

payShield Manager

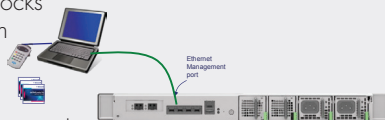
Quick start guide | MKT00011-00-02

THALES

thalessecurity.com

Prerequisites:

- payShield 10K is installed in the rack
- Your laptop is connected to the payShield 10K Management port via Ethernet
NOTE: The Remote payShield Manager license, (PS10-LIC-RMGT), provides the option to connect to the payShield 10K remotely.
- The payShield 10K key locks are in the locked position putting the HSM in the ONLINE state
- Your security officers are present
- At least 5 smart cards are readily available



Notes:

- The payShield 10K is configured to use DHCP on the Management port by default. The default network interface name is "<serial number>-mgmt". For example, if the unit's serial number is A4665000014P, then the default name would be A4665000014P-mgmt
- You may need to use the "Configure Management" port ('CM') command from the local console as described in the *payShield 10K Installation and User Guide* to change the method in which it obtains an IP address and to set the IP address to an address compatible with your organization's internal network

Smart card reader driver:

You may need to download the driver for your smart card reader

For the **cyberJack® secoder (USB)**:

1. Follow this link: www.reiner-sct.com/lang/en/support/support-anfrage/?product=77304824&productGroup=77304735#choice3

2. Click **Driver downloads**

For the **HID® OMNIKEY® smart card reader**:

1. Follow this link: www.hidglobal.com/drivers

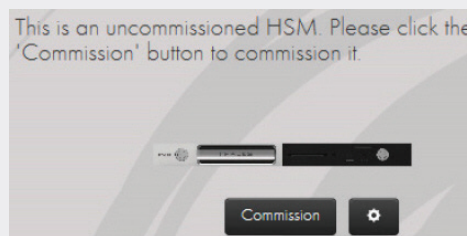
2. Select brand: OMNIKEY

3. Select product: OMNIKEY 3821 USB CARD READER

4. Click based on the appropriate operating system

Procedure:

- From your browser, enter the DHCP name or IP address associated with your payShield 10K Management port
- On the Welcome page: Click **Commission**
NOTE: If logistical work is needed, you will be prompted. Follow the prompts as directed:
 - Install the Extension Component
 - Enable the Extension Component
 - Install the Local Application ComponentThe system displays:



- Click the tool icon
- Click **Configure card reader**
- Select appropriate card reader and click **Done**. You are returned to the Welcome page
- Click **Commission**
- Expand **Create New Security Domain**
*NOTE: If you are using an existing security domain, you can skip directly to the step: Expand **Install Existing Security Domain**.*

Create New Security Domain

Create Security Domain

This wizard guides you through the workflow of generating the cryptographic material for a new security domain, and of splitting this material onto 3 or more smart cards.

Each smart card receives a share of the security domain. The smart cards may later be used to perform certain security-critical operations such as commissioning a payShield or a smart card.

Press 'Start' to begin.

- Press **Start**
- Follow the prompts and enter the details for your security domain
- Click **Next**
- Follow the wizard as each officer is prompted to insert a smart card into the smart card reader and create a PIN
NOTE: The minimum PIN length is 6 digits.

Create Security Domain

Insert a smart card to receive a CTA share into:
SmartCard 0

Create Security Domain

Enter PIN via the smart card terminal keypad.

- After the final security officer has confirmed a PIN, click **Finish**
- Expand **Install Existing Security Domain**

Install Existing Security Domain

- Follow the wizard as each officer is prompted to insert their smart card into the smart card reader followed by the PIN
- When done, click **Next**

Commission payShield

Load Security Domain (from CTA set)

Security domain loading progress: (3 / 3)

Smart card operations progress: 100%

Done loading security domain. Click 'Next' to continue.

The system displays the Security Domain Parameters:

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	techwriter@thalessec.com
Email	support@thalessec.com

Next

- Click **Next**

The system displays:

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

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

- Download and then click **Next**

NOTE: If the system detects that you need to create a set of HSM Recovery Keys, you are prompted to do so.

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: [text box] [text box]

HRK Passphrase 2: [text box] [text box]

Back Next Cancel

- Enter both passphrases twice and then click **Next**
NOTE: Each passphrase must contain a minimum of 2 uppercase characters, 2 lowercase characters, 2 digits, and 2 symbols.
- Enter a PIN via the smart card reader keypad and press **OK**
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.
- Remove the smart card

The system prompts you to Designate/Commission the Left key card

- Insert a smart card into the smart card reader

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.

Next Cancel

- Click **Next**
- Enter the PIN and press **OK**

NOTE: If you are using a card that is already commissioned, the system will prompt as shown below:

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.

OK Cancel

- Click **OK**

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

- Click **Next**
- Enter a new PIN and press **OK**
- Follow the prompts to repeat this process to create the Right key card
- When done, click **Finish**
- Restart your Internet browser, enter the name (for DHCP) or IP address associated with your HSM and click **Log In**

