

# SafeNet ProtectToolkitSafeNet ProtectServer Network HSM

Installation and Configuration Guide

## Document Information

<b>Product Version</b>	5.3
<b>Document Part Number</b>	007-013682-001
<b>Release Date</b>	05 December 2016

## Revision History

<b>Revision</b>	<b>Date</b>	<b>Reason</b>
Rev. A	05 December 2016	Initial release

## Trademarks, Copyrights, and Third-Party Software

Copyright 2009-2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

## Disclaimer

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

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

# CONTENTS

<b>PREFACE</b>	<b>About the SafeNet ProtectServer Network HSM Installation and Configuration Guide</b>	<b>6</b>
Customer Release Notes		6
Gemalto Rebranding		6
Audience		7
Document Conventions		7
Notes		7
Cautions		7
Warnings		8
Command Syntax and Typeface Conventions		8
Support Contacts		8
<b>1</b>	<b>Product Overview</b>	<b>10</b>
Front panel view		10
Rear panel view		11
Cryptographic architecture		12
Summary of Cryptographic Service Provider setup		13
<b>2</b>	<b>Hardware Installation</b>	<b>14</b>
Installation procedure		14
<b>3</b>	<b>Testing and Configuration</b>	<b>16</b>
Step 1: Access the Console		16
Step 2: Power on and Log in		17
Step 3: Run System Test		18
hsmstate		18
psesh:> hsm state		18
Step 4: Network Configuration		18
Setting the IP address		19
Setting the hostname and default gateway		19
Setting a name server		20
Setting access control		20
Restarting networking		21
Step 5: SSH Network Access		21
Powering off the SafeNet ProtectServer Network HSM		21
Upgrading the SafeNet ProtectServer Network HSM		21
Troubleshooting		22
<b>4</b>	<b>PSESH Command Reference</b>	<b>23</b>
About PSESH		24
Accessing PSESH		25
exit		26

files .....	27
help .....	28
hsm .....	29
network .....	30
network dns .....	32
network interface .....	33
network interface delete .....	34
network interface dhcp .....	35
network interface static .....	36
network iptables .....	37
network iptables addrule .....	39
network iptables delrule .....	40
network route .....	41
network route add .....	42
network route clear .....	43
network route delete .....	44
network route show .....	45
package .....	46
service .....	47
status .....	49
sysconf .....	53
sysconf appliance .....	54
sysconf snmp .....	55
sysconf snmp config .....	57
sysconf timezone .....	58
syslog .....	59
syslog export .....	60
syslog period .....	61
syslog remotehost .....	62
syslog remotehost add .....	63
syslog remotehost clear .....	64
syslog remotehost delete .....	65
syslog remotehost list .....	66
syslog rotate .....	67
syslog rotations .....	68
syslog show .....	69
syslog tail .....	70
syslog tarlogs .....	71
user password .....	72
 APPENDIX A    Technical Specifications .....	 73
 APPENDIX B    Glossary of terms .....	 74

# PREFACE

## About the SafeNet ProtectServer Network HSM Installation and Configuration Guide

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). It contains the following sections:

- "Product Overview" on page 10
- "Hardware Installation" on page 14
- "Testing and Configuration" on page 16
- "PSESH Command Reference" on page 23
- "Technical Specifications" on page 73
- "Glossary of terms" on page 74

This preface also includes the following information about this document:

- "Customer Release Notes" below
- "Gemalto Rebranding" below
- "Audience" on the next page
- "Document Conventions" on the next page
- "Support Contacts" on page 8

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

## Customer Release Notes

---

The customer release notes (CRN) provide important information about this release that is not included in the customer documentation. It is strongly recommended that you read the CRN to fully understand the capabilities, limitations, and known issues for this release. You can view or download the latest version of the CRN for this release at the following location:

[http://www.securedbysafenet.com/releasenotes/ptk/crn\\_ptk\\_5-3.pdf](http://www.securedbysafenet.com/releasenotes/ptk/crn_ptk_5-3.pdf)

## 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 Luna name has been removed from the SafeNet HSM product line, with the SafeNet name being 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 Gemalto 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
<b>bold</b>	The bold attribute is used to indicate the following: <ul style="list-style-type: none"> <li>Command-line commands and options (Type <b>dir /p.</b>)</li> <li>Button names (Click <b>Save As.</b>)</li> <li>Check box and radio button names (Select the <b>Print Duplex</b> check box.)</li> <li>Dialog box titles (On the <b>Protect Document</b> dialog box, click <b>Yes.</b>)</li> <li>Field names (<b>User Name:</b> Enter the name of the user.)</li> <li>Menu names (On the <b>File</b> menu, click <b>Save.</b>) (Click <b>Menu &gt; Go To &gt; Folders.</b>)</li> <li>User input (In the <b>Date</b> box, type <b>April 1.</b>)</li> </ul>
<i>italics</i>	In type, the italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[ <b>optional</b> ] [<optional>]	Represent optional <b>keywords</b> 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.
{ <b>a b c</b> } {<a> <b> <c>}	Represent required alternate <b>keywords</b> 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.
[ <b>a b c</b> ] [<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 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	
<b>Address</b>	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA	
<b>Phone</b>	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
<b>Web</b>	<a href="https://safenet.gemalto.com">https://safenet.gemalto.com</a>	
<b>Support and Downloads</b>	<a href="https://safenet.gemalto.com/technical-support">https://safenet.gemalto.com/technical-support</a> Provides access to the Gemalto Knowledge Base and quick downloads for various products.	
<b>Technical Support Customer Portal</b>	<a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a> 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.	

# 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. Together with high-level SafeNet application programming interface (API) software, it provides cryptographic services for a wide range of secure applications.

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

The full range of cryptographic services required by Public Key Infrastructure (PKI) users is supported by the 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.

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

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

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

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

## Front panel view

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

**Figure 1: SafeNet ProtectServer Network HSM front panel**



## Ports

The front panel is equipped with the following ports:

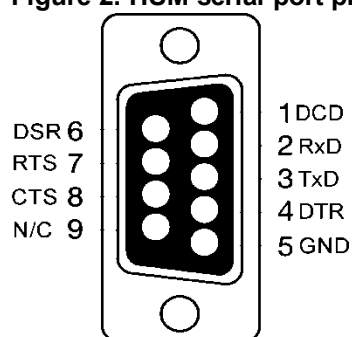
VGA	Connects a VGA monitor to the appliance.
-----	--

Console	Provides console access to the appliance. See <a href="#">"Testing and Configuration" on page 16</a> .
USB	Connects USB devices such as a keyboard or mouse to the appliance.
eth0 eth1	Autosensing 10/100/1000 Mb/s Ethernet RJ45 ports for connecting the appliance to the network.
HSM USB	Connects a smart card reader to the appliance using the included USB-to-serial cable.

## HSM serial port pin configuration

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

**Figure 2: HSM serial port pinout**



## LEDs

The front panel is equipped with the following LEDs:

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

## Reset button

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

## Rear panel view

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

**Figure 3: SafeNet ProtectServer Network HSM rear panel**



## Tamper lock

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

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



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

## Cryptographic architecture

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

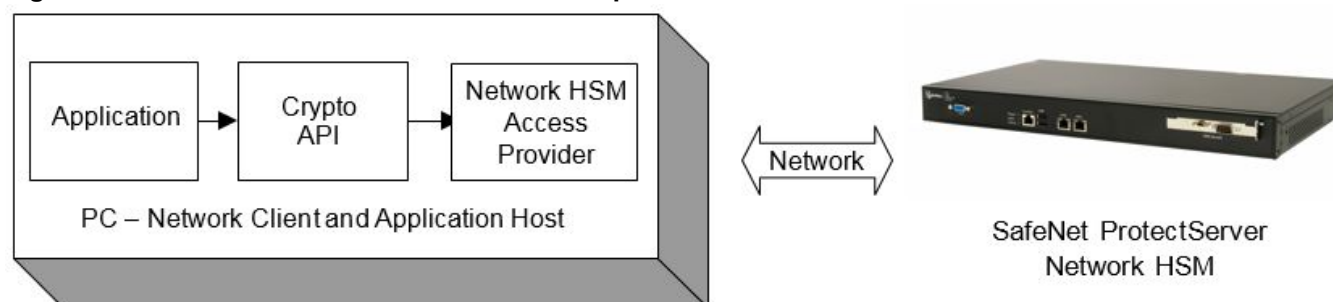
- One or more hardware security modules (HSMs) for key processing and storage.
- High-level cryptographic API software. This software uses the HSM's cryptographic capabilities to provide security services to applications.
- Access provider software to allow communication between the API software and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

Operating in network mode, a standalone SafeNet ProtectServer Network HSM can provide key processing and storage.

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

The figure below depicts a cryptographic service provider using the SafeNet ProtectServer Network HSM in network mode.

**Figure 1: SafeNet ProtectServer Network HSM implementation**



## Summary of Cryptographic Service Provider setup

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

1. **Install the SafeNet ProtectServer Network HSM** (See ["Hardware Installation" on page 14](#)).
2. **Check that the SafeNet ProtectServer Network HSM is operating correctly** (see ["Testing and Configuration" on page 16](#)).
3. **Configure the SafeNet ProtectServer Network HSM network settings** (see ["Testing and Configuration" on page 16](#)).
4. **Install and configure the Network HSM Access Provider software** (see the *SafeNet HSM Access Provider Installation Guide*).
5. **Install the high-level cryptographic API software.**

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

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

6. **Configure the high-level cryptographic API to allow preferred operating modes.** Some of these tasks may include:

- establishing a trusted channel or secure messaging system (SMS) between the API and the Safenet ProtectServer Network HSM.
- establishing communication between the network client and the Safenet ProtectServer Network HSM.

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

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

# Hardware Installation

This chapter describes how to install the SafeNet ProtectServer Network HSM.

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

After installation, confirm that the unit is operating correctly and configure the network settings. These steps are covered in ["Testing and Configuration" on page 16](#).

## 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.



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

---

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



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

---

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

## Smart Card Reader Installation

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

The SafeNet ProtectServer Network HSM supports two different card readers:

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

## 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, connect it to the HSM USB port with the included USB-to-serial cable.

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

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

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



Next, see ["Testing and Configuration" on page 16](#).

# Testing and Configuration

This chapter provides a step-by-step overview of how to confirm correct operation of the Safenet ProtectServer Network HSM, and configure its network settings. These instructions assume that the installation process covered in ["Hardware Installation" on page 14](#) is complete, and that the user is experienced in configuring Unix/Linux operating systems.

This chapter contains the following sections:

- ["Step 1: Access the Console" below](#)
- ["Step 2: Power on and Log in" on the next page](#)
- ["Step 3: Run System Test" on page 18](#)
- ["Step 4: Network Configuration" on page 18](#)
- ["Step 5: SSH Network Access" on page 21](#)
- ["Powering off the SafeNet ProtectServer Network HSM" on page 21](#)
- ["Upgrading the SafeNet ProtectServer Network HSM" on page 21](#)
- ["Troubleshooting" on page 22](#)

## Step 1: Access the Console

---

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

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



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

---



**Figure 1: Serial cable: RJ45 to DB9**

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

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

## Step 2: Power on and Log in

Power on the SafeNet ProtectServer Network HSM and the monitor (if applicable). A green LED on the front of the device will illuminate and the startup messages will be displayed on the monitor.

Power-up is complete when the SafeNet ProtectServer Network HSM login prompt appears:

```
Protect Server External 5.3.0
PSe-II login:
```

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 23](#).
- If you log in as **root**, you can manually configure the network settings using standard Linux commands.

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

User name	Default password
<b>root</b>	<b>password</b>
<b>admin</b>	<b>password</b>
<b>pseoperator</b>	<b>password</b>



**CAUTION:** We *strongly* recommend that you 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 Gemalto and have it re-imaged, which is not a warranty service.

## Step 3: Run System Test

Before field testing and deployment, run the diagnostic utility.

### hsmstate

As **root**, type **hsmstate** at a command line prompt. If the unit is functioning correctly, a message is returned that includes the following:

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

### PSE\_status

As **root**, you can also use the **PSE\_status** command to verify that the HSM is functioning correctly.

This command displays the current status of the SafeNet ProtectServer Network HSM and the status and process ID (pid) of the **etnetserver** process. If the unit is functioning correctly, a message is returned that includes the following:

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

```
PSE status NORMAL
```

### psesh:> hsm state

If you logged in as **admin** or **pseoperator**, use the command **hsm state** to display the current status.

```
psesh:>hsm state
```

```
HSM device 0:  HSM in NORMAL MODE. RESPONDING to requests. Usage Level=0%
State = (0x8000, 0xffffffff)
Host Interface  = PSIE2
```

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

You can also use the PSESH command **status** to check all the HSM's processes. For more information, see ["PSESH Command Reference" on page 23](#) and ["status" on page 49](#).

## Step 4: Network Configuration

IPv4 and IPv6 network addressing are supported. IPv4 addressing can be configured manually (as **root**) as described below, or by using PSESH (as **admin** or **pseoperator**) as described in ["PSESH Command Reference" on page 23](#). IPv6 addressing must be configured manually by logging in as **root** and using standard Linux commands.

## Setting the IP address

### With PSESH (recommended)


It is recommended that you use **psesh:> network interface** to configure the IPv4 address, instead of the manual procedure below. See ["network interface" on page 33](#) for command syntax.

### Manually

The SafeNet ProtectServer Network HSM is equipped with two NICs (eth0 and eth1). Dual-stack support allows you to configure the interfaces with both an IPv4 and IPv6 address. Refer to the Linux documentation for the commands required to set the IPv6 address.

The IP address for each NIC is specified in these files:

NIC	Configuration file
eth0	<code>/etc/sysconfig/network-scripts/ifcfg-eth0</code>
eth1	<code>/etc/sysconfig/network-scripts/ifcfg-eth1</code>

 **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 the IP address and network mask for each NIC. You must configure at least one of the NICs. The second needs to be configured only if you want to use it.

## Setting the hostname and default gateway

### With PSESH (recommended)

It is recommended that you use **psesh:> network interface dhcp** or **psesh:> network interface static** to set the hostname and gateway, instead of using the manual procedure below. See ["network interface dhcp" on page 35](#) and ["network interface static" on page 36](#) for command syntax.

### Manually

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

### With PSESH (recommended)

It is recommended that you use **psesh:> network dns** to set the name server, instead of using the manual procedure below. See ["network dns" on page 32](#) for command syntax.

### Manually

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

### With PSESH (recommended)

It is recommended that you use **psesh:>network iptables** to configure the iptables instead of using the manual procedure below. See ["network iptables" on page 37](#) for command syntax.

### Manually

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**

## Restarting networking

After making any change to the networking configuration, reboot the SafeNet ProtectServer Network HSM. As **admin** or **pseoperator**, enter the PSESH command **sysconf appliance reboot**.

As **root**, enter the following Linux command to restart networking:

**/etc/init.d/networking restart**

## Step 5: 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 need an SSH client such as **puTTY** (available for free from [www.putty.org](http://www.putty.org)).



**Note:** You cannot log in as **root** when accessing the SafeNet ProtectServer Network HSM over an SSH connection. After three failed remote login attempts, the account will be locked out for 10 minutes.

## 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.

### To upgrade the HSM:

1. Select and download the desired SafeNet ProtectServer Network HSM image upgrade file from the SafeNet Web

site at <https://safenet.gemalto.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.



**Note:** 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.



**Note:** 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, 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

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

# 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.

The commands are presented alphabetically 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
<a href="#">exit</a>	Exit the PSESH shell. See " <a href="#">exit</a> " on page 26.
<a href="#">files</a>	Manage the files that have been transferred to the appliance's SCP directory. See " <a href="#">files</a> " on page 27.
<a href="#">help</a>	Display syntax help for the specified command. You can use the <b>?</b> symbol instead of the string <b>help</b> as an alternative way of displaying the help. See " <a href="#">help</a> " on page 28.
<a href="#">hsm</a>	Display the current state of the HSM, or reset the HSM if it becomes unresponsive. See " <a href="#">hsm</a> " on page 29
<a href="#">network</a>	View or configure the network settings for the SafeNet ProtectServer Network HSM appliance. See " <a href="#">network</a> " on page 30.
<a href="#">package</a>	Manage the software packages installed on the appliance. See " <a href="#">package</a> " on page 46.
<a href="#">service</a>	Manage the services on the appliance. See " <a href="#">service</a> " on page 47.
<a href="#">status</a>	Display the current status of the appliance. See " <a href="#">status</a> " on page 49.
<a href="#">sysconf</a>	Configure the appliance time, date, or SNMP settings, or reboot or power-off the appliance. See " <a href="#">sysconf</a> " on page 53.
<a href="#">syslog</a>	Display or archive the syslog. See " <a href="#">syslog</a> " on page 59
<a href="#">user</a>	Set or change the password of the current user. See " <a href="#">user password</a> " on page 72.

## 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
<b>pseoperator</b>	<p>The <b>pseoperator</b> user is responsible for configuring the appliance for client access.</p> <p>The <b>pseoperator</b> 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.</p>
<b>admin</b>	<p>The <b>admin</b> user is responsible for managing the appliance.</p> <p>The <b>admin</b> user is able to execute all of the PSESH commands available to the <b>pseoperator</b>, 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 <b>pseoperator</b> user.</p>

## 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 <b>help</b> , <b>hel</b> , <b>he</b> , but not just <b>h</b> (because there is also an <b>hsm</b> command and typing just " <b>h</b> " is not sufficient to indicate whether you want <b>help</b> or <b>hsm</b> ).
Command completion	You can use the TAB key to automatically complete partially typed 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 <b>help</b> <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:>
```



**Note:** After three failed remote login attempts, the account will be locked out for 10 minutes.

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

## 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
<b>clear</b>	<b>c</b>	Delete all of the files in the appliance's SCP directory.
<b>delfile</b> <filename>	<b>d</b>	Delete the specified file from the appliance's SCP directory.
<b>show</b>	<b>s</b>	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 PTKpcihsM6-5.2.0-4.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 **?** 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**]

Option	Shortcut	Description
<b>reset</b>	<b>r</b>	Reset the HSM if it has stopped responding, but your computer is still responsive. This command closes out any login status and open sessions.
<b>state</b>	<b>s</b>	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)
```

```
[PSe-II] psesh:>hsm reset
```

```
Executing this command will disrupt all client connections. Proceed [y/n]?
> y
Proceeding to reset....
HSM reset successful.
```

```
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
  interface
  iptables
  route
```

Option	Shortcut	Description
<a href="#">dns</a>	<b>dn</b>	Add or delete DNS name servers and domains. See " <a href="#">network dns</a> " on page 32.
<a href="#">interface</a>	<b>in</b>	Configure the appliance network interfaces. See " <a href="#">network interface</a> " on page 33.
<a href="#">iptables</a>	<b>ip</b>	Configure the iptables firewall for the appliance. You can use this command to configure the iptables ACCEPT and DROP rules. See " <a href="#">network iptables</a> " on page 37.
<a href="#">route</a>	<b>r</b>	Manually configure routes on the SafeNet ProtectServer Network HSM appliance. See " <a href="#">network route</a> " on page 41.

```
network [domain <domain> | hostname <hostname> | ping <hostname_or_IP> | show]
```

Parameter	Shortcut	Description
<b>domain</b> <domain>	<b>do</b>	Set the domain for the appliance. Enter this keyword followed by the domain name.
<b>hostname</b> <hostname>	<b>h</b>	Set the hostname for the appliance.
<b>ping</b> <hostname_or_IP>	<b>p</b>	Test connectivity from the appliance to the specified hostname or IP address.
<b>show</b>	<b>s</b>	Display the current network configuration.

### Example

```
psesh:>network domain hmsdomain
Success: DomainName hmsdomain set.
Command Result : 0 (Success)
```

```
psesh:>network hostname hsmhost
Success: Hostname hsmhost set.
```

Command Result : 0 (Success)

psesh:>**network show**

```

Hostname:          "hsmhost"
Domain:           "hsmdomain"

IP Address (eth0): 172.20.11.40
HW Address (eth0): 00:01:4E:02:D1:59
Mask (eth0):       255.255.255.0
Gateway (eth0):    <not set>

Name Servers:      172.20.10.20      172.16.2.14
Search Domain(s):  <not set>

```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.20.11.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
169.254.0.0	0.0.0.0	255.255.0.0	U	1002	0	0	eth0
0.0.0.0	172.20.11.10	0.0.0.0	UG	0	0	0	eth0

Link status

```

eth0: Configured
      Link detected: yes

```

```

eth1: Not configured

```

Command Result : 0 (Success)

psesh:>**network ping 10.124.0.65**

```

PING 10.124.0.65 (10.124.0.65) 56(84) bytes of data.
64 bytes from 10.124.0.65: icmp_seq=1 ttl=126 time=18.5 ms

```

--- 10.124.0.65 ping statistics ---

```

1 packets transmitted, 1 received, 0% packet loss, time 18ms
rtt min/avg/max/mdev = 18.534/18.534/18.534/0.000 ms

```

Command Result : 0 (Success)

## 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.

### User Access

admin, pseoperator

### Syntax

**network dns**

```
add {nameserver <IPAddress> | searchdomain <netdomain>}
delete {nameserver <IPAddress> | searchdomain <netdomain>}
```

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

### User Access

admin, pseoperator

### Syntax

```
network interface
  dhcp
  delete
  static
```

Option	Shortcut	Description
<code>delete</code>	<code>del</code>	Delete the network configuration for a network interface (eth0 or eth1). See <a href="#">"network interface delete" on the next page</a>
<code>dhcp</code>	<code>dh</code>	Set a network interface with a DHCP IP configuration. See <a href="#">"network interface dhcp" on page 35</a> .
<code>static</code>	<code>s</code>	Sets a network interface with a static IP configuration. See <a href="#">"network interface static" on page 36</a> .

## network interface delete

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

### User Access

admin, pseoperator

### Syntax

**network interface delete -device <netdevice>**

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

### Example

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

Interface eth1 removed successfully.

Command Result : 0 (Success)

## network interface dhcp

Configure the network interface to request a dynamic IP address.



**Note:** DHCP is not recommended.

### User Access

admin, pseoperator

### Syntax

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

Parameter	Shortcut	Description
<b>-device</b> <netdevice>	<b>-d</b>	Specifies the interface you want to configure to use DHCP. <b>Valid values:</b> eth0, eth1
<b>-force</b>	<b>-f</b>	Force the action without prompting for confirmation.

### Example

```
psesh:>network interface dhcp -device eth0
```

NOTICE: The network service must be restarted for new network settings to take effect.  
If you are sure that you wish to restart the network, then type 'proceed', otherwise type 'quit'

```
> proceed
Proceeding...
e1000e: eth0 NIC Link is Down
Restarting network service...
Shutting down loopback interface:                [ OK ]
Bringing up loopback interface:                    [ OK ]
Bringing up interface eth0:
Determining IP information for eth0...ADDRCONF(NETDEV_UP): eth0: link is not ready
e1000e: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
done.
```

```
[ OK ]
```

Command Result : 0 (Success)

## network interface static

Configure a static IP address on the specified network interface.

### User Access

admin, pseoperator

### Syntax

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

Parameter	Shortcut	Description
<b>-device</b> <netdevice>	<b>-d</b>	Specifies the interface you want to configure. <b>Valid values:</b> eth0, eth1
<b>-ip</b> <ipaddress>	<b>-i</b>	Specifies the IP address to assign to the specified device.
<b>-netmask</b> <ipaddress>	<b>-n</b>	Specifies the network mask, in IP address format, to assign to the specified device.
<b>-gateway</b> <ipaddress>	<b>-g</b>	Specifies the gateway to assign to the specified device.
<b>-force</b>	<b>-f</b>	Force the action without prompting.

### Example

```
psesh:>network interface static -device eth0 -ip 172.20.11.40 -netmask 255.255.255.0
```

NOTICE: The network service must be restarted for new network settings to take effect.  
If you are sure that you wish to restart the network, then type 'proceed', otherwise type 'quit'

```
> proceed
Proceeding...
e1000e: eth0 NIC Link is Down
Restarting network service...
Shutting down loopback interface:                [ OK ]
Bringing up loopback interface:                    [ OK ]
Bringing up interface eth0: ADDRCONF(NETDEV_UP): eth0: link is not ready
Determining if ip address 172.20.11.40 is already in use for device eth0...
                                                    [ OK ]
e1000e: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready

Command Result : 0 (Success)
```

## 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.

### User Access

admin, pseoperator

### Syntax

```
network iptables
  addrule
  clear
  delrule
  save
  show
```

Option	Shortcut	Description
<a href="#">addrule</a>	<b>a</b>	Add an ACCEPT or DROP rule to the iptables firewall for the appliance. See " <a href="#">network iptables addrule</a> " on page 39.
<b>clear</b>	<b>c</b>	Clear the iptables for the device. This returns the iptables to a factory default state.
<a href="#">delrule</a>	<b>d</b>	Deletes the specified "INPUT" chain rule in iptables. Run <b>network iptables show</b> to see the rule numbers. See " <a href="#">network iptables delrule</a> " on page 40
<b>save</b>	<b>sa</b>	Saves the iptables changes. You must execute this command or any changes will be discarded on the next appliance restart.
<b>show</b>	<b>sh</b>	Display the current iptables configuration.

### Example

```
psesh:>network iptables show
```

Current iptables rules:

```
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     all  --  172.20.11.105          anywhere
DROP       all  --  172.20.11.105          anywhere
DROP       all  --  172-0-11-0.lightspeed.wlfrct.sbcglobal.net/255.0.255.0  anywhere
```

Command Result : 0 (Success)

```
psesh:>network iptables clear
```

```
WARNING: This will delete all configured rules and reset iptables to factory default. Proceed [y/n]?
```

```
> y
```

```
Proceeding....
```

```
clearing iptables...
```

```
Restarting network service...please wait
```

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

```
psesh:>network iptables save
```

```
WARNING: This will save all the iptables changes and restart the network services. Proceed[y/n]?
```

```
>
```

```
Exiting....
```

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

## 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.

### User Access

admin, pseoperator

### Syntax

**network iptables addrule**

```
accept {host -ip <ip_address> | network -net <ip_address> -mask <network_mask>}
drop {host -ip <ip_address> | network -net <ip_address> -mask <network_mask>}
```

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

### Example

```
psesh:>network iptables addrule accept host -ip 172.20.11.105
ACCEPT rule added for host 172.20.11.105
Command Result : 0 (Success)
```

```
psesh:>network iptables addrule drop network -net 172.20.11.212 -mask 255.0.255.0
DROP rule added for 172.20.11.212/255.0.255.0 network
Command Result : 0 (Success)
```

## network iptables delrule

Deletes the specified "INPUT" chain rule in iptables. Run network iptables show to see the rule order.

### User Access

admin, pseoperator

### Syntax

```
network iptables delrule -rulenum <number>
```

Parameter	Shortcut	Description
<b>-rulenum</b> <number>	<b>-r</b>	The number of the rule to be deleted.

### Example

```
psesh:>network iptables delrule -rulenum 2
```

```
iptables: Rule 2 deleted.
```

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



## network route

Manage and view network route configurations.

### User Access

admin, pseoperator

### Syntax

```
network route
  add
  clear
  delete
  show
```

Option	Shortcut	Description
<a href="#">add</a>	<b>a</b>	Adds a manually configured network route. See " <a href="#">network route add</a> " on the next page. <b>Note:</b> This command should only be used on the advice of a network administrator.
<a href="#">clear</a>	<b>s</b>	Deletes all manually configured network routes. See " <a href="#">network route clear</a> " on page 43. <b>Note:</b> This command should only be used on the advice of a network administrator.
<a href="#">delete</a>	<b>d</b>	Deletes one manually configured network route. See " <a href="#">network route delete</a> " on page 44. <b>Note:</b> This command should only be used on the advice of a network administrator.
<a href="#">show</a>	<b>c</b>	Shows the current network route configuration. See " <a href="#">network route show</a> " on page 45.

## network route add

Manually add a network route to the appliance's routing tables.



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

### User Access

admin, pseoperator

### 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. <b>Valid values:</b> host, network
<IPAddress>		Specifies the IP address of the route you want to add.
-device <interface>	-d	Specifies the interface you want to configure. <b>Valid values:</b> eth0, eth1
-metric <metric>	-m	Specifies the routing metric for the route. <b>Range:</b> 0-65535
-netmask <IPAddress>	-n	Specifies the network mask for the route, in IP address format.
-gateway <IPAddress>	-g	Specifies the IP address of the gateway for the route.
-force	-f	Force the action without prompting.

## network route clear

Delete all manually-configured network routes from the appliance's routing tables.



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

### User Access

admin, pseoperator

### Syntax

**network route clear**

### Example

```
psesh:>network route clear
```

WARNING !! This command deletes all manually configured routes and restarts the network service.

If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

```
>proceed
Proceeding...
Restarting network service...
ip_tables: (C) 200-2006 Netfilter Core Team
Shutting down interface eth0: e1000e: eth0 NIC Link is Down
[ OK ]
Shutting down loopback interface: [ OK ]
Bringing up loopback interface: [ OK ]
Bringing up interface eth0
Determining IP information for eth0...ADDRCONF(NETDEV_UP): eth0: link is not ready
e1000e: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
done.
[ OK ]

ip_tables: (C) 200-2006 Netfilter Core Team
Routing table successfully updated.
```

Command Result : 0 (Success)

## network route delete

Delete a manually-configured network route from the appliance's routing tables.



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

### User Access

admin, pseoperator

### Syntax

```
network route delete <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 delete. <b>Valid values:</b> host, network
<ip_address>		Specifies the IP address of the route you want to delete.
-device <interface>	-d	Specifies the interface you want to configure. <b>Valid values:</b> eth0, eth1
-metric <metric>	-m	Specifies the routing metric for the route. <b>Range:</b> 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.

## network route show

Shows the current network route configuration.

### User Access

admin, pseoperator

### Syntax

**network route show**

### Example

psesh:>**network route show**

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.20.11.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
169.254.0.0	0.0.0.0	255.255.0.0	U	1002	0	0	eth0
0.0.0.0	172.20.11.10	0.0.0.0	UG	0	0	0	eth0

Command Result : 0 (Success)

# package

Manage the software packages installed on the appliance.

## User access

admin

## Syntax

```
package
  list {all | ptk}
  update -file <packagefile>
```

Parameter	Shortcut	Description
<b>list</b> [all   ptk]	<b>l</b> {a   p}	List the packages currently installed on the appliance. Use the <b>all</b> flag to list all packages. Use the <b>ptk</b> flag to list the SafeNet ProtectToolkit packages only.
<b>update -file</b> <packagefile>	<b>u -f</b>	Update the specified package file. Before you can update a package, you must use <b>scp/pscp</b> to securely copy the update package file to the appliance's SCP directory.

## Example

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

```
filesystem-2.4.30-3.el6.i686
ncurses-base-5.7-3.20090208.el6.i686
kbd-misc-1.15-11.el6.noarch
```

```
...
```

```
pciutils-3.1.10-4.el6.i686
audit-2.3.7-5.el6.i686
e2fsprogs-1.41.12-21.el6.i686
acl-2.2.49-6.el6.i686
PTKpcihsmK6-5.2.0-5.i386
PTKnetsrv-5.2.0-5.i386
```

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

```
psesh:>package list ptk
```

```
PTKpcihsmK6-5.2.0-5.i386
PTKnetsrv-5.2.0-5.i386
```

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

## 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
<b>list</b>	<b>l</b>	List the services you can manage on the appliance.
<b>restart</b> <service>	<b>r</b>	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. <b>Valid values:</b> network, etnetserver, iptables, snmp, ssh, syslog
<b>start</b> <service>	<b>star</b>	Start the specified service. <b>Valid values:</b> network, etnetserver, iptables, snmp, ssh, syslog
<b>status</b> <service>	<b>stat</b>	Display the status (stopped, running) of the specified service. <b>Valid values:</b> network, etnetserver, iptables, snmp, ssh, syslog
<b>stop</b> <service>	<b>sto</b>	Stop the specified service.. <b>Valid values:</b> 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**

Shutting down system logger: [ OK ]

Command Result : 0 (Success)

psesh:>service **restart syslog**

Shutting down system logger: [ OK ]

Starting system logger: [ OK ]

Command Result : 0 (Success)

psesh:>service **status ssh**

ssh is running

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 ]

Determining IP information for eth0... done. [ OK ]

Determining IP information for eth1... done. [ OK ]

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
```

Option	Shortcut	Description
cpu	c	Display the current CPU load. The CPU load data is presented as a series of five entries, as follows: <ol style="list-style-type: none"> <li>1. The average CPU load for the previous minute. This value is 0.14 in the example below.</li> <li>2. The average CPU load for the previous five minutes. This value is 0.10 in the example below.</li> <li>3. The average CPU load for the previous ten minutes. This value is 0.08 in the example below.</li> <li>4. The number of currently running processes and the total number of processes. The example below shows 1 of 68 processes running.</li> <li>5. The last process ID used. This value is 11162 in the example below.</li> </ol>
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.

Option	Shortcut	Description
<b>time</b>	<b>t</b>	Display the time currently configured on the appliance, using the 24 hour clock.
<b>zone</b>	<b>z</b>	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 Fri Aug 5 07:26:15 EDT 2016, I am up 2:29

Command Result : 0 (Success)

psesh:>**status date**

Fri Aug 5 07:29:04 EDT 2016

Command Result : 0 (Success)

psesh:>**status disk**

```
===== Hard Disk utilization =====
Filesystem      1K-blocks   Used Available Use% Mounted on
/dev/sda2        3681872 696168   2795344   20% /
/dev/sda1        194241  20086   163915   11% /boot
```

Command Result : 0 (Success)

psesh:>**status interface**

```
eth0      Link encap:Ethernet HWaddr 00:01:4E:02:D1:59
          inet addr:172.20.11.40 Bcast:172.20.11.255 Mask:255.255.255.0
          inet6 addr: fe80::201:4eff:fe02:d159/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:20849 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2183 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2034969 (1.9 MiB) TX bytes:291093 (284.2 KiB)
          Interrupt:16 Memory:fe9a0000-fe9c0000

eth1      Link encap:Ethernet HWaddr 00:01:4E:02:D1:5A
          BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
          Interrupt:17 Memory:feaa0000-feac0000
```

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

Command Result : 0 (Success)

psesh:>**status mac**

```
eth0 00:01:4E:02:D1:59
```

Command Result : 0 (Success)

psesh:>**status mem**

	total	used	free	shared	buffers	cached
Mem:	1019668	127360	892308	164	6928	67688
-/+ buffers/cache:		52744	966924			
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	172.20.11.40:22	10.124.0.34:52153	ESTABLISHED
tcp	0	0	:::12396	:::*	LISTEN
udp	0	0	0.0.0.0:68	0.0.0.0:*	

Active UNIX domain sockets (servers and established)

Proto	RefCnt	Flags	Type	State	I-Node	Path
unix	2	[ ACC ]	STREAM	LISTENING	8394	@/com/ubuntu/upstart
unix	2	[ ]	DGRAM		8828	@/org/kernel/udev/udev
unix	4	[ ]	DGRAM		12263	/dev/log
unix	2	[ ]	DGRAM		12661	
unix	2	[ ]	DGRAM		12266	
unix	2	[ ]	DGRAM		12109	
unix	2	[ ]	DGRAM		12055	
unix	2	[ ]	DGRAM		10517	
unix	3	[ ]	DGRAM		8845	
unix	3	[ ]	DGRAM		8844	

Command Result : 0 (Success)

psesh:>**status time**

```
07:31:41
```

Command Result : 0 (Success)

```
psesh:>status zone
```

```
EDT
```

```
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
```

Option	Shortcut	Description
<a href="#">appliance</a>	<b>a</b>	Reboot or power-off the appliance. See " <a href="#">sysconf appliance</a> " on the <a href="#">next page</a> .
<a href="#">snmp</a>	<b>s</b>	Configure the SNMP settings on the appliance. See " <a href="#">sysconf snmp</a> " on <a href="#">page 55</a> .
<b>time</b>	<b>t</b>	Set the appliance time and date.
<a href="#">timezone</a>	<b>timez</b>	Display or set the appliance timezone. See " <a href="#">sysconf timezone</a> " on <a href="#">page 58</a> .

## sysconf appliance

Reboot or power-off the appliance.

### User Access

admin, pseoperator

### Syntax

**sysconf appliance** {poweroff | reboot}

Option	Shortcut	Description
<b>poweroff</b>	<b>p</b>	Power-off the appliance.
<b>reboot</b>	<b>r</b>	Reboot the appliance.

### Example

```
psesh:>sysconf appliance poweroff
```

```
WARNING !! This command will power off the appliance.
           All clients will be disconnected and the appliance will require a manual power on
           for further access.
```

```
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'
```

```
> proceed
Proceeding...
```

```
Broadcast message from root@PSE-II
(/dev/pts/0) at 7:58 ...
```

```
The system is going down for power off NOW!
Power off commencing
```

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

```
psesh:>sysconf appliance reboot
```

```
WARNING !! This command will reboot the appliance.
           All clients will be disconnected.
```

```
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'
```

```
> proceed
Proceeding...
```

```
Broadcast message from root@PSE-II
(/dev/pts/0) at 7:55 ...
```

```
The system is going down for reboot NOW!
Reboot commencing
```

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

## 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**}

Option	Shortcut	Description
<b>config</b>	<b>c</b>	Configure the SNMP settings for the appliance. See " <a href="#">sysconf snmp config</a> " on page 57.
<b>disable</b>	<b>d</b>	Disable SNMP on the appliance and stop the SNMP service.
<b>enable</b>	<b>e</b>	Enable SNMP on the appliance and start the SNMP service.
<b>show</b>	<b>s</b>	Display the current SNMP settings for the appliance.

### Example

```
psesh:>sysconf snmp disable
```

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

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

```
psesh:>sysconf snmp enable
```

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

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

```
psesh:>sysconf snmp show
```

```
SNMP is running
```

```
SNMP is enabled
```

```
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
<b>-community</b> <string>	<b>-com</b>	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.
<b>-contact</b> <string>	<b>-con</b>	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.
<b>-ip</b> <IPaddress>	<b>-i</b>	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.
<b>-location</b> <string>	<b>-l</b>	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.

### User Access

admin, pseoperator

### Syntax

```
sysconf timezone {set <timezone> | show}
```

Parameter	Shortcut	Description
<b>set</b> <timezone>	<b>se</b>	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 <b>/usr/share/zoneinfo</b> directory on any Redhat distribution.
<b>show</b>	<b>sh</b>	Display the currently configured time zone.

### Example

```
psesh:>sysconf timezone set Canada/Eastern
```

```
Timezone set to Canada/Eastern
Command Result : 0 (Success)
```

```
psesh:>sysconf timezone show
```

```
EDT
```

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

# syslog

Manage system logs, and configure automatic log-keeping behavior.

## User access

admin, pseoperator

## Syntax

```
syslog
  export
  period
  remotehost
  rotate
  rotations
  show
  tail
  tarlogs
```

Option	Shortcut	Description
<a href="#">export</a>	<b>e</b>	Export syslog to file for transfer from appliance. See <a href="#">"syslog export" on the next page</a> .
<a href="#">period</a>	<b>p</b>	Sets the time between syslog rotations. See <a href="#">"syslog period" on page 61</a> .
<a href="#">remotehost</a>	<b>re</b>	Configures syslog to send logs to remote hosts. See <a href="#">"syslog remotehost" on page 62</a> .
<a href="#">rotate</a>	<b>rotate</b>	Rotates log files immediately, if they have not already been rotated on the same date. Logs cannot be rotated more than once per day. See <a href="#">"syslog rotate" on page 67</a> .
<a href="#">rotations</a>	<b>rotati</b>	Sets the number of old syslogs that are kept. See <a href="#">"syslog rotations" on page 68</a> .
<a href="#">show</a>	<b>s</b>	Display the current log rotation configuration and the configured log levels. See <a href="#">"syslog show" on page 69</a> .
<a href="#">tail</a>	<b>tai</b>	Display the last entries of the specified syslog. See <a href="#">"syslog tail" on page 70</a> .
<a href="#">tarlogs</a>	<b>tar</b>	Create an archive of the syslog. See <a href="#">"syslog tarlogs" on page 71</a> .

## syslog export

---

Prepare system logs for transfer from appliance. This command copies the current system log file to the export directory so that the user can use scp to transfer the file to another computer. Can be used for offline storage of old log files or to send to Technical Support for troubleshooting the SafeNet appliance.

### Syntax

**syslog export**

### Example

```
psesh:>syslog export
```

System log files successfully prepared for secure transfer.  
Use scp from a client machine to get the file named: "syslog"

Command Result : 0 (Success)

## syslog period

Set the time between syslog rotations.

### Syntax

**syslog period** <syslogperiod>

Parameter	Shortcut	Description
<syslogperiod>		Specifies the log rotation period. <b>Valid values:</b> daily, weekly, monthly

### Example

```
psesh:>syslog period daily
```

Log period set to daily.

Command Result : 0 (Success)

## syslog remotehost

Access the **syslog remotehost** commands to manage the syslog remote hosts.

### Syntax

```
syslog remotehost
  add
  clear
  delete
  list
```

Option	Shortcut	Description
<a href="#">add</a>	<b>a</b>	Add a remote host. See " <a href="#">syslog remotehost add</a> " on the next page.
<a href="#">clear</a>	<b>c</b>	Delete All Remote Logging Servers. See " <a href="#">syslog remotehost clear</a> " on page 64.
<a href="#">delete</a>	<b>d</b>	Delete a remote host. See " <a href="#">syslog remotehost delete</a> " on page 65.
<a href="#">list</a>	<b>l</b>	List all syslog remote hosts. See " <a href="#">syslog remotehost list</a> " on page 66.

## syslog remotehost add

Add a remote host receiving the logs. Can be any system that provides the remote syslog service.



**Note:** For this function to work you must open receiving udp port 514 on the remote log server.

### Syntax

**syslog remotehost add** <hostname\_or\_IP\_address>

Parameter	Shortcut	Description
<hostname_or_IP_address>		Specifies the hostname or the IP address of the remote computer system that will be accepting and storing the syslogs.

### Example

```
psesh:>syslog remotehost add mylinuxbox
```

```
mylinuxbox added successfully
```

```
Please restart syslog with <service restart syslog> command
```

```
Make sure syslog service is started on mylinuxbox with -r option
```

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

## syslog remotehost clear

Delete all remote logging servers.

### Syntax

```
syslog remotehost clear [-force]
```

Parameter	Shortcut	Description
<code>-force</code>	<code>-f</code>	Force the action; useful for scripting.

### Example

```
psesh:>syslog remotehost clear
```

```
All remote hosts receiving the logs will be deleted.
Are you sure you wish to continue?
```

```
Type proceed to continue, or quit to quit now -> proceed
```

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

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



## syslog remotehost delete

Delete a remote host receiving the logs. Use **syslog remotehost list** to see which systems are receiving the logs.

### Syntax

```
syslog remotehost delete <hostname_or_IP_address>
```

Parameter	Shortcut	Description
<hostname_or_IP_address>		Specifies the hostname or the IP address of the remote computer system to delete from the list.

### Example

```
pshesh:>syslog remotehost delete mylinuxbox
```

```
mylinuxbox deleted successfully
```

```
Please restart syslog with <service restart syslog> command  
to stop logs to be sent to mylinuxbox
```

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

## syslog remotehost list

---

List the syslog remote hosts.

### Syntax

```
syslog remotehost list
```

### Example

```
psesh:>syslog remotehost list
```

```
List of syslog remote hosts:  
mylinuxbox
```

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

## syslog rotate

---

Rotate log files immediately, if they have not already been rotated on the same date. Logs cannot be rotated more than once per day.



**Note:** Using this command followed by "sysconf cleanup logs" causes all grow-able log files to be deleted.

---

EXCEPTION: The syslog rotate command does not rotate the NTP log file nor the hsm.log file. The HSM log is a small log file that provides critical information about the HSM. It does not grow very much throughout the life of the HSM.

### Syntax

```
syslog rotate
```

### Example

```
lunash:>syslog rotate
```

Command Result : 0 (Success)

## syslog rotations

Set the number of history files to keep when rotating system log files. For example, two rotations would keep the current log files and the most recent set; three rotations would keep the current log files and the two most recent sets. Specify a whole number less than 100.

### Syntax

**syslog rotations** <syslog\_rotations>

Parameter	Shortcut	Description
<syslog_rotations>		An integer that specifies the number of history files to keep when rotating system log files. <b>Range:</b> 1 to 100

### Example

```
psesh:> syslog rotations 5
```

```
Log rotations set to 5
```

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

## syslog show

Display the current log rotation configuration, and show the configured log levels. Optionally show a list of the log files.

### Syntax

**syslog show** [-files]

Parameter	Shortcut	Description
<b>-files</b>	<b>-f</b>	Binary option. If this option is present, a list of all log files is presented. If this option is absent, then a summary of log configuration is shown, without the file list.

### Example

```
psesh:>syslog show -files
```

Syslog configuration

```
Rotations:          4
Rotation Period:    weekly
```

Configured Log Levels:

```
-----
syslog:
cron:      *                               /var/log/cron
boot:      *                               /var/log/boot
```

Note: '\*' means all log levels.

```
LogFileName          Size Date Time
-----
anaconda.ifcfg.log    4550 Aug 5 09:49
anaconda.log          20753 Aug 5 09:49
anaconda.program.log  38069 Aug 5 09:49
anaconda.storage.log 102111 Aug 5 09:49
anaconda.syslog       78833 Aug 5 09:49
anaconda.yum.log      25369 Aug 5 09:49
audit                 4096 Aug 5 09:53
boot.log              1870 Aug 5 10:44
btmp                  768 Aug 5 09:54
cron                  1445 Aug 5 10:50
dmesg                 44346 Aug 5 09:52
dracut.log            149964 Aug 5 09:49
lastlog               146000 Aug 5 10:36
maillog               191 Aug 5 09:53
messages              59317 Aug 5 11:00
secure                2858 Aug 5 10:37
spooler                0 Aug 5 09:43
tallylog              0 Aug 5 09:42
wtmp                  11904 Aug 5 10:37
```

Command Result : 0 (Success)

## syslog tail

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

### User access

admin, pseoperator

### Syntax

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

Parameter	Shortcut	Description
<b>-entries</b> <logentries>	<b>-e</b>	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. <b>Range:</b> 0-2147483647
<b>-logname</b> <logname>	<b>-l</b>	Specifies the name of the log you want to display. Enter this keyword followed by the log name. <b>Valid values:</b> messages, secure
<b>-search</b> <string>	<b>-s</b>	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
```

```
Aug  5 12:00:17 PSe-II snmpd[3963]: Connection from UDP: [172.16.21.19]:62386->[172.20.11.150]
Aug  5 12:00:18 PSe-II snmpd[3963]: Connection from UDP: [172.16.21.19]:62386->[172.20.11.150]
Aug  5 12:04:16 PSe-II psesh [4341]: info : 0 : pssh user login : admin : 172.16.181.182/51177
Aug  5 12:04:28 PSe-II psesh [4341]: info : 0 : Command: help syslog : admin :
172.16.181.182/51177
Aug  5 12:06:36 PSe-II psesh [4341]: info : 0 : Command: help syslog tar : admin :
172.16.181.182/51177
Aug  5 12:07:32 PSe-II psesh [4341]: info : 0 : Command: syslog tail : admin :
172.16.181.182/51177
Aug  5 12:09:55 PSe-II psesh [4341]: info : 0 : Command: syslog tarlogs : admin :
172.16.181.182/51177
Aug  5 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
Aug  5 12:14:59 PSe-II psesh [4341]: info : 0 : Command: syslog tail -logname messages -entries
10 : admin : 172.16.181.182/51177
Aug  5 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)

## syslog tarlogs

---

Create an archive of the syslog.

### User access

admin, pseoperator

### Syntax

```
syslog tarlogs
```

### Example

```
psesh:>syslog tarlogs
```

```
Generating package list...
```

```
Generating tarlogs...
```

```
The tar file containing logs is now available via scp as filename 'pselogs.tgz'.
```

```
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)

```
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.

Command Result : 0 (Success)



# 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%

# APPENDIX B

## Glossary of terms

### 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"