THALES

# ProtectToolkit 5.9.1
# ProtectServer HSM and ProtectToolkit

## INSTALLATION AND CONFIGURATION GUIDE

## Document Information

| | |
|---|---|
| **Last Updated** | 2024-04-18 12:25:26-04:00 |

### Trademarks, Copyrights, and Third-Party Software

Copyright 2009-2024 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

### Disclaimer

All information herein is either public information or is the property of and owned solely by Thales Group and/or its subsidiaries 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 Group's information.

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

- The copyright notice, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any publicly accessible 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 Group 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 Group 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 Group 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 Group 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 Group 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 Group 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.

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of Thales Group.

# CONTENTS

# **PREFACE:** About the ProtectServer HSM and ProtectToolkit Installation Guide

This guide provides hardware installation and configuration procedures for your ProtectServer cryptographic services hardware security module (HSM) and installation procedures for the ProtectToolkit client software. Refer to the section(s) relevant for your ProtectServer HSM model:

- "ProtectServer PCIe 2 Hardware Installation" on page 11
- "ProtectServer External 2 Installation and Configuration" on page 19
- "ProtectServer External 2 Plus Installation and Configuration" on page 38
- "ProtectToolkit Software Installation" on page 60
- "Configuration Items" on page 85

This preface also includes the following information about this document:

- "Document Conventions" below
- "Support Contacts" on page 10

For information regarding the document status and revision history, see "Document Information" on page 2.

## Document Conventions

This document uses standard conventions for describing the user interface and for alerting you to important information.

### Notes

Notes are used to alert you to important or helpful information. They use the following format:

> **NOTE** Take note. Contains important or helpful information.

### Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. They use the following format:

> **CAUTION!** Exercise caution. Contains important information that may help prevent unexpected results or data loss.

## Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. They use the following format:

> ****WARNING** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.**

## Command Syntax and Typeface Conventions

| Format | Convention |
|---|---|
| **bold** | The bold attribute is used to indicate the following:<br>> Command-line commands and options (Type **dir /p**.)<br>> Button names (Click **Save As**.)<br>> Check box and radio button names (Select the **Print Duplex** check box.)<br>> Dialog box titles (On the **Protect Document** dialog box, click **Yes**.)<br>> Field names (**User Name:** Enter the name of the user.)<br>> Menu names (On the **File** menu, click **Save**.) (Click **Menu > Go To > Folders**.)<br>> User input (In the **Date** box, type **April 1**.) |
| *italics* | In type, the italic attribute is used for emphasis or cross-references to other documents in this documentation set. |
| <variable> | In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets. |
| [**optional**]<br>[<optional>] | Represent optional **keywords** or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task. |
| {**a**\|**b**\|**c**}<br>{<a>\|<b>\|<c>} | Represent required alternate **keywords** or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars. |
| [**a**\|**b**\|**c**]<br>[<a>\|<b>\|<c>] | Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars. |

# Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

## Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

## Telephone

The support portal also lists telephone numbers for voice contact (Contact Us).

# CHAPTER 1: ProtectServer PCIe 2 Hardware Installation

The ProtectServer PCIe 2 is the second-generation intelligent ProtectServer cryptographic services PCIe adapter, replacing the ProtectServer PSI-E.

ProtectServer may employ either generic processing or high-speed DES and RSA hardware acceleration. Key storage security is ensured by persistent, tamper-protected memory. Multiple adapters may be installed in a single host computer to improve throughput or provide redundancy.

This guide provides instructions for installing a ProtectServer cryptographic services hardware adapter. To ensure a successful installation, perform the following tasks in the order indicated:

1. Ensure that you have all of the required components, as listed in "ProtectServer PCIe 2 Required Items" on the next page.
2. Install and connect the hardware, as described in "ProtectServer PCIe 2 Installation" on page 13.

The ProtectServer PCIe 2 has been tested with a variety of representative systems/servers with compliant PCI express slots. When a compatibility problem with a current brand and model computer arises, that information is made available via the Thales Support Portal. To troubleshoot a ProtectServer PCIe 2 installation issue that you are experiencing, refer to ProtectServer PCIe 2Installation Issues.

# ProtectServer PCIe 2 Required Items

This section provides a list of the components you should have received with your ProtectServer PCIe 2 order.

## Contents Received

The following table contains the standard items you received with your order.

| Qty | Item |
|---|---|
| 1 | **ProtectServer PCIe 2 Adapter Card**, short-form-factor (performance level 25, 220, or 1500, as ordered, indicated on label).<br> |
| 1 | **Smart card reader**<br> |
| 5 | **Smart cards** (in a single media case)<br>Each smart card contains a total of 64 kilobytes of storage space.<br> THALES<br>ProtectServer<br>HSM Smartcard<br>FW V5.03.01 and above |

> **NOTE** The smart cards and smart card reader are only included with your order if you purchased your ProtectServer HSM with a ProtectServer HSM Accessory Kit.

## Optional Items

The following items can be used with your ProtectServer HSM. Contact your Thales sales representative to order these items.

- **SafeNet 110 Time-Based OTP Token** (enables multifactor authentication on ProtectServer HSM tokens)

  Thales recommends ordering at least two (2) OTP tokens for each slot on the HSM (one each for the Security Officer and Token User).

  PN: 955-000237-001

- **ProtectServer-compatible Verifone PIN pad** (enables manual key component entry)

  PN: 934-000087-001

# ProtectServer PCIe 2 Installation

Follow these general steps to install and commission a ProtectServer PCIe 2 card and its associated software. More detailed instructions are provided in the following sections.

### To install and commission a ProtectServer PCIe 2 card

1. Ensure you have all the necessary components on the list provided. For more information, see "Adapter Features" on the next page.
2. Move the battery jumper from the OFF position to the ON position (see "The Battery Jumper Header" on the next page).
3. If you plan to use an external tamper detector, ensure that it has a two-conductor cable compatible with the tamper-detect connector on the SafeNet adapter (detailed in "Adapter Modification for External Tamper Detectors" on page 17).
4. Install the ProtectServer PCIe 2 card in the host computer system. See "Installing the Adapter" on page 15.
5. Install the ProtectServer HSM Access Provider package and confirm that the adapter and driver are working correctly. See "ProtectServer HSM Access Provider Installation" on page 15.
6. Install the smart card reader if provided, or another serial device. See "Smart Card Reader Installation" on page 15.

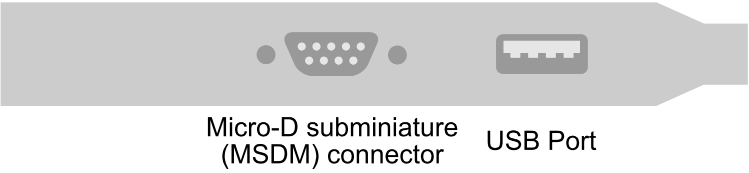
7. Install the SafeNet application programming interface (API) or the supplied net server software. See "Completing Installation" on page 16.

## Adapter Features

The ProtectServer PCIe 2 is a standard PCIe device that fits into any motherboard PCIe slot of formats x4, x8, or x16.

### The Card Faceplate

The card faceplate has two ports:



### The MDSM Connector

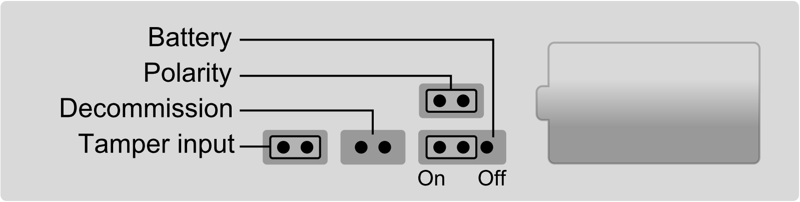
The micro-D subminiature (MDSM) connector is not used.

### The USB Port

The USB port connects a serial device, such as a smart card reader, to the card with the included USB-to-serial adapter.

## The Rear Face

The battery and a series of jumper headers are located on the rear face of the card.



### The Battery

The battery maintains the internal flash memory.

You can use the **ctcheck -b batterystatus** command to test the battery's condition. If the battery status is reported as **LOW**, back up the keys on the HSM and return the HSM to your nearest Thales service centre for battery/HSM replacement. For more information about returning an HSM back to Thales, refer to RMA and Shipping Back to Thales.

> **CAUTION!** Do not attempt to disconnect the battery. Disconnecting the battery will shut down the HSM and trigger a tamper event, which will erase all key material on the HSM.

## The Battery Jumper Header

The battery jumper is a three-pin jumper used to engage or disengage the battery.

The battery is in the ON position when a jumper is inserted on the center and left pins, as shown in "ProtectServer PCIe 2 Installation" on page 13.

The battery is in the OFF position when a jumper is inserted on the center and right pins. This setting is not required for normal operation.

> **CAUTION!** Do not change the jumper setting unless instructed by Thales support.

### The Decommission Jumper Header

This header is currently unused; do not change its default setting (open).

### The Tamper-Input Header

The tamper-input header connects an external tamper device to the card. By default, it has a jumper in place across both pins. To use an external tamper device, run a two-wire cable to your chassis-tamper switch or similar device to open the circuit in the case of a tamper event.

### The Polarity Jumper Header

The polarity jumper header is used to configure the card's operating mode. Do not change this jumper setting.

## Installing the Adapter

The adapter is a PCI Express Specification 1.1-compliant device. It can be fitted in any spare PCIe slot on the motherboard of formats x4, x8, or x16. If necessary, please consult the documentation accompanying your host system motherboard to find the PCIe slots.

If you are using a tamper-detection device, route the cable to it before closing the computer cover.

## ProtectServer HSM Access Provider Installation

After successful installation of the adapter:

1. Install the ProtectServer HSM Access Provider package (**PTKpcihsmK6**).
2. Confirm the adapter and driver package are operating correctly.

These steps are covered in detail, for both Windows and Unix/Linux systems, in "ProtectToolkit Software Installation" on page 60.

## Smart Card Reader Installation

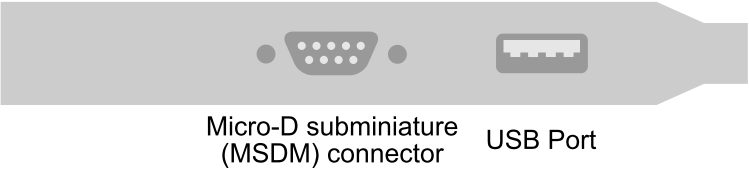
The ProtectServer PCIe 2 supports the use of smart cards with a SafeNet-supplied smart card reader. Readers not supplied by Thales are unsupported.

The ProtectServer PCIe 2 supports two different card readers:

- the new USB card reader (introduced in 5.2)
- the legacy card reader, which provides a serial interface for data (via a USB-to-serial cable) and a PS/2 interface for power (direct or via a PS/2 to USB adapter)

### Installing the USB smart card reader

To install the USB card reader, simply plug the card reader into the HSM USB port.



### Installing the legacy card reader

To install the smart card reader, use the included USB-to-serial cable to connect it to the HSM USB port on the card faceplate as shown in "The connected legacy card reader" below (The illustration shows the card reader connected to a ProtectServer External 2).

The legacy card reader must also be connected to a PS/2 port for power. Many newer servers have USB ports, but do not provide a PS/2 connection.

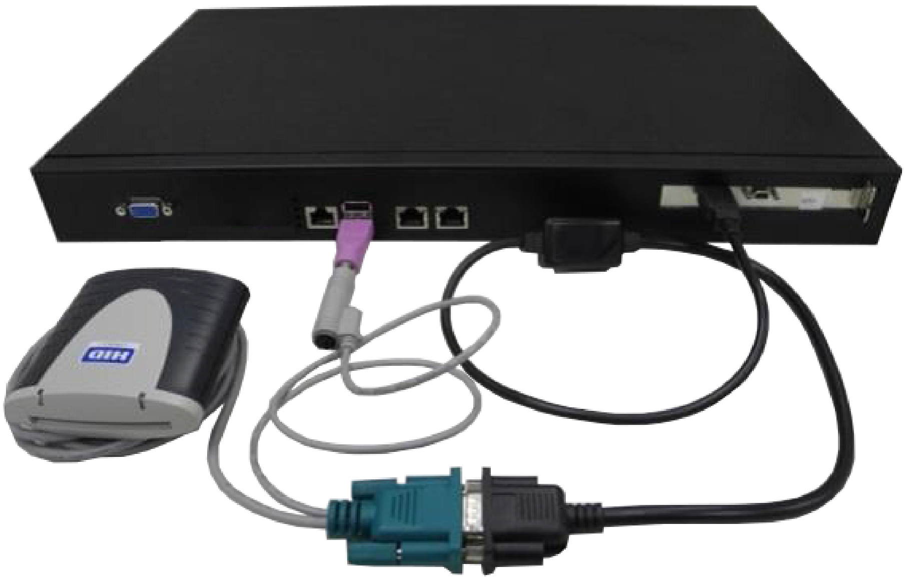
The options are:

> Use a PS/2-to-USB adapter (pink) to connect the card reader to a USB port on the host computer.

> If you prefer not to expose USB ports on your crypto server (for security reasons), use a PS/2-to-USB adapter to connect the card reader to a standalone powered USB hub.

The USB connection is for power only. No data transfer occurs.

**Figure 1: The connected legacy card reader**



## Completing Installation

After you have installed the ProtectServer HSM Access Provider, install the supplied SafeNet API or net server software. For more information about installing ProtectToolkit, see "ProtectToolkit Software Installation" on page 60.

# ProtectServer PCIe 2 Storage Capacity

The ProtectServer PCIe 2 has the following storage capacity:

- Functionality Module (FM) storage: 8 MB.
- Secure Memory File System (SMFS) storage for keys and cryptographic materials: 4 MB shared between the firmware and FMs.

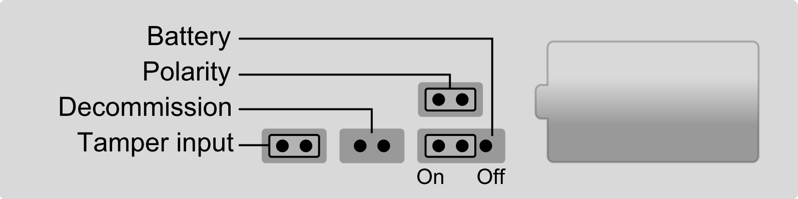
# Hardware Reference

This appendix contains hardware specifications and instructions on how to fit the HSM with an external tamper detector such as a micro switch.

## Adapter Modification for External Tamper Detectors

Connect additional tamper detection devices using the tamper input header, located on the rear face of the card, as illustrated in "Rear face of the card" below.

**Figure 2: Rear face of the card**



### To fit an external tamper detection device

1. Remove the default jumper/shunt that bridges the two posts in the ProtectServer PCIe 2's tamper input header (see "Rear face of the card" above).
2. Connect your external tamper device in the shunt's place.

   The cable end from your tamper-detection device must match the Molex socket on the adapter, which is designed to fit with an insertable connector housing (Molex part 35507-0200).

   a. Crimp a pair of 2 mm WTB crimp terminals (Molex part 50212-8100) to the ends of your tamper detector's two-wire connector cable.

   b. Insert the crimped terminal sockets into the Molex connector housing.
3. Plug the newly-fitted connector cable into the PCIe adapter's tamper input header.

The external tamper detector must provide the following conditions:

- In the **untampered** condition, the device must provide a low-impedance path (short circuit) between the tamper-detection posts.
- In the **tampered** condition, the device must show an open circuit.

## The Battery

The adapter is fitted with a backup battery, which maintains cryptographic keys and the correct time when the host computer is shut down, or when the adapter is otherwise disconnected from a power source.

The battery has an expected lifetime of ten years. It should not require replacement within the normal lifetime of the adapter.

### Testing the battery

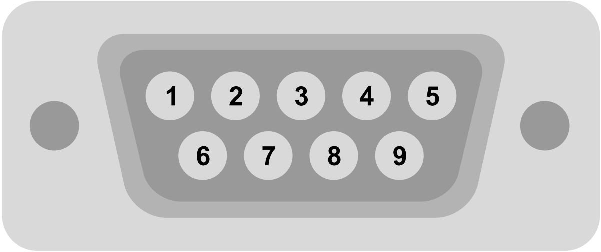
You can use the utilities provided with the adapter to query the state of the battery. In ProtectToolkit-C, use **ctcheck -b batterystatus** to return a state of **Good**/**Low**. For more information about querying the state of the battery of the HSM, see the reference guide for your ProtectToolkit software.

The real-time clock (RTC) and memory retain their data as long as the adapter is in a powered system. The RTC performs a daily battery check. If it detects a low-battery warning, the battery may need to be replaced. If the adapter has been de-powered or removed from its system, the data in its memory is suspect. If the adapter has been continuously powered, then the data in memory can be trusted and you can make a backup before sending the adapter to a Thales service centre for battery/HSM replacement. For more information about returning an HSM back to Thales, refer to RMA and Shipping Back to Thales.

## Port Specifications

The USB-to-serial cable provides an RS232 port with pin outs as shown in "Adapter serial connector" below. This port can be used for connecting a smart card reader or another serial device.

**Figure 3: Adapter serial connector**



**1**: DCD
**2**: RxD
**3**: TxD
**4**: DTR
**5**: GND
**6**: DSR
**7**: RTS
**8**: CTS
**9**: N/C

# CHAPTER 2: ProtectServer External 2 Installation and Configuration

These steps summarize the overall procedure of setting up a cryptographic service provider using a ProtectServer External 2 in network mode. Relevant links to more detailed documentation are provided at each step.

1. Install the ProtectServer External 2 (See "Installing the ProtectServer External 2 Hardware" on page 25).
2. Check that the ProtectServer External 2 is operating correctly (see "First Login and System Test" on page 28).
3. Configure the ProtectServer External 2 network settings (see "Network Configuration" on page 31).
4. Install and configure the ProtectServer HSM Access Provider software and ProtectToolkit software on your operating system. See the following sections:
   - "Installing ProtectToolkit on Windows" on page 63
   - "Installing ProtectToolkit on Unix/Linux" on page 69
   - "Installing ProtectToolkit on Linux Manually" on page 74
5. Configure the high-level cryptographic API to allow preferred operating modes. Some of these tasks may include:
   - establishing a trusted channel or secure messaging system (SMS) between the API and the ProtectServer External 2.
   - establishing communication between the network client and the ProtectServer External 2.

   Please refer to the relevant high-level cryptographic API documentation:
   - *ProtectToolkit-C Administration Guide*
   - *ProtectToolkit-J Reference Guide*
   - *ProtectToolkit-M User Guide*

# Product Overview

The ProtectServer External 2 is a self-contained, security-hardened server providing hardware-based cryptographic functionality through a TCP/IP network connection. Together with high-level SafeNet application programming interface (API) software, it provides cryptographic services for a wide range of secure applications.

The ProtectServer External 2 is PC-based. The enclosure is a heavy-duty steel case with common PC ports and controls. Necessary software components come pre-installed on a Linux operating system. Network setting configuration is required, as described in this document.

The full range of cryptographic services required by Public Key Infrastructure (PKI) users is supported by the ProtectServer External 2's dedicated hardware cryptographic accelerator. These services include encryption, decryption, signature generation and verification, and key management with a tamper resistant and battery-backed key storage.

The ProtectServer External 2 must be used with one of SafeNet's high-level cryptographic APIs. The following table shows the provider types and their corresponding SafeNet APIs:

| API | SafeNet Product Required |
|---|---|
| PKCS #11 | ProtectToolkit-C |
| JCA / JCE | ProtectToolkit-J |
| Microsoft IIS and CA | ProtectToolkit-M |

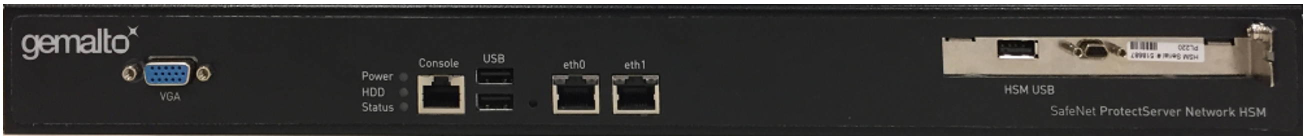
These APIs interface directly with the product's FIPS 140-2 Level 3 certified core using high-speed hardware-based cryptographic processing. Key storage is tamper-resistant and battery-backed.

A smart card reader, supplied with the HSM, allows for the secure loading and backup of keys.

## Front panel view

The features on the front panel of the ProtectServer External 2 are illustrated below:

**Figure 4: ProtectServer External 2 front panel**



### Ports

The front panel is equipped with the following ports:

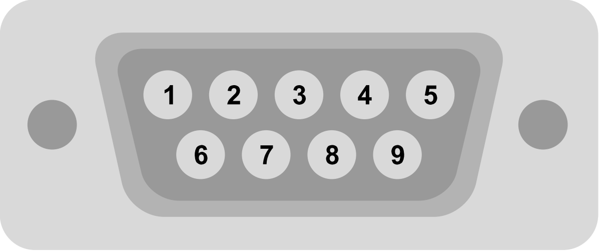
| | |
|---|---|
| VGA | Connects a VGA monitor to the appliance. |
| Console | Provides console access to the appliance. See "Access the Console" on page 29. |
| USB | Connects USB devices such as a keyboard or mouse to the appliance. |

| | |
|---|---|
| eth0<br>eth1 | Autosensing 10/100/1000 Mb/s Ethernet RJ45 ports for connecting the appliance to the network. |
| HSM USB | Connects a smart card reader to the appliance using the included USB-to-serial cable. |

### HSM serial port pin configuration

The serial port uses a standard RS232 male DB9 pinout. The USB-to-serial cable connects to this port.

**Figure 5: HSM serial port pinout**



**1**: DCD
**2**: RxD
**3**: TxD
**4**: DTR
**5**: GND
**6**: DSR
**7**: RTS
**8**: CTS
**9**: N/C

### LEDs

The front panel is equipped with the following LEDs:

| | |
|---|---|
| Power | Illuminates green to indicate that the unit is powered on. |
| HDD | Flashes amber to indicate hard disk activity. |
| Status | Flashes green on startup. |

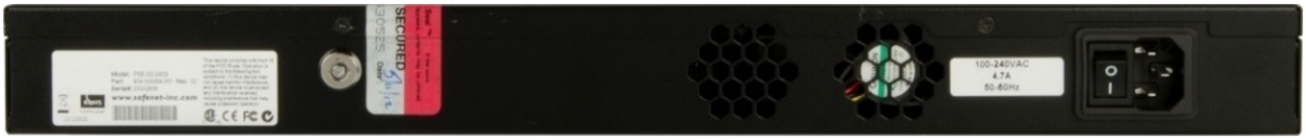
### Reset button

The reset button is located between the USB and Ethernet ports. Pressing the reset button forces an immediate restart of the appliance. Although it does not power off the appliance, it does restart the software. Pressing the reset button is service-affecting and is not recommended under normal operating conditions.

## Rear panel view

The features on the rear panel of the ProtectServer External 2 are illustrated below:

**Figure 6: ProtectServer External 2 rear panel**



### Tamper lock

The tamper lock is used during commissioning or decommissioning of the appliance to destroy any keys currently stored on the HSM.

With the key in the horizontal (Active) position, the HSM is in normal operating mode. Turning the key to the vertical (Tamper) position places the HSM in a tamper state, and any keys stored on the HSM are destroyed.

**CAUTION!** Turning the tamper key from the Active position to the Tamper position deletes any keys currently stored on the HSM. Deleted keys are not recoverable. Ensure that you always back up your keys. To avoid accidentally deleting the keys on an operational ProtectServer External 2, remove the tamper key after commission and store it in a safe place.

## Cryptographic Architecture

A hardware-based cryptographic system consists of three general components:

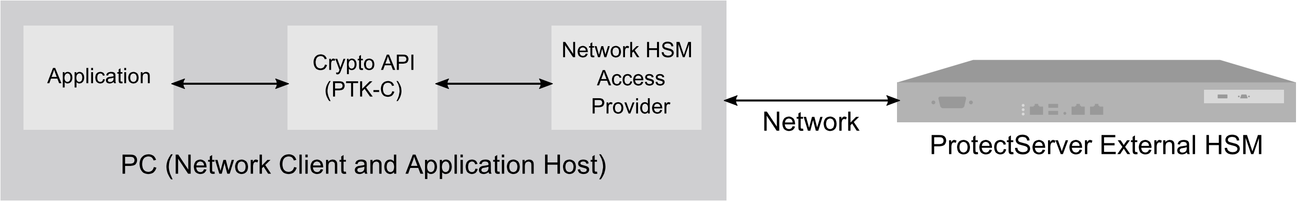
- One or more hardware security modules (HSMs) for key processing and storage.
- High-level cryptographic API software. This software uses the HSM's cryptographic capabilities to provide security services to applications.
- Access provider software to allow communication between the API software and the HSMs.

Operating in network mode, a standalone ProtectServer External 2 can provide key processing and storage.

In network mode, access provider software is installed on the machine hosting the cryptographic API software. The access provider allows communication between the API and the ProtectServer External 2 over a TCP/IP connection. The HSM can therefore be located remotely, improving the security of cryptographic key data

The figure below depicts a cryptographic service provider using the ProtectServer External 2 in network mode.

**Figure 7: ProtectServer External 2 implementation**


Application
Crypto API (PTK-C)
Network HSM Access Provider
PC (Network Client and Application Host)
Network
ProtectServer External HSM

## Technical Specifications

The ProtectServer External 2 specifications are as follows:

### Hardware

- One smart card reader secure USB port (requires the included USB-to-serial cable)
- Protective, heavy duty steel, industrial PC case
- Intel® Atom™ CPU E3827 1.74GHz
- 2 GB RAM
- 4 GB solid state flash memory hard disk (DOM)
- 10/100/1000 Mbps autosensing Network Interface with RJ45 LAN connector

### Pre-installed Software

- Linux operating system
- ProtectServer HSM Access Provider software
- ProtectServer HSM Net Server software

### Power Supply

- Nominal power consumption: 43 W
- Input AC voltage range: 100-240 V
- Input frequency range: 50-60 Hz

### Physical properties

- 437 mm (W) x 270 mm (D) x 44 mm (H) (1U)
- 19” rack mounting brackets included
- Weight 5 kg (11 lb)

### Operating Environment

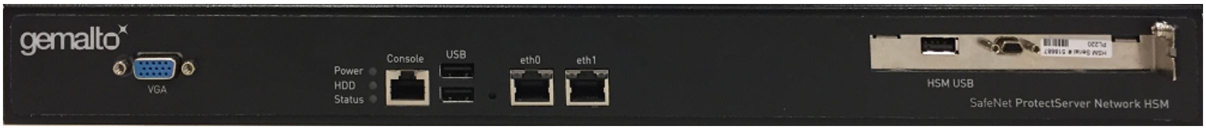
- Temperature: 0 to 40°C (32 to 104°F)
- Relative Humidity: 5 to 85%

# ProtectServer External 2 Required Items

This section provides a list of components that you should have received with your ProtectServer External 2 order.

## Contents Received

The following table contains the standard items you received with your order:

| Qty | Item |
|---|---|
| 1 | **ProtectServer External 2 standalone appliance**<br><br> gemalto<br>VGA<br>Power<br>HDD<br>Status<br>Console<br>USB<br>eth0<br>eth1<br>HSM USB<br>SafeNet ProtectServer Network HSM |
| 1 | **Smart card reader**<br> <br> |
| 5 | **Smart cards** (in a single media case)<br>Each smart card contains a total of 64 kilobytes of storage space.<br> <br> THALES<br>ProtectServer<br>HSM Smartcard<br>FW V5.03.01 and above |

**NOTE**

- The smart cards and smart card reader are only included with your order if you purchased your ProtectServer HSM with a ProtectServer HSM Accessory Kit.
- Power cables are no longer included with the shipment from our factory. Please source your power cables locally for the intended deployment destination.
- To configure your ProtectServer External 2, you will need to supply and connect a keyboard, mouse, and display monitor. After the appliance is placed into service, the keyboard, mouse and monitor can be disconnected from the appliance.

## Optional Items

The following items can be used with your ProtectServer HSM. Contact your Thales sales representative to order these items.

- **SafeNet 110 Time-Based OTP Token** (enables multifactor authentication on ProtectServer HSM tokens)

  Thales recommends ordering at least two (2) OTP tokens for each slot on the HSM (one each for the Security Officer and Token User).

  PN: 955-000237-001

- **ProtectServer-compatible Verifone PIN pad** (enables manual key component entry)

  PN: 934-000087-001

# Installing the ProtectServer External 2 Hardware

Since the ProtectServer External 2 is delivered with the necessary software pre-installed, no software installation is necessary on the unit itself.

After installation, confirm that the unit is operating correctly and configure the network settings. These steps are covered in "First Login and System Test" on page 28 and "Network Configuration" on page 31.

### To install the hardware

1. Choose a suitable location to site the equipment. You can mount the ProtectServer External 2 in a standard 19-inch rack.

   > **NOTE** The power supply cord acts as the unit's disconnect device. The main outlet socket to which the unit is connected must be easily accessible.

2. Connect the ProtectServer External 2 to the network by inserting standard Ethernet cables into the LAN connectors located on the unit's front face (labelled *eth0* and *eth1*). The client machine(s) with SafeNet cryptographic API software installed should be hosted on the same network.

   > **NOTE** The ProtectServer External 2 is equipped with two NICs (*eth0* and *eth1*) incorporating an IPv4/IPv6 dual stack, allowing you to configure both an IPv4 and IPv6 address on each interface. If you intend to use both NICs, connect Ethernet cables to both LAN connectors.

3. Connect the power cable to the unit and a suitable power source. The ProtectServer External 2 is equipped with an autosensing power supply that can accept 100-240V at 50-60Hz.

## Smart Card Reader Installation

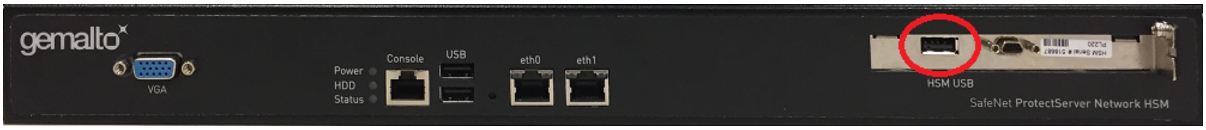
The unit supports the use of smart cards with a Thales-supplied smart card reader. Other smart card readers are not supported.

The ProtectServer External 2 supports two different card readers:

- the new USB card reader (introduced in 5.2)
- the legacy card reader, which provides a serial interface for data (via a USB-to-serial cable) and a PS/2 interface for power (direct or via a PS/2 to USB adapter)

### To install the USB card reader

Simply plug the card reader into the HSM USB port, as illustrated below.



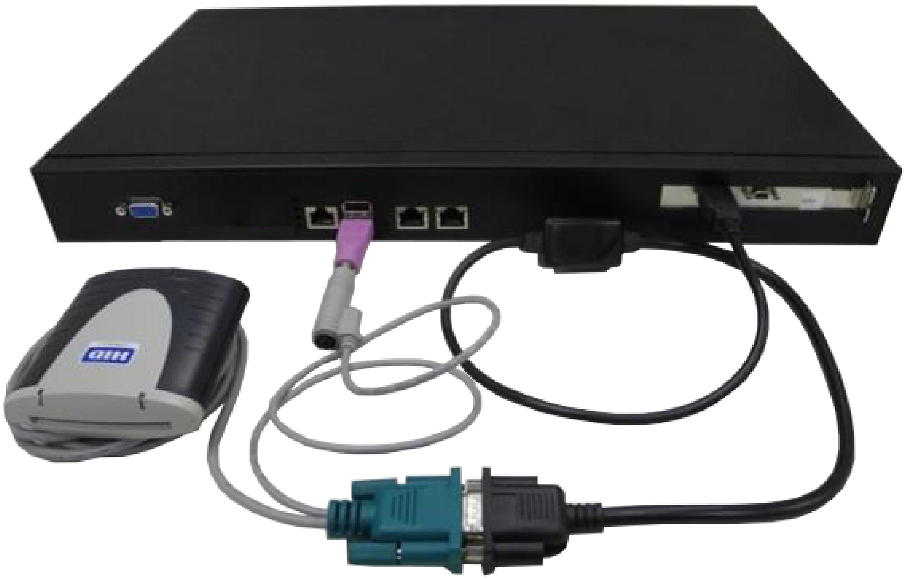
### Installing the legacy card reader

To install the smart card reader, connect it to the HSM USB port with the included USB-to-serial cable.

The legacy card reader must also be connected to a PS/2 port for its power. Many newer servers have USB ports, but do not provide a PS/2 connection.

If there is no available PS/2 connection, there are two options:

- Connect a PS/2-to-USB adapter (pink in the image below) between the card reader and a USB port on the ProtectServer External 2.
- If, for security reasons, you prefer to not expose USB ports on your crypto server, connect a PS/2-to-USB adapter cable between the card reader and a standalone powered USB hub. It should be noted that the USB connection is for power only. No data transfer occurs.



Next, see "First Login and System Test" on page 28.

# Deployment Guidelines

Users must consider the following best practices for security and compliance when deploying the ProtectServer External 2 for their network/application environment:

- "Secure Messaging System (SMS)" below
- "Networking and Firewall Configuration" on the next page
- "Separation of Roles" on the next page

## Secure Messaging System (SMS)

The ProtectServer External 2 stores cryptographic keys and objects in tamper-resistant secure memory, which is erased when a tamper is detected. The stored keys are accessed through PKCS#11 calls from the client. Client calls to a ProtectServer External 2 traverse the network layer (TCP/IP). In the default security mode, this communication channel between the HSM and the client is unencrypted. Configure the HSM security policy to improve this channel's security. Refer to Security Flags in the "Security Policies and User Roles" section of the *ProtectToolkit-C Administration Guide* for descriptions of the available flags and how they affect your implementation.

The Secure Messaging System (SMS) enhances the security of the client-HSM channel. SMS provides an encrypted channel between the client and the HSM and authenticates messages on that channel using a Message Authentication Code (MAC) approved by the FIPS 140-2 standard. Refer to Secure Messaging in the "Cryptoki Configuration" section of the *ProtectToolkit-C Administration Guide* for a detailed description of SMS functionality.

> **NOTE** SMS encrypts and authenticates messages between the client and HSM, but does not provide means for the HSM to authenticate client credentials or vice-versa.

The HSM supports the following SMS modes:

- HIMK
- ADH
- ADH2 (PTK 5.4 and above)

For secure deployment, use ADH or ADH2. Refer to Secure Messaging in the "Cryptoki Configuration" section of the *ProtectToolkit-C Administration Guide* for descriptions of the difference between these modes.

The SMS feature is flexible and can be configured to:

- Encrypt/decrypt all messages
- Sign/verify all messages
- Allow only FIPS-approved mechanisms
- Rotate signing and encryption keys after a specified number of packets or hours
- All of the above

For maximum security, enable all of the above features. See Security Flags in the "Security Policies and User Roles" section of the *ProtectToolkit-C Administration Guide* for flag descriptions and setup instructions.

> **NOTE** Enabling FIPS mode will block all mechanisms that are not FIPS-approved. If you are using unapproved mechanisms and understand the implications, do not enable FIPS mode.

## Networking and Firewall Configuration

There is no means to authenticate the client to the HSM or vice-versa. It is therefore recommended that the HSM and client are connected to the same secure network segment, to prevent sensitive data from traveling through insecure intermediate network(s). This configuration prevents Man-in-the-Middle and other malicious attacks. If possible, connect the HSM directly to the client using a cross-cable.

The ProtectServer External 2 includes two network ports, each of which can be connected to a different network. It is highly recommended that you keep the management network and the network running your applications isolated from each other at all times. Further restrictions on communication between network segments can be enforced by means of static routes. See "Network Configuration" on page 31 for instructions on setting up static routes.

The ProtectServer External 2 supports an iptables-based firewall. The firewall must be configured with appropriate rules to restrict access to identified network resources only. See "Network Configuration" on page 31 for details on setting iptables.

## Separation of Roles

The ProtectServer External 2 has two role categories: Appliance and HSM users. For optimal security, maintain these roles and their credentials separately; do not share between users. Do not share the appliance management, HSM Administration, and User terminals.

### Appliance Users

The following roles can log in to the PSE shell (PSESH) to configure and manage the appliance:

- admin
- pseoperator
- audit

See Using PSESH in the *PSESH Command Reference Guide* for the responsibilities of each role.

### HSM Users

The following roles can log in to manage the HSM token and perform cryptographic operations:

- Administration Security Officer (ASO)
- Administrator
- Security Officer (SO)
- Token Owner (User)

See User Roles in the *ProtectToolkit-C Administration Guide* for the responsibilities of each role.

# First Login and System Test

When starting up your ProtectServer External 2 for the first time, follow these steps:

- "Access the Console" below
- "Power on and Login" below
- "Run System Test" on the next page

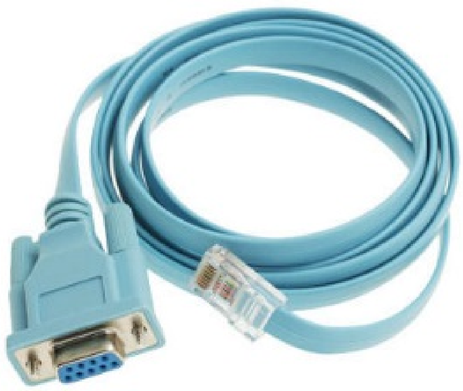
## Access the Console

To test the system and configure the network, you must first access the ProtectServer External 2 console. There are two options:

- *Direct access.* Connect a keyboard and monitor (not included) to the USB (keyboard) and VGA (monitor) ports located on the unit's front panel.
- *Console access.* Connect the RJ45 console port to a terminal emulation device, such as a laptop or terminal server.

> **NOTE** To access the appliance through the console port, you will need the appropriate cable. If your terminal device is equipped with a DB9 serial port, you require a cable with an RJ45 connector on one end and a DB9 serial port on the other end (see "Serial cable: RJ45 to DB9" below). If your terminal device is equipped with an RJ45 serial port, you can use a standard Ethernet cable. Serial cables are not included.

**Figure 8: Serial cable: RJ45 to DB9**



If you are using a serial connection, configure your local VT100 or terminal emulator settings as follows:

| | |
|---|---|
| Speed (bits per second) | 115200 |
| Word length (data bits) | 8 |
| Parity | No |
| Stop bit | 1 |

## Power on and Login

Power on the ProtectServer External 2 and the (optional) monitor. A green LED on the front of the device will illuminate and the startup messages will be displayed on the monitor:

```
Welcome to SafeNet Protect Server External II v5.9.1
=====================================================

System is booting, this may take few minutes...

SafeNet Protect Server System boot Successful
```

If you are using a serial connection, no startup messages are displayed.

Power-up is complete when the login prompt appears:

```
Protect Server External 5.9.1
PSE-II login:
```

You can login as **admin** or **pseoperator** to access the PSE shell (PSESH), which provides a CLI for configuring and managing the appliance. See the *PSESH Command Reference Guide* for command syntax.

The default passwords for the **admin** and **pseoperator** users are:

| User name | Default password |
|---|---|
| **admin** | **password** |
| **pseoperator** | **password** |

After logging in, you will be prompted to change the password for the account. Please remember your password. To change the account password at any time, login to the account and use the command **user password**.

The **admin** user can reset all account passwords to their factory defaults at any time with the PSESH command **sysconf appliance factory**. This command will also reset the SNMP and network settings to their factory defaults.

> **CAUTION!** Executing **sysconf appliance factory** over an SSH connection may cause you to lose connection with the appliance when the IP address is reset. To avoid this, use a serial connection instead when using this command.

## Run System Test

Before field testing and deployment, run the diagnostic utility. Use **hsm state** to display the current status:

```
psesh:>hsm state

HSM device 0:   HSM in NORMAL MODE. RESPONDING to requests. Usage Level=0%
State = (0x8000, 0xffffffff)
Host Interface   = PSIe2

Command Result : 0 (Success)
```

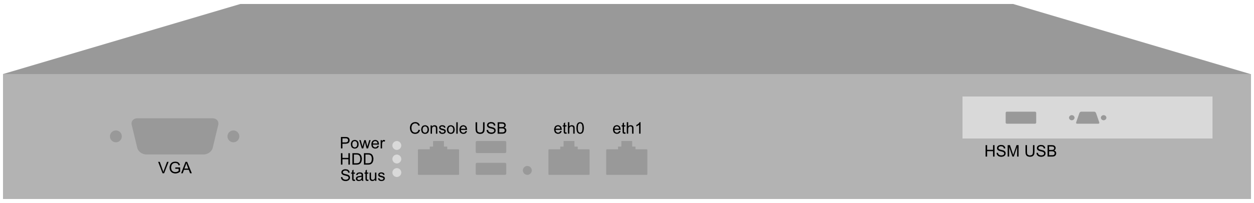
You can also use the PSESH command **status** to check each of the HSM's processes. See the *PSESH Command Reference Guide* for command syntax.

Continue to "Network Configuration" on the next page

# Network Configuration

The ProtectServer External 2 is intended to be installed in a data center and accessed remotely over a network. Network access is provided by two Ethernet LAN ports. The ProtectServer External 2 is also equipped with an RJ-45 console port, used to provide serial access to the appliance for initial network configuration.

The network device interfaces (eth0 and eth1) and console port are located on the front of the appliance, as illustrated below:



## Console port

Connect a serial device to the ProtectServer External 2 to perform initial network configuration via PSESH. Use the **Console** port to configure at least one of the network interfaces. Once you have configured an interface, you can connect the appliance to the network and access PSESH to complete the network configuration.

## Appliance configuration

The following network parameters are configured at the appliance level:

- Appliance hostname. A hostname is optional, unless you are using DNS.

## Ethernet LAN device configuration

The ProtectServer External 2 is equipped with two individually-configurable Ethernet LAN network devices. You can configure the following network settings for each device:

- IPv4 or IPv6 address. You can configure IPv4 addresses using static or DHCP addressing. IPv6 addresses must be configured as static addresses.
- Network gateway. Devices must use a gateway appropriate for the network (IPv4 or IPv6).
- Network mask. IPv4 devices must use dotted-quad format (for example, 255.255.255.0). IPv6 devices can use full or shorthand syntax.
- Static network route.
- DNS configuration. Although you configure DNS at the device level, the settings you configure for a device are available to all devices on the appliance if the configured device is connected to the network. To ensure DNS access, it is recommended that you configure each device. You can configure the following settings:
  - DNS nameservers
  - DNS search domains

  These settings apply to static network configurations only. If you are using DHCP, the DNS search domains and DNS nameservers configured on the DHCP server are used.
- Network device bonding

## Gathering Appliance Network Information

Before you begin, obtain the following information (see your network administrator for most of these items):

### HSM Appliance Network Parameters

- IP address and subnet mask for each LAN port you want to use (if you are using static IP addressing)
- Hostname for the HSM appliance (registered with network DNS)
- Domain name (per port)
- Default gateway IP address (per port)
- DNS Name Server IP address(es) (per port)
- Search Domain name(s) (per port)
- Device subnet mask (per port)

### DNS Entries

- Ensure that you have configured your DNS Server(s) with the correct entries for the appliance and the client.
- If you are using DHCP, then all references to the client and the HSM appliance (as in certificates) should use hostnames.

## Configuring the Network Parameters

You can use the serial connection to configure all of your network parameters, or configure a single port and use it to access the appliance over the network and complete the configuration.

> **NOTE** Use a locally-connected serial terminal when changing the appliance IP address, to avoid SSH admin console disconnection.

### To configure the appliance and port network parameters

It is recommended that you configure and test each device. You need to know the IP address of at least one network interface to establish an SSH connection to the appliance.

1. Login to the appliance as **admin** or **pseoperator**.
2. Configure the IP address, network mask, and gateway (optional) on at least one of the Ethernet LAN ports (eth0 or eth1). You can specify a static address, or retrieve one from a DHCP server. You can configure each port to use an IPv4 or IPv6 address.

> **NOTE** IPv6 addresses must be configured as static addresses.

| | |
|---|---|
| **Static** | psesh:> **network interface static -device** <netdevice> **-ip** <IP_address> **-netmask** <netmask> [-**gateway** <IP_address>] |
| **DHCP** | psesh:> **network interface dhcp -device** <netdevice> |
| **IPv6** | psesh:> **network interface ipv6 -device** <netdevice> **-ip** <IP> [**-gateway** <IP>] |

Either of these commands will prompt you to restart the network service.

3. [Optional] Configure network interface bonding. This allows the two network devices to function as a single interface, with a single MAC address, improving bandwidth and providing redundancy.

> **NOTE** Configure network interface bonding with static IPv4 addresses only. If DHCP is used, the bond will be broken if one interface is assigned a different IP.

psesh:>**network interface bonding config -ip** <IP> **-netmask** <IP> **-gateway** <IP>] [**-mode** <mode>]

psesh:>**network interface bonding enable**

psesh:>**sysconf appliance reboot**

Multiple bonding modes provide different options for load-balancing between the two physical interfaces:

- **0**: Balance Round Robin. Packets are transmitted alternately on each device in the bond, providing load balancing and fault tolerance.
- **1**: Active-Backup. One bonded device is active and the other serves as a backup. The backup only becomes active if the active device loses connectivity.
- **2**: Balance XOR. Transmits based on an XOR formula, where the source MAC address is XOR'd with the destination MAC address. The same bonded device is selected for each destination MAC address, providing load balancing and fault tolerance.
- **3**: Broadcast. All packets are transmitted on both bonded interfaces, providing fault tolerance.
- **4**: 802.3ad (Dynamic Link Aggregation). Creates aggregated groups that share the same speed and duplex settings. This mode requires a switch that supports IEEE 802.3ad dynamic links. The dvice used for an outgoing packet is selected by the transmit hash policy (by default, a simple XOR). This policy can be changed via the xmit_hash_policy option. **NOTE:** Check the 802.3ad standard to ensure that your transmit policy is 802.3ad-compliant. In particular, check section 43.2.4 for packet mis-ordering requirements. Non-compliance tolerance may vary between different peer implementations.
- **5**: Balance TLB (Transmit Load Balancing). Outgoing traffic is distributed according to the current load and queue on each bonded device. Incoming traffic is received by the current device.
- **6**: Balance ALB (Adaptive Load Balancing). Both outgoing and incoming traffic is load-balanced like outgoing traffic in mode 5. Incoming load balancing is governed by ARP negotiation. The bonding driver intercepts the ARP replies sent by the appliance and overwrites the source hardware address with the unique hardware address of one of the bonded devices. Different clients will therefore use different hardware addresses for the appliance.

4. [Optional] Set the appliance hostname and domain name.

   psesh:> **network hostname** <hostname>

   psesh:> **network domain** <netdomain>

   You must configure your DNS server to resolve the hostname to the IP address configured on the Ethernet port of the appliance. Do this for each Ethernet port connected to a network. See your network administrator for assistance.

5. [Optional] Add a domain name server to the network configuration for the appliance. The name server is added to the appliance DNS table. There is one DNS table that applies to all network devices (ports) on the appliance.

psesh:> **network dns add nameserver** <IP_address> **-device** <net_device>

> **NOTE** The domain name settings apply to static network configurations only. If you are using DHCP, the DNS name servers configured on the DHCP server are used.

When you add a DNS server to a specific network device, it is added to the DNS table for the appliance and becomes available to both devices, provided the device you added it to is connected to the network. For example, if you add a DNS server to eth0, eth1 will be able to access the DNS server if eth0 is connected to the network. If eth0 is disconnected from the network, eth1 also loses DNS server access. To ensure that any DNS server you add is available in the event of a network or port failure, it is recommended that you add it to both network-connected devices.

6. [Optional] Add a search domain to the network configuration. These are automatically appended to an internet address you specify in PSESH. For example, if you add the search domain **mycompany.com**, entering the command **network ping hsm1** would search for the domain **hsm1.mycompany.com**. If the domain resolves, it pings the device with that hostname.

   lunash:> **network dns add searchdomain** <domain> **-device** <net_device>

   The search domain is added to the appliance DNS table.

   > **NOTE** The search domain settings apply to static network configurations only. If you are using DHCP, the DNS search domains configured on the DHCP server are used.

   When you add a DNS search domain to a specific network device, it is added to the DNS table for the appliance and becomes available to both devices, provided the device you added it to is connected to the network. For example, if you add a DNS server to eth0, eth1 will be able to access the DNS server if eth0 is connected to the network. If eth0 is disconnected from the network, eth1 also loses DNS server access. To ensure that any DNS server you add is available in the event of a network or port failure, it is recommended that you add it to both network-connected devices.

   If you have chosen to perform setup via SSH, you will likely lose your network connection as you confirm the change of IP address from the default setting.

7. [Optional] Add iptables ACCEPT and DROP rules to manage network access to the appliance.

   By default, the ProtectServer External 2 allows access to all networks and hosts. The default policy for the INPUT and OUTPUT chain is set to ACCEPT. The default policy for the FORWARD chain is set to DROP, since the ProtectServer External 2 is not used to forward packets, as in a router or proxy.

   > **CAUTION!** If you are configuring iptables via SSH, a malformed rule can cause a lockout.

   a. To add an ACCEPT rule, specify a host or network:

      psesh:> **network iptables addrule accept host -ip** <IP_address>

      psesh:> **network iptables addrule accept network -net** <IP_address> **-mask** <netmask>

   b. To add a DROP rule, specify a host or network:

      psesh:> **network iptables addrule drop host -ip** <IP_address>

      psesh:> **network iptables addrule drop network -net** <IP_address> **-mask** <netmask>

   c. To see the current list of rules:

psesh:> **network iptables show**

d. To delete a rule, specify the rule's position on the list:

   psesh:> **network iptables delrule -rulenum** <number>

   A rule's number is based on its current list position, so executing **network iptables delrule -rulenum 1** multiple times will eventually delete the entire list.

e. Save your iptables changes:

   psesh:> **network iptables save**

   You must execute this command, or any changes will be lost on the next appliance reboot.

8. After making any change to the network configuration, reboot the appliance:

   psesh:> **sysconf appliance reboot**

9. View the new network settings:

   psesh:> **network show**

### SSH Network Access

After you have completed the network configuration, you can access the ProtectServer External 2 over the network using the SSH protocol. You need an SSH client such as puTTY (available for free from www.putty.org).

## Powering off the ProtectServer External 2

Use PSESH to power off the appliance before toggling the power switch.

#### To power off the ProtectServer External 2

1. While logged in to PSESH as **admin** or **pseoperator**, issue the command:

   psesh:> **sysconf appliance poweroff**

   Wait for the appliance to perform shutdown procedures. The fan and LEDs will remain operational.

2. Toggle the power switch, located on the rear of the ProtectServer External 2, to the off position. The fan and LEDs will turn off.

## Updating the Appliance Software Image

Thales provides secure update packages on the Customer Support Portal that allow the appliance administrator to update the appliance software image on your ProtectServer External 2 and take advantage of new PSESH functionality. If you are updating the appliance software from version 5.6.0 or earlier, you must first install the secure package update patch, also available from the Support Portal.

> "Installing the Secure Update Package Patch" on the next page

> "Updating the Appliance Software" on page 37

## Installing the Secure Update Package Patch

The following procedure allows you to install the secure package update patch on your ProtectServer External 2 appliance running appliance software 5.2.0 to 5.6.0. The procedure is different depending on your appliance's current software version. You only need to apply the patch once; future updates require "Updating the Appliance Software" on the next page only.

### Prerequisites

- Download the patch (**SPKG-0.1-1.i386.rpm**) from the Thales Customer Support Portal (see "Support Contacts" on page 10).
- If you are installing the patch on a ProtectServer External 2 running software version 5.2.0, ensure that you have **root** access.
- If you are installing the patch on a ProtectServer External 2 running software version 5.4.0, 5.5.0, or 5.6.0, ensure that you have **admin** access.
- If you are running appliance software version 5.7.0, you do not need to apply this patch. Continue to "Updating the Appliance Software" on the next page.

### To install the secure package update patch on a ProtectServer External 2 with appliance software 5.2.0

1. Use **scp** (Linux/UNIX) or **pscp** (Windows) to securely transfer the patch file to the appliance filesystem. Enter the **root** password when prompted.

   ```
   pscp <filepath>\SPKG-0.1-1.i386.rpm root@<appliance_hostname/IP>:/tmp
   ```

   ```
   scp <filepath>/SPKG-0.1-1.i386.rpm root@<appliance_hostname/IP>:/tmp
   ```

2. Connect to the appliance using a monitor and keyboard, serial connection, or SSH, and log in as **root**.
3. Update the RPM package.

   ```
   # rpm -Uvh "SPKG-0.1-1.i386.rpm"
   ```

4. Log out as **root**.

### To install the secure package update patch on a ProtectServer External 2 with appliance software 5.4.0, 5.5.0, or 5.6.0

1. Use **scp** (Linux/UNIX) or **pscp** (Windows) to securely transfer the patch file to the appliance filesystem. Enter the **admin** password when prompted.

   ```
   pscp <filepath>\SPKG-0.1-1.i386.rpm admin@<appliance_hostname/IP>:
   ```

   ```
   scp <filepath>/SPKG-0.1-1.i386.rpm admin@<appliance_hostname/IP>:
   ```

2. Connect to the appliance using a monitor and keyboard, serial connection, or SSH, and log in as **admin**.
3. [Optional] Confirm that the package is available by listing all packages on the appliance.

   ```
   psesh:>package list all
   ```

4. Install the secure package update patch.

   ```
   psesh:>package update -file SPKG-0.1-1.i386.rpm
   ```

5. Exit PSESH.

psesh:>**exit**

## Updating the Appliance Software

The following procedure allows you to update the software image on your ProtectServer External 2 appliance using a secure package.

### Prerequisites

- Download the secure package file from the Thales Customer Support Portal (see "Support Contacts" on page 10).
- You must have **admin** access to the appliance.
- The Admin token must be initialized. See CTCONF in the "Command Line Utilities Reference" section of the *ProtectToolkit-C Administration Guide* for more information about initializing the Admin token.

### To update the appliance software

1. Use **scp** (Linux/UNIX) or **pscp** (Windows) to securely transfer the secure package file to the appliance filesystem. Enter the **admin** password when prompted.

   **pscp** <filepath>****<filename> **admin@**<appliance_hostname/IP>**:**

   **scp** <filepath>**/**<filename> **admin@**<appliance_hostname/IP>**:**

2. Connect to the appliance using a monitor and keyboard, serial connection, or SSH, and log in as **admin**.
3. [Optional] Confirm that the package is available to install.

   psesh:>**package listfile**

4. Install the secure package, specifying the package filename and the authorization code. If the HSM is initialized, enter the Admin Token PIN when prompted.

   psesh:>**package install -spkgfile** <filename> **-authcode** <authcode>

5. Reboot the appliance to complete the update.

   psesh:>**sysconf appliance reboot**

# **CHAPTER 3:** ProtectServer External 2 Plus Installation and Configuration

These steps summarize the overall procedure of setting up a cryptographic service provider using a ProtectServer External 2 Plus in network mode. Relevant links to more detailed documentation are provided at each step.

1. Install the ProtectServer External 2 Plus (See "ProtectServer Network HSM Plus Hardware Installation" on page 1).
2. Check that the ProtectServer External 2 Plus is operating correctly (see "First Login and System Test" on page 51).
3. Configure the ProtectServer External 2 Plusnetwork settings (see "Network Configuration" on page 53).
4. Install and configure the ProtectServer HSM Access Provider software and ProtectToolkit software on your operating system. See the following sections:
   - "Installing ProtectToolkit on Windows" on page 63
   - "Installing ProtectToolkit on Unix/Linux" on page 69
   - "Installing ProtectToolkit on Linux Manually" on page 74
5. Configure the high-level cryptographic API to allow preferred operating modes. Some of these tasks may include:
   - establishing a trusted channel or secure messaging system (SMS) between the API and the ProtectServer External 2.
   - establishing communication between the network client and the ProtectServer External 2.

   Please refer to the relevant high-level cryptographic API documentation:

   - *ProtectToolkit-C Administration Guide*
   - *ProtectToolkit-J Reference Guide*
   - *ProtectToolkit-M User Guide*

# Product Overview

The ProtectServer External 2 Plus is a self-contained, security-hardened server providing hardware-based cryptographic functionality through a TCP/IP network connection. Together with high-level SafeNet application programming interface (API) software, it provides cryptographic services for a wide range of secure applications.

The ProtectServer External 2 Plus is PC-based. The enclosure is a heavy-duty steel case with common PC ports and controls. Necessary software components come pre-installed on a Linux operating system. Network setting configuration is required, as described in this document.

The full range of cryptographic services required by Public Key Infrastructure (PKI) users is supported by theProtectServer External 2 Plus's dedicated hardware cryptographic accelerator. These services include encryption, decryption, signature generation and verification, and key management with a tamper resistant and battery-backed key storage.

The ProtectServer External 2 Plus must be used with one of SafeNet's high-level cryptographic APIs. The following table shows the provider types and their corresponding SafeNet APIs:

| API | SafeNet Product Required |
|---|---|
| PKCS #11 | ProtectToolkit-C |
| JCA / JCE | ProtectToolkit-J |
| Microsoft IIS and CA | ProtectToolkit-M |

These APIs interface directly with the product's FIPS 140-2 Level 3 certified core using high-speed DES and RSA hardware-based cryptographic processing. Key storage is tamper-resistant and battery-backed.

A smart card reader, supplied with the HSM, allows for the secure loading and backup of keys.

## Physical Features

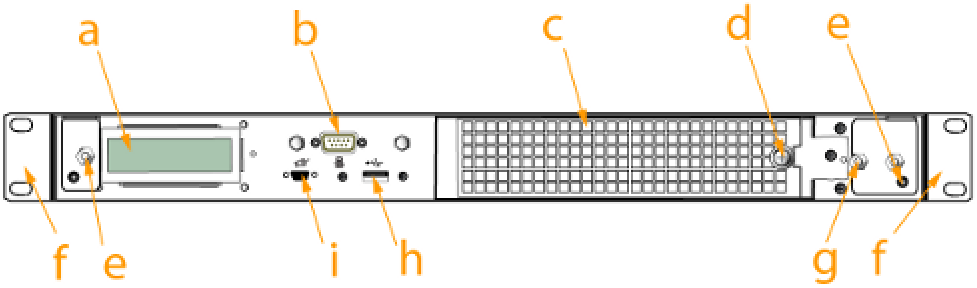
The standard appliance is the 1U-high, rack-mount device:

Here are some of the physical features of the ProtectServer External 2 Plus:

### Front panel view

The features on the front panel of the ProtectServer External 2 Plus are illustrated below:

Figure 9: ProtectServer External 2 Plus front panel

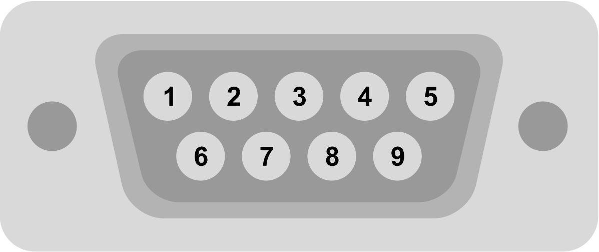


| Item | Name | Description |
|---|---|---|
| a | LCD system status screen | Displays "ProtectServer +" when system is operational. |
| b | Serial (console) port | Local connection for initial setup, and for admin account reset (local-only action for security purposes). |
| c | Ventilation fan-filter cover | Removable bracket allows cleaning of air filter. |
| d | Fan filter cover retaining screw | A captive thumb-screw (no tool needed). |
| e | Mounts for removable front bezel | The protective front bezel mounts on the appliance front panel. Spring clips behind the bezel engage the mounting posts at the left and right ends of the appliances front panel. |
| f | Rack-mount tabs (removable) | Use the tabs on the front and the sliding tabs towards the rear of the appliance to support your SafeNet appliance in a compatible equipment rack. |
| g | Securing screw for fan bay | Torx screw secures the fan bay.<br>**CAUTION!** Opening the fan bay will trigger a tamper event on the device. |
| h/i | USB ports | Unconfigured USB ports. These ports are not necessary for any ProtectServer operations and are left unconfigured for security purposes. |

## HSM serial port pin configuration

The serial port on the USB-to-serial cable, illustrated below, uses a standard RS232 male DB9 pinout:

**Figure 10: HSM serial port pinout**

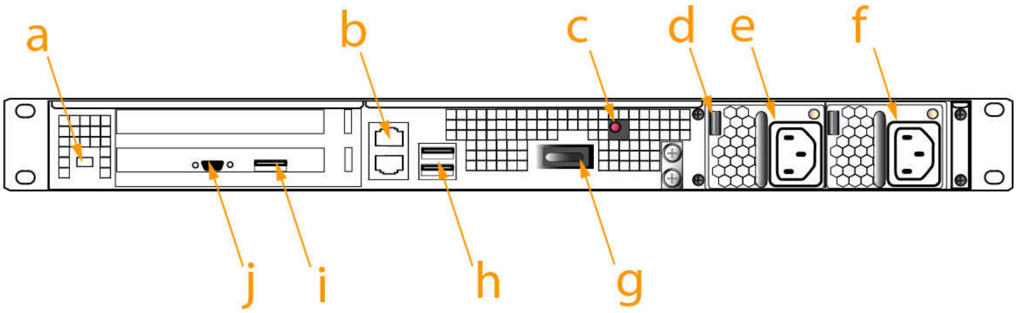


**1**: DCD
**2**: RxD
**3**: TxD
**4**: DTR
**5**: GND
**6**: DSR
**7**: RTS
**8**: CTS
**9**: N/C

## Rear panel view

The features on the rear panel of the ProtectServer External 2 Plus are illustrated below:

**Figure 11: ProtectServer External 2 Plus rear panel**



| Item | Name | Description |
|---|---|---|
| a | Kensington security slot | Attach an industry-standard locking cable for additional physical security. |
| b | Ethernet ports | For network connection of your SafeNet appliance. |
| c | Tamper switch | Recessed for safety, the tamper switch is used during commissioning or decommissioning of the appliance to destroy any keys currently stored on the HSM.<br>**CAUTION!** Activating the tamper switch deletes any keys currently stored on the HSM. Deleted keys are not recoverable. Ensure that you always back up your keys. To avoid accidentally deleting the keys on an operational ProtectServer External 2 Plus, ensure the users with access to the appliance are familiar with the switch. |
| d | Power supply release tab | Press tab to release the catch, and remove the power supply from the appliance. |
| e | Removable power supply | One of two redundant power supplies. |

| Item | Name | Description |
|---|---|---|
| f | Second removable power supply | The other of two redundant power supplies. |
| g | Start/stop switch | Use to stop the system if the command-line shutdown is not available; use to restart the system if it has been switched off. |
| h | USB ports | Unconfigured USB ports. These ports are not necessary for any ProtectServer operations and are left unconfigured for security purposes. |
| i | HSM USB port | Connects USB devices such as the USB smart card reader and the legacy card reader to the HSM. |
| j | Unused port | This port is not used for the ProtectServer External 2 Plus; we recommend that you do not remove the covers that are installed at the factory. |

## Cryptographic architecture

A hardware-based cryptographic system consists of three general components:

> One or more hardware security modules (HSMs) for key processing and storage.

> High-level cryptographic API software. This software uses the HSM's cryptographic capabilities to provide security services to applications.

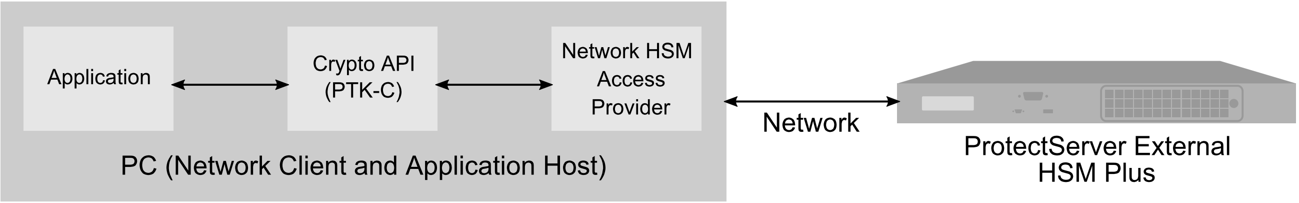
> Access provider software to allow communication between the API software and the HSMs.

Operating in network mode, a standalone ProtectServer External 2 Plus can provide key processing and storage.

In network mode, access provider software is installed on the machine hosting the cryptographic API software. The access provider allows communication between the API and the ProtectServer Network HSM Plus over a TCP/IP connection. The HSM can therefore be located remotely, improving the security of cryptographic key data

The figure below depicts a cryptographic service provider using the ProtectServer External 2 Plus in network mode.

**Figure 12: ProtectServer External 2 Plus implementation**


Application
Crypto API (PTK-C)
Network HSM Access Provider
PC (Network Client and Application Host)
Network
ProtectServer External HSM Plus

## Technical Specifications

The ProtectServer External 2 Plus specifications are as follows:

### Hardware

- Protective, heavy duty steel, industrial PC case
- Intel® Pentium® CPU G6950 2.80GHz
- 2 GB RAM
- 250 GB hard disk drive
- 10/100/1000 Mbps autosensing Network Interface with RJ45 LAN connector
- Dual power supplies

### Pre-installed Software

- Linux operating system
- SafeNet PCI HSM Access Provider software
- SafeNet HSM Net Server software

### Power Supply

- Nominal power consumption: 156 W
- Input AC voltage range: 100-240 V
- Input frequency range: 50-60 Hz

### Physical properties

- 482 mm (W) x 533 mm (D) x 44 mm (H) (1U)
- 19” rack mounting brackets included
- Weight 12.7 kg (28 lb)

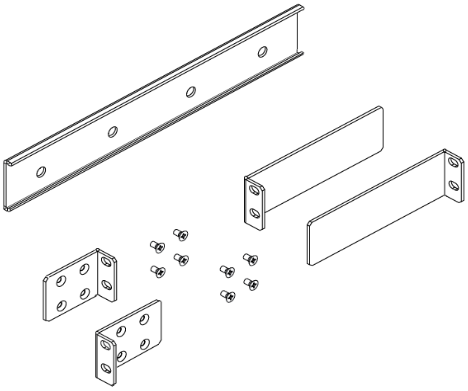
### Operating Environment

- Temperature: 0 to 40 °C (32 to 104 °F)
- Relative Humidity: 5 to 85%

# ProtectServer External 2 Plus Required Items

Follow this checklist to verify that you have all of the items required for the installation.

| Qty | Item |
|---|---|
| 1 | **ProtectServer External 2 Plus Appliance**<br> |
| 1 | **Null-Modem Serial Cable**<br> |
| 1 | **USB 2.0 to RS232 Serial Adapter**<br> |
| 1 | **Smart card reader**<br> |

| Qty | Item |
|---|---|
| 5 | **Smart cards** (in a single media case)<br>Each smart card contains a total of 64 kilobytes of storage space.<br> <br> THALES<br>ProtectServer<br>HSM Smartcard<br>FW V5.03.01 and above |
| 1 | Set of:<br>> 2 front Mounting Brackets with Screws<br>> 2 Side Bracket Guides<br>> 2 Sliding Rear Brackets (fit into the guides for rear support adjustable positioning).<br> |
| 1 | **Client / SDK Software** |

> **NOTE**
>
> - The smart cards and smart card reader are only included with your order if you purchased your ProtectServer HSM with a ProtectServer HSM Accessory Kit.
> - Power cables are no longer included with the shipment from our factory. Many customers are buying HSMs from one country, but shipping them for final deployment to different countries, which has resulted in many wasted power cables that are incorrect format for destination countries. Please source your power cables locally for the deployment destination.
> - Software is available by download from Thales. Physical media for software and documentation are special-request items.

## Optional Items

The following items can be used with your ProtectServer HSM. Contact your Thales sales representative to order these items.

> **SafeNet 110 Time-Based OTP Token** (enables multifactor authentication on ProtectServer HSM tokens)

Thales recommends ordering at least two (2) OTP tokens for each slot on the HSM (one each for the Security Officer and Token User).

PN: 955-000237-001

> **ProtectServer-compatible Verifone PIN pad** (enables manual key component entry)

PN: 934-000087-001

# Installing the ProtectServer External 2 Plus Hardware

This section provides basic hardware installation instructions (mounting in a rack, connecting cables, etc.). The ProtectServer External 2 Plus appliance comes with front brackets and side-rails and sliders for the rear brackets, packed separately in the carton.

## Installation Notes

1. Any computer that is to act as a client to the ProtectServer External 2 Plus appliance must have the Client software installed. Windows users should log in to your computer as a user with Administrator privileges.
2. A computer that is to be used only for administering the ProtectServer External 2 Plus does not need the Client software - only an SSH client such as the PuTTY program that we have provided for Windows, or the SSH utilities that come standard with most Linux and UNIX platforms.
3. Both tasks (Client, and administration) can be performed on a single computer, but in normal practice they are often separate tasks for separate computers.

## Installing the ProtectServer External 2 Plus Hardware

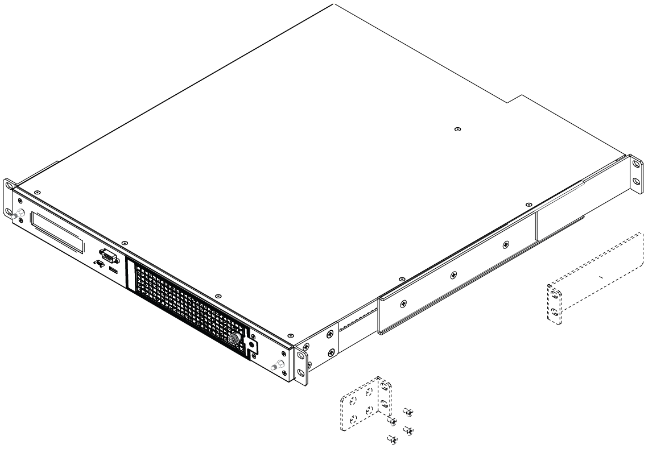
You can optionally install the brackets if they suit your equipment rack. The front brackets can be installed with their tabs forward (for flush-mount of the appliance) or reversed, to allow the front of the appliance to stand out from the rack. The rear brackets install in either direction - as appropriate for your rack post spacing - with the brackets simply sliding into the rails on each side of the appliance.

The supplied brackets are designed and intended for 4-point support of the appliance, in racks with rear-post depth up to 22 inches.

> **CAUTION!** Do not attempt to mount the appliance using only the front brackets - damage can occur.

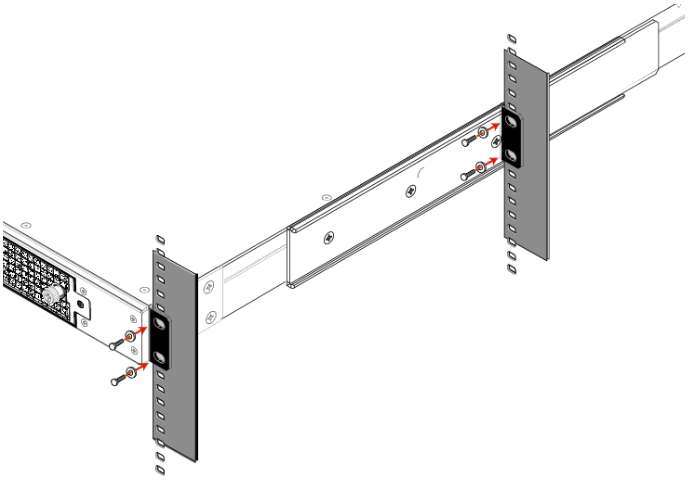
### To install the ProtectServer External 2 Plus hardware

1. Install and adjust rails and brackets to suit your equipment rack



2. Mount the appliance in your equipment rack. Alternatively, ignore the rails and mounting tabs, and rest the ProtectServer External 2 Plus appliance on a mounting tray or shelf suitable for your specific style and brand of equipment rack.

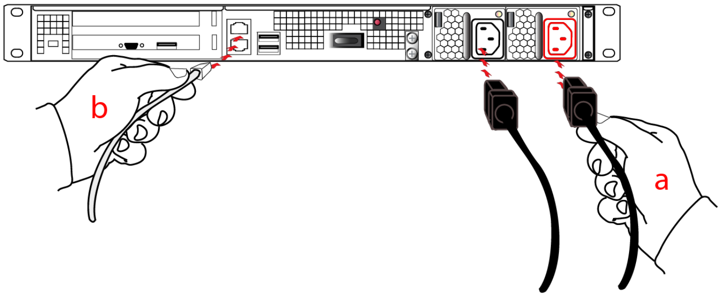
> **CAUTION!** Support the weight of the appliance until all four brackets are secured.



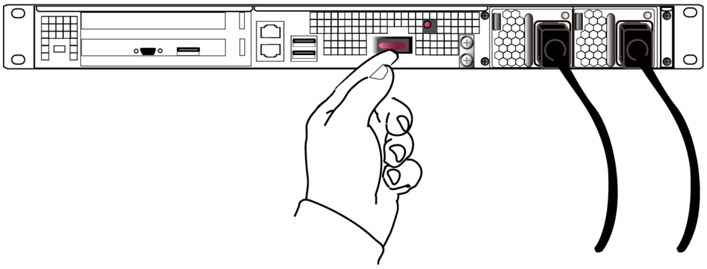
3. Insert the power (a) and network (b) cables at the rear panel.

   The ProtectServer External 2 Plus is equipped with two NICs (*eth0* and *eth1*) incorporating an IPv4/IPv6 dual stack, allowing you to configure both an IPv4 and IPv6 address on each interface. If you intend to use both NICs, connect Ethernet cables to both LAN connectors.

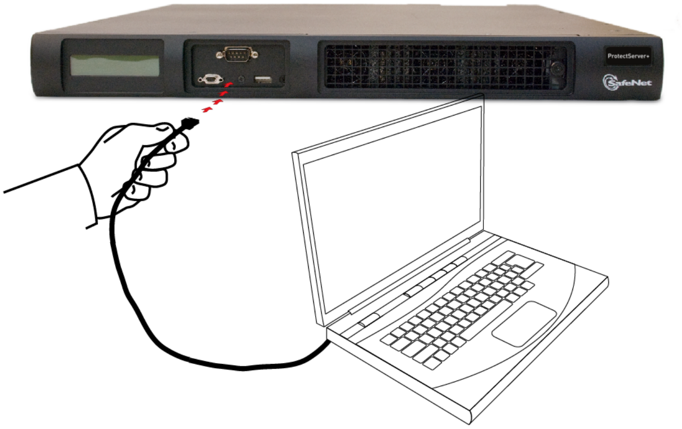
   For proper redundancy and best reliability, the power cables should connect to two independent power sources.



4. Press and release the Start/Stop switch, on the rear panel.



5. Connect a terminal to the serial connector on the front panel.



6. If you have already installed ProtectToolkit client software, refer to the *ProtectToolkit-C Administration Guide*.

## Smart Card Reader Installation

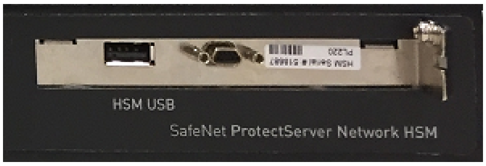
The unit supports the use of smart cards with a SafeNet-supplied smart card reader. Other smart card readers are not supported.

The ProtectServer Network HSM Plus supports two different card readers:

- the new USB card reader (introduced in 5.2)
- the legacy card reader, which provides a serial interface for data (via a USB-to-serial cable) and a PS/2 interface for power (direct or via a PS/2 to USB adapter)

### Installing the USB smart card reader

To install the USB card reader, simply plug the card reader into the HSM USB port on the back of the device, as illustrated below.



### Installing the legacy card reader

To install the smart card reader, connect it to the HSM USB port with the included USB-to-serial cable.

The legacy card reader must also be connected to a PS/2 port for its power. Many newer servers have USB ports, but do not provide a PS/2 connection.

If there is no available PS/2 connection, there are two options:

> Connect a PS/2-to-USB adapter between the card reader and a USB port on the ProtectServer Network HSM Plus.

> If, for security reasons, you prefer to not expose USB ports on your crypto server, connect a PS/2-to-USB adapter cable between the card reader and a standalone powered USB hub.

**NOTE** The USB connection is for power only. No data transfer occurs over this connection.

Next, see "First Login and System Test" on page 51.

# Deployment Guidelines

Users must consider the following best practices for security and compliance when deploying the ProtectServer External 2 Plus for their network/application environment:

> "Secure Messaging System (SMS)" on the next page

> "Networking and Firewall Configuration" on the next page

> "Separation of Roles" on page 51

## Secure Messaging System (SMS)

ProtectServer HSMs store cryptographic keys and objects in tamper-resistant secure memory, which is erased when a tamper is detected. The stored keys are accessed through PKCS#11 calls from the client. Client calls to a Network HSM traverse the network layer (TCP/IP). In the default security mode, this communication channel between the HSM and the client is unencrypted. Configure the HSM security policy to improve this channel's security. Refer to Security Flags in the "Security Policies and User Roles" section of the *ProtectToolkit-C Administration Guide* for descriptions of the available flags and how they affect your implementation.

The Secure Messaging System (SMS) enhances the security of the client-HSM channel. SMS provides an encrypted channel between the client and the HSM and authenticates messages on that channel using a Message Authentication Code (MAC) approved by the FIPS 140-2 standard. Refer to Secure Messaging in the "Cryptoki Configuration" section of the *ProtectToolkit-C Administration Guide* for a detailed description of SMS functionality.

> **NOTE** SMS encrypts and authenticates messages between the client and HSM, but does not provide means for the HSM to authenticate client credentials or vice-versa.

The HSM supports the following SMS modes:

- HIMK
- ADH
- ADH2 (PTK 5.4 and above)

For secure deployment, use ADH or ADH2. Refer to Secure Messaging in the "Cryptoki Configuration" section of the *ProtectToolkit-C Administration Guide* for descriptions of the difference between these modes.

The SMS feature is flexible and can be configured to:

- Encrypt/decrypt all messages
- Sign/verify all messages
- Allow only FIPS-approved mechanisms
- Rotate signing and encryption keys after a specified number of packets or hours
- All of the above

For maximum security, enable all of the above features. See Security Flags in the "Security Policies and User Roles" section of the *ProtectToolkit-C Administration Guide* for flag descriptions and setup instructions.

> **NOTE** Enabling FIPS mode will block all mechanisms that are not FIPS-approved. If you are using unapproved mechanisms and understand the implications, do not enable FIPS mode.

## Networking and Firewall Configuration

There is no means to authenticate the client to the HSM or vice-versa. It is therefore recommended that the HSM and client are connected to the same secure network segment, to prevent sensitive data from traveling through insecure intermediate network(s). This configuration prevents Man-in-the-Middle and other malicious attacks. If possible, connect the HSM directly to the client using a cross-cable.

The ProtectServer External 2 Plus includes two network ports, each of which can be connected to a different network. It is highly recommended that you keep the management network and the network running your applications isolated from each other at all times. Further restrictions on communication between network segments can be enforced by means of static routes. See "Network Configuration" on page 53 for instructions on setting up static routes.

The ProtectServer External 2 Plus supports an iptables-based firewall. The firewall must be configured with appropriate rules to restrict access to identified network resources only. See "Network Configuration" on page 53 for details on setting iptables.

## Separation of Roles

The ProtectServer External 2 Plus has two role categories: Appliance and HSM users. For optimal security, maintain these roles and their credentials separately; do not share between users. Do not share the appliance management, HSM Administration, and User terminals.

### Appliance Users

The following roles can log in to the PSE shell (PSESH) to configure and manage the appliance:

- admin
- pseoperator
- audit

See Using PSESH in the *PSESH Command Reference Guide* for the responsibilities of each role.

### HSM Users

The following roles can log in to manage the HSM token and perform cryptographic operations:

- Administration Security Officer (ASO)
- Administrator
- Security Officer (SO)
- Token Owner (User)

See User Roles in the *ProtectToolkit-C Administration Guide* for the responsibilities of each role.

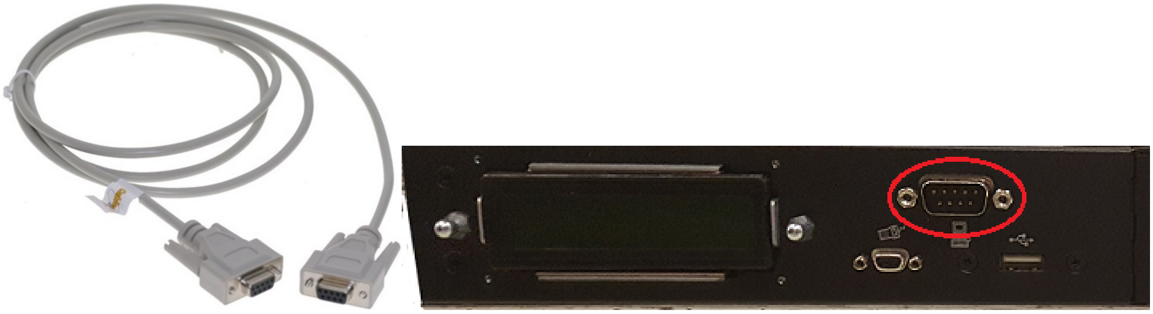
# First Login and System Test

When starting up your ProtectServer External 2 Plus for the first time, follow these steps:

- "Access the Console" below
- "Power on and Log in" on the next page
- "Run System Test" on page 53

## Access the Console

To test the system and configure the network, you must first access the ProtectServer External 2 Plus console. You must connect a terminal directly to the serial port on the front end of the appliance with a null modem serial cable. Use the console port to configure at least one of the network interfaces.



### To access the console

1. Connect a null-modem serial cable (supplied) between the serial port on the HSM appliance front panel and a dumb terminal or a PC or laptop that will serve as the administration machine.
2. Use a terminal emulation package provided with your operating system. Set the Serial connection parameters:
   - Serial port baud rate: 115200
   - N,8,1 (no parity, 8 data-bits, one stop-bit)
   - VT-100 terminal emulation
   - hardware flow control selected

## Power on and Log in

Power on the ProtectServer External 2 Plus. Power-up is complete when the login prompt appears:

```
Protect Server External 5.9.1.0
PSE+ login:
```

You can log in as **admin** or **pseoperator** to access the PSE shell (PSESH), which provides a CLI for configuring and managing the appliance. See the *PSESH Command Reference Guide* for command syntax. There is a third account, **audit**, which is used to configure audit logging on the appliance. This account cannot be used to perform administrative tasks.

The default passwords for the **admin** and **pseoperator** users are:

| User name | Default password |
|---|---|
| **admin** | **password** |
| **pseoperator** | **password** |

After logging in, you will be prompted to change the password for the account. Please remember your password. To change the account password at any time, login to the account and use the command **user password**.

The **admin** user can reset all account passwords to their factory defaults at any time with the PSESH command **sysconf appliance factory**. This command will also reset the SNMP and network settings to their factory defaults.

> **CAUTION!** Executing **sysconf appliance factory** over an SSH connection may cause you to lose connection with the appliance when the IP address is reset. To avoid this, use a serial connection instead when using this command.

## Run System Test

Before field testing and deployment, run the diagnostic utility. While logged in as the **admin** or **pseoperator** enter the command **hsm state** to display the current status:

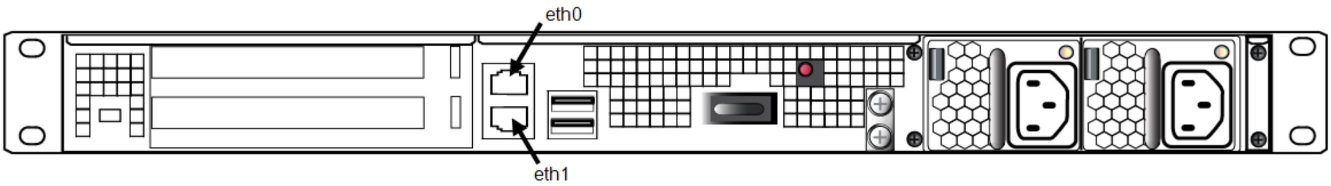
```
psesh:>hsm state

HSM device 0:   HSM in NORMAL MODE. RESPONDING to requests. Usage Level=0%
State = (0x8000, 0xffffffff)
Host Interface   = PSIe2

Command Result : 0 (Success)
```

You can also use the PSESH command **status** to check each of the HSM's processes. See the *PSESH Command Reference Guide* for command syntax.

# Network Configuration

The ProtectServer External 2 Plus is intended to be installed in a data center and accessed remotely over a network. Network access is provided by two Ethernet LAN ports.

The network device interfaces (eth0 and eth1) are located on the back of the appliance, as illustrated below:



## Appliance configuration

The following network parameters are configured at the appliance level:

- Appliance hostname. A hostname is optional, unless you are using DNS.

## Ethernet LAN device configuration

The ProtectServer External 2 Plus is equipped with two individually-configurable Ethernet LAN network devices. You can configure the following network settings for each device:

- IPv4 or IPv6 address. You can configure IPv4 addresses using static or DHCP addressing. IPv6 addresses must be configured as static addresses.
- Network gateway. Devices must use a gateway appropriate for the network (IPv4 or IPv6).
- Network mask. IPv4 devices must use dotted-quad format (for example, 255.255.255.0). IPv6 devices can use full or shorthand syntax.
- Static network route.

- DNS configuration. Although you configure DNS at the device level, the settings you configure for a device are available to all devices on the appliance if the configured device is connected to the network. To ensure DNS access, it is recommended that you configure each device. You can configure the following settings:
  - DNS nameservers
  - DNS search domains

  These settings apply to static network configurations only. If you are using DHCP, the DNS search domains and DNS nameservers configured on the DHCP server are used.

## Gathering Appliance Network Information

Before you begin, obtain the following information (see your network administrator for most of these items):

### HSM Appliance Network Parameters

- IP address and subnet mask for each LAN port you want to use (if you are using static IP addressing)
- Hostname for the HSM appliance (registered with network DNS)
- Domain name (per port)
- Default gateway IP address (per port)
- DNS Name Server IP address(es) (per port)
- Search Domain name(s) (per port)
- Device subnet mask (per port)

### DNS Entries

- Ensure that you have configured your DNS Server(s) with the correct entries for the appliance and the client.
- If you are using DHCP, then all references to the Client and the HSM appliance (as in Certificates) should use hostnames.

## Configuring the Network Parameters

You can use the serial connection to configure all of your network parameters, or configure a single port and use it to access the appliance over the network and complete the configuration.

> **NOTE** Use a locally-connected serial terminal when changing the appliance IP address, to avoid SSH admin console disconnection.

### To configure the appliance and port network parameters:

It is recommended that you configure and test each device. You need to know the IP address of at least one network interface to establish an SSH connection to the appliance.

1. Login to the appliance as **admin** or **pseoperator**.
2. Configure the IP address, network mask, and gateway (optional) on at least one of the Ethernet LAN ports (eth0 or eth1). You can specify a static address, or retrieve one from a DHCP server. You can configure each port to use an IPv4 or IPv6 address.

> **NOTE** IPv6 addresses must be configured as static addresses.

| | |
|---|---|
| **Static** | psesh:> **network interface static -device** <netdevice> **-ip** <IP> **-netmask** <IP> [**-gateway** <IP>] |
| **DHCP** | psesh:> **network interface dhcp -device** <netdevice> |
| **IPv6** | psesh:> **networkinterfaceipv6-device** <netdevice> **-ip** <IP> [**-gateway** <IP>] |

Either of these commands will prompt you to restart the network service.

3. [Optional] Configure network interface bonding. This allows the two network devices to function as a single interface, with a single MAC address, improving bandwidth and providing redundancy.

> **NOTE** Configure network interface bonding with static IPv4 addresses only. If DHCP is used, the bond will be broken if one interface is assigned a different IP.

psesh:>**network interface bonding config -ip** <IP> **-netmask** <IP> [**-gateway** <IP>] [**-mode** <mode>]

psesh:>**network interface bonding enable**

psesh:>**sysconf appliance reboot**

Multiple bonding modes provide different options for load-balancing between the two physical interfaces:

- **0**: Balance Round Robin. Packets are transmitted alternately on each device in the bond, providing load balancing and fault tolerance.
- **1**: Active-Backup. One bonded device is active and the other serves as a backup. The backup only becomes active if the active device loses connectivity.
- **2**: Balance XOR. Transmits based on an XOR formula, where the source MAC address is XOR'd with the destination MAC address. The same bonded device is selected for each destination MAC address, providing load balancing and fault tolerance.
- **3**: Broadcast. All packets are transmitted on both bonded interfaces, providing fault tolerance.
- **4**: 802.3ad (Dynamic Link Aggregation). Creates aggregated groups that share the same speed and duplex settings. This mode requires a switch that supports IEEE 802.3ad dynamic links. The dvice used for an outgoing packet is selected by the transmit hash policy (by default, a simple XOR). This policy can be changed via the xmit_hash_policy option. **NOTE:** Check the 802.3ad standard to ensure that your transmit policy is 802.3ad-compliant. In particular, check section 43.2.4 for packet mis-ordering requirements. Non-compliance tolerance may vary between different peer implementations.
- **5**: Balance TLB (Transmit Load Balancing). Outgoing traffic is distributed according to the current load and queue on each bonded device. Incoming traffic is received by the current device.
- **6**: Balance ALB (Adaptive Load Balancing). Both outgoing and incoming traffic is load-balanced like outgoing traffic in mode 5. Incoming load balancing is governed by ARP negotiation. The bonding driver intercepts the ARP replies sent by the appliance and overwrites the source hardware address with the unique hardware address of one of the bonded devices. Different clients will therefore use different hardware addresses for the appliance.

4. [Optional] Set the appliance hostname and domain name.

psesh:> **network hostname** <hostname>

psesh:> **network domain** <netdomain>

You must configure your DNS server to resolve the hostname to the IP address configured on the Ethernet port of the appliance. Do this for each Ethernet port connected to a network. See your network administrator for assistance.

5. [Optional] Add a domain name server to the network configuration for the appliance. The name server is added to the appliance DNS table. There is one DNS table that applies to all network devices (ports) on the appliance.

   psesh:> **network dns add nameserver** <IP_address> **-device** <net_device>

   > **NOTE** The domain name settings apply to static network configurations only. If you are using DHCP, the DNS name servers configured on the DHCP server are used.

   When you add a DNS server to a specific network device, it is added to the DNS table for the appliance and becomes available to both devices, provided the device you added it to is connected to the network. For example, if you add a DNS server to eth0, eth1 will be able to access the DNS server if eth0 is connected to the network. If eth0 is disconnected from the network, eth1 also loses DNS server access. To ensure that any DNS server you add is available in the event of a network or port failure, it is recommended that you add it to both network-connected devices.

6. [Optional] Add a search domain to the network configuration. These are automatically appended to an internet address you specify in PSESH. For example, if you add the search domain **mycompany.com**, entering the command **network ping hsm1** would search for the domain **hsm1.mycompany.com**. If the domain resolves, it pings the device with that hostname.

   lunash:> **network dns add searchdomain** <domain> **-device** <net_device>

   The search domain is added to the appliance DNS table.

   > **NOTE** The search domain settings apply to static network configurations only. If you are using DHCP, the DNS search domains configured on the DHCP server are used.

   When you add a DNS search domain to a specific network device, it is added to the DNS table for the appliance and becomes available to both devices, provided the device you added it to is connected to the network. For example, if you add a DNS server to eth0, eth1 will be able to access the DNS server if eth0 is connected to the network. If eth0 is disconnected from the network, eth1 also loses DNS server access. To ensure that any DNS server you add is available in the event of a network or port failure, it is recommended that you add it to both network-connected devices.

   If you have chosen to perform setup via SSH, you will likely lose your network connection as you confirm the change of IP address from the default setting.

7. [Optional] Add iptables ACCEPT and DROP rules to manage network access to the appliance.

   By default, the ProtectServer Network HSM allows access to all networks and hosts. The default policy for the INPUT and OUTPUT chain is set to ACCEPT. The default policy for the FORWARD chain is set to DROP, since the ProtectServer Network HSM is not used to forward packets, as in a router or proxy.

   > **CAUTION!** If you are configuring iptables via SSH, a malformed rule can cause a lockout.

   a. To add an ACCEPT rule, specify a host or network:

psesh:> **network iptables addrule accept host -ip** <IP_address>

psesh:> **network iptables addrule accept network -net** <IP_address> **-mask** <netmask>

b. To add a DROP rule, specify a host or network:

psesh:> **network iptables addrule drop host -ip** <IP_address>

psesh:> **network iptables addrule drop network -net** <IP_address> **-mask** <netmask>

c. To see the current list of rules:

psesh:> **network iptables show**

d. To delete a rule, specify the rule's position on the list:

psesh:> **network iptables delrule -rulenum** <number>

A rule's number is based on its current list position, so executing **network iptables delrule -rulenum 1** multiple times will eventually delete the entire list.

e. Save your iptables changes:

psesh:> **network iptables save**

You must execute this command, or any changes will be lost on the next appliance reboot.

8. After making any change to the network configuration, reboot the appliance:

psesh:> **sysconf appliance reboot**

9. View the new network settings:

psesh:> **network show**

### SSH Network Access

After you have completed the network configuration, you can access the ProtectServer External 2 Plus over the network using the SSH protocol. You need an SSH client such as puTTY (available for free from www.putty.org).

## Powering off the ProtectServer External 2 Plus

Use PSESH to power off the appliance.

#### To power off the ProtectServer External 2 Plus

While logged in to PSESH as **admin** or **pseoperator**, issue the command:

psesh:> **sysconf appliance poweroff**

Wait for the appliance to perform shutdown procedures. the fan and LEDs will remain operational until shutdown is complete.

## Updating the Appliance Software Image

Thales provides secure update packages on the Customer Support Portal that allow the appliance administrator to update the appliance software image on your ProtectServer External 2 Plus and take advantage of new PSESH functionality. If you are updating the appliance software from version 5.6.0 or earlier, you must first install the secure package update patch, also available from the Support Portal.

- "Installing the Secure Update Package Patch" below
- "Updating the Appliance Software" on the next page

## Installing the Secure Update Package Patch

The following procedure allows you to install the secure package update patch on your ProtectServer External 2 Plus appliance running appliance software 5.2.0 to 5.6.0. You only need to apply the patch once; future updates require "Updating the Appliance Software" on the next page only.

### Prerequisites

- Download the patch (**SPKG-0.1-1.i386.rpm**) from the Thales Customer Support Portal (see "Support Contacts" on page 10).
- If you are installing the patch on a ProtectServer External 2 running software version 5.2.0, ensure that you have **root** access.
- If you are installing the patch on a ProtectServer External 2 running software version 5.4.0, 5.5.0, or 5.6.0, ensure that you have **admin** access.
- If you are running appliance software version 5.7.0, you do not need to apply this patch. Continue to "Updating the Appliance Software Image" on the previous page.

### To install the secure package update patch on a ProtectServer External 2 Plus with appliance software 5.2.0

1. Use **scp** (Linux/UNIX) or **pscp** (Windows) to securely transfer the patch file to the appliance filesystem. Enter the **root** password when prompted.

   **pscp** <filepath>**\SPKG-0.1-1.i386.rpm root@**<appliance_hostname/IP>**:**/tmp

   **scp** <filepath>**/SPKG-0.1-1.i386.rpm root@**<appliance_hostname/IP>**:**/tmp

2. Connect to the appliance using a monitor and keyboard, serial connection, or SSH, and log in as **root**.
3. Update the RPM package.

   # **rpm -Uvh "SPKG-0.1-1.i386.rpm"**

4. Log out as **root**.

### To install the secure package update patch on a ProtectServer External 2 Plus with appliance software 5.4.0, 5.5.0, or 5.6.0

1. Use **scp** (Linux/UNIX) or **pscp** (Windows) to securely transfer the patch file to the appliance filesystem. Enter the **admin** password when prompted.

   **pscp** <filepath>**\SPKG-0.1-1.i386.rpm admin@**<appliance_hostname/IP>**:**

   **scp** <filepath>**/SPKG-0.1-1.i386.rpm admin@**<appliance_hostname/IP>**:**

2. Connect to the appliance using a monitor and keyboard, serial connection, or SSH, and log in as **admin**.
3. [Optional] Confirm that the package is available by listing all packages on the appliance.

   psesh:>**package list all**

4. Install the secure package update patch.

   psesh:>**package update -file SPKG-0.1-1.i386.rpm**

5. Exit PSESH.

   psesh:>**exit**

## Updating the Appliance Software

The following procedure allows you to update the software image on your ProtectServer External 2 Plus appliance using a secure package.

### Prerequisites

- Download the secure package file from the Thales Customer Support Portal (see "Support Contacts" on page 10).
- You must have **admin** access to the appliance.
- The Admin token must be initialized. See CTCONF in the "Command Line Utilities Reference" section of the *ProtectToolkit-C Administration Guide* for more information about initializing the Admin token.

### To update the appliance software

1. Use **scp** (Linux/UNIX) or **pscp** (Windows) to securely transfer the secure package file to the appliance filesystem. Enter the **admin** password when prompted.

   **pscp** <filepath>****<filename> **admin@**<appliance_hostname/IP>**:**

   **scp** <filepath>**/**<filename> **admin@**<appliance_hostname/IP>**:**

2. Connect to the appliance using a monitor and keyboard, serial connection, or SSH, and log in as **admin**.
3. [Optional] Confirm that the package is available to install.

   psesh:>**package listfile**

4. Install the secure package, specifying the package filename and the authorization code. If the HSM is initialized, enter the Admin Token PIN when prompted.

   psesh:>**package install -spkgfile** <filename> **-authcode** <authcode>

5. Reboot the appliance to complete the update.

   psesh:>**sysconf appliance reboot**

# CHAPTER 4: ProtectToolkit Software Installation

This section contains instructions for installing the various ProtectToolkit software components and configuring them for your client machine. Refer to the system requirements below, and then the section for your client operating system:

## System Requirements

ProtectToolkit 5.9.1 has the following prerequisites for installation:

- Java runtime (required for graphical user interface utilities only). The product has been tested using Java runtime version 6.x, 7.x, 8.x, 9.x, 10.x, and 11.x.

> **NOTE**
>
> - The older (minor) versions of Java 7 or Java 8 could cause issues with the SAFENET java library (**jprov_sfnt.jar**). Thales Group recommends updating Java 7/8 to the latest version.
> - Warnings appear when compiling some of the provided Java samples with Java runtime 9, 10, or 11 installed. These warnings can be safely ignored.

- .NET versions 3.5 and 4.5 (Windows only). All required .NET versions are available for download from Microsoft.
- Microsoft Visual C++ 2005, 2008, 2010 (Windows only). All required MSVC versions are available for download from Microsoft.

> **NOTE** The Java runtime, .NET and Microsoft Visual C++ must be installed first.

### Supported Platforms

The supported platforms are listed in the following table.

C=ProtectToolkit-C, PKCS #11 v2.10/2.20

M=ProtectToolkit-M, MS CSP 2.0 with CNG

J=ProtectToolkit-J, Java runtime 6.x/7.x/8.x/9.x/10.x/11.x.

> **NOTE** Do not upgrade to ProtectToolkit 5.9.1 if you are using the legacy PSG HSM.

| Operating System | | OS type | 64-bit PTK | 64-bit PTK supported hardware | 32-bit PTK | 32-bit PTK supported hardware |
|---|---|---|---|---|---|---|
| Windows | 10 | 64-bit | C/M/J | PCIe2, PSE2, PSE2+ | C/J | PSE2, PSE2+ |
| | Server 2019 | 64-bit | C/M/J | PCIe2, PSE2, PSE2+ | C/J | PSE2, PSE2+ |
| | Server 2016 | 64-bit | C/M/J | PCIe2, PSE2, PSE2+ | C/J | PSE2, PSE2+ |
| | Server 2012 R2 | 64-bit | C/M/J | PCIe2, PSE2, PSE2+ | C/J | PSE2, PSE2+ |
| | Server 2008 (R1 and R2) | 64-bit | C/M/J | PCIe2, PSE2, PSE2+ | C/J | PSE2, PSE2+ |
| | 7 | 32-bit | - | - | C/J (KSP support) | PCIe2, PSE2, PSE2+ |
| | 7 | 64-bit | C/M/J | PCIe2, PSE2, PSE2+ | C/J | PSE2, PSE2+ |
| Linux | RHEL 8.7* | 64-bit | C/J | PCIe2, PSE2, PSE2+ | - | - |
| | RHEL 7 | 64-bit | C/J | PCIe2, PSE2, PSE2+ | C/J | PSE2, PSE2+ |
| | RHEL 6 | 32-bit | - | - | C/J | PCIe2, PSE2, PSE2+ |
| | RHEL 6 | 64-bit | C/J | PCIe2, PSE2, PSE2+ | C/J | PSE2, PSE2+ |
| | SUSE12 | 64-bit | C/J | PCIe2, PSE2, PSE2+ | C/J | PSE2, PSE2+ |

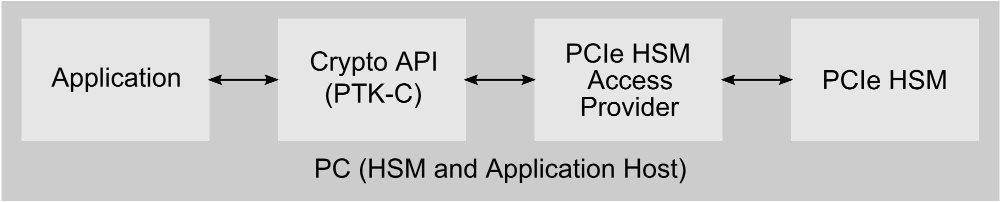
| Operating System | | OS type | 64-bit PTK | 64-bit PTK supported hardware | 32-bit PTK | 32-bit PTK supported hardware |
|---|---|---|---|---|---|---|
| AIX | 7.2 | 64-bit | C/J | PSE2, PSE2+ | C/J | PSE2, PSE2+ |
| | 7.1 | 64-bit | C/J | PSE2, PSE2+ | C/J | PSE2, PSE2+ |
| | 6.1 | 64-bit | C/J | PSE2, PSE2+ | C/J | PSE2, PSE2+ |
| Solaris | 11 (SPARC, x86)<br>10 (SPARC, x86) | 64-bit | C/J | PSE2, PSE2+ | C/J | PSE2, PSE2+ |
| HP-UX | 11 | 64-bit | C/J | PSE2, PSE2+ | C/J | PSE2, PSE2+ |

* Requires the RHEL 8.7 Support Patch.

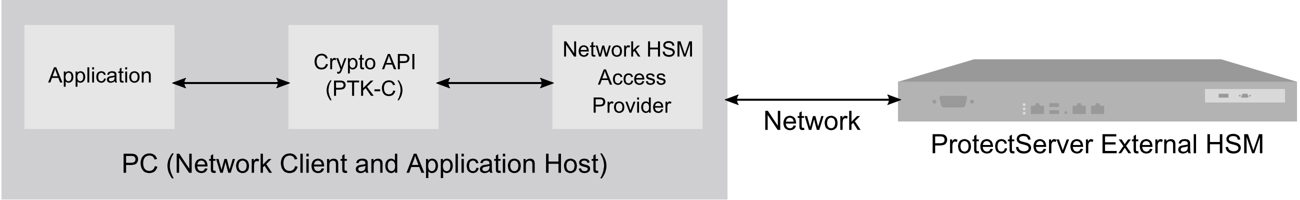
# Operating Modes

ProtectToolkit-C can be used in one of three *operating modes*. These are:

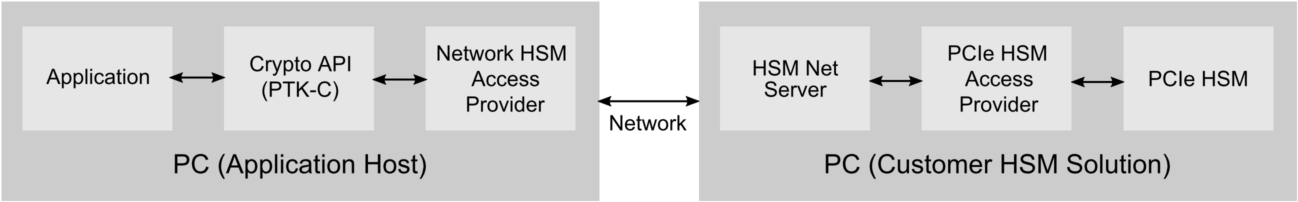
> **PCI mode** in conjunction with a locally-installed ProtectServer PCIe 2.



> **Network mode** over a TCP/IP network, in conjunction with a compatible product such as the ProtectServer External 2.


Application
Crypto API (PTK-C)
Network HSM Access Provider
PC (Network Client and Application Host)
Network
ProtectServer External HSM

A machine with a ProtectServer PCIe 2 installed may also be used as a server in network mode.



> **Software-only mode** on a local machine without access to a hardware security module.

Within the client/server runtime environment, the server performs cryptographic processing at the request of the client. The server itself will only operate in one of the hardware runtime modes.

The software-only version is available for a variety of platforms, including Windows NT and Solaris, and is typically used as a development and testing environment for applications that will eventually use the hardware variant of ProtectToolkit-C.

# Installing ProtectToolkit on Windows

This section provides instructions for installing ProtectToolkit on a Windows client. If you would like to upgrade a ProtectToolkit component, you must first uninstall the component (See "Uninstalling ProtectToolkit" on page 68) and then reinstall it by following the instructions in this section.

This section contains the following subsections:

> "Prerequisites" below

> "Installing the ProtectServer HSM Access Provider on Windows" on the next page

> "Installing ProtectToolkit-C on Windows" on page 65

> "Installing ProtectToolkit-J on Windows" on page 66

> "Installing ProtectToolkit-M on Windows" on page 67

> "Configuring ProtectToolkit" on page 67

> "Uninstalling ProtectToolkit" on page 68

## Prerequisites

> Review the "System Requirements" on page 60 to ensure your operating system is supported and that you have installed the required Java runtime, MSVC, and .NET components.

> Review the "Operating Modes" on the previous page as they apply to your HSM deployment.

> Ensure that your ProtectServer HSM is installed and configured for access over a network (if applicable):

- "ProtectServer PCIe 2 Installation" on page 13
- "Installing the ProtectServer External 2 Hardware" on page 25
- "Installing the ProtectServer External 2 Plus Hardware" on page 46

If you are planning to operate ProtectToolkit in PCIe or network mode, you must install the ProtectServer HSM Access Provider software before installing ProtectToolkit components. See "Installing the ProtectServer HSM Access Provider on Windows" on the next page

If you are setting up ProtectToolkit to run in Software-only mode, HSM setup and ProtectServer HSM Access Provider installation are unnecessary.

> Download the latest ProtectToolkit product installation packages from the Thales Customer Portal.

> Ensure that you have administrator privileges on the system.

> For ProtectToolkit-M:

- Microsoft Internet Information Services (IIS) should be installed, configured, and working if integration with IIS is desired.
- A ProtectServer HSM must be available.

## Installing the ProtectServer HSM Access Provider on Windows

This section provides instructions for installing the ProtectServer HSM Access Provider software on a Windows client. The following Access Provider installation packages are available:

- **PTKpcihsmK6.msi** installs the device driver for a compatible, locally-installed cryptographic services adapter such as the ProtectServer PCIe 2.
- **PTKnethsm.msi** installs the Net Client software required to provide cryptographic services using SafeNet hardware devices over a TCP/IP network.
- **PTKnetsrv.msi** installs the components required to make an installed ProtectServer PCIe 2 HSM available on the network to other ProtectToolkit clients.

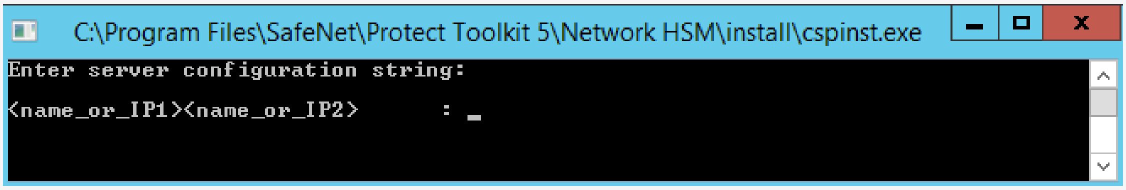
### To install the ProtectServer HSM Access Provider on Windows

1. Run the ProtectServer HSM Access Provider installation package that is relevant to your HSM deployment:
   - **ProtectServer External 2 in Network Mode:**
     - Install **PTKnethsm.msi** on the local machine.
   - **ProtectServer PCIe2 in Network Mode:**
     1. Install **PTKpcihsmK6.msi** on the server machine.
     2. Install **PTKnetsrv.msi** on the server machine.
     3. Install **PTKnethsm.msi** on the local machine.
   - **ProtectServer PCIe2 in PCIe Mode:**
     - Install **PTKpcihsmK6.msi** on the local machine.
2. Work through the installation wizard to complete the installation.

**NOTE** The following information applies to the installation of **PTKpcihsmK6.msi** and **PTKnethsm.msi**:

> If you are installing **PTKpcihsmK6.msi**, a reboot may be required to successfully load the driver.

> If you are installing **PTKnethsm.msi** the following command window appears during installation:



C:\Program Files\SafeNet\Protect Toolkit 5\Network HSM\install\cspinst.exe

```
Enter server configuration string:
<name_or_IP1><name_or_IP2>      : _
```

Specify the hostname or IP address of one or more HSMs on the network, separated by single spaces. The server listening port is **12396**. If you do not enter a configuration string, the default server **Localhost** is used. This setting can be used for testing purposes, to simulate access to HSM slots across a network when the HSM is in fact located in the local (client) machine.

The server configuration string is stored in the Windows registry as a configuration item (**ET_HSM_NETCLIENT_SERVERLIST**). After installation, change this configuration item's value to permanently change server details. To change server details temporarily, use an environment variable to override the registry setting.

For more information about configuration items, see "Configuration Items" on page 85.

## Installing ProtectToolkit-C on Windows

This section provides instructions for installing ProtectToolkit-C on a Windows client.

### To install ProtectToolkit-C on Windows

1. Run the installation package for the ProtectToolkit-C component that you would like to install:
   - **PTKcprt.msi** installs all the necessary tools and interfaces for a PTK-C Cryptoki service provider.
   - **PTKcpsdk.msi** installs the PTK-C software development platform. Header files are included, in addition to the PTK-C Runtime.

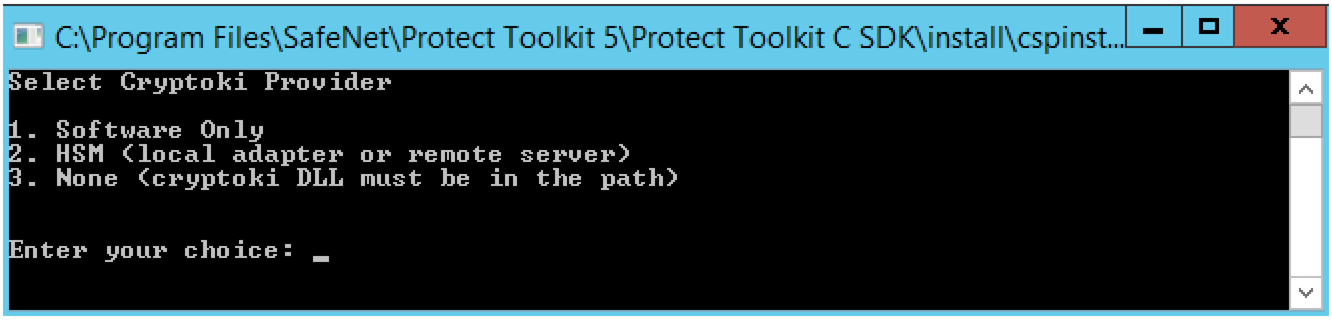
   **NOTE** The **PTK-C Runtime** and **PTK-C SDK** packages cannot be installed at the same time. To switch between them, first uninstall the package you no longer wish to use.

   – **PTKfmsdk.msi** installs the Functionality Module (FM) development platform. Install this component if you plan to develop FMs to add custom functionality to the ProtectServer HSM. Requires the **PTK-C SDK** component as a prerequisite.

   **NOTE** Thales recommends that you develop and test FMs in Software Emulation mode before installing them on your production HSMs. This installation package is located in the folder for your architecture in the installation directory.

2. Work through the installation wizard to complete the installation.

If you selected the ProtectToolkit-C SDK package, a command window is displayed during the installation process (shown below) that gives the option to update the **PATH** to include the required Cryptoki provider. This will make the correct installed programs and libraries available from the command prompt.


C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\install\cspinst...

```
Select Cryptoki Provider

1. Software Only
2. HSM (local adapter or remote server)
3. None (cryptoki DLL must be in the path)


Enter your choice: _
```

| If... | then select... |
|---|---|
| The SDK is to be used without access to a HSM (software-only mode)<br>**CAUTION!** Software-only mode is not secure, as cryptographic material is stored on the host system and not a ProtectServer HSM. | Software Only |
| An HSM will be available (PCI or network operating modes) | HSM |
| The Cryptoki provider required is already in the path (this might be the case if you are upgrading) | None |

For more information about the available options see "Operating Modes" on page 62.

> **NOTE** The Cryptoki provider can be changed after installing the **PTK-C SDK** package. For more information about changing the Cryptoki provider, see "Changing the Cryptoki Provider" on page 68 below.

## Installing ProtectToolkit-J on Windows

This section provides instructions for installing ProtectToolkit-J on a Windows client.

The Provider may be statically installed into the Java Runtime Environment by adding an entry, similar to the following, into the **java.security** properties file located in **$JAVA_HOME/lib/security/java.security security.provider.2 = au.com.safenet.crypto.provider.SAFENETProvider**

Alternatively, the Provider may be installed dynamically by an application at runtime by using the **java.security.Security.addProvider()** method. For example:

**Security.addProvider(new au.com.safenet.crypto.provider.SAFENETProvider());**

If the Provider is to be used on a specific Slot, the format for the above references should be:

**au.com.safenet.crypto.provider.slot <*n*>.SAFENETProvider**

### To install ProtectToolkit-J on Windows

1. Run the installation package for the ProtectToolkit-J component that you would like to install:
   - **PTKjprt.msi** installs all the necessary tools and interfaces for a PTK-J Cryptoki service provider, using the Java Cryptographic Architecture (JCA) / Java Cryptographic Extension (JCE) interface. **NOTE:** PTK-J requires the PTK-C Runtime component as a prerequisite.
     - **PTKjpsdk.msi** installs the PTK-J software development platform, for developing Java applications for use with your ProtectServer HSM.
2. Work through the installation wizard to complete the installation.

The installation program will create a new program group named **Safenet\ProtectToolkit J\Runtime** and add it to your **Start** menu. Program files are saved to **C:\Program Files\SafeNet\Protect Toolkit 5**.

## Installing ProtectToolkit-M on Windows

This section provides instructions for installing ProtectToolkit-M on a Windows client.

Full support for ProtectToolkit-M is provided on 64-bit versions of Windows only. 32-bit versions support KSP only.

### To install ProtectToolkit-M on Windows

1. Run the installation package for the ProtectToolkit-M component that you would like to install:
   - **PTKmprt32.msi** or **PTKmprt64.msi** installs the necessary tools and interfaces tor a PTK-M Cryptoki service provider, using Microsoft's cryptographic API. **NOTE:** PTK-M requires the PTK-C Runtime component as a prerequisite.
   - **Win32\SafenetKSP32.msi** or **Win64\SafenetKSP64.msi** installs components for using PTK-M with Microsoft's updated Cryptography Next Generation API (CNG).
2. Work through the installation wizard to complete the installation.

## Configuring ProtectToolkit

When you have completed the installation, refer to "Configuration Items" on page 85 for additional PTK client configuration options, then to the guides for your installed components:

> *ProtectToolkit-C Administration Guide*

> *ProtectToolkit-J Reference Guide*

> *ProtectToolkit-M User Guide*

> *ProtectToolkit FM SDK Programming Guide*

If you have installed ProtectToolkit-C and intend to use PCIe or network operating modes:

> Configure the secure messaging system (SMS). Refer to Secure Messaging in the "Cryptoki Configuration" section of the *ProtectToolkit-C Administration Guide*.

> Establish network communication (network operating mode only) by configuring the client to use one or more servers that are available on the same network. Refer to "Specifying the Network Server(s)" on page 93.

If you have installed ProtectToolkit-C and intend to use software-only mode:

> Customize the installation to optimize performance. Refer to "Software-Only Mode Configuration" on page 92.

## Changing the Cryptoki Provider

The **setmode** executable binary file allows the user to toggle between software-only and HSM (PCI or network HSM) operating modes, after installing the **PTK-C SDK** package.

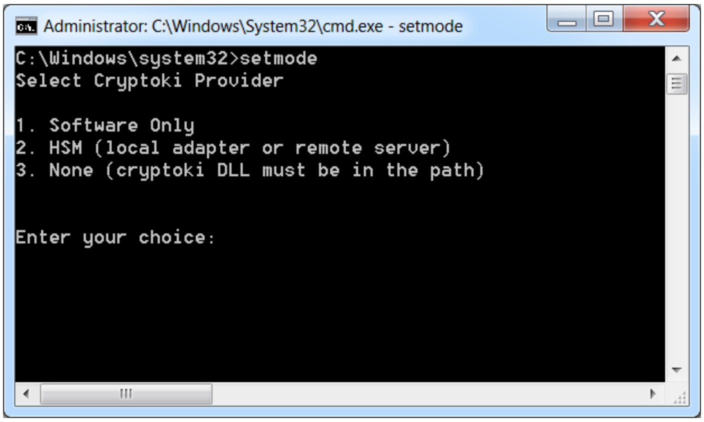
> **CAUTION!** Software-only mode is not secure, as cryptographic material is stored on the host system and not a ProtectServer HSM.

### To change the active Cryptoki provider

1. Execute **setmode** from the command line or open the **SetMode.cmd** file in the SafeNet install directory (default path: **C:\Program Files\SafeNet\Protect Toolkit 5\Protect Toolkit C SDK\bin\SetMode.cmd**).

   > **NOTE** This tool edits the Windows registry, so you must have Administrator privileges on the client machine or an Unauthorized Access error will be returned. If you receive this error, open the command prompt or **SetMode.cmd** file by right-clicking and selecting **Run as Administrator**.

   The **Select Cryptoki Provider** dialog appears.



```
C:\Windows\system32>setmode
Select Cryptoki Provider

1. Software Only
2. HSM (local adapter or remote server)
3. None (cryptoki DLL must be in the path)


Enter your choice:
```

2. Select your desired operating mode and click **Next** to complete the operation.

## Uninstalling ProtectToolkit

You can modify an existing ProtectToolkit client installation/configuration or upgrade a PTK component by uninstalling and then reinstalling the PTK component.

### To uninstall ProtectToolkit components from Windows

1. Navigate to **Programs and Features** in the Windows Control Panel.
2. Locate and select the PTK component that you would like to uninstall.

> **NOTE** If you are uninstalling ProtectToolkit-M:
>
> - Tamper the HSM to destroy key information stored on the HSM that is no longer required. See Tampering the HSM in the "Administrative Tasks" section of the *ProtectToolkit-M User Guide* for more information.
> - Uninstall the PCIe HSM access provider (if it is installed) before uninstalling the ProtectToolkit-M software. Failure to do so may prevent the ProtectToolkit-M software from uninstalling correctly.

3. Select **Uninstall**.

# Installing ProtectToolkit on Unix/Linux

Installation and uninstallation commands are different for each of the supported Unix platforms. To account for these differences, the package should be installed using the Unix Installation Utility. Manual commands specific to your operating system can be used, but this is not the recommended method. The Installation Utility is more likely to result in a problem-free installation or uninstallation. The latest versions of the client software and HSM firmware can be found on the Thales Technical Support Customer Portal. See "Support Contacts" on page 10 for more information.

The utility provides a simple menu-driven interface. In addition to installing and uninstalling the access provider on Unix systems, it can also:

- List already-installed packages
- List directory contents, for the current platform or all platforms
- Install a package from the directory (which also installs the utility in **/usr/bin**)
- Change the default operating mode (hardware or software-only).

Whenever the utility installs a package, it also installs itself on the host system's hard disk (in **/usr/bin/safeNet-install.sh**). This copy can be used to uninstall or configure the software.

You must become the superuser of the host system before adding or removing any packages.

> **NOTE** If you are installing ProtectToolkit 5.9.1 on an AIX system, you must first download ProtectToolkit 5.9 from the Thales Support Portal and install it by following the procedures described in this section.

The following procedures are described below:

- "Utility Startup" on the next page
- "Available Packages" on page 71
- "Installing a package" on page 71
- "Setting up your environment" on page 72
- "Changing the Cryptoki provider" on page 72
- "Configuring ProtectToolkit" on page 73
- "Uninstalling a package" on page 73

> "Boot Service Operation on Unix/Linux Platforms" on page 74

## Utility Startup

Options can be specified when executing the **safeNet-install.sh** command. These options are not normally required and are mainly useful for troubleshooting. To troubleshoot an issue you are experiencing while using the installation utility, refer to ProtectToolkit 5.9.1 Installation Issues in the *ProtectServer HSM and ProtectToolkit Troubleshooting Guide*.

### Syntax

**safeNet-install.sh** [**-h**] [**-p**] [**-s** <size>] [**-v**]

| Option | Description |
|---|---|
| **-h** | Show help. |
| **-p** | Plain mode. In this mode the '**tput**' is not used for video enhancements. |
| **-s**<size> | Override the screen size (default = '**tput lines/cols**' or **24x80**). |
| **-v** | Print the version of this script. |

If you wish to enter platform-specific commands manually, use the commands given in "Installing ProtectToolkit on Linux Manually" on page 74.

### To start up the utility

1. The Thales Unix Installation Utility is located in the installation image's root directory. Unzip the image by following standard procedure for your platform and installation.
2. Change to the unzipped directory and start the utility. The utility scans the system and the directory and displays the Main Menu.

```
Gemalto Unix Installation Utility:
Hostname: 66 (Linux 2.6.32-504.16.2.el6.i686)
Main menu

1 list Gemalto packages already installed
2 list packages on CD
3 install a package from this CD
4 uninstall a Gemalto package
5 Set the default cryptoki and/or hsm link

q quit the utility



Choice (1 2 3 4 q) [Redraw]:
```

> **NOTE** Enter '**b**' to go back to the previous menu and '**q**' to quit the utility. You can also quit with the system **INTR** key (normally **^C**).

## Available Packages

This section provides a description of each available ProtectToolkit package and its prerequisites. The packages are listed below in their most ideal installation order.

> **NOTE** Install only the packages required for your deployment.

- **SafeNet Network HSM Access Provider:** installs the components required to access a ProtectServer HSM over the network, whether a ProtectServer External 2, ProtectServer External 2 Plus, or ProtectServer PCIe 2 configured for network access.
- **SafeNet PCIe HSM Access Provider (Device Driver):** installs the device driver components for a ProtectServer PCIe 2 HSM installed in the host system.
- **SafeNet HSM Net Server:** installs the components required to make an installed ProtectServer PCIe 2 HSM available on the network to other ProtectToolkit clients. Requires an installed ProtectServer PCIe 2 and the **SafeNet PCIe HSM Access Provider** package as prerequisites.
- **SafeNet ProtectToolkit C Runtime:** installs all the necessary tools and interfaces for a ProtectToolkit-C based Cryptoki service provider. Requires the correct **Access Provider** package for your deployment as a prerequisite.
- **SafeNet ProtectToolkit C SDK:** installs the PTK-C software development platform. Header files are included, in addition to the **PTK-C Runtime**. Requires the correct **Access Provider** package for your deployment as a prerequisite.

> **NOTE** The **PTK-C Runtime** and **PTK-C SDK** packages cannot be installed at the same time. To switch between them, first uninstall the package you no longer wish to use.

- **SafeNet ProtectToolkit J Runtime:** installs all the necessary tools and interfaces for a PTK-J Cryptoki service provider, using the Java Cryptographic Architecture (JCA) / Java Cryptographic Extension (JCE) interface. **NOTE:** PTK-J requires the **PTK-C Runtime** component as a prerequisite.
- **SafeNet ProtectToolkit J SDK:** installs the PTK-J software development platform, for developing Java applications for use with your ProtectServer HSM.
- **SafeNet ProtectToolkit FM SDK:** installs the ProtectToolkit Functionality Module Software Development Kit for building FMs or host applications. Requires the **PTK-C SDK** as a prerequisite. You must also install the **FM Toolchain**.

> **NOTE** You cannot install the ProtectToolkit runtime and FM SDK on the same machine. It is recommended that you do your FM development on a separate machine.

- **SafeNet 1.i686.rpm FM Toolchain:** installs the components required to compile and run your Functionality Modules. Requires the **PTK-C SDK** and **FM SDK** as prerequisites.

## Installing a package

Should you encounter any problems, please see "Installing ProtectToolkit on Unix/Linux" on page 69.

### To install a package

1. Select **install a package from this CD** from the utility's Main Menu.

   A list of installable SafeNet packages is displayed.

2. Select the package required by typing the appropriate menu number followed by **Enter**.

   The utility verifies the action and executes the appropriate command for your platform.

3. On some platforms, you may be prompted for additional installation options. On Linux, for example, you can add a **-nodeps** option to suppress the checking of dependencies. These options should be selected with appropriate care.
4. You may now need to respond to any platform-specific messages (for example: to confirm you wish to proceed with the installation).
5. After installation, the utility will return **Success** or **Failure**, scan the system again, and display the current installation status. Press the **Enter** key to continue.

## Setting up your environment

After installing the software on Linux platforms, you must run the ProtectToolkit**setvars.sh** script to configure your environment for the ProtectToolkit software. You cannot run the script directly, but instead you must source it or add it to a startup file (for example, **.bashrc**). If you source the script, your environment will be set for the current session only. If you add it to your startup file, your environment will be set each time you log in.

### To set up your environment

1. Go to the ProtectToolkit software installation directory:

   **cd /opt/safenet/protecttoolkit5/ptk**

2. Source the **setvars.sh** script:

   **. ./setvars.sh**

Once installed and configured, the software is ready to use under **/opt/safenet**.

When you have completed the installation, refer to "Configuration Items" on page 85 for additional PTK client configuration options, then to the guides for your installed components:

- *ProtectToolkit-C Administration Guide*
- *ProtectToolkit-J Reference Guide*
- *ProtectToolkit FM SDK Programming Guide*

## Changing the Cryptoki provider

On Unix/Linux systems, the software-only Cryptoki provider is made active by default. If you plan to use this instance of ProtectToolkit-C with a ProtectServer HSM, you will need to change the Cryptoki provider. Software-only mode is not secure, as cryptographic material is stored on the host system. You can use the Unix Installation Utility to change modes.

### To change the Cryptoki provider

1. From the **Main menu**, select **Set the default cryptoki and/or HSM link**.

The **Cryptoki Selection** screen is displayed.

```
Gemalto Unix Installation Utility:
Hostname: 66 (Linux 2.6.32-504.16.2.el6.i686)
Main Menu >> Check/Set Default Cryptoki & HSM Menu

-------------------- Cryptoki Selection --------------------
1   SafeNet ProtectToolkit C SDK Software (emulator)
2 * SafeNet ProtectToolkit C SDK Runtime (hardware)
3 * SafeNet Network HSM Access Provider

b back
q quit the utility



Choice (1 2 3 b q) [Redraw]:
```

2. Select **SafeNet ProtectToolkit C SDK Runtime (hardware)** and confirm your selection.

## Configuring ProtectToolkit

When you have completed the installation, refer to "Configuration Items" on page 85 for additional PTK client configuration options, then to the guides for your installed components:

> *ProtectToolkit-C Administration Guide*

> *ProtectToolkit-J Reference Guide*

> *ProtectToolkit-M User Guide*

> *ProtectToolkit FM SDK Programming Guide*

If you have installed ProtectToolkit-C and intend to use PCI or network operating modes:

> Configure the secure messaging system (SMS). Refer to Secure Messaging in the "Cryptoki Configuration" section of the *ProtectToolkit-C Administration Guide*.

> Establish network communication (network operating mode only). by configuring the client to use one or more servers that are available on the same network. Refer to "Specifying the Network Server(s)" on page 93.

If you have installed ProtectToolkit-C and intend to use software-only mode:

> Customize the installation to optimize performance. Refer to "Software-Only Mode Configuration" on page 92 .

## Uninstalling a package

Should you encounter any problems, please see "Installing ProtectToolkit on Unix/Linux" on page 69.

### To uninstall a package

1. Select **Uninstall a SafeNet package** from the utility's **Main Menu**.

   A list of installed SafeNet packages is displayed.

2. Select the required package by typing the appropriate menu number and pressing **Enter**.

   The utility verifies the action and executes the appropriate command for your platform.

3. On some platforms, you may be prompted for additional uninstallation options. On Linux, for example, you can add a **-nodeps** option to suppress the checking of dependencies. These options should be selected with appropriate care.
4. After completing uninstallation, the utility will return **Success** or **Failure**, scan the system again, and display the current installation status.
5. You may now need to respond to any platform-specific messages to confirm that you wish to proceed with the uninstallation. Press the **Enter** key to continue.

## Boot Service Operation on Unix/Linux Platforms

To run the server as an **rc.d(init.d)**service, run the following script:

```
/opt/safenet/protecttoolkit5/netsrv/bin/etnetsrv_install_rc
```

# Installing ProtectToolkit on Linux Manually

The simplest way to complete installation or uninstallation of ProtectToolkit compnents, or to change the Cryptoki provider, is to use the **Unix Installation Utility**. The utility ensures that the correct commands for your platform are executed automatically. See "Installing ProtectToolkit on Unix/Linux" on page 69 for more information.

You must become the superuser of the host system before adding or removing any packages.

> **NOTE** If you are installing ProtectToolkit 5.9.1 on an AIX system, you must first download ProtectToolkit 5.9 from the Thales Support Portal and install it by following the procedures described in this section.

If you wish to install ProtectToolkit components manually, use the commands described in this section after extracting the installation files you downloaded from the Thales Support Portal:

> "Manual Linux Installation for Network Mode" below

> "Manual Linux Installation for PCIe Mode" on the next page

- "Signing the ProtectServer PCIe 2 Driver for UEFI Secure Boot" on the next page

> "Manual Linux Installation for Net Server Mode" on page 77

> "Installing ProtectToolkit-C Manually on Linux" on page 78

- "Changing the Cryptoki Provider manually" on page 78

> "Installing ProtectToolkit-J Manually on Linux" on page 79

> "Installing the ProtectToolkit FMSDK Manually on Linux" on page 80

> "Configuring ProtectToolkit" on page 80

## Manual Linux Installation for Network Mode

Use the following commands to install or uninstall the Network Access Provider package. It includes the components required to access a ProtectServer HSM over the network, whether a ProtectServer External 2, ProtectServer External 2 Plus, or ProtectServer PCIe 2 configured for network access.

### To install the Network Access Provider manually

Execute the following as **root** (where x.x.x-yy is the PTK version number). Specify the location you chose for the installation files:

```
# cd /output-unix/Linux64/network_hsm_access_provider
rpm -i PTKnethsm-x.x.x-yy.x86_64.rpm
```

### To uninstall the Network Access Provider manually

Use the **rpm(8)** command with the appropriate package name as a parameter.

```
# rpm -e PTKnethsm
```

## Manual Linux Installation for PCIe Mode

Use the following commands to install or uninstall the PCIe Access Provider package. It includes the device driver components for a ProtectServer PCIe 2 HSM installed in the host system.

### To install the PCie access provider manually

Execute the following as **root** (where x.x.x-yy is the PTK version number). Specify the location you chose for the installation files:

```
# cd /output-unix/Linux64/pci_hsm_access_provider_PSI-E2
rpm -i PTKpcihsmK6-x.x.x-yy.x86_64.rpm
```

If the compile fails, or the driver does not come up automatically (**hsmstate** fails), you will need to correct the problem and then **cd /opt/ETpcihsm/src** and invoke **make(1)** as root. The **Makefile** in that directory has some notes to help you get the driver compiled correctly.

### To uninstall the PCie access provider manually

Use the **rpm(8)** command with the appropriate package name as a parameter.

```
# rpm -e PTKpcihsmK6
```

## Signing the ProtectServer PCIe 2 Driver for UEFI Secure Boot

Red Hat Enterprise Linux 7 (RHEL 7) can be installed and run on systems where UEFI Secure Boot is enabled. With Secure Boot enabled, the RHEL kernel requires all kernel modules, including device drivers, to be signed by a key that is trusted by the EFI boot loader. If a module is not signed, it is prevented from loading at runtime and the dependent device will not work.

To use ProtectServer PCIe 2 in a Secure Boot-enabled environment, the driver must be signed and trusted by the OS and boot loader.

The following procedure includes:

- Generating RSA signing keys and certificates
- Signing the ProtectServer PCIe driver
- Enrolling the signing public key into the system keyring
- Loading the signed driver

> **NOTE** This procedure applies only to a CentOS 7 environment with UEFI Secure Boot enabled. The steps have been tested on RHEL release 7.6.1810. The **mokutil** utility on earlier versions of Red Hat might show inconsistent behavior. If you encounter problems, upgrade your OS.
>
> Steps may vary on other Linux platforms, but the general procedure is the same.

### Prerequisites

- UEFI Secure Boot must be enabled on the Linux system.
- The ProtectServer PCIe 2 Access Provider must be installed.

  The driver will fail to load and **service vkd status** may return `vkd is not running`.

  System logs might display the error message `could not insert module vkd.ko: Required key not available`. This appears because the driver module **vkd.ko** needs to be signed.
- Driver signing requires that the following tools be available on the system:

| Tool | Provided by Package | Used on | Purpose |
|---|---|---|---|
| **openssl** | *openssl* | Build system | Generates public and private X.509 key pair |
| **sign-file** | *kernel-devel* | Build system | Perl script used to sign kernel modules |
| **perl** | *perl* | Build system | Perl interpreter used to run the signing script |
| **mokutil** | *mokutil* | Target system | Optional tool used to manually enroll the public key |
| **keyctl** | *keyutils* | Target system | Optional tool used to display public keys in the system key ring |

### To sign and load the ProtectServer PCIe 2 driver

1. Create a configuration file with parameters for generating a key pair that satisfies RHEL 7 kernel module signing requirements.

   **# vi** <configuration_filename>**.config**

   ```
   [ req ]
   default_bits = 4096
   distinguished_name = req_distinguished_name
   prompt = no
   string_mask = utf8only
   x509_extensions = myexts

   [ req_distinguished_name ]
   O = Organization
   CN = Organization signing key
   emailAddress = E-mail address

   [ myexts ]
   ```

```
basicConstraints=critical,CA:FALSE
keyUsage=digitalSignature
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid
```

2. Use the **openssl** tool to generate a signing key pair. Specify the configuration file you created, and public and private keys named **MOK.der** and **MOK.priv**. You can use the default locations specified in the command below or specify your own filepaths.

   # **openssl req -x509 -new -nodes -utf8 -sha256 -days 36500 -batch -config** <configuration_filename>**.config -outform DER -out** <public_keyname>**.der -keyout** <private_keyname>**.priv**

3. Use the Machine Owner Key utility (**mokutil**) to enroll your public key on the machine(s) where you wish to load the ProtectServer PCIe 2 driver. When RHEL 7 boots on a UEFI Secure Boot-enabled system, the keys on the MOK list are added to the system keyring.

   a. Request that your public key be added to the MOK list.

      # **mokutil --import** <public_keyname>**.der**

      You are prompted to enter and confirm a password for the request.

   b. Reboot the machine.

      During reboot, the MOK enrollment request is noticed by `shim.efi`, which launches `MokManager.efi` so that you can complete the enrollment from the UEFI console.

   c. When prompted, press any key to perform MOK management.

   d. From the list of options, select **Enroll MOK**.

   e. Select **Continue** and then **Yes** to confirm that you want to enroll the key.

   f. Enter the password you created for the enrollment request.

   g. Select **Reboot** to reboot the machine.

4. Sign the ProtectServer PCIe HSM driver with the private key. This is accomplished using a perl script. You must specify both the private and public key files and the driver file that you wish to sign (vkd.ko).

   **# perl /usr/src/kernels/$**(uname **-r**) **/scripts/sign-file sha256** <private_keyname>**.priv** <public_keyname>**.der /lib/modules/$**(uname **-r**)**/kernel/drivers/crypto/vkd.ko**

5. Load the ProtectServer PCIe driver.

   **# service vkd restart**

## Manual Linux Installation for Net Server Mode

Use the following commands to install or uninstall the Net Server Access Provider package. It includes the components required to make an installed ProtectServer PCIe 2 HSM available on the network to other ProtectToolkit clients. Requires an installed ProtectServer PCIe 2 and the **PCIe HSM Access Provider** package as prerequisites.

### To install the Net Server Access Provider manually

Execute the following as **root** (where x.x.x-yy is the PTK version number). Specify the location you chose for the installation files:

```
# cd /output-unix/Linux64/hsm_net_server
rpm -i PTKnetsrv-x.x.x-yy.x86_64.rpm
```

### To uninstall the Net Server Access Provider manually

Use the **rpm(8)** command with the appropriate package name as a parameter.

```
# rpm -e PTKnetsrv
```

## Installing ProtectToolkit-C Manually on Linux

Use the following commands to install or uninstall ProtectToolkit-C.

### To install ProtectToolkit-C manually

1. Choose the PTK-C package you wish to install:
   - **ProtectToolkit C Runtime:** installs all the necessary tools and interfaces for a ProtectToolkit-C based Cryptoki service provider. Requires the correct **Access Provider** package for your deployment as a prerequisite.
   - **ProtectToolkit C SDK:** installs the PTK-C software development platform. Header files are included, in addition to the **PTK-C Runtime**. Requires the correct **Access Provider** package for your deployment as a prerequisite.

   > **NOTE** The Runtime and SDK packages cannot be installed concurrently. To switch from one package to the other, uninstall the package that is no longer required and then install the new one.

2. Execute the following as **root** for your selected package (where x.x.x-yy is the PTK version number). Specify the location you chose for the installation files:
   - **ProtectToolkit C Runtime:**

     ```
     # cd /output-unix/Linux64/PTKC_Runtime
     rpm -i PTKcprt-x.x.x-yy.x86_64.rpm
     ```

   - **ProtectToolkit C SDK:**

     ```
     # cd /output-unix/Linux64/hsm_net_server
     rpm -i PTKcpsdk-x.x.x-yy.x86_64.rpm
     ```

3. Add the **/opt/safenet/protecttoolkit5/ptk/bin** directory to the execution path and the **/opt/safenet/protecttoolkit5/ptk/lib** directory to the library path. The following commands may be used to configure your paths for the **sh**(1) shell.

Once installed, the software is ready to use under **/opt/safenet/protecttoolkit5.**

### To uninstall the ProtectToolkit-C packages manually

Use the **rpm(8)** command with the appropriate package name as a parameter.

```
# rpm -e PTKcprt
# rpm -e PTKcpsdk
```

## Changing the Cryptoki Provider manually

This section applies to the SDK package only.

Different ProtectToolkit-C Cryptoki provider files are required if an HSM is present (PCI or network mode) or not (software-only mode).

Both Cryptoki provider files are installed with the SDK package. On Unix/Linux systems, the software-only Cryptoki provider is made active by default.

### To change the default Cryptoki provider selection

Remove the soft-link:

```
/opt/safenet/protecttoolkit5/ptk/lib/libcryptoki.so or
/opt/safenet/protecttoolkit5/ptk/lib/libcryptoki.a (for AIX)
```

and recreate it to point to the SafeNet HSM Cryptoki provider. For example, the following shell commands may be used to enable the HSM (executed as the super-user):

```
# cd /opt/safenet/protecttoolkit5/ptk/lib
# rm libcryptoki.so
# ln -s libcthsm.so libcryptoki.so
```

The following shell commands may be used to enable the software emulation (executed as the super-user):

```
# cd /opt/safenet/protecttoolkit5/ptk/lib
# rm libcryptoki.so
# ln -s libctsw.so libcryptoki.so
```

## Installing ProtectToolkit-J Manually on Linux

Use the following commands to install or uninstall ProtectToolkit-J.

> **NOTE** PTK-J requires the **PTK-C Runtime** component as a prerequisite.

### To install ProtectToolkit-J manually

1. First, install the **ProtectToolkit J Runtime** package, which includes all the necessary tools and interfaces for a PTK-J Cryptoki service provider, using the Java Cryptographic Architecture (JCA) / Java Cryptographic Extension (JCE) interface.

   Execute the following as **root** (where x.x.x-yy is the PTK version number). Specify the location you chose for the installation files:

   ```
   # cd /output-unix/Linux64/PTKJ_Runtime
   rpm -i PTKjprov-x.x.x-yy.x86_64.rpm
   ```

2. If desired, install the **ProtectToolkit J SDK**, for developing Java applications for use with your ProtectServer HSM.

   Execute the following as **root** (where x.x.x-yy is the PTK version number). Specify the location you chose for the installation files:

   ```
   # cd /output-unix/Linux64/PTKJ_SDK
   rpm -i PTKjpsdk-x.x.x-yy.x86_64.rpm
   ```

### To uninstall the ProtectToolkit-J packages manually

Use the **rpm(8)** command with the appropriate package name as a parameter.

```
# rpm -e PTKjpsdk
# rpm -e PTKjprov
```

## Installing the ProtectToolkit FMSDK Manually on Linux

Use the following commands to install or uninstall the ProtectToolkit Functionality Module Software Development Kit for building FMs or host applications.

> **NOTE** PTK-J requires the **PTK-C Runtime** component as a prerequisite.
>
> You cannot install the ProtectToolkit runtime and FM SDK on the same machine. It is recommended that you do your FM development on a separate machine.

### To install the FMSDK packages manually

1. First, install the FMSDK package. Execute the following as **root** (where x.x.x-yy is the PTK version number). Specify the location you chose for the installation files:

```
# cd /output-unix/Linux64/fm_sdk
rpm -i PTKfmsdk-x.x.x-yy.x86_64.rpm
```

2. Install the FM Toolchain package, which includes the components required to compile and run your Functionality Modules.

   Execute the following as **root** (where x.x.x is the PTK version number). Specify the location you chose for the installation files:

```
# cd /output-unix/Linux64/fm_toolchain
rpm -i eldk-x.x.x.i686.rpm
```

### To uninstall the ProtectToolkit FMSDK packages manually

Use the **rpm(8)** command with the appropriate package name as a parameter.

```
# rpm -e eldk
# rpm -e PTKfmsdk
```

## Configuring ProtectToolkit

When you have completed the installation, refer to "Configuration Items" on page 85 for additional PTK client configuration options, then to the guides for your installed components:

- *ProtectToolkit-C Administration Guide*
- *ProtectToolkit-J Reference Guide*
- *ProtectToolkit-M User Guide*
- *ProtectToolkit FM SDK Programming Guide*

If you have installed ProtectToolkit-C and intend to use PCI or network operating modes:

- Configure the secure messaging system (SMS). Refer to Secure Messaging in the "Cryptoki Configuration" section of the *ProtectToolkit-C Administration Guide*.
- Establish network communication (network operating mode only). by configuring the client to use one or more servers that are available on the same network. Refer to "Specifying the Network Server(s)" on page 93.

If you have installed ProtectToolkit-C and intend to use software-only mode:

- Customize the installation to optimize performance. Refer to "Software-Only Mode Configuration" on page 92.

# Utilities Command Reference

This chapter provides command reference details for the Unix Installation Utility and the SafeNet hardware maintenance utilities.

## Unix Installation Utility

This utility is for use on Unix systems only. The platforms supported are AIX, Linux, and Solaris. The utility handles installation, uninstallation, and configuration tasks using a simple menu-driven interface.

The utility is described in "safeNet-install.sh" on the next page.

## Hardware Maintenance Utilities

The SafeNet hardware maintenance utilities are installed during the ProtectServer PCIe 2 and ProtectServer External 2 Access Provider installations. The utilities are named **hsmstate** and **hsmreset**.

The utilities are described in "hsmstate" on page 83 and "hsmreset" on page 84.

# safeNet-install.sh

This utility is for use on Unix systems only. It handles installation, uninstallation and configuration tasks using a simple, menu-driven interface.

Whenever the utility installs a SafeNet package, it also installs itself on the host system hard disk (in **/usr/bin/safeNet-install.sh**). This copy can be used to uninstall or configure the software.

For more information, see "Installing ProtectToolkit on Unix/Linux" on page 69.

## Syntax

**safeNet-install.sh** [**-h**] [**-p**] [**-s** <size>] [**-v**]

| Option | Description |
|---|---|
| **-h** | Show help. |
| **-p** | Plain mode. In this mode the '**tput**' is not used for video enhancements. |
| **-s**<size> | Override the screen size (default = '**tput lines/cols**' or **24x80**). |
| **-v** | Print the version of this script. |

# hsmstate

The utility displays the current status of the HSM(s). By default, it reports all HSMs found in the system. The states reported may include:

```
HSM in NORMAL MODE.

HSM is responding to tamper.

HSM is initializing performing POST.
```

## Syntax

**hsmstate** [**-d**<devicenum>] [**-h**] [**-?**] [**-v**] [**-q**]

| Option | Description |
|---|---|
| **-d** <devicenum> | The utility reports only on the present device specified. To list the available devices, run **hsmstate** without any options included. |
| **-h, -?** | Display helpful usage information. |
| **-v** | Verbose flag. This will display a more detailed report about the HSM. |
| **-q** | Quick mode. Prints the state of the HSM and then exits (does not send any requests). |

## Examples

The command **hsmstate** will show all devices found in the system. For example:

```
HSM device 0:      HSM in NORMAL MODE. RESPONDING
HSM device 1:      HSM in NORMAL MODE. RESPONDING
HSM device 2:      HSM in NORMAL MODE. RESPONDING
```

The command **hsmstate -d1 -v** will show a report with full details about device 1. For example:

```
HSM device 1:      HSM in NORMAL MODE. RESPONDING to requests.
State = (0x8000, 0x41403)
I2O_INBOARD_MF_OFFSET = 0kb Reserved memory at beginning of PCI Window
I2O_FRAME_LENGTH = 4kb Length of an I2O Message Frame in KiloBytes
I2O_NUM_FRAMES = 20  Number of message frames in one direction
Host Interface version = V0.3
```

> **NOTE** The information presented with the **-v** option may only be required when contacting technical support.

# hsmreset

This utility clears the HSM of any outstanding requests and prepares it to continue normal operation. It can be used when the HSM is in a normal or halt state.

## Syntax

**hsmreset** [**-d**<instance>] [**-f**] [**-h**] [**-?**] [**-v**]

| Option | Description |
|---|---|
| **-d** <instance> | This option will reset only the device specified. To list the available devices, run **hsmstate** without any options included. |
| **-f** | Force an HSM reset without prompting for confirmation. |
| **-h, -?** | Display helpful usage information. |
| **-v** | Verbose flag. This will display a more detailed report about the HSM. |

## Example

The command **hsmreset** will reset the first HSM. Upon execution, the following message displays:

```
HSM is in normal mode. Resetting it might disturb other applications.
Continue [N/Y]:
```

Type **Y** to complete the operation.

# CHAPTER 5: Configuration Items

This chapter contains instructions for making configuration changes on ProtectServer client and server systems. The procedure for editing configuration items is different for ProtectServer External 2 HSMs, client machines, and systems hosting ProtectServer PCIe 2 HSMs. Please refer to the section relevant to your system:

- "Overview" below
- "Client/PCIe HSM Server Configuration" on the next page
- "ProtectServer External 2 Server Configuration" on page 87

Configuration options are described here:

- "Network Mode Client Configuration Items" on page 89
- "PCI Mode Client Configuration Items" on page 89
- "Network Mode Server Configuration Items" on page 91
- "Software-Only Mode Configuration" on page 92
- "Specifying the Network Server(s)" on page 93

## Overview

During installation, configuration items are created on the host system. Configuration changes are made by editing the values associated with these items. This chapter describes how to make such changes on your system.

Item values can exist at four configuration levels. When a configuration item is queried, item locations are searched in order of level precedence:

1. **Temporary:** Any changes made at the temporary configuration level override any corresponding entries at the user, system, and default levels.
2. **User:** Changes made at the user level override any corresponding entries at the system and default levels.
3. **System:** System changes override default-level entries.
4. **Default:** If no changes have been made at any other level, the default value for the configuration item is used. Default configuration values cannot be changed.

On Windows operating systems, user and system configuration information is stored in the Registry. On Unix-based systems, configuration files are used. Temporary configuration items are applied using environment variables on both Windows and Unix-based platforms.

Regardless of the platform, a common naming convention for configuration items has been followed. Understanding this naming convention will help you locate and change the appropriate configuration items when required.

Configuration items are hierarchical in structure, with the root node **ET**. Child nodes of the root represent the class of the item, and are typically product abbreviations, such as **PTKC** (ProtectToolkit-C) or **HSM** (Hardware Security Module). Nodes under class represent the component, such as **LOGGER** or **SMS**. Finally, nodes under component represent the configuration item, such as **FILE**, **MODE**, or **NAME**. Configuration items therefore take the form:

**ET_<class>_<component>_<item>**

For a list of configurable items, see:

> "PCI Mode Client Configuration Items" on page 89

> "Network Mode Client Configuration Items" on page 89

> "Network Mode Server Configuration Items" on page 91

# Client/PCIe HSM Server Configuration

The procedure for configuring client/PCIe HSM host systems differs between Windows and Linux. Please refer to the relevant section below:

## Windows

### Temporary

Temporary configuration changes are made using environment variables. Since environment variables are not hierarchical, the hierarchy is implicitly defined by the name of the variable.

#### In Network mode, to temporarily change the length of time the HSM will wait before timing out a connection attempt

In a command prompt, enter **set ET_HSM_NETCLIENT_CONNECT_TIMEOUT_SECS=<time_in_seconds>**

### User

User configuration changes are made in the registry tree starting from **HKEY_CURRENT_USER\SOFTWARE\SafeNet**.

#### In Network mode, to change the length of time the HSM will wait before timing out a connection attempt

1. Open **regedit** to **HKEY_CURRENT_USER\SOFTWARE\SafeNet**.
2. Add a new key entitled **HSM** and open it.
3. Add a new key entitled **NETCLIENT** and open it.
4. Add a new string named **ET_HSM_NETCLIENT_CONNECT_TIMEOUT_SECS**.
5. Set the value data to the desired time in seconds.

### System

System configuration changes are made in the registry tree starting from **HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet**.

The name of the ProtectToolkit-C file where the logger library writes log information (**ctlog.log**) is stored in the Windows registry as a string value for the entry:
**ET_PTKC_LOGGER_FILE**

This is located in the key:
**HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\PTKC\LOGGER**

## Unix

### Temporary

Temporary configuration changes are made using environment variables. Since environment variables are not hierarchical in nature, the hierarchy is implicitly defined by the name of the variable.

### User

User Configuration is a set of files located in the **$HOME/.safenet** directory.

### System

System Configuration is a set of files located in the **/etc/default** directory.

The User and System Configuration files are of the form: **et_<class>**. Entries in the file are of the form: **ET_<class>_<component>_<item>=<value>**.

The name of the ProtectToolkit-C file where the logger library writes log information (**ctlog.log**) is stored in the **/etc/default/et_ptkc** file as the entry:

**ET_PTKC_LOGGER_FILE=/ctlog.log**

# ProtectServer External 2 Server Configuration

Server configuration settings on the ProtectServer External 2 are edited by transferring a new configuration file to the appliance, and applying it using PSESH.

### To change the ProtectServer External 2 server configuration

1. Create a text file on your client machine that lists each configuration item and its desired value. For a list of editable configuration items and their valid values, see "Network Mode Server Configuration Items" on page 91.

   For example:

   ```
   ET_HSM_NETSERVER_OLD_WORKER_COUNT=5
   ET_HSM_NETSERVER_V2_WORKER_COUNT=12
   ET_HSM_NETSERVER_READ_TIMEOUT_SECS=40
   ET_HSM_NETSERVER_WRITE_TIMEOUT_SECS=40
   ET_HSM_NETSERVER_CONN_TIMEOUT_COUNT=5
   ET_HSM_NETSERVER_FRAG_SIZE=5000
   ET_HSM_NETSERVER_ALLOW_RESET=OnHalt
   ET_HSM_NETSERVER_PORT=12396
   ET_HSM_NETSERVER_LOG_CHANNEL=0
   ET_HSM_NETSERVER_LOG_NAME=etnetserver
   ET_HSM_NETSERVER_LOG_LEVEL=0
   ```

2. Transfer the configuration file (et_hsm.txt in the example below) to the **admin** or **pseoperator** user on the appliance using **pscp** (Windows) or **scp** (Linux/UNIX):

<table>
<tr><td><b>Windows</b></td><td><b>pscp</b> &lt;filename&gt; admin@&lt;server_host/IP&gt;:<pre>pscp  et_hsm.txt admin@192.168.0.123:
admin@192.168.0.123's password: ********
et_hsm.txt                | 0 kB |   0.4 kB/s | ETA: 00:00:00 | 100%</pre></td></tr>
<tr><td><b>Linux/UNIX</b></td><td><b>scp</b> &lt;filename&gt; admin@&lt;server_host/IP&gt;:<pre>scp et_hsm.txt admin@192.168.0.123:
admin@192.168.0.123's password: ********
et_hsm.txt                | 0 kB |   0.4 kB/s | ETA: 00:00:00 | 100%</pre></td></tr>
</table>

3. Login to PSESH as **admin** or **pseoperator**.

4. If desired, check to ensure that the configuration file was transferred to the appliance.

   psesh:>**files show**

   ```
   psesh:>files show

   SCP Folder Content
   ------------------

   total 0.4K
   0.4K et_hsm.txt

   Command Result : 0 (Success)
   ```

5. Set the etnetserver configuration file. See sysconf etnetcfg in the "PSESH Commands" section of the *PSESH Command Reference Guide* for syntax.

   psesh:>**sysconf etnetcfg set** <filename>

   ```
   psesh:>sysconf etnetcfg set et_hsm.txt

   WARNING !!  This command will modify the settings of the appliance.
               It could affect client connections, and result in an unusable system.
   If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

   > proceed
   Proceeding...
   The config file has been set. To apply the changes, please restart etnetserver


   Command Result : 0 (Success)
   ```

6. Restart the etnetserver service.

   psesh:>**service restart etnetserver**

7. View the new configuration to confirm the changes.

   psesh:>**sysconf etnetcfg show**

   ```
   psesh:>sysconf etnetcfg show


   etnetserver is running

   Current etnetserver configuration
   ```

```
ET_HSM_NETSERVER_OLD_WORKER_COUNT=5
ET_HSM_NETSERVER_V2_WORKER_COUNT=12
ET_HSM_NETSERVER_READ_TIMEOUT_SECS=40
ET_HSM_NETSERVER_WRITE_TIMEOUT_SECS=40
ET_HSM_NETSERVER_CONN_TIMEOUT_COUNT=5
ET_HSM_NETSERVER_FRAG_SIZE=5000
ET_HSM_NETSERVER_ALLOW_RESET=OnHalt
ET_HSM_NETSERVER_PORT=12396
ET_HSM_NETSERVER_LOG_CHANNEL=0
ET_HSM_NETSERVER_LOG_NAME=etnetserver
ET_HSM_NETSERVER_LOG_LEVEL=0

Command Result : 0 (Success)
```

# PCI Mode Client Configuration Items

Currently, there is only one modifiable configuration item for PCI mode.

> **NOTE** Thales recommends leaving configuration items at the their default value or setting them to a valid value specified in the following table. If the value of a configuration item must be changed and no valid values are given, contact Thales Customer Support for assistance.

For more information about using configuration items see "Configuration Items" on page 85.

| Configuration Item | Meaning |
|---|---|
| `ET_HSM_PCICLIENT_READ_TIMEOUT_SECS` | Determines the time in seconds the PCI driver will wait before timing out on a read operation. It should be set long enough to avoid an unintentional timeout, which causes the driver to shut down the HSM.<br>The default timeout should be long enough for general use. The value should only be modified if the client-side application is expected to wait for a longer duration, as in the case of key entry on a PIN pad.<br>Default=**600** |

# Network Mode Client Configuration Items

The available client configuration items for Network mode and their default values are listed in the following table.

> **NOTE** Thales recommends leaving configuration items at the their default value or setting them to a valid value specified in the following table. If the value of a configuration item must be changed and no valid values are given, contact Thales Customer Support for assistance.

For more information about using configuration items see "Configuration Items" on page 85.

| Configuration Item | Meaning |
|---|---|
| `ET_HSM_NETCLIENT_HEARTBEAT =[ON\|OFF]` | If **ON**, net client is to request and support heartbeat messages from the network server.<br>Default=**OFF** |
| `ET_HSM_NETCLIENT_INACTIVITY_PERIOD_SECS` | Number of seconds of no network activity before a connection is considered inactive.<br>If heartbeat is enabled, a heartbeat message is sent to the network server after this period expires, to keep the connection alive.<br>Default=**60** |
| `ET_HSM_NETCLIENT_LOG_CHANNEL` | Channel (destination) to write log entries to. Values are platform-dependent.<br>For Windows, valid values are:<br>> **0** - Windows Event Log<br>> **1** - Standard out<br>> **2** - Standard error<br>Default=**0**<br>For Unix, valid values are from **0** to **7** inclusive, and map to syslog **LOG_LOCAL#** values.<br>Default=**0** |
| `ET_HSM_NETCLIENT_LOG_NAME` | Name of application/context to associate with log entries.<br>Default=**etnetclient** |
| `ET_HSM_NETCLIENT_READ_TIMEOUT_SECS` | Seconds to allow before timing out a TCP/IP read operation.<br>Default=**300** |
| `ET_HSM_NETCLIENT_SERVERLIST =[host[:port] [host[:port]…]]` | Space separated list of hosts (with optional port number) to connect to.<br>Default host=**localhost**<br>Default port=**12396**<br>IPv6 addresses must be enclosed in square brackets. |
| `ET_HSM_NETCLIENT_WRITE_TIMEOUT_SECS` | Seconds to allow before timing out a TCP/IP write operation.<br>Default=**60** |
| `ET_HSM_NETCLIENT_CONNECT_TIMEOUT_SECS` | Number of seconds before a connection attempt is timed out.<br>Default=**60** |
| `ET_HSM_NETCLIENT_TRACE_DATA =[ON\|OFF]` | If **ON**, user data will be traced.<br>Default=**OFF** |

| Configuration Item | Meaning |
|---|---|
| `ET_HSM_NETCLIENT_TRACE_LEVEL` | The amount of trace to be generated.<br>Valid values are:<br>> **0** - Error only<br>> **1** - Include connections status<br>> **2** - Include API call flow<br>Default=**0** |

# Network Mode Server Configuration Items

The available server configuration items for Network mode and their default values are listed in the following table.

> **NOTE** Thales recommends leaving configuration items at the their default value or setting them to a valid value specified in the following table. If the value of a configuration item must be changed and no valid values are given, contact Thales Customer Support for assistance.

For more information about using configuration items see "Configuration Items" on page 85.

| Configuration Item | Meaning |
|---|---|
| `ET_HSM_NETSERVER_OLD_WORKER_COUNT` | Number of threads to reserve for processing old ProtectToolkit-C remote client connections.<br>Default: **3** |
| `ET_HSM_NETSERVER_V2_WORKER_COUNT` | Number of worker threads, per HSM, to reserve for processing new net client connections.<br>Default: **10** |
| `ET_HSM_NETSERVER_READ_TIMEOUT_SECS` | Number of seconds before a connection is timed out in a read operation.<br>Default: **30** |
| `ET_HSM_NETSERVER_WRITE_TIMEOUT_SECS` | Number of seconds before a connection is timed out in a write operation.<br>Default: **30** |
| `ET_HSM_NETSERVER_CONN_TIMEOUT_COUNT` | Number of inactivity timeouts on a connection that would cause the connection to be closed by the server. Each inactivity timeout period is 60 seconds.<br>Default: **3** |

| Configuration Item | Meaning |
|---|---|
| `ET_HSM_NETSERVER_FRAG_SIZE` | The threshold value, in number of bytes, where output buffers are coalesced together before being sent via TCP. Servers with fast CPUs can keep this number high, and servers with slow CPUs need to keep this number low for best performance. This is an integer configuration item.<br>Default: **5000** |
| `ET_HSM_NETSERVER_ALLOW_RESET` | Whether the server will allow the reset command to be issued or not. This is a string configuration item with the following valid values:<br>> **Always**: Always allow reset<br>> **Never**: Never allow reset<br>> **OnHalt** (default): Allow reset only when the HSM is not in normal mode |
| `ET_HSM_NETSERVER_PORT` | TCP port number to use.<br>Default=**12396** |
| `ET_HSM_NETSERVER_LOG_CHANNEL` | Channel (destination) to write log entries to. Values are platform-dependent.<br>For Windows, valid values are:<br>> **0** (default): Windows Event Log<br>> **1**: Standard out<br>> **2**: Standard error<br>For Unix, valid values are from **0** to **7** inclusive, and map to syslog **LOG_LOCAL#** values.<br>Default=**0** |
| `ET_HSM_NETSERVER_LOG_NAME` | Name of application/context to associate with log entries.<br>Default=**etnetserver** |
| `ET_HSM_NETSERVER_LOG_LEVEL` | Amount of tracing to generate.<br>Valid values are:<br>> **0**(default): Startup and Errors<br>> **1**: Startup + errors + client connections |

# Software-Only Mode Configuration

After installing the ProtectToolkit-C Software Development Kit (SDK) on your computer system further changes, as detailed in this section, may be made to customize the installation and optimize its performance.

## Storage Location Assignment

The software only variant of ProtectToolkit-C uses the local file system for storing keys and configuration information. By default, the directory **C:\cryptoki** is used under Windows and **$HOME/.cryptoki/cryptoki** under UNIX. It is possible to use a storage location other than the default location for your system by setting the value of the ET_PTKC_SW_DATAPATH configuration item to that of the path required.

For example, on a UNIX machine, to temporarily set the location to **/usr/local/cryptoki** the following **/bin/sh** shell commands would be used:

```
# ET_PTKC_SW_DATAPATH=/usr/local/cryptoki
# export ET_PTKC_SW_DATAPATH
```

This change can be made at the temporary, user or system levels on both UNIX and Windows platforms. Refer to "Configuration Items" on page 85 for further details on how to go about this if required.

# Specifying the Network Server(s)

By default, the net client will attempt to use the local machine as its server. Default values are:

- Server Name = **127.0.0.1**
- Server Port = **12396**

It is necessary to configure the client to use a different host by using the ET_HSM_NETCLIENT_SERVERLIST configuration item. Several servers may also be specified using this configuration item in which case the services from each server will be available seamlessly to the client.

You can use hostnames, IPv4 addresses, or IPv6 addresses to specify your network servers.

The full syntax for the ET_HSM_NETCLIENT_SERVERLIST configuration item is:

ET_HSM_NETCLIENT_SERVERLIST=server1[:port1] [server2[:port2]]

## UNIX/ Example

### To set the net server to the hostname ptkc.mydomain.com at the system level

1. Open the file: **/etc/default/et_hsm**
2. Make the entry: **et_hsm_netclient_serverlist=ptkc.mydomain.com**

## Windows Example

### To set the net server to the hostname ptkc.mydomain.com at the system level

1. Locate the registry key:

   **HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\HSM\NETCLIENT**
2. Assign the value **ptkc.mydomain.com** to the entry:

   **ET_HSM_NETCLIENT_SERVERLIST**

## Using IPv6 addressing

When specifying a host by its IPv6 address, you must enclose the IPv6 address in square brackets.. All other rules which apply to IPv4 addressing also apply for IPv6 addressing. For example, the following command is valid for a server with an IPv6 address of 2001:db8::221:5eff:fe46:f17e:

```
export ET_HSM_NETCLIENT_SERVERLIST=[2001:db8::221:5eff:fe46:f17e]
```

Symbolic server names are also supported and they must be declared in the /etc/hosts and /etc/networks files. For example, if the /etc/hosts file contains the following entry:

```
2001:db8::221:5eff:fe46:f17e  ServerV6
```

then you can run the following command:

```
export ET_HSM_NETCLIENT_SERVERLIST=[ServerV6]
```

Since the interface ports listen for both IPv6 and IPv4, you can specify both IPv4 and IPv6 addresses in the ET_HSM_NETCLIENT_SERVERLIST configuration item, as follows:

```
export ET_HSM_NETCLIENT_SERVERLIST=[<IPv6_address>] <IPv4_address>…
```