



SafeNet ProtectServer Network HSM 5.9

INSTALLATION AND CONFIGURATION GUIDE



Document Information

Product Version	5.9
Document Part Number	007-013682-007
Release Date	08 January 2020

Revision History

Revision	Date	Reason
Rev. A	08 January 2020	Initial release

Trademarks, Copyrights, and Third-Party Software

Copyright 2009-2020 Thales. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales 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 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'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 makes no warranty as to the value or accuracy of information contained herein.

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

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

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

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.

CONTENTS

Preface: About the ProtectServer Network HSM Installation and Configuration Guide	5
Gemalto Rebranding	5
Audience	6
Document Conventions	6
Support Contacts	8
Chapter 1: Product Overview	9
Front panel view	9
Rear panel view	10
Cryptographic Architecture	11
Summary of Cryptographic Service Provider setup	12
Chapter 2: ProtectServer Network HSM Hardware Installation	13
ProtectServer Network HSM Required Items	14
Installing the ProtectServer Network HSM Hardware	15
Chapter 3: Deployment Guidelines	17
Secure Messaging System (SMS)	17
Networking and Firewall Configuration	18
Separation of Roles	18
Chapter 4: Testing and Configuration	20
First Login and System Test	20
Access the Console	20
Power on and Login	21
Run System Test	22
Network Configuration	22
Gathering Appliance Network Information	23
Configuring the Network Parameters	24
SSH Network Access	26
Powering off the ProtectServer Network HSM	27
Troubleshooting	27
Updating the Appliance Software Image	27
Installing the Secure Update Package Patch	28
Updating the Appliance Software	29
Appendix A: Technical Specifications	30
Glossary	31

PREFACE: About the ProtectServer Network HSM Installation and Configuration Guide

This Guide is provided as an instructional aid for the installation and configuration of a ProtectServer Network HSM cryptographic services hardware security module (HSM). It contains the following sections:

- > ["Product Overview" on page 9](#)
- > ["ProtectServer Network HSM Hardware Installation" on page 13](#)
- > ["Testing and Configuration" on page 20](#)
- > ["Technical Specifications" on page 30](#)
- > ["Updating the Appliance Software Image" on page 27](#)

This preface also includes the following information about this document:

- > ["Gemalto Rebranding" below](#)
- > ["Audience" on the next page](#)
- > ["Document Conventions" on the next page](#)
- > ["Support Contacts" on page 8](#)

For information regarding the document status and revision history, see ["Document Information" on page 2](#).

Gemalto Rebranding

In early 2015, Gemalto completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the SafeNet name has been retained. As a result, the product names for SafeNet HSMs have changed as follows:

Old product name	New product name
ProtectServer External 2 (PSE2)	SafeNet ProtectServer Network HSM
ProtectServer Internal Express 2 (PSI-E2)	SafeNet ProtectServer PCIe HSM
ProtectServer HSM Access Provider	SafeNet ProtectServer HSM Access Provider
ProtectToolkit C (PTK-C)	SafeNet ProtectToolkit-C
ProtectToolkit J (PTK-J)	SafeNet ProtectToolkit-J
ProtectToolkit M (PTK-M)	SafeNet ProtectToolkit-M
ProtectToolkit FM SDK	SafeNet ProtectToolkit FM SDK

NOTE These branding changes apply to the documentation only. The SafeNet HSM software and utilities continue to use the old names.

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet ProtectToolkit users and security officers, key manager administrators, and network administrators.

All products manufactured and distributed by Thales are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

It is assumed that the users of this document are proficient with security concepts.

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	<p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"> > Command-line commands and options (Type dir /p.) > Button names (Click Save As.) > Check box and radio button names (Select the Print Duplex check box.) > Dialog box titles (On the Protect Document dialog box, click Yes.) > Field names (User Name: Enter the name of the user.) > Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) > User input (In the Date box, type April 1.)
<i>italics</i>	In type, the italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<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} {<a> <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] [<a> <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: Product Overview

The ProtectServer Network HSM 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 Network HSM 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 Network HSM'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 Network HSM 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	SafeNet ProtectToolkit-C
JCA / JCE	SafeNet ProtectToolkit-J
Microsoft IIS and CA	SafeNet 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.

Front panel view

The features on the front panel of the ProtectServer Network HSM are illustrated below:

Figure 1: ProtectServer Network HSM front panel



Ports

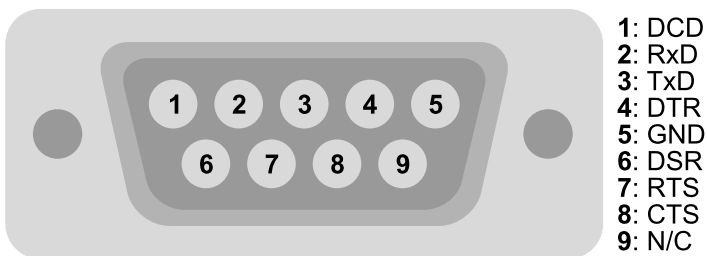
The front panel is equipped with the following ports:

VGA	Connects a VGA monitor to the appliance.
Console	Provides console access to the appliance. See "Testing and Configuration" on page 20 .
USB	Connects USB devices such as a keyboard or mouse to the appliance.
eth0 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 2: HSM serial port pinout



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 Network HSM are illustrated below:

Figure 3: ProtectServer Network HSM 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 Network HSM, remove the tamper key after commission and store it in a safe place.

Cryptographic Architecture

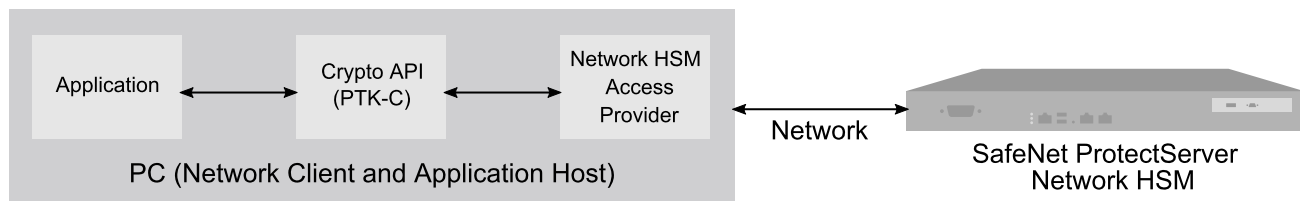
A hardware-based cryptographic system consists of three general components:

- > 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 Network HSM 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 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 Network HSM in network mode.

Figure 4: ProtectServer Network HSM implementation

Summary of Cryptographic Service Provider setup

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

1. **Install the ProtectServer Network HSM** (See ["Installing the ProtectServer Network HSM Hardware" on page 15](#)).
2. **Check that the ProtectServer Network HSM is operating correctly** (see ["Testing and Configuration" on page 20](#)).
3. **Configure the ProtectServer Network HSM network settings** (see ["Testing and Configuration" on page 20](#)).
4. **Install and configure the ProtectServer HSM Access Provider software** (see the *ProtectServer HSM Access Provider Installation Guide*).
5. **Install the high-level cryptographic API software.**

Please refer to the relevant installation guide supplied with the product:

- *SafeNet ProtectToolkit-C Administration Guide*
- *SafeNet ProtectToolkit-J Installation Guide*
- *SafeNet ProtectToolkit-M User Guide*

6. **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 Network HSM.
- establishing communication between the network client and the ProtectServer Network HSM.

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

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

CHAPTER 2: ProtectServer Network HSM Hardware Installation

This chapter describes how to install and connect a ProtectServer Network HSM. 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 Network HSM Required Items" on the next page](#)
2. Install and connect the hardware, as described in ["Installing the ProtectServer Network HSM Hardware" on page 15](#)

ProtectServer Network HSM Required Items

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

Contents Received

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


Qty	Item
1	ProtectServer Network HSM standalone appliance 
1	Smart card reader 
2	Smart cards (in a single media case) 

NOTE 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 Network HSM, 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 table describes additional items which you can use with your ProtectServer HSM. Contact your Thales sales representative to order these items.

Qty	Item
1+	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 
1	ProtectServer-compatible Verifone PIN pad (enables manual key component entry) PN: 934-000087-001

Installing the ProtectServer Network HSM Hardware

Since the ProtectServer Network HSM 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 ["Testing and Configuration" on page 20](#).

To install the hardware

1. Choose a suitable location to site the equipment. You can mount the ProtectServer Network HSM 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 Network HSM 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 Network HSM 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 Network HSM 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 SafeNet-supplied smart card reader. Other smart card readers are not supported.

The ProtectServer Network HSM 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 Network HSM.
- > 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 ["Testing and Configuration" on page 20](#).

CHAPTER 3: Deployment Guidelines

Users must consider the following best practices for security and compliance when deploying the ProtectServer Network HSM 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 Network HSM 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 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" on page 1](#) in the *SafeNet 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" on page 1](#) in the *SafeNet 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" on page 1](#) in the *SafeNet 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" on page 1](#) in the *SafeNet 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 Network HSM 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 22](#) for instructions on setting up static routes.

The ProtectServer Network HSM 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 22](#) for details on setting iptables.

Separation of Roles

The ProtectServer Network HSM 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" on page 1](#) 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" on page 1](#) in the *SafeNet ProtectToolkit-C Administration Guide* for the responsibilities of each role.

CHAPTER 4: Testing and Configuration

This chapter provides a step-by-step overview of how to confirm correct operation of the ProtectServer Network HSM, and configure its network settings. These instructions assume that the installation process covered in ["Installing the ProtectServer Network HSM Hardware" on page 15](#) is complete.

This chapter contains the following sections:

- > ["First Login and System Test" below](#)
- > ["Network Configuration" on page 22](#)
- > ["Powering off the ProtectServer Network HSM" on page 27](#)
- > ["Troubleshooting" on page 27](#)

First Login and System Test

When starting up your ProtectServer Network HSM for the first time, follow these steps:

- > ["Access the Console" below](#)
- > ["Power on and Login" on the next page](#)
- > ["Run System Test" on page 22](#)

Access the Console

To test the system and configure the network, you must first access the ProtectServer Network HSM 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" on the next page](#)). If your terminal device is equipped with an RJ45 serial port, you can use a standard Ethernet cable. Serial cables are not included.

Figure 5: 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 Network HSM 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 v5.9.0
=====
```

```
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 5.9.0
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
```

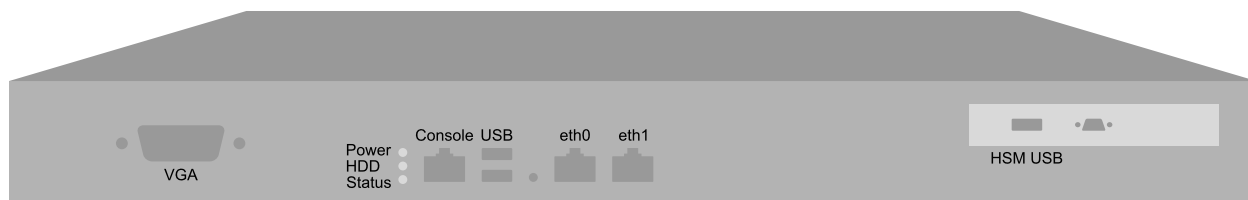
```
Command Result : 0 (Success)
```

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.

Network Configuration

The ProtectServer Network HSM 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 Network HSM 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:



Serial port

Connect a serial device to the ProtectServer Network HSM 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 Network HSM 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 the addresses using static or DHCP addressing.
- > 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.

Static	psesh:> network interface static -device <netdevice> -ip <IP_address> -netmask <netmask> [-gateway <IP_address>]
DHCP	psesh:> network interface dhcp -device <netdevice>

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 Use network interface bonding with static IP 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 device 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 Network HSM 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 Network HSM

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

To power off the ProtectServer Network HSM

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 Network HSM, to the off position. The fan and LEDs will turn off.

Troubleshooting

Each ProtectServer Network HSM is tested during manufacture to ensure a high level of quality. In the unlikely event the unit is not functioning correctly please re-check the installation procedure, paying particular attention to the power source and network cable connection. Running the diagnostic command **hsm state**, as described in ["First Login and System Test" on page 20](#), is the only method available to test the unit.

NOTE The unit has no user serviceable parts. Please do not disassemble the unit to resolve problems unless directed by a Thales support engineer.

If it ever becomes necessary to get into the BIOS, press **<Delete>** as the ProtectServer Network HSM boots.

For further assistance contact your supplier or Thales support with the following details at hand:

- > The product serial number (at the back of the unit)
- > A detailed description of the current system configuration
- > Details of any error messages pertaining to the problem

For contact numbers in your home country, see ["Support Contacts" on page 8](#).

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 Network HSM 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 29](#)

Installing the Secure Update Package Patch

The following procedure allows you to install the secure package update patch on your ProtectServer Network HSM 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 8](#)).
- > If you are installing the patch on a ProtectServer Network HSM running software version 5.2.0 or 5.3.0, ensure that you have **root** access.
- > If you are installing the patch on a ProtectServer Network HSM running software version 5.4.0 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 Network HSM with appliance software 5.2.0 or 5.3.0

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>:
scp <filepath>/SPKG-0.1-1.i386.rpm root@<appliance_hostname/IP>:
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 Network HSM with appliance software 5.4.0 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 Network HSM appliance using a secure package.

Prerequisites

- > Download the secure package file from the Thales Customer Support Portal (see ["Support Contacts" on page 8](#)).
- > You must have **admin** access to the appliance.
- > If the Admin Token is initialized, you require the Admin Token PIN.

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
```

APPENDIX A: Technical Specifications

The ProtectServer Network HSM 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%

Glossary

A

Adapter

The printed circuit board responsible for cryptographic processing in a HSM

AES

Advanced Encryption Standard

API

Application Programming Interface

ASO

Administration Security Officer

Asymmetric Cipher

An encryption algorithm that uses different keys for encryption and decryption. These ciphers are usually also known as public-key ciphers as one of the keys is generally public and the other is private. RSA and ElGamal are two asymmetric algorithms

B

Block Cipher

A cipher that processes input in a fixed block size greater than 8 bits. A common block size is 64 bits

Bus

One of the sets of conductors (wires, PCB tracks or connections) in an IC

C

CA

Certification Authority

CAST

Encryption algorithm developed by Carlisle Adams and Stafford Tavares

Certificate

A binding of an identity (individual, group, etc.) to a public key which is generally signed by another identity. A certificate chain is a list of certificates that indicates a chain of trust, i.e. the second certificate has signed the first, the

third has signed the second and so on

CMOS

Complementary Metal-Oxide Semiconductor. A common data storage component

Cprov

ProtectToolkit C - SafeNet's PKCS #11 Cryptoki Provider

Cryptoki

Cryptographic Token Interface Standard. (aka PKCS#11)

CSA

Cryptographic Services Adapter

CSPs

Microsoft Cryptographic Service Providers

D

Decryption

The process of recovering the plaintext from the ciphertext

DES

Cryptographic algorithm named as the Data Encryption Standard

Digital Signature

A mechanism that allows a recipient or third party to verify the originator of a document and to ensure that the document has not be altered in transit

DLL

Dynamically Linked Library. A library which is linked to application programs when they are loaded or run rather than as the final phase of compilation

DSA

Digital Signature Algorithm

E

Encryption

The process of converting the plaintext data into the ciphertext so that the content of the data is no longer obvious. Some algorithms perform this function in such a way that there is no known mechanism, other than decryption with the appropriate key, to recover the plaintext. With other algorithms there are known flaws which reduce the difficulty in recovering the plaintext

F

FIPS

Federal Information Protection Standards

FM

Functionality Module. A segment of custom program code operating inside the CSA800 HSM to provide additional or changed functionality of the hardware

FMSW

Functionality Module Dispatch Switcher

H

HA

High Availability

HIFACE

Host Interface. It is used to communicate with the host system

HSM

Hardware Security Module

I

IDEA

International Data Encryption Algorithm

IIS

Microsoft Internet Information Services

IP

Internet Protocol

J

JCA

Java Cryptography Architecture

JCE

Java Cryptography Extension

K

Keyset

A keyset is the definition given to an allocated memory space on the HSM. It contains the key information for a specific user

KWRAP

Key Wrapping Key

M

MAC

Message authentication code. A mechanism that allows a recipient of a message to determine if a message has been tampered with. Broadly there are two types of MAC algorithms, one is based on symmetric encryption algorithms and the second is based on Message Digest algorithms. This second class of MAC algorithms are known as HMAC algorithms. A DES based MAC is defined in FIPS PUB 113, see <http://www.itl.nist.gov/div897/pubs/fip113.htm>. For information on HMAC algorithms see RFC-2104 at <http://www.ietf.org/rfc/rfc2104.txt>

Message Digest

A condensed representation of a data stream. A message digest will convert an arbitrary data stream into a fixed size output. This output will always be the same for the same input stream however the input cannot be reconstructed from the digest

MSCAPI

Microsoft Cryptographic API

MSDN

Microsoft Developer Network

P

Padding

A mechanism for extending the input data so that it is of the required size for a block cipher. The PKCS documents contain details on the most common padding mechanisms of PKCS#1 and PKCS#5

PCI

Peripheral Component Interconnect

PEM

Privacy Enhanced Mail

PIN

Personal Identification Number

PKCS

Public Key Cryptographic Standard. A set of standards developed by RSA Laboratories for Public Key Cryptographic processing

PKCS #11

Cryptographic Token Interface Standard developed by RSA Laboratories

PKI

Public Key Infrastructure

ProtectServer

SafeNet HSM

ProtectToolkit C

SafeNet's implementation of PKCS#11. Protecttoolkit C represents a suite of products including various PKCS#11 runtimes including software only, hardware adapter, and host security module based variants. A Remote client and server are also available

ProtectToolkit J

SafeNet's implementation of JCE. Runs on top of ProtectToolkit C

R**RC2/RC4**

Ciphers designed by RSA Data Security, Inc.

RFC

Request for Comments, proposed specifications for various protocols and algorithms archived by the Internet Engineering Task Force (IETF), see <http://www.ietf.org>

RNG

Random Number Generator

RSA

Cryptographic algorithm by Ron Rivest, Adi Shamir and Leonard Adelman

RTC

Real Time Clock

S

SDK

Software Development Kits Other documentation may refer to the SafeNet Cprov and Protect Toolkit J SDKs. These SDKs have been renamed ProtectToolkit C and ProtectToolkit J respectively. ⌚ The names Cprov and ProtectToolkit C refer to the same device in the context of this or previous manuals. ⌚ The names Protect Toolkit J and ProtectToolkit J refer to the same device in the context of this or previous manuals.

Slot

PKCS#11 slot which is capable of holding a token

SlotPKCS#11

Slot which is capable of holding a token

SO

Security Officer

Symmetric Cipher

An encryption algorithm that uses the same key for encryption and decryption. DES, RC4 and IDEA are all symmetric algorithms

T

TC

Trusted Channel

TCP/IP

Transmission Control Protocol / Internet Protocol

Token

PKCS#11 token that provides cryptographic services and access controlled secure key storage

TokenPKCS#11

Token that provides cryptographic services and access controlled secure key storage

U

URI

Universal Resource Identifier

V

VA

Validation Authority

X

X.509

Digital Certificate Standard

X.509 Certificate

Section 3.3.3 of X.509v3 defines a certificate as: "user certificate; public key certificate; certificate: The public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it"