THALES

SafeNet ProtectServer Access Provider 5.9

INSTALLATION 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

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.

CONTENTS

PREFACE: About the ProtectServer HSM Access Provider Installation Guide

Before a SafeNet ProtectServer Hardware Security Module (HSM) can be used, an access provider package must be installed. These packages include any required device drivers.

This guide will assist users in installing, troubleshooting, and configuring access provider software. It contains the following sections:

- "Operating Modes and Access Providers" on page 10

  This chapter covers concepts and procedures that are key to understanding the installation process and the different operating modes.

- "Installation for PCIe Mode" on page 21
- "Installation for Network Mode" on page 26
- "ProtectServer PCIe HSM Server Configuration for Network Mode" on page 28
- "Using the Unix Installation Utility" on page 17
- "Utilities Command Reference" on page 37

  This chapter describes two command-line utilities, **hsmstate** and **hsmreset**, and the Unix Installation Utility, **safeNet-install.sh**.

- "Configuration Items" on page 29

  Information on reconfiguring the access provider software after a successful installation is provided here.

- "Troubleshooting" on page 41

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 9

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	The bold attribute is used to indicate the following: > 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**.)
italics	In type, the italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* 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>|<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**] [<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: Operating Modes and Access Providers

SafeNet high-level cryptographic APIs such as SafeNet ProtectToolkit-C can be used in one of three *operating modes*. These are:

> **PCIe mode** in conjunction with a locally-installed ProtectServer PCIe HSM cryptographic services adapter. See "PCIe Mode Setup Procedure" on page 13.

> **Network mode** over a TCP/IP network, in conjunction with a compatible product such as the ProtectServer Network HSM. A machine with a SafeNet ProtectServer PCIe HSM installed may also be used as a server in network mode. See:
>
> - "Network Mode Setup using a ProtectServer Network HSM" on page 14
> - "Network Mode Setup using a ProtectServer PCIe HSM Adapter" on page 15

> **Software-only mode** on a local machine without access to a hardware adapter, for development and testing purposes.
>
> In software-only mode, it is not necessary to install access provider software.

In PCI and network modes, access provider software allows the high-level cryptographic API to access an associated HSM. The access provider software packages also include device drivers required by the API to access maintenance utilities and other software associated with the selected operating mode.

Access Provider Types

To use a high-level cryptographic API in either PCIe mode or Network mode, the relevant HSM access provider must be installed.

ProtectServer PCIe HSM Access Provider

The ProtectServer PCIe HSM Access Provider software package (file name: **PTKpcihsm2**) contains the device driver for a compatible, locally-installed SafeNet cryptographic services adapter such as the ProtectServer PCIe HSM (see "PCIe Mode Setup Procedure" on page 13).

> In PCIe mode, **PTKpcihsm2** must be installed with the high-level cryptographic API on the local machine.

> In network mode, **PTKpcihsm2** must be installed on the server side, where the ProtectServer PCIe HSM is installed. See "Network Mode Setup using a ProtectServer PCIe HSM Adapter" on page 15.

ProtectServer Network HSM Access Provider

In network mode, the ProtectServer Network HSM Access Provider software package (filename: **PTKnethsm**) must be installed with the high-level cryptographic API on the client-side machine (see "Network Mode Setup using a ProtectServer Network HSM" on page 14 and "Network Mode Setup using a ProtectServer PCIe

HSM Adapter" on page 15). The package includes the Net Client software required to provide cryptographic services using SafeNet hardware devices over a TCP/IP network.

HSM Network Server

When using a ProtectServer PCIe HSM in network mode, the SafeNet HSM Net Server package (filename: **PTKnetsvr**) must be installed in the server side machine with the HSM adapter (see "Network Mode Setup using a ProtectServer PCIe HSM Adapter" on page 15). The SafeNet cryptographic services adapter and the ProtectServer PCIe HSM Access Provider software package (file name: **PTKpcihsm2**) must be installed first.

System Requirements

- A PC with a Pentium-class processor or better and a spare PCI Express bus interface slot (if installing an adapter card).
- A SafeNet hardware security module (not required when using Software-Only operating mode for development and testing).
- Java runtime (required for graphical user interface utilities only). The product has been tested using Java runtime version 6.x, 7.x, and 8.x. It may also operate correctly using other versions of the runtime, but Thales does not support other versions.
- .NET versions 3.5 and 4.5 (Windows only). All required .NET versions are available for download from Microsoft.
- Microsoft Visual C++ 2005, 2008, and 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=SafeNet ProtectToolkit-C, PKCS #11 v2.10/2.20

M=SafeNet ProtectToolkit-M, MS CSP 2.0 with CNG

J=SafeNet ProtectToolkit-J, Java runtime 6.x/7.x/8.x

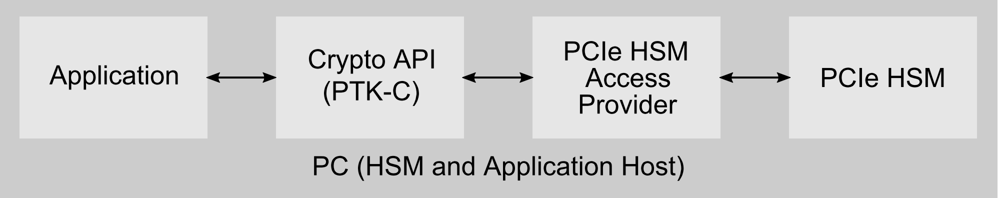
Operating System		OS type	64-bit PTK	64-bit PTK supported hardware	32-bit PTK	32-bit PTK supported hardware
Windows	10	64-bit	C/M/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	Server 2016	64-bit	C/M/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	Server 2012 R2	64-bit	C/M/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	Server 2008 (R1 and R2)	64-bit	C/M/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	7	32-bit	-	-	C/J (KSP support)	PCIe HSM Network HSM Network HSM Plus
	7	64-bit	C/M/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
Linux	RHEL 7	64-bit	C/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	RHEL 6	32-bit	-	-	C/J	PCIe HSM Network HSM Network HSM Plus
	RHEL 6	64-bit	C/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	SUSE12	64-bit	C/J	PCIe HSM Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus

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	Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	7.1	64-bit	C/J	Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
	6.1	64-bit	C/J	Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
Solaris	11 (SPARC, x86) 10 (SPARC, x86)	64-bit	C/J	Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus
HP-UX	11	64-bit	C/J	Network HSM Network HSM Plus	C/J	Network HSM Network HSM Plus

PCIe Mode Setup Procedure

In PCIe mode, an access provider package and associated HSM are installed in the same machine:

Figure 1: PCIe Mode



To set up a ProtectServer PCIe HSM adapter in PCIe Mode

1. **Install the ProtectServer PCIe HSM card in the client machine.**

   Please consult the relevant installation manual, such as the *ProtectServer PCIe HSM Installation Guide*.

2. **Install the necessary third-party software.**

   Install the Java runtime, .NET (Windows only) and MSCV (Windows only) software. See "System Requirements" on page 11.

3. **Install the ProtectServer PCIe HSM Access Provider software package.**

   The ProtectServer PCIe HSM Access Provider software package (file name: **PTKpcihsm2**) contains the device driver for a compatible, locally-installed SafeNet cryptographic services adapter such as the ProtectServer PCIe HSM.

   For more information on installing the access provider, see "Installation for PCIe Mode" on page 21.

4. **Make any necessary configuration changes to the access provider.**

Configuration changes can be made on a temporary, user, or system level. See "Configuration Items" on page 29 for details. For a list of configurable items, see "PCI Mode Client Configuration Items" on page 33.

5. **Install the SafeNet high-level cryptographic API and confirm correct operation of the hardware.**

   Refer to the relevant installation guide provided with the API:

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

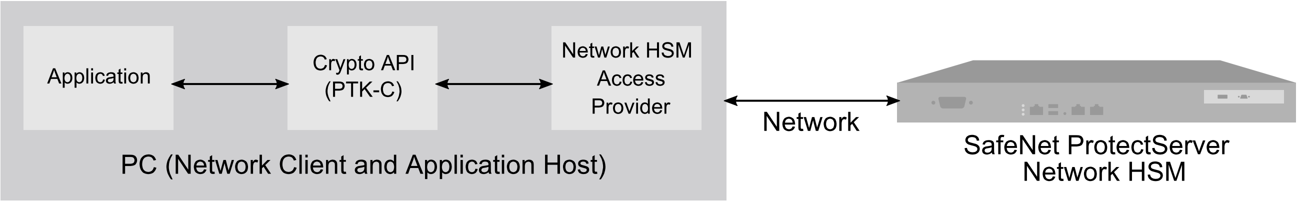
6. **Configure the API as necessary.**

   This may include establishing a trusted channel, called the Secure Message System. See the relevant installation/administration guide for details.

Network Mode Setup using a ProtectServer Network HSM

In network mode, the application and API are located remotely from the HSM across a network.

Figure 2: Network Mode using a ProtectServer Network HSM


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

To set up a ProtectServer Network HSM with a client in Network Mode

1. **Install the ProtectServer Network HSM on the same network as the client machine and verify its availability on the network.**

   This includes assigning an IP address, hostname, gateway, and access control. Consult the relevant installation manual:

   - *ProtectServer Network HSM Installation/Configuration Guide*

2. **Install the necessary third-party software on the client machine.**

   Install the Java runtime, .NET (Windows only) and MSCV (Windows only) software. See "System Requirements" on page 11.

3. **Install the ProtectServer Network HSM Access Provider software package on the client machine.**

   The ProtectServer Network HSM Access Provider software package (filename: **PTKnethsm**) must be installed with the high-level cryptographic API on the client-side machine. The software package includes the Net Client software required for SafeNet hardware devices to provide cryptographic services over a TCP/IP network.

   For more information on installing the access provider, consult the section relevant to your system in "Installation for Network Mode" on page 26

4. **Make any necessary configuration changes to the access provider.**

Configuration changes can be made on a temporary, user, or system level. See "Configuration Items" on page 29 for details. For a list of configurable items, see "Network Mode Client Configuration Items" on page 33.

5. **Install the SafeNet high-level cryptographic API on the client machine and confirm correct operation of the hardware.**

   Refer to the relevant installation guide provided with the API:

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

6. **Configure the API as necessary.**

   This may include tasks such as:

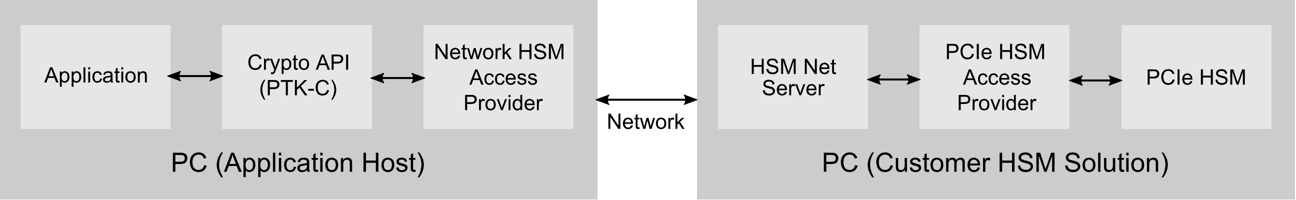
   - establishing a trusted channel or secure messaging system (SMS) between the API and the ProtectServer Network HSM
   - establishing network communication between the client and one or more servers on the same network

   See the relevant installation/administration guide for details.

Network Mode Setup using a ProtectServer PCIe HSM Adapter

If a PCIe adapter is used as a network HSM, SafeNet HSM Net Server software must be installed on the same machine.

Figure 3: Network Mode using a ProtectServer PCIe HSM adapter



To set up a ProtectServer PCIe HSM adapter in Network Mode

1. **Install the ProtectServer PCIe HSM adapter card in the server machine.**

   Please consult the relevant installation manual, such as the *ProtectServer PCIe HSM Installation Guide*.

2. **Install the necessary third-party software on the server machine.**

   Install the Java runtime, .NET (Windows only) and MSCV (Windows only) software. See "System Requirements" on page 11.

3. **Install the ProtectServer PCIe HSM Access Provider software package on the server machine.**

   The ProtectServer PCIe HSMAccess Provider software package (file name: **PTKpcihsm2**) contains the device driver for a compatible, locally-installed SafeNet cryptographic services adapter such as the ProtectServer.

   For more information on installing the access provider, see "Installation for PCIe Mode" on page 21.

4. **Install the Net Server software package on the server machine.**

When using a ProtectServer PCIe HSM in network mode, the SafeNet HSM Net Server package (filename: **PTKnetsvr**) must be installed in the server-side machine with the HSM adapter. For details, consult the section relevant to your system:

- For Windows operating systems, see "ProtectServer PCIe HSM Server Configuration for Network Mode" on page 28
- For Linux operating systems, see "Using the Unix Installation Utility" on page 17.

5. **Make any necessary configuration changes on the server machine.**

   Configuration changes can be made on a temporary, user, or system level. See "Configuration Items" on page 29 for details. For a list of configurable items, see "Network Mode Server Configuration Items" on page 34.

6. **Install the necessary third-party software on the client machine.**

   Install the Java runtime, .NET (Windows only) and MSCV (Windows only) software. See "System Requirements" on page 11.

7. **Install the ProtectServer Network HSM Access Provider software package on the client machine.**

   The ProtectServer Network HSM Access Provider software package (filename: **PTKnethsm**) must be installed with the high-level cryptographic API on the client-side machine. The software package includes the Net Client software required for SafeNet hardware devices to provide cryptographic services over a TCP/IP network.

   For more information on installing and configuring the access provider, consult the section relevant to your system.

   - For Windows operating systems, see "Installation for Network Mode" on page 26.
   - For Linux operating systems, see "Using the Unix Installation Utility" on page 17.

8. **Make any necessary configuration changes on the client machine.**

   See "Configuration Items" on page 29 for details. For a list of configurable items, see "Network Mode Client Configuration Items" on page 33.

9. **Install the SafeNet high-level cryptographic API on the client machine and confirm correct operation of the hardware.**

   Refer to the relevant installation guide provided with the API:

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

10. **Configure the API as necessary.**

    This may include tasks such as:

    - establishing a trusted channel or secure messaging system (SMS) between the API and the networked HSM server
    - establishing network communication between the client and one or more servers on the same network

    See the relevant installation/administration guide for details.

CHAPTER 2: Using the Unix Installation Utility

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 9 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 SafeNet 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 SafeNet 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.

Utility Startup

Should you encounter any problems while following this procedure, please see "Unix Installation Utility Troubleshooting" on page 19. Options can be specified when executing the **safeNet-install.sh** command. These options are not normally required and are mainly useful for troubleshooting. For more information, see "safeNet-install.sh" on page 38.

To start up the utility

1. The Thales Unix Installation Utility is located in the root installer directory. Unpack the .tar archive to create this directory.
2. Change to the installer directory and start the utility. For example:

   ```
   # cd /misc/cd
   # ./safeNet-install.sh
   ```

   The utility scans the system and the directory and displays the Main Menu.

   ```
   Gemalto Unix Installation Utility (version 5.3.0):
   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
   ```

```
  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**).

Installing an Access Provider Package

Should you encounter any problems, please see "Unix Installation Utility Troubleshooting" on the next page.

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 SafeNet ProtectToolkit **setvars.sh** script to configure your environment for the SafeNet 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 SafeNet 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**.

Uninstalling an Access Provider Package

Should you encounter any problems, please see "Unix Installation Utility Troubleshooting" below.

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
```

Unix Installation Utility Troubleshooting

Problem	Solution
Packages to install or uninstall are not visible	If no packages are shown to install or uninstall, close the utility, check that you are logged on as **root**, and ensure your current directory is on the DVD or directory before running the utility again.

Problem	Solution
The screen is confused or does not display correctly	This utility relies on the **TERM** environment parameter when creating colors and measuring screen size, so make sure this is set correctly. The most common values are **xterm** or **vt100**. For example, to set **TERM** to **vt100**: **# TERM=vt100# export TERM** > If the screen is confused, run the utility in "plain" mode as follows: **# ./safeNet-install.sh –p** > If the size of the terminal is not correctly set by **termcap** (for example: the headings disappear off the top of the screen), override the screen size with the **-s** option: **# ./safeNet-install.sh -s 24x80** > If using an X system terminal window, do not resize the window while running the utility, as it cannot sense the change.
The backspace key does not operate correctly	On some terminals, the backspace key does not operate correctly. If, after typing a number and then backspace, the terminal returns "**2^H**" instead of an actual backspace: > Type the current **KILL** character (normally **^U**) and then enter the desired number (you will need to do this each time a backspace is required) > Exit the utility (perhaps with **^C**) and use the **stty(1)** command to correct the erase character before restarting the utility: **# stty erase ^H** where **^H** is the character created by pressing the backspace key. This will fix the problem semi-permanently, for the current session in that terminal.

CHAPTER 3: Installation for PCIe Mode

This chapter provides instructions for installing the ProtectServer PCIe HSM Access Provider. Please see the appropriate section for your host system:

> "Windows Installation for PCIe Mode" below

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

- "Signing the ProtectServer PCIe HSM Driver for UEFI Secure Boot" on page 23

Windows Installation for PCIe Mode

This section provides instructions for Windows operating systems. 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 9 for more information.

Before following the procedure below, ensure that you are logged in as a member of the Windows **administrator** group.

Upgrading

If you are upgrading the access provider, you must uninstall any currently-installed version by using the Windows **Programs and Features** control panel.

> **CAUTION!** If uninstallation is not carried out first, the system may lock up. See "Troubleshooting" on page 41 for recovery instructions.

To install the ProtectServer PCIe HSM Access Provider

1. Locate the installer directory and execute the file **PTKpcihsm2.msi**.
2. Work through the installation wizard.

   By default, the ProtectServer PCIe HSM Access Provider package is installed in the following directory:

   \Program Files\SafeNet\Protect Toolkit 5\PCI HSM 2
3. A prompt during the installation allows you to change the default destination. Unless there is good reason, the default should be accepted.
4. You will be prompted to install the driver. The driver is required.

> **NOTE** A reboot may be required to successfully load the driver.

To verify correct installation

From a command prompt, execute the **hsmstate** utility. If the adapter has been correctly installed, the response will include:

```
HSM in NORMAL MODE. RESPONDING
```

For more information, see "hsmstate" on page 39.

Making Configuration Changes

Finally, make any necessary configuration changes. Currently, the only configurable setting in PCIe mode is the **ET_HSM_PCICLIENT_READ_TIMEOUT_SECS** variable. This setting determines the time in seconds the PCIe 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. See "Configuration Items" on page 29 for instructions on how to change this setting, and "PCI Mode Client Configuration Items" on page 33 for a description of the variable.

Linux Installation for PCIe Mode

This chapter provides instructions for Linux operating systems.

The Unix Installation Utility

The simplest way to install or uninstall an access provider package on any of the Linux/Unix platforms is to use the Unix Installation Utility. The utility ensures that the correct commands for your platform are automatically executed.

If you wish to enter Linux commands manually, see "Manual Linux Installation Commands" on the next page.

Linux install preparation

Before adding or removing any packages, you must become the super-user on the host system.

The Linux driver is distributed as source code and must be compiled for the running kernel before loading as a dynamic module. In most cases, the installation script will do this automatically, provided the following conditions are met:

- The same version of the C compiler (**gcc**) used to compile the kernel must be available.
- The **rpmbuild** package is installed.
- The appropriate kernel source package for the running system is installed. The kernel source is usually installed in **/usr/src/linux-<VER>** with a symbolic link from either:
  - **/lib/modules/<VER>/build** or
  - **/lib/modules/<VER>/source**

  where **<VER>** is the kernel version as reported by **uname –r**

To install the ProtectServer PCIe HSM Access Provider

1. Mount the installation CD-ROM and navigate to its directory. For example:

   # cd /cdrom/cdrom0/

2. Use the Unix Installation Utility.

   Select the ProtectServer PCIe HSM Access Provider device driver package from the **Install** Menu. This will install the ProtectServer PCIe HSM Access Provider package, including the device driver and test utilities, as well as the manual pages for these programs to the default directory (**/opt/safenet**).

   See "Using the Unix Installation Utility" on page 17 for more information.

   > **NOTE** A reboot may be required to successfully load the driver.

Manual Linux Installation Commands

To install the access provider manually

The access provider is installed by executing the following as **root** (super-user):

```
# cd /cdrom/cdrom0/Linux/pci_hsm_access_provider
rpm -i PTKpcihsm2-X.X-X.i386.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 access provider manually

To remove the software from your host system, simply use the **rpm(8)** command with the appropriate package name as a parameter.

For example:

```
# rpm -e PTKpcihsm2
```

Making Configuration Changes

Finally, make any necessary configuration changes. Currently, the only configurable setting in PCIe mode is the **ET_HSM_PCICLIENT_READ_TIMEOUT_SECS** variable. This setting determines the time in seconds the PCIe 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. See "Configuration Items" on page 29 for instructions on how to change this setting, and "PCI Mode Client Configuration Items" on page 33 for a description of the variable.

Signing the ProtectServer PCIe HSM 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 HSMin 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 HSM 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 HSM 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 unique file names for the public and private keys.

   # **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 HSM 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**

CHAPTER 4: Installation for Network Mode

To operate in network mode, a SafeNet high-level cryptographic API such as SafeNet ProtectToolkit-C requires that the ProtectServer Network HSM Access Provider be installed. See "Operating Modes and Access Providers" on page 10 for more about network mode.

The ProtectServer Network HSM Access Provider package (**PTKnethsm**) must be installed on the client machine along with the API. This chapter provides installation instructions for Windows operating systems. For Linux installation, see "Using the Unix Installation Utility" on page 17.

> "Network Mode Client Configuration Items" on page 33

Windows Installation

Before following the procedure below, ensure you are logged in as a member of the Windows **administrator** group.

Upgrading

If you are upgrading the access provider, you must uninstall any previous version by using the Windows **Programs and Features** control panel before proceeding. 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 9 for more information.

> **CAUTION!** If uninstallation is not carried out first, the system may lock up. See "Troubleshooting" on page 41 for recovery instructions.

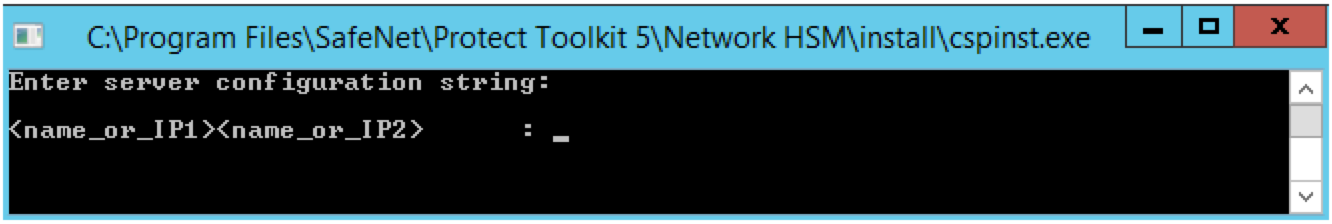
To install the ProtectServer Network HSM Access Provider

1. Unpack the .tar archive and execute the file **PTKnethsm.msi**.
2. Work through the installation wizard to complete the installation.

   By default, the ProtectServer Network HSM Access Provider package is installed in the following directory:

   \Program Files\SafeNet\Protect Toolkit 5\Network HSM

   A prompt during the installation allows you to change the default destination. Unless there is good reason, the default should be accepted.
3. When the command window below is displayed, specify the hostname or IP address of slots on 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.



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

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

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 29.

To verify the installation

From a command prompt, type **hsmstate** to execute the **hsmstate** utility. If the Network HSM is correctly configured, the following will be returned:

```
HSM device 0:   HSM in NORMAL MODE. RESPONDING. Usage Level=0%
```

You should see a response entry for each configured device slot. For more information about the **hsmstate** utility, refer to the section in "Utilities Command Reference" on page 37.

CHAPTER 5: ProtectServer PCIe HSM Server Configuration for Network Mode

The SafeNet HSM Net Server package (filename: **PTKnetsvr**) can be installed on machines hosting a SafeNet cryptographic services adapter such as the ProtectServer PCIe HSM. This allows it to act as an HSM server for clients running a cryptographic API such as SafeNet ProtectToolkit-C in network mode. The cryptographic services adapter and the ProtectServer PCIe HSM Access Provider software package (file name: **PTKpcihsm2**) must be installed on the server first.

Installation instructions for Windows operating systems are provided in this chapter. For Linux/Unix operating systems, see "Using the Unix Installation Utility" on page 17. 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 9 for more information.

Windows Installation

Before following the procedure below, ensure that:

- you are logged in as a member of the Windows administrator group.
- the ProtectServer PCIe HSM has been installed.
- the ProtectServer PCIe HSM Access Provider (**PTKpcihsm2**) has been installed. See "Installation for PCIe Mode" on page 21.

Upgrading

If you are upgrading the Net Server package, you must uninstall any previous version by using the Windows **Programs and Features** control panel before proceeding.

To install the SafeNet HSM Net Server package

1. In the installer directory, locate and execute the file **PTKnetsrv.msi**.
2. Work through the wizard to complete the installation.

CHAPTER 6: Configuration Items

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

> "Overview" below

> "Client/PCIe HSM Server Configuration" on the next page

> "ProtectServer Network HSM Server Configuration" on page 31

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** (SafeNet 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 33

> "Network Mode Client Configuration Items" on page 33

> "Network Mode Server Configuration Items" on page 34

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 SafeNet 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 SafeNet 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 Network HSM Server Configuration

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

To change the ProtectServer Network HSM server configuration

1. Create a text file on your client workstation 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 34.

   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 appliance using **pscp** (Windows) or **scp** (Linux/UNIX):

Windows	**pscp** <filename> **admin@**<server_host/IP>:
	`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%`

Linux/UNIX	**scp** <filename> **admin@**<server_host/IP>:
	`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%`

3. Login to PSESH as **admin**.
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" on page 1 in 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. For more information about using configuration items see "Configuration Items" on page 29.

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. 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. 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. For more information about using configuration items see "Configuration Items" on page 29.

Configuration Item	Table Section Outside Table: Meaning
`ET_HSM_NETCLIENT_HEARTBEAT =[ON|OFF]`	If **ON**, net client is to request and support heartbeat messages from the Network Server. Default=**OFF**

Configuration Item	Table Section Outside Table: Meaning
`ET_HSM_NETCLIENT_LOG_CHANNEL`	Channel (destination) to write log entries to. Values are platform-dependent. For Windows, valid values are: > **0** – Windows Event Log > **1** – Standard out > **2** – Standard error Default=**0** For Unix, valid values are from **0** to **7** inclusive, and map to syslog **LOG_LOCAL#** values. Default=**0**
`ET_HSM_NETCLIENT_LOG_NAME`	Name of application/context to associate with log entries. Default=**etnetclient**
`ET_HSM_NETCLIENT_READ_TIMEOUT_SECS`	Seconds to allow before timing out a TCP/IP read operation. Default=**300**
`ET_HSM_NETCLIENT_SERVERLIST =[host[:port] [host[:port]…]]`	Space separated list of hosts (with optional port number) to connect to. Default host=**localhost** Default port=**12396** 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. Default=**60**
`ET_HSM_NETCLIENT_CONNECT_TIMEOUT_SECS`	Number of seconds before a connection attempt is timed out. Default=**60**

Network Mode Server Configuration Items

The available server configuration items for Network mode and their default values are listed in the following table. For more information about using configuration items see "Configuration Items" on page 29.

Configuration Item	Meaning
`ET_HSM_NETSERVER_OLD_WORKER_COUNT`	Number of threads to reserve for processing old SafeNet ProtectToolkit-C remote client connections. Default: **3**

Configuration Item	Meaning
`ET_HSM_NETSERVER_V2_WORKER_COUNT`	Number of worker threads, per HSM, to reserve for processing new net client connections. Default: **10**
`ET_HSM_NETSERVER_READ_TIMEOUT_SECS`	Number of seconds before a connection is timed out in a read operation. Default: **30**
`ET_HSM_NETSERVER_WRITE_TIMEOUT_SECS`	Number of seconds before a connection is timed out in a write operation. 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. Default: **3**
`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. 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: > **Always**: Always allow reset > **Never**: Never allow reset > **OnHalt** (default): Allow reset only when the HSM is not in normal mode
`ET_HSM_NETSERVER_PORT`	TCP port number to use. Default=**12396**
`ET_HSM_NETSERVER_LOG_CHANNEL`	Channel (destination) to write log entries to. Values are platform-dependent. For Windows, valid values are: > **0** (default): Windows Event Log > **1**: Standard out > **2**: Standard error For Unix, valid values are from **0** to **7** inclusive, and map to syslog **LOG_LOCAL#** values. Default=**0**

Configuration Item	Meaning
`ET_HSM_NETSERVER_LOG_NAME`	Name of application/context to associate with log entries. Default=**etnetserver**
`ET_HSM_NETSERVER_LOG_LEVEL`	Amount of tracing to generate. Valid values are: > **0**(default): Startup and Errors > **1**: Startup + errors + client connections

CHAPTER 7: 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 HSM and ProtectServer Network HSM Access Provider installations. The utilities are named **hsmstate** and **hsmreset**.

The utilities are described in "hsmstate" on page 39 and "hsmreset" on page 40.

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 "Using the Unix Installation Utility" on page 17

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 8: Troubleshooting

If you have difficulties during installation, please first check that you have followed all the installation instructions in this guide and other applicable guides where referenced. The information in this section may be of further assistance. If you still cannot resolve the issue, please contact your supplier or Thales support. See "Document Information" on page 2 for contact information.

Known Issues

Problem	Solution
The system locks up after installation of the ProtectServer PCIe HSM Access Provider device driver package. This may happen if a prior version of the device driver exists on the system.	1. Power down and remove the adapter. 2. Power up. 3. Uninstall all versions (old and new) of the ProtectServer PCIe HSMAccess Provider / device driver package. 4. Power down and reinstall the adapter. 5. Power up and reinstall the ProtectServer PCIe HSM AccessProvider package.
Following reinstallation of a previously removed adapter or the addition of another adapter, the device driver cannot find the device or an adapter is not responding.	Confirm that the adapter(s) are firmly seated in the PCIe slot, then uninstall theProtectServer PCIe HSM AccessProvider package. Following this, perform a fresh install of the ProtectServer PCIe HSM Access Provider package.

Fault Diagnosis Utilities

The SafeNet hardware maintenance utilities **hsmstate** and **hsmreset** can be used to carry out simple fault diagnosis. These utilities are included in the ProtectServer HSM Access Provider installation.

For more information, see the *ProtectServer HSM Access Provider Installation Guide*.

Fault Diagnosis Procedure

From a command prompt, execute **hsmstate**. The output from the utility should include "... `NORMAL mode, Responding`".

If the utility reports "... `HALTED due to a failure`":

1. Execute **hsmreset**.
2. Following the reset, check to see if the **hsmstate** is now reporting NORMAL operation.

If the utility reports "... `waiting for tamper cause to be removed`":

1. Check to see that any connected external tamper detectors are correctly configured.
2. Make sure the adapter is sitting firmly and correctly in the PCIe slot.

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"