ProtectServer External 2 (PSE2)

Installation Guide

SafeNet

THE
DATA
PROTECTION
COMPANY

Part Number 007-007474-007
Version 5.1

Trademarks

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 SafeNet.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures.

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To ensure FCC compliance only devices also known to comply should be connected to the adapter's serial ports. If such devices do not feature their own cables shielded cables must be used.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. Send your comments, together with your personal and/or company details to the address below:

SafeNet, Inc.
4690 Millennium Drive
Belcamp, Maryland USA 21017

Technical Support

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

Contact method	Contact
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA

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

Revision History

Revision	Date	Reason
A	27 October 2014	Release 5.0
B	12 August 2015	Release 5.1

Contents

Chapter 1
Introduction

This Guide is provided as an instructional aid for the installation and configuration of a ProtectServer External 2 (PSE2) cryptographic services hardware security module (HSM).

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

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

Chapter 4 describes the installation procedure.

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

The technical specification for the product is in Appendix A.

NOTE:
This release applies to the second-generation ProtectServer External appliance, named ProtectServer External 2 (PSE2). This new hardware variant is ROHS-compliant, and uses all the software that accompanied the original PSE, namely Ptk-C, Ptk-J, Ptk-M, and all of their documents, libraries, utilities, etc.

Chapter 2
Product overview

The Protect Server External 2 (PSE2) is a self-contained, security-hardened server providing hardware based cryptographic functionality through a TCP/IP network connection. The product is used, together with SafeNet high level application programming interface (API) software, to implement cryptographic service providers for a wide range of secure applications.

The PSE2 is PC based. The enclosure (pictured) is a heavy duty steel case and common PC ports and controls are provided. The unit is delivered with the necessary software components pre-installed on a Linux operating system, in a “ready to operate” state. Network setting configuration is required, as described in this document.

The full range of cryptographic services required by Public Key Infrastructure (PKI) users is supported by using the PSE2’s dedicated hardware cryptographic accelerator. These services include encryption, decryption, signature generation and verification, and key management with a tamper resistant and battery-backed key storage.

To implement a cryptographic service provider, use the PSE2 with one of SafeNet’s high level cryptographic APIs. The provider types that can be implemented and the corresponding SafeNet high level cryptographic API required are shown in the following table.

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

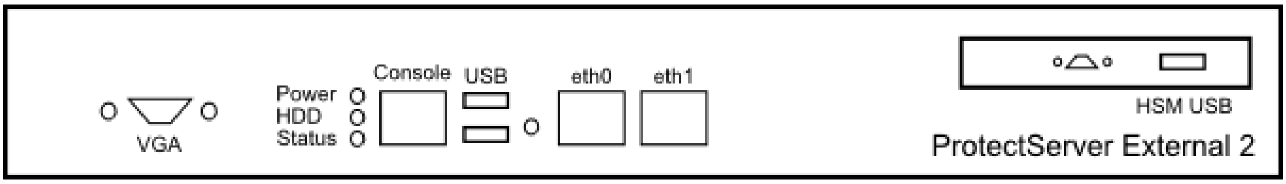
To provide the highest level of security, these APIs interface directly with the product’s FIPS 140-1 Level 3 certified core. High-speed DES and RSA hardware based cryptographic processing is used. Key storage is tamper resistant and battery-backed.

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

Front panel view

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

Figure 1: PSE2 front panel



Ports

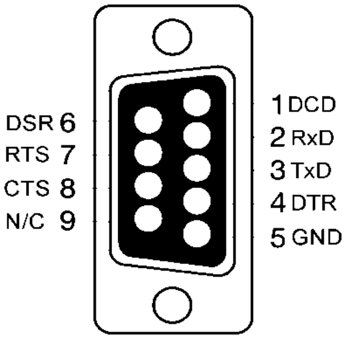
The front panel is equipped with the following ports:

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

HSM serial port pin configuration

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

Figure 2: HSM serial port pinout



LEDs

The front panel is equipped with the following LEDs:

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

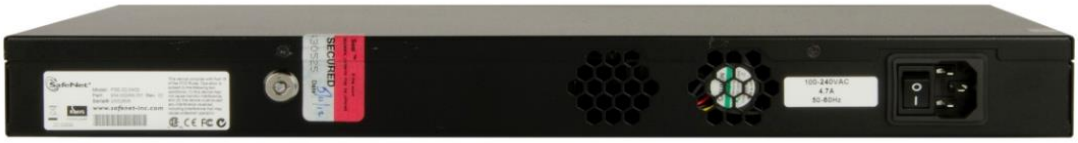
Reset button

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

Rear panel view

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

Figure 3: PSE2 rear panel



Tamper lock

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

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

CAUTION!
Turning the tamper key from the Active position to the Tamper position causes any keys currently stored on the HSM to be deleted. Once the keys are deleted they are not recoverable. Ensure that you always back up your keys. To avoid accidentally deleting the keys on an operational PSE2, remove the tamper key after installation/commissioning and store it in a safe place.

Chapter 3
Implementation overview

Implementation architecture

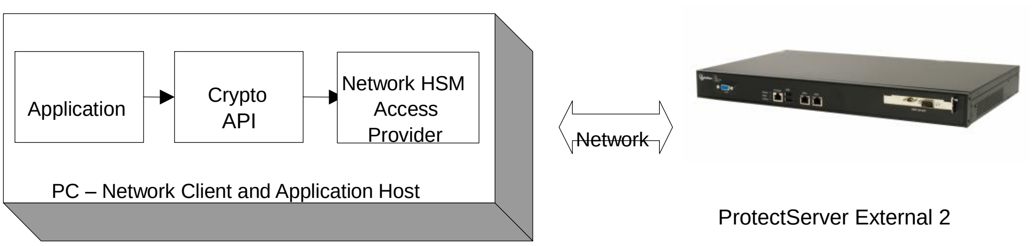
To implement a hardware based cryptographic service provider, essentially three elements are required.

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

Where key processing and storage is to be implemented using a standalone SafeNet Protect Server External 2 (PSE2) HSM, the cryptographic service provider will operate in network mode.

In network mode, Network HSM Access Provider software is installed on the same machine used to host the cryptographic API software. It is used to implement the connection between and the PSE2 and the cryptographic host using a TCP/IP network connection. The PSE2 can then be located at any distance from the machine hosting the access provider, cryptographic API and application software.

A network mode implementation of a cryptographic service provider using the PSE2 is shown in the next figure.


Application
Crypto API
Network HSM Access Provider
PC – Network Client and Application Host
Network
ProtectServer External 2

Implementation steps

The installation and configuration of the PSE2 is part of the setup of the overall network operating mode.

The following is a summary (with references to the location of detail) of the steps to setup a cryptographic service provider, using the network operating mode and a PSE2:

1. Install the PSE2

See "Installation" on page 7.

2. Test the PSE2

To confirm the correct operation of the unit, test the PSe. See "Testing and configuration" on page 9 for details.

3. Configure the PSE2 network settings

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

4. Install and configure the Network HSM Access Provider software

Network HSM Access Provider software must be installed on the network client and configured to support operation in network mode. Full details are in the *Hardware Security Module Access Provider Install & Configuration Guide* supplied with the software.

5. Install the high level cryptographic API

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

6. Configure the high-level cryptographic API

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

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

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

Chapter 4
Installation

This chapter provides information on how to install the Protect Server External 2 (PSE2).

Since the PSE2 is delivered with the necessary software components pre-installed, no software installation is necessary on the unit itself.

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

Installation procedure

To install the hardware

1. Choose a suitable location to site the equipment. You can mount the PSE2 in a standard 19-inch rack, as described in the Quickstart Guide.

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

2. Connect the PSE2 to the network that hosts the client machine(s) where the SafeNet cryptographic API software is installed. Connect the PSE2 to the network by inserting standard Ethernet cables into the LAN connectors located on the front of the PSE2. The LAN connectors are autosensing 10/100/1000 Mb/s Ethernet RJ45 ports.

   Note:
   The PSE2 is equipped with two NICs (**eth0** and **eth1**), each of which can be configured with its own IP address. 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 PSE2 is equipped with an autosensing power supply that can accept 100-240V at 50-60Hz.

Smart Card Reader Installation

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

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

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

The options are:

- Connect a PS/2-to-USB adapter cable between the card reader and a USB port on the PSE2.
- If you prefer to not expose USB ports on your crypto server (for security reasons), then connect a PS/2-to-USB adapter cable between the card reader and a standalone powered USB hub.

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

Note:
You must use the supplied SafeNet smart card reader. Smart card readers, other than those supplied by SafeNet, are not supported.

Chapter 5
Testing and configuration

This chapter provides information on how to:

- test the Protect Server External 2 (PSE2) to confirm correct operation
- configure network settings.

The assumptions are:

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

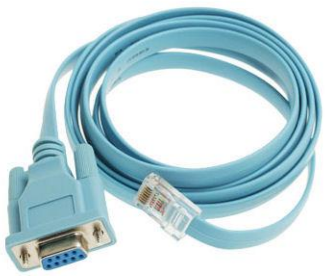
Troubleshooting information is at the end of this chapter.

Equipment requirements

To complete the system test and configure the network you must be able to access the PSE2 console. You can access the console directly by connecting a keyboard and monitor (not included) to the USB (keyboard) and VGA (monitor) ports located on the front panel of the PSE2, or you can access the console remotely by connecting the RJ45 console port to a terminal emulation device, such as a laptop or terminal server.

Note:
If you want to access the PSE2 console remotely using the console port, you will need a cable. If your terminal device is equipped with a DB9 serial port, you require a cable with an RJ45 connector on one end and a DB9 serial port on the other end, as illustrated in Figure 4. If your terminal device is equipped with an RJ45 serial port, you can use an RJ45-to-RJ45 cable, such as an Ethernet cable. Serial cables are not included.

Figure 4: Serial cable: RJ45 to DB9



Procedure overview

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

1. Connect a keyboard/monitor or serial cable to the PSE2

In order to access the PSE2 console, you must do one of the following:

- connect a keyboard and monitor (not included) to the **USB** (keyboard) and **VGA** (monitor) ports located on the front panel of the PSE2.

- use a serial cable (not included) to connect the RJ45 console port to a terminal emulation device, such as a laptop or terminal server.

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

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

2. Power on the PSE2

Power on the PSE2 and the monitor (if applicable). A green LED on the front of the device will come on and the startup messages will be displayed to the screen. Power-on is complete when the **PSE2 login:** prompt is displayed.

3. Login to the console

Following boot up, the PSE2 will prompt for login credentials. If you are using a monitor/keyboard, you can log in as **admin** or **root**. If you are using a serial connection, you can log in as **admin** only.

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

User name	Default password
root	password
admin	password

At this time, we **strongly** recommend that you use the “passwd” command to 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 “obtain an RMA number, ship the unit back to us and have it re-imaged”, which is not a warranty service).

4. Run the system test to confirm correct operation

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

5. Set the IP address for each processing module

Refer to "Setting the IP address" on page 11 for details.

6. Set the hostname (if required).

Refer to "Setting a hostname and default gateway" on page 12 for details.

7. Set the name server IP address (if required)

Refer to "Setting a name server" on page 12 for details.

8. Set access control (if required)

Refer to "Setting access control" on page 12 for details.

9. **Verify that you have SSH network access to the PSe (if required)**

   Refer to "SSH network access" on page 13 for details

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

System testing

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

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

```
NORMAL MODE. RESPONDING.
```

You can also use the *PSE_status* command to verify that the PSE2 is functioning correctly, as described below.

The PSE_status command

Syntax

```
PSE_status
```

Description

This utility displays the current status of the Protect Server External 2 (PSE2). It provides the following information:

- the status of the HSM installed in the PSE2. If the unit is functioning correctly, a message that includes the following is returned:

  ```
  PSE status NORMAL
  ```

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

Example

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

Setting the IP address

The PSE2 is equipped with two NICs (**eth0** and **eth1**), each of which can be configured with its own IP address. The IP address for each NIC is specified in the following files:

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

This 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
```

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

Setting a hostname and default gateway

Set the default gateway (that this SafeNet PSE2 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

The PSE2 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 PSE2 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

Access control on the Protect Server External 2 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`**(8)** 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 now be restored before connections to the PSe are allowed. The following command will restore the previously saved active configuration.

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

SSH network access

After you have completed the network configuration, you can access the PSE2 over the network using the SSH protocol. To access the PSE2 using SSH, you require an SSH client such as puTTY (available for free from www.putty.org).

Note:
You must log in as the admin user when accessing the PSE2 over an SSH connection.

Restarting networking

After making any change to the networking configuration, reboot the PSE2 or enter the following command to restart networking:

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

Powering off the PSE2

You must be logged in as root to power off the PSE2.

To power off the PSE2

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 PSE2, to the off position. The fan and LEDs will turn off.

Upgrading the PSe

You can upgrade the PSE2 to a later revision using USB media, such as USB memory sticks or a USB-connected CDROM drive.

Process

1. Select and download the desired PSE2 image upgrade file from the SafeNet Web site at http://www.safenet-inc.com.
2. Place the upgrade files onto the root directory of a USB memory stick or onto a CDROM.
3. Connect the CDROM drive or memory stick to any USB port on the back of the PSe. The operating system maps the new hardware and adds a /etc/fstab entry.
4. The relevant directory is created in /media (examples: /media/usbflash, or /media/cdrecorder) but does not automount - complete with mount command (example: mount /media/usbflash).
5. Use umount command to unmount when finished and the device is to be removed.

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

Troubleshooting

Each Protect Server External 2 is tested during manufacture to ensure a high level of quality. In the unlikely event the unit is not functioning correctly please re-check the installation procedure, paying particular attention to the power source and network cable connection. Running the diagnostic utility program *hsmstate* as discussed in the System Testing section is the only method available to test the unit.

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

Note:
If it ever becomes necessary to get into the BIOS then press <Delete> as the PSE2 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

Appendix A
Technical specifications

The Protect Server External 2 specifications are as follows:

Hardware

- One smart card reader secure USB port (requires the included USB-to-serial cable)
- Protective, heavy duty steel, industrial PC case
- ATOM D425 CPU
- 1 Gb RAM
- 2 Gb solid state flash memory hard disk (DOM)
- 10/100/1000 Mbps autosensing Network Interface with RJ45 LAN connector

Pre-installed Software

- Linux operating system
- SafeNet PCI HSM Access Provider software
- SafeNet HSM Net Server software

Power Supply

• Nominal power consumption:	43 W
• Input AC voltage range:	100-240 V
• Input frequency range:	50-60 Hz

Physical properties

- 437 mm (W) x 270 mm (D) x 44 mm (H) (1U)
- 19” rack mounting brackets included
- Weight 5 kg (11 lb)

Operating Environment

- Temperature: 0 to 40 °C (32 to 104 °F)
- Relative Humidity: 5 to 85%

END OF DOCUMENT