

payShield® 10K

Installation and User Guide

007-001512-021



Date: November 2024

Rev: A1

Doc. Number: 007-001512-021

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Copyright © 2018-2024 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Follow this link to find the End User Licensing Agreement: <https://cpl.thalesgroup.com/legal>

Contents

1 Introduction	1-1
1.1 Documentation Overview	1-1
1.2 Audience	1-1
1.3 payShield 10K General Description	1-1
1.4 Typical Configuration.....	1-2
1.4.1 Command Flow	1-3
1.5 Smart Cards	1-4
1.6 Customer Trust Authority (CTA)	1-5
1.6.1 Customer Security Domain	1-5
1.7 Keys	1-6
1.7.1 Encryption Mechanism.....	1-6
1.7.2 HSM Recovery Key	1-6
1.7.3 Local Master Keys (LMKs).....	1-6
1.7.3.1 Multiple LMKs	1-7
1.7.4 Zone Master Key	1-7
1.7.4.1 Zone PIN Key	1-7
1.7.5 Terminal Master Key	1-7
1.7.5.1 Terminal PIN Key	1-8
1.7.6 Terminal Authentication Key	1-8
1.7.7 Terminal Encryption Key	1-8
1.7.8 PIN Verification Key	1-8
1.7.9 Card Verification Key	1-8
1.7.10 Master Session Key	1-9
1.8 Key Shares	1-9
1.9 Host Commands supporting multiple LMKs	1-9
1.9.1 LMK Usage in Host Commands.....	1-10
1.10 payShield 10K license packages.....	1-11
1.11 Trusted Management Device (TMD).....	1-12
1.11.1 Introduction.....	1-12
1.11.2 Background	1-12
1.11.3 Description	1-13
1.11.4 How Keys Are Shared With payShield and 3rd Parties	1-13
1.11.5 Example Sequence of Steps to Set-Up and Transfer Keys	1-14
2 Backwards Compatibility and Differences.....	2-17
2.1 payShield 9000 / payShield 10K.....	2-17
2.1.1 Host Interface and Commands.....	2-17
2.1.2 Options for Managing payShield 10K.....	2-17
2.1.3 Modifications made to the console commands	2-18
2.1.4 Feature Comparison.....	2-19
2.1.5 Front Panel.....	2-21
2.1.6 Front Panel LEDs	2-21
2.1.7 Front Panel Key Lock Positions	2-21
2.1.8 Rear Panel	2-22
2.1.9 Enhanced Security Features	2-22
2.1.10 Diagnostics.....	2-23
2.1.11 Monitoring.....	2-23
2.1.12 Transitioning Smart Cards	2-23
2.1.12.1 Transitioning legacy Manager Smart Cards	2-24

2.1.12.2 Transitioning non-supported legacy HSM Smart Cards	2-24
2.1.12.3 Copying a card at the console	2-25
2.1.13 User Documentation	2-25
3 Physical Description	3-27
3.1 Front panel	3-27
3.1.1 Key locks and keys	3-27
3.1.1.1 Changing the HSM state via the key locks	3-27
3.1.2 Smart Card Reader	3-28
3.1.3 Front panel LEDs	3-28
3.1.3.1 Health LED	3-29
3.1.3.2 Service LED	3-29
3.1.3.3 Tamper LED	3-30
3.1.3.4 Boot-up LED Sequence	3-30
3.1.3.5 Blue LED	3-30
3.1.4 Air Inlets	3-30
3.2 Rear panel	3-31
3.2.1 AC/DC power supplies	3-31
3.2.1.1 Overview	3-31
3.2.1.2 Alternative Power Supply - Power Supply Type 2	3-32
3.2.1.3 Power Supply LED Status	3-33
3.2.1.4 Swapping out the Power Supply	3-33
3.2.2 Fan trays	3-34
3.2.3 Battery	3-34
3.2.4 AC Power on/off switch	3-35
3.2.5 PCIe card interface	3-35
3.2.6 Ethernet ports	3-35
3.2.7 USB Type A port	3-35
3.2.8 Erase Button and LED	3-36
3.2.8.1 Erase procedure	3-36
3.2.9 Ground Lug	3-37
4 Installation	4-39
4.1 Pre-installation tasks	4-39
4.1.1 Mechanical and Electrical Specifications	4-39
4.1.1.1 Physical Characteristics	4-39
4.1.1.2 Power Considerations	4-39
4.1.1.3 Environmental Considerations	4-40
4.1.1.4 Battery consideration	4-40
4.2 Installation Procedure	4-40
5 payShield PS10-D: 10G Ethernet Hardware Platform Variant	5-45
5.1 Introduction	5-45
5.2 Rear Panel Overview	5-46
5.3 General Notes	5-46
5.4 Installing 10Gb ports	5-46
5.5 Power Consumption	5-47
6 payShield 10K FICON Platform Variant	6-49
6.1 Introduction	6-49
6.2 Installing the payShield 10K PS10-F	6-49
6.2.1 Device overview	6-50
6.2.2 Assure safety	6-50
6.2.3 Unpack	6-50

6.2.3.1	Gather additional equipment	6-51
6.2.4	Insert the SFP	6-52
6.2.5	Determine the location for the payShield 10K	6-53
6.2.6	Mount the rack	6-54
6.2.7	Lock the unit into the rack	6-55
6.2.8	Connect cables and power on	6-55
6.2.9	Configuring the payShield 10K	6-57
6.2.10	Connect the console terminal	6-57
6.2.11	Connect cables for payShield Manager	6-58
6.2.12	Configure payShield Manager	6-58
6.2.13	Configure the Host ports	6-58
6.2.13.1	Configure the FICON Interface	6-58
6.2.14	Test connections	6-60
6.2.15	Basic Installation Troubleshooting	6-60
6.3	Replacing the Transceivers	6-61
6.3.1	FICON Diagnostic Test	6-62
6.4	Device Emulation	6-62
6.5	Performance	6-62
6.5.1	Overview	6-62
6.5.2	Test examples	6-63
6.6	Security Resource Manager (SRM)	6-63
6.7	Z Series I/O Configuration for FICON-attached payShield 10K	6-64
6.7.1	Relationship between the HSM Configuration and the I/O Definition	6-64
6.7.2	Relationship between the I/O Definition and Application	6-65
6.7.3	Relationship between the I/O Definition and the SRM Configuration	6-65
7	payShield Management Options	7-67
8	Commission using payShield Manager	8-69
8.1	Introduction	8-69
8.2	Prerequisites	8-69
8.3	Preparing for Commissioning	8-70
8.3.1	Configuring payShield 10K for Static IP (if required)	8-70
8.3.2	Install Smart Card Reader Driver	8-70
8.3.3	Check the Proxy Configuration	8-70
8.3.4	Configure DNS	8-70
8.3.5	Connect to the Network	8-71
8.4	Connecting, Installing Browser Extensions, Configuring Smart Card Reader	8-72
8.4.1	Connecting to payShield 10K	8-72
8.4.2	Installing Thales Browser Extensions	8-73
8.4.3	Configure the Smart Card reader	8-77
8.5	Commissioning payShield 10K	8-78
8.5.1	Open the Commissioning Wizard page	8-79
8.5.2	Create a new Security Domain	8-80
8.5.3	Load the Security Domain	8-85
8.5.4	Set HSM Recovery Key (HRK) passphrases	8-90
8.5.5	Create Left and Right Remote Access Control key cards	8-91
8.5.6	Adding Additional Warranted HSMs to the Security Domain	8-96
8.6	Using payShield Manager with MacOS Catalina	8-96
8.7	Configuring the Ports and the Host Interface	8-100
8.7.1	Management Port	8-100
8.7.2	Host Ethernet Ports	8-100
8.7.3	Host FICON Ports	8-101
8.7.4	Host Printer Ports	8-101
8.7.5	Configure the Software	8-102

9 Using payShield Manager.....	9-103
9.1 Introduction to payShield Manager.....	9-103
9.2 Logging into payShield Manager	9-103
9.3 Top Tab descriptions	9-106
9.3.1 Summary Tab	9-106
9.3.2 Status Tab	9-107
9.3.3 Operational Tab.....	9-108
9.3.4 Domain Tab	9-109
9.3.4.1 payShield Security Group.....	9-110
9.3.4.2 Security Domain	9-111
9.3.5 Configuration Tab	9-112
9.4 Virtual Console Tab	9-114
9.4.1 Quick Links	9-114
9.4.2 Terminate Session.....	9-115
9.5 Lower screen icons.....	9-115
9.5.1 payShield 10K States	9-115
9.5.1.1 Online	9-116
9.5.1.2 Offline	9-116
9.5.1.3 Secure	9-116
9.5.1.4 Switching to Online or Offline State.....	9-116
9.5.1.5 Switching to Secure State.....	9-116
9.5.2 Time Remaining.....	9-116
9.5.3 Information.....	9-117
9.5.4 User	9-117
9.5.5 Status.....	9-118
9.5.6 Smart Card Operations	9-118
9.5.7 User Login/Logout	9-118
9.5.7.1 Login Additional Users	9-118
9.5.7.2 User Logout	9-119
9.6 Summary Page.....	9-119
9.6.1 Summary Dashboard.....	9-120
9.6.2 Health Dashboard	9-120
9.6.2.1 How to resolve reported errors	9-120
9.6.3 Configuration Dashboard.....	9-123
9.6.4 Local Master Key.....	9-124
9.7 Status page.....	9-124
9.7.1 Device Information.....	9-125
9.7.2 Utilization Statistics	9-126
9.7.3 Health Statistics/Diagnostics	9-130
9.7.3.1 HealthStats	9-131
9.7.3.2 Diagnostics	9-132
9.7.3.3 Maintenance	9-134
9.7.4 Error Log	9-135
9.7.5 Audit Log	9-136
9.7.6 Software Info	9-138
9.7.6.1 Software - how to update software	9-138
9.7.7 FIPS/Licensing.....	9-140
9.7.7.1 License Summary - how to update Licensing	9-140
9.7.7.2 Installed Licenses	9-142
9.7.7.3 NIST Validated Algorithms	9-143
9.8 Operational	9-144
9.8.1 Local Master Keys	9-144
9.8.1.1 Generate LMK - create trusted officer	9-145
9.8.1.2 Verify an LMK Card	9-153

9.8.1.3 Create an Authorizing Card	9-154
9.8.1.4 Duplicate an LMK Card	9-154
9.8.1.5 Generate an LMK	9-155
9.8.1.6 Install an LMK from RLMK Card Set	9-155
9.8.1.7 Delete an Installed LMK	9-156
9.8.1.8 Replace an installed LMK	9-156
9.8.1.9 Set the Default LMK	9-157
9.8.1.10 Set the Management LMK	9-157
9.8.1.11 Enter Authorized State	9-157
9.8.1.12 Single Authorization Mode	9-158
9.8.1.13 Multiple Authorization Mode	9-158
9.8.1.14 Configuring Authorized Activities	9-159
9.8.1.15 Key Change Storage	9-161
9.8.1.16 Install LMK from RLMK card set	9-162
9.8.1.17 Delete an installed LMK	9-162
9.8.1.18 Replace an Old LMK	9-162
9.9 Domain	9-163
9.9.1 payShield Security Group	9-163
9.9.2 Security Domain	9-164
9.9.2.1 Commission a Smart Card	9-165
9.9.2.2 Decommission a Card	9-168
9.9.2.3 Copy a Domain Card	9-168
9.9.2.4 Create a New Security Domain	9-168
9.9.2.5 HRK Operations	9-168
9.10 Configuration Tab	9-170
9.10.1 Host Settings	9-171
9.10.1.1 Host Message Header Length:	9-171
9.10.1.2 Active Host Interface	9-171
9.10.1.3 Ethernet	9-172
9.10.1.4 IP	9-173
9.10.1.5 Access Control List (ACL)	9-174
9.10.1.6 TCP/UDP	9-175
9.10.1.7 TLS tab	9-177
9.10.2 Printer Settings	9-189
9.10.3 Security Settings	9-190
9.10.3.1 General Tab	9-190
9.10.3.2 Initial Tab	9-192
9.10.3.3 Security Parameter Descriptions	9-193
9.10.4 Management Settings	9-193
9.10.4.1 Management - Interface	9-193
9.10.4.2 Management - Timeouts	9-194
9.10.4.3 Management - TLS Certificate	9-195
9.10.5 Auxiliary Settings	9-197
9.10.6 General Settings	9-198
9.10.6.1 PIN Blocks	9-198
9.10.6.2 Alarms	9-199
9.10.6.3 Fraud	9-200
9.10.6.4 Date and Time	9-201
9.10.6.5 Remote Syslog	9-208
9.10.6.6 Miscellaneous	9-212
9.10.7 Configure Commands	9-212
9.10.8 Audit Settings	9-214
9.10.8.1 Audit - General	9-215
9.10.8.2 Audit - Console Commands	9-216
9.10.8.3 Audit - Host Commands	9-217

9.10.8.4 Audit - Management Commands	9-218
9.10.9 SNMP Settings	9-218
9.10.10 Load/Save Settings	9-220
9.10.11 payShield TMD - Manage MZMK	9-223
9.10.11.1 Initiate Manage MZMK	9-224
9.10.11.2 Display Fingerprint of the Public Key	9-226
9.10.11.3 Create Master Zone Master Key (MZMK).....	9-227
9.10.11.4 MZMK Information	9-229
9.10.11.5 Export Data.....	9-230
9.11 Settings per LMK	9-231
9.11.1 Overview	9-231
9.11.2 Enable the feature	9-231
9.11.3 Assigning Security Settings per LMK ID	9-233
9.11.4 Enabling Host Commands for Each LMK ID	9-236
9.11.5 Assigning PIN Blocks to LMKs.....	9-236
10 Migrating LMKs	10-239
10.1 Introduction	10-239
10.2 Multiple LMKs	10-239
10.3 Overview of the process	10-239
10.4 Generating new LMK component Smart Cards	10-240
10.4.1 Types of LMK component cards	10-241
10.5 Formatting LMK Smart Cards	10-241
10.5.1 HSM LMK Cards	10-241
10.5.2 payShield Manager LMK Cards.....	10-241
10.6 Generating LMK Component Cards	10-241
10.6.1 HSM LMK Cards	10-241
10.6.2 payShield Manager RLMK Cards	10-242
10.7 Creating Copies of LMK Component Cards	10-242
10.7.1 Duplicating HSM LMK cards	10-242
10.7.2 Duplicating a payShield Manager RLMK card	10-242
10.8 Loading the new LMK	10-242
10.8.1 Using the Console	10-243
10.8.1.1 Loading (or forming) the LMK.....	10-243
10.8.1.2 Checking the LMK	10-243
10.8.2 Using payShield Manager	10-243
10.8.2.1 Installing the LMK.....	10-243
10.8.2.2 Checking the LMK	10-243
10.9 Loading the old LMK.....	10-244
10.9.1 Using the Console	10-244
10.9.2 Using payShield Manager	10-244
10.10 Migrating keys between Variant LMKs	10-244
10.10.1 BW Host command	10-245
10.10.2 BX Response to the Host	10-248
10.11 Migrating keys from Variant to Key Block LMKs	10-249
10.11.1 BW Host command	10-249
10.11.2 BX Response to the Host	10-251
10.12 Migrating keys between Key Block LMKs	10-251
10.12.1 BW Host command	10-251
10.12.2 BX Response to the Host	10-252
10.13 Migrating keys from Key Block to Variant LMKs	10-253
10.14 Migrating keys for PCI HSM compliance	10-253
10.15 Re-encrypting PINs	10-253
10.15.1 BG Host Command	10-254

10.15.2 BH Response	10-254
10.16 Re-encrypting decimalization tables	10-255
10.17 Switching to the new LMK	10-256
10.18 Taking advantage of Multiple LMKs	10-257
10.19 Clean-up after migration to a new LMK.	10-258
10.19.1 Deleting the Old LMK from Key Change Storage.	10-258
10.19.1.1 Using the console	10-258
10.19.1.2 Using payShield Manager.	10-258
10.19.1.3 Using a Host Command	10-259
11 TLS Certificate Management.	11-261
11.1 Introduction	11-261
11.2 General Description.	11-261
11.2.1 What TLS Provides	11-261
11.2.2 How TLS Works	11-261
11.3 TLS for Host Connections on payShield 10K	11-263
11.3.1 TLS Support for Host Connections.	11-263
11.3.2 Host TLS Certificates	11-263
11.3.3 Client Certificates	11-264
11.3.4 Managing Host TLS Keys and Certificates.	11-264
11.3.4.1 Overview	11-264
11.3.4.2 Host TLS Key Stores.	11-265
11.3.4.3 Using payShield Manager	11-266
11.3.4.4 Using the Console.	11-267
11.3.4.5 Use Cases.	11-269
11.3.5 TLS for Host Connections - General Information	11-270
11.3.5.1 Supported Cipher Suites	11-270
11.3.5.2 Cipher Suite Negotiation	11-270
11.3.5.3 Out-of-Date Certificates.	11-270
11.3.5.4 Performance Considerations.	11-271
11.3.5.5 Security Considerations	11-271
11.3.5.6 Port Setting	11-271
11.3.5.7 OpenSSL Configuration File	11-271
11.3.5.8 Working with IBM z/OS Mainframes	11-272
11.3.5.9 FICON Interface	11-272
11.4 TLS for payShield Manager.	11-272
11.4.1 Overview	11-272
11.4.2 Managing payShield Manager TLS Keys and Certificates	11-273
11.4.2.1 Overview	11-273
11.4.2.2 Management TLS Key Store	11-273
11.4.2.3 Management TLS - Initial Configuration	11-273
11.4.2.4 Changing the payShield Manager TLS Keys and Certificates	11-274
11.4.2.5 Exporting the Chain of Trust and Viewing and Deleting Certificates.	11-275
11.5 General Information for TLS for payShield 10K	11-276
11.5.1 HSM Recovery Key (HRK).	11-276
11.5.2 Upgrading and Downgrading Software	11-276
11.5.3 Support for USB Memory Devices	11-276
11.5.4 Import Certificate	11-277
11.5.4.1 General Information.	11-277
11.5.4.2 TLS Management	11-277
11.5.4.3 TLS Management via the Virtual Console.	11-279
11.5.4.4 Secure Host Communications.	11-279
12 Fraud Detection Functions	12-281

13 Utilization Data	13-283
13.1 Data Provided to the User	13-283
13.2 Data Collection Period	13-283
13.3 Interpreting the Output	13-284
13.3.1 Overall HSM Loading	13-284
13.3.1.1 Output using the Console	13-285
13.3.1.2 Output using payShield Manager	13-287
13.3.2 Host command Volumes	13-287
13.3.2.1 Output using the Console	13-288
13.3.2.2 Output using payShield Manager	13-288
13.3.4 Reporting Mechanisms	13-288
13.5 Console Commands	13-289
13.6 payShield Manager Commands	13-289
13.7 Host commands	13-290
13.8 Managing Utilization Data	13-290
14 Health Check Data	14-291
14.1 Data Provided to the User	14-291
14.1.1 Accumulated Counts	14-291
14.1.1.1 Output using the Console	14-292
14.1.1.2 Output using payShield Manager	14-292
14.1.2 Instantaneous Status	14-293
14.1.2.1 Output using the Console	14-294
14.1.2.2 Output using payShield Manager	14-294
14.1.4 Reporting Mechanisms	14-294
14.3 Console Commands	14-295
14.4 payShield Manager Commands	14-295
14.5 Host commands	14-295
15 Audit Log	15-297
15.1 Introduction	15-297
15.2 Overview	15-297
15.3 Correct Use of the Audit Log	15-297
15.4 Forcibly recorded items	15-298
15.4.1 PCI HSM Compliance	15-298
15.5 Recording Deletion in Audit Log	15-299
15.6 Discretionary Audit Log entries	15-299
15.7 Audit Log Protection	15-300
15.8 Configuring the Audit Log	15-300
15.8.1 AUDITOOPTIONS Console command	15-300
15.8.2 payShield Manager Auditing screen	15-300
15.9 Viewing the Audit Log	15-302
15.9.1 AUDITLOG Console command	15-302
15.10 payShield Manager Audit Log Screen	15-303
15.11 Printing the Audit Log	15-304
15.11.1 AUDITPRINT Console command / Q2 Host command	15-304
15.11.2 Audit Record Format	15-305
15.11.3 Q4 Host command	15-311
15.11.3 payShield Manager Audit Log Screen	15-311
15.12 Retrieving Audit Log entries to the host system	15-312
15.12.1 Q2 Host command	15-312
15.12.2 SNMP	15-312
15.12.3 payShield Monitor	15-312
15.13 Deleting records from the Audit Log	15-312

15.13.1 CLEARAUDIT Console command	15-312
15.13.2 payShield Manager Audit Log Screen	15-313
15.13.3 Q6 Host command	15-313
15.14 Other Audit Log Management Functions.	15-313
15.14.1 Translating MAC on LMK Refresh	15-313
15.14.2 Verifying an Audit Log Record	15-313
16 Performance	16-315
16.1 Overview	16-315
16.2 Performance Ratings 25 cps to 2500 cps	16-315
16.3 Performance Rating 10,000 cps	16-315
16.4 Achieving Maximum Performance.	16-316
16.5 Host Commands Excluded from Performance Ratings.	16-316
17 Network Time Protocol (NTP)	17-317
17.1 Overview	17-317
17.2 Server Status Terminology	17-318
17.3 Authentication Status Terminology	17-319
18 SNMP	18-321
18.1 Introduction	18-321
18.1.1 Security Guidelines for SNMP Configuration	18-321
18.2 Network Connectivity.	18-321
18.3 SNMP Version.	18-322
18.4 Configuring Traps	18-322
18.5 Information Provided by the payShield 10K through SNMP	18-322
18.5.1 Traps Issued by the payShield 10K	18-323
18.5.2 Tamper.	18-323
18.5.3 Powering Up.	18-323
18.5.4 Use of the Erase Button	18-323
18.5.5 Fraud Detection	18-323
18.5.6 Installation of a New License	18-323
18.5.7 Installation of New Software	18-324
18.5.8 Power Supply Unit (PSU) Failure.	18-324
18.5.9 Abnormal Fan Speed	18-324
18.5.10 New Error Log Entry.	18-324
18.5.11 Invalid or Unexpected Data Received at a Host Port.	18-324
18.5.12 Actual or Impending Battery Problem.	18-324
18.5.13 Security Settings	18-325
19 Remote Syslog	19-327
19.1 Summary	19-327
19.2 Secure Operation	19-327
19.3 Configuration.	19-327
19.4 Operation.	19-328
Appendix A - Console Commands	20-329
Appendix B - Error Log Codes.	21-331
B.1 General.	21-331
B.2 Description	21-331
B.3 Severity.	21-331
B.4 Error Codes.	21-332
B.5 Sub-Codes	21-332
B 5.1 Sub-Codes for Main Error Code = 1 (Utility System Errors)	21-333

B 5.2 Sub-Codes for Main Error Code = 2 (Cryptographic System Errors)	21-334
B 5.3 Sub-Codes for Main Error Code = 3 (Application System Errors).....	21-335
B 5.4 Sub-Codes for Main Error Code = 4 (Key Manager System Errors).....	21-336
B 5.5 Sub-Codes for Main Error Code = 5 (Encrypted File System Errors).....	21-336
B.6 Multiple Entries.....	21-336
Appendix C - Commission payShield Manager using Console commands . .	22-339
C.1 Background information	22-339
C.2 Prerequisites	22-339
C.3 Procedure.....	22-340
C3.1 Secure the HSM.....	22-340
C3.2 Generate a Customer Trust Authority	22-340
C3.3 Create the HRK passphrases	22-342
C3.4 Commission the HSM	22-343
C3.5 Commission Smart Cards	22-345
C3.6 Migrate LMK Cards to become RLMK Cards.....	22-345
Appendix D - Audit Log Messages.....	23-347
Appendix E - SNMP MIB Security Settings	24-353

Revision Status

Part Number	Revision	Date	Changes
PUGD0535-001	001	March 2019	Initial Issue
PUGD0535-002	002	December 2019	Editorial updates Addition of FF1 License Correction in Section 2.1.4, Feature Comparison
PUGD0535-003	003	January 2020	Editorial updates
PUGD0535-004	004	March 2020	FF1 license (Section 1.10, “payShield 10K license packages”, on page 11) payShield Monitor updated VR command updated payShield Monitor dashboard updated (Section 9.6.1, “Summary Dashboard”, on page 120) payShield Monitor Summary License updated (Section 9.7.7.1, “License Summary - how to update Licensing”, on page 140) payShield Monitor Software tab modified (Section 9.7.6.1, “Software - how to update software”, on page 138)
PUGD0535-004	004a	April 2020	Minor editorial changes
PUGD0535-005	005	October 202000	payShield 10K 10G Ethernet Hardware Platform Variant support documented in Chapter 5, “payShield PS10-D: 10G Ethernet Hardware Platform Variant” . Links to Chapter 5 added to: Chapter 1, “Introduction” , Chapter 2, “Backwards Compatibility and Differences” , Chapter 3, “Physical Description” , Chapter 4, “Installation”
PUGD0535-006	006	January 2021	Editorial updates Trusted Management Device update (Section 1.11, “Trusted Management Device (TMD)”, on page 12)
PUGD0535-007	007	March 2021	FICON chapter added: Chapter 6, “payShield 10K FICON Platform Variant” Links to Chapter 6 added to: Chapter 1, “Introduction” , Chapter 2, “Backwards Compatibility and Differences” , Chapter 3, “Physical Description” , Chapter 4, “Installation” Console Commands moved to a stand-alone manual: “Console Guide” Error Log limit increased to 10,000 entries (Section 2.1.10, “Diagnostics”, on page 23.)
PUGD0535-008	008	May 2021	Updates to Section 9.10.6.2, “Alarms”, on page 199
PUGD0535-009	009	June 2021	Console Command Section moved to a stand-alone document. See Console Guide . Description of Temperature Alarm moved to payShield 10K Security Manual Updated Security Settings
PUGD0535-010	010	September 2021	Updated to include new Sections: Chapter 12, “Fraud Detection Functions” Chapter 13, “Utilization Data” Chapter 14, “Health Check Data” Chapter 15, “Audit Log”

Part Number	Revision	Date	Changes
PUGD0535-011	011	November 2021	<p>payShield Manager updated to accommodate Thales Trusted Management Device (TMD). See: Chapter 8, “Commission using payShield Manager”</p> <p>Updated to include new topics: Tamper Protection, Information for Security Auditors and Compliance Chapter 16, “Performance”</p> <p>Link to Audit Record Format Section 15.11.1.1, “Audit Record Format”, on page 305</p>
007-001512-005	005	February 2022	<p>New document number</p> <p>Smart Card update</p> <p>Editorial update to Sections: Section 9.10.11, “payShield TMD - Manage MZMK”, on page 223</p> <p>Section 9.10.11.5, “Export Data”, on page 230</p> <p>Updated to include: Appendix C Error Log Codes</p> <p>Updated to remove “Tamper Protection” as this topic is covered in the payShield 10K Security Manual</p> <p>See the payShield 10K Security Manual for Security Auditor Information. (Topic deleted from this manual.)</p>
007-001512-006	006	June 2022	Version 1.6a document number
007-001512-006	006 Rev B	July 2022	<p>Section 9.10.11, “payShield TMD - Manage MZMK”, on page 223 updated to include Security Setting Notice (“Enable multiple authorized activities” set to YES)</p>
007-001512-007	007	November 2022	<p>Updated to note new licenses (PS10-PRM-Y and PS10U-PRM-X2Y / 10,000 cps):</p> <p>Section 1.10, “payShield 10K license packages”, on page 11</p> <p>Section 2.1.4, “Feature Comparison”, on page 19</p> <p>Chapter 16, “Performance” page 315</p> <p>Updated to include Power Supply Type 2: Section 3.2.1, “AC/DC power supplies”, on page 31</p>
007-001512-007	007 Rev B	January 2023	<p>Updates to the following sections to direct readers to the payShield 10K Security Manual for the list of supported Cipher Suites:</p> <p>Section 11.3.5.1, “Supported Cipher Suites”, on page 270 and Section 11.3.5.2, “Cipher Suite Negotiation”, on page 270</p> <p>Updates to the following sections to reflect Microsoft Edge:</p> <p>Section 8.3.3, “Check the Proxy Configuration”, on page 70</p> <p>Appendix B, “Prerequisites”, page 339</p>
007-001512-008	008 Beta	January 2023	<p>Updates to the following sections to reflect the number of TLS sessions increased to 256 per host (total 512 for the two host ports):</p> <p>Section 3.2.6, “Ethernet ports”, on page 35</p> <p>Section 9.10.1.6, “TCP/UDP”, on page 175</p>

Part Number	Revision	Date	Changes
007-001512-008	008	May 2023	<p>Clarification added to Appendix A Console Commands to refer users to the payShield 10K Console Guide for a complete discussion of console commands.</p> <p>Update to the following section to reflect the Thales IDBridge CT700 Smart Card Reader with PIN Pad as the recommended reader: Section 8.3.2, "Install Smart Card Reader Driver", on page 70</p> <p>New section added, Section 8.7, "Configuring the Ports and the Host Interface", on page 100.</p> <p>Update to Section 15.11.1.1, "Audit Record Format", on page 305, Field 4, Command Code Type.</p> <p>Update to Section 2.1.4, "Feature Comparison", on page 19 to reflect:</p> <ul style="list-style-type: none"> PS10-S 60 W max PS10-D 70 W max (with 4 x optical transceivers); 80 W max (with 4 x copper transceivers) PS10-F (with 1 x FICON transceiver) 80 W max <p>Update to Section 5.5, "Power Consumption", on page 47</p>
007-001512-009	009	September 2023	Updates for NTP: Section 9.10.6.4, "Date and Time", on page 201 and addition of new chapter: Chapter 17, "Network Time Protocol (NTP)"
007-001512-020	020 Beta	March 2024	<p>Update to Section 9.11, "Settings per LMK", on page 231</p> <p>Update to include Section 9.10.6.5, "Remote Syslog", on page 208</p> <p>Editorial updates to Chapter 9, "Using payShield Manager"</p>
007-001512-020	020 Rev B1	August 2024	Update to Section 9.10.6.5, "Remote Syslog", on page 208 to include steps to delete a remote syslog server.
007-001512-020	020 Rev C1	September 2024	Version 2.0c Rev C1 document number
007-001512-021	021 Rev A1	November 2024	<p>Update to Section 9.10.10, "Load/Save Settings", on page 220 to provide additional information</p> <p>Editorial and technical information updates to Chapter 9, "Using payShield Manager", e.g., updated section numbers, updated TLS management content, etc.</p> <p>New chapters and appendix added:</p> <ul style="list-style-type: none"> - Chapter 18, "SNMP" - Chapter 19, "Remote Syslog" - Appendix E, SNMP MIB Security Settings

1 Introduction

1.1 Documentation Overview

Documentation for the payShield 10K Hardware Security Module (HSM) is streamlined into the following manuals:

- payShield 10K Installation and User Guide
- payShield 10K Security Manual
- payShield 10K Host Programmer's Manual
- payShield 10K Applications Using payShield 10K
- payShield 10K Core Host Commands Manual
- payShield 10K Legacy Command Reference Manual
- payShield 10K Console Guide
- payShield 10K Host Command Examples
- payShield 10K Regulatory Users Warnings and Cautions

1.2 Audience

The manual's audience includes:

- Network installers
- Trusted officers/data security administrators
 - Physical key holders
 - Physical card holders
 - Compliance officers

1.3 payShield 10K General Description



The payShield 10K payment hardware security module (HSM) provides cryptographic functions to support network and point-to-point data security. The payShield 10K acts a peripheral device to a Host computer. It 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 secured by physical locks, electronic switches and tamper-detection circuits. It supports a large number of standard commands and can be customized to perform client-specific cryptographic commands.

Standard command functions include:

- Generating and verifying PINs, such as those used with bank accounts and credit cards
- PIN solicitation, to obtain a new PIN from a card holder (against a reference number)
- Generating encrypted card values, such as Card Verification Values (CVV) for the plastic card industry
- 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

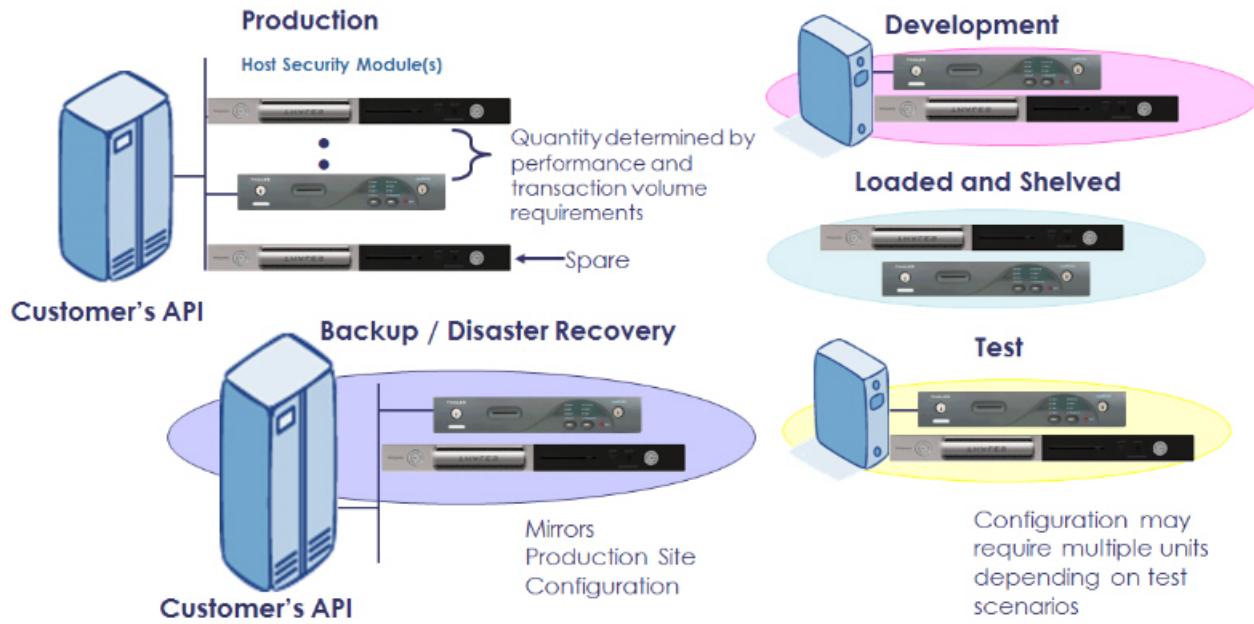
1.4 Typical Configuration

A typical payShield 10K configuration consists of two or more payShield units connected as “live” units. A multi-unit configuration permits concurrent operation for high throughput, and, under control of the application program, provides automatic and immediate backup in the event of a fault in a single unit.

Typically, redundancy is built into the system design by providing more capacity than is required to allow commands to be switched away from a failed or withdrawn unit. Optionally, it is possible to have a backup unit not connected to the Host but ready for connection in place of a faulty unit. This is not the preferred practice because the unit may remain idle for a long time and may itself have developed a fault.

In addition to the “live” units, a typical system contains at least one HSM connected to a test or development computer system. This allows changes in the environment to be tested, without disturbing the live system.

The figure that follows illustrates a deployment architecture that includes both payShield 9000s and payShield 10Ks.



1.4.1 Command Flow

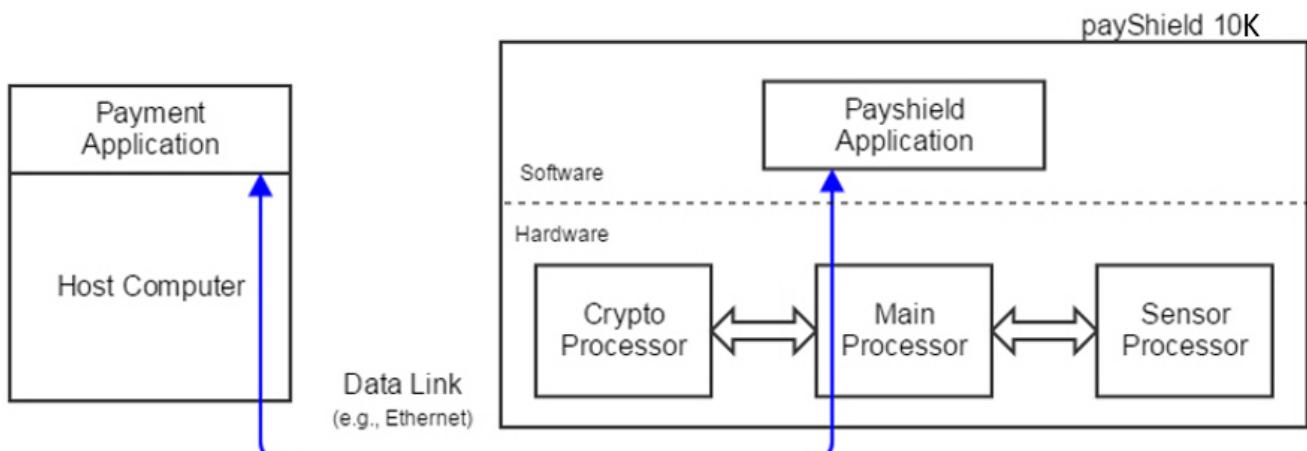
Note: The payShield 10K is normally online to the Host and does not require operator monitoring or intervention.

The HSM processes 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, to the HSM.
- The HSM processes the command messages and generates response messages, which also contain a variable number of fields (depending upon the message type).

Note: Some commands, mainly involving plain text data, are entered by the user via the associated HSM console.

The flow of data through components is represented in the figure that follows.



The throughput of the HSM depends on the types of commands that are executed, and the method and speed of the Host connection.

1.5 Smart Cards

The payShield 10K uses Smart Cards to provide a convenient means of handling sensitive information.

Smart Cards are used for storing three distinct types of information:

- Key components - particularly the Local Master Key (LMK)
- Authorizing Officer credentials
- HSM alarm, security and Host settings

There are two types of Smart Cards:

- payShield Manager Smart Cards

There are 2 types of payShield Manager Smart Cards.

Note: Both cards function identically; however, the card containing bar code is only for software releases 1.5a and above.

- HSM Smart Cards

There are 2 types of HSM Smart Cards.



The differences between Smart Cards are identified in the following table.

Operations	payShield Manager Smart Card	HSM Smart Card
Formatting	Can only be formatted using payShield Manager	Can only be formatted using the FC command using USB-C console
Save Settings (Alarm, Host, Security, Audit, Command, Pin Block)	Can be used to save payShield 10K settings via payShield Manager and remote card reader only	Can be used to save payShield 10K settings via USB-C console and embedded card reader only
Customer Trust Authority (CTA)	Can be used as CTA cards both on embedded and remote card reader	Cannot be used on an embedded card reader
Local Master Key (LMK)	Can be used as LMK card both on embedded card reader and remote card reader	Can be used as LMK card from embedded card reader only

Note: Follow this link for additional information: [Section 2.1.12, “Transitioning Smart Cards”, on page 23](#).

1.6 Customer Trust Authority (CTA)

Every commissioned HSM or Smart Card contains an Elliptic Curve Digital Signature Algorithm (ECDSA) public/private key pair. In order to have confidence in the authenticity of the various public keys, each such key is held in the form of a certificate.

The certificate is signed by a private key that is also created by the user on an HSM. This root private key is normally described as a Customer Trust Authority (CTA).

The CTA is split across a number of CTA Smart Cards. ([Section 1.8, “Key Shares”, on page 9](#) further explains the split/sharing concept.) The CTA is temporarily loaded into an HSM prior to signing the Smart Card or HSM public key certificates. The corresponding CTA public key (used to verify the certificates) is stored on each Smart Card and in the HSM.

A CTA must be reassembled onto a payShield in order to perform certain operations, including commissioning a payShield. After a CTA has been created, it may be used to commission multiple payShields and numerous Smart Cards to be used in the same security domain.

The CTA functionality is standard in all payShield HSMs that support payShield Manager. All user interaction with the CTA functionality is via either the console interface or payShield Manager.

1.6.1 Customer Security Domain

The term “customer security domain” is used to describe the set of Smart Cards and HSMs, such that (secure) remote communication between the cards and the HSM in the group is permitted.

A necessary condition for a Smart Card and an HSM to communicate is that their public keys are both signed by the same CTA. However, this is not a sufficient condition, and it is quite possible to have non-overlapping security groups created via the same CTA.

In addition to having matching CTAs, whitelists within each HSM define which Smart Cards can communicate with a specific HSM and what role they possess.

1.7 Keys

1.7.1 Encryption Mechanism

The HSM mechanism for encryption of locally stored keys uses a double length DES key, i.e., the Local Master Key (LMK), stored in the tamper-resistant memory of the HSM. All other cryptographic keys are encrypted under the LMK and stored external to the HSM, usually in a key database on the Host system that is accessible by Host applications. In order to provide key separation (e.g., key encryption keys, MAC keys, PIN verification keys, etc.), different key types are encrypted under different variants of the LMK. Hence, if the “wrong” key is provided in a command, either accidentally or deliberately, a key parity error occurs (highly likely) or a processing error occurs (occasionally).

1.7.2 HSM Recovery Key

One concern relating to the HSMs used in the remote management solution is that if an HSM becomes “tampered”, the public and private keys are removed from memory and it becomes necessary to generate a new key pair. This could involve a considerable operational inconvenience.

Therefore, a recovery mechanism involving an AES HSM Recovery Key (HRK) is available to simplify the task of restoring a public/private key pair to the HSM’s secure memory and re-establishing the previous security group.

1.7.3 Local Master Keys (LMKs)

Each payShield 10K has its own master key. This key is known as the “Local Master Key”. Every generated key is then encrypted under this Local Master Key.

The LMK is used to protect (by encryption) all of the operational keys plus some additional sensitive data that are processed by the HSM.

The payShield 10K can support multiple LMKs, such that up to 20 LMKs, of different types, can be in use at any one time. Each LMK can be managed by a separate security team. This allows a single payShield 10K to be used for multiple purposes - such as different applications or different clients.

The LMK may be common to a number of HSMs. Storing only a single key in the HSM minimizes recovery and operational downtime, in the event of a problem with the unit.

There are two types of LMKs:

- Variant LMK

A Variant LMK is a set of 40 double- or triple-length DES keys, arranged in pairs, with different pairs (and variants of those pairs) being used to encrypt different types of keys.

Note: The term “Variant LMK” refers to the “variant” method of encrypting keys; a Variant LMK is not itself a variant of any other key.

- Key Block LMK

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

Note: The term “Key Block LMK” refers to the “key block” method of encrypting keys; a Key Block LMK is not itself stored in the key block format.

For an HSM to operate, the LMKs must be created and loaded. Because the DES /AES algorithms depend on a key for secrecy, and because the security of all keys and data encrypted for storage depend on the LMKs, they must be created and maintained in a secure manner. Provision is made to allow the LMKs to be changed and keys or data encrypted under them to be translated to encryption under the new LMKs.

All keys when stored locally (i.e., not in transit between systems) are encrypted under the LMK.

1.7.3.1 Multiple LMKs

The availability of multiple LMKs makes it easier to migrate operational keys from an old LMK to a new one. Such LMK migration should be performed every few years for security purposes, but may also be necessary for operational reasons, e.g., when upgrading from double- to triple-length Variant LMKs or from Variant LMKs to Key Block LMKs.

Although the payShield 10K allows for changing the LMK, it means that all operational keys need to be translated from encryption under the old LMK to encryption under the new LMK before they can be used. A “big bang” approach typically requires very careful planning and coordination, with possible downtime or need for additional HSM capacity. The use of multiple LMKs allows users to adopt a phased approach to LMK change.

It is possible to install multiple LMKs within a single payShield 10K. The precise details of the number and type of installed LMKs are controlled via the payShield 10K's license file.

1.7.4 Zone Master Key

A Zone Master Key (ZMK) is a key-encrypting key which is distributed manually between two (or more) communicating sites, within a shared network, in order that further keys can be exchanged automatically (without the need for manual intervention). The ZMK is used to encrypt keys of a lower level for transmission. For local storage, a ZMK is encrypted under one of the LMK pairs.

Within the VISA environment this is known as a ZCMK.

The payShield 10K supports the use of a single-length, double-length or triple-length DES ZMK, or a 128-bit, 192-bit or 256-bit AES ZMK.

1.7.4.1 Zone PIN Key

A Zone PIN Key (ZPK) is a data encrypting key which is distributed automatically, and is used to encrypt PINs for transfer between communicating parties (for example, between acquirers and issuers). For transmission, a ZPK is encrypted under a ZMK; for local storage it is encrypted under one of the LMK pairs.

The payShield 10K supports the use of a single-length, double-length or triple-length DES ZPK.

1.7.5 Terminal Master Key

A Terminal Master Key (TMK) is a key-encrypting key which is distributed manually, or automatically under a previously installed TMK. It is used to distribute data-encrypting keys, within a local (non-shared) network, to an ATM or POS terminal or similar. The TMK is used to encrypt other TMKs or keys of a lower level for transmission. For local storage, a TMK is encrypted under one of the LMK pairs.

The payShield 10K supports the use of a single-length, double-length or triple-length DES TMK, or a 128-bit, 192-bit or 256-bit AES TMK.

1.7.5.1 Terminal PIN Key

A Terminal PIN Key (TPK) is a data-encrypting key which is used to encrypt PINs for transmission, within a local network, between a terminal and the terminal data acquirer. For transmission, a TPK is encrypted under a TMK; for local storage, it is encrypted under one of the LMK pairs.

The payShield 10K supports the use of a single-length, double-length or triple-length DES TPK.

1.7.6 Terminal Authentication Key

A Terminal Authentication Key (TAK) is a data-encrypting key which is used to generate and verify a Message Authentication Code (MAC) when data is transmitted, within a local network, between a terminal and the terminal data acquirer. For transmission, a TAK is encrypted under a TMK or ZMK; for local storage it is encrypted under one of the LMK pairs.

The payShield 10K supports the use of a single-length, double-length or triple-length DES TAK, or a 128-bit, 192-bit or 256-bit AES TAK.

1.7.7 Terminal Encryption Key

A Terminal Encryption Key (TEK) is a data-encrypting key which is used to encrypt and decrypt messages for transmission, within a local network, between a terminal and the terminal data acquirer. For transmission, a TEK is encrypted under a TMK or ZMK; for local storage it is encrypted under one of the LMK pairs.

The payShield 10K supports the use of a single-length, double-length or triple-length DES TEK, or a 128-bit, 192-bit or 256-bit AES TEK.

1.7.8 PIN Verification Key

A PIN Verification Key (PVK) is a data-encrypting key which is used to generate and verify PIN verification data and thus verify the authenticity of a PIN. For transmission, a PVK is encrypted under a TMK or under a ZMK; for local storage, it is encrypted under one of the LMK pairs.

The payShield 10K supports the use of a single-length, double-length or triple-length DES PVK.

1.7.9 Card Verification Key

A Card Verification Key (CVK) is similar to a PIN Verification Key, but for Card information instead of a PIN.

The payShield supports the use of a single-length, double-length or triple-length DES CVK.

1.7.10 Master Session Key

The master/session key management scheme involves setting up a master key between two communicating parties (for example, an acquirer and an issuer or an acquirer and a terminal) under which data-encrypting keys are exchanged for use during a session. Key installation and updating must be organized by the institutions involved (i.e., within the application programs).

The HSM supports master/session key management in both shared and local networks, but distinguishes between the two and maintains separate key hierarchies.

1.8 Key Shares

Note: The term “Security Administrator” is interchangeable with “Security Officer” and “Administrator”.

By assigning key and policy management to more than one Security Administrator a strong separation of duties over HSM management is enforced. Each Security Administrator is assigned a Smart Card. Each Smart Card has a “key share”. To create a “key”, each “key share” must be presented. With “key sharing”, no one person has complete control over the security of data.

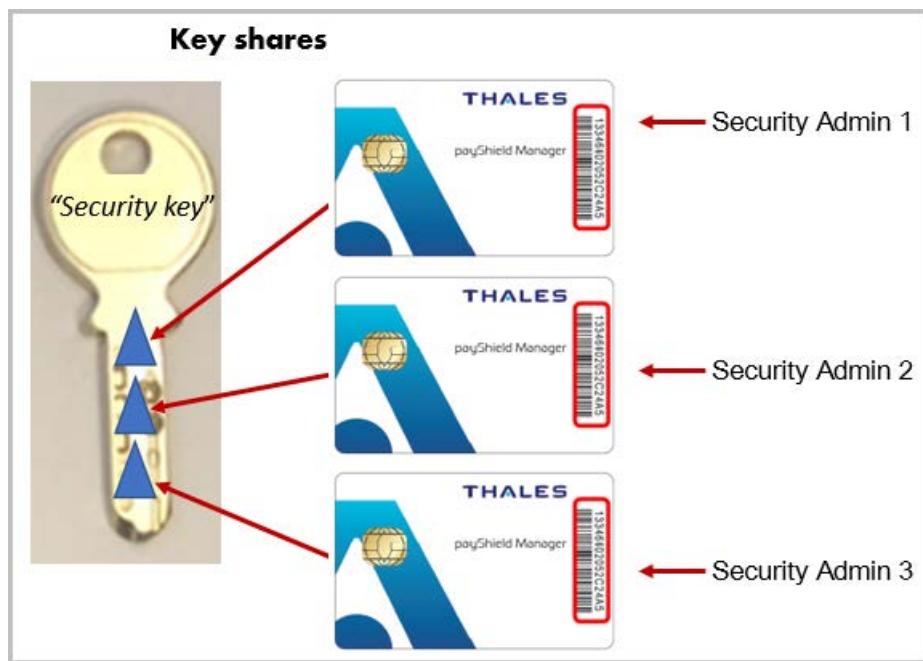


Figure 1

"key share" concept overview

1.9 Host Commands supporting multiple LMKs

The basic mechanism for Host commands to support multiple LMKs and LMK schemes is as follows:

Two additional (optional) fields are added at the end of each Host command request message. These fields are:

Field	Length & Type	Details
Delimiter	1 A	Value "%". Optional; if present, the LMK Identifier field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.

For Ethernet-attached Host computers, the HSM can infer the LMK Identifier to use for a particular command from the TCP port on which the command is received. Historically, Host commands sent via TCP/IP have been directed to the HSM's Well-Known Port, and this continues to be supported. However, Host commands directed to [the Well-Known Port +1] will automatically use LMK Id 00; Host commands directed to [the Well-Known Port +2] will automatically use LMK Id 01; etc. The situation for an HSM using the default Well-Known Port value of 1500 is summarized in the table below:

Command received on TCP Port	LMK Used
1500	Default LMK ID (or % nn construct)
1501	LMK ID 00
1502	LMK ID 01
1503	LMK ID 02

1.9.1 LMK Usage in Host Commands

The HSM uses the following mechanisms to determine which LMK Id to use with a Host command:

- The Management LMK is automatically used for command processing and the Delimiter and LMK Identifier fields should not be included in the command message. The only commands that belong in this category are the “Q0”, “Q2”, “Q4” and “Q8” commands.
- For commands using key blocks, the LMK that is identified in the key block header(s) is used; if the Delimiter and LMK Identifier are present in the command message, then all LMK identifiers must agree.
- If the Delimiter and LMK Identifier are present at the end of the command message, then the specified LMK is used in the command processing.
- For commands received via the Ethernet Host port using TCP/IP, the HSM infers the LMK Id to use based on the specific TCP port on which the command was received.
- For all other commands where the Delimiter and LMK Identifier are not present in the command message, the Default LMK is used in command processing.

1.10 payShield 10K license packages

The tables that follow summarize payShield 10K license packages.

Product Description		Additional Information
PS10-CLA-L	Classic package - 25 cps	
PS10-CLA-S	Classic package - 60 cps	
PS10-CLA-M	Classic package - 250 cps	
PS10-CLA-H	Classic package - 1000 cps	
PS10-CLA-X	Classic package - 2500 cps	
PS10-PRM-L	Premium package - 25 cps	
PS10-PRM-S	Premium package - 60 cps	
PS10-PRM-M	Premium package - 250 cps	
PS10-PRM-H	Premium package - 1000 cps	
PS10-PRM-X	Premium package - 2500 cps	
PS10-PRM-Y	Premium Package - 10,000 cps*	
PS10U-CLA-L2S	Classic pack perf upg - 25 to 60 cps	Classic pack performance upgrade - 25 to 60 cps
PS10U-CLA-S2M	Classic pack perf upg - 60 to 250 cps	Classic pack performance upgrade - 60 to 250 cps
PS10U-CLA-M2H	Classic pack perf upg - 250 to 1000 cps	Classic pack Performance upgrade - 250 to 1000 cps
PS10U-CLA-H2X	Classic pack perf upg - 1000 to 2500 cps	Classic pack performance upgrade - 1000 to 2500 cps
PS10U-CLA2PRM	Package upgrade - Classic to Premium	Package upgrade - Classic to Premium
PS10U-PRM-L2S	Premium pack perf upg - 25 to 60 cps	Premium pack performance upgrade - 25 to 60 cps
PS10U-PRM-S2M	Premium pack perf upg - 60 to 250 cps	Premium pack performance upgrade - 60 to 250 cps
PS10U-PRM-M2H	Premium pack perf upg - 250 to 1000 cps	Premium pack performance upgrade - 250 to 1000 cps
PS10U-PRM-H2X	Premium pack perf upg - 1000 to 2500 cps	Premium pack performance upgrade - 1000 to 2500 cps
PS10U-PRM-X2Y	Premium Pack perf upg - 2500 to 10,000 cps*	Premium pack performance upgrade - 2500 to 10,000 cps

* Only available for the Premium package and not supported by FICON

Optional Licenses

Product Description		Additional Information
PS10-LIC-RMGT	Remote payShield Manager license	License to operate payShield Manager remotely as well as locally
PS10-LIC-LMKx2	payShield LMK x 2 license	License for multiple LMKx2
PS10-LIC-LMKx5	payShield LMK x 5 license	License for multiple LMKx5
PS10-LIC-LMKx10	payShield LMK x 10 license	License for multiple LMKx10
PS10-LIC-LMKx20	payShield LMK x 20 license	License for multiple LMKx20
PS10-LIC-FF1	FF1 license	License enables the use of the FF1 Format Preserving Encryption (FPE) algorithm within the M0, M2 and M4 Host Commands.
PS10-LIC-VDSP	Visa Data Secure Platform (DSP) license	License for Visa Data Secure Platform (DSP). Requires written confirmation from customer that they have an agreement with VISA.
PS10-LIC-LEGACY	Miscellaneous Legacy Commands license	License for Miscellaneous Legacy Commands

1.11 Trusted Management Device (TMD)

1.11.1 Introduction

This section provides an outline of the Trusted Management Device (TMD) provided by Thales to securely manage key components to meet the latest standards from PCI. The TMD replaces the Thales Key Management Device (KMD) which is end of sale.

For further detailed information on the TMD, please refer to the *Thales TMD User Guide*.

1.11.2 Background

Secure key management is crucial to the security of the system in which the payShield 10K is used. One particular area of importance is the exchange of symmetric encryption keys between parties in the payment network (such as an Acquirer and a Switch) who need to exchange data securely. There is a large number of such keys, and these need to be refreshed regularly, and so there is a frequent need to exchange working keys between parties. In order to protect these keys while they are being exchanged electronically, the working keys are encrypted by a master key (such as a Zone Master Key, or ZMK).

The master key still needs to be provided by one party to the other, and this transfer also has to be secured. However, master keys need to be transferred only infrequently, and so a less automated mechanism is acceptable. In general the institution providing the master key will issue it in the form of a number (typically 3) of components to different officers in the receiving institution, and these officers will come together and enter their components individually into a secure system.

In the past it has been acceptable to enter the components directly into the payment HSM such as the payShield 10K using the Console interface. However the latest PCI standards require use of a Secure Cryptographic Device (SCD) such as the Thales Trusted Management Device (TMD). This replaces the Thales Key Management Device (KMD) which is end of life.

1.11.3 Description

The TMD offers secure, flexible and efficient key management for payment HSMs. It is a compact, intuitive, self-contained secure cryptographic device (SCD) that enables you to perform symmetric key management tasks including securely forming keys from separate components or splitting existing keys retrospectively into new components. The TMD generates and shares keys in a manner that is compliant with relevant security standards, including X9 TR-31, ANSI X9.24-1 and PCI PIN Security.

Unlike traditional approaches, these critical key management tasks can be carried out without any physical connection to a production HSM, providing greater operational flexibility without compromising security. For example, a single payShield TMD can form keys for multiple payment HSMs distributed across multiple data centers, enabling large payment processors to create and distribute thousands of Key Encrypting Keys (KEKs) or Zone Master Keys (ZMKs) in a timely and secure manner while eliminating data entry errors.

Each TMD shares one or more Master ZMKs (MZMKs) with the HSMs to facilitate secure exchange of key material. The TMD does not require access to the Local Master Keys (LMKs) used by the production HSMs. Keys exchanged between TMD and an HSM are encrypted under the appropriate MZMK.



1.11.4 How Keys Are Shared With payShield and 3rd Parties

The following table shows how keys are typically shared securely between the TMD, payShield 10K and third parties. Other options are available for example to secure the transfer of keys.

Phase	Internal System		External Party	Key	Secure Method of Transfer
Set-Up	TMD	payShield 10K	---	MZMK	Component form on Smart Card
	TMD		Third Party	ZMK	Components in Printed form
	TMD	payShield 10K		ZMK	Encrypted under MZMK
Production	payShield 10K		Third Party	Application and Session Keys (e.g. ZPK, PVK etc.)	Encrypted under ZMK

Note, keys can be transferred in both directions.

1.11.5 Example Sequence of Steps to Set-Up and Transfer Keys

This section shows a typical sequence of steps that are used to set up the keys required. Please note:

- From the payShield 10K perspective, the MZMK is a standard ZMK.
- The TMD has comprehensive facilities to manage TMD Administrators and Operators using Smart Cards and these are set up when the first MZMK is installed – see the *Thales TMD User Guide*

Note: The host application in the description below is the customer's payment application.

The main steps are:

1. Sharing the MZMK between the payShield 10K and the TMD:
 - a) Use the payShield 10K Console Command **GS** to generate MZMK components on HSM Smart Cards and to display the MZMK encrypted under the LMK.
 - b) Install the MZMK in the TMD from the components on the Smart Card generated above.
 - c) Enter the MZMK encrypted under the LMK into the host application database for subsequent use.
2. Sharing the ZMK with a third party.
 - a) Use the TMD to import the ZMK in component form from a third party and display the ZMK encrypted under the MZMK.
 - b) Enter the ZMK encrypted under the MZMK into the host application.
 - c) The Host application uses Host command **A6** (or **BY**) to translate the ZMK from encryption under the MZMK to encryption under the LMK and stores in the Host application for subsequent use.
Note: Instead of using a Host command in step c), the Console Command **IK** can be used with the payShield Manager Virtual Console (or the standard Console) to translate the ZMK from encryption under the MZMK to encryption under the LMK. This can then be entered into the Host application for subsequent use.
3. Sharing Application or Session Keys with Third Party
 - a) Application or Session keys (e.g. ZPK, PVK) received from the 3rd party encrypted under a ZMK are translated to encryption under an LMK using Host Command **A6**.
 - b) Host application exports Application or Session keys (e.g. ZPK, PVK) to 3rd party by translating from encryption under a LMK to encryption under the ZMK using Host Command **A8**.
4. Option - Sharing Application Keys within Component Form with Third Party
 - a) Use the TMD to import the application key (e.g. PVK, CVK) in component form and output key encrypted under the MZMK on the display.
 - b) Enter key encrypted under the MZMK into the payment application
 - c) The Host application uses Host Command **A6** to translate the key encrypted under the MZMK to encryption under the LMK and stores in the host application.

The ZMK can be generated by the payShield 10K instead of by the third party. In this case, the payShield 10K is used to generate the ZMK (using Host Command **A0**), encrypt the ZMK under a MZMK (using Host Command **A8** or Console Command **KE**) for import into the TMD. The TMD can then be used generate and print the ZMK Components securely for transfer to a third party. As noted above, the payShield Manager Virtual Console or the standard Console can be used with Console Command KE.

There are also a number of alternative options provided with the TMD and these are documented in the *Thales TMD User Guide*. These include:

- Except for the first MZMK, subsequent MZMKs can be generated using the TMD and stored in component form on a Smart Card. The Console Command **FK** is then used to import from components on the Smart Card and display the key encrypted under the LMK. This is then entered into the Host application for subsequent use.
- Key components or encrypted keys generated by the TMD can be displayed on the TMD screen, printed or written to USB memory stick.
- Key components or encrypted keys received from third parties can be entered on the TMD screen, scanned in using QR code or read from USB memory stick if provided in the supported format.

2 Backwards Compatibility and Differences

2.1 payShield 9000 / payShield 10K

Where possible, the payShield 10K provides Host commands that are backwards compatible with implementations on older versions of Thales HSMs, specifically the payShield 9000.

- LMKs generated and written to payShield 9000 Smart Cards using the GK console command work in the payShield 10K
- LMKs set up using payShield Manager work in the payShield 10K using payShield Manager
- Customers who have set up Customer Trust Authorities (CTAs) for payShield Manager on the payShield 9000 can use those same CTAs in payShield 10K

payShield 10K does not support the old Remote HSM Manager. If you have set up LMK cards using the old Remote HSM Manager, migrate the cards to payShield Manager using the payShield 9000. Once migrated, the cards can be used on the payShield 10K.

Note: pay Shield 9000 cards storing **security, command or PIN Block configuration settings** cannot be used on the payShield 10K. Conversely, payShield 10K cards storing security, command or PIN Block configuration settings cannot be used on the payShield 9000.

2.1.1 Host Interface and Commands

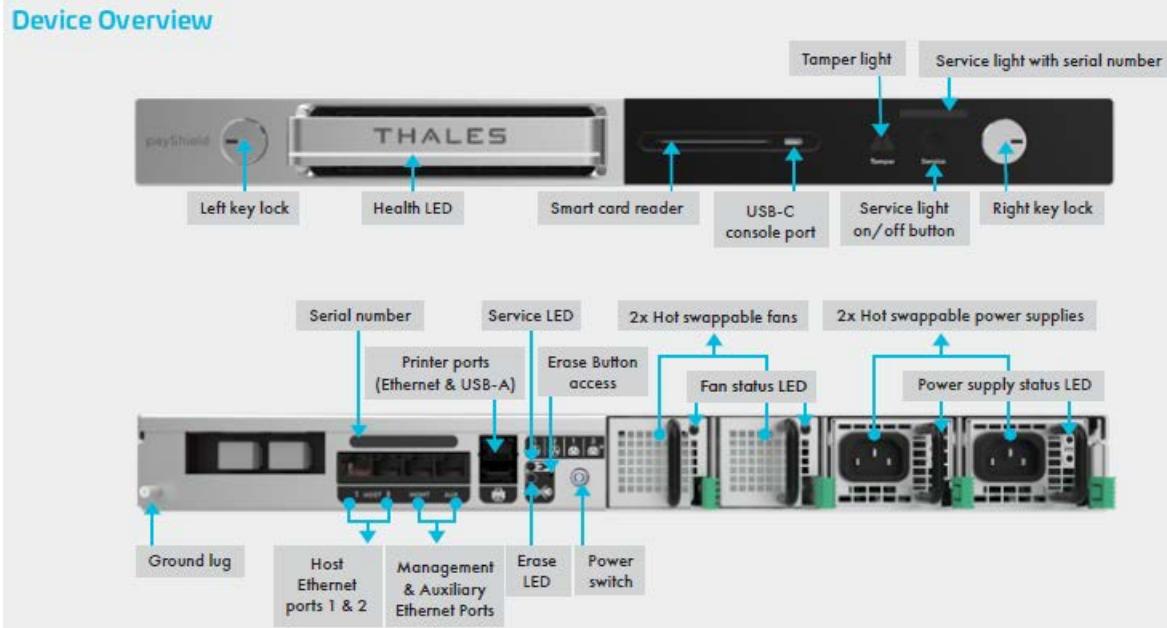
The only major differences between the Host Interface and Commands for payShield 9000 and for the payShield 10K are as follows:

- Legacy commands must be ordered separately through a license (PS10-LIC-LEGACY).
- Asynchronous Communication capability has been removed from Host1 and Host2 ports.
- The LG Host command to “Set HSM Response Delay” has been depreciated because ASYNC communications are not supported, so it now only returns a ‘00’.

2.1.2 Options for Managing payShield 10K

- Connecting a Console (USB-C on front panel).
- Local payShield Manager, Ethernet directly into management port.
- Remote payShield Manager, Ethernet into network.

Device Overview



Note: Local payShield Manager comes as part of the payShield package and creates a GUI user interface that is much easier to use than the console. Once customer trust has been set up between the payShield and the payShield Manager Smart Cards, you can easily choose to add the remote licenses with minimal set up at a later date.

2.1.3 Modifications made to the console commands

Command	Description
'CC' (Configure Console)	Removed Command because the console is now self-configuring.
'QC' (Query Console)	Removed Command because the console is now self-configuring.
SNMPADD (Add SNMP)	Modified for payShield 10K MIB
SNMP DEL (Delete SNMP)	Modified for payShield 10K MIB
TRAP (Displays Traps configured)	Modified for payShield 10K MIB
TRAPADD (Add a trap)	Modified for payShield 10K MIB
'CH' (Configure Host)	Modified to remove Asynchronous Communications option.
'QH' (Query Host)	Modified to remove Asynchronous Communications option.
'VR' (view software revision)	Modified to reflect payShield 10K Version options.
UPLOAD (upload new code)	Added for secure code and license loading at the console.
AUDITPRINT (print Audit Log)	Removed because of the increase in Audit size. Logs can be uploaded and then printed.
'SS' (Save settings to Smart Card)	Modified for 10K settings.
'RS' (Retrieve HSM settings from Smart Card)	Modified for 10K settings, cannot be used for 9K settings and conversely, 9K settings cannot be used for 10K.
'RI' (Initialize Domain Authority)	Removed because old HSM Manager is not supported in the 10K.

Command	Description
'RH' (Generate an HSM certificate)	Removed because old HSM Manager is not supported in the 10K.
ROUTE (Add static IP Route)	Removed, this command was only relevant to HSM 8000. This can be done using the 'CH' command and entering the 'gateway' address.
'CS' (Configure Security)	Modified for 10K
'QS' (Query Security)	Modified for 10K
'DT' (Diagnostic Test)	Modified for 10K (added new tolerances for Voltage and Temperature and added hot swappable fans and power supplies).
AUDITOOPTIONS (Set up audit options)	Modified for 10K
AUDITLOG (Manage Audit Log)	Modified for 10K, increased size to 100,000 entries.
'CL' (Configure Alarm)	Modified for 10K
NETSTAT (Show network statistics)	Modified because of 10K OS version
PING (Test TCP/IP network)	Modified because of 10K OS version
TRACERT (Trace TCP/IP route)	Modified because of 10K OS version
'QL' (Query Alarm)	Modified for 10K
NETSTAT (Show network statistics)	Modified because of 10K OS version
PING (Test TCP/IP network)	Modified because of 10K OS version
TRACERT (Trace TCP/IP route)	Modified because of 10K OS version

2.1.4 Feature Comparison

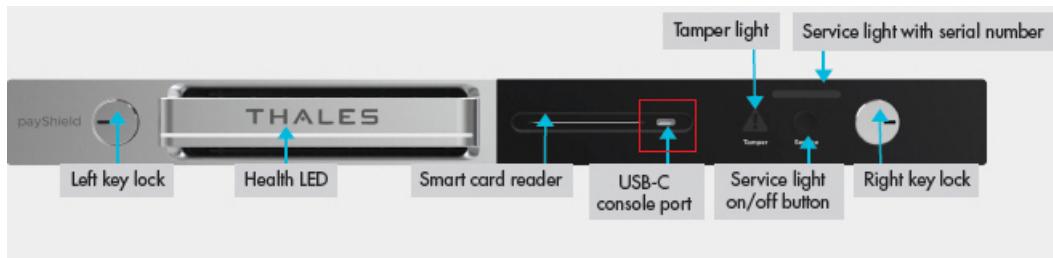
Note: For the 10G Ethernet Platform Variant, follow this link: [Chapter 5, “payShield PS10-D: 10G Ethernet Hardware Platform Variant”](#).

Note: For the FICON Platform Variant, follow this link: [Chapter 6, “payShield 10K FICON Platform Variant”](#).

Feature	payShield 9000	payShield 10K
Form Factor	2U Chassis	1U Chassis
Code loading mechanism	FTP interface or USB stick	HTTPS via payShield Manager or the secure “UPLOAD” console command using the USB-C for the console and the USB-A for the USB memory stick with the software or license update.
Security sub-system	TSPP designed to meet FIPS 140-2 Level 3 and PCI HSM Version 1	TASP 1.0 designed to meet FIPS 140-2 Level 3 and PCI HSM Version 3
PIN block translate performance	20, 50, 150, 250, 800 and 1500 cps (transactions per second)	25, 60, 250, 1000, 2500 and 10,000 cps (commands per second)
Power supply options	Choice of single or redundant power supplies, not Field Replaceable	Dual, Field Replaceable and Hot Swappable
Fan options	Fixed, not Field Replaceable	Dual, Field Replaceable and Hot Swappable
Management port connections	Six USB-A ports Ethernet for local/remote management	USB-C port on front panel USB-A port on rear panel Ethernet for local/remote management Ethernet for AUX (payShield Monitor)
Host interface connectivity	Dual, 10/100/1000 Mbps Ethernet, Async and FICON	Dual, 10/100/1000 Mbps Ethernet PCIe slot for FICON or 10Gig Ethernet (supported after product launch) (Async no longer supported)
Dimensions	3.35 x 18.82 x 16.42" (85 x 478 x 417mm)	19" x 29" x 1.75" (482.6mm x 736.6mm x 44.45mm)
Weight	7.5kg (16.5lb)	15.9 kilograms (35 lbs)
Electrical Supply	100 to 240V AC Universal input, 47 to 63 Hz	90-264V AC Universal input, 47 to 63 Hz
Power Consumption	100W (maximum)	PS10-S 60 W max PS10-D 70 W max (with 4 x optical transceivers); 80 W max (with 4 x copper transceivers) PS10-F (with 1 x FICON transceiver) 80 W max
Operating Temperature	0 deg C to +40 deg C	0 deg C to +40 deg C
Humidity	0% to 90% (non-condensing)	5% to 85% (non-condensing @ +30C)
MTBF	179K hours and an Annual Failure Rate (AFR) of 4.7%.	555K hours without redundant power supplies and fans and an AFR of 1.57% 2,445K hours with redundant power supplies and fans and an AFR of 0.35%

Note: Should temperatures exceed the operational range, return the payShield to the operational range.

2.1.5 Front Panel



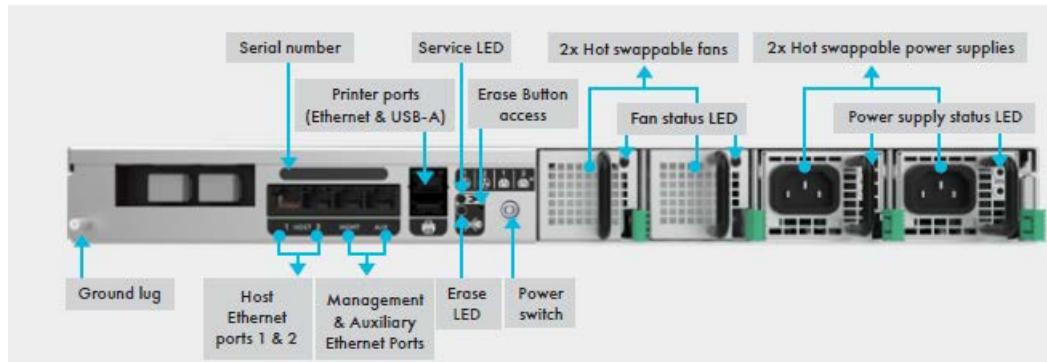
2.1.6 Front Panel LEDs

LED Indicator	LED Color	Description
Front Panel Health	Solid White	Unit booting, firmware validation in process, payShield functional, there are no errors in the error log.
Front Panel Health	Solid Red	Unit booting, application initialization in process, payShield failed diagnostic test or there are errors in the error log.
Front Panel Tamper	Off	No Tamper has been detected.
Front Panel Tamper	Solid Red	A high Tamper has been detected, contact Thales support.
Front Panel Tamper	Flashing Red	A medium Tamper has been detected, customer key material has been erased.
Front Panel Service	Off	Service has not been designated for this unit.
Front Panel Service	Solid Blue	This unit has been designated for service.

2.1.7 Front Panel Key Lock Positions



2.1.8 Rear Panel



2.1.9 Enhanced Security Features

payShield 10K software has been designed, where practical, to be secure by default. Most security settings affecting configurations are set to their most secure value by default.

Attention: All Host commands, most console commands and all PIN Blocks have been disabled by default.

Note: The security parameters required may vary depending on your security policy and system environment, and Thales recommends that you review the *payShield 10K Security Manual* as well as consult your internal Security Manager for full details.

payShield 10K has been designed with the following enhanced physical security features:

- A tamper resistant and responsive design
- Fully locked-down chassis lid with no ability to open
- Tamper sensors for chassis lid, crypto processor cover, motion, voltage and temperature
- Two levels of tamper:
 - Medium tamper erases all sensitive data
 - High tamper erases all sensitive data and permanently disables use of the unit
- Sensitive data immediately erased in the event of any tamper attempt

Compliance with PCI HSM Version 3 requirements introduce some rules which may cause incompatibility between PCI HSM compliant payShield 10K HSMs and earlier non-compliant HSMs:

- In most cases, security settings default to the most secure option
- All Host and console commands are disabled.
- All PIN blocks are disabled

Note: The console command CONFIGCMD is not disabled by default.

Control is provided in the security settings to allow the user to select whether to operate in the “classic” manner or in the PCI HSM compliant manner.

Three new settings have been added to the “Security Configuration Settings” for PCI HSM V3:

- Enforce PCI HSMv3 Key Equivalence for Key Wrapping?
- Enforce minimum key strength of 1024-bits for RSA signature verification?
- Enforce minimum key strength of 2048-bits for RSA?

Note: Once the security configuration settings are all PCI HSM compliant, they cannot be changed without all customer key material being deleted and the configuration settings set back to factory default.

2.1.10 Diagnostics

- The Audit Log size has been increased to 100,000 entries.
- The Error Log size has increased to 10,000 entries.

Error and Audit Logs can be uploaded for printing but **printing Audit Logs directly from the Console or Virtual Console in payShield Manager has been disabled.**

Diagnostic tests for the hot swappable fan and power supply components have been added.

2.1.11 Monitoring

Changes have been made to payShield Monitor and SNMP.

- There is a new payShield 10K MIB.
- The SNMP port list is modified to allow the user to select between AUX port and Management ports only. Host ports are no longer supported.
- SNMP V1/V2 have been removed and community strings are no longer displayed, only version 3 is supported. Consequently, the prompt that was in the SNMP console commands for version has been removed.
- The prompt to enter a port for the trap now supports a default port of 162.
- AES-128 is provided as a privacy algorithm option in the payShield 10K.
- Objects related to ASYNC Host communications have been removed.
- Objects for the auxiliary Ethernet interface, Field Replaceable Units (FRUs) and battery state have been added.
- Objects for internal sensor processor and boot versions have been added.

2.1.12 Transitioning Smart Cards

As discussed in [Section 1.5, “Smart Cards”, on page 4](#), the payShield 10K supports payShield Manager Smart Cards and HSM Smart Cards. The sections that follow provide guidance for migrating from non-supported Smart Cards to supported Smart Cards.

2.1.12.1 Transitioning legacy Manager Smart Cards

If you are using the old HSM Manager, you will need to migrate your legacy cards (see below) using payShield Manager on the payShield 9000, if you want to keep the same domain. This means updating the payShield 9000 to version 3.0 or above and then going through the payShield 9000 migration process, as outlined in the *payShield 9000 payShield Manager Manual*.

You will then have your CTA and LMK cards and ADMIN cards on the JAVA cards, which can be read by payShield Manager on the payShield 10K.

Non-supported Remote HSM Manager Smart Cards:



JAVA cards which can be read by payShield Manager on the payShield 10K:



2.1.12.2 Transitioning non-supported legacy HSM Smart Cards

The legacy cards, shown below, are not supported in the payShield 10K.

Non-supported legacy HSM Smart Cards:



You will need to use your payShield 9000 to copy the information stored on the non-supported cards on to the supported LMK “component” cards before loading them into the payShield 10K.

Supported HSM Smart Cards:



2.1.12.3 Copying a card at the console

1. Connect the console using the USB-C and Tera Term or PuTTY.
- Note:** The payShield can be in the Online, Offline or Secure mode.
2. Use the ‘FC’ command (format card) to format X number of the supported cards.
 3. Put the payShield into Secure mode.
 4. Use the ‘DC’ (Duplicate LMK Component Set) command to duplicate the component from the old card onto the new card.
 5. Load the LMK into the payShield 10K.
 6. Confirm that the LMK is working in the 10K.
 7. Destroy the old LMK cards.

2.1.13 User Documentation

The payShield 10K user manuals are now available for download from the Thales support website.

Follow the link below and to download all the user manuals:

<https://supportportal.thalesgroup.com/csm>

3 Physical Description

Note: For the 10G Ethernet Platform Variant, follow this link: [Chapter 5, “payShield PS10-D: 10G Ethernet Hardware Platform Variant”](#).

Note: For the payShield FICON Platform Variant, follow this link: [Chapter 6, “payShield 10K FICON Platform Variant”](#)

The payShield 10K can both stand alone or be part several units installed in a standard 19-inch cabinet.

- Overall rack dimensions (WxDxH) 1U rack 19" x 29" x 1.75" (482.6mm x 736.6mm x 44.5mm)

The unit is supported on telescopic runners that slide out via the front of the cabinet.

3.1 Front panel

3.1.1 Key locks and keys

The front panel is equipped with two key locks. Each lock has its own key. Each key is assigned to a “key holder” (i.e., a Security Officer/Administrator). To physically lock the unit into the rack, each key holder inserts their key into the appropriate lock and turns the lock to the locked position.

When in the locked position, the HSM cannot be removed from the rack.

The mechanical locking of the unit into the rack provides low level resistance to a direct attack. Note that the unit itself cannot be opened.

To remove the unit from the rack, both key holders insert their respective keys and turn the locks to the unlocked position.

3.1.1.1 Changing the HSM state via the key locks



Micro-switches attached to the locks allow the security state of the HSM to be changed.

Turning the cam lock keys changes the state of the HSM.

HSM states:

- Online (both locks are locked)
- Offline (one lock is locked and the other is unlocked)

- Secure (both locks are unlocked).

3.1.2 Smart Card Reader

The Smart Card Reader is an ISO card complaint type with automatic card ejection. The card is ejected at a standard point in HSM operation.

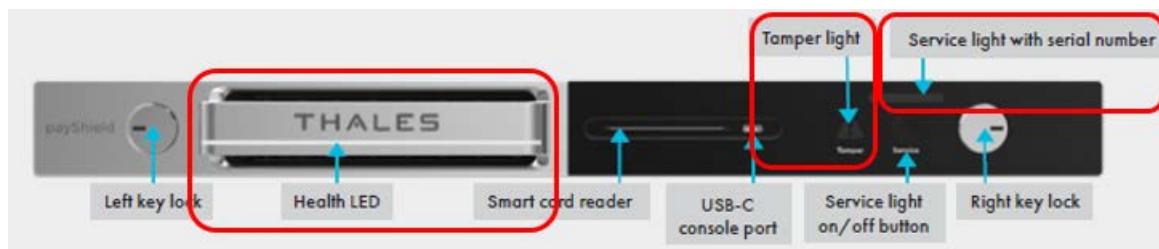
For example:

- At completion of a smart card related instruction from payShield Manager
- At completion of a smart card related Console command
- When the user presses the <Delete> key
- When the user presses CTRL-C key combination
- After a RESET
- During diagnostic testing

3.1.3 Front panel LEDs

There are three LED indicators on the front panel:

- Health (illuminating bar)
- Service (upper right)
- Tamper (warning triangle shape with exclamation mark)



3.1.3.1 Health LED

The Health LED is software controlled and readily identifies whether the unit is operational or if a fault condition exists.

LED Display	Indicates
Off	Power is off
White	Unit is operating properly
Flashing	Unit is booting. (Refer to Section 3.1.3.4, "Boot-up LED Sequence", on page 30)
Red	Errors exist. (Using payShield Manager, Navigate to Status > Error Log . Refer Section 9.3.2, "Status Tab", on page 107 for additional information.)

Note: After the Error Log has been read, the red LED reverts to white.

3.1.3.2 Service LED

The service switch is a momentary contact pushbutton switch used to signal that the Blue Service LED should be cleared.

The Service LED can be turned on by anyone either in the facility or remotely.

Note: There is also a Service LED on the back of the unit that mirrors the Service LED on the front of the unit.

Pushing the button toggles the state of the service function between on and off.

LED Display	Indicates
Off	No maintenance requested
Blue	The HSM has been selected for maintenance by an officer using payShield Manager or the button has been pushed by an operator in the data center

3.1.3.3 Tamper LED

The Tamper indicator illuminates when the HSM is triggered into an alarmed state by a security compromise. All secure data stored in the HSM is erased. When the sensor causing the alarm is no longer triggering, the HSM automatically reboots, and the Tamper LED is extinguished.

Note: To extinguish the LED, the HSM must be rebooted by powering off and powering on again. Following an alarm condition, the LMK(s) will need to be reloaded into the HSM. If the alarm condition is still present after rebooting, the Alarm LED remains illuminated; in this case the HSM must be returned to Thales for investigation and repair.

The tamper LED indicates if the unit is in a tampered state.

LED Display	Indicates
Off	No tamper
Flashing Red	Medium tamper
Solid Red	High tamper

3.1.3.4 Boot-up LED Sequence

As the system powers up, the LEDs display changes as the HSM moves through the power up sequence. The table below provides a key to the LED sequence.

LED Displays	Process
<ul style="list-style-type: none"> All LEDs are turned on Health LED toggles white/red twice 	System LED test power up occurring
Health LED flashing white	Firmware Validation occurring
Health LED solid white	Firmware Validation complete
Health LED flashing Red	Application initialization occurring
Solid white or Solid red (Solid red indicates that there are errors in the Error Log.)	Unit Operational

Table 1 *Power up LED sequence*

3.1.3.5 Blue LED

The blue service LED is indicates that the HSM requires service.

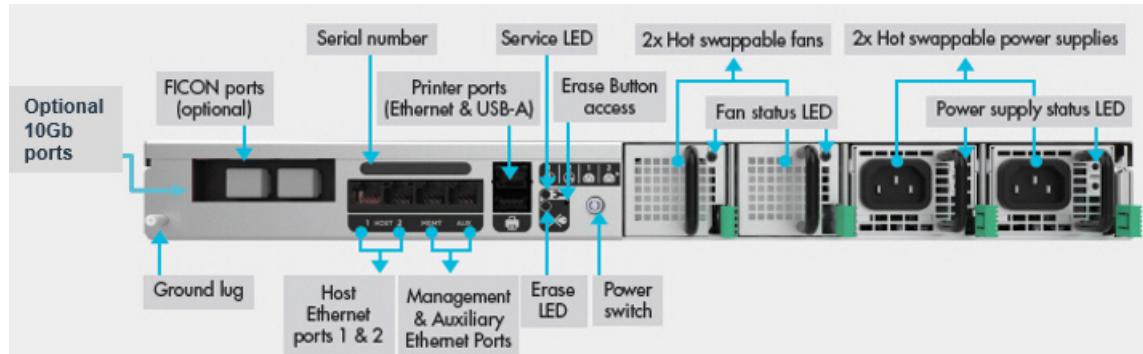
3.1.4 Air Inlets

The air inlets on the payShield 10K provide a cooling air entryway for the system and for power supplies.

3.2 Rear panel

Note: Follow this link for: Chapter 5, “payShield PS10-D: 10G Ethernet Hardware Platform Variant”.

Note: Follow this link for: Chapter 6, “payShield 10K FICON Platform Variant”.



3.2.1 AC/DC power supplies

3.2.1.1 Overview

The payShield 10K is equipped with dual power supply units allowing the HSM to receive power from two independent supplies. This redundancy is designed to help prevent any operational break in the event of:

- An outage in either one of the power supplies
- Failure of either of the power distribution units within the HSM

Each supply has the following features:

- 450W power factor corrected high efficiency supply
- Universal AC Inlet, 90 to 264V 50/60 Hz
- 12V main output and 5V standby
- Over-voltage, over-current, over temperature protection
- Latching mechanism to hold the supply in place
- Internal variable speed fan for independent cooling
- Integral LEDs to provide operational status
- Management, status, and control signals on the internal interface

3.2.1.2 Alternative Power Supply - Power Supply Type 2

From November 2022, an alternative model of PS10-S payShield 10K Standard Build is being made available supporting an alternative power supply - Power Supply Type 2. The performance and functionality of the new model is identical to the original model - the only difference relates to the type of power supply that can be installed. Key points are:

- The original “PS10-S payShield 10K Standard Build” model will only accept the original power supply, and the new “PS10-S payShield 10K Standard Build (Power Supply Type 2)” model will only accept Power Supply Type 2.
- The only difference between the models is the type of power supply that can be installed in the HSM.
- The power supply connectors inside the payShield 10K HSM are different, so it is not possible to install an incompatible power supply.
- The PS10-D, PS10-F and PS10-S Special Edition models do not support Power Supply Type 2.
- There are no changes to the power cords. The existing power cords can be used with both the original power supply and Power Supply Type 2.
- The orientation of the power supply sockets for the power supply cables is different as shown below:



Rear view of payShield 10K
fitted with original power supply



Rear view of payShield 10K
fitted with power supply type 2

- The model numbers of the power supplies differ and are shown in payShield Manager and when using the “VR” Console Command as follows:
 - Model number of original power supply: D1U54P-W-450-12-HA4C
 - Model Number of Power Supply Type 2: CDR-4011-1M

3.2.1.3 Power Supply LED Status

Each power supply provides status information using an LED which is visible from the rear of payShield 10K. A description of the information provided is given below:

LED STATUS INDICATORS FOR THE ORIGINAL POWER SUPPLY	
INPUT LED	
CONDITION	LED STATUS
Input Voltage Present	Solid Green
Input Voltage fault or warning	Blinking Green
Input off	Off
POWER LED	
CONDITION	LED STATUS
Fault concurrent indication via PMBus Status_x registers	Solid Amber
Warning, concurrent indication via PMBus Status_x registers	Blinking Amber
Standby, 12Vdc Main output off, Vstby On	Blinking Green
Power Good 12Vdc Main output on, Vstby On	Solid Green
Power Off 12Vdc Main output off, Vstby Off	Off

LED STATUS INDICATORS FOR POWER SUPPLY TYPE 2	
POWER LED	
CONDITION	LED STATUS
5Vdc Fault (e.g. over current, short circuit, over temperature, over voltage or a PSU Fan fault)	Off
12Vdc Fault (e.g. over current, short circuit, over temperature, over voltage or a PSU Fan fault)	Solid Amber
Power Good	Solid Green
Power Off	Off

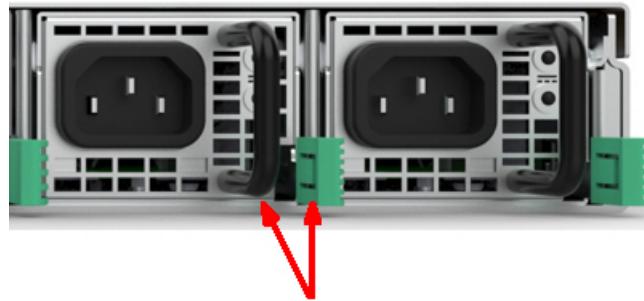
3.2.1.4 Swapping out the Power Supply

Note: The power supplies can be independently removed and replaced without removing the mains power from the other power supply. Each has a positive retention latch and status indicators.

1. Remove the AC supply cord from the PSU that you will be removing.

Note: This is an important safety issue so you are not left holding a PSU that is still connected to the mains.

2. Using thumb and forefinger, gently press lever to the left to release the hold.

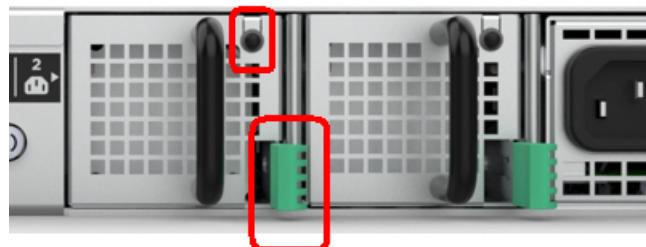


3. Slide the power supply out of chassis.
4. Slide the new power supply into chassis.

Latches click as the power supply is secured into the chassis.

3.2.2 Fan trays

There are two redundant fans. Each fan has a positive retention latch and a status indicator.



Each fan tray can be independently removed and replaced without taking the system out of service.

Each fan tray contains the following elements:

- 20 CFM fan
- Latching mechanism to hold the tray in the chassis
- Status LED
- EEPROM for manufacturing data
- Temperature based fan speed control

3.2.3 Battery

The HSM contains one battery that provides power to the sensor processor. This battery is designed to last the lifetime of the product and requires no maintenance.

3.2.4 AC Power on/off switch

The AC Power on/off switch provides a way to remove primary voltage from the system. The switch illuminates when ON and is unlit when turned OFF.

Note: A standby voltage is always present when the HSM is connected to the mains power. This standby voltage minimizes the drain on the battery and controls the startup sequence when the power is turned on.

3.2.5 PCIe card interface

The HSM has a single PCIe interface slot.

3.2.6 Ethernet ports

Note: Follow this link for a description of the 10G Ethernet Hardware Platform Variant: [Chapter 5, “payShield PS10-D: 10G Ethernet Hardware Platform Variant”](#).

The HSM has five Ethernet ports.

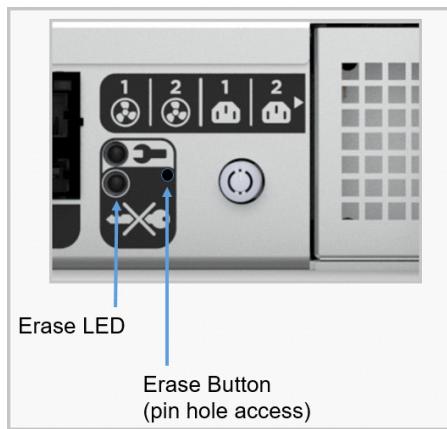
- Two host ports
Having two “hot” Ethernet host ports supports network resiliency. You can design dual independent network paths to the HSM, each port with its own IP address, both active, 128 threads on each.
- One management port
payShield Manager uses this port for communication between the HSM and the Management PC.
- One service port
- One printer port

Note: When connecting serial or parallel interface devices to USB ports, it is essential that a USB adapter is acquired from Thales. Adapters are available for USB-Serial, USB-Centronics parallel, and USB-25 Pin parallel. Adapters from other sources must not be used as the payShield 10K will not have the required drivers.

3.2.7 USB Type A port

There is a single USB host interface with a type A connector. This interface provides power for the attached device, if it is required.

3.2.8 Erase Button and LED



The HSM has a recessed erase button. When pressed, critical security parameters are removed. This does erase volatile memory.

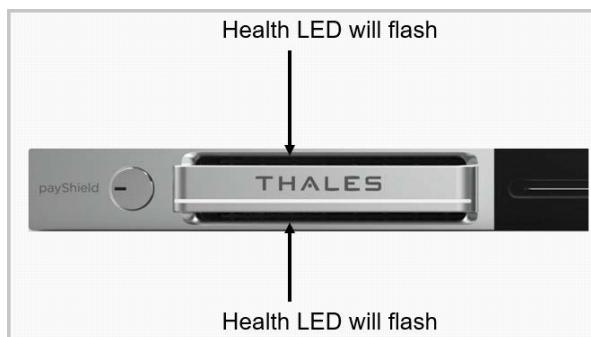
3.2.8.1 Erase procedure

Press the Erase button located on the payShield 10K's rear panel for 3 seconds. This requires a thin probe (like a straightened paper clip) to be inserted into the hole until a slight “click” is felt. Do not press too hard.

If the payShield 10K is not operational when, for example, there is a fault with the power supply, pressing the erase button will erase the LMK(s) (and all other secret information such as any remote management security keys, and any keys held in user storage).

Note:

- After pressing the Erase button for 3 seconds, the Erase LED is turned on if the erase operation is successful. The Erase LED will remain on if the Erase button continues to be held and will remain on for 3 seconds after the Erase button is released.
- If the unit is operational, pressing the Erase button generates an entry in the system Error log. This in turn causes the front panel Health LED to flash. If the error log entries are displayed, a number of new entries will be observed. One of these entries will note that the “Erase: button has been engaged”.



- The erase procedure can be carried out with the HSM powered from the mains. If the HSM is powered when the Erase button is pressed, the HSM will immediately reboot but the result will be the same (i.e. the Health LED flashes.)
- If the HSM is not operational (i.e. no LEDs are illuminated when connected to the power mains), the above procedure will still cause the erasure of the LMK and any other sensitive key material; however, no entry will be generated in the error log. The erase mechanism does not depend on the HSM being operational.
- At this stage all secret information will have been erased from the HSM and it will no longer be able to perform any cryptographic operations. However, it will still contain some other information, which in certain circumstances may be considered sensitive. Examples of this are: IP addresses, security settings, and Note configuration information.

3.2.9 Ground Lug

A single ground lug is provided for system grounding of the chassis.

4 Installation

Note: For the 10G Ethernet Platform Variant, follow this link: [Chapter 5, “payShield PS10-D: 10G Ethernet Hardware Platform Variant”](#).

Note: For the FICON Platform Variant, follow this link: [Chapter 6, “payShield 10K FICON Platform Variant”](#).

4.1 Pre-installation tasks

Before installing, you will need to address space, network and power requirements.

Note: When planning the equipment installation, consideration should be given to the clearances required for servicing the equipment such as removing the unit from the front or removing power supplies and fan trays in the rear. This is typically at least 3 feet in the front of the rack and 1 foot behind the rack.

Attention: Read the *payShield 10K Regulatory User Warnings and Cautions* document prior to installing the payShield 10K.

4.1.1 Mechanical and Electrical Specifications

4.1.1.1 Physical Characteristics

Characteristic	payShield 10K
Form Factor	1U Chassis
Rack Mount	1U 19"
Dimensions	19" x 29" x 1.75" (482.6mm x 736.6mm x 44.45mm)
Weight	15.9 kilograms (35 lbs)
Electrical Supply	0-264V AC Universal input, 47 to 63 Hz
Power Consumption	60W (maximum)
Operating Temperature	0 deg C to +40 deg C
Operating Humidity	5% to 85% non-condensing @ +30C

4.1.1.2 Power Considerations

The payShield 10K is a Class I product and must be connected to a power supply system which provides an earth continuity connection.

Suitable cabling to the supply should be provided within the rack system. Consideration should be given to the rating information of the unit and the effects that overloading of circuits might have on the cabling and over-current protection devices. Ensure the wiring is in accordance with the requirements of any local wiring regulations.

4.1.1.3 Environmental Considerations

Consideration must be given to the airflow and temperature when the units are installed in a rack to ensure that this temperature is not exceeded.

Once installed, ventilation holes must not become obstructed, as that could reduce the airflow through the unit.

4.1.1.4 Battery consideration

Each HSM has a battery that maintains sensitive key material stored in protected memory while the external AC power is removed. Without any AC power, the battery will maintain the contents of protected memory for a minimum of 10 years. When the HSM is running on AC power, the battery is not used, and discharge is minimal.

4.2 Installation Procedure

Typically, the HSM is located within a protected corporate data center with multiple layers of security and access controls.

Note: Follow this link should you need to review the environmental considerations: [Section 4.1.1, “Mechanical and Electrical Specifications”, on page 39.](#)

Prerequisite:

- A Phillips screwdriver, #2.
1. Read the *payShield 10K Regulatory User Warnings and Cautions* document.
 2. Gather the necessary personnel, e.g., security/trusted officers, trusted installer.
 3. Verify that the shipment never left the custody of the shipper and log the receipt of the shipment in accordance with your security policies.
 4. Unpack the Thales shipping container.

The box contains:

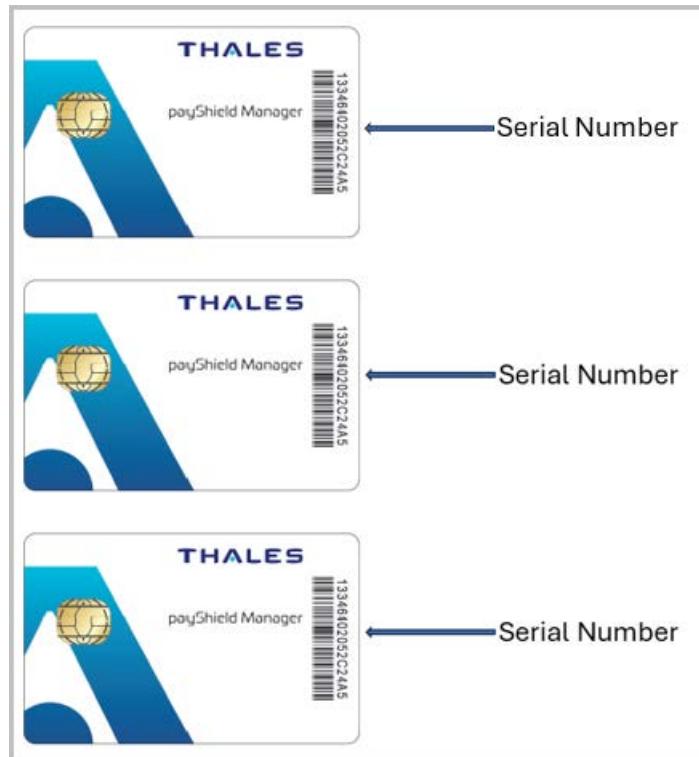
- 1 payShield 10K HSM
- 2 AC power cables
- 4 security keys (2 copies - 4 total keys)
- 1 USB-C to USB-A cable (for console connectivity)

Note: In certain circumstances, the security keys and the smart cards may be delivered to your two designated key-holders under separate cover (i.e., not included in the box). If the security keys have been delivered separately, the presence of both designated key-holders is required.

5. Confirm the contents of the box.
 - Verify that the serial number on the bag matches the shipping document.
6. Record the HSM serial numbers in accordance with your security policy.

7. Record the serial number of each smart card in accordance with your security policy.

Note: The serial number is located along the right edge of the smart card.



Note: Each card may be assigned to an individual Security Officer. Each officer should also maintain a record of their smart card's serial number.

8. Store the serial number records in accordance with your security policy.

9. Mount the rack.

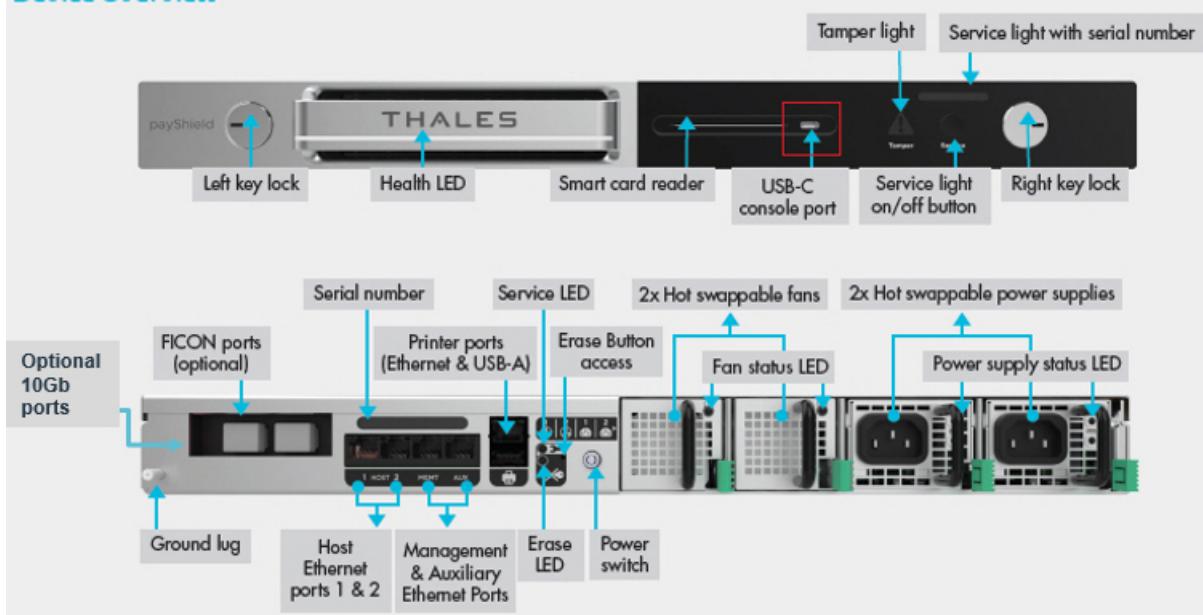
- a) Unpack the Thales box containing the Thales Universal Rack Mount Kit. The Mount Kit contains 2 rails and 10 M4 x 6 mm screws.

Note: The 1U 1000 mm Universal Rack Mount Kit is pre-assembled for use with square hole and unthreaded round hole racks. This rack kit is suitable for racks and cabinets where the depth between front and rear posts is in the range 685.8mm – 939.8mm.

- b) Remove inner rail from rack mount assembly.
 - Slide the inner rail until the safety catch locks.
 - Depress the safety catch and continue sliding to separate the inner and outer rails.
- c) Attach inner rail to the chassis.
 - Position the inner rail on the side of the product with the safety catch toward the rear.
 - Align the rear hole of the rail with the rear hole on the chassis and attach using the M4 x 6mm screws provided.
 - Align the other 4 holes with the counter sink in the rail with the corresponding holes in the chassis, insert the M4 x 6mm screws, and tighten all the screws.

- Repeat this to attach the second inner rail to the other side of the chassis.
- d) Adjust rail length. (The rails support a range of rack mounting depths.)
- Loosen the two rear retaining plate screws to enable the rear bracket to be extended.
- e) Install outer rails into the rack.
- Align the bracket marked “FRONT” with the holes in the front post.
 - Once aligned, push the bracket forward until the snap mechanism engages.
 - Slide the rear bracket towards the rear post of the rack.
 - Align the bracket with the holes in the rear post at the same vertical position used for the front and snap it in.
 - Tighten the two rear retaining screws.
- Attention:** Slide the bearing retainer all the way forward to avoid damaging the rail kit when the product is installed.
- f) Insert product into the outer rails.
- With both the left and right bearing retainers moved the entire way forward, align the inner rails mounted on the product with the outer rails mounted in the rack.
 - You may need to apply gentle pressure to the ends of the inner rails to align them with the outer rails.
 - Slide the product into the rack until the safety latches engage.
- g) Push the safety catches in on both sides and slide the product fully into the rack. When sliding the unit into the rack for the first time, the last few inches of travel may experience some resistance as the bearing retainers meet their backstops. The resistance can be overcome by applying slightly more force to the front of the unit to achieve full insertion into the rack.
10. Physically lock the unit into the rack.
- Each key holder inserts their key into their respective lock and turns the lock to the locked position.
11. Connect your HSM to your Host using an Ethernet connection.
12. Connect the power cables.
13. Push the power switch (located on the back of the unit) to turn the unit on.

Device Overview



As the system powers up, the LEDs display changes as the HSM moves through the power up sequence. The table below provides a key to the LED sequence.

LED Displays	Process
<ul style="list-style-type: none"> All LEDs are turned on Health LED toggles white/red twice 	System LED test power up occurring
Health LED flashing white	Firmware Validation occurring
Health LED solid white	Firmware Validation complete
Health LED flashing Red	Application initialization occurring
Solid white or Solid red (Solid red indicates that there is an error in the error log. The light extinguishes when you read the error log.)	Unit Operational

Table 2 Power up LED sequence

- Follow this link to connect using payShield Manager: [Chapter 7, “payShield Management Options”](#).
- Follow this link to connect using the console: [Chapter , “Commission payShield Manager using Console commands”](#)

5 payShield PS10-D: 10G Ethernet Hardware Platform Variant

5.1 Introduction

A variant of the standard payShield 10K hardware platform is available supporting 10G Ethernet. This can be ordered in place of the standard PS10-S payShield 10K Ethernet Hardware Platform using the following part number:

Part Number	Description
971-000055-001	PS10-D payShield 10K 10G Ethernet Hardware Platform

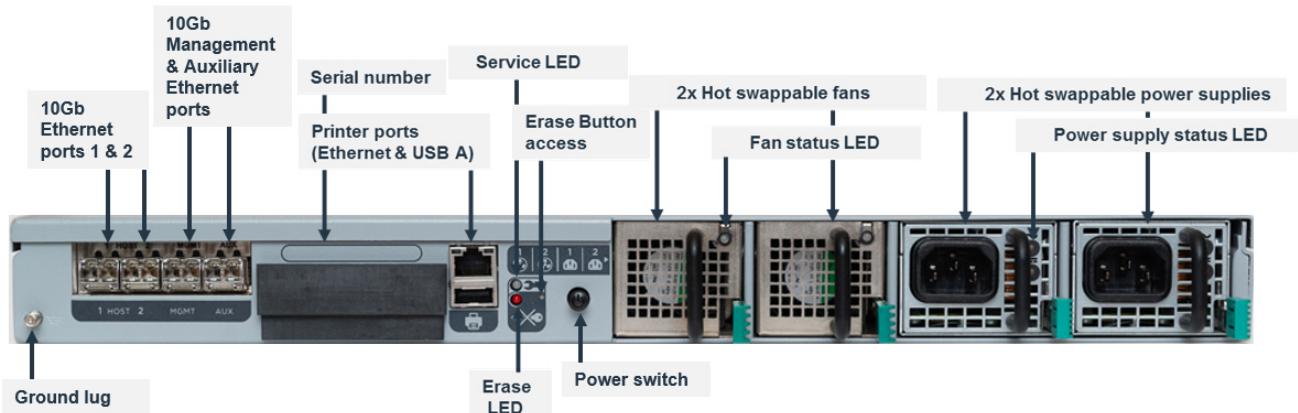
10G (or 1G) Ethernet only is provided on all four Ethernet ports, i.e., Host Port1, Host Port2, Management Port and the Auxiliary port. Transceivers for connection to either copper or optical networks must also be ordered for each port using the part number below:

Part Number	Transceiver type
971-000042-001	PS10-D-SFP+10G-OPT payShield 10K 10G Transceiver SFP+ Short Range 1GbE/10GbE Optical (1 off)
971-000043-001	PS10-D-SFP+10G-CPR payShield 10K 10G Transceiver SFP+ 10GbE RJ-45 Copper (1 off)

As with the standard PS10-S model, a Software Package with Performance must be ordered together with the Hardware Platform as well as any optional licenses and hardware accessories as required.

Support for the PS10-D model is provided in base software version v1.1a and above.

5.2 Rear Panel Overview



5.3 General Notes

- payShield 10K 10G Ethernet Hardware Platform has 4 ports for connecting to a 10G network using the transceivers ordered separately. The transceivers must be connected to a switch or router that supports 10G Ethernet.
- All 4 ports support hot plugin.
- The port settings can be viewed using the QH, QM, and QA console commands, using payShield Manager and using SNMP.
- The speed of the interface is NOT configurable. The only option allowed is “Auto select”. The actual value is negotiated by the interface. The Optical and Copper transceivers can be 1GbE or 10GbE, auto-selected by negotiation.
- When the 10G ports are present, the QUAD Small Form-factor Pluggable (SFP) ports replace the covered Native Ethernet ports.

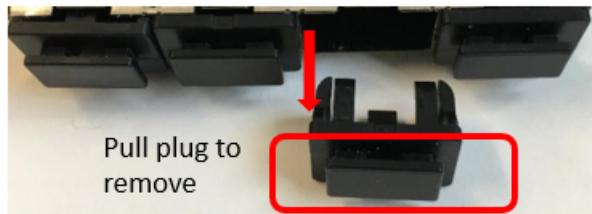
5.4 Installing 10Gb ports

Note: The SFP transceivers can be independently removed and replaced without removing the mains power.

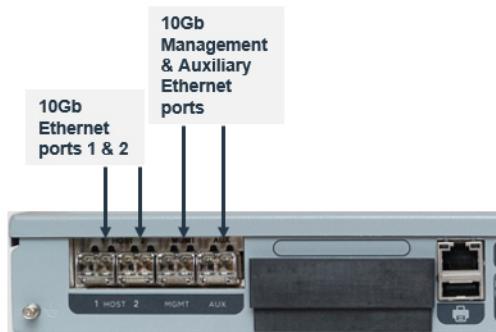
1. Remove the SFP transceivers from packaging.

Note: The package contains 4 International Integrated Reporting Council (IIRC) SFPs.

2. Remove the plugs that cover the SFP ports.



3. Slide each SFP into a port slot. (Each SFP can be either copper or optical or a mixture.)
 - If a mixture, the media type SFP must match the site requirement.
 - Host 1 in port 1, Host 2 in port 2, Management in port 3, AUX in port 4.



4. After removing any cable connection dust covers, attach the cables to ports.

5.5 Power Consumption

- When using 4 optical ports, the max is 70W
- When using 4 copper ports, the max is 80 W
- When using a mixture, the max is 70W to 80W depending on usage

6 payShield 10K FICON Platform Variant

6.1 Introduction

The payShield 10K can be ordered with an auto-sensing factory-fitted FICON (Fiber Connection) interface. This provides a port for connection to an IBM mainframe host computer to allow Host Commands and responses to be transmitted using a FICON fiber optic interface.

Part Number	Model Number	Description
971-700027-001	PS10-F	payShield 10K FICON Hardware Platform

The HSM's FICON interface supports speeds of 32 Gbps, with the option of 8 Gbps or 16 Gbps, if available. If using a switched fabric, the connecting switch must have the connecting port type set to fabric port (F_port).

The FICON interface can be ordered with a choice of transceivers to support. One Transceiver MUST be ordered with each payShield 10K FICON Platform:

Part Number	Model Number	Transceiver type
971-000075-001	PS10-F-XCV-S	payShield 10K FICON Short Wave Transceiver
971-000074-001	PS10-F-XCV-L	payShield 10K FICON Long Wave Transceiver

The FICON interface must be specified when the payShield 10K is ordered. It is installed in the factory and cannot be added to an existing payShield 10K.

The only package and performance license available for the payShield 10K FICON is the following which MUST be ordered together with the Hardware Platform, Transceiver as well as any optional licenses and hardware accessories as required:

Part Number	Model Number	Description
971-701630-001	PS10-PRM-X	Premium package - 2500 cps

Support for this model is provided in base software version v1.3a and above.

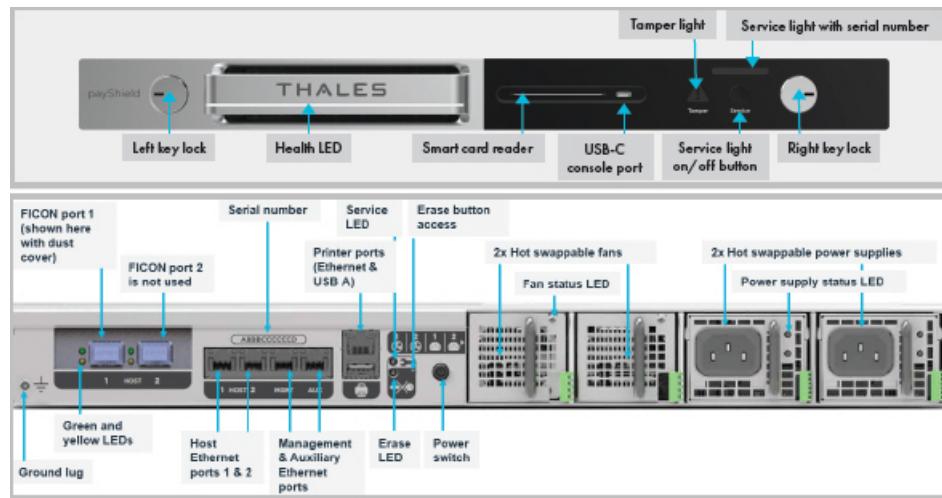
The recommended emulation is for a DUMMY device running on a NOCHECK Control Unit, although 3490 tape drive emulation is also supported. Please note the device should NOT be defined as a 3490 on a z/OS system, as the operating system will issue requests to the device to check if a tape is mounted and, if so, what the tape volume serial number is.

The FICON interface is fully integrated into the HSM's application software, and the Utilization and Health Check reporting facilities will report on the FICON interface.

6.2 Installing the payShield 10K PS10-F

Note: The data provided below can also be found in the *payShield 10K PS10-F Installation Quick start guide*. The quick start guide ships with the product.

6.2.1 Device overview



6.2.2 Assure safety

Before installing, and using this product, please read the Warnings and Cautions in the payShield 10K Regulatory User Warnings & Cautions document.

6.2.3 Unpack

1. Remove from packaging:
 - Remove the Accessories box
 - Remove the payShield 10K from the packaging, checking that the tamper evident bag containing the unit is not tampered
 - Check that the serial number on the tamper evident bag matches that supplied by email or shipment confirmation by Thales
2. Remove the accessories from the Accessories box.
3. Verify the shipment's contents:
 - payShield 10K PS10-F Host Security Module
 - HSM Rail Kit
 - 2 AC power cables
 - 4 Security keys in tamper evident bags (2 copies -- 4 total keys)
 - USB-C to USB-A cable (for console connectivity)
 - Either a FICON Short Wave Small form-factor pluggable transceiver (SFP) or FICON Long Wave SFP (ordered separately)
 - Loopback device

- payShield 10K Regulatory User Warnings & Cautions document
 - payShield 10K PS 10-F Installation Quick start guide
 - payShield Manager Quick start guide
 - Specification of the Host Bus Adapter (HBA)
4. Carry out the following checks:
- Check that the tamper evident bag containing the keys is not tampered and the serial number matches that supplied by email or shipment confirmation by Thales
 - Locate the serial number on the key tag and verify that it matches the serial number on the unit

Note: The HSM FICON interface supports speeds up to 32Gbps, with the option of 8Gbps or 16Gbps, if available. If using a switched fabric, the connection switch must have the connecting port type set to fabric port.

6.2.3.1 Gather additional equipment

Note: Based on your order, additional items may be included in your shipment. In certain circumstances, the security keys and Smart Cards may be delivered under separate cover to the two designated keyholders.

- For printer ports:
 - Printer Interface cable (Optional) - Printer communication is via USB peripheral cable for payShield Manager
- For payShield Manager:
 - A standard Ethernet cable for the Management Port
 - A standard desktop PC or laptop with a web browser supported by payShield Manager, (e.g. Chrome or Firefox)
- For the console terminal:
 - A standard desktop PC or laptop using terminal emulation software
- For FICON ports:
 - FICON interface cables - see tables below:

Characteristic	Short Wavelength Transceiver	Long Wavelength Transceiver
Data Rate	8.5Gb/s (8GFC) (auto-detected) 14.025Gb/s (16GFC) (auto-detected) 28.05Gb/s (32GFC) (auto-detected)	8.5Gb/s (8GFC) (auto-detected) 14.025Gb/s (16GFC) (auto-detected) 28.05Gb/s (32GFC) (auto-detected)
Optics	Short wave (850 nm) laser	Long wave (1310 nm) laser
Cable Types	Multimode: OM4 – 50/125 µm OM3 – 50/125 µm OM2 – 50/125 µm OM1 – 62.5/125 µm	Single Mode: OS2 – 9 µm OS1 – 9 µm
Connector Type	LC	LC
Minimum cable length	0.5 meters	0.5 meters

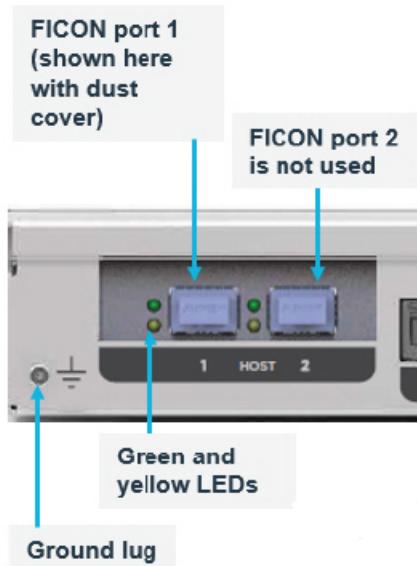
Characteristic	Short Wavelength Transceiver			Long Wavelength Transceiver			
	Cable	Data Rate	Meters	Cable	Data Rate	K'meters	
Max. cable length (Maximum cable length may be less than shown in this table, dependent on the fiber material used in the cable.)	OM1	8.5Gb/s (8GFC)	25M	OS1 & OS2	8.5Gb/s (8GFC)	10 Km	
		14.025Gb/s (16GFC)	Not specified		14.025Gb/s (16GFC)	10 Km	
		28.05Gb/s (32GFC)	Not specified		28.05Gb/s (32GFC)	10 Km	
	OM2	8.5Gb/s (8GFC)	50M				
		14.025Gb/s (16GFC)	35M				
		28.05Gb/s (32GFC)	20M				
	OM3	8.5Gb/s (8 GFC)	150M				
		14.025Gb/s (16GFC)	100M				
		28.05Gb/s (32GFC)	70M				
	OM4	8.5Gb/s (8GFC)	190M				
		14.025Gb/s (16GFC)	125M				
		28.05Gb/s (32GFC)	100M				

- Optional accessories:
 - USB to 25 pin parallel printer cable
 - payShield Manager Smart Cards
 - payShield Manager Starter Kit
 - payShield Manager Reader

6.2.4 Insert the SFP

Attention: Handle the transceivers delicately taking care not to damage them. Observe standard ESD (Electrostatic Discharge) precautions for handling electronic components.

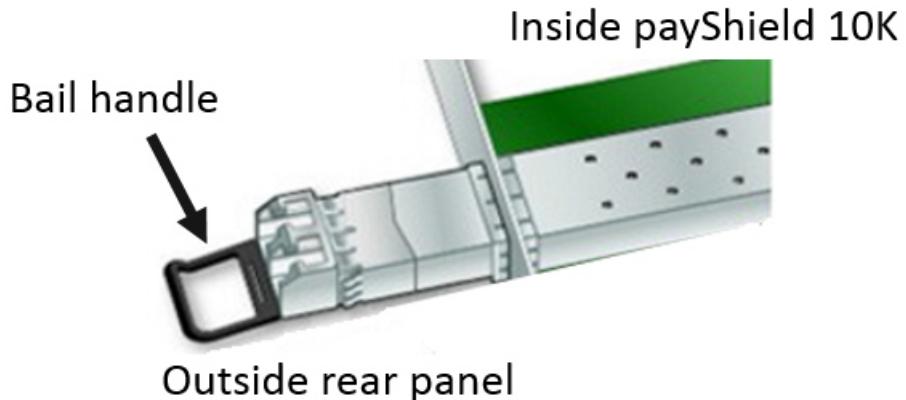
1. Remove the dust cover from FICON port 1. (Port 2 is not used.)



Note: If it is required to adapt a payShield 10K ordered with Shortwave transceivers to Longwave (or vice versa) this can be done by removing the supplied transceiver and replacing it with the required type. The specification of the replacement transceiver to be used can be obtained through Thales Support:

<https://supportportal.thalesgroup.com/csm>

2. Slide the transceiver into the housing. When the latch engages, it clicks.
3. Push the transceiver bail handle into place.



6.2.5 Determine the location for the payShield 10K

To ensure that temperature ranges are not exceeded, consider airflow and temperature when installing the HSM in the rack. Once installed, ventilation holes must not become obstructed, as that would reduce the air flow through the unit.

Operating temperature	0°– 40°C
Storage temperature	-5°C to 45°C
Transportation temperature	-25°C to 70°C
Operating humidity	5 – 85% (Relative non-condensing at 30°C)
Storage humidity	5 – 93% (Relative non-condensing at 30°C)
Transportation humidity	5 – 93% (Relative non-condensing at 40°C)
Altitude	-100m to 2000m AMSL (Above Mean Sea Level)
Overall rack dimensions (WxDxH)	1U rack 19" x 29" x 1.75" (482.6mm x 736.6 mm x 44.5mm)
Maximum Operating Power Consumption	80W

6.2.6 Mount the rack

1. Unpack the Thales box containing the Thales Universal Rack Mount Kit. The Mount Kit contains 2 rails and 10 M4 x 6 mm screws.

Note: The 1U 1000 mm Universal Rack Mount Kit is pre-assembled for use with square hole and unthreaded round hole racks. This rack kit is suitable for racks and cabinets where the depth between front and rear posts is in the range 685.8mm – 939.8mm.

2. Remove inner rail from rack mount assembly.
 - Slide the inner rail until the safety catch locks
 - Depress the safety catch and continue sliding to separate the inner and outer rails
3. Attach inner rail to the chassis.
 - Position the inner rail on the side of the product with the safety catch toward the rear
 - Align the rear hole of the rail with the rear hole on the chassis and attach using the M4 x 6mm screws provided
 - Align the other 4 holes with the counter sink in the rail with the corresponding holes in the chassis, insert the M4 x 6mm screws, and tighten all the screws
 - Repeat this to attach the second inner rail to the other side of the chassis
4. Adjust rail length. (The rails support a range of rack mounting depths.)
5. Loosen the two rear retaining plate screws to enable the rear bracket to be extended.
6. Install outer rails into the rack.
 - Align the bracket marked “FRONT” with the holes in the front post
 - Once aligned, push the bracket forward until the snap mechanism engages
 - Slide the rear bracket towards the rear post of the rack
 - Align the bracket with the holes in the rear post at the same vertical position used for the front and snap it in
 - Tighten the two rear retaining screws

Attention: Slide the bearing retainer all the way forward to avoid damaging the rail kit when the product is installed.

7. Insert product into the outer rails.

- With both the left and right bearing retainers moved the entire way forward, align the inner rails mounted on the product with the outer rails mounted in the rack
- You may need to apply gentle pressure to the ends of the inner rails to align them with the outer rails
- Slide the product into the rack until the safety latches engage

8. Push the safety catches in on both sides and slide the product fully into the rack.

When sliding the unit into the rack for the first time, the last few inches of travel may experience some resistance as the bearing retainers meet their backstops. The resistance can be overcome by applying slightly more force to the front of the unit to achieve full insertion into the rack.

6.2.7 Lock the unit into the rack

The payShield 10K is physically locked into the rack via the two key locks located on the front of the unit.

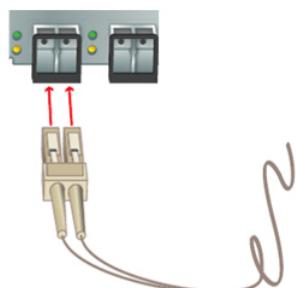
Note: Each lock has its own key and each key is owned by a Security Officer/Administrator.

To physically lock the unit into the rack, each key holder inserts their key into their respective lock and turns the lock to the locked position.



6.2.8 Connect cables and power on

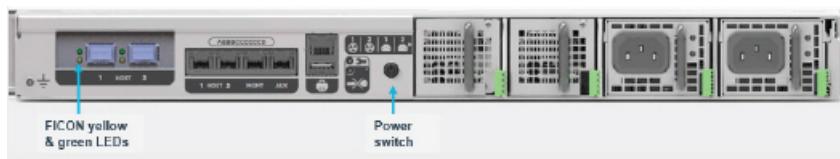
1. Plug the cable connectors into the LC connectors of Port 1:



2. Connect the power supplies.



3. Push the power switch; the unit has power when the power switch is pressed in.



Note: When power is applied to the unit, there is a period of time before the unit is operational and either the console or payShield Manager is available.

4. Wait for the health LED to turn solid white or solid red before proceeding.

Note: Once the payShield is powered up, the FICON interface performs a Power On Self-test, (POST). At a minimum, the following tests are performed by POST:

- Flash boot image checksum test
- Internal ASIC RAM tests for proper ECC parity operation
- Loopback test

5. Watch the LEDs on Port 1 for POST results.

Note: The yellow LED indicates port activity while the green LED indicates firmware operation.

The following table summarizes POST conditions and results.

Note: For the link rate conditions, a 1s pause occurs when the yellow LED is off between each group of fast blinks (2, 3, 4 or 5). Observe the LED sequence for several seconds to be sure you have correctly identified the pattern.

Yellow LED	Green LED	State
Off	Off	No SFP module is installed or a boot failure occurred (dead board)
On	Off	POST failure (dead board)
Slow blink	Off	Boot failure after POST
Flashing	Off	POST processing is in progress
Off	On	Failure in the common code module
On	On	Failure in the common code module
3 fast blinks	On	Normal (link up at 8GFC)
4 fast blinks	On	Normal (link up at 16GFC)
5 fast blinks	On	Normal (link up at 32GFC)
Fast blink	Fast blink	Beaconing

6.2.9 Configuring the payShield 10K

The payShield 10K can be configured via payShield Manager or via the Console terminal.

Note: For payShield Manager and Host operation, the payShield must be Online, i.e., the front panel keys are in the locked position.

Additional instruction is provided in the following:

- [Chapter 7, “payShield Management Options”](#)
- [Chapter 8, “Commission using payShield Manager”](#)
- [*payShield Manager Quick start guide*](#)
- [*payShield 10K Console Guide*](#)

6.2.10 Connect the console terminal

The console terminal is pre-configured to communicate with the HSM via the USB-C to USB-A cable.

- Use the supplied USB-C to USB-A cable to connect the USB-C port on the front of the payShield 10K to your laptop

Note: If your laptop has a USB-C port, instead of a USB-A port, you will need to order or provide a standard USB-C to USB-C cable.

- For Windows, ensure that all Windows updates have been applied and the laptop is connected to the internet before connecting to the payShield. Upon connection, Windows will detect the new hardware and install the driver. The device will appear as a new COM port.
- If the laptop cannot be connected to the internet, the drivers are available for download and manual installation from the Microsoft Update Catalog:

www.catalog.update.microsoft.com/Search.aspx?q=PI%20USB%20to%20serial



- Download the CAB file for the laptop operating system and extract the files into a folder
- Expand the “Other devices” section of the Device Manager and look for “Gadget Serial v2.4”. Right click on that and select the option to install the driver. Choose the option to browse for the driver and select the folder from the previous step.

Note: You may need to be signed in with an administrator account to install drivers.

- Using a standard terminal emulation program, select the set-up for serial terminal emulation and configure it as follows:
 - Baud Rate: 9600 bps
 - Word Length: 8 bits
 - Parity: None

- Stop Bits: 1 bit
- Test the connection:
 - Press the <Return> key on the console/laptop keyboard

The HSM should respond by displaying “Online>”, “Offline>”, or “Secure>” based on the position of the keys. The appearance of this prompt indicates that the correct communications between the console and the HSM have been established, but that no command has been entered.

6.2.11 Connect cables for payShield Manager

payShield Manager provides a secure GUI interface with an authenticated, encrypted connection allowing a full remote or local management of the payShield 10K.

Remote payShield Manager requires an Ethernet cable from the Management Port into your network.

If you are not using DHCP, then you may need to use the console to set up the static IP address for payShield Manager. (Refer to the *payShield Manager Quick start guide*. For the Console, refer to the *payShield 10K Console Guide*.)

6.2.12 Configure payShield Manager

Follow the instructions provided in the *payShield Manager Quick start guide* to complete the configuration of payShield Manager.

6.2.13 Configure the Host ports

Note: Depending upon the configuration connection required between the Host and the payShield 10K, you may require additional information from your Network or Systems Support Group in order to complete this step.

6.2.13.1 Configure the FICON Interface

The FICON interface is configured using either payShield Manager or the CH Console command. FICON should be selected as the active host interface – for example, by selecting the FICON option in the payShield Manager Configuration Tab Host settings option or specifying F in the CH Console command:

```
Host interface [[E]thernet, [F]icon] (E) : F <Return>
```

The following parameters are required to configure the interface:

Parameter	Type	Min	Max	Default	Explanation
Message header length	Numeric	-	-	-	The same as in Ethernet
Control Unit Image	Numeric	0	255	0	This is the control unit address defined in the mainframe I/O definition. (CUADD on CNTLUNIT statement.) *
Unit Address	Numeric	0	255	0	The starting unit address for this control unit. 16 devices are enumerated from this point. (UNITADD on CNTLUNIT statement.) *
Missing Interrupt Handler (mih) Minutes	Numeric	0	60	0	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.

* In most circumstances, installations will code 0 (the default) for both the Control Unit Image and the Unit Address.

Examples (using the Console)

Execute the Configure Host Port (CH) command:

Secure>CH

```
Please make a selection. The current setting is in parentheses.
Message header length [1-255] (4):
Disable host connections when no LMKs are installed? [Y/N] (N):
Host interface [[E]thernet, [F]icon] (F):F
Control Unit Image [0-255] (0): 1
Unit address [0-255] (0): 1
Missing Interrupt Handler (mih) Minutes [0-60] (0): 5
Save HOST settings to smart card? [Y/N]: N
To read the current configuration, use the QH command.
```

Secure>qh

```
Message header length: 04
Disable host connections when no LMKs are installed: NO
Protocol: FICON
Control Unit Image: 1
Control Unit Address: 1
Missing Interrupt Handler (mih): 5 minutes
```

Secure>

6.2.14 Test connections

The way in which you do this will vary, depending upon your system configuration; for example: Ethernet environment – issue a PING command (both from the payShield 10K to the Host, and from the Host to the payShield 10K).

The FICON board and transceivers can be tested using the FICONTEST Console command.

payShield Manager users can run this command from the payShield Manager virtual console. Note, that to run FICONTEST, you will need the loopback device provided with your transceiver.



6.2.15 Basic Installation Troubleshooting

If you are having difficulty in establishing communications between the payShield 10K and the Host, make the following checks.

Note: The LED indications will also assist in identifying issues; follow this link for LED details: [Section 6.2.8, "Connect cables and power on", on page 55](#).

- Confirm the presence of the FICON Interface:
 - Looking at the rear panel of the HSM and checking that there is a FICON interface. If no FICON interface is fitted, the FICON interface is replaced with a blanking plate.
 - Use the CH and QH Console commands or payShield Manager to confirm that FICON is configured.
- Run the VR Console command or payShield Manager to check that:
 - The serial number begins with a F
 - The “Host Configuration” entry includes the word “FICON”.
- If you cannot get the port into an online state at the switch:
 1. Check that the payShield 10K is in the Online state (i.e., both keylocks are in a vertical position).
 2. Check that you are using Port 1 of the payShield 10K FICON interface.
 3. Check that you have selected FICON as the Host interface (using the CH Console command or payShield Manager), and entered the correct parameters.
 4. Check that the optical transceivers, in the payShield 10K and the Host (or switch, etc.), that the HSM is connected to are using the same wavelength. The wavelength (850 nm or 1310nm) used by the payShield 10K transceiver is printed on the transceiver’s label.
 5. Check that the fiber optic cable being used is compatible with the transceiver.
 6. Check that the transceiver at the Host, switch, etc., supports at least one of the speed options supported by the payShield 10K transceiver – 2, 4, or 8 Gbps. Other speeds (e.g., 1 Gbps) will not work.

7. Check that the FICON interface is operating on the payShield 10K by connecting a loopback cable between the connectors on the transceiver. The green LED should light up permanently, and the yellow LED should blink 4 times repeatedly. Run the FICONTEST Console command.
 8. If using a switched fabric, check that the connecting switch has the connecting port type set to fabric port (F_port), auto-negotiation.
- If the port is online at the switch, but you cannot get paths or the device online:
 1. Check security or firmware issues with the switch. Some switches can be configured such that they will only allow a specific port to talk to a specific world-wide port name (WWPN). Some switches have been reported as having firmware issues which cause the same problem: once a given device with a WWPN is plugged into the switch, it will not talk to any other WWPN and shuts down, and the switch has to be re-booted.
 2. Check the domain ID in the IOGEN at the Host. (If other devices on other control units for the same CHID and switch are working, then the domain ID is not incorrect.)
 3. If the switch has a port offset, check that this has been used in the IOGEN for the control unit switch port, and has been entered in Hex.
 4. Check for correct zoning.
 5. Check that the device type for the payShield 10K has been set up as 3490 or Dummy.
 6. Check that the Control Unit Image set up at the HSM (e.g., using the CH Console command) matches the Control Unit Image in the IOGEN.
 7. Check that the range of Unit Addresses set up at the HSM (i.e., the 16 starting from the specified address) match those in the IOGEN.

6.3 Replacing the Transceivers

Note: If it is required to adapt a payShield 10K ordered with Shortwave transceivers to Longwave (or vice versa) this can be done by removing the supplied transceiver and replacing it with the required type. The specification of the replacement transceiver to be used can be obtained through Thales Support:

<https://supportportal.thalesgroup.com/csm>

A transceiver can be fitted as outlined below.

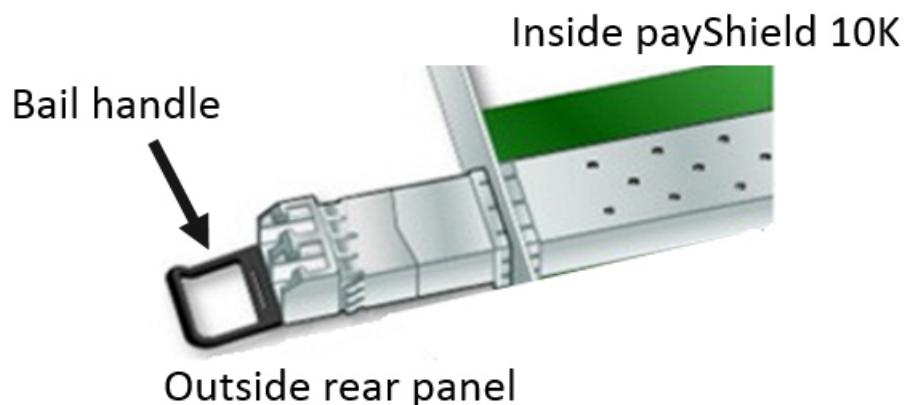
Note: SFPs are hot pluggable/swappable.

Important: Please note that:

- This is a delicate operation – take care not to damage the transceivers.
- Observe standard ESD (Electrostatic Discharge) precautions for handling electronic components.
- The fitted or replacement transceiver may be different from the type shown below.

1. To remove a transceiver, pull the bail (handle) out and down to release the latch and gently pull the transceiver out without forcing it: after the latch is released, the transceiver slides out easily.

The following diagram shows a transceiver partially extracted.



2. Store the removed transceiver in an ESD-safe place.
3. Install the new transceiver by sliding it into the housing. When the latch engages, it clicks.
4. Push the bail of the new transceiver back into place.

Note: Ensure that a dust plug is inserted into any port socket which does not have a transceiver fitted.

6.3.1 FICON Diagnostic Test

Refer to: [Section 6.2.14, “Test connections”, on page 60](#)

6.4 Device Emulation

The recommended emulation is for a DUMMY device running on a NOCHECK Control Unit, although 3490 tape drive emulation is also supported. Please note the device should NOT be defined as a 3490 on a z/OS system, as the operating system will issue requests to the device to check if a tape is mounted and, if so, what the tape volume serial number is.

6.5 Performance

6.5.1 Overview

The results of the performance tests undertaken by Thales are described in this section. To achieve maximum performance it is important to note that multiple connections must be made to payShield 10K and the graph shown below shows how performance varies with the number of devices used.

Note: For payShield 10K PS10-F, only one performance license is available – the Premium package at 2500 cps.

6.5.2 Test examples

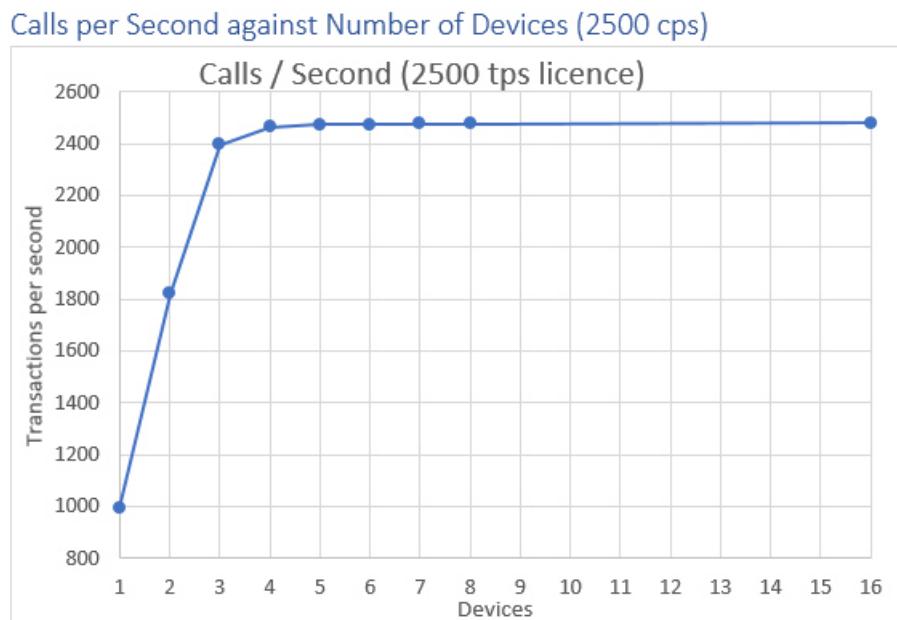
Performance testing of the payShield 10K PS10-F was undertaken to verify the performance of the product.

The tests included a variety of test data sets and the performance using the 'CA' Host Command against different numbers of concurrent connections to the payShield.

The following test configuration was used:

- Testing was performed using an LPAR on an IBM z13s (2965), with a single CPU and 4096MB of memory.
- payShield 10K PS10-F was at 16Gbps through a CISCO FICON switch.
- The CISCO FICON switch had 16Gbps ports between the mainframe and the server.
- Testing was performed using the Thales Secure Resource Manager (SRM) software v2.7, with custom test programs developed by Thales.
- The test system was a minimal z/OS configuration using z/OS 2.4 ADCCD November 2019 edition.

The graph below shows the number of devices used, the elapsed time and average number of calls per second. 32 jobs were used in the tests.



6.6 Security Resource Manager (SRM)

The Secure Resource Manager (SRM) is an optional software product from Thales which can more effectively manage estates of payShield 10K HSMs attached to IBM mainframes. It directs commands from multiple applications to the appropriate HSM.

FICON-enabled payShield 10Ks connect to the host application using the Thales SRM software for IBM hosts, subject to the following conditions:

SRM software version 2.6 or later must be used.

Where version 2.6 software is used, the following patches must be installed:

- SL26001
- SL26002
- SL26004

Where version 2.7 software is used, the following patches must be installed:

- SL27001
- SL27003

6.7 Z Series I/O Configuration for FICON-attached payShield 10K

This section discusses how a payShield 10K PS10-F should be configured for use on a z Series Mainframe, so that it can be used by applications running on an Operating System (usually z/OS) within that Mainframe.

This section is presented in four parts:

- Relationship between the payShield 10K configuration and the I/O Definition shows which parts of the I/O Definition need to match the HSM configuration, in order for the device to be accessible
- Relationship between the I/O Definition and the application shows how the application can address the HSM, specifically each of the logical devices provided by the HSM
- Relationship between the I/O Definition and the SRM Configuration demonstrates this relationship, using the z/OS SRM application as an example
- The example presents the specifications required to correctly configure a slightly more complicated example, where two HSM devices were attached to one z Series Mainframe and used by two different Operating Systems running on that Mainframe.

Note that the description and the example present standard configurations. Some users will require more complicated configurations, for example to allow the HSM to be shared between multiple Operating Systems. Specifying this for an HSM, is achieved in the same way as any similarly attached device, by adjusting the I/O Definition appropriately. So by reviewing the information presented here, users will have enough knowledge to configure the HSM in the way that they require.

6.7.1 Relationship between the HSM Configuration and the I/O Definition

z Series Mainframes see a FICON connected HSM as a Control Unit with associated logical devices. Like any such device, to configure this for use in a z Series Mainframe the I/O definition must be updated to:

- Define paths to the Control Unit
- Define the associated logical devices, which the executing operating system will reference

Paths to the Control Unit are specific to each installation and have no impact on the actual configuration of the HSM device.

By contrast, the Control Unit specification included in the I/O Definition and the HSM configuration must match. Specifically the Control Unit Address must match the Control Image specification and the Unit addresses must match the Control Unit Address. This relationship is shown in the following.

An example I/O definition for an HSM “Control Unit” is as follows.

```
CNTLUNIT CUNUMBR=02A0,PATH=(...),UNITADD=((00,16)),UNIT=DUMMY,
CUADD=00
```

In this case, the Control Unit is at address 0, and the 16 devices are defined starting at 0. Note that you should always define 16 devices and the type of control unit should be specified as DUMMY.

The HSM configuration which matches this I/O Definition is shown below. Note the colors which indicate the values that should match.

```
Message header length: 04
Protocol: FICON
Control Unit Image: 0
Control Unit Address: 0
Missing Interrupt Handler (mih): 0
```

The protocol must be specified as FICON. The header length will vary depending on the application that is using this HSM. Note that if the HSM is shared between applications, they must all use the same header length.

6.7.2 Relationship between the I/O Definition and Application

In addition to the control unit specification, the I/O Definition will also include the specification of an IODEVICE, which specifies how the Operating System will address and use the device. The IODEVICE specification also ties back to the Control Unit specification.

Here is a sample IODEVICE specification:

```
IODEVICE ADDRESS=(02A0,16),CUNUMBR=(02A0),UNIT=DUMMY,UNITADD=00
```

The most important part is the Address and the number that follows this address. In this case, the HSM device will be known to the Operating System as device 02A0 – 02AF. These 16 devices can be bought online and used individually as though they were distinct devices. However they are all managed by the one HSM unit. If that HSM unit is powered down, or disconnected, all 16 devices will fail at that time.

Other parts of the IODEVICE specification relate back to our previous Control Unit specification. Firstly the associated Control Unit is specified by the CUMNUMBER (in this case 02A0). The UNITADD matches back to the similarly named parameter on the Control Unit specification, and the quantity of devices specified (16) matches back to that specified in the UNITADD parameter on the Control Unit specification too.

6.7.3 Relationship between the I/O Definition and the SRM Configuration

The IBM Secure Resource Manager (SRM) available from Thales is an example of an application that can use FICON connected HSM devices from within the z/OS Operating system.

Using the IODEVICE specification presented previously, the z/OS system will provide access to devices using the following addresses: 02A0 – 02AF.

7 payShield Management Options

Thales recommends that payShield Manager is used to manage payShield 10K. payShield Manager provides a secure, authenticated connection allowing a full “remote console”.

payShield Manager is a web-based management application. Management is performed over the network using a web-based interface hosted on payShield. The operator can be either local or remote to the payShield 10K.

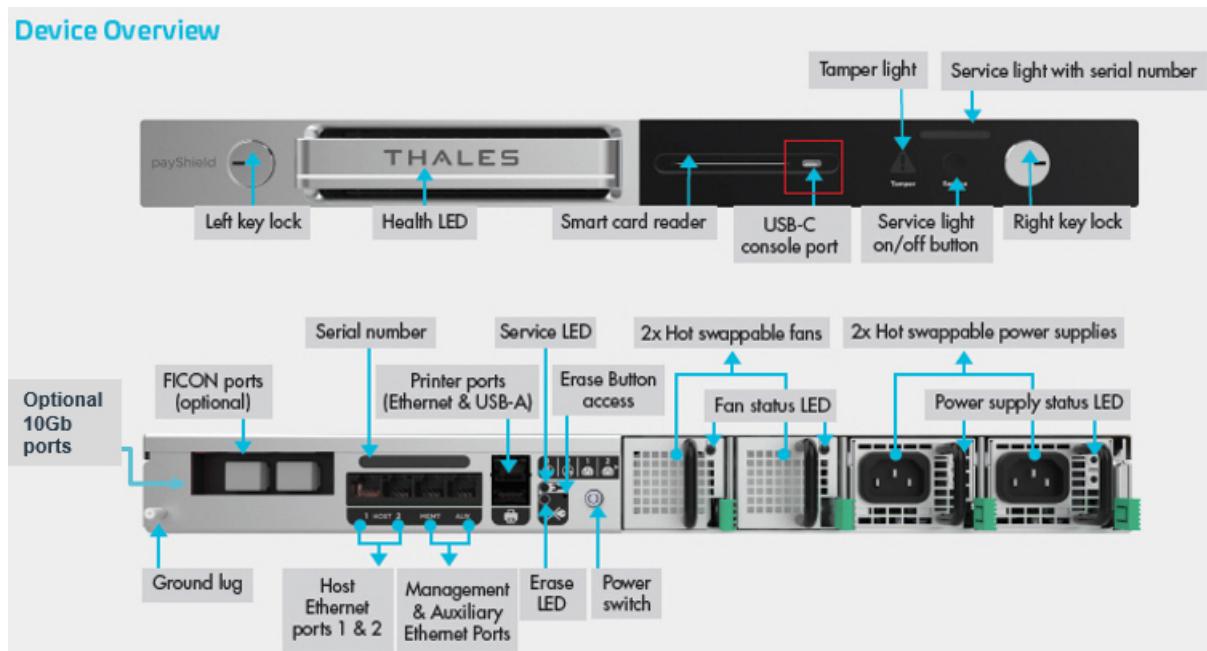
The key feature of using payShield Manager remotely is that it does not require a visit to the Data Center. Rather management is undertaken using a standard web-browser connecting to the payShield 10K over TCP/IP networks, where the payShield 10K is located within a protected corporate data center with multiple layers of security and access controls.

With a standard PC with a supported web-browser, together with the USB connected payShield Manager Reader and payShield Manager smart cards, users connect to the payShield 10K via HTTP(s) using a configured IP address or the HSM’s system name.

To use payShield Manager locally, the PC hosting payShield Manager is connected directly into the payShield 10K’s Ethernet management port. Local payShield Manager is included in all payShield 10K license packages.

To use payShield Manager remotely the PC hosting payShield Manager is connected remotely via the network again to the payShield 10K’s Ethernet management port. The Remote payShield Manager License is required to use this option.

payShield 10K can also be managed using the Console. Here the smart card reader on the front panel is used together with LMK Component Smart cards. The Console Commands are described in *payShield 10K Console Guide*.



8 Commission using payShield Manager

8.1 Introduction

This chapter describes how to commission the payShield 10K using payShield Manager. The same method is used whether you are commissioning locally or remotely.

The steps included take a payShield 10K installed in the Data Center, as described in [Chapter 9, “Using payShield Manager”](#), to a state ready for generating / loading the Local Master Key and updating the configuration – this is covered in [Chapter 9, “Using payShield Manager”](#).

8.2 Prerequisites

The following are required before starting the commissioning procedure:

- payShield 10K installed in a cabinet with the keys on the front panel set to “online” as covered in [Chapter 4, “Installation”](#).
- The payShield 10K serial number in order to use the default network name to access the device.
- PC or Workstation with the operating system / browser combinations supported by payShield Manager. The table that follows indicates the combinations of operating system and browser supported by payShield Manager in this release. It is possible that other combinations will work, either completely or partially, but this should not be relied upon. Please note that payShield Manager no longer supports Internet Explorer as this is no longer supported by Microsoft.

Operating System	Windows 10 64-bit	Linux Ubuntu 18 64-bit	MacOS Big Sur	Mac OS Ventura
Supported Browsers	Chrome 64-bit Firefox 64-bit Edge 64-bit	Chrome 64-bit Firefox 64-bit	Chrome 64-bit	Chrome 64-bit

- Administration permissions for the PC or Workstation to install drivers and update the configuration etc.
- payShield Manager USB attached smart card reader with PIN Pad
- payShield Manager smart cards in sufficient quantity to complete the commissioning process
- Popups are enable on your browser for the payShield Manager domain

8.3 Preparing for Commissioning

The following subsections define the steps that need to be taken before commissioning starts:

8.3.1 Configuring payShield 10K for Static IP (if required)

The payShield 10K management port is configured for DHCP when delivered, allowing it to be managed remotely following installation in the Data Center. If a Static IP address needs to be set up, this must be configured in the Data Center using the Console Commands before continuing. Refer to the *payShield 10K Console Guide*.

8.3.2 Install Smart Card Reader Driver

You may need to download the driver for your reader:

- 971-000136-001 – PS10-RMGT-RDR3 – payShield Manager Smart Card Reader – for Software V1.4A (1.8.3) and above –uses the Thales IDBridge CT700 Smart Card Reader with PIN Pad and is the recommended reader. The driver for Windows is: GemPcCCID.exe. The driver for Linux and MacOS is included with the operating systems.
- 971-700008-002 – HSM-RMGT-RDR2 – payShield HSM Manager Smart Card Reader – for all software versions – uses the cyberJack ® RFID comfort Smart Card Reader with PIN Pad.
The driver is:

<https://www.reiner-sct.com/support/support-anfrage/?productGroup=77304735&product=77304824&q=driver#choice4>

8.3.3 Check the Proxy Configuration

Your Internet browser will need to be configured to direct traffic through a proxy.

When you are configuring the browser proxy settings, click **Use this proxy server for all protocols**. For Microsoft Edge and Mozilla Firefox, this setting is via a check box.

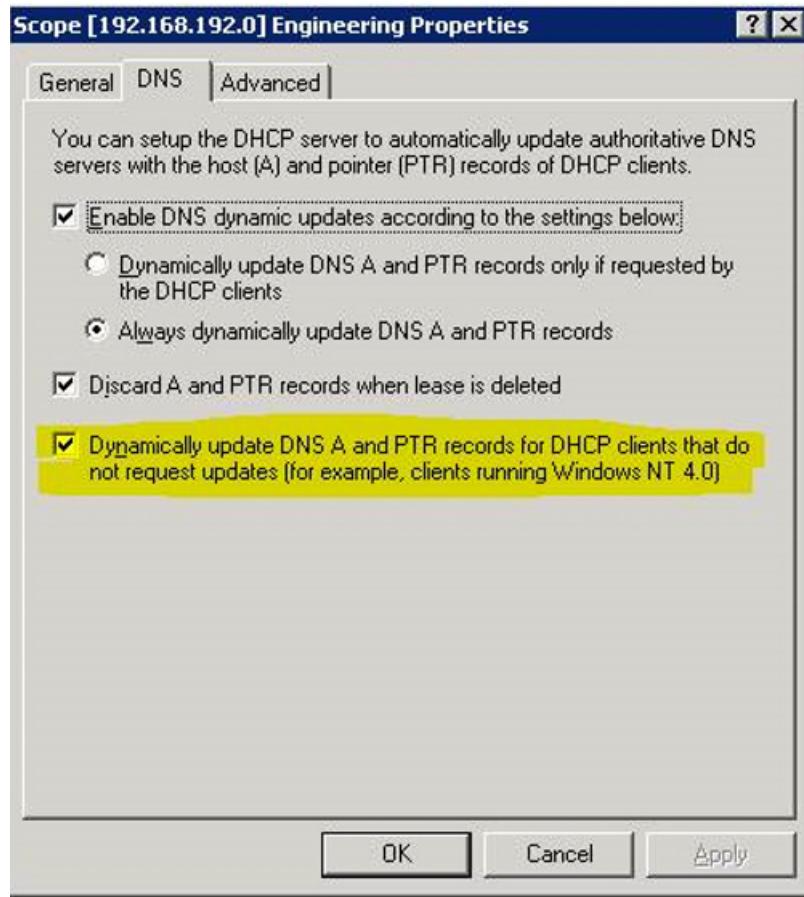
If this setting is not selected, the payShield Manager Welcome page will display, but you will not be able to login.

8.3.4 Configure DNS

When configuring the DNS in a Windows Server environment, select the setting:

- Dynamically update DNS A and PTR records for DHCP clients that do not request updates.

Note: The DHCP request from the payShield 10K is going to request an IP address and also request a name (with -h option on DHCP client). This option pushes the name and assigned IP address to the DNS.



8.3.5 Connect to the Network

Connect the laptop or Workstation to be used for payShield Manager to payShield 10K using Ethernet as follows:

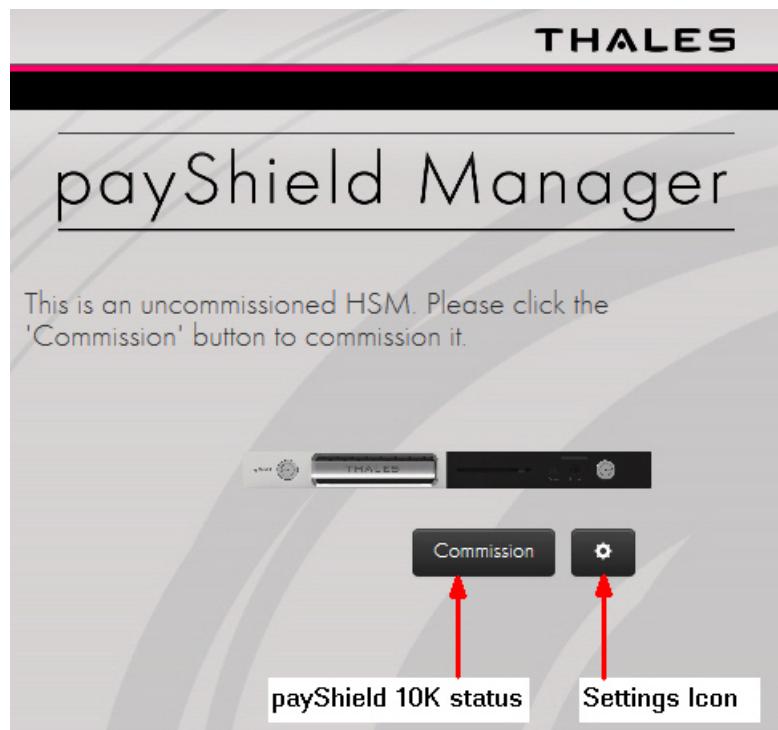
- To use payShield Manager locally, the PC hosting payShield Manager is connected directly into the payShield 10K's Ethernet management port on the rear panel. Local payShield Manager is included in all payShield 10K license packages.
- To use payShield Manager remotely, the PC hosting payShield Manager is connected remotely via the network again to the payShield 10K's Ethernet management port. The Remote payShield Manager License is required to use this option.

8.4 Connecting, Installing Browser Extensions, Configuring Smart Card Reader

8.4.1 Connecting to payShield 10K

To connect to payShield 10K using payShield Manager and display the “landing page” proceed as follows:

From your laptop / workstation to be used for payShield Manager, enter the network name or the IP address assigned to access the page. The landing page below displays:



Notes:

- The default network interface name for payShield 10K is “<serial number>-mgmt”
- Refreshing the landing page can repair most connectivity issues with accessing the landing page. However, once logged in, refreshing any page will end the current session and you will be required to log back in.
- The Settings/Tools Icon: Allows card reader configuration, the TLS certificate to be downloaded, and the Smart Card to be inspected. Additionally, selecting the icon displays the bridge’s current version.
- If you are already commissioned, simply insert a right or left RACC into the connected Smart Card reader, click Log In and enter your PIN. If the PIN is correct an authentication process will begin which will take several seconds to complete and you can use the functionality described in [Chapter 9, “Using payShield Manager”](#).

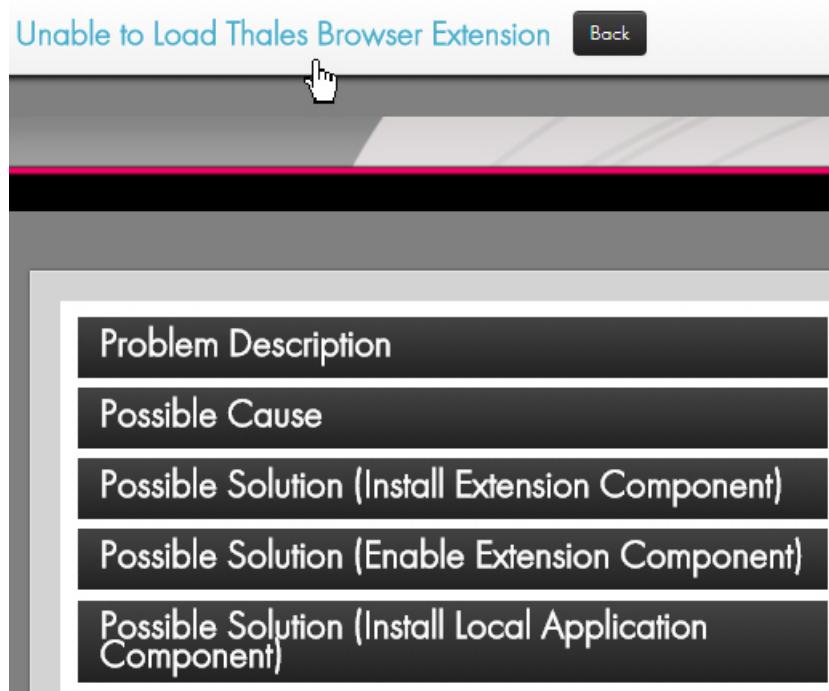
Note: When using MacOS Catalina there are a few additional steps to be carried out before the landing page can be accessed. These are described in [Section 8.6, “Using payShield Manager with MacOS Catalina”, on page 96](#).

8.4.2 Installing Thales Browser Extensions

From the landing page, click **Commission**.

If the **Unable to load Thales Browser Extension** message displays (as shown in the screen shot below), follow the steps below.

Otherwise, continue to [Section 8.4.3, “Configure the Smart Card reader”, on page 77](#).



Note the following procedure is for Chrome. For other Internet browsers, payShield Manager will guide the user through a similar but slightly different process to load the required extensions.

Additional actions are needed to load the Thales Browser Extension. Follow the prompts as described below.

1. Open the **Problem Description** and **Possible Cause** drop downs for insight.
2. Open the **Possible Solution** drop down menus.
3. Follow the instructions under **Possible Solution (Install Extension Component)**.

Possible Solution (Install Extension Component)

The problem may be fixed by installing the Browser Extension Component (if it is not already installed):

1. Start the **Extensions** configuration page by clicking on $\equiv \rightarrow \text{Settings} \rightarrow \text{Extensions}$
2. Try to locate the extension labeled **Thales Smart Card Bridge**. If present, then the extension is already loaded, so skip the next steps and proceed.
3. Navigate to the **Chrome Web Store**.
4. Search for the extension named **Thales Smart Card Bridge** and install it.

Afterwards, return to the login screen by clicking the 'Back' button on this page and try again.

4. Follow the instructions under **Possible Solution (Enable Extension Component)**.

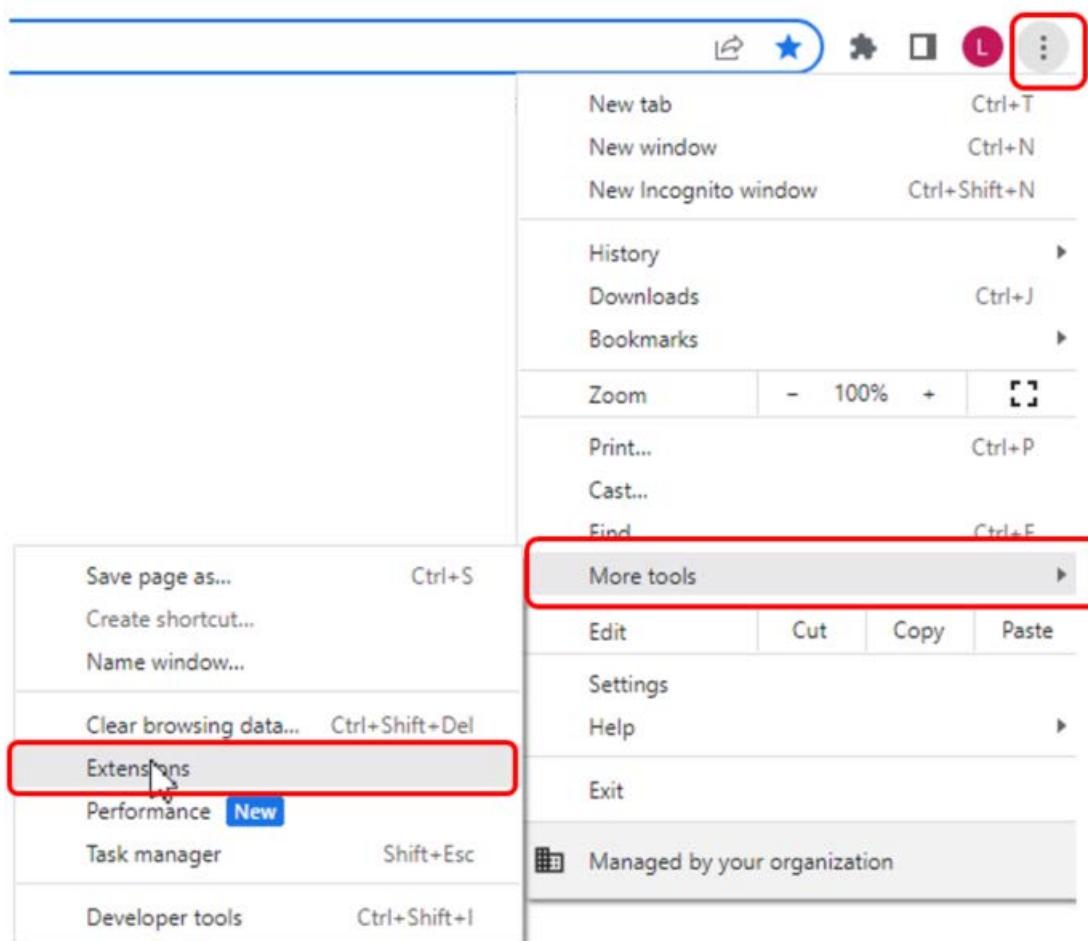
Possible Solution (Enable Extension Component)

The problem may be fixed by enabling the Browser Extension Component (if it is disabled):

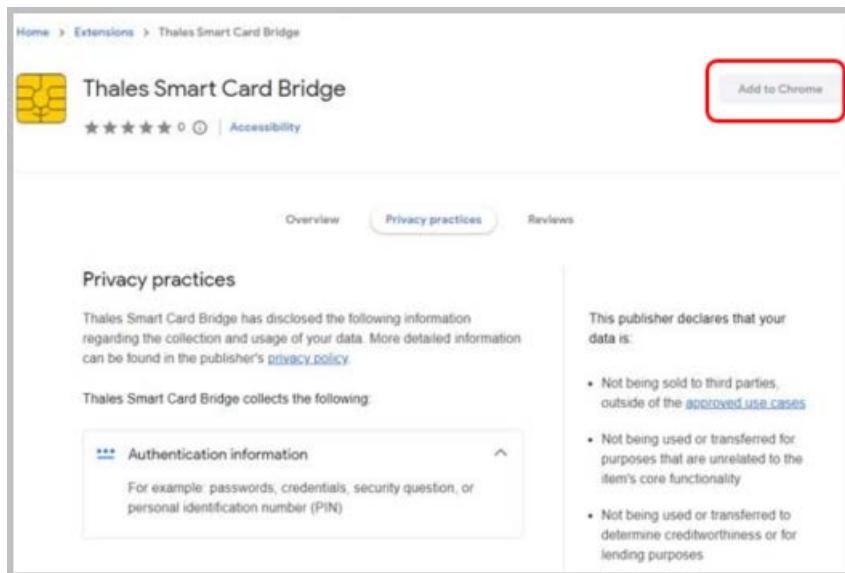
1. Start the **Extensions** configuration page by clicking on $\equiv \rightarrow \text{Settings} \rightarrow \text{Extensions}$
2. Locate the extension labeled **Thales Smart Card Bridge**. If not found, then see the previous "Possible Solution" describing how to install it.
3. Ensure that the **Enabled** checkbox is checked.

Afterwards, return to the login screen by clicking the 'Back' button on this page and try again.

a) Navigate to **Extensions**:



- b) Scroll through the list of Extensions, if a Thales Extension is not present, you will need to add it.:
- c) Open the Chrome Web Store:
<https://chrome.google.com/webstore/category/extensions>
- d) In the left column, click **Extensions**.
- e) Enter **Thales** into the search bar; the Thales Smart Card Bridge page opens.

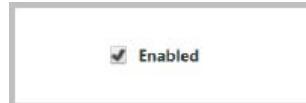


f) Click **Add to Chrome**.

g) Click **Add extension**.

A confirmation message displays.

- To confirm that the extension is enabled, navigate to: **More Tools > Extensions**
- Scroll to the Thales extension and confirm that the Enabled box is checked.



5. Follow the instructions under **Possible Solutions (Install the Local Application Component)**.

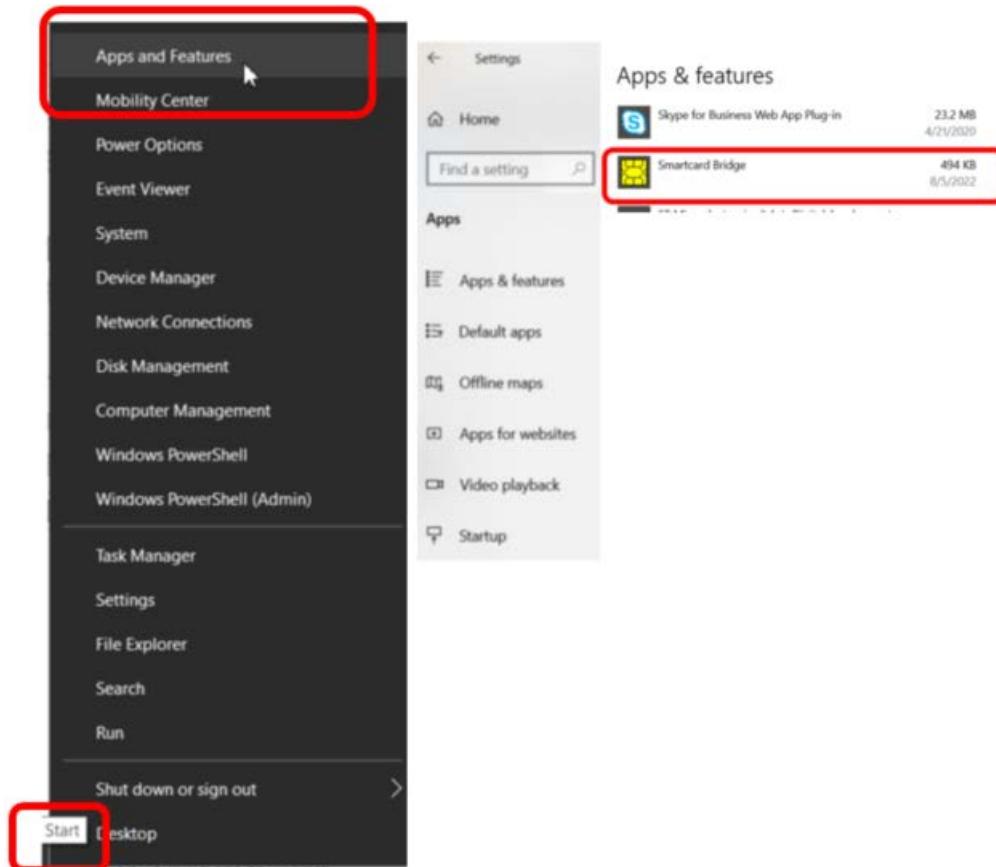
Possible Solution (Install Local Application Component)

The problem may be fixed by (re)installing the Local Application Component of the Thales Smart Card Bridge

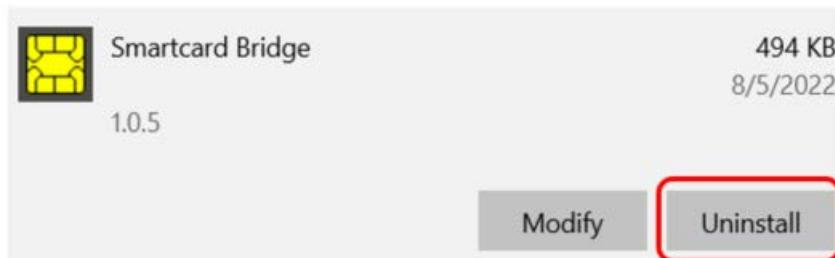
- Start the Control Panel Programs and Features via one of the following ways:
 - Run the command `control -name Microsoft.ProgramsAndFeatures`
 - Click on `Start` → `Control Panel` → `Programs` → `Programs and Features`
- Locate the program named `Smartcard Bridge`. If it exists, then select it and uninstall it by clicking `Uninstall`.
- Click on this button to download the Local Application Component of the `Thales Smart Card Bridge`
- When asked if you want to run `ThalesScBridge_ChromeFirefox.msi`, click `Run` to install it.

Afterwards, return to the login screen by clicking the 'Back' button on this page and try again.

- Navigate to **Start > Apps and Features > Smartcard Bridge.**



- Click **Uninstall**.



- If you find an existing Smart Card Bridge, select it and click to **Uninstall**.
- Return to your payShield Manager window.
- Click the blue button as shown below to download the ThalesScBridge_ChromeFoxFire.msi.

[Thales Smart Card Bridge](#)

- Click **Run** to start the Smart Card Bridge Setup Wizard.

- Click **Next**
- Click **Next** to confirm.
- Follow the instructions as prompted.
- Click Back to return to the payShield Landing page.



- Close your payShield session.

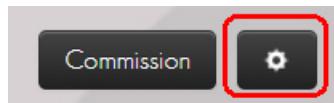
6. From your Internet browser, enter the network name or IP address of your payShield.
Example:



The landing page opens.

8.4.3 Configure the Smart Card reader

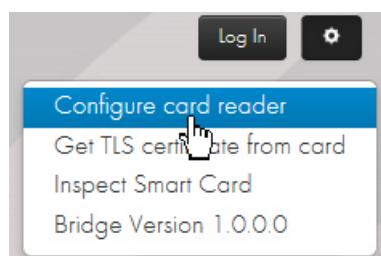
1. From the landing page, click on the **Settings** icon.



2. Confirm that the pop-up menu displays:

Bridge Version 1.0.0.0

3. Click **Configure card reader**.



The Change Default Smart Card Terminal window opens.

Change Default Smart Card Terminal

The following table shows the smart card terminals detected on this computer. The radio buttons in the right column show which one is used by this application. You may select a different card terminal by clicking a different radio button.

Card Terminal Name	Card Present	Secure PIN Entry	Selected
Broadcom Corp Contacted SmartCard 0			<input checked="" type="radio"/>
REINER SCT cyberJack secoder TLS USB 1		✓	<input type="radio"/>

Done

Note: In the image above, the PC has an internal Smart Card reader, for example: Smart Card 0. **Do not Click** this internal Smart Card reader. **It is not a trusted verification device.**

In the example above, **REINER SCT cyberJack secoder TLS USB1** is the trusted verification device.

Note: If after selecting the trusted verification Smart Card reader, you unplug the reader from your PC and/or reboot, you may need to come back and repeat this selection process.

4. Select the trusted verification device.

5. Click **Done**.

You are returned to the landing page.

8.5 Commissioning payShield 10K

This section describes the steps required to complete the commissioning of the payShield 10K ready for LMK generation / LMK installation and configuration.

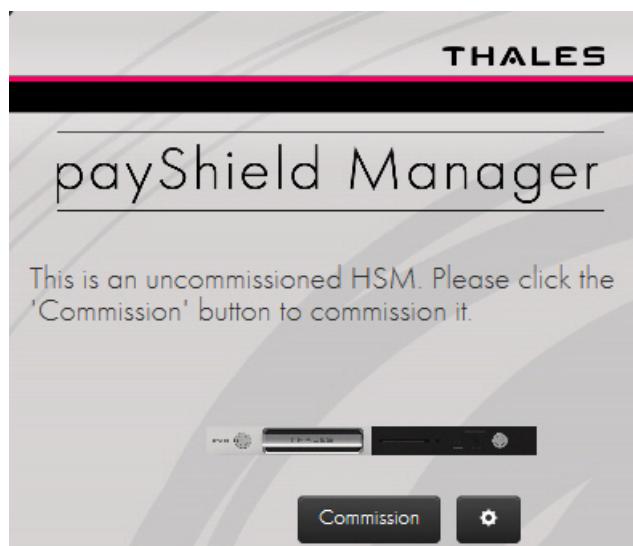
Table 3 *Commissioning Checklist*

Step	Task	Go to Section	DONE
1.	Load a Security Domain: <ul style="list-style-type: none"> • Install an existing security domain. This can be a payShield 9000 domain. OR: • Create a new security domain. 	<ul style="list-style-type: none"> • Section 8.5.3, “Load the Security Domain”, on page 85 • Section 8.5.2, “Create a new Security Domain”, on page 80 	

Table 3 Commissioning Checklist

Step	Task	Go to Section	DONE
2.	Set the HSM Recovery Key (HRK) passphrases.	Section 8.5.4, “Set HSM Recovery Key (HRK) passphrases”, on page 90	
3.	Create left and right key RACCs.	Section 8.5.5, “Create Left and Right Remote Access Control key cards”, on page 91	
4.	Create your trusted officers/authorizing officers.	Section 9.3.3, “Operational Tab”, on page 108	

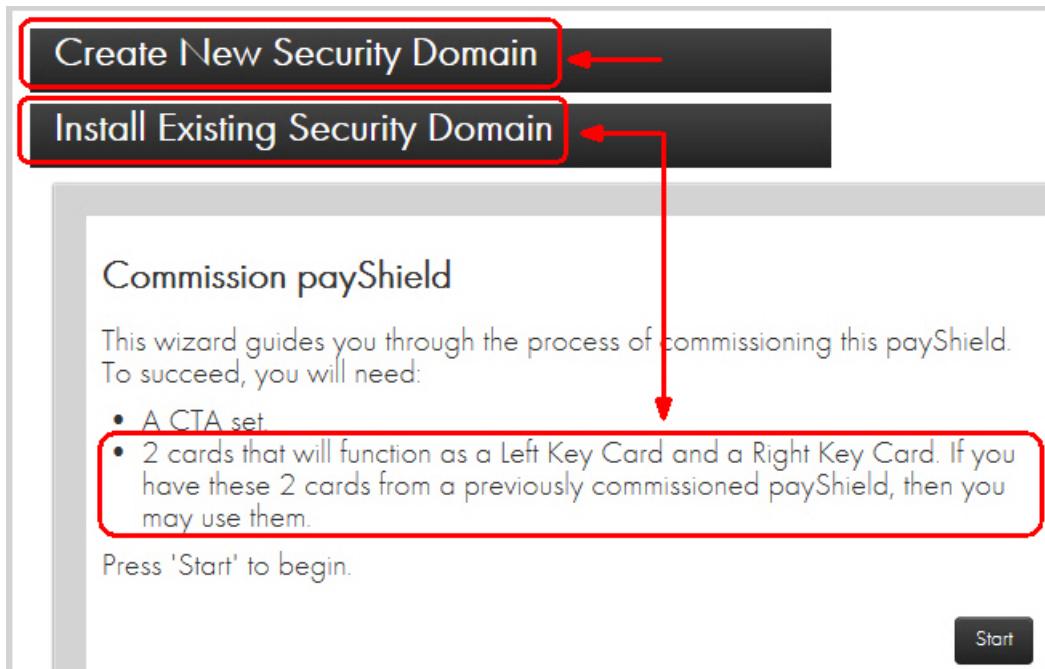
8.5.1 Open the Commissioning Wizard page



1. Click **Commission**.

The payShield Manager's **Commission HSM** wizard landing page opens.

From the landing page you have two options:



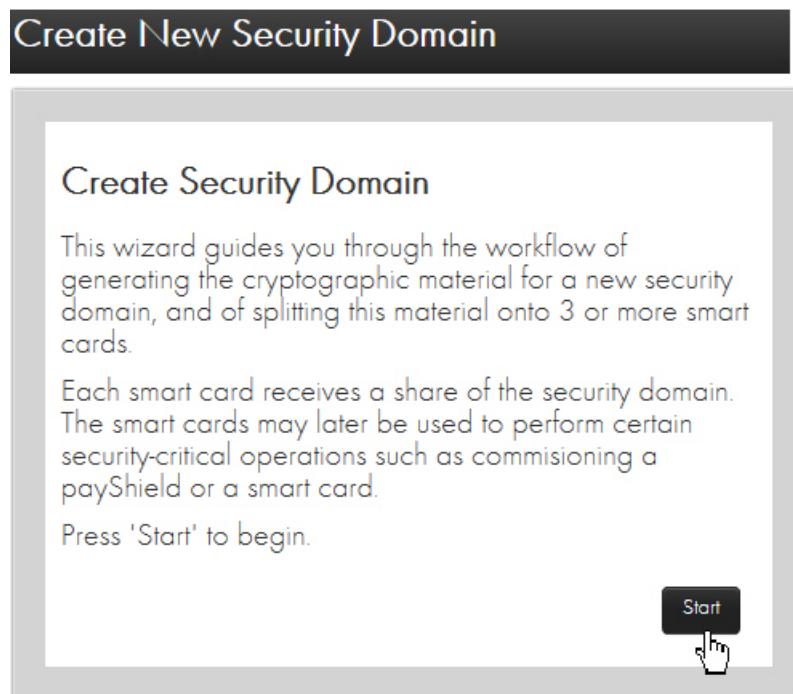
- If you already have a Security Domain (i.e., you have previously created a security domain with these cards), you are ready to install, i.e., continue to [Section 8.5.3, “Load the Security Domain”, on page 85](#).
- If you are unsure of the status of your cards and prefer to create a new security domain, i.e., continue to [Section 8.5.2, “Create a new Security Domain”, on page 80](#).

Note: When re-using existing Smart Cards, you must know the PIN. You will continue to use the existing PIN. The system will not prompt you to create a new PIN. The existing PIN is not erased.

8.5.2 Create a new Security Domain

Note: A Security Domain is made up of any number of HSMs and a set of Remote Access Cards.

1. Expand **Create New Security Domain**.



2. Click **Start**.

The **Security Domain Parameters** window displays.

3. Enter your parameters.

Attention: When determining the total number of security domain shares, carefully contemplate the size of the quorum.

Security Domain Parameters	
Enter the details for your security domain.	
Total Number of Security Domain Shares (3 - 9)	<input type="text" value="8"/>
Size of Security Domain Shares Quorum (3 - 8)	<input type="text" value="3"/>

For example, if the security domain is shared over 8 Smart Cards, and the quorum is set to 3, any three security officers out of the eight would need to be present to rebuild the Customer Trust Authority (CTA).

If the security domain is **shared over just 3 Smart Cards**, for example, there is less flexibility. The **same three security officers** would need to be readily available.

- Total Number of Security Domain Shares:

This is the number of Smart Cards onto which the CTA shares will be distributed. Valid values are 3-9.

- **Size of Security Domain Shares Quorum:**

This is the number of Smart Cards holding CTA shares that must be present in order to reassemble a CTA to perform various operations (including commissioning a payShield). The minimum value is 3.

- **Country, State, Locality, Organization, Common Name, Unit, Email:**

These are parameters that are included in the X.509 certificate corresponding to the CTA. The Common Name is the only required parameter and should concisely describe the security domain.

Security Domain Parameters

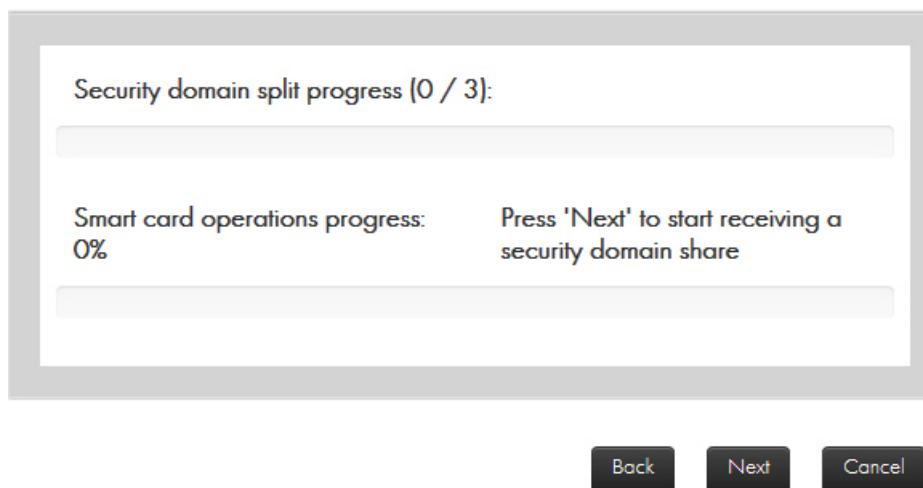
Enter the details for your security domain.

Total Number of Security Domain Shares (3 - 9)	3
Size of Security Domain Shares Quorum (3 - 3)	3
Country	US
State	FL
Locality	Plantation
Organization	System Test
Unit	ST-12
Common Name	SystemTest12
Email	admin1@thalesesec.com 

Next **Cancel**

4. Click **Next**.
5. Follow the wizard instructions to commission each Smart Card (i.e., assign key shares to each security officer's Smart Card).

Create Security Domain



Note: Each Smart Card will hold a share of the CTA.

6. Click **Next**.
7. Follow the prompt and insert your Smart Card into your Smart Card reader.

Create Security Domain

Insert a smart card to receive a CTA share into:
 <Smart Card Reader> SmartCard 0

Cancel

Note: If your Smart Card is brand new, continue to Step e.

- a) If the system detects that you have **already commissioned the Smart Card**, you are alerted:

Create Security Domain

The smart card is commissioned. If you proceed, all information on it WILL BE LOST. Is it OK to recommission the smart card?

OK Cancel

Attention: If you Click **OK**, information on the card will be lost **but the original PIN remains**. Clicking OK does not erase the PIN.

- b) Click **OK**.

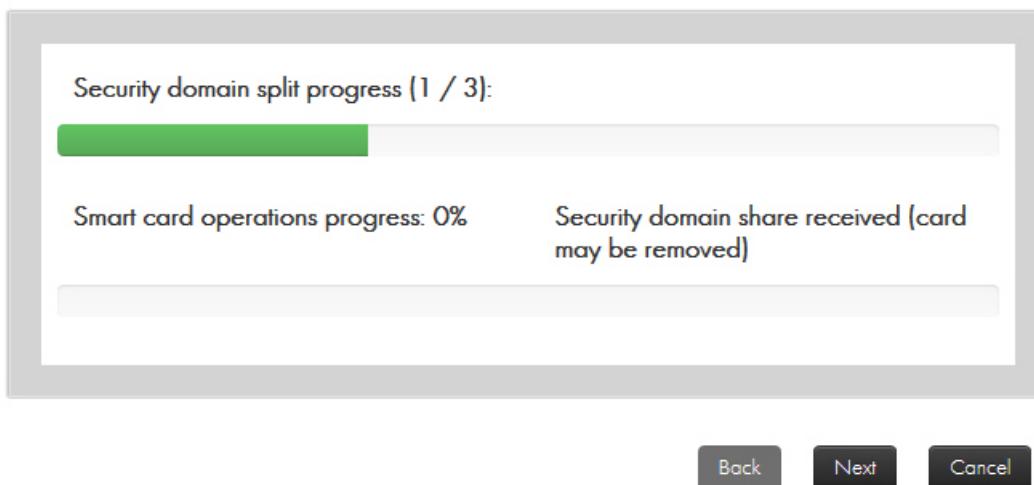
The system prompts for the **original PIN**.

Create Security Domain

Enter PIN via the smart card terminal keypad.

- c) Enter the original PIN.
 - d) Press **OK** on the card reader.
- The system prompts for a new PIN.
- e) Enter a new PIN (for example, a 6-digit PIN).
 - f) Press **OK** on the card reader.
 - g) Enter the new PIN again to confirm.
 - h) Press **OK** on the card reader.

Create Security Domain



The system will display **Security domain share received (card may be removed)**.

- i) Click **Next**.
- j) Remove the card and repeat the process for each card (i.e., for each security officer).
- k) After the final security officer has confirmed a PIN, click **Finish**.

At this point a set of security domain credentials, i.e., a Customer Trust Authority (CTA), has been created and split into some number of Smart Cards with each trusted officer holding one share.

Note: This CTA can be loaded into any uncommissioned HSM.

It is important to note that these cards are critical in the remote management process. They are required each time an HSM or a Smart Card is added to the security domain.

Note: It is a best practice to back up these cards and store the backups in a secure off-site location.

8.5.3 Load the Security Domain

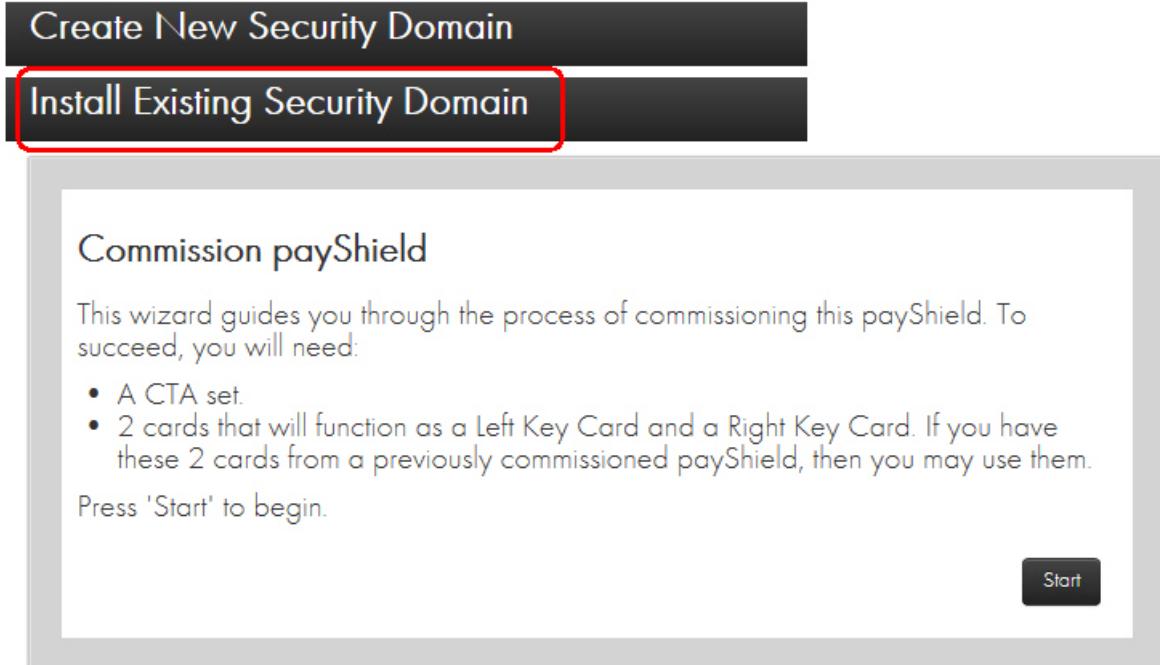
When you load a Security Domain, you are associating your payShield to that particular domain. You can associate the payShield with the newly created Security Domain (just created by following [Section 8.5.2, "Create a new Security Domain", on page 80](#)) or you can add this payShield to an existing Security Domain of your choice.

Prerequisites:

- The Smart Cards that make up the Security Domain
- 2 Smart Cards (that will function as a Left Key Card and a Right Key Card)

Note: If you have these cards from a previously commissioned payShield, you may use them.

1. Expand the **Install Existing Security Domain** accordion.



2. Click **Start**.

3. Each security officer performs the following:

- Place their Smart Card in the reader.

Load Security Domain

Insert a smart card with a CTA share into:
OMNIKEY CardMan 3821 0

Cancel

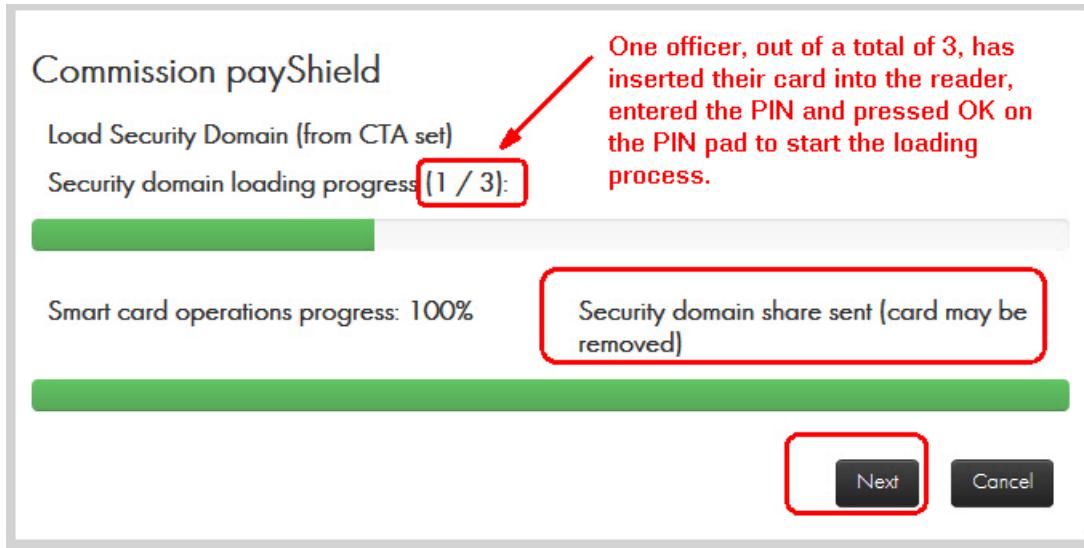
System prompts:

Load Security Domain

Enter PIN via the smart card terminal keypad.

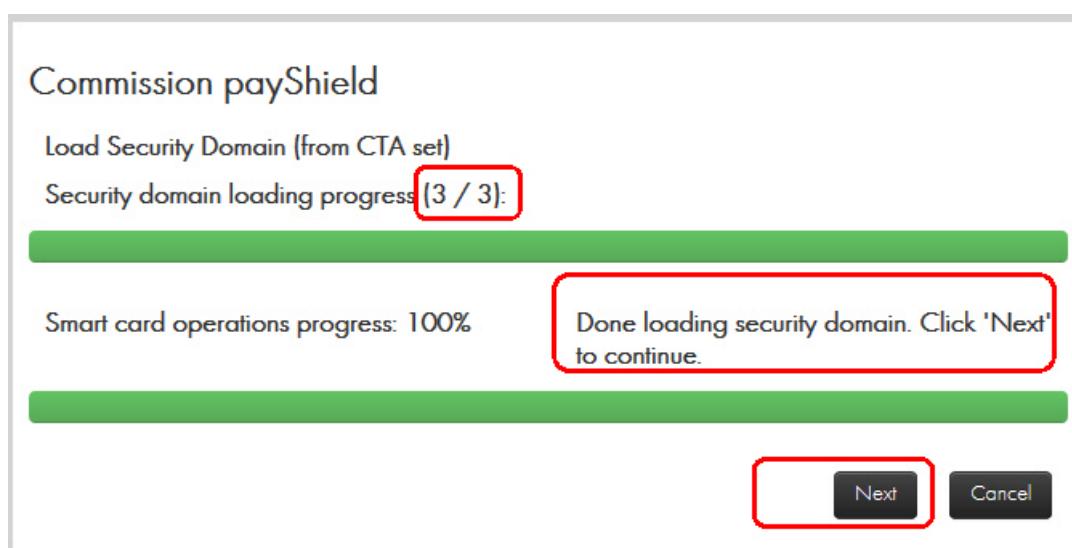
- Enter PIN.
- Click **OK** on the PIN pad.

The system displays:



4. Remove card and click **Next**.
5. Repeat the steps above for security officer.

Note: As each officer enters their Smart Card, a key share is loaded into the domain.



- When done, click **Next**.

The system displays:

Security Domain Parameters	
Total Number of Security Domain Shares	3
Size of Security Domain Shares Quorum	3
Country	us
State	Fl
Locality	Plantation
Organization	Documentation
Unit	
Common Name	tech-writer-thalesesec.com
Email	support@thalesesec.com

Next Cancel

7. Click **Next**.

The system displays:

Commission payShield

Download TLS Certificate

After the commissioning the payShield via this wizard, by default, subsequent TLS connections to the payShield will be secured with a new TLS certificate that the payShield presents to your browser, and that your browser verifies by following a certificate chain of trust to a trust anchor's certificate. The trust anchor's certificate is available on your smart cards and may be downloaded now.

Please press the 'Download' button to download the trust anchor certificate to a local file.

[Download Certificate !\[\]\(5fc8d2a6599355e04b49efe83b24f838_img.jpg\)](#)

After downloading the certificate and after commissioning this payShield, please ask your computer administrator to configure your browser to trust this certificate as a trust anchor. Thus, subsequent TLS connections to this payShield (and all other payShields commissioned with this set of smart cards) will be trusted by your browser.

[Next](#)

[Cancel](#)

This certificate can then be imported into the browser in order to trust subsequent TLS connections to the commissioned payShield. Depending on your organization's IT policy, a PC administrator may be required to perform this configuration.

Note: If you do not need to Download the Certificate:

- Continue to [Section 8.5.5, “Create Left and Right Remote Access Control key cards”, on page 91.](#)

8. Click **Download Certificate to download the certificate.**

The system displays:

Get TLS Certificate from Smart Card

Insert your smart card into:
OMNIKEY CardMan 3821 0

[Cancel](#)

- a) Insert your Smart Card.
- b) Enter your PIN.

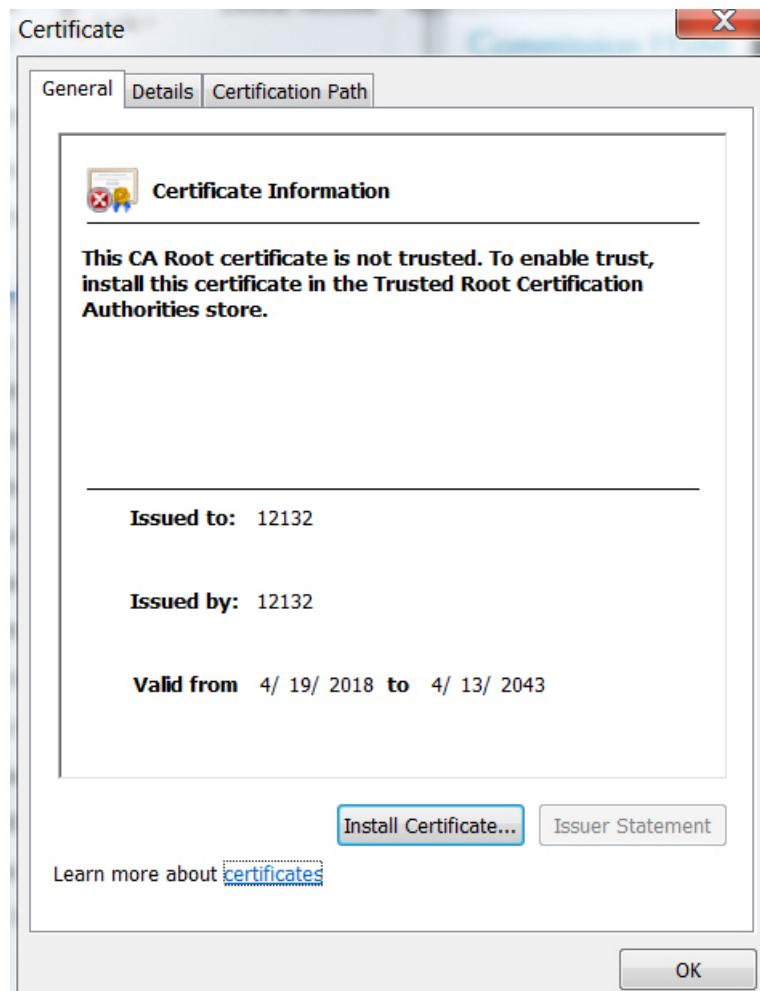
- c) Press **OK**.

The system displays (example):



- d) Save your file to an appropriate location.

- e) Open the certificate for details.



Note: For additional data, open the **Details** tab and the **Certification Path** tab.

- f) Click **Install Certificate**.

The Certificate Import Wizard opens.

- g) Follow the prompts.

9. Click **OK**.

8.5.4 Set HSM Recovery Key (HRK) passphrases

Note: You cannot use any HRK that was previously attempted to be set within the last 10 attempts. This encompasses all attempts.

- If you do not have HRK passphrases:
 - The system prompts you to create them. Continue to Step 1 below.
- If you already have HRK passphrases:
 - The system prompts you to create your Left Key Card. Continue to [Section 8.5.5, “Create Left and Right Remote Access Control key cards”, on page 91](#).

1. Enter the HRK passphrases two times.

The HRK passphrase must contain at least:

- 2 uppercase characters
- 2 lowercase characters
- 2 digits
- 2 symbols

Commission payShield

Enter HRK Passphrases

We now need to set the initial HRK passphrases. Please type them in the text boxes below.

To send them to the payShield, we will need to encrypt them with a smart card commissioned under this security domain (e.g. a security domain share, or a Key Card that was previously commissioned under this same security domain while commissioning another payShield).

HRK Passphrase 1:

HRK Passphrase 2:

Back Next Cancel

2. Click **Next**.

The system displays:

Commission payShield

Enter PIN via the smart card terminal keypad.

3. Enter a PIN.

Note: Although the system will accept a minimum PIN length of 6 digits, PINs MUST consist of 8 or more digits to align with the practices identified in the *payShield 10K Security Manual*.

4. Remove the Smart Card.

The system prompts you to Designate/Commission the Left Key Card.

8.5.5 Create Left and Right Remote Access Control key cards

If you already have Left and Right key cards, i.e., cards that have been created on a payShield 9000, you may use them.

1. Insert a Smart Card into the Smart Card reader.

Commission payShield

Designate/Commission the Left Key Card

We must now designate a smart card that will be used as a Left Key Card for logging into this payShield. You will need either:

- A Key Card that was previously commissioned under this same security domain (e.g. while commissioning a different HSM).
- A blank card that we will commission under this security domain.



2. Click **Next**.

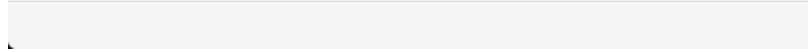
Commission payShield

Insert your smart card into:
OMNIKEY CardMan 3821 0

The system displays:

Commission payShield

Enter PIN via the smart card terminal keypad.



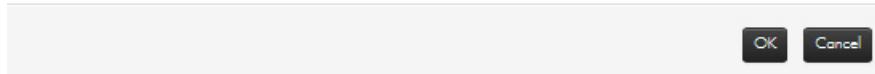
Note: PINs are entered via the Smart Card terminal keypad. Remember to press **OK** after entering a PIN.

3. Enter the PIN.
4. Press **OK**.

The system displays:

Prepare Key RACC

The card is already commissioned to a different security domain. Do you want to recommission the card? This will destroy the CTA share currently on the card.



5. Click **OK**.

Commission payShield

Designate/Commission the Left Key Card

We must now designate a smart card that will be used as a Left Key Card for logging into this payShield. You will need either:

- A Key Card that was previously commissioned under this same security domain (e.g. while commissioning a different HSM).
- A blank card that we will commission under this security domain.

Smart card operations progress: 100%

Left Key Smart Card 5268028274068542
successfully prepared. Smart card may be
removed.



Next **Cancel**

-
6. Enter a new PIN.
 7. Press **OK**.
 8. Click **Next**.

The system is ready to create the right key card.

Commission payShield

Designate/Commission the Right Key Card

We must now designate a smart card that will be used as a Right Key Card for logging into this payShield.
You will need either:

- A Key Card that was previously commissioned under this same security domain (e.g. while commissioning a different HSM).
- A blank card that we will commission under this security domain.

Next

Cancel

9. Click **Next**.

10. Insert the Smart Card into the reader.

Commission payShield

Enter PIN via the smart card terminal keypad.

11. Enter the PIN.

12. Press **OK**.

13. Insert the card into the Smart Card reader.

The system prompts

Prepare Key RACC

The card is already commissioned to a different security domain. Do you want to recommission the card?

OK

Cancel

14. Click **OK**.

The system starts to process.

Commission payShield

Designate/Commission the Right Key Card

We must now designate a smart card that will be used as a Right Key Card for logging into this payShield. You will need either:

- A Key Card that was previously commissioned under this same security domain (e.g. while commissioning a different HSM).
- A blank card that we will commission under this security domain.

Smart card operations progress: 3%

Generate session keys on card



Next

Cancel

The system prompts completion.

Commission payShield

Designate/Commission the Right Key Card

We must now designate a smart card that will be used as a Right Key Card for logging into this payShield. You will need either:

- A Key Card that was previously commissioned under this same security domain (e.g. while commissioning a different HSM).
- A blank card that we will commission under this security domain.

Smart card operations progress: 100%

Right Key Smart Card 5268027567068542
successfully prepared. Smart card may be
removed.



Next

Cancel

15. Remove the Smart Card.

16. Click **Next**.

Commission payShield

Finalize payShield Commissioning

We can now commission this payShield. The following Key Cards have been designated

- Left Key: 5268028274068542
- Right Key: 5268027567068542

Please take note of this information and/or mark the cards appropriately.

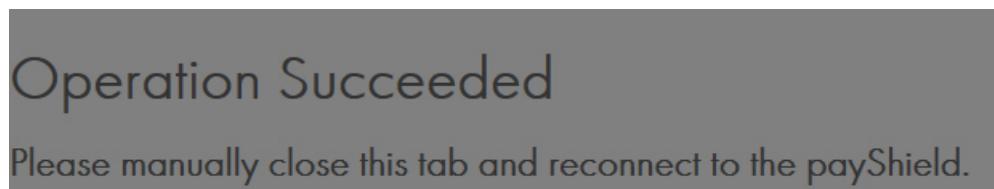
Commissioning progress: 100%

Commissioning complete. Press 'Finish' to close this page. You will need to reconnect in a few seconds.

Finish

17. Click **Finish**.

The system displays:



18. Restart your Internet browser, enter the IP address associated with your HSM.

The system displays:



8.5.6 Adding Additional Warranted HSMs to the Security Domain

New payShield HSMs that have Thales warranting on them can be added by using the instructions for Remote Commissioning of a warranted payShield.

1. Log into payShield Manager using the address of the new HSM to be commissioned.
2. Select the **Commission** when it comes up on the browser.
3. Remotely load the security domain (CTA) when prompted by the wizard.
4. Set the HRK passphrase for the HSM, when prompted by the wizard.

Passphrases require the following:

- At least 2 upper case characters
 - At least 2 lower case characters
 - At least 2 numbers
 - At least 2 special characters
5. Create (or sign existing) left and right key RACCs. If a set of cards is used for each individual HSM, then they will be commissioned first.
 6. Restart the web-browser.

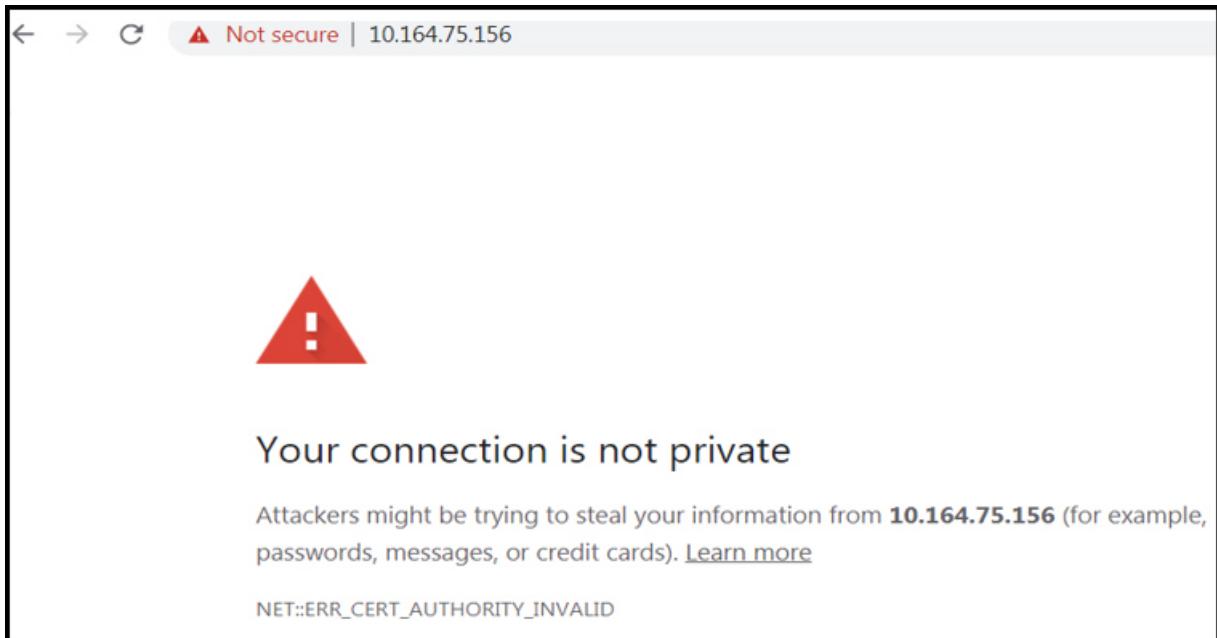
Follow this link for additional information: [Chapter 9, “Using payShield Manager”](#).

8.6 Using payShield Manager with MacOS Catalina

The following steps are required to be undertaken when using payShield Manager with MacOS Catalina Version 10.15.7 and above.

The procedure describes the steps required using Google Chrome Version 86.0.4240.111. The procedure may vary when using other versions of Chrome or other browsers.

When accessing the landing page, if the following message is shown by the browser, carry out the following steps:

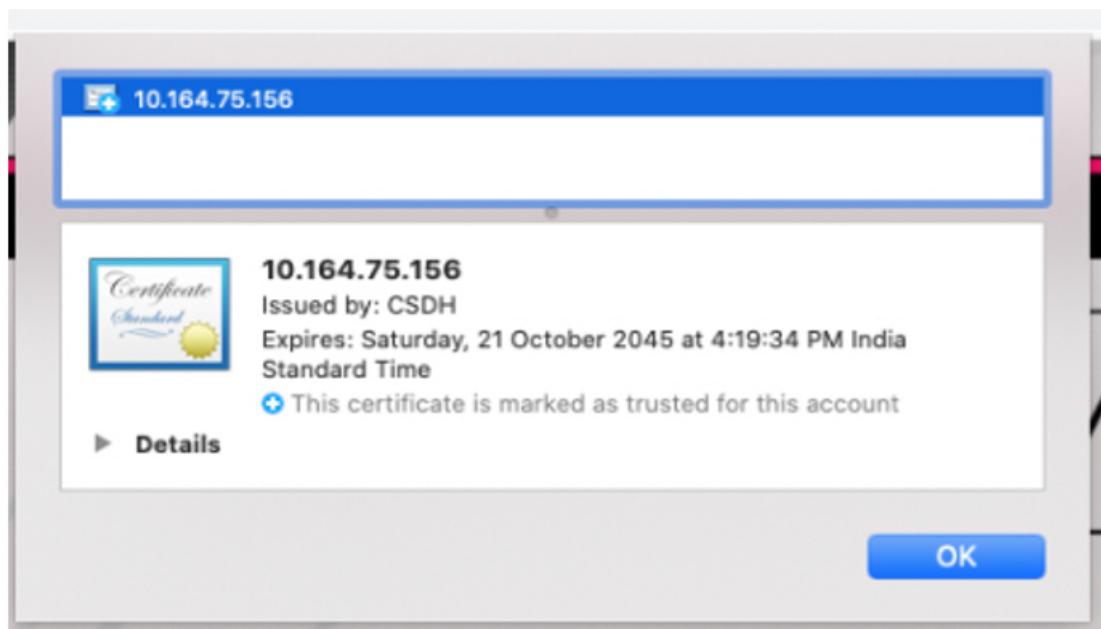


1. Save the Certificate to the Desktop.

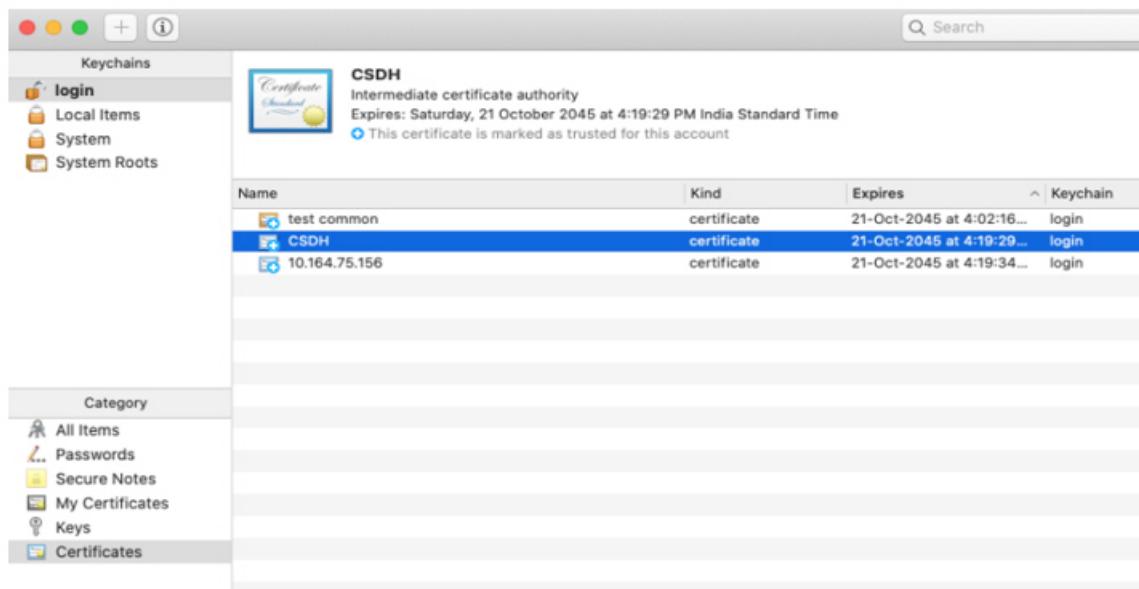
- Click on:

Not secure > Certificate

- The following dialogue is displayed which allows the certificate to be saved. Click the certificate icon and literally drag the icon to the desktop.



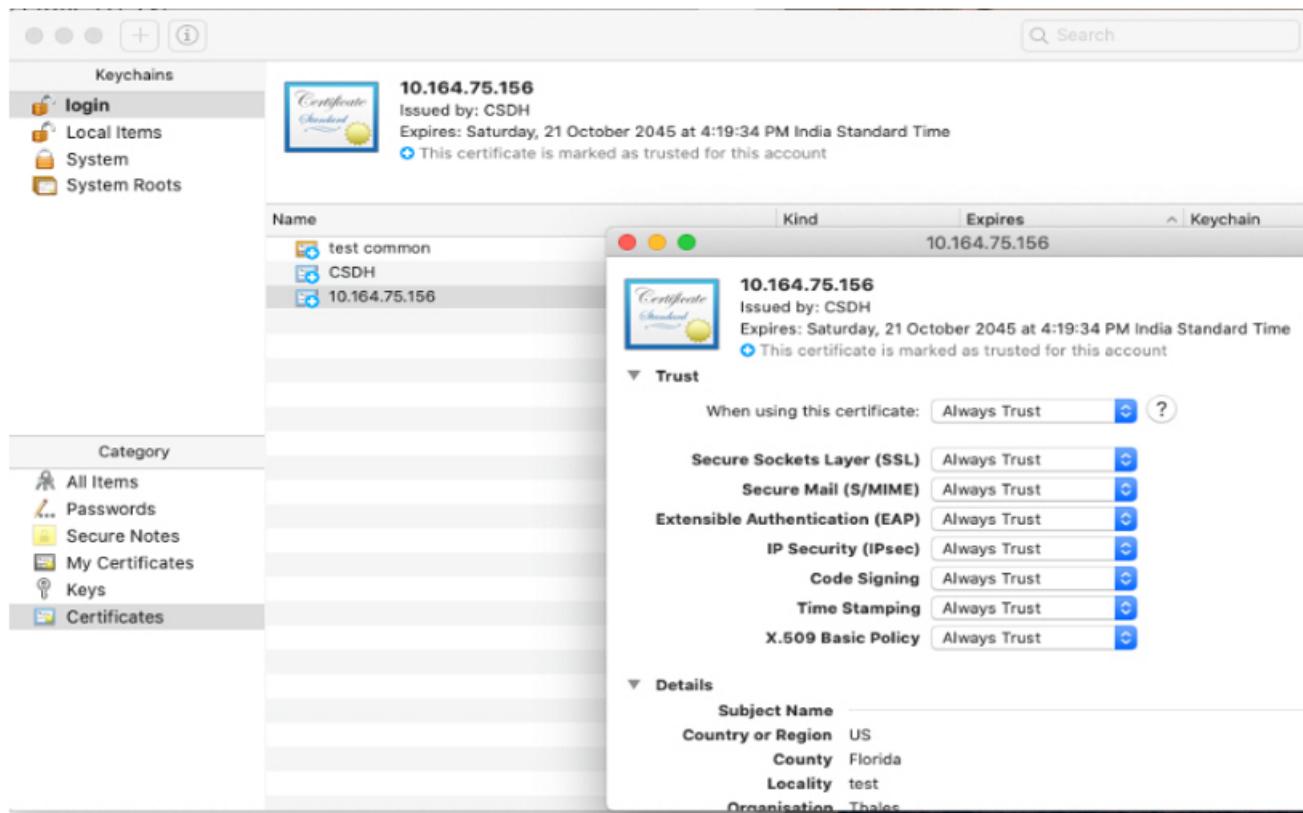
2. Add the Certificate to Keychain Access.



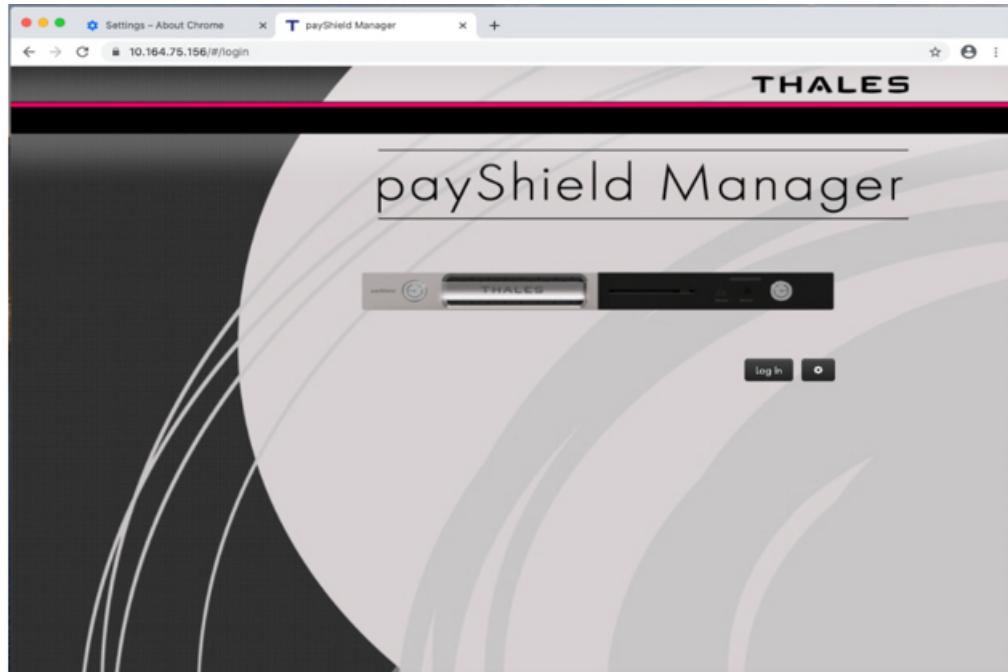
- Open the Keychain Access Application and Navigate to the Certificates panel.
- Drag the certificate into the Certificates panel.
- The certificate is now installed and recognizable to Keychain Access.

Note: You only want one certificate, if two exist please delete one. You do not want duplicate certificate entries.

3. Trust the Certificate.



- Double-click on the certificate in order to manage the system preferences for handling the certificate.
 - Expand the Trust panel and set the preference to “Always Trust” the certificate.
4. Restart the Browser/System.
 - Restart the browser of the system.
 5. Open payShield Manager.
 - Open payShield Manager;
 - Click Advanced and then proceed anyway.



8.7 Configuring the Ports and the Host Interface

8.7.1 Management Port

The Management port is an Ethernet port that is used for managing the HSM. It cannot be used to process host commands. This is configured automatically as part of the commissioning process undertaken earlier.

Where a firewall is used to protect the network link to the Management port, the following ports should be opened as appropriate:

Port	Protocol	Purpose
80	TCP	payShield Manager
443	TCP	payShield Manager

It is recommended that the Management Ethernet port and Host Ethernet port(s) have independent IP subnets.

8.7.2 Host Ethernet Ports

The payShield HSM Host interfaces are configured using payShield Manager - see [Section 9.10, “Configuration Tab”, on page 170](#).

Where a firewall is used to protect the network link to the host port, the following ports should be opened as appropriate:

Port	Protocol	Purpose
161	UDP	SNMP Requests - Utilization and Health Check data
162	UDP	SNMP Traps.
xxxx	TCP/UDP	Well-known port for command traffic between host and payShield, as defined in host port parameters. Default is 1500. Use of this port results in the default LMK being used unless the command explicitly identifies another LMK.
xxxx + n	TCP/UDP	Well-known port for command traffic between host and payShield where LMK n-1 is to be used. For example, if the default well-known port has been defined as 1500, then 1501 is used if LMK 0 is required for the command, 1502 is used if LMK 1 is required for the command, and so on. An explicit identification of the LMK in the command overrides the LMK implied by the port number.

It is recommended that the Management Ethernet port and Host Ethernet ports are all on different IP subnets.

8.7.3 Host FICON Ports

The host interface for the payShield 10K FICON model can be configured for either Ethernet or FICON connection. The connection type is configured using payShield Manager as described in [Section 9.10, “Configuration Tab”, on page 170](#).

8.7.4 Host Printer Ports

The payShield 10K printer port is configured using payShield Manager as described in [Section 9.10, “Configuration Tab”, on page 170](#).

payShield 10K is compatible with several types of printers:

- a serial printer (connected via a USB-to-serial converter cable),
- a parallel printer (connected via a USB-to-parallel converter cable),
- or a native-USB printer.

8.7.5 Configure the Software

The following parameters are configured using payShield Manager as described in [Section 9.10, “Configuration Tab”, on page 170](#).

- The 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.
- The availability of a UDP port
- The availability and number of TCP ports. The number of TCP/IP sockets available has a maximum of 64.
- The Keep-Alive timer, which enables TCP to periodically check whether the other end of a connection is still open. This enables the HSM to free resources by closing any unused connections.
- The Well-Known-Port address, which is the published TCP port address of the HSM, in the range 0000010 to 6553510 representing an address in the range 000016 to FFFF16.
- The IP address for each of the host ports, i.e. the Internet Protocol addresses of the unit's host ports in the system. The addresses are four decimal numbers, each not exceeding 255.
- The subnet mask for each host port, used to define the network class. This is four decimal numbers, each not exceeding 255. It is recommended that the Ethernet ports on the HSM are on different subnets from each other.
- The default gateway for each host port, used to define the IP address to which off-subnet traffic is to be sent to for onward routing. This is four decimal numbers, each not exceeding 255.

Note: The payShield 10K automatically detects whether an incoming command message uses ASCII or EBCDIC characters, and processes the command accordingly, returning the result in the same format.

9 Using payShield Manager

9.1 Introduction to payShield Manager

This Chapter describes in detail the functionality provided by payShield Manager. It assumes the commissioning process has been completed as described in [Chapter 8, “Commission using payShield Manager”](#). A description, of how the Local Master Key (LMK) is generated and installed and how the configuration is updated, is included.

payShield Manager provides the following features:

- HSM Configuration – communication port settings, security settings, etc.
- HSM Installation – generation and installation of LMKs from Smart Cards
- HSM Key Management – generate keys, import keys, export keys, etc.
- HSM Maintenance – viewing, printing, and erasing of audit logs, error logs, version info, etc.
- HSM State Changes – transitions between Online, Offline, Secure and Authorized
- HSM Firmware and license loading

Please note:

- Only one payShield Manager session is allowed at a time
- When accessing the payShield 10K via the payShield Manager, the local console is disabled. Once the payShield Manager session ends, local console access is restored.
- If the physical keys on the front panel are changed from the Online position, the payShield Manager session terminates abruptly and the local console is restored

payShield 10K software release 2.0a includes a new feature, “Settings per LMK”. The Settings per LMK feature is supported by payShield Manager as well as by the Console.

An overview of the functionality provided is documented in the *payShield 10K Programmers Manual*.

Follow this link for further information on using this new feature: [Section 9.11, “Settings per LMK”, on page 231](#).

9.2 Logging into payShield Manager

1. Enter the IP address of your payShield 10K into your Internet browser and click **Enter**.

Note: Only one tab in one browser window can be connected to the payShield 10k. To monitor multiple 10ks within the same browser, each should be loaded into a separate browser tab.

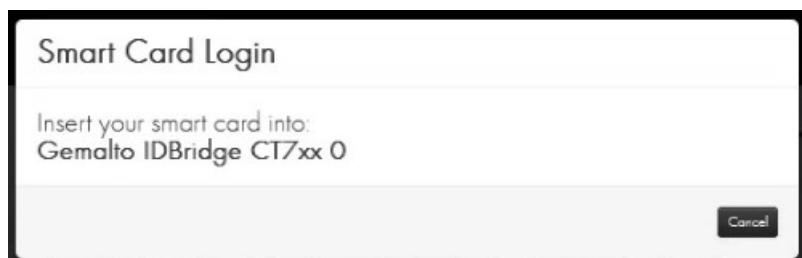
The payShield Manager welcome page displays.

Note: When using MacOS Catalina there are a few additional steps to be carried out before the landing page can be accessed. These are described in [Section 8.6, “Using payShield Manager with MacOS Catalina”, on page 96](#).



2. Click **Log In**.

The system prompts you to insert your Smart Card into the Smart Card reader.

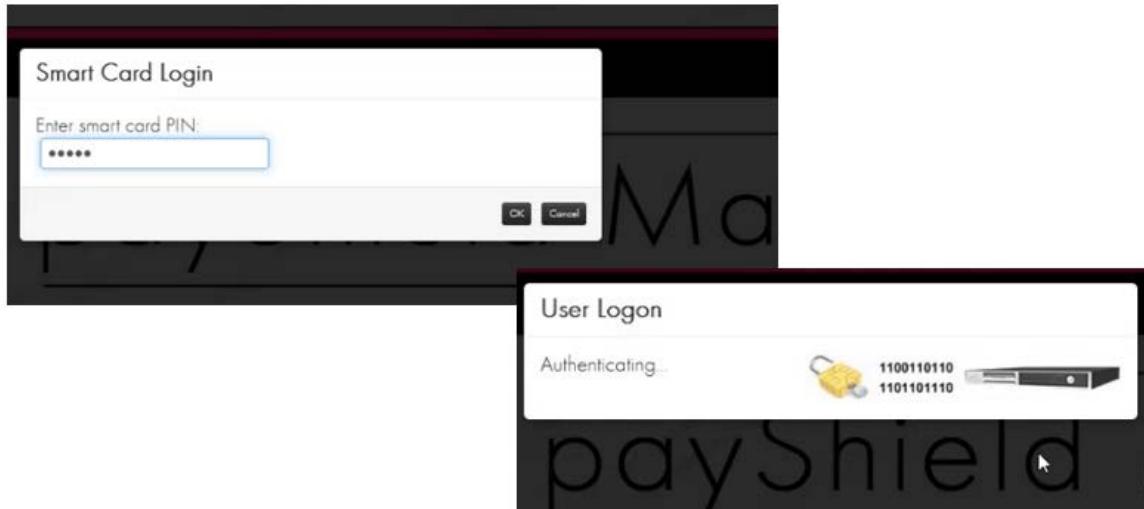


Note: To reach the Secure state, both Right and Left Administrators must perform steps 3 through 5 below.

3. Insert your Administrator Smart Card into the Smart Card reader.

Note: If the system does not appear to be reading your Smart Card, check your Smart Card reader configuration.

4. Enter your PIN into the card reader.

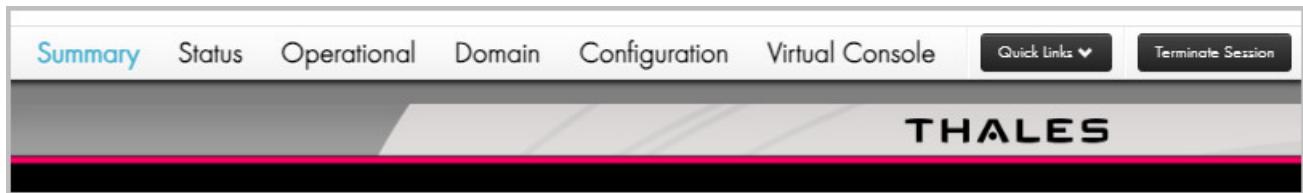


5. Click **OK** on the card reader.
6. The following page displays and the unit is in the Online state.

A screenshot of the Thales payShield 10K Summary Dashboard. The top navigation bar includes links for Summary, Status, Operational, Domain, Configuration, Virtual Console, Quick Links, and Terminate Session. The main header features the THALES logo. On the left, there is a vertical sidebar with four buttons: "Summary Dashboard", "Health Dashboard", "Configuration Dashboard", and "Local Master Key". At the bottom right of the dashboard area, there is a button labeled "State: Online" with an upward arrow. A red arrow points from the text "The following page displays and the unit is in the Online state." in the previous step to this "State: Online" button. The footer contains copyright information: "Copyright © 2014-2020 Thales Group. All Rights Reserved." and a row of small icons.

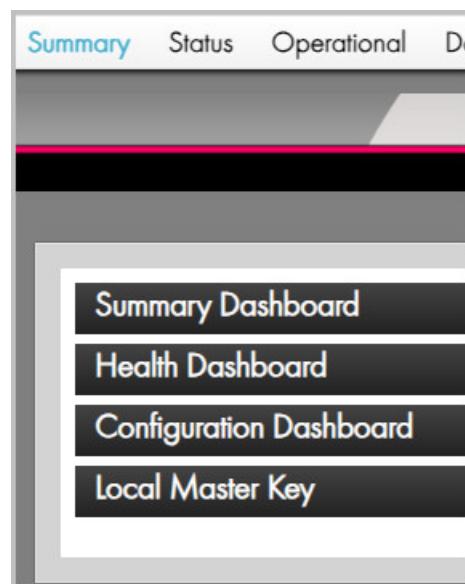
Note: Refer to [Section 9.5.1.5, “Switching to Secure State”, on page 116](#) for additional information.

9.3 Top Tab descriptions



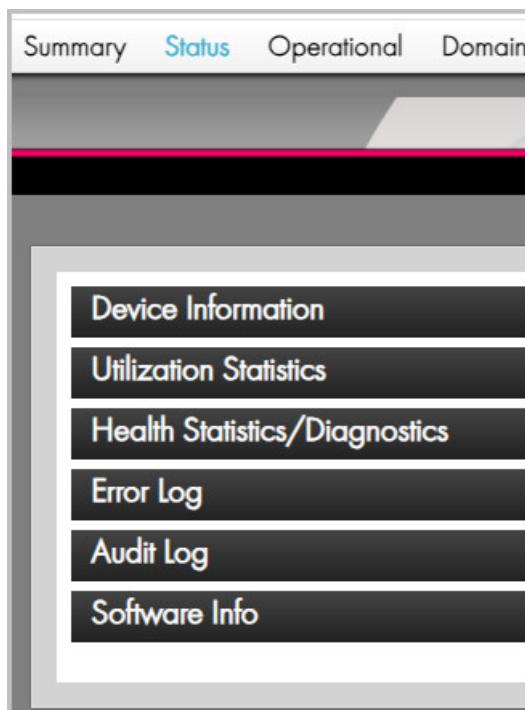
9.3.1 Summary Tab

Opening the Summary tab displays the following:



9.3.2 Status Tab

Opening the Status tab displays:

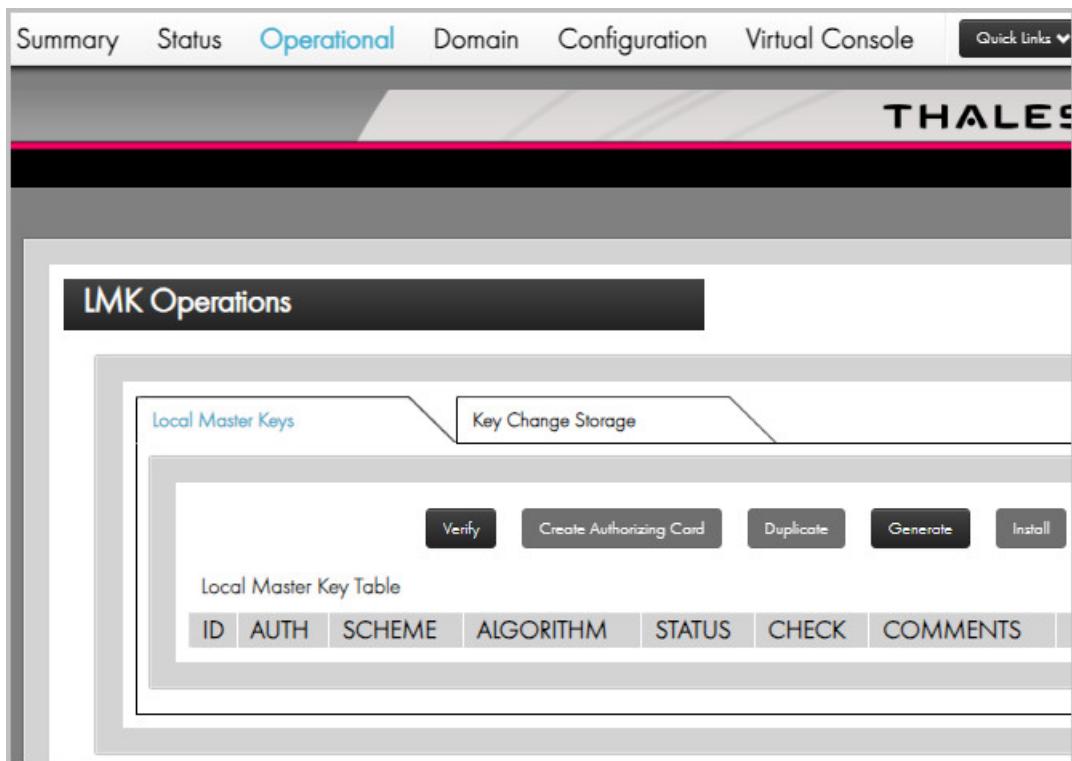


From here, you can:

- View detailed device information
- Cause a reboot of the HSM
- View/download/reset utilization statistics and configure their collection
- View/download/reset health statistics, configure their collection and reset the fraud detection
- Run diagnostics and configure the automated run-time
- View/download the error log and clear it
- View/download the audit log and clear it
- View detailed software versions
- Upgrade the software
- View detailed license information
- Install licenses
- View details on the NIST Validated Algorithms

9.3.3 Operational Tab

Opening the Operational tab displays:



From here you can:

- For each individual LMK
 - Replace an LMK
 - Delete an LMK
 - Set an LMK as the default LMK
 - Set an LMK as the default Management LMK
 - Set Authorized Activities
- For each individual LMK in Key Change Storage
 - Replace an LMK
 - Delete an LMK
- Verify LMK Smart Card shares
- Create Authorizing Officer Smart Cards
- Duplicate LMK Smart Card shares
- Generate LMKs

- Install LMKs

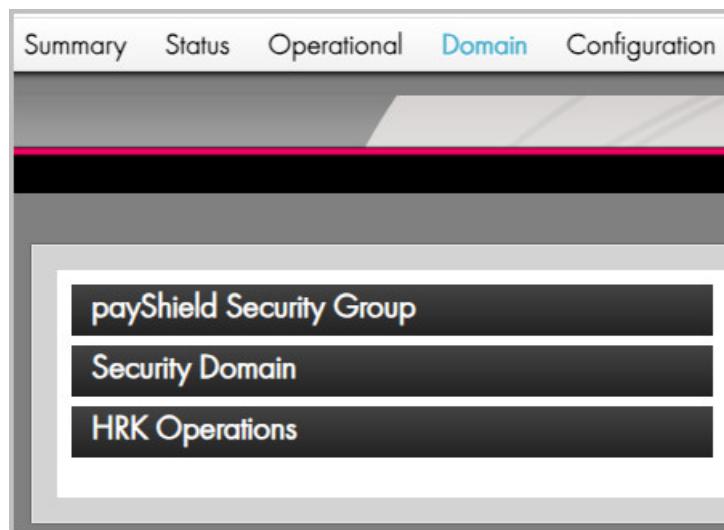
Note: Installing an LMK loads an old LMK component set into the Key Change Storage. This then allows you to translate key material from encryption under one LMK to encryption under another LMK. The current LMK must be installed before an “old” LMK can be installed. Note that attempts to load both Live and Test into the same slot (as new and old LMKs) will be rejected.

- Install LMKs into the Key Change Storage (old LMKs)

Note: “Old” LMKs are stored in a table within the secure memory of the HSM, with each “old” LMK occupying a different “slot” within the table.

9.3.4 Domain Tab

Opening the Domain tab displays:



From here you can:

- View and manage the payShield Security Group’s Smart Card whitelist
- View and manage the Security Domain
 - View the certificate chain and its fields
 - Commission a Smart Card for this Security Domain
 - Decommission a Smart Card
 - Copy a Domain Smart Card
 - Create a new Security Domain (CTA)
- Change the HRK passphrases
- Migrate Legacy Cards (if the payShield is a migrated unit)

9.3.4.1 payShield Security Group

The screenshot shows the payShield 10K software interface. At the top, there is a navigation bar with tabs: Inventory, Status, Operational, Domain (which is highlighted in blue), Configuration, and Virtual Console. To the right of the tabs are Quick Links and Terminal buttons. Below the navigation bar, the THALES logo is displayed. The main content area has a title bar "payShield Security Group". Inside this bar, a message says "The following smartcards are members of this HSM's security group:". Below this message is a table with three rows, each representing a category of smart cards: Left Key Cards, Right Key Cards, and Restricted Cards. Each row has three columns: Smart Card Type, Serial Number, and Certificate Number (Hexadecimal). The "Left Key Cards" row contains one card entry with serial number 5324016447068938 and certificate number C021E13F21948098. The "Right Key Cards" row contains one card entry with serial number 5324017424068938 and certificate number F9EC9ECB9B547F3C. The "Restricted Cards" row currently has no entries. At the bottom of the table are "Undo" and "Apply" buttons.

Smart Card Type	Serial Number	Certificate Number (Hexadecimal)
Left Key Cards	5324016447068938	C021E13F21948098
Right Key Cards	5324017424068938	F9EC9ECB9B547F3C
Restricted Cards		

9.3.4.2 Security Domain

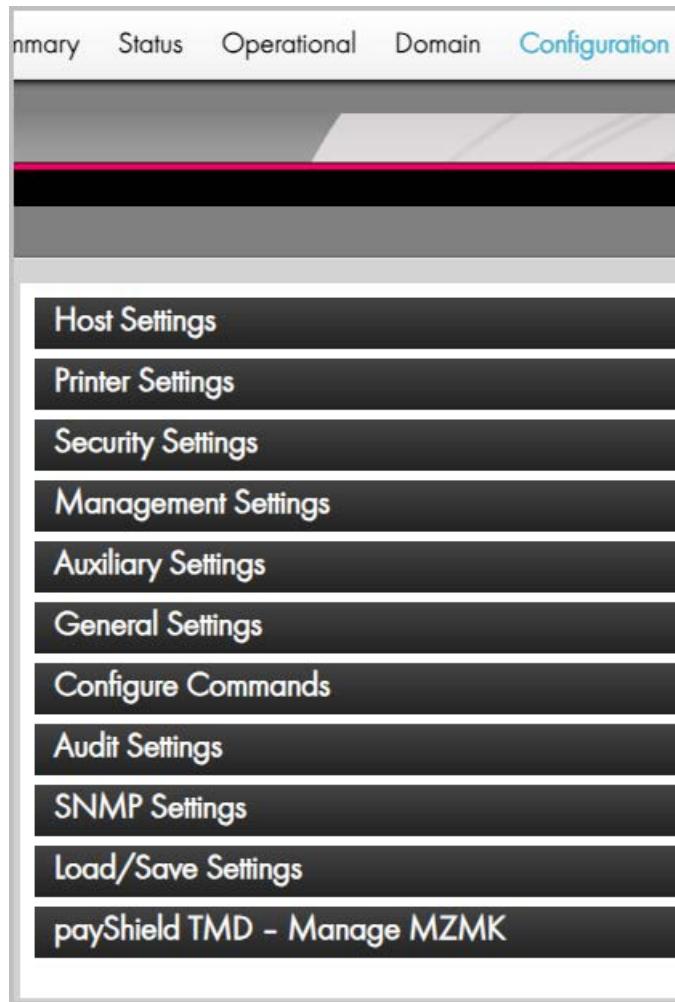
The screenshot shows the payShield 10K web interface. At the top, there is a navigation bar with links: 'mary', 'Status', 'Operational', 'Domain' (which is highlighted in blue), 'Configuration', 'Virtual Console', 'Quick links ▾', and 'Terminate Session'. Below the navigation bar, the title 'payShield Security Group' is displayed. Underneath it, the section 'Security Domain' is shown. In the center of the page, there are four buttons: 'Commission Card', 'Decommission Card', 'Copy Domain Card', and 'New Domain'. To the left, under 'Certificate Chain', there is a collapsible section showing certificate details: 'Subject: payShield 10K for docs' and 'Subject: S0000372494A'. To the right, under 'Certificate Fields', is a table:

Field	Value
Version	3 (0x2)
Serial number	94:a8:b8:69:59:ff:8:ee:97:45:fc
Signature algorithm	ecdsa-with-SHA256
Signature hash algorithm	SHA256
Issuer	C=US, ST=Florida, L=Plantation, O=D
Valid from	Nov 30 18:54:26 2022
Valid to	Nov 24 18:54:26 2047
Subject	C=US, ST=Florida, L=Plantation, O=D
Public key	ECC (521 bits)
Public key parameters	id-ecPublicKey (secp521r1)

Below the table, there is a section labeled 'Certificate Field Value' with a single row containing the value '3 (0x2)'.

9.3.5 Configuration Tab

Opening the Configuration tab displays:



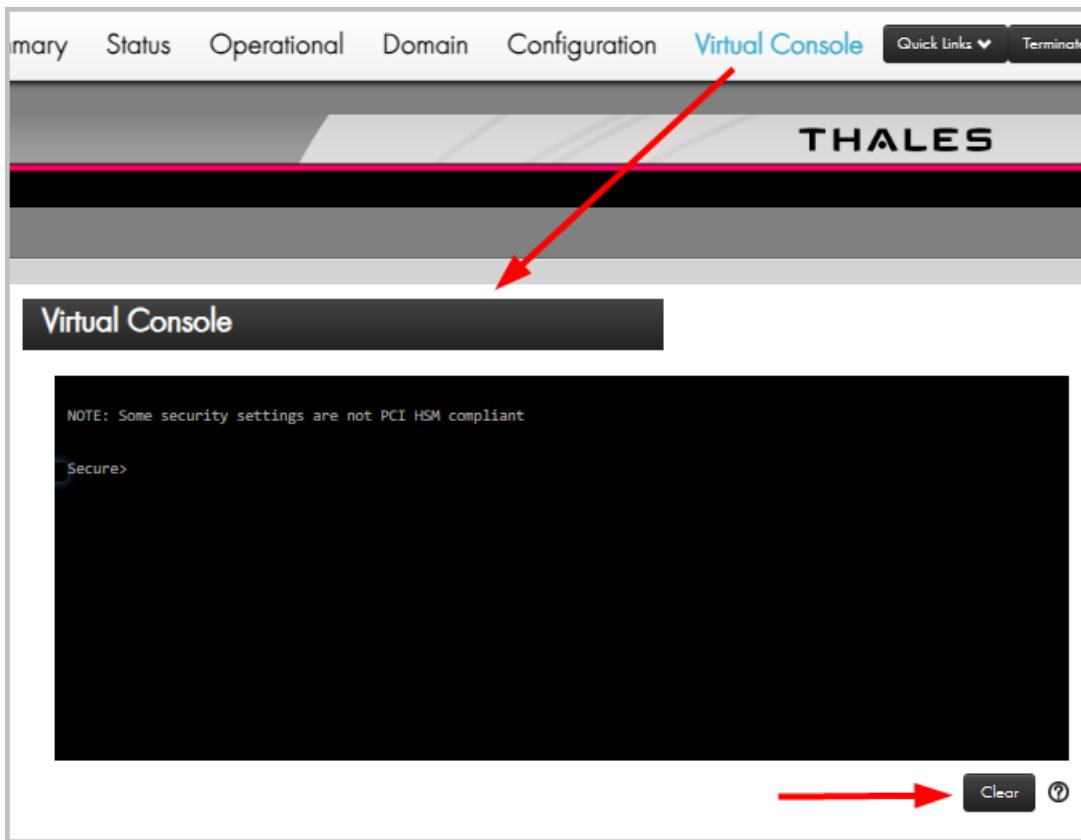
From here you can:

- View and manage the HSM's Host Interface Settings including:
 - Setting the Host message header length
 - Setting and configuring the interface type (Ethernet/FICON)
 - Setting the IP, ACL, TCP/UDP, and TLS parameters for Ethernet
 - View the Chain of Trust and Import TLS certificates for Host connections
 - Configuring the connection settings for FICON
- View and manage the console interface settings
- View and manage the printer settings
- View and manage the security settings

- View and manage the management interface settings
 - IP settings
 - Timeouts
 - View the Chain of Trust and Import TLS certificates for payShield Manager
- View and select the PIN block formats that the HSM should process
- View and manage the alarm settings
- View and manage the fraud settings
- View and set the HSM's date and time
- Configure a Remote Syslog Server
- View and set the HSM's system name and description
- Set audit operations and set the audit counter value
- Select audit-able console, Host, and management commands
- View and manage the SNMP settings
- Load/save the HSM's settings to a Smart Card
- Create new MZMK and Export to a TMD
- Reset the HSM's settings to factory default state

9.4 Virtual Console Tab

Opening the Virtual Console tab displays:



Selecting this tab causes the UI to open a virtual console window. Commands can be entered as if you were on the local console (physically located) at the HSM. Note that not all commands are available.

Note: The following commands may **not** be used in the virtual console: A, CO, DC, EJECT, FC, GK, GS, LK, LO, NP, RC, RS, SS, VC, XA, XD, XE, XH, XI, XK, XR, XT, XX, and XZ.

The virtual console works the same as the local console and all console operations are supported with the exception of commands that may invoke the use of the HSM's local facilities (e.g., the internal Smart Card reader).

Note: In the current implementation of the virtual console, a cursor may not be present. However, the virtual console is still active and functional.



WARNING: The Virtual Console must not be used to enter or display components of production keys – the Trusted Management Device (TMD) should be used for this purpose.

9.4.1 Quick Links

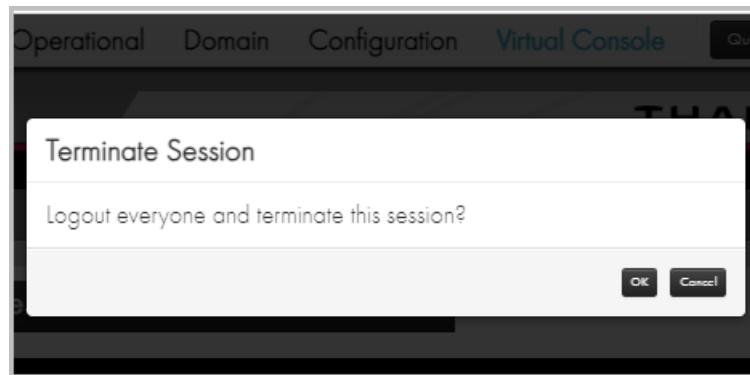
Opening Quick Links displays shortcuts to Host interface settings, security settings, load/save settings, and LMK Operations.



9.4.2 Terminate Session

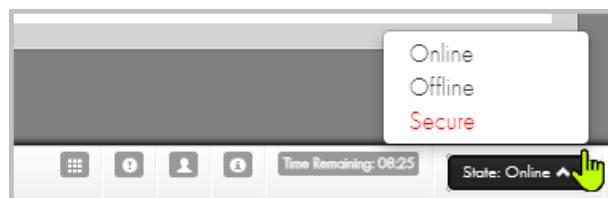
Logs out all users and ends the current session.

Note: The system will prompt for confirmation prior to terminating the session.



9.5 Lower screen icons

The icons are described from right to left.



9.5.1 payShield 10K States

The allowed state transitions are based on the type of users logged in.

For example:

- If only a left or only a right RACC are logged into the HSM, then the available states are Online and Offline.

- If at least one left **and** one right RACC are logged into the HSM, then all three state transitions are allowed.

9.5.1.1 Online

In the Online state, the HSM permits communication with a Host computer system by way of the HSM's Host port.

9.5.1.2 Offline

In the Offline state, the HSM prevents communication with the Host computer system. Usually this state is required when changing configuration parameters.

9.5.1.3 Secure

In the Secure state, the HSM prevents communication with the Host computer system. This state is required for certain highly sensitive functions (for example, generating or loading LMKs into the HSM).

9.5.1.4 Switching to Online or Offline State

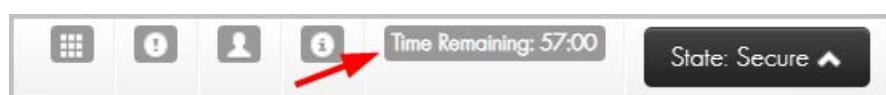
To switch the HSM into the Online or Offline state, simply click the appropriate option from the State button's menu list.

9.5.1.5 Switching to Secure State

Switching the HSM into its Secure state requires one left and one right ACC smart card (both belonging to the HSM in which you wish to switch to secure state) to be authenticated. The action is similar to providing both the left and right physical keys locally and turning them to the Secure position.

Assuming you logged in with a left RACC, you would simply have to login the right RACC before the "State" button would present the option to move to the "Secure" state.

9.5.2 Time Remaining

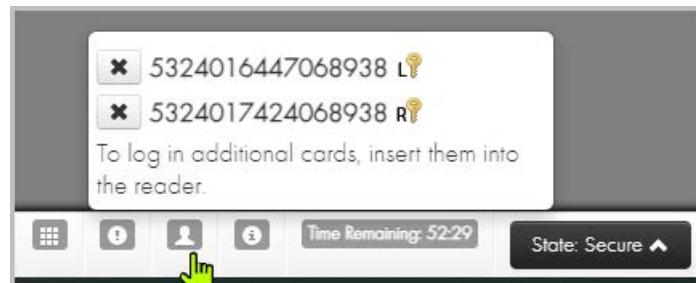


Shows the amount of time left before the automatic termination of the session.

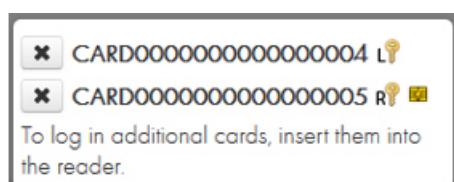
9.5.3 Information



9.5.4 User

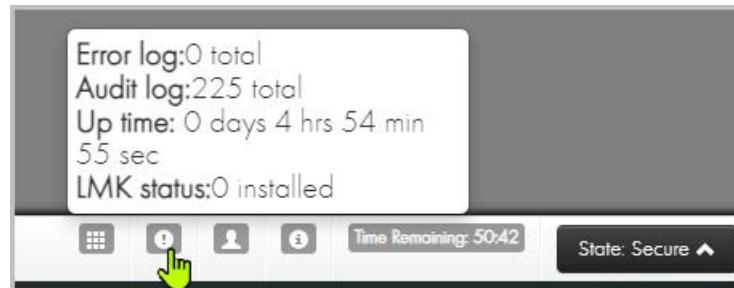


Selecting this button shows information on card user(s) and **allows an individual user to logout of the session** by selecting the next to their card's serial number.



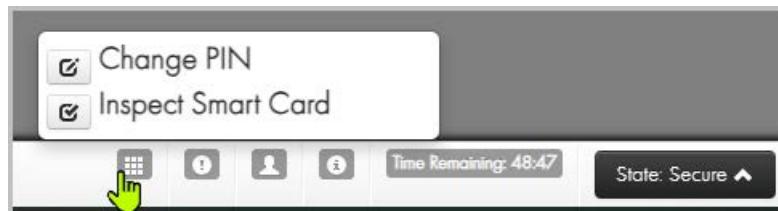
The icon next to a card serial number indicates that you are a Left RACC. While the icon next to a card serial number indicates that you are a Right RACC. The symbol next to the card serial number indicates that the card is currently inserted into the reader.

9.5.5 Status



Selecting this button displays the number of Error and Audit Log entries, the system up time, and number of LMKS installed.

9.5.6 Smart Card Operations



Selecting this button allows you to do Smart Card operations such as Change PIN and Inspect Smart Card.

To change the PIN on a Smart Card, select the “Change PIN” operation and follow the wizard which requires that you insert your Smart Card, enter the current PIN, and finally enter the new PIN.

To view the Smart Card details including **getting the Certificate Number** on the Smart Card, click the “Inspect Smart Card” operation. The Certificate Number is required to manually enter Smart Cards into the whitelist from the **Domain > payShield Security Group** tab.

9.5.7 User Login/Logout

9.5.7.1 Login Additional Users

Smart Card Login

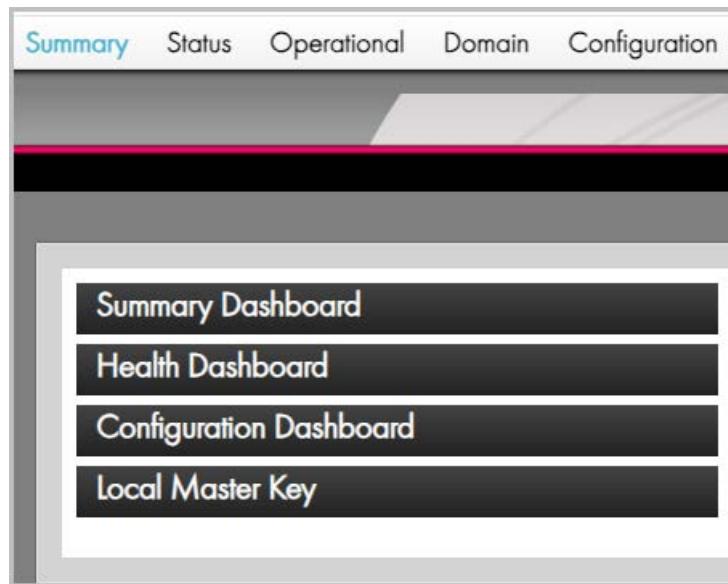
Enter PIN via the smart card terminal keypad.

To login additional users, insert the new user's Smart Card into the Smart Card reader after the initial login (and when not in the middle of a wizard that calls for a Smart Card to be inserted – e.g., Loading an LMK). The system will automatically prompt you for your PIN and begin the authentication process. Once the authentication has completed successfully, the allowed Host interface state transitions and logged in users will be updated.

9.5.7.2 User Logout

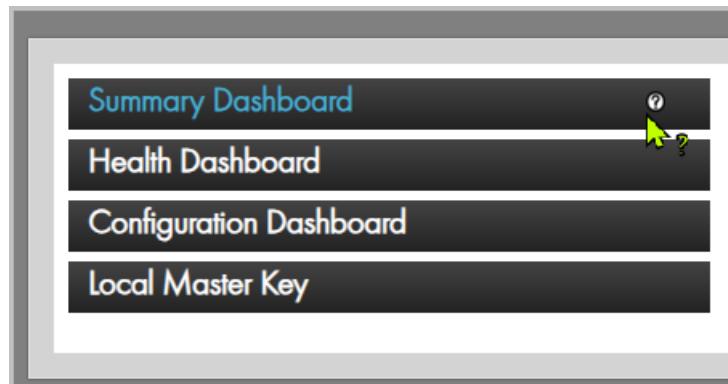
To logout a logged in user, press the  button at the bottom right of the main page, find the user in the list, and press the  button next to it.

9.6 Summary Page



After a successful login, you will be greeted with the main page as shown above. Each element will be described next.

Note: To access Online help, select the question mark, as shown below.



9.6.1 Summary Dashboard

Summary Dashboard	
Name:	pS10K
Description:	payShield 10K
Model:	PS10-S (971-700035-001)
Serial Number:	S0000372494A
Software:	2000-0000
Base Release:	2.0a
LMKs Installed:	0
HRK Installed:	Yes

When expanded, this section displays a table containing Name, Description, Model Number, Serial Number, Software Version, Base Release, the number of LMKs Installed, and the presence of an Installed HRK.

9.6.2 Health Dashboard

Health Dashboard	
Error Log:	0 total
Audit Log:	225 total
PSU #1:	AC Failure (XQ1816RE1108)
PSU #2:	OK (XQ1816RE2131)
Fan #1:	OK (Warning - Serial Number Not Detected)
Fan #2:	OK (Warning - Serial Number Not Detected)
Up Time:	0 days 5 hrs 4 min 23 sec
Instantaneous HSM Load:	0%
Number of Reboots:	0

When expanded this section displays a table containing an Error Log counter, an Audit Log counter, Power Supply Unit status (#1 and #2), Fan status, System Up-Time, Instantaneous HSM Load (%), and the number of Reboots.

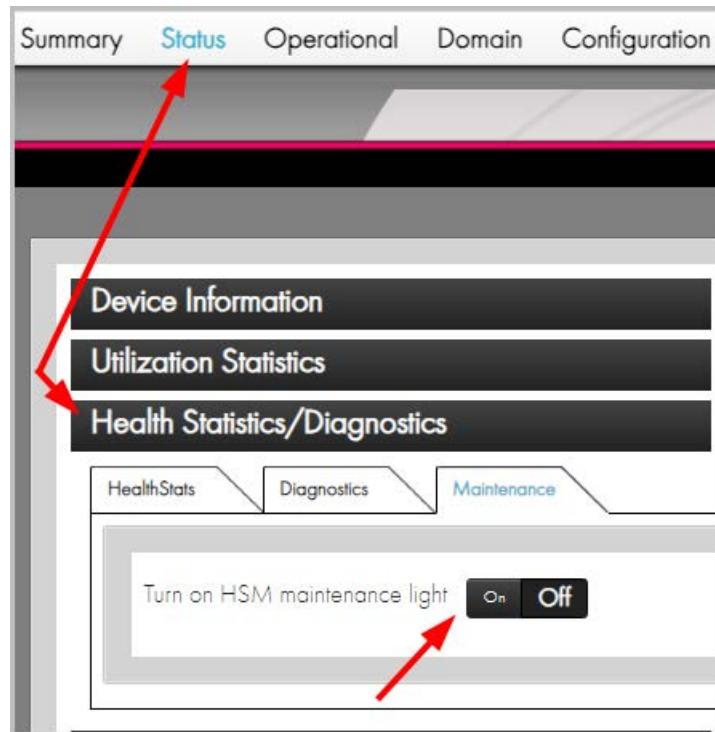
9.6.2.1 How to resolve reported errors

In the example above, the dashboard identifies Failure with Power Supply #1.

The payShield 10K handle light is red.

Follow these steps to resolve:

1. Navigate to **Status > Maintenance**.



2. Click **On**.

Lights on the payShield 10K turn blue (lights in two locations: front and rear of the panel).

Note: The HSM Maintenance light can be switched to blue via two means: via payShield Manager, as documented above, or manually by a Security Officer who is at the unit.

This light is for informational purposes only and does not impact the status of the payShield 10K in any manner other than turning on the blue service light in on the front and rear panels of the payShield. If the service light is turned on or off, it will be recorded as an event in the Audit Log.

3. Review the error code.

The Health dashboard reports “**NotDetected**” when the power supply is removed.

Health Dashboard

Error Log:	0 total
Audit Log:	225 total
PSU #1:	Not Detected
PSU #2:	OK (XQ1816RE2131)
Fan #1:	OK (Warning - Serial Number Not Detected)
Fan #2:	OK (Warning - Serial Number Not Detected)
Up Time:	0 days 5 hrs 4 min 23 sec
Instantaneous HSM Load:	0%
Number of Reboots:	0

Versus reporting a fault code indicating no electrical power.

Health Dashboard

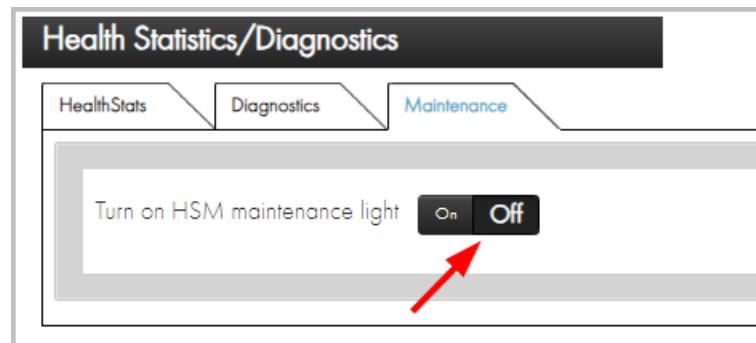
Error Log:	0 total
Audit Log:	225 total
PSU #1:	AC Failure (XQ1816RE1108)
PSU #2:	OK (XQ1816RE2131)
Fan #1:	OK (Warning - Serial Number Not Detected)
Fan #2:	OK (Warning - Serial Number Not Detected)
Up Time:	0 days 5 hrs 4 min 23 sec
Instantaneous HSM Load:	0%
Number of Reboots:	0

- Repair appropriately, i.e., physically replace the power supply / restore lost power.

Health Dashboard	
Error Log:	0 total
Audit Log:	229 total
PSU #1:	OK (XQ1816RE1108)
PSU #2:	OK (XQ1816RE2131)
Fan #1:	OK (Warning - Serial Number Not Detected)
Fan #2:	OK (Warning - Serial Number Not Detected)
Up Time:	0 days 5 hrs 32 min 4 sec
Instantaneous HSM Load:	0%
Number of Reboots:	0

5. Navigate to **Status > Health Statistics/Diagnostics > Maintenance**.

6. Set the maintenance light to **Off**.



Note: Turning the maintenance light to off can also be performed manually at the unit.

9.6.3 Configuration Dashboard

Configuration Dashboard	
Host #1:	10.194.184.193 mask 255.255.240.0
Host #2:	10.194.184.194 mask 255.255.240.0
Management:	10.194.184.195 mask 255.255.240.0
Auxiliary:	10.194.184.196 mask 255.255.240.0
Printer:	No valid printer configured - no printer found in system
PCI-HSM:	Some security settings are not PCI HSM compliant
Management Chain of Trust Validated:	Yes

When expanded this section displays a table containing Host 1 IP address, Host 2 IP addresses, the management IP address, a summary of the printer configuration, PCI-HSM compliance, and Management Chain of Trust Validation status.

9.6.4 Local Master Key

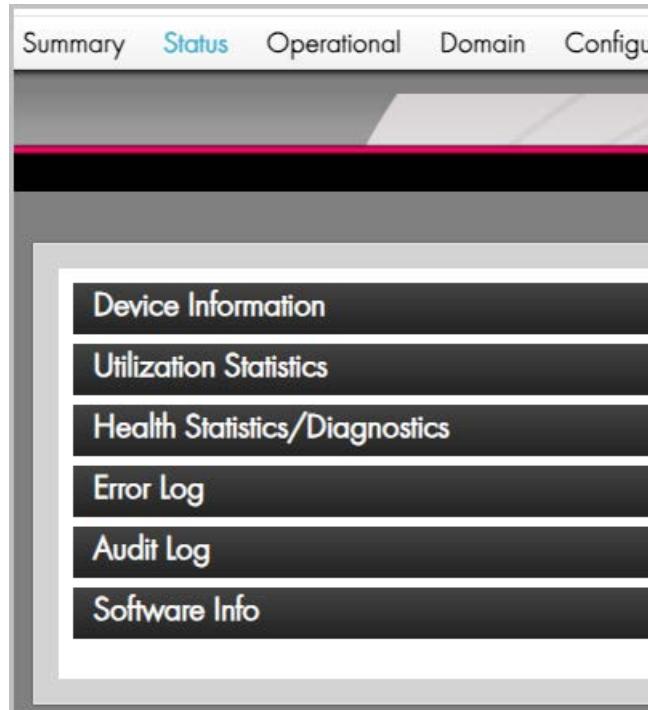
Local Master Key						
Local Master Key Table						
ID	AUTH	SCHEME	ALGORITHM	STATUS	CHECK	COMMENTS
Key Change Storage Table						
ID	OLD/NEW	SCHEME	ALGORITHM	STATUS	CHECK	COMMENTS

When expanded, this section displays two tables. The first is the Local Master Key Table showing ID, AUTH, SCHEME, ALGORITHM, STATUS, CHECK, and COMMENTS.

The second table shown is the Key Change Storage Table. This table displays ID, OLD/NEW, SCHEME, ALGORITHM, STATUS, CHECK, and COMMENTS.

Note: These collapsible menus and the content within are designed to provide a quick overview of the current status of the HSM. The values cannot be interacted with or changed from the Summary page.

9.7 Status page



The Status Page can be reached by selecting the “Status” button which is the second button from the left at the top of the frame.

9.7.1 Device Information

Name:	pS10K
Description:	payShield 10K
Serial Number:	S0000372494A
Unit Info:	Licensed
Model:	PS10-S (971-700035-001)
Performance:	2500 cps
Date of Manufacture:	19 Nov 2018
PSU #1:	Model Number: D1U54P-W-450-12-HA4C Serial Number: XQ1816RE1108
PSU #2:	Model Number: D1U54P-W-450-12-HA4C Serial Number: XQ1816RE2131
Fan #1 Serial Number:	Warning - Serial Number Not Detected
Fan #2 Serial Number:	Warning - Serial Number Not Detected

Reboot

The Device Information section contains a table that displays the System Name of the HSM Unit, the Unit Description, Serial Number, Unit Info, Model number, Performance in calls per seconds (cps), the Date of Manufacture, PSU serial numbers, and Fan serial numbers.

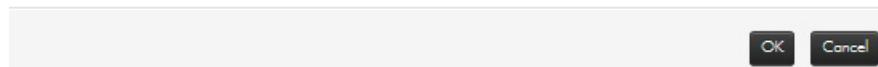
Note: These fields are for easy viewing and are not editable.

Additionally, the Reboot option is within Device Information.

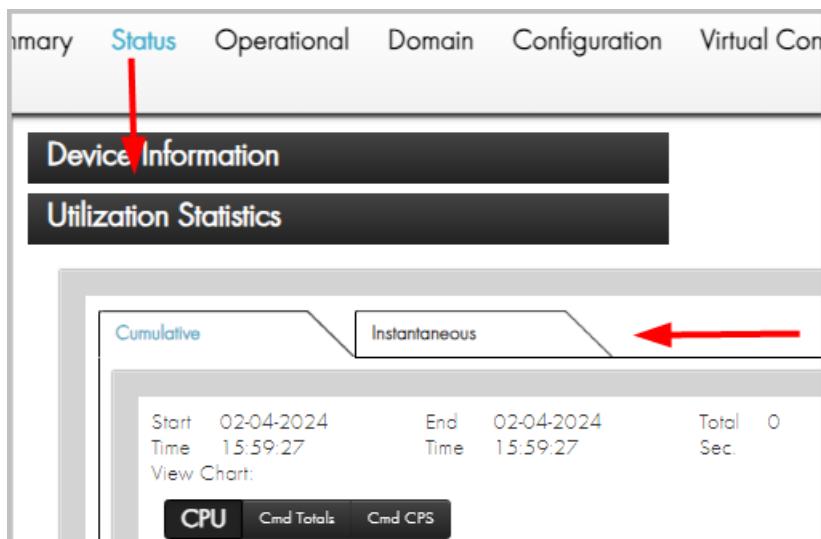
- You must be in the Secure state for a reboot.
- After selecting **Reboot**, the system prompts for confirmation.

Reboot HSM

This action will reboot the HSM, making it unavailable for a short period of time.



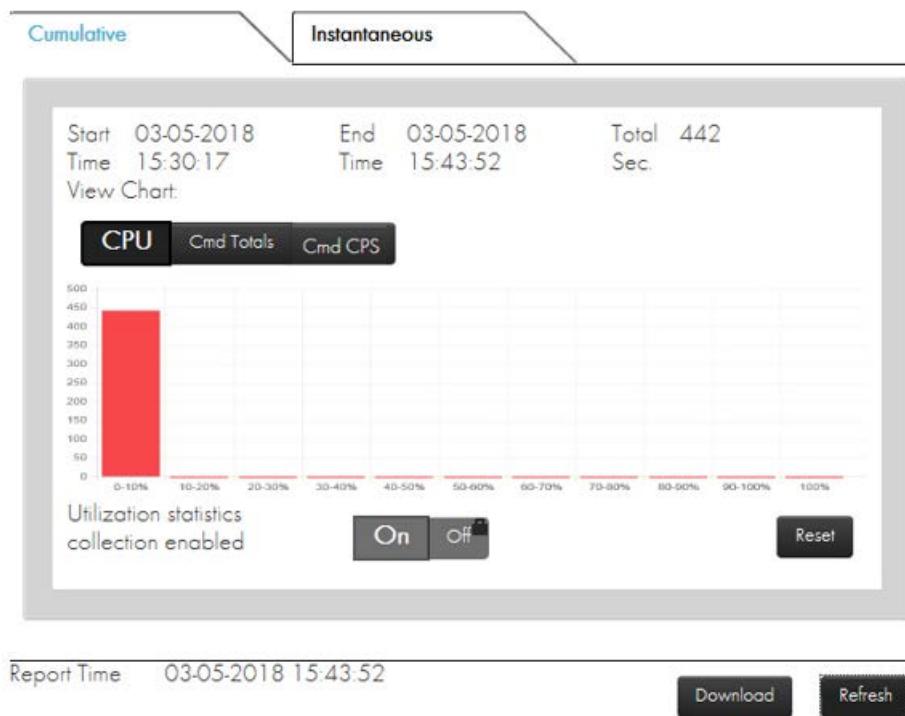
9.7.2 Utilization Statistics



The Utilization Statistics section contains a set of click-able tabs. The first tab is titled “**Cumulative**” and the second tab is titled “**Instantaneous**”.

The two tabs provide information showing static statistics about CPU Load, Command Totals and Command CPS.

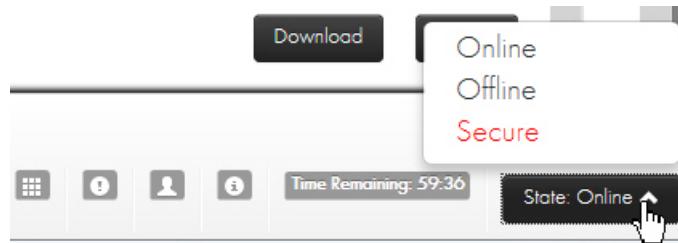
- Cumulative statistics:
Displays data accumulated since the last time that you reset the utilization data. It will continue to accumulate until the next time that the data is explicitly reset. The collected data is persistent over re-starts and power being switched off.
- Instantaneous statistics:
Displays data for the current loading of the HSM, helping Administrators investigate throughput or performance issues as they occur.



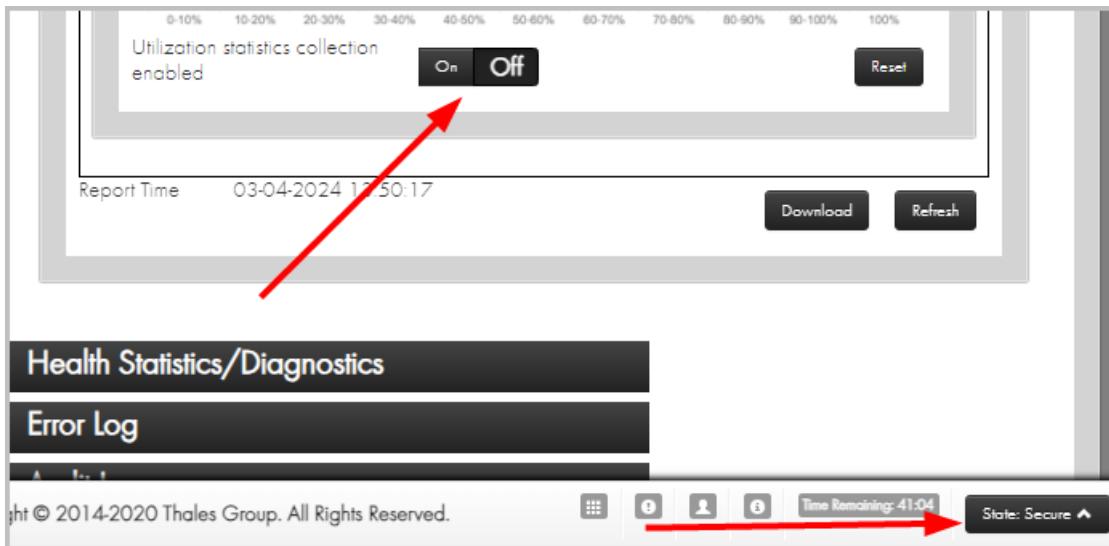
CPU: This data indicates how heavily the HSM is loaded.

Cmd Totals: This data indicates how many times each Host command has been processed.

Cmd CPS: This data indicates the average calls per second (cps) for each command that has been processed. The rated performance of the HSM relates to how many CA Host commands the HSM could run in a second. The speed a command runs may depend on the options or payload associated with it.



On/Off: In Offline or Secure state, the Utilization statistics collection can be turned on or off.



Additionally, while in the Offline or Secure state:

- Click **Refresh** to refresh statistics.
- Click **Reset** to reset the statistics.

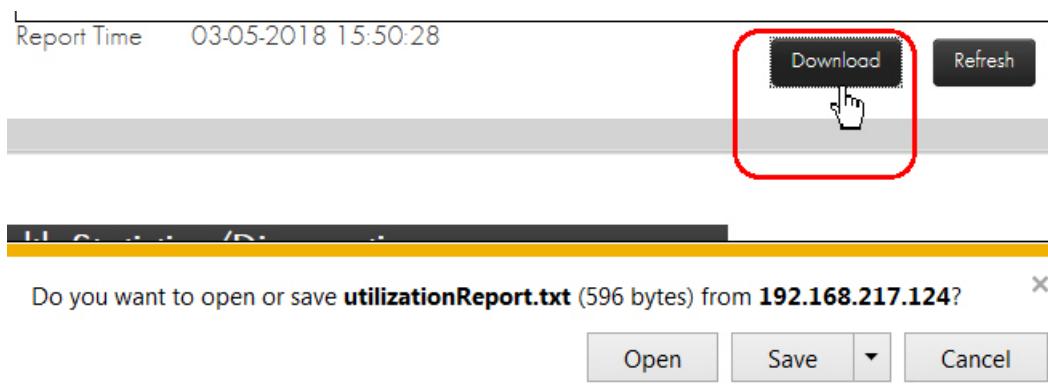
Reset Statistics

You are about to reset the CPU and command utilization statistics. Are you sure?

OK **Cancel**

In any state:

- Click **Download** to save to a text file.

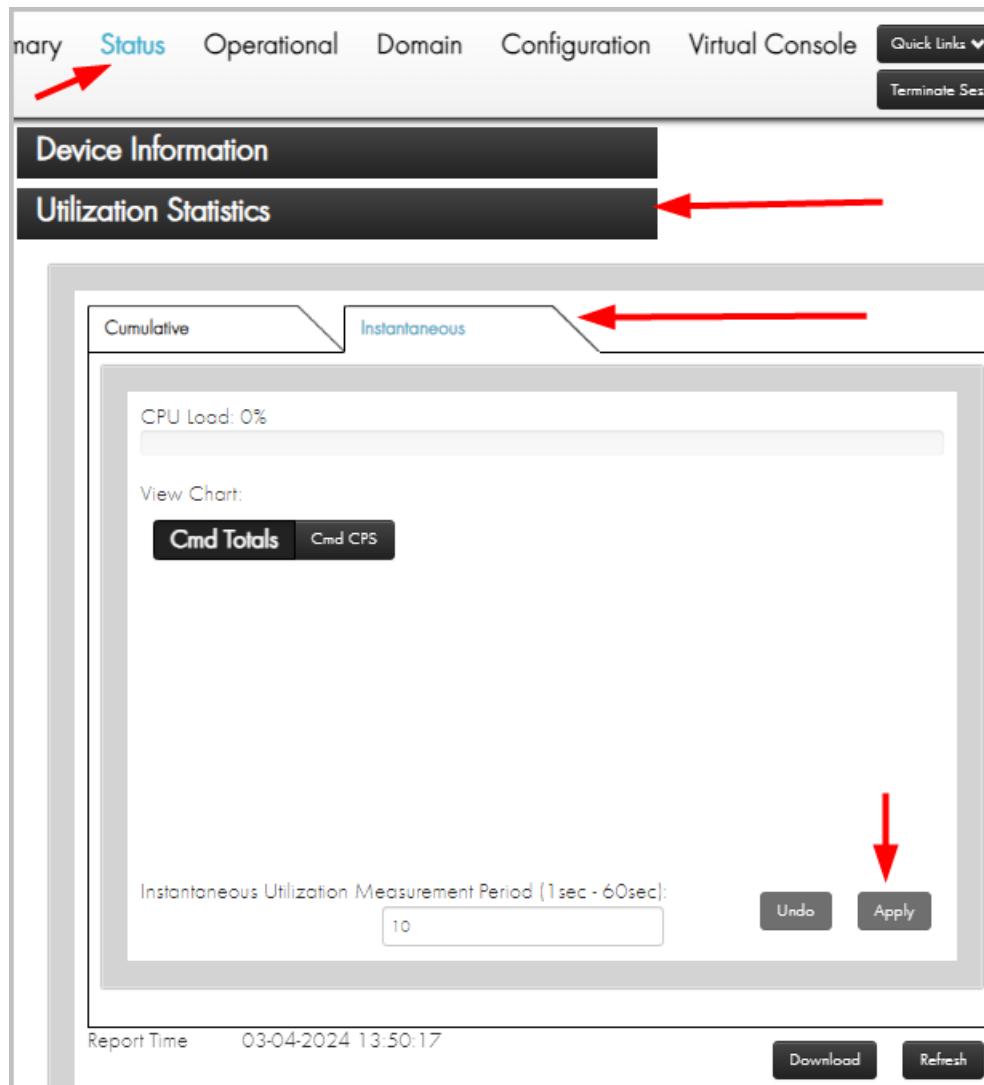


From the Instantaneous view, you can change the measurement period as follows:

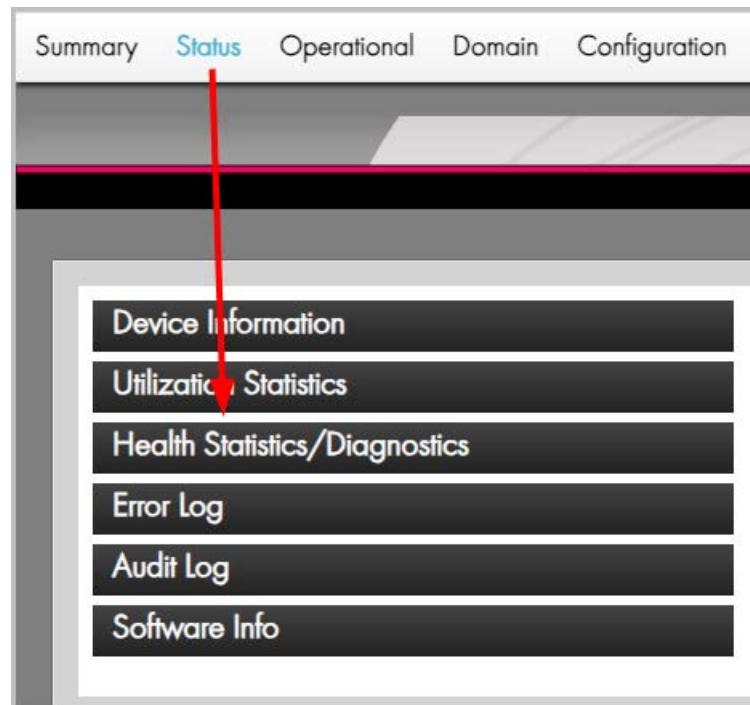
1. Enter the new value in the Measurement Period field.

2. Click **Apply**.

Clicking **Undo** restores the prior setting.



9.7.3 Health Statistics/Diagnostics



9.7.3.1 HealthStats

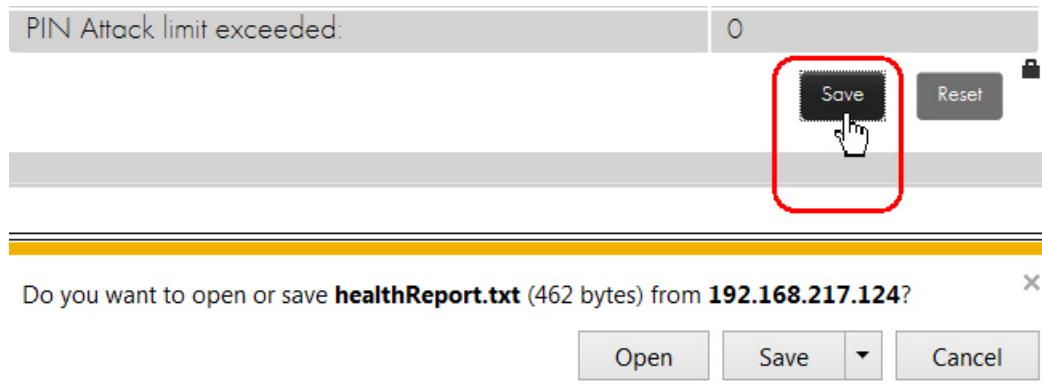
The screenshot shows the payShield 10K Management Interface. At the top, there is a navigation bar with tabs: Primary, Status (which is highlighted in blue), Operational, Domain, Configuration, Virtual Console, Quick Links (with a dropdown arrow), and Terminate Session. Below the navigation bar, there are three main sections: Device Information, Utilization Statistics, and Health Statistics/Diagnostics. The Health Statistics/Diagnostics section is currently active. At the bottom of this section, there is a table with various statistics and a row of buttons: Enable/Disable Health Check Data Collection (with 'Enable' and 'Disable' buttons), Save, and Reset.

HSM Serial Number:	S0000372494A
Report Generation Time:	03-04-2024 14:07:47
Report Start Time:	02-04-2024 15:59:27
Report End Time:	02-04-2024 15:59:27
Number of reboots:	0
Number of tampers:	0
PIN verification failures/minute limit exceeded:	0
PIN verification failures/hour limit exceeded:	0
PIN Attack Limit exceeded:	0

In this section, you can enable and disable the collection of health statistics as well as reset the currently gathered statistics.

In Offline or Secure state, the Health Check Data Collection can be turned on or off using the buttons presented on this page. You may reset the Health Check Data in Offline or Secure state when Authorized using the management LMK.

In any state, the Health Check Data can be saved to a text file by selecting **Save**.



9.7.3.2 Diagnostics

Health Statistics/Diagnostics

HealthStats Diagnostics Maintenance

Periodically run all diagnostic tests at: 9:00 AM

Selected Tests to Run Now

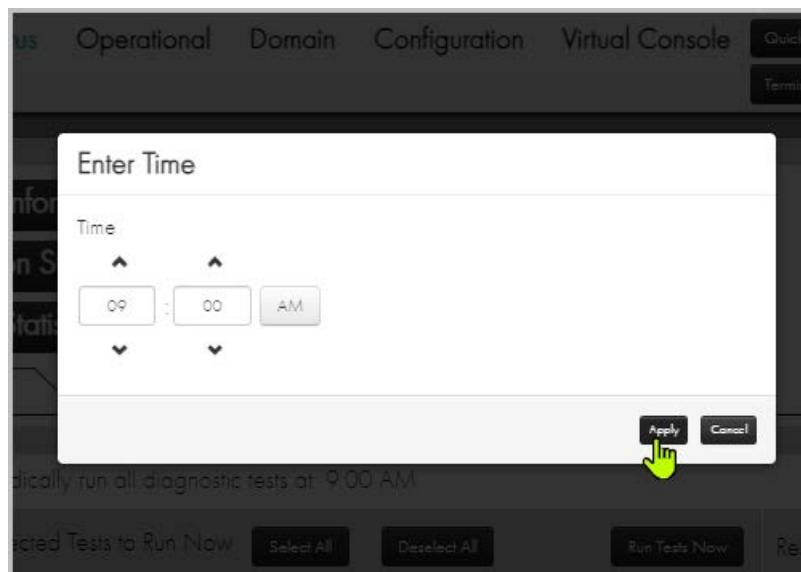
	Result(s)
<input checked="" type="checkbox"/> Battery	
<input checked="" type="checkbox"/> RSA	
<input checked="" type="checkbox"/> AES	
<input checked="" type="checkbox"/> DES	
<input checked="" type="checkbox"/> MD5	
<input checked="" type="checkbox"/> Memory	
<input checked="" type="checkbox"/> Power	
<input checked="" type="checkbox"/> RNG	
<input checked="" type="checkbox"/> RTC	
<input checked="" type="checkbox"/> SHA	
<input checked="" type="checkbox"/> ECDSA	
<input checked="" type="checkbox"/> HMAC	
<input checked="" type="checkbox"/> SCR	
<input checked="" type="checkbox"/> Temperature	
<input checked="" type="checkbox"/> Fans	
<input checked="" type="checkbox"/> Voltages	
<input checked="" type="checkbox"/> Health	

Select All Deselect All Run Tests Now

The Diagnostics tab contains a list of tests that are run periodically and can be run immediately. Tests that are run immediately will display their result(s) upon completion. Automated tests do not report results on this screen. (Failures of those results are placed in the Error Log. No entry means the tests passed.)

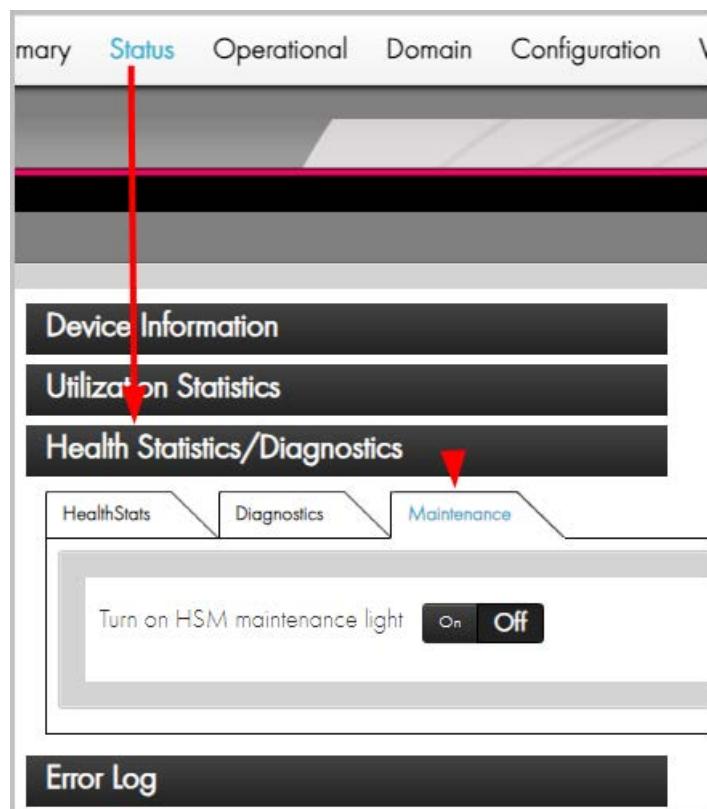
To run test(s) immediately, check the box next to the test and select the “Run Tests Now” button. After a short time, the results are displayed next to the test.

When in Offline or Secure state, you can change the automatic run time by selecting the  control to the right of the self-test time. The prompt appears.



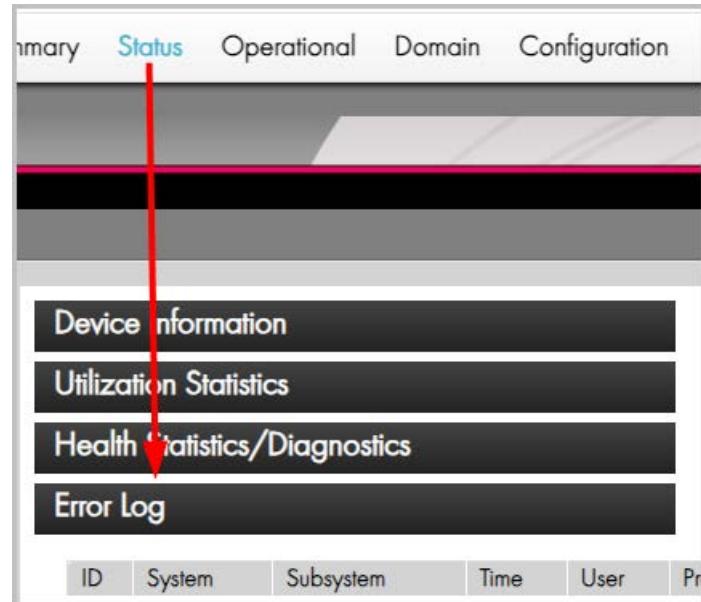
Note: For the self-tests to be run at the desired time, the HSM Date and Time must be correctly set.

9.7.3.3 Maintenance



The payShield 10K has a service light on the front and rear panel of the HSM. This light can be toggled on or off only through payShield Manager or directly in front of the payShield using the On/Off button. This light is for informational purposes only and does not impact the status of the payShield 10K in any manner other than turning on the blue service light in on the front and rear panels of the payShield. If the service light is turned on or off, it will be recorded as an event in the Audit Log.

9.7.4 Error Log



Error Log							
ID	System	Subsystem	Time	User	Process	File	Message
1	3	24	Jul 10 16:41:55 2023	bullshark	healthmon:	healthmon_1358	Power Supply 1 voltage is invalid
2	3	24	Jul 10 16:41:55 2023	bullshark	healthmon:	healthmon_1248	CPLD status AC_POWER_SUPPLY_1_12V bit is asserted
3	3	24	Jul 10 16:47:50 2023	bullshark	healthmon:	healthmon_1400	Power Supply 1 voltage is invalid
4	3	24	Jul 10 16:47:50 2023	bullshark	healthmon:	healthmon_1289	CPLD status AC_POWER_SUPPLY_1_12V bit is asserted
5	3	24	Jul 11 12:27:30 2023	bullshark	healthmon:	healthmon_1400	Power Supply 1 voltage is invalid
6	3	24	Jul 11 12:27:30 2023	bullshark	healthmon:	healthmon_1289	CPLD status AC_POWER_SUPPLY_1_12V bit is asserted
7	3	24	Jul 11 12:42:30 2023	bullshark	healthmon:	healthmon_1400	Power Supply 1 voltage is invalid
8	3	24	Jul 11 12:42:30 2023	bullshark	healthmon:	healthmon_1289	CPLD status AC_POWER_SUPPLY_1_12V bit is asserted
9	3	24	Jul 12 01:20:24 2023	bullshark	healthmon:	healthmon_1400	Power Supply 1 voltage is invalid
10	3	24	Jul 12 01:20:24 2023	bullshark	healthmon:	healthmon_1289	CPLD status AC_POWER_SUPPLY_1_12V bit is asserted

Download Get More Reload Clear

The Error Log stores fault information for use by Thales support personnel. The Error Log is used to log unexpected software errors, hardware failures, and alarm events. Only catastrophic errors cause the HSM to reboot.

For each entry in the log, the following information is displayed:

- ID
- System
- Subsystem
- Time
- User
- Process

- File
- Message

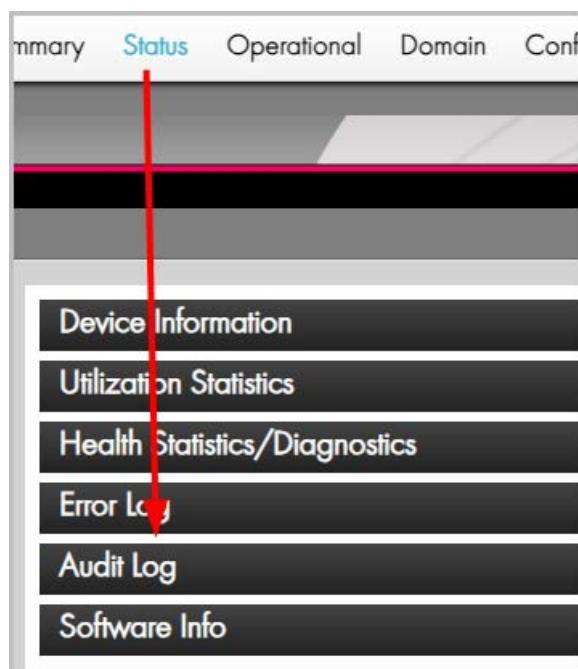
Below the log table there are options to Download, Get More, Reload, and Clear.

Selecting Download retrieves a Comma-Separated-File (CSV) text file (which can be directly imported into a spreadsheet, for example, of all the log entries. Upon completion of the download, the UI displays the SHA-256 Hash of the downloaded file. You can use offline tools to compute the hash yourself and compare it with the value displayed in the UI to ensure that the log is accurate. The hash is computed over the file itself, not the value of its contents. Copy/Pasting the contents into a hash function will give incorrect results.

Note: If the log is very long, it may take a while to retrieve and can impact performance of the HSM.

- Selecting **Get More** returns the next batch of log entries.
- Selecting **Reload** gets the first batch of log entries.
- Selecting **Clear**, which is only available in secure state, clears all error log entries.

9.7.5 Audit Log



Note: The items in the Audit Log includes both:

Configuration > Audit Settings) and

- Items identified via configuration settings page **Configuration > Audit Settings** and
- Items that are included automatically.

Certain sensitive functions, such as key management,.

The screenshot shows the payShield 10K Management Interface. At the top, there is a navigation bar with tabs: Summary, Status, Operational, Domain, Configuration, Virtual Console, Quick Links, and Terminal. The Status tab is currently selected. Below the navigation bar, there is a table with various system status metrics. At the bottom of this section are two buttons: Save and Reset.

Below the table, there are two tabs: Error Log (which is currently active) and Audit Log. The Audit Log tab is shown below, displaying a table of audit records. The table has columns: Counter, Time, Command Code Type, Command Code, Response Code, and Text. Three entries are listed:

Counter	Time	Command Code Type	Command Code	Response Code	Text
305	Apr 03, 2024 16:26:09	A	SE	00	Remote (14818134) - HSM state changed to Secure - Current users: (Right: 5324017424068938 Left: 5324016447068938)
304	Apr 03, 2024 16:26:03	A	02	00	Remote (14818134) - (Client: 10.105.188.128) - Login (Left: 5324016447068938) - Current users: (Right: 5324017424068938 Left: 5324016447068938)
303	Apr 03, 2024 16:25:55	A	KE	00	Smartcard activated: 5324016447068938

At the bottom of the Audit Log table, there are four buttons: Download, Get More, Reload, and Clear. A red arrow points to the Download button, and another red arrow points to the scroll bar on the right side of the table.

The Audit Log can contain up to 100,000 entries for audit records. The audit records are added to the log until it is full and for each subsequent record, the oldest record in the log is deleted to make room for the new one.

Whenever the HSM state is altered through power-up, state changes, or payShield Manager commands, the Audit Log is updated with the Time/Date, the Command Code Type, the Command Code, the Response Code, and a Text field with a brief description.

The Audit Log can be configured to record the execution of any payShield Manager, console or Host command. Configure the Audit Log in the **"Audit Settings"** menu on the "Configuration" page. Refer to [Section 9.10, "Configuration Tab", on page 170](#).

Note: Some events are always audited, even if you have not specified auditing activity.

Below the log table there are options to **Download**, **Get More**, **Reload**, and **Clear**.

The Download option retrieves a Comma-Separated-File (CSV) text file (which can be directly imported into a spreadsheet, for example) of all the log entries. Upon completion of the download, the UI displays the SHA-256 Hash of the downloaded file. Using offline tools, you can manually compute the hash and compare your calculation with the value displayed in the UI, to ensure that the log is accurate.

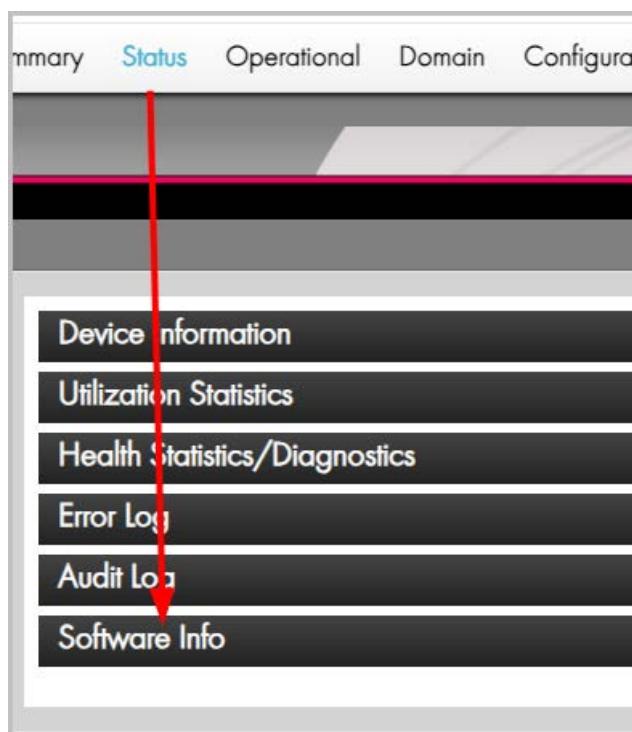
Note: The hash is computed over the file itself, not the value of its contents. Copy/Pasting the contents into a hash function will give incorrect results.

Note: If the log is very long, it may take a while to retrieve and can impact performance of the HSM.

- Selecting **Get More** returns the next batch of log entries
- Selecting **Reload** gets the first batch of log entries
- Selecting **Clear**, which is only available in secure state, clears all error log entries

The Audit Log messages are shown in Appendix F.

9.7.6 Software Info



The Software tab provides information on the versions of the currently installed software and allows new software to be loaded.

9.7.6.1 Software - how to update software

Note: With Release 1.0e, the Software tab has been updated. “Build Number” was changed to “Firmware Version” and a new entry “Deployment Version” has been added. Both fields are used only to assist Thales Support.

The figure below shows both 1.0d and 1.0e screens for clarification purposes.

"Firmware Version" was formerly referred to as "Build Number" and is used to assist Thales Support only

"Deployment Version" was added to assist Thales Support only

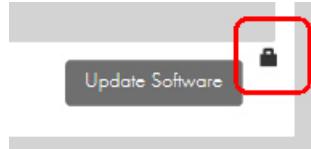
Software	FIPS/Licensing
Base Release	1.0d
Revision	15009020
Build Number	0062
PCI HSM Compliance	Some security settings are not PCI HSM compliant
Bootstrap	1.1.28
AGS Cryptographic Library	1.10.0960
Sensor Processor Application Version	1.1.29
Sensor Processor Boot Version	0.0.1
CPID Version	1.2.3

Software	FIPS/licensing
Base Release	1.0e
Revision	15009021
Firmware Version	1.3.0
Deployment Version	1.3.0
PCI HSM Compliance	Some security settings are not PCI HSM compliant
Bootstrap	1.1.39
AGS Cryptographic Library	1.10.FA73
Sensor Processor Application Version	1.1.29
Sensor Processor Boot Version	1.0.0
CPID Version	1.2.3

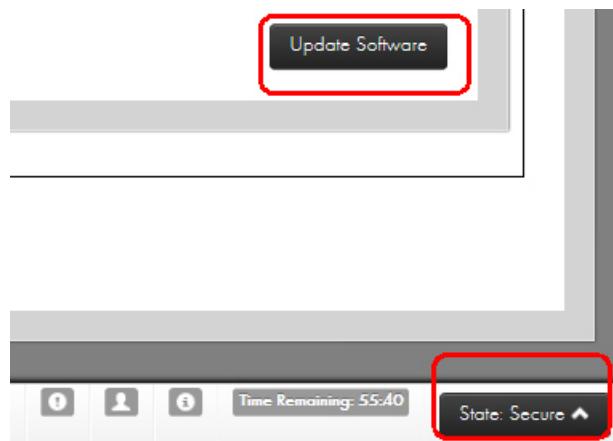
To update software:

1. Both Left and Right Administrators log on.
2. Click the **Secure State**.

Once the state is Secure, the lock image is removed and the Update Software option is enabled.

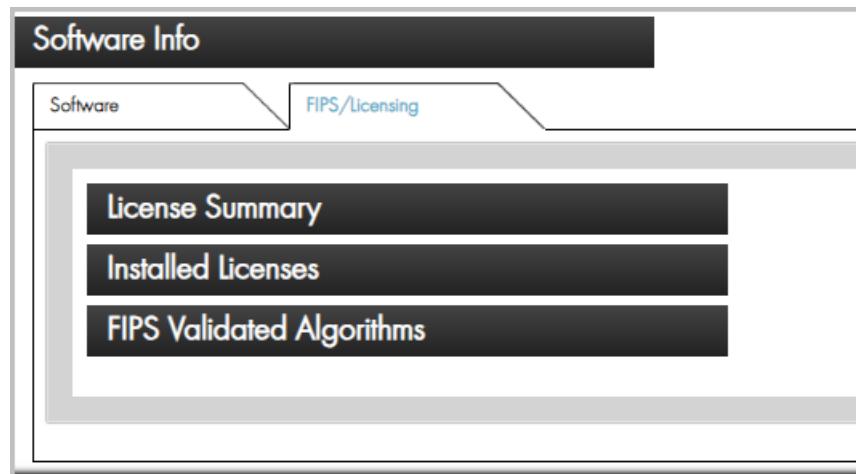


3. Click **Update Software**.



! Software updates can take several minutes. The Health LED located on the front of the unit will switch color during the process; upon completion the LED returns to white.

9.7.7 FIPS/Licensing



The FIPS/Licensing tab has three tabs.

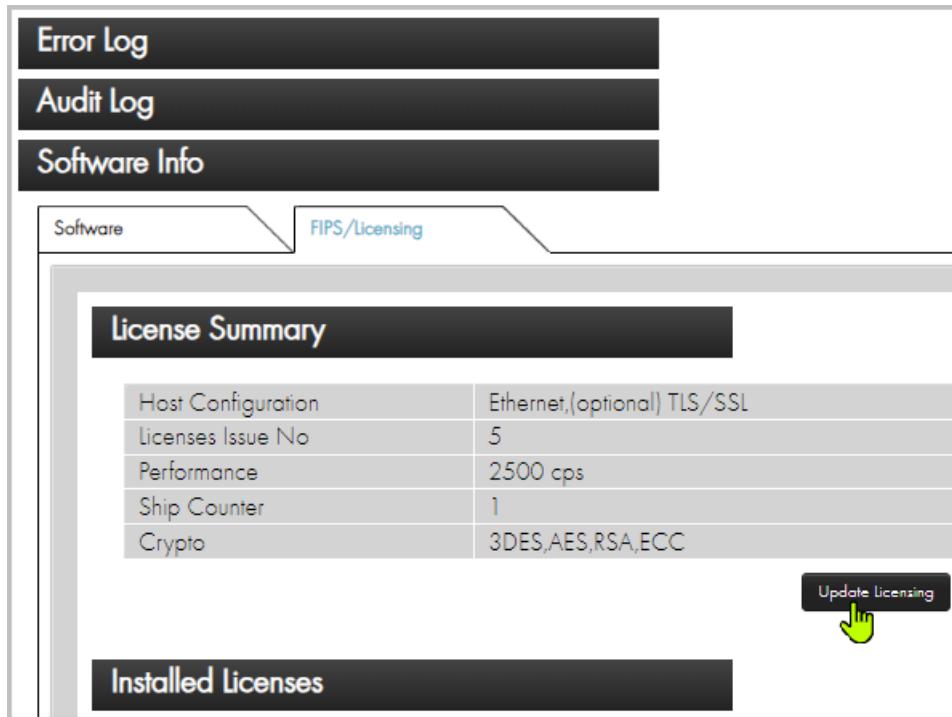
9.7.7.1 License Summary - how to update Licensing

This tab displays data about the connected HSM license information including the performance number, the crypto algorithms licensed in the box, and the number of licensed LMKs.

Host Configuration	Ethernet,(optional) TLS/SSL
Licenses Issue No	5
Performance	2500 cps
Ship Counter	1
Crypto	3DES,AES,RSA,ECC

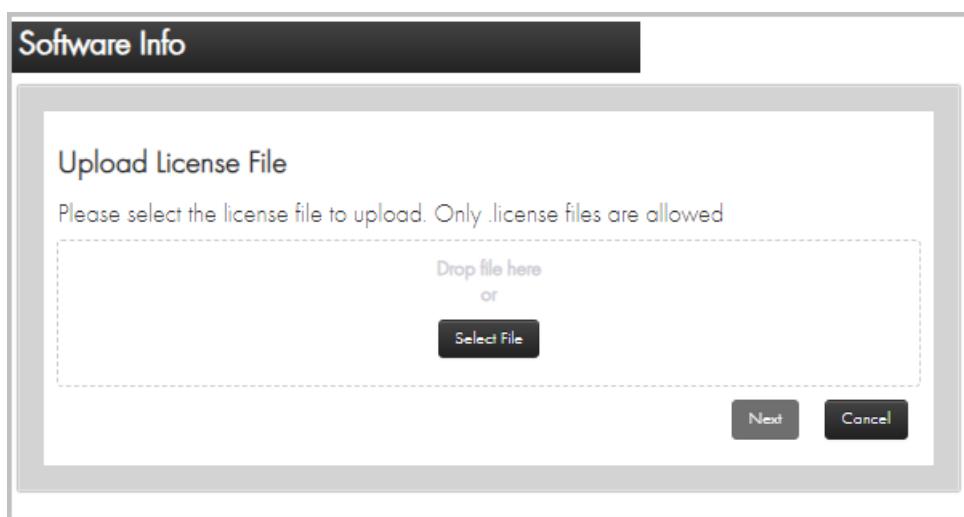
Update Licensing

To update the license:



1. Click **Update Licensing**.

Note: This can be performed from the **Offline** or **Secure** state.



2. Select or drag and drop the file.
3. Click **Next**.
4. Continue as prompted.

9.7.7.2 Installed Licenses

This tab provides a list of all licenses currently installed on the HSM.

The screenshot shows the 'Software Info' section of the payShield 10K software. A red arrow points from the 'Status' tab at the top to the 'Software Info' section. Inside 'Software Info', another red arrow points from the 'FIPS/Licensing' tab to the 'Installed Licenses' tab. The 'Installed Licenses' tab is highlighted. Below it, the 'Premium Package' and 'Optional Licenses' sections are visible.

Premium Package

- Premium Key Management
- Magnetic Stripe Issuing
- Magnetic Stripe Transaction Processing
- EMV Chip, Contactless & Mobile Issuing
- EMV Transaction Processing
- Premium Data Protection

Optional Licenses

- Legacy Commands
- FF1
- LMKx22
- LMKx22
- Remote payShield Manager
- Visa DSP

9.7.7.3 NIST Validated Algorithms

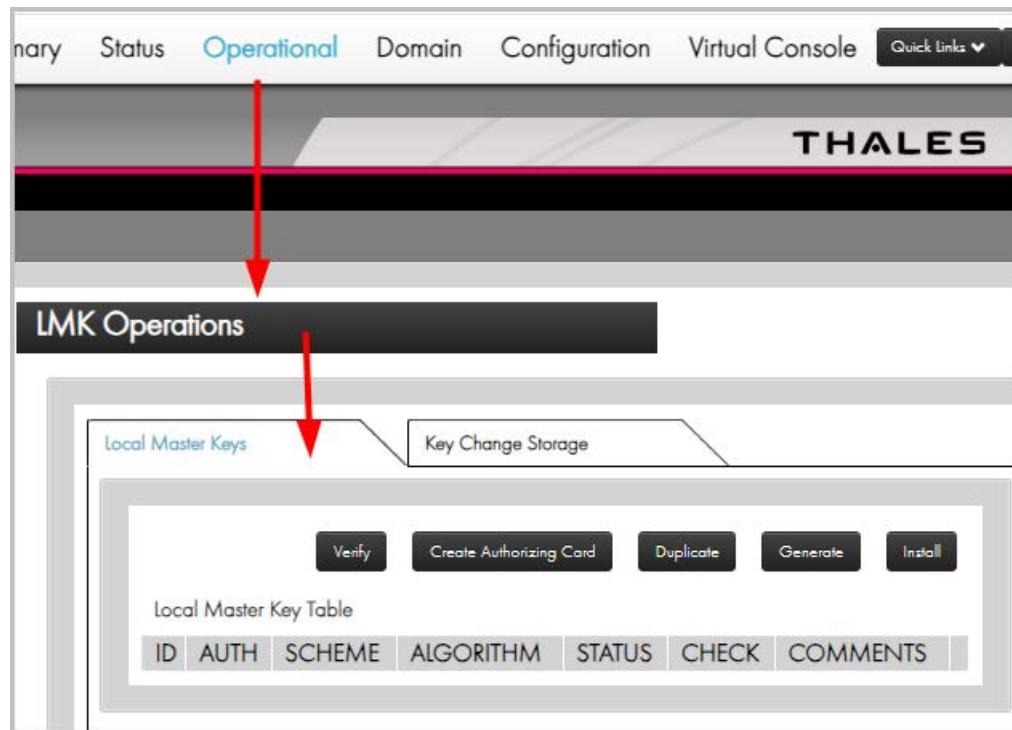
This tab lists all of the currently available NIST Validated Algorithms.

The screenshot shows the software's main interface with several tabs at the top: Primary, Status, Operational, Domain, Configuration, and Virtual Console. The 'Status' tab is highlighted in blue. Below the tabs, there are three dark grey horizontal bars labeled 'Error Log', 'Audit Log', and 'Software Info'. Under 'Software Info', there are two tabs: 'Software' and 'FIPS/Licensing', with 'Software' currently selected. The main content area has a light grey background and displays three sections: 'License Summary', 'Installed Licenses', and 'FIPS Validated Algorithms'. A red arrow points from the 'Status' tab towards the 'FIPS Validated Algorithms' section. Below this section, the heading 'FIPS Validated Algorithms' is followed by a table listing ten entries:

Algorithm	Description	Status
DRBG/RNG	TASP-DRBG v1.1	Approved
SHA	TASP-SHA v1.0	Approved
HMAC	TASP-HMAC v1.0	Approved
TDES	TASP-TDES v1.0	Approved
AES	TASP-AES v1.0	Approved
CMAC	TASP-CMAC v1.0	Approved
RSA	TASP-RSA v1.0	Approved
AES	TASP-AES v1.0	Approved
TDES	TASP-TDES v1.0	Approved
ECC	TASP-ECC v1.0	Approved

9.8 Operational

The Operational section handles all functions relating to Local Master Keys.



9.8.1 Local Master Keys

Note: Each LMK has its own security setting.

LMKs are used to encrypt operational keys used for encryption, MACing, digital signing, etc. LMKs are secret, internal to the HSM, and do not exist outside of the HSM except as components or shares held in Smart Cards. Each HSM can have a unique LMK, or an organization can install the same LMKs on multiple HSMs within a logical system.

LMKs provide separation between different types of keys to ensure that keys can be used only for their intended purpose. The payShield 10K supports two types of LMK, both of which provide key separation:

- **Variant LMKs.** These are double- or triple-length Triple-DES keys and provide key separation by encrypting different types of key with different variants of the LMK. Double-length Variant LMKs have been in use for many years, and are the most widely used type of LMK. Triple-length Variant LMKs were introduced for later versions of the payShield.
- **Key Block LMKs.** These are either triple-length Triple-DES keys, or 256-bit AES keys, and key separation is provided by parameters in the key block which govern characteristics such as usage and exportability of the protected key.

Key Block LMKs are newer technology than Variant LMKs and so are still less widely used, but provide security benefits.

This tab provides a table that shows and allows the management of all loaded LMKs stored in the tamper-proof area of memory in the HSM.

The LMK holders become what are called the “**trusted officers**” because they hold components or shares of the Master Key that encrypts all other keys as well as two of the (up to 9 possible component holders). They also become “**authorizing officers**” (not to be confused with the administrators) and can authorize key management functions such as generating, importing or exporting keys. They can also authorize changes to configuration settings and other sensitive functions.

9.8.1.1 Generate LMK - create trusted officer

Prerequisite: Your Smart Card has already been commissioned, i.e., it already has the Security Domain stored on it.

To determine your status, navigate to **Summary > Local Master Key**. In the example below, you see that there are no LMKs listed.

The screenshot shows a software interface with a navigation bar at the top containing links: Summary, Status, Operational, Domain, Configuration, Virtual Console, and Quick Links. The THALES logo is visible on the right side of the header. Below the header, there are four dark grey buttons labeled "Summary Dashboard", "Health Dashboard", "Configuration Dashboard", and "Local Master Key". The "Local Master Key" button is highlighted with a light blue background and a yellow hand cursor is positioned over it. Below these buttons, there are two tables. The first table is titled "Local Master Key Table" and has columns: ID, AUTH, SCHEME, ALGORITHM, STATUS, CHECK, and COMMENTS. The second table is titled "Key Change Storage Table" and has columns: ID, OLD/NEW, SCHEME, ALGORITHM, STATUS, CHECK, and COMMENTS.

By design, when you created your Left and Right LMK cards, no data is stored on the cards. The Left and Right LMK cards are used for things that do store data on cards.

For example, they are used for creating:

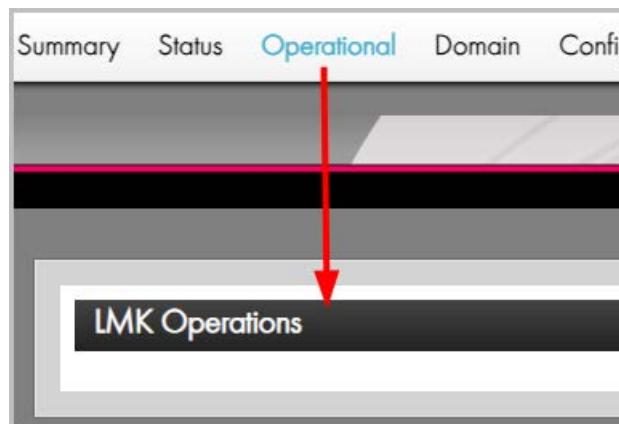
- CTA shares
- LMK shares
- Settings

To add “authorizing officer” functionality to your Left and Right LMK, follow the steps below.

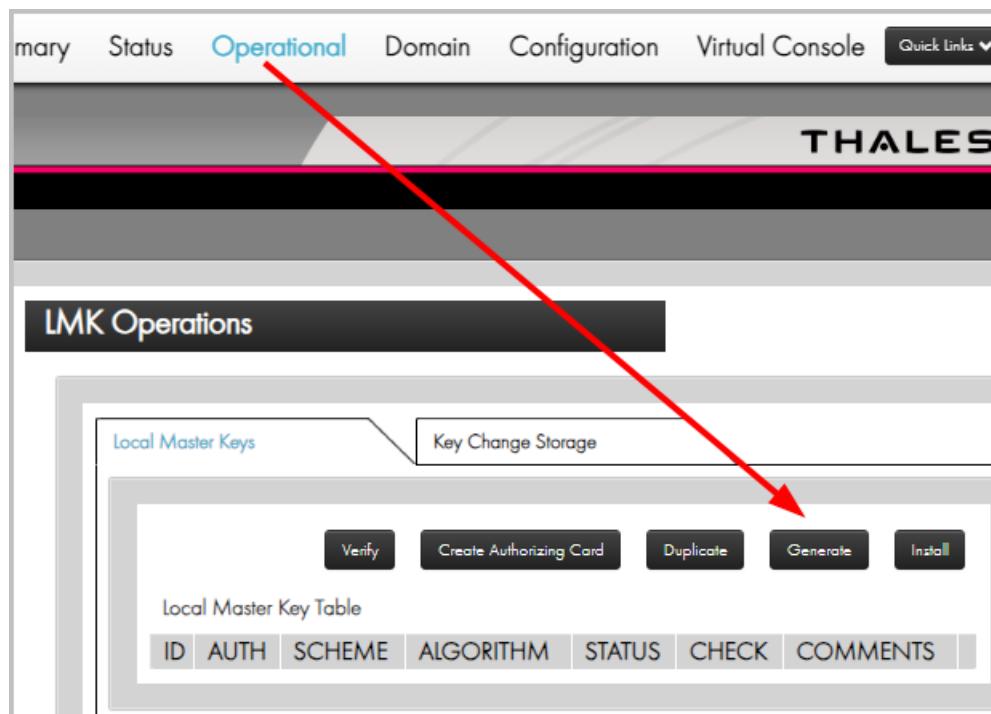
1. Verify that you are in the **Secure** state.



2. Navigate to the **Operational** tab.



3. Expand **LMK Operations**.



4. Click **Generate**.

The Generate LMK screen displays showing the default settings.

mary Status **Operational** Domain Configuration Virtual Console Quick Links ▾ Terms

THALES

LMK Operations

Generate LMK

Number of LMK shares to create (2 - 9) You will need this many commissioned payShield Manager Smart Cards.	2
Number of shares to rebuild LMK (2 - 2)	2
Scheme	Variant
Algorithm	2DES
Status	Live

Next Cancel

5. Enter your preferred settings from the drop downs:

LMK Operations

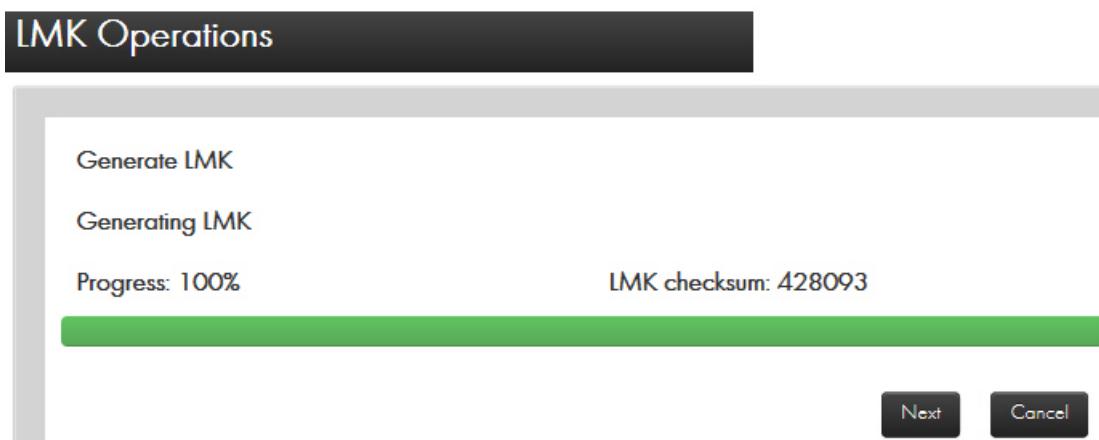
Generate LMK

Number of LMK shares to create (2 - 9) You will need this many commissioned payShield Manager Smart Cards.	2
Number of shares to rebuild LMK (2 - 2)	2
Scheme	Variant
Algorithm	Variant Keyblock
Status	Live

Next Cancel



6. Click **Next**.

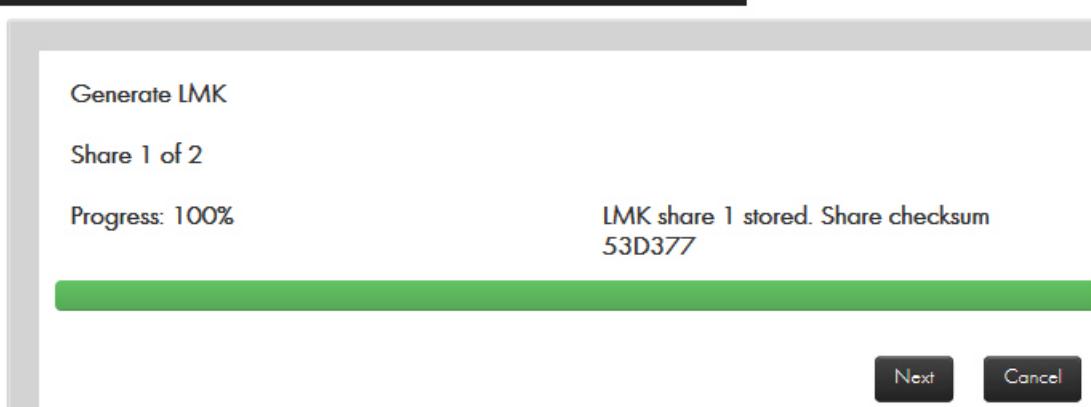


7. Click **Next**.



8. Insert your Smart Card into the card reader, enter the PIN, and press **OK**.

LMK Operations



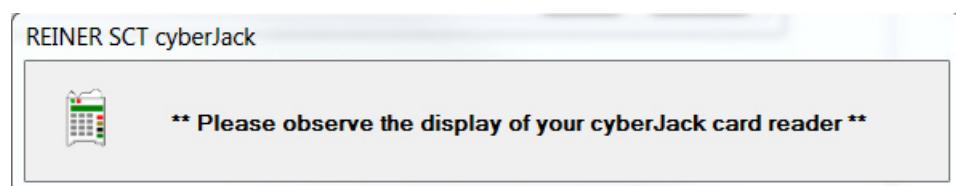
9. Click **Next**.

Generate LMK

Remove the smart card from:
REINER SCT cyberJack secoder TLS USB 1

Cancel

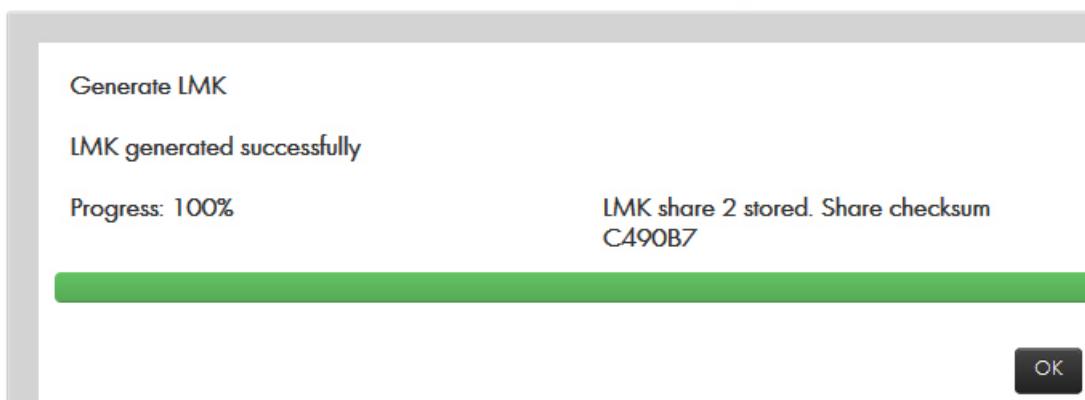
10. Remove your Smart Card from the card reader.



11. Insert the second Smart Card into the card reader.

12. Enter your PIN and press **OK**.

LMK Operations



13. Click **OK**.

Generate LMK

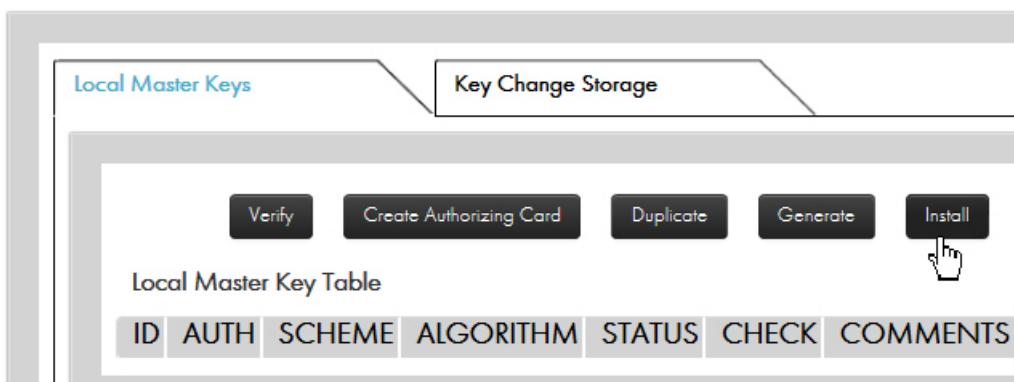
Remove the smart card from:
REINER SCT cyberJack secoder TLS USB 1

Cancel

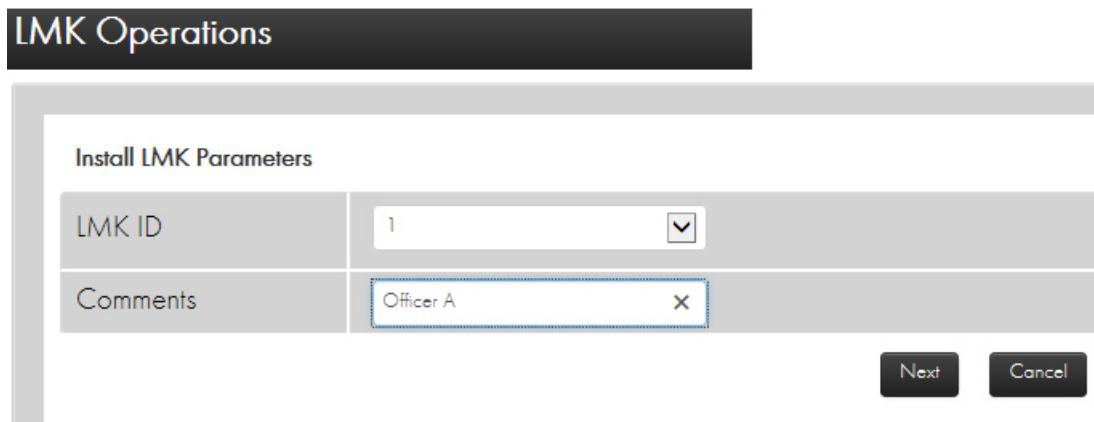
14. Remove the Smart Card from the card reader.

15. Click **Install**.

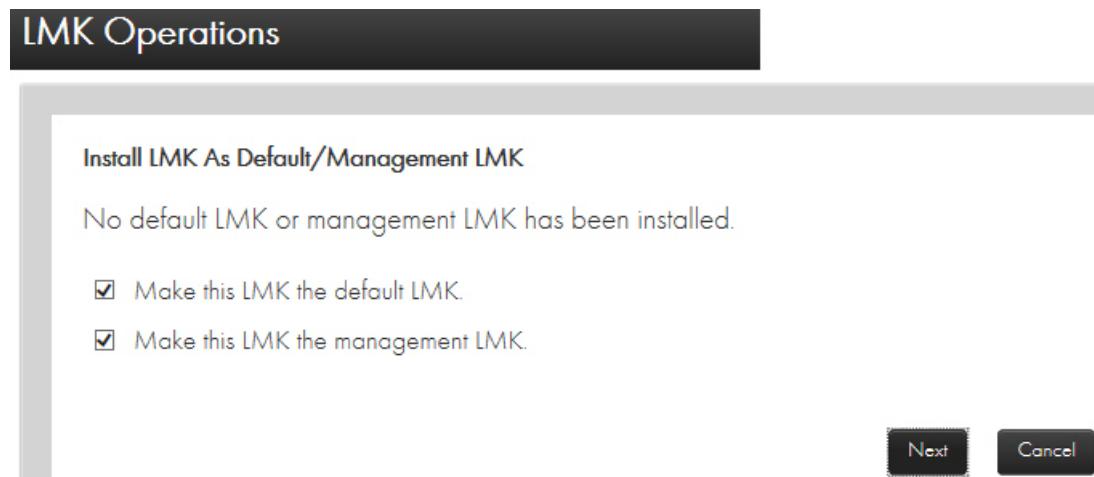
LMK Operations



16. Enter the LMK Parameters.

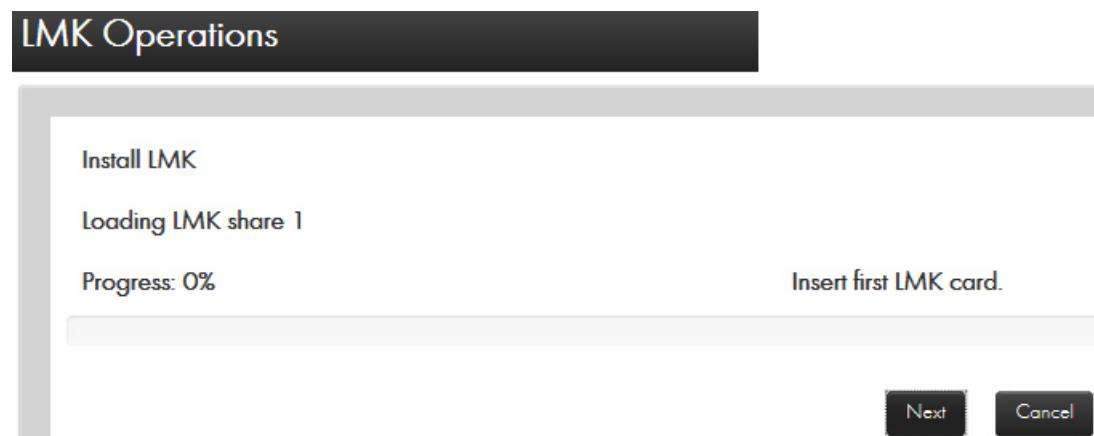


17. Click **Next**.



18. Click your preferences or use the default settings.

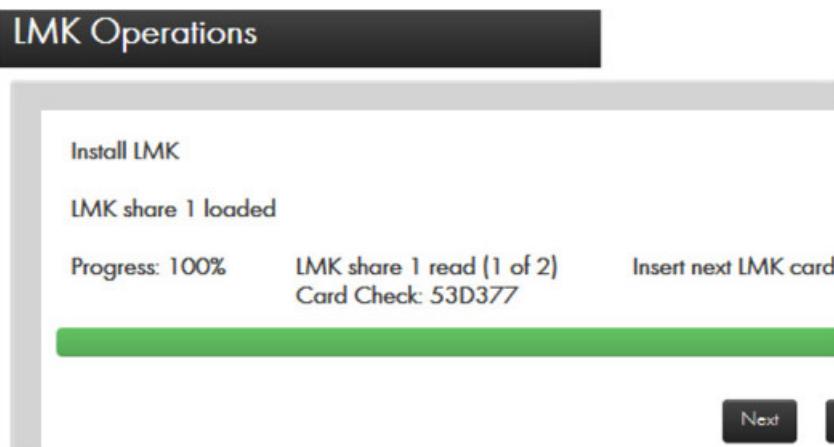
19. Click **Next**.



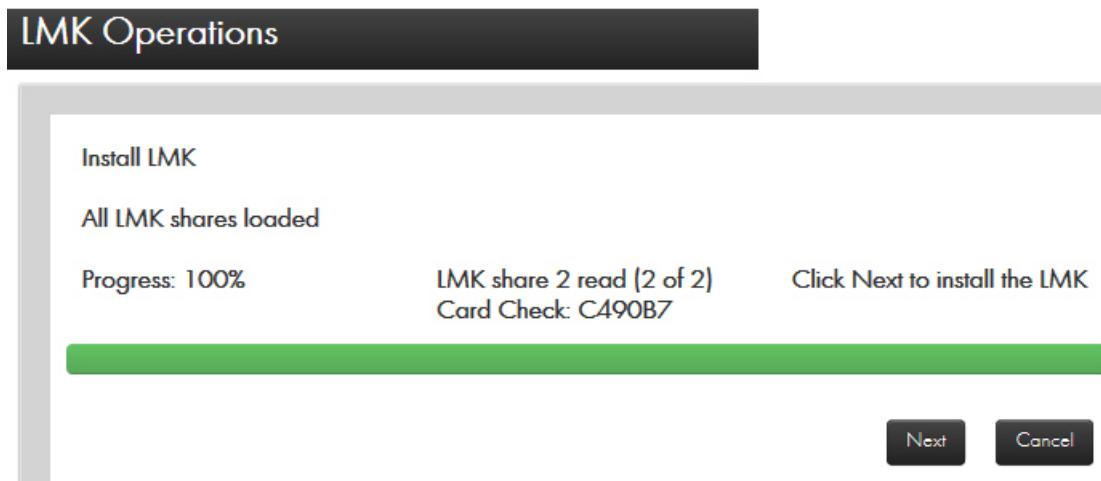
20. Follow the prompt and insert the first LMK card and then enter your PIN.



21. Select **OK**.
22. Insert the next LMK card, enter your PIN and press **OK**.

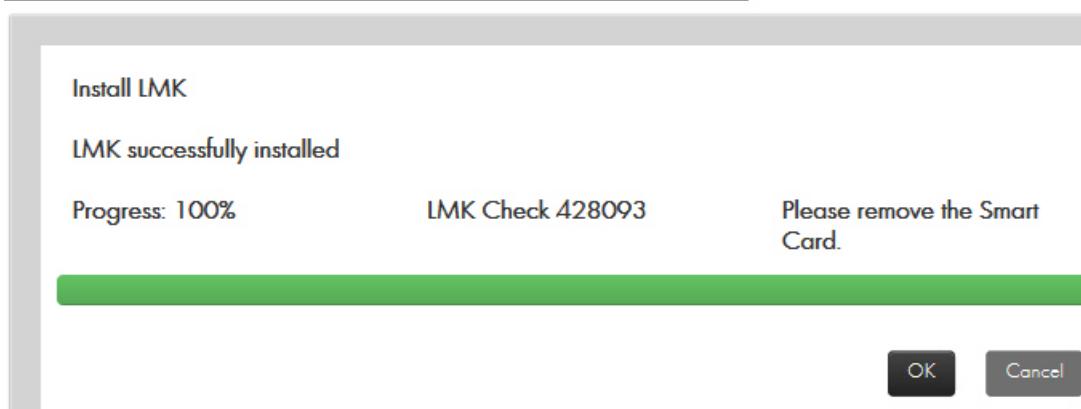


23. Click **Next** to install the LMK.



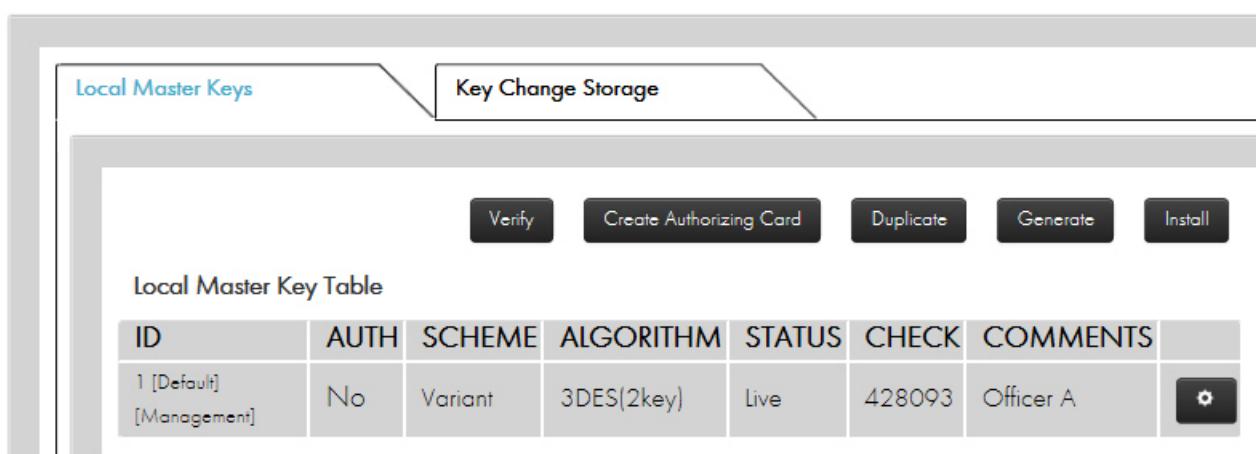
24. Remove the Smart Card from the reader.

LMK Operations



25. Click **OK**.

LMK Operations



The Local Master Key Table populates.

9.8.1.2 Verify an LMK Card

1. Click **Verify**.
2. Insert one of the cards of the card set containing the RLMK you wish to verify.
3. Enter the PIN.
4. Select **OK**.

The HSM will read the LMK data from the card, and when completed will display a table showing the following:

- LMK Share
- Quorum Size

- Scheme
- Algorithm
- Status
- Checksum

9.8.1.3 Create an Authorizing Card

When in Offline or Secure state, you can create an Authorizing Card (used to enter Authorized state) for a RLMK card.

Prerequisite: The payShield 10K is in the Offline or Secure state.

1. Click **Create Authorizing Card**.

A system prompt displays.

2. Insert the RLMK card that you wish to create an Authorizing Card for.

3. Enter the card's PIN.

The system reads the RLMK card and prompting displays.

4. Insert a **prior commissioned card** to use as an Authorizing Card.

5. Enter the Authorizing card's PIN.

6. Remove the Authorizing Card upon completion.

7. Click **OK**.

9.8.1.4 Duplicate an LMK Card

Prerequisite: The payShield 10K is in the Secure state.

1. Click **Duplicate Card**.

A system prompt displays.

2. Insert the RLMK card that you wish to duplicate.

3. Enter the card's PIN.

The system reads the RLMK card.

4. Click **OK**.

A system prompt displays.

5. Remove the RLMK card.

6. Insert a **prior commissioned card**.

7. Enter the card's PIN.

The system duplicates the card.

8. Remove the new card.
9. Click **OK**.

9.8.1.5 Generate an LMK

You can create a new LMK to be stored on RLMK cards.

Prerequisite: The payShield 10K is in the Secure state.

1. Click **Generate**.

A system prompt displays.

2. Follow the prompts and enter the following information about the new LMK:

- Number of LMK shares (Default: 2)
- Number of shares to rebuild (Default: 2)
- Key scheme (Variant or Key Block)
- Algorithm
- Status (Live or Test)

3. Click **Next**.

A LMK is generated and a checksum displayed.

4. Click **Next**.

A system prompt displays.

5. Insert a **prior commissioned card** to write the LMK share to.

6. Enter the card's PIN.

When the HSM is finished writing to the card, it displays a checksum for that LMK share.

7. Click **Next**.

8. Repeat this process until all shares have been written.

9. When complete, click **OK** to return to the main LMK screen.

9.8.1.6 Install an LMK from RLMK Card Set

1. Click **Install**.

2. Specify the ID for the new LMK as well as a brief comment describing the LMK.

3. Click **Next**.

4. Insert the RLMK card containing the first LMK share for the new LMK.

5. Enter the card's PIN.

6. Continue inserting LMK share cards when prompted until the entire LMK has been read from the card set.

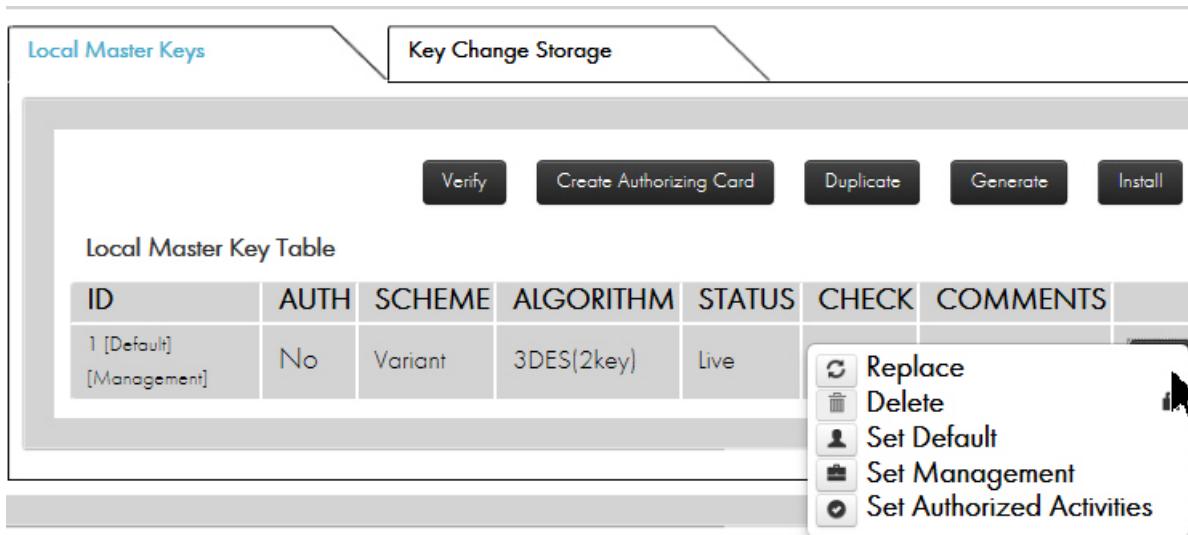
7. When all cards have been read, click **Next** to install the LMK.
8. Once installed, remove the last card or click **OK** to return to the main LMK screen.

Note: The first 2 RLMK cards will contain the authorizing password used to enter authorized state.

9.8.1.7 Delete an Installed LMK

In Secure state and authorized under the LMK you wish to delete, you can delete an LMK that has already been installed.

1. Click the  button next to the LMK that you wish to remove.
2. Click **Delete**.



3. When prompted, click **OK** to confirm the deletion.

Note: You cannot delete the current Default LMK without first assigning a new Default LMK.

9.8.1.8 Replace an installed LMK

Prerequisite: The payShield 10K is in the Secure state.

1. Click the  button next to the LMK you wish to replace.
2. Click **Replace**.
3. Specify the LMK ID for the new LMK as well as a brief comment describing the LMK.
4. Click **Next**.
5. Insert the RLMK card containing the first LMK share for the new LMK.
6. Enter the card's PIN.
7. Continue inserting LMK share cards when prompted until the entire LMK has been read from the card set.

8. When all cards have been read, click **Next** to install the LMK.
9. Once installed, remove the last card or click **OK** to return to the main LMK screen.

9.8.1.9 Set the Default LMK

The Default LMK is a specified LMK (when using Multiple LMKs) to provide a backward compatible mode of use for the HSM.

Prerequisite: The payShield 10K is in the Secure state.

1. Click the  button next to the LMK that you want to make the Default LMK.
2. Click **Set Default**.
3. When prompted to confirm, click **OK**.

9.8.1.10 Set the Management LMK

The Management LMK is a specified LMK (when using Multiple LMKs) that is used by the HSM for purposes that are not linked to a particular LMK; for example, authenticating audit trail records.

Prerequisite: The payShield 10K is in the Secure state.

1. Click the  button next to the LMK that you want to make the Management LMK.
2. Click **Set Management**.
3. When prompted to confirm, click **OK**.

9.8.1.11 Enter Authorized State

Authorized State is a mode of operation of the HSM that permits one or more specified sensitive functions to be performed. It requires two Authorizing Officers using their Smart Cards and PINs to confirm the activity.

In any state, you may enter Authorized state by clicking the  button next to the LMK you wish to authorize and select **Set Authorized Activities**.

Depending on the authorization mode selected (single or multi-authorization) from the initial security settings, you will either begin to enter the authorized state (in single authorization mode) or be presented with a menu of authorized activities (in multi-authorization mode).

Note:

- Remote authorization will not work if the Initial Security setting “Use default card issuer password” is checked. The payShield Manager only allows Authorization using Smart Cards.
- Authorized activities may continue, as specified in the authorization, even after the payShield Manager session has terminated. For example, suppose the Console PIN activity has been authorized for 300 minutes using the payShield Manager. The activity will remain authorized for 300 minutes regardless of the state of the payShield Manager.

Configure Authorized Activities

Activities authorized here will remain authorized until the configured time has elapsed. The activities will continue to be authorized even if your session ends before that time. This applies to both console and remote activities.

Category	Subcategory	Authorization
admin		<input checked="" type="radio"/> Not Authorized <input type="radio"/> Authorized For [] Minutes <input type="radio"/>
audit		<input checked="" type="radio"/> Not Authorized <input type="radio"/> Authorized For [] Minutes <input type="radio"/>
command		<input checked="" type="checkbox"/> Not Authorized <input type="checkbox"/> Authorized For [] Minutes <input type="checkbox"/>
component		<input checked="" type="checkbox"/> Not Authorized <input type="checkbox"/> Authorized For [] Minutes <input type="checkbox"/>
		<input checked="" type="radio"/> Not Authorized <input type="radio"/> Authorized For [] Minutes <input type="radio"/>

9.8.1.12 Single Authorization Mode

You will be prompted to enter a card containing the first of the LMKs authorizing PIN. Insert the card and enter the PIN. You will then be prompted to enter a card containing the second of the LMKs authorizing PIN. Insert the card and enter the PIN. Upon success, the activities will be authorized following the rules for single authorization mode.

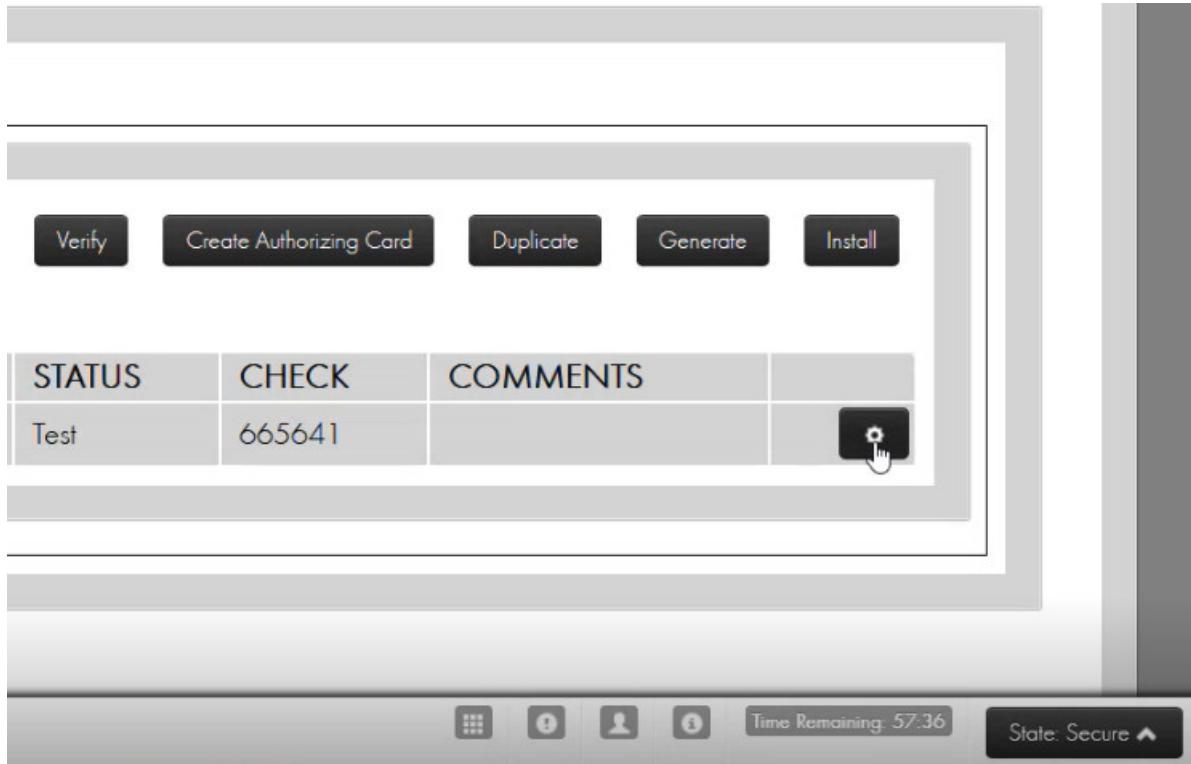
9.8.1.13 Multiple Authorization Mode

You will be presented with two tabs displaying the Host and Console commands, which you can authorize. Place check marks next to the commands that you want to authorize. Additionally, you can specify that the authorization for each command should persist or last for a specified amount of time. For convenience, at the bottom of each tab there are two buttons to allow for adding or removing authorization for all commands. When you are finished Clicking commands, click “**Next**”.

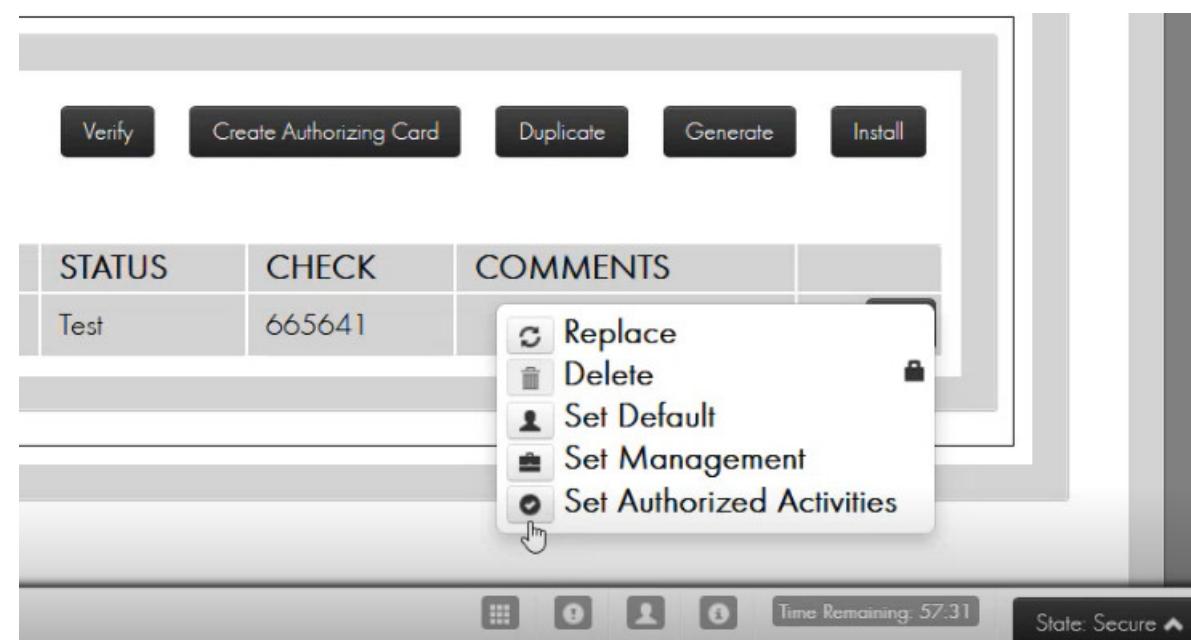
You will be prompted to enter a card containing the first of the LMKs authorizing PIN or passwords. Insert the card and enter the PIN. You will then be prompted to enter a card containing the second of the LMKs authorizing passwords. Insert the card and enter the PIN. Upon success, the activities will be authorized following the rules for single authorization mode.

9.8.1.14 Configuring Authorized Activities

1. Click the  button.



The drop down menu opens.



2. Select **Set Authorized Activities**.

The system responds:

10K Operations

Configure Authorized Activities

Activities authorized here will remain authorized until the configured time has elapsed. The activities will continue to be before that time. This applies to both console and remote activities.



Category	Subcategory	Authorization			
admin		<input checked="" type="radio"/> Not Authorized	<input type="radio"/> Authorized For	0	Minutes
audit		<input checked="" type="radio"/> Not Authorized	<input type="radio"/> Authorized For	0	Minutes
command		<input checked="" type="radio"/> Not Authorized	<input type="radio"/> Authorized For	0	Minutes
component		<input checked="" type="radio"/> Not Authorized	<input type="radio"/> Authorized For	0	Minutes

- To authorize the Admin, open the **Console** tab and select **Authorized For**.



Subcategory	Authorization
	<input checked="" type="radio"/> Not Authorized <input type="radio"/> Authorized For
	<input checked="" type="radio"/> Not Authorized <input type="radio"/> Authorized For

- Select **Next** to register your selection.



The system processes your selection:

LMK Operations

Configure Authorized Activities

Transmitting authorized activities.

Please wait (may take a while) ...

- Follow the prompts as you re-enter your security credentials.

LMK Operations

Configure Authorized Activities

Progress: 0%

Insert a card containing the LMK's first authorizing password.



Next

9.8.1.15 Key Change Storage

This tab provides a table that shows and allows the management of the Key Change Storage table, which is a tamper-proof area of memory in the HSM that stores “old” LMK(s), used to permit translation of keys following an LMK change.

Local Master Keys	Key Change Storage					
Key Change Storage Table						
ID	OLD/NEW	SCHEME	ALGORITHM	STATUS	CHECK	COMMENTS

9.8.1.16 Install LMK from RLMK card set

When authorized under the given LMK and in secure state you can install an “old” LMK into the same ID for that LMK of the Key Change Storage table by clicking the “**Install**” button.

Note: You can install an “old” LMK in the Key Change Storage table when there is an LMK in the same ID of the LMK table. For example, if there is an LMK in ID 1, you may install an “old” LMK in ID 1 of the Key Change Storage table.

Install LMK

An LMK already exists for this slot. All existing LMKS for this slot will be erased upon installation of new LMK. Do you wish to proceed?

OK **Cancel**

Specify the ID for the old LMK as well as a brief comment describing the LMK and click “**Next**”. Insert the RLMK card containing the first LMK share for the LMK and enter the card’s PIN. Continue inserting LMK share cards when prompted until the entire LMK has been read from the card set. When all cards have been read, click “**Next**” to install the LMK. Once installed, remove the last card or click “**OK**” to return to the main LMK screen.

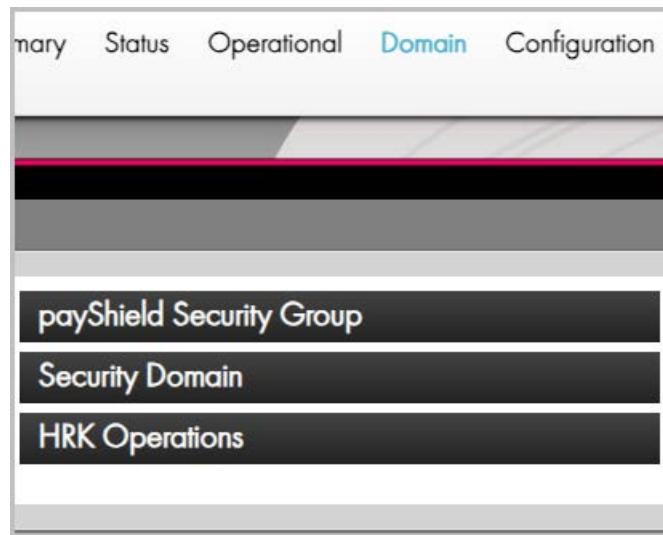
9.8.1.17 Delete an installed LMK

In Secure state, you can delete an old LMK that has already been installed by clicking on the  button next to the old LMK you wish to remove and Click “**Delete**”. When prompted, click “**OK**” to confirm that you want to delete.

9.8.1.18 Replace an Old LMK

In Secure state and authorized under the desired LMK, you can replace an installed old LMK by clicking on the  button next to the LMK you wish to replace and click “**Replace**”. The ID for the old LMK is pre-set (and cannot be changed). Enter a brief comment describing the LMK and click “**Next**”. Insert the RLMK card containing the first LMK share for the LMK and enter the card’s PIN. Continue inserting LMK share cards when prompted until the entire LMK has been read from the card set. When all cards have been read, click “**Next**” to install the LMK. Once installed, remove the last card or click “**OK**” to return to the main LMK screen.

9.9 Domain



9.9.1 payShield Security Group

payShield Security Group

The following smartcards are members of this HSM's security group:

Smart Card Type	Serial Number	Certificate Number (Hexadecimal)
Left Key Cards	5324016447068938	C021E13F21948098 [lock icon] [minus icon] [plus icon]
Right Key Cards	5324017424068938	F9EC9ECB9B547F3C [lock icon] [minus icon] [plus icon]
Restricted Cards		

Undo **Apply**

Security Domain

HRK Operations

In this tab, you can control which RACCs are usable as Left, Right and Restricted Key Cards. Each section provides a list of all card serial numbers that are usable as that type of card. To remove a card, click the minus icon next to the card you want to remove. Note that you cannot remove the last of either the Left or Right Key Card.

If both a Left and Right Key Card have logged into the HSM, you may add a new card (independent of the HSM's state) by entering the Key Card's serial number and Certificate Number in the text box for the appropriate section and click the plus icon. Select the “**Apply**” button after adding all the desired card serial numbers.

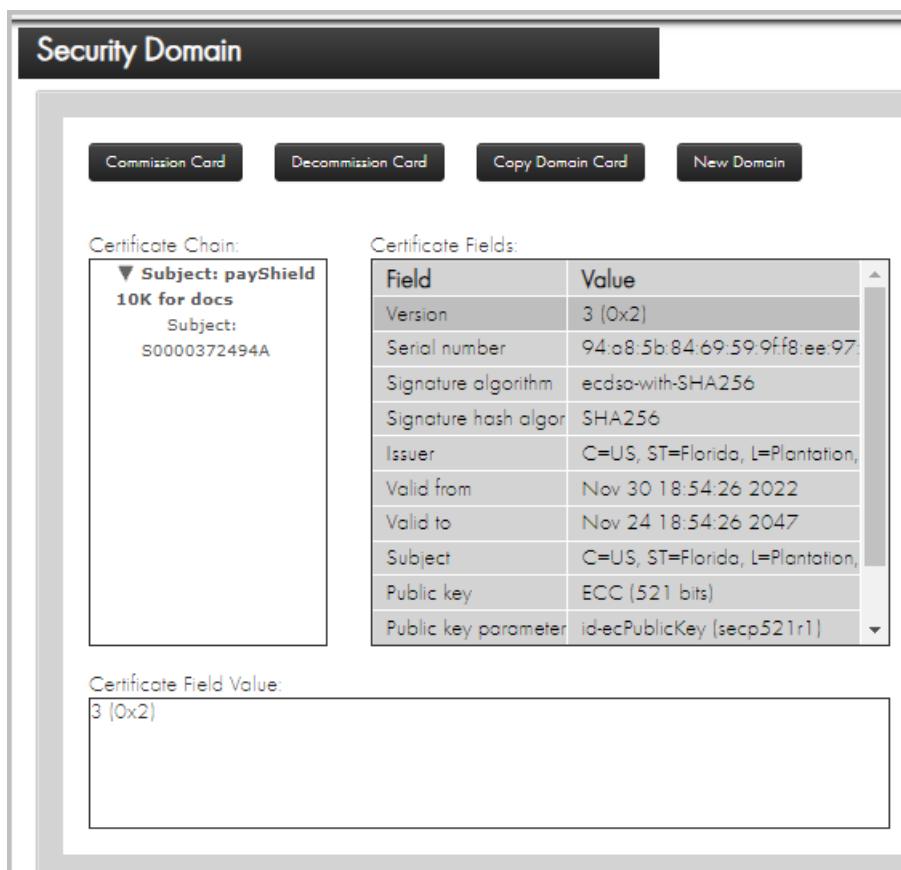
Note:

To get the Smart Card's Certificate Number:

- Remove any Smart Card currently inserted in the Smart Card reader
- Select the  button on the bottom right of the main page
- Click to view the Smart Card Details
- Insert the Smart Card you wish to add to the whitelist in the Smart Card reader

9.9.2 Security Domain

In this tab, you control the domain and cards. Additionally, a table is displayed showing information on the loaded certificates.



The screenshot shows the 'Security Domain' tab interface. At the top, there are four buttons: 'Commission Card', 'Decommission Card', 'Copy Domain Card', and 'New Domain'. Below these buttons, there are two sections: 'Certificate Chain' and 'Certificate Fields'.

Certificate Chain:

```

▼ Subject: payShield
  10K for docs
    Subject:
    S0000372494A
  
```

Certificate Fields:

Field	Value
Version	3 (0x2)
Serial number	94:a8:5b:84:69:59:9f:f8:ee:97
Signature algorithm	ecdsa-with-SHA256
Signature hash algor	SHA256
Issuer	C=US, ST=Florida, L=Plantation,
Valid from	Nov 30 18:54:26 2022
Valid to	Nov 24 18:54:26 2047
Subject	C=US, ST=Florida, L=Plantation,
Public key	ECC (521 bits)
Public key parameter	id-ecPublicKey (secp521r1)

Certificate Field Value:

```

3 (0x2)
  
```

The following sections describe the available operations.

9.9.2.1 Commission a Smart Card

When you commission a Smart Card, you are adding it to a security domain.

Note: As described below, you may commission a card by clicking on the “**Commission Card**” button. Click “**Next**” to begin. When prompted, enter the first CTA card and enter the card’s PIN. Continue entering cards when prompted until the entire CTA card set has been loaded.

When the entire CTA has been loaded, you will be shown a table containing information on the security domain. Click “**Next**” to commission your new cards. When prompted, enter the card (either a new Smart Card or a card that was previously commissioned) to commission, and enter the card’s new PIN. When the card has been commissioned, you may continue to commission additional cards by clicking “**Next**”.

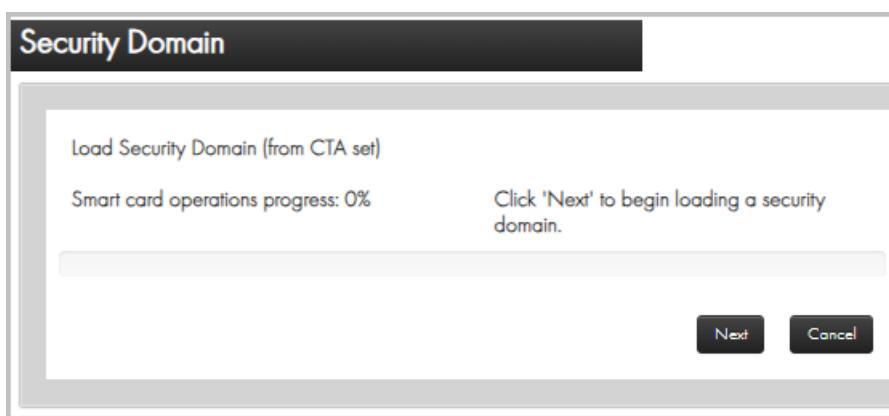
Prerequisite:

You have logged on and the HSM is in the **Secure** state.



1. Navigate to: **Domain > Security Domain**
2. Click **Commission Card**.

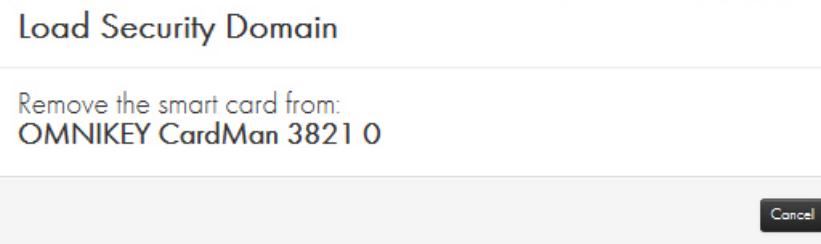
The Loading screen displays with prompts.



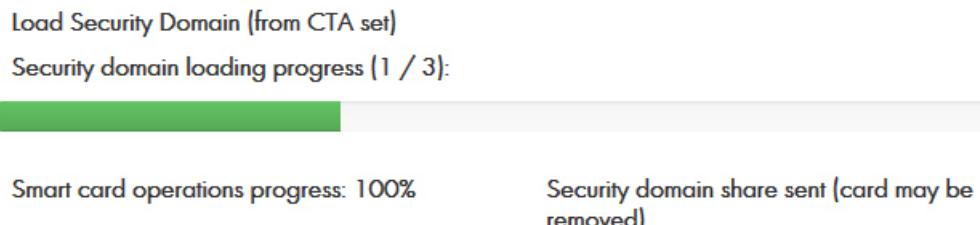
3. Insert one card from your existing CTA into the card reader.

Note: You must move efficiently, as this operation will timeout.

4. Click **Next**.

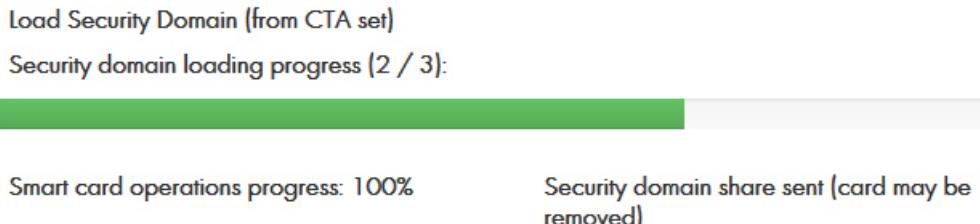


5. Click **Next**.

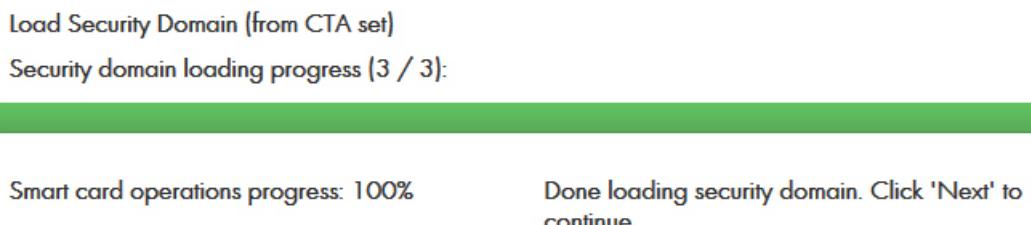


Next **Cancel**

6. Click **Next**.



Next **Cancel**



Next **Cancel**

7. Click **Next**.

Security Domain

Security Domain Parameters	
Total Number of Security Domain Shares	3
Size of Security Domain Shares Quorum	3
Country	
State	
Locality	
Organization	
Unit	
Common Name	12132
Email	

Next **Cancel**

8. Click **Next**.

Security Domain

Commission Smart Card	
<input checked="" type="checkbox"/> User must change PIN on first use	
Smart card operations progress: 0%	None
<div style="height: 40px;"></div>	

Next **Cancel**

9. Click **Next**.

Commission Smart Card

Insert the smart card to be commissioned into:
OMNIKEY CardMan 3821 0

Cancel

10. Enter your PIN and press **OK**.

11. Enter the new PIN two times followed by **OK**.

Note: Follow this link, should you need to return to: [Section 3.6, “Migrate LMK Cards to become RLMK Cards”, on page 345](#).

9.9.2.2 Decommission a Card

Decommissioning a card is essentially erasing the certificates from it. Once decommissioned, the card cannot be used in an HSM until it has been commissioned again.

In any state, you may decommission a card by clicking on the “**Decommission Card**” button. Click “**Next**” to begin. Click “**OK**” in the warning dialogue to continue. When prompted, insert the card you want to decommission.

9.9.2.3 Copy a Domain Card

In Secure state, you may create a duplicate of a domain (CTA share) card by clicking on the “**Copy Domain Card**” button. When prompted, enter the CTA card to be copied and enter the card’s PIN.

When prompted, remove the CTA card, insert a prior commissioned card to write the CTA share onto and enter the card’s PIN.

9.9.2.4 Create a New Security Domain

In Secure state, you may create a new Security Domain by clicking on the “**New Domain**” button. You will be prompted to enter the following information:

- Number of Security Domain Shares
- Quorum Size
- Country, State, Location
- Organization, Unit
- Common Name
- Email

Once all information has been entered, click “**Next**” to proceed. When prompted, enter a new or previously commissioned Smart Card (if it is already commissioned, it will confirm that you wish to overwrite the current data) to store the first CTA share and enter a PIN for the card twice. Continue clicking “**Next**” and inserting additional cards until all CTA shares have been written. When finished, click “**Finish**” to return to the Security Domain screen.

9.9.2.5 HRK Operations

The HRK is used to encrypt the HSM’s private key used by the HSM in establishing TLS/SSL sessions for the Host and management interfaces.

This tab is used to change the Administrator passphrases for the HRK.

payShield Security Group

Security Domain

HRK Operations

The HSM Recovery Key (HRK) protects the certificates and private keys that help secure host and management connections, and minimizes the recovery time in the event of an accidental tamper (e.g. caused by the motion sensor).

HRK Installed: Yes

[Change HRK Passphrase](#)

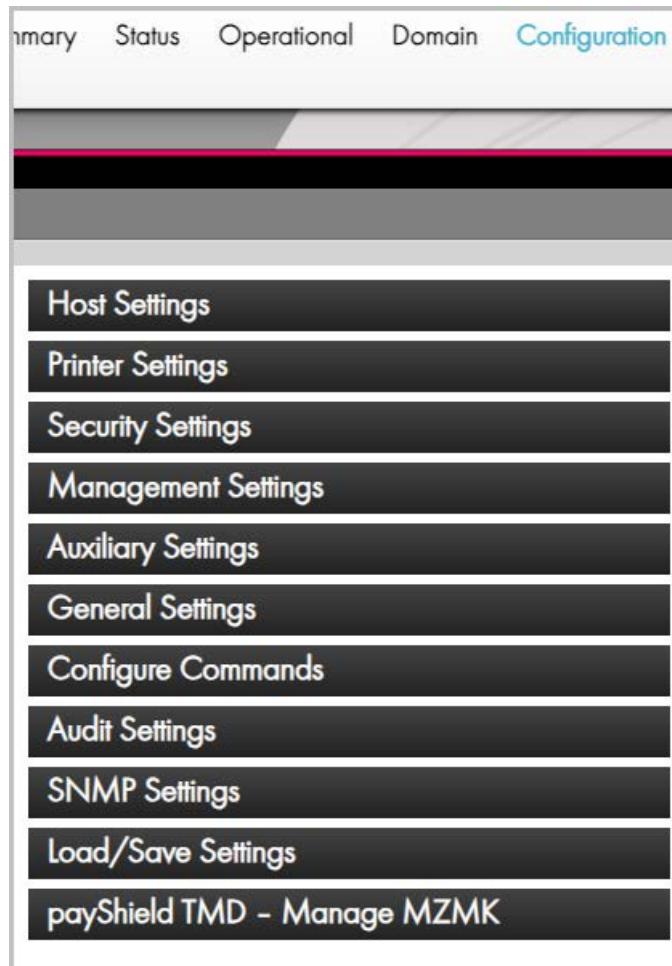
To change a passphrase, click “**Change HRK Passphrase**”. In the table, specify which Administrator you want to change the passphrase for, use the keyboard to enter the current passphrase, use the keyboard to enter the new passphrase twice in the appropriate boxes, and click “**Next**”.

Passphrases require the following:

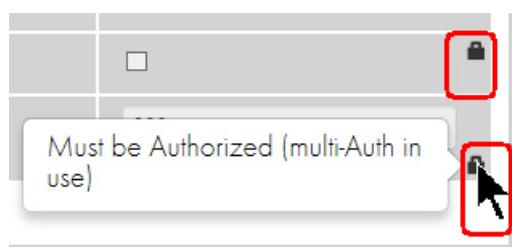
- At least 2 upper case characters
- At least 2 lower case characters
- At least 2 numbers
- At least 2 special characters

Note: In order to send the passphrases securely to the payShield, the browser requires a commissioned Smart Card (e.g., it can be any one of the security domain’s commissioned Smart Cards). Follow the instructions displayed by the wizard for presenting the commissioned Smart Card. Changing the HRK passphrases takes about a minute.

9.10 Configuration Tab



Note: Presence of a lock icon, indicates the setting/action requires proper authorization.



9.10.1 Host Settings

Host Settings

Host Message Header Length	4																														
Disable host connections when no LMKs are installed?	No																														
Active host interface																															
<input checked="" type="button"/> Ethernet <input type="button"/> FICON																															
This section allows the configuration of the IP settings for each Ethernet interface.																															
<table border="1"> <thead> <tr> <th></th> <th>Interface 1</th> <th>Interface 2</th> </tr> </thead> <tbody> <tr> <td>Enabled</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>MAC address</td> <td>00:d0:fa:05:b3:89</td> <td>00:d0:fa:05:b3:86</td> </tr> <tr> <td>Dynamic</td> <td><input type="checkbox"/> Obtain IP Settings via DHCP</td> <td><input type="checkbox"/> Obtain IP Settings via DHCP</td> </tr> <tr> <td>Network Name</td> <td></td> <td></td> </tr> <tr> <td>IP address</td> <td>10.194.184.193</td> <td>10.194.184.194</td> </tr> <tr> <td>Subnet mask</td> <td>255.255.240.0</td> <td>255.255.240.0</td> </tr> <tr> <td>Gateway</td> <td>10.194.176.1</td> <td>10.194.176.1</td> </tr> <tr> <td>Configured Port speed</td> <td>Autoselect</td> <td>Autoselect</td> </tr> <tr> <td>Actual Port Speed</td> <td>1 Gbps Full-Duplex</td> <td>1 Gbps Full-Duplex</td> </tr> </tbody> </table>			Interface 1	Interface 2	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	MAC address	00:d0:fa:05:b3:89	00:d0:fa:05:b3:86	Dynamic	<input type="checkbox"/> Obtain IP Settings via DHCP	<input type="checkbox"/> Obtain IP Settings via DHCP	Network Name			IP address	10.194.184.193	10.194.184.194	Subnet mask	255.255.240.0	255.255.240.0	Gateway	10.194.176.1	10.194.176.1	Configured Port speed	Autoselect	Autoselect	Actual Port Speed	1 Gbps Full-Duplex	1 Gbps Full-Duplex
	Interface 1	Interface 2																													
Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>																													
MAC address	00:d0:fa:05:b3:89	00:d0:fa:05:b3:86																													
Dynamic	<input type="checkbox"/> Obtain IP Settings via DHCP	<input type="checkbox"/> Obtain IP Settings via DHCP																													
Network Name																															
IP address	10.194.184.193	10.194.184.194																													
Subnet mask	255.255.240.0	255.255.240.0																													
Gateway	10.194.176.1	10.194.176.1																													
Configured Port speed	Autoselect	Autoselect																													
Actual Port Speed	1 Gbps Full-Duplex	1 Gbps Full-Duplex																													
<input type="button"/> Undo <input type="button"/> Apply																															

9.10.1.1 Host 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.

9.10.1.2 Active Host Interface

The current active Host interface for the HSM is emphasized as shown below. In this case, the Ethernet interface is the current active Host interface.

Active host interface



In Offline or Secure state, you may choose the “**Ethernet**”, or “**FICON**” as the active Host interface port by selecting the appropriate button, completing the settings for the interface (as explained below), and selecting the “**Apply**” button.

Note: Interfaces are licensed. If an interface is not available, your HSM may not be licensed for it. Review the interface license. Navigate to **Status > Software Info > FIPS/Licensing**.

Host Configuration	Ethernet,(optional) TLS/SSL
Licenses Issue No	5
Performance	2500 cps
Ship Counter	1
Crypto	3DES,AES,RSA,ECC

9.10.1.3 Ethernet

The payShield provides 2 Host Ethernet interfaces and allows the port speed and duplexity to be set independently.

The HSM's Host Ethernet interfaces support the delivery of Host commands via TCP/IP or UDP/IP.

The two Host Ethernet interfaces support speeds of 10, 100, and 1,000 Mbits/sec each and require unique IP addresses.

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

After making alterations to the Ethernet settings, press “**Apply**” to commit the changes to the HSM.

9.10.1.4 IP

In this section, network settings may be set up for each Ethernet interface provided the unit is in Offline or Secure state.

You may enable each interface independently using the “**Enabled**” check box. You must have at least one interface enabled when Ethernet is the clicked Active Host Interface.

The screenshot shows the "Host Settings" window with the "IP" tab selected under the "Ethernet" tab. The window displays configuration for two interfaces:

	Interface 1	Interface 2
Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
MAC address	00:d0:fa:05:b3:89	00:d0:fa:05:b3:86
Dynamic	<input type="checkbox"/> Obtain IP Settings via DHCP	<input type="checkbox"/> Obtain IP Settings via DHCP
Network Name		
IP address	10.194.184.193	10.194.184.194
Subnet mask	255.255.240.0	255.255.240.0
Gateway	10.194.176.1	10.194.176.1
Configured Port speed	Autoselect	Autoselect
Actual Port Speed	1 Gbps Full-Duplex	1 Gbps Full-Duplex

At the bottom right are "Undo" and "Apply" buttons.

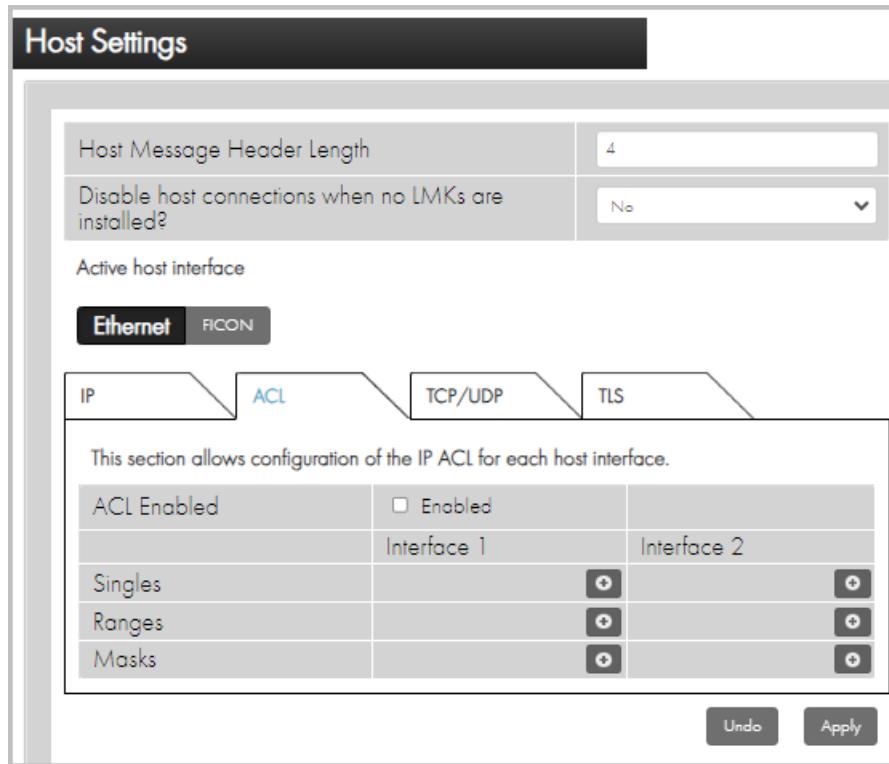
The following items are set up for each Host port:

- **MAC address**
 - A read only field showing the MAC address of the Host Ethernet port.
- **Dynamic**

- If checked, this port will be configured using DHCP instead of manually configured and the “Network Name” field becomes editable while the “IP address”, “Subnet mask”, and “Gateway” fields become read-only.
- Network Name
 - The HSM will specify this user-friendly name in the DHCP request as the desired name for this interface. If your DNS is configured properly, the given Network Name can be used to address this HSM interface.
- IP Address
 - When DHCP is not employed, a static IP address for the payShield 10K’s Host port may be specified. This must be a unique IP address on the Host network.
 - Example: 192.168.001.010
- Subnet Mask
 - When DHCP is not employed, a subnet mask for the payShield 10K’s Host port may be specified. This is used to define the network class.
 - Example: 255.255.255.000
- Gateway
 - When DHCP is not employed, a default gateway address for the payShield 10K’s Host port may be specified. This is the IP address of the default gateway in the network.
 - Example: 192.168.001.001
- Configured Port Speed
 - The speed and duplexity at which the Host port is to run.
- Actual Port Speed
 - A read only field that displays the actual speed as reported by the Ethernet interface.

9.10.1.5 Access Control List (ACL)

In this section, an Access Control List to restrict access to each of the HSM’s Ethernet Host Interfaces may be enabled and setup provided the unit is in offline or secure state.



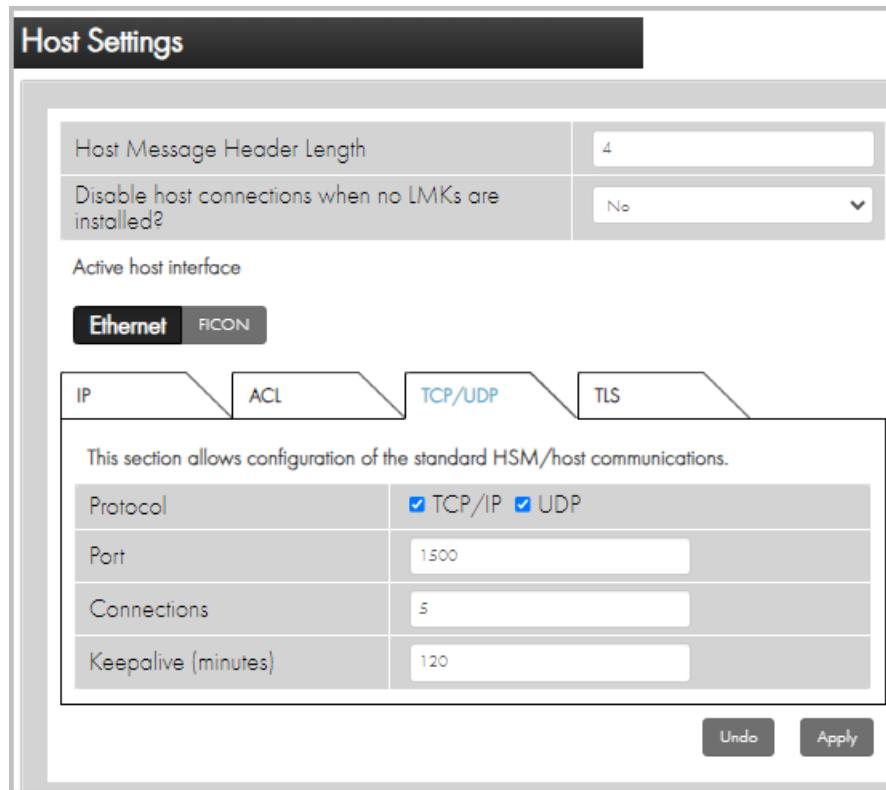
Each interface may have its own set of ACLs. Control may be restricted using any combination of:

- Singles
 - A single IP address.
 - Example: 192.168.1.5
- Ranges
 - A range of addresses consisting of a starting address and an ending address.
 - Example: 192.168.1.5 / 192.168.1.10
- Masks
 - A range of addresses consisting of a base address and a subnet mask.
 - Example: 192.168.1.90 / 255.255.255.128

Entries may be added or removed using the plus and minus icons in each section.

9.10.1.6 TCP/UDP

In this section, TCP and UDP protocol settings may be altered provided the unit is in Offline or Secure state.



The following options are available:

- Protocol
 - Specify which protocols (TCP and/or UDP) the HSM should accept as incoming connections. If unchecked, any incoming traffic conforming to that protocol will be discarded.
- Port
 - The base port to be used for communication with connecting Hosts.
- Connections
 - The maximum number of simultaneous connections to allow (up to 256).
- Keepalive
 - The amount of time (in minutes) that an idle connection should be kept open.

Port Settings

Port	Protocol	Purpose
xxxx	TCP/UDP	Well-known port for command traffic between host and payShield, as defined in host port parameters. Default is 1500. Use of this port results in the default LMK being used unless the command explicitly identifies another LMK.

Port Settings

Port	Protocol	Purpose
xxxx + n	TCP/UDP	Well-known port for command traffic between host and payShield where LMK n-1 is to be used. For example, if the default well-known port has been defined as 1500, then 1501 is used if LMK 0 is required for the command, 1502 is used if LMK 1 is required for the command, and so on. An explicit identification of the LMK in the command overrides the LMK implied by the port number.

9.10.1.7 TLS tab

Please refer to [Chapter 11, “TLS Certificate Management”](#) for further information on the process required to manage these TLS certificates.

This section allows configuration of secured HSM/host communications.

Protocol	<input checked="" type="checkbox"/> Enable TLS
Port	2500
Active Host TLS Store	A

Certificate Chain:

Certificate Fields:

Certificate Field Value:

Import/Copy Host TLS Store Certificates

This section allows Import and Copy of Host TLS store certificates based on the Selected Host TLS Store as the destination store.

Selected Host TLS Store	<input checked="" type="radio"/> A	<input type="radio"/> B
<input type="button" value="Import Host TLS Certificate"/> <input type="button" value="Copy Host TLS Certificate"/>		

The following options are available:

- Protocol

- Tick box for TLS checked (enabled) and unchecked (disabled).
- Port
 - Port number for TLS
- Active Host TLS Store
 - Displays the Host TLS Store currently Active (A or B)
 - In Secure State, the Host TLS Store can be changed from A to B or vice versa
- Certificate Chain
 - The certificate chain consists of multiple certificates, starting from the end-entity (server) certificate and leading up to a trusted root or intermediate certificate. The chain represents the trust hierarchy and ensures the authenticity of the end-entity certificate.
- Certificate Fields
 - A TLS certificate contains various fields that hold specific information. The important fields include Common Name (CN), Organization (O), Organizational Unit (OU), Locality (L), State/Province (ST), Country (C), Validity Dates (Not Before and Not After), Public Key, and others. These fields provide details about the certificate and the entity it represents.
- Certificate Field Values
 - The values within certificate fields hold specific information related to the certificate. For example, the Common Name field contains the domain name for which the certificate is issued. The Organization field contains the name of the organization. The validity dates indicate the time period during which the certificate is considered valid.
- Importing/Copying Host TLS Store Certificates
 - Importing Host TLS Store Certificates

To import Host TLS certificate(s) into the selected Host TLS store from a file.
 - Copying Host TLS Store Certificates

To copy Host TLS certificates from one Host TLS Store to the other. Once imported, the certificate can be used for secure communication.

Note: Hovering over the TLS icon open the help text shown below.

Display and/or import/copy the Host TLS Certificate/Chain of Trust.

Importing Certificates

Prerequisites:

- The system time has to be set to 24 hour UTC format
- A CSR needs to have been signed by an external CA to obtain the certificate to import
- No more than 64 certificates can be imported in a Host TLS store of HSM
- The maximum length (depth) for the Chain of Trust is 6

Requirements:

- Key types allowed: RSA, ECDSA (P256, P384 and P521)
- File must have .crt extension
- Certificate should be v3 ONLY
- The Chain of Trust should be imported first [from the HSM Server Certificate's Issuer to the Root CA] followed by the HSM Server Certificate for the Selected Host TLS Store
- Import the certificates as individual X509 PEM encoded files or multiple certificates in a single file

Copying Key Pair and Certificates

Prerequisites:

- The system time has to be set to 24 hour UTC format
- Private key should be present in the source Host TLS store to perform copy operation from source to destination store
- No more than 64 certificates can be present in a Host TLS store of HSM
- The maximum length (depth) for the Chain of Trust is 6

Requirements:

- Private key should be either present in the destination Host TLS store or selected for copy operation, In order to select any certificate to copy
- The Chain of Trust should also be selected for copy operation [from the HSM Server Certificate's Issuer to the Root CA] along with the HSM Server Certificate for the Selected Host TLS Store
- To perform copy operation, Certificates are enabled for selection only if they are not already present in the destination Host TLS store [certificate's unique identity is defined by the combined value of their Issuer Name and Serial Number]

In order to establish a TLS/SSL connection:

- Generate a key pair and export a Certificate Request (CSR) using the SG console command
- Get the CSR signed by an external CA to obtain the HSM Server Certificate
- Import the Chain of Trust into the payShield (from the HSM Server Certificate's Issuer to the Root CA)
- Import the HSM Server Certificate
- Generate a Client Certificate for any client connecting to the HSM [you can use the same CA that signed the HSM Certificate or a different one]
- Import the Client certificate and Client Root CA

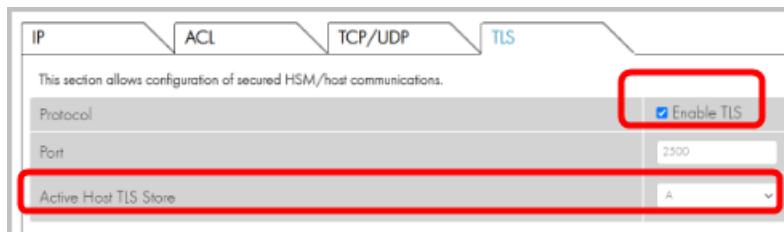
Active Host TLS Store

When managing TLS certificates and key pairs for secure communications, there are two types of Host TLS stores: active and inactive:

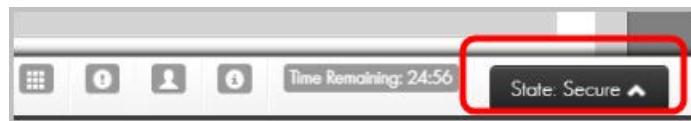
- The active Host TLS store is where TLS certificates and key pairs are actively utilized and accessible for establishing secure connections.
- The inactive Host TLS store is used when migrating to a new set of TLS certificates and/or the HSM key. The HSM key can be generated and the TLS certificates imported while the HSM is Online with Secure State only required to select this key store for use as the active Host TLS key store.

The “Active Host TLS Store” can be changed from A to B or vice versa when:

- The Enable TLS setting is selected;
- And the HSM is in the Secure state.



- The HSM is in the Secure state.



Note: Additional help text appears when hover over an icon.

This section allows configuration of secured HSM/host communications.

Protocol	<input checked="" type="checkbox"/> Enable TLS
Port	2500
Active Host TLS Store	A

Must be in secure state

A screenshot of the TLS configuration screen. It shows three rows of settings: Protocol (checkbox checked), Port (2500), and Active Host TLS Store (A). A tooltip "Must be in secure state" is visible near the bottom right. The TLS tab is highlighted in blue at the top.

This section allows configuration of secured HSM/host communications.

Protocol	<input type="checkbox"/> Enable TLS
Port	2500
Active Host TLS Store	A

TLS should be enabled

A screenshot of the TLS configuration screen for Host TLS Store B. It shows the same three rows of settings as the previous screen, but the "Enable TLS" checkbox is unchecked. A tooltip "TLS should be enabled" is visible near the bottom right. The TLS tab is highlighted in blue at the top.

Chain of Trust

There are two Host TLS Stores available in the HSM: Store A and Store B.

When the Active Host TLS Store A is selected, the information for all certificates related to the Chain of Trust of that specific store are displayed.

The examples that follow, the Chain of Trust for Host TLS Store A is shown, while Host TLS Store B is empty and does not have any displayed information.

Active Host TLS store A's Chain of Trust information:

The screenshot shows the 'Active Host TLS Store' interface. At the top right, there is a dropdown menu with 'A' selected, which is highlighted with a red box. Below the menu, the 'Certificate Chain' section displays a hierarchical list of certificate subjects, starting from 'Subject: EcserverRootCA.thalesesec.com' down to 'Subject: S00000000001G'. To the right of this, the 'Certificate Fields' section is shown as a table:

Field	Value
Version	3 (0x2)
Serial number	52:e1:0c:34:ad:2:2
Signature algorithm	ecdsa-with-SHA2
Signature hash algorithm	SHA256
Issuer	C-US, ST-Florida
Valid from	Jun 12 10:45:40
Valid to	Jun 12 10:45:40
Subject	C-US, ST-Florida

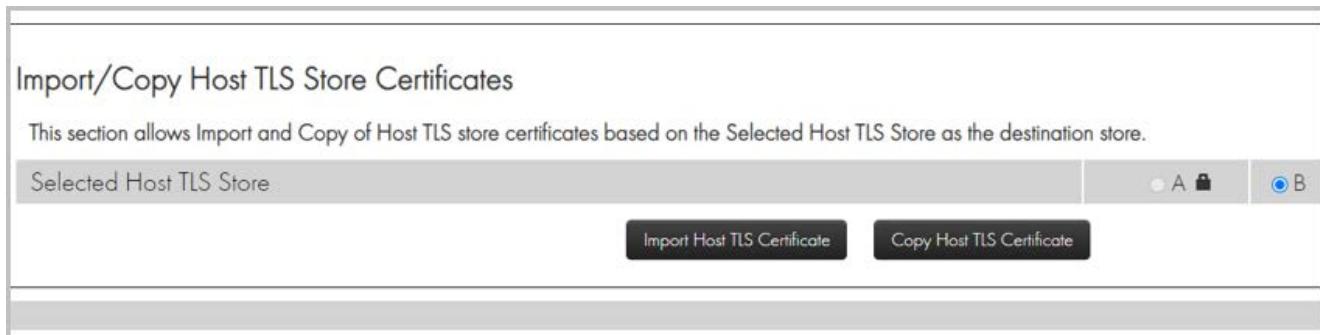
Below these sections, a 'Certificate Field Value' section shows the value '3 (0x2)'.

Selected Host TLS Store option



To select the Host TLS store to be used to import or the destination of the copy operation, select the radio button options for Host TLS Store A (represented by "A") or Host TLS Store B (represented by "B"). The currently selected active Host Key Store can only be selected in Secure State.

Import Host TLS Store Certificates



Note: Both the Import and Copy buttons remain enabled regardless of the HSM state.

From the “Import/Copy Host TLS Store Certification” pane, you can import and copy Host TLS Store Certificates to a specific destination store. In the given example, the destination store is identified as Host TLS Store B.

When clicking on the “Import Host TLS Certificate” button, the Host TLS key certificates can be imported from a file into the TLS Store that has been selected as the destination. If the Inactive Host TLS store has been selected, this operation can be carried out in Online State. If the active Key Store has been selected, Secure State is required for this operation.



Note: When the HSM is **Online** and **TLS is enabled**, the copy certificate operation can only be performed from the Active Host TLS Store to the Inactive Host TLS Store.

Copy Host TLS Certificate operation

Selection scenarios - when TLS is enabled and HSM is in Online/Offline state

With TLS enabled and the HSM is in **Online** state, we can only select the Inactive Host TLS Store; (in the example below, the Active Host TLS Store is “A”, so the Inactive Host TLS Store is “B”).

The screenshot displays two main sections of the software interface:

- Certificate Management Section:**
 - Port: 2500
 - Active Host TLS Store: A dropdown menu is highlighted with a red box.
 - Certificate Chain:**
 - Subject: EserverRootCA.thalesesec.com
 - Subject: EserverIntCA1.thalesesec.com
 - Subject: EserverIntCA2.thalesesec.com
 - Subject: EserverIntCA3.thalesesec.com
 - Subject: EserverIntCA4.thalesesec.com
 - Subject: EserverIntCA5.thalesesec.com
 - Subject: 5000000001G
 - Certificate Fields:**

Signature hash algorithm	SHA256
Issuer	C=US, ST:CN=Eserveric.com
Valid from	Jun 12 10
Valid to	Jun 12 10
Subject	C=US, ST:CN=Eserveric.com
Public key	ECC (521)
Public key parameters	id-ecPublicKey
Signature algorithm	SHA256
Signature	30:81:87:09:12:3d:9f:b6:14:05:d8:dd:80:6b:4f:3c:61
 - Certificate Field Value:**

```
3 [0x2]
```
- Import/Copy Host TLS Store Certificates Section:**
 - This section allows Import and Copy of Host TLS store certificates based on the Selected Host TLS Store as the destination store.
 - Selected Host TLS Store: A dropdown menu is highlighted with a red box.
 - Buttons: Import Host TLS Certificate (disabled), Copy Host TLS Certificate (highlighted with a red box).
 - Status Bar: 2020 Thales Group. All Rights Reserved. Time Remaining: 24:21. State: Online (highlighted with a red box).

In the example below, the **Copy Host TLS Certificates** User interface shows the keypair and the list of certificates that can be selected for the copy operations. When no items are selected, **Apply** is disabled.

Copy Host TLS Certificates	
Select the certificates to be copied from Active Host TLS Store A to Inactive Host TLS Store B.	
Group	Selected
Private Key	<input type="checkbox"/>
➤ CA Certificates	<input type="checkbox"/>
➤ Server Certificates	<input type="checkbox"/>
➤ Client Certificates	<input type="checkbox"/>

Remove Selection **Select All** **Apply** **Cancel**

Hence, we can only perform the copy keypair/certificate operation from Active Host TLS Store to Inactive Host TLS Store.

The keypair and certificates for copy can be individually selected or selected in a group.

Copy Host TLS Certificates	
Select the certificates to be copied from Active Host TLS Store A to Inactive Host TLS Store B.	
Group	Selected
Private Key	<input checked="" type="checkbox"/>
➤ CA Certificates	<input checked="" type="checkbox"/>
➤ Server Certificates	<input type="checkbox"/>
➤ Client Certificates	<input type="checkbox"/>

Remove Selection **Select All** **Apply** **Cancel**

Group	Common Name	Issuer	Serial Number	Valid From	Valid To	Selected
▼ CA Certificates	EserverInCA1.thalesesec.com	C=US ST=Florida CN=EserverRootCA.thalesesec.com	0ba2e8	Jun 12 10:45:40 2024	Jun 12 10:45:40 2025	<input checked="" type="checkbox"/>
	EserverInCA3.thalesesec.com	C=US ST=Florida CN=EserverInCA2.thalesesec.com	0ba2eo	Jun 12 10:45:41 2024	Jun 12 10:45:41 2025	<input checked="" type="checkbox"/>
	EserverInCA5.thalesesec.com	C=US ST=Florida CN=EserverInCA4.thalesesec.com	0ba2ec	Jun 12 10:45:41 2024	Jun 12 10:45:41 2025	<input checked="" type="checkbox"/>
	EcclientRootCA.thalesesec.com	C=US ST=Florida CN=EcclientRootCA.thalesesec.com	02cc71c86e0729b6f45e80c02511950da69b2	Jun 12 10:45:48 2024	Jun 12 10:45:48 2025	<input checked="" type="checkbox"/>

After the copy operation has been started, a new user interface displays:

Copy Host TLS Certificates

Select the certificates to be copied from Active Host TLS Store A to Inactive Host TLS Store B.

Group	Selected
Private Key	<input checked="" type="checkbox"/>
> CA Certificates	<input type="checkbox"/>
> Server Certificates	<input type="checkbox"/>
> Client Certificates	<input type="checkbox"/>

The following options appear in the bottom right corner of the screen:

Remove Selection removes the selection for all the items in the copy operation selection list.

Select All selects all items in the copy operation selection list.

Apply performs the copy operation for the selected items from source to destination Host TLS store. This button is only enabled when at least one item is selected for the copy operation.

Cancel cancels the copy operation.

Operation performed - when TLS is enabled and HSM is in Online/Offline state

After selecting the items for copy, **Apply** is enabled.

Copy Host TLS Certificates

Select the certificates to be copied from Active Host TLS Store A to Inactive Host TLS Store B.

Group	Selected
Private Key	<input checked="" type="checkbox"/>
> CA Certificates	<input type="checkbox"/>
> Server Certificates	<input type="checkbox"/>
> Client Certificates	<input type="checkbox"/>

Select **Apply**.

PROCESSING appears as the operation continues.

Upon completion a **SUCCESS** message displays:

Copy Host TLS Certificates

Status of the Copy Operation from Active Host TLS Store A to Inactive Host TLS Store B : **SUCCESS**

Show Summary is a toggle switch with **Hide Summary**.

The screenshot shows a 'Copy Host TLS Certificates' window. At the top, it says 'Status of the Copy Operation from Active Host TLS Store A to Inactive Host TLS Store B' followed by 'SUCCESS'. Below this is a table with columns 'Valid From', 'Valid To', and 'Status'. All entries in the 'Status' column are 'SUCCESS'. A tooltip 'Copied Successfully' appears over the last row. At the bottom of the table are two buttons: 'Show Summary' (which is highlighted with a red box) and 'Done'.

Select **Done** when finished.

Scenario - when TLS is enabled and HSM is in Secure state

The screenshot shows a configuration form with three fields: 'Protocol' (checkbox checked), 'Port' (2500), and 'Active Host TLS Store' (A). The 'Protocol' field has a red box around its checkbox.

When TLS is **enabled** and the HSM is in **Secure** state, either TLS store ("A" or "B") can be selected to perform the copy operation.

Scenario - when TLS is disabled and the HSM in any state

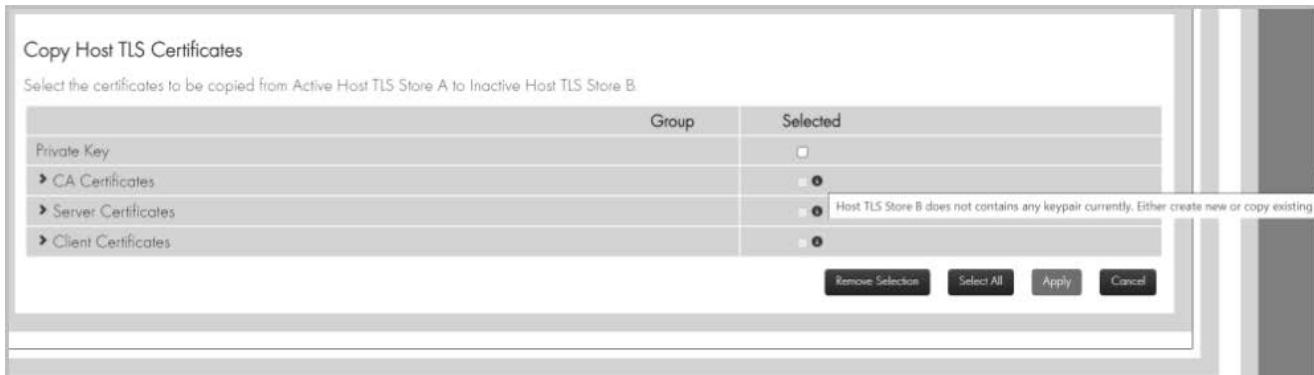
The screenshot shows the same configuration form as above, but the 'Protocol' checkbox is now unselected (unchecked).

When TLS is disabled, regardless of the HSM state, keypair and certificates can be copied from any one Host TLS store to another.

Copy Host TLS Certificate operation - Error scenarios

When source Host TLS store does not contains any keypair

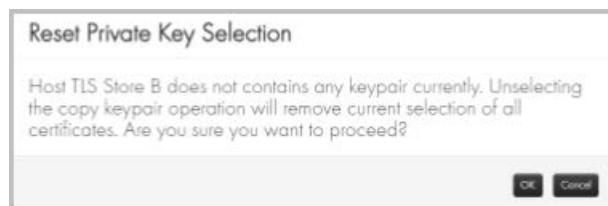
If the source Host TLS store does not contain a keypair, it is not possible to perform any copy operations. When there is no keypair in the source Host TLS store, all copy operations are disabled.



When destination Host TLS store does not contains any keypair

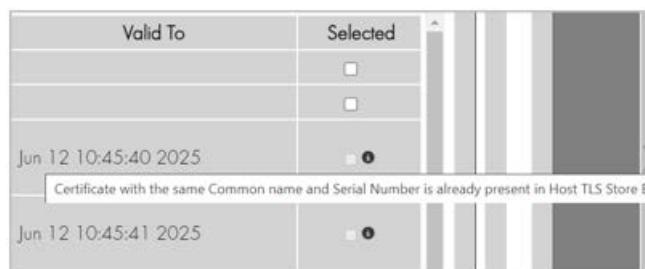
If the destination Host TLS store (Selected Host TLS Store) does not already have a keypair, there are two options to proceed: either go back and create a new keypair using the “SG” console command, or select the “Copy Private Key” operation from the source store. Only then will the options to select certificates for the copy operation be enabled. Otherwise, the options will remain disabled and an info icon will provide a hint when hovered over.

If the destination Host TLS store (Selected Host TLS Store) does not already have a keypair, and we have selected the “Copy Private Key” operation from the source store, the certificate selection options are enabled. However, if we try to deselect the “Copy Private Key” operation after selecting some certificates for the copy operation, a confirmation prompt displays.



When certificate(s) is/are already present in the Selected (destination) Host TLS store

A certificate is identified by its “Issuer Name” and “Serial Number”. If a certificate that is already present in the Selected (destination) Host TLS store is included in the copy operation selection list, the selection option for that certificate will be disabled.



If we encounter this scenario where some certificates are disabled within a group, selecting the group option will automatically select all the enabled certificates within that group.

Copy Host TLS Certificates

Select the certificates to be copied from Active Host TLS Store A to Inactive Host TLS Store B.

Group	Common Name	Issuer	Serial Number	Valid From	Valid To	Selected
Private Key						<input type="checkbox"/>
▶ CA Certificates						<input checked="" type="checkbox"/>
EcservcertCA1.thesecure.com	C=US ST=Florida CN=EcservRootCA.thesecure.com	0ba2e8		Jun 12 10:45:40 2024	Jun 12 10:45:40 2025	<input type="checkbox"/>
EcservcertCA3.thesecure.com	C=US ST=Florida CN=EcservcertCA2.thesecure.com	0ba2ea		Jun 12 10:45:41 2024	Jun 12 10:45:41 2025	<input type="checkbox"/>
EcservcertCA5.thesecure.com	C=US ST=Florida CN=EcservcertCA4.thesecure.com	0ba2ec		Jun 12 10:45:41 2024	Jun 12 10:45:41 2025	<input type="checkbox"/>
EcservRootCA.thesecure.com	C=US ST=Florida CN=EcservRootCA.thesecure.com	02cc71c8de0729bb6145e8bc0802511950da69b2		Jun 12 10:45:48 2024	Jun 12 10:45:48 2025	<input checked="" type="checkbox"/>
EcservcertCA4.thesecure.com	C=US ST=Florida CN=EcservcertCA3.thesecure.com	0ba2eb		Jun 12 10:45:41 2024	Jun 12 10:45:41 2025	<input type="checkbox"/>
EcservcertCA2.thesecure.com	C=US ST=Florida CN=EcservcertCA1.thesecure.com	0ba2e9		Jun 12 10:45:40 2024	Jun 12 10:45:40 2025	<input type="checkbox"/>
EcservRootCA2.thesecure.com	C=US ST=Florida CN=EcservRootCA.thesecure.com	52e10c34ad03e55224807a29a1scffbb5-506b76c8		Jun 12 10:45:40 2024	Jun 12 10:45:40 2025	<input type="checkbox"/>

Buttons: Remove Selection | Select All | Apply | Cancel

If all the certificates present in a certificate group are already present in the Selected (destination) Host TLS store, then the selection option for the group will also be disabled.

Valid To	Selected
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input checked="" type="checkbox"/>
2025	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/>
2025	<input checked="" type="checkbox"/>

All the certificates of this group are already present in Host TLS Store B

Buttons: Remove Selection | Select All | Apply | Cancel

When there are no certificates present for a group in the Source Host TLS store

If the Source Host TLS store (the store other than the Selected Host TLS store) does not contain any certificates for a specific group, the group selection option will be disabled and there will be no dropdown icon present for that group.

In the example below, the Active Host TLS Store A is the Source Host TLS store and does not have any client certificates. As a result, in the “Copy Host TLS Certificates” user interface, there is no dropdown icon for client certificates and the group selection option for client certificates remains disabled.

Copy Host TLS Certificates

Select the certificates to be copied from Active Host TLS Store A to Inactive Host TLS Store B.

Selected	
Private Key	<input type="checkbox"/>
▶ CA Certificates	<input type="checkbox"/>
▶ Server Certificates	<input type="checkbox"/>
Client Certificates	<input checked="" type="checkbox"/>

No certificate of this group is present in Host TLS Store A to copy

Buttons: Remove Selection | Select All | Apply | Cancel

9.10.2 Printer Settings

You can alter the configuration of connected printers when the unit is in the Offline or Secure state and there is at least one parallel or serial USB adapter attached to the HSM that has not been designated as a Host Interface.

This is accomplished by adjusting the settings explained below and then selecting the “**Apply**” button to commit the changes to the HSM. Once configured and still in the Offline or Secure state, you can send a test page to the printer using the “**Print Test Page**” button.

Printer Port Settings	
Printer Port	<input type="button" value="▼"/>
Printer Status	
Timeout	120000 <small>milliseconds</small>
Delay	0 <small>milliseconds</small>
Line Feed Order	<input type="button" value="standard"/>
Baud Rate	<input type="button" value="▼"/>
Data Bits	<input type="button" value="▼"/>
Stop Bits	<input type="button" value="▼"/>
Parity	<input type="button" value="▼"/>
Flow Control	<input type="button" value="▼"/>
Offline Control	<input type="button" value="▼"/>

Options:

- Printer Port
 - Click the serial or parallel USB adapter that the printer is connected to. Note that once the adapter is designated as a printer interface, it cannot be used as a Console Port.
- Printer Status
 - Read-only field showing the current status of the printer.
- Timeout
 - The time in milliseconds before giving up on an attempt to communicate with the printer.
- Delay
 - The time to wait before attempting to communicate with the printer.

- Line Feed Order
 - May be either standard (<LF><CR>) or reversed (<CR><LF>).
- Baud Rate (serial only)
 - The number of bits per second to transfer. Default: 115200.
- Data Bits (serial only)
 - The number of bits per character. Default: 8.
- Stop Bits (serial only)
 - Number of bits sent at the end of each character. Default: 1
- Parity (serial only)
 - Means of checking for errors in transmission. May be set to None, Odd, or Even. Default: None.
- Flow Control
 - Specifies whether to use any hardware or software mechanisms to control the flow of data. Default: None.
- Offline Control
 - Specifies whether to use DTR or RTS signals to detect if the printer is offline. Click none to disable this feature. Default: None.

9.10.3 Security Settings

You can alter the security configuration of the unit when it is in the Secure state by adjusting the settings explained below and selecting the “**Apply**” button to commit the changes to the HSM. Note that changing any settings in the “Initial” tab result in deleting all the LMKs stored in the unit.

9.10.3.1 General Tab

The General Tab is used to view and manage the security settings shown below.

Please note that when “Settings per LMK” is enabled, these settings apply to the HSM and cannot be configured separately for each LMK ID.

- Follow this link for information on configuring “Settings per LMK”: [Section 9.11, “Settings per LMK”, on page 231](#).
- For an overview of the feature’s functionality, refer to the: *payShield 10K Programmers Manual*, Section 9.9.

Security Settings

General Initial

These settings can only be modified when the HSM is in the Secure state.

Echo	Off
User storage key length	Double
Display general information on payShield Manager landing page	No
Default LMK identifier	0
Management LMK identifier	0
Solicitation batch size	1024
<input checked="" type="checkbox"/> Use default card issuer password	
Card issuer password (local)	
Confirm Card Issuer Password (local)	
Warning: Modifying the following setting will cause all installed LMKs to be erased.	
<input checked="" type="checkbox"/> Enable Settings per LMK	

9.10.3.2 Initial Tab

The Initial Tab is used to view and manage the other security settings which are shown below. Please note that when “Settings per LMK” is enabled, these settings can be configured separately for each LMK ID.

General

LMK ID	4
PIN length	6
Atalla ZMK variant support	DF
Transaction key scheme	None
Warning: Modifying the following settings will cause selected installed LMK to be erased.	
<input type="checkbox"/> Enforce Atalla variant match to Thales key type	
<input type="checkbox"/> Enable clear PINs	
<input type="checkbox"/> Enable ZMK translate command	
<input type="checkbox"/> Enable X9.17 for import	
<input type="checkbox"/> Enable X9.17 for export	
ZMK Length	Double
Decimlization Tables	Encrypted
<input checked="" type="checkbox"/> Enable decimalization table checks	
PIN Encryption Algorithm	Via
Use deprecated proprietary format [Tag J] when using PIN Blocks under AES Key Block LMK	No
<input checked="" type="checkbox"/> Authorized state required when importing a key under an RSA key	
Minimum HMAC length in bytes	10
<input type="checkbox"/> Enable PKCS#11 import and export for HMAC keys	
<input type="checkbox"/> Enable ANSI X9.17 import and export for HMAC keys	
Enable ZEK/TEK encryption of ASCII data or Binary data or None	None
<input checked="" type="checkbox"/> Restrict Key Check Values to 6 hex-chars	
<input checked="" type="checkbox"/> Return PIN Length in PIN Translation Response	
<input checked="" type="checkbox"/> Enable multiple authorized activities	
<input checked="" type="checkbox"/> Allow persistent authorized activities	
<input checked="" type="checkbox"/> Enable variable length PIN offset	
<input checked="" type="checkbox"/> Enable weak PIN checking	
<input type="checkbox"/> Check new PINs using global list of weak PINs	
<input type="checkbox"/> Check new PINs using local list of weak PINs	
<input type="checkbox"/> Check new PINs using rules	
<input checked="" type="checkbox"/> Enable PIN Block format 34 as output format for PIN translations to ZPK	
<input type="checkbox"/> Enable translation of account number for LMK encrypted PINs	
<input checked="" type="checkbox"/> Use HSM clock for date/time validation	
<input type="checkbox"/> Additional padding to disguise key length	
<input checked="" type="checkbox"/> Key export and import in trusted format only	
<input checked="" type="checkbox"/> Protect MULTOS cipher data checksums	
<input type="checkbox"/> Enable Key Scheme Tag 'X' (X9.17) for storing keys under LMK	
<input type="checkbox"/> Enable use of Tokens in PIN Translation	
<input type="checkbox"/> Enable use of Tokens in PIN Verification	
<input checked="" type="checkbox"/> Enable PIN Translation to BDK Encryption	

Initial

<input type="checkbox"/> Ensure LMK Identifier in command corresponds with host port	
<input type="checkbox"/> Ignore LMK ID in Key Block Header	
<input type="checkbox"/> Enable import and export of RSA Private keys	
<input type="checkbox"/> Enable import of a ZMK	
<input type="checkbox"/> Enable export of a ZMK	
The following settings affect PCI HSM compliance:	
<input checked="" type="checkbox"/> Prevent single-DES keys masquerading as double or triple-length key	
Card/password authorization (local)	Card
<input type="checkbox"/> Restrict PIN block usage for PCI HSM compliance	
<input type="checkbox"/> Enforce key type 002 separation for PCI HSM compliance	
<input checked="" type="checkbox"/> Enforce authorization time limit	
<input checked="" type="checkbox"/> Enforce multiple key components	
<input checked="" type="checkbox"/> Disable single-DES	
<input checked="" type="checkbox"/> Enforce PCI HSMv3 Key Equivalence	
<input checked="" type="checkbox"/> Enforce minimum key strength of 2048-bits for RSA	
<input checked="" type="checkbox"/> Enforce minimum key strength of 1024-bits for RSA signature verification	

Undo **Apply**

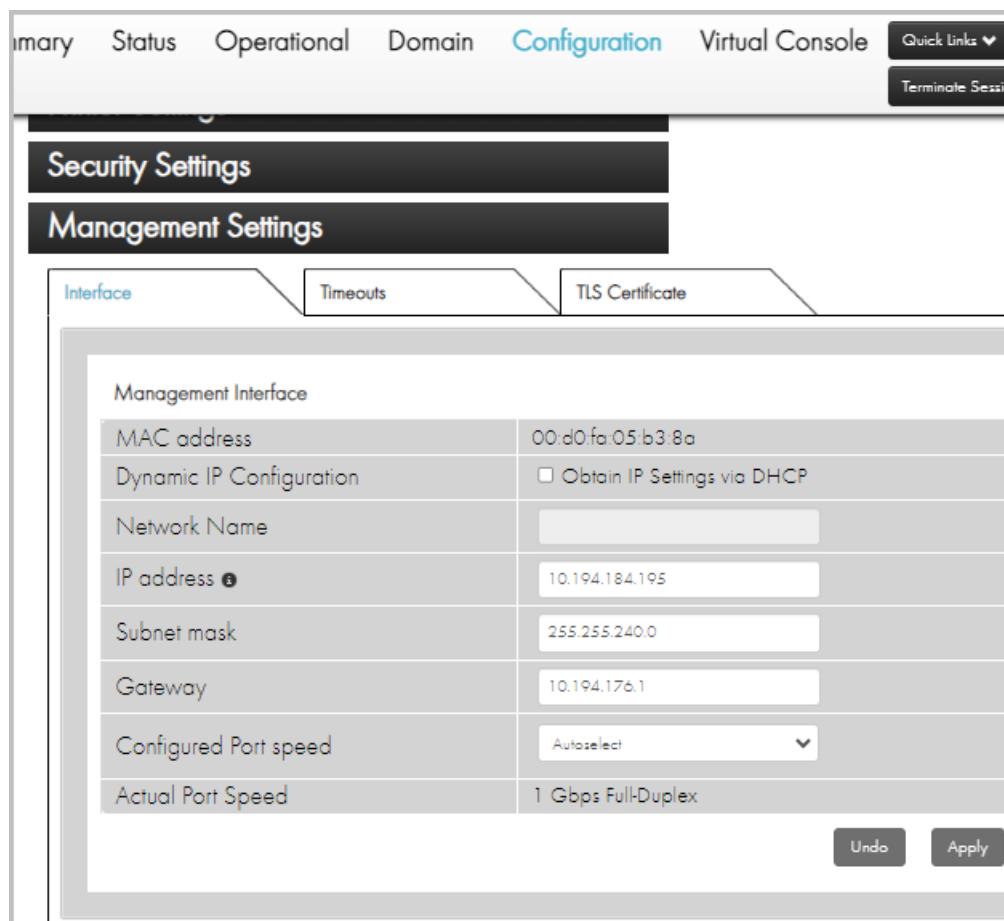
9.10.3.3 Security Parameter Descriptions

Refer to the *payShield 10K Security Manual* for a full description of the security parameters and their settings.

9.10.4 Management Settings

You can alter the management settings when the HSM is in the Offline or Secure state. Select the “**Apply**” button to commit the changes to the HSM.

9.10.4.1 Management - Interface



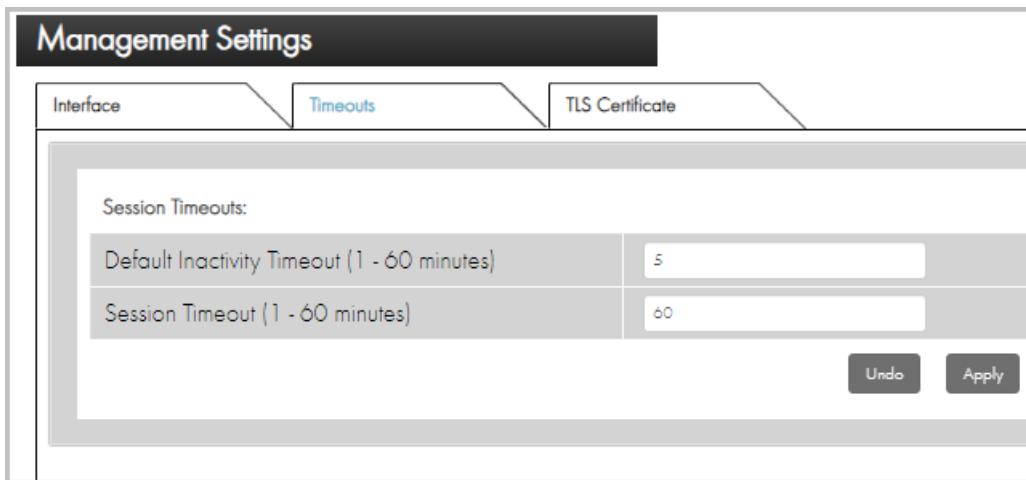
In this section, network settings can be adjusted for the Management Ethernet interface. The following options are available:

- MAC address:
 - A read only field showing the MAC address of the management port.
- Dynamic IP Configuration:

- If checked, the management port will be configured using DHCP instead of manually configured and the “Network Name” field becomes editable while the “IP address”, “Subnet mask”, and “Gateway” fields become un-editable.
- Network Name:
 - The HSM will specify this user-friendly name (following section 3.14 of RFC1533) in the DHCP request as the desired name for this interface. If your DNS is configured properly, the given Network Name can be used to address this HSM interface.
- IP address:
 - When DHCP is not employed, you can specify a static IP address for the payShield 10K’s management port. This must be a unique IP address on the management network.
 - Example: 192.168.002.010
- Subnet mask:
 - When DHCP is not employed, you can specify a subnet mask for the payShield 10K’s management port. This is used to define the network class. It is highly recommended that the management network and Host network are not the same.
 - Example: 255.255.255.000
- Gateway:
 - When DHCP is not employed, you can specify a default gateway address for the payShield 10K’s management port. This is the IP address of the default gateway in the network.
 - Example: 192.168.002.001
- Configured Port Speed:
 - The speed and duplexity at which the management port is to run.
- Actual Port Speed:
 - A read only field that displays the actual speed as reported by the Ethernet interface.

9.10.4.2 Management - Timeouts

This tab allows for configuration of the different timeout options for management sessions.

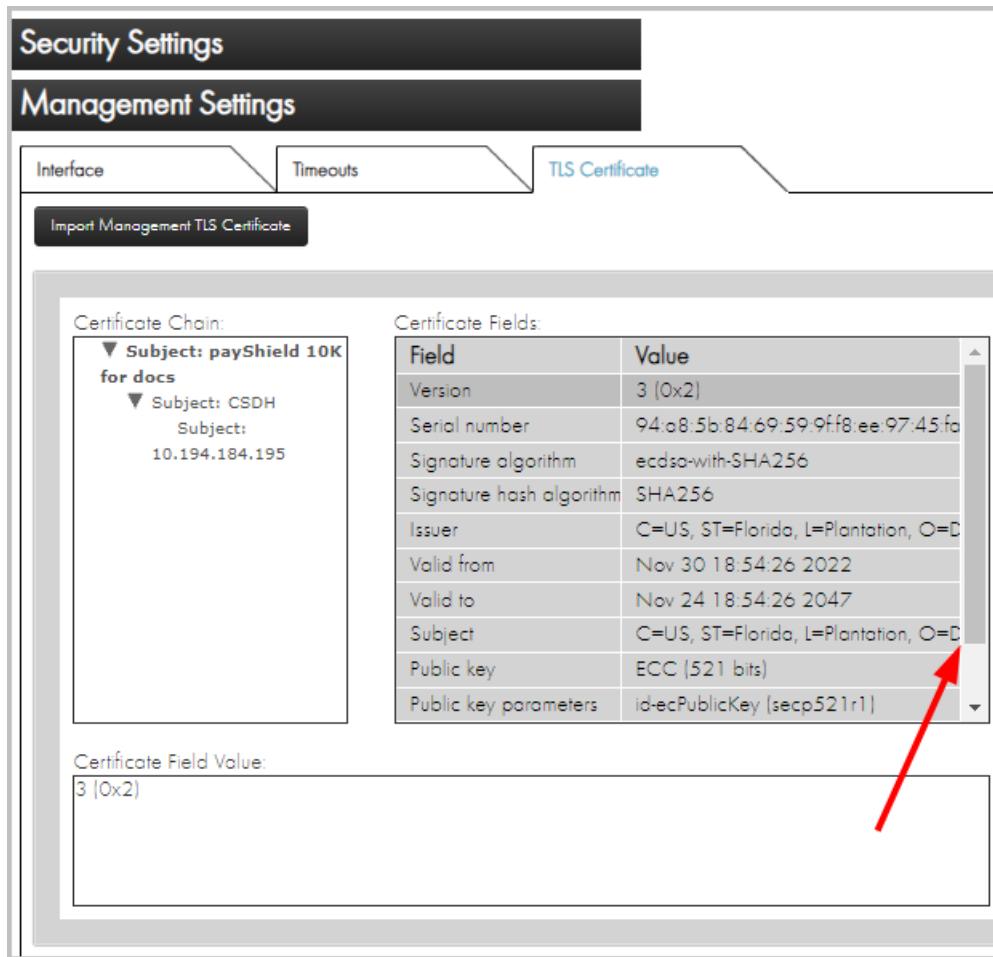


- Default Inactivity Timeout:
 - This timeout is triggered when the payShield Manager detects no user activity. After the configured time has elapsed, the inactive user will be automatically logged out.
- Session Timeout:
 - This timeout begins upon logon and continuously counts down, irrespective of activity. When the timer reaches 0, the user is automatically logged out.
 - The Time Remaining counter, seeded with this value, is located in the bottom right of the management screen. As the time approaches zero, the counter will display in red alerting the user that session time is expiring.

9.10.4.3 Management - TLS Certificate

The Management Settings are used to manage the TLS certificates used with payShield Manager.

Further information on the process required to manage these TLS certificates are given in [Chapter 11, “TLS Certificate Management”](#).



The display shows the following information on the currently configured TLS certificates used for payShield Manager:

- Certificate Chain
 - The certificate chain consists of multiple certificates, starting from the end-entity (server) certificate and leading up to a trusted root or intermediate certificate. The chain represents the trust hierarchy and ensures the authenticity of the end-entity certificate.
- Certificate Fields
 - A TLS certificate contains various fields that hold specific information. The important fields include Common Name (CN), Organization (O), Organizational Unit (OU), Locality (L), State/Province (ST), Country (C), Validity Dates (Not Before and Not After), Public Key, and others. These fields provide details about the certificate and the entity it represents.

- Certificate Field Values
 - The values within certificate fields hold specific information related to the certificate. For example, the Common Name field contains the domain name for which the certificate is issued. The Organization field contains the name of the organization. The validity dates indicate the time period during which the certificate is considered valid.

The option to import the TLS certificates used for payShield Manager from a file on the payShield Manager workstation is provided using the “Import Management Certificate” option. The process required to be followed in order to do this is covered in [Chapter 11, “TLS Certificate Management”](#).

When clicking on the “Import Host TLS Certificate” button, the file containing the CA, Intermediate CA and Management Certificate (as explained in [Chapter 11](#) these must all be concatenated in one file) is selected and if suitable certificates are provided the certificates are imported. The user is then logged out of payShield Manager automatically and can log in again as required using the new Management TLS key and certificates.

9.10.5 Auxiliary Settings

The screenshot shows a software interface titled "Auxiliary Settings". A sub-menu "Interface" is open, displaying configuration options for an "Auxiliary Interface". The configuration table includes the following fields:

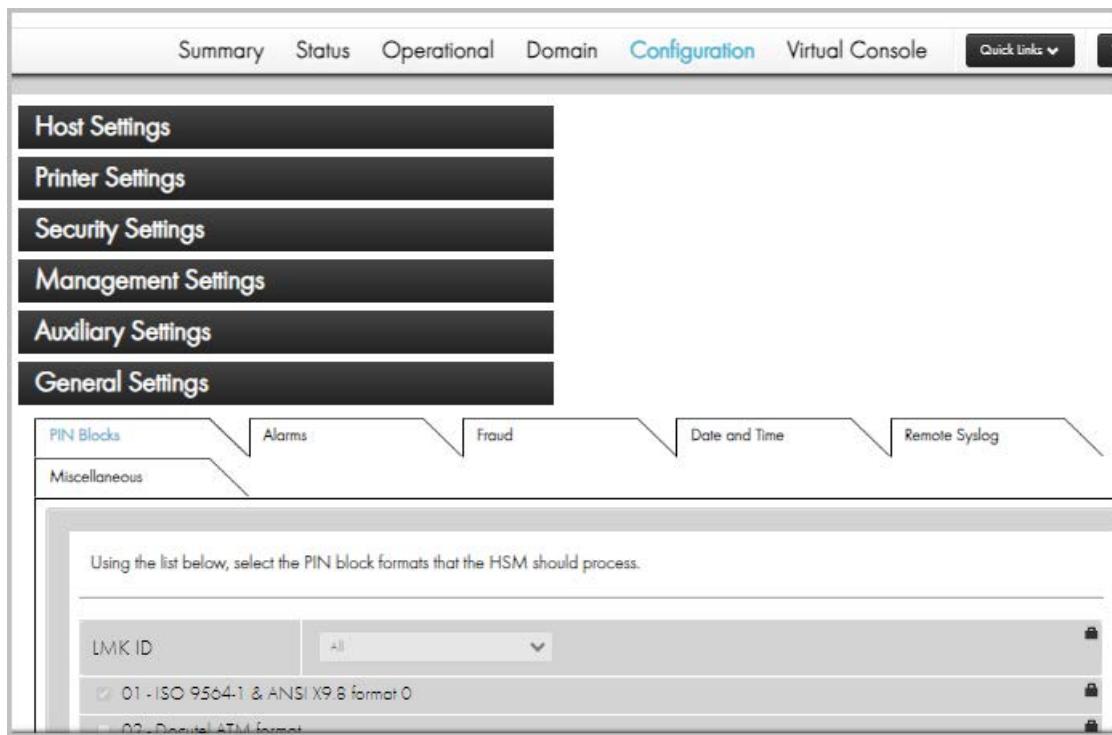
Auxiliary Interface	
MAC address	00:d0:fa:05:b3:87
Dynamic IP Configuration	<input type="checkbox"/> Obtain IP Settings via DHCP
Network Name	<input type="text"/>
IP address ⓘ	10.194.184.196
Subnet mask	255.255.240.0
Gateway	10.194.176.1
Configured Port speed	Autoselect
Actual Port Speed	1 Gbps Full-Duplex

At the bottom right of the configuration window are "Undo" and "Apply" buttons.

9.10.6 General Settings

General Settings include tabs for:

- PIN Blocks
- Alarms
- Fraud
- Date and Time
- Remote Syslog
- Miscellaneous

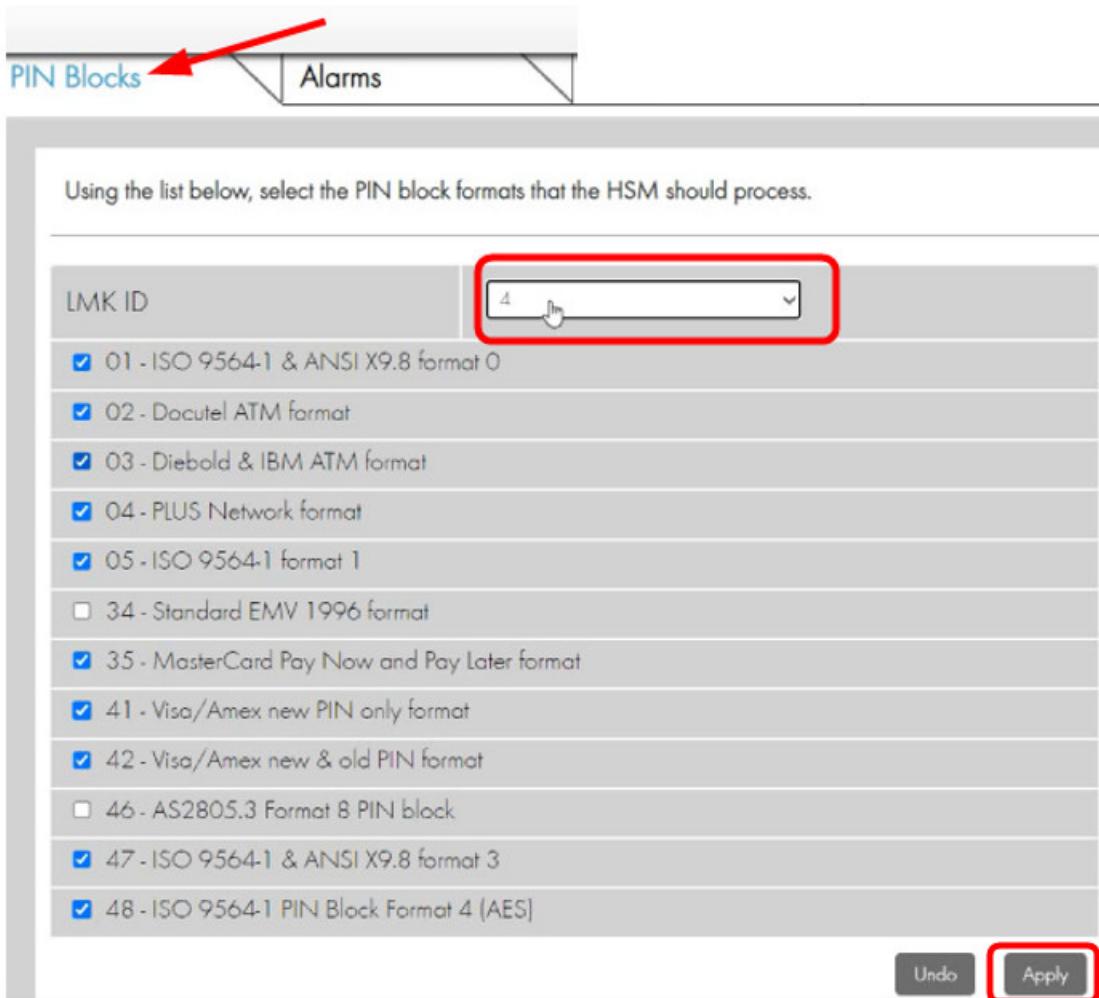


9.10.6.1 PIN Blocks

This tab allows you to click which PIN Block formats should be enabled on the HSM when in the Offline or Secure state.

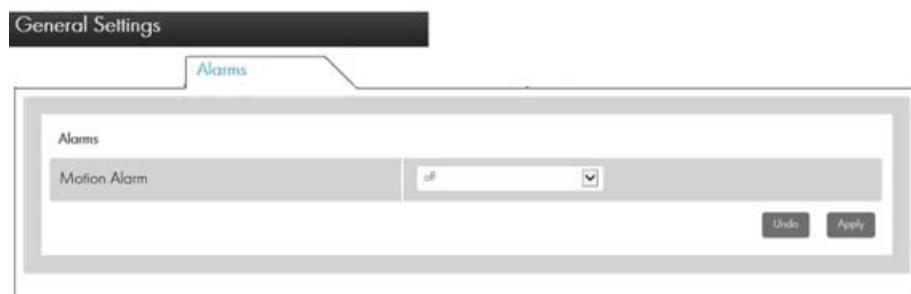
A Host system would typically not use all the PIN Block formats supported by the HSM. A simple but effective method of locking-down the HSM is to disable (uncheck) all unused PIN block formats: the subsequent use of a disabled format would result in an error code (69) being returned. Select the “**Apply**”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

When “Settings per LMK” is enabled, PIN Block formats can be set differently for each LMK ID. The LMK ID is selected using the drop down box at the top of the list.



9.10.6.2 Alarms

This tab allows you to enable or disable the Motion Alarm when the unit is in the Secure state. Select the “**Apply**” button to commit the changes to the HSM.



- The ADXL362 accelerometer in the PayShield 10K acts as a “Motion Sensor” detecting tilt movements. An alarm triggers an alert if the HSM is moved (for example, slid out of the rack).
 - Users can configure the motion sensor’s threshold sensitivity to one of three levels: low, medium, high, corresponding to different movement thresholds
 - When powered by battery, the alarm maintains the same capabilities as when powered from main power.
 - The anti-theft feature relies on tilt angle for determining when to trigger a tamper.

Motion Sensor hardware filter settings:

- Low Sensitivity - 171 milli-g
- Medium Sensitivity - 65 milli-g
- High Sensitivity - 25 milli-g

The Motion sensor activity time is 6 ticks @50Hz (.12 seconds)

The Hardware filter is a reference setting which tracks the absolute change in acceleration in all three axes ignoring acceleration due to gravity (g). The filter is dynamically updated as the device is tilted.

Motion Sensor tilt threshold values:

- Low Sensitivity - 171 milli-g (Tilt angle 10.0 degrees +-1 degree)
- Medium Sensitivity - 65 milli-g (Tilt angle 6.0 degrees +-1 degree)
- High Sensitivity – 25 milli-g (Tilt angle 1.5 degrees +-1 degree)

9.10.6.3 Fraud

This tab allows you to configure fraud detection settings when the unit is Offline or in Secure state and properly authorized. Select the “**Apply**” button to commit the changes to the HSM.

Fraud Detection:	
HSM reaction to Exceeding Fraud Limits?	<input type="button" value="Logging Only"/>
The HSM's built in fraud detection system will detect when any of the following limits is reached:	
PIN Validation failures per minute limit (0-65535):	100
PIN Validation failures per hour limit (0-65535):	1000
PIN Attack limit (0-65535):	100

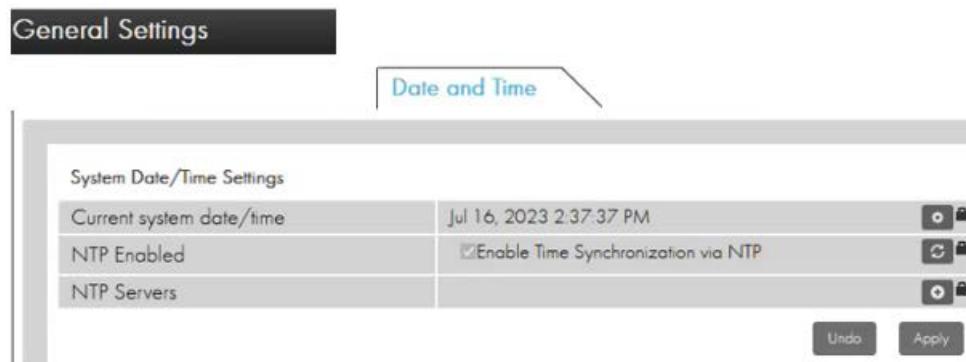
Options:

- HSM Reaction to Exceeding Fraud Limits:

Click from one of the following options:

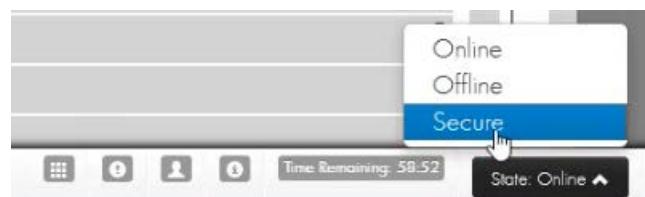
- Logging Only: The Health Check data will show how often the limits have been exceeded (if gathering of Health Check statistics is enabled). An entry is also made in the Audit Log when any of the limits are exceeded.
- On: The Health Check data will log the limits being exceeded, but in addition, the HSM will start returning error code 39 or delete its LMKs. An entry is also made in the Audit Log when any of the limits are exceeded.
- PIN Validation failures per minute limit:
 - The number of PIN validation failures permitted in a one-minute period before a fraud alert is triggered.
- PIN Validation failures per hour limit:
 - The number of PIN validation failures permitted in a one-hour period before a fraud alert is triggered.
- PIN Attack limit:
 - The number of PIN attacks permitted before a fraud alert is triggered.

9.10.6.4 Date and Time



This tab allows you to view or set the system date and time configuration. The time and date used by payShield 10K can either use the internal clock or alternatively the time and date can be obtained from a Network Time Protocol (NTP) server which will provide the time synchronized across multiple systems.

To set or change the confirmation for either of these activities, both AUTH state (using activity SETTIME) and SECURE state are required.



Setting the Internal Clock

The “Current system date/time” setting provides a basic chronological reference.

To set the date and time, click the gear icon. In the dialogue box that appears, click the new date and time values and click “**Apply**”.

Note: Setting the date or time back may prevent the payShield Manager from allowing a user to login. Care must be taken when changing the date back such that it is not earlier than the creation date/time of any of the Smart Cards that will be used to access the HSM.

Configuring NTP

Selecting NTP enabled provides the following:

- Accuracy: NTP synchronizes with precise time sources, i.e., atomic clocks
- Automatic synchronization: Devices correct time drifts by regularly checking with NTP servers
- UTC Reference: NTP uses Coordinated Universal Time, allowing devices to adjust for local time zones
- Network consistency: NTP ensures synchronized time across multiple devices

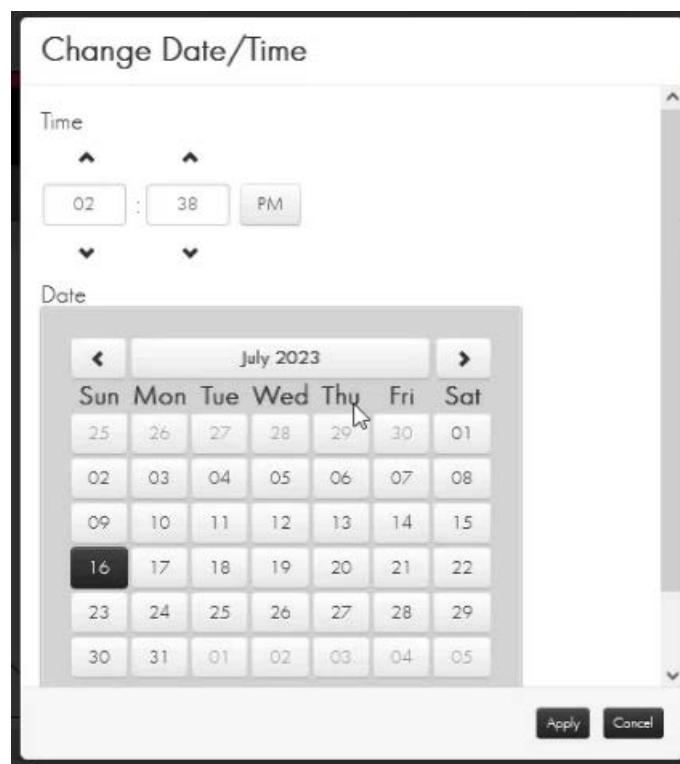
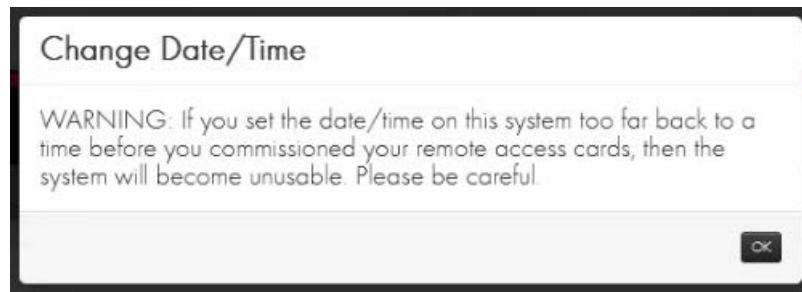
It is important to note that the payShield 10K internal clock must be set to within 15 minutes of the NTP Server in UTC format. The internal clock will not synchronize if the NTP Server is outside this range.

To Enable NTP, select the tick box:

System Date/Time Settings		
Current system date/time	Jul 16, 2023 2:38:04 PM	
NTP Enabled	<input checked="" type="checkbox"/> Enable Time Synchronization via NTP	
NTP Servers		
		Undo
		Apply

Note: You can disable NTP at any time and go back to the original date and time.

System Date/Time Settings		
Current system date/time	Jul 16, 2023 2:38:14 PM	
NTP Enabled	<input type="checkbox"/> Enable Time Synchronization via NTP	
NTP Servers		
		Undo
		Apply



NTP Servers

To add a NTP server, select the plus sign.

A screenshot of the "System Date/Time Settings" screen. It shows the current system date/time as "Jul 16, 2023 2:38:28 PM". Under "NTP Enabled", there is a checked checkbox for "Enable Time Synchronization via NTP". At the bottom right, there are "Undo", "Apply", and "Add" buttons. The "Add" button is highlighted with a red box and a cursor icon pointing to it.

Enter the IP address of the server:

System Date/Time Settings		
Current system date/time	Jul 16, 2023 2:38:55 PM	<input type="button" value=""/>
NTP Enabled	<input checked="" type="checkbox"/> Enable Time Synchronization via NTP	<input type="button" value=""/>
NTP Servers	<input type="button" value=""/> 10.194.191	<input type="button" value=""/> <input type="button" value=""/>
<input type="button" value="Undo"/> <input type="button" value="Apply"/>		

Select **Apply** to save.

System Date/Time Settings														
Current system date/time	Jul 16, 2023 2:39:32 PM													
NTP Enabled	<input checked="" type="checkbox"/> Enable Time Synchronization via NTP													
NTP Servers	<input type="button" value=""/> 10.194.191.62													
NTP Servers Status														
Server Status														
Name/IP Address		MS	Stratum	Poll	Reach	LastRx	Last Sample							
10.194.191.62		^?	9	6	3	1	-44643m[-44643m] +/- 12ms							
Authentication Status														
Name/IP Address		Mode	KeyID	Type	Klen	Last Atmp	NAK							
10.194.191.62		-	0	0	0	-	0							
		Cook	Clen											
		0	0											

Both the server status and the authentication status are reported.

NTP Server Authentication

Authentication is provided using Symmetric Authentication. Here a key is shared between the NTP Server and payShield 10K to provide an additional level of security. The key is entered in plain text as described below. The use of Symmetric Authentication is recommended but the NTP server can be used without authentication if required.

Jul 16, 2023 2:39:47 PM

Enable Time Synchronization via NTP

10.194.191.62
Symmetric Authentication Key

Server Status

Name/IP Address	MS	Stratum	Poll	Reach	LastRx	Last Sample
10.194.191.62	^?	9	6	3	2	-44643m[-44643m] +/- 12ms

Authentication Status

Name/IP Address	Mode	KeyID	Type	Klen	Last Atmp	NAK	Cook	Clen
10.194.191.62	-	0	0	0	-	0	0	0

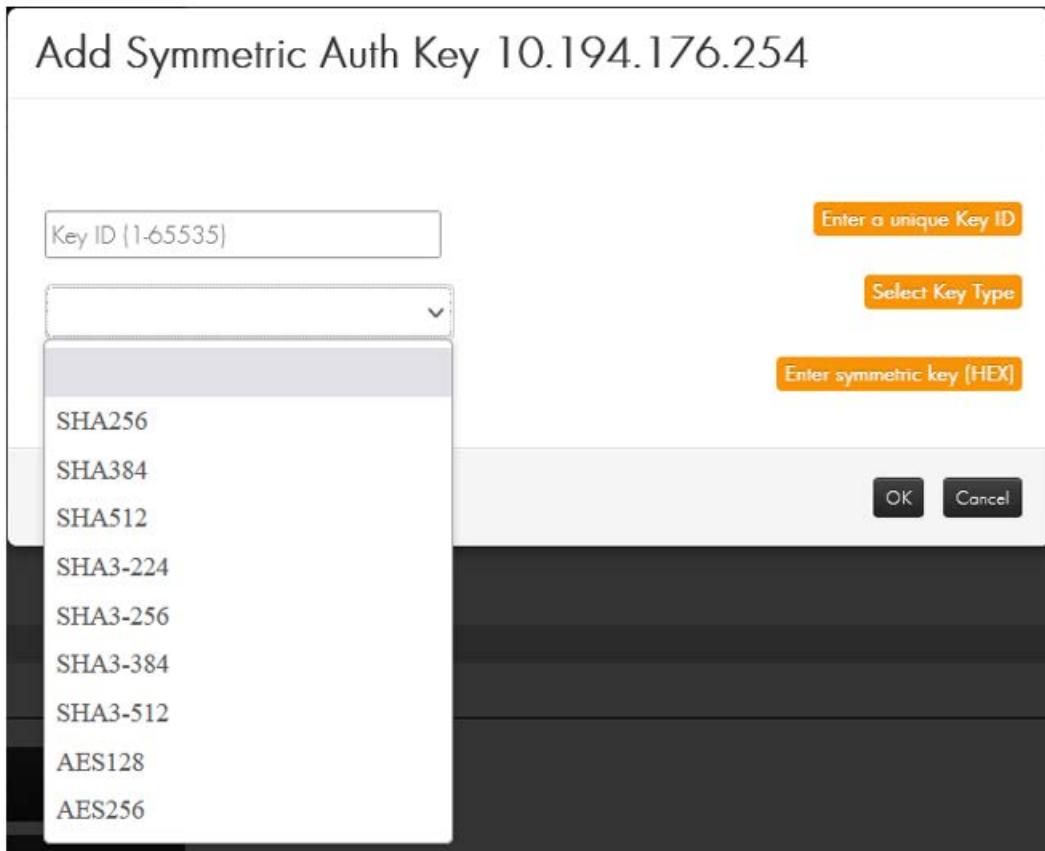
Undo Apply

Populate the data:

Add Symmetric Auth Key 10.194.191.62

Key ID (1-65535)	Enter a unique Key ID
	Select Key Type
Symmetric Key	Enter symmetric key (HEX)
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Note: The Key ID would have already been created on the server by the Administrator.



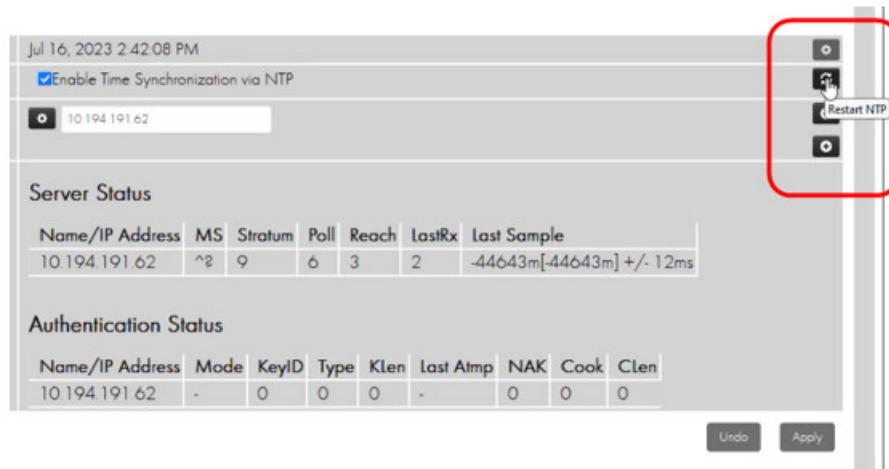
Note: The Symmetric Key must be in HEX. It can be entered via cut and paste or via keystroke.

Select **OK**.

Name/IP Address	MS	Stratum	Poll	Reach	LastRx	Last Sample
10.194.191.62	^2	9	6	3	2	-44643m[-44643m] +/- 12ms

Name/IP Address	Mode	KeyId	Type	Klen	Last Atmp	NAK	Cook	Clen
10.194.191.62	-	0	0	0	-	0	0	0

Select **Apply** to save.



Select **Restart NTP** to perform a restart. The restart will be noted in the Audit Log.

Audit Log

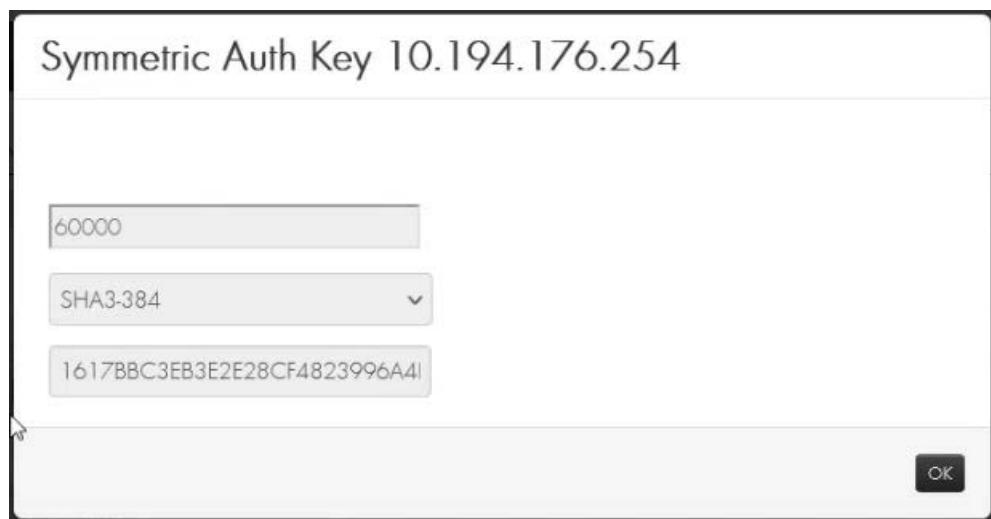
485	Jul 16, 2023 14:39:32	A	20	00		Remote (80fb17c) - N 7307001092072979
484	Jul 16, 2023 14:39:31	A	20	00		Remote (80fb17c) - N 7307001092072979
483	Jul 16, 2023 14:39:30	A	20	00		Remote (80fb17c) - N 7307001092072979
482	Jul 16, 2023 14:39:29	A	20	00		Remote (80fb17c) - N 7307001092072979
481	Jul 16, 2023 14:39:28	A	20	00		Remote (80fb17c) - N 7307001092072979
480	Jul 16, 2023 14:39:28	A	00	00		NTP service restarted

Note: To review your NTP Servers, select the setting icon.

System Date/Time Settings

Current system date/time	Aug 28, 2023 2:37:19 PM
NTP Enabled	<input checked="" type="checkbox"/> Enable Time Synchronization via NTP
NTP Servers	<div style="display: flex; align-items: center;"> 0.194.176.254 </div> <div style="margin-top: 10px;"> 10.194.191.62 </div>

A pop-up display opens:



9.10.6.5 Remote Syslog

This tab allows the user to configure a Remote Syslog Server's address, allowing a payShield 10K to send local error and audit logs to a remote syslog server. Users are able to configure up to two remote syslog servers and can choose to communicate with the remote server(s) over the payShield 10K's management or auxiliary interface. The user also has the option to choose non-default ports (i.e., supported custom ports) in the range of 49300 through 49320 or, if preferred, use the default ports 601 and 514.

Note: To delete a remote syslog server, click this link: [To delete](#):

The feature is enabled and disabled via a toggle switch.



To enable:

1. Enter the **Secure** state.

Note: In the example above: syslog is enabled; one server is added; custom port 49300; default management Interface.

2. Select the check box for **Enable Remote Syslog**.

3. Configure either one or two servers as required:

- Enter the both Server IP addresses.
- Enter both server port numbers.
- Select your interface.

4. Click **Apply**.

The feature is now enabled.

5. View the audit log for confirmation; navigate to:

Status > Audit Log

The screenshot shows the 'Status' tab selected in the top navigation bar. Below it is a sidebar with links: Device Information, Utilization Statistics, Health Statistics/Diagnostics, Error Log, and Audit Log. The main area displays a table titled 'Audit Log' with columns: Counter, Time, Code Type, Code, Code, and Text. The table contains five rows of log entries. A red arrow points from the sidebar's 'Audit Log' link to the table. At the bottom right of the table are buttons for Download, Get More, Reload, and Clear.

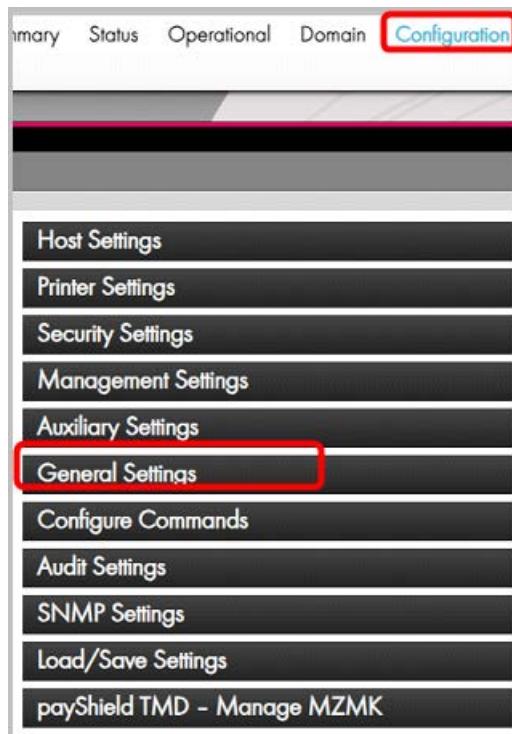
Counter	Time	Code Type	Code	Code	Text
711	Jul 11, 2024 00:32:05	A	00	00	SYSLOG server interface updated to Auxiliary interface
710	Jul 11, 2024 00:32:05	A	00	00	SYSLOG server Port updated to 601
709	Jul 11, 2024 00:32:05	A	00	00	SYSLOG server IP address updated to 10.194.172.186
708	Jul 11, 2024 00:30:47	A	00	00	SYSLOG server Port updated to 49300
707	Jul 11, 2024 00:30:47	A	00	00	SYSLOG server IP address updated to 10.194.172.185
	Jul 11, 2024				

The logs from both the Error Log and the Audit Log are now supplied to the remote syslog server(s).

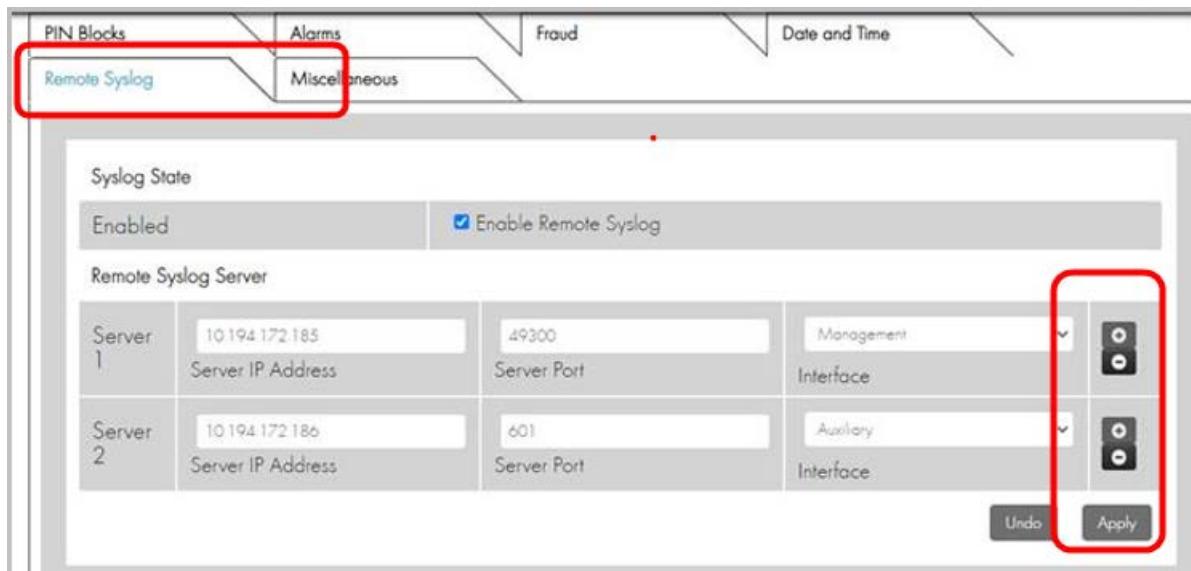
To delete:

1. Login to payShield Manager and navigate to **General Settings**.

Configuration > General Settings



2. Select the **Remote Syslog** tab.



3. Mark the server for deletion by selecting the corresponding minus sign.
4. Click **Apply**.
5. Confirm the deletion:
 - Open the Audit Log and verify the deletion "SYLOG server <IP address> is removed"

9.10.6.6 Miscellaneous

This tab allows the user to set the HSM System Name, Description, Location and Contact fields, which are displayed as a more user-friendly way of identifying a particular HSM. These may be altered in any state. Press the “**Apply**” button to commit the changes to the HSM. Location and Contact fields are optional. These fields are also used for SNMP MIB-2 system objects (sysName, sysDescr, sysLocation, sysContact).

The HSM System Name is displayed in the Landing Page under the Summary section when enabled in the security settings. Configuration for information on enabling the display of the name on the Landing Page.

System Name Configuration: (also used for SNMP MIB-2 system settings)	
Name (1-20 characters)	10Krangle
Description (1-80 characters)	payShield 10K
Location (0-80 characters)	Plantation
Contact (0-80 characters)	support@thalessecurity.com

Undo Apply

9.10.7 Configure Commands

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 Configure Commands option allows users to click which console and Host commands are to be enabled/disabled when the unit is in Secure state.

Commands can be enabled or disabled by checking or unchecking the appropriate box(es) in the tables. Checked items are enabled; unchecked items are disabled.

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

This section is split into two tabs: one for Console Commands, and one for Host Commands. While Console Commands may be enabled or disabled as desired, enabling a Host Command also requires that the corresponding license file to be installed.

When “Settings per LMK” is enabled, Host Commands can enabled or disabled separately for each LMK ID. The LMK ID is selected using the drop down box at the top of the list.

Configure Commands

Console Host

Name	Enabled	
A6 (Set KMC Sequence Number)	<input checked="" type="checkbox"/>	
CK (Generate a Check Value)	<input checked="" type="checkbox"/>	
CV (Generate a Card Verification Value)	<input checked="" type="checkbox"/>	
EC (Encrypt Clear Component)	<input checked="" type="checkbox"/>	
ED (Encrypt Decimalization Table)	<input checked="" type="checkbox"/>	
FK (Form Key from Components)	<input checked="" type="checkbox"/>	
GC (Generate Key Component)	<input checked="" type="checkbox"/>	
GK (Generate LMK Component)	<input checked="" type="checkbox"/>	

Commands Hash: 0c0a63

Undo Apply

Configure Commands

Console Host

LMK ID	0	1	2	3	4	Licensed	Enabled	
Name								
A0 (Generate a Key)	0	1	2	3	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
A2 (Generate and Print a Component)						<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
A4 (Form a key from encrypted components)						<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
A6 (Import a Key)						<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
A8 (Export a Key)						<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
AA						<input type="checkbox"/>	<input type="checkbox"/>	

Commands Hash: c62313

Undo **Apply**

After making changes, press the “**Apply**” button to commit the changes to the HSM.



The UI will generate a SHA-256 Hash over a set of available commands. You can use offline tools to compute the hash and compare it with the value displayed to ensure that two or more HSMs have the same set of commands available.

9.10.8 Audit Settings

Navigate to: Configuration > Audit Settings > General

Screenshot of the Configuration > Audit Settings > General page. The top navigation bar includes tabs for Summary, Status, Operational, Domain, Configuration (which is highlighted in blue), and Virtual Console. A 'Quick Links' dropdown is also present. The left sidebar has four sections: Auxiliary Settings, General Settings, Configure Commands, and Audit Settings (which is also highlighted). Below the sidebar is a note: "Certain sensitive functions, such as key management, authorizations, configuration and diagnostic tests are always recorded in the audit log and their auditing cannot be disabled." A red arrow points from this note to the audit options table. The table has tabs for General, Console Cmds, Host Cmds, and Manager, with General selected. The table lists audit options with checkboxes and lock icons:

Using the list below, select the Audit Options that the HSM should process.			
Audit User Actions	<input checked="" type="checkbox"/>		
Audit Error Responses to Host Commands	<input type="checkbox"/>		
Audit utilization data resets	<input checked="" type="checkbox"/>		
Audit diagnostic self tests	<input type="checkbox"/>		
Audit ACL connection failures	<input type="checkbox"/>		
Audit Counter Value (decimal)	306		

The HSM's standard auditing capabilities include auditing (i.e., logging) of various events in the HSM's Audit Log. The Auditing accordion allows users to click which items are to be audited and which are not when the unit is Offline or in Secure state and properly authorized.

After making changes press the “**Apply**” button to commit the changes to the HSM.

9.10.8.1 Audit - General

Certain sensitive functions, such as key management, authorizations, configurations and diagnostic tests are always recorded in the Audit Log and their auditing cannot be disabled.

To view the audit settings, navigate to: **Configure > Audit > Settings**

The screenshot shows the 'Audit Settings' page under the 'Configuration' tab. The left sidebar lists 'Auxiliary Settings', 'General Settings', 'Configure Commands', and 'Audit Settings'. A red arrow points from the 'Audit Settings' link to the 'General' tab in the main content area. The main content area contains a note about auditing sensitive functions and a table of audit options:

Using the list below, select the Audit Options that the HSM should process.			
Audit User Actions	<input checked="" type="checkbox"/>		
Audit Error Responses to Host Commands	<input type="checkbox"/>		
Audit utilization data resets	<input checked="" type="checkbox"/>		
Audit diagnostic self tests	<input type="checkbox"/>		
Audit ACL connection failures	<input type="checkbox"/>		
Audit Counter Value (decimal)	306		

In the General tab, users can enable auditing of the following events:

- User Actions
- Error Responses to Host Commands
- Utilization Data Resets
- Diagnostic Self Tests
- ACL Connection Failures

Users can also set the audit counter value.

Note: Notification is provided when the Audit Log is 80%, 95% and 100% full.

Note: Typically, you do not audit commands that run all the time.

9.10.8.2 Audit - Console Commands

The screenshot shows the 'Configuration' tab selected in the top navigation bar. Below it, the 'Audit Settings' section is active. A note states: 'Certain sensitive functions, such as key management, authorizations, configuration and diagnostic tests are always recorded in the audit log and their auditing cannot be disabled.' A sub-section titled 'Console Cmds' is selected. It displays a list of console commands with checkboxes for enabling auditing. The 'Audit' column contains lock icons.

Console Command	Audit
A6	<input type="checkbox"/>
AUDITLOG	<input type="checkbox"/>
CA	<input type="checkbox"/>
CK	<input type="checkbox"/>
CLEARERR	<input type="checkbox"/>
CLEARAUDIT	<input type="checkbox"/>
CO	<input type="checkbox"/>
CONFIGACL	<input type="checkbox"/>
CP	<input type="checkbox"/>

At the bottom right are 'Undo' and 'Apply' buttons.

It is possible to audit any of the console commands. Activities can be enabled or disabled by checking or un-checking the appropriate box(es). Checked items are enabled; uncheck items are disabled.

9.10.8.3 Audit - Host Commands

A red arrow points from the 'Audit Settings' link in the top navigation bar to the 'Host Cmds' tab in the sub-navigation bar. Another red arrow points from the 'Host Cmds' tab to the audit log message below it.

Certain sensitive functions, such as key management, authorizations, configuration and diagnostic tests are always recorded in the audit log and their auditing cannot be disabled.

General Console Cmds **Host Cmds** Manager

Using the list below, select the Host Commands that the HSM should Audit.

A0	<input type="checkbox"/>	
A2	<input type="checkbox"/>	
A4	<input type="checkbox"/>	
A6	<input type="checkbox"/>	
A8	<input type="checkbox"/>	
AA	<input type="checkbox"/>	
AC	<input type="checkbox"/>	
AE	<input type="checkbox"/>	
AG	<input type="checkbox"/>	

Undo Apply

It is possible to audit any of the Host commands available in the HSM's license. Activities can be enabled or disabled by checking or unchecking the appropriate box(es). Checked items are enabled; unchecked items are disabled.

9.10.8.4 Audit - Management Commands

Certain sensitive functions, such as key management, authorizations, configuration and diagnostic tests are always recorded in the audit log and their auditing cannot be disabled.

Using the list below, select the management commands that the HSM should audit.

CTA share read from smartcard	<input type="checkbox"/>	
CTA share load from smartcard	<input type="checkbox"/>	
Health statistics report	<input type="checkbox"/>	
Health statistics reset	<input type="checkbox"/>	
Error log retrieve	<input type="checkbox"/>	
Error log download	<input type="checkbox"/>	
Audit log retrieve	<input type="checkbox"/>	
Audit log download	<input type="checkbox"/>	
Printer settings	<input type="checkbox"/>	

Undo Apply

In the Manager tab, you can enable auditing of all HSM Manager events, such as logins, state changes and configuration changes.

9.10.9 SNMP Settings

This section allows you to SNMP settings of the HSM when the unit is in any state.

The screenshot shows the 'Configuration' tab selected in the top navigation bar. The left sidebar lists several settings sections: Security Settings, Management Settings, Auxiliary Settings, General Settings, Configure Commands, Audit Settings, and **SNMP Settings**. A red arrow points from the 'Configuration' tab towards the 'SNMP Settings' section. The main content area displays the 'SNMP State' configuration, which includes an 'Enabled' checkbox (unchecked) and a dropdown menu set to 'Management'. Below this is a table titled 'Version 3 (V3) Users' with columns for Name, Authentication Algorithm, and Privacy Algorithm. The 'Name' column contains a placeholder input field, and the 'Authentication Algorithm' and 'Privacy Algorithm' columns each have dropdown menus set to 'None'.

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

- “Instantaneous” utilization data relating to HSM loading and Host command volumes
- Current status of HSM health check factors

Note: Only SNMP V3 is supported.

- **SNMP State**

This section controls the state of the SNMP service using the following fields:

- Enabled: Check this box to enable SNMP reporting, uncheck it to disable
- Enabled on Port: Which Ethernet port to use for SNMP traffic
- You must specify the authentication and privacy algorithms to be used
- To add a V3 user, enter the following fields and then click the plus icon:
Name
Authentication Algorithm (and password)
Privacy Algorithm (and password)

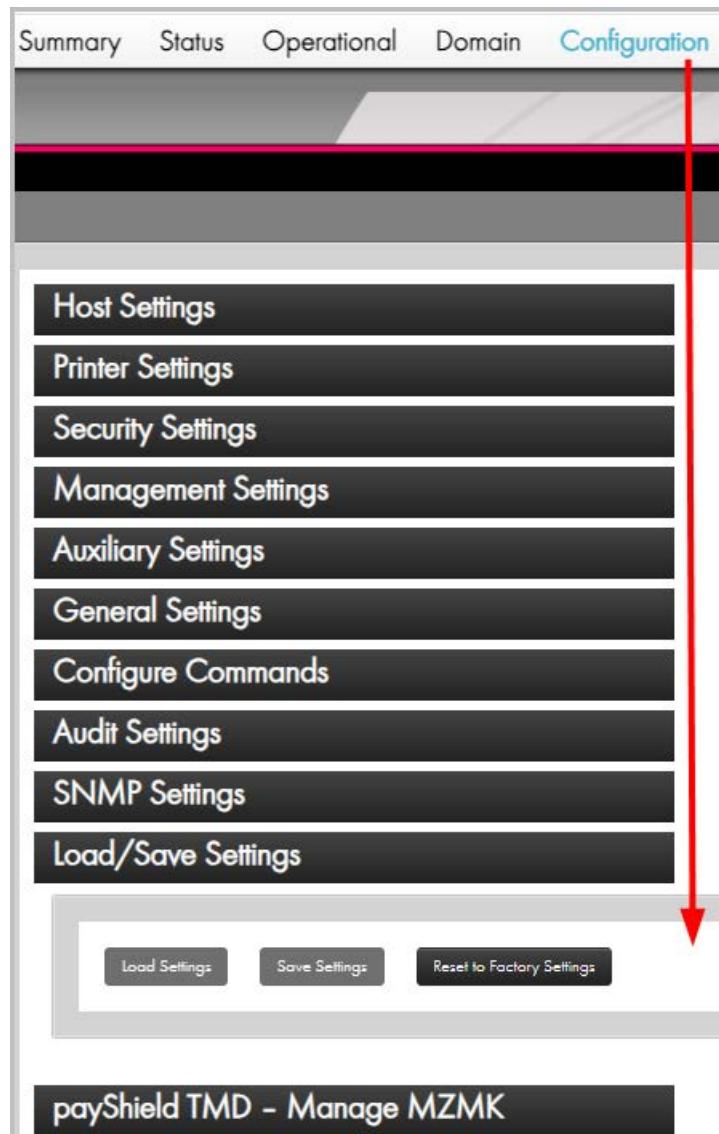
- To delete a User, click the minus icon next to that user

Note: SNMP MIB-2 system values corresponding to MIB2system values in console SNMP command (sysName, sysDescr, sysLocation, sysContact) can be set under **General Settings** tab.

Port	Protocol	Purpose
161	UDP	SNMP Requests - Utilization and Health Check data
162	UDP	SNMP Traps

9.10.10 Load/Save Settings

In this section you can save the active configuration to a Smart Card, reload configuration data from a settings Smart Card, or reset the HSM to its Factory Default settings.



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

Saving or restoring settings must be done in Secure state with proper authorization. You may “Reset to Factory Settings” when in secure state.

When “Settings per LMK” is enabled, settings for each LMK ID are saved separately to individual smart cards for each LMK ID. The LMK ID required is selected when saving or restoring settings.

The settings saved when using payShield Manager are as follows:

- Alarm Settings
- Audit Settings
- The Console Commands that are enabled
- Fraud Settings

- Access Control List (ACL) for Host Interfaces 1 & 2
- Host Port Settings
- Host Commands that are enabled
- Management Port Settings
- PIN Block formats that are enabled
- Printer Port Settings
- Remote Syslog Settings
- Security Settings
- SNMP Settings
- Utilization Data settings

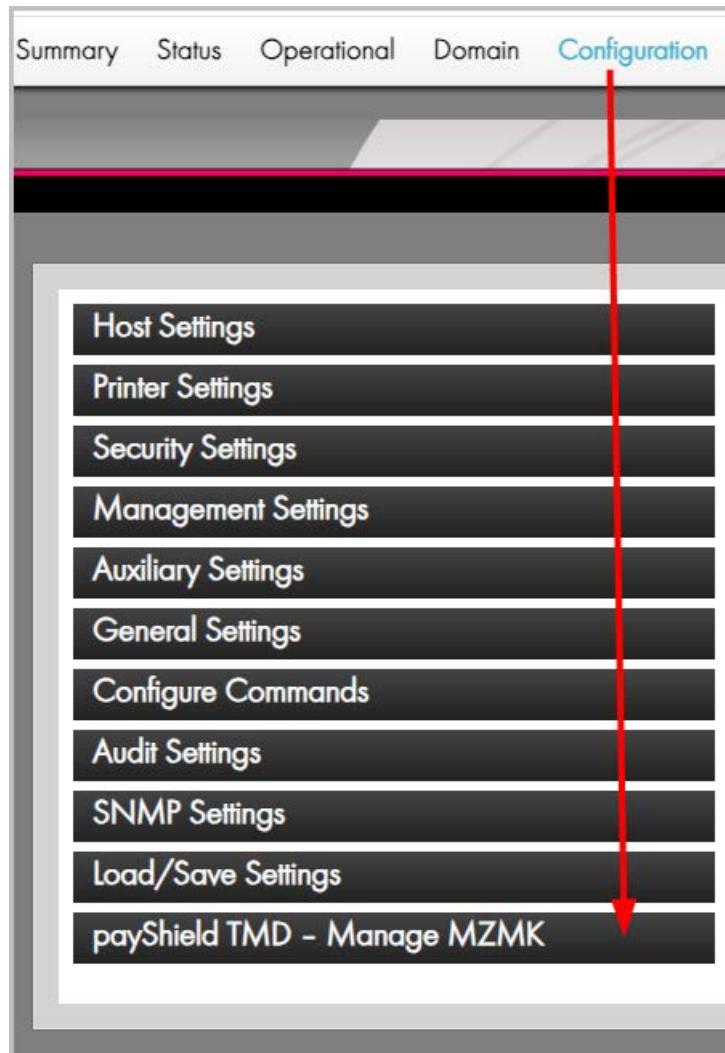
Please note that the following settings are not currently saved to smart card:

- Time set to run automatic self-tests
- Auxiliary Port Settings
- Health Check Statistics Gathering Setting
- NTP Settings
- payShield Manager Serial and Certificate numbers allocated for use as a Left Key or a Right Key

Also note that when duplicating the configuration of a payShield 10K to another device:

- The LMK, CTA, TLS Certificates, and Licenses need to be installed separately on the new device.
- The current time must be set separately on the new device.
- Data stored in User Storage is managed by the application and so the application is responsible for duplicating this data to the new device.

9.10.11 payShield TMD - Manage MZMK



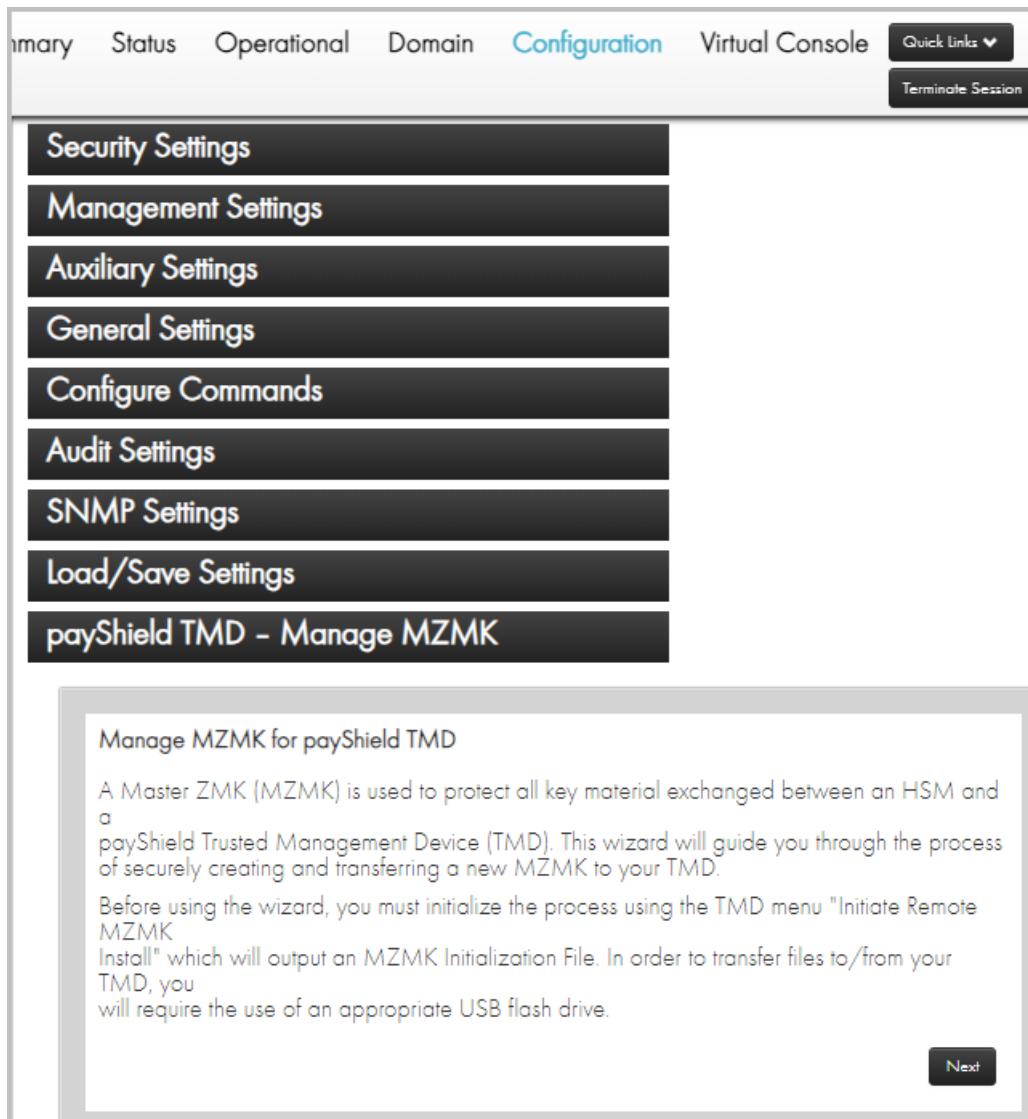
This section describes the steps required when using payShield Manager to share the MZMK with the TMD using the Elliptic Curve Key Agreement Algorithm (ECKA). First the payShield TMD's ECC public key from a USB drive is loaded into payShield Manager and then a Master Zone Master Key (MZMK) is generated in the HSM. The MZMK can be double/triple-length DES key, or a 128/192/256-bit AES key. The MZMK is encrypted under the selected LMK and displayed for the user to copy. The MZMK derivation data - required to share the MZMK with the TMD using ECKA - is then exported in a CSV file and is required to be transferred into TMD using appropriate flash drive.

As a prerequisite to setup the MZMK, create an ECC key pair on the payShield TMD and save the Public key along with its fingerprint on a USB drive.

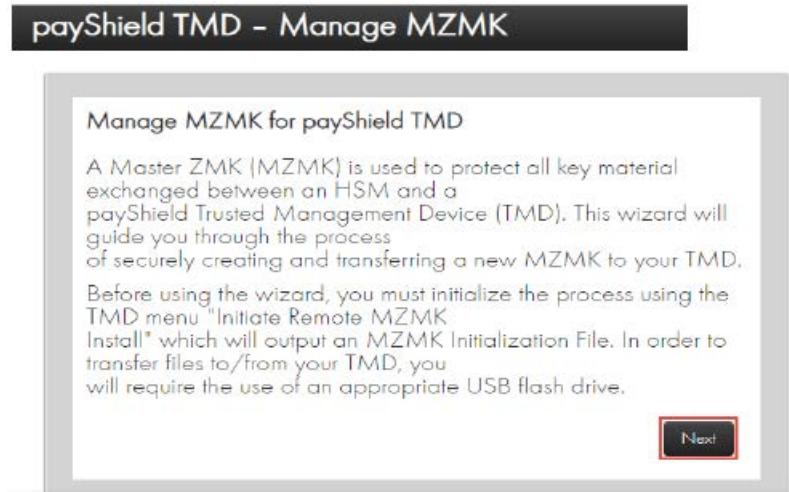
Note: This feature requires security setting “**Enable multiple authorized activities**” set to YES.

9.10.11.1 Initiate Manage MZMK

1. Expand the payShield TMD - Manage MZMK menu.
2. The following is displayed:



Follow the wizard instructions to manage MZMK for payShield TMD.



1. Click **Next**.

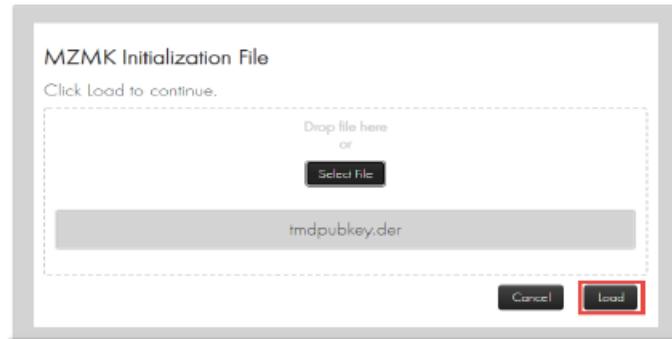
payShield Manager displays:



To read an MZMK Initialization File containing the TMD's Public Key from the USB flash drive,

- Insert the USB drive that carries the key in the USB port of your computer
- Select or drag and drop the file from the USB.

payShield Manager displays (example):

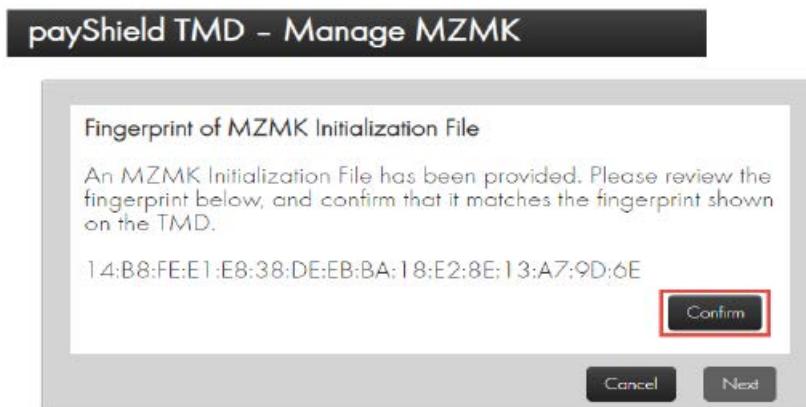


Note: The Load button is enabled once payShield Manager detects the file.

2. Click **Load** to load the public key.

9.10.11.2 Display Fingerprint of the Public Key

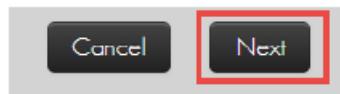
Once you load the MZMK Initialization File in payShield Manager, its fingerprint is displayed on the screen. You must confirm the fingerprint by comparing it with that of TMD's public key to proceed.



3. Click **Confirm** to validate the fingerprint of the TMD's Public Key.
4. If the fingerprint does not match, press **Cancel** to abort and select the appropriate file containing the TMD's public key.



After confirming the fingerprint, the **Next** button is enabled.



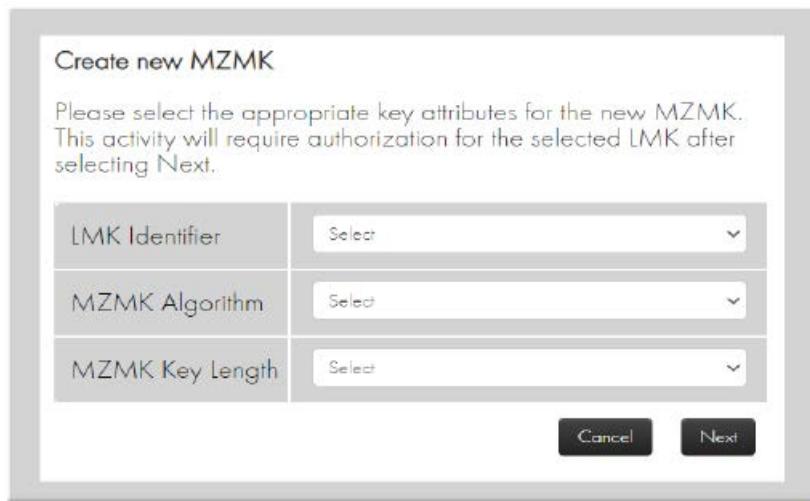
- Click **Next** to proceed to create the MZMK.

9.10.11.3 Create Master Zone Master Key (MZMK)

The wizard leads the user to the **Create new MZMK** section.

- Specify the MZMK attributes, i.e., LMK Identifier, MZMK Algorithm and MZMK Key Length.

Note: It is recommended that the user create the MZMK with maximum key length, so that it can be used to encrypt other keys with smaller or equal length.



Once you select LMK Identifier, the system automatically populates the default Algorithm and Key Length that corresponds with the selected LMK Identifier. Users can manually select their preferred key length.

- Select your preferred **LMK Identifier** from the drop down.



- Select the MZMK Algorithm from the available options, i.e., AES (shown in example) or 3DES.

Note: AES is the default algorithm when AES KeyBlock LMK is selected.



4. Select the Key Length, as per the algorithm selected.

- For Algorithm TDES
 - Double Length
 - Triple Length (default)
- For Algorithm AES
 - 128 bit
 - 192 bit
 - 256 bit (default)



payShield TMD - Manage MZMK

Create new MZMK

Please select the appropriate key attributes for the new MZMK. This activity will require authorization for the selected LMK after selecting Next.

LMK Identifier	2 , KeyBlock , AES-256 , 9D04AO , Keyblock Test ▾
MZMK Algorithm	AES ▾
MZMK Key Length	256 bit ▾

Cancel
Next

5. Click **Next**.

Note: Selecting an invalid combination will generate an error, i.e., “Invalid LMK Scheme and algo”.

After selecting **Next**, this activity will require authorization for the selected LMK. It requires two Authorizing Officers using their Smart Cards and PINs to confirm the activity.

You will be prompted to enter a card containing the first of the selected LMK's authorizing PIN. Insert the card and enter the PIN. You will then be prompted to enter a card containing the second of the selected LMK's authorizing PIN. Insert the card and enter the PIN. Upon success, the activity is authorized.

9.10.11.4 MZMK Information

This page displays the Master Zone Master Key (MZMK) encrypted under the selected LMK and the Key Check Value (KCV) of the key. The user can copy and/or export the encrypted key along with KCV for further use.

Manage Remote MZMK

Master Zone Master Key [MZMK]	
This page displays encrypted MZMK under LMK and its Key Check Value (KCV). Please copy or export and save the encrypted key and KCV; it will not be stored.	
Encrypted MZMK	AAAAAAAAAAAAAAA1111111111111222222222222233333333333333
KCV of MZMK	332211
Cancel Export Next	

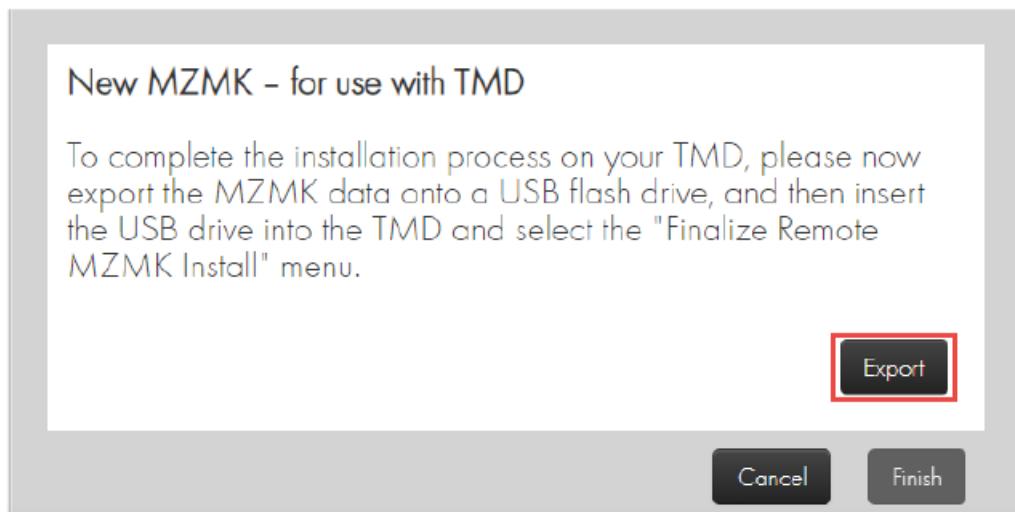
1. Click **Copy** to copy the Encrypted MZMK and the KCV of the MZMK onto the clipboard for future reference.
2. Click **Export** to download it for future reference.



3. Save the file containing Encrypted MZMK and KCV to an appropriate location.
4. Click **Next**.

9.10.11.5 Export Data

This page allows users to export the MZMK derivation data required for ECKA and save it on an appropriate USB drive.



5. Click **Export** to save data on the USB drive.

The CSV file includes exported data comprising Shared Info, MZMK Check Value, HSM Public Key, etc. Once the CSV file has been exported, the **Finish** button is enabled.



6. Click **Finish**.
7. Should you need to abort the operation, click **Cancel**.

The wizard returns to the Manage MZMK screen.

9.11 Settings per LMK

9.11.1 Overview

With the introduction of the Enable Settings per LMK on the Configuration page, security officers are able to configure the following on a per-LMK basis:

- Security Settings
- Enabled Host Commands
- Enabled PIN Blocks

The Enable Settings per LMK setting uses a toggle check box to enable or disable the setting.

Note: When “Settings per LMK” is enabled, host commands are processed based on the TCP port number.

A more detailed overview of the Feature is given in the *payShield 10K Programmer’s Manual*.

9.11.2 Enable the feature

The process for enabling settings per LMK is summarized as follows:

1. Place the unit in Secure State.
2. Disable UDP (and FICON).
3. Navigate to the Security General tab.
4. Toggle on the check box for Enable Settings per LMK.
5. Reinstall the LMK which is deleted in the previous step as a security measure.

The sections that follow, demonstrate the navigation process.

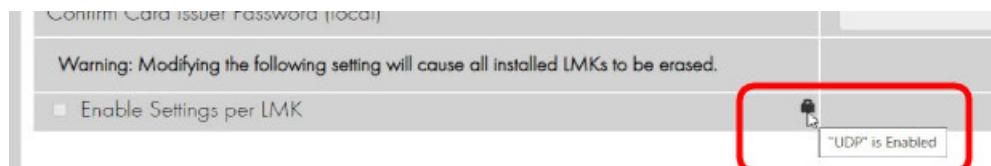
Prerequisite: The payShield 10K is in the **Secure State**.

1. Confirm that the unit is in the Secure state.

Note: Refer to: [Section 9.5.1.3, “Secure”, on page 116](#), if you need assistance.

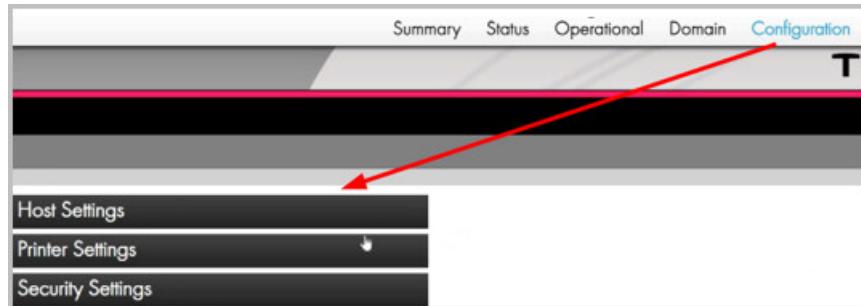
2. Determine if UDP is Enabled or Disabled.

Hover over the lock icon to activate the help text that displays the current state.

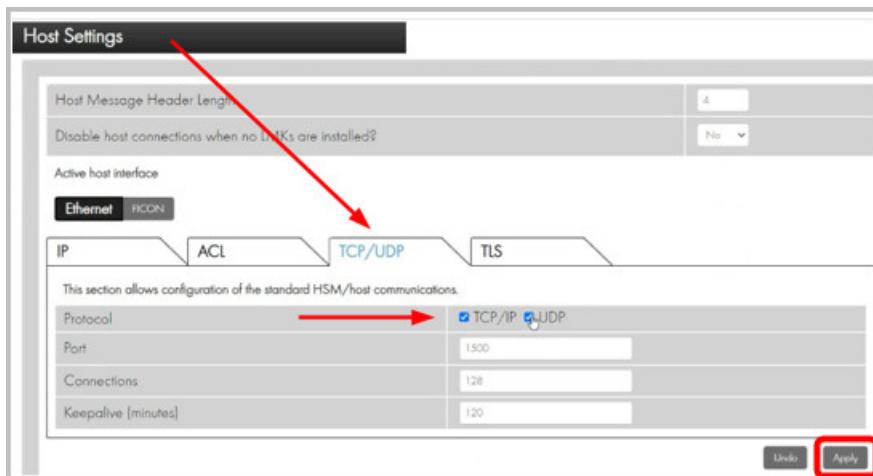


3. Navigate to the TCP/UPD tab to **disable** UDP:

- **Configuration > Host Settings > TCP/UPD**

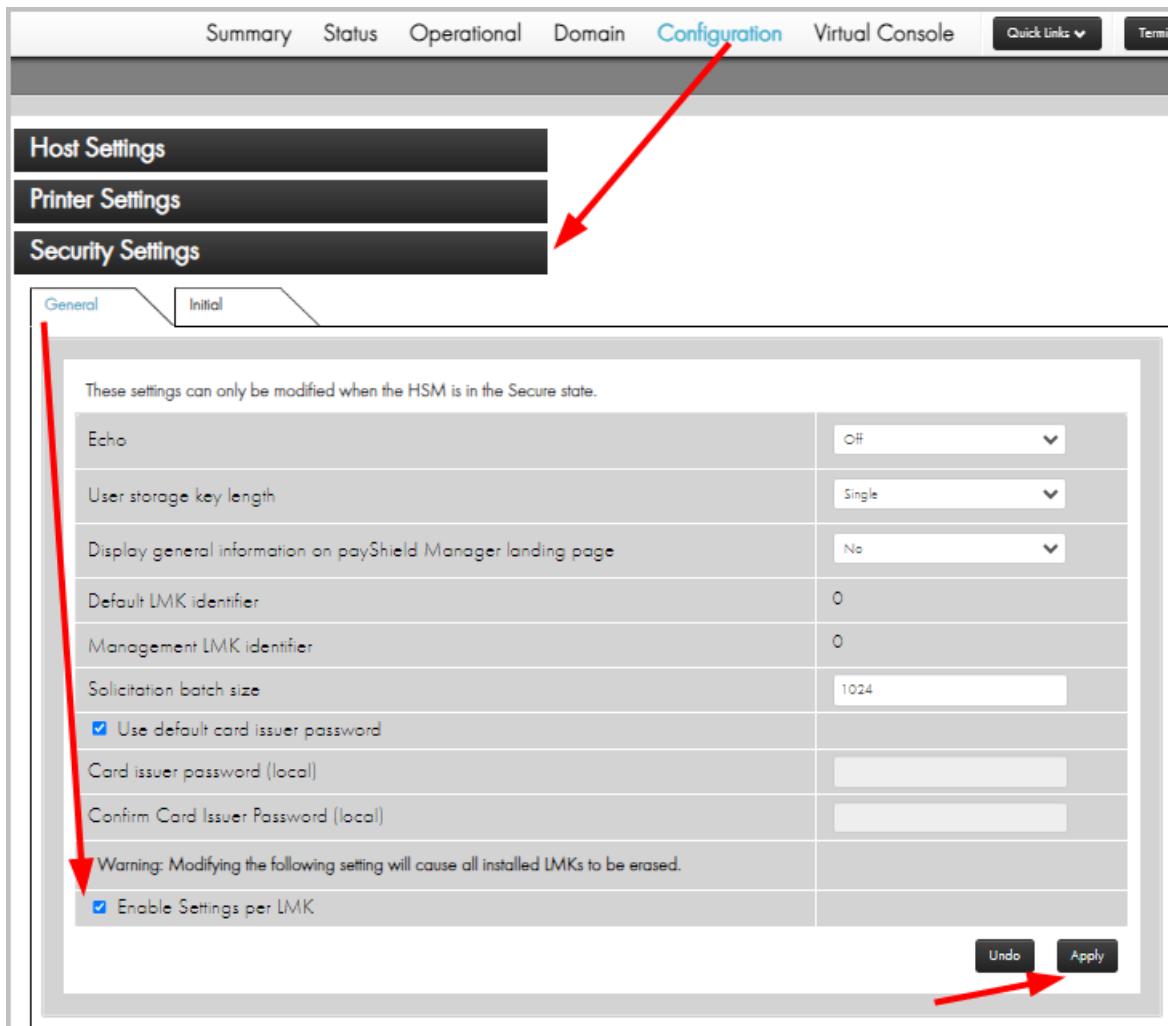


Note: FICON is a separate product option.



4. Toggle off the UDP check box and then click **Apply**.
5. Select the “Enable Settings per LMK” setting.
6. Click **Apply**.

Note: The LMKs will be erased at this point for security reasons and now must be reinstalled.



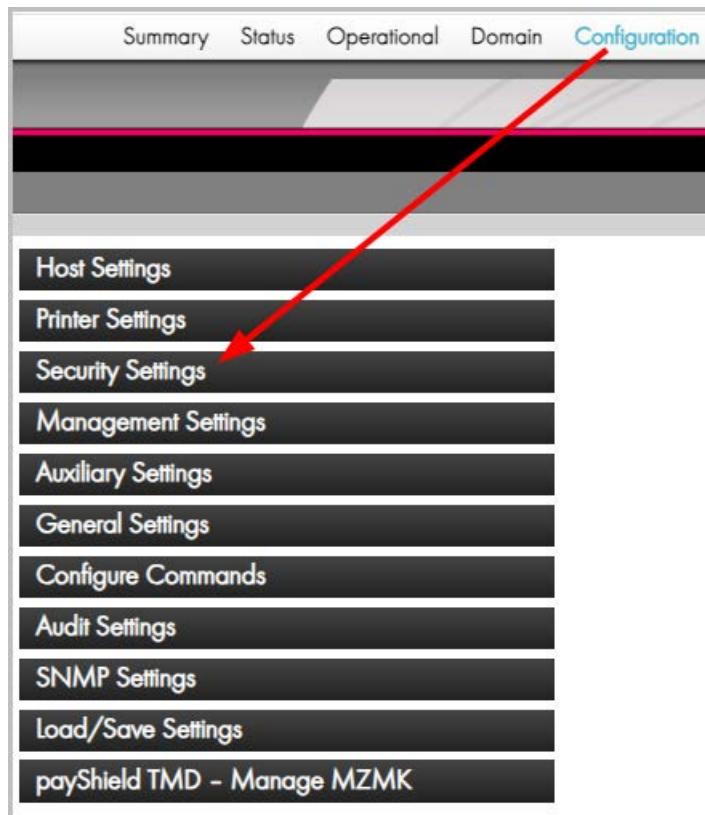
Note: To enable/disable the Settings per LMK via the console, refer to the *payShield 10K Console Guide*.

9.11.3 Assigning Security Settings per LMK ID

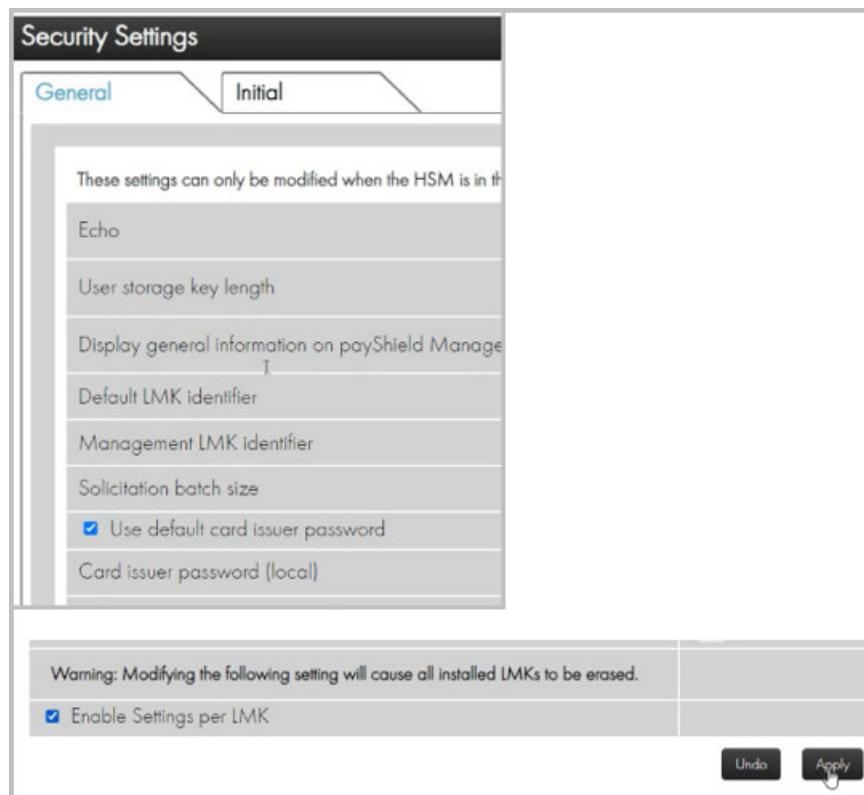
Note: The payShield Model D with 10Gbit/s Ethernet ports provide increased speed.

The process of assigning settings to specific LMKs is basically the same as in earlier releases - the only difference is that the LMK ID must be selected using the drop-down box first.

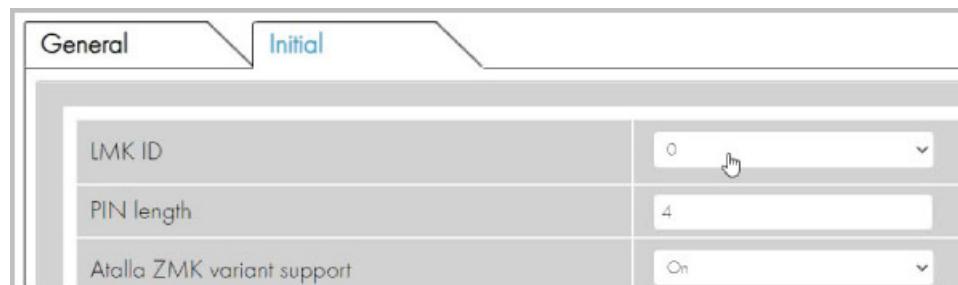
1. From the **Configuration tab**, scroll to **Security Settings**.



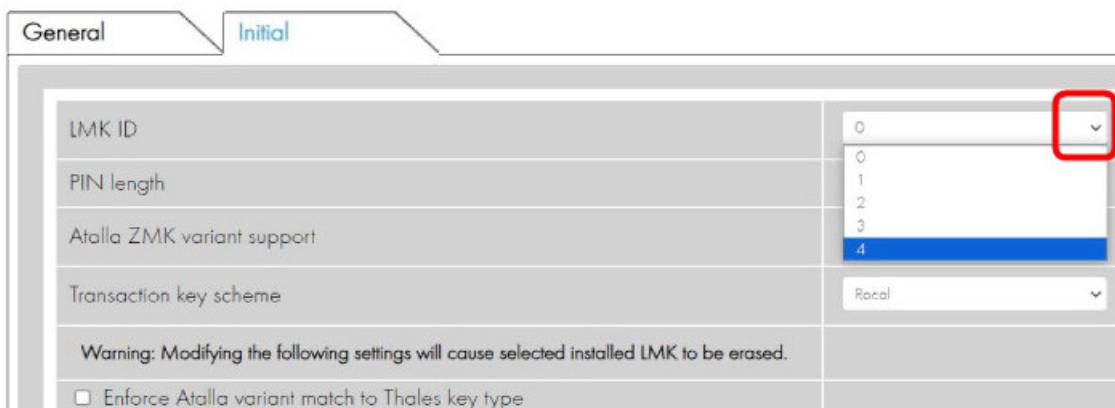
The General tab opens.



2. Select the Initial tab.



3. Open the LMK ID drop down and select the LMK ID (in the example LMK ID 4).

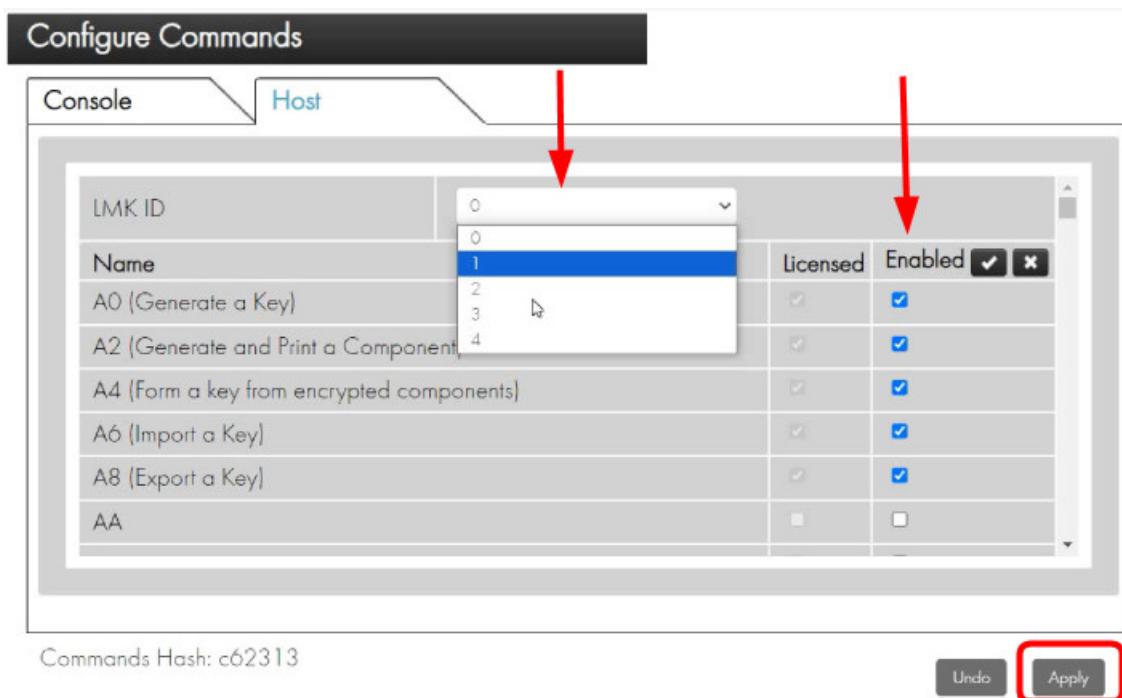


Now you are ready to select the setting to be associated with LMK ID 4, for example.

4. Toggle on the check boxes for the settings to be assigned to LMK ID 4, as in the example; when finished, click **Apply**.
5. Repeat this process for each LMK ID as required.

9.11.4 Enabling Host Commands for Each LMK ID

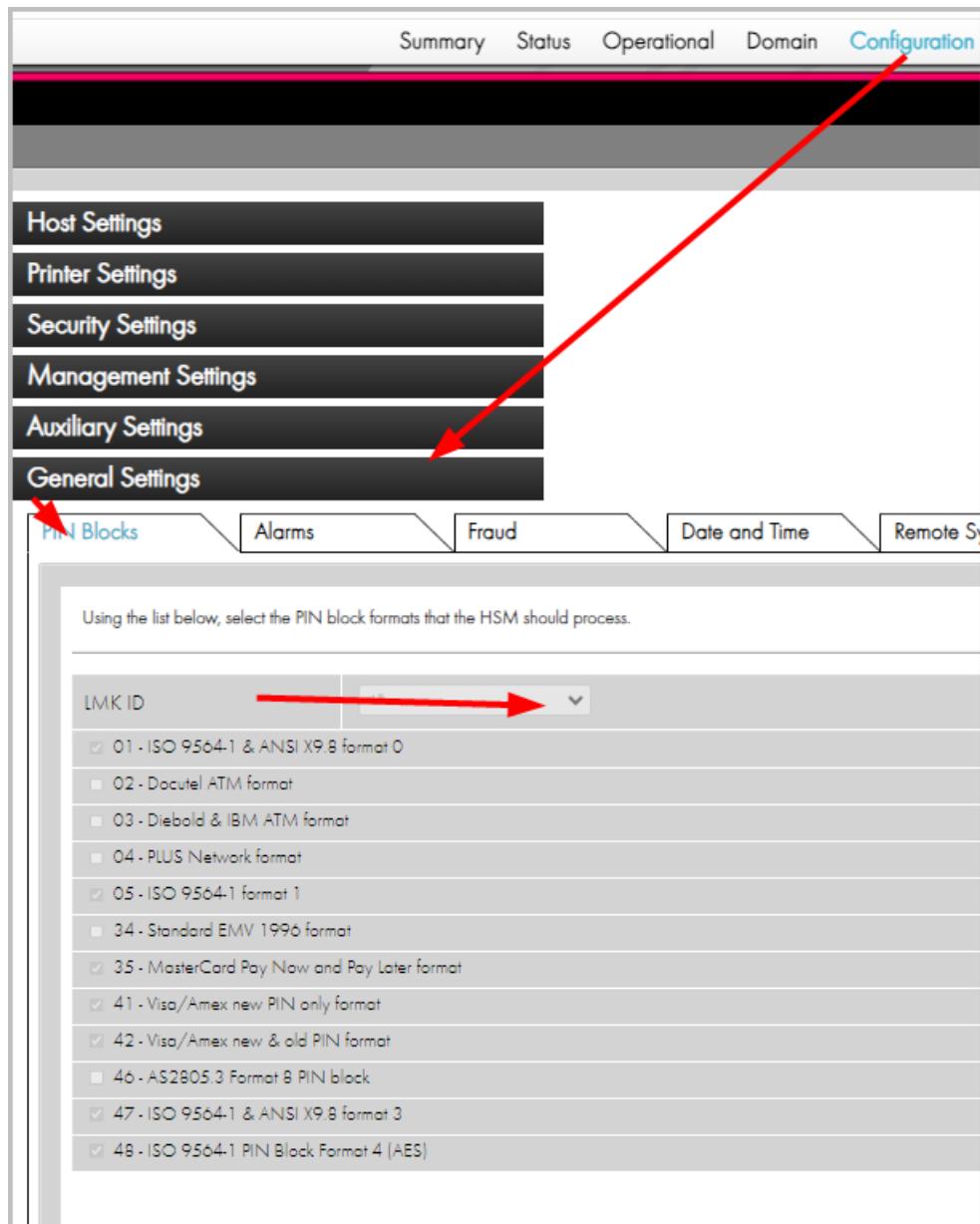
1. Navigate to the Host command tab:
 - Configuration > Configure Commands > Host
2. Open the LMK ID drop down.
3. Toggle the check box for each setting to be associated with your chosen LMK ID.
4. Click **Apply**.



5. Repeat this process for each LMK as required.

9.11.5 Assigning PIN Blocks to LMKs

1. Navigate to the Host command tab:
 - Configuration > General Settings > PIN Blocks
2. Open the LMK ID drop down.
3. Toggle the check box for each setting to be associated with your chosen LMK ID.
4. Click **Apply**.



5. Repeat this process for each LMK.

10 Migrating LMKs

10.1 Introduction

Thales payment HSMs have always provided a facility to migrate between LMKs, for example, to re-encrypt operational keys and other data from encryption under one (old) LMK to encryption under another (new) LMK. The need to do this is more important than in the past because:

- Card schemes are requesting that customers change their master keys every 2 years
- Adoption of Key Block LMKs, with their added security, requires a migration from Variant LMKs

This chapter outlines the migration process.

10.2 Multiple LMKs

By default, the payShield 10K is delivered with the ability to install one or two LMKs. If two LMKs are installed, one must be a Variant type and one must be a Key Block type.

Each LMK can be managed by its own team of security officers.

The multiple LMK facility can be used to provide separation between multiple clients, applications, or purposes serviced on the same HSM, and they also make the process of migrating LMKs easier.

10.3 Overview of the process

The LMK Migration process takes keys which are encrypted under an old LMK and re-encrypts them under a new LMK. Both the old and the new LMKs must be installed in the payShield 10K.

There are two types of LMK storage:

- LMK Live storage.
Transaction processing and other LMK functions can make use only of LMKs in Live storage.
- Key Change storage.

LMKs in Key Change storage cannot be used for any purpose other than as part of the LMK migration process. Where multiple LMKs are deployed, there is one Key Change storage “slot” for each LMK in the Main storage.

There are 2 ways of allocating old/new keys to Main/Key Change storage:

- The new LMK (which has not yet been deployed for live operation) is loaded into Live storage, and the old LMK (which is still being used for live processing) is loaded into Key Change storage using the LO console command.

It means that the payShield 10K being used for migration cannot be used to process transactions until the LMK migration process is completed and the new LMK comes into operational use, but it is then immediately ready to process transactions because the new LMK is already loaded in Live storage.

- The old LMK (still being used for live operation but about to be obsoleted) is left in Main Live, and the new LMK (which has not yet been deployed for live operation) is loaded into Key Change storage using the LN console command.

This option means that the payShield 10K can continue processing transactions using the current LMK at the same time as it is used for migrating keys to the new LMK. On the other hand, when the new LMK is ready to go live, the new LMK must be loaded into Live storage before any transactions can be processed.

At a high level, the steps to migrate an old LMK to a new LMK are as follows:

1. Create Smart Cards with components for the new LMK.
2. Load the new LMK (**from components cards**) into either LMK Live storage or LMK Key Change storage.

Either:

- leave the old LMK in LMK Live storage and load the new LMK (from component cards) into LMK Key Change storage
- or
- load the new LMK (**from component cards**) into LMK Live storage and load the old LMK (from components cards) into LMK Key Change storage in the same HSM.

3. Re-encrypt the operational keys from the old LMK to the new LMK and hold these in a pending new key database.
4. Re-encrypt PINs from the old LMK to the new LMK and hold these in a pending new PIN database.
5. Re-encrypt decimalization tables from the old LMK to the new LMK and hold these in a pending new decimalization table database.
6. If the new LMKs have been loaded into Key Change storage, re-load them into Live storage.
7. Make the pending key/PIN/decimalization table databases the live databases.

10.4 Generating new LMK component Smart Cards

LMKs are set up in the payShield 10K by loading a number (typically 3) of components which are then combined within the HSM to form the LMK. (The formed LMK is never available outside of the HSM.) The LMK components are loaded from LMK Smart Cards.

The first stage, therefore, is to create Smart Cards which have the components for the new LMK. These components have completely random values, and are created on any payShield 10K.

Each component must be held by a different security officer, and access to the component cards must be securely controlled (e.g., by storing the card securely and requiring security officers to check the cards out and in).

All component cards are required to load (or form) an LMK, and so loss of any card or absence of a card holder prevents the LMK from being loaded (or re-loaded at a later date, if necessary). Therefore at least one backup should be made of each component card.

Note that the terms “LMK card” and “LMK component card” are interchangeable. Only LMK components are ever written to cards - the whole LMK is never written to a card.

10.4.1 Types of LMK component cards

There are two types of LMK component cards:

- HSM LMK cards - using the card reader built into the HSM. This type of card is created and used by operators using a console and the HSM card reader.
- payShield Manager RLMK cards - created by operators using payShield Manager and the card reader attached to the remote management PC.

The principles are the same for both types of card, although the detail of the processes is different. The two types of card are incompatible, although either type of card can be created from the other.

10.5 Formatting LMK Smart Cards

10.5.1 HSM LMK Cards

Before they can be written to, Smart Cards must be formatted.

Cards which have been used previously and are no longer required can be re-formatted to enable the new components to be written to them.

Do not re-format the component cards for the old LMK that you are about to migrate from.

Each component holder should format their own card plus at least one backup per component.

HSM LMK Smart Cards are formatted using the FC console command.

10.5.2 payShield Manager LMK Cards

With payShield Manager, the LMK components are written to RLMK cards which are provided by Thales. RLMK cards do not require formatting.

10.6 Generating LMK Component Cards

10.6.1 HSM LMK Cards

Each component holder should now generate a component and write it to their Smart Card and backup card(s). This is done using the GK console command. Refer to the payShield 10K Console Guide for additional information.

Various warnings and errors may be reported during this process. These are easy to understand, and appropriate responses should be made.

10.6.2 payShield Manager RLMK Cards

LMK components for use with payShield Manager are written to RLMK cards using the Generate button in payShield Manager's **Operational > LMK Operations > Local Master Keys** tab.

These cards use a quorum (i.e., "m of n") approach to define how many of the cards must be used when loading an LMK. The operator provides the following information when generating the LMK:

- Number of LMK shares, i.e. "n" (Default: 2)
- Number of shares to rebuild, i.e. "m" (Default: 2)
- Key scheme (Variant or Key Block)
- Algorithm
- Status (Live or Test)

10.7 Creating Copies of LMK Component Cards

Because all component cards are needed when the LMK is loaded, copies of each LMK card should be made to allow for misplacement or for issuing to deputies.

10.7.1 Duplicating HSM LMK cards

- During LMK card generation
Multiple copies may be made at the time of generating the LMK card.
- Using a console command
It is possible at any time to copy an existing HSM LMK card using the DC console command.
Refer to the *payShield 10K Console Guide* for additional information.

10.7.2 Duplicating a payShield Manager RLMK card

A copy of an existing RLMK component card can be made using the Duplicate button in payShield Manager's **Operational > LMK Operations > Local Master Keys** tab.

10.8 Loading the new LMK

In the previous sections, we explained how to create a set of cards containing the components for the new LMK. Each component is "owned" by a different security officer, with no one security officer having access to more than one component. One holder of each of the required number of components must be present to allow the LMK to be loaded onto the payShield 10K using the component Smart Cards.

The new LMK now needs to be installed into either LMK Live storage or LMK Key Change storage depending on the approach being taken.

The new LMK can be loaded using a Console or payShield Manager.

10.8.1 Using the Console

10.8.1.1 Loading (or forming) the LMK

The LMK is loaded using either:

- the LK console command if the new LMK is to be loaded into LMK Live storage, or
- the LN console command if the new LMK is to be loaded into LMK Key Change storage.

The payShield 10K must be in the Secure state. In addition, if the LN console command is being used, then the HSM must be in the Authorized state. If multiple authorized states is enabled, the activity category is admin (with no sub-category), and the console interface should be selected.

The Smart Cards used must be HSM cards - not cards created for payShield Manager.

10.8.1.2 Checking the LMK

It is recommended that a check is made that the new LMK has been properly loaded.

This can be done using the A console command, to put the HSM into authorized state (followed by the C command to cancel the authorized state). The A command can be run in any HSM state. The operation of this command depends on whether multiple authorized activities has been enabled in the security settings (e.g., by using the CS console command).

Refer to the *payShield 10K Console Guide* for additional information.

10.8.2 Using payShield Manager

10.8.2.1 Installing the LMK

The new LMK is loaded using the Install button in the appropriate payShield Manager tab:

- **Operational > LMK Operations > Local Master Keys** where the new LMK is to be loaded into LMK Live storage, or
- **Operational > LMK Operations > Key Change Storage** where the new LMK is to be loaded into LMK Key Change storage.

The LMK ID will need to be specified.

10.8.2.2 Checking the LMK

The installed LMK can be checked by viewing the LMK list.

Navigate to either of the following:

- **Operational > LMK Operations > Local Master Keys**
- **Operational > LMK Operations > Key Change Storage**

10.9 Loading the old LMK

So far, you have created a set of cards containing the components for the new LMK, and used them to load into the HSM the “new” LMK that keys and data to be re-encrypted to.

To migrate keys from encryption under an old (current) LMK to encryption under the new LMK, we also need to have the old LMK loaded in the HSM. The old LMK can be left in LMK Lives storage or loaded into LMK Key Change Storage, depending on the approach being taken.

If the old LMK is to be loaded into Key Change Storage, this can be done using a Console or payShield Manager.

10.9.1 Using the Console

The old LMK is loaded into Key Change Storage using the LO console command.

Refer to the *payShield 10K Console Guide* for additional information.

The payShield 10K must be in Secure state. In addition, the HSM must be in Authorized state. If multiple authorized states are enabled, the activity category is *admin* (with no sub-category), and the console interface should be selected.

The use of the LO console command is the same as for the LK console command mentioned previously, except that no existing LMK needs to be erased and so you will not be prompted to confirm an erasure.

After loading the old LMK, the HSM should be returned to Online state by turning the physical keys.

10.9.2 Using payShield Manager

The old LMK is loaded using the Install button in payShield Manager's **Operational > LMK Operations > Key Change Storage** tab. This can only be done if there is an LMK with the same ID in the LMK table.

10.10 Migrating keys between Variant LMKs

We now have installed in the HSM both the old LMK that the operational keys are currently encrypted under and the new LMK that they need to be encrypted under for the future. We now need to take each existing operational key in the old key database (encrypted under the old LMK), re-encrypt it using the new LMK, and put it in a new key database.

In order to do this, an application needs to be set up at the host that:

- Takes each operational key (encrypted under the old LMK) from the old key database
- Sends the encrypted key to the HSM using the BW host command.
- Receives the BX response from the HSM containing the operational key encrypted under the new LMK.

- Puts the operational key encrypted under the new LMK into the new key database.

10.10.1 BW Host command

This section examines the BW host command as it is used to convert an operational key encrypted under an old LMK of the Variant type to encryption under a new LMK of the Variant type.

The BW host command automatically adapts its processing depending on where the old and new LMKs are stored:

- If the old LMK was loaded into Key Change storage (e.g., the LO console command was used), then keys and data are re-encrypted from encryption under the (old) LMK in Key Change storage to encryption under the (new) LMK in Live storage.
- If the new LMK was loaded into Key Change storage (e.g., the LN console command was used), then keys and data are re-encrypted from encryption under the (old) LMK in Live storage to encryption under the (new) LMK in Key Change storage.

The table below indicates the structure of the BW host command when it is used in this way.

Field	Length & Type	Notes
Message Header	m A	This field contains whatever the user wants. The length of the field is defined using the <i>CH</i> console command or <i>Configuration / Host Settings</i> in payShield Manager. It is subsequently returned unchanged in the response to the host.
Command Code	2 A	Must have the value 'BW'.

Field	Length & Type	Notes
Key Type code	2 H	Indicates the LMK under which the key is encrypted: '00' : LMK pair 04-05 (Key Type 000) '01' : LMK pair 06-07 (Key Type 001) '02' : LMK pair 14-15 (Key Type 002) '03' : LMK pair 16-17 (Key Type 003) '04' : LMK pair 18-19 (Key Type 004) '05' : LMK pair 20-21 (Key Type 005) '06' : LMK pair 22-23 (Key Type 006) '07' : LMK pair 24-25 (Key Type 007) '08' : LMK pair 26-27 (Key Type 008) '09' : LMK pair 28-29 (Key Type 009) '0A' : LMK pair 30-31 (Key Type 00A) '0B' : LMK pair 32-33 (Key Type 00B) '10' : Variant 1 of LMK pair 04-05 (Key Type 100) '42' : Variant 4 of LMK pair 14-15 (Key Type 402) 'FF' : Use this value where the key type is specified after the first ';' delimiter below. This allows key types other than those listed above to be specified.
Key length flag	1 N	'0' : for single-length key '1' : for double-length key '2' : for triple-length key.
Key	16/32 H or 1 A + 32/48 H	The operational key to be translated, encrypted under the old LMK.
Delimiter	1 A	Optional. Only present if 'FF' was supplied above for the Key Type code and the following field is present. Value ':'.
Key Type	3 H	Where 'FF' was entered for Key Type Code, this is the 3-digit key type code of the key being translated.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ':'.
Reserved	1 A	Optional. If present must be '0' (zero).
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0' (zero)).
Reserved	1 A	Optional. If present must be '0' (zero).
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	Where the user is using multiple LMKs on the same HSM, this allows the ID of the LMK being migrated to be selected. Minimum value = '00'; maximum value is defined by license. This field must be present if the above Delimiter is present. If the field is not present, then the default LMK will be used.

Field	Length & Type	Notes
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19'.
Message Trailer	n A	Optional. The contents of the trailer is as required by the user, and is returned unchanged in the response. Maximum length 32 characters.

10.10.2 BX Response to the Host

In response to the *BW* host command, the payShield 10K returns the following BX response to the host:

Field	Length & Type	Notes
Message Header	m A	This is a play-back of the header provided in the <i>BW</i> command.
Response Code	2 A	Has the value 'BX'.
Error code	2 N	Indicating the general outcome of the <i>BW</i> command: '00' : No error '04' : Invalid key type code '05' : Invalid key length flag '10' : Key parity error '44' : migration not allowed: key migration requested when the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y". '45' : Invalid key migration destination key type. '68' : Command disabled or any standard error code.
Key	16/32 H or 1 A + 32/48 H	The resulting key, re-encrypted under the new LMK.
End Message Delimiter	1 C	Present only if a message trailer is present. Value X'19'.
Message Trailer	n A	This is simply a play-back of any trailer included in the <i>BW</i> command.

10.11 Migrating keys from Variant to Key Block LMKs

Key Block LMKs provide additional security compared to Variant LMKs.

The BW host command already described for Variant LMK > Variant LMK migration can also be used for Variant LMK > Key Block LMK migration. When used for this purpose, the BW command and BX response are modified as indicated below.

Note that it is not possible to migrate from:

- Key Block LMKs to Variant LMKs.
- AES Key Block LMKs to TDES Key Block LMKs.

10.11.1 BW Host command

The table below indicates the structure of the BW host command when it is used to migrate from Variant-type LMKs to Key Block-type LMKs. Only the differences compared to Variant LMK > Variant LMK migration are described.

Field	Length & Type	Notes
Message Header	m A	(As for Variant LMK \Rightarrow Variant LMK)
Command Code	2 A	Must have the value 'BW'.
Key Type code	2 H	(As for Variant LMK \Rightarrow Variant LMK)
Key length flag	1 N	(As for Variant LMK \Rightarrow Variant LMK)
Key	16/32 H or 1 A + 32/48 H	(As for Variant LMK \Rightarrow Variant LMK)
Delimiter	1 A	(As for Variant LMK \Rightarrow Variant LMK)
Key Type	3 H	(As for Variant LMK \Rightarrow Variant LMK)
Delimiter	1 A	(As for Variant LMK \Rightarrow Variant LMK)
Reserved	1 A	(As for Variant LMK \Rightarrow Variant LMK)
Key Scheme (LMK)	1 A	(As for Variant LMK \Rightarrow Variant LMK)
Reserved	1 A	(As for Variant LMK \Rightarrow Variant LMK)
Delimiter	1 A	(As for Variant LMK \Rightarrow Variant LMK)
LMK Identifier	2 N	(As for Variant LMK \Rightarrow Variant LMK)
Delimiter	1 A	Must have value '#'
Key Usage	2 A	The required key usage for the key encrypted under the Key Block LMK. This information is included in the Key Block header and should be determined using the Key Usage Table. This field determines type of the operational key (e.g. RSA private key, BDK, ZEK), and enforces key separation.

Field	Length & Type	Notes
Mode of Use	1 A	The required mode of use for the key encrypted under the Key Block LMK. This information is included in the Key Block header, and should be determined using the Mode of Use Table. This field determines how the operational key can be used (e.g. encryption, decryption, MACing).
Key Version Number	2 N	A value from '00' to '99', for inclusion in the Key Block header. Determined by the user. '00' denotes that key versioning is not in use for this key.
Exportability	1A	The required exportability for the key encrypted under the Key Block LMK. This information is included in the Key Block header, and should be determined using the Exportability Table. This field determines how the operational key can be exported (e.g. no export allowed, may only be exported as a Key Block).
Number of Optional Blocks	2 N	A value from '00' to '08', identifying how many optional data blocks the user wants to add into the Key Block Header. Optional data blocks are used to identify parameters (such as key validity dates, key status, algorithm). For a value greater than 0, the following three fields must be repeated for each optional block.
Optional Block Identifier	2 A	Note that the value 'PB' may not be used.
Optional Block Length	2H	The length in bytes of the optional block (including the Identifier and Length). A value of X'04' indicates that the block contains only the identifier and length, and so the next field would not be present.
Optional Data Block	N A	The payload of the optional data block.
End Message Delimiter	1 C	(As for Variant LMK \Rightarrow Variant LMK)
Message Trailer	n A	(As for Variant LMK \Rightarrow Variant LMK)

10.11.2 BX Response to the Host

In response to the BW host command, the payShield 10K returns the following BX response to the host:

Field	Length & Type	Notes
Message Header	m A	(As for Variant LMK \Rightarrow Variant LMK)
Response Code	2 A	Has the value 'BX'. (As for Variant LMK Variant LMK)
Error code	2 N	(As for Variant LMK \Rightarrow Variant LMK)
Key	1 A + n A	The operational key, encrypted under the new Key Block LMK.
End Message Delimiter	1 C	(As for Variant LMK \Rightarrow Variant LMK)
Message Trailer	n A	(As for Variant LMK \Rightarrow Variant LMK)

10.12 Migrating keys between Key Block LMKs

Migration of operational keys between Key Block LMKs is supported in addition to the Variant LMK > Variant LMK and Variant LMK > Key Block LMK migrations already described. This section describes the BW host command when used for this purpose.

Note that it is not possible to migrate from:

- Key Block LMKs to Variant LMKs.
- AES Key Block LMKs to TDES Key Block LMKs.

10.12.1 BW Host command

The table below indicates the structure of the BW host command when it is used to migrate between Key Block-type LMKs.

Field	Length & Type	Notes
Message Header	m A	(As for Variant LMK \Rightarrow Key Block LMK)
Command Code	2 A	Must have the value 'BW'.
Key Type code	2 H	Must be set to 'FF'.
Key length flag	1 H	Must be set to 'F'.
Key	1 A + n A	The operational key to be translated, encrypted under the old Key Block LMK.

Field	Length & Type	Notes
Delimiter	1 A	Must have value ':'.
Key Type	3 H	Must be set to 'FFF'.
Delimiter	1 A	(As for Variant LMK ⇒ Key Block LMK)
Reserved	1 A	(As for Variant LMK ⇒ Key Block LMK)
Key Scheme (LMK)	1 A	(As for Variant LMK ⇒ Key Block LMK)
Reserved	1 A	(As for Variant LMK ⇒ Key Block LMK)
Delimiter	1 A	(As for Variant LMK ⇒ Key Block LMK)
LMK Identifier	2 N	(As for Variant LMK ⇒ Key Block LMK)
Delimiter	1 A	(As for Variant LMK ⇒ Key Block LMK)
Key Usage	2 A	(As for Variant LMK ⇒ Key Block LMK)
Mode of Use	1 A	(As for Variant LMK ⇒ Key Block LMK)
Key Version Number	2 N	(As for Variant LMK ⇒ Key Block LMK)
Exportability	1 A	(As for Variant LMK ⇒ Key Block LMK)
Number of Optional Blocks	2 N	(As for Variant LMK ⇒ Key Block LMK)
Optional Block Identifier	2 A	(As for Variant LMK ⇒ Key Block LMK)
Optional Block Length	2 H	(As for Variant LMK ⇒ Key Block LMK)
Optional Data Block	N A	(As for Variant LMK ⇒ Key Block LMK)
End Message Delimiter	1 C	(As for Variant LMK ⇒ Key Block LMK)
Message Trailer	n A	(As for Variant LMK ⇒ Key Block LMK)

10.12.2 BX Response to the Host

In response to the BW host command, the payShield 10K returns the following BX response to the host:

Field	Length & Type	Notes
Message Header	m A	(As for Variant LMK ⇒ Key Block LMK)
Response Code	2 A	Has the value 'BX'. (As for Variant LMK Key Block LMK)
Error code	2 N	(As for Variant LMK ⇒ Key Block LMK)

Field	Length & Type	Notes
Key	1 A + n A	(As for Variant LMK \Rightarrow Key Block LMK)
End Message Delimiter	1 C	(As for Variant LMK \Rightarrow Key Block LMK)
Message Trailer	n A	(As for Variant LMK \Rightarrow Key Block LMK)

10.13 Migrating keys from Key Block to Variant LMKs

This migration is not permitted because Variant LMKs are not as strong as key block LMKs.

10.14 Migrating keys for PCI HSM compliance

When it is required to make a payShield 10K compliant with the requirements of the PCI PTS HSM security standard, it may be necessary to move some keys from Variant key type 002 (LMK pair 14-15, Variant 0) to other key types.

Although this can be done as a separate operation, it can be achieved at the same time as migrating between LMKs using the BW host command by entering 'F2' as the Key Type Code, and the desired destination key type in the Key Type field.

10.15 Re-encrypting PINs

Where PINs have been stored encrypted under the old LMK (in LMK Live storage or LMK Key Change storage) these will need to be re-encrypted using the new LMK (in LMK Key Change storage or LMK Live storage). This can be done by using the BG host command.

A host application will take each PIN from the old PIN database, re-encrypt it using the BG host command, and store the re-encrypted PIN into the new PIN database.

10.15.1 BG Host Command

The structure of the BG host command is as follows:

Field	Length & Type	Notes
Message Header	m A	This field contains whatever the user wants. The length of the field is defined using the <i>CH</i> console command or <i>Configuration / Host Settings</i> in payShield Manager. It is subsequently returned unchanged in the response to the host.
Command Code	2 A	Has the value 'BG'.
Account Number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN	L ₁ N Or L ₁ H	The PIN encrypted under the old LMK, where L ₁ is the old encrypted PIN length. L ₁ N applies where PIN encryption algorithm A (Visa method) is specified in the security settings, and L ₁ H applies where PIN encryption algorithm B (Racal method) is specified.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	Where the user is using multiple LMKs on the same HSM, this allows the required LMK to be selected. Minimum value = '00'; maximum value is defined by license. This field must be present if the above Delimiter (%) is present. If the field is not present, then the default LMK will be used.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19'.
Message Trailer	n A	Optional. The contents of the trailer is as required by the user, and is returned unchanged in the response. Maximum length 32 characters.

10.15.2 BH Response

The HSM returns the following BH response to the host's BG command:

Field	Length & Type	Notes
Message Header	m A	This is a play-back of the header provided in the <i>BG</i> command.
Response Code	2 A	Has the value 'BH'.

Field	Length & Type	Notes
Error code	2 N	Indicating the general outcome of the <i>BG</i> command: '00' : No error '68' : Command disabled or any standard error code.
PIN	L ₂ N Or L ₂ H	The PIN encrypted under the new LMK, where L ₂ is the new encrypted PIN length. L ₂ N applies where PIN encryption algorithm A (Visa method) is specified in the security settings, and L ₂ H applies where PIN encryption algorithm B (Racal method) is specified.
End Message Delimiter	1 C	Present only if a message trailer is present. Value X'19'.
Message Trailer	n A	This is simply a play-back of any trailer included in the <i>BW</i> command.

10.16 Re-encrypting decimalization tables

For security, it is recommended that decimalization tables be encrypted. They are encrypted under the LMK, and so will need to be re-encrypted when migrating to a new LMK.

This is achieved by having a host application which takes each decimalization table from the old decimalization table database and re-encrypting it under the new LMK using the *LO* host command (not to be confused with the *LO* console command discussed earlier!) and then storing it in a new decimalization table database. The new LMK can be in either Key Change storage or Live storage.

The structure of the *LO* host command is as follows:

Field	Length & Type	Notes
Message Header	m A	This field contains whatever the user wants. The length of the field is defined using the <i>CH</i> console command or <i>Configuration / Host Settings</i> in payShield Manager. It is subsequently returned unchanged in the response to the host.
Command Code	2 A	Most have the value 'LO'.
Decimalization Table (old LMK)	16 H	A decimalization table encrypted under the old LMK.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.

Field	Length & Type	Notes
LMK Identifier	2 N	Where the user is using multiple LMKs on the same HSM, this allows the required LMK to be selected. Minimum value = '00'; maximum value is defined by license. This field must be present if the above Delimiter (%) is present. If the field is not present, then the default LMK will be used.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19'.
Message Trailer	n A	Optional. The contents of the trailer is as required by the user, and is returned unchanged in the response. Maximum length 32 characters.

The payShield 10K returns the following LP response to the host:

Field	Length & Type	Notes
Message Header	m A	This is a play-back of the header provided in the LO command.
Response Code	2 A	Has the value 'LP'.
Error code	2 N	Indicating the general outcome of the LO command: '00' : No error '68' : Command disabled or any standard error code
Decimalization Table (new LMK)	16 H	The decimalization table encrypted under the new LMK.
End Message Delimiter	1 C	Present only if a message trailer is present. Value X'19'.
Message Trailer	n A	This is simply a play-back of any trailer included in the BW command.

10.17 Switching to the new LMK

Following the activities described above, the system is now in the following state:

- Old databases of operational keys, PINs, and decimalization tables, encrypted under the old LMK, are still being used for production.
- New databases of operational keys, PINs, and decimalization tables, encrypted under the new LMK are pending but not yet being used for production.

- One or more HSMs may have been taken out of service in order to re-encrypt the operational keys, PINs, and decimalization tables.
- These would be HSMs that have the old (current) LMK (which is still being used on other HSMs for production) loaded in Key Change Storage (e.g. by using the LO console command), and the new LMK (not yet in use for production work) in their Live storage.
- In this case there are other HSMs with the old LMK in their Live storage, which are doing production work using keys, PINs, and decimalization tables in the old versions of the databases.
- Production host applications are still using the old databases of operational keys, PINs, and decimalization tables.

In order to start using the new LMK, the following changes must be synchronized:

- Host production applications start using the new databases of operational keys, PINs, and decimalization tables.
- If the re-encryption of keys was done on an HSM with the new LMK in Live storage, then this HSM is immediately ready to start processing transactions using the new LMK. However, the new LMK needs to be loaded into LMK Live storage on those HSMs that were processing transactions using the old LMK.
- On the other hand, if the re-encryption of keys was done on an HSM with the new LMK in Key Change storage, then the new LMK needs to be loaded into LMK Live storage on all the HSMs in the system.

A total interruption of service can be avoided by a gradual switchover from the old LMK to the new - but in this case the host applications must know whether an HSM is using the old or new LMK and must retrieve the key or data from the appropriate database.

The use of the Multiple LMK feature of the payShield 10K offers additional options, and is described in the following section.

10.18 Taking advantage of Multiple LMKs

The payShield 10K supports multiple concurrent LMKs. The base product allows the user to implement one Variant-type LMK and one Key Block-type LMK, and optional licenses are available to provide up to 20 LMKs in any combination of types.

The multiple LMK feature offers a number of valuable benefits, and provides additional flexibility to simplify the process.

Here is an example of how the multiple LMK feature can be used where the old (still Live) LMK is in LMK Key Change storage and the new (future) LMK is in LMK Live storage:

- Let us take as a starting point a production system which has the live LMK at LMK 00.
- LMK 00 is set up as the default LMK. This means that it is the LMK that is used by default in host commands where no LMK is identified: this provides backwards compatibility to applications developed before the multiple LMK facility was introduced.
- The future, new LMK is loaded as LMK 01 in LMK Live storage (see Loading the new LMK).
- The existing, "old" LMK, which is LMK 00 and is being used for production, is also loaded into LMK Key Change Storage for LMK 01 (see Loading the old LMK.)

- The BW, BG, and LO host commands can now be used to re-encrypt operational keys, PINs, and decimalization tables from the old LMK (which is in Key Change Storage, and also still in LMK 00 and therefore available for production) to the new LMK, which is loaded as LMK 01. This is achieved by setting the LMK Identifier in the host commands to a value of "01". This must be preceded by a delimiter of "%".
- When all of the operational keys, PINs, and decimalization tables have been re-encrypted under the new LMK, the host application can start using the new key database when one of the following actions have been taken:
 - The new LMK is re-loaded on the payShield 10K as LMK 00.
Or
 - Host commands sent to the payShield 10K are amended to use LMK 01 by either:
 - Specifying the value "01" for the LMK identifier in host commands
Or
 - Directing commands to the relevant TCP port.

The benefit of this approach is that there is no need to take one or more HSMs out of productive use while the LMK migration is being performed, and therefore the key migration using the BW host command can be spread over as many HSMs as desired.

Multiple LMKs could also be used to avoid a "big bang" switchover from old to new LMKs: with the old LMK in one Live storage slot and the new LMK in a second Live storage slot, individual elements of the system can be moved to the new LMK one at a time.

10.19 Clean-up after migration to a new LMK

10.19.1 Deleting the Old LMK from Key Change Storage

The LMK in Key Change Storage should be deleted once it is no longer needed. There are multiple ways of doing this.

10.19.1.1 Using the console

The LMK can be deleted from Key Change Storage using the DO console command. The payShield 10K must be in Secure state.

10.19.1.2 Using payShield Manager

The LMK is deleted using the  button displayed against the LMK in payShield Manager's **Operational > LMK Operations > Key Change Storage** tab. This can only be done in Secure state.

10.19.1.3 Using a Host Command

The BS host command allows the host to erase the LMK in Key Change Storage. The structure of the command is given in the following table:

Field	Length & Type	Notes
Message Header	m A	This field contains whatever the user wants. The length of the field is defined using the <i>CH</i> console command or <i>Configuration / Host Settings</i> in payShield Manager. It is subsequently returned unchanged in the response to the host.
Command Code	2 A	Must have the value 'BS'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	Where the user is using multiple LMKs on the same HSM, this allows the host to select which Old LMK is to be deleted. Minimum value = '00'; maximum value is defined by license. This field must be present if the above Delimiter (%) is present. If the field is not present, then the default LMK will be used.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19'.
Message Trailer	n A	Optional. The contents of the trailer is as required by the user, and is returned unchanged in the response. Maximum length 32 characters.

The BT response has the following structure:

Field	Length & Type	Notes
Message Header	m A	This is a play-back of the header provided in the <i>BS</i> command.
Response Code	2 A	Has the value 'BT'.
Error code	2 N	Indicating the general outcome of the <i>BS</i> command: '00' : No error '68' : Command disabled or any standard error code
End Message Delimiter	1 C	Present only if a message trailer is present. Value X'19'.

Field	Length & Type	Notes
Message Trailer	n A	This is simply a play-back of any trailer included in the BW command.

11 TLS Certificate Management

11.1 Introduction

payShield 10K supports the use of TLS to secure traffic to applications using the host port and for payShield Manager.

This chapter provides a general description of TLS and details on configuring and managing the TLS keys and certificates for the host port and for payShield Manager.

11.2 General Description

To meet this emerging requirement for secure host communications, payShield 10K supports the use of TLS to secure traffic between host applications and HSM. TLS 1.2 is the preferred protocol.

Note: This capability is available for Ethernet connections: it is not appropriate for FICON interfaces.

11.2.1 What TLS Provides

TLS provides a high level of security for sessions between an Ethernet connected client application and server application with no prior knowledge of each other and without any prior exchange of encryption keys. A mutually trusted third party (the CA, or Certificate Authority) is used to certify that the client and server are the owners of their respective private and public key pairs used in establishing the communication session.

This trusted environment provides:

- Authentication - the server may authenticate itself to the client (typically a browser), or the client and server may mutually authenticate themselves to each other.
- Privacy - the communications traffic is encrypted.
- Integrity assurance - using hash and signature algorithms.

Note that TLS works between applications. This means that both communicating applications must be TLS-enabled, rather than the host and client devices. Proxies can be implemented to allow non-TLS-enabled applications to be used over a TLS-protected link; here, the authentication is from/to the proxy rather than the application.

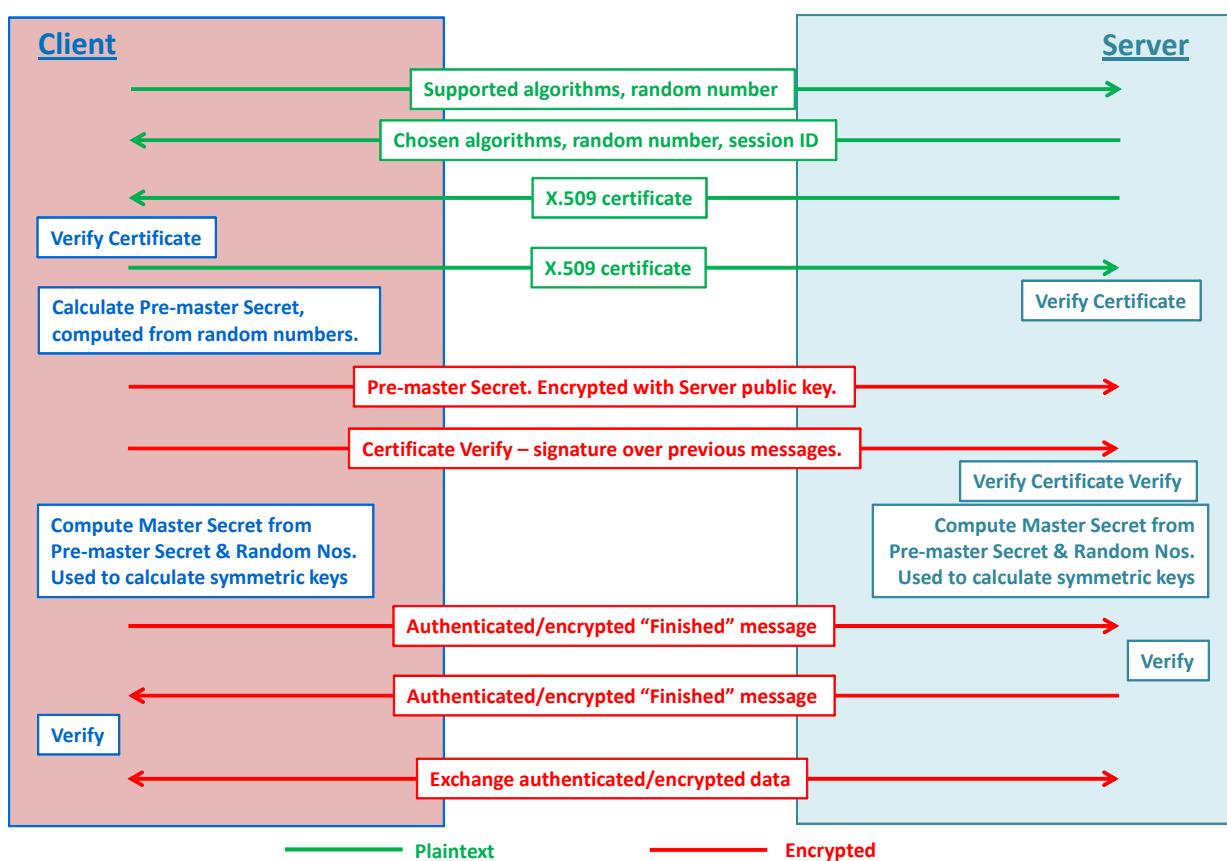
11.2.2 How TLS Works

The process for setting up a TLS session can be summarized as follows:

1. Both the client and server have their own private (secret) and public keys.
2. The public keys are certified by Certificate Authorities (CAs).
3. The public key certificates can include multiple, chained CA hierarchies - e.g., the public key can be certified by one CA (e.g., operated by the organization owning the key), and this CA certificate is then certified by a higher-level CA (e.g., a third-party CA trusted by both the key owner and the key user).

4. The client and server can use different CAs.
5. The client and server applications negotiate which cipher suite they will use and exchange some information (but not keys) that will be needed to establish the session. The cipher suite defines the algorithms and key lengths that will be used to establish and protect the session.
6. The client and server applications exchange certificates (including their public keys).
7. The client and server validate each other's certificate and extract the public key. The validation may be performed by contacting the CA online or by using previously stored CA materials.
8. The client application sends an encrypted "Pre-master" secret to the Server application.
9. Server and client applications both independently compute a Master secret from the Pre-master secret and use this to calculate the symmetric keys to be used to protect the exchanged data. The keys therefore do not need to be exchanged.
10. Following a successful client-server handshake, the application data is exchanged in records, with the data encrypted using the independently computed keys, and MAC'd using the hashing algorithm in the agreed cipher suite.

The following diagram illustrates this, with some additional detail:



11.3 TLS for Host Connections on payShield 10K

11.3.1 TLS Support for Host Connections

payShield 10K provides support for client-server TLS for applications connecting to payShield 10K using the host port. Further details are provided in this section, but some key points are:

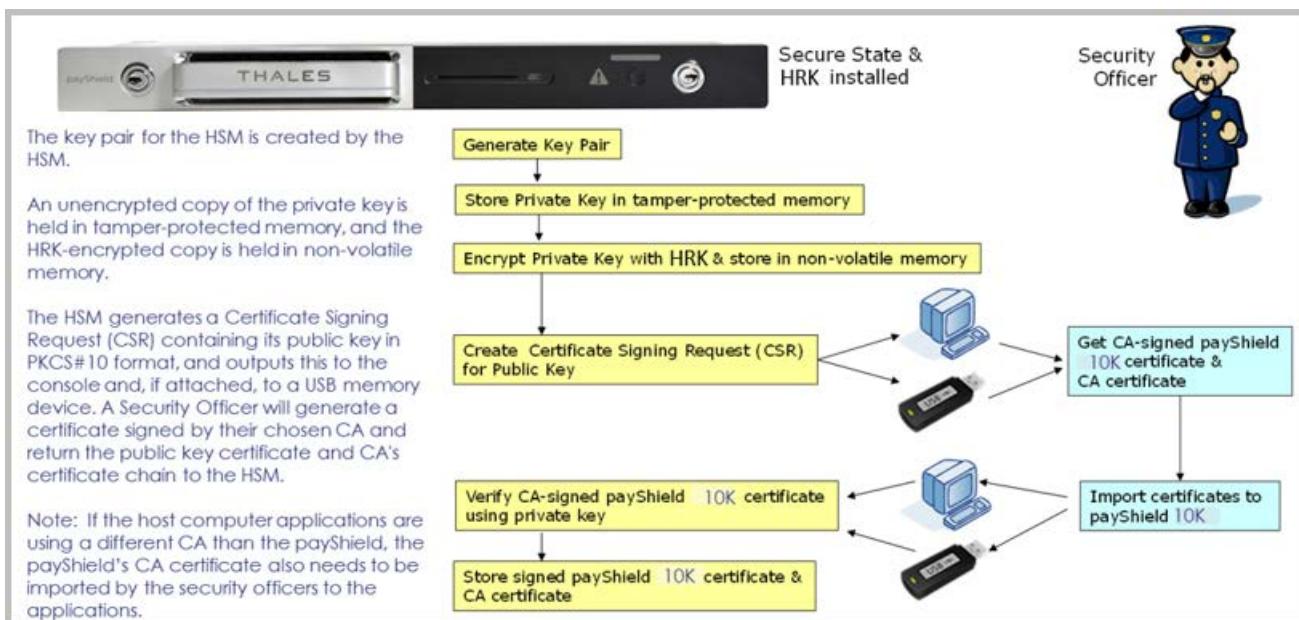
- payShield Manager provides the facilities to manage the Host TLS, client, Intermediate CA and CA certificates required to establish TLS sessions. Console commands are also provided.
- payShield 10K supports TLS v1.2.
- payShield 10K can simultaneously support TLS and non-secured (TCP or UDP) traffic. It is possible to disable all TLS or non-secured traffic.
- The client certificates must be installed on payShield 10K providing a "Whitelist" of applications that are entitled to use the HSM.

11.3.2 Host TLS Certificates

The Host TLS key pair for the HSM is created by the HSM.

An unencrypted copy of the private key is held in tamper-protected memory, and the HSM Recovery Key (HRK)-encrypted copy is held in non-volatile memory.

The HSM generates a Certificate Signing Request (CSR) containing its public key in PKCS#10 format, and outputs this to the payShield Manager Virtual Console (or if using the Console, the Console display and optionally to a USB memory device). A security officer will generate a certificate signed by their chosen CA and return the public key certificate and CA's certificate chain to the HSM.



If the clients are using a different CA to the HSM, the HSM's CA certificate also needs to be imported by the security officers to the client's applications.

Intermediate CA certificates can be included to a maximum certificate chain depth of 6. These must include the X509 v3 optional extensions of Subject Key Identifier and Authority Key Identifier. The signed Host TLS (server) certificate must include the Authority Key Identifier extension.

11.3.3 Client Certificates

Each application that wishes to establish a secure communications session using TLS needs to provide to the payShield 10K a public key in the form of a certificate signed by a CA (or by a hierarchy of CAs). The way that this certificate is obtained depends on the standard procedures of the organization and its selected CA mechanism.

The application certificates and their associated CA chain certificates are imported by the security officer into the HSM from a file using payShield Manager (or if using the console, a USB memory device).

The set of client endpoint certificates forms an effective "Whitelist" of applications that are entitled to use the HSM through TLS. This is used by the payShield 10K to mitigate against "man-in-the-middle" attacks.

Intermediate CA certificates can be included to a maximum certificate chain depth of 6. These must include the X509 v3 optional extensions of Subject Key Identifier and Authority Key Identifier. The signed application (client) certificate must include the Authority Key Identifier extension.

11.3.4 Managing Host TLS Keys and Certificates

11.3.4.1 Overview

The following sections discuss the procedure used for configuring TLS for the Host Ports on payShield 10K.

With the release of 2.1a software, an additional inactive key store is provided to allow the Host TLS key, and all the required certificates to be installed without affecting live operation. To select the key and certificates in the inactive key store for use requires payShield 10K to be placed offline in secure state to configure the store as the active store.

The new facility provides additional flexibility to the configuration process. The new facility is backward compatible so the functionality previously provided can be used using Secure State. When upgrading or downgrading from/to a release supporting this functionality, the existing TLS store is maintained.

When using the new facility, the recommended steps for initially setting up TLS are as follows, noting that all steps can be undertaken in online state except the last step:

1. Use either Key Store A or B to generate new Host TLS Key Pair, exporting the self-signed Host TLS Public Key Certificate.
2. Arrange for the self-signed Host TLS Public Key Certificate to be signed by the relevant CA (or Intermediate CA).
3. Import the self-signed root CA and Intermediate CA certificates.
4. Import the Host TLS Certificate from Step 2.
5. Import the Client CA Certificates.
6. Enable TLS, selecting the relevant Key Store (requires Secure State).

To change the Host TLS Key Pair and the Client Certificates the recommended steps, noting that all steps can be undertaken in online state except the last step:

1. Use the inactive Key Store to delete any existing keys and certificates.
2. Generate new Host TLS Key Pair, exporting the self-signed Host TLS Public Key Certificate.
3. Arrange for the self-signed Host TLS Public Key Certificate to be signed by the relevant CA (or Intermediate CA).
4. Import the Host TLS Certificate from Step 3.
5. Import the Client CA Certificates.
6. Select the relevant Key Store (requires Secure State).

A facility is provided to allow selected Host TLS Key and certificates to be copied from the active to the inactive key store for added flexibility. This allows for example:

- The Host TLS key pair and certificates to remain the same and the client certificates changed.
- The client certificates to be changed while the Host TLS Key Pair remains the same.

Further details are given in the following sections. Details of the user interfaces are given in the Installation and User Manual (for payShield Manager) and also the Console Guide. Information on the security aspects is given in the Security Manual.

11.3.4.2 Host TLS Key Stores

For Host TLS, two key stores are now provided – A and B. Each Key Store contains the following:

- Host TLS private Key
 - The private key is stored in the Key Store used for the Management Port in tamper-protected memory and (in HKR-encrypted form) in non-volatile memory.
- Host TLS Public Key Certificate
- Client TLS Public Key Certificates
- Self-Signed Root CA Certificate(s)
 - This can be common for the Host and Client, or separate.
- Intermediate Public Key Certificates (if required)
 - A hierarchy of 6 maximum is supported.
- A maximum of 64 certificates per key store is supported.
 - Note the certificates stored in the Management Key Store are managed separately.

Please note:

- Before a key store can be used to store certificates, it must contain a Host TLS Private Key.
- Only one Host TLS Private Key can be stored in each Key Store at a time.
- If TLS is disabled, then both Key Stores A and B are inactive and can be managed in Online State.
- When importing certificates, the certificates higher in the chain of trust must be imported first so the imported certificate can be validated. For example, The Self Signed Root CA certificate must be imported before the Intermediate Public Key Certificate.

11.3.4.3 Using payShield Manager

payShield Manager is used to Manage Host TLS Key Store A and B as follows. Ensure the correct key store is selected i.e., Host TLS instead of Management TLS. A pre-requisite is the system time must be set to 24-hour UTC format:

Generate a new Host TLS Key Pair

Use the Virtual Console and the ‘SG’ Console Command

- This process generates the Host TLS key pair.
- The private key is stored in the selected Key Store in tamper-protected memory and (in HRK-encrypted form) in non-volatile memory.
- The Self-Signed Host TLS Public Key certificate (Certificate Request) is output to the Virtual Console display and can be copied to a file for submission to the CA

Import Certificates

Use the TLS Certificate Tab from the Host Settings option from the Configuration Menu:

- Certificates are imported into the selected Key Store from a file stored on the payShield Manager workstation.

The following certificates are required to be imported:

- Self-Signed root CA for both the Host TLS Certificate and the Client Certificates (if different).
- Where a chained CA hierarchy is being used, certificates for each intermediate CA signed by the next CA up in the hierarchy.
- The Host TLS Public Key Certificate.
- All client certificates.

The certificates MUST be imported in the correct order in the hierarchy to allow them to be verified as each certificate is imported.

Multiple Certificates can be included in the file, but as noted above the certificates must be in the correct order to allow the Chain of Trust to be verified (e.g., the Intermediate CA Public Key Certificate must be earlier in the file than the Client Certificate).

The File must have extension “.crt”.

The certificates must include the X509 v3 optional extensions of Subject Key Identifier and Authority Key Identifier.

The signed application (client) certificate must include the Authority Key Identifier extension.

The certificates must be X509 PEM encoded.

- The option to copy the Host TLS Private Key and the Certificates from Key Store A to Key Store B (or vice versa) is also provided.

It is only possible to copy to the active Key Store in Secure State.

For the copy operation to be carried out:

- A Host TLS private key must be present in the source Key Store.
- The Host TLS private key must either be selected to be copied or the destination Key Store must already contain a Host TLS private key.
- If the Host TLS private key is selected for the copy operation, the Host TLS certificate and chain of trust (i.e., appropriate root CA public key certificate together with the intermediate CA certificates).

Export Chain of Trust

Use the Virtual Console and the '**SE**' Console Command.

- The Chain of Trust is output to the Virtual Console Display and is used to import into the Client applications.
- Note the chain of trust is also shown in the payShield Manager TLS Certificate Tab selected from the Host Settings option in the Configuration Menu:

Delete Installed Certificates

Use the Virtual Console and the '**SD**' Console Command

- The installed Host TLS Private Key and certificates are shown in numbered order on the Virtual Console Display.
- The item(s) to delete can then be selected.

11.3.4.4 Using the Console

The local Console is used to Manage TLS Key Store A and B as follows:

Generate a new Host TLS Key Pair

Use the 'SG' Console Command

- This process generates the Host TLS key pair.
- The private key is stored in the selected Key Store in tamper-protected memory and (in HRK-encrypted form) in non-volatile memory.
- The Self-Signed Host TLS Public Key certificate (Certificate Request) is output to the Console display and optionally to a file on a USB memory device installed in the USB-A socket on the payShield 10K rear panel.

Import Certificates

Use the 'SI' Console Command

- Certificates are imported into the selected Key Store from a file the USB-A socket on the payShield 10K rear panel.

- The certificates MUST be imported in the correct order in the hierarchy to allow them to be verified as each certificate is imported.
 - Multiple Certificates can be included in the file, but as noted above the certificates must be in the correct order to allow the Chain of Trust to be verified (e.g., the Intermediate CA Public Key Certificate must be earlier in the file than the Client Certificate).
 - The File must have extension ".crt".
 - The certificates must include the X509 v3 optional extensions of Subject Key Identifier and Authority Key Identifier.
 - The signed application (client) certificate must include the Authority Key Identifier extension.
 - The certificates must be X509 PEM encoded.
- The option to copy the Host TLS Private Key and the Certificates from the Active Key Store to the inactive Key Store is also provided. This operation can be carried out in Online State.
 - It is only possible to copy from the active Key Store to the inactive Key Store in Online State.
 - For the copy operation to be carried out:
A Host TLS private key must be present in the source Key Store.
The Host TLS private key must either be selected to be copied or the destination Key Store must already contain a Host TLS private key.
If the Host TLS private key is selected for the copy operation, the Host TLS certificate and chain of trust (i.e., appropriate root CA public key certificate together with the intermediate CA certificates).

Export Chain of Trust

Use the 'SE' Console Command

- The Chain of Trust is shown on the Console Display and can be saved to a file on a USB memory device. This is used to import into the Client applications.

View Installed Certificates

Use the 'SV' Console Command

- The installed certificates in the selected Key Store are shown on the Console Display.

Delete Installed Certificates

Use the 'SD' Console Command

- The installed Host TLS Private Key and certificates are shown in numbered order on the Console Display.
- The item(s) to delete are then selected.

11.3.4.5 Use Cases

The following use cases provide examples of how the inactive Key Store can be used to perform some of the most common operations.

Please note:

- These are examples using payShield Manager to illustrate the process only.
- The same procedure can be used when using the local Console using the equivalent commands. The 'SI' Console Command is used to import certificates in place of the payShield Manager tab referenced below.

Use Case	Procedure
Configure Host TLS for the first time	<p>Use inactive Key Store A in Online State:</p> <ul style="list-style-type: none"> • Virtual Console SG - Generate Host TLS Key Pair and Self-Signed Certificate <ul style="list-style-type: none"> – Host TLS Self-Signed Certificate signed by CA or Intermediate CA • Configuration Menu / Host Settings / TLS Certificate Tab - Install CA Root Certificate, Intermediate Certificates (if required) and Host TLS Certificate in HSM • Configuration Menu / Host Settings / TLS Certificate Tab - Install Client Certificates, Intermediate Certificates (if required) and CA Root Certificate (if different from CA Root certificate used for Host TLS certificate) in HSM. <p>Select Secure State and then:</p> <ul style="list-style-type: none"> • Configuration Menu / Host Settings / TLS Certificate Tab – enable TLS for host communications selecting Key Store A as the active store.
Renew Host TLS private key Only	<p>Use inactive Key Store in Online State:</p> <ul style="list-style-type: none"> • Virtual Console SD - Delete Host TLS Key, Host TLS Certificate and remaining certificates from the inactive Key Store as required. • Virtual Console SG - Generate new HOST TLS Key Pair and Host TLS Self-Signed Certificate in the Inactive Key Store. <ul style="list-style-type: none"> – Host TLS Self-Signed Certificate signed by CA or Intermediate CA • Configuration Menu / Host Settings / TLS Certificate Tab - Host TLS Certificate installed in Inactive Key Store • Configuration Menu / Host Settings / TLS Certificate Tab - Copy all certificates from Active Key Store to Inactive Key Store except the Host TLS Certificate (and the Host TLS private key). <p>Select Secure State:</p> <ul style="list-style-type: none"> • Configuration Menu / Host Settings – Change the status of the inactive Key Store to active.

Use Case	Procedure
Renew Client TLS Certificate Only	<p>Use Inactive Key Store in Online State:</p> <ul style="list-style-type: none"> • Virtual Console SD - Delete Host TLS Key and certificates from the inactive Key Store as required. • Configuration Menu / Host Settings / TLS Certificate Tab - Copy Host TLS private key, and all certificates from the Active Key Store to Inactive Key Store. • Configuration Menu / Host Settings / TLS Certificate Tab - Install new Client TLS Certificates (existing Client TLS Certificates can be kept allowing the client to rollover to use the new certificate later as required). <p>Select Secure State:</p> <ul style="list-style-type: none"> • Configuration Menu / Host Settings / TLS Certificate Tab Settings – Change the status of the inactive Key Store to active. <p>Once the clients have rolled over to use the new Client certificates, if the old Client certificate is required to be deleted:</p> <p>Select Secure State:</p> <ul style="list-style-type: none"> • Virtual Console SD - Delete old client certificates from the Active Key Store.

11.3.5 TLS for Host Connections - General Information

11.3.5.1 Supported Cipher Suites

Refer to the payShield 10K Security Manual.

11.3.5.2 Cipher Suite Negotiation

When negotiating Cipher Suites, the HSM's preferences will take precedence over the client's preferences.

Ephemeral key cipher suites are preferred by the payShield 10K. When selected, every new handshake will require new ephemeral keys to be generated; this provides perfect forward secrecy such that if an attacker should ever break the cryptography being used for a connection, then this will be of no use to the attacker in a subsequent connection.

When performing a renegotiation of an existing connection, the payShield 10K will always force a new session to be negotiated; this protects against a known renegotiation vulnerability.

Connections will not use data compression, protecting against the CRIME vulnerability.

11.3.5.3 Out-of-Date Certificates

If an attempt to establish a Secure Host Communications session is made using an out-of-date (i.e., expired or not yet valid) certificate, the connection fails. As a result, it is important for users to have suitable processes in place to manage certificate introduction and expiry.

As an option, users can audit attempts to use out-of-date certificates.

Users can choose to record, in the payShield 10K's Audit Log, any attempts made to establish a Host TLS session using an out-of-date certificate. This option is enabled/disabled in the audit options configuration in payShield Manager or the Console.

11.3.5.4 Performance Considerations

For payShield 10K, there is no noticeable difference in performance when implementing Secure Host Communications.

11.3.5.5 Security Considerations

TLS can only provide a secure environment when implemented correctly. When implementing TLS on the payShield 10K, the guidance in the latest version of PCI's Data Security Standards (DSS) requirements should be followed.

11.3.5.6 Port Setting

A well-known port must be specified for TLS - the default is 2500. This is analogous to the well-known port for unsecured host traffic, and can be used in the same way to identify the LMK required for the host command, i.e.:

- 2500 = default LMK
- 2501 = LMK 0
- 2502 = LMK 1
- etc.

The number of connections/threads for each port can also be specified. If a value of 5 was configured and both Ethernet ports were enabled, a total of 10 connections/threads would be available. These connections/threads are shared between secured and non-secured traffic.

These settings are configured in the payShield Manager Configuration Menu / Host Settings / TLS Certificate Tab or using the 'CH' Console Command.

11.3.5.7 OpenSSL Configuration File

Where OpenSSL is being used to provide TLS support on the client system, the configuration file must contain the following:

```
[ v3_client ]  
  
basicConstraints      = CA:FALSE  
#extendedKeyUsage    = clientAuth  
keyUsage              = keyAgreement, digitalSignature  
authorityKeyIdentifier = keyid,issuer
```

```
[ v3_server ]  
  
basicConstraints      = CA:FALSE  
extendedKeyUsage     = serverAuth  
keyUsage              = keyAgreement, keyEncipherment,  
digitalSignature, nonRepudiation  
authorityKeyIdentifier = keyid,issuer  
  
[ v3_ca ]  
  
basicConstraints      = CA:true  
subjectKeyIdentifier  = hash  
authorityKeyIdentifier = keyid,issuer
```

11.3.5.8 Working with IBM z/OS Mainframes

Users who have payShield 10K working with IBM z/OS host systems should make use of the AT-f feature in z/OS. Contact Thales Support (<https://supportportal.thalesgroup.com/csm>) for assistance.

Relevant information is also available on the IBM website: <https://www.ibm.com/docs/en/zos/3.1.0>.

11.3.5.9 FICON Interface

Please note that TLS is not appropriate for FICON interfaces.

11.4 TLS for payShield Manager

11.4.1 Overview

payShield Manager uses the payShield 10K Management Port for secure communications. The connection between the web browser and payShield 10K is protected using the TLS protocol.

For the most secure management operations, sensitive data is further protected using keys protected by the HSM and the payShield Manager smart card. These keys are never exposed outside of either device.

The payShield Manager TLS keys and certificates are generated automatically as part of the commissioning process using the CTA CA key. Once commissioning has completed, these can be managed using either payShield Manager or the Console as follows:

- Using the Configuration Menu / Management Settings / TLS Certificate Tab in payShield Manager
- Using the Console Commands SG, SI, SE, SV and SD.

11.4.2 Managing payShield Manager TLS Keys and Certificates

11.4.2.1 Overview

The following sections discuss the procedure used for configuring TLS for payShield Manager.

The process is similar to that used to manage the Host TLS certificates given in the previous sections with several important differences:

- For the payShield Manager TLS, only one Key Store for payShield Manager Keys and Certificates is provided.
- To import certificates, the payShield Manager menu option is given in the Configuration Menu / Host Settings / TLS Certificate Tab
- For other functionality, the same Virtual Console or Console commands are used, selecting the “Management TLS” option at the first prompt.
- Management of the payShield Manager Keys and Certificates requires Secure State, except when viewing the certificates.

11.4.2.2 Management TLS Key Store

One Management TLS Key Store is used (which is separate from the Host TLS Key Stores) and this contains the following:

- Management TLS private Key
 - The private key is stored in the Key Store in tamper-protected memory and (in HRK-encrypted form) in non-volatile memory.
- Management TLS Public Key Certificate
- Self-Signed Root CA Certificate(s)
- Intermediate CA Public Key Certificates (if required)

11.4.2.3 Management TLS - Initial Configuration

The payShield Manager TLS keys and certificates are generated automatically as part of the commissioning process. The Management TLS private key is generated, and the public key is signed by the Customer Trust Authority (CTA) private key during this process. Once commissioning is complete, there are no additional steps required to configure TLS for payShield Manager and it is fully operational after commissioning has completed.

11.4.2.4 Changing the payShield Manager TLS Keys and Certificates

The payShield Manager TLS Key and certificate can be changed using payShield Manager. The public key can be signed by the Customer Trust Authority or by an external CA. The following process is used when in Secure State to undertake this process:

Generate a new payShield Manager TLS Key Pair

- Use the Virtual Console and the ‘SG’ Console Command
 - Select Management TLS
 - Select the CA required to sign the public key certificate – the options are either an external CA or the payShield 10K Customer Trust Authority (CTA).

This process generates the Management TLS key pair.

The private key is stored in the Key Store used for the Management Port in tamper-protected memory and (in HKR-encrypted form) in non-volatile memory.

If the certificate is to be signed by an external CA, the Self-Signed Management TLS Public Key certificate (Certificate Request) is output to the Virtual Console display and can be copied to a file for submission to the CA. The certificate is then imported as shown below (in [Import Management Certificates](#)).

If the certificate is to be signed by the CTA, the process completes, and the user is logged out. When logging in again, the new TLS keys are used and the private key and certificate can be viewed using the standard commands.

Import Management Certificates

When the payShield Manager TLS public key certificate is signed by an external CA, the certificate can be imported as follows:

- Use Import Certificate Button from the TLS Certificate Tab from the Management Settings option from the Configuration Menu.

Certificates are imported into the Management TLS Key Store from one file stored on the payShield Manager workstation.

The following certificates are required to be included in the file:

Self-Signed root CA for the Management TLS Certificate.

Where a chained CA hierarchy is being used, certificates for each intermediate CA signed by the next CA up in the hierarchy.

- The Management TLS Public Key Certificate.
 - The certificates all MUST be stored in one file and in the correct order in the file hierarchy to allow them to be verified as each certificate is imported.
 - The File must have extension ".crt".
 - The certificates must include the X509 v3 optional extensions of Subject Key Identifier and Authority Key Identifier.

- The signed application (client) certificate must include the Authority Key Identifier extension.
- The certificates must be X509 PEM encoded.
- If the process completes successfully an "Operation Successfully Completed" message is displayed and the user is logged out. When logging in again, the new TLS keys are used, and the private key and certificate can be viewed using the standard commands.
- If the process does not complete, the existing keys and certificates can continue to be used.

The local Console can be used in a similar way to change the keys and certificates if required, noting:

- The 'SI' (import Certificate) Console Command is used in place of the equivalent payShield Manager menu given above.
- The file containing the certificates must be supplied on USB memory device and contain all the certificates required in the correct order as explained above.

11.4.2.5 Exporting the Chain of Trust and Viewing and Deleting Certificates

The payShield Manager Virtual Console is used as follows to perform the following:

Export Chain of Trust

Use the Virtual Console in Secure State and the '**SE**' Console Command in Secure State.

- Select Management TLS
- The Chain of Trust is output to the Virtual Console Display.

View Installed Certificates

Use the Virtual Console and the '**SV**' Console Command in any State:

- Select Management TLS
- The installed certificates in the selected Key Store are shown on the Virtual Console Display.

Delete Installed Certificates

Use the Virtual Console and the '**SD**' Console Command in Secure State:

- Select Management TLS
- The installed Host TLS Private Key and certificates are shown in numbered order on the Virtual Console Display.
- The item(s) to delete can then be selected.
- **WARNING:** Ensure the Management TLS private key and public key certificates currently being used are NOT deleted, otherwise connection to payShield 10K will be lost.

The local Console can be used in a similar way to achieve the above.

11.5 General Information for TLS for payShield 10K

11.5.1 HSM Recovery Key (HRK)

The HSM Recovery Key (HRK) is used to encrypt the Host and Management TLS private keys and the in establishing the TLS sessions.

The HRK-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 keys can therefore be recovered after a tamper event, once the HRK is installed, by decrypting the encrypted version.

The HRK is generated during initial configuration of payShield Manager (or using the local Console commands) using 2 passphrases entered by security officers. These passphrases must be provided to reconstitute the HRK 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.

Two different passphrases are required for the HRK, each entered by a different security officer. These passphrases must be stored securely (in the same way as key components) to allow subsequent HRK recovery if the HSM enters a tampered state. The passphrases must be of an acceptable complexity. Spaces are allowed.

Functionality is provided in both payShield Manager and the Console to change the HRK and to reinstall the HRK in the event of a tamper.

11.5.2 Upgrading and Downgrading Software

When upgrading to a version supporting the new functionality in 2.1a or downgrading from 2.1a to an earlier release, the keys, certificates and configuration for Host TLS and Management connections will remain in place to allow operation to continue without user intervention.

When upgrading to the version of Software supporting two Key Stores (i.e., 2.1a), if TLS is enabled, the Host TLS private Key and certificates will be stored in Key Store A and Key Store A will be automatically configured as active.

When downgrading from a version supporting two Key Stores (i.e., 2.1a or later) to an earlier version that does not support two Key Stores (i.e., earlier than 2.1a) if TLS is enabled, the Host TLS private key and certificates from the currently selected active Key Store (A or B) will be available in the original Key Store.

11.5.3 Support for USB Memory Devices

When using the local Console instead payShield Manager, USB memory devices are used to transfer material such as certificates in and out of the payShield 10K. The Operating System used in the payShield 10K supports most types of USB memory devices 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.

=====

11.5.4 Import Certificate



From this tab, when in the **Secure** state, you can load a TLS certificate into the payShield.

11.5.4.1 General Information

Note: Refer to the *payShield 10K Security Manual, Chapter 5, “Secure Host Communications”, Section 5.3 “Overview of TLS on the payShield 10K”* for additional information.

payShield 10K supports the use of TLS to secure traffic between Host applications and the HSM. TLS v1.2 is the preferred protocol.

Note that TLS works between applications. This means that both communicating applications must be TLS-enabled, rather than the Host and client devices. Proxies can be implemented to allow non-TLS-enabled applications to be used over a TLS-protected link: here, the authentication is from/to the proxy rather than the application.

The following prerequisites apply to both TLS Management Certificates and Secure Host Communication Certificates:

1. The system time has to be set to 24 hour UTC format
2. A CSR needs to have been signed by an external CA to obtain the certificate to import
3. No more than 256 certificates can be imported onto the HSM
4. The maximum length (depth) for the Chain of Trust is 6

11.5.4.2 TLS Management

Follow the steps below to install a certificate for securing payShield Manager connections.

1. Both Left and Right Administrators log on.
2. Click the **Secure State**.
3. Click the **TLS Management** tab.
4. Click **Import TLS Management Certificate**.



5. Select or drag and drop the file.

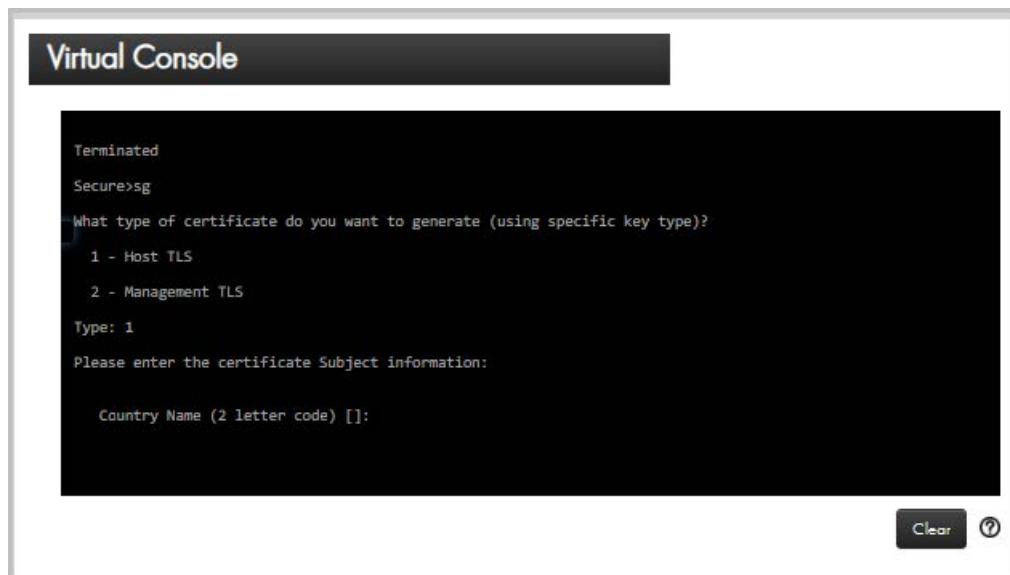


6. Click **Next**.
7. Continue as prompted.

11.5.4.3 TLS Management via the Virtual Console

The SG command will generate (or use the existing) HSM's public/private key pair for use with secure host communications, and extract the public key in the form of a Certificate Signing Request (“.CSR”)

1. Verify that the HSM is in the secure state.
 - Open the **Virtual Console** drop down
 - Verify the HSM is in the secure state.
 The “**Secure>**” prompt is displayed.
2. At the secure prompt, enter **SG**.
 - Follow the prompts as displayed on the following page.



The screenshot shows a terminal window titled "Virtual Console". The session has terminated, indicated by "Terminated" at the top. The user typed "Secure>sg" and received a prompt: "What type of certificate do you want to generate (using specific key type)?". Two options are listed: "1 - Host TLS" and "2 - Management TLS". The user selected "Type: 1". The next prompt is "Please enter the certificate Subject information:". A field for "Country Name (2 letter code) []:" is present. In the bottom right corner of the terminal window, there are "Clear" and "?" buttons.

3. Continue to [Section 11.5.4.4, “Secure Host Communications”, on page 279](#).

11.5.4.4 Secure Host Communications

Follow the steps below to install a certificate for securing Host connections.

1. Both Left and Right Administrators log on.
2. Click the **Secure State**.
3. Click the **TLS Management** tab.



4. Select or drag and drop the file.

Please select the certificate file to import. Only .crt files are allowed.

Drop file here
or

5. Click **Next**.
6. Continue as prompted.

12 Fraud Detection Functions

The payShield 10K HSM has fraud detection functions designed to detect and prevent “brute force” attacks, where (for example) large numbers of PINs are submitted until the correct PIN is discovered.

The detection works by counting how many failed PIN verifies are detected in one minute and in one hour. Each time that these counts exceed limits specified in the A5 Console command or in payShield Manager at Configuration / General Settings / Fraud, the PIN Attack Counter is incremented. If the PIN Attack Counter exceeds the specified PIN Attack Limit, then a PIN Attack is assumed.

The A5 Console command or payShield Manager at Configuration / General Settings / Fraud also determines how the HSM will react. The user can select “On” for full pro-active response to the limits being exceeded, or “Logging Only” in order to record (in the Health Check Data) the limits being exceeded without taking any further action.

An entry is always made in the Audit Log if any of the limits are exceeded.

If the Logging Only option has been selected, then the payShield 10K will provide counts of how many times the per-minute and per-hour limits have been exceeded and the total number of PIN Attacks detected. This information is provided as part of the Health Check Data provided by the HEALTHSTATS command or payShield Manager Status / Health Statistics/Diagnostics, and is therefore only available if Health Check data has been enabled using the HEALTHENABLE Console command or Status / Health Statistics/Diagnostics in payShield Manager. The counts can be reset using the “Reset All Stats” option in the HEALTHSTATS command or at Status / Health Statistics/Diagnostics in payShield Manager.

Note that the term “Logging” here refers to capture of the information in the Health Check data. Audit Log entries are always made when the limits are exceeded.

If the “On” option has been selected, then the reporting provided by the Logging Only option is again provided. In addition, if either of the per-minute or per-hour counts exceeds the specified limits, the HSM forces all PIN verification commands to return an error 39 in their response. The HSM will continue to return error 39 until the Console command A7 is used to re-enable PIN verification. If the PIN Attack Counter reaches the PIN attack limit, then the HSM will clear the LMKs from its memory. Installing the LMKs will set the PIN attack counter to 0.

The following list specifies the PIN verification host commands to which the limits apply:

- DA - Verify a Terminal PIN Using the IBM Method
- EA - Verify an Interchange PIN Using the IBM Method
- CG - Verify a Terminal PIN Using the Diebold Method
- EG - Verify an Interchange PIN Using the Diebold Method
- DC - Verify a Terminal PIN Using the Visa Method
- EC - Verify an Interchange PIN Using the Visa Method
- BC - Verify a Terminal PIN Using the Comparison Method
- BE - Verify an Interchange PIN Using the Comparison Method

13 Utilization Data

The payShield 10K provides users with data about how heavily utilized the HSM is. This is designed to allow users to re-balance loading between their various payShield 10Ks, and to optimize their purchasing of additional capacity.

The Utilization Data facilities involve the Console and payShield Manager, and the Host interface. Detailed information concerning the commands and operations involved are described in the relevant manuals. This chapter provides a high-level overview of the Utilization Data capability and how it works.

13.1 Data Provided to the User

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

- Overall HSM Loading.

This data is provided as an instantaneous snapshot of current loading or as a series of numbers indicating since the last data reset for how many seconds the HSM was loaded from 0-10% of its capacity, for how many seconds the loading was in the range 10-20%, for how many seconds it was in the range 20-30%, and so on.

- Host Command Volumes.

This data indicates how many times each Host command has been processed, and the average calls per second (CPS) for each command.

13.2 Data Collection Period

Data is collected over 2 types of periods:

- “Since Last Reset”

Data is accumulated since the last time that the user reset the utilization data. This data includes the number of seconds that the data is accumulated over, allowing average transaction rates to be calculated. Data will continue to accumulate until the next time the data is explicitly reset. There is no facility at the HSM to select data between 2 dates (other than between last reset and now), but the accumulated data can be retrieved at any time without resetting it. This means that time-series data can be achieved by regular retrieval of data to an external host computer. (payShield Monitor can provide statistics between selected end and start dates/times.)

Data collection can be suspended and resumed without resetting the data. This means that meaningful results can still be returned if the HSM is temporarily taken out of service or re-purposed.

Data accumulation, including the number of seconds that the data is accumulated over, is automatically suspended when the HSM is not online.

The collected data is persistent over re-starts and power loss, but is reset when new software is installed on the HSM.

- “Instantaneous data”

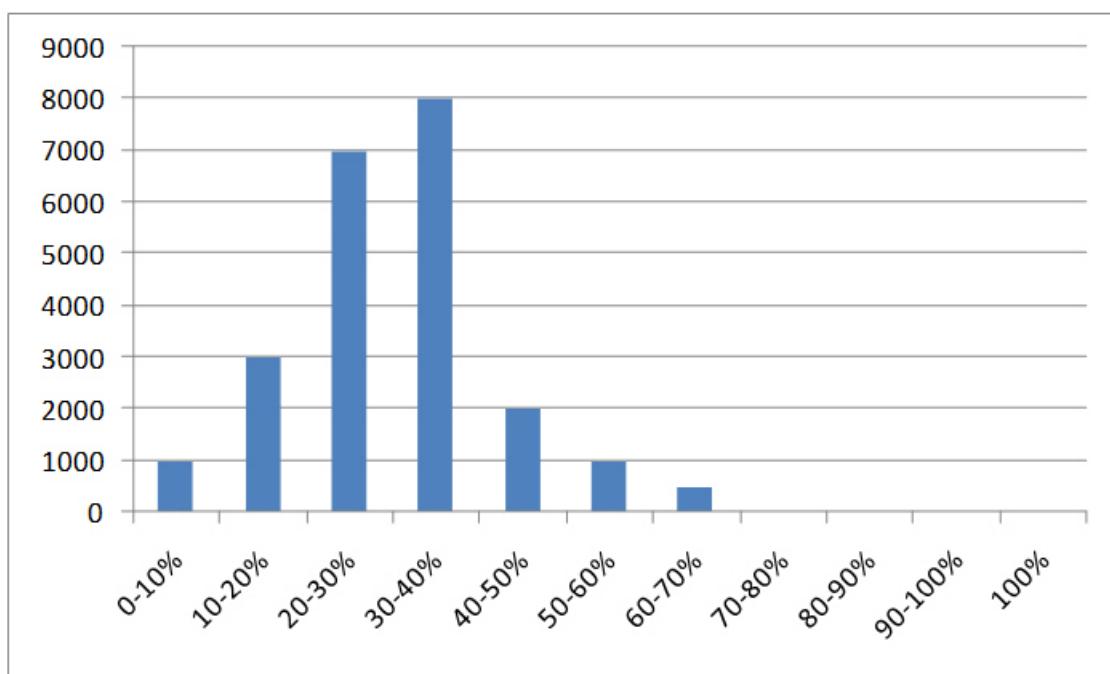
It is also possible to get a view of the loading of the HSM right now by asking for instantaneous data, helping administrators investigate throughput or performance issues as they are occurring. This provides utilization data over the most recent period: the length of this period can be configured from 1 to 60 seconds.

13.3 Interpreting the Output

13.3.1 Overall HSM Loading

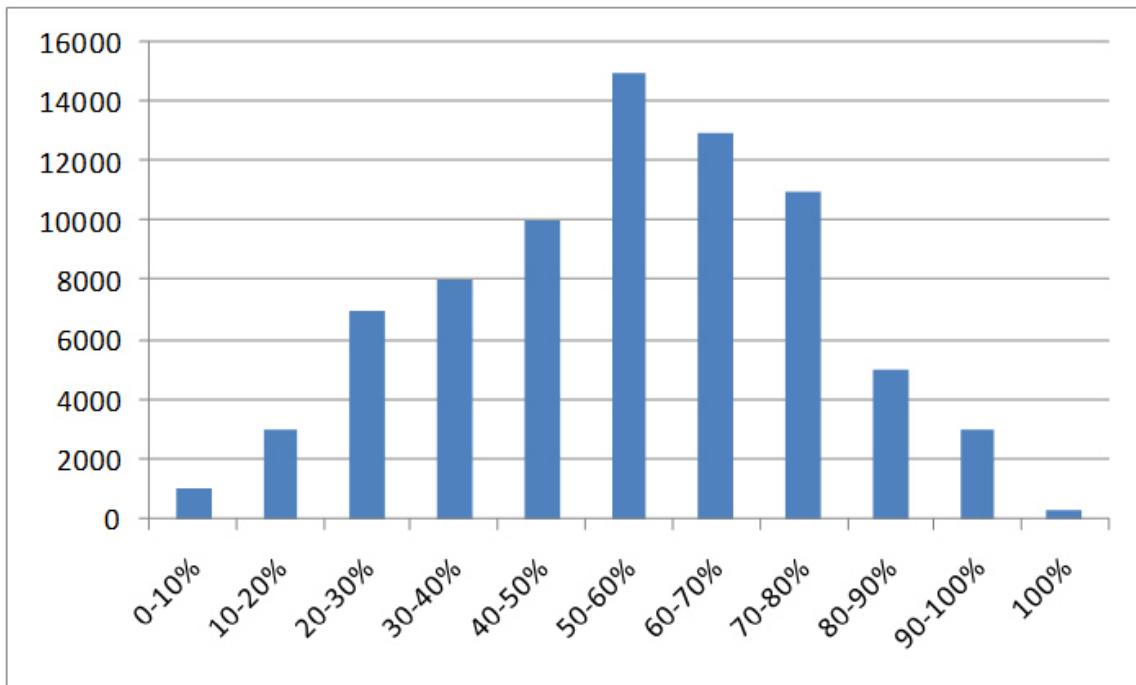
The data provided allows the user to create histograms of the following format:

Chart Example 1:



This example indicates an HSM which is “comfortably” loaded and could take on more work. It shows that on 1,000 occasions (i.e. 1-second periods) it was under 10% loaded; on 3,000 occasions it was loaded between 10 and 20%, and so on. The most common loading was in the range 30-40%, and it was never more than 70% loaded.

Chart Example 2:



This example depicts an HSM which is under stress, and which needs its load reducing by re-balancing workload between the HSM estate or by adding additional capacity.

Note the “100%” column in these examples: this indicates how frequently the HSM was working at its full capacity - and 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.

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

13.3.1.1 Output using the Console

For users working at a Console, the information is provided as a table of numbers. The output from the UTILSTATS command for data accumulated since the last reset includes data of the following format:

```
HSM Serial Number:→ → A4665271570Q

Report Generation Time: 05-Mar-2011 23:19.59
Report Start Time: → 01-Jan-2011 14:25.01
Report End Time: → 05-Mar-2011 23:19.59
Total number of secs: 123,456

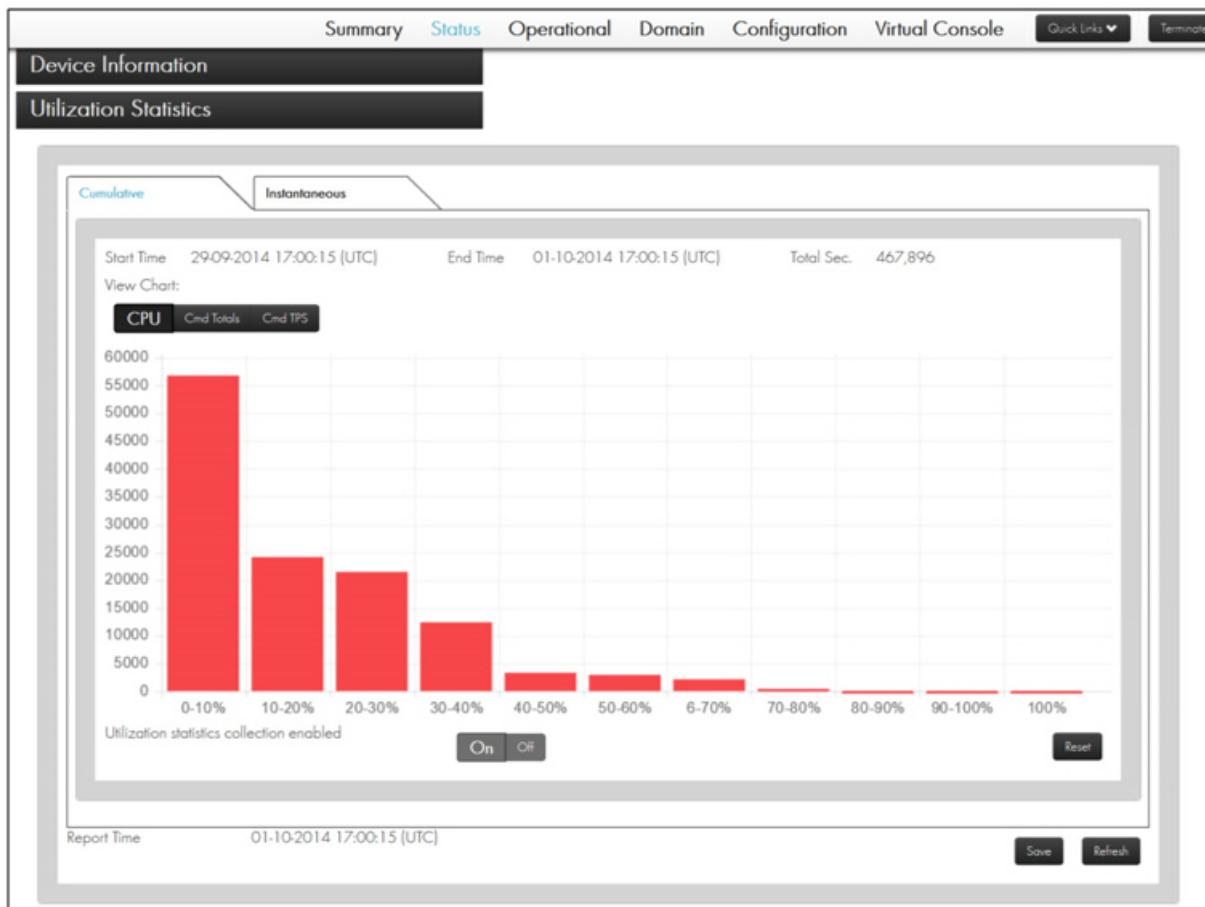
HSM Loading:
  0-10%: → 56,789
  10-20%: → 24,109
  20-30%: → 21,445
  30-40%: → 12,382
  40-50%: → 3,288
  50-60%: → 2,917
  60-70%: → 2,123
  70-80%: → 403
  80-90%: → 0
  90-100%: → 0
  100%: → 0
```

Instantaneous loading is presented in the following format:

```
Instantaneous HSM Load: 15%
```

13.3.1.2 Output using payShield Manager

For users managing the payShield 10K using payShield manager, the output is presented in graphical form:



13.3.2 Host command Volumes

Data is provided for each Host command that has been used since the collection of data started. It shows for each command the number of times that command has been run, and the average transactions per second for that command over the data collection period.

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 cps 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.

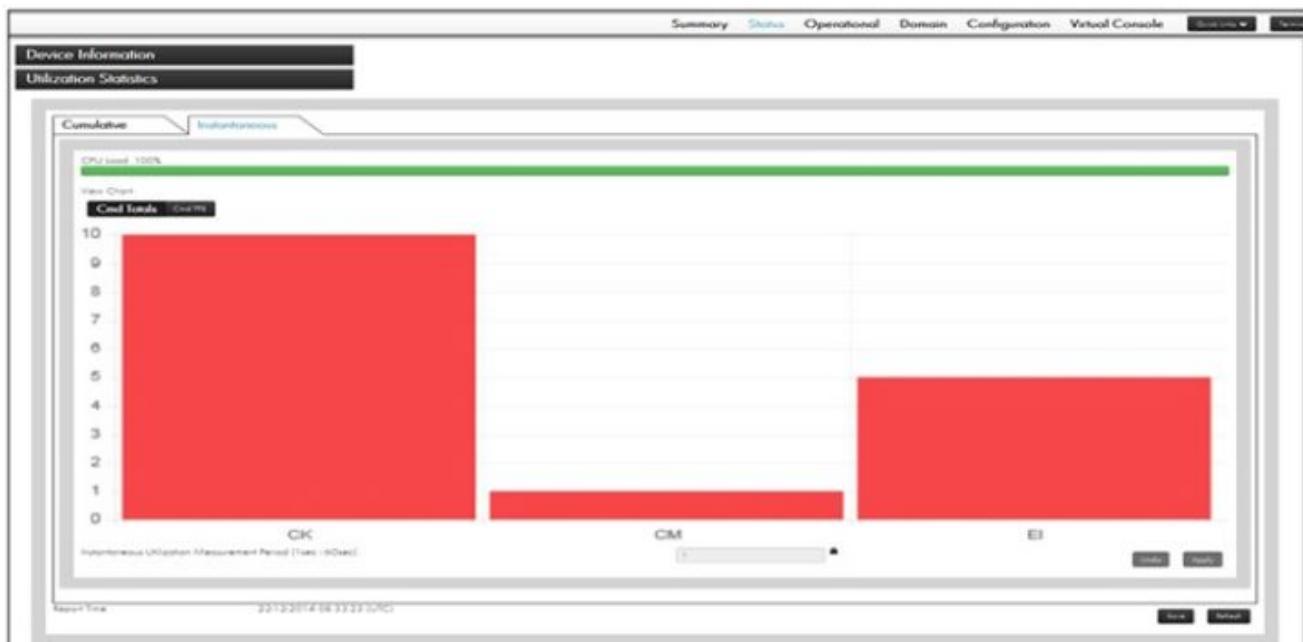
13.3.2.1 Output using the Console

For users working at a Console, the information is provided as a table of numbers. The output from the UTILSTATS command for both data accumulated since the last reset and for “instantaneous” data includes data of the following format:

Host Command Volumes:						
Cmd	Code	→	Total Transactions	→	Average TPS	→
A0	→	→	589 →	→	→	0.00
DA	→	→	692,442 →	→	→	5.61
CA	→	→	15,927,678 →	→	→	129.02
EI	→	→	23,456 →	→	→	0.19
M0	→	→	168,558 →	→	→	1.37

13.3.2.2 Output using payShield Manager

For users managing the payShield 10K using payShield manager, the output is presented in graphical form:



13.4 Reporting Mechanisms

The Utilization data can be accessed using:

- The Console

- payShield Manager
- Host commands
- Printing at the HSM-attached printer
- SNMP

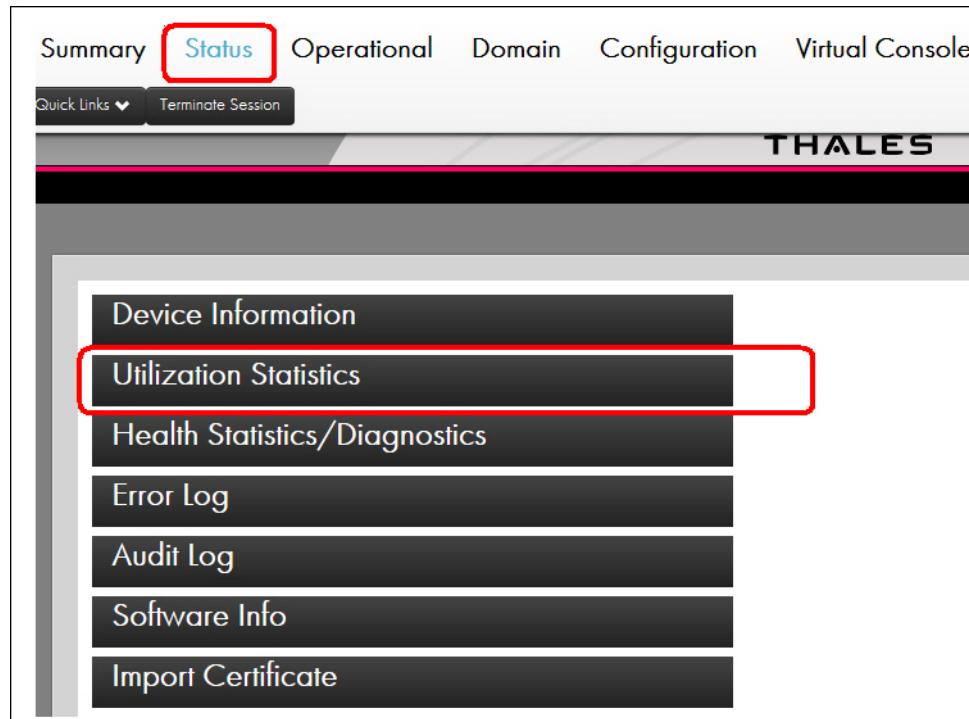
This data can also be accessed using payShield Monitor - please see the payShield Monitor manuals for further information.

13.5 Console Commands

- UTILCFG - allows the data collection period for “instantaneous” data to be configured
- UTILENABLE - allows gathering of utilization data to be suspended or resumed
- UTILSTATS - allows the utilization data to be viewed at the Console, printed at an HSM-attached printer, and reset
- SNMP - displays SNMP Users that are currently set up
- SNMPADD - allows SNMP Users to be added
- SNMPDEL - allows SNMP Users to be removed

13.6 payShield Manager Commands

In payShield Manager, the following path is available to manage and view the utilization statistics.



Follow this link to: [Section 9.7.2, “Utilization Statistics”, on page 126](#) for additional details.

13.7 Host commands

The following Host commands are available to operate the Utilization Data facility. These commands are described in detail in the *payShield 10K Core Host command Reference Manual*.

- J2 - Get HSM Loading data
- J4 - Get Host Command Volumes
- J6 - Reset Utilization Data

Note that Instantaneous Utilization data is expected to be used by administrators on an ad hoc, event-driven, basis; it is therefore not provided via the Host command interface.

13.8 Managing Utilization Data

It is important that users periodically reset the Utilization Data before the maximum record size of 4,294,967,295 is reached; as in software releases prior to v1.3d there will be a performance impact if this limit is reached.

For software versions v1.3d and later, entries are made in the Error Log and notification is made via SNMP when the Utilization Data is within 10%, 5% and then also when the once maximum limit is reached at which point the Utilization Data is reset automatically.

14 Health Check Data

The payShield 10K provides users with data to help them assess the health state of the HSM.

The Health Check Data facilities involve the Console, payShield Manager, and the Host interface. Detailed information concerning the commands and operations involved are described in the relevant manuals. This chapter provides a high-level overview of the Health Check Data capability and how it works.

See payShield Monitor manuals for information about accessing Health Check Data for the whole estate of payShield 10Ks by using payShield Monitor.

14.1 Data Provided to the User

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

- Accumulated Counts and
- Instantaneous Status

14.1.1 Accumulated Counts

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

- Re-starts
- Tamper*
- Fraud Detection thresholds being exceeded

Note: Users can elect to set Fraud Detection thresholds and monitor whether these are being exceeded without the HSM ceasing to be fully functional.

Collection of data can be suspended and resumed without resetting the data. This means that meaningful results can still be returned if the HSM is temporarily taken out of service or re-purposed.

The collected data is persistent over re-starts and power being switched off, but is reset if new software is installed on the HSM.

* 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.

14.1.1.1 Output using the Console

For users working at a Console, the information is provided as part of the output from the *HEALTHSTATS* command:

```
HSM Serial Number: A4665271570Q

Report Generation Time: 05-Jan-2011 04:35.29
Report Start Time: 23-Dec-2010 01:29.41
Report End Time: 05-Jan-2011 04:35.29
Number of reboots: 18
Number of tampers: 6
Failed PIN verifies/minute limit exceeded: 29
Failed PIN verifies/hour limit exceeded: 1
```

14.1.1.2 Output using payShield Manager

payShield Manager users will see output in the following format:

Status / Health Statistics / Diagnostics

The screenshot shows the payShield Manager web interface. At the top, there is a navigation bar with tabs: Summary, Status, Operational, Domain, Configuration, Virtual Console, a dropdown for 'Quick Links', and a 'Logout' button. Below the navigation bar, there is a sidebar with three main categories: Device Information, Utilization Statistics, and Health Statistics/Diagnostics. Under Health Statistics/Diagnostics, there are two sub-tabs: 'HealthStats' (which is selected) and 'Diagnostics'. Below these tabs, there is a section titled 'Enable/Disable Health Check Data Collection' with 'Enable' and 'Disable' buttons. The main content area displays a table of device statistics. At the bottom right of this area are 'Save' and 'Reset' buttons. At the very bottom of the page, there are links for Error Log, Audit Log, and Software Info.

HSM Serial Number:	B46652712260
Report Generation Time:	05-06-2014 14:23:11 (UTC)
Report Start Time:	05-06-2014 14:20:00 (UTC)
Report End Time:	05-06-2014 14:23:10 (UTC)
Number of reboots:	12
Number of tampers:	15
PIN verification failures/minute limit exceeded:	57
PIN verification failures/hour limit exceeded:	4
PIN Attack limit exceeded:	15

Follow this link to [Section 9.7.3, “Health Statistics/Diagnostics”, on page 130](#).

14.1.2 Instantaneous Status

This provides a range of HSM health check data 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/PayShield Manager service is running
- Tamper state*
- LMK information:
 - Numbers loaded
 - Types of LMK - test/production; variant/key block
 - Authorized state
 - Number of authorized activities
- Fraud Detection status
 - Whether PIN Verifications per min./hour have been exceeded
 - If PIN Attack limit exceeded

* 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.

14.1.2.1 Output using the Console

Instantaneous Health Check Data is presented as part of the DT Console command:

```
payShield Health Check Status

TCP Server: Up
UDP Server: Up
Async Server: Not Enabled
Local/Remote Manager Server: Up
Host Ethernet Link 1: Up
Host Ethernet Link 2: Down
Host Async Link: Not Enabled
Unit Tampered?: Yes
Cause: Case Tampered
Date: 07-Feb-2011 06:28.15
```

14.1.2.2 Output using payShield Manager

payShield Manager users will see output in the Diagnostics Tab under Health Statistics/Diagnostics in the Status section.

14.2 Reporting Mechanisms

The Health Check data can be accessed using:

- The Console
- payShield Manager
- Host commands
- Printing at the HSM-attached printer
- SNMP - for instantaneous status only

This data can also be accessed via payShield Monitor. The relevant manuals should be consulted for further information.

14.3 Console Commands

The following Console commands are available to operate the Health Check Data facility. These commands are described in detail in the *payShield 10K Console Guide*.

- A5 - Fraud detection: to allow Health Check counters to be accumulated without the HSM ceasing to execute commands
- AUDITOOPTIONS - to allow data resets to be recorded
- DT - Diagnostics: this has been enhanced to display the Instantaneous Health Check data
- HEALTHENABLE - allows gathering of Health Check counters to be suspended or resumed
- HEALTHSTATS - allows the Health Check counters to be viewed at the Console, printed at an HSM-attached printer, and reset
- SNMP - displays SNMP v3 Users that are currently set up
- SNMPADD - allows SNMP Users to be added
- SNMPDEL - allows SNMP Users to be removed

14.4 payShield Manager Commands

Follow this link to: [Section 9.7.3, “Health Statistics/Diagnostics”, on page 130.](#)

14.5 Host commands

The following Host commands are available to operate the Health Check Data facility. These commands are described in detail in the *payShield 10K Core Host command Reference Manual*.

- J8 - Get Health Check counts
- JK - Get Instantaneous Health Check status
- JI - Reset Health Check Data

15 Audit Log

15.1 Introduction

The payShield 10K provides an Audit Logging capability, enabling security officers to select a number of activities and functions whose usage is recorded in an Audit Log. Certain items are always recorded in the Audit Log, and this cannot be disabled.

The purpose of the Audit Log is to enable security officers to make regular checks on security-related actions that the payShield 10K is being asked to perform, and to assist in forensic examination of any suspected security breaches.

The Audit Log also provides facilities for its entries to be viewed, printed, and archived to a host computer.

This chapter describes the capabilities and usage of the Audit Log.

15.2 Overview

The Audit Log is held securely in non-volatile memory in the payShield 10K: it survives power cycling, payShield 10K restarts, tamper attempts, and software upgrades.

It always records certain events and use of functions. In addition, security officers can elect to log other events and functions.

The Audit Log can be viewed, printed, erased, and retrieved or archived to a host computer. The Audit Log contains 100,000 entries for audit records. When the Audit Log is filled, the earliest entry is deleted to allow the most recent entry to be added. It is therefore important that entries are archived to a host computer frequently enough such that the Audit Log does not get filled. The frequency with which this needs to be performed will depend on how many items are being recorded.

A message authentication code (MAC) is associated with each individual audit entry, enabling easy detection of any fraudulent attempt to modify the audit record.

15.3 Correct Use of the Audit Log

The Audit Log has been designed to capture information which will be examined when investigating any potential security issues: it is not intended for use as a general log of what the HSM is being used for, for example by logging all Host commands (which can impact on performance).

Audit Log entries should be reviewed at regular and frequent intervals to allow:

- Any necessary actions to be taken
- Any records that need to be retained for future reference to be printed or archived to the host system

- The Audit Log to be cleared

Warning: It is important that the Audit Log is kept as small as possible to optimize performance. Only enable auditing for as few Host commands as possible - enable auditing for all Host commands will severely impact performance and operation. It is particularly important that the Audit Log is not allowed to reach its maximum size.

Logging high-frequency events which correspond to normal usage of the HSM and which have no significance in terms of security introduces a number of problems:

- Creating too many records to allow significant records to be found and interpreted
- Causing loss of audit records if the Audit Log capacity is exhausted before the audit records have been archived
- Negatively impacting on performance, because of the additional processing required to create and record audit records, especially when the Audit Log capacity is exhausted and the log needs to be "rotated" (i.e. the oldest record deleted to allow the new record to be added)

Later sections describe how the options for recording events to the Audit Log can be configured. It is recommended that as few Host commands as possible are audited: error responses to Host commands may well be indicative of a security threat, and the audit options allow such responses to be logged without having to audit normally executing Host commands.

15.4 Forcibly recorded items

A number of items are always recorded in the Audit Log: this cannot be disabled.

15.4.1 PCI HSM Compliance

Most of these forcible recorded items were introduced to meet requirements of PCI HSM certification. These items are:

- Use of Smart Cards to authenticate users to the payShield or payShield Manager. The serial number of the Smart Card is recorded as part of the Audit Log record.
- Use of the A and C Console commands to initiate and cancel authorization of activities. The Audit Log entry shows for how long the activity was authorized.
- Use of the following Console commands or the equivalent payShield Manager actions. The Audit Log records made in this way will indicate the successful completion of the command.

Console Command	
Current commands	
CV	Generate a Card Verification Value
FK	Form Key from Components
IK	Import a Key
LK	Load LMK
LO	Load 'Old' LMK into Key Change Storage
LN	Load 'New' LMK into Key Change Storage
PV	Generate a Visa PIN Verification Value
RL	Load RMK

Console Command	
Legacy Commands	
BK	Form a Key from Components
D	Form a ZMK from Encrypted Components
DE	Form a ZMK from Clear Components
IV	Import a CVK or PVK

15.5 Recording Deletion in Audit Log

The Audit Log will include a record to indicate that the Audit Log has been erased.

15.6 Discretionary Audit Log entries

It is possible to request that any of the following events are recorded in the Audit Log:

- Use of combination of any Console commands or payShield Manager actions

The Audit Log records made in this way will indicate the initiation of the command rather than its successful completion. This is different to the way that a forcibly audited command would be recorded, where the successful completion of the command/action is recorded.
- Auditing activity on host ports:
 - Use of any desired selection of Host commands. As discussed in an earlier section, this facility should be used carefully to avoid logging of high volumes of Host commands which are executing normally: it is generally better to log just error responses (see next item), as these may well be indicative of a security issue
 - Receipt of an error response to a Host command
 - Failures to establish host connections arising from the Access Control List (ACL).
 - Attempts to use out-of-date certificates when trying to establish Secure Host Communication sessions.
- User actions:
 - Clearing of Audit Log
 - Loading an LMK or an Old/New LMK
 - Erasing an LMK or an Old/New LMK
 - Loading a license file - successful
 - Loading a license file - failed
 - Change of state
 - Power cycle
 - Resetting of Utilization Data
- Results of automatic daily self-tests - indicating whether the tests were successful or identifying any specific tests that failed

15.7 Audit Log Protection

The payShield 10K provides a number of features specifically aimed at protecting the Audit Log:

- Each Audit Log record is MACed using a unique MACing key protected by the LMK. A Host command is available to allow the MAC to be verified at a later time.
- Audit Log entries can be archived by printing to a printer attached to the payShield 10K
- Audit Log entries can be retrieved to the host system for secure electronic archiving
- Console actions to configure or delete the Audit Log require Authorization using the Management LMK. Equivalent actions on payShield Manager require Security Officers to be logged on
- Host commands to delete Audit Log records must be authorized
- Deletion of the Audit Log always results in a record of this event being added into the otherwise now blank Audit Log

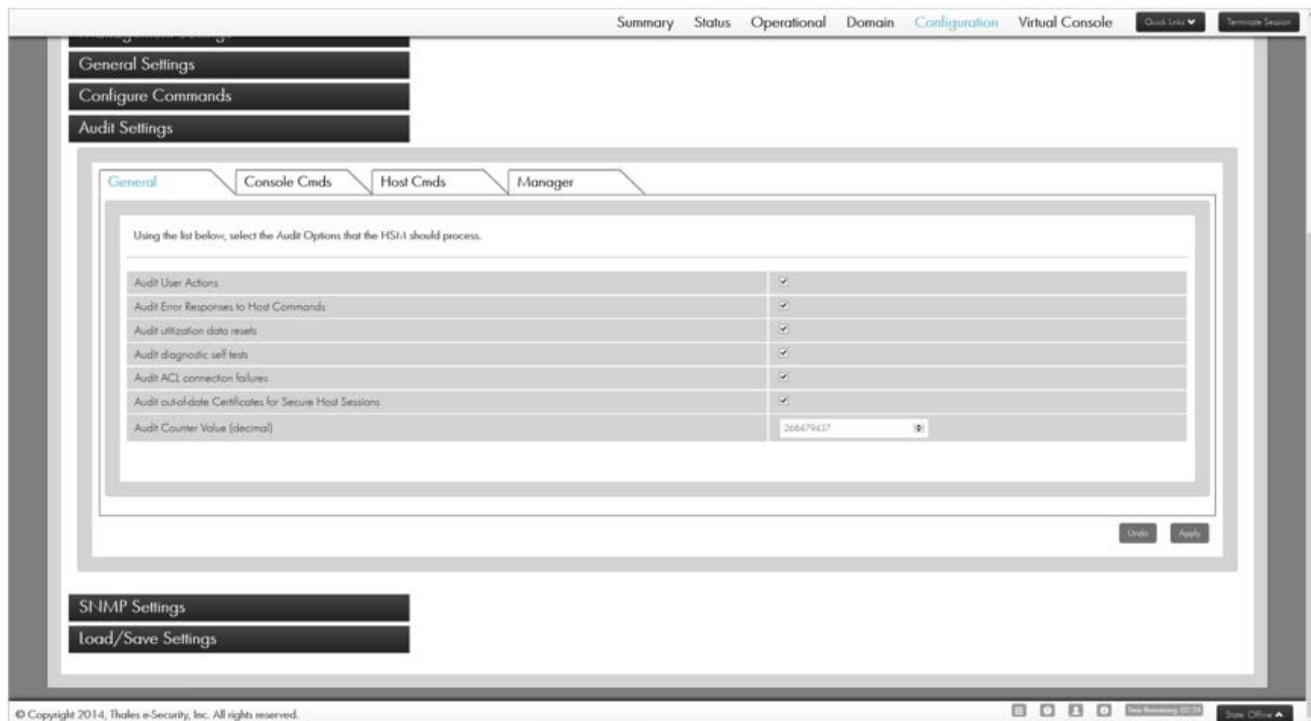
15.8 Configuring the Audit Log

15.8.1 AUDITOOPTIONS Console command

When a Console (i.e. dumb character terminal) is used to manage the payShield 10K, the AUDITOOPTIONS Console command is used to configure the auditing options - see the *payShield 10K Console Manual* for full details and examples.

15.8.2 payShield Manager Auditing screen

The payShield Manager Audit Settings screen on the Configuration page performs the same functions as the AUDITOOPTIONS Console command.



The *General* tab controls which of the following events are currently audited:

- User Actions
- Error Responses to Host commands
- Utilization Data Resets
- Diagnostic Self Tests
- ACL Connection Failures
- Out-of-date Certificates for Secure Host Sessions

The *Console Cmds* tab controls which Console commands are currently audited.

The *Host Cmds* tab controls which Host commands are currently audited.

The *Manager* tab controls which payShield Manager actions are currently audited.

15.9 Viewing the Audit Log

15.9.1 AUDITLOG Console command

The **AUDITLOG** command allows the Audit Log to be viewed on the Console. The most recent entries are displayed first. Note that even at the maximum supported line speed of 115.2 Kbps, a full Audit Log with 100,000 entries will take 10-20 minutes to display.

Here is an example of output from AUDITLOG:

```
Offline> AUDITLOG <Return>
Audit Log (10 entries)
Counter    Time        Date      Command/Event
-----
0000010B  13:55:00  02/Jul/2020 Diagnostic self test failure: Power
0000010A  16:45:07  01/Jul/2020 Authorised activity admin..host was cancelled for
          LMK id 0
00000109  16:45:05  01/Jul/2020 Authorised activity admin..Console:123 was cancelled
00000108  15:54:02  01/Jul/2020 Key I/O command BK executed
00000107  15:35:55  01/Jul/2020 Activity component..Console:123 was authorised for
          LMK id 0
00000106  15:08:48  01/Jul/2020 Smart Card activated: 20025151
00000105  15:08:48  01/Jul/2020 Smart Card activated: 20025132
00000104  10:42:32  01/Jul/2020 Host command CA, response 00
00000103  10:36:03  01/Jul/2020 Host command CA, response 69
00000102  10:34:57  01/Jul/2020 System restarted
00000101  10:32:48  01/Jul/2020 Keylock turned to Online
00000100  10:32:21  01/Jul/2020 Console command CH
000000FF  09:01:56  01/Jul/2020 Diagnostic self tests passed.
```

Offline>

This example provides the following information:

- The unit's automatic self tests ran successfully on the 1st of July at 09:01:56 (Counter = 000000FF), but on the 2nd of July at 13:55:00 they failed because of a power supply unit failure (Counter = 0000010B).
- On the 1st July at 10:32:21 the *CH* command was run at the Console (Counter = 00000100). This is a discretionary Audit Log entry.
- On the 1st July at 15:54:02 the *BK* Console command was successfully executed (Counter = 00000108). This is a forcibly recorded item.
- On the 1st July at 10:32:48 the user turned the metal key(s) to put the payShield 10K into Online state (Counter = 00000101).
- On the 1st July at 10:34:57 the system restarted – e.g. because the power was cycled or the user pressed the Reset button on the front panel (Counter = 00000102).

- On the 1st July at 10:36:03 (Counter = 00000103) the CA Host command was run but received a response of 69 (PIN Block format has been disabled). However, at 10:42:32 (Counter = 00000104) the CA command was run successfully (response = 00).
- On the 1st July at 15:08:48 the Smart Cards with serial numbers 20025132 and 20025151 were used to authenticate security officers to the payShield 10K. Subsequently the following authorization activities were performed under the oversight of the “owners” of these Smart Cards:
 - at 15:35:55 all component Console commands were authorized for LMK 0 for a duration of 2 hours and 3 minutes (123 minutes) (Counter = 00000107)
 - at 16:45:05 the authorization of admin Console commands for LMK 0, originally authorized for 123 minutes, was cancelled (Counter = 00000109)
 - at 16:45:07 the authorization for all admin Host commands for LMK 0 was cancelled (Counter = 0000010A).

15.10 payShield Manager Audit Log Screen

When using payShield Manager, the Audit Log screen on the Status page displays the current contents of the Audit Log:

The screenshot shows a web browser window titled "payShield Manager" with the URL "https://a4655000014p-mgmt/main/status". The page has a navigation bar with tabs: Summary, Status, Operational, Domain, Configuration, Virtual Console, Quick Links, and Terminate Session. Below the navigation bar is a large THALES logo. On the left, there is a vertical sidebar with five menu items: Device Information, Utilization Statistics, Health Statistics/Diagnostics, Error Log, and Audit Log. The Audit Log item is highlighted. The main content area contains a table of audit log entries. The table has columns: Counter, Time, Command Type, Command Code, Response Code, and Text. The entries are as follows:

Counter	Time	Command Type	Command Code	Response Code	Text
1518	Apr 10, 2015 15:14:42	C	00	00	Remote Mgmt cmd - a6f4031f- invalid request for /accessControl /loggedInUsers
1517	Apr 10, 2015 15:14:42	C	00	00	Remote Mgmt cmd - a6f4031f- invalid request for /status/currentStatus
1516	Apr 10, 2015 14:45:08	C	00	00	Remote Mgmt cmd - 0c01a1d7- invalid request for /accessControl /dologin
1515	Apr 10, 2015 14:42:42	A	11	00	LMKs loaded
1514	Apr 10, 2015 14:42:21	A	KE	00	Smartcard activated: 20001352

At the bottom of the table, it says "Latest SHA-256 Hash: 3F47EA5A6CEE8188B6362065DD581CCDF70C7A6DE3FAD319857A8852E600AC33". Below the table are buttons for Download, Get More, Reload, and Clear. At the very bottom of the page, there is a copyright notice: "© Copyright 2014, Thales e-Security, Inc. All rights reserved." and a status bar with icons and text.

The Download button allows the Audit Log to be saved as a file, which can then be printed if required.

15.11 Printing the Audit Log

15.11.1 AUDITPRINT Console command / Q2 Host command

Both the AUDITPRINT Console command and the Q2 Host command send the Audit Log to a printer attached to the payShield 10K. The commands can be used to print all Audit Log records or just those that have not been archived: a flag is set against each printed record to indicate that it has been archived in this way.

The output has the following format:

Counter	Time	Date	Command	MAC	Key	MAC
1001CF33	135209	180511	H M2 06	AA69C75033EA50810209D24F17E93786		ACBC947DA5E06947
1001CF34	135209	180511	H M2 06	5D53F23A43A7AC692C77754FB00EBCA6		E3DFFE68209F4A1E
1001CF35	135209	180511	H M2 06	787C6FC766E544CD4A2EF56DB1DE1C14		D5321C3CF8E36DCB
1001CF36	135209	180511	H M2 06	34D3B4CE59DDC0BA4C128EF88721D50C		86D18019F2E1D717
1001CF37	135209	180511	H M2 06	F893D165B7CADC6DC44A59CF33F895FE		C5C14C8D93892004
1001CF38	135209	180511	H M2 06	C364F9C499C89514A3EB6BBA75BC2C87		55BB024854727C41
1001CF39	135209	180511	H M2 06	D229ACB7F9C5EEA7FB55761EEB9947D7		BB6E67CA6DEF2584
1001CF3A	135209	180511	H M2 06	0F5A3BAB8A93FEC30E9C125E585FB005		1D84136FA9162B1B
1001CF3B	135209	180511	H M2 06	7F78D6858D729710477C0CEF18917281		CB6746ADAE4B65AC
1001CF3C	135209	180511	H M2 06	C1EA998068CD989A5383A8EA7B52EB1C		F2B5A526C100EAB3
1001CF3D	135209	180511	H M2 06	5BA7D93E19DA1EEA14AAA1BCDB1CB45B		2DCF25D8E0DE381F
1001CF3E	135209	180511	H M2 06	9C019A9DF544F2F31300CCD54DF44DF1		7FA5EA6DA98043C9
1001CF3F	135209	180511	H M2 06	D4AD0D70A5EBFE61B5BAF2DC509FB478		36D504B7E837778B
1001CF40	135209	180511	H M2 06	B29D7E22350640A702255D1A024777AE		C8495DF637BA3E6A
1001CF41	135209	180511	H M2 06	4B6C7887A7662663FDD76EEE6FE9BE27		749BD7153ADD5A01
1001CF42	135209	180511	H M2 06	A9048C7578CBE29227FA824AE51B0323		4FB59F661352A05B
1001CF43	135209	180511	H M2 06	27D6C576FE6F1B0537A51175777C5820		B6EE89EF4F65F7BC

- For Host commands, the entry has the format shown in the above example. “H” identifies the entry as a Host command, “M2” represents the Host command that was used, and “06” was the response code.
- For a Console command, the entry is of the format “C XX 00”. “C” identifies the event as a Console command. “XX” identifies the Console command: in the case of a 2-character Console command, this is the actual command code, whereas for other Console commands, a 2 hexadecimal code (defined in the *payShield 10K Core Host Command Reference Manual*) is used. “00” is always reported in the response code field.
- For a Fraud Detection event, the entry has the format “F XX 99”, where “F” identifies that this is for a Fraud Detection event, “XX” represents the command code that caused the event to arise, and the response code field identifies which Fraud Detection threshold was exceeded. (See [Chapter 12, “Fraud Detection Functions](#) for more information about the Fraud Detection facility in the payShield 10K.)
- For user actions, the entry has the format “A XX 00”. “A” identifies this as a user action, “XX” represents the identity of the User Action (defined in the *payShield 10K Core Host Command Reference Manual*), and the response code is always set to “00”.

Note: Each record is MACed with a unique, random MACing key, to allow the integrity of the record to be confirmed.

15.11.1.1 Audit Record Format

This section provides an expanded description of the Audit Record format.

Field #	Name	Length	Description
1	Audit Counter	4 bytes	Binary counter (0..4294967295), indicating the position of this record within the audit log.
2	Date/Time Stamp	6 bytes	The following six fields are BCD encoded: Hour (00..23) Minute (00..59) Second (00.59) Day (01..31) Month (01..12) Year (00..99) (years since 2000).
3	Command Code / Action Code	2 bytes	For Command Code Types 00, 01 and 10, this field contains the relevant Command Code. For Command Code Type 11, this contains an Action Code.
4	Command Code Type *	2 bits	00 - Host Command 01 - Console Command 10 - Fraud Event 11 - User Action
5	Archived Status Bit	1 bit	1 = archived, 0 = not archived.
6	Retrieved Status Bit	1 bit	1 = retrieved, 0 = not retrieved.
7	Unused	12 bits	Set to binary 0.
8	Response Error Code	2 bytes	2 digit Response Code from host command's response message.
9	Audit Record MAC	8 bytes	MAC generated over fields 1..8 using the following Random MAC Key.
10	Random MAC Key	16 bytes	Key used to generate the audit record MAC. Encrypted under the LMK.

*In the output from AUDITPRINT Console command, the Command Code Type is changed to an alphabetic indicator as follows:

- Host Command:
 - “H” (in place of “00” in the Q2 Host command)
- Console Command:
 - “C” (in place of “01” in the Q2 Host command)

- Fraud Event:
 - “F” (in place of “10” in the Q2 Host command)
- User Action
 - “A” (in place of “11” in the Q2 Host command)

Command Code Types:

- Command Code Type 00 – Host Command

Audited host commands have their command code in the record's Command Code field and the corresponding response error code in the Response Error Code field.

- Command Code Type 01 – Console Command

Audited console commands have their command code* in the record's Command Code field and 00 in the Response Error Code field.

*The payShield HSM has some console commands that do not have exactly two characters in length. In addition, there are some actions which are not strictly Console activities but are designated as Console commands in the Audit record. For storage within the audit record, these longer commands should be mapped to the following twocharacter strings:

Console Command	Audit Record Command Code
User actions performed using payShield Manager, include log retrieval, log clearing, logins, disconnections, state changes, setting audit options, and automatic audit log entry arising from a key or component entry action made using payShield Manager.	'00'
AUDITLOG	'01'
AUDITOPTIONS	'02'
CLEARAUDIT	'03'
CLEARERR	'04'
EJECT	'05'
ERRLOG	'06'
GETCMDS	'07'
GETTIME	'08'
SETTIME	'09'
A	'0A'
B	'0B'
Console Command	Audit Record Command Code
C	'0C'
D	'0D'
F	'0E'
K	'0F'
N	'10'
R	'11'
T	'12'
V	'13'

Z	'14'
\$	'15'
CONFIGCMDS	'16'
CONFIGPB	'17'
PING	'18'
TRACERT	'19'
NETSTAT	'1A'
AUDITPRINT	'1B'
SYSLOG	'1C'
UTILCFG	'1D'
UTILENABLE	'1E'
UTISTATS	'1F'
HEALTHENABLE	'20'
HEALTHSTATS	'21'
SNMP	'22'
SNMPADD	'23'
SNMPDEL	'24'
Console Command	Audit Record Command Code
RESET	'25'
ROUTE	'26'
TRAP	'27'
TRAPADD	'28'
TRAPDEL	'11'
CONFIGACL	'2A'

Note: Some of the above Console commands are not currently in use; they are reserved for future use.

Command Code Type 10 – Fraud Event

The command code type 'Fraud Event' represents the fraud detection functions built into the payShield 10K.

When a fraud event is detected, the command code of the command that caused the fraud event to be detected is recorded in the audit record's Command Code field. The Response Error Code field is then set as follows:

Fraud Event	Audit Record Response Code
Limit for number of PIN verifications per minute exceeded	01
Limit for number of PIN verifications per hour exceeded	02
Limit for total number of failed PIN verifications exceeded	03

Command Code Type 11 – User Action

The command code type 'User Action' represents the actions under user control that do not involve a Console or Host command, for example, changing to/from Online, Offline and Secure mode, into/out of authorized state, and power cycling the HSM.

Note: User actions cannot be enabled or disabled individually.

The following table indicates the contents of the Action Code field for each possible User Action:

Audited User Action	Audit Record Action Code
Automatic audit log entry arising from Authorization Cancelled (i.e.single authorized state)	'A0' (zero)
Automatic audit log entry arising from Authorization ON (i.e. singleauthorized state)	'A1'
Automatic audit log entry arising from Authorization Activity ON(i.e. multiple authorized states)	'AA'
Automatic audit log entry arising from Authorization ActivityCancelled (i.e. multiple authorized states)	'AC'
Automatic audit log entry arising from Authorization Timeout	'AT'
Audit log cleared	'CL'
Automatic audit log entry arising from Diagnostic Event (Self test)	'DE'
Automatic audit log entry arising from Key/component Entry at the Console or using a Smart Card to authenticate a user at the Console or payShield Manager.	'KE'
LMK erased	'LE'
License file load failure	'LF'
LMK loaded	'LL'
License file successfully loaded	'LS'
Old LMK erased	'OE'
Change to Offline	'OF'
Old LMK loaded	'OL'
Automatic audit log entry arising from Authorization ActivityCancelled (i.e. multiple authorized states)	'AC'
Automatic audit log entry arising from Authorization Timeout	'AT'
Audit log cleared	'CL'
Automatic audit log entry arising from Diagnostic Event (Self test)	'DE'

Audited User Action	Audit Record Action Code
Automatic audit log entry arising from Key/component Entry at the Console or using a Smart Card to authenticate a user at the Console or payShield Manager.	'KE'
LMK erased	'LE'
License file load failure	'LF'
LMK loaded	'LL'
License file successfully loaded	'LS'
Old LMK erased	'OE'
Change to Offline	'OF'
Old LMK loaded	'OL'
Change to Online	'ON'
Cycle power supply	'PW'
Change to Secure	'SE'
Utilization Reset	'UT'

The Response Code for all User Action records is 00.

15.11.2 Q4 Host command

The Q4 Host command is used to archive Audit Log records to a printer attached to the payShield 10K: a flag is set against the record to indicate that it has been archived in this way.

There are options to print/archive the next non-archived record, to print/archive all non-archived records, or to print/archive all records.

See the *payShield 10K Core Host Command Reference Manual* for a full description of the Q4 command.

15.11.3 payShield Manager Audit Log Screen

As described above, the payShield Manager Audit Log screen on the Status page displays the current contents of the Audit Log. The Download button allows the Audit Log to be saved as a file, which can then be printed if required.

15.12 Retrieving Audit Log entries to the host system

15.12.1 Q2 Host command

The Q2 Host command is used to copy individual Audit Log entries to the host computer system. The command retrieves the next record that has not previously been retrieved by the host.

See the *payShield 10K Core Host Command Reference Manual* for a full description of the Q4 command.

The format of the record is fully described at Appendix B of the *payShield 10K Core Host Command Reference Manual*. It is very similar to that described previously for the printed record, except that:

- 2-digit numeric codes are used in place of the single alphabetic character identifying the event type
- The record includes the Archived and Retrieved status flags

15.12.2 SNMP

Functions are provided when using SNMP to retrieve information about the Audit Log. Please see the section on SNMP in the *payShield 10K Programmer's Guide*.

15.12.3 payShield Monitor

payShield Monitor also allows customers to view information on the Audit Log. Please see the payShield Monitor manuals for more information.

15.13 Deleting records from the Audit Log

It is important that records are deleted from the Audit Log before a significant volume of entries builds up. If the size of the Audit Log grows to multiple thousands of entries, the following will result:

- Performance of executing Host commands will begin to drop
- If the Audit Log reaches its maximum size of 100,000 records there will be a major drop in performance because of the processing required to “rotate” the Audit Log such that the oldest record is deleted to allow the newest record to be added
- The rotation of the Audit Log when it has reached its maximum size results in the oldest records being lost

The payShield 10K user should implement processes to investigate new Audit Log entries, print Audit Log entries or retrieve them to a host system, and then clear the Audit Log.

15.13.1 CLEARAUDIT Console command

The *CLEARAUDIT* Console Command deletes all records in the Audit Log. This command must be authorized, and when used results in a record of the deletion being put into the fresh, otherwise empty Audit Log.

15.13.2 payShield Manager Audit Log Screen

This dialogue box has been discussed earlier in the document. The *Clear* button can be used by Security Officers to delete all Audit Log entries.

15.13.3 Q6 Host command

The Q6 Host command can be used under authorization to delete from the Audit Log either:

- all records previously retrieved to the host, or
- all archived records

15.14 Other Audit Log Management Functions

15.14.1 Translating MAC on LMK Refresh

The MAC calculated on a record uses a MACing key which is encrypted under the LMK. When the LMK is changed, the MACing keys need to be translated to the new LMK. This is done by using the Q0 Host command.

15.14.2 Verifying an Audit Log Record

The MAC on an Audit Log record can be verified by using the Q8 Host command.

16 Performance

16.1 Overview

License Packages are provided with payShield 10K and these define both the functionality and the performance provided. Each License Package (e.g. Classic or Premium) includes a License for a specified performance in terms of calls per second. These vary from 25 cps to 10,000 cps and further information on the performance provided is given below.

Note that the License Packages available are listed in [Section 1.10, “payShield 10K license packages”, on page 11](#) together with the upgrades available to increase performance as required.

16.2 Performance Ratings 25 cps to 2500 cps

The performance for ratings from 25 cps to 2500 cps give an approximate number of calls per second when using Key Blocks and a secure connection configured between the Host and the payShield 10K. The requirements for achieving maximum performance are given in [Section 16.4, “Achieving Maximum Performance”](#) and the exclusions in [Section 16.5, “Host Commands Excluded from Performance Ratings”](#).

The performance ratings are comparable to the payShield 9000 tps rating. Note that the performance of RSA signature generation and verification is greatly enhanced in the payShield 10K when compared to the payShield 9000 and will operate approximately at the calls per second rating of the License.

16.3 Performance Rating 10,000 cps

The performance for rating for 10,000 cps gives an approximate number of calls per second for the host commands listed below.

- CA - Translate a PIN from TPK to ZPK/BDK (3DES DUKPT) Encryption
- CC - Translate a PIN from One ZPK to Another

The performance of the other host commands (excluding those listed in [Section 16.5, “Host Commands Excluded from Performance Ratings”](#) below) are between 2,500 cps and 10,000 cps.

Note:

- The requirements for achieving maximum performance are given in [Section 16.4, “Achieving Maximum Performance”](#). In addition to achieve maximum performance for 10,000 cps, the gathering of Utilization Statistics should be turned OFF.
- 10,000 cps is only available for the Premium package
- The payShield 10K FICON Hardware Platform does not support 10,000 cps

16.4 Achieving Maximum Performance

The performance achieved in practice will depend on environment in which the payShield 10K is operating, including network configuration, network traffic, the Host Application and the Host Platform. In particular, the following aspects should be considered to achieve maximum performance:

- Sufficient multiple threads should be used
- The host interface should have no other traffic
- Command/response processing at the host should not introduce any delays

16.5 Host Commands Excluded from Performance Ratings

The following Host Commands are excluded from the performance ratings:

- Host Commands generating RSA Keys
- Host Commands processing a large amount of data, e.g. commands performing Message Authentication, Message Encryption, Message Hashing

17 Network Time Protocol (NTP)

17.1 Overview

Support for Network Time Protocol (NTP) is provided as an option with payShield 10K instead of using the on-board real time clock. This allows the payShield 10K clock to synchronize to an NTP Server which is typically used by all systems on the network. The alternative is to use the payShield 10K real time clock, which in common with other systems is subject to a level of drift.

payShield 10K includes a time stamp in the Error Log and the Audit log and use of accurate time in these logs can help with determining the correct sequence of events between systems when, for example, an investigation is required. If all the systems included in the investigation use the same time source, then this improves the ability of the investigator to determine the exact sequence of events.

The payShield 10K clock is also used for other less time critical purposes, e.g. to check the validity dates and times of the validity of certificates.

The payShield 10K **MUST** use an NTP Server that is located inside the firewall provided by the data center. The payShield 10K **MUST NOT** use an external NTP Server located on the Internet.

When NTP is configured, it is important to note that the time zone used by payShield 10K will be Universal Time Coordinated (UTC), allowing all systems globally to use the same time zone. The impact this has on existing systems must be taken into account before configuring the use of NTP on a payShield 10K. For example, if the time is set forwards when changing from local to UTC, payShield Manager smart cards issued before the current time in UTC will not be able to be used until the time they were issued is reached in UTC.

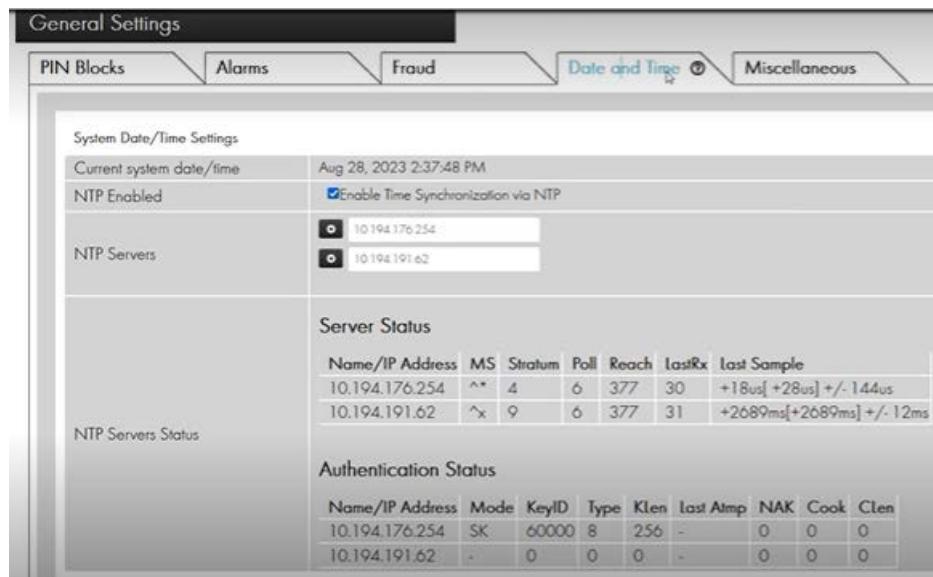
It is important to note that the payShield 10K internal clock must be set to within 15 minutes of the NTP Server in UTC format. The internal clock will not synchronize if the NTP Server is outside this range.

Up to four NTP Servers are supported for redundancy purposes. This allows the time to be taken from another NTP Server should there be a problem connecting with the NTP Server being used.

The network address of the NTP Server is provided using an IP address. The use of Fully Qualified Domain Names (FQDN) is not supported. The management payShield 10K Management port is used for NTP.

To provide a level of authentication, support for symmetric authentication is provided. Here the symmetric key used by the NTP Server is entered into a payShield 10K using payShield Manager (or the Console). A number of algorithms are supported including SHA256, SHA384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, AES128 and AES256. It is recommended that authentication is used, however, if this isn't available the NTP Server can be used without authentication.

NTP is managed using the Date and Time option in the Configuration tab in payShield Manager. This is described in more detail in [Section 9.10.6.4, “Date and Time”, on page 201](#) of this guide. As an alternative, NTP can be managed using the SETTIME command in the Console - for more details please refer to the [*payShield 10K Console Guide*](#). Both payShield Manager and the Console provide detailed information on the NTP status. An example from payShield Manager is shown below and an explanation of the terminology used is given in the following sections:



17.2 Server Status Terminology

Below is an explanation of the terminology used for the Server Status:

Name/IP address

This shows the IP address of the source.

M

This indicates the mode of the source. ^ means a server, = means a peer and # indicates a locally connected reference clock.

S

This column indicates the selection state of the source.

* indicates the best source which is currently selected for synchronization.

+ indicates other sources selected for synchronization, which are combined with the best source.

- indicates a source which is considered to be selectable for synchronization, but not currently selected.

x indicates a source where the time is inconsistent with a majority of other sources.

~ indicates a source whose time appears to have too much variability.

? indicates a source which is not considered to be selectable for synchronization for other reasons (e.g. unreachable, not synchronized, or does not have enough measurements).

Stratum

This shows the stratum of the source, as reported in its most recently received sample. Stratum 1 indicates a computer with a locally attached reference clock. A computer that is synchronized to a stratum 1 computer is at stratum 2. A computer that is synchronized to a stratum 2 computer is at stratum 3, and so on.

Poll

This shows the rate at which the source is being polled, as a base-2 logarithm of the interval in seconds. Thus, a value of 6 would indicate that a measurement is being made every 64 seconds. The polling rate is automatically varied in response to prevailing conditions.

Reach

This shows the source's reachability register printed as an octal number. The register has 8 bits and is updated on every received or missed packet from the source. A value of 377 indicates that a valid reply was received for all from the last eight transmissions.

LastRx

This column shows how long ago the last good sample (which is shown in the next column) was received from the source. Measurements that failed some tests are ignored. This is normally in seconds. The letters m, h, d or y indicate minutes, hours, days, or years.

Last sample

This column shows the offset between the local clock and the source at the last measurement. The number in the square brackets shows the actual measured offset. This can be suffixed by ns (indicating nanoseconds), us (indicating microseconds), ms (indicating milliseconds), or s (indicating seconds). The number to the left of the square brackets shows the original measurement, adjusted to allow for any slews applied to the local clock since. The number following the +/- indicator shows the margin of error in the measurement. Positive offsets indicate that the local clock is ahead of the source.

17.3 Authentication Status Terminology

Name/IP address

This column shows the name or the IP address of the source.

Mode

This column shows which mechanism authenticates NTP packets received from the source. SK means a symmetric key, and - means authentication is disabled.

KeyID

This column shows an identifier of the key used for authentication. With a symmetric key, it is the ID from the key file.

Type

This column shows an identifier of the algorithm used for authentication. With a symmetric key, the following identifiers are applicable:

- 1: SHA256
- 2: SHA384
- 3: SHA512
- 4: SHA3-224
- 5: SHA3-256
- 6: SHA3-384
- 7: SHA3-512
- 8: AES128
- 9: AES256

KLen

This column shows the length of the key in bits.

Last

This column shows how long ago the last successful key establishment was performed. It is in seconds, or letters m, h, d or y indicate minutes, hours, days, or years.

Atmp

This column shows the number of attempts to perform the key establishment since the last successful key establishment. A number larger than 1 indicates a problem with the network or server.

NAK

This column is only used for NTS authentication which is not currently supported.

Cook

This column is only used for NTS authentication which is not currently supported.

CLen

This column is only used for NTS authentication which is not currently supported.

18 SNMP

18.1 Introduction

The payShield 10K supports industry-standard SNMP (Simple Network Management Protocol) to provide information about the payShield 10K's state to external management devices. Information can be obtained from the payShield 10K in two operational modes:

- By the management device polling the payShield 10K to request information
- By the payShield 10K automatically providing an SNMP “Trap” when a significant event has occurred. The use of traps reduces network traffic compared with polling, but some polling will generally still be required, for example to detect if the HSM has been taken offline or has failed.

The information provided by the payShield 10K is defined in its SNMP MIB (Management Information Base). The MIB is provided with the payShield 10K software and can be viewed using a standard text editor.

18.1.1 Security Guidelines for SNMP Configuration

For SNMP configurations, the recommended security guidelines are:

1. Configure SNMP with authPriv.
2. Choose SHA as the Authentication algorithm.
3. Choose AES as Privacy algorithm.
4. Set strong and distinct passwords for Auth and Priv algorithms. The passwords should not be the same. The passwords must be 8 to 19 characters, and should be made up of a combination of alpha-numeric and permitted special character values.

18.2 Network Connectivity

SNMP traffic to and from the payShield 10K can use any one of the following Ethernet ports:

- Management Port
- Auxiliary Port

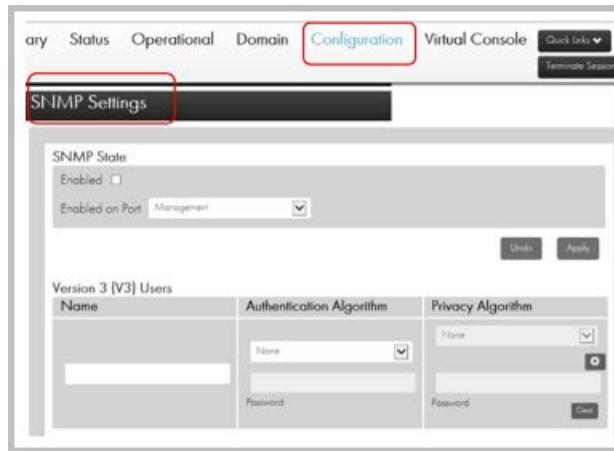
SNMP is enabled/disabled and the desired port selected via the SNMP console command or via payShield Manager.

The ports themselves are configured using the CH, CM, and CA console commands.

payShield Manager users navigate as follows:

- to configure host ports:
 - Configuration / Host Settings
- to configure the management port:

- Configuration / Management Settings.



SNMP traffic to the payShield 10K is received on UDP port 161, and SNMP traffic is sent to a specified UDP port (usually 162) at the management device.

18.3 SNMP Version

The payShield 10K supports SNMP version 3.

Users are set up under a username with details of authentication/privacy algorithms and passwords. This configuration is done using the SNMPADD (or SNMPDEL to delete a User) console command or payShield Manager Configuration / SNMP Settings.

18.4 Configuring Traps

For Traps to be sent by the payShield 10K, both SNMP (e.g., using the SNMP console command) and traps (e.g., using the TRAP console command) must be enabled.

Multiple traps can be configured:

- Current Traps can be viewed using the TRAP console command.
- The UDP port at the management device and the User who is to receive the trap are configured using the TRAPADD console command.
- Traps are deleted using the TRAPDEL console command.

18.5 Information Provided by the payShield 10K through SNMP

Note: Refer to the SNMP MIB provided with the software load for the detailed definition of information available.

18.5.1 Traps Issued by the payShield 10K

A Trap message is issued whenever a test in the daily diagnostic self-tests fails.

The trap is issued using the ps10KDiagnosticTestFailureAlarm MIB object, and the following supporting information is provided:

- The test which has failed is identified in ps10KDiagnosticID.
- The failed test is also described as a string in ps10KDiagnosticString

Note: Refer to the copy of the SNMP MIB that is provided with the software load for additional information.

18.5.2 Tamper

If the payShield 10K detects a tamper, a Trap is sent when the unit restarts.

The Trap is issued as MIB object ps10KTamperAlarm, and the following supporting information is provided:

- Cause of the tamper is reported in ps10KStateTamperCause
- Date and time of the tamper is reported in ps10KStateTamperDate
- Current state of the unit is reported in ps10KStateTamperState

18.5.3 Powering Up

When the payShield 10K is powered up, a Trap is sent using MIB object ps10KPowerOnAlarm.

18.5.4 Use of the Erase Button

When the Erase button on the payShield 10K is used, a Trap is sent using MIB object ps10KEraseAlarm and the following information is provided:

- Date and time of the use of the Erase button is provided in ps10KAlarmEraseTimeandDate

18.5.5 Fraud Detection

If a fraud attempt is detected, a Trap is issued in the ps10KFraudAlarm MIB object. The following supporting information is available:

- Cause of the fraud detection in ps10KFraudType

18.5.6 Installation of a New License

A Trap is issued when an attempt is made to install a new license on the payShield 10K, using MIB object ps10KNewLicenseAlarm.

18.5.7 Installation of New Software

A Trap is issued when an attempt is made to install new software on the payShield 10K, using MIB object ps10KNewSoftwareAlarm.

18.5.8 Power Supply Unit (PSU) Failure

When a PSU failure is detected, a Trap is issued using MIB object ps10KPSUFailureAlarm. Supporting information is:

- Identity of the failed PSU in ps10KPsuNumber

18.5.9 Abnormal Fan Speed

When a fan running at an abnormal rotational speed is detected, a Trap is issued using MIB object ps10KFanAlarm, with the following supporting information:

- Identity (1 or 2) of the abnormal fan in ps10KFanID
- Nature of the abnormality in ps10KFanState

18.5.10 New Error Log Entry

If a new entry is put into the Error Log a trap is issued using MIB object ps10KErrorlogAlarm. The following supporting information is provided:

- New error log entry in ps10KErrorLogData

18.5.11 Invalid or Unexpected Data Received at a Host Port

A Trap is issued if there is a protocol violation in data received at a host port. This is notified in MIB object ps10KHostPortBadDataAlarm. The following supporting information is also provided:

- Physical port involved, in ps10KBadDataPhysicalPort
- Protocol involved in ps10KBadDataProtocol

18.5.12 Actual or Impending Battery Problem

The payShield 10K cannot function if the battery maintaining the volatile memory fails. If the battery fails or is expected to do so shortly a Trap is issued using MIB object ps10KBatteryAlarm. The following supporting information is provided:

- battery state in ps10KBatteryState

18.5.13 Security Settings

Security settings are available via SNMP to enable verification that they are set correctly, as required.

Each setting is given a reference number and the text associated with the current status of each setting is returned.

The Security Settings are only available when the SNMP user is configured to use both authentication and privacy, (i.e., authPriv) – if not an error is returned.

Note that the settings are read only – the security settings cannot be changed using SNMP.

The reference numbers used for the Security Settings when these are retrieved using SNMP are shown in Appendix E, [SNMP MIB Security Settings](#).

19 Remote Syslog

19.1 Summary

A new “Remote syslog” feature is included in payShield 10K software release 2.0a and above. This facilitates the transmission of local error and audit logs to a remote syslog server.

Users can configure up to two remote syslog servers and choose to use either the payShield 10K management or the auxiliary interface.

Additionally, users have the option to utilize the default ports 601 or 514 or select non-default ports within the range of 49300 through 49320 for remote syslog.

Configuration of the feature is undertaken using either payShield Manager or the Console.

19.2 Secure Operation

The user is responsible for securing access from payShield 10K to the remote syslog servers. The user is expected to fully control the remote syslog server, including its security and access control.

TCP is supported for the connection to the remote syslog server. This implies the logs are sent in clear text with no encryption or integrity control. The user is responsible for:

- deploying the payShield 10K and the remote syslog servers in secure networks protected from unauthorized access,
- securing the remote syslog servers, and
- securely storing the logs.

When the remote syslog server is initially configured, we recommend users ensure that the remote syslog server is receiving logs correctly.

The user is responsible for updating the payShield 10K remote syslog settings if the IP address of the remote server changes.

19.3 Configuration

Remote syslog is enabled, and the settings viewed or configured, using either payShield Manager or the Console. To change configuration settings, the payShield 10K must be in the Secure state.

The configuration options are:

- Enable or Disable Remote syslog
- Specify Remote syslog server IP address

- Specify Remote syslog server port (default ports 601 or 514 or non-default ports in the range 49300 through 49320)
- Select payShield 10K interface (either Management or Auxiliary)

When using payShield Cloud HSM, the ability to configure Remote syslog server is provided only to the end user.

Note that connection to the remote syslog server uses TCP. UDP and TLS are not supported.

For payShield Manager, configuration is provided in the Remote syslog tab in the General Settings option in the Configuration Tab. Please refer to the payShield 10K Installation and User Guide, Chapter 9.

For the Console, please refer to the ‘SYSLOG’ Configure Remote Syslog command in the *payShield 10K Console Guide*.

19.4 Operation

When first enabled and configured and a TCP connection to the server is established, all locally stored error and audit logs are sent to the remote syslog server.

Once this is completed, new entries in the error or audit logs are sent to the remote syslog server in real-time.

Error and audit logs sent to the remote syslog server are formatted according to the RFC 5424 specification. The identity of the HSM is typically added to the logs by the Remote syslog server depending on how this is configured by the user.

With Remote syslog enabled, the error and audit logs will continue to be stored locally on the payShield and the existing functionality to view, download, retrieve the log via host commands etc. is not impacted.

Configuration of Remote syslog is audited in the standard way. Audit actions logged include:

- Remote syslog enable/disable
- Remote syslog server add/modify
- Remote syslog server IP address/port change

If payShield 10K is reset to factory settings, the Remote syslog server configuration will return to the default settings.

Appendix A - Console Commands

A full description of the over 80 console commands provided with the payShield 10K are now fully documented in the following manual:

- *payShield 10K Console Guide*

Overview of enabling console commands

All Host commands are disabled by default. Please refer to the *payShield 10K Host Command Manual*.

However, all console commands are enabled by default.

A brief discussion of enabling and disabling console commands follows. Please refer to the *payShield 10K Console Guide* for full command documentation.

- Enabling and disabling console commands:

Command syntax:

<+ or -> C <command code>

Where:

"+" enables and

"-" disables

You can use the wild card character (*) as character 1 or 2 of the <command code>.

For example:

* = all console commands

S* = all console commands that begin with "S"

Multiple commands can be issued with a cumulative effect.

For example:

-C* (disables all console commands)

+CG* (enables all console commands beginning with "G")

Appendix B - Error Log Codes

B.1 General

The error log lists each error with a severity, an error code and a sub-code. The error log only contains the numerical part of the error code and sub-code. Sub-codes relate to a specific error code.

This Appendix describes the Error Log as viewed when using the Console. When viewing the Error log using payShield Manager please refer to the payShield Manager User's Guide.

The text below will make use of the following example of an error log entry:

```
1: Nov 30 00:43:18  ERROR: [Tamper(1) Latched at [2000/00/00, 00:42:57]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
```

B.2 Description

The error description is contained within a pair of square brackets:

```
1: Nov 30 00:43:18  ERROR: [Tamper(1) Latched at [2000/00/00, 00:42:57]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
```

The meaning of some of these descriptions will be obvious (e.g. "[Power Supply: FAILED (PSU 2 Failed)]", whereas the full meaning of some messages will require interpretation by Thales.

B.3 Severity

A severity level is provided by the error message:

```
1: Nov 30 00:43:18  ERROR: [Tamper(1) Latched at [2000/00/00, 00:42:57]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
```

The meaning of the severity level is given in the following table:

No.	Code	Meaning
0	LOG_EMERG	System is unusable.
1	LOG_ALERT	Action must be taken immediately.
2	LOG_CRIT	Critical conditions.
3	LOG_ERR	Error conditions.
4	LOG_WARNING	Warning conditions
5	LOG_NOTICE	Normal but significant condition.
6	LOG_INFO	Informational.
7	LOG_DEBUG	Debug-level message.

B.4 Error Codes

The error log entry includes a main error code:

1: Nov 30 00:43:18 ERROR: [Tamper(1) Latched at [2000/00/00, 00:42:57]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)

The main error code indicates the general source of the error, as per the following table:

No.	Shown as ...	Code	Meaning
1	0x00000001	LS_UTIL	Utility system
2	0x00000002	LS_CRYPTO	Cryptographic system
3	0x00000003	LS_APP	Application system
4	0x00000004	LS_KEYMGR	Key Manager system
5	0x00000005	LS_ENCFS	Encrypted File System

B.5 Sub-Codes

The error log entry also includes a sub-code to provide a more detailed source of the error:

1: Nov 30 00:43:18 ERROR: [Tamper(1) Latched at [2000/00/00, 00:42:57]] (Severity: 2,
Code = 0x00000004, **Sub-Code = 0x00000000**)

The value of sub-codes depends on the value of the main error code, as described in the tables below. A value of **0x00000000** indicates that a more detailed sub-code is not appropriate.

B 5.1 Sub-Codes for Main Error Code = 1 (Utility System Errors)

No.	Shown as ...	Code	Meaning
1	0x00000001	LSS_UTIL_CONFIG	Configuration utility sub-system
2	0x00000002	LSS_UTIL_UNUSED	Deprecated (was Encrypted File utility sub-system)
3	0x00000003	LSS_UTIL_I2C	I2C utility sub-system
4	0x00000004	LSS_UTIL_INCOMINGD	Incoming daemon utility sub-system
5	0x00000005	LSS_UTIL_LED	LED utility sub-system
6	0x00000006	LSS_UTIL_NAMESPACE	Namespace utility sub-system
7	0x00000007	LSS_UTIL_PATCH	Program patch utility sub-system
8	0x00000008	LSS_UTIL_PROC	Process manager utility sub-system
9	0x00000009	LSS_UTIL_PSHAPE	Performance shaping utility sub-system
10	0x0000000A	LSS_UTIL_SMARTCARD	Smartcard utility sub-system
11	0x0000000B	LSS_UTIL_SPARTAN	Spartan FPGA management utility sub-system
12	0x0000000C	LSS_UTIL_SWITCH	User switch (push-button & keylock) utility sub-system
13	0x0000000D	LSS_UTIL_SYSID	System ID utility sub-system
14	0x0000000E	LSS_UTIL_UPDATER	System update utility sub-system
15	0x0000000F	LSS_UTIL_SHMEM	Shared memory utility sub-system
16	0x00000010	LSS_UTIL_LICENSING	License management utility sub-system
17	0x00000011	LSS_UTIL_SCR	Smartcard Reader utility sub-system
18	0x00000012	LSS_UTIL_EEPROM	Resident configuration utility sub-system
19	0x00000013	LSS_UTIL_MEM	Memory utility sub-system
20	0x00000014	LSS_UTIL_EVENT	Event manager utility sub-system
21	0x00000015	LSS_UTIL_THREADPOOL	Thread-pool manager utility sub-system
22	0x00000016	LSS_UTIL_COOKIE	Cookie manager

B 5.2 Sub-Codes for Main Error Code = 2 (Cryptographic System Errors)

No.	Shown as ...	Code	Meaning
1	0x00000001	LSS_CRYPTO_DES	DES cryptographic sub-system
2	0x00000002	LSS_CRYPTO_RNG	Random number generator cryptographic sub-system
3	0x00000003	LSS_CRYPTO_SHA	SHA cryptographic sub-system
4	0x00000004	LSS_CRYPTO_SEC	Security engine cryptographic sub-system
5	0x00000005	LSS_CRYPTO_RMAPI	Resource management API cryptographic sub-system
6	0x00000006	LSS_CRYPTO_RM_SEC	Resource management security engine cryptographic sub-system
7	0x00000007	LSS_CRYPTO_RM_SW	Resource management software cryptographic sub-system
8	0x00000008	LSS_CRYPTO_RSA	RSA cryptographic sub-system
9	0x00000009	LSS_CRYPTO_BIGINT	Big integer cryptographic sub-system
10	0x0000000A	LSS_CRYPTO_ESS	ESS API cryptographic sub-system
11	0x0000000B	LSS_CRYPTO_AES	AES cryptographic sub-system
12	0x0000000C	LSS_CRYPTO_HASH	Hash cryptographic sub-system

B 5.3 Sub-Codes for Main Error Code = 3 (Application System Errors)

No.	Shown as ...	Sub-code	Meaning
1	0x00000001	LSS_APP_DIAG	Diagnostic application sub-system
2	0x00000002	LSS_APP_AUTH	Authorization application sub-system
3	0x00000003	LSS_APP_LMK	LMK application sub-system
4	0x00000004	LSS_APP_COMMWS	Communications (TCP, UDP, Async, FICON) application sub-system
5	0x00000005	LSS_APP_GENERAL	General application sub-system
6	0x00000006	LSS_APP_AUDITLOG	Audit log application sub-system
7	0x00000007	LSS_APP_CONFIG	Configuration application sub-system
8	0x00000008	LSS_APP_CONSOLE	Console application sub-system
9	0x00000009	LSS_APP_HOSTCMD	Host command application sub-system
10	0x0000000A	LSS_APP_PINBLOCK	PIN block application sub-system
11	0x0000000B	LSS_APP_USRSTORE	User storage application sub-system
12	0x0000000C	LSS_APP_CHIPCARD	Chip card application sub-system
13	0x0000000D	LSS_APP_DES	DES application sub-system
14	0x0000000E	LSS_APP_FRAUD	Fraud application sub-system
15	0x0000000F	LSS_APP_KEYBLOCK	Key Block application sub-system
16	0x00000010	LSS_APP_KEYMAN	Key manager application sub-system
17	0x00000011	LSS_APP_MAC	MAC application sub-system
18	0x00000012	LSS_APP_MGMT	payShield Manager application sub-system
19	0x00000013	LSS_APP_PARSE	Parsing application sub-system
20	0x00000014	LSS_APP_PRINT	Printing application sub-system
21	0x00000015	LSS_APP_RSA	RSA application sub-system
22	0x00000016	LSS_APP_VISA	VISA application sub-system
23	0x00000017	LSS_APP_VPN	VPN for remote management application sub-system
24	0x00000018	LSS_APP_X509CERT	X.509 certificate application sub-system
25	0x00000019	LSS_APP_STATE	System state application sub-system
26	0x0000001A	LSS_APP_POWER	Power management application sub-system
27	0x0000001B	LSS_APP_STORAGE	Storage application sub-system
28	0x0000001C	LSS_APP_COMMANDS	Command processing application sub-system
29	0x0000001D	LSS_APP_DIGEST	Digest application sub-system

No.	Shown as ...	Sub-code	Meaning
30	0x0000001E	LSS_APP_LICENSE	Licensing application sub-system
31	0x0000001F	LSS_APP_UTILIZATION	Utilization application sub-system
32	0x00000020	LSS_APP_SNMP	SNMP application sub-system

B 5.4 Sub-Codes for Main Error Code = 4 (Key Manager System Errors)

There are currently no sub-codes.

B 5.5 Sub-Codes for Main Error Code = 5 (Encrypted File System Errors)

There are currently no sub-codes.

B.6 Multiple Entries

A single cause may result in multiple entries being made in the error log. The following example arises from a triggering of the temperature alarm, which initiates a tamper condition:

```
PayShield 10K Error Log
-----
1: Nov 30 00:43:18  ERROR: [Tamper(1) Latched at [2000/00/00, 00:42:57]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
2: Nov 30 00:43:18  ERROR: [Tamper Latched State [LR1 = 0x0004, LR2 = 0x0000]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
3: Nov 30 00:43:18  ERROR: [ Tamper LR1 [0x0004 = Temperature exceeded maximum
operational range]] (Severity: 2, Code = 0x00000004, Sub-Code = 0x00000000)
4: Nov 30 00:43:18  ERROR: [Tamper Current State [CR1 = 0x0004, CR2 = 0x8000]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
5: Nov 30 00:43:40  ERROR: [Tamper(2) Latched at [2000/00/00, 00:43:19]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
6: Nov 30 00:43:41  ERROR: [Tamper Latched State [LR1 = 0x0004, LR2 = 0x0000]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
7: Nov 30 00:43:41  ERROR: [ Tamper LR1 [0x0004 = Temperature exceeded maximum
operational range]] (Severity: 2, Code = 0x00000004, Sub-Code = 0x00000000)
8: Nov 30 00:43:41  ERROR: [Tamper Current State [CR1 = 0x0004, CR2 = 0x8000]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
9: Nov 30 00:43:41  ERROR: [ Tamper CR1 [0x0004 = Temperature exceeded maximum
operational range]] (Severity: 2, Code = 0x00000004, Sub-Code = 0x00000000)
10: Nov 30 00:43:41  ERROR: [ Tamper CR2 [0x8000 = DS3640 TEI asserted]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
```

```
11: Nov 30 00:43:41  ERROR: [Tamper State is 0x0004 and retry count exceeded (2)]  
(Severity: 2, Code = 0x00000004, Sub-Code = 0x00000000)  
12: Nov 30 00:43:47  ERROR: [Temperature:      FAILED - temperature too high ] (Severity:  
3, Code = 0x00000001, Sub-Code = 0x0000000E)
```

The messages show that a tamper event occurred and is still ongoing. The value of "0x0004" for the LR1 and CR1 elements indicate that the tamper cause was the temperature rising above the maximum acceptable level; a value of "0x0002" would have indicated a temperature that was too low.

Appendix C - Commission payShield Manager using Console commands

This chapter describes how to commission a payShield 10K using Console commands.

Note: payShield Manager for payShield 10K is usually commissioned remotely. However if for any reason the payShield 10K is no longer warranted, the Console can be used to set up payShield Manager as described in this section.

C.1 Background information

The payShield relies on a trust model with 2 parallel key hierarchies consisting of key material and signed certificates installed at the Thales factory (the Pre-placed Trust) and key material and signed certificates locally or remotely installed by the customer (i.e., the Customer Trust Authority or CTA).

Key management material on an HSM can be in one of two states:

- Warranted
 - The payShield only has the Pre-placed Trust. This is the factory default state. A unit will return to this state upon tamper.
- Commissioned
 - The payShield has Customer Trust (i.e., the customer has placed trust elements on the HSM).

The Pre-placed Trust is only used to facilitate the secure, authenticated loading of Customer Trust in a remote environment. Once Customer Trust is installed in an HSM, it is considered Commissioned and management operations can be used.

Follow the steps in the following checklist to ready the payShield for use.

Table 4 *Installation Checklist*

Step	Tasks
1.	Secure the HSM
2.	Generate a Customer Trust Authority
3.	Create the HRK passphrases
4.	Commission the HSM
5.	Commission Smart Cards
6.	Migrate LMK Cards to become RLMK Cards

C.2 Prerequisites

- The Remote payShield Manager license (i.e., PS10-LIC-RMGT) is installed.

- A payShield HSM is connected via the Management Port to a secure WAN.
- You are using DHCP to connect and you know the IP address of the HSM.
- A laptop/desktop PC with access to an Internet browser, e.g., Chrome, Microsoft Edge, Firefox.
- A sufficient number (to meet the requirements established in your organization's security policies) of payShield Manager Smart Cards formatted for LMK type cards.
- The trusted officers, that will hold the shares in the Customer Trust Authority, are present.

C.3 Procedure

All commands are entered via the console terminal.

C3.1 Secure the HSM

1. Place the HSM in the Secure state.
 - Place the keys in the locks located on the front of the unit.
 - Turn the keys to the locked position.



C3.2 Generate a Customer Trust Authority

The XI Console command generates the Customer Trust Authority. The shares are then stored on the Smart Cards.

Note: The presence of the trusted officers is required.

1. Place the HSM in the Secure state.
 - Place the keys in the locks located on the front of the unit.
 - Turn the keys to the locked position.
2. At the prompt, enter **XI** and press **ENTER**.

Secure> **XI** <ENTER>

Follow the prompts and enter appropriately.

```
Secure> XI <Return>
Please enter the certificate Subject information:
Country Name (2 letter code) [US]: US <Return>
State or Province Name (full name) []: Florida <Return>
Locality Name (eg, city) []: Plantation <Return>
Organization Name (eg, company) []: Thales <Return>
Organizational Unit Name (eg, section) []: Production <Return>
Common Name (e.g. server FQDN or YOUR name) [CTA]: CTA <Return>
Email Address []: info@thalesesec.com <Return>
Enter number of Customer Trust Authority private key shares [3-9]: 3
<Return>
Enter number of shares to recover the Customer Trust Authority private
key [3-3]: 3 <Return>
Issued to: CTA, Issued by: CTA
Validity : Jan 9 10:28:49 2015 GMT to Jan 3 10:28:49 2040 GMT
Unique ID: EE3CB7CE8343B464CC04278188CF7EB3 - 3DE05514 (Root)
Insert payShield Manager Smart Card 1 of 3 and press ENTER: <Return>
Enter new PIN for smart card: ***** <Return>
Re-enter new PIN: ***** <Return>
Working....
CTA share written to smart card.
Insert payShield Manager Smart Card 2 of 3 and press ENTER: <Return>
Enter new PIN for smart card: ***** <Return>
Re-enter new PIN: ***** <Return>
Working....
CTA share written to smart card.
Insert payShield Manager Smart Card 3 of 3 and press ENTER: <Return>
Enter new PIN for smart card: ***** <Return>
Re-enter new PIN: ***** <Return>
Working....
CTA share written to smart card.
Successfully generated a Customer Trust Authority
Secure>
```

Notes:

- The Country, State, Locality, Organization, Common Name, and Email parameter values are those that are included in the X.509 certificate corresponding to the CTA. The Common Name is the only required parameter and it should concisely describe the security domain.
- Enter the number of Customer Trust Authority private key shares you wish to create.
This is the number of Smart Cards onto which the CTA shares will be distributed.
Valid values are: 3-9.
- Enter the number of shares to recover the Customer Trust Authority private key.
This is the number of Smart Cards holding CTA shares that must be present in order to reassemble a CTA to perform various operations (including commissioning a payShield).
The minimum value is: 3.

The payShield will display information regarding the Customer Trust Authority that was just created and prompt you to store the CTA components onto Smart Cards.

```
Issued to: Group1, Issued by: Group1
Validity : Apr 9 07:02:16 2015 GMT to Apr 2 07:02:16 2040 GMT
Unique ID: B07EA9A049325E02BF84B48A3644CCC3 - 702788CA (Root)
Insert payShield Manager Smart Card 1 of 3 and press ENTER:
```

- Follow the on-screen directions:
 - One by one, place a Smart Card into the integrated reader of the HSM.
 - Each officer should create a PIN and the HSM will write a share of the CTA to the Smart Card.

Note: If the Smart Cards were previously commissioned, it will prompt you for the current PIN.

Upon completion, the following message displays:

```
Successfully generated a Customer Trust Authority
```

C3.3 Create the HRK passphrases

The SK Console command generates a new HSM Recovery Key (HRK). Once installed, the HRK is used to back-up secret key material inside the HSM into persistent memory. This back-up process is known as “key synchronization”.

This process backs up the following secret key material:

- Secure Host Communications key material:
 - HSM's private key
- Remote Management key material:
 - HSM's private key
 - HSM's public key certificate
 - CA public key certificate

The HMK is used to encrypt the HSM's private key. The HSM uses the HSM's private key when establishing the TLS/SSL session.

1. At the prompt, enter **SK** and press **ENTER**.

Secure> **SK** <ENTER>

Example:

```
Secure> SK <Return>
***** NOTE *****
Passphrase rules as follows:
1 - Must be between 8 and 30 characters long.
2 - Can contain spaces
3 - Must be comprised of (at a minimum):
2 digits
2 uppercase characters
2 lowercase characters
2 symbols (e.g. !/?.#:'')
Enter administrator 1 passphrase: ****
Re-enter administrator 1 passphrase: ****
Enter administrator 2 passphrase: ****
Re-enter administrator 2 passphrase: ****
Creating HRK. Please, wait ... DONE
Successfully generated an HRK
Secure>
```

Notes:

- When prompted, create two passphrases.

Passphrases require the following:

- At least 2 upper case characters (e.g., AA)
- At least 2 lower case characters (e.g., aa)
- At least 2 numbers (e.g., 11)
- At least 2 special characters (e.g., !!)

You will enter both passphrases twice. Upon completion, the unit will set the HMK passphrase.

The first time the unit is turned on, the HRK is generated with default passphrases. The passphrase can be the same among one or more payShields based upon your organization's security policy.

C3.4 Commission the HSM

The XH Console command commissions the factory warranted HSM.

Note: The presence of two trusted officers is required along with the following:

- The Customer Trust Authority Smart Cards (i.e., the CTA cards that you just created)

- Two payShield Manager Smart Cards (different than the CTA shares)

Note: These Smart Cards will be used as the Left and Right RACCs that replace both the physical keys on the front panel and the trusted officers. The cards can be key RACCs used for other HSMs in the same security domain.

The same Left and/or Right RACCs can be used in several payShields.

Note: Trust equates to access. You need the CTA cards to obtain access and then you use the other cards to change the lock state of the HSM.

1. At the prompt, enter **XH** and press **ENTER**.

Secure> **XH** <ENTER>

One by one, insert and assign a PIN for each Smart Card.

The HSM creates the CTA private key.

Example:

```
Secure> XH <Return>
Please have all Customer Trust Authority (CTA) payShield Manager smart
cards available
Insert first CTA payShield Manager Smart Card and press ENTER: <Return>
Enter PIN: ***** <Return>
Insert CTA payShield Manager Smart Card 2 of 3 and press ENTER: <Return>
Enter PIN: ***** <Return>
Insert CTA payShield Manager Smart Card 3 of 3 and press ENTER: <Return>
Enter PIN: ***** <Return>
Starting the commissioning of the HSM process...
Please insert left key card and press ENTER: <Return>
Enter PIN: ***** <Return>
Please insert right key card and press ENTER: <Return>
Enter PIN: ***** <Return>
Successfully commissioned HSM
Secure>
```

Notes:

- Insert the left Smart Card and press **ENTER**.

This card becomes the left RACC.

- Insert the right Smart Card and press **ENTER**.

This card becomes the right RACC.

These are used to access the payShield after completing the commissioning procedure. These also replace the physical keys that put the payShield into the **Offline** or **Secure** state.

If the Smart Card has been previously commissioned with a different CTA (security domain), the system will query for confirmation prior to proceeding to erase and reprogram with the current CTA.

Upon completion, the following message displays:

Successfully commissioned HSM.

payShield Manager can now provide remote access to the HSM.

C3.5 Commission Smart Cards

Note: All cards used remotely must be commissioned prior to use. This includes the following:

- RLMK cards
- Authorizing Officer cards
- Restricted cards
- Administrator cards (both Right and Left cards)

1. From the payShield Manager landing page, Click **Login**.

2. Follow this link to continue: [Section 9.9.2.1, “Commission a Smart Card”, on page 165](#).

Note: A link is provided to return you to the section below.

C3.6 Migrate LMK Cards to become RLMK Cards

The XT Console command transfers an existing HSM LMK stored on legacy Thales Smart Cards to payShield Manager RLMK cards for use through the payShield Manager.

In order to transfer a Variant LMK you will be required to fully reassemble the LMK (bring all the components together). Then, the fully formed Variant LMK is split among shares onto the pre-commissioned payShield Manager RLMK cards.

For Key Block LMKs, they are not stored as components on non-payShield Manager Smart Cards, but as shares. However, you must bring a quorum of share holders together, reconstitute the LMK, and then split it among shares onto the pre-commissioned payShield Manager RLMK cards.

1. At the prompt, enter **XT** and press **ENTER**.

Follow the prompts and enter appropriately.

Example:

```
Secure> XT <Return>
Please have all the local LMK components and enough commissioned RACCs
to receive the LMK ready.
Insert card and press ENTER: <Return>
Enter PIN: ***** <Return>
Check: 268604
Load more components? [Y/N]: N <Return>
LMK Check: 268604
LMK key scheme: Variant
LMK algorithm: 3DES(2key)
LMK status: Test
Is this the LMK you wish to transfer? [Y/N]: Y <Return>
Enter the number of shares to split the LMK into: [2-9]: 2 <Return>
The number of shares required to reconstitute the LMK is fixed for
variants: 2 <Return>
Insert a commissioned card 1 of 2 and press ENTER: <Return>
Enter PIN: ***** <Return>
Card Check: E0CBF4
LMK share written to smart card.
Insert a commissioned card 2 of 2 and press ENTER: <Return>
Enter PIN: ***** <Return>
Card Check: E0CBF4
LMK share written to smart card.
Want to test the reassembly of the LMK? Y <Return>
Please have all the RLMK shares ready
Insert RLMK card and press ENTER: <Return>
Enter PIN: ***** <Return>
```

Appendix D - Audit Log Messages

The following table lists all of the Audit Log messages.

Category	Audit Log Messages	Notes
Access Control List (ACL)	TCP/TLS connection from x.x.x.x to y.y.y.y refused due to ACL UDP traffic from x.x.x.x to y.y.y.y refused due to ACL	<i>Optional (controlled by "Audit ACL connection failures" audit option; Disabled by default)</i> x.x.x.x - source IP address y.y.y.y - destination IP address (Host 1 or Host 2)
Audit log	Audit log was cleared Cleared all retrieved audit logs Cleared all archived audit logs	
Authentication	Authentication cmd XX executed	"XX" is the authentication related console command (such as CO, KD, SP, XD, XH, XR) that was executed
Authorization	Activity A was authorized for LMK id 0-19 Activity A:T was authorized for LMK id 0-19 Authorization activity A:T was cancelled Authorization activity A was cancelled for LMK id 0-19 Authorization activity A:T has expired for LMK id 0-19 HSM was authorized for LMK id 0-19 HSM authorization was cancelled for LMK id 0-19	A - activity list, T - timeout
Bootup	System Restarted	
Console command	Console command XX	"XX" is the console command that was executed Audit of desired console commands is done via "auditoptions" console command or via payShield Manager Security sensitive console commands are always audited.
Commissioning	HSM commissioned HSM decommissioned HSM commission failed; error "error message"	
Diagnostics	Diagnostic self tests passed Diagnostic self test failure: "test name"	<i>Optional (controlled by "Audit diagnostic self tests" audit option; Disabled by default)</i> "test name" is name of the failed diagnostic self test
Firmware update	Firmware update attempted Firmware update package validation failed Firmware update failed Firmware update to revision XXXX-XXXX and bootstrap version y.y.y successful/failed	"Firmware update failed" is generated when firmware update fails and version info is not available (such as package validation failure) Where XXXX-XXXX is the firmware revision If bootstrap was present in the update package, "and bootstrap version y.y.y" is included in the log (where y.y.y is the bootstrap version)

Category	Audit Log Messages	Notes
Fraud	Fraud event detected executing Host command XX - Limit of number of PIN verification failures per minute exceeded Fraud event detected executing Host command XX - Limit of number of PIN verification failures per hour exceeded Fraud event detected executing Host command XX - PIN attack limit exceeded	"XX" is the Host command that was executed
FRU (Field Replaceable Units - fans, PSUs)	FAN 1/2 removed FAN 1/2 restored Fan 1/2 replaced: "fru serial number" Power Supply 1/2 removed Power Supply 1/2 restored Power Supply 1/2 replaced: "fru serial number" Power Supply 1/2 AC outage Power Supply 1/2 AC restored	"fru serial number" is the FRU serial number
Health	Health Check Statistics reset to 0	
Host command	Host command XX Host command XX, response EE	Audit of desired Host commands is done via "auditoptions" console command or via payShield Manager <i>Optional (controlled by "Audit Error Responses to Host Commands" audit option; Disabled by default)</i> XX is the Host command EE is the error response to the Host command
Key Management	Smartcard activated: "card serial number" Smartcard PIN changed Key management command XX executed Loaded CTA share from smartcard Stored CTA share on smartcard Smartcard serial number read error	"card serial number" is the Smart Card serial number XX is the key management command that was executed
Keylock	Keylock turned to Online/Offline/Secure	
Licensing	New license file loaded License file load failed	
LMK	LMKs loaded LMKs erased Keychange LMKs loaded Keychange LMKs erased	
Maintenance	payShield "device serial number" maintenance light switch ON/OFF	"device serial number" is the 10K device serial number

Category	Audit Log Messages	Notes
Management	<p>Format of the audit logs for payShield Manager commands is as follows:</p> <p>Remote (xxxxxxxx) - "command string" - Current users: (None / Left: SSSS / Right: SSSS / Guest: SSSS)</p> <p>xxxxxxxx is the session cookie id SSSS is the card serial number</p> <p>Below are the various management command strings/messages when the command is successful. A few of these are configurable (enabled/disabled via payShield Manager Audit Settings).</p> <p>HSM state changed to Online/Offline/Secure Login / Logout Session terminated Single authorized state entered Single authorized state cancelled</p> <p><continued next page></p>	<p>Security sensitive management actions/commands are always audited.</p> <p>"Current Users:" will list all the logged in users.</p>

Category	Audit Log Messages	Notes
Management	CTA generated CTA share read from smartcard (optional - disabled by default) CTA share loaded from smartcard (optional - disabled by default) CTA share created on smartcard CTA share stored on smartcard RACC commissioned Left RACC prepared for commissioning Right RACC prepared for commissioning Key RACC for commissioning prepared HSM commissioned Periodic self diagnostic tests schedule changed Diagnostic tests executed Alarm settings modified HSM date and time updated PIN block settings modified Fraud settings modified Fraud detection re-enabled Enabled Host commands modified Enabled console commands modified Audit settings modified Host commands audit modified Console commands audit modified Remote management commands audit modified Health statistics report generated (optional - disabled by default) Health statistics reset (optional - disabled by default) HRK passphrase set HRK passphrase 1 changed HRK passphrase 2 changed General Host settings modified Ethernet Host settings modified ACL Host settings modified Error log cleared Error log retrieved (optional - disabled by default) Error log downloaded (optional - disabled by default) Audit log cleared <continued on next page>	

Category	Audit Log Messages	Notes
Management (continued)	Audit log retrieved (optional - disabled by default) Audit log downloaded (optional - disabled by default) New LMK installed / deleted Keychange old LMK installed Keychange new LMK installed Keychange LMK deleted LMK generated LMK copied LMK verified Authorizing officer card created Management interface settings modified Printer settings modified (optional - disabled by default) Test page printed (optional - disabled by default) General security settings modified Initial security settings modified SNMP state changed (optional - disabled by default) SNMP port changed (optional - disabled by default) SNMP user added (optional - disabled by default) SNMP user deleted VR info retrieved (optional - enabled by default) Licensing info retrieved (optional - disabled by default) Firmware update attempted License updated (optional - enabled by default) Utilstats settings modified (optional - disabled by default) Utilstats state changed (optional - disabled by default) Utilstats reset (optional - disabled by default) Miscellaneous settings modified (optional - disabled by default) Multiple authorized state changed Whitelist modified Session timeout settings modified Management TLS certificate imported Host TLS certificate imported LMK share loaded LMK share stored LMK split LMK reassembled LMK password loaded LMK password stored HSM settings loaded from smartcard HSM settings saved to Smart Card (optional - enabled by default) HSM settings reset to factory state HSM rebooted Failure audit logs are generated for most of the above commands/actions when the command fails: Login / Logout failed Failed to generate CTA Failed to read CTA share from smartcard Failed to load CTA share from smartcard Failed to create CTA share on smartcard Failed to store CTA share on smartcard Failed to commission RACC Failed to prepare left RACC for commissioning Failed to prepare right RACC for commissioning <continued next page>	

Category	Audit Log Messages	Notes
Management (Continued)	Failed to commission HSM Failed to update license Failed to set HRK passphrases Failed to change HRK passphrase 1 Failed to change HRK passphrase 2 Failed to update HSM date and time Failed to install keychange old LMK Failed to delete new LMK Failed to generate LMK Failed to copy LMK Failed to verify LMK Failed to load LMK share Failed to store LMK share Failed to split LMK Failed to reassemble LMK Failed to create authorizing officer card Failed to import management TLS certificate Failed to import Host TLS certificate Failed to load HSM settings from smartcard Failed to save HSM settings to smartcard Failed to reset to HSM settings to factory state Failed to enter single authorized state Failed to modify whitelist	
Reboot	System rebooted due to firmware update System rebooted due to management request System rebooted due to critical diagnostic test failure - “failed test name”	
Secure Host Comms	Certificate not yet valid. Unique ID: “Cert ID” Certificate has expired. Unique ID: “Cert ID” Error in Cert. Not Before Field. Unique ID: “Cert ID” Error in Cert. Not After Field. Unique ID: “Cert ID”	“Cert ID” is the certificate's unique ID
Settings	HSM settings saved to smartcard HSM settings loaded from smartcard HSM settings saved to smartcard (remote) HSM settings loaded from smartcard (remote)	“(remote)” refers to settings save/restore from payShield Manager
SNMP	SNMP user added/deleted SNMP trap receiver added/deleted	
Tamper	Tamper Detected “tamper text” High Tamper Detected “tamper text” Tamper Cleared	“tamper text” provides tamper details
Utilization	Utilization Statistics reset to 0	Optional (controlled by “Audit utilization data resets” audit option; Enabled by default)

Appendix E - SNMP MIB Security Settings

A full description of the Security Settings retrieved using SNMP is provided in the *payShield 10K Security Manual*, in the section titled: “Security Parameter Descriptions”.

Serial no.	Security Setting	OID
1	Echo:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.1
2	User storage key length:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.2
3	Display general information on payShield Manager Landing Page:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.3
4	Default LMK identifier:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.4
5	Management LMK identifier:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.5
6	Solicitation batch size:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.6
7	Enable settings per LMK:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.7
8	PIN length:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.8
9	Encrypted PIN length:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.9
10	Atalla ZMK variant support:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.10
11	Enforce Atalla variant match to Thales key type:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.11
12	Transaction key support:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.12
13	Select clear PINs:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.13
14	Enable ZMK translate command:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.14
15	Enable X9.17 for import:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.15
16	Enable X9.17 for export:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.16
17	ZMK length:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.17
18	Decimalization tables:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.18
19	Decimalization table checks:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.19
20	PIN encryption algorithm:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.20
21	Use deprecated proprietary format (Tag J) when using PIN Blocks under AES Key Block LMK:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.21
22	Authorized State required when importing a key under an RSA key:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.22
23	Minimum HMAC length in bytes:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.23
24	Enable PKCS#11 import and export for HMAC keys:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.24
25	Enable ANSI X9.17 import and export for HMAC keys:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.25

Serial no.	Security Setting	OID
26	Enable ZEK/TEK encryption of ASCII data or Binary data or None:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.26
27	Restrict key check values to 6 hex chars:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.27
28	Return PIN Length in PIN Translation Response:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.28
29	Enable multiple authorized activities:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.29
30	Allow persistent authorized activities:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.30
31	Enable variable length PIN offset:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.31
32	Enable weak PIN checking:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.32
33	Check new PINs using global list of weak PINs:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.33
34	Check new PINs using local list of weak PINs:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.34
35	Check new PINs using rules:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.35
36	Enable PIN block Format 34 as output format for PIN translations to ZPK:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.36
37	Enable translation of account number for LMK encrypted PINs:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.37
38	Use HSM clock for date/time validation:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.38
39	Additional padding to disguise key length:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.39
40	Key export and import in trusted format only:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.40
41	Protect MULTOS cipher data checksums:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.41
42	Enable Key Scheme Tag 'X' (X9.17) for storing keys under LMK:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.42
43	Enable use of Tokens in PIN Translation:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.43
44	Enable use of Tokens in PIN Verification:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.44
45	Enable PIN Translation to BDK Encryption:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.45
46	Ensure LMK Identifier in command corresponds with host port:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.46
47	Ignore LMK ID in Key Block Header:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.47
48	Enable import and export of RSA Private keys:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.48
49	Enable import of a ZMK:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.49
50	Enable export of a ZMK:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.50
51	Prevent single-DES keys masquerading as double or triple-length keys:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.51
52	Single-DES:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.52
53	Card/password authorization (local):	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.53
54	Restrict PIN block usage for PCI HSM Compliance:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.54

Serial no.	Security Setting	OID
55	Enforce key type 002 separation for PCI HSM compliance:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.55
56	Enforce Authorization Time Limit:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.56
57	Enforce Multiple Key Components:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.57
58	Enforce PCI HSMv3 Key Equivalence:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.58
59	Enforce minimum key strength of 1024-bits for RSA signature verification:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.59
60	Enforce minimum key strength of 2048-bits for RSA:	.1.3.6.1.4.1.4096.2.2.10000.15.7.1.2.60

Technical Support Contacts

Our team of knowledgeable and friendly support staff are available to help. If your product is under warranty or you hold a support contract with Thales, do not hesitate to contact us using the link below. For more information, consult our standard Terms and Conditions for Warranty and Support.

<https://supportportal.thalesgroup.com/csm>



Contact us

For all office locations and contact
information, please visit
cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <

