SafeNet ProtectServer Network HSM

Installation and Configuration Guide

gemalto
security to be free

Part Number 007-007474-008
Version 5.2

Trademarks

Gemalto Rebranding

In early 2015, Gemalto NV completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the HSM product portfolio has been streamlined under the SafeNet brand. As a result, the ProtectServer/ProtectToolkit product line has been rebranded as follows:

Old product name	New product name
Protect Server External 2 (PSE2)	SafeNet ProtectServer Network HSM
Protect Server Internal Express 2 (PSI-E2)	SafeNet ProtectServer PCIe HSM
ProtectToolkit	SafeNet ProtectToolkit

Disclaimer

All information herein is either public information or is the property of and owned solely by Gemalto NV. 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 Gemalto's information.

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

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

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

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto 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, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto 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 Gemalto 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.

Gemalto 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 Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto 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.

Technical Support

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or Gemalto support. Gemalto 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 Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact method	Contact	
Address	Gemalto NV 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	Global	+1 410-931-7520
	Australia	1800.020.183
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	000.800.100.4290
	Netherlands	0800.022.2996
	New Zealand	0800.440.359
	Portugal	800.1302.029
	Singapore	800.863.499
	Spain	900.938.717
	Sweden	020.791.028
	Switzerland	0800.564.849
	United Kingdom	0800.056.3158
	United States	(800) 545-6608
Web	www.safenet-inc.com	
Support and Downloads	www.safenet-inc.com/support Provides access to the Gemalto Knowledge Base and quick downloads for various products.	
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

Revision History

Revision	Date	Reason
A	14 March 2016	Release 5.2

Contents

Chapter 1
Introduction

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

Chapter 2 gives an overview of the product. Both functionality and physical characteristics are described.

Chapter 3 covers how the product is used to implement a cryptographic service provider and the setup steps are given. References to further documentation are cited where needed.

Chapter 4 describes the installation procedure.

Chapter 5 deals with testing and network setting configuration. A troubleshooting section is included at the end of the chapter.

Chapter 6 provides a command reference for PSESH, the appliance shell interface, which you use to configure, monitor, and maintain the applaince.

The technical specification for the product is in Appendix A.

Chapter 2
Product overview

The SafeNet ProtectServer Network HSM is a self-contained, security-hardened server providing hardware based cryptographic functionality through a TCP/IP network connection. The product is used, together with SafeNet high level application programming interface (API) software, to implement cryptographic service providers for a wide range of secure applications.

The SafeNet ProtectServer Network HSM is PC based. The enclosure is a heavy duty steel case and common PC ports and controls are provided. The unit is delivered with the necessary software components pre-installed on a Linux operating system, in a "ready to operate" state. 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 using the SafeNet 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.

To implement a cryptographic service provider, use the SafeNet ProtectServer Network HSM with one of SafeNet's high level cryptographic APIs. The provider types that can be implemented and the corresponding SafeNet high level cryptographic API required are shown in the following table.

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

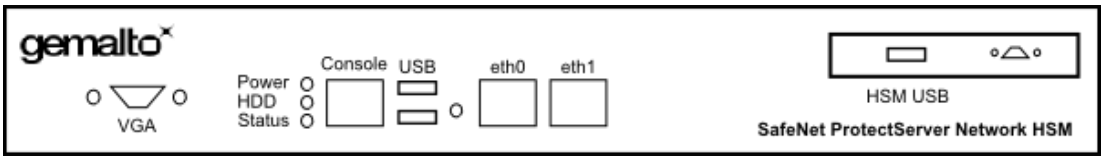
To provide the highest level of security, these APIs interface directly with the product's FIPS 140-1 Level 3 certified core. High-speed DES and RSA hardware based cryptographic processing is used. Key storage is tamper resistant and battery-backed.

A smart card reader RS232 (V.24) serial port (male DB9 connector) is provided on the processing module for the secure loading and backup of keys. One smart card reader with smart cards is also supplied with the unit.

Front panel view

Figure 1 illustrates the front panel of the ProtectServer External 2 appliance.

Figure 1: SafeNet ProtectServer Network HSM front panel



Ports

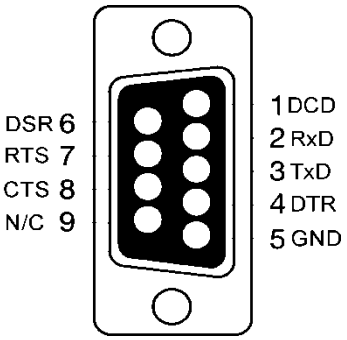
The front panel is equipped with the following ports:

VGA	Used to connect a VGA monitor to the appliance.
Console	Used to provide console access to the appliance. See "Equipment requirements" on page 9.
USB	Used to connect USB devices such as a keyboard or mouse to the appliance.
eth0 **eth1**	Used to connect the appliance to the network.
HSM USB	Used to connect a smart card reader to the appliance using the included USB-to-serial cable.

HSM serial port pin configuration

The serial port on the USB-to-serial cable uses a standard RS232 male DB9 pinout, as illustrated in Figure 2.

Figure 2: HSM serial port pinout



LEDs

The front panel is equipped with the following LEDs:

Power	Lights green to indicate that the unit is powered on.
HDD	Flashes amber to indicate hard disk activity.
Status	Flashes green on startup. Otherwise not used.

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

Figure 3 illustrates the rear panel of the ProtectServer External 2 appliance.

Figure 3: SafeNet ProtectServer Network HSM rear panel

Tamper lock

The tamper lock allows you to set the tamper state of the HSM inside the appliance. You can use the tamper lock during commissioning or decommisioning of the appliance to destroy any keys currently stored on the HSM.

When the key is in the horizontal (Active) position, the HSM is in normal operating mode. When the key is in the vertical (Tamper) position, the HSM is in the tamper state, and any keys previously stored on the HSM are destroyed.

CAUTION!
Turning the tamper key from the Active position to the Tamper position causes any keys currently stored on the HSM to be deleted. Once the keys are deleted they are not recoverable. Ensure that you always back up your keys. To avoid accidentally deleting the keys on an operational SafeNet ProtectServer Network HSM, remove the tamper key after installation/commissioning and store it in a safe place.

Chapter 3
Implementation overview

Implementation architecture

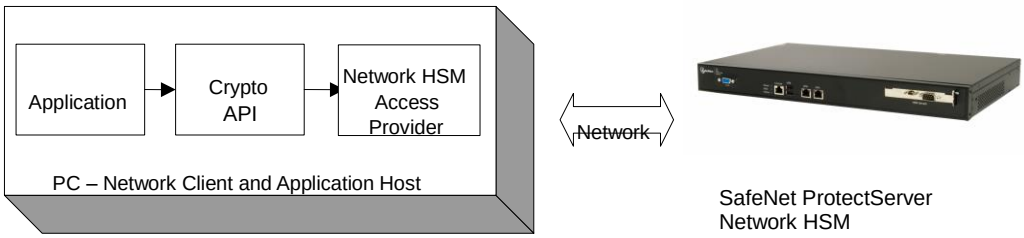
To implement a hardware based cryptographic service provider, essentially three elements are required.

1. One or more hardware security modules (HSMs) for key processing and storage.
2. High level cryptographic API software. This software uses HSM services when providing “cryptographic service provider” functionality to applications.
3. Access provider software to implement the connection between the cryptographic API software and the HSMs.

Where key processing and storage is to be implemented using a standalone SafeNet ProtectServer Network HSM, the cryptographic service provider will operate in network mode.

In network mode, Network HSM Access Provider software is installed on the same machine used to host the cryptographic API software. It is used to implement the connection between and the SafeNet ProtectServer Network HSM and the cryptographic host using a TCP/IP network connection. The SafeNet ProtectServer Network HSM can then be located at any distance from the machine hosting the access provider, cryptographic API and application software.

A network mode implementation of a cryptographic service provider using the SafeNet ProtectServer Network HSMis shown in the next figure.



Implementation steps

The installation and configuration of the SafeNet ProtectServer Network HSM is part of the setup of the overall network operating mode.

The following is a summary (with references to the location of detail) of the steps to setup a cryptographic service provider, using the network operating mode and a SafeNet ProtectServer Network HSM:

1. **Install the SafeNet ProtectServer Network HSM**

   See "Installation" on page 7.

2. **Test the SafeNet ProtectServer Network HSM**

   To confirm the correct operation of the unit, see "Testing and configuration" on page 9.

3. **Configure the SafeNet ProtectServer Network HSM network settings**

   See "Testing and configuration" on page 9 for details.

4. **Install and configure the Network HSM Access Provider software**

   Network HSM Access Provider software must be installed on the network client and configured to support operation in network mode. Full details are in the *SafeNet ProtectServer HSM Access Provider Installation Guide*.

5. **Install the high level cryptographic API**

   Install the high level cryptographic API to be used on the network client. Please refer to the relevant installation guide supplied with the product for further details.

6. **Configure the high-level cryptographic API**

   Generally, further operating mode related configuration of the cryptographic API might be needed to finalize installation. Tasks might include:

   - establishing a trusted channel (secure messaging system (SMS)) between the API and the Protect Server External 2.
   - establishing network communication between the network client and the Protect Server External 2.

For further information refer to the high-level cryptographic API documentation, such as the *ProtectToolkit C Administration Guide.*

Chapter 4
Installation

This chapter provides information on how to install the SafeNet ProtectServer Network HSM.

Since the SafeNet ProtectServer Network HSM is delivered with the necessary software components pre-installed, no software installation is necessary on the unit itself.

Once installation is complete, the unit can be tested to confirm correct operation and to configure the network settings. These steps are covered in "Testing and configuration" on page 9.

Installation procedure

To install the hardware

1. Choose a suitable location to site the equipment. You can mount the SafeNet ProtectServer Network HSM in a standard 19-inch rack, as described in the Quickstart Guide.

> **Note:**
> The plug in the power supply cord is the disconnect device for this equipment. The equipment must therefore be installed near to the mains outlet socket to which it is connected and the mains outlet socket must be easily accessible.

2. Connect the SafeNet ProtectServer Network HSM to the network that hosts the client machine(s) where the SafeNet cryptographic API software is installed. Connect the SafeNet ProtectServer Network HSM to the network by inserting standard Ethernet cables into the LAN connectors located on the front of the SafeNet ProtectServer Network HSM. The LAN connectors are autosensing 10/100/1000 Mb/s Ethernet RJ45 ports.

> **Note:**
> The SafeNet ProtectServer Network HSM is equipped with two NICs (**eth0** and **eth1**), each of which can be configured with its own IP address. The NICs incorporate 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 SafeNet ProtectServer Network HSM is equipped with an autosensing power supply that can accept 100-240V at 50-60Hz.

Smart Card Reader Installation

The ProtectServer offers functionality supporting the use of smart cards. To make use of these features, you must use a SafeNet-supplied smart card reader. Smart card readers, other than those supplied by SafeNet, are not supported.

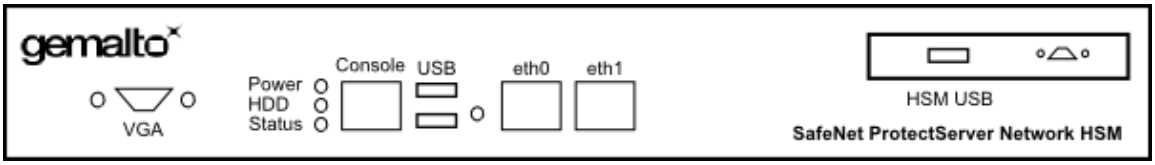
The SafeNet ProtectServer Network HSM supports two different card readers, as follows:

- 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 inteface for power (direct or via a PS/2 to USB adapter)

Installing the USB smart card reader

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



Installing the legacy card reader

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

The card reader qualified with the ProtectServer product also requires connection to a PS/2 port for its power. Many newer servers have USB ports, but do not provide a PS/2 connection.

The options are:

- Connect a PS/2-to-USB adapter cable (pink) between the card reader and a USB port on the SafeNet ProtectServer Network HSM.
- If you prefer to not expose USB ports on your crypto server (for security reasons), then connect a PS/2-to-USB adapter cable between the card reader and a standalone powered USB hub.

Again, the USB connection is for power only. No data transfer occurs.

Chapter 5
Testing and configuration

This chapter provides information on how to:

- test the SafeNet ProtectServer Network HSM to confirm correct operation
- configure network settings.

The assumptions are:

- The installation steps covered in the previous chapter are complete.
- You are familiar with Unix/Linux operating systems and are experienced with their configuration.

Troubleshooting information is at the end of this chapter.

Equipment requirements

To complete the system test and configure the network you must be able to access the SafeNet ProtectServer Network HSM console. You can access the console directly by connecting a keyboard and monitor (not included) to the USB (keyboard) and VGA (monitor) ports located on the front panel of the SafeNet ProtectServer Network HSM, or you can access the console remotely by connecting the RJ45 console port to a terminal emulation device, such as a laptop or terminal server.

Note:
If you want to access the SafeNet ProtectServer Network HSM console remotely using the console port, you will need a 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, as illustrated in Figure 4. If your terminal device is equipped with an RJ45 serial port, you can use an RJ45-to-RJ45 cable, such as an Ethernet cable. Serial cables are not included.

Figure 4: Serial cable: RJ45 to DB9

Procedure overview

Perform the following steps to complete system testing and network configuration. Refer to the indicated sections for more detail if required.

1. **Connect a keyboard/monitor or serial cable to the SafeNet ProtectServer Network HSM**

   In order to access the SafeNet ProtectServer Network HSM console, you must do one of the following:

- connect a keyboard and monitor (not included) to the **USB** (keyboard) and **VGA** (monitor) ports located on the front panel of the SafeNet ProtectServer Network HSM.
- use a serial cable (not included) to connect the RJ45 console port to a terminal emulation device, such as a laptop or terminal server.

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

2. Power on the SafeNet ProtectServer Network HSM

Power on the SafeNet ProtectServer Network HSM and the monitor (if applicable). A green LED on the front of the device will come on and the startup messages will be displayed to the screen. Power-on is complete when the **SafeNet ProtectServer Network HSM login:** prompt is displayed.

3. Login to the console

Following boot up, the SafeNet ProtectServer Network HSM will prompt for login credentials. If you are using a monitor/keyboard, you can log in as **pseoperator**, **admin** or **root**. If you are using a serial connection, you can log in as **pseoperator** or **admin**.

- If you log in as **pseoperator** or **admin**, you are placed in the PSE shell (PSESH), which provides a CLI for configuring and managing the appliance. See “PSESH Command Reference” on page 15.
- If you log in as **root**, you can manually congfigure the network settings using standard Linux commands.

The default passwords for the **root**, **admin,** and **pseoperator** users are as follows:

User name	Default password
root	password
admin	password
pseoperator	password

We **strongly** recommend that you use enter a new password for the admin and root users. Please remember the passwords. There is no recovery option if you lose the system’s root password,other than to obtain an RMA number, ship the unit back to us and have it re-imaged, which is not a warranty service.

4. Run the system test to confirm correct operation

Refer to "System testing" on page 11 for details.

5. **Configure the network settings**

   Refer to “Network configuration” on page 11 for details.

6. **Verify that you have SSH network access to the SafeNet ProtectServer Network HSM (if required)**

   Refer to "SSH network access" on page 14 for details.

7. **Detach keyboard and monitor if no longer required (if applicable)**

System testing

Before field test and deployment we recommend that you run the diagnostic utility *hsmstate* to ensure that the unit is functioning correctly. To do this type *hsmstate* at a command line prompt.

If the unit is functioning correctly a message that includes the following is returned:

```
NORMAL MODE. RESPONDING.
```

You can also use the **PSE_status** command, or the PSESH **status** command (see “PSESH Command Reference” on page 15) to verify that the PSE2 is functioning correctly, as described below.

The PSE_status command

Syntax

```
PSE_status
```

Description

This utility displays the current status of the SafeNet ProtectServer Network HSM. It provides the following information:

- the status of the HSM installed in the SafeNet ProtectServer Network HSM. If the unit is functioning correctly, a message that includes the following is returned:

```
PSE status NORMAL
```

- the status and process ID (pid) of the *etnetserver* process.

Example

```
[admin@PSe ~] PSE_status
1) HSM device 0:      HSM in NORMAL MODE.
2) etnetserver (pid 1026) is running...
PSE status NORMAL
```

Network configuration

IPv4 or IPv6 addressing is supported:

- If you are using IPv4 addressing, you can configure the network settings manually (as **root**) as described below, or using PSESH (as **admin** or **pseoperator**) as described in “PSESH Command Reference” on page 15. PSESH is recommended.

- If you are using IPv6 addressing, you must configure the network settings manually (as **root**). See “Using IPv6 addressing”, below.

Using IPv6 addressing

IPv6 addressing is supported on the appliance, but must be configured manually by logging in as **root** and using standard Linux commands.

IPv6 support is implemented as a dual stack, allowing the appliance to support both IPv4 and IPv6 simultaneously. That is, you can configure both IPv4 and IPv6 addresses on the eth0 and eth1 interfaces.

Manually setting the IP address

You can configure the etho and eth1 interfaces with both an IPv4 and IPv6 IP address. Refer to the Linux documentation for the commands required to set the IPv6 address, if required.

Note: It is recommended that you use psesh:>**network config interface** to configure the IPv4 IP address.

The SafeNet ProtectServer Network HSM is equipped with two NICs (eth0 and eth1), each of which can be configured with its own IP address(es). The IP address for each NIC is specified in the following files:

NIC	Configuration file
eth0	/etc/sysconfig/network-scripts/ifcfg-eth0
eth1	/etc/sysconfig/network-scripts/ifcfg-eth1 **Note:** If you want to use the **eth1** interface, you must create this file. The recommended method is to copy, rename, and edit the **ifcfg-eth0** file.

The entries in the **ifcfg-eth**[**0**|**1**] files are similar to the following:

```
DEVICE= "eth0"
BOOTPROTO="static"
HWADDR="00:0D:48:3B:15:30"
IPADDR="192.168.9.35"
NETMASK="255.255.255.0"
NM_CONTROLLED="yes"
ONBOOT=yes
IPV6INIT=yes
IPV6ADDR=2607:f0d0:1002:0011:0000:0000:0000:0002
IPV6_DEFAULTGW=2607:f0d0:1002:0011:0000:0000:0000:0001
```

Edit the files, as required, to specify an IP address and network mask for each NIC. You must configure one of the NICs. You only need to configure the second NIC if you intend to use it.

Manually setting a hostname and default gateway

Note: It is recommended that you use psesh:>**network config interface** and psesh:>**network config hostname** to set the hostname and gateway, instead of using the manual procedure below.

Set the default gateway (that this SafeNet ProtectServer Network HSM should use) by editing the file `/etc/sysconfig/network`.

If you ever want to address the unit by its name using the loopback connection, you can set the hostname by editing the `/etc/hosts` file and the `/etc/sysconfig/network` file (which governs external connections).

Setting a name server

Note: It is recommended that you use psesh:>**network config dns** to set the name server, instead of using the manual procedure below.

The SafeNet ProtectServer Network HSM processing modules do not have the resources to operate as their own name servers. If name resolution is required, it needs to be provided by a DNS server on the network. In order for the SafeNet ProtectServer Network HSM to use the DNS server, you must add an entry for the DNS server to the file */etc/resolv.conf*, in the following format:

```
nameserver <IP-ADDRESS>
```

Setting access control

Note: It is recommended that you use psesh:>**network config iptables** to configure the iptables, instead of using the manual procedure below.

Access control on the SafeNet ProtectServer Network HSM is performed using `iptables(8)`. Below is a list of `iptables(8)` commands:

```
iptables -[ADC] chain rule-specification [options]
iptables -I chain [rulenum] rule-specification [options]
iptables -R chain rulenum rule-specification [options]
iptables -D chain rulenum [options]
iptables -[LFZ] [chain] [options]
iptables -N chain
iptables -X [chain]
iptables -P chain target [options]
iptables –L [chain]
```

The following `iptables` configuration prevents access to all but one IP address:

1. `iptables -F INPUT` (deletes any previous chains in the INPUT table)
2. `iptables -A INPUT -s [ip-address] -j ACCEPT` (sets an IP address which can be accepted)
3. `iptables -A INPUT -j DROP` (drops everything else)

Once a table configuration has been created that provides suitable network access, it can be stored as the active network configuration using the following command:

```
/etc/init.d/iptables save active
```

Before `iptables(8)` is completely configured it should have an inactive table defined. This is less critical as there is very little running in the operating system by the time the inactive table is loaded. The following is a suitable inactive table:

```
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
```

```
iptables -A FORWARD -j DROP
/etc/init.d/iptables save inactive
```

The active iptables configuration must be restored before connections to the SafeNet ProtectServer Network HSM are allowed. The following command restores the previously saved active configuration.

```
/etc/init.d/iptables stop
/etc/init.d/iptables start
```

SSH network access

After you have completed the network configuration, you can access the SafeNet ProtectServer Network HSM over the network using the SSH protocol. To access the SafeNet ProtectServer Network HSM using SSH, you require an SSH client such as puTTY (available for free from www.putty.org).

Note: You cannot log in as **root** when accessing the SafeNet ProtectServer Network HSM over an SSH connection.

Restarting networking

After making any change to the networking configuration, reboot the SafeNet ProtectServer Network HSM or enter the following command to restart networking:

```
/etc/init.d/networking restart
```

Powering off the SafeNet ProtectServer Network HSM

Note: It is recommended that you use psesh:> **sysconf appliance poweroff** to power off the appliance.

You can also manually power off the appliance. You must be logged in as root to do so.

To manually power off the SafeNet ProtectServer Network HSM

1. Enter the *shutdown* or *poweroff* command to shut down the operating system. The fan and LEDs will remain operational.
2. Toggle the power switch, located on the rear of the SafeNet ProtectServer Network HSM, to the off position. The fan and LEDs will turn off.

Upgrading the SafeNet ProtectServer Network HSM

You can upgrade the SafeNet ProtectServer Network HSM to a later revision using USB media, such as USB memory sticks or a USB-connected CDROM drive.

Process

1. Select and download the desired SafeNet ProtectServer Network HSM image upgrade file from the SafeNet Web site at http://www.safenet-inc.com.
2. Place the upgrade files onto the root directory of a USB memory stick or onto a CDROM.

3. Connect the CDROM drive or memory stick to any USB port on the back of the SafeNet ProtectServer Network HSM. The operating system maps the new hardware and adds a /etc/fstab entry.
4. The relevant directory is created in /media (examples: /media/usbflash, or /media/cdrecorder) but does not automount - complete with mount command (example: mount /media/usbflash).
5. Use umount command to unmount when finished and the device is to be removed.

Notes:
When mounting multiple devices at once, or mounting and unmounting many times in the same session, you might wish to check /etc/fstab to see where the device is associated.
The mount point will always default to the /media directory, but specific directories listed above (usbflash, cdrecorder) are just examples. The name can vary depending on the device capability and how it is detected.

Troubleshooting

Each SafeNet 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 utility program *hsmstate* as discussed in the System Testing section 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 SafeNet support engineer.

Note:
If it ever becomes necessary to get into the BIOS then press <Delete> as the SafeNet ProtectServer Network HSM boots.

For further assistance contact your supplier or SafeNet 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

Chapter 6
PSESH Command Reference

This chapter describes how to access and use the PSESH shell command line tool to configure your SafeNet ProtectServer Network HSM appliances. It provides detailed syntax descriptions for each available command.

About PSESH

The PSESH shell command line tool provides access to the SafeNet ProtectServer Network HSM shell for performing basic appliance configuration tasks such as network configuration and appliance software package updates and management.

PSESH commands are not case sensitive.

Access to PSESH is via SSH or the local console.

Users

PSESH supports the following users:

User	Description
pseoperator	The **pseoperator** user is responsible for configuring the appliance for client access. The **pseoperator** user is able to execute the PSESH commands used to configure the appliance network parameters such as IP addresses, iptables, and routes etc., as well as appliance settings such as the date/time, SNMP configuration, etc.
admin	The **admin** user is responsible for managing the appliance. The **admin** user is able to execute all of the PSESH commands available to the **pseoperator**, as well as commands used to perform package upgrades/installations, troubleshooting, viewing log files, and extracting log files. The admin user is also able to reset the password for the **pseoperator** user.

Features

PSESH provides the following features:

Feature	Description
Command history	You can scroll through the commands you have entered on the PSESH command line using the up/down arrows keys.
Command shortcuts	You must type sufficient letters of a command or sub-command to make the input unique in the current syntax. For example, you could invoke system syntax help with “help”, “hel”, “he”, but not just “h” (because there is also an "hsm" command and typing just "h" is not sufficient to indicate whether you want "help" or "hsm").
Command	You can use the TAB key to automatically complete partially typed

Feature	Description
completion	commands. This allows you to type only enough characters to uniquely identify the command, and then press TAB to automatically fill in the rest of the characters for the command.
Command syntax help	To display help information for a command, type **help** <command_name> , or **?** <command_name>.

Accessing PSESH

You can access PSESH by connecting a keyboard and monitor to the appliance, using a serial connection, or using an SSH client (such as puTTY in Windows or the **ssh** command in Linux) after the network settings have been configured.

To access PSESH

1. Connect to the appliance (monitor and keyboard, serial connection, or SSH)

   When a successful connection is made, a terminal window opens and the prompt "login as:" appears.

   You can log in as **admin** or **pseoperator**:

   - **pseoperator** – The ‘pseoperator’ user is responsible for configuring/preparing the HSM for client access by configuring network parameters such as the IP addresses, iptables, routes etc., as well as device’s date/time, snmp settings, etc.
   - **admin** – In addition to the ‘pseoperator’ commands, ‘admin’ user will be responsible for package upgrades/installs. ‘admin’ will also be able to reset ‘pseoperator’ password and run commands for troubleshooting and viewing and extracting log files.

2. You are prompted for the password. If this is the first time you have connected, the default password is "password". You will be prompted to enter a new password.

Once you have logged in, the system presents the PSESH prompt, which includes the hostname that you have assigned to the appliance:

```
[myPSE] psesh:>
```

You can now issue any PSESH command. For a summary, type "?" or "help" and press Enter.

Command Reference

This section describes the commands available in the SafeNet ProtectServer Network HSM command shell (psesh). The commands are described in alphabetical order and provide:

- a brief description of the command function
- the command syntax and parameter descriptions
- usage examples.

The top level commands are as follows:

Command	Description
exit	Exit the PSESH shell.
files	Manage the files that have been transferred to the appliance's SCP directory.
help	Display syntax help for the specified command. You can use the ? symbol instead of the string "help" as an alternative way of displaying the help.
hsm	Display the current state of the HSM, or reset the HSM if it becomes unresponsive.
network	View or configure the network settings for the SafeNet ProtectServer Network HSM appliance.
package	Manage the software packages installed the appliance.
service	Manage the services on the appliance.
status	Display the current status of the appliance.
sysconf	Configure the appliance time, date, or SNMP settings, or reboot or power-off the appliance.
syslog	Display or archive the syslog.
user	Set or change the password of the current user.

exit

Exit the PSESH shell. This ends the PSESH session.

User access

admin, pseoperator

Syntax

exit

Example

```
psesh:> exit
```

files

Manage the files that have been transferred to the appliance using SCP. These files are automatically placed in the SCP directory, and cannot be moved.

User access

admin, pseoperator

Syntax

files [**clear** | **delfile –file** <filename> | **show**]

Parameter	Shortcut	Description

clear	**c**	Delete all of the files in the appliance's SCP directory.
delfile <filename>	**d** <filename>	Delete the specified file from the appliance's SCP directory.
show	**s**	List all of the files that currently reside in the appliance's SCP directory.

Example

```
psesh:> files show

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

total 861K

248K PTKnetsrv-5.2.0-4.i386.rpm

613K PTKpcihsmK6-5.2.0-4.i386.rpm

Command Result : 0 (Success)


psesh:>files delete PTKnetsrv-5.2.0-4.i386.rpm

This will delete file 'PTKnetsrv-5.2.0-4.i386.rpm' in the scp folder.
Continue [y/n]?

> y

Proceeding....

File 'PTKnetsrv-5.2.0-4.i386.rpm' deleted.

Command Result : 0 (Success)


psesh:>files clear

This will delete all the files in the scp folder. Continue [y/n]?

> y

Proceeding....

All files deleted.

Command Result : 0 (Success)
```

help

Display syntax help for the specified command. You can use the ? symbol instead of the string "help" as an alternative way of displaying the help.

User access

admin, pseoperator

Syntax

help <command>

Example

```
psesh:> help help
```

```
Type "help" or "?" (without the double quotation marks) to see help
and syntax information for any Luna Shell command.

"help" or "?" with no arguments lists the top level commands with
brief descriptions.

"help" or "?" followed by one or more arguments (command names, sub-
commands, options) yields increasingly detailed information.

For example:

The command "? hsm" returns general information on the "hsm"
commands.

The command "help hsm state" returns information on the "hsm state"
subcommands.

The '-force' option, on any command that supports that option, causes
the command to proceed silently, without prompting you for input -
this is useful for scripting.

Command Result : 0 (Success)


psesh:> ? hsm

Syntax:      hsm

The following subcommands are available:

Name                 (short)    Description

-------------------------------------------------------------

state                s          Shows HSM State

reset                r          Reset HSM

Command Result : 0 (Success)
```

hsm

Display the current state of the HSM, or reset the HSM if it becomes unresponsive.

User access

admin, pseoperator

Syntax

hsm [**state** | **reset**]

Parameter	Shortcut	Description
reset	**r**	Reset the HSM if it has stopped responding, but your computer is still responsive. This command closes out any login status and open sessions.
state	**s**	Display the current state of the HSM.

Example

```
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)


psesh:>hsm reset
Executing this command will disrupt all client connections. Proceed
[y/n]?
> n
Exiting....
Command Result : 0 (Success)
```

network

View or configure the network settings for the SafeNet ProtectServer Network HSM appliance.

User access

admin, pseoperator

Syntax

network [**dns** | **domain** <domain> **| hostname** <hostname> **| interface | iptables | ping** <hostname_or_IP> **| route** | **show**]

Parameter	Shortcut	Description
dns	**dn**	Add or delete DNS name servers and domains. See “network dns”, below.
domain	**do**	Set the domain for the appliance. Enter this keyword followed by the domain name.
hostname	**h**	Set the hostname for the appliance.
interface	**in**	Configure the appliance network interfaces. See “network interface”, below.
iptables	**ip**	Configure the iptables firewall for the appliance. You can use this command to configure the iptables ACCEPT and DROP rules. See “network iptables”, below.
ping	**p**	Test connectivity from the appliance to the specified hostname or IP address.
route	**r**	Manually configure routes on the SafeNet ProtectServer Network HSM appliance. See “network route”, below.
show	**s**	Display the current network configuration.

network dns

Configure the Domain Name Server (DNS) settings on the SafeNet ProtectServer Network HSM appliance. You can use this command to add or delete a DNS name server or search domain.

Syntax

network dns [**add** | **delete**] [**nameserver** <dns_name_server> | **searchdomain** <dns_search_domain>]

Parameter	Shortcut	Description
add nameserver <dns_name_server>	**a n**	Add a DNS name server to the list of servers used to provide DNS services to the appliance.
add searchdomain <dns_search_domain>	**a s**	Add a DNS search domain to the list of search domains that are automatically appended to URLs provided by the appliance.
delete nameserver <dns_name_server>	**d n**	Delete a DNS name server from the list of servers used to provide DNS services to the appliance.
delete searchdomain <dns_search_domain>	**d s**	Delete a DNS search domain from the list of search domains that are automatically appended to URLs provided by the appliance.

Example

```
psesh:> net dns add nameserver 192.16.0.2
Success: Nameserver 192.16.0.2 added

psesh:> net dns add searchdomain 192.16.0.0
Success: Searchdomain entry 192.16.0.0 added

psesh:> net dns delete -nameserver 192.16.0.2
Success: Nameserver 192.16.0.2 deleted

psesh:> net dns delete -searchdomain 192.16.0.0
Success: Searchdomain entry 192.16.0.0 deleted
```

network interface

Configure the appliance network interfaces. You can use static IP addressing or DHCP. Static addressing is the default.

Syntax

network interface {**static** | **dhcp** | **delete**}

Parameter	Shortcut	Description
delete	**de**	Delete the network configuration for a network interface (eth0 or eth1). See “network interface delete”, below.
dhcp	**dh**	Delete a DNS name server from the list of servers used to provide DNS services to the appliance.
static	**s**	Delete a DNS search domain from the list of search domains that are automatically appended to URLs provided by the appliance.

network interface delete

Delete the network configuration for a network interface (eth0 or eth1).

Syntax

network interface delete -device <netdevice>

Parameter	Shortcut	Description
-device <netdevice>	**-d**	Specifies the interface whose configuration you want to delete. **Valid values:** eth0, eth1

Example

```
psesh:> network interface delete -device eth1

Interface eth1 removed successfully.

'network -interface' successful. Ethernet device eth1 set to ip
address (null).
```

network interface dhcp

Configure the network interface to request a dynamic IP address.

Note: DHCP is not recommended.

Syntax

network interface dhcp -device <netdevice> [**-force**]

Parameter	Shortcut	Description
-device <netdevice>	**-d**	Specifies the interface you want to configure to use DHCP. **Valid values:** eth0, eth1

network interface static

Configure a static IP address on the specified network interface.

Syntax

network interface static -device <netdevice> **-ip** <ipaddress> **-netmask** <ipaddress> [**-gateway** <ipaddress>] [**-force**]

Parameter	Shortcut	Description
-device <netdevice>	**-d**	Specifies the interface you want to configure. **Valid values:** eth0, eth1
-ip <ipaddress>	**-i**	Specifies the IP address to assign to the specified device.
-netmask <ipaddress>	**-n**	Specifies the network mask, in IP address format, to assign to the specified device.

-gateway <ipaddress>	**-g**	Specifies the gateway to assign to the specified device.
-force	**-f**	Force the action without prompting.

Example

```
psesh:> net -interface -static -device eth1 -ip 192.22.101.77 -
gateway 192.16.0.2 -netmask  255.255.0.0

   'net -interface' successful.

Ethernet device eth1 set to ip address 192.22.101.77.
```

network iptables

Configure the iptables firewall for the appliance. You can use this command to configure the iptables ACCEPT and DROP rules.

By default, the SafeNet 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 SafeNet ProtectServer Network HSM is not used to forward packets, as in a router or proxy.

Syntax

network iptables [**show** | **addrule** | **delrule** | **save** | **clear**]

Parameter	Shortcut	Description
addrule	**a**	Add an ACCEPT or DROP rule to the iptables firewall for the appliance. See “network iptables addrule”, below.
clear	**c**	Add a host or network DROP rule to the iptable for the appliance.
delrule <ip_address>	**d**	Specifies the IP address of the host you are adding the rule for.
save	**sa**	Specifies the IP address and network mask for the network you are adding the rule for.
show	**sh**	Display the current iptables configuration.

network iptables addrule

Add an ACCEPT or DROP rule to the iptables firewall for the appliance.

WARNING! These rules govern network access to the appliance. Adding a malformed rule may cause a lockout.

Note: You must use the **network iptables save** command to save your changes. Failure to do so will result in your changes being discarded on the next appliance restart.

Syntax

network iptables addrule {**accept** | **drop**} {**host –ip** <ip_address> | **network –net** <ip_address> **-mask** <network_mask>}

Parameter	Shortcut	Description
accept	**a**	Add a host or network ACCEPT rule to the iptable for the appliance.
drop	**d**	Add a host or network DROP rule to the iptable for the appliance.
host –ip <ip_address>	**h -i**	Specifies the IP address of the host you are adding the rule for.
network –net <ip_address> **-mask** <network_mask>	**n –n -m**	Specifies the IP address and network mask for the network you are adding the rule for.

network route

Manually add a network route to the routing table for the appliance.

CAUTION: Use this command only under the advice and supervision of your network administrator.

Syntax

network route add <route_type> <ipaddress> [**-device** <interface>] [**-metric** <metric>] [**-netmask** <ipaddress>] [**-gateway** <ipaddress>] [**-force**]

Parameter	Shortcut	Description
<route_type>		Specifies the type of route you want to add. **Valid values:** host, network
<ip_address>		Specifies the IP address of the route you want to add.
-device <interface>	**-d**	Specifies the interface you want to configure. **Valid values:** eth0, eth1
-metric <metric>	**-m**	Specifies the routing metric for the route. **Range:** 0-65535
–netmask <ip_address>	**-n**	Specifies the network mask for the route, in IP address format.
-gateway <ip_address>	**-g**	Specifies the IP address of the gateway for the route.
-force	**-f**	Force the action without prompting.

package

Manage the software packages installed the appliance.

User access

admin

Syntax

package {**list** [**all** | **ptk**] | **update**}

Parameter	Shortcut	Description
list [all | ptk]	**l a** **l p**	List the packages currently installed on the appliance. Use the **all** flag to list all packages. Use the **ptk** flag to list the PTK packages only.
update –file <package_file>	**u**	Update the specified package file. Before you can update a package, you must use **scp**/**pscp** to securely copy the update package file to the appliance's SCP directory.

Example

```
psesh:>package list ptk

PTKpcihsmK6-5.2.0-4.i386
PTKnetsrv-5.2.0-4.i386

Command Result : 0 (Success)

psesh:>package update –file PTKpcihsmK6-5.2.0-4.i386
```

service

Manage the following services on the appliance:

- **network** - Network service (needed for etnetserver, ssh, and scp)
- **etnetserver** - HSM service required for client connections
- **iptables** - Firewall service
- **snmp** - SNMP agent service
- **ssh** - Secure shell service (needed for ssh and scp)
- **syslog** - Syslog service

User access

admin, pseoperator

Syntax

service {**list** | **restart** <service> | **start** <service> | **status** <service> | **stop** <service>}

Parameter	Shortcut	Description
list	**l**	List the services you can manage on the appliance.

restart <service>	**r**	Restart the specified service. Services require restarting if their configurations have changed. For example, after changing any network settings using the network commands, you should restart the network service to ensure the new settings take effect. Restarting a service isn't always the same as stopping and then starting a service. If you restart the network service while connected to the appliance via the network (ssh), you will not lose your connection (assuming no changes were made that would cause a connection loss). However, if you were to stop the network service, you would immediately lose your connection, and you would need to log in via the local console to start the service again. **Valid values:** network, etnetserver, iptables, snmp, ssh, syslog
start <service>	**star**	Stop the specified service. **Valid values:** network, etnetserver, iptables, snmp, ssh, syslog
status <service>	**stat**	Display the status (stopped, not stopped) of the specified service. **Valid values:** network, etnetserver, iptables, snmp, ssh, syslog
stop <service>	**sto**	Stop the specified service.. **Valid values:** network, etnetserver, iptables, snmp, ssh, syslog

Example

```
psesh:>service list

The following are valid PSe service names:
  network     - Network service (Needed for etnetserver, ssh and scp)
  etnetserver - HSM service required for client connections
  iptables    - Firewall Service
  snmp        - SNMP agent service
  ssh         - Secure shell service (Needed for ssh and scp)
  syslog      - Syslog service

Command Result : 0 (Success)

psesh:>service stop syslog

Starting kernel logger:                                [  OK  ]
Starting system logger:                                [  OK  ]

Command Result : 0 (Success)

psesh:>service start syslog

Starting system logger:                                [  OK  ]
Starting kernel logger:                                [  OK  ]
```

```
Command Result : 0 (Success)

psesh:>service restart network

Shutting down interface eth0:                              [  OK  ]
Shutting down interface eth1:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:                                [  OK  ]
Bringing up interface eth1:                                [  OK  ]

Command Result : 0 (Success)

psesh:>service status network

eth0 is up

Command Result : 0 (Success)
```

status

Display the current status of the appliance.

User access

admin, pseoperator

Syntax

status {**cpu** | **date** | **disk** | **interface** | **mac** | **mem** | **netstat** | **ps** | **time** | **zone**}

Parameter	Shortcut	Description
cpu	**c**	Display the current CPU load. The CPU load data is presented as a series of five entries, as follows: 1.The average CPU load for the previous minute. This value is 0.14 in the example below. 2.The average CPU load for the previous five minutes. This value is 0.10 in the example below. 3.The average CPU load for the previous ten minutes. This value is 0.08 in the example below. 4.The number of currently running processes and the total number of processes. The example below shows 1 of 68 processes running. 5.The last process ID used. This value is 11162 in the example below.
date	**da**	Display the current date and time.
disk	**di**	Display hard disk utilization.
interface	**i**	Display configuration and status information for the eth0 and eth1 interfaces.
mac	**ma**	Display the MAC address of the eth0 and eth1 interfaces, if they have been configured.
mem	**me**	Display the current memory usage.

netstat	**n**	Display the current network connections.
ps	**p**	Display the status of all active processes.
time	**t**	Display the time currently configured on the appliance, using the 24 hour clock.
zone	**z**	Display the currently configured time zone.

Example

```
psesh:>status cpu

CPU Load Averages:
0.14 0.10 0.08 1/68 11162

System uptime:
At Tue Jan 26 06:35:23 EST 2016, I am up 4 days and 23:38 hours.

Command Result : 0 (Success)


psesh:>status date

Tue Jan 26 06:42:45 EST 2016

Command Result : 0 (Success)


psesh:>status disk

==================+ Hard Disk utilization ==================
Filesystem     1K-blocks   Used Available Use% Mounted on
/dev/sda2        3681872 697972   2793540  20% /
/dev/sda1         194241  20079    163922  11% /boot

Command Result : 0 (Success)


psesh:>status interface

eth0  Link encap:Ethernet  HWaddr 00:0D:48:3B:5E:E4
      inet addr:172.20.11.150  Bcast:172.20.11.255 Mask:255.255.255.0
      inet6 addr: fe80::20d:48ff:fe3b:5ee4/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:1431830 errors:0 dropped:0 overruns:0 frame:0
      TX packets:557730 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:681075738 (649.5 MiB)  TX bytes:272653499 (260.0 MiB)
      Interrupt:16 Memory:fe9a0000-fe9c0000

eth1  Link encap:Ethernet  HWaddr 00:0D:48:3B:5E:E5
      BROADCAST MULTICAST  MTU:1500  Metric:1
      RX packets:269 errors:0 dropped:0 overruns:0 frame:0
      TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:29400 (28.7 KiB)  TX bytes:2178 (2.1 KiB)
      Interrupt:17 Memory:feaa0000-feac0000

ETH0 (Speed|Duplex): 1000Mb/s|Full
ETH1 (Speed|Duplex): Unknown!|Unknown!

Command Result : 0 (Success)
```

```
psesh:>status mac

eth0 00:0D:48:3B:5E:E4

Command Result : 0 (Success)


psesh:>status mem

             total    used    free  shared   buffers  cached
Mem:       1019668  167744  851924     164     35332   67256
-/+ buffers/cache:   65156  954512
Swap:            0       0       0

Command Result : 0 (Success)


psesh:>status netstat

Active Internet connections (servers and established)

Proto Recv-Q Send-Q Local Address    Foreign Address    State
tcp        0      0 0.0.0.0:22       0.0.0.0:*          LISTEN
tcp        0      0 172.20.11.150:22 172.20.10.102:57457
ESTABLISHED
tcp        0      0 :::12396         :::*               LISTEN

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags    Type    State      I-Node Path
unix  5      [ ]      DGRAM              10269  /dev/log
unix  2      [ ACC ]  STREAM  LISTENING  8394 @/com/ubuntu /upstart
unix  2      [ ]      DGRAM              8828 @/org/kernel/udev/udevd
unix  2      [ ]      DGRAM              24040
unix  2      [ ]      DGRAM              24010
unix  2      [ ]      DGRAM              10425
unix  3      [ ]      DGRAM              8845
unix  3      [ ]      DGRAM              8844

Command Result : 0 (Success)


psesh:>status ps

USER  PID %CPU %MEM    VSZ   RSS TTY    STAT START   TIME COMMAND
root    1  0.0  0.1   2900  1404 ?      Ss   Jan21   0:02 /sbin/init
root    2  0.0  0.0      0     0 ?      S    Jan21   0:00 [kthreadd]
.
.
root 3221  0.0  0.0      0     0 ?      S    07:01   0:00 [flush-8:0]
root 3226  0.0  0.1   2984  1080 pts/0  S+   07:04   0:00 /bin/sh S
root 3227  0.0  0.0   2856   956 pts/0  R+   07:04   0:00 ps auxw


Command Result : 0 (Success)


psesh:>status time
07:09:22

Command Result : 0 (Success)


psesh:>status zone
EST

Command Result : 0 (Success)
```

sysconf

Configure the appliance time, date, or SNMP settings, or reboot or power-off the appliance.

User access

admin, pseoperator

Syntax

sysconf {**appliance** | **snmp** | **time** | **timezone**}

Parameter	Shortcut	Description
appliance	**a**	Reboot or power-off the appliance. See “sysconf appliance”, below.
snmp	**s**	Configure the SNMP settings on the appliance. See “sysconf snmp”, below.
time	**t**	Set the appliance time and date.
timezone	**timez**	Display or set the appliance timezone. See “sysconf timezone”, below.

sysconf appliance

Reboot or power-off the appliance.

Syntax

sysconf appliance {**poweroff** | **reboot**}

Parameter	Shortcut	Description
poweroff	**p**	Power-off the appliance.
reboot	**r**	Reboot the appliance.

sysconf snmp

Enable or disable the SNMP service, or display or configure the SNMP settings for the appliance.

Syntax

sysconf snmp {config | disable | enable | show}

Parameter	Shortcut	Description
config	**c**	Configure the SNMP settings for the appliance. See “sysconf snmp config”, below.
disable	**d**	Disable SNMP on the appliance and stop the SNMP service.
enable	**e**	Enable SNMP on the appliance and start the SNMP service.

show	**s**	Display the current SNMP settings for the appliance.

Example

```
lunash:>sysconf snmp enable

SNMP is enabled
Starting snmpd:          [  OK  ]
SNMP is started

Command Result : 0 (Success)


lunash:>sysconf snmp disable

SNMP is disabled
Stopping snmpd:        [  OK  ]
SNMP is stopped

Command Result : 0 (Success)


psesh:>sysconf snmp show

SNMP is not running

SNMP is disabled


Current SNMP configuration


######################################################################

#             SafeNet ProtectServer SNMP v2c snmpd.conf              #

######################################################################

agentuser root
syslocation TESTLAB
syscontact TESTCONTACT
com2sec secName 192.168.11.17 COMMUNITY
group secNameGroup v2c secName
view systemview included .1.3.6.1.2.1.1
view systemview included .1.3.6.1.2.1.2
view systemview included .1.3.6.1.2.1.25.1
view systemview included .1.3.6.1.2.1.25.2
view systemview included .1.3.6.1.2.1.25.3
view systemview included .1.3.6.1.2.1.25.4
access secNameGroup " " any noauth exact systemview none none

Command Result : 0 (Success)
```

sysconf snmp config

Configure the SNMP server on the appliance.

Syntax

sysconf snmp config -contact <string> **-location** <string> **-ip** <ipaddress> **-community** <string>

Parameter	Shortcut	Description

-community	**-com**	Specifies the community string for the SNMP server on the appliance. SNMP community strings function as passwords that are embedded in every SNMP packet to authenticate access to the Management Information Base (MIB) on the appliance. Enter this keyword followed by the community string.
-contact	**-con**	Specifies the contact information for the SNMP server on the appliance. Enter this keyword followed by the contact information string. Enclose the string in quotes if it contains spaces.
-ip	**-i**	Specifies the IP address of the SNMP trap destination. Enter this keyword followed by the IP address of the host used to accept SNMP traps that originate on the appliance.
-location	**-l**	Specifies the location of the SNMP server on the appliance. Enter this keyword followed by the location string. Enclose the string in quotes if it contains spaces.

sysconf timezone

Display or set the timezone on the appliance.

Syntax

sysconf timezone {**set** | **show**}

Parameter	Shortcut	Description
set	**se**	Set the time zone on the appliance. The appliance uses the Linux standard for specifying the time zone. This standard provides several different methods for specifying the time zone. For example, if you are located in Toronto, Canada, you could specify the time zone as EST, Canada/Eastern, America/Toronto, or GMT-5. For a list of valid time zones, refer to the /usr/share/zoneinfo directory on any Redhat distribution.
show	**sh**	Display the currently configured time zone.

Example

```
psesh:> sysconf timezone set America/Toronto
```

```
Timezone set to America/Toronto
psesh:> sysconf timezone show
EST
```

syslog

Display or archive the syslog.

User access

admin, pseoperator

Syntax

syslog {**tail** | **tarlogs**}

Parameter	Shortcut	Description
tail	**se**	Display the last entries of the specified syslog. See "syslog tail", below.
tarlogs	**sh**	Create an archive of the syslog

Example

```
psesh:>syslog tar
Generating package list...
Generating tarlogs...
The tar file containing logs is now available via scp as filename
'pselogs.tgz'.
Command Result : 0 (Success)
```

syslog tail

Display the last entries of the syslog. If no number is included, the command displays the entire syslog.

Syntax

syslog tail -logname <logname> [**-entries** <logentries>] [**-search** <string>]

Parameter	Shortcut	Description
-entries <integer>	**-e**	Specifies the number of entries to display. If this parameter is not specified, the entire log is displayed. Enter this keyword followed by the number of log entries you want to display. **Range:** 0-2147483647
-logname <logname>	**-l**	Species the name of the log you want to display. Enter this keyword followed by the log name. **Valid values:** messages, secure
-search <string>	**-s**	Search the log for the specified string. Enter this keyword followed by the string you want to find.

Example

```
psesh:>syslog tail -logname messages -entries 10

Feb 12 12:00:17 PSe-II snmpd[3963]: Connection from UDP:
[172.16.21.19]:62386->[172.20.11.150]

Feb 12 12:00:18 PSe-II snmpd[3963]: Connection from UDP:
[172.16.21.19]:62386->[172.20.11.150]

Feb 12 12:04:16 PSe-II psesh [4341]: info : 0 : pssh user login :
admin : 172.16.181.182/51177

Feb 12 12:04:28 PSe-II psesh [4341]: info : 0 : Command: help syslog
: admin : 172.16.181.182/51177

Feb 12 12:06:36 PSe-II psesh [4341]: info : 0 : Command: help syslog
tar : admin : 172.16.181.182/51177

Feb 12 12:07:32 PSe-II psesh [4341]: info : 0 : Command: syslog tail
: admin : 172.16.181.182/51177

Feb 12 12:09:55 PSe-II psesh [4341]: info : 0 : Command: syslog
tarlogs  : admin : 172.16.181.182/51177

Feb 12 12:09:57 PSe-II rsyslogd: [origin software="rsyslogd"
swVersion="5.8.10" x-pid="927" x-info="http://www.rsyslog.com"]
rsyslogd was HUPed

Feb 12 12:14:59 PSe-II psesh [4341]: info : 0 : Command: syslog tail
-logname messages -entries 10 : admin : 172.16.181.182/51177

Feb 12 12:15:16 PSe-II psesh [4341]: info : 0 : Command: syslog tail
-logname messages -entries 10 : admin : 172.16.181.182/51177

Command Result : 0 (Success)
```

user password

Set or change the password for the current user. The admin user can also use the **–user** parameter to change the password for the **pseoperator** user. Although there are no restrictions on the password you can use, warnings are displayed if the password is short, simple, or uses a dictionary word.

User access

admin, pseoperator

Syntax

user password [-user <username>**]**

Example

```
psesh:>user password

Changing password for user admin.

New password:

BAD PASSWORD: it is too short
BAD PASSWORD: is too simple

Retype new password:

Sorry, passwords do not match.

New password:

BAD PASSWORD: it is too short
BAD PASSWORD: is too simple
```

```
Retype new password:
passwd: all authentication tokens updated successfully.
Command Result : 0 (Success)
[PSe-II] psesh:>user password
Changing password for user admin.
New password:
BAD PASSWORD: it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
Command Result : 0 (Success)
psesh:>user password –user pseoperator
Changing password for user pseoperator.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Appendix A
Technical specifications

The SafeNet 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
- ATOM D425 CPU
- 1 Gb RAM
- 2 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
- SafeNet PCI HSM Access Provider software
- SafeNet 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%

END OF DOCUMENT