software is written, the programmer must insert one of the test strings in the message header field of each valid transaction to the HSM.

  The HSM searches for the strings and accepts a transaction only if it contains one of them. It allows a maximum of 20 characters (including delimiters) to be entered. The strings, delimited by commas, can contain any

alphanumeric character, and do not need to be the same length. If more than one string is defined, the HSM accepts a transaction if it matches any one of them.

In addition, a test string offset (the **IMS Identifier Offset**) is required. This value allows the test string to be placed at any fixed position in the message header, by specifying the number of characters to skip before the comparison is made. It can be any value from zero to the message header length (but if the header length minus the offset is less than the length of a test string, that particular string will never be found).

All messages that do not have one of the test strings at the defined offset are ignored, and the HSM responds with a PA2 AID at the next poll.

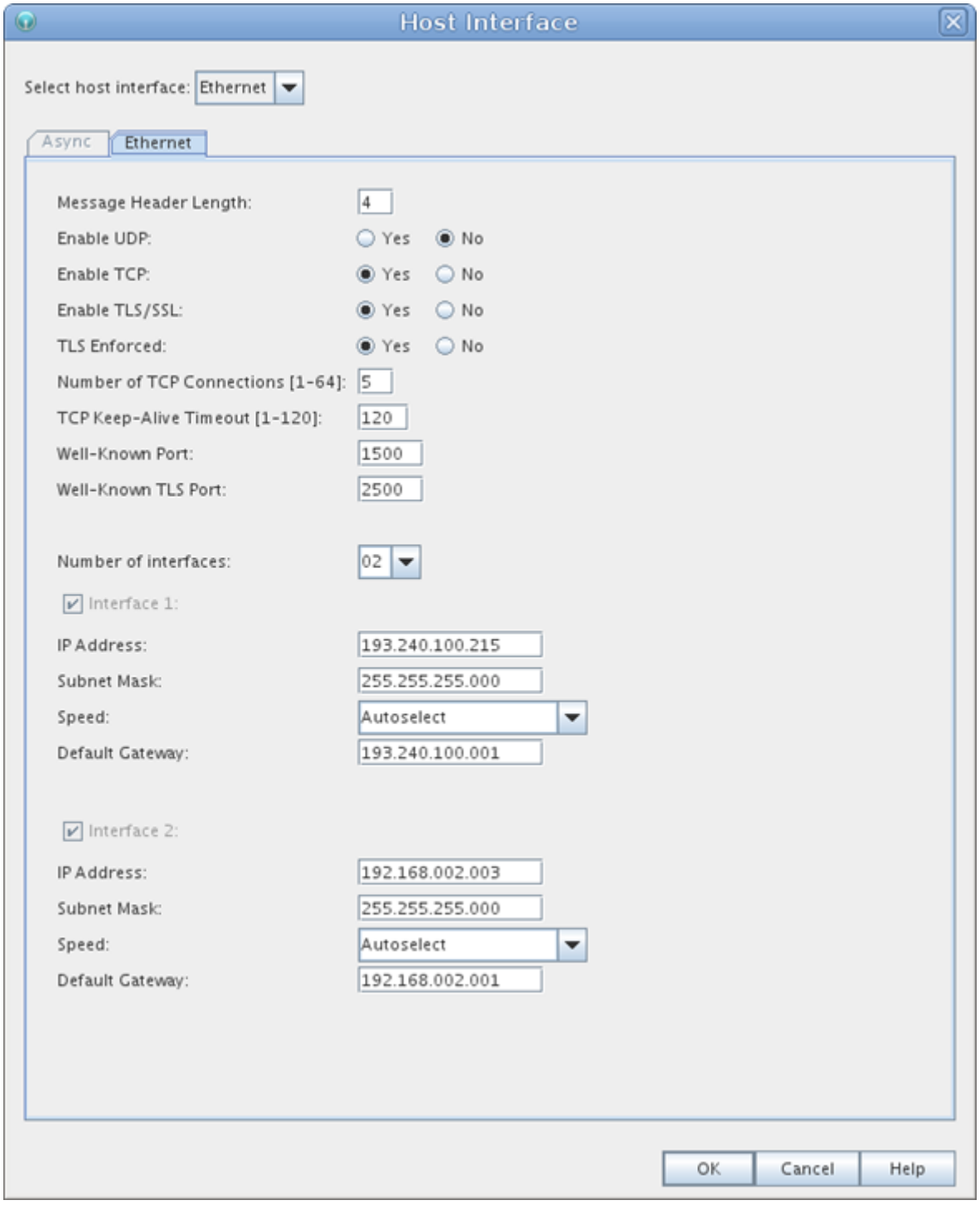
- **CICS**

  In CICS applications, the HSM searches the beginning of each transaction for the DFH string, which identifies all CICS system messages. If it is found, the message is ignored and the HSM responds with the CLEAR AID at the next poll.

- **General**

  Select this option when the host application is not running under IMS or CICS.

Ethernet Mode



The above example is for the payShield 9000, which provides 2 Host Ethernet interfaces and allows the port speed and duplexity to be set.

The HSM's Host Ethernet interface(s) support(s) the delivery of host commands via TCP/IP or UDP. The HSM 8000 has a single Host Ethernet interface supporting speeds of 10 and 100 Mbits/sec. The payShield 9000 (version 1.1 or later)

provides two Host Ethernet interfaces supporting speeds of 10, 100, and 1,000 Mbits/sec.

It is recommended that the Management Ethernet Port is on different IP subnet from the Host Ethernet Ports.

Notes relating to payShield 9000:

1. ***Where dual Ethernet host ports are in use, 2 different IP addresses at the Host computer must be used to drive the 2 ports on the HSM.***
2. ***The ROUTE Console command can be used to set up static routes from the HSM's Host ports to a Host IP address on a different subnet from the HSM.***

The following parameters can be configured.

Message Header Length

Each transaction to the HSM begins with a string of characters (header) which the Host can use to identify the transaction (or for any other purpose). The HSM returns the string unchanged to the Host in the response message. The length of the header can be set to any value between 1 and 255; the default value is 4.

Enable UDP

If this setting is No, then all UDP traffic received at the host port is discarded.

Enable TCP

If this setting is No, then all TCP traffic received at the host port is discarded.

Enable TLS/SSL

If this setting is Yes, then the use of TLS or SSL to protect host communications is enabled. (Requires installation of optional license HSM9-LIC036.)

TLS Enforced

If TLS/SSL has been enabled, setting the TLS Enforced setting to Yes means that only TLS can be used, and use of SSL is disallowed.

Enable ACL

If this setting is set to Yes, Access Control Lists are applied to control the IP addresses of which hosts can communicate with the HSM. The ACLs are set up using the **Edit / ACL** menu.

Number of TCP Connections

The payShield 9000 supports up to 64 concurrent TCP connections on each host port (unless UDP is also enabled, in which case the maximum is 63). Use this field to set the maximum number of concurrent connections that the HSM should allow: the same limit will apply to both host ports in the case of a payShield 9000.

If TLS/SSL is enabled, these connections are shared by the TLS/SSL and non-TLS/SSL traffic.

To achieve maximum throughput on the HSM it needs to be driven with multiple connections (or threads). Optimum performance is normally achieved with 4-8 threads (depending on the HSM performance model and the commands being processed). Running with only a single thread can significantly reduce the

throughput of the HSM, and means that you will not be able to reach the rated throughput for the machine.

TCP Keep Alive Timeout

This setting enables the HSM's TCP stack to periodically check whether the other end of a connection is still open. This allows the HSM to free resources by closing any unused connections.

Well-known Port

The Well-Known-Port address, which is the published TCP Port address of the HSM for non-TLS/SSL traffic, in the range 0 to 65535.

The HSM's default Well-Known Port for non-TLS/SSL traffic is 1500.

Well-known TLS Port.

The Well-Known-Port address, which is the published TCP Port address of the HSM for TLS/SSL traffic, in the range 0 to 65535.

The HSM's default Well-Known Port for TLS/SSL traffic is 2500.

The following items are set up for each host port:

IP Address

The IP address of the payShield 9000's host port. This must be a unique IP address on the host network. Note that DHCP allocation of the HSM's IP address is not supported.

Example: `192.168.001.010`

Subnet Mask

The subnet mask, which is used to define the network class.

Example: `255.255.255.000`

Speed *(payShield 9000 only)*

The speed and duplexity at which the host port is to run. This is available only for payShield 9000 HSMs.

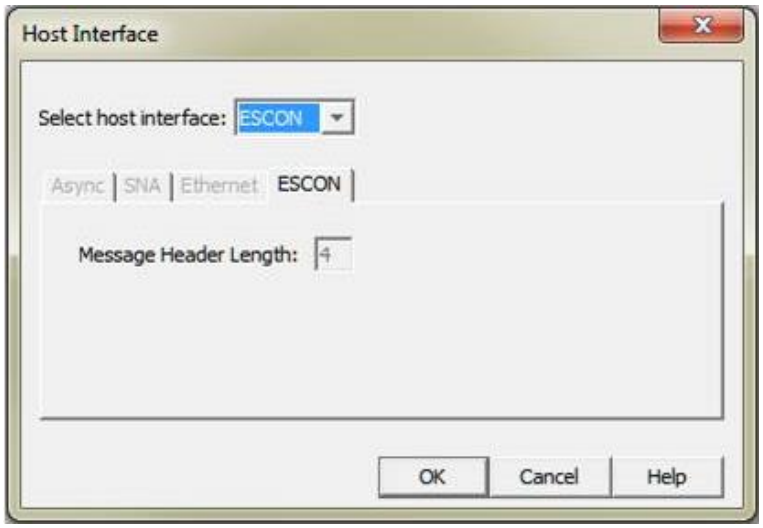
Default Gateway

The default gateway address, which is the IP address of the default gateway in the system.

Example: `192.168.001.001`

> ***Note:*** *When upgrading from a version of payShield 9000 software that does not support Default Gateways (i.e. versions up to 1.3) to a version that does support Default Gateways (i.e. versions 1.4 onwards), a default value for the Default Gateway IP address will be provided by the software. If the IP address for the port that was previously set up was A.B.C.D, then the default value of the Default Gateway IP address will be A.B.C.1.*

ESCON Mode *(HSM 8000 only)*



The HSM 8000 can be ordered with an optional ESCON option which provides one Host port with an ESCON interface.

The ESCON interface is a factory-fit option, and cannot be added to existing HSM 8000 units.

The ESCON interface is not available on the payShield 9000 (which supports FICON instead).

The following parameter is the only one that needs to be configured.

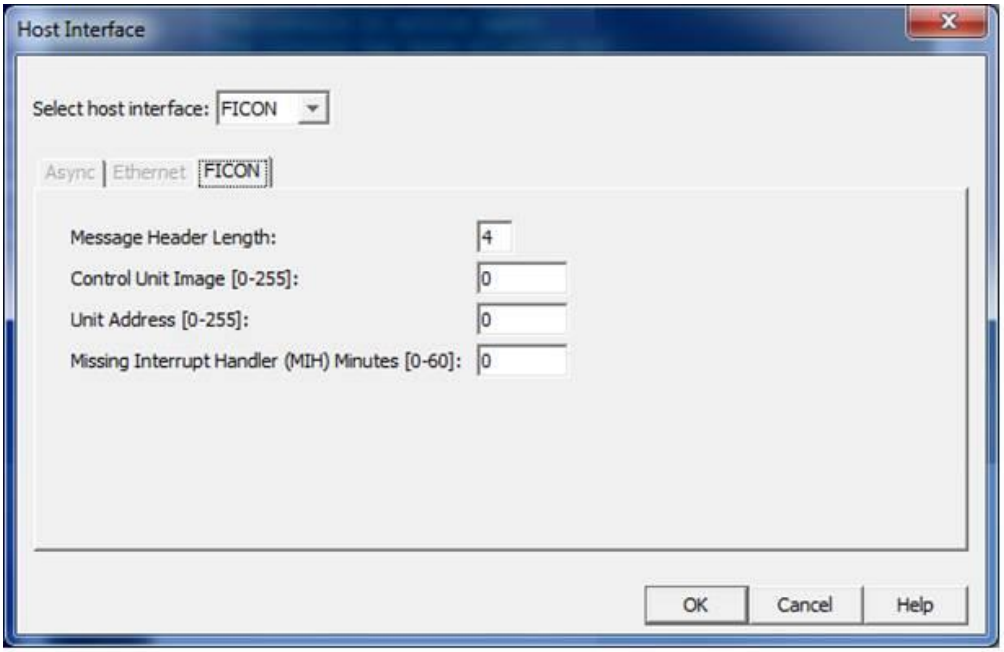
Message Header Length

Each transaction to the HSM begins with a string of characters (header) which the Host can use to identify the transaction (or for any other purpose). The HSM returns the string unchanged to the Host in the response message. The length of the header can be set to any value between 1 and 255; the default value is 4.

Note

When using the ESCON Host interface and turning the HSM 8000 to Online state, the HSM 8000 must be re-started.

FICON Mode *(payShield 9000 only)*



The payShield 9000 can be ordered with an optional FICON option which provides one Host port with auto-sensing FICON interface, which supports speeds of 2, 4, or 8 Gbps. Longwave and shortwave versions are available.

The FICON interface is a factory-fit option, and cannot be added to existing payShield 9000 units.

The following parameters can be configured.

Message Header Length

Each transaction to the HSM begins with a string of characters (header) which the Host can use to identify the transaction (or for any other purpose). The HSM returns the string unchanged to the Host in the response message. The length of the header can be set to any value between 1 and 255; the default value is 4.

Control Unit Image

This is the control unit address defined in the mainframe I/O definition. (CUADD on CNTLUNIT statement.) The value can be set to any value between 0 and 255; the default value is 0, and in most circumstances, installations will code 0 (the default) for the Control Unit Image.

Unit Address

The starting unit address for this control unit. 16 devices are enumerated from this point. (UNITADD on CNTLUNIT statement.) The value can be set to any value between 0 and 255; the default value is 0, and in most circumstances, installations will code 0 (the default) for the Unit Address.

Missing Interrupt Handler (mih) Minutes

This specifies the missing interrupt handler value to be used in the read device characteristics CCW for the mainframe. If set to 0, the mainframe setting is used. The value can be set to any value between 0 and 60; the default value is 0.

Printer Interface

A printer can be connected to allow the HSM to print PIN mailers or generate and print components of manually-distributed keys. A parallel or serial printer can be used.

On the HSM 8000:

- The printer port is used to drive a standard parallel printer (not a "Win-printer" type) implementing compatibility, nibble and byte mode data transfer. The interface is a 25-way 'D' type female connector (printer port) on the rear panel of the HSM. There are no configuration parameters for the parallel printer port.
- The auxiliary interface is used to drive a serial printer. The interface is a 25 way 'D' type plug (serial port) on the rear panel of the HSM. Character transmission rates and formats are specified by the user and can be configured at the time of HSM installation.

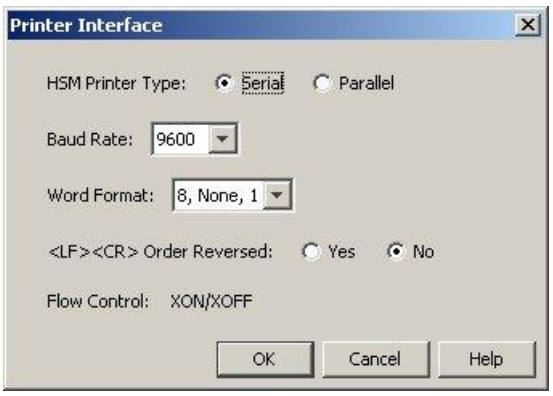
On the payShield 9000:

- A printer can be connected to any of the USB ports.
- A serial printer can be connected using a USB-Serial adaptor cable. This must be obtained from Thales, as these adaptors are intelligent devices and use a driver included in the HSM software. If it is not required to connect a console, the USB-Serial adaptor delivered with the payShield 9000 can be used to attach a serial printer.
- A parallel printer can be connected using a USB-Parallel 25-Pin or USB-Parallel Centronics adaptor cable. These adaptors must be obtained from Thales, as these adaptors are intelligent devices and use a driver included in the HSM software.
- A USB port which has been configured for printer connection cannot subsequently be used for Console connection or Asynchronous Host communications.

It is recommended that printers are located in a secure access-controlled area.

The **Printer Interface** option from the **Edit** menu allows users to configure the HSM's printer port settings.

When you select this menu option, the screen shown below is displayed.



The following parameters can be configured.

HSM Printer Type

This setting determines whether the HSM routes output to the serial or parallel printer.

Baud Rate (Serial Printers only)

Select the baud rate that matches the serial printer.

Word Format (Serial Printers only)

Select the word format (no. of data bits, parity, no. of parity bits) that matches the serial printer.

<LF> <CR> Order Reversed

Most printers send the characters <LF> followed by <CR> when starting a new line. Some, however, send these characters in the reverse order.

Select the option that is appropriate for your HSM printer.

Flow Control (Serial Printers only)

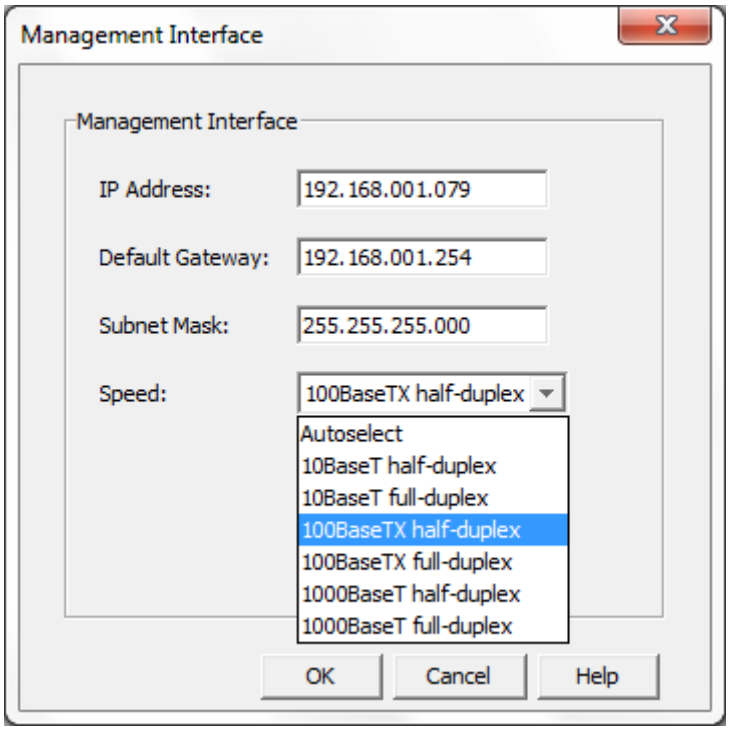
Select the flow control (XON/XOFF, hardware) that matches the serial printer.

Note: Only XON/XOFF is currently supported.

Management Interface

The **Management Interface** option from the **Edit** menu allows users to configure the HSM's management interface settings.

When you select this menu option, the screen shown below is displayed.



This example is for the payShield 9000, which allows the port speed and duplexity to be selected.

It is recommended that the Management Ethernet port is on a different subnet to the Host Ethernet Ports.

The following parameters can be configured.

IP Address

The IP address of the payShield 9000's management port. This must be a unique IP address on the management network. Note that DHCP allocation of the HSM's IP address is not supported.

Example: `192.168.002.010`

Default Gateway

The default gateway address, which is the IP address of the default gateway on the management network.

Example: `192.168.002.001`

> ***Note:*** *When upgrading from a version of payShield 9000 software that does not support Default Gateways (i.e. versions up to 1.3) to a version that does support Default Gateways (i.e. versions 1.4 onwards), a default value for the Default Gateway IP address will be provided by the software. If the IP address for the port that was previously set up was A.B.C.D, then the default value of the Default Gateway IP address will be A.B.C.1.*

Subnet Mask

The subnet mask, which is used to define the network class.

Example: `255.255.255.000`

Speed *(payShield 9000 only)*

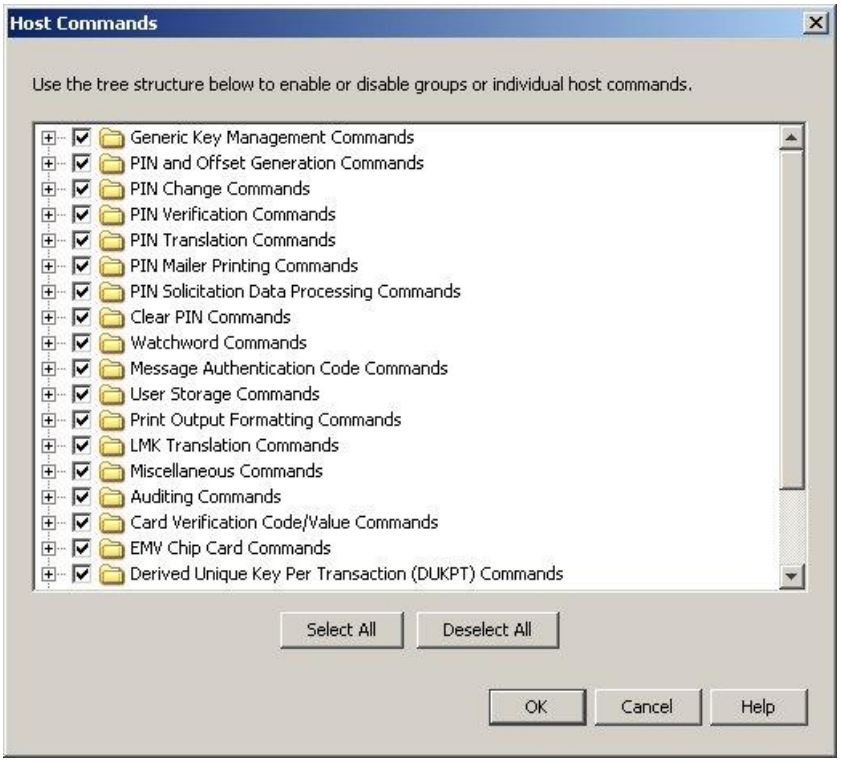
The speed and duplexity at which the host port is to run. This is available only for payShield 9000 HSMs.

Host Commands

Whilst new commands are added to the HSM software on a regular basis, old commands are rarely removed. As far as is possible, the HSM maintains backward compatibility with existing systems. A side effect is that host systems tend to use a subset of the commands actually provided by the HSM, leaving many commands unused.

The **Host Commands** option from the **Edit** menu allows users to select which host commands are to be enabled and which disabled.

When you select this menu option, the screen shown below is displayed.



Commands can be enabled or disabled in groups or individually by checking or unchecking the appropriate box(es) in the tree-like structure displayed. Checked items are enabled; unchecked items are disabled.

A simple but effective method of locking-down the HSM is to disable all unused host commands: the subsequent use of disabled commands would result in an error code (68) being returned.

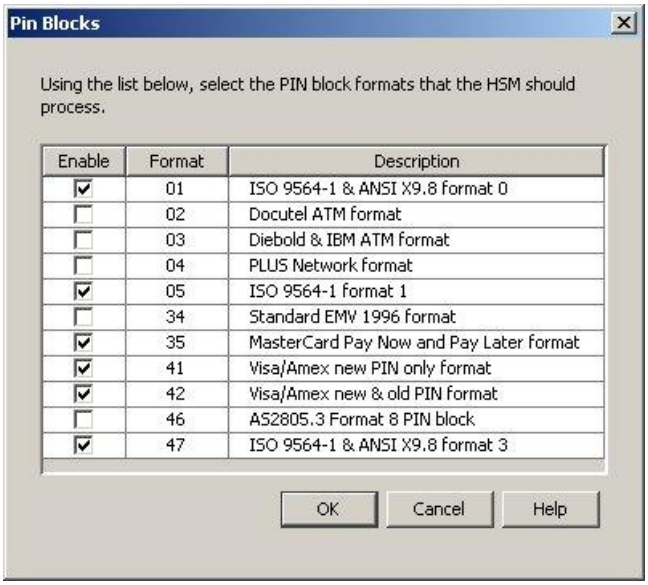
The **Select All** and **Deselect All** buttons switch all commands on or off and can be used if that provides a faster route to selecting the commands that are to be made available.

PIN Blocks

Like new commands, new PIN Block formats are added to the HSM software on a regular basis, and, as is the case for old commands, old PIN Block formats are not removed for reasons of backward compatibility. From a security perspective, some PIN Blocks are better than others: the better PIN blocks are diversified using the account number, and incorporate a certain number of random bytes for padding.

The **PIN Blocks** option from the **Edit** menu allows users to select which PIN Block formats are to be enabled and which disabled.

When you select this menu option, the screen shown below is displayed.



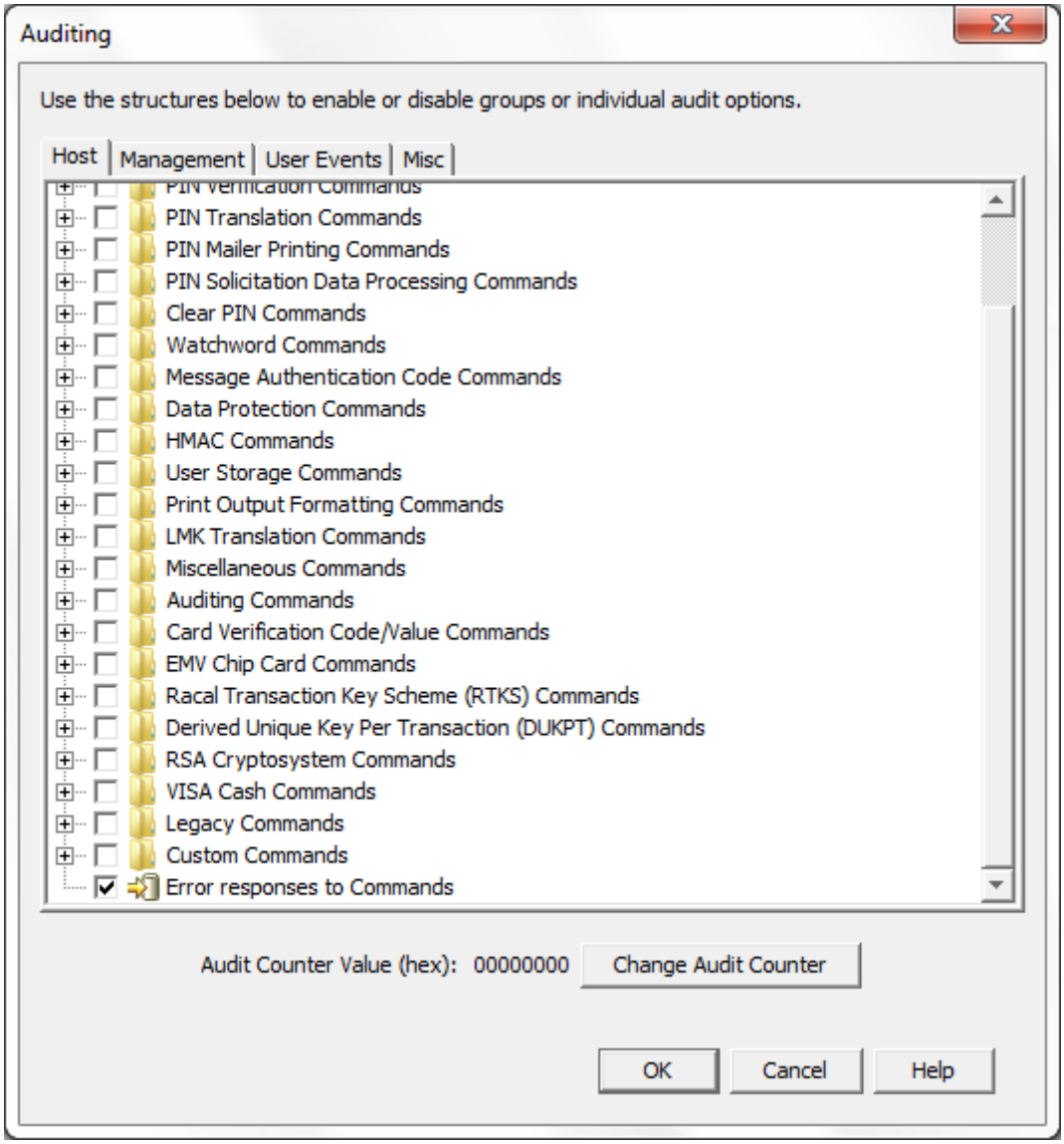
A host system would typically not use all the PIN Block formats supported by the HSM. A simple but effective method of locking-down the HSM is to disable (uncheck) all unused PIN block formats: the subsequent use of a disabled format would result in an error code (69) being returned.

Note: usage of PIN Block formats is also controlled by some of the items in the **Initial Settings** menu.

Auditing

The HSM's standard auditing capabilities include auditing (i.e. logging) of various events in the HSM's Audit Log. The **Auditing** option from the **Edit** menu allows users to select which items are to be audited and which are not.

When you select this menu option, the screen shown below is displayed.



Additional information about the Audit Log and how to manage it can be found at Chapter 17 of the *payShield 9000 General Information Manual*.

"Host" tab

It is possible to audit any of the host commands available in the HSM's license. Activities can be enabled or disabled in groups or individually by checking or unchecking the appropriate box(es) in the tree-like structure displayed. Checked items are enabled; unchecked items are disabled.

It is also possible to audit error responses returned to Host commands. This will result in an Audlit Log entry each time a relevant error response is returned to a Host command. In this context, "relevant" means an error that may require attention by the HSM operator: non-00 error codes are not audited where they are purely advisory or informational, or where they reflect business as usual (e.g. a customer entering an incorrect PIN). The non-00 error codes which are not audited are given in Appendix O of the *payShield 9000 Console Reference Manual*.

"Management" tab

It is possible to audit any of the listed HSM Manager menu items. Activities can be enabled or disabled in groups or individually by checking or unchecking the appropriate box(es) in the tree-like structure displayed. Checked items are enabled; unchecked items are disabled.

"User Events" tab

It is possible to select auditing of the following user events:

> *Power cycle* (i.e. off/on)

> *State change* (i.e. online/offline/secure)

> *Audit log cleared*

> *License file loaded*

> *LMK loaded/erased*

> *Old LMK loaded/erased*

"Misc" tab

This tab allows the following items to be audited:

- Self testing. This records the running of automatic (daily) self tests and any failures detected by the self tests.
- Attempts to use out-of-date certificates when establishing Secure Host Communication sessions.
- Failed communication attempts by host systems whose IP addresses were not included in the HSM's Access Control Lists.

Enforced Auditing *(payShield 9000 only)*

For conformance with the requirements of PCI HSM, certain events are always audited irrespective of what the user has specified. These events are:

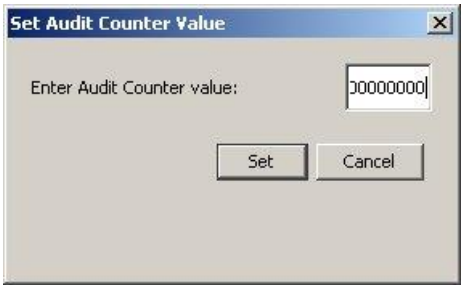
- Use of smartcards to authenticate users at HSM Manager
- Authorization of activities and cancellation of authorization.
- Key/component entry actions.

In all cases, the audited event will appear in the HSM's internal audit log.

Note: Auditing host or HSM Manager commands may impact HSM performance.

The audit log can hold a maximum of 2,000 entries (50,000 on the payShield 9000 from v1.4a). When the log is full, one entry is removed for every new one added. Records are removed in chronological sequence.

The **Change Audit Counter** button allows you to reset the current audit record number. When you click this button, the screen shown below is displayed.



Enter the new counter value you require, in Hex, and then click **Set**.

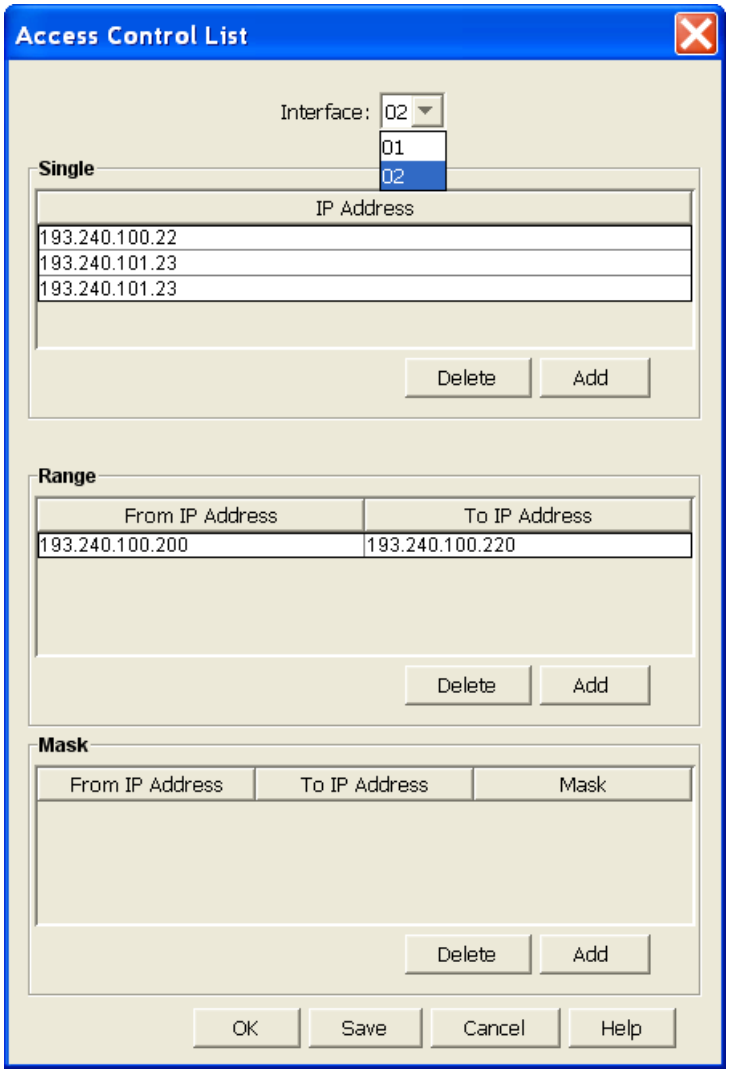
Note: To view the contents of the audit log, either use the host command Q2 to retrieve audit records or select **Logs** from the **View** menu.

ACLs (Access Control Lists)

The **ACL** option from the Edit menu enables users configure Access Control Lists for the payShield 9000 host ports. If the use of ACLs has been enabled in the Host Interface menu, connections to hosts will only be allowed if the host IP address appears in the ACL. A separate ACL is maintained for each of the host ports.

ACLs are relevant only to Ethernet connections (including those using Secure host Communications).

Entries in the ACL can consist of a single IP address, a range of IP addresses, or an IP address mask. Multiple entries can be made, and IP addresses in the various entries can overlap.

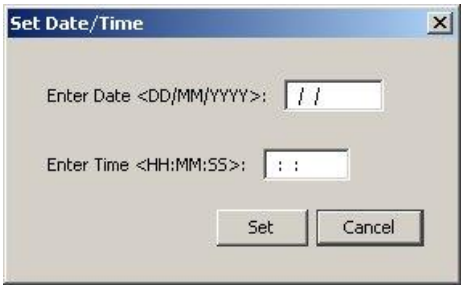


HSM Date / Time

The **HSM Date / Time** option from the **Edit** menu allows users to view and set the system time and date used by the HSM for the audit log entries. You should use this command to adjust the time for the local timezone.

When you select this menu option, the screen below is displayed - showing the current HSM date and time settings.

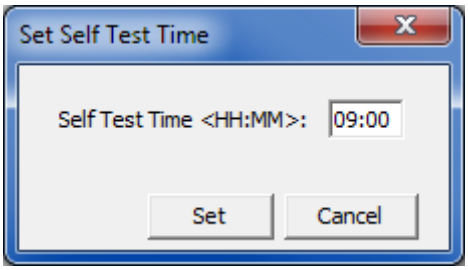
To change these setting, click on the **Set Date/Time** button. The screen shown below is displayed.



Enter the new date and time you require, in the formats shown, and then click on **Set**.

Set Self Test Time *(payShield 9000 only)*

The **Set Self Test Time** option from the **Edit** menu lets you set the time at which the payShield 9000's automatic, daily, self-tests are run. The default is 09:00 (9am). Any other time using the 24-hour clock (also known as "military time") can specified by using **Set**.



For the self tests to be run at the desired time, the HSM Date and Time must be correctly set, as described above.

Authorize

The HSM must be set into an Authorized state before certain 'privileged' functions can be performed. This can be achieved only by operators using their smartcard. The Authorized state is required for all operations that are more sensitive than normal, such as the entry of ZMK components and any other functions that involve clear unencrypted secret data.

The HSM has two possible authorization modes: Single or Multiple Authorization States:

- *Single* – gives operators access to all commands (an all-or-nothing on/off switch).
- *Multiple Authorization States* (or *activities*) – allow the authorization of commands that are available to operators to be restricted – only those necessary to perform the required task(s) are allowed. This enhances security.

The mode is defined by the **Initial Settings** option on the **Edit** menu. The default setting is Multiple Authorized States. This provides a higher level of security.

The way in which the Authorize function works depends upon the authorization mode currently being used.

Single mode

When running in Single authorization mode, the **Authorize** option from the **Edit** menu allows users to switch authorized mode on and off.

When you select this menu option, the screen shown below is displayed.

Check or uncheck the box, as required and then click on the **OK** button.

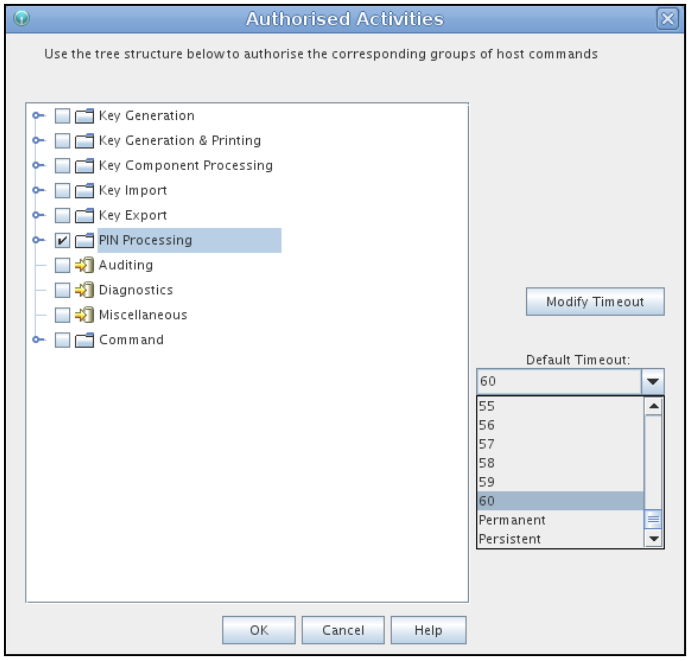
Note that on the payShield 9000 where the security setting *Enforce Authorization Time Limit has been set to "YES"*, authorisation of Console commands will expire after 12 hours in order to comply with the requirements of PCI HSM (see Chapter 10 of the *payShield 9000 General Information Manual*). This has no effect on users of HSM Manager, but will affect users who use the Console to manage the HSM. (Host commands and HSM 8000 Console commands continue to be authorised permanently.)

Multiple mode

When running in multiple authorization mode, the **Authorize** option from the **Edit** menu allows users to select which functions are to be authorized.

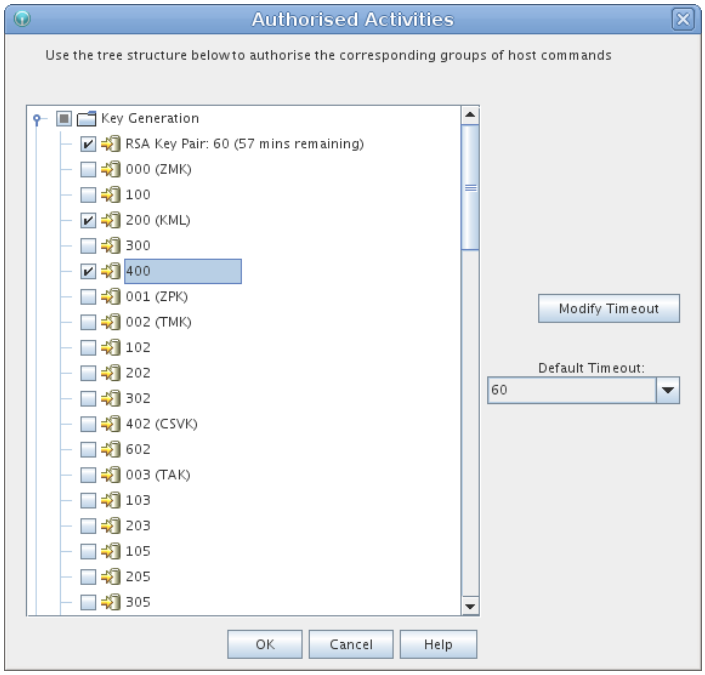
Note: The authorization is limited to the LMK of the operator that is logged in; i.e. the operator pertaining to LMK 01 can only authorize activities which use LMK 01.

When you select this menu option, the screen shown below is displayed.



Functions can be authorized or unauthorized in complete categories by checking or unchecking the appropriate box(es) in the tree-like structure displayed: in the above example, all host commands relevant to PIN processing are being authorized. Checked items are authorized; unchecked items are unauthorized.

It is also possible to authorize individual sub-categories of activity. A category can be expanded to show its sub-categories by clicking on the expansion symbol at the left-hand side against the category. This results in a dialogue box as follows:



In this example, the Key generation category has been expanded and the required sub-categories selected.

You can also set a Timeout period for the authorization. The drop-down list provides a range of periods from 1 to 60 minutes, or *Permanent*. Once the authorization period has elapsed, the HSM reverts to an unauthorized state. The *Persistent* option appears if this has been enabled in the Initial Settings: using this option also applies the *Permanent* setting.

Saving and Reusing Configuration Parameter Settings

HSM Manager allows the configuration parameters you define using the following menu options to be saved to a file and then re-loaded, if required again in the future.

- *General Settings*
- *Advanced Settings*
- *Initial Settings*
- *Host Interface*
- *Management Interface*
- *Printer Interface*
- *Host Commands*
- *PIN Blocks*
- *Audit settings*

Saving parameter settings to a file

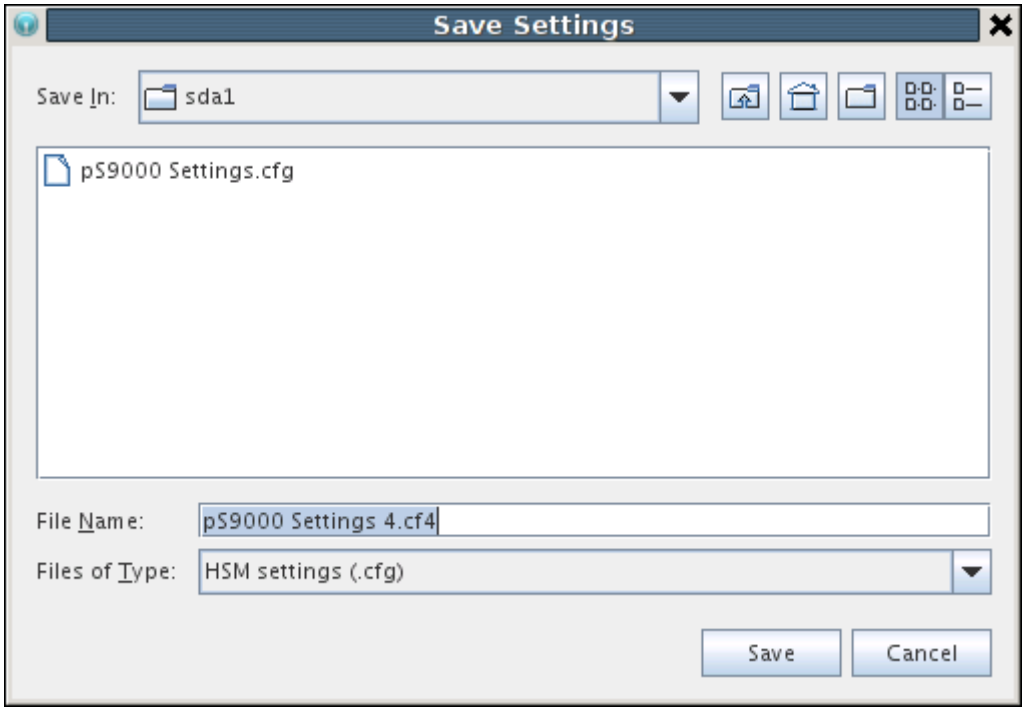
Saving your parameter settings allows you to make changes and then, if necessary, revert to your previous configuration.

To save your current parameter settings to a file, select the **Save Settings** option from the HSM Manager **File** menu. The resulting file has a .cfg extension, and can be read using standard text editors.

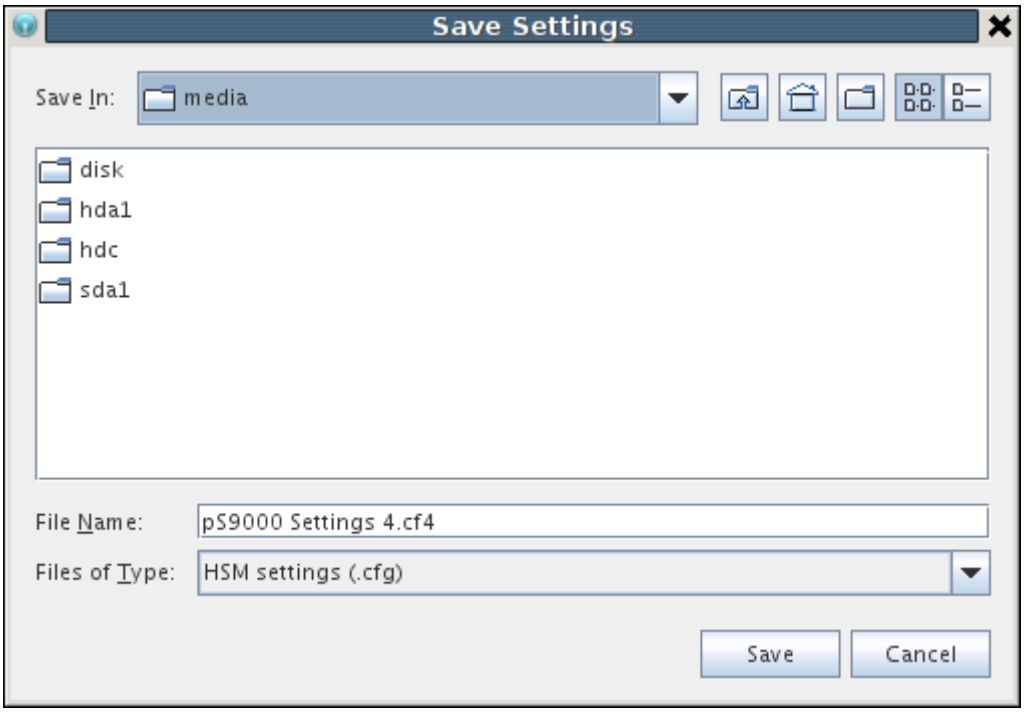
The following procedure can be used to save the settings to a USB Drive (such as a memory stick).

1. Follow the procedure for *Mounting the USB Drive* under *Capturing Screenshots to a USB Drive* in *Chapter 10: Knoppix Tools*.

2. Select *Save Settings* in the HSM Manager *Edit* menu. This will present the *Save Settings* dialogue box:



3. Use the *Save in:* drop-down menu to select the folder that contains your USB Drive. (In the example in Chapter 10, this is *media*):



The offered *Save In* location may already show the USB device. If instead "Knoppix" is offered, use the pull-down menu to select "/" and then double-click on "Media" in the main pane.

(You can also save the settings temporarily within Knoppix by selecting / in the *Save in:* menu and double-clicking on *tmp*.)

4. Double-click on the name of your USB Drive - in the example in Chapter 10, this is *disk*. This will display the list of any existing .cfg files on the USB Drive.
5. Edit the file name, if required, and click on *Save*.
6. You will then be offered a dialogue box which lets you choose whether to encrypt the data:

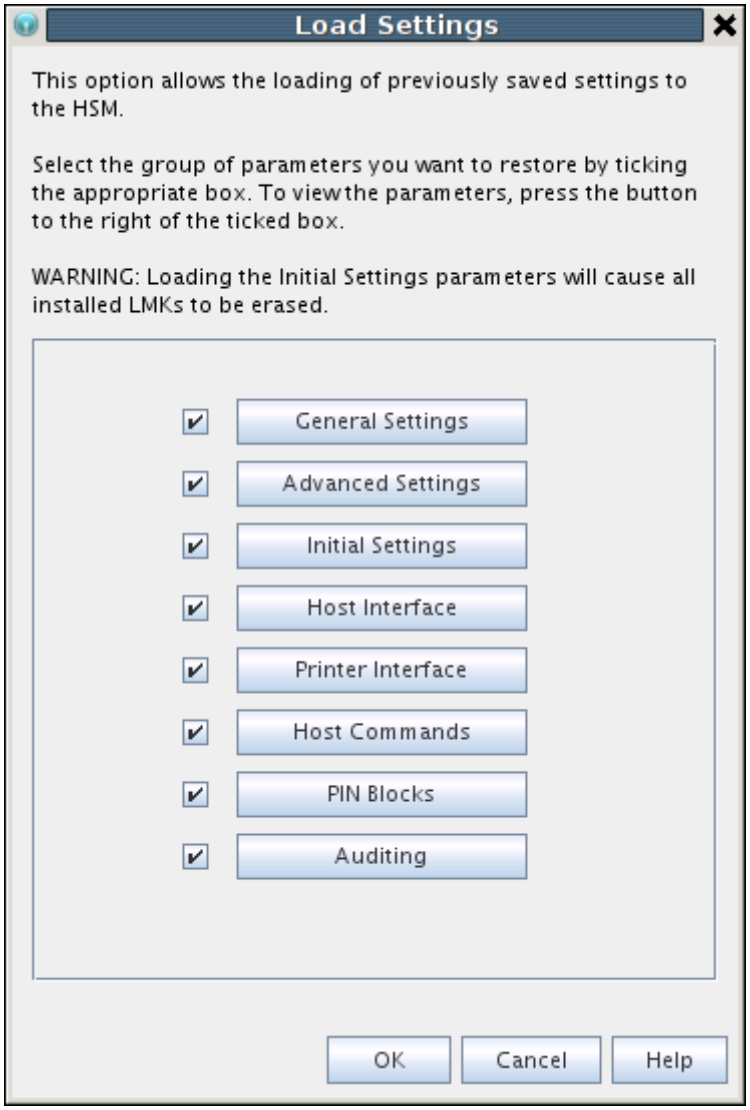
7. If additional settings are to be saved, steps 1, 3, and 4 can be omitted.

Reloading parameter settings from a file

To reload parameter settings that you have previously saved to a file, select the **Load Settings** option from the HSM Manager **File** menu.

The procedure for loading settings from a USB Drive is the same as steps 1-5 for saving the settings as described above (except that *Load* is used instead of *Save* at step 5).

You will then be presented with a selection screen to let you choose which settings you want to load:



To view settings saved to a file in the Knoppix /tmp directory, follow the procedure outlined in Chapter 10 under *Capturing and Viewing Screenshots temporarily in Knoppix*.

>> Chapter 5 – Viewing Information and Managing Logs

Overview

This chapter describes the facilities provided by HSM Manager that allow authorized users to view/erase the HSM's internal logs and view the firmware details.

These functions are provided by the HSM Manager **View** menu, and include:

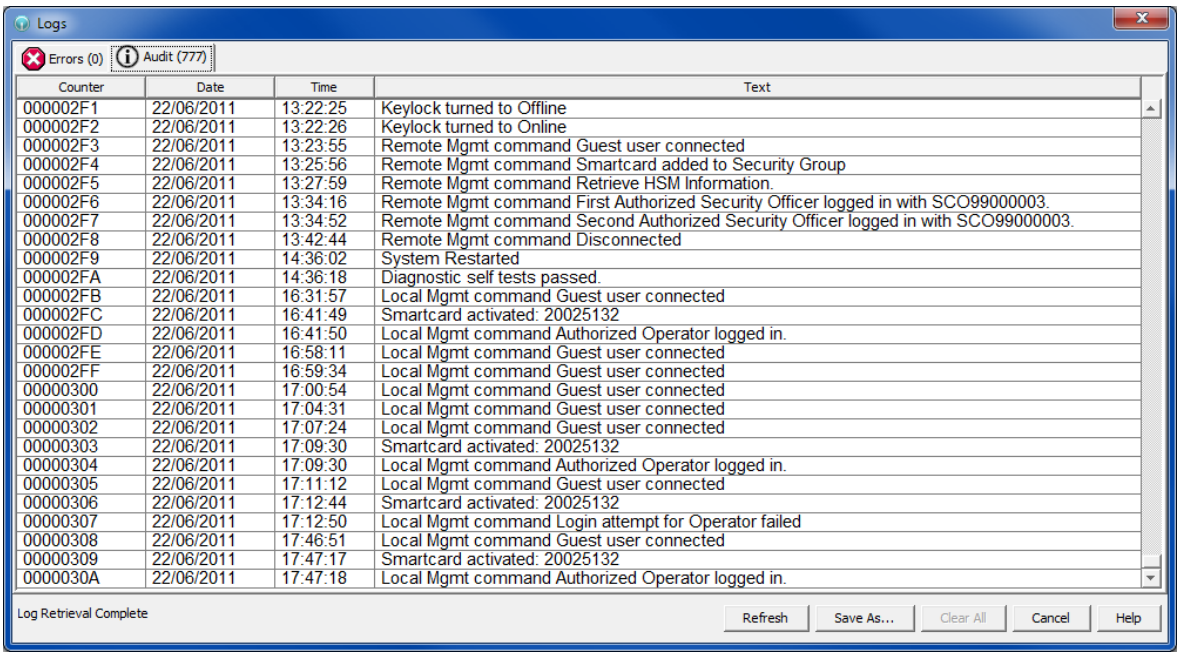
- **Logs** – to view/erase the HSM's internal error and audit log.
- **HSM Information** – to view the HSM information (firmware, licenses, etc.).
- **Remote Details** – to view the remote management configuration details.

Refer to *Appendix A - User Roles and Access Rights* to determine the access requirements for individual functions.

Managing the Audit and Error Logs

The **Logs** option from the **View** menu allows users to view and manage the HSM's error and audit logs.

When you select this menu option, the screen shown below is displayed. This screen consists of two tabs: one for the audit log and one for the error log. Each tab, along with the log name, displays the number of log entries returned from the device. Each log is displayed in a scrollable pane. The scrollbar is only visible if the number of log entries exceeds the amount that can fit in the window.



Counter	Date	Time	Text
000002F1	22/06/2011	13:22:25	Keylock turned to Offline
000002F2	22/06/2011	13:22:26	Keylock turned to Online
000002F3	22/06/2011	13:23:55	Remote Mgmt command Guest user connected
000002F4	22/06/2011	13:25:56	Remote Mgmt command Smartcard added to Security Group
000002F5	22/06/2011	13:27:59	Remote Mgmt command Retrieve HSM Information.
000002F6	22/06/2011	13:34:16	Remote Mgmt command First Authorized Security Officer logged in with SCO99000003.
000002F7	22/06/2011	13:34:52	Remote Mgmt command Second Authorized Security Officer logged in with SCO99000003.
000002F8	22/06/2011	13:42:44	Remote Mgmt command Disconnected
000002F9	22/06/2011	14:36:02	System Restarted
000002FA	22/06/2011	14:36:18	Diagnostic self tests passed.
000002FB	22/06/2011	16:31:57	Local Mgmt command Guest user connected
000002FC	22/06/2011	16:41:49	Smartcard activated: 20025132
000002FD	22/06/2011	16:41:50	Local Mgmt command Authorized Operator logged in.
000002FE	22/06/2011	16:58:11	Local Mgmt command Guest user connected
000002FF	22/06/2011	16:59:34	Local Mgmt command Guest user connected
00000300	22/06/2011	17:00:54	Local Mgmt command Guest user connected
00000301	22/06/2011	17:04:31	Local Mgmt command Guest user connected
00000302	22/06/2011	17:07:24	Local Mgmt command Guest user connected
00000303	22/06/2011	17:09:30	Smartcard activated: 20025132
00000304	22/06/2011	17:09:30	Local Mgmt command Authorized Operator logged in.
00000305	22/06/2011	17:11:12	Local Mgmt command Guest user connected
00000306	22/06/2011	17:12:44	Smartcard activated: 20025132
00000307	22/06/2011	17:12:50	Local Mgmt command Login attempt for Operator failed
00000308	22/06/2011	17:46:51	Local Mgmt command Guest user connected
00000309	22/06/2011	17:47:17	Smartcard activated: 20025132
0000030A	22/06/2011	17:47:18	Local Mgmt command Authorized Operator logged in.

Select the tab appropriate to log you want to work with.

Notes:

- From v4.2.0 the Audit Log, because of its potential length, is displayed with most recent entries first. The Error Log continues to be displayed with oldest records first.
- From v4.2.0, power supply errors are added to the error log as soon as they are detected. In earlier versions, these errors appeared in the error log only at startup.

For both logs, the following buttons are displayed at the bottom of the screen.

> **Refresh** - re-displays the screen to include any additional entries which have occurred since you started to view or carried out the last refresh.

> **Save As** - allows you to save the current log to a file. See the section on *Saving parameter settings to a file* for guidance on how to use this facility.

> **Clear All** - clears the log.

> **Cancel** - closes the log display window.

> **Help** - displays on-screen help.

Error log

The Error log stores fault information for use by Thales e-Security support personnel. The Error Log file has enough space for about 500 error codes and sub-codes entries. It is important to regularly view and clear the Error Log. It the Error Log file is allowed to reach its maximum size, the next error report will cause the existing Error Log file to be erased. The error log is used to log unexpected software errors, hardware failures and alarm events.

Newly detected errors cause the Error LED on the front panel to flash until such time as the Error Log is viewed.

Appendix A of the *payShield 9000 General Information Manual* describes the Error Log when viewed from the Console. There are some differences when viewing the Error log through HSM Manager, and these are described below.

Here is an example of part of an Error Log output. In this case, the Error Log has been saved to a text file: the same information is displayed when the Error Log is viewed in HSM Manager:

```
ERROR LOG - # of Entries: 101
 Date        Time       Severity       Code  Text
 …
 15/01/2014  16:13:47   MAJOR          3     Power Supply:    FAILED (PSU 2 Failed)
 15/01/2014  16:13:48   RECOVERABLE    4     Tamper(1) Latched at [2014/01/15, 16:13:23]
 15/01/2014  16:13:48   RECOVERABLE    4     Tamper  Latched  State  [LR1  =  0x0100,  LR2  =
0x0010]
 15/01/2014  16:13:48   RECOVERABLE    4        Tamper   LR1   [0x0100   =   Microcontroller
signaled tamper condition]
 15/01/2014  16:13:48   RECOVERABLE    4        Tamper LR2 [0x0010 = Case switch two open]
 15/01/2014  16:14:14   MAJOR          3     Power Supply:    FAILED (PSU 2 Failed)
 15/01/2014  16:14:14   RECOVERABLE    4     Tamper(2) Latched at [2014/01/15, 16:13:48]
 15/01/2014  16:14:14   RECOVERABLE    4     Tamper  Latched  State  [LR1  =  0x0100,  LR2  =
0x0010]
```

```
 15/01/2014  16:14:14   RECOVERABLE    4        Tamper   LR1   [0x0100   =   Microcontroller
signaled tamper condition]
 15/01/2014  16:14:14   RECOVERABLE    4        Tamper LR2 [0x0010 = Case switch two open]
 15/01/2014  16:14:14   RECOVERABLE    4     Tamper  Current  State  [CR1  =  0x0000,  CR2  =
0x8000]
 15/01/2014  16:14:14   RECOVERABLE    4        Tamper CR2 [0x8000 = DS3640 TEI asserted]
 15/01/2014  16:14:14   RECOVERABLE    4     Attempting to clear tamper(2)
 15/01/2014  16:14:15   RECOVERABLE    4     Tamper cleared on try (2)
 …
```

Date / Time

The date and time at which the specific error log entry was generated. This field reflects the HSM's internal real-time clock – not necessarily the local time.

Severity

The severity description of the error that occurred. These Severity descriptions are described in a different way to those described in the *payShield 9000 General Information Manual*. The following severity descriptions are used :

- *Informative* - Something abnormal happened, but was not important.
- *Recoverable* - Something abnormal happened, but the unit recovered from it without rebooting or losing data.
- *Major* - Something abnormal happened, but the unit recovered from it but may have lost data/information due to restarting a process or re-initializing hardware. The unit may not function in a full capacity.
- *Catastrophic* - Something abnormal happened, and the unit had to reboot to recover.

Only catastrophic errors cause the HSM to reboot.

Code

The error code, which indicates the type of error that occurred. This corresponds to the Error Code described in the *payShield 9000 General Information Manual*, but displayed as a simple decimal integer: for example, an error code of `0x00000004` (as described in the *payShield 9000 General Information Manual)* is displayed in HSM Manager as "4".

The Error Sub-Codes as described in the *payShield 9000 General Information Manual* are not displayed in HSM Manager.

Text

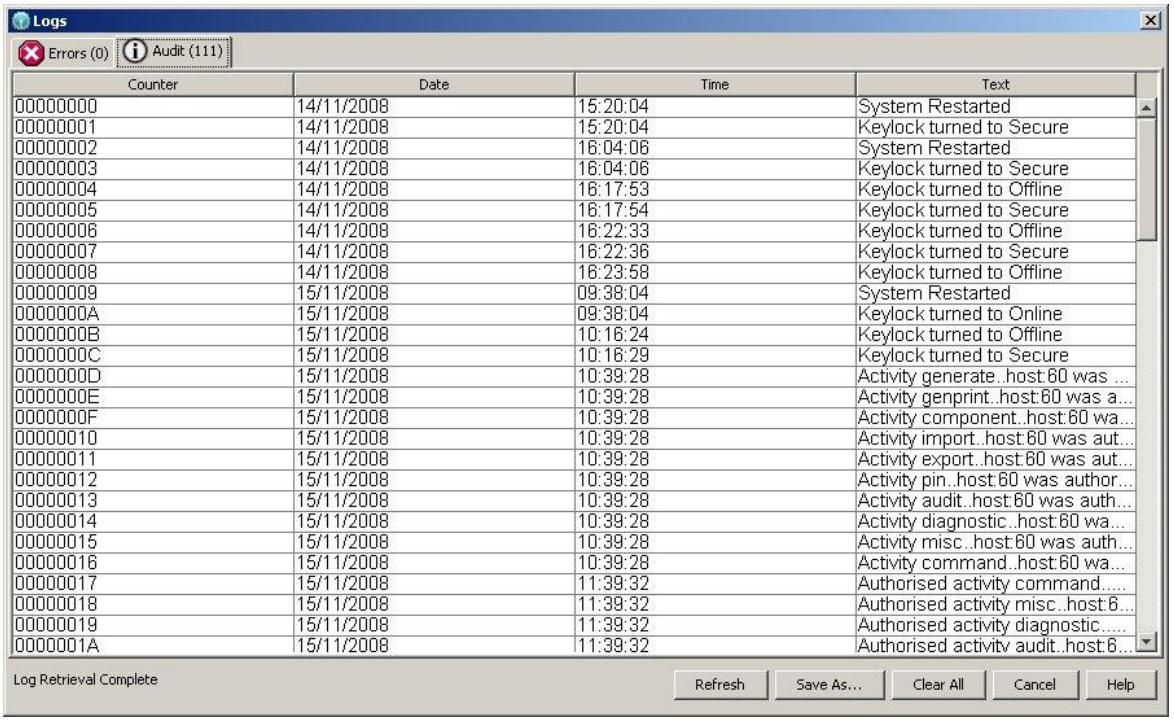
A description of the error code. This is the same as the error code Description as outlined in the *payShield 9000 General Information Manual* – i.e. the same as the text contained inside the square brackets ([…]) in the console output.

Audit log

The Audit journal contains 2,000 entries (50,000 for payShield 9000 from v1.4a) for audit records. Whenever the HSM state is altered through power-up, state changes or HSM Manager commands, the Audit log is updated with the action and the time and date. The Audit log can also be configured to record execution of almost any HSM Manager or host command, using the **Auditing** option on the HSM

Manager **Edit** menu (see *Chapter 4 - Configuration Functions*, for details). The audit records are added to the log until it is 100% full and for each subsequent record the earliest (i.e. oldest) record in the log is deleted to make room for the new one.

A number of host commands are available which allow the host computer to extract and archive (print) audit records from the HSM.



Counter	Date	Time	Text
00000000	14/11/2008	15:20:04	System Restarted
00000001	14/11/2008	15:20:04	Keylock turned to Secure
00000002	14/11/2008	16:04:06	System Restarted
00000003	14/11/2008	16:04:06	Keylock turned to Secure
00000004	14/11/2008	16:17:53	Keylock turned to Offline
00000005	14/11/2008	16:17:54	Keylock turned to Secure
00000006	14/11/2008	16:22:33	Keylock turned to Offline
00000007	14/11/2008	16:22:36	Keylock turned to Secure
00000008	14/11/2008	16:23:58	Keylock turned to Offline
00000009	15/11/2008	09:38:04	System Restarted
0000000A	15/11/2008	09:38:04	Keylock turned to Online
0000000B	15/11/2008	10:16:24	Keylock turned to Offline
0000000C	15/11/2008	10:16:29	Keylock turned to Secure
0000000D	15/11/2008	10:39:28	Activity generate..host:60 was ...
0000000E	15/11/2008	10:39:28	Activity genprint..host:60 was a...
0000000F	15/11/2008	10:39:28	Activity component..host:60 wa...
00000010	15/11/2008	10:39:28	Activity import..host:60 was aut...
00000011	15/11/2008	10:39:28	Activity export..host:60 was aut...
00000012	15/11/2008	10:39:28	Activity pin..host:60 was author...
00000013	15/11/2008	10:39:28	Activity audit..host:60 was auth...
00000014	15/11/2008	10:39:28	Activity diagnostic..host:60 wa...
00000015	15/11/2008	10:39:28	Activity misc..host:60 was auth...
00000016	15/11/2008	10:39:28	Activity command..host:60 wa...
00000017	15/11/2008	11:39:32	Authorised activity command.....
00000018	15/11/2008	11:39:32	Authorised activity misc..host:6...
00000019	15/11/2008	11:39:32	Authorised activity diagnostic.....
0000001A	15/11/2008	11:39:32	Authorised activity audit..host:6...

From payShield 9000 software v2.2a, the Audit Log is displayed with the most recent entries shown first: up to software version 2.1 the Audit Log was displayed with oldest entries first. This change has been made to make it more convenient to view the Audit Log when it contains a large number of entries.

For each entry in the audit log, the following information is displayed.

Counter

A hexadecimal reference number for the log entry.

Date / Time

The date and time at which the specific audit log entry was generated. This field reflects the HSM's internal real-time clock – not necessarily the local time.

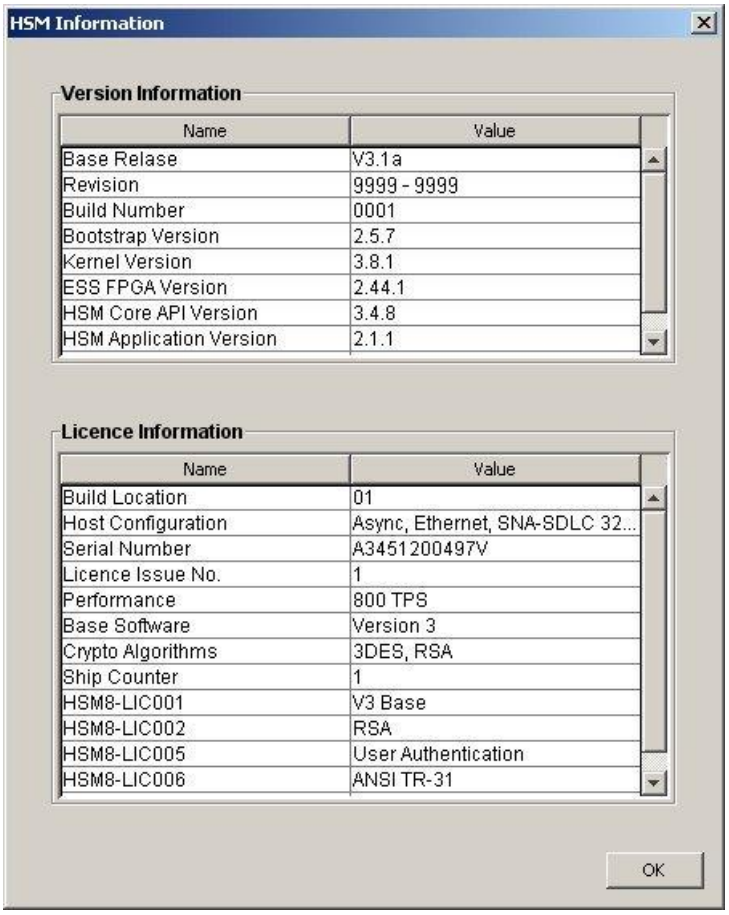
Text

A description of the auditable event.

Viewing HSM Information

The **HSM Information** option from the **View** menu allows users to view information about the HSM's version and license information.

The details are displayed on the screen shown below.



When you are finished, click on **OK**.

Remote Details

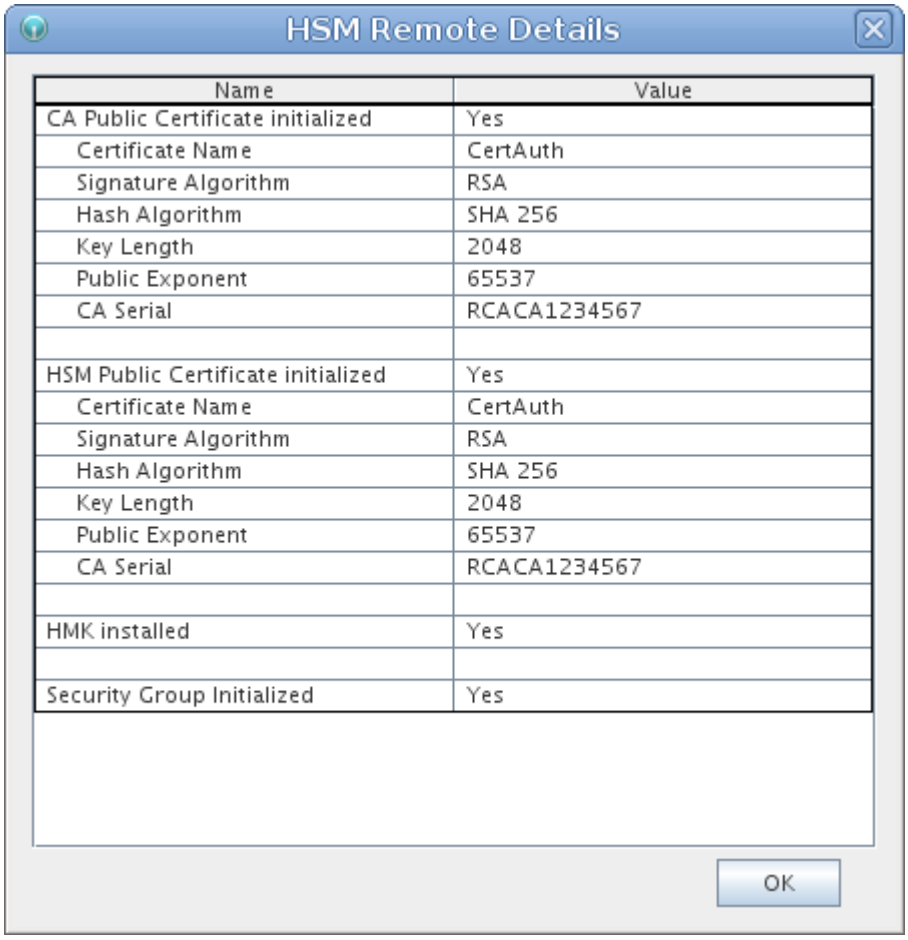
The **Remote Details** option from the **View** menu allows users to view the current 'remote' configuration information from the HSM.

Note: This information is only relevant if the HSM is configured for remote management, using the Remote HSM Manager product.

The displayed information includes:

- Details of the CA's public key certificate
- Details of the HSM's public key certificate
- Verification that an HMK is installed in the HSM
- Verification that the HSM's Security Group is initialized

The details are displayed on the screen, as shown in the example below.



When you are finished, click on **OK**.

>> Chapter 6 – Managing LMKs

Overview

This chapter describes the facilities provided by HSM Manager that allow authorized users to manage the generation, installation and uninstallation of Local Master Keys (LMKs).

These functions are provided by the HSM Manager **LMKs** menu, and include:

- **Generate Keys** – to generate a new LMK onto operator smartcards.
- **Install LMK** – to load a new LMK from operator smartcards into the HSM.
- **Install Old LMK** – to load an old LMK from operator smartcards into the "key change storage" area.
- **Copy LMK Component Card** – to create a copy of an existing LMK component card.
- **Create Authorizing Officer Card** – to create an LMK Authorizing Officer smartcard from an existing LMK Component Card.
- **Uninstall LMK** – to uninstall an LMK from the HSM.

Refer to *Appendix A - User Roles and Access Rights* to determine the access requirements for individual functions.

Types of LMKs

A **Variant LMK** is a set of 40 DES keys, arranged in pairs, with different pairs (and variants of those pairs) being used to encrypt different types of keys. This is the standard LMK format supported in all versions of Racal/Thales HSM firmware.

Note: The term "Variant LMK" refers to the fact that variants are applied to the LMK prior to using the LMK; a Variant LMK is not itself a variant of any other key.

A **Keyblock LMK** is either a triple-length DES key, or a 256-bit AES key, and is used to encrypt keys in a keyblock format. A Keyblock LMK is not compatible with a Variant LMK, and it can only be used to encrypt keys in the keyblock format.

Note: The term "Keyblock LMK" refers to the 'keyblock' method of encrypting keys; a Keyblock LMK is not itself stored in the keyblock format.

The LMKs can also be assigned, at the time they are generated, a status of "Live" or "Test" to indicate the intended usage of the LMK. The HSM will reject any attempt to translate keys from a "Test" LMK to a "Live" LMK, and vice versa.

Multiple LMKs

With HSM 8000 version 3.0 (and later) software and all versions of payShield 9000 software, it is possible to install multiple LMKs within a single HSM. The HSM contains a number of "slots", with each slot potentially containing a current and previous (or "old") LMK. The number of LMK slots available is determined by the HSM's license file, as shown below.

License	Description
Default – no specific multi-LMK license	Two concurrent LMKs can be installed; however, one must be a Variant LMK, and the other a Keyblock LMK.
LIC012 LMK x 2 (optional license)	Two concurrent LMKs can be installed; they can be any combination of Variant and Keyblock LMKs.
LIC013 LMK x 5 (optional license)	Five concurrent LMKs can be installed; they can be any combination of Variant and Keyblock LMKs.
LIC021 LMK x 10 (optional license)	Ten concurrent LMKs can be installed; they can be any combination of Variant and Keyblock LMKs.

Note: In HSM Manager, the "current" LMK is the LMK associated with the operator smartcard(s) used to log into the HSM in the current session.

LMK Table

LMKs are stored in a table within the secure memory of the HSM, with each LMK occupying a different 'slot' within the table. Each slot has the following attributes.

Attribute	Description
LMK ID	A 2-digit number which uniquely indicates the location of each LMK within the table. All references to LMKs are made by specifying the LMK Identifier.
Key Scheme	• "Variant" for traditional Racal/Thales LMK – key encryption performed using the *variant* method. • "Keyblock" for key encryption performed using the *keyblock* method.
Algorithm	• "3DES (2key)" is used by Variant LMKs. • "3DES (3key)" or "AES (256-bit)" is used by Keyblock LMKs. Notes: • 3DES Keyblock LMKs are supported on HSM 8000 v3.0 onwards, and all versions of payShield 9000 software. • AES Keyblock LMKs are supported on payShield 9000 v2.0 onwards (requires AES algorithm license). • Other algorithm types may be supported in future software releases.
Status	• "Test" indicates that the LMK is used for testing purposes. • "Live" indicates that the LMK is used for live production purposes. When installing LMKs, the HSM will prevent any mixing of Test and Live LMKs within the same slot (i.e. LMK Value and Old LMK Value must have the same status).
Comments	User-entered text, which can be used to help identify LMKs.
Authorization	Indicates the authorization status of the HSM for this particular LMK – either a flag (for Authorized State) or a list of authorized activities.
LMK Check Value	The check value of the LMK.
Old LMK Check Value	The check value of the 'old' LMK (in Key Change Storage).

The LMK table (but not the actual LMK values) is displayed on the HSM Manager main screen.

Generating an LMK

The **Generate LMK** option from the **LMKs** menu allows users to generate component(s) of an LMK, and store them on smartcards.

This function may be used to generate Variant or Keyblock LMK components.

When you select this option, the *Generate LMK Wizard* is started. This takes you through the entire process.

The wizard has the following steps.

Step 1

You are prompted to specify the type of LMK: variant or keyblock.

A *Variant LMK* is backward compatible with LMKs in all previous versions of HSM software. It consists of a set of 20 DES (double-length) key pairs, with variants of the LMK pairs used to protect the different types of working keys.

A *Keyblock LMK* consists of either a triple-length DES key or a 256-bit AES key, and can only be used for protecting keyblocks. DES Keyblock LMKs are supported in all versions of payShield 9000 software, and HSM 8000 software versions 3.0 onwards. AES Keyblock LMKs are supported in payShield 9000 software versions 2.0 onwards (requires AES algorithm license).

Note: Although called a Variant and Keyblock LMKs, the terms "variant" and "keyblock" refer to the keys that are encrypted by that LMK, and not the LMK value itself.

Step 2

You are prompted to specify the environment the new LMK will be used in.

Attempts to load Live and Test LMKs into the same slot (as new and old LMKs) will be rejected.

Step 3

You are prompted to specify, the following details:

- Component Number

  This is a number between 1 and 9, which identifies the specific LMK component on the smartcard.

- Secret / Random Values

  Three values A, B and C are required for generation of an LMK component. If these values are entered into the fields provided, the LMK component is derived from these values. In subsequent installations, if the same values are entered for A, B and C, then the same LMK component will be generated. Alternatively, the HSM can generate random values for the contents of A, B and C, in which case, it will not be possible to recalculate the same LMK component, as the values for A, B and C are not exposed.

Step 4

You are prompted to insert the smartcard that is to hold the LMK component into the HSM.

Step 5

You are prompted to enter the PIN into the wizard: the PIN must be entered within 60 seconds.

Step 6

Component details are written to the smartcard, which is then ejected.

The checksum for the component is displayed and you are asked whether or not you want to create another copy of the component.

If you choose to create another copy, the wizard returns to Step 4.

Step 7

You are asked whether you want to create another component for the LMK.

If so, the wizard returns to Step 3. Otherwise, click on **Finish** to complete the process.

Installing an LMK

The **Install LMK** option from the **LMKs** menu allows users to install an LMK into the HSM.

When you select this option, the *Install LMK Wizard* is started. This takes you through the entire process.

The wizard has the following steps.

Step 1

You are prompted for the following information about the LMK you are about to install:

> LMK ID

This is the 2-digit identifier that indicates which LMK slot is to receive the new LMK.

Notes:

- If there are no LMKs currently installed, then this value will be fixed to the "Management LMK ID" value, as stored in the Initial Settings dialog; see *Chapter 4 - Configuration Functions* for details.
- If there are LMKs installed, but none of them, are the Management LMK, you will only be able to overwrite the LMK you have logged in with or to install the Management LMK.
- If you are logged in using the Management LMK then you can install new LMKs; otherwise you can only overwrite the LMK you are logged in with.

> LMK Description

This is a free-form text field, used for information purposes only, which will be shown on the HSM Manager main screen.

Note: Attempts to load both Live and Test LMKs into the same slot (as new and old LMKs) will be rejected.

Step 2

You are prompted to enter the number of components that make up the LMK.

Step 3

You are prompted to insert the smartcard for the first LMK component into the HSM.

Step 4

You are prompted to enter the PIN into the wizard: the PIN must be entered within 60 seconds.

Step 5

Information is loaded from the smartcard and the LMK component checksum value is displayed.

The wizard then repeats Steps 3 and 4 for each component smartcard. After which it continues with Step 6.

Step 6

Details of the new LMK are displayed.

Click on **Finish** to complete the process.

Installing an Old LMK

The **Install Old LMK** option from the **LMKs** menu allows users to load an old LMK component set into Key Change Storage. This then allows you to translate key material from encryption under one LMK to encryption under another LMK.

The current LMK must be installed before an "old" LMK can be installed. Also note that it is possible to install a Variant LMK as the "old" LMK, and with a Keyblock LMK as the "new" LMK.

Note: Attempts to load both Live and Test LMKs into the same slot (as new and old LMKs) will be rejected.

Note: Attempts to load an "old" AES Keyblock LMK when the current LMK is either a Variant LMK or 3-DES Keyblock LMK will be rejected.

When you select this option, the *Install Old LMK Wizard* is started. This takes you through the entire process.

The wizard has the following steps.

Step 1

The number of the current LMK, the one you used to login under and the one you will load into key change storage is displayed.

You are prompted for a description. This is a free-form text field, used for information purposes only, which will be shown on the HSM Manager main screen.

Step 2

You are prompted to enter the number of components that make up the LMK.

Step 3

You are prompted to insert the smartcard for the first LMK component into the HSM.

Step 4

You are prompted to enter the PIN into the wizard: the PIN must be entered within 60 seconds.

Step 5

Information is loaded from the smartcard and the LMK component checksum value is displayed.

The wizard then repeats Steps 3 and 4 for each component smartcard. After which it continues with Step 6.

Step 6

Details of the old LMK are displayed.

Click on **Finish** to complete the process.

Copying an LMK Component Card

The **Copy LMK Component Card** option from the **LMKs** menu allows users to create a copy of an LMK component on another smartcard.

When you select this option, the *Copy LMK Component Card Wizard* is started. This takes you through the entire process.

The wizard has the following steps.

Step 1

Information about the wizard is displayed.

Step 2

You are prompted to insert the smartcard containing the LMK component into the HSM.

Step 3

You are prompted to enter the PIN into the wizard: the PIN must be entered within 60 seconds.

Step 4

Information is read from the card.

You are then prompted to insert a blank smartcard, onto which the details will be copied into the HSM.

Step 5

You are prompted to enter the PIN of the new card into the wizard.

Step 6

Component details are copied onto the new card, and the checksum value is displayed.

Click on **Finish** to complete the process.

Creating an Authorizing Officer Card

The **Create Authorizing Officer Card** option from the **LMKs** menu allows users to create a new operator smartcard, by copying the details of the 1st or 2nd LMK component smartcard. These cards can be used to log into the HSM Manager.

When you select this option, the *Create Authorizing Officer Card Wizard* is started. This takes you through the entire process.

The wizard has the following steps.

Step 1

The wizard displays information about the process.

Step 2

You are prompted to insert an existing LMK Authorizing Officer smartcard containing the LMK component #1 or #2 into the HSM.

Step 3

You are prompted to enter the card PIN into the wizard: the PIN must be entered within 60 seconds.

Step 4

Information is read from the card.

You are then prompted to insert a blank smartcard into the HSM.

Step 5

You are prompted to enter the PIN of the new card into the wizard.

Step 6

The new LMK Authorizing Officer card is created.

Click on **Finish** to complete the process.

Uninstall LMK

The **Uninstall LMK** option from the **LMKs** menu allows users to remove an LMK from the HSM.

When you select this option, the *Uninstall LMK Wizard* is started. This takes you through the entire process. Follow the on-screen prompts to erase either both current and old LMK, or just the old LMK, from the given slot.

Notes:

1. You can only uninstall the current LMK, the one you used to login under.
2. You are not allowed to uninstall the Management LMK while other LMKs are still installed.

The wizard has the following steps.

Step 1

The number and description of the current LMK, the one you used to login under, is displayed and you are prompted to select whether you want to uninstall just the old LMK or both the old and new one.

You must click in the check box to enable the **Next** button.

Step 2

The LMK details are removed from the HSM.

Click on **Finish** to complete the process.

Note: Once the LMK has been uninstalled, you are automatically logged out of HSM Manager.

>> Chapter 7 – Managing Keys

Overview

This chapter describes the facilities provided by HSM Manager to support generic key management operations.

These functions are provided by the HSM Manager **Keys** menu, and include:

- **Generate Keys** - to generate a random key, and encrypt it under the current LMK, and optionally export it under a specified ZMK.
- **Import Keys** - to import a key from encryption under a specified ZMK to encryption under the current LMK.
- **Export Keys** - to export a supplied key from encryption under the current LMK to encryption under a supplied ZMK.
- **Generate Components** - to generate key components which can later be combined to form a key using the **Form Key from Components** option.
- **Encrypt Components** - to encrypt an existing key component, under the current LMK.
- **Form Key from Components** - to form a new key from existing components, generated using the **Generate Components** option.

Refer to *Appendix A - User Roles and Access Rights* to determine the access requirements for individual functions.

Generating Keys

The **Generate Keys** option from the **Keys** menu allows users to generate a random key and return it encrypted under the current LMK and optionally under a ZMK (for transmission to another party).

When using a Variant LMK or 3-DES Keyblock LMK, this wizard can only generate a single-, double- or triple-length DES key. When an AES Keyblock LMK is used, this wizard can generate a double- or triple-length DES key or a 128-bit, 192-bit or 256-bit AES key.

When you select this option, the *Generate Key Wizard* is started. This takes you through the entire process. The procedure varies depending upon the type of LMK you are logged in under.

Variant LMK

If you are logged in under a variant LMK, the *Generate Key Wizard* has the following steps.

Step 1

Select the following information, using the drop-down lists provided:

- *Key Type* - The type of key. See the Key Type Table in Chapter 4 of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command Reference Manual*.
- *Key Length* - The length of the key: Single, Double or Triple.
- *Key Scheme* - The encryption scheme of the key. See the Key Scheme Table at Appendix C of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command reference Manual*.

Step 2

The wizard prompts you to say whether or not you intend sharing this key with a third party. If you are, you must supply a ZMK and select the appropriate export key scheme.

Step 3 (If exporting to a TR-31 format only)

Depending upon the export key scheme selected in Step 2, you may be prompted for an exportability code. Select the options you require, using the drop-down lists provided:

- *Key Usage* - The intended usage of the key. See the Key Usage table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.
- *Mode of Use* - Any specific restrictions on the way in which the key is used within the HSM. See the Mode of Use table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.
- *Exportability* - Whether the key can be exported from the HSM. See the Exportability table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.

Step 4

The key details are generated and can be saved to a file, if required.

The following information is displayed:

- The key check value
- The key value encrypted under the current LMK
- The key value encrypted under the supplied ZMK (if sharing was selected)

Click on **Save** to save the details to a disk file, if required.

Finally, click on **Finish** to complete the process.

Keyblock LMK

If you are logged in under a keyblock LMK, the *Generate Key Wizard* has the following steps.

Step 1

Select the following information, using the drop-down lists provided:

- *Key Algorithm* – The algorithm with which the key is to be used (DES or AES). Note that the AES algorithm can only be selected when using an AES Keyblock LMK.
- *Key Length* – The length of the key: Single, Double or Triple (for DES keys) or 128-bit, 192-bit or 256-bit (for AES keys). Note that an AES key can only be generated when using an AES Keyblock LMK.
- *Key Usage* - The intended usage of the key. See the Key Usage table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.
- *Mode of Use* - Any specific restrictions on the way in which the key is used within the HSM. See the Mode of Use table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.
- *Exportability* - Whether the key can be exported from the HSM. See the Exportability table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.

Step 2

The wizard prompts you to say whether or not you intend sharing this key with a third party. If you are, you must supply a ZMK and select the appropriate export key scheme.

Step 3

Depending upon the export key scheme selected in Step 2, you may be prompted for an exportability code. Select the option you require, using the drop-down list provided.

Step 4

The key details are generated and can be saved to a file, if required.

The following information is displayed:

- The key check value
- The key value encrypted under the current LMK
- The key value encrypted under the supplied ZMK (if sharing was selected)

Click on **Save** to save the details to a disk file, if required.

Finally, click on **Finish** to complete the process.

Importing Keys

The **Import Keys** option from the **Keys** menu allows users to import a key from encryption under a ZMK to encryption under an LMK. If the key imported does not have odd parity a warning will be issued and odd parity will be forced on the key before encryption under the current LMK.

When using a Variant LMK or 3-DES Keyblock LMK, this wizard can only import a single-, double- or triple-length DES key. When an AES Keyblock LMK is used, this wizard can import a double- or triple-length DES key or 128-bit, 192-bit or a 256-bit AES key.

When you select this option, the *Import Key Wizard* is started. This takes you through the entire process. The procedure varies depending upon the type of LMK you are logged in under.

Variant LMK

If you are logged in under a variant LMK, the *Import Key Wizard* has the following steps.

Step 1

Enter the following information:

> *Key Encrypting Key* - The value used to encrypt the key

> *Key Value* - The key value

Step 2

Select the following information, using the drop-down lists provided:

> *Key Type* - The type of key. See the Key Type Table in Chapter 4 of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command Reference Manual*.

> *Key Scheme* - The encryption scheme of the key. See the Key Scheme Table at Appendix C of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command reference Manual*.

Step 3

The key details are generated and can be saved to a file, if required.

The following information is displayed:

> The key check value

> The key value encrypted under the current LMK

Click on **Save** to save the details to a disk file, if required.

Finally, click on **Finish** to complete the process.

Keyblock LMK

If you are logged in under a keyblock LMK, the *Import Key Wizard* has the following steps.

Step 1

Enter the following information:

> *Key Encrypting Key* - The value used to encrypt the key

> *Key Value* - The key value

Step 2

There is no Step 2 in a keyblock LMK key import procedure.

Step 3

The key details are generated and can be saved to a file, if required.

The following information is displayed:

- The key check value
- The key value encrypted under the current LMK

Click on **Save** to save the details to a disk file, if required.

Finally, click on **Finish** to complete the process.

Exporting Keys

The **Export Keys** option from the **Keys** menu allows users to translate a key from encryption under the current LMK to encryption under a ZMK.

When you select this option, the *Export Key Wizard* is started. This takes you through the entire process. The procedure varies depending upon the type of LMK you are logged in under.

Variant LMK

If you are logged in under a variant LMK, the *Export Key Wizard* has the following steps.

Note: Export from a Variant LMK to Thales Keyblock is not permitted.

Step 1

Enter the following information:

- *Key Encrypting Key* - The ZMK value used to encrypt the key
- *Key Value* - The key value
- *Output key scheme* - The encryption scheme of the key. See the Key Scheme Table at Appendix C of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command reference Manual*.

Step 2

The wizard then prompts you for the following details:

- *Key Type* - The type of key. See the Key Type Table in Chapter 4 of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command Reference Manual*.

If you exporting to a TR-31 format and selected R as the Output key format in Step 1, you must also specify:

- *Key Usage* - The intended usage of the key. See the Key Usage table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.
- *Mode of Use* - Any specific restrictions on the way in which the key is used within the HSM. See the Mode of Use table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.
- *Exportability* - Whether the key can be exported from the HSM. See the Exportability table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.

Step 3

The key details are generated and can be saved to a file, if required.

The following information is displayed:

> The key check value

> The key value (encrypted under the supplied ZMK)

Click on **Save** to save the details to a disk file, if required.

Finally, click on **Finish** to complete the process.

Keyblock LMK

If you are logged in under a keyblock LMK, the *Export Key Wizard* has the following steps.

Step 1

Enter the following information:

> *Key Encrypting Key* - The ZMK value used to encrypt the key

> *Key Value* - The key value

> *Output key scheme* - The encryption scheme of the key. See the Key Scheme Table at Appendix C of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command reference Manual*.

Step 2

The wizard then prompts you for the following details:

> *Key Type* - The type of key. See the Key Type Table in Chapter 4 of the payShield 9000 General Information Manual.

If you exporting to a TR-31 format and selected R as the Output key format in Step 1, you must also specify:

> *Key Usage* - The intended usage of the key. See the Key Usage table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.

> *Mode of Use* - Any specific restrictions on the way in which the key is used within the HSM. See the Mode of Use table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.

> *Exportability* - Whether the key can be exported from the HSM. See the Exportability table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.

Step 3

The key details are generated and can be saved to a file, if required.

The following information is displayed:

- The key check value
- The key value encrypted under the supplied ZMK)

Click on **Save** to save the details to a disk file, if required.

Finally, click on **Finish** to complete the process.

Generating Key Components

The **Generate Components** option from the **Keys** menu allows users to generate a key component and display it in plain and encrypted forms.

When using a Variant LMK or 3-DES Keyblock LMK, this wizard can only generate a single-, double- or triple-length DES key component. When an AES Keyblock LMK is used, this wizard can generate a double- or triple-length DES key component or a 128-bit, 192-bit or 256-bit AES key component.

The component is displayed on screen and can be saved to disk and / or to a smartcard.

When you select this option, the *Generate Components Wizard* is started. This takes you through the entire process. The procedure varies depending upon the type of LMK you are logged in under.

Variant LMK

If you are logged in under a variant LMK, the *Generate Components Wizard* has the following steps.

Step 1

Select the following information, using the drop-down lists provided:

- *Key Type* - The type of key component. See the Key Type Table in Chapter 4 of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command Reference Manual*.
- *Key Length* - The length of the key component: Single, Double or Triple.
- *Key Scheme* - The encryption scheme of the key component. See the Key Scheme Table at Appendix C of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command reference Manual*.
- *Number of Components* - Select the number of key components you want to be generated: 1 to 9.

Step 2

The component details are generated.

The following information is displayed for each component:

- The component number
- The key check value
- The plaintext component value

Click on **Save** to save the details to a disk file, if required.

Finally, click on **Finish** to complete the process.

Keyblock LMK

If you are logged in under a keyblock LMK, the *Generate Components Wizard* has the following steps.

Step 1

Select the following information, using the drop-down lists provided:

- *Key Algorithm* - The algorithm with which the key/component is to be used (DES or AES). Note that the AES algorithm can only be selected when using an AES Keyblock LMK.
- *Key Length* - The length of the key: Single, Double or Triple (for DES keys) or 128-bit, 192-bit or 256-bit (for AES keys). Note that an AES key can only be generated when using an AES Keyblock LMK.
- *Key Scheme* - See the Key Scheme Table at Appendix C of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command reference Manual*.
- *Key Usage* - The intended usage of the key. See the Key Usage table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.
- *Mode of Use* - Any specific restrictions on the way in which the key is used within the HSM. See the Mode of Use table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.
- *Exportability* - Whether the key can be exported from the HSM. See the Exportability table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.
- *Number of Components* - Select the number of key components you want to be generated: 1 to 9.
- *Component Number* - If you selected 1 as the Number of Components, use this drop-down to select the component number to be generated.

Step 2

The component details are generated.

The following information is displayed for each component:

- The component number
- The key check value
- The plaintext component value

Click on **Save** to save the details to a disk file, if required.

Finally, click on **Finish** to complete the process.

Encrypting Key Components

The **Encrypt Components** option from the **Keys** menu allows users to generate an encrypted key component from its plaintext version.

When using a Variant LMK or 3-DES Keyblock LMK, this wizard can only encrypt a single-, double- or triple-length DES key component. When an AES Keyblock LMK is used, this wizard can encrypt a single-, double- or triple-length DES key component or a 128-bit, 192-bit or 256-bit AES key component.

The component check value and encrypted value is displayed on screen and can be saved to disk.

When you select this option, the *Encrypt Components Wizard* is started. This takes you through the entire process. The procedure varies depending upon the type of LMK you are logged in under.

Variant LMK

If you are logged in under a variant LMK, the Encrypt Components wizard has the following steps.

Step 1

Enter the plaintext component value.

Step 2

Select the following information, using the drop-down lists provided:

- *Key Type* - The type of key component. See the Key Type Table in Chapter 4 of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command Reference Manual*.
- *Key Scheme* - The encryption scheme of the key component. See the Key Scheme Table at Appendix C of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command reference Manual*.

Step 3

The encrypted component details are generated and the following information is displayed:

- The component check value
- The encrypted component value

Click on **Save** to save the details to a disk file, if required.

Finally, click on **Finish** to complete the process.

Keyblock LMK

If you are logged in under a keyblock LMK, the *Encrypt Components Wizard* has the following steps.

Step 1

Enter the plaintext component value.

Step 2

Select the following information, using the drop-down lists provided:

- *Key Algorithm* - The algorithm with which the key/component is to be used (DES or AES). Note that the AES algorithm can only be selected when using an AES Keyblock LMK.

- *Key Length* - The length of the key: Single, Double or Triple (for DES keys) or 128-bit, 192-bit or 256-bit (for AES keys). Note that an AES key can only be generated when using an AES Keyblock LMK.
- *Key Usage* - The intended usage of the key. See the Key Usage table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.
- *Mode of Use* - Any specific restrictions on the way in which the key is used within the HSM. See the Mode of Use table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.
- *Exportability* - Whether the key can be exported from the HSM. See the Exportability table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.
- *Component Number* - the number of the key component.

Step 3

The encrypted component details are generated and the following information is displayed:

- The component check value
- The encrypted component value

Click on **Save** to save the details to a disk file, if required.

Finally, click on **Finish** to complete the process.

Forming a Key From Components

The Form Key from Components option from the **Keys** menu allows users to form a new key from existing components. Key components can be generated using the *Generate Key Component Wizard*.

Once the components have been combined to form the key, the key is then encrypted under the current LMK. The key details are displayed on screen and can be saved to disk.

When you select this option, the *Form Key from Components Wizard* is started. This takes you through the entire process. The procedure varies depending upon the type of LMK you are logged in under.

Variant LMK

If you are logged in under a variant LMK, the *Form Key from Components Wizard* has the following steps.

Step 1

Select the method by which the key will be formed from its components. One of the following:

- *Encrypted* – the components will be entered encrypted under the current LMK.
- *Half* - half of a double-length key. This is not recommended.
- *Third* - one third of a triple-length key. This is not recommended.
- *Plaintext* – the components will be entered in plaintext.

Step 2

Select the following information, using the drop-down lists provided:

- *Key Type* - The type of key component. See the Key Type Table in Chapter 4 of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command Reference Manual*.
- *Key Length* - The length of the key component: Single, Double or Triple.
- *Key Scheme* - The encryption scheme of the key component. See the Key Scheme Table at Appendix C of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command reference Manual*.

Step 3

Enter the component value.

Step 4

The component check value is displayed.

If the key has another component, ensure that the **Enter another component** box is checked. If this box is checked, you are returned to Step 3 and prompted for the next component details. This continues until you uncheck the box.

Step 5

Once you have entered all the components required to form the key, the key check value and the LMK-encrypted key value is displayed.

Click on **Save** to save the details to a disk file, if required.

Finally, click on **Finish** to complete the process.

Keyblock LMK

If you are logged in under a keyblock LMK, the *Form Key from Components Wizard* has the following steps.

Step 1

Select the method by which the key will be formed from its components. One of the following:

- *Encrypted* – the components will be entered encrypted under the current LMK.
- *Half* - half of a double-length key. This is not recommended.
- *Third* - one third of a triple-length key. This is not recommended.
- *Plaintext* – the components will be entered in plaintext.

Step 2

Select the following information, using the drop-down lists provided:

- *Key Algorithm* - The algorithm with which the key is to be used (DES or AES). Note that the AES algorithm can only be selected when using an AES Keyblock LMK.
- *Key Length* - The length of the key: Single, Double or Triple (for DES keys) or 128-bit, 192-bit or 256-bit (for AES keys). Note that an AES key can only be formed when using an AES Keyblock LMK.
- *Key Usage* - The intended usage of the key. See the Key Usage table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.
- *Mode of Use* - Any specific restrictions on the way in which the key is used within the HSM. See the Mode of Use table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.
- *Exportability* - Whether the key can be exported from the HSM. See the Exportability table in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.

Step 3

Enter the component value.

Step 4

The component check value is displayed.

If the key has another component, ensure that the **Enter another component** box is checked. If this box is checked, you are returned to Step 3 and prompted for the next component details. This continues until you uncheck the box.

Step 5

Once you have entered all the components required to form the key, the key check value and the LMK-encrypted key value is displayed.

Click on **Save** to save the details to a disk file, if required.

Finally, click on **Finish** to complete the process.

>> Chapter 8 – Changing the HSM State

The HSM can be in one of three states:

- *Online*

  Mode of operation of the HSM that permits communication with a host computer system via the HSM's host port.

  Note: when using the HSM 8000 ESCON Host interface and turning the HSM 8000 to Online state, the HSM 8000 must be re-started.

- *Offline*

  Mode of operation of the HSM that prevents online communication with the host computer system; usually required when changing configuration parameters.

- *Secure*

  Mode of operation of the HSM that prevents online communication with the host computer system, and is required for certain highly sensitive functions (for example, generating or loading LMKs into the HSM).

The HSM state is changed using the physical keys on the HSM's front panel, as follows:

- *Online*

  Both keys are in locked position (both keys can be removed).

- *Offline*

  One (either) key is in the locked position, and the other in the unlocked position.

- *Secure*

  Both keys are in the unlocked position. (Note that the HSM can be removed/installed in a 19" rack while the keys are in this position.)

>> Chapter 9 – HSM Manager Tools

Overview

This chapter describes the various utilities provided by HSM Manager.

These functions are provided by the HSM Manager **Tools** menu, and include:

- **Smartcard**:
  - **Format Card** - to erase and format a smartcard.
  - **Eject** - to eject a smartcard inserted in the HSM's smartcard reader.
  - **Change PIN** - to change the PIN of a smartcard.
  - **Verify Card** - to verify the contents of an LMK component smartcard.
- **Diagnostics**:
  - **Ping** - to check the network connection from the HSM to a specific IP address; for example, the host computer.
  - **Tracert** - to check the connection route between the HSM and the host computer.
  - **Netstat** - to check the HSM's network activity.
  - **Route** - to configure the HSM's static TCP/IP routing table.
  - **FiconTest** - to check the HSM's FICON interface. (*payShield 9000 only*)
- **Utilities**:
  - **Calculate Key Check Value** - to calculate and display the key check value for an encrypted key.
  - **Encrypt Decimalization Table** - to encrypt a 16 digit decimalization table for use with host commands using IBM 3624 PIN Generation and Verification.
  - **Translate Decimalization Table** - to translate an encrypted decimalization table from encryption under an old LMK to encryption under the corresponding new LMK.
  - **Generate MAC on IPB** - to generate a MAC on an IPB (Issuer Proprietary Bitmask)
  - **Generate Visa CVV** - to generate a Visa CVV (Card Verification Value).
  - **Generate Visa PVV** - to generate a Visa PVV (PIN Verification Value).
- **Utilisation and Health Check Data** *(payShield 9000 only)*:
  - **Configure Statistics** – to set the configuration for Utilisation Statistics reporting.
  - **Health Check Data** – to display data for an instantaneous Health Check and accumulated Health Check counters.
  - **HSM Loading Value** – to display statistics showing how heavily loaded the HSM is.
  - **Host Command Statistics** – to display how often each host command has been run.

- **Reset Statistics** – to reset the accumulated statistics for Utilisation and Health Check data.

> **SNMP** *(payShield 9000 only)*:

- **Display** – show SNMP Communities/Users
- **Add** – add SNMP Communities/Users.
- **Delete** – remove SNMP Communities/Users

> **Secure Host Communications** *(payShield 9000 only)*:

- **Generate Certificate Signing Request**
- **Export HSM CA Certificate**
- **Import Signed Certificate**
- **Generate HMK**
- **Recover HMK**
- **Change HMK Passphrase**
- **View Certificates**
- **Delete Certificates**

> **Reset Fraud Detection** - allows the HSM to be reset after a suspected fraudulent attack has been detected.

> **Return to Factory Settings**

Refer to *Appendix A - User Roles and Access Rights* to determine the access requirements for individual functions.

Format Card

The **Format Card** option from the **Tools | Smartcard** menu allows operators to erase and format a smartcard.

When you select this option, the *Format Smartcard Wizard* is started. This takes you through the entire process.

The wizard has the following steps.

Step 1

You are prompted to insert the smartcard into the HSM.

Step 2

You are prompted to enter the PIN (twice for confirmation) into the wizard.

A screen is then displayed, allowing you to enter the following information for storage on the card:

> Date and time - the default is the current date and time.

> The User ID

> The Issuer ID

Step 3

The card is then formatted, and the entered information is written to the card.

Click on **Finish** to complete the process.

Eject

The **Eject** option from the **Tools | Smartcard** menu allows users to eject a smartcard which is currently inserted in the HSM.

Changing a Smartcard PIN

The **Change PIN** option from the **Tools | Smartcard** menu allows users to change the PIN held on a smartcard. The minimum PIN length is 5 digits, but a length of 8 digits is recommended.

When you select this option, the *Change PIN Wizard* is started. This takes you through the entire process.

The wizard has the following steps.

Step 1

You are prompted to insert the smartcard into the HSM.

Step 2

Enter the current PIN (which must be entered within 60 seconds); and then enter and confirm the new PIN into the wizard.

The PIN is then changed.

Click on **Finish**, to complete the process.

Verifying an HSM Card

The **Verify Card** option from the **Tools | Smartcard** menu allows users to verify the contents of an LMK component card.

When you select this option, the *Verify Card Wizard* is started. This takes you through the entire process.

The wizard has the following steps.

Step 1

You are prompted to insert the smartcard into the HSM.

Step 2

You are prompted to enter the PIN into the wizard: the PIN must be entered within 60 seconds.

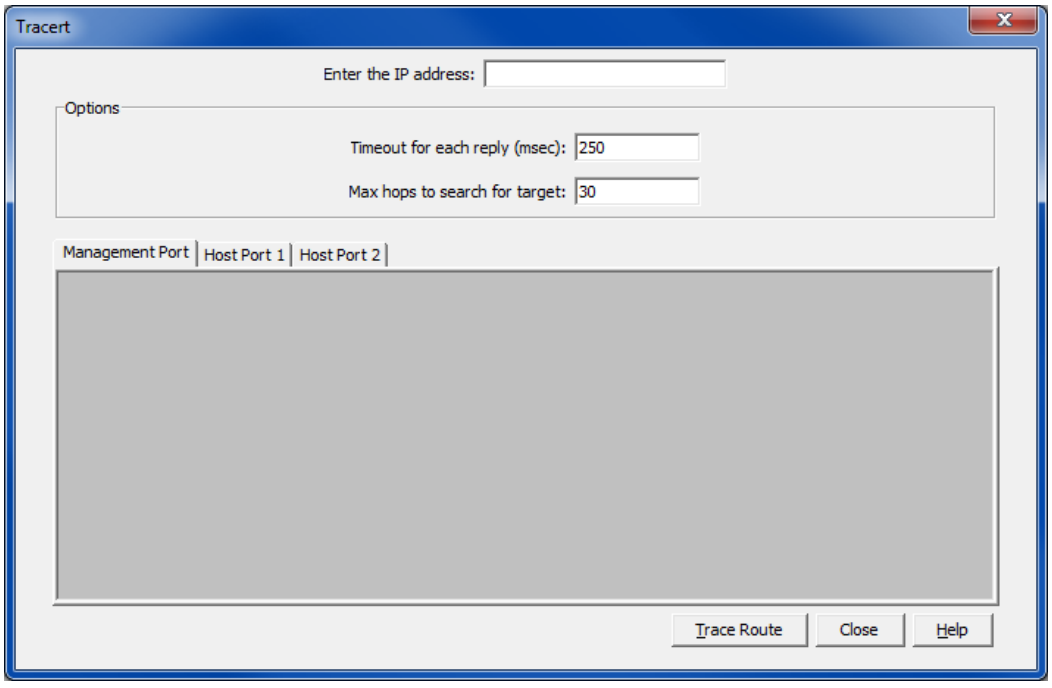
The HSM reads the LMK component from the smartcard, computes the check value, compares this with the check value stored on the card, and displays the result.

Click on **Finish**, to complete the process.

Ping

The **Ping** option from the **Tools | Diagnostics** menu allows users to check the network connection from the HSM to a specific IP address; for example, the host computer.

When you select this menu option, the screen below is displayed.



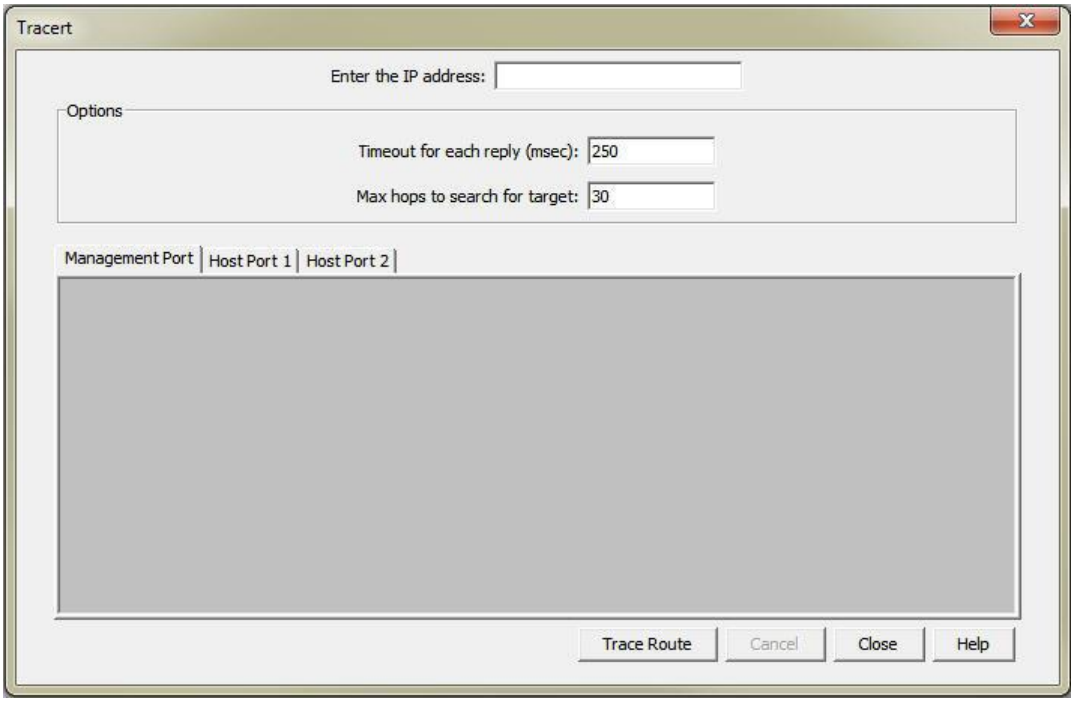
The above example is for the payShield 9000, which provides 2 Host Ethernet interfaces.

Enter the ping details and then click on **Ping**. The ping results are then displayed.

Tracert

The **Tracert** option from the **Tools | Diagnostics** menu allows users to check the connection route between the HSM and devices on the host or management network.

When you select this menu option, the screen below is displayed.



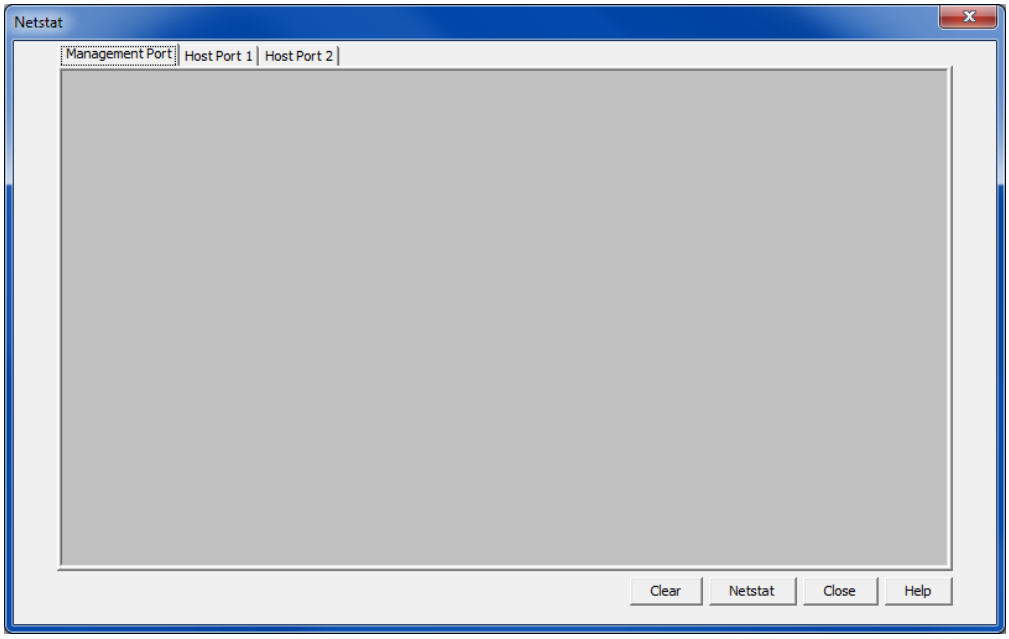
The above example is for the payShield 9000, which provides 2 Host Ethernet interfaces.

Enter the trace details and then click on **Trace Route**. The results are displayed.

Netstat

The **Netstat** option from the **Tools | Diagnostics** menu allows users to check the HSM's network activity.

When you select this menu option, the screen below is displayed.



The above example is for the payShield 9000, which provides 2 Host Ethernet interfaces.

Select the Management Port or Host Port tab and, if required, check the **Display Ethernet Statistics** box.

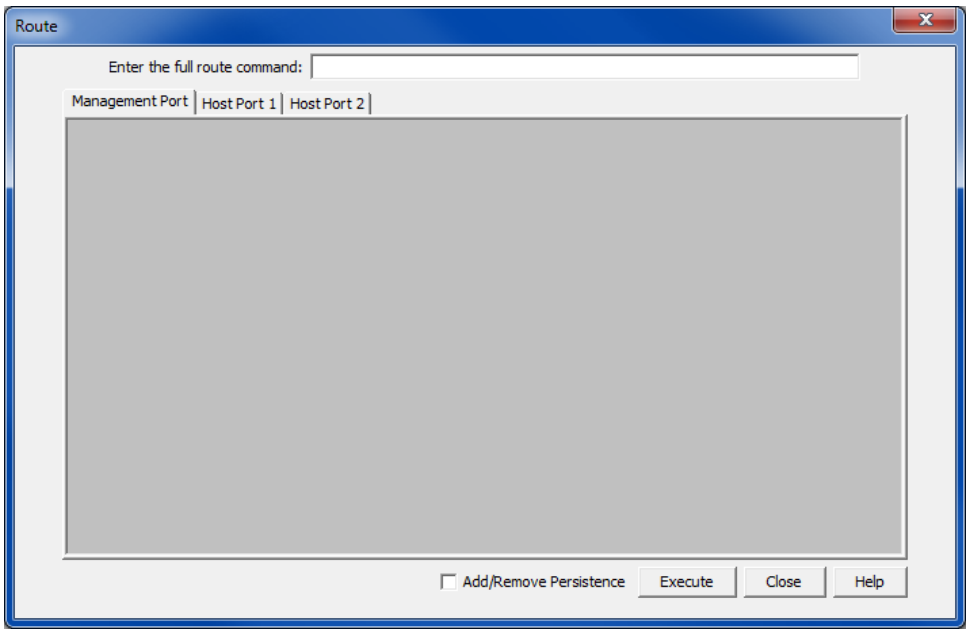
Click on the **Netstat** button. The network statistics are displayed.

To clear the current display and run the monitoring again, click on **Clear**.

Route *(payShield 9000 only)*

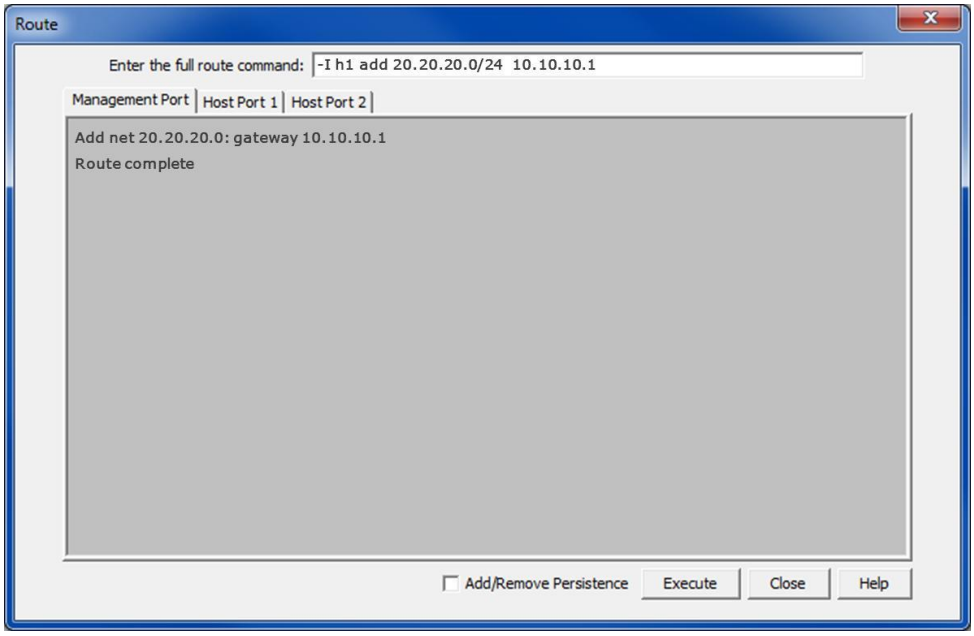
The **Route** option from the **Tools | Diagnostics** menu allows users to configure static routes for routing TCP/IP traffic from the HSM.

When you select this menu option, the screen below is displayed.



Enter the route details and then click on **Execute**. The results are displayed.

The screen below shows a route being added:



To clear the current display and run the monitoring again, click on **Clear**.

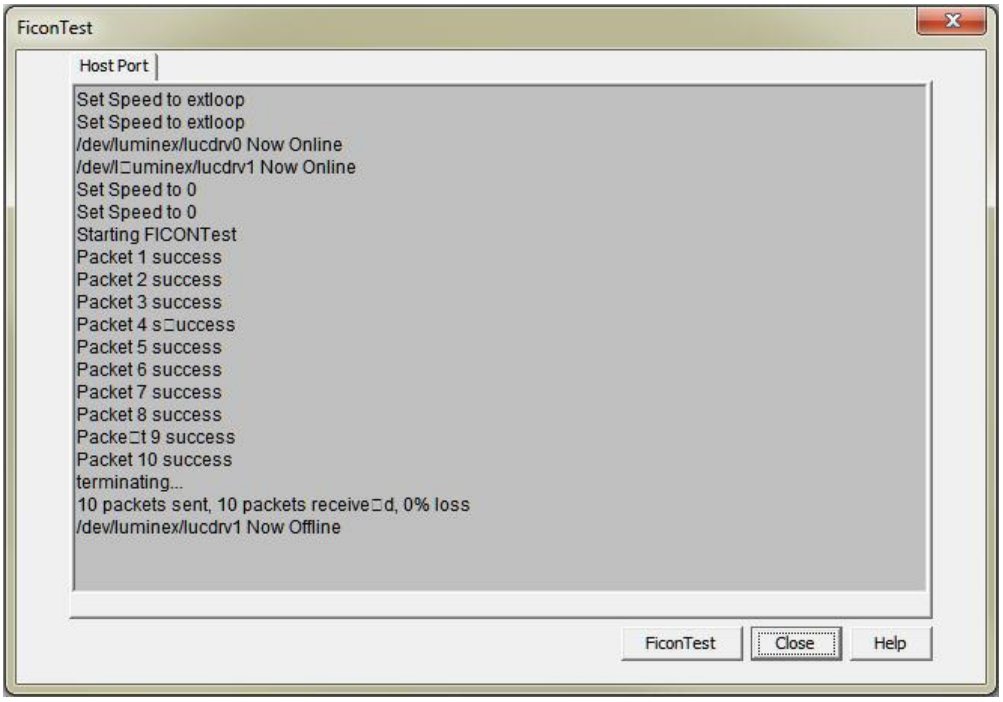
Note: When upgrading from a version of payShield 9000 software that does not support Default Gateways (i.e. versions up to 1.3) to a version that does support Default Gateways (i.e. versions 1.4 onwards), any existing routes previously set up using the ROUTE command will be deleted. If it is required to continue using static routes (despite the availability of Default Gateways), these should be re-entered using the ROUTE command.

FiconTest *(payShield 9000 only)*

The **FiconTest** option from the **Tools | Diagnostics** menu allows users to check the payShield 9000 FICON Host interface: FICON is a factory-fit option for the payShield 9000. The test sends 10 test packets and reports on their success.

For payShield 9000 units with a single FICON port, the loopback cable supplied with the unit should be attached to the active transceiver before FiconTest is run.

For payShield units with 2 FICON ports the supplied loopback cable can be used to test each transceiver in turn, or a standard FICON patch cable can be used to connect one transceiver to the other.



Calculating a Key Check Value

The **Calculate Key Check Value** option from the **Tools | Utilities** menu allows users to generate a key check value (KCV) for a key.

When you select this option, the *Calculate Key Check Value Wizard* is started. This takes you through the entire process.

The wizard has the following steps.

Step 1

Enter the encrypted key value.

For variant LMKs, select the key type from the drop-down list.

Step 2

The HSM calculates and displays the key check value and the encrypted key value you entered in Step 1.

Click on **Finish**, to complete the process.

Encrypting the Decimalization Table

The **Encrypt Decimalization Table** option from the **Tools | Utilities** menu allows users to encrypt a 16 digit decimalization table for use with host commands using IBM 3624 PIN Generation and Verification.

When you select this option, the *Encrypt Decimalization Table Wizard* is started. This takes you through the entire process.

The wizard has the following steps.

Step 1

Enter the decimalization table value.

This is a 16 decimal digit number that specify the mapping between hexadecimal and decimal numbers.

The HSM, by default, checks that the decimalization table contains at least 8 different digits, with no digit repeated more than 4 times. This feature may be disabled using the **Enable decimalization table checks** option under Initial Settings. Disabling of this feature is not recommended.

Step 2

The HSM calculates and displays the encrypted decimalization table value and the value you entered in Step 1.

Click on **Finish**, to complete the process.

Translating the Decimalization Table

The **Translate Decimalization Table** option from the **Tools | Utilities** menu allows users to translate an encrypted decimalization table from encryption under an old LMK to encryption under the corresponding new LMK.

When you select this option, the *Translate Decimalization Table Wizard* is started. This takes you through the entire process.

The wizard has the following steps.

Step 1

Enter the encrypted decimalization table value, encrypted under the old LMK. This is the result of encrypting the decimalization table using the **Encrypt Decimalization Table** function.

The HSM, by default, checks that the decimalization table contains at least 8 different digits, with no digit repeated more than 4 times. This feature may be disabled using the **Enable decimalization table checks** option under Initial Settings. Disabling of this feature is not recommended.

Step 2

The HSM calculates and displays the encrypted decimalization table value, encrypted under the new LMK, and the value you entered in Step 1.

Click on **Finish**, to complete the process.

Generate MAC on IPB

The **Generate MAC on IPB** option from the **Tools | Utilities** menu allows users to generate a MAC on an IPB (Issuer Proprietary Bitmask) for subsequent inclusion in the HSM host command that provides CAP/DPA verification.

When you select this option, the *Generate MAC on IPB Wizard* is started. This takes you through the entire process.

The wizard has the following steps.

Step 1

Enter the IPB. This is an 8-byte string, represented as 16 hex ASCII characters.

Step 2

The HSM calculates and displays the 4 digit MAC, and the value you entered in Step 1.

Click on **Finish**, to complete the process.

Generate Visa CVV

The **Generate Visa CVV** option from the **Tools | Utilities** menu allows users to generate a Visa CVV (Card Verification Value). The CVV is used as a check value on the data stored on the magnetic stripe of a card.

When you select this option, the *Generate Visa CVV Wizard* is started. This takes you through the entire process. This wizard can also be used to generate a Visa CVV2, iCVV and MasterCard CVC, CVC2, and Chip CVC.

The wizard has the following steps.

Step 1

Enter the CVK to be used to generate the CVV.

If you are logged on under a variant LMK, you can enter either two single length keys or one double-length key.

Step 2

Enter the following information:

- *PAN* - a 1 to 19 digit code.
- *Expiry date* - in MM/YY format.
- *Service code* - a 3-digit code.

Step 3

The HSM calculates and displays the CVV, and the PAN value you entered in Step 2.

Click on **Finish**, to complete the process.

Generate Visa PVV

The **Generate Visa PVV** option from the **Tools | Utilities** menu allows users to generate a Visa PVV (PIN Verification Value). The PVV is essentially an encrypted value of the PIN and is stored by a card issuer, and is potentially also stored on the magnetic stripe of a card.

When you select this option, the *Generate Visa PVV Wizard* is started. This takes you through the entire process.

The wizard has the following steps.

Step 1

Enter the PVK to be used to generate the PVV.

If you are logged on under a variant LMK, you can enter either two single length keys or one double-length key.

Step 2

Enter the following information:

- *PAN* - a 1 to 19 digit code.
- *PVK indicator* - a single-digit code value.
- *PIN* - the PIN number on the card

Step 3

The HSM calculates and displays the PVV, and the PAN value you entered in Step 2.

Click on **Finish**, to complete the process.

Utilization and Health Check Data *(payShield 9000 only)*

From version 1.1 of the payShield 9000 firmware, the HSM provides users with data about how heavily utilized the HSM is and data to help them assess the health state of the HSM.

These capabilities are not available on the HSM 8000.

Utilization Data

This is designed to allow users to re-balance loading between their various payShield 9000s, and to optimize their purchasing of additional capacity.

The Utilization Data facility provides 2 sets of data to the user:

- Overall HSM Loading. This data indicates how heavily loaded the HSM is.
- Host Command Volumes. This data indicates how many times each host command has been processed, and the average transactions per second (tps) for each command. It is important to recognize that not all commands hade the same effect on HSM loading. The rated performance of the HSM (e.g. 1,500 tps for the X performance model) relates to how many CA host commands (PIN Block Translation) the HSM could run in a second. Most other host commands will run at the same speed as the CA command, but some will run more slowly (and impose a greater load on the HSM) and a few will run faster.

  Even looking at an individual command, the speed it runs at may depend on the options or payload associated with it. For example, the speed of commands using RSA keys is heavily dependent on the RSA key length; and commands which encrypt/decrypt blocks of data run more slowly with larger data blocks.

There are 2 types of period over which the data is collected:

- Since Last Reset. Data is accumulated since the last time that the user reset the utilization data. It will continue to accumulate until the next time the data is explicitly reset. The accumulated data can be retrieved at any time without resetting it, allowing time-series data to be created by regular retrieval of data to an external host computer.

  Collection of data can be suspended and resumed without resetting the data.

  The collected data is persistent over re-starts and power being switched off.
- "Instantaneous" data. It is possible to get a view of the loading of the HSM right now by asking for instantaneous data, helping administrators

investigate throughput or performance issues as they are occurring. This provides utilization data over the most recent period: the length of this period can be configured from 1 to 60 seconds.

The following functions, described elsewhere in this manual or in other relevant manuals, allow utilization data to be viewed and managed:

- HSM Manager:
  - Tools -> HSM Utilisation Statistics -> Configure Statistics
  - Tools -> HSM Utilisation Statistics -> HSM Loading Value -> Since Last Reset
  - Tools -> HSM Utilisation Statistics -> HSM Loading Value -> Instantaneous
  - Tools -> HSM Utilisation Statistics -> Host Command Statistics -> Since Last Reset
  - Tools -> HSM Utilisation Statistics -> Host Command Statistics -> Instantaneous
  - Tools -> HSM Utilisation Statistics -> Reset Statistics
  - Tools -> SNMP -> Display -> V1/V2 Communities
  - Tools -> SNMP -> Display -> V3 User
  - Tools -> SNMP -> Add -> V1/V2 Communities
  - Tools -> SNMP -> Add -> V3 User
  - Tools -> SNMP -> Delete -> V1/V2 Communities
  - Tools -> SNMP -> Delete -> V3 User
- Console Commands:
  - UTILCFG
  - UTILENABLE
  - UTILSTATS
  - SNMP
  - SNMPADD
  - SNMPDEL
- Host Commands:
  - J2 – Get HSM Loading data
  - J4 – Get Host Command Volumes
  - J6 – Reset Utilization Data

Health Check Data

The Health Check Data facility provides 2 sets of data to the user:

- Accumulated Counts. This data provides counts of certain HSM health-related events since the last time that the user reset the Health Check Data.

- Instantaneous Status. This provides the current status of a range of HSM health factors.

Note: requesting the Health Check data causes the payShield 9000 to perform self-tests: as a result, you will hear the fans changing speed.

The following functions, described elsewhere in this manual or in other relevant manuals, allow utilization data to be viewed and managed:

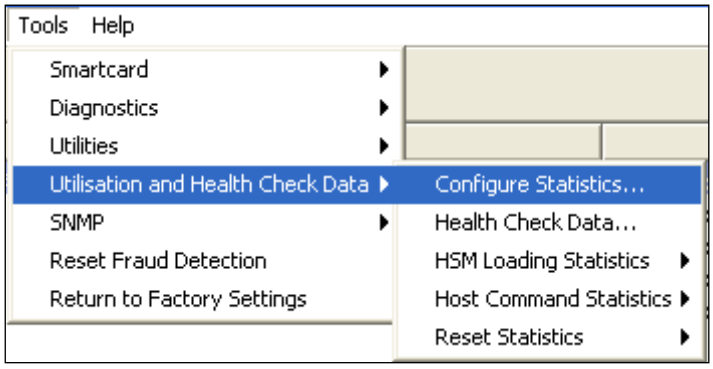
- HSM Manager:
  - Edit -> Advanced Settings (Fraud detection)
  - Tools -> HSM Utilisation Statistics -> Configure Statistics
  - Tools -> HSM Utilisation Statistics -> Health Check Data
  - Tools -> HSM Utilisation Statistics -> Reset Statistics
  - Tools -> SNMP -> Display -> V1/V2 Communities
  - Tools -> SNMP -> Display -> V3 User
  - Tools -> SNMP -> Add -> V1/V2 Communities
  - Tools -> SNMP -> Add -> V3 User
  - Tools -> SNMP -> Delete -> V1/V2 Communities
  - Tools -> SNMP -> Delete -> V3 User
- Console Commands:
  - HEALTHENABLE
  - HEALTHSTATS
  - SNMP
  - SNMPADD
  - SNMPDEL
  - A5
  - AUDITOPTIONS
  - DT
- Host Commands:
  - J8 – Get Health Check counts
  - JK – Get Instantaneous Health Check status
  - JI – Reset Health Check Data

Reporting Mechanisms

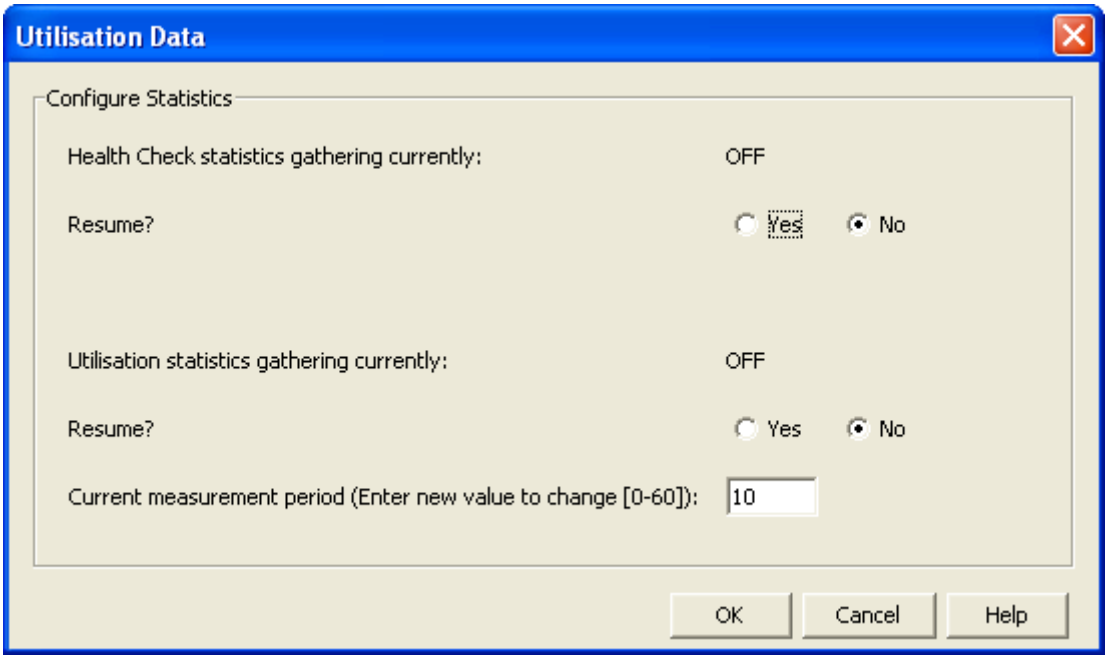
- The Utilization and Health Check data can be accessed using:
- the Console.
- Local HSM Manager (with graphical output). The data can also be saved to a USB Drive: see the section on *Saving parameter settings to a file* for guidance on how to use this facility.

- Remote HSM Manager (with graphical output). The data can also be saved to a USB Drive: see the section on *Saving parameter settings to a file* for guidance on how to use this facility.
- Host commands
- Printing at the HSM-attached printer
- SNMP

Configure Statistics *(payShield 9000 only)*



These capabilities are only available on the payShield 9000. They are not available on the HSM 8000.



Enabling/disabling Statistics Gathering

This dialog lets you enable or disable the gathering of statistics relating to the HSM's utilisation (i.e. the overall HSM loading, and counts of each host command) and to the HSM's health.

Disabling the statistics does not reset them. The statistics already gathered are retained, but new data is not added to them. Users may wish to disable statistics gathering if the HSM is temporarily taken out of service or re-purposed.

Enabling statistics restarts the accumulation of statistics, and adds new statistics to any which were gathered before statistics gathering was disabled.

Statistics gathering can be disabled/enabled as frequently as desired. The HSM will record the number of seconds that elapse while statistics gathering is enabled, so that transaction rates are calculated only over the period during which data was collected.

Gathering of statistics will be automatically disabled during periods when the HSM is not online.

Gathering of statistics will be disabled following software installation on the HSM.

To enable or disable the gathering of the statistics, the HSM must be in Offline or Secure mode with an operator logged in.

If you want to reset the gathered statistics to zero, use the Reset Statistics menu item.

Setting the Instantaneous Measurement Period

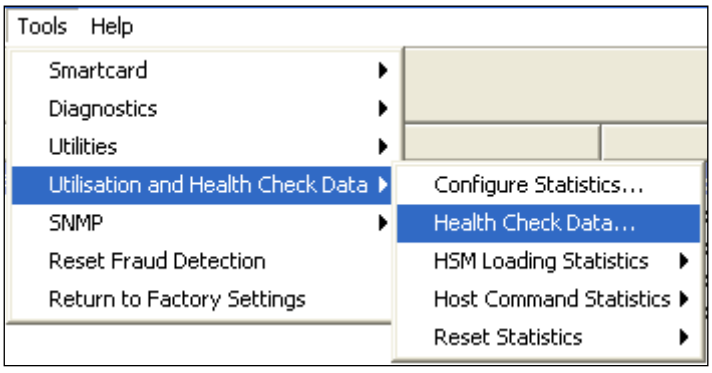
For utilisation data, users can request "instantaneous" statistics on HSM loading and command volumes. This could be useful, for example, to help understand what is happening on the HSM right now if there is a perceived issue with system throughput.

You can set the "instantaneous" measurement period. This is the number of seconds over which utilization data is gathered when the user asks for instantaneous statistics.

The period can be set from 1 to 60 seconds. Although a very short period will provide data relating to the immediate period before the instantaneous statistics were requested, it is likely to give unrepresentative data. It is suggested that a setting of 10 seconds will give a good compromise between immediacy and meaningfulness.

The HSM must be in Offline or Secure state to change this setting.

Health Check Data *(payShield 9000 only)*

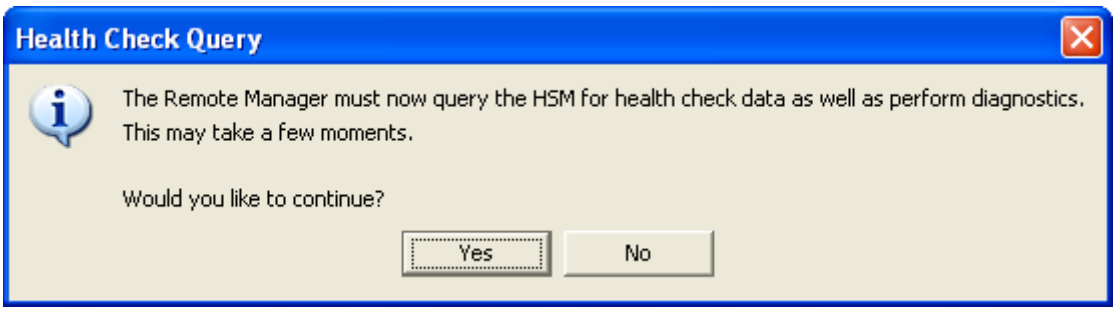


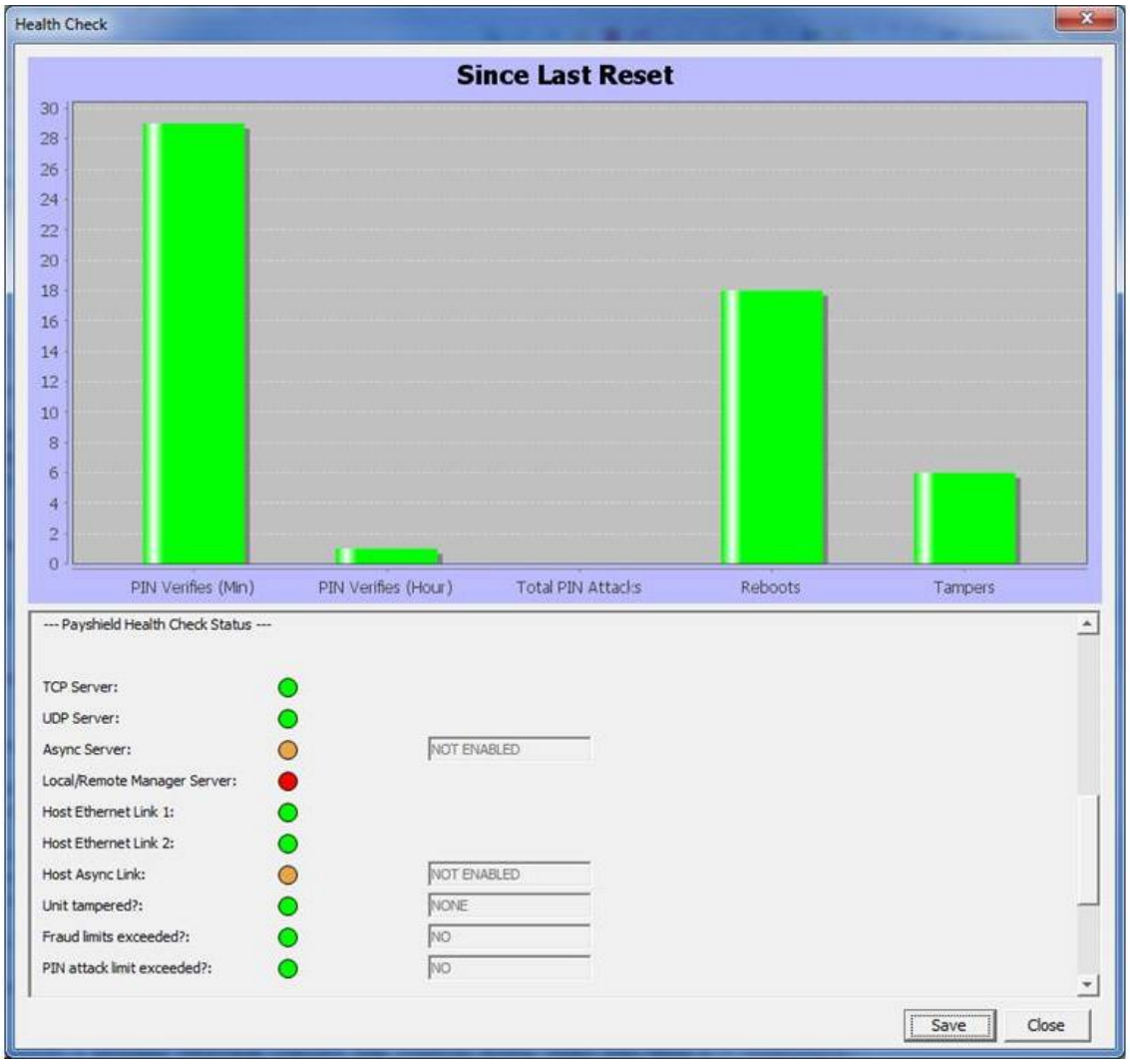
These capabilities are only available on the payShield 9000. They are not available on the HSM 8000.

This menu item provides all of the Health Check data that the HSM reports on, as well as other items provided by the DT console command.

The accumulated counts can be saved in text format to a file by using the "Save" button.

When this facility is used, there is a delay while the HSM performs its diagnostics: the user is asked to confirm that they want to proceed:





Accumulated Health Check Statistics

This data provides counts of certain HSM health-related events since the last time that the user reset the Health Check Data. These counts relate to:

- Re-starts

- Tampers*
- Fraud Detection thresholds being exceeded.

This last item is an important enhancement to the HSM's Fraud Detection functionality. Prior to version 1.1, if the Fraud Detection thresholds were exceeded the HSM would cease satisfying PIN verification commands and would ultimately erase its LMKs: this was a barrier to some users deploying the Fraud Detection functionality. Now, from version 1.1, users can elect to set Fraud Detection thresholds and monitor whether these are being exceeded without the HSM ceasing to be fully functional. ***NOTE***: if gathering of health check statistics has been suspended at any time, the counts displayed through the health check data will not be an accurate reflection of the counts that are used by the HSM to decide whether to cease satisfying commands or to delete its LMKs.

This data is represented as a bar chart and consists of the number of times that health-related events have occurred since the health check data was reset – see "*Reset Statistics*". The counts are gathered during the periods of time that the gathering of Health Check statistics was enabled – see the Configure Statistics dialog.

Because there can be a very large ratio between the tallest and shortest bars, it may be difficult to see if there are bars with small values. You can check on this by using the "Area Zoom" feature: hold the left mouse button down and drag your mouse ***downwards*** over any part of the display and release the button - the display will zoom into that part of the y-axis covered by the mouse movement. So if you drag the mouse over a section of the display from just above the x-axis to just below the x-axis, you will be able to see if there are any very low-value bars. To zoom back out, left-click and drag your mouse ***upwards*** anywhere on the display area.

Collection of data can be suspended and resumed without resetting the data.

The collected data is persistent over re-starts and power being switched off.

** Note that if you use the Erase button to delete LMKs, this will count as a tamper in the accumulated counts. But as the HSM automatically clears the tamper state in this circumstance, the Instantaneous Status (see below) will report that the HSM is not in a tampered state.*

Instantaneous Health Check Report

This provides the status of a range of HSM health factors current at the point in time when a request is made. This will report on:

- Host port status
- Whether Host Command service is running
- Whether Console service is running
- Whether Local/Remote HSM Manager service is running
- Tamper state*
- LMK information:
    - Numbers loaded
    - Types of LMK – test/production; variant/keyblock
    - No. of authorized activities

- Fraud Detection status
    - Whether PIN Verifications per min./hour have been exceeded
    - If PIN Attack limit exceeded

This data, presented as "traffic lights", indicated the status of the various health-related factors that the HSM can report on. Some "lights" are accompanied by a text box showing additional information.

A green "light" indicates that the reported item is functioning normally; a red "light" indicates that there is probably an issue which requires attention; an amber "light" indicates that the reported service is not enabled.

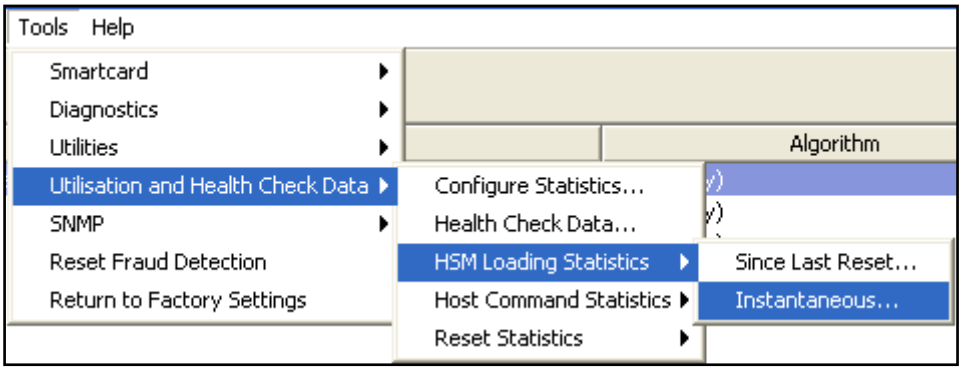
** Note that if you use the Erase button to delete LMKs, this will count as a tamper in the accumulated counts (see above). But as the HSM automatically clears the tamper state in this circumstance, the Instantaneous Status will report that the HSM is not in a tampered state.*

HSM Loading *(payShield 9000 only)*

These capabilities are only available on the payShield 9000. They are not available on the HSM 8000.

This displays statistics indicating how heavily loaded the HSM is. Two options are available:

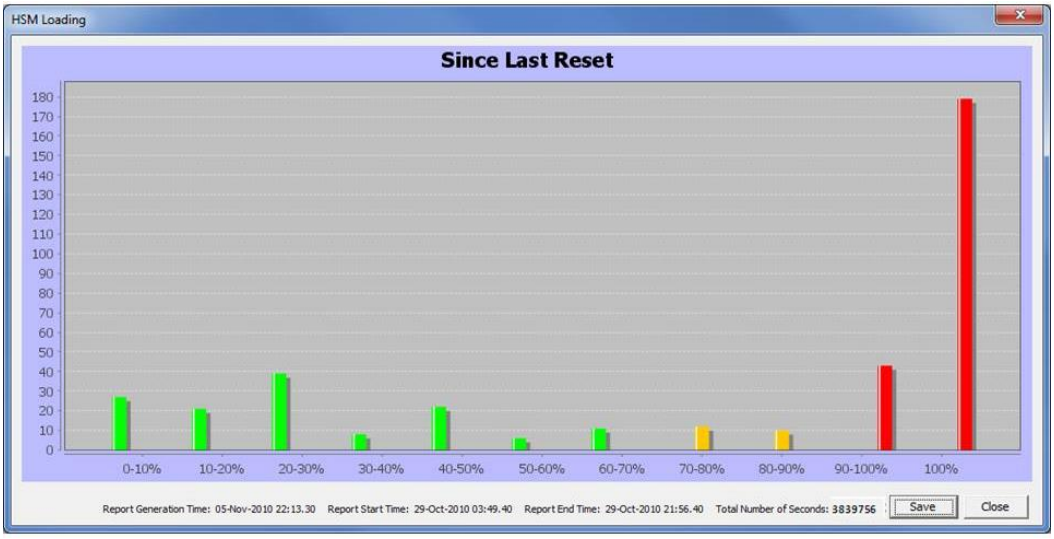
- Accumulated Data since the last Reset
- Instantaneous Data



Accumulated Utilization Data Since the Last Reset

Every second, the HSM measures how heavily loaded it is (as a percentage of its processing capacity). It accumulates counts of how many seconds the loading was between 0-10% of the HSM's capacity, how many times the loading fell in the range 10-20% of capacity, how many times the loading fell into the range 20-30%, and so on.

To be precise, the range 0-10% means from 0% to 9.99999...%, and so on. In addition to the "90-100%" data point, there is a "100%" data point: this indicates how frequently the HSM was working at its full capacity. If this data point is not zero, it is most likely that some of the demanded load (i.e. what the HSM was being asked to do) would have experienced significant latency or even time-outs at the host.



This utilization data is presented as a bar graph. The x-axis is the intervals of percentage of capacity (i.e. 0-10%, 10-20%, …) and the y-axis is a count of how many times the loading of the HSM fell into each of the intervals of capacity.

If the bars are predominantly below 50% of capacity, and there are no bars above 80% of capacity then the HSM is probably "comfortably" loaded. On the other hand, if there are significant bars over 50% of capacity and there are some bars in excess of 90% then the HSM is probably under stress: additional HSM capacity or a shifting of workload to another HSM is recommended. Urgent action is needed if you are seeing a 100% bar, as this indicates that the HSM cannot meet your peak demand.

Because there can be a very large ratio between the tallest and shortest bars, it may be difficult to see if there are bars with small values. You can check on this by using the "Area Zoom" feature: hold the left mouse button down and drag your mouse ***downwards*** over any part of the display and release the button - the display will zoom into that part of the y-axis covered by the mouse movement. So if you drag the mouse over a section of the display from just above the x-axis to just below the x-axis, you will be able to see if there are any very low-value bars. To zoom back out, left-click and drag your mouse ***upwards*** anywhere on display area.

The data can be saved in text format to a file by using the "Save" button.

This data is accumulated since the last time that a user reset the accumulation data. The data is persistent across system re-starts.

It is also possible to suspend and restart gathering of this data. This is useful, for example, if the machine is to be taken out of service temporarily or temporarily used for another application.

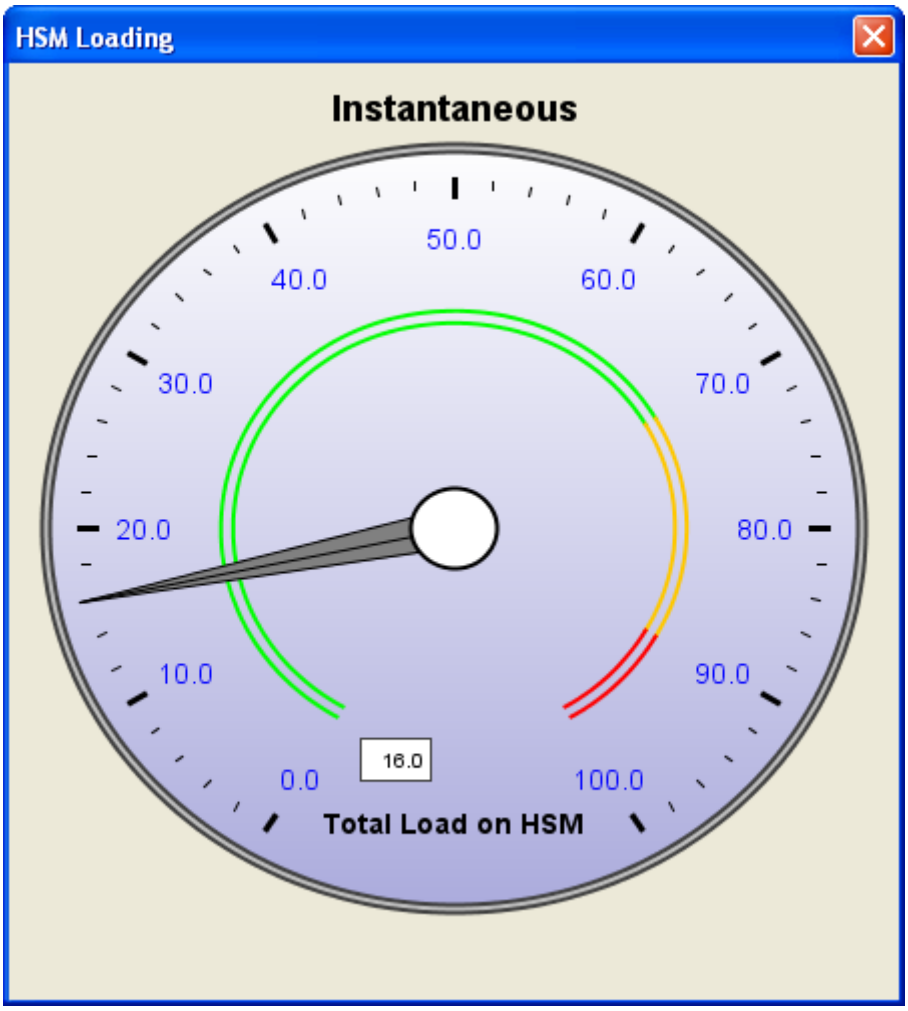
To achieve maximum throughput on the HSM it needs to be driven with multiple connections (or threads). Optimum performance is normally achieved with 4-8 threads (depending on the HSM performance model and the commands being processed). Running with only a single thread can significantly reduce the throughput of the HSM, and means that you will not be able to reach the rated throughput for the machine.

Instantaneous Utilization Data

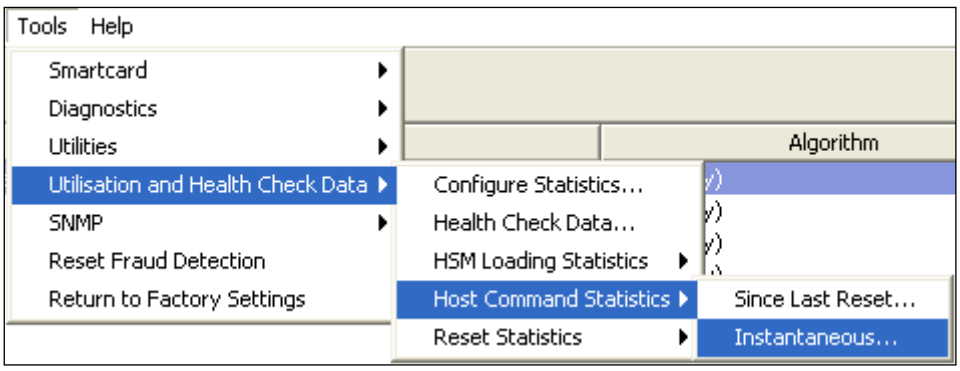
This provides you with an immediate assessment of the loading of the HSM. This is useful, for example, to perform real-time diagnostics if you are experiencing system-wide throughput or performance issues and want to understand whether the HSM is a bottleneck.

The "instantaneous" data is averaged over a period of time immediately before the data was requested which can be configured.

The information is displayed as a dial ranging from 0% to 100%. This is updated in real time – so keeping this display open while the HSM is in use lets you see immediately how the loading on the HSM is changing.



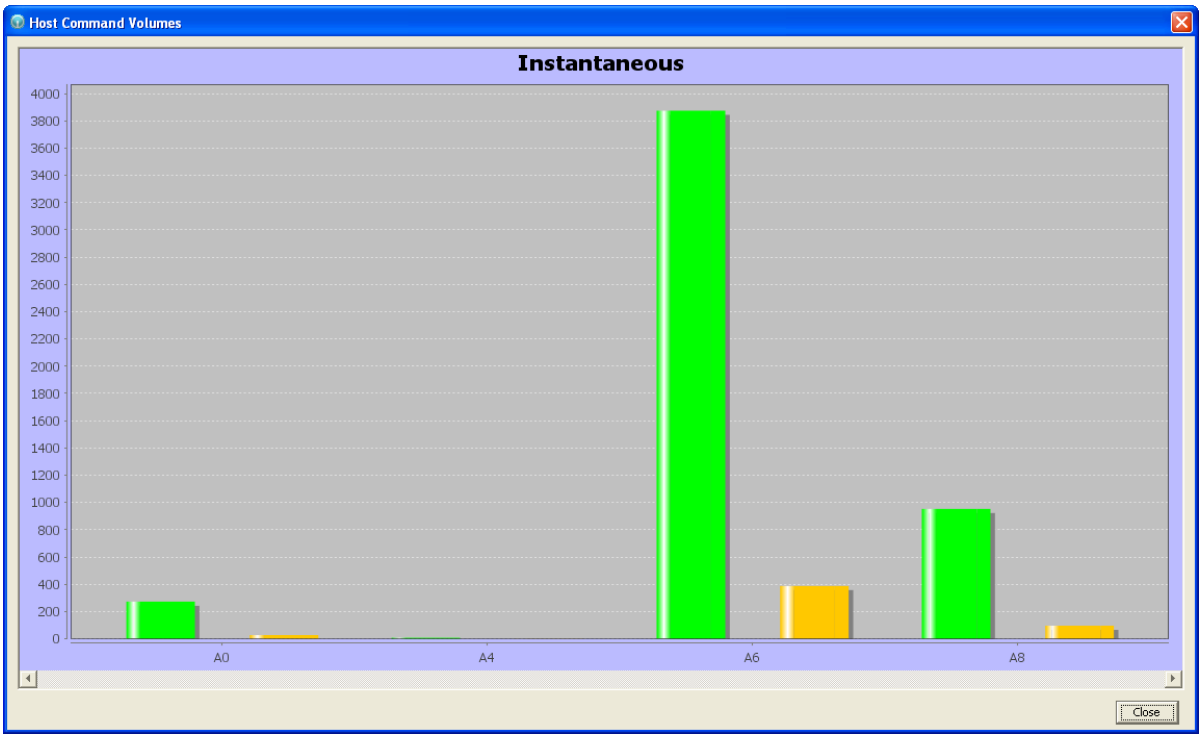
Host Command Volumes



These capabilities are only available on the payShield 9000. They are not available on the HSM 8000.

This data shows how often each Host command has been run. The user can select whether they want counts which are:

- accumulated since the last time that utilization data was reset, showing how often each host command was use. The accumulated data is persistent over re-starts, and gathering of the data can be suspended and resumed at any time.
- "instantaneous" – i.e. collected over a configurable, brief period immediately preceding the time when the report was requested.



These charts shows the number of times each command was run during the period (in green) and the average transactions per second over the period (in yellow).The accumulated counts can be saved in text format to a file by using the "Save" button.

Because there can be a very large ratio between the tallest and shortest bars, it may be difficult to see if there are bars with small values. You can check on this by using the "Area Zoom" feature: hold the left mouse button down and drag your mouse ***downwards*** over any part of the display and release the button - the display will zoom into that part of the y-axis covered by the mouse movement. So if you drag the mouse over a section of the display from just above the x-axis to just below the x-axis, you will be able to see if there are any very low-value bars. To zoom back out, left-click and drag your mouse ***upwards*** anywhere on display area.

It is important to recognize that not all commands have the same effect on HSM loading. The rated performance of the HSM (e.g. 1,500 tps for the X performance model) relates to how many CA host commands (PIN Block Translation) the HSM could run in a second. Most other host commands will run at the same speed as

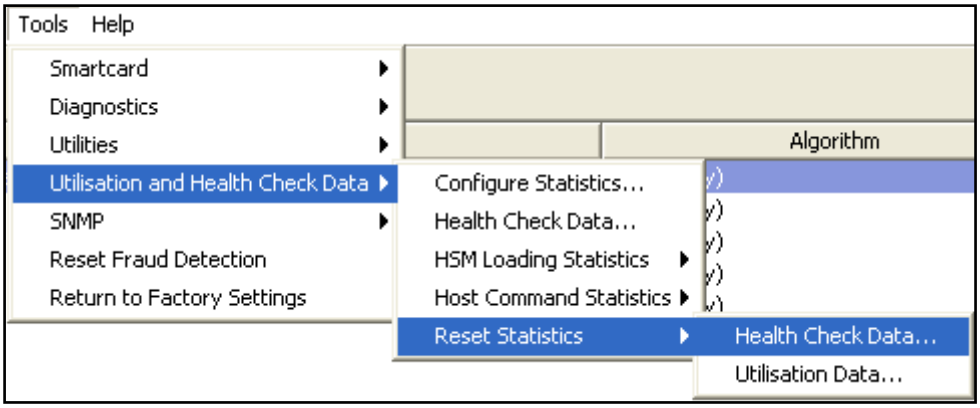
the CA command, but some will run more slowly (and impose a greater load on the HSM) and a few will run faster.

To achieve maximum throughput on the HSM it needs to be driven with multiple connections (or threads). Optimum performance is normally achieved with 4-8 threads (depending on the HSM performance model and the commands being processed). Running with only a single thread can significantly reduce the throughput of the HSM, and means that you will not be able to reach the rated throughput for the machine.

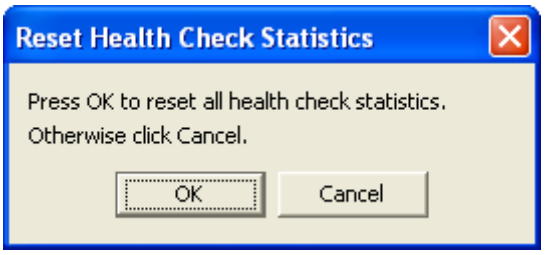
Reset Statistics *(payShield 9000 only)*

These capabilities are only available on the payShield 9000. They are not available on the HSM 8000.

The accumulated data for utilisation (i.e. HSM loading and Host Command volumes) and for health check data can be reset to zero using these menu items.



The user is asked to confirm that they want to reset the statistics:



The selected accumulated counts will be erased, and will restart from zero.

To reset health check statistics, an Operator for the Management LMK must be logged in.

Note that statistics will also be reset when new software is loaded on the HSM.

SNMP *(payShield 9000 only)*

Note: SNMP capabilities are only available on the payShield 9000. They are not available on the HSM 8000.

SNMP can be used to retrieve on demand from the HSM:

"Instantaneous" utilization data relating to HSM loading and host command volumes.

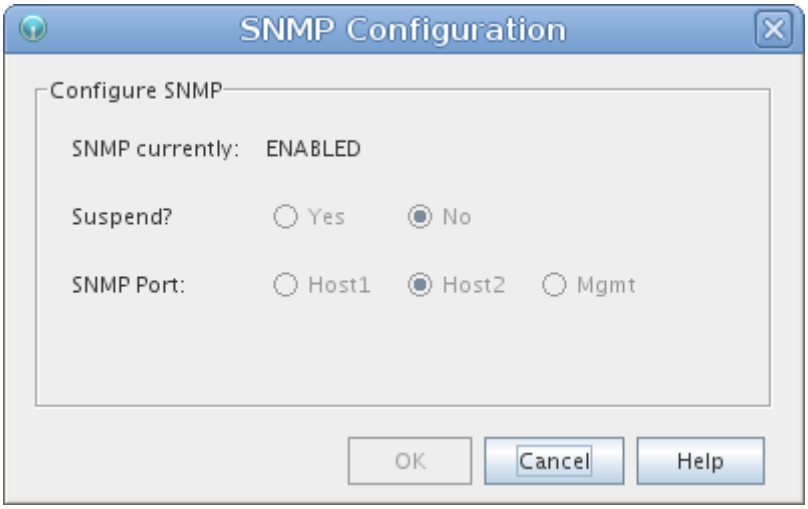
Current status of HSM health check factors.

Versions 1, 2, and 3 of SNMP are supported by the payShield 9000.

The payShield 9000 software CD includes an SNMP MIB which should be used to configure the SNMP Manager to retrieve the instantaneous utilization current health check data from the HSM.

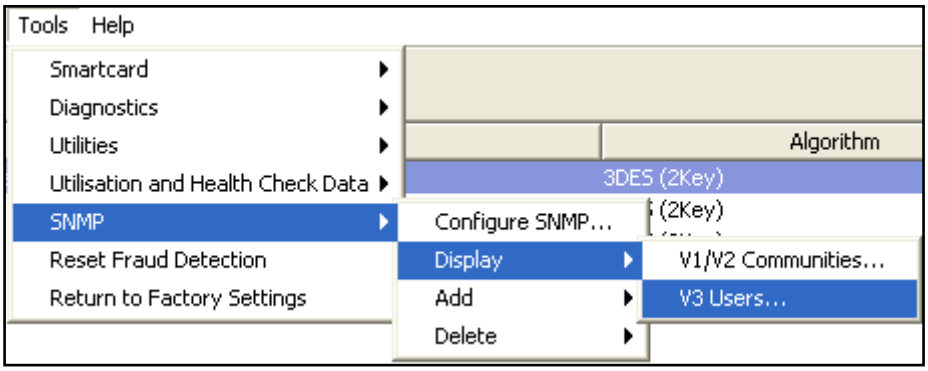
Configure SNMP *(payShield 9000 only)*

This capability is selected from the *Tools / SNMP* option, and displays the following dialogue box:



This allows SNMP reporting to suspended or activated, and selection of the Ethernet port which will be used for SNMP traffic.

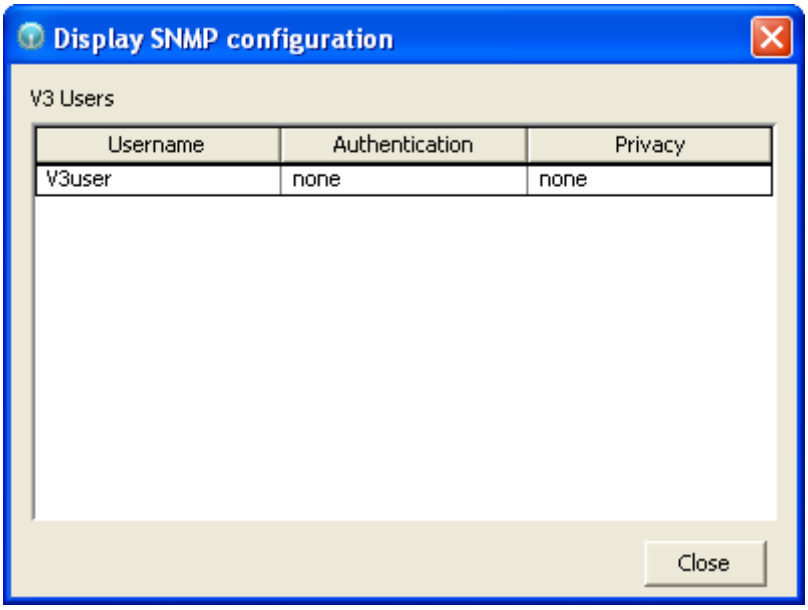
(SNMP) Display *(payShield 9000 only)*



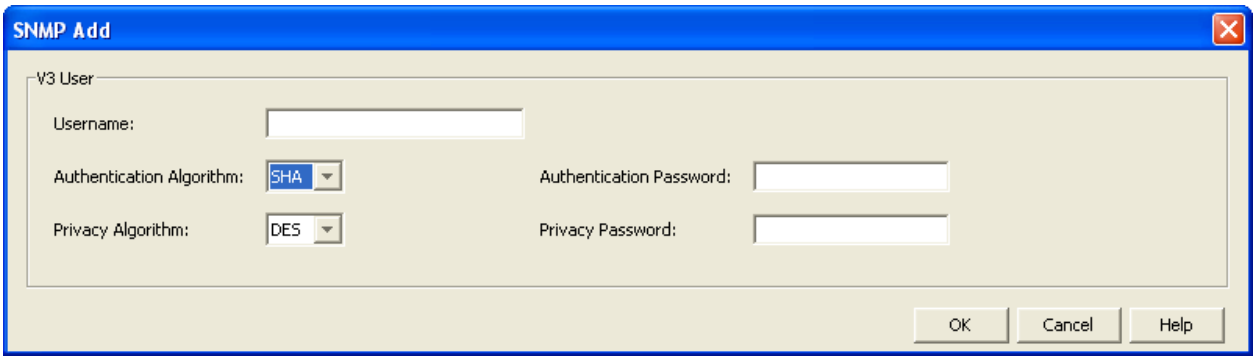
Selecting this menu item will display the Users and Communities set up for SNMP.

SNMP versions 1 and 2 use Communities.

SNMP version3 uses Users. In this environment, authentication and privacy algorithms must be specified.



(SNMP) Add *(payShield 9000 only)*



This menu item enables SNMP Users and Communities to be added.

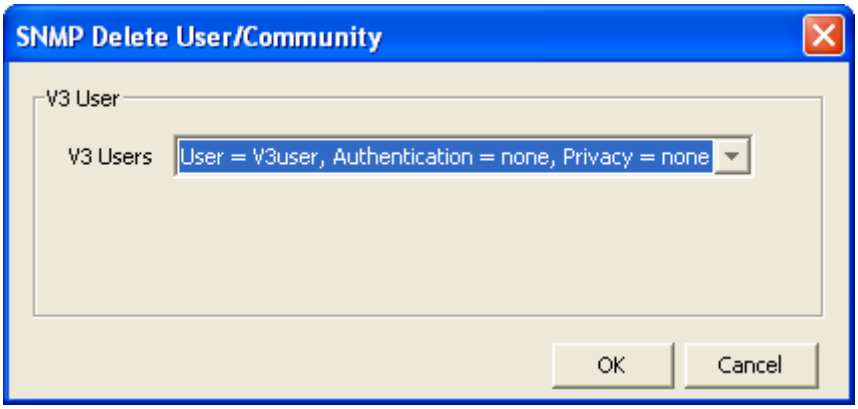
SNMP versions 1 and 2 use Communities.

SNMP version3 uses Users.

The HSM must be in Secure state with an Operator logged in to add Communities or Users.

Note: The HSM is delivered with no Users or Communities set up.

(SNMP) Delete *(payShield 9000 only)*



Selecting this menu item will enables SNMP Users and Communities to be deleted.

SNMP versions 1 and 2 use Communities.

SNMP version3 uses Users. In this environment, authentication and privacy algorithms must be specified.

The HSM must be in Secure state with an Operator logged in to remove Communities or Users.

Secure Host Communications *(payShield 9000 only)*

Notes:

- *Secure Host Communications capabilities are only available on the payShield 9000. They are not available on the HSM 8000.*
- *USB memory sticks are used to transfer material such as certificates in and out of the payShield 9000. The required format for the USB memory stick is FAT32. The Operating System used in the payShield 9000 supports most types of USB memory stick, but may not have the drivers for some of the newer types. If difficulties are experienced when trying to read from or write to a USB device, an alternative memory stick should be used.*

The Secure Host Communications sub-menu provides access to the following actions, described below, which are used to configure the payShield 9000 to use TLS or SSL to protect the link between the payShield 9000 and the host computer:

- Tools -> Secure Host Communications -> Generate Certificate Signing Request
- Tools -> Secure Host Communications -> Export HSM CA Certificate
- Tools -> Secure Host Communications -> Import Signed Certificate
- Tools -> Secure Host Communications -> Generate HMK
- Tools -> Secure Host Communications -> Recover HMK
- Tools -> Secure Host Communications -> Change HMK Passphrase
- Tools -> Secure Host Communications -> View Certificates
- Tools -> Secure Host Communications -> Delete Certificates

A description of the payShield 9000 Secure Host Communications capability is provided in Chapter 14 of the *payShield 9000 General Information Manual*.

Generate Certificate Signing Request *(payShield 9000 only)*

Notes:

- *Secure Host Communications capabilities are only available on the payShield 9000. They are not available on the HSM 8000.*
- *USB memory sticks are used to transfer material such as certificates in and out of the payShield 9000. The required format for the USB memory stick is FAT32. The Operating System used in the payShield 9000 supports most types of USB memory stick, but may not have the drivers for some of the newer types. If difficulties are experienced when trying to read from or write to a USB device, an alternative memory stick should be used.*

This process generates the HSM PKI key pair, stores the private key in tamper-protected memory and (in HMK-encrypted form) in non-volatile memory, and creates a Certificate Signing Request for the public key. See Chapter 14 of the *payShield 9000 General Information Manual* for more information.

Choosing this menu item brings up a wizard to guide the user through the process:

When completing the key type field, note that the client certificate must use the same key type. The permissible options are:

- RSA (2048-bit only)
- ECDSA P-256
- ECDSA P-384
- ECDSA P-521

Export HSM CA Certificate *(payShield 9000 only)*

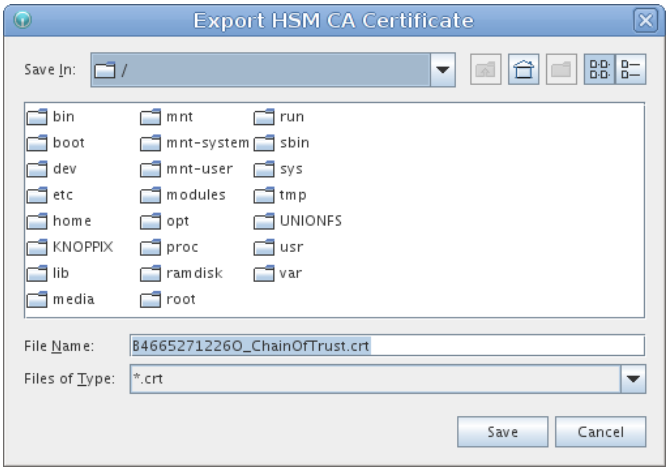
Notes:

- *Secure Host Communications capabilities are only available on the payShield 9000. They are not available on the HSM 8000.*
- *USB memory sticks are used to transfer material such as certificates in and out of the payShield 9000. The required format for the USB memory stick is FAT32. The Operating System used in the payShield 9000 supports most types of USB memory stick, but may not have the drivers for some of the newer types. If difficulties are experienced when trying to read from or write to a USB device, an alternative memory stick should be used.*

The CA certificate used by the HSM must be made available to the host applications. It can be exported using this function while the HSM is in Secure state. See Chapter 14 of the *payShield 9000 General Information Manual* for more information.

When selecting this function, a wizard will be presented to guide you through the process.

You will be required to specify where you want the certificate stored: this will typically be on a USB memory device: Chapter 10 explains how to mount a USB memory device. Select the root directory from the *Save in:* option box :



Double click on the directory where you want to save to (typically *media*) and on any sub-directories within that.

Import Signed Certificate *(payShield 9000 only)*

Notes:

- *Secure Host Communications capabilities are only available on the payShield 9000. They are not available on the HSM 8000.*
- *USB memory sticks are used to transfer material such as certificates in and out of the payShield 9000. The required format for the USB memory stick is FAT32. The Operating System used in the payShield 9000 supports most types of USB memory stick, but may not have the drivers for some of the newer types. If difficulties are experienced when trying to read from or write to a USB device, an alternative memory stick should be used.*

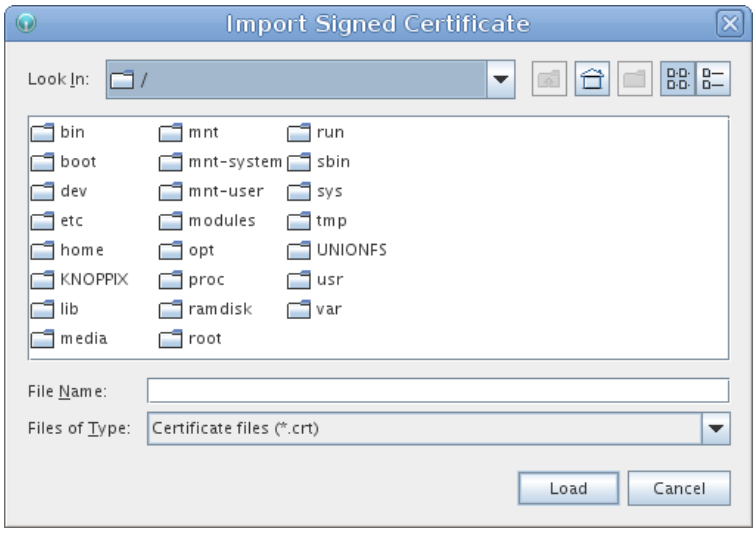
Following the certificate signing request, the signed certificate for the HSM's public key will need to be imported. It will also be necessary to import:

- all signed certificates for applications
- Self-signed certificate for the root CA
- Where a chained CA hierarchy is being used, certificates for each intermediate CA signed by the next CA up in the hierarchy.

This is achieved using this function while the HSM is in Secure state. See Chapter 14 of the *payShield 9000 General Information Manual* for more information.

When selecting this function, a wizard will be presented to guide you through the process.

You will be required to specify where the required certificate certificate stored: this will typically be on a USB memory device: Chapter 10 explains how to mount a USB memory device. Select the root directory from the *Save in:* option box :



Double click on the directory where the certificate is stored (typically *media*) and on any sub-directories within that.

Generate HMK *(payShield 9000 only)*

Note: Secure Host Communications capabilities are only available on the payShield 9000. They are not available on the HSM 8000.

This action is used to generate the HSM Master Key (HMK). The HMK is used to encrypt the private key used by the SSL in establishing the TLS/SSL session.

The HMK-encrypted private key is held outside of the tamper-protected memory such that if the HSM detects a tamper event it is not lost: the unencrypted private key used during live running is held in tamper-protected memory and is lost if the HSM detects a tamper event.

The private key can therefore be recovered after a tamper event by decrypting the encrypted version using the HMK.

The HMK is also used to allow recovery of the HSM's private key, the certified public key and the CA self-signed public key certificate used for Remote HSM Manager.

The HMK is generated by the HSM using 2 passphrases entered by security officers. These passphrases must be provided to reconstitute the HMK when recovering the private key after a tamper event. It is held in tamper-protected memory such that it is automatically erased if the HSM detects an attempted tamper.

The HMK also performs the role previously played by the RMK (Recovery Master Key) in recovering the private key for the Remote HSM Manager CA.

See Chapter 14 of the *payShield 9000 General Information Manual* for more information.

Passphrases must contain at least the following characters, and cannot be re-used for 10 generations:

- 2 digits
- 2 uppercase characters
- 2 lowercase characters
- 2 symbols (ex. !/?.#:')

Recover HMK *(payShield 9000 only)*

Note: Secure Host Communications capabilities are only available on the payShield 9000. They are not available on the HSM 8000.

If the HSM detects a tamper event, its private PKI key used to establish TLS/SSL sessions is deleted. An HMK-encrypted copy of the private key is held in non-volatile memory, and the key itself can be recovered and restored to tamper-protected

memory by entering the passphrases used at HMK generation command while the HSM is in Secure state.

See Chapter 14 of the *payShield 9000 General Information Manual* for more information.

Change HMK Passphrase *(payShield 9000 only)*

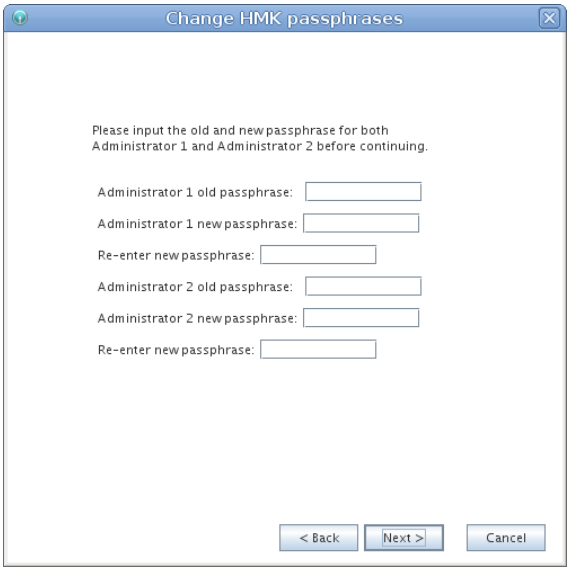
Note: Secure Host Communications capabilities are only available on the payShield 9000. They are not available on the HSM 8000.

The HMK passphrase should be changed regularly as best security practise, and will need to be changed if a security officer is replaced by another person. This is accomplished using this function while the HSM is in Secure state.

See Chapter 14 of the *payShield 9000 General Information Manual* for more information.

You will be taken through the process by a wizard:

You will need to enter both the old and the new passphrases for the selected users:



View Certificates *(payShield 9000 only)*

Note: Secure Host Communications capabilities are only available on the payShield 9000. They are not available on the HSM 8000.

The payShield 9000 will establish TLS/SSL sessions only with applications for which it has stored a copy of their certificate. All stored certificates including the payShield's own certificate and CA certificates) can be viewed using this function.

See Chapter 14 of the *payShield 9000 General Information Manual* for more information.

Delete Certificates *(payShield 9000 only)*

Note: Secure Host Communications capabilities are only available on the payShield 9000. They are not available on the HSM 8000.

Where it is no longer required to establish TLS/SSL connections with an application or where a certificate has been withdrawn or updated, it will be necessary to delete the certificate stored on the payShield 9000. This can be achieved using this function while the HSM is in Secure state.

See Chapter 14 of the *payShield 9000 General Information Manual* for more information.

Resetting Fraud Detection

If the HSM detects what it thinks is an attempt at PIN fraud, you must reset the fraud detection facility before normal host processing can be resumed.

Note: The HSM fraud detection values are entered using the **Advanced Settings** option on the **Edit** menu.

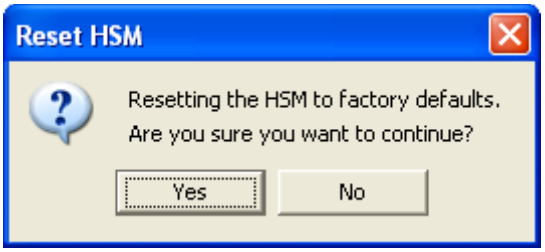
When you select the **Reset Fraud Detection** option from the **Tools** menu, a message is displayed asking you to confirm that you want to reset the fraud detection function.

Click **OK**.

Return to Factory Settings

This utility is only available when using Local HSM Manager – it is not available when using Remote HSM Manager. The HSM must be in Secure state with an Operator logged in.

The user is asked to confirm that they want to use this facility:



Use of this utility returns the HSM into the state it was in when it was shipped from the factory. This is to make the machine secure when it is taken out of service

either temporarily (e.g. for off-site servicing) or permanently (e.g. if disposing of the unit).

This utility will erase or reset to their initial values:

- LMKs
- Data in user memory
- Port configurations
- Security settings
- Fraud detection settings
- Audit logs and error logs
- Audit option settings
- Utilisation and health check statistics (payShield 9000 only)

This utility cannot reset firmware or licenses installed on the HSM. Therefore after use of this facility, the HSM will still have the most recently installed firmware and license – which may be different from the firmware and license when the HSM was shipped from the factory.

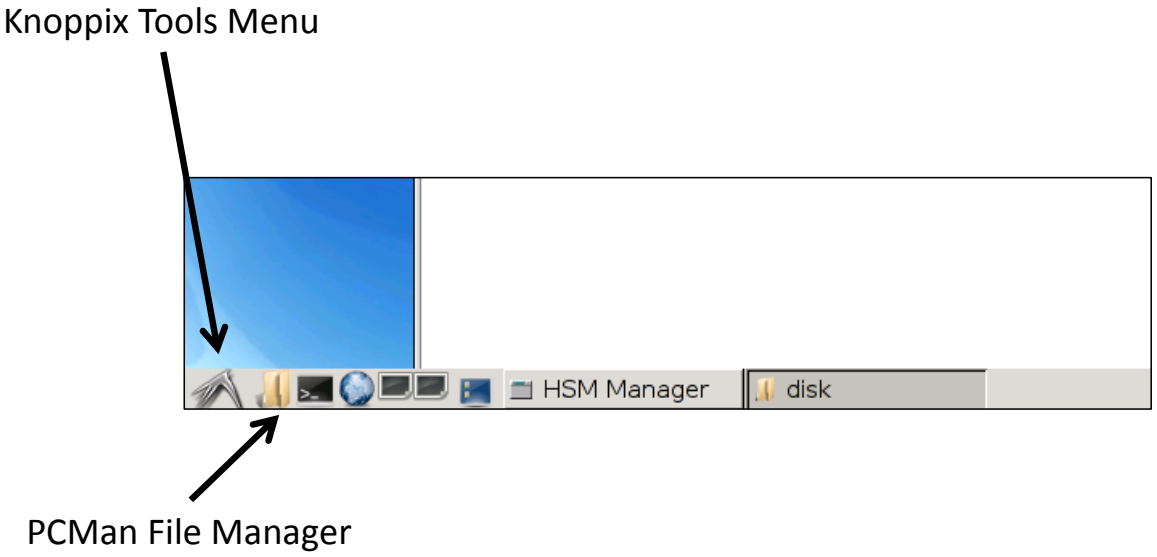
For this utility to take effect, you will be reminded that you need to re-boot the HSM:

>> Chapter 10 – Knoppix Tools

Overview

The HSM Manager application is developed for the Knoppix operating system (an implementation of Linux). The HSM Manager workstation loads Knoppix when booting up from the HSM Manager CD.

Knoppix provides a number of tools and utilities, accessible from the Knoppix Tools Menu icon at the bottom-left of the desktop:



In general, users will not need to use any of these tools. However, certain tools may be useful, and their operation is described below. These notes are designed to guide users who are not familiar with the Knoppix (or Linux) operating system: users who are experienced in Knoppix may wish to follow other procedures.

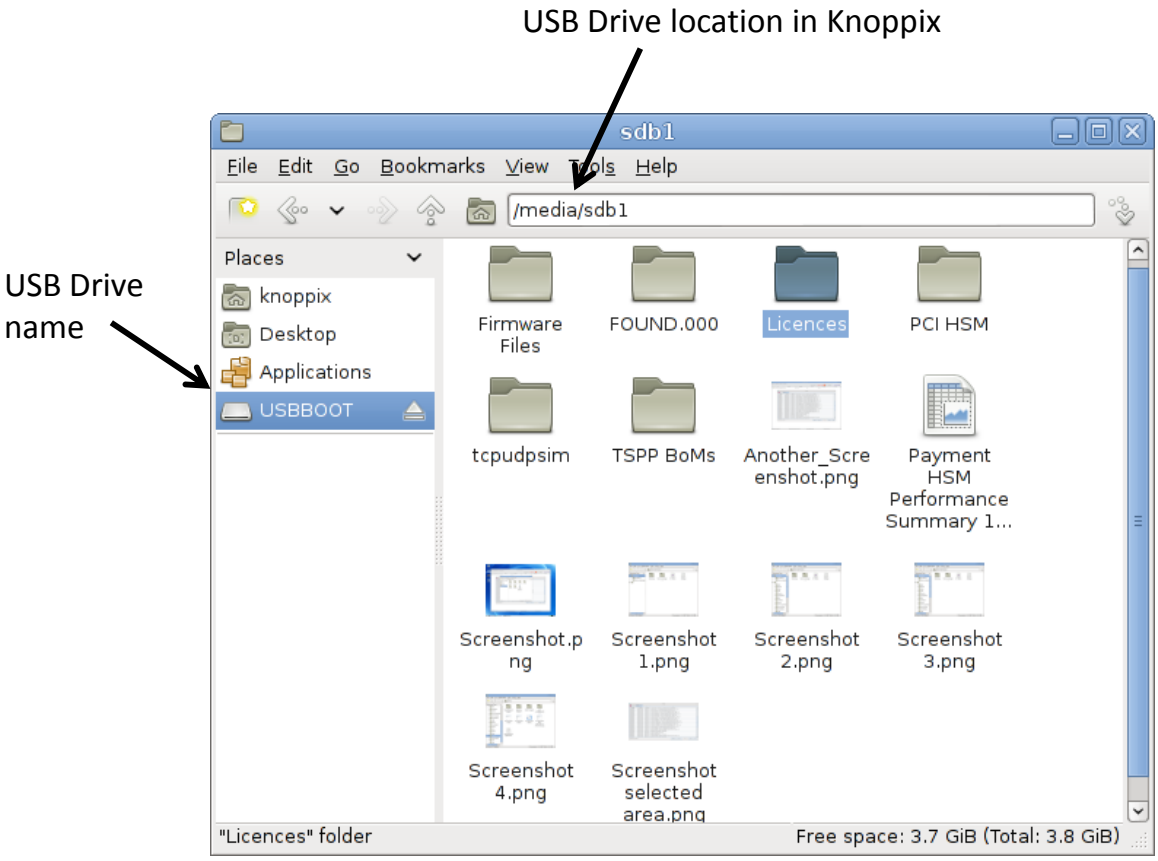
Capturing Screenshots to a USB Drive

It may be useful to capture screenshots for purposes such as training or to record settings in human-readable form.

Mounting the USB Drive

1. Insert the USB Drive (e.g. a memory stick) into a USB port on the HSM Manager workstation.
2. Start the *PCMan File Manager* tool. This is available from the *Accessories* menu within the Knoppix Tools Menu.
3. The file manager window will open. In the View menu, click on the check box *Side Pane / Show Side Pane*.

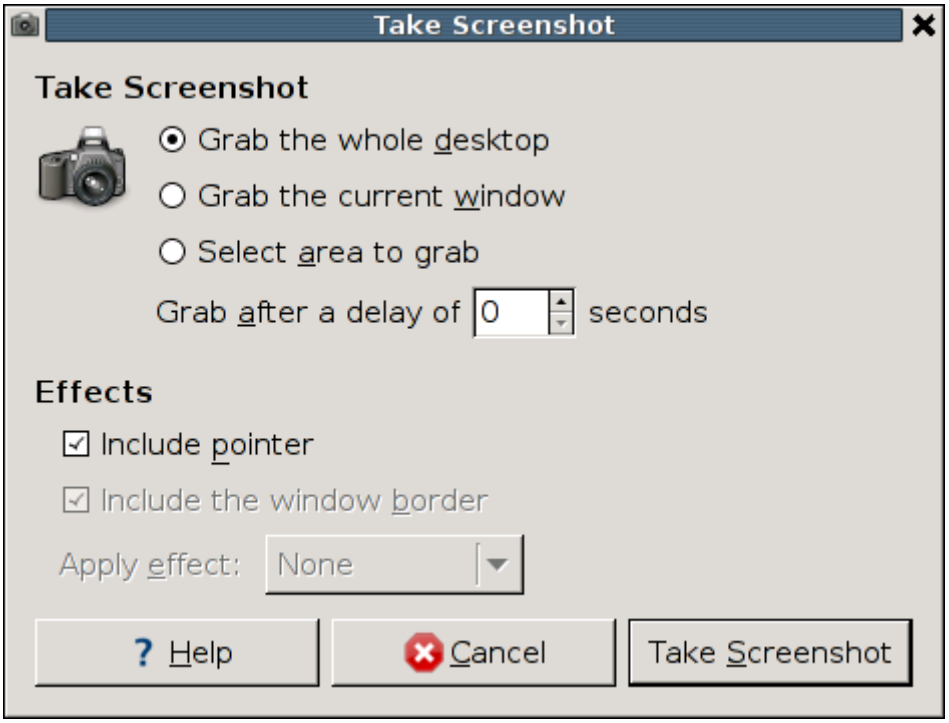
4. Click on the USB drive in the left-hand pane. (*Note that the name of the USB Drive may change when you do this.*) If "Directory Tree" is displayed at the left hand side just below the navigation bar, then select "Places" instead. The contents of the USB Drive will appear in the main (right) pane, and the USB Drive location in Knoppix will appear in the pathname panel (*/media/sdb1*in the example below).



Taking the Screenshot

5. Take the screenshot by using either:
   a. the *Screenshot* icon on the desktop.
   b. the *Screenshot* tool from the *Accessories* menu in the *Knoppix Tools* menu.

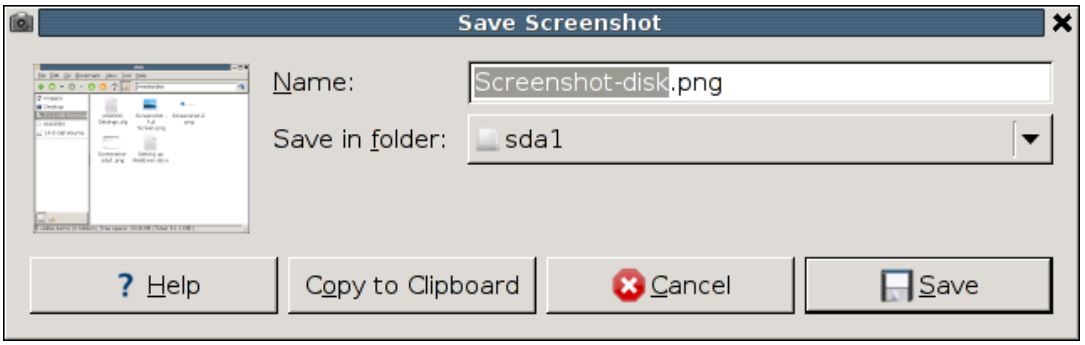
   This allows you to capture the whole desktop, the current window, or any rectangular area that you want to capture.



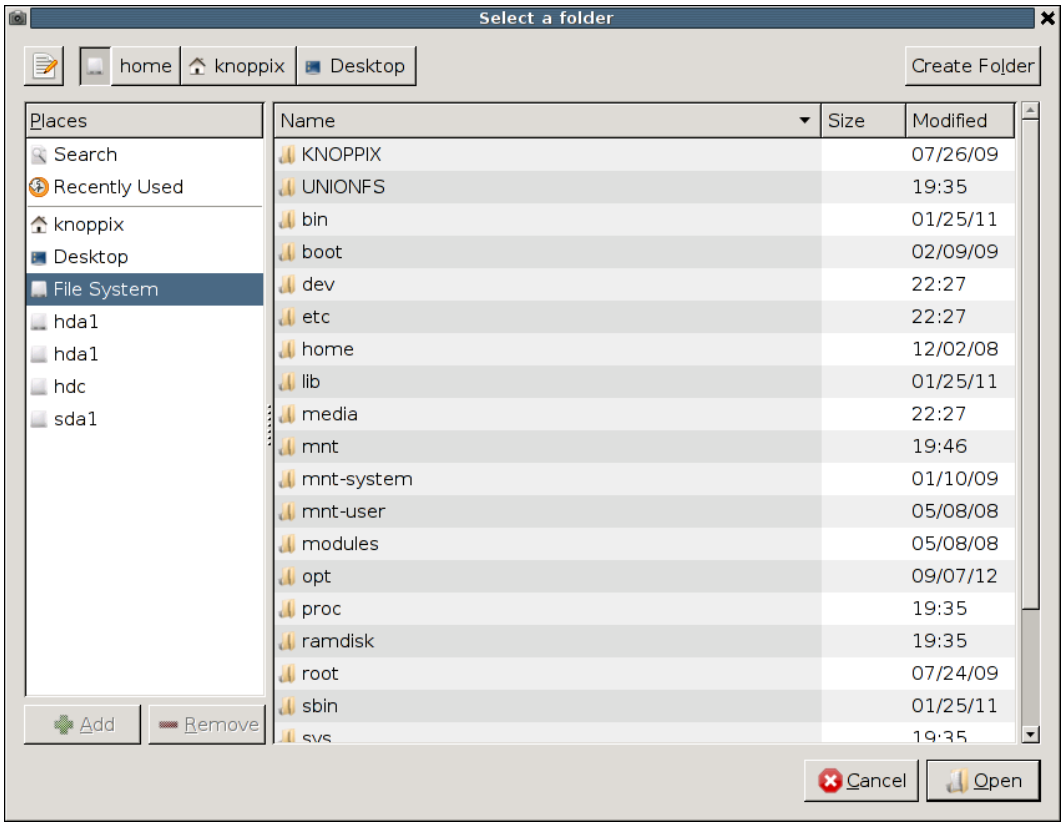
Click on *Take Screenshot*. If you have chosen *Select Area to Grab*, position the pointer at one corner of the desired section and then hold down the left button on the mouse and drag it over the desired section of the desktop.

Saving the Screenshot

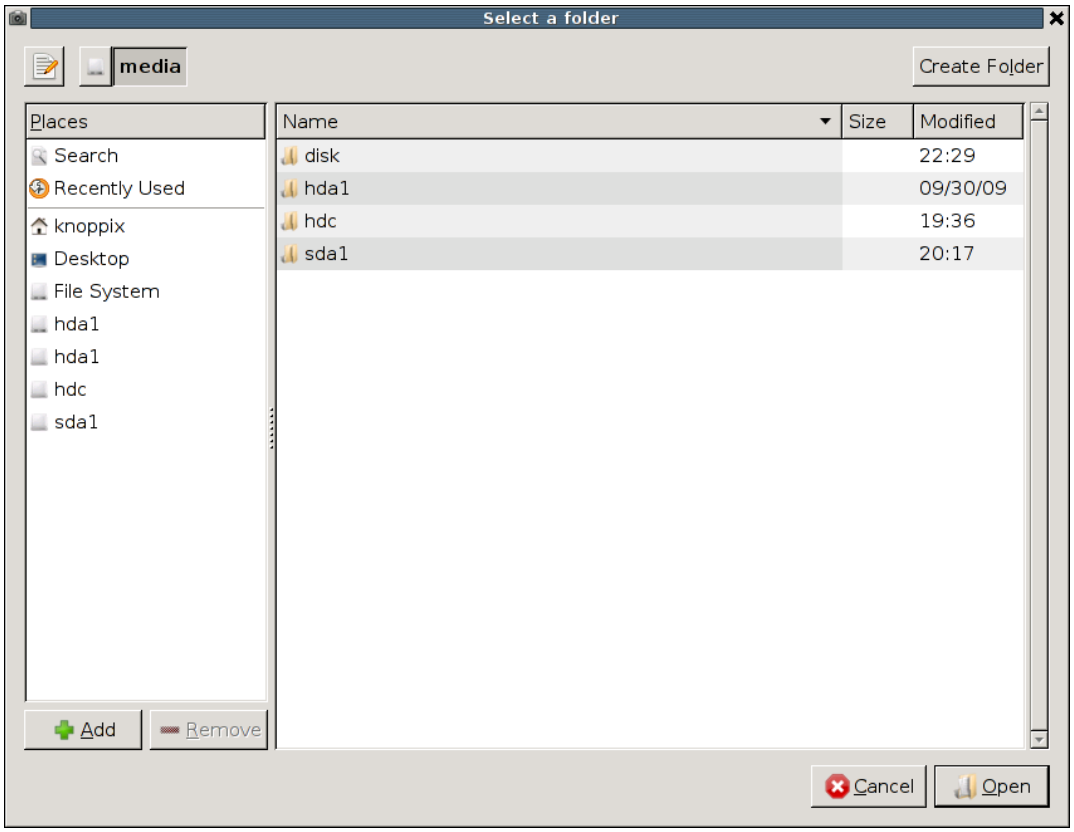
6. A Save Screenshot dialogue box will be presented:



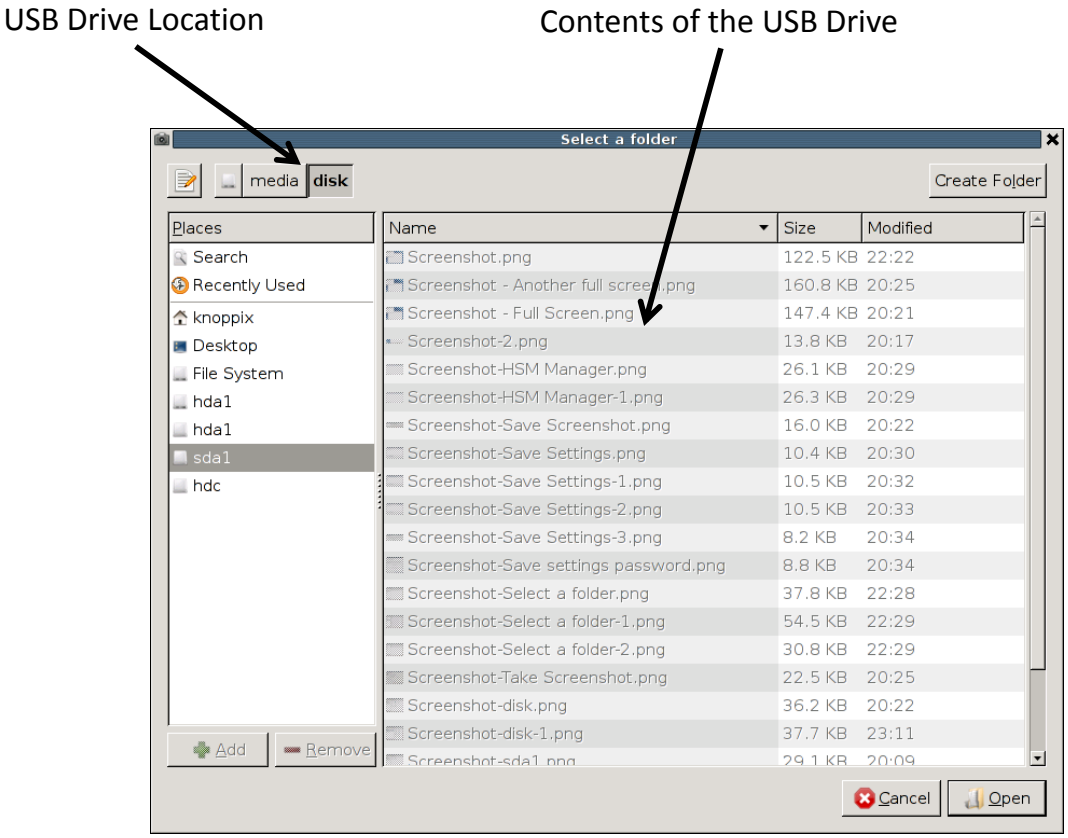
7. You now need to select the folder (which represents your USB drive) to save the screenshot to. Use the *Save in folder:* drop-down menu and select *Other*. You are now presented with a map of the file system. Double-click on *File System* in the left pane.



8. Identify in the main (right) pane the folder that contains your USB Drive: this is given in the USB Drive location - see the screenshot at *step 4* above, and in this example the folder is *media*. (You could also use the folder *tmp* to temporarily store the screenshot within Knoppix.) Double-click on the folder to display the locations within it:



9. In the list of locations, identify the location that corresponds to your USB Drive: this is given in the USB Drive location - see the screenshot at *step 4* above, and in this example, the location is *disk*. Double-click on this entry to display the contents of the USB Drive and the USB Drive location:



10. Click on *Open*.

11. In the Save Screenshot dialogue box (see *step 6* above) edit the suggested filename (if required) and click on *Save*.

    Hint: if you get an error message indicating that Knoppix was unable to capture the screenshot, try editing the suggested filename to something simpler and shorter.

Saving Further Screenshots

If you want to take more screenshots and save them to the USB drive, you need to perform only steps *5*, *6*, and *11*.

Unmounting the USB Drive

When you have finished saving to the USB Drive, you must Unmount it before removing the USB Drive. To do this, right-click on the entry for the USB Drive in the file manager window (see *step 4* above) and select *Unmount Volume*.(You can ignore any "Unable to unmount device" error message.)

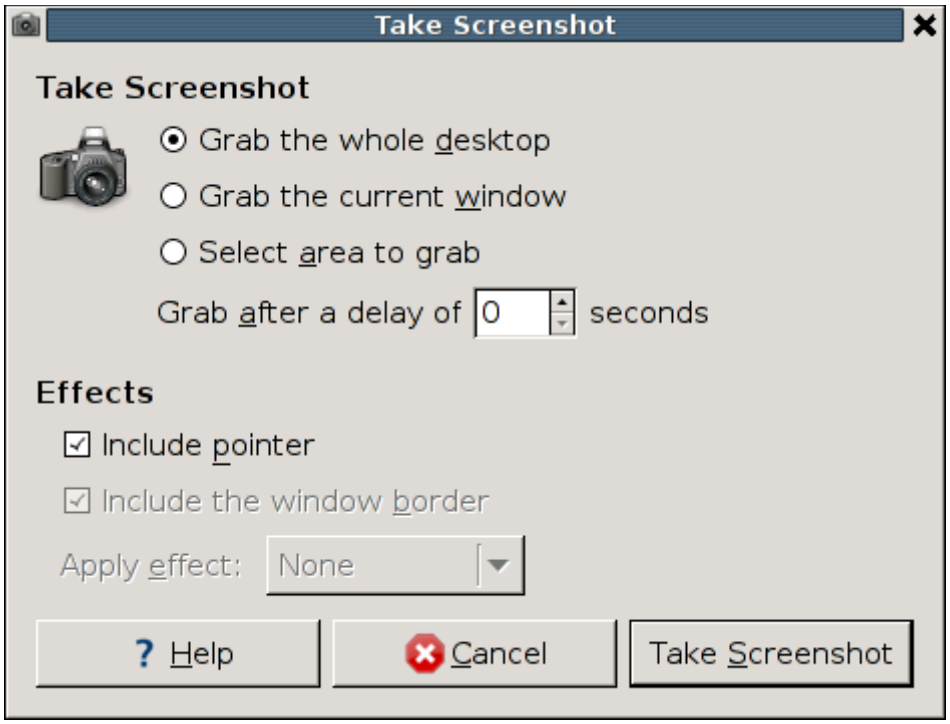
Capturing and Viewing Screenshots temporarily in Knoppix

Screenshots can also be saved temporarily within the Knoppix file system - any screenshots saved in this way will be lost when you exit from Knoppix. It is recommended that the /tmp directory is used for this purpose: you may not be able to save to other locations (including the Desktop) because of restricted permissions.

The preceding section on saving to a USB Drive indicates how you would elect to save to the /tmp folder.

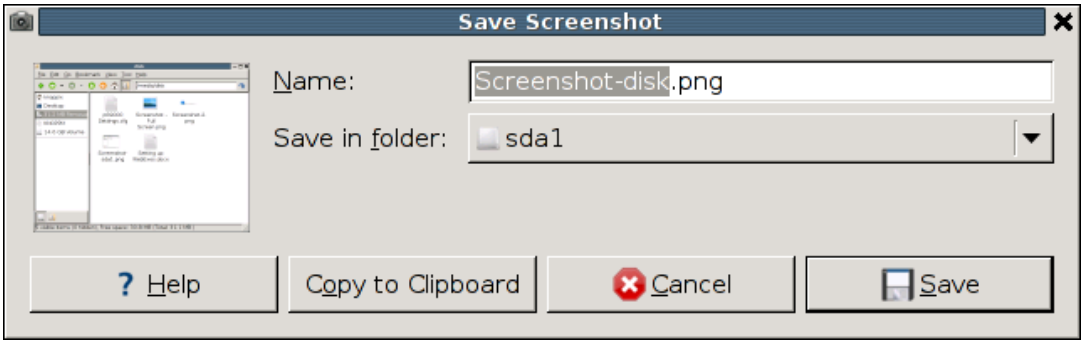
In order to save a screenshot to the /tmp folder:

1. Take the screenshot by using the *Screenshot* tool from the *Accessories* menu in the *Knoppix Tools* menu. This presents the *Take a Screenshot* dialogue box, which allows you to capture the whole desktop, the current window, or any rectangular area that you want to capture.



Click on *Take Screenshot*. If you have chosen *Select Area to Grab*, position the pointer at one corner of the desired section and then hold down the left button on the mouse and drag it over the desired section of the desktop.

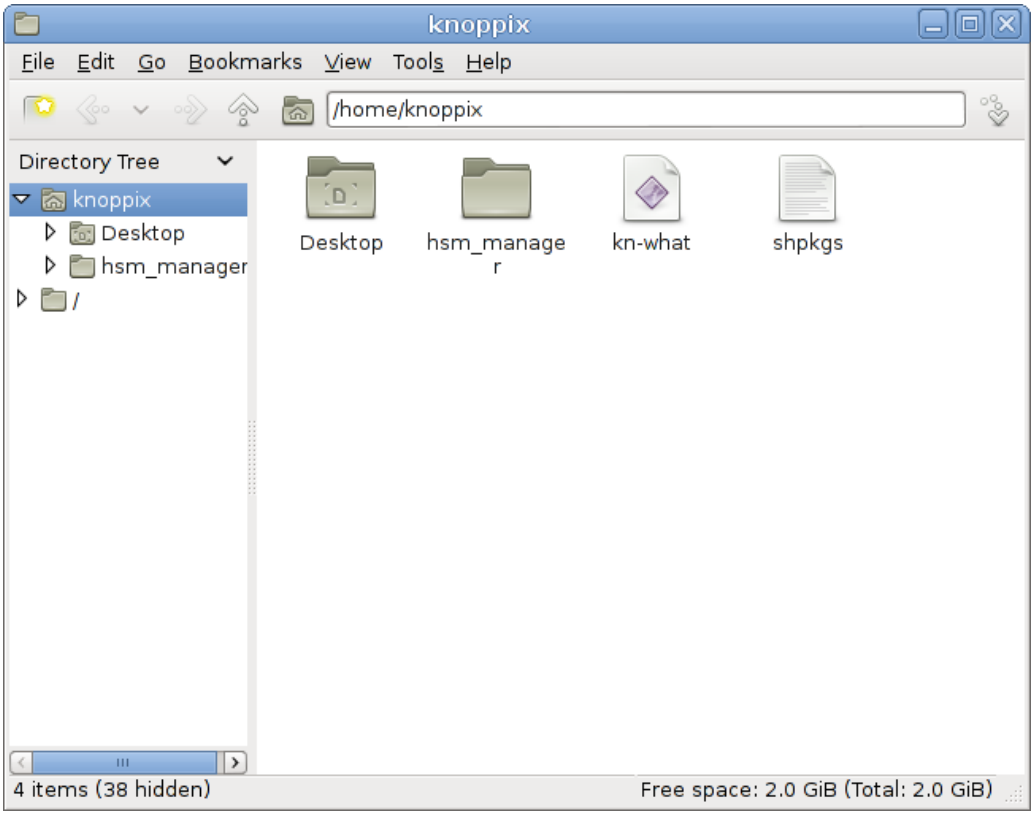
2. The *Save Screenshot* dialogue box will be presented.



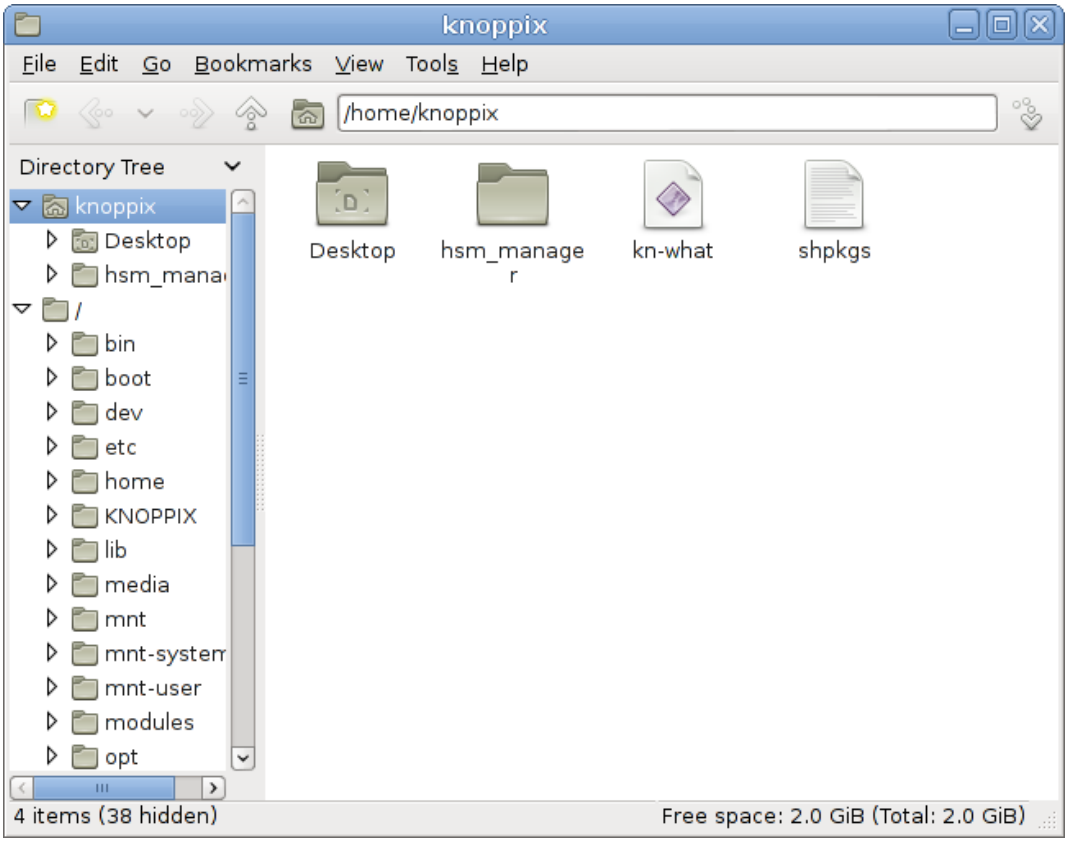
3. From the *Save in folder* pull down menu select *Other* to open the *Select a Folder* dialogue box. Click on *File System* in the left-hand pane, and then *tmp* in the main right-hand pane. Click *Open* at the bottom of the dialogue box: the Select a Folder dialogue box will close, leaving the *Save Screenshot* dialogue box open.
4. Click on Save.

If you want to view a screenshot (or any other file saved in /tmp):

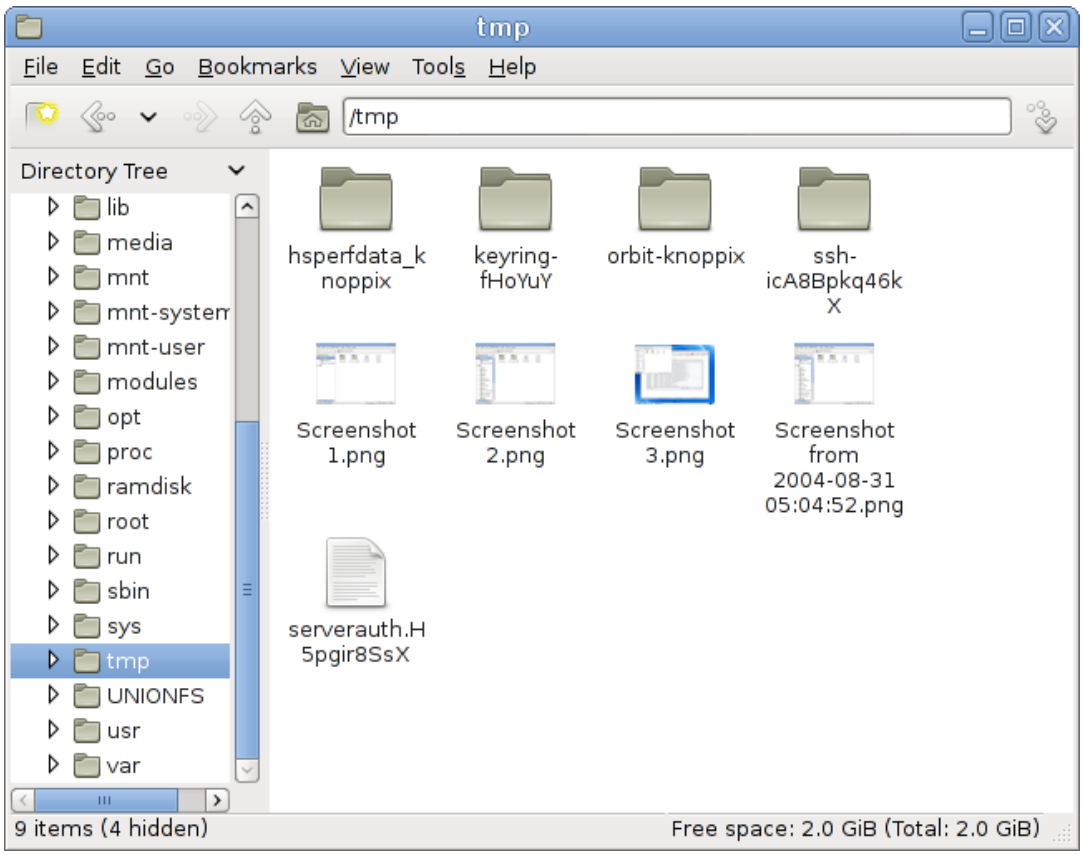
1. Start the *PCMan File Manager* tool. This is available from the *Accessories* menu within the Knoppix Tools menu.
2. The file manager window will open. In the View menu, click on the checkbox *Side Pane / Show Side Pane*. If "Places" is displayed on the left hand side just below the navigation bar, select "Directory Tree" instead:



3. Click on the root folder icon to expand it:



4. Scroll down to the /tmp folder and click on it: the files in the /tmp folder will be displayed in the main, right-hand panel.



5. In the main (right) pane, click on the file that you want to view.

>> Appendix A – User Roles & Access Rights

Menu	Function	Guest (No LMKs installed)	Guest (with LMKs installed)	Operator	Security Officer
File	Connect	n/a	n/a	n/a	n/a
	Disconnect	■	■	●	●
	Login		■	■	■
	Logout			●	●
	Load Settings	■[1]		✪[1]	✪
	Save Settings	■		✪	✪
	Load Firmware	■	■	●	●
	Load Licence	■	■	●	●
	Exit	■	■	●	●
Edit	General Settings	■	□	○ ✪	○ ✪
	Advanced Settings	■	□	○ ✪	○ ✪
	Initial Settings	■	□	○ ✪	○ ✪
	Host Interface	■	□	○ ✪	○ ✪
	Management Interface	■	□	○ ✪	○ ✪
	Printer Interface	■	□	○ ✪	○ ✪
	Host Commands	■	□	○ ✪	○ ✪
	PIN Blocks	■	□	○ ✪	○ ✪
	Auditing			○	○ ✪
	HSM Date/Time	■	□	○ ✪	○ ✪
	Authorize				●
View	Logs (Error)	■	□	○ ✪	○ ✪
	Logs (Audit)	■	□	○	○ ✪
	HSM Information	■	■	●	●
	Remote Details	■	■	●	●
LMK	Generate LMK	■		●	●
	Install LMK	■		●	●
	Install Old LMK				●
	Copy LMK Component Card	■		●	●
	Uninstall LMK				●
Keys	Generate Keys			●[2]	●[2]
	Key Import			●[2]	●[2]
	Key Export			●[2]	●[2]
	Generate Components			●[2]	●[2]
	Encrypt Components				●[2]
	Form Key from Components				●[2]
Security	Initialize Group	n/a	n/a	n/a	n/a

Menu	Function		Guest (No LMKs installed)	Guest (with LMKs installed)	Operator	Security Officer
Group	Add Card to Group		■	■	●	●
	Delete Card from Group		■	■	●	●
	Delete Group		■	■	●	●
	Display Group Details		■	■	●	●
State	Go Offline		■	■	●	●
	Go Online		■	■	●	●
	Go Secure		■	■	●	●
Tools	**Smartcard**	Personalize Card	■	■	●	●
		Edit Details	■	■	●	●
		Change PIN	■		●	●
		Verify Card	■	■	●	●
	Tools	Ping	■		●	●
		Tracert	■		●	●
		Netstat	■		●	●
		Route	■		●	●
		FiconTest	■		●	●
	Return to Factory Settings				●	●
	Utilization Statistics	Configure Statistics	□	□	●	●
		Health Check Data	■	■	●	●
		HSM Loading	■	■	●	●
		Host Command Statistics	■	■	●	●
		Reset Statistics			✪	✪
	SNMP	Display	■	□	✪	✪
		Add			●	●
		Delete			●	●
	Utilities	Calculate Key Check Value			●	●
		Encrypt Decimalization Table				●
		Translate Decimalization Table				●
		Generate MAC on IPB				●
		Generate CVV/CVC				●
		Generate VISA PVV				●
	Reset Fraud Detection		■			●
	Restart HSM		■	■	●	●

■ Function permitted (parameters can be modified)
□ Function permitted (parameters can only be viewed)
● Function permitted (parameters can be modified) – when logged on using any installed LMK
○ Function permitted (parameters can only be viewed) – when logged on using any installed LMK
✪ Function permitted (parameters can be modified when logged on using the management LMK)

Notes:

1. Audit Settings are not loaded.
2. Operations using variant keys will follow the rules imposed by the Key Type Table (see Chapter 4 of the payShield 9000 General Information Manual for full details).

>> Appendix B – Fraud Detection Functions

A description of the Fraud Detection functions can be found in Chapter 7 of the payShield 9000 General Information Manual or Appendix J of the HSM 8000 Console Reference Manual.

>> Appendix C – Key Type Table (Variant LMKs)

The HSM provides a set of commands for key generation, key export and key import. An export command is one that translates a key from LMK encryption to encryption under a ZMK, for sending to another party. Import is the reverse, for receiving keys and translating to local storage. The Key Type Table (see Chapter 4 of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command reference Manual*) controls 'permitted actions' for HSM Manager and host commands used to generate, import and export keys.

Errors are reported when an action breaks the rules imposed by the table. For example:

```
29 : Key function not permitted
```

The table shows the actions that can be applied to each specific LMK pair.

>> Appendix D – Key Scheme Table

Whenever a key is entered into the HSM, it must be prefixed by a Key Scheme Tag which allows the HSM to interpret the key correctly. The Key Scheme Table can be found at Appendix C of the *payShield 9000 General Information Manual* or Chapter 1 of the *HSM 8000 Host Command Reference Manual*.

>> Appendix E – Keyblock LMKs

Information about Keyblock LMKs can be found in Chapter 5 of the *payShield 9000 General Information Manual* or Appendix F of the *HSM 8000 Console reference Manual*.

>> Appendix F – Knoppix "Cheat Codes"

The HSM Manager software includes the Knoppix operating system (an implementation of Linux). Certain types of PC hardware may display issues when booting from Knoppix – for example:

- the screen goes blank
- a kernel panic message is displayed
- the screen flickers
- the user is dropped into a minimal shell
- Knoppix freezes while booting.

These can often be resolved by using one or more "Cheat Codes" when starting up HSM Manager.

When booting from the HSM Manager CD, the first page that is displayed is a Knoppix title page ending with a "*boot:*" prompt. If no input is made for 10 seconds, the boot process will continue automatically. This boot prompt allows one or more "Cheat Codes" to be entered to modify how the hardware boots up. Different Cheat Codes will be needed for different hardware types – most hardware will not require the use of any Cheat Codes at all.

Structure of the Cheat Code Command Line

At the "*boot:*" prompt, a single command line can be entered, beginning with the word "*knoppix*" followed by one or more Cheat Codes separated with spaces. Some Cheat Codes require parameters.

The full set of Cheat Codes is described on the Knoppix web site: at the time of writing, the appropriate URL is http://knoppix.net/wiki/Cheat_Codes .

The notes below describe some specific Cheat Code command lines which have resolved issues with running HSM Manager on particular hardware types.

Cheat Codes relevant to HSM Manager

If difficulties are encountered when trying to boot from the HSM Manager CD, the following command lines should be tried in the order specified below.

```
boot: knoppix  vga=0
boot: knoppix  acpi=off  pnpbios=off  noapic  noapm
boot: knoppix  vga=0  debug  -b  3
```

This command line is useful for laptop hardware. It causes the boot process to stop at various stages in the boot process: the response "**exit**" should be entered at each prompt to move to the next stage. (Press **Ctrl-D** when asked for the root password for maintenance.) At the end of the process there will be the message

"INIT: Entering runlevel: 3"

followed by a prompt: you should enter "**`init 5`**" at this stage, after which the boot sequence will continue to completion.

>> Glossary

The Glossary can be found in Appendix G of the payShield 9000 General Information Manual.

>> General Abbreviations

The General Abbreviations can be found in Appendix H of the payShield 9000 General Information Manual.

Americas

THALES e-SECURITY
900 South Pine Island Road
Suite 710
Plantation
Florida
33324. USA

T: +1 888 744 4976
or +1 954 888 6200

F: +1 954 888 6211

E: sales@thalesesec.com

Asia Pacific

THALES TRANSPORT & SECURITY (HONG KONG) LTD.
Sunlight Tower
Unit 4101, 41/F
248 Queen's Road East
Wanchai
Hong Kong, PRC

T: +852 2815 8633

F: +852 2815 8141

E: asia.sales@thales-esecurity.com

Europe, Middle East, Africa

THALES e-SECURITY
Meadow View House
Long Crendon
Aylesbury
Buckinghamshire
HP18 9EQ. UK

T: +44 (0)1844 201800

F: +44 (0)1844 208550

E: emea.sales@thales-esecurity.com

THALES