THALES

SafeNet ProtectServer HSM 5.9

PSESH COMMAND REFERENCE GUIDE

Document Information

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

Revision History

Revision	Date	Reason
Rev. A	08 January 2020	Initial release

Trademarks, Copyrights, and Third-Party Software

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales's information.

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

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

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

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

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

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

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

CONTENTS

PREFACE: About the PSESH Command Reference Guide

This document describes how to access and use the PSESH command line interface. It contains the following chapters:

- "Using PSESH" on page 10
- "PSESH Commands" on page 13

This preface also includes the following information about this document:

- "Gemalto Rebranding" below
- "Audience" on the next page
- "Document Conventions" on the next page
- "Support Contacts" on page 9

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

Gemalto Rebranding

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

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

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

Audience

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

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

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

Document Conventions

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

Notes

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

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

Cautions

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

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

Warnings

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

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

Command Syntax and Typeface Conventions

Format	Convention
bold	The bold attribute is used to indicate the following: > Command-line commands and options (Type **dir /p**.) > Button names (Click **Save As**.) > Check box and radio button names (Select the **Print Duplex** check box.) > Dialog box titles (On the **Protect Document** dialog box, click **Yes**.) > Field names (**User Name:** Enter the name of the user.) > Menu names (On the **File** menu, click **Save**.) (Click **Menu > Go To > Folders**.) > User input (In the **Date** box, type **April 1**.)
italics	In type, the italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[**optional**] [<optional>]	Represent optional **keywords** or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.

{**a**|**b**|**c**}
{<a>|<b>|<c>}
	Represent required alternate **keywords** or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

[**a**|**b**|**c**] [<a>|<b>|<c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Support Contacts

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

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

Customer Support Portal

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

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

Telephone

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

CHAPTER 1: Using 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.

This chapter contains the following sections:

Users

The following users can access PSESH:

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

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.
Console history	You can scroll up to see the console history with SHIFT+PageUp.
Command shortcuts	You must type sufficient letters of a command or sub-command to make the input unique in the current syntax. For example, you could invoke system syntax help with **help**, **hel**, **he**, but not just **h** (because there is also an **hsm** command and typing just "**h**" is not sufficient to indicate whether you want **help** or **hsm**).
Command 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 **help** <command_name>, or **?** <command_name>.

Accessing PSESH

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

To access PSESH

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

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

   You can log in as **admin**, **pseoperator**, or **audit** (see "Users" on the previous page for details on these roles).

2. You are prompted for the password. If this is the first time you have signed in as this user, 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, includes the hostname you assigned to the appliance:

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

> **NOTE** After three failed SSH 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**.

Admin account lockout and recovery

As a security measure, the **admin** account is locked out after 10 consecutive failed login attempts using the console (serial port or keyboard and monitor). Further login attempts will produce a message like the following:

```
Your admin account is locked due to 11 failed logins.
You will need to tamper the HSM and reboot the system to reset the admin password.
```

> **CAUTION!** Tampering the HSM will destroy all tokens and stored objects. Back up any important cryptographic objects using the SafeNet ProtectToolkit client software before you proceed.

To recover the admin account

1. Tamper the HSM by turning the tamper lock key or pressing the tamper switch. See:
   - "Tamper lock" on page 1 in the *SafeNet ProtectServer Network HSM Installation and Configuration Guide*
   - "Rear panel view" on page 1 in the *SafeNet ProtectServer Network HSM Plus Installation and Configuration Guide*
2. Reboot the appliance using one of the following methods:
   - Log in to PSESH as **pseoperator** and run **sysconf appliance reboot**.
   - Hard reboot (SafeNet ProtectServer Network HSM): Press the recessed reset button on the appliance's front panel (see "Reset button" on page 1)
   - Hard reboot (SafeNet ProtectServer Network HSM Plus): Press the start/stop switch on the appliance's rear panel (see "Rear panel view" on page 1). Wait at least 15 seconds, and press the start/stop switch again to restart the system.

   After a successful reboot, the following message is displayed, followed by the login prompt:

   ```
   Protect Server External II v5.9.0

   Warning: This is a password recovery process.
            The HSM is tampered and rebooted after max password retry failures.
            The admin password is reset to factory default now.
            You are required to change the password at the first login.

   myPSE login:
   ```
3. Log in to the unlocked **admin** account using the default password ("**password**"). You are prompted to set a new password for the **admin** account.
4. Set a new **admin** password.
5. The password recovery process halts the SSH service on the appliance. Restart the SSH service with the following command:

   psesh:>**service restart ssh**

CHAPTER 2: PSESH Commands

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:

Argument(s)	Description
audit	Manage HSM auditing tasks. Only available to the **audit** user. See "audit" on the next page.
exit	Exit the PSESH shell. See "exit" on page 19.
files	Manage the files that have been transferred to the appliance's SCP directory. See "files" on page 20.
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. See "help" on page 21.
hsm	Display the current state of the HSM, or reset the HSM if it becomes unresponsive. See "hsm" on page 22.
network	View or configure the network settings for the SafeNet ProtectServer Network HSM appliance. See "network" on page 24.
package	Manage the software packages installed on the appliance. See "package" on page 47.
service	Manage the services on the appliance. See "service" on page 49.
status	Display the current status of the appliance. See "status" on page 51.
sysconf	Configure the appliance time, date, or SNMP settings, or reboot or power-off the appliance. See "sysconf" on page 55.
syslog	Display or archive the syslog. See "syslog" on page 64
user	Set or change the password of the current user. See "user password" on page 79.

audit

Manage HSM auditing tasks, including audit logging configuration, log rotation scheduling, and settings for the **audit** user role. This command and its subcommands are only available to the **audit** account on the appliance.

The **audit** appliance role also has access to the following commands common to the **admin** and **pseoperator** roles:

- "syslog tarlogs" on page 78
- "user password" on page 79

Syntax

audit

```
audit
log
service
```

Argument(s)	Shortcut	Description
audit	**a**	Manage **audit** user role settings. See "audit audit" on the next page.
log	**l**	Manage the appliance logging settings. See "audit log" on page 16.
service	**s**	Enable or disable the audit logging service. See "audit service" on page 18.

audit audit

Configure the **audit** user role.

Syntax

audit audit {**init** | **changepwd** | **secret**}

Argument(s)	Shortcut	Description
changepwd	**c**	Change the **audit** user password.
init	**i**	Initialize the **audit** user role.
secret	**s**	Generate the Audit secret key in the Admin token. You will be prompted to enter at least 3 parameters If an Audit key is already present, it will be deleted. You must restart the HSM to put the new key in service.

Examples

```
psesh:>audit audit init

Please Enter the SO PIN:
Please Enter the new Auditor's PIN:
Please re-enter the new Auditor's PIN:

Command Result : 0 (Success)


psesh:>audit audit secret

Please Enter the Auditor's PIN:
Please enter number of params (minimum 3): 3
Please enter parameter #0:12345678
Please enter parameter #1:87654321
Please enter parameter #2:01020304
Audit Key created successfully

Command Result : 0 (Success)


psesh:>audit audit changepwd

Please Enter the old Auditor's PIN:
Please Enter the new Auditor's PIN:
Please re-enter the new Auditor's PIN:

Command Result : 0 (Success)
```

audit log

Configure the appliance logging settings.

Syntax

audit log

clear
rotation
show

Argument(s)	Shortcut	Description
clear	**c**	Destroy all audit logs currently on the HSM, without first backing them up to the appliance directory. **CAUTION!** To back up the logs before deleting them, use **"syslog tarlogs" on page 78** instead.
rotation	**r**	Set the appliance logging rotation schedule. See "audit log rotation" on the next page.
show	**s**	Display the current appliance logging settings.

Example

```
psesh:>audit log show

Audit Logs Service is enabled.
Using Hourly rotation

Command Result : 0 (Success)


psesh:>audit log clear

   *** WARNING ***

        All audit logs for this HSM will be destroyed (without backup)!!!

        It is recommended to create a backup of audit logs first using "syslog tarlogs" command
        before destroying the logs!!!

        Are you sure you wish to continue?

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


Command Result : 0 (Success)
```

audit log rotation

Set the audit log rotation schedule. By default, the logs do not rotate.

Syntax

audit log rotation [**-hourly** | **-daily** | **-weekly**]

Argument(s)	Shortcut	Description
-daily	**-d**	Set a daily log rotation schedule.
-hourly	**-h**	Set an hourly log rotation schedule.
-weekly	**-w**	Set a weekly log rotation schedule.

Example

```
psesh:>audit log rotation -daily

Setting Daily rotation.

Command Result : 0 (Success)
```

audit service

Enable or disable the audit logging service.

Syntax

audit service {**enable** | **disable**}

Argument(s)	Shortcut	Description
enable	**e**	Enable the audit logging service.
disable	**d**	Disable the audit logging service.

Examples

```
psesh:>audit service enable

Audit Log is enabled
Starting audittrace:                                        [  OK   ]
Audit Log is started

Command Result : 0 (Success)
```

```
psesh:>audit service disable

Audit Log Service is disabled
Stopping audittrace:                                        [  OK   ]
Audit Log Service is stopped

Command Result : 0 (Success)
```

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** | **delete -file** <filename> | **show**]

Argument(s)	Shortcut	Description
clear	**c**	Delete all of the files in the appliance's SCP directory.
delete -file <filename>	**d**	Delete the specified file from the appliance's SCP directory.
show	**s**	List all of the files that currently reside in the appliance's SCP directory.

Example

```
psesh:> files show
SCP Folder Content
------------------
total 861K
248K PTKnetsrv-5.2.0-4.i386.rpm
613K PTKpcihsmK6-5.2.0-4.i386.rpm
Command Result : 0 (Success)


psesh:>files delete PTKnetsrv-5.2.0-4.i386.rpm
This will delete file 'PTKnetsrv-5.2.0-4.i386.rpm' in the scp folder. Continue [y/n]?
> y
Proceeding....
File 'PTKnetsrv-5.2.0-4.i386.rpm' deleted.
Command Result : 0 (Success)


psesh:>files clear
This will delete all the files in the scp folder. Continue [y/n]?
> y
Proceeding....
All files deleted.
Command Result : 0 (Success)
```

help

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

User access

admin, **pseoperator**

Syntax

help <command>

Example

```
psesh:>help help

Syntax:      help [<command>]

Type "help" or "?" (without the double quotation marks) to see help and syntax information for any
PSE 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                st         Shows HSM State
 reset                r          Reset HSM
 show                 sh         Show Characteristics of the HSM

Command Result : 0 (Success)
```

hsm

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

User access

admin, **pseoperator**

Syntax

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

Argument(s)	Shortcut	Description
reset	**r**	Reset the HSM if it has stopped responding, but your computer is still responsive. This command closes out any login status and open sessions.
show	**sh**	Display information about the appliance and the HSM, including appliance image and HSM firmware versions.
state	**st**	Display the current state of the HSM adapter.

Example

```
psesh:>hsm show

Appliance Details:
==================
        Version         : Protect Server External II v5.9.0
        ETNetServer     : Server active

HSM Details:
==================
        Model             : PSI-E2:PL1500
        Serial Number     : 518687
        Firmware Version  : 5.06.00
        Hardware Status   : BATTERY OK  PCB v0  FPGA v0  EXT PINS 0

Command Result : 0 (Success)


psesh:>hsm state

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

Command Result : 0 (Success)


psesh:>hsm reset

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

```
HSM reset successful.

Command Result : 0 (Success)
```

network

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

User access

admin, **pseoperator**

Syntax

network

dns
interface
iptables
route

network [**domain** <domain> | **hostname** <hostname> | **ping** <hostname/IP> | **show**]

Argument(s)	Shortcut	Description
dns	**dn**	Add or delete DNS name servers and domains. See "network dns" on page 26.
domain <domain>	**do**	Set the domain for the appliance. Enter this keyword followed by the domain name.
hostname <hostname>	**h**	Set the hostname for the appliance.
interface	**in**	Configure the appliance network interfaces. See "network interface" on page 27.
iptables	**ip**	Configure the iptables firewall for the appliance. You can use this command to configure the iptables ACCEPT and DROP rules. See "network iptables" on page 38.
ping <hostname/IP>	**p**	Test connectivity from the appliance to the specified hostname or IP address.
route	**r**	Manually configure routes on the SafeNet ProtectServer Network HSM appliance. See "network route" on page 42.
show	**s**	Display the current network configuration

Example

```
psesh:>network domain hsmdomain
Success: DomainName hsmdomain 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** <IP_address> | **searchdomain** <netdomain>}

delete {**nameserver** <IP_address> | **searchdomain** <netdomain>}

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

Example

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


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


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


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

network interface

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

User Access
admin, **pseoperator**

Syntax
network interface

- **bonding**
- **dhcp**
- **delete**
- **static**

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

Argument(s)	Shortcut	Description
bonding	**b**	Configure network interface bonding. See "network interface bonding" on the next page.
delete	**del**	Delete the network configuration for a network interface (eth0 or eth1). See "network interface delete" on page 35.
-device <netdevice>	**-d**	Specifies the interface you want to configure. **Valid values:** eth0, eth1
dhcp	**dh**	Set a network interface with a DHCP IP configuration. See "network interface dhcp" on page 36.
-force	**-f**	Force the action without prompting.
-gateway <IP>	**-g**	Specifies the gateway to assign to the specified device.
-ip <IP>	**-i**	Specifies the IP address to assign to the specified device.
-netmask <IP>	**-n**	Specifies the network mask, in dotted-decimal format (for example, 255.255.255.0), to assign to the specified device.
static	**s**	Sets a network interface with a static IP configuration. See "network interface static" on page 37.

network interface bonding

Bond two network interfaces into a single virtual device. Creating a bonded interface provides redundant failover in the event of a port failure, and improves bandwidth. When bonded, two interfaces appear as a single physical device with the same MAC address.

User Access
admin, **pseoperator**

Syntax
network interface bonding

config
disable
enable
show

Argument(s)	Shortcut	Description
config	**c**	Configure the network bonding interface. See "network interface bonding config" on the next page.
disable	**d**	Disable the bonding interface. See "network interface bonding disable" on page 32.
enable	**e**	Enable the bonding interface using the current configuration. See "network interface bonding enable" on page 33.
show	**s**	Show bond configuration information. See "network interface bonding show" on page 34.

network interface bonding config

Configure the network bonding interface. There are multiple modes available.

User Access
admin, **pseoperator**

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

Argument(s)	Shortcut	Description
-gateway <IP>	**-g**	Specifies the gateway to assign to the bonded device.
-ip <IP>	**-i**	Specifies the IP address to assign to the bonded device.

Argument(s)	Shortcut	Description
-mode <mode>	**-m**	Specifies the bonding mode (default: **0**). **Valid Values:** > **0**: Balance Round Robin. Packets are transmitted alternately on each device in the bond, providing load balancing and fault tolerance. > **1**: Active-Backup. One bonded device is active and the other serves as a backup. The backup only becomes active if the active device loses connectivity. > **2**: Balance XOR. Transmits based on an XOR formula, where the source MAC address is XOR'd with the destination MAC address. The same bonded device is selected for each destination MAC address, providing load balancing and fault tolerance. > **3**: Broadcast. All packets are transmitted on both bonded interfaces, providing fault tolerance. > **4**: 802.3ad (Dynamic Link Aggregation). Creates aggregated groups that share the same speed and duplex settings. This mode requires a switch that supports IEEE 802.3ad dynamic links. The dvice used for an outgoing packet is selected by the transmit hash policy (by default, a simple XOR). This policy can be changed via the xmit_hash_policy option. **NOTE:** Check the 802.3ad standard to ensure that your transmit policy is 802.3ad-compliant. In particular, check section 43.2.4 for packet mis-ordering requirements. Non-compliance tolerance may vary between different peer implementations. > **5**: Balance TLB (Transmit Load Balancing). Outgoing traffic is distributed according to the current load and queue on each bonded device. Incoming traffic is received by the current device. > **6**: Balance ALB (Adaptive Load Balancing). Both outgoing and incoming traffic is load-balanced like outgoing traffic in mode 5. Incoming load balancing is governed by ARP negotiation. The bonding driver intercepts the ARP replies sent by the appliance and overwrites the source hardware address with the unique hardware address of one of the bonded devices. Different clients will therefore use different hardware addresses for the appliance.
-netmask <IP>	**-n**	Specifies the network mask, in dotted-decimal format (for example, 255.255.255.0), to assign to the bonded device.

Example

```
psesh:>network interface bonding config -ip 192.20.11.10 -netmask 255.255.255.0 -mode 1
```

```
NIC Bonding configured

Command Result : 0 (Success)
```

network interface bonding disable

Disable network interface bonding.

User Access

admin, **pseoperator**

Syntax

network interface bonding disable

Example

```
psesh:>network interface bonding disable

NIC Bonding disabled

Command Result : 0 (Success)
```

network interface bonding enable

Enable the current bonding configuration.

User Access

admin, **pseoperator**

Syntax

network interface bonding enable

Example

```
psesh:>network interface bonding enable

NIC Bonding enabled
MUST RESTART SYSTEM TO SET THE CORRECT BONDING PARAMETERS!!!

Command Result : 0 (Success)
```

network interface bonding show

Display the current bond configuration.

User Access

admin, **pseoperator**

Syntax

network interface bonding show

Example

```
psesh:>network interface bonding show

Bonding is configured, but not enabled.

========== Bonding Interface ==========
BOOTPROTO=static
IPADDR=192.20.11.99
NETMASK=255.255.255.0
BOND MODE= (Balance Round Robin)
=======================================

Command Result : 0 (Success)
```

network interface delete

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

User Access
admin, **pseoperator**

Syntax
network interface delete -device <netdevice>

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

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

Interface eth1 removed successfully.

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**]

Argument(s)	Shortcut	Description
-device <netdevice>	**-d**	Specifies the interface you want to configure to use DHCP. **Valid values:** eth0, eth1
-force	**-f**	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...ADDCONF(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** <IP_address> **-netmask** <IP_address> [**-gateway** <IP_address>] [**-force**]

Argument(s)	Shortcut	Description
-device <netdevice>	**-d**	Specifies the interface you want to configure. **Valid values:** eth0, eth1
-ip <IP_address>	**-i**	Specifies the IP address to assign to the specified device.
-netmask <IP_address>	**-n**	Specifies the network mask, in dotted-decimal format (for example, 255.255.255.0), to assign to the specified device.
-gateway <IP_address>	**-g**	Specifies the gateway to assign to the specified device.
-force	**-f**	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

Argument(s)	Shortcut	Description
addrule	**a**	Add an ACCEPT or DROP rule to the iptables firewall for the appliance. See "network iptables addrule" on page 40.
clear	**c**	Clear the iptables for the device. This returns the iptables to a factory default state.
delrule	**d**	Deletes the specified "INPUT" chain rule in iptables. Run **network iptables show** to see the rule numbers. See "network iptables delrule" on page 41
save	**sa**	Saves the iptables changes. You must execute this command or any changes will be discarded on the next appliance restart.
show	**sh**	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** <netmask>}

drop {**host -ip** <IP_address> | **network -net** <IP_address> **-mask** <netmask>}

Argument(s)	Shortcut	Description
accept	**a**	Add a host or network ACCEPT rule to the iptable for the appliance.
drop	**d**	Add a host or network DROP rule to the iptable for the appliance.
host –ip <IP_address>	**h –i**	Specifies the IP address of the host you are adding the rule for.
network –net <IP_address> **–mask** <netmask>	**n –n –m**	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>

Argument(s)	Shortcut	Description
-rulenum <number>	**-r**	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**

Argument(s)	Shortcut	Description
add	**a**	Adds a manually configured network route. See "network route add" on the next page. **Note:** This command should only be used on the advice of a network administrator.
clear	**c**	Deletes all manually configured network routes. See "network route clear" on page 44. **Note:** This command should only be used on the advice of a network administrator.
delete	**d**	Deletes one manually configured network route. See "network route delete" on page 45. **Note:** This command should only be used on the advice of a network administrator.
show	**s**	Shows the current network route configuration. See "network route show" on page 46.

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> <IP_address> [**-device** <interface>] [**-metric** <metric>] [**-netmask** <netmask>] **-gateway** <IP_address>] [**-force**]

Argument(s)	Shortcut	Description
<route_type>		Specifies the type of route you want to add. **Valid values:** host, network
<IP_address>		Specifies the IP address of the route you want to add.
-device <interface>	**-d**	Specifies the interface you want to configure. **Valid values:** eth0, eth1
-metric <metric>	**-m**	Specifies the routing metric for the route. **Range:** 0-65535
–netmask <netmask>	**-n**	Specifies the network mask for the route, in dotted-decimal format (for example, 255.255.255.0).
-gateway <IP_address>	**-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> <IP_address> [**-device** <interface>] [**-metric** <metric>] [**-netmask** <netmask>] [**-gateway** <IP_address>] [**-force**]

Argument(s)	Shortcut	Table Section Outside Table: Description
<route_type>		Specifies the type of route you want to delete. **Valid values:** 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. **Valid values:** eth0, eth1
-metric <metric>	**-m**	Specifies the routing metric for the route. **Range:** 0-65535
–netmask <netmask>	**-n**	Specifies the network mask for the route, in dotted-decimal format (for example, 255.255.255.0).
-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**}

install –spkgfile <spkg_file> **–authcode** <auth_code>

listfile

Argument(s)	Shortcut	Description
list {**all** | **ptk**}	**l** {**a** | **p**}	List the packages currently installed on the appliance. Use the **all** flag to list all packages. Use the **ptk** flag to list the SafeNet ProtectToolkit packages only.
install –spkgfile <spkg_file> **–authcode** <auth_code>	**i –s –a**	Install the update contained in the specified secure package file (***.spkg**). You must include the authorization code string found in the included **authcode.txt** file. Specify the string itself; you cannot specify the **.txt** file with the **–authcode** parameter. Use **scp**/**pscp** to securely transfer the secure package file to the appliance.
listfile	**listf**	Display a list of all the secure package files you have transferred to the appliance.

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)
```

```
psesh:>package install -s test.spkg -a 5C6DF95B7F6837FD62E000

Please Enter the Admin Token PIN:

Decryption Successful

Signature Verification Successful

Preparing packages for installation...
dummy-package2-1.0-1
Preparing packages for installation...
dummy-package1-1.0-1

RPM installation Successful

SPKG package installation successful.


Command Result : 0 (Success)
```

> **NOTE** When installing a secure package on SafeNet ProtectServer Network HSM Plus, the following error message may be displayed:
>
> `IRQ 16/viper0: IRQF_DISABLED is not guaranteed on shared IRQs`
>
> This does not affect any part of the installation and can be safely ignored.

```
psesh:>package listfile

Available Packages:

test.spkg
test2.spkg
test3.spkg
test4.spkg
test_rsa2.spkg

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
- **audittrace** - HSM service required for audit logging (this service can only be affected by the **audit** user)
- **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>}

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

Example

```
psesh:>service list

   The following are valid PSe service names:
      network      - Network service (Needed for etnetserver, ssh and scp)
      etnetserver  - HSM service required for client connections
      audittrace   - HSM service required for audit logs
      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**

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

Argument(s)	Shortcut	Description
mem	**me**	Display the current memory usage.
netstat	**n**	Display the current network connections.
ps	**p**	Display the status of all active processes.
time	**t**	Display the time currently configured on the appliance, using the 24 hour clock.
zone	**z**	Display the currently configured time zone.

Example

```
psesh:>status cpu

CPU Load Averages:
0.14 0.10 0.08 1/68 11162

System uptime:
At 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/udevd
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**
- **etnetcfg**
- **snmp**
- **time**
- **timezone**

Argument(s)	Shortcut	Description
appliance	**a**	Reboot or power-off the appliance. See "sysconf appliance" on the next page.
etnetcfg	**e**	View or change the configuration file used to determine HSM appliance server settings. See "sysconf etnetcfg" on page 58.
snmp	**s**	Configure the SNMP settings on the appliance. See "sysconf snmp" on page 59.
time	**t**	Set the appliance time and date. See "sysconf time" on page 62.
timezone	**timez**	Display or set the appliance timezone. See "sysconf timezone" on page 63.

sysconf appliance

Reboot or power-off the appliance, or reset appliance account passwords and configuration settings to factory defaults.

User Access
admin, **pseoperator**

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

Argument(s)	Shortcut	Description
factory	**f**	Reset all appliance account passwords, SNMP, and network configuration to factory settings. Available to the **admin** user only.
poweroff	**p**	Power-off the appliance.
reboot	**r**	Reboot the appliance.

Example

```
psesh:>sysconf appliance factory


WARNING !!  This command will reset the appliance to factory defaults.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'

> proceed
Proceeding...
Changing password for user admin.
passwd: all authentication tokens updated successfully.
Changing password for user audit.
passwd: all authentication tokens updated successfully.
Changing password for user pseoperator.
passwd: all authentication tokens updated successfully.
Shutting down interface eth0:  [  OK  ]
Shutting down interface eth1:  [  OK  ]
Shutting down loopback interface:  [  OK  ]
Bringing up loopback interface:  [  OK  ]
Bringing up interface eth0:  Determining if ip address 172.20.9.35 is already in use for device
eth0...
[  OK  ]
Bringing up interface eth1:  Determining if ip address 192.168.1.100 is already in use for device
eth1...
[  OK  ]


Command Result : 0 (Success)
```

```
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

It is now safe to poweroff the appliance.

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 etnetcfg

View or change the configuration file used to determine HSM appliance server settings.

User Access

admin

Syntax

sysconf etnetcfg {**set** <filename> | **show**}

Argument(s)	Shortcut	Description
set <filename>	**se**	Use the specified configuration file as the basis for HSM appliance server settings. This file must be transferred to the appliance using **scp**/**pscp**.
show	**sh**	View the current etnetserver configuration settings.

Example

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

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

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


Command Result : 0 (Success)


psesh:>sysconf etnetcfg show


etnetserver is running

Current etnetserver configuration

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

Command Result : 0 (Success)
```

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**}

Argument(s)	Shortcut	Description
config	**c**	Configure the SNMP settings for the appliance. See "sysconf snmp config" on page 61.
disable	**d**	Disable SNMP on the appliance and stop the SNMP service.
enable	**e**	Enable SNMP on the appliance and start the SNMP service.
show	**s**	Display the current SNMP settings for the appliance.

Example

```
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** <IP_address> **-community** <string>

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

sysconf time

Set the time and date on the appliance.

User Access

admin, **pseoperator**

Syntax

sysconf time <time> <date>

Argument(s)	Shortcut	Description
<time>		Set the time on the appliance. Time must be specified in 24-hour format (HH:MM).
<date>		Set the date on the appliance (YYYYMMDD).

Example

```
psesh:>sysconf time 09:41 20191202

Mon Dec  2 09:41:00 EST 2019


Command Result : 0 (Success)
```

sysconf timezone

Display or set the timezone on the appliance.

User Access

admin, **pseoperator**

Syntax

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

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

Example

```
psesh:>sysconf timezone set 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
    cleanup
    export
    period
    remotehost
    rotate
    rotations
    show
    tail
    tarlogs
```

Argument(s)	Shortcut	Description
cleanup	**c**	Create an archive of the current logs and then delete all log files. See "syslog cleanup" on the next page.
export	**e**	Export syslog to file for transfer from appliance. See "syslog export" on page 66.
period	**p**	Sets the time between syslog rotations. See "syslog period" on page 67.
remotehost	**re**	Configures syslog to send logs to remote hosts. See "syslog remotehost" on page 68.
rotate	**rotate**	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 "syslog rotate" on page 73.
rotations	**rotati**	Sets the number of old syslogs that are kept. See "syslog rotations" on page 74.
show	**s**	Display the current log rotation configuration and the configured log levels. See "syslog show" on page 75.
tail	**tai**	Display the last entries of the specified syslog. See "syslog tail" on page 77.
tarlogs	**tar**	Create an archive of the syslog. See "syslog tarlogs" on page 78.

syslog cleanup

Creates a .tar archive of logs currently on the HSM, and deletes all log files. The resulting archive is saved to the appliance SCP directory for transfer, named "**logs_cleanup_YYYYMMDD_hhmm.tgz**".

Syntax

syslog cleanup

Example

```
psesh:>syslog cleanup



WARNING !!  This command creates an archive of the current logs and then DELETES ALL THE LOG
FILES.
If you are sure that you wish to proceed, then type 'proceed', otherwise type 'quit'.

> proceed
Proceeding...
Creating tarlogs then deleting all log files ...

The tar file containing logs is now available via scp as filename "logs_cleanup_20191105_
1607.tgz".
Please copy "logs_cleanup_20191105_1607.tgz" to a client machine with scp.

Deleting log files ...
restart the rsyslogd service if it's running



Command Result : 0 (Success)
```

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 ProtectServer 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>

Argument(s)	Description
<syslogperiod>	Specifies the log rotation period. **Valid values:** 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
```

Argument(s)	Shortcut	Description
add	**a**	Add a remote host. See "syslog remotehost add" on the next page.
clear	**c**	Delete All Remote Logging Servers. See "syslog remotehost clear" on page 70.
delete	**d**	Delete a remote host. See "syslog remotehost delete" on page 71.
list	**l**	List all syslog remote hosts. See "syslog remotehost list" on page 72.

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/IP>

Argument(s)	Description
<hostname/IP>	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**]

Argument(s)	Shortcut	Description
-force	**-f**	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/IP>

Argument(s)	Description
<hostname/IP>	Specifies the hostname or the IP address of the remote computer system to delete from the list.

Example

```
psesh:>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.

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>

Argument(s)	Description
<syslog_rotations>	An integer that specifies the number of history files to keep when rotating system log files. **Range:** 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**]

Argument(s)	Shortcut	Description
-files	**-f**	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>]

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

Example

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

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** or **audit** 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**, **audit**

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)
```

Glossary

A

Adapter

The printed circuit board responsible for cryptographic processing in a HSM

AES

Advanced Encryption Standard

API

Application Programming Interface

ASO

Administration Security Officer

Asymmetric Cipher

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

B

Block Cipher

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

Bus

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

C

CA

Certification Authority

CAST

Encryption algorithm developed by Carlisle Adams and Stafford Tavares

Certificate

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

CMOS

Complementary Metal-Oxide Semiconductor. A common data storage component

Cprov

ProtectToolkit C - SafeNet's PKCS #11 Cryptoki Provider

Cryptoki

Cryptographic Token Interface Standard. (aka PKCS#11)

CSA

Cryptographic Services Adapter

CSPs

Microsoft Cryptographic Service Providers

D

Decryption

The process of recovering the plaintext from the ciphertext

DES

Cryptographic algorithm named as the Data Encryption Standard

Digital Signature

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

DLL

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

DSA

Digital Signature Algorithm

E

Encryption

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

F

FIPS

Federal Information Protection Standards

FM

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

FMSW

Functionality Module Dispatch Switcher

H

HA

High Availability

HIFACE

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

HSM

Hardware Security Module

I

IDEA

International Data Encryption Algorithm

IIS

Microsoft Internet Information Services

IP

Internet Protocol

J

JCA

Java Cryptography Architecture

JCE

Java Cryptography Extension

K

Keyset

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

KWRAP

Key Wrapping Key

M

MAC

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

Message Digest

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

MSCAPI

Microsoft Cryptographic API

MSDN

Microsoft Developer Network

P

Padding

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

PCI

Peripheral Component Interconnect

PEM

Privacy Enhanced Mail

PIN

Personal Identification Number

PKCS

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

PKCS #11

Cryptographic Token Interface Standard developed by RSA Laboratories

PKI

Public Key Infrastructure

ProtectServer

SafeNet HSM

ProtectToolkit C

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

ProtectToolkit J

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

R

RC2/RC4

Ciphers designed by RSA Data Security, Inc.

RFC

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

RNG

Random Number Generator

RSA

Cryptographic algorithm by Ron Rivest, Adi Shamir and Leonard Adelman

RTC

Real Time Clock

S

SDK

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

Slot

PKCS#11 slot which is capable of holding a token

SlotPKCS#11

Slot which is capable of holding a token

SO

Security Officer

Symmetric Cipher

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

T

TC

Trusted Channel

TCP/IP

Transmission Control Protocol / Internet Protocol

Token

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

TokenPKCS#11

Token that provides cryptographic services and access controlled secure key storage

U

URI

Universal Resource Identifier

V

VA

Validation Authority

X

X.509

Digital Certificate Standard

X.509 Certificate

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