THALES

SafeNet Luna Network HSM Client 10.1

INSTALLATION GUIDE

Document Information

Product Version	10.1
Document Part Number	007-000553-001
Release Date	23 January 2020

Revision History

Revision	Date	Reason
Rev. A	23 January 2020	Initial release

Trademarks, Copyrights, and Third-Party Software

Disclaimer

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.

Regulatory Compliance
This product complies with the following regulatory regulations. To ensure compliancy, ensure that you install the products as specified in the installation instructions and use only Thales-supplied or approved accessories.

USA, FCC
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.

Canada
This class B digital apparatus meets all requirements of the Canadian interference-causing equipment regulations.

Europe
This product is in conformity with the protection requirements of EC Council Directive 2014/30/EU. This product satisfies the CLASS B limits of EN55032.

CONTENTS

PREFACE: About the Installation Guide

This document describes how to install the SafeNet Luna HSM hardware and the SafeNet Luna HSM Client software. Refer to the following chapters to verify the security and integrity of your new hardware shipment and install the hardware and software components applicable to you:

> "Verifying the Integrity of Your Shipment" on page 10

> "SafeNet Luna Network HSM Hardware Installation" on page 11

> "SafeNet Luna PED Received Items" on page 34. For instructions on setting up the SafeNet Luna PED, see "PED Authentication" on page 1 in the *Administration Guide*.

> "SafeNet Luna HSM Client Software Installation" on page 37

The preface includes the following information about this document:

> "Customer Release Notes" below

> "Audience" below

> "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.

Customer Release Notes

The customer release notes (CRN) provide important information about this release that is not included in the customer documentation. Read the CRN to fully understand the capabilities, limitations, and known issues for this release. You can view or download the latest version of the CRN from the Technical Support Customer Portal at https://supportportal.gemalto.com.

Audience

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

All products manufactured and distributed by Thales Group 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.)

Format	Convention
<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.gemalto.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. (KB0013367)

Email Support

You can also contact technical support by email at technical.support@gemalto.com.

CHAPTER 1:   Verifying the Integrity of Your Shipment

> **CAUTION!** Gemalto employs a number of security measures to allow you to verify that your new hardware was not intercepted in transit or otherwise tampered with before you received it. To verify the authenticity and handling history of your received items, review the following checklist before you unpack your new hardware, and then follow the checklist as you unpack each received item.

Step	Yes	No
1. Do the items received (individual items, part numbers) match those listed in the enclosed packing list? If yes, go to the next step. If no, contact Thales support.		
2. Before you received the product, did you receive an advanced shipping notification providing details regarding the shipment (part numbers and serial numbers for the product and tamper-evident bags)? If yes, go to the next step. If no, contact Thales support.		
3. Are all of the tamper-evident bag serial numbers and tamper-evident label serial numbers listed in the advanced shipping notification present, and do they match the actual tamper-evident bag/label serial numbers received? If yes, go to the next step. If no, contact Thales support.		
4. Did you receive any tamper-evident bag/label serial numbers that are not listed on the advance shipping notification? If yes, contact Thales support. If no, go to the next step.		
5. Are there any signs of physical tampering? If tamper-evident labels are affixed to the received product, have any of these labels been damaged? Have the tamper evident bags been damaged in any way? The tamper seals on the sides indicate tampering if they show the **ALERT** markings as illustrated below. If yes, contact Thales support. If no, go to the next step.		
6. Once you have verified all of the received items, you can proceed with the installation.		

CHAPTER 2:   SafeNet Luna Network HSM Hardware Installation

This chapter describes how to install and connect a SafeNet Luna Network HSM. To ensure a successful installation, perform the following tasks in the order indicated:

1. Before unpacking your new hardware, refer to "Verifying the Integrity of Your Shipment" on page 10 for safe unpacking instructions.

2. Ensure that you have all of the required components, as listed in "SafeNet Luna Network HSM Required Items" on the next page

3. If you plan to mount the hardware in an equipment rack, follow the instructions in "Rack-Mounting the SafeNet Luna Network HSM" on page 19.

4. Install and connect the hardware, as described in "Installing the SafeNet Luna Network HSM Hardware" on page 26

SafeNet Luna Network HSM Required Items

This section provides a list of the components you should have received with your SafeNet Luna Network HSM order. The specific items you received depend on whether you ordered a password-authenticated or a PED-authenticated SafeNet Luna Network HSM, and whether your order included a backup device or other options as described below.

Basic SafeNet Luna Network HSM order items

The standard items that you should have received as your basic order for a SafeNet Luna Network HSM are:

Qty	Item
1	**SafeNet Luna Network HSM Appliance** Your order should include one password-authenticated or PED-authenticated SafeNet Luna Network HSM. The different HSM models appear physically identical.
2	**Power Supply Cord** One for each power supply, with connectors appropriate to your region of operation.

Qty	Item
1	**Adapter Cable: RJ45 to USB with a standard eight-pin, eight connector (8P8C) modular connector** Used to open a terminal connection to the HSM during initial configuration.
1	**Front Ear Bracket Set** Set includes: > (2) front ear brackets > (4) bracket screws

Qty	Item
1	**Friction Rail Mounting Bracket Set** See "Using the Supplied Mounting Brackets" on page 19 for installation instructions. Set includes: > (2) side rails > (8) side rail screws > (2) sliding rear brackets (fit into the rails for rear support adjustable positioning) **CAUTION!** The included mounting hardware is meant for static positioning of the appliance. The long tab that slides into the bracket, applied to each side of the appliance, is adjustable for fitting the appliance into racks of varying depth - it must not be used to extend the appliance out of the rack. Optional gliding rails with rolling bearings are available for situations where rolling excursion of the appliance, while attached to the rack, is required for maintenance. See "Optional Items" on page 17.
1	**Friction Rail Rack Mounting Screws/Cage Nuts** Set includes: > (8) M5 cage nuts > (8) M5x14 rack screws If you did not receive this set, you can request one from Thales Group (part number: 216-000035-001) or obtain your own suitable screws/nuts.

Qty	Item
1	**Secure Locking Bezel**
	For maximum physical security, this faceplate bezel can restrict access to the SafeNet Luna Network HSM's front-facing inputs. Includes set of three (3) keys for each lock (locks are keyed differently).

PED-Authenticated SafeNet Luna Network HSM order items

If you ordered a PED-authenticated SafeNet Luna Network HSM, you should have received some combination of the following items in addition to the items in the basic order.

Note that you can use PED keys that you already own and use with other HSMs -- PED keys can be used with multiple HSMs if that is appropriate in your context. You should purchase the number of PEDs you need for your own convenient operation, and for backup/standby units as your security policies might require.

Qty	Item
1+	**Standard or Remote-Capable Luna PED**
	Your order should include at least one PED device.
	If you intend to back up your SafeNet Luna Network HSM to a SafeNet Luna Backup HSM, then you require a Luna PED to connect to that Backup HSM.
	If you intend to combine remote operation and backup, you might prefer to have a second PED. It is possible to use a single Luna PED for both connections, and to simply change between local and remote mode as needed.
	Note that you can use PED keys that you already own and use with other HSMs if appropriate. You should purchase the number you need for your own convenient operation, and for backup/standby units as your security policies might require.

Qty	Item
1	**Luna PED cable**
	The PED device connects to your HSM using a Type A to Mini B USB cable .
1	**Luna PED Power Supply Kit**
	If you ordered a Luna PED, your order should include a Luna PED power supply kit with the appropriate connection for your region. The power supply is auto-sensing and includes replaceable mains plug modules for international use.

Qty	Item
1	**Set of PED Keys and Labels** Your order should include a set of iKey PED keys and peel-and-stick labels.

Optional Items

You may have also ordered one or more of these optional items:

Qty	Item
1	**Sliding Rail Mounting Bracket Set** The SafeNet Luna Network HSM will fit into any standard 19-inch server rack. The optional sliding rail mounts allow for easy removal and access to the rear face of the HSM. See "Using the Optional Sliding Rail System" on page 22 for installation instructions. The set includes: **>** (2) sliding rail mounts with removable side rails **>** (2) transformer brackets **>** (6) rail screws

Qty	Item
1	**Sliding Rail Rack Mounting Screws** Set includes: **>** (8) M5x8 flat-headed screws If you did not receive this set, you can request one from Thales Group (part number: 216-000034-001) or obtain your own suitable screws. If you do not use the screws included in this kit, ensure that the screw heads are flat enough so as not to interfere with the locking bezel.
1	**SafeNet Luna Backup HSM** You can back up your selected SafeNet Luna Network HSM partition contents (root keys, certificates, other items) to a SafeNet Luna Backup HSM. The SafeNet Luna Backup HSM is suitable for off-site storage and for backing up multiple HSM partitions. It can back up contents of password-authenticated or of PED-authenticated HSMs. It must be initialized as one type or the other before the backup operation starts. The SafeNet Luna Backup HSM can be connected directly to an HSM, or it can be connected to a separate computer to back up remotely-located HSMs in conjunction with a Remote PED. The authentication method for a Backup HSM must match the authentication method (password or PED) for any HSM with which it is used. The SafeNet Luna Backup HSM ships with an external power supply.
2	**SFP 10 Gbps Optical Ethernet transceiver modules** If you ordered the 10 Gbps Optical Ethernet option, two of the RJ45 ports on the appliance are replaced by SFP+ connectors (protected by dust covers during shipping). The SFP 10G Optical transceiver modules are packed separately, within the appliance packaging, and must be inserted in the appliance before use.

Rack-Mounting the SafeNet Luna Network HSM

The SafeNet Luna Network HSM appliance comes with front ear brackets, side rails, rear slider brackets, and the necessary screws packed separately in the carton. You may also have ordered the optional sliding rail mounting system. See "SafeNet Luna Network HSM Required Items" on page 12 for details. Instructions for installing both systems are provided below:

> If you intend to use the supplied mounting brackets, see "Using the Supplied Mounting Brackets" below.

> If your order included the optional sliding rail mounting system, see "Using the Optional Sliding Rail System" on page 22. The sliding rails are recommended for ease of installation and maintenance.

> **CAUTION!**   Do not attempt to mount the appliance using only the front brackets – damage can occur.

Using the Supplied Mounting Brackets

Install and adjust the rails and brackets to suit your equipment rack. The standard mounting bracket set is designed for use in racks with a maximum depth of 27 inches (686 mm). For racks larger than 27 inches, a mounting tray or shelf is recommended.

> **CAUTION!**   The included mounting hardware is meant for static positioning of the appliance. The long tab that slides into the bracket, applied to each side of the appliance, is adjustable for fitting the appliance into racks of varying depth - it must not be used to extend the appliance out of the rack.
>
> Optional gliding rails with rolling bearings are available for situations where rolling excursion of the appliance, while attached to the rack, is required for maintenance. See "Using the Optional Sliding Rail System" on page 22 (below).

Ensure you have all the necessary components before proceeding. In addition to the supplied components, you will need:

> #2 Philips screwdriver

> hydraulic equipment lift

> **CAUTION!**   If you are installing the appliance in a rack without a mounting tray or shelf, ensure that the appliance is supported at all times or damage may occur. Use of a hydraulic equipment lift is strongly recommended. If you do not have access to a lift, you will need at least one assistant to mount the appliance.

To mount the SafeNet Luna Network HSM hardware

1. Install the two front ear mounting brackets on the HSM chassis using the included screws and a #2 Phillips screwdriver.
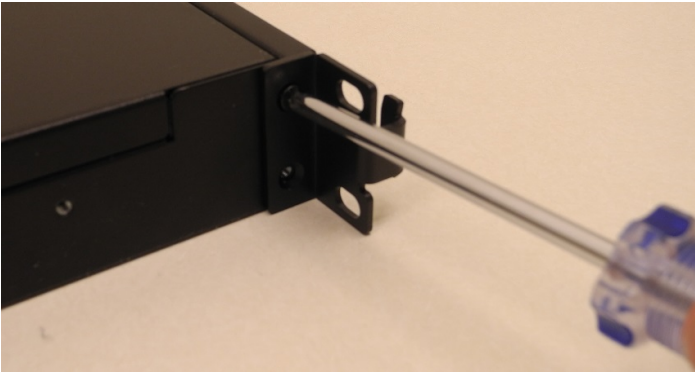
2. Fit eight cage nuts into the rack space where you want to install the appliance. Ensure that they are spaced correctly.

3. Install the two side rails on either side of the HSM chassis, using the included screws and a Phillips screwdriver. Note how the sliding rear brackets fit into the side rails.
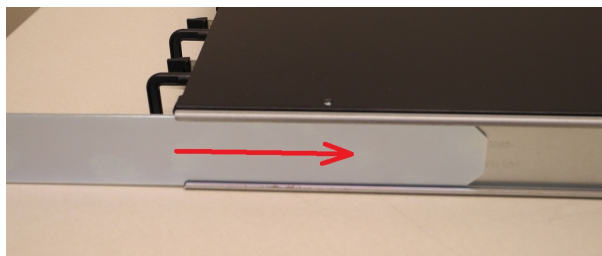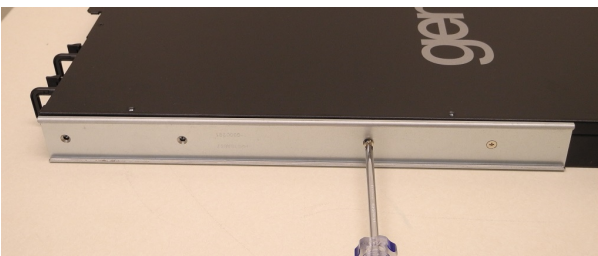
4. Install the two sliding rear brackets in your equipment rack using four rack mounting screws.

> **NOTE**   While any standard equipment rack screws should fit the brackets, certain large-headed screws may interfere with the operation of the secure locking bezel.
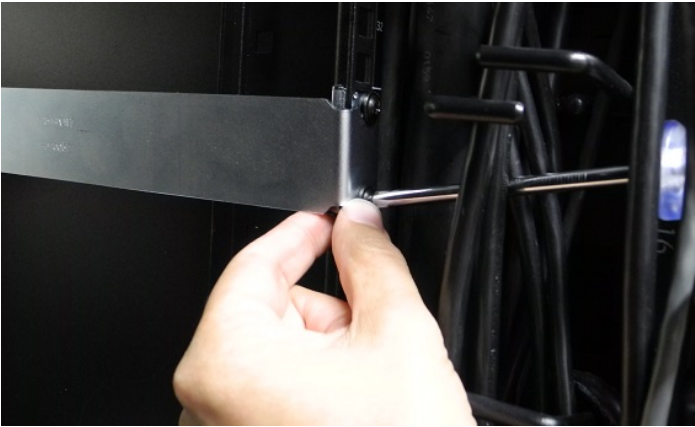
5. Using a hydraulic lift, raise the HSM to the level of the brackets and extend the lift into the rack.

> **CAUTION!** Perform the next step from the rear of the server rack. Do not push the HSM off the lift without supporting its rear end.

6. From the rear of the server rack, pull the appliance back towards you until the sliding rear brackets fit into the side rails. Pull the appliance back onto the rear brackets until the front ear brackets meet the equipment rack.
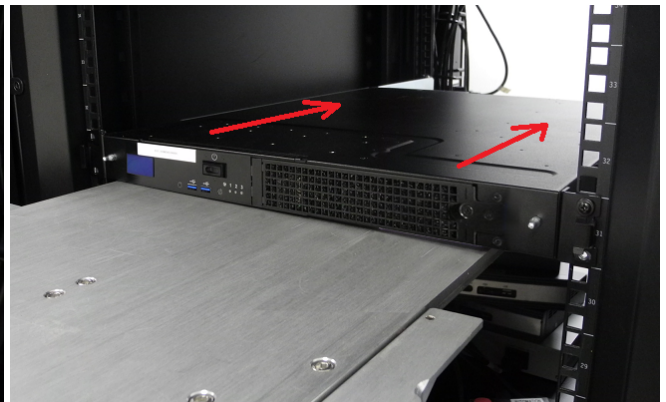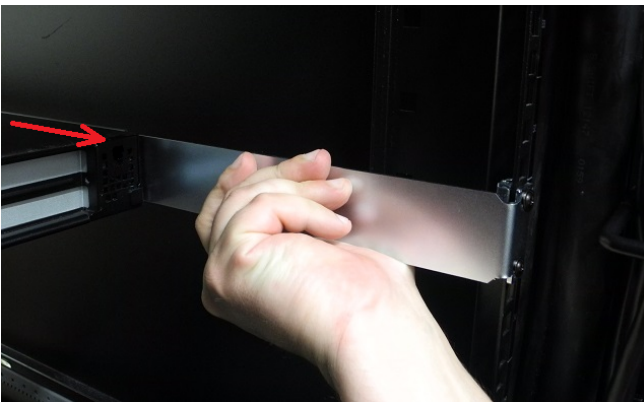
> **CAUTION!** Support the weight of the appliance with the hydraulic lift until all four brackets are secured.

7. Secure the front ear brackets using rack mounting screws.

See "SafeNet Luna Network HSM Hardware Installation" on page 11 to continue the installation process.

Using the Optional Sliding Rail System

The optional sliding rail system allows for the appliance to be extended out in front of the equipment rack, possibly easing access to other racked appliances. This is rarely necessary. After configuration, the SafeNet Luna Network HSM should remain secured in the rack with the locking bezel installed. Some security standards require the use of this bezel. Leaving the HSM uncovered for ease of access might compromise physical security.

The sliding rail mounts fit into any standard 19" equipment rack.

Ensure you have all the necessary components before proceeding. In addition to the supplied components, you will need a #2 Philips screwdriver.

To mount the SafeNet Luna Network HSM hardware

1. Install the two front ear mounting brackets on the HSM chassis using the included screws and a #2 Phillips screwdriver.
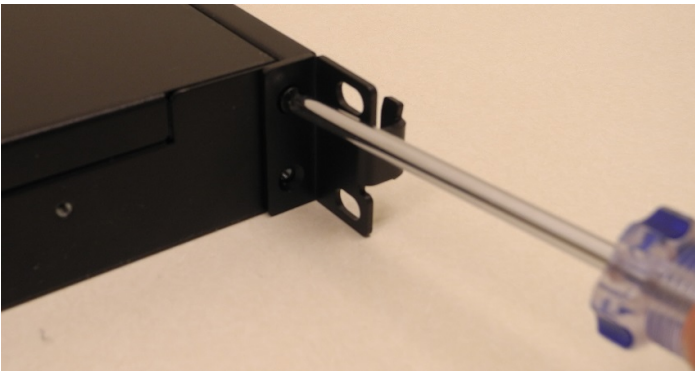
2. Fit the front end of each mount into either side of the rack and pull the spring-loaded latch at the rear to snap it in place.
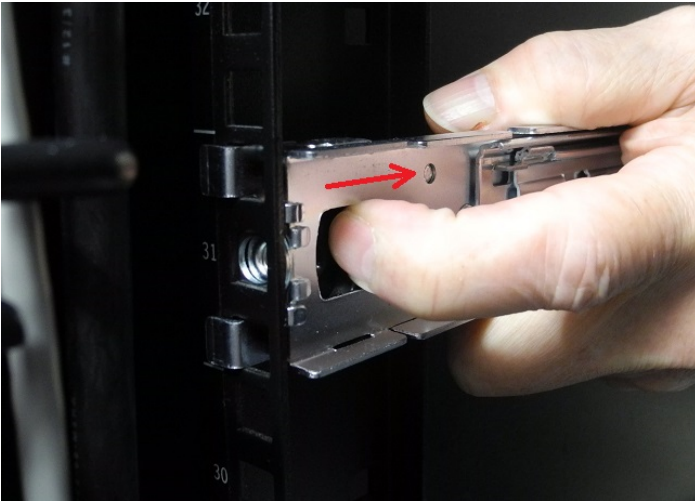
3. Secure the rear end of each mount to the rack with two wide flat-headed screws.
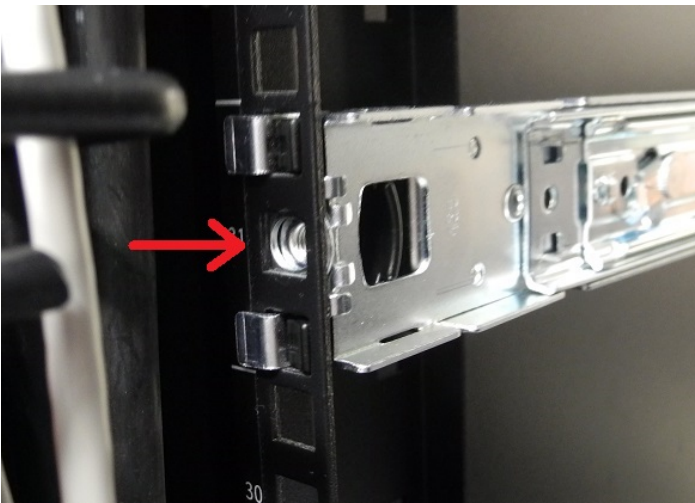
4. Fasten the transformer bracket to each sliding mount with two wide flat-headed screws.
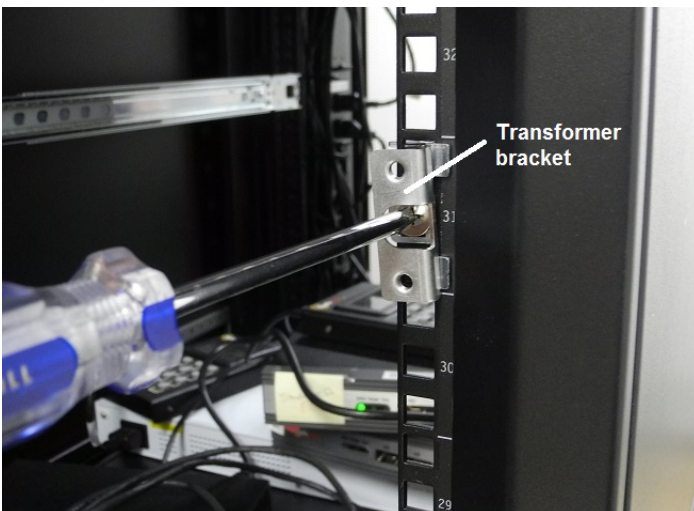
5. Loosely thread two small flat-headed screws into each side of the SafeNet Luna Network HSM. Fit each sliding rail over the screw heads and slide it forward into place before tightening the screws. Fasten each sliding rail with a third screw where it lines up with the hole in the HSM chassis.

6. Fit the sliding rails onto the rack mounts until they lock into place.
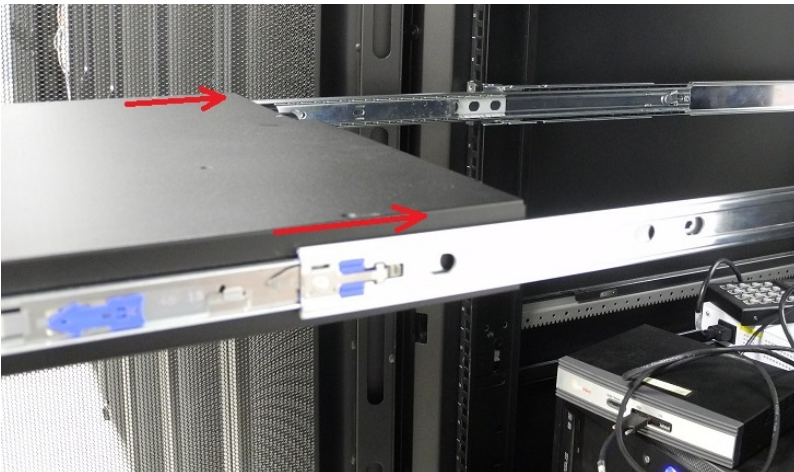
7. The HSM now moves smoothly and securely on the rails. Push the HSM all the way back and secure it to the transformer bracket with four rack screws.

> **NOTE** Screws with heads that are too large can prevent the locking bezel from fitting to the faceplate. Use the screws included with the SafeNet Luna Network HSM, or other screws with suitable heads.

See "Installing the SafeNet Luna Network HSM Hardware" on the next page to continue the installation process.

Installing the SafeNet Luna Network HSM Hardware

This section provides basic SafeNet Luna Network HSM hardware installation instructions (connecting cables, booting, etc.). If you intend to mount the appliance in a standard equipment rack, see "Rack-Mounting the SafeNet Luna Network HSM" on page 19 before following these instructions.

> **NOTE**   Certain security standards require the HSM to be locked in an equipment rack with restricted physical access. If your organization uses such standards, see "Rack-Mounting the SafeNet Luna Network HSM" on page 19.

Installation Notes

> Any computer that is to act as a client to the SafeNet Luna Network HSM appliance must have the Client software installed. Windows users should log in to their computer as a user with Administrator privileges.

> A computer that is to be used only for administering the SafeNet Luna Network HSM does not need the Client software – only an SSH client such as the provided PuTTY program for Windows, or the SSH utilities that come standard with most Linux and UNIX platforms.

> A computer that is to be used for Remote PED workstation operation against a SafeNet Luna Network HSM must have the PEDServer software and PED USB driver installed. Applies to select Windows platforms only.

> All three tasks (Client, administration, and Remote PED) can be performed on a single computer, but in normal practice they are often separate tasks for separate computers.

> See "About Remote PED" on page 1 in the *Administration Guide* if you will be using Remote PED.

Installing the SafeNet Luna Network HSM Hardware

Follow these instructions to install and begin configuring the appliance.

To install the SafeNet Luna Network HSM hardware

1. Insert the power (a) and network (b) cables at the rear panel.

   For proper redundancy and best reliability, the power cables should connect to two completely independent power sources.
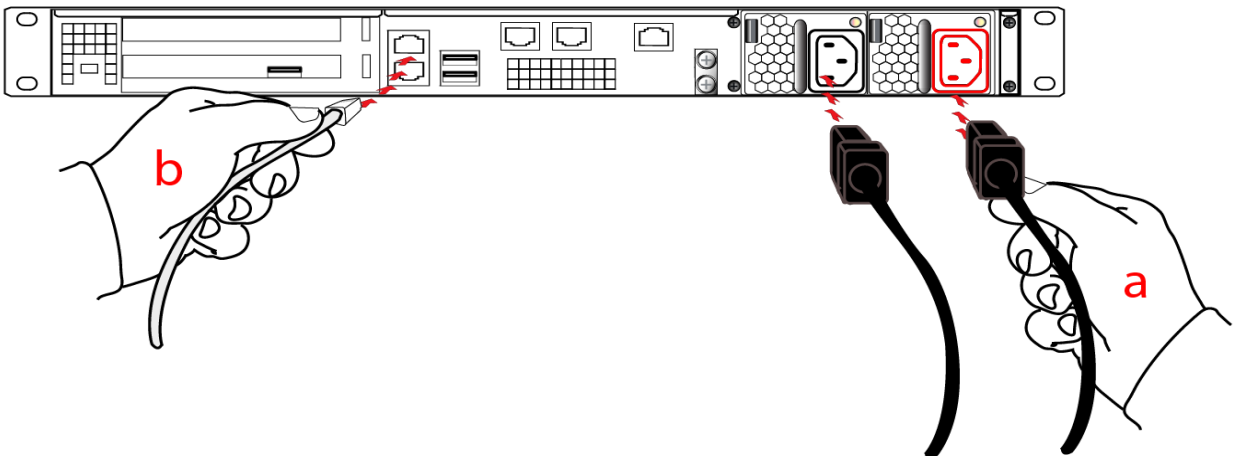
2. If you have a PED-authenticated SafeNet Luna Network HSM, connect the PED directly to the HSM card's USB port (on the rear panel's left side), using the included USB-to-MiniUSB PED cable. See also "Local PED Setup" on page 1 in the *Administration Guide*. If you have a password-authenticated HSM, skip to the next step.
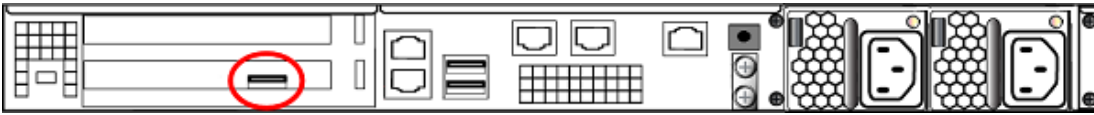
> **NOTE** If you have an older PED, the PED must be connected to a suitable power source. The USB 2.0 connection does not provide enough power to run the PED.
>
> Refreshed-hardware PEDs - identifiable by the part number on the manufacturer's label: 808-000060-002 or 808-000060-003, or by firmware 2.8.0 or later - is powered by the USB connection and does not require a separate, external AC power adapter.

3. Press and release the Start/Stop switch on the front panel.
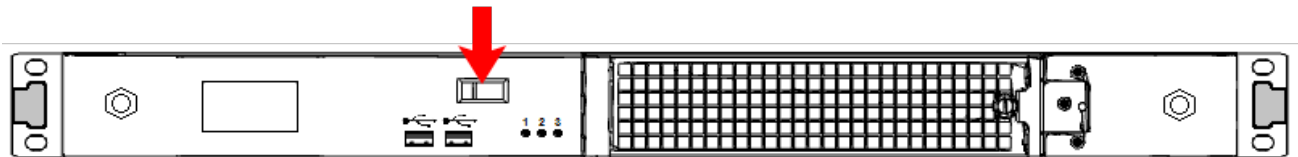
4. Connect the terminal port on the HSM appliance's rear panel to a dumb terminal, PC, or laptop, using the USB-to-RJ45 adapter cable (supplied). This terminal provides serial access to LunaSH for initial network configuration. See "Open a Connection" on page 1 for more information.
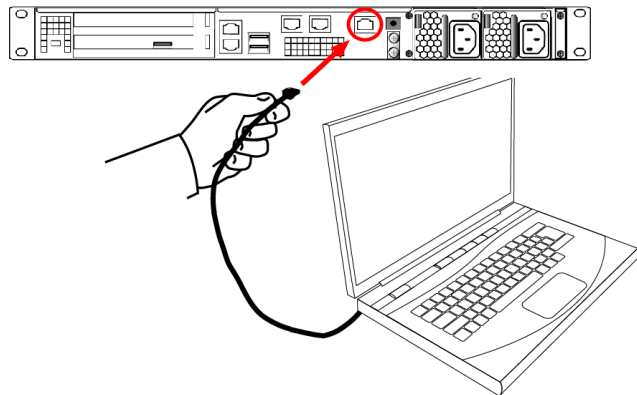
5. If you have already installed SafeNet Luna HSM Client software, consult the *Configuration Guide* to configure your SafeNet Luna Network HSM and peripheral devices, if appropriate.

6. For maximum physical access security, when you are finished configuring the HSM, fit the locking bezel over the HSM's faceplate. Certain security standards require the use of these physical access measures. The locks fit over the posts highlighted below.

Turn the keys to the vertical position to lock the bezel. The keys cannot be removed if the bezel is unlocked. The two locks are keyed differently, so the keys can be issued to different security personnel and kept in secure, separate locations.

> **NOTE** Leaving the keys in the bezel could interfere with closing the rack door, and compromise security.

Installing optional 10 Gigabit Optical Ethernet

If you ordered the 10G Optical Ethernet option, then the two side-by-side RJ45 ports are replaced by optical-ready SFP+ connectors. The SFP optical Ethernet modules are packed separately, within the Network HSM shipping carton.

The original SafeNet Luna Network HSM, with copper-only 1G Ethernet, looks like this (below) at the back panel.

Bond0 — Eth0 Eth1 (1G Copper RJ45)
Bond1 — Eth2 Eth3 (1G Copper RJ45)
Serial (RJ45)
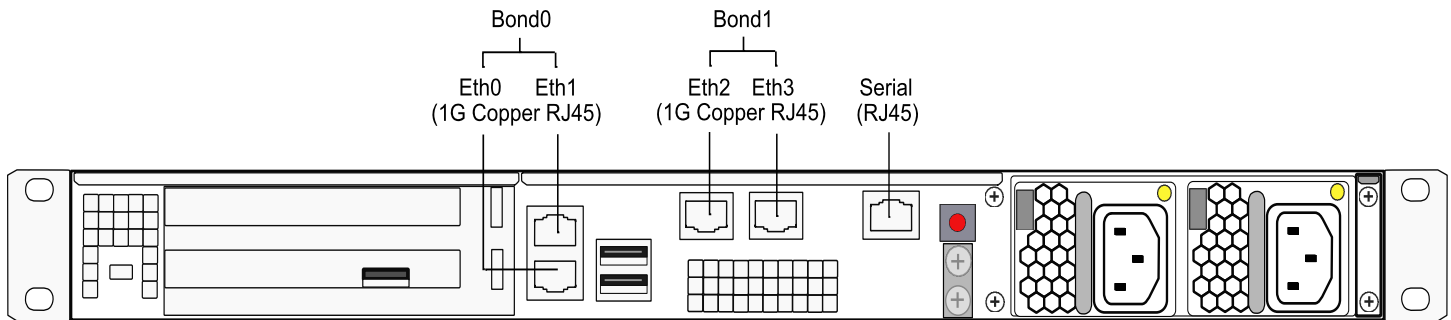
The SafeNet Luna Network HSM with the 10G Optical Ethernet option looks like this, below. The two optical-ready connectors are protected by dust covers during shipping and handling.

> **NOTE**   The physical ports assigned Ethernet port numbers by system software are changed; the new optical ports become Eth0 and Eth1, while the remaining RJ45 1G copper ports are labeled Eth2 and Eth3. This could require change to setup scripting, if you have previously installed and configured Network HSM appliances with copper-only Ethernet ports.

Bond 1 — Eth2 Eth3 (1G copper RJ45)
Bond 0 — Eth0 Eth1 (SFP+ Connectors) Dust covers in place
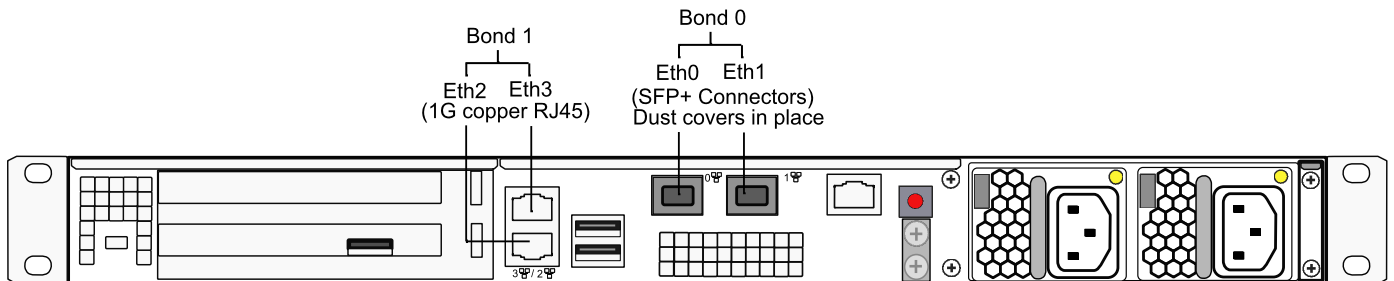
To install the SFP modules

1. Locate the SFP modules in the accessory box, within the Network HSM shipping carton.

2. Remove the dust plug from one of the two SFP+ connectors on the back panel of the Network HSM.

3. Remove an SFP module from its packaging and slide it into the selected connector slot, ensuring that the module seats firmly, making a positive connection at the back of the slot.

10G Optical Module Sockets

Open SFP+ connector

Dust cover (remove to install SFP module)
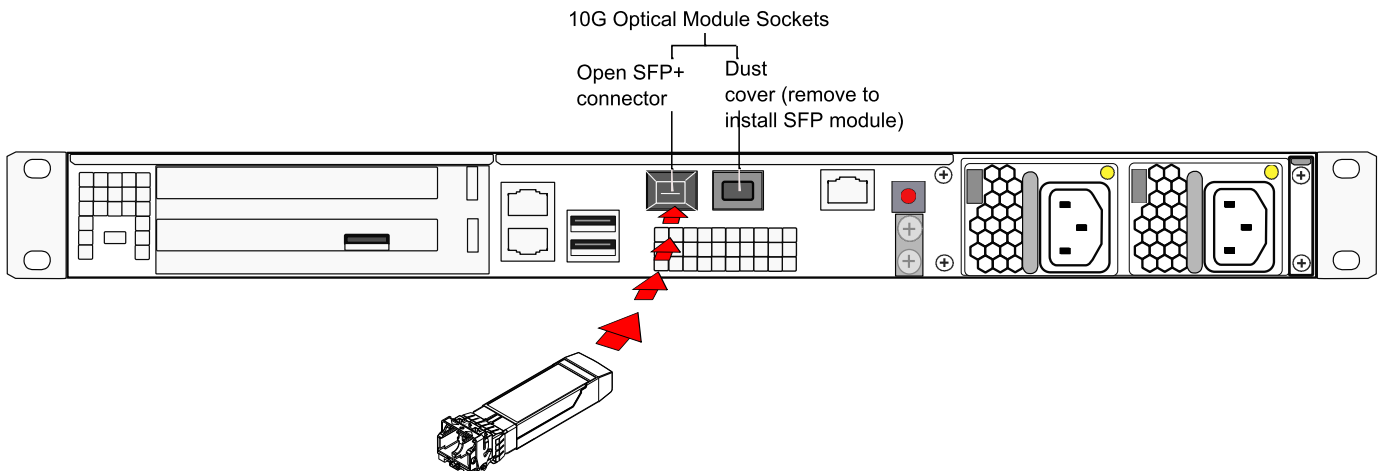
4. Repeat for the other 10G module if desired.

To connect a Dual L-to-L optical cable to an installed 10G SFP module

1. Remove the dust plug from the installed 10G SFP Ethernet module.

2. Insert the dual cable connector as shown.

10G Optical Module installed

Accepts LC-to-LC duplex cable
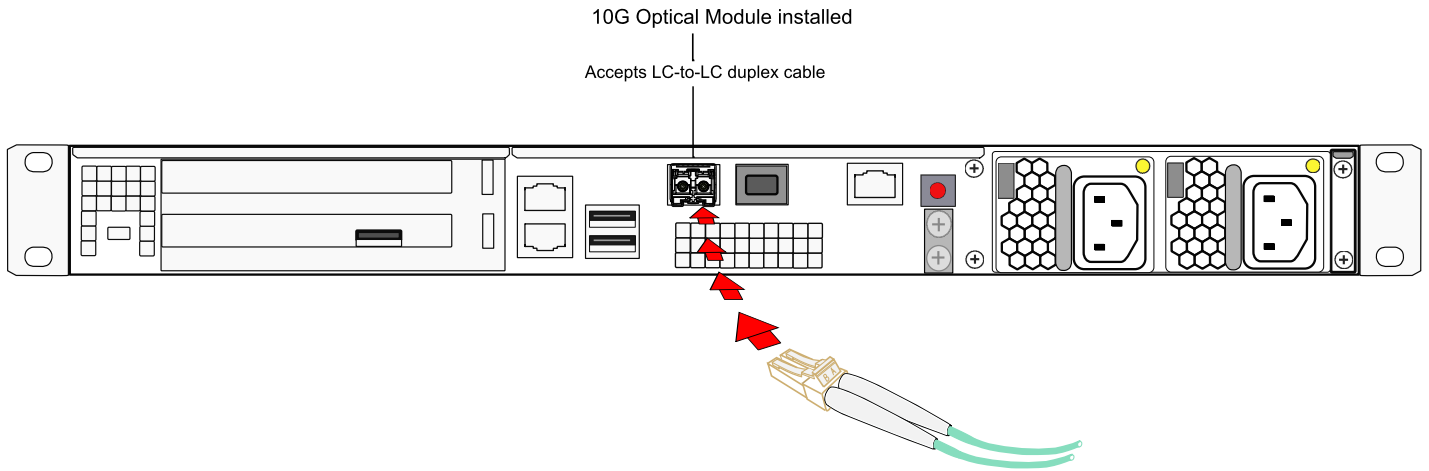
CHAPTER 3:   SafeNet Luna G7-based Backup HSM Hardware Installation

The following topics describe how to install and connect a G7-based SafeNet Luna Backup HSM. To ensure a successful installation, perform the following tasks in the order indicated:

1. Ensure that you have all of the required components, as listed in "SafeNet Luna Backup HSM Received Items" below

2. Install and connect the hardware, as described in "Installing the SafeNet Luna Backup HSM Hardware" on page 33

> **CAUTION!**   To ensure the security and integrity of your new device, refer to "Verifying the Integrity of Your Shipment" on page 10 before unpacking your new SafeNet Luna Backup HSM.

The G7-based SafeNet Luna Backup HSM complies with the following:

R-R-SFN-LG7-01
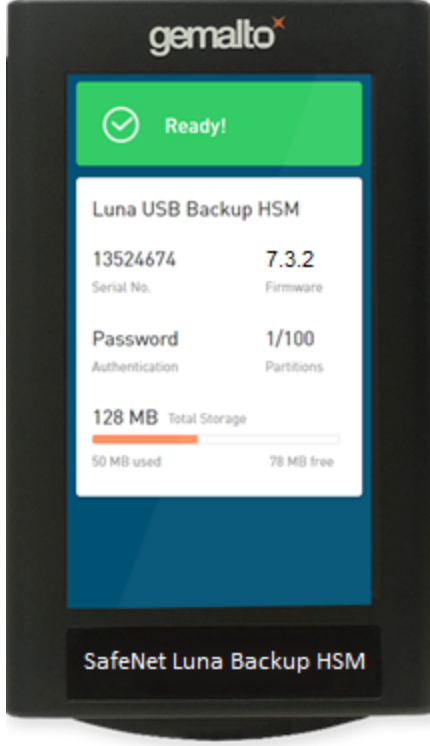
SafeNet Luna Backup HSM Received Items

This section provides a list of the components you should have received with your order.

Included Items
The following items are included with your new backup HSM.

Quantity	Item
1	**SafeNet Luna Backup HSM**
1	**USB 3.0 Cable: Type A to Type C**

Quantity	Item
1	**5V Power Supply** with replaceable plug modules for international use. **NOTE** On most workstations, the USB connection provides adequate power to the backup HSM. If you are using a low-power workstation, such as a netbook, the USB connection may not provide adequate power, in which case you will also need to connect the external power supply.

Installing the SafeNet Luna Backup HSM Hardware

The backup HSM is a USB device. To install the backup HSM, connect it to a SafeNet Luna HSM Client workstation using the included USB cable. The workstation must be running SafeNet Luna HSM Client software that supports the backup HSM and provides the required drivers. Refer to the release notes and see "Backing Up Partition Objects to a G7 Backup HSM" on page 1 in the *Administration Guide* for more information.

> **NOTE** On most workstations, the USB connection provides adequate power to the Backup HSM and it will begin the boot sequence. If you are using a low-power workstation, such as a netbook, the USB connection may not provide adequate power, in which case you will also need to connect the external power supply.

CHAPTER 4:   SafeNet Luna PED Received Items

This chapter describes the items you received with your SafeNet Luna PED device. For instructions on setting up the PED, see "PED Authentication" on page 1 in the *Administration Guide*.

Required Items

The following items are included with your PED. All are required for a successful installation.

Qty	Item
1	**SafeNet Luna PED** (with firmware 2.7.1 or newer)

Qty	Item
1	**PED Power Supply** kit with replaceable mains plug modules for international use (employed when the PED is operated in Remote PED mode) **NOTE:** If your PED has firmware 2.8.0 or newer, it contains refreshed internal hardware and is powered by USB connection. Refreshed PEDs are not shipped with the external power supply, as they do not need it.
1	**Cable, USB 2.0, Type A to Mini B connectors** (for Remote PED operation).

Qty	Item
1	**Cable, Data, 9-pin, Micro-D to Micro-D connectors** (for local PED operation prior to HSM firmware versions 7.x.).
1	**Ten-pack of iKey 1000 PED keys**, and sheets of peel-and-stick labels

CHAPTER 5: SafeNet Luna HSM Client Software Installation

This chapter describes how to install the SafeNet Luna HSM Client software. After installing the hardware, you need to install the SafeNet Luna HSM Client software before you can begin configuring your SafeNet Luna HSM(s).

You can install the client for all SafeNet General Purpose HSMs, or for a specific type (Network or PCIe). Install the client as follows:

> For SafeNet Luna Network HSM, install the SafeNet Luna HSM Client on any computer that must connect to the appliance as a client.

> For SafeNet Luna PCIe HSM, install the SafeNet Luna HSM Client on the workstation into which the SafeNet Luna PCIe HSM is installed.

> For SafeNet Luna USB HSM, install the SafeNet Luna HSM Client on the workstation to which the SafeNet Luna USB HSM is connected.

> Install the SafeNet Luna HSM Client on any computer that is to have a SafeNet Remote PED connected.

Choose the instructions for your operating system:

> For AIX, see "AIX SafeNet Luna HSM Client Installation" on the next page.

> For Linux, see "Linux SafeNet Luna HSM Client Installation" on page 44

> For Solaris, see "Solaris SafeNet Luna HSM Client Installation" on page 65

> For Windows, see "Windows SafeNet Luna HSM Client Installation" on page 71 The following supplemental topic also applies to Windows:

   • "Scripted/Unattended Windows Installation/Uninstallation" on page 81

> "Adding a DPoD HSM on Demand Service" on page 86

> **NOTE** Not all operating systems are supported for each SafeNet Luna HSM type. Refer to the Customer Release Notes (see "Customer Release Notes" on page 6) for the most current information on supported platforms.

AIX SafeNet Luna HSM Client Installation

These instructions assume that you have already acquired the SafeNet Luna HSM Client software, usually in the form of a downloaded .tar archive.

You must install the SafeNet Luna HSM Client software on each client workstation you will use to access a SafeNet Luna HSM. This section describes how to install the client on a workstation running AIX, and contains the following topics:

> "Prerequisites" below

> "Installing the Client Software" below

> "Controlling User Access to Your Attached HSMs and Partitions" on page 41

> "Uninstalling the SafeNet Luna HSM Client Software" on page 42

> "Installing Java" on page 42

> "Scripted or Unattended Installation" on page 42

> "Interrupting the Installation" on page 43

Applicability to specific versions of AIX is summarized in the Customer Release Notes for the current release.

> **NOTE** Before installing a SafeNet system, you should confirm that the product you have received is in factory condition and has not been tampered with in transit. Refer to the Content Sheet included with your product shipment. If you have any questions about the condition of the product that you have received, please contact Thales Group Technical Support.

Prerequisites

Each computer that connects to the SafeNet Luna Network HSM appliance as a Client must have the cryptoki library, the vtl client shell and other utilities and supporting files installed. Each computer that is connected to a SafeNet Luna Remote Backup HSM must have the cryptoki library and other utilities and supporting files installed - in this case, that would be a Windows or Linux computer with the "Luna Backup HSM" option chosen when Luna Client software is installed.

Installing the Client Software

Check the SafeNet Luna HSM Customer Release Notes for any installation-related issues or instructions before you begin the following software installation process.

To install the SafeNet Luna HSM Client software on AIX:

1. Log on to the client system, open a console or terminal window, and use **su** or **sudo** to gain administrative permissions for the installation.

2. If you downloaded the software, copy or move the .tar archive (which usually has a name like "LunaClient_ 7.x.y-nn_AIX.tar") to a suitable directory where you can untar the archive and launch the installation script.

3. Enter the following command to extract the contents from the archive:

   tar xvf <filename>**.tar**

4. Change directory to the software version suitable for your system.

5. Install the client software as follows:

- To see the 'help', or a list of available installer options, type:

  sh install.sh -? or **./sh install.sh --help**

- To install all available products and optional components, type:

  sh install.sh all

- To selectively install individual products and optional components, type the command without arguments:

  sh install.sh

> **NOTE**   Do not interrupt the installation script in progress. An uninterruptible power supply (UPS) is recommended. See "Interrupting the Installation" on page 43 for more information.

6. Type **y** if you agree to be bound by the license agreement:

```
[mylunaclient-1 32]$ sh install.sh

IMPORTANT:  The terms and conditions of use outlined in the software
license agreement (Document #008-010005-001_EULA_HSM_SW_revN) shipped with the product
("License") constitute a legal agreement between you and SafeNet.
Please read the License contained in the packaging of this
product in its entirety before installing this product.

Do you agree to the License contained in the product packaging?

If you select 'yes' or 'y' you agree to be bound by all the terms
and conditions set out in the License.

If you select 'no' or 'n', this product will not be installed.

(y/n)
```

7. A list of installable SafeNet products appears (might be different, depending on your platform). Select as many as you require, by typing the number of each (in any order) and pressing Enter. As each item is selected, the list updates, with a "*" in front of any item that has been selected. This example shows item 1 has been selected.

```
Products
Choose Luna Products to be installed
    *[1]: Luna Network HSM
     [N|n]: Next
     [Q|q]: Quit

Enter selection: 1
```

> **NOTE**   When the above was captured, the AIX client supported only SafeNet Luna Network HSM. To install the SafeNet Luna Backup HSM, you will need one of the other supported host platforms.

8. When selection is complete, type **N** or **n** for "Next", and press **Enter**. If you wish to make a change, simply type a number again and press **Enter** to de-select a single item.

9. The next list is called "Advanced" and includes additional items to install. Some items might be pre-selected to provide the optimum SafeNet Luna HSM experience for the majority of customers, but you can change any selection in the list.

```
Products
Choose Luna Products to be installed
     [1]: Luna Network HSM
     [N|n]: Next
     [Q|q]: Quit

Enter selection: 1

Advanced
Choose Luna Components to be installed

  [1]: Luna SDK

 *[2]: Luna JSP (Java)

 *[3]: Luna JCProv (Java)

  [B|b]: Back to Products selection

  [I|i]: Install

  [Q|q]: Quit

 Enter selection:
```

If you wish to make a change, simply type a number again and press **Enter** to select or de-select a single item.

If the script detects an existing cryptoki library, it stops and suggests that you uninstall your previous SafeNet software before starting the SafeNet Luna HSM Client installation again.

10. The system installs all packages related to the products and any optional components that you selected. By default, the Client programs are installed in the **/usr/safenet/lunaclient** directory.

> **NOTE** When installing, ensure that the full path of a package does not contain any space characters. (The IBM examples do not show any spaces, implying that this might be a system requirement.)

11. Although FMs are supported on Linux and Windows clients only in this release, the FM architecture requires a configuration file setting to allow partition login on an FM-enabled HSM. If the HSM you will be using with this client is FM-enabled (see "Preparing the SafeNet Luna Network HSM to Use FMs" on page 1 for more information), you must add the following entry to the [Misc] section of the Chrystoki.conf file:

[Misc]

LoginAllowedOnFMEnabledHSMs=1

> **NOTE** As a general rule, do not modify the Chrystoki.conf/crystoki.ini file, unless directed to do so by Gemalto Technical Support. If you do modify the file, never insert TAB characters - use individual space characters. Avoid modifying the PED timeout settings. These are now hardcoded in the appliance, but the numbers in the Chrystoki.conf file must match.

Controlling User Access to Your Attached HSMs and Partitions

By default, only the root user has access to your attached HSMs and partitions. You can specify a set of non-root users that are permitted to access your attached HSMs and partitions, by adding them to the **hsmusers** group.

> **NOTE** The client software installation automatically creates the hsmusers group if one does not already exist on your system. The hsmusers group is retained when you uninstall the client software, allowing you to upgrade your client software while retaining your hsmusers group configuration.

Adding users to hsmusers group

To allow non-root users or applications access your attached HSMs and partitions, assign the users to the **hsmusers** group. The users you assign to the hsmusers group must exist on the client workstation. Users you add to the hsmusers group are able to access your attached HSMs and partitions. Users who are not part of the hsmusers group are not able to access your attached HSMs and partitions.

To add a user to hsmusers group

1. Ensure that you have **sudo** privileges on the client workstation.

2. Add a user to the hsmusers group:

   sudo gpasswd --add <username> **hsmusers**

   where <username> is the name of the user you want to add to the hsmusers group.

Removing users from hsmusers group

Should you wish to rescind a user's access to your attached HSMs and partitions, you can remove them from the hsmusers group.

> **NOTE** The user you delete will continue to have access to the HSM until you reboot the client workstation.

To remove a user from hsmusers group

1. Ensure that you have **sudo** privileges on the client workstation.

2. Remove a user from the hsmusers group:

   sudo gpasswd -d <username> **hsmusers**

   where <username> is the name of the user you want to remove from the hsmusers group. You must log in again to see the change.

Uninstalling the SafeNet Luna HSM Client Software

You may need to uninstall the SafeNet Luna HSM Client software prior to upgrading to a new release, or if the software is no longer required.

To uninstall the SafeNet Luna HSM Client software:

1. Log in as root. (use sudo instead)

2. Go to the client installation directory:

   cd /usr/safenet/lunaclient/bin

3. Run the uninstall script:

   sudo sh uninstall.sh

Installing Java

If you install the Luna Java Security Provider (JSP), refer to SafeNet JSP Overview and Installation for additional setup procedures for your operating system.

Scripted or Unattended Installation

If you prefer to run the installation from a script, rather than interactively, run the command with the options **-p** <list of SafeNet products> and **-c** <list of SafeNet components>. To see the syntax, run the command with **help** like this:

```
[myhost]$ sudo sh install.sh help
[sudo] password for fred

At least one product should be specified.

usage:
        install.sh      - Luna Client install through menu
        install.sh help - Display scriptable install options
        install.sh all  - Complete Luna Client install

        install.sh -p [sa|pci|g5|rb] [-c sdk|jsp|jcprov|ldpc|snmp]

        -p <list of Luna products>
        -c <list of Luna components>  - Optional. All components are installed if not provided

Luna products options
    sa     - SafeNet Luna Network HSM
    pci    - SafeNet Luna PCIe HSM
    g5     - SafeNet Luna USB HSM
    rb     - SafeNet Luna Backup HSM

Luna components options
    sdk    - Luna SDK
    jsp    - Luna JSP (Java)
    jcprov - Luna JCPROV (Java)
    snmp   - Luna SNMP subagent


[myhost]$
```

For scripted/automated installation, your script will need to capture and respond to the License Agreement prompt, and to the confirmation prompt. For example:

```
[myhost]$ sudo sh install.sh all

IMPORTANT: The terms and conditions of use outlined in the software
license agreement (Document #008-010005-001_053110) shipped with the product
("License") constitute a legal agreement between you and SafeNet Inc.
Please read the License contained in the packaging of this
product in its entirety before installing this product.

Do you agree to the License contained in the product packaging?

If you select 'yes' or 'y' you agree to be bound by all the terms
and conditions se out in the License.

If you select 'no' or 'n', this product will not be installed.

(y/n) y

Complete SafeNet Luna HSM Client will be installed. This includes SafeNet Luna Network HSM,
SafeNet Luna PCIe HSM, SafeNet Luna USB HSM AND SafeNet Luna Backup HSM.

Select 'yes' or 'y' to proceed with the install.

Select 'no' or 'n', to cancel this install.

Continue (y/n)?  y
```

Interrupting the Installation

Do not interrupt the installation script in progress, and ensure that your host computer is served by an uninterruptible power supply (UPS). If you press [Ctrl] [C], or otherwise interrupt the installation (OS problem, power outage, other), some components will not be installed. It is not possible to resume an interrupted install process. The result of an interruption depends on where, in the process, the interruption occurred (what remained to install before the process was stopped).

As long as the cryptoki RPM package is installed, any subsequent installation attempt results in refusal with the message "A version of SafeNet Luna HSM Client is already installed."

If components are missing or are not working properly after an interrupted installation, or if you wish to install any additional components at a later date (following an interrupted installation, as described), you would need to uninstall everything first. If **sh uninstall.sh** is unable to do it, then you must uninstall all packages manually.

Because interruption of the install.sh script is not recommended, and mitigation is possible, this is considered a low-likelihood corner case, fully addressed by these comments.

After Installation

When you have installed the software onto a Client, the next task is to configure the SafeNet Luna HSM, as described in the *Configuration Guide*.

Linux SafeNet Luna HSM Client Installation

You must install the SafeNet Luna HSM Client software on each client workstation you will use to access a SafeNet Luna HSM. This section describes how to install the client on a workstation running Linux, and contains the following topics:

Refer to the Customer Release Notes for a complete list of the supported Linux operating systems. These instructions assume that you have already acquired the SafeNet Luna HSM Client software.

Prerequisites

Before starting the installation, ensure that you have satisfied the following prerequisites:

Components Required to Build the PCIe Driver and the Backup HSM Driver
On Linux, the PCIe driver module (and optionally the Backup HSM driver) is built by the client as part of the installation if you choose to install the Luna PCIe HSM component or the Backup HSM. To build the driver, the client requires the following items:

> Kernel headers for build

> kernel-devel package

> rpmbuild package

> C and C++ compilers

> make command

If any one of these items is missing, the driver build will fail and the client software will not be installed.

> **NOTE**   The installed *kernel* and *kernel-devel* versions on the Client system must match, in order for the drivers to compile successfully. In general, if the versions do not match, or if you are not sure, use this command **yum install kernel-devel-`uname -r`** before installing SafeNet Luna HSM Client. Note the required backticks, (the key to the left of the 1/! key on the keyboard) surrounding **`uname –r`** (or equivalent command **yum install kernel-devel-$(uname -r)**).
>
> To check installed versions related to the currently running kernel: **rpm -qa kernel * | grep $(uname -r)**.

Debian Requires alien

The SafeNet Luna HSM Client software is provided as RPM packages. If you are installing on a Debian system, you must have **alien** installed to allow the SafeNet Luna HSM Client installation script to convert the RPM packages to DEB packages. The installation script will stop with a message if you attempt to install on a Debian system without **alien** installed. This applies to any other supported Debian-based Linux distribution, such as Ubuntu.

SUSE Linux on IBM PPC

JCE un-restriction files must be downloaded from IBM, not from SUN, for this platform. Attempting to use SUN JCE un-restriction files on IBM PowerPC systems with SUSE Linux causes signing errors.

Installing the Client Software

It is recommended that you refer to the SafeNet Luna HSM Customer Release Notes for any installation-related issues or instructions before installing the client software.

> **CAUTION!**   You must install the client software using root-level privileges. For security reasons, we recommend that you do not log in as root (or use su root) to run the installation script, but instead use the sudo command to run the installation script, as detailed below.

The installation script

The installation script is **install.sh** and is usually launched with **sh install.sh** followed by any options or parameters.

> interactive: **sh install.sh** [**-install_directory** <prefix>]

> all: **sh install.sh all** [**-install_directory** <prefix>]

> scriptable: **sh install.sh -p** [**network**|**pci**|**usb**|**backup**|**ped**] [**-c sdk**|**jsp**|**jcprov**|**ldpc**|**snmp**] [**-install_ directory** <prefix>]

The options on the script are:

> device(s)

  • "network" is the SafeNet Luna Network HSM (software only, no drivers)

  • "pci" is the SafeNet Luna PCIe HSM (software plus driver for the PCI HSM)

  • "usb" is the SafeNet Luna USB and Backup HSMs (software plus driver for the G5-based and G7-based HSMs)

  • "backup" is software to enable Remote Backup

  • "ped" is software for the SafeNet Luna Remote PED

> components include the optional Software Development kit, Java providers, SNMP instance (not needed for Network HSM which has it built in)

By default, the Client programs are installed in the **/usr/safenet/lunaclient** directory.

Flexible Install paths

You can change the installation path for scriptable (non-interactive) installs by changing the prefix with the script option **-install_directory** <prefix>

The prefix, or major location is your choice, and replaces the /usr default portion.

> **NOTE** Avoid the use of space characters in directory names.

The script option **-install_directory** <prefix> is available for scriptable installation, where either "all" or a list of products and components is specified on the command line. The script option **-install_directory** <prefix> is not used with interactive installation; instead, you are prompted.

The **/safenet/lunaclient** portion is appended by the install script, and provides a predictable structure for additional subdirectories to contain certificate files, and optionally STC files.

Regardless of **-install_directory** <prefix> provided, some files are not affected by that option (for example, the Chrystoki.conf configuration file goes under /etc, service files need to be in the service directory expected by Linux in order to run at boot time, and so on).

To install the SafeNet Luna HSM Client software on a Linux workstation

1. Ensure that you have **sudo** privileges on the client workstation.

2. Access the installation software:

   Copy or move the **.tar** archive to a suitable directory where you can untar the archive and extract the contents:

   tar xvf <filename>**.tar**

3. Go to the untarred directory for your operating system (**32** or **64**-bit):

   cd /<untarred_dir>**/**<**32**/**64**>

4. To install the software, run the **install.sh** installation script. You can run the script in interactive mode, or you can script the installation, as described in "Scripted or Unattended Installation" on page 50.

   - To display the help, or a list of available installer options, type:

     sudo sh install.sh -? or **sudo sh install.sh help**

   - To install all available products and optional components, type:

     sudo sh install.sh all

   - To selectively install individual products and optional components, type the command without arguments:

     sudo sh install.sh

   > **NOTE** Do not interrupt the installation script in progress. An uninterruptible power supply (UPS) is recommended. See "Interrupting the Installation" on page 51 for more information.

5. Type **y** if you agree to be bound by the license agreement. You must accept the license agreement before you can install the software.

6. A list of installable SafeNet devices is displayed. Select as many as you require, by typing the number of each (in any order) and pressing **Enter**. As each item is selected, the list updates, with a ***** in front of any item that has been selected.

This example shows items 1 and 3 have been selected, and item 4 is about to be selected. The selections work as a toggle - if you wish to make a change, simply type a number again and press **Enter** to de-select it.

```
Products
Choose Luna Products to be installed

    *[1]: Luna Network HSM

     [2]: Luna PCIe HSM

    *[3]: Luna USB HSM

     [4]: Luna Backup HSM

     [5]: Luna Remote PED

     [N|n]: Next

     [Q|q]: Quit
Enter selection: 4
```

When selection is complete, type **N** or **n** for "Next", and press **Enter**. The "Advanced" menu is displayed.

```
Advanced
Choose Luna Components to be installed

   [1]: Luna SDK

   [2]: Luna JSP (Java)

   [3]: Luna JCProv (Java)

   [4]: Luna SNMP subagent

   [5]: Luna Functionality Module Tools

   [6]: Luna Functionality Module Software Development Kit

   [B|b]: Back to Products selection

   [I|i]: Install

   [Q|q]: Quit

 Enter selection:
```

7. Select or de-select any additional items you want to install. Selected items are indicated with a *****. Some items might be pre-selected to provide the optimum experience for the majority of customers, but you can change any selection in the list. When the Components list is adjusted to your satisfaction, press **Enter**.

> **NOTE**   The installer includes the Luna SNMP Subagent as an option. If you select this option, you will need to move the SafeNet MIB files to the appropriate directory for your SNMP application after installation is complete, and you will need to start the SafeNet subagent and configure it for use with your agent. See the *Administration Guide* for more information.
>
> **Luna SDK required with FMs** - If you choose the Functionality Module (FM) options, the interactive install.sh script populates the Luna SDK as well, because of dependencies in the FM samples. If you run the installer with command-line options (non-interactive), and you choose FM items without also choosing Luna SDK, the script just gives a warning and stops.
>
> ELDK (the Embedded Linux Development Kit) is installed with FMs - The ELDK package is installed as part of the FM SDK component, for Linux, and must reside at /opt/eldk-5.6. It is not relocatable.

If the script detects an existing cryptoki library, it stops and suggests that you uninstall your previous SafeNet software before starting the SafeNet Luna HSM Client installation again.

8. The system installs all packages related to the products and any optional components that you selected.

9. [Optional] For easy use of the SafeNet Luna HSM Client tools, add their directories to the $PATH.

    a. Edit your system's **bash_profile** file using an editing tool.

        vi ~/.bash_profile

    b. Add the following lines to the end of the file:

        export PATH="$PATH:/usr/safenet/lunaclient/bin"

        export PATH="$PATH:/usr/safenet/lunaclient/sbin"

    c. Source the updated **bash_profile**.

        source ~/.bash_profile

Installing the Minimal Client Software

The minimal client package contains the minimum run-time libraries required for a cryptography application to connect to SafeNet Network HSM using PKCS#11 or Java APIs, or Functionality Modules on an FM-enabled HSM. Minimal client install is intended for container instances to interact with SafeNet HSM partitions or services.

Installing is as simple as copying the tarball and untarring it where you want it. A copy of a configured Chrystoki.conf file, along with client and server certificate files (and optionally, STC configuration files) must be available to any instance of Luna Minimal Client at run time.

See for a general example using Docker.

Controlling User Access to Your Attached HSMs and Partitions

By default, only the root user has access to your attached HSMs and partitions. You can specify a set of non-root users that are permitted to access your attached HSMs and partitions, by adding them to the **hsmusers** group.

> **NOTE** The client software installation automatically creates the hsmusers group if one does not already exist on your system. The hsmusers group is retained when you uninstall the client software, allowing you to upgrade your client software while retaining your hsmusers group configuration.

Adding users to hsmusers group

To allow non-root users or applications access your attached HSMs and partitions, assign the users to the **hsmusers** group. The users you assign to the hsmusers group must exist on the client workstation. Users you add to the hsmusers group are able to access your attached HSMs and partitions. Users who are not part of the hsmusers group are not able to access your attached HSMs and partitions.

To add a user to hsmusers group

1. Ensure that you have **sudo** privileges on the client workstation.

2. Add a user to the hsmusers group:

    sudo gpasswd --add <username> **hsmusers**

    where <username> is the name of the user you want to add to the hsmusers group.

Removing users from hsmusers group

Should you wish to rescind a user's access to your attached HSMs and partitions, you can remove them from the hsmusers group.

> **NOTE** The user you delete will continue to have access to the HSM until you reboot the client workstation.

To remove a user from hsmusers group

1. Ensure that you have **sudo** privileges on the client workstation.

2. Remove a user from the hsmusers group:

    sudo gpasswd -d <username> **hsmusers**

    where <username> is the name of the user you want to remove from the hsmusers group. You must log in again to see the change.

Uninstalling the Client Software or Removing Components

You may need to uninstall the client software before upgrading to a new version, or if it is no longer required.

To uninstall the client software

1. Ensure that you have **sudo** privileges on the client workstation.

2. Go to the client installation directory:

    cd /usr/safenet/lunaclient/bin

3. Run the uninstall script:

    sudo sh uninstall.sh

> **CAUTION!** The hsmusers group is not removed when the client software is uninstalled. Should you install the client again on the same system, all users previously in the group will have access to your attached HSMs and partitions by default. You must remove users from the group if you want to restrict their access. See "Removing users from hsmusers group" on the previous page.

To remove individual components

To uninstall the JSP component or the SDK component, you must uninstall SafeNet Luna HSM Client completely, then re-run the installation script without selecting the unwanted component(s).

Java

If you install the Luna Java Security Provider (JSP), refer to SafeNet JSP Overview and Installation for additional setup procedures for your operating system.

Scripted or Unattended Installation

If you prefer to run the installation from a script, rather than interactively, run the command with the options **-p** <list of SafeNet products> and **-c** <list of SafeNet components>. To see the syntax, run the command with **help** like this:

```
[myhost]$ sudo sh install.sh help
[sudo] password for fred

At least one product should be specified.

usage:
        install.sh      - Luna Client install through menu
        install.sh help - Display scriptable install options
        install.sh all  - Complete Luna Client install

        install.sh -p [network|pci|usb|backup|ped] [-c sdk|jsp|jcprov|ldpc|snmp]

        -p <list of Luna products>
        -c <list of Luna components>  - Optional. All components are installed if not provided

Luna products options
   network - Luna Network HSM
   pci     - Luna PCIe HSM
   usb     - Luna USB HSM
   backup  - Luna Backup HSM
   ped     - Luna Remote PED

Luna components options
   sdk     - Luna SDK
   jsp     - Luna JSP (Java)
   jcprov  - Luna JCPROV (Java)
   snmp    - Luna SNMP subagent


[myhost]$
```

For scripted/automated installation, your script will need to capture and respond to the License Agreement prompt, and to the confirmation prompt. For example:

```
[myhost]$ sudo sh install.sh all

IMPORTANT: The terms and conditions of use outlined in the software
license agreement (Document #008-010005-001_053110) shipped with the product
("License") constitute a legal agreement between you and SafeNet Inc.
Please read the License contained in the packaging of this
product in its entirety before installing this product.

Do you agree to the License contained in the product packaging?

If you select 'yes' or 'y' you agree to be bound by all the terms
and conditions se out in the License.

If you select 'no' or 'n', this product will not be installed.

(y/n) y


Complete Luna Client will be installed. This includes SafeNet Luna Network HSM,
SafeNet Luna PCIe HSM, SafeNet Luna USB HSM, SafeNet Luna Backup HSM and SafeNet Luna Remote PED.

Select 'yes' or 'y' to proceed with the install.

Select 'no' or 'n', to cancel this install.

Continue (y/n)?  y
```

Interrupting the Installation

Do not interrupt the installation script in progress, and ensure that your host computer is served by an uninterruptible power supply (UPS). If you press [CTRL] [C], or otherwise interrupt the installation (OS problem, power outage, other), some components will not be installed. It is not possible to resume an interrupted install process. The result of an interruption depends on where, in the process, the interruption occurred (what remained to install before the process was stopped).

As long as the cryptoki RPM package is installed, any subsequent installation attempt results in refusal with the message "A version of SafeNet Luna HSM Client is already installed."

If components are missing or are not working properly after an interrupted installation, or if you wish to install any additional components at a later date (following an interrupted installation, as described), you would need to uninstall everything first. If **sh uninstall.sh** is unable to do it, then you must uninstall all packages manually.

Luna Minimal Client Install for Linux - Overview

Minimal client install is intended for container instances to interact with SafeNet Luna HSM partitions, and contains the minimum run-time libraries required for a cryptography application to connect to SafeNet Luna Network HSM using PKCS#11 or Java APIs, in addition to some configuration tools. The Luna Minimal Install is provided as a tarball that you can unpack where desired, and choose the files that you need.

> **NOTE**   The minimal client does not have an installer, and **omits** drivers and other material, for backup HSMs, for Luna PED, or for the SafeNet Luna PCIe HSM. For any of those, you would use the full SafeNet Luna HSM Client Installer.

Mandatory files for configuration and secure communication, where to get them and where to keep them

The SafeNet Luna Minimal Client, when installed on minimalist or micro-service containers, requires that you have the appropriate files and folders available

> Chrystoki.conf configuration file (includes settings, and pointers to resources),

> certificates folders (for secure communications protocols, NTLS or STC)

> libraries and plugins required for secure communications protocols.

The Luna Minimal Client tarball includes a "template" version of the Chrystoki.conf file that you can edit for any non-default settings needed by your application, and to reflect the actual paths to resources.

Alternatively, you might already have a configured Chrystoki.conf file that you can copy into the Docker container with the minimal client, or that you can leave at an external location that is mountable from within the Docker container.

Similarly, the Docker container with the minimal client must have access to the certificates (local host certificate, and certificates from any registered application partitions or SafeNet Data Protection on Demand (DPoD)'s HSM on Demand services) for secure communication. Those can reside inside the container, or can reside on an external mountable drive - either way, the paths in the Chrystoki.conf file must point to their location.

Configure and link, inside your Docker container
You will need to untar the Minimal Client tarball in your container, or open it elsewhere and copy the desired files to your container.

If you already have a Chrystoki.conf file with most, or all, of your desired settings, you can copy it into the container and edit it manually.

If you do not have suitable Chrystoki.conf file, the minimal client tarball contains a config template file that you can modify with the configurator utility.

At the same time, you can create and exchange certificates by means of the included vtl utility. Ensure that the resulting certificates are pointed-to in Chrystoki.conf file. For example instructions, see "Installing Luna Minimal Client on Linux Using Docker" on page 57.

Configure and link, exterior to your Docker container
To configure Chrystoki.conf and to establish an NTLS or STC link outside your Docker container, for later use by one-or-more Docker containers, you can

> Untar the Luna Minimal Client tarball at the desired staging location, use configurator or manually edit the Chrystoki.conf file, and use vtl to establish the secure link to SafeNet Luna Network HSM appliance.

   OR

> Install the full SafeNet Luna HSM Client, and follow the instructions in the Configuration Guide to create/update the Chrystoki.conf file, and create and exchange certificates for a secure link to a Network HSM appliance.

The above could be done before the Docker container is created, or after one exists.

Whether you elect to pre-configure externally, with a full SafeNet Luna HSM Client Installation or with a copy of the Luna Minimal Client, or from inside each Docker container after it is created (and populated and configured with the Luna Minimal Client), two general networking approaches are possible:

[Network OPTION] Dynamic *private* IP address per container

If each Docker container (default) has a *private* IP address dynamically assigned to the container at run time:

- A single set of configuration file and certificate folders is needed, that will apply to any container within that hidden/translated subnet.

- Each container can mount the needed configuration from the one location on the host.

- Because all containers have the same IP address and appear as the same client, you must *disable* **ntls ipchecking** on the SafeNet Luna Network HSM appliance.

[Network OPTION] Unique *public* IP address per container

If a unique *public* IP address is assigned to each Docker container, visible to the SafeNet Luna Network HSM appliance:

- A separate NTLS configuration is performed, either externally on the host computer, for each proposed container IP, with the resulting configuration file and certificates folders saved to unique mountable locations on the host file system, OR configuration and certificate exchange is performed from the minimal client within each container after it is created.

- Each container gets its own configuration file and unique certificates whether mounted externally or residing inside the container.

- Because each container has its own unique public IP address, and is considered its own client, keep **ntls ipcheck** *enabled* on the SafeNet Luna Network HSM appliance.

DPoD

With the additional tools included in the minimal install archive, as of release 7.6, the expanded minimal client has the needed tools for local (in-container) configuration. If you intend to connect with DPoD's HSM-on-Demand services, see "From Linux Minimal Client Create a Docker Container to Access a DPOD HSM on Demand Service" on page 61 for additional steps.

Included in the Minimal Client

The following components are included in the SafeNet Luna Minimal Client tar ball:

Component	Used or needed for...
JCPROV	
LunaClient-Minimal-<release_version>**.x86_64/jcprov/jcprov.jar**	JCPROV jar file
LunaClient-Minimal-<release_version>**.x86_64/jcprov/64/libjcprov.so**	JCPROV library

Component	Used or needed for...
JSP	
LunaClient-Minimal-<release_version>**.x86_64/jsp/LunaProvider.jar**	JSP jar file
LunaClient-Minimal-<release_version>**.x86_64/jsp/64/libLunaAPI.so**	JSP library
LIBRARIES	
LunaClient-Minimal-<release_version>**.x86_64/libs/64/libCryptoki2.so**	Library to address cryptographic functions of the HSM
LunaClient-Minimal-<release_version>**.x86_64/libs/64/libCryptoki2_64.so**	Symbolic link pointing to libCryptoki2.so, needed for FM hostapps compiled against libCryptoki2_64.so
LunaClient-Minimal-<release_version>**.x86_64/libs/64/libethsm.so**	Library to interact with Functionality Modules
LunaClient-Minimal-<release_version>**.x86_64/libs/64/libSoftToken.so**	Library for STC connection (alternative to NTLS)
LunaClient-Minimal-<release_version>**.x86_64/libs/64/libcklog2.so**	Logging library - invoked by **vtl cklog enable** command to log commands before passing them to the cryptoki library and the HSM.
PLUG-INS	
LunaClient-Minimal-<release_version>**.x86_64/plugins/libdpod.plugin**	Enable connection protocol with DPoD services (See also the related XTC and REST sections of chrystoki.conf file)
CONFIGURATION FILES	
LunaClient-Minimal-<release_version>**.x86_64/Chrystoki-template.conf**	Chrystoki.conf template in case you don't already have a conf file.
LunaClient-Minimal-<release_version>**.x86_64/openssl.cnf**	Configuration file for OpenSSL.
BINARIES/TOOLS	

Component	Used or needed for...
LunaClient-Minimal-<release_version>**.x86_ 64/bin/64/mkfm**	Allow client to connect to Functionality Modules (if you have installed any in the HSM)
LunaClient-Minimal-<release_version>**.x86_ 64/bin/64/configurator**	Configuration file management tool
LunaClient-Minimal-<release_version>**.x86_ 64/bin/64/ckdemo**	Demonstrates individual, atomic, PKCS#11 operations in the HSM
LunaClient-Minimal-<release_version>**.x86_ 64/bin/64/lunacm**	Partition administration tool
LunaClient-Minimal-<release_version>**.x86_ 64/bin/64/cmu**	Certificate Management Utility
LunaClient-Minimal-<release_version>**.x86_ 64/bin/64/multitoken**	Perform multiple crypto commands on multiple slots
LunaClient-Minimal-<release_version>**.x86_ 64/bin/64/pscp** **LunaClient-Minimal-**<release_version>**.x86_ 64/bin/64/plink**	Used for One Step NTLS
LunaClient-Minimal-<release_version>**.x86_ 64/bin/64/salogin**	Persistent application connection tool
LunaClient-Minimal-<release_version>**.x86_ 64/bin/64/vtl**	Configuration tool (certificate creation and exchange, registration of clients with partitions, logging, etc.)
LICENSE AGREEMENT	
LunaClient-Minimal-<release_version>**.x86_64/008- 010068-001 _EULA_HSM7_SW_revB.pdf**	
LunaClient-Minimal-<release_version>**.x86_64/008- 010068-001 _EULA_HSM7_SW_revB.txt**	

The configuration template file is included, in case you wish to populate it via direct editing (perhaps by script). Otherwise, a configuration file is created and modified when you perform a full (non-minimal) installation and configuration elsewhere, and you can simply have your Docker containers mount the external location to make use of the resulting chrystoki.conf file and certificate folders.

Installation Prerequisites

Ensure that you have the following prerequisites before installing the SafeNet Luna Minimal Client:

> A Linux host system with Docker installed (see https://www.docker.com/ for Docker download and install)

> A copy of the Luna Minimal Client tarball package

> A SafeNet Luna Network HSM 7.x appliance, already initialized and ready to use (or an account for access to DPoD HSM on Demand services) -- follow the instructions in the Configuration Guide (see "Planning Your Configuration" on page 1) to perform any of the actions not already done:

  • Configure the SafeNet Luna Network HSM network settings.

  • Initialize the HSM.

  • Create an application partition on the Network HSM.

  • Exchange host certificates between SafeNet Luna HSM Client and the SafeNet Luna Network HSM and register each with the other (On the client side, add the Network HSM's certificate to the server certs folder and to the CAFile. On the Network HSM, register the client with lunash:>**client register**).

  • Start the NTLS service on the appliance with lunash:>**service restart ntls**, and assign the client to the application partition with lunash:>**client assign partition**.

  • On the client side, use LunaCM to configure the application partition (see "Configure Application Partitions" on page 1), initializing the partition and creating roles as appropriate.

  • After configuring SafeNet Luna HSM Client on a host system, edit the Chrystoki.conf file for use in containers, as described in "Preparing the Configuration File for Use with Luna Minimal Client and Docker" below below.

> A working knowledge of Docker.

Preparing the Configuration File for Use with Luna Minimal Client and Docker

Make the following edits to the Chrystoki.conf file before using it in the containers:

1. Change all the library paths (for example LibUNIX64) to **/usr/local/luna/libs/64**

2. Change the certificate and client token paths to the the directory you are making available to the containers at run-time (for example **/usr/local/luna/config/certs**)

Entry in Chrystoki.conf	Value in the host system	Value in the containers
ClientPrivKeyFile	/usr/safenet/lunaclient/cert/client	/usr/local/luna/config/certs
ClientCertFile	/usr/safenet/lunaclient/cert/client	/usr/local/luna/config/certs
ServerCAFile	/usr/safenet/lunaclient/cert/server	/usr/local/luna/config/certs/
PartitionPolicyTemplatePath	/usr/safenet/lunaclient/data/partition_policy_templates	/usr/local/luna/config/ppt/partition_policy_templates
LibUNIX64	/usr/safenet/lunaclient/lib/libCryptoki2_64.so	/usr/local/luna/libs/64/libCryptoki2.so
ClientTokenLib	/usr/safenet/lunaclient/lib/libSoftToken.so	/usr/local/luna/libs/64/libSoftToken.so

Entry in Chrystoki.conf	Value in the host system	Value in the containers
SoftTokenDir	/usr/safenet/lunaclient/configData/token	/usr/local/luna/config/stc/token
ClientIdentitiesDir	/usr/safenet/lunaclient/data/client_identities	/usr/local/luna/config/stc/client_identities
PartitionIdentitiesDir	/usr/safenet/lunaclient/data/psrtition_identities	/usr/local/luna/config/stc/partition_identities
ToolsDir	/usr/safenet/lunaclient/bin	/usr/local/luna/bin/64
SSLConfigFile	/usr/safenet/lunaclient/bin/openssl.cnf	/usr/local/luna/openssl.cnf

Ready to Install Minimal Client

For detailed instructions, see "Installing Luna Minimal Client on Linux Using Docker" below.

For additional instructions on using the minimal client with Functionality Modules, see "Create a SafeNet Luna HSM Client Docker image for use with Functionality Modules " on page 62.

For additional instructions on using the minimal client with DPoD HSM on Demand services, see "From Linux Minimal Client Create a Docker Container to Access a DPOD HSM on Demand Service" on page 61.

Installing Luna Minimal Client on Linux Using Docker

The following procedure allows you to install the Luna Minimal Client in a Docker container on Linux, so that applications in that container can access SafeNet Luna Network HSM   partitions. For an overview description of Luna Minimal Client and its prerequisites, see "Luna Minimal Client Install for Linux - Overview" on page 51.

> **NOTE**   If SELinux is enabled in Enforcing mode, you must assign proper permissions to any container that needs to access the config directory.

To install the SafeNet Luna Minimal Client software on a Linux 64-bit Docker instance:

This example uses NTLS. The use of STC is optional.
This example is based on CentOS 7; other operating systems might require adjustments to the commands and to the docker file.

1. Create a directory. In this example:

   ```
   $HOME/luna-docker
   ```

   The name is not important, only that you use it consistently.

2. Create the following subdirectories under that first directory:

   ```
   $HOME/luna-docker/config
   $HOME/luna-docker/config/certs
   ```

   additionally, if you are configuring STC:

```
$HOME/luna-docker/config/stc
$HOME/luna-docker/config/stc/client_identities
$HOME/luna-docker/config/stc/partition_identities
$HOME/luna-docker/config/stc/token/001
```

and create an empty file

```
$HOME/luna-docker/config/stc/token/001/token.db
```

The contents of the config directory are needed by the Docker containers.

3. Copy the Luna Minimal Client tarball to **$HOME/luna-docker**.

4. Untar the Luna Minimal Client tarball.

>**tar -xf $HOME/luna-docker/LunaClient-Minimal-**<release_version>**.x86_64.tar -C $HOME/luna-docker**

5. Copy the Chrystoki.conf file from the Minimal Client directory to **$HOME/luna-docker/config**.

>**cp $HOME/luna-docker/LunaClient-Minimal-**<release_version>**.x86_64/Chrystoki-template.conf $HOME/luna-docker/config/Chrystoki.conf**

6. Define the following environment variable:

>**export ChrystokiConfigurationPath=$HOME/luna-docker/config**

7. [Optional] If you choose to use STC, review the SafeNet Luna Network HSM documentation and modify the following instructions. The goal is to have an HSM partition created and registered with the full SafeNet Luna HSM Client before you create the Docker image and containers.

8. Update the Chrystoki.conf file paths so the tools work as expected

>**MIN_CLIENT_DIR=$HOME/luna-docker/LunaClient-Minimal-**<release_version>**.x86_64**

>**$MIN_CLIENT_DIR/bin/64/configurator setValue -s Chrystoki2 -e LibUNIX -v $MIN_CLIENT_DIR/libs/64/libCryptoki2.so**

>**$MIN_CLIENT_DIR/bin/64/configurator setValue -s Chrystoki2 -e LibUNIX64 -v $MIN_CLIENT_DIR/libs/64/libCryptoki2_64.so**

>**$MIN_CLIENT_DIR/bin/64/configurator setValue -s Misc -e ToolsDir -v $MIN_CLIENT_DIR/bin/64**

>**$MIN_CLIENT_DIR/bin/64/configurator setValue -s "LunaSA Client" -e SSLConfigFile -v $MIN_CLIENT_DIR/openssl.cnf**

>**$MIN_CLIENT_DIR/bin/64/configurator setValue -s "LunaSA Client" -e ClientPrivKeyFile -v $HOME/luna-docker/config/certs/dockerlunaclientKey.pem**

>**$MIN_CLIENT_DIR/bin/64/configurator setValue -s "LunaSA Client" -e ClientCertFile -v $HOME/luna-docker/config/certs/dockerlunaclient.pem**

>**$MIN_CLIENT_DIR/bin/64/configurator setValue -s "LunaSA Client" -e ServerCAFile -v $HOME/luna-docker/config/certs/CAFile.pem**

>**$MIN_CLIENT_DIR/bin/64/configurator setValue -s "Secure Trusted Channel" -e ClientTokenLib -v $MIN_CLIENT_DIR/libs/64/libSoftToken.so**

>**$MIN_CLIENT_DIR/bin/64/configurator setValue -s "Secure Trusted Channel" -e SoftTokenDir -v $HOME/luna-docker/config/stc/token**

>**$MIN_CLIENT_DIR/bin/64/configurator setValue -s "Secure Trusted Channel" -e ClientIdentitiesDir -v $HOME/luna-docker/config/stc/client_identities**

>**$MIN_CLIENT_DIR/bin/64/configurator setValue -s "Secure Trusted Channel" -e PartitionIdentitiesDir -v $HOME/luna-docker/config/stc/partition_identities**

9. Create a SafeNet Luna HSM Client certificate for the Docker containers.

>**$MIN_CLIENT_DIR/bin/64/vtl createCert -n** <cert_name>

10. Copy the client certificate to the SafeNet Luna Network HSM appliance.

>**scp $HOME/luna-docker/config/certs/**<cert_name>**.pem admin@**<Network_HSM_IP>**:**

11. Copy the appliance server certificate (**server.pem**) to **$HOME/luna-docker/config/certs**

>**scp admin@**<Network_HSM_IP>**:server.pem $HOME/luna-docker/config/certs**

12. Register the appliance server certificate with the Client.

>**$MIN_CLIENT_DIR/bin/64/vtl addServer -c $HOME/luna-docker/config/certs/server.pem -n** <Network_HSM_IP>

13. Connect via SSH to the SafeNet Luna Network HSM appliance and log in to LunaSH.

>**ssh admin@**<Network_HSM_IP>

14. Create a partition, if one does not already exist on the HSM.

lunash:>**partition create -partition** <partition_name>

15. Register the full SafeNet Luna HSM Client with the appliance, and assign the partition to the client ("client register" on page 1 and "client assignpartition" on page 1).

lunash:>**client register -client** <client_name> {**-ip** <client_IP> | **-hostname** <client_hostname>}

lunash:>**client assignpartition -client** <client_name> **-partition** <partition_name>

lunash:>**ntls ipcheck disable**

lunash:>**exit**

16. On the Client workstation, run LunaCM, set the active slot to the registered partition, and initialize it ("partition init" on page 1).

>**$MIN_CLIENT_DIR/bin/64/lunacm**

lunacm:>**slot set -slot** <slotnum>

lunacm:>**partition init -label** <partition_label>

lunash:>**exit**

17. Update the paths of the libraries, certs and general fields to their future Docker image locations within the **$ChrystokiConfigurationPath/Chrystoki.conf**.

>**sed -i -e 's#'$HOME'/luna-docker/config#/usr/local/luna/config#g' -e 's#'$HOME'/luna-docker/LunaClient-Minimal-\([0-9\.-]\+\)x86_64#/usr/local/luna#g' $ChrystokiConfigurationPath/Chrystoki.conf**

Create a SafeNet Luna HSM Client Docker image

The minimal client tarball includes files necessary for basic operation, and some tools; copy any additional files you want to include in the docker image to **$HOME/luna-docker/**. This example includes the entire Luna Minimal Client.

18. Create a file named Dockerfile with the following contents:

```
FROM ubuntu:xenial
#FROM centos:centos7

ARG MIN_CLIENT
COPY $MIN_CLIENT.tar /tmp
RUN mkdir -p /usr/local/luna
RUN tar xvf /tmp/$MIN_CLIENT.tar --strip 1 -C /usr/local/luna
ENV ChrystokiConfigurationPath=/usr/local/luna/config
ENV PATH="/usr/local/luna/bin/64:${PATH}"

# The package below is necessary for One-Step NTLS if you want to setup NTLS within the Docker
container.
# The only requirement beyond glibc.i686 (required by plink and pscp) would be a configured
Chrystoki.conf
# The minimal client documentation section 8 has example commands, you should modify the value
parameter ("-v")
#    to point to desired files/directories.
# One-Step NTLS uses the section "Misc" entry "ToolsDir" to find the plink/pscp binaries,
# The Chrystoki.conf needs the following entries to be updated for One-Step NTLS to work:
# Section        | Entry
# ------------------------
# Chrystoki2     | LibUNIX
# Chrystoki2     | LibUNIX64
# Misc           | ToolsDir
# "LunaSA Client" | SSLConfigFile
# "LunaSA Client" | ClientPrivKeyFile
# "LunaSA Client" | ClientCertFile
# "LunaSA Client" | ServerCAFile
# Syntax: configurator setValue -s <Section> -e <Entry> -v <value>
# Example: configurator setValue -s Misc -e ToolsDir -v /usr/local/luna/bin/64
# Ubuntu:
#RUN dpkg --add-architecture i386
#RUN apt-get update
#RUN apt-get -y install libc6:i386
# Centos:
#RUN yum install -y glibc.i686

ENTRYPOINT  /bin/bash
#End of the Dockerfile
```

19. Build a Docker image.

>**docker build . --build-arg MIN_CLIENT=LunaClient-Minimal-**<release_version>**.x86_64 -t lunaclient-image**

20. Use the following command to verify the Docker image has been created:

>**docker images**

Run the Docker container

21. Make the contents of the config directory available to the Containers when you create them, by mounting the config directory as a volume.

   >**docker run -it --name lunaclient -v $PWD/config:/usr/local/luna/config lunaclient-image**

22. From the Docker container, verify that the container has a connection to the SafeNet Luna Network HSM partition.

Functionality Modules (FMs) with Luna Minimal Client

To use FMs with the minimal client, see "Create a SafeNet Luna HSM Client Docker image for use with Functionality Modules " on the next page.

SafeNet Data Protection on Demand (DPoD)'s HSM on Demand Service with Luna Minimal Client

To connect to SafeNet Data Protection on Demand (DPoD)'s HSM on Demand services with the minimal client, see "From Linux Minimal Client Create a Docker Container to Access a DPOD HSM on Demand Service" below.

From Linux Minimal Client Create a Docker Container to Access a DPOD HSM on Demand Service

This section describes steps to view SafeNet Data Protection on Demand (DPoD)'s HSM on Demand services from a Luna Minimal Client. This example assumes that you have followed the steps in "Installing Luna Minimal Client on Linux Using Docker" on page 57, or have otherwise created the appropriate directories and Dockerfile. This section assumes you have purchased a DPOD service.

1. Download the DPOD client configuration zip file.

2. Unzip the DPOD client configuration zip file.

   >**cd $HOME/luna-docker**

   >**mkdir $HOME/luna-docker/dpod**

   >**unzip** </path/to/DPOD-ServClient>**.zip -d $HOME/luna-docker/dpod**

3. Copy the DPOD certificates into the certificate directory on the shared volume so that the Docker container can use them.

   >**cp $HOME/luna-docker/dpod/server-certificate.pem $HOME/luna-docker/config/certs/**

   >**cp $HOME/luna-docker/dpod/partition-ca-certificate.pem $HOME/luna-docker/config/certs/**

   >**cp $HOME/luna-docker/dpod/partition-certificate.pem $HOME/luna-docker/config/certs**/

4. Copy over the entire REST and XTC sections from the unzipped Chrystoki.conf located at **$HOME/luna-docker/dpod/Chrystoki.conf**:

   >**cat $HOME/luna-docker/dpod/Chrystoki.conf**

   >**vi $HOME/luna-docker/config/Chrystoki.conf**

5. Update **$HOME/luna-docker/config/Chrystoki.conf** with the expected paths that will be used by the Docker container.

    >**export ChrystokiConfigurationPath=$HOME/luna-docker/config**

    >**MIN_CLIENT_DIR=$HOME/luna-docker/LunaClient-Minimal-**<release_version>**.x86_64**

    >**$MIN_CLIENT_DIR/bin/64/configurator setValue -s XTC -e PartitionCAPath -v /usr/local/luna/config/certs/partition-ca-certificate.pe**m

    >**$MIN_CLIENT_DIR/bin/64/configurator setValue -s XTC -e PartitionCertPath00 -v /usr/local/luna/config/certs/partition-certificate.pem**

    >**$MIN_CLIENT_DIR/bin/64/configurator setValue -s REST -e SSLClientSideVerifyFile -v /usr/local/luna/config/certs/server-certificate.pem**

6. The Luna Minimal Client now includes a DPOD plugin which allows the LUNA client to be able to communicate with a DPOD service. That file can be located under **$HOME/luna-docker/LunaClient-Minimal-**<release_version>**.x86_64/plugins/libdpod.plugin**. This example uses the Dockerfile mentioned above which extracts the Luna Minimal Client tarball into the Docker image.

    >**$MIN_CLIENT_DIR/bin/64/configurator setValue -s Misc -e PluginModuleDir -v /usr/local/luna/plugins**

7. Attach the Docker container. If it is stopped you must start the container first.

    >**docker ps -a**

    >**docker start** <container_id>

    >**docker attach** <container_id>

8. At this point you should be able to see the DPOD service

    >**lunacm**

Create a SafeNet Luna HSM Client Docker image for use with Functionality Modules

The example "Installing Luna Minimal Client on Linux Using Docker" on page 57 uses the Luna Minimal Client to gain connection to a SafeNet Luna Network HSM partition. This section explores some additional steps to sign a Functionality Module (FM) from a Docker container, and also execute a Host Application in order to communicate with the Functionality Module in the SafeNet Luna Network HSM.

FMs consist of two components - the FM itself, that resides in the HSM, extending its functionality, and the Host Application component that resides with the clients that need to connect with that FM.

Due to the size of the FM SDK and ELDK, those have not been included in the Minimal Client as they would greatly expand the size of the minimal client. The assumption is that you installed the full SafeNet Luna HSM Client with HSM Software Development Kit, FM Software Development Kit and other components, and then created and compiled your Functionality Modules elsewhere, and that you would be importing FM components and using FMs, but not developing and compiling them inside a Docker container.

But the above-mentioned use-cases should help in common tasks such as signing Functionality Modules or Communicating with them via Host Applications.

1. On a Linux client with the Functionality Module SDK Component installed (which also installs the Embedded Linux Development Kit (ELDK)), compile the sample FMs and Host application binaries.

   >**make -C /usr/safenet/lunafmsdk/samples/pinenc all**

   >**make -C /usr/safenet/lunafmsdk/samples/skeleton all**

   >**make -C /usr/safenet/lunafmsdk/samples/wrap-comp all**

2. Create a directory on the shared volume to store the Host applications and unsigned FM binaries.

   >**mkdir $HOME/luna-docker/config/fm**

3. Copy the generated files over.

   >**cp /usr/safenet/lunafmsdk/samples/pinenc/fm/bin-ppc/* $HOME/luna-docker/config/fm/**

   >**cp /usr/safenet/lunafmsdk/samples/skeleton/fm/bin-ppc/* $HOME/luna-docker/config/fm/**

   >**cp /usr/safenet/lunafmsdk/samples/wrap-comp/fm/bin-ppc/* $HOME/luna-docker/config/fm/**

   >**cp /usr/safenet/lunafmsdk/samples/pinenc/host/output/bin/* $HOME/luna-docker/config/fm/**

   >**cp /usr/safenet/lunafmsdk/samples/skeleton/host/output/bin/* $HOME/luna-docker/config/fm/**

   >**cp /usr/safenet/lunafmsdk/samples/wrap-comp/host/output/bin/* $HOME/luna-docker/config/fm/**

4. Go back to the Docker container. If it is stopped you must start the container first.

   >**docker ps -a**

   >**docker star**t <container_id>

   >**docker attach** <container_id>

5. If you have not already done so, enable **LoginAllowedOnFMEnabledHSMs=1** in the Chrystoki.conf file, else you will be prompted on your first **partition init** or **role login** attempt to do so in LunaCM.

   >**configurator setValue -s Misc -e LoginAllowedOnFMEnabledHSMs -v 1**

6. Ensure that the "Partition SO" and "Crypto Officer" users are initialized via LunaCM. ("Initialize the Partition SO and Crypto Officer Roles on a PW-Auth Partition" on page 1 or "Initialize the Partition SO and Crypto Officer Roles on a PED-Auth Partition" on page 1).

7. Generate a key pair and Self-Signed Certificate, then sign the FM binary using **mkfm** and export the Self-Signed Certificate.

   >**cmu generatekeypair -labelpublic=fmpub -labelprivate=fmpri -sign=1 -verify=1 -keytype=rsa -mech=pkcs -publicexponent=3 -modulusbits=2048 -slot** <slotnum>

   >**cmu list -slot** <slotnum>

   >**cmu selfsigncertificate -publichandle=**<public_key_handle**> -privatehandle=**<private_key_handle> **-label=FmSign -serialnumber=1 -cn=FmSign -startdate=20180606 -enddate=20201231 -slot** <slotnum>

   >**mkfm -f /usr/local/luna/config/fm/pinenc.bin -o /usr/local/luna/config/fm/pinenc.fm -kSLOTID=**<slotnum>**/fmpri**

   >**mkfm -f /usr/local/luna/config/fm/skeleton.bin -o /usr/local/luna/config/fm/skeleton.fm -kSLOTID=**<slotnum>**/fmpri**

>**mkfm -f /usr/local/luna/config/fm/wrap-comp.bin -o /usr/local/luna/config/fm/wrapcomp.fm -kSLOTID=**<slotnum>**/fmpri**

>**cmu export -slot** <slotnum> **-label FmSign -outputfile=/usr/local/luna/config/fm/FmSign.cert**

8. Copy the signed FMs and Self-Signed Certificate to the SafeNet Luna Network HSM appliance. If your Docker container supports scp, then use that. If you've uncommented the pre-requisites in the Dockerfile regarding **pscp** and **plink**, then you could use that as well. If the above two scenarios are not applicable, you can always copy the files from the shared fm directory volume:

> **scp $HOME/luna-docker/config/fm/pinenc.fm admin@**<Network_HSM_IP>:

>**scp $HOME/luna-docker/config/fm/skeleton.fm admin@**<Network_HSM_IP>:

>**scp $HOME/luna-docker/config/fm/wrapcomp.fm admin@**<Network_HSM_IP>:

>**scp $HOME/luna-docker/config/fm/FmSign.cert admin@**<Network_HSM_IP>:

9. Connect via SSH to the SafeNet Luna Network HSM appliance and log in to LunaSH.

>**ssh admin@**<Network_HSM_IP>

10. Login as the HSM Admin (SO), then load the Functionality Modules.

lunash:>**hsm login**

lunash:>**hsm fm load -fmFile pinenc.fm -certFile FmSign.cert**

lunash:>**hsm fm load -fmFile skeleton.fm -certFile FmSign.cert**

lunash:>**hsm fm load -fmFile wrapcomp.fm -certFile FmSign.cert**

lunash:>**hsm fm status**

11. If the **hsm fm status** command, in the previous step, mentioned "reboot HSM to activate" on any of the FMs, then you must reboot the HSM. Upon restarting the HSM, SO login status will be reset, thus you will have to login as SO later.

lunash:>**hsm restart**

lunash:>**hsm login**

12. Activate Secure Memory File System (SMFS); you must be logged in as the HSM Admin. If you check the status of the FMs, they should all be "Enabled" status now.

lunash:>**hsm fm smfs activate**

lunash:>**hsm fm status**

13. Verify that the Host Application can interact with the FM. If you have trouble loading the shared libraries, you can set the LD_LIBRARY_PATH environment variable.

>**export LD_LIBRARY_PATH="/usr/local/luna/libs/64"**

>**/usr/local/luna/config/fm/pinenctest -s**<slotnum> **ge**n

>**/usr/local/luna/config/fm/pinenctest -d**<slotnum> **test**

>**/usr/local/luna/config/fm/skeleton -s**<slotnum> **-t "Hello all"**

>**/usr/local/luna/config/fm/wrapcomptest -s**<slotnum>

Solaris SafeNet Luna HSM Client Installation

These instructions assume that you have already acquired the SafeNet Luna HSM Client software, in the form of a downloaded .tar archive.

You must install the SafeNet Luna HSM Client software on each client workstation you will use to access a SafeNet Luna HSM. This section describes how to install the client on a workstation running Solaris, and contains the following topics:

> "Prerequisites" below

> "Installing the Client Software" on the next page

> "Controlling User Access to Your Attached HSMs and Partitions" on page 68

> "Uninstalling the SafeNet Luna HSM Client Software" on page 69

> "Java" on page 69

> "Scripted or Unattended Installation" on page 69

> "Interrupting the installation - [Ctrl] [C]" on page 70

Applicability to specific versions of Solaris is summarized in the Customer Release Notes for the current release.

> **NOTE**   Before installing a SafeNet system, you should confirm that the product you have received is in factory condition and has not been tampered with in transit. Refer to the Startup Guide included with your product shipment. If you have any questions about the condition of the product that you have received, contact Gemalto Support.

Each computer that connects to the SafeNet Luna Network HSM appliance as a client must have the cryptoki library, the vtl client shell and other utilities and supporting files installed.

Each computer that contains, or is connected to a SafeNet Luna USB HSM or a SafeNet Luna PCIe HSM must have the cryptoki library and other utilities and supporting files installed.

> **NOTE**   This example shows all the SafeNet Luna HSM Client products and components. Some items are not supported on all operating systems and therefore do not appear as you proceed through the installation script.

Prerequisites

Before starting the installation, ensure that you have satisfied the following prerequisites:

Random Number Generator (RNG) or Entropy Gathering Daemon (EGD)
Ensure that you have a Random Number Generator (RNG) or Entropy Gathering Daemon (EGD) on your system in one of the following locations:

> /dev/egd-pool

> /etc/egd-pool,

> /etc/entropy

>   /var/run/egd-pool

RNG/EGD

Cryptographic algorithms, including those that assure the security of communication – such as in OpenSSL and other protocols – depend upon random numbers for the creation of strong keys and certificates. A readily available source of random data is the entropy that exists in complex computer processes. Utilities exist for every operating system, to gather bits of system entropy into a pool, which can then be used by other processes.

Windows and Linux have these installed by default. Other systems might not. See your system administrator.

Entropy Pool

In the case of SafeNet Luna Network HSM, the SafeNet Luna HSM Client administration tool (**vtl**) expects to find a source of randomness at **/dev/random**. If one is not found, **vtl** fails, because the link cannot be secured from the Client end.

If your system does have an entropy pool, but the random number generator (RNG) is not in the expected place, then you can create a symbolic link between the actual location and one of the following:

>   /dev/random

>   /dev/egd-pool

>   /etc/egd-pool

>   /etc/entropy

>   /var/run/egd-pool

If your system does not have an entropy-gathering daemon or random number generator, please direct your system administrator to install one, and point it to one of the named devices.

Installing the Client Software

It is recommended that you refer to the SafeNet Luna HSM Customer Release Notes for any installation-related issues or instructions before you begin the following software installation process.

> **CAUTION!**   You must be logged in as **root** when you run the installation script.

By default, the Client programs are installed in the **/opt/safenet/lunaclient/bin** directory.

To install the SafeNet Luna HSM Client software on a Solaris workstation

1. Log on to the client system, open a console or terminal window, and use **su** to gain administrative permissions for the installation.

2. Access the SafeNet Luna HSM Client software:

   a. Copy or move the **.tar** archive to a suitable directory where you can untar the archive and launch the installation script.

   b. Extract the contents from the archive:

   tar xvf <filename>**.tar**

3. Go to the install directory for your architecture:

Architecture	Path
Solaris Sparc 64-bit	LunaClient_7.X.0_SolarisXXSparc/64
Solaris x86 64-bit	LunaClient_7.X.0_SolarisXXx86/64

4. To see the help, or a list of available installer options, type:

   sh install.sh -? or **sh install.sh --help**

   To install all available products and optional components, type:

   sh install.sh all

   To selectively install individual products and optional components, type the command without arguments:

   sh install.sh

5. Type **y** if you agree to be bound by the license agreement.

6. A list of installable SafeNet products is displayed (might be different, depending on your platform). Select as many as you require, by typing the number of each (in any order) and pressing **Enter**. As each item is selected, the list updates, with a "*" in front of any item that has been selected. The following example shows that items 1 and 3 have been selected, and item 4 is about to be selected.

```
Products
Choose Luna Products to be installed
    *[1]: SafeNet Luna Network HSM
     [2]: SafeNet Luna PCIe HSM
    *[3]: SafeNet Luna USB HSM
     [4]: SafeNet Luna Backup HSM
     [N|n]: Next
     [Q|q]: Quit
Enter selection: 4
```

7. When the selection is complete, type **N** or **n** for "Next", and press **Enter**. If you wish to make a change, simply type a number again and press **Enter** to de-select a single item.

8. The next list is titled "Advanced" and includes additional items to install. Some items might be pre-selected to provide the optimum SafeNet Luna HSM experience for the majority of customers, but you can change any selection in the list. When the Components list is adjusted to your satisfaction, press **Enter**.

   > **NOTE** The installer includes the SafeNet SNMP Subagent as an option. If you select this option, you will need to move the SafeNet MIB files to the appropriate directory for your SNMP application after installation is complete, and you will need to start the SafeNet subagent and configure for use with your agent. See the *Administration Guide* for more information.

9. If the script detects an existing cryptoki library, it stops and suggests that you uninstall your previous SafeNet software before starting the SafeNet Luna HSM Client installation again.

10. The system installs all packages related to the products and any optional components that you selected.

11. Although FMs are supported on Linux and Windows clients only in this release, the FM architecture requires a configuration file setting to allow partition login on an FM-enabled HSM. If the HSM you will be using with this client is FM-enabled (see "Preparing the SafeNet Luna Network HSM to Use FMs" on

for more information), you must add the following entry to the [Misc] section of the Chrystoki.conf file:

[Misc]

LoginAllowedOnFMEnabledHSMs=1

> **NOTE** As a general rule, do not modify the Chrystoki.conf/crystoki.ini file, unless directed to do so by Gemalto Technical Support. If you do modify the file, never insert TAB characters - use individual space characters. Avoid modifying the PED timeout settings. These are now hardcoded in the appliance, but the numbers in the Chrystoki.conf file must match.

Controlling User Access to Your Attached HSMs and Partitions

By default, only the root user has access to your attached HSMs and partitions. You can specify a set of non-root users that are permitted to access your attached HSMs and partitions, by adding them to the **hsmusers** group.

> **NOTE** The client software installation automatically creates the **hsmusers** group if one does not already exist on your system. The **hsmusers** group is retained when you uninstall the client software, allowing you to upgrade your client software while retaining your **hsmusers** group configuration.

Adding users to hsmusers group

To allow non-root users or applications access your attached HSMs and partitions, assign the users to the **hsmusers** group. The users you assign to the **hsmusers** group must exist on the client workstation. Users you add to the **hsmusers** group are able to access your attached HSMs and partitions. Users who are not part of the **hsmusers** group are not able to access your attached HSMs and partitions.

To add a user to hsmusers group

1. Ensure that you have **sudo** privileges on the client workstation.

2. Add a user to the **hsmusers** group:

    sudo gpasswd --add <username> **hsmusers**

    where <username> is the name of the user you want to add to the **hsmusers** group.

Removing users from hsmusers group

Should you wish to rescind a user's access to your attached HSMs and partitions, you can remove them from the **hsmusers** group.

> **NOTE** The user you delete will continue to have access to the HSM until you reboot the client workstation.

To remove a user from hsmusers group

1. Ensure that you have **sudo** privileges on the client workstation.

2. Remove a user from the **hsmusers** group:

sudo gpasswd -d <username> **hsmusers**

where <username> is the name of the user you want to remove from the **hsmusers** group. You must log in again to see the change.

Uninstalling the SafeNet Luna HSM Client Software

1. **cd /opt/safenet/lunaclient/bin**

2. **sh uninstall.sh**

Java

If you install the Luna Java Security Provider (JSP), refer to SafeNet JSP Overview and Installation for additional setup procedures for your operating system.

Scripted or Unattended Installation

If you prefer to run the installation from a script, rather than interactively, run the command with the options **-p** <list of SafeNet products> and **-c** <list of SafeNet components>. To see the syntax, run the command with **help** like this:

```
[myhost]$ sudo sh install.sh help
[sudo] password for fred

At least one product should be specified.

usage:
       install.sh      - Luna Client install through menu
       install.sh help - Display scriptable install options
       install.sh all  - Complete Luna Client install

       install.sh -p [sa|pci|g5|rb] [-c sdk|jsp|jcprov|ldpc|snmp]

       -p <list of Luna products>
       -c <list of Luna components>  - Optional. All components are installed if not provided

Luna products options
   sa     - SafeNet Luna Network HSM
   pci    - SafeNet Luna PCIe HSM
   g5     - SafeNet Luna USB HSM
   rb     - SafeNet Luna Backup HSM

Luna components options
   sdk    - Luna SDK
   jsp    - Luna JSP (Java)
   jcprov - Luna JCPROV (Java)
   snmp   - Luna SNMP subagent


[myhost]$
```

For scripted/automated installation, your script will need to capture and respond to the License Agreement prompt, and to the confirmation prompt. For example:

```
[myhost]$ sudo sh install.sh all

IMPORTANT: The terms and conditions of use outlined in the software
```

```
license agreement (Document #008-010005-001_053110) shipped with the product
("License") constitute a legal agreement between you and SafeNet Inc.
Please read the License contained in the packaging of this
product in its entirety before installing this product.

Do you agree to the License contained in the product packaging?

If you select 'yes' or 'y' you agree to be bound by all the terms
and conditions se out in the License.

If you select 'no' or 'n', this product will not be installed.

(y/n) y

Complete Luna Client will be installed. This includes SafeNet Luna Network HSM,
SafeNet Luna PCIe HSM, SafeNet Luna USB HSM AND SafeNet Luna Backup HSM.

Select 'yes' or 'y' to proceed with the install.

Select 'no' or 'n', to cancel this install.

Continue (y/n)?  y
```

Interrupting the installation - [Ctrl] [C]

Do not interrupt the installation script in progress, and ensure that your host computer is served by an uninterruptible power supply (UPS). If you press [Ctrl] [C], or otherwise interrupt the installation (OS problem, power outage, other), some components will not be installed. It is not possible to resume an interrupted install process. The result of an interruption depends on where, in the process, the interruption occurred (what remained to install before the process was stopped).

As long as the cryptoki package is installed, any subsequent installation attempt results in refusal with the message "A version of Luna Client is already installed." Removing the library allows the script to clean up remaining components, so that you can install again.

What to do if installation is incomplete or damaged

1. If SNFTlibcryptoki has been installed, uninstall it manually.

2. Run the Client install script again. Now that SNFTlibcryptoki is removed, the install script removes any stray packages and files.

3. Install again, to perform a clean installation.

After Installation

When you have installed the software onto a Client, the next task is to configure the SafeNet Luna HSM, as described in the *Configuration Guide*.

Windows SafeNet Luna HSM Client Installation

This section describes how to install the SafeNet Luna HSM Client software on Windows. It contains the following topics:

> "Required Client Software" below

> "Prerequisites" below

> "Installing the SafeNet Luna HSM Client Software" below

> "Modifying the Installed Windows SafeNet Luna HSM Client Software" on page 75

> "Java" on page 76

> "SafeNet CSP and KSP" on page 76

> "Uninstalling the SafeNet Luna HSM Client Software" on page 77

> "After Installation" on page 79

> "Troubleshooting" on page 79

Applicability to specific versions of Windows is summarized in the Customer Release Notes for this release.

> **NOTE** Before installing a SafeNet Luna HSM system, confirm that the product you have received is in factory condition and has not been tampered with in transit. Refer to the Startup Guide included with your product shipment. If you have any questions about the condition of the product that you have received, contact Technical Support immediately.

Required Client Software

Each computer that connects to a SafeNet Luna Network HSM as a Client must have the cryptoki library, the **vtl** client shell and other utilities and supporting files installed.

Each computer that contains, or is connected to a SafeNet Luna PCIe HSM or a SafeNet Luna USB HSM must have the cryptoki library and other utilities and supporting files installed.

Prerequisites

The SafeNet Luna HSM Client installer requires the Microsoft Universal C Runtime (Universal CRT) to run properly. Universal CRT requires your Windows machine to be up to date. Before running the installer, ensure that you have the Universal C Runtime in Windows (KB2999226) update and its prerequisites installed on your machine. The following updates must be installed in order:

1. March 2014 Windows servicing stack update (See https://support.microsoft.com/en-us/help/2919442)

2. April 2014 Windows update (See https://support.microsoft.com/en-us/help/2919355)

3. Universal C Runtime update (See https://support.microsoft.com/en-us/kb/2999226)

Installing the SafeNet Luna HSM Client Software

The supported Windows servers are 64-bit. Hardware drivers are 64-bit only.

For compatibility of our HSMs with Windows CAPI we have SafeNet CSP, and for the newer Windows CNG we have SafeNet KSP. See "SafeNet CSP and KSP" on page 76 for more information.

Interactive (prompted, this page) and non-interactive (no prompts "Scripted/Unattended Windows Installation/Uninstallation" on page 81) installation options are available.

To install the SafeNet Luna HSM Client software

1. Log into Windows as "Administrator", or as a user with administrator privileges (see "Troubleshooting" on page 79).

2. Uninstall any previous versions of the Client software before you proceed (see "Uninstalling the SafeNet Luna HSM Client Software" on page 77).

> **NOTE**   If you do not uninstall previous SafeNet Luna HSM Client versions, you might face installation issues, such as failure to install the new client.

3. Download the SafeNet Luna HSM Client from the Thales Group Support Portal at https://supportportal.gemalto.com and extract the .zip to an appropriate folder.

4. In the extracted directory, locate the folder for your Windows architecture and double click **LunaHSMClient.exe**.

LunaHSMClient
Luna HSM Client
Gemalto Inc.
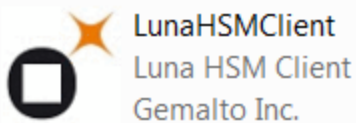
5. The Custom Setup dialog allows you to choose which software components you wish to install. Click a product to select the components to install, or click Select All to install all available components.

   The installer includes the SafeNet SNMP Subagent as an option with any of the SafeNet Luna HSMs, except SafeNet Luna Network HSM, which has agent and subagent built in. After installation of the SafeNet SNMP Subagent is complete, you will need to move the SafeNet MIB files to the appropriate directory for your SNMP application, and you will need to start the SafeNet subagent and configure for use with your agent, as described in SNMP Monitoring in the *Administration Guide*.

> **NOTE** **Dependencies and considerations when installing:**
> **>** The FM Tools and FM SDK are useful to you only if you will be using or creating Functionality Modules, to add custom abilities to your HSMs.
> **>** The FM SDK requires that you install PCIe HSM software and drivers.
> **>** Similarly, if you are using third-party software to make standard cryptographic calls to the HSM, and are not creating application programs, then you can forego loading the Software Development Kit.
> **>** There is no harm in installing unneeded components; they do not conflict.
> **>** The FM SDK option remains gray/unselectable until "Software SDK" is selected, because some of the FM SDK samples have dependencies on General Cryptoki Samples that are part of "Software SDK".

After you select the components you want to install, click **Install**.

a. Agree to the terms of the License Agreement to proceed with installation. To view the agreement text, click the link in the dialog. The installer loads a PDF version if a PDF reader is available; otherwise it launches a text editor and a plain-text version of the agreement.

b. If Windows presents a security notice asking if you wish to install the device driver from SafeNet, click "Always trust software from SafeNet Canada" and click **Install** to accept.

c. If you choose not to install the driver(s), your SafeNet Luna HSM Client cannot function with any locally-connected SafeNet hardware (which includes SafeNet Luna PCIe HSM, SafeNet Luna USB HSM, or SafeNet Luna Backup HSMs).

6. When the installation completes, the button options are Uninstall, Modify, or Quit; click **Quit** to finish.

If you launch the installer again, you should see the final dialog, above, allowing you to modify the current SafeNet Luna HSM Client installation if desired, or to uninstall.

7. [Optional] For easy use of the SafeNet Luna HSM Client command-line tools, add the directory to the system PATH variable.

   "C:\Program Files\SafeNet\Lunaclient"

Modifying the Installed Windows SafeNet Luna HSM Client Software

If you wish to modify the installation (perhaps to add a component or product that you did not previously install), you must re-run the current installer and ensure that the desired options are selected.

> **NOTE**   This feature has software and/or firmware dependencies. See Version Dependencies by Feature for more information.

To modify the installed SafeNet Luna HSM Client software

1. Run the **LunaHSMClient.exe** program again. Because the software is already installed on your computer, the following dialog is displayed (in this example, devices and features were previously installed, and the task is to uninstall a couple of items):

2. Select or deselect individual Devices or Features, as desired.

3. Click **Modify**. The client software is updated (items are added or removed).

   If you are uninstalling some items, or if you are adding features, the dialog shows a progress bar briefly, and then shows the current status.

   If you are adding a Luna Device, then you might be prompted with the operating system pop-up to accept/trust the driver. Do so.

4. Click **Quit** when the modification is complete.

> **NOTE** You can also use **Programs and Features** in the Windows Control Panel to launch the Uninstall/Modify dialog for the client software.

Java

If you install the Luna Java Security Provider (JSP), refer to SafeNet JSP Overview and Installation for additional setup procedures for your operating system.

SafeNet CSP and KSP

Thales Group provides SafeNet CSP for applications running in older Windows crypto environments running Microsoft Certificate Services (CAPI), and SafeNet KSP for newer Windows clients running Cryptography Next Generation (CNP). Consult Microsoft documentation to determine which one is appropriate for your client operating system.

> SafeNet CSP Registration Utilities

> SafeNet KSP for CNG Registration Utilities

If the **SafeNet CSP (CAPI) / SafeNet KSP(CNG)** option is selected at installation time, the **SafeNetKSP.dll** file is installed in **C:\Windows\System32** (used for 64-bit KSP).

> **NOTE** The **cryptoki.ini** file, which specifies many configuration settings for your HSM and related software, includes a line that specifies the path to the appropriate libNT for use with your application(s). Verify that the path is correct.

USB-powered PED

The SafeNet Luna PIN Entry Device (PED) v2.8 contains new hardware that enables the PED to be USB-powered; there is no longer a requirement for an external DC power Adapter. PED v2.8 is functionally equivalent to your existing (previous-generation) PEDs and is compatible with HSM versions, 5.x, 6.x, and 7.x.

PED v2.8 ships with firmware 2.8.0. Note that you cannot upgrade existing PEDs to the 2.8.0 version; existing PEDs continue to need a separate DC power adapter for remote PED and upgrade use. The model number on the manufacturer's label identifies the refreshed PED: PED-06-0001. An installed driver is required; see step 1, below.

To use the new USB-powered PED

1. Ensure the SafeNet Luna HSM Client software is installed on the Windows computer that will act as the PED Server to your SafeNet Luna HSM. Installing the Remote PED component of the SafeNet Luna HSM Client installs the required driver.

    > **NOTE** A USB connection, without the driver software, only illuminates the PED screen, with no menu. An installed and running PED driver, on the connected computer, is required for the PED to fully boot and to display its menu.

2. Connect the PED to the computer where you installed the Remote PED component of the SafeNet Luna HSM Client, using the USB micro connector on the PED and a USB socket on your computer.

3. After you connect the PED to the host computer, it will take 30 to 60 seconds for initial boot-up, during which time a series of messages are displayed, as listed below:

    BOOT V.1.1.0-1

    CORE V.3.0.0-1

    Loading PED...

    Entering...

4. After the boot process is complete, the PED displays **Local PED mode** and the **Awaiting command...** prompt. Your new PED is now ready for use.

5. To enter Remote PED mode, if needed, exit Local PED mode with the "< " key, and from the **Select Mode** menu, select option **7 Remote PED**.

Uninstalling the SafeNet Luna HSM Client Software

You need to uninstall SafeNet Luna HSM Client before installing a new version. If you wish to modify the installation (perhaps to add a component or product that you did not previously install), you must uninstall the current installation and re-install with the desired options. If you have a SafeNet Luna Backup HSM connected to the client workstation, either disconnect it or stop the PEDclient service (pedclient mode stop) before you proceed.

To uninstall the SafeNet Luna HSM Client software

1. Run the **LunaHSMClient.exe** program again. Because the software is already installed on your computer, the following dialog is displayed, showing which components are currently installed (for this example, all Devices and all Features were previously installed):
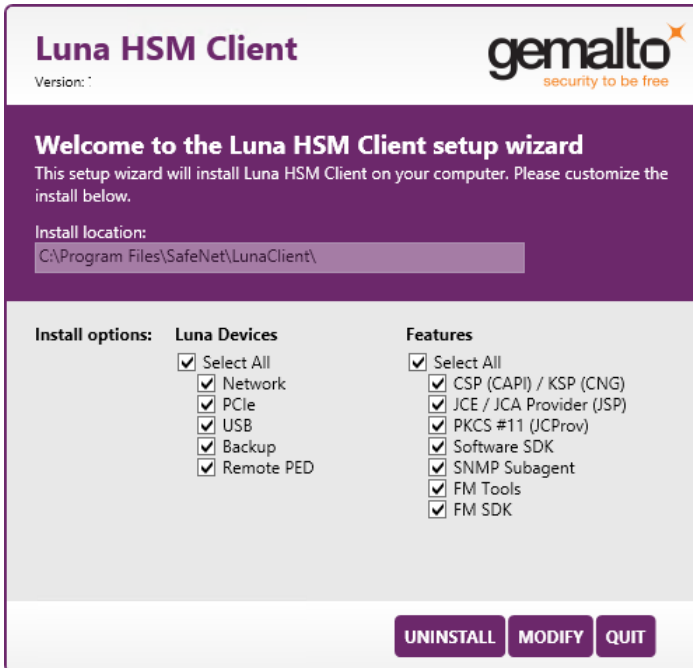
2. Click **Uninstall**. The client software is uninstalled.
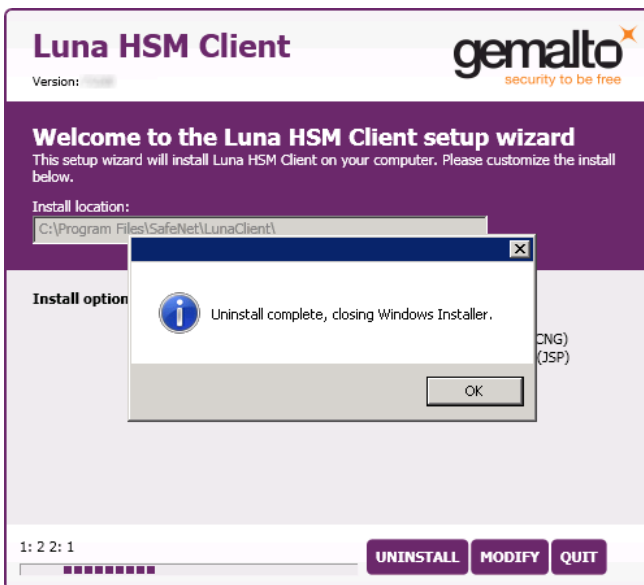
3. When the uninstallation is complete, click **OK** to dismiss the operating system's confirmation dialog.

> **NOTE**   You can also use **Programs and Features** in the Windows Control Panel to uninstall the client software.

Uninstall if not present

If the SafeNet Luna HSM Client software has been uninstalled, and you launch the installer in uninstall mode, from the command line, the installer starts, looks for the installed software, fails to find it, and presents a Windows dialog to that effect.
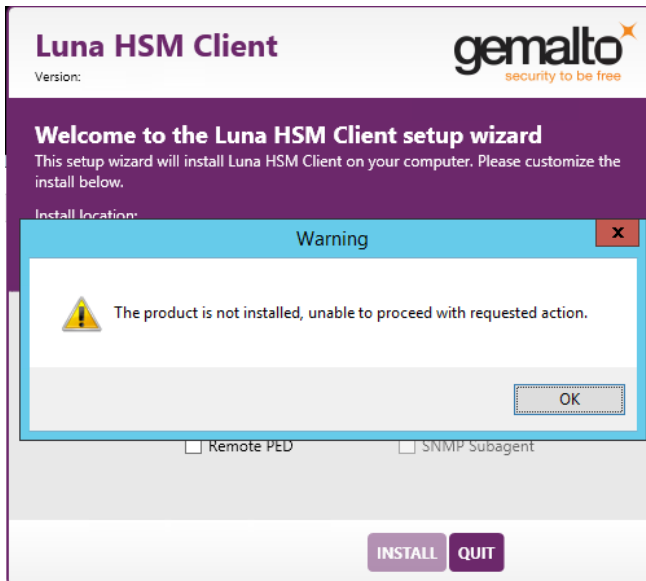
If the SafeNet Luna HSM Client software has been uninstalled, nothing related to the client appears in Windows Control Panel, so nothing exists to launch from that avenue.

After Installation

When you have installed the software, the next task is to configure the SafeNet Luna HSM, as described in the *Configuration Guide*.

Open a new command-line/console window to allow the library path to be found before you run LunaCM or other utilities that require the library.

Troubleshooting

If you are not the Administrator of the computer on which SafeNet Luna HSM Client is being installed, or if the bundle of permissions in your user profile does not allow you to launch the installer with "Run as Administrator", then some services might not install properly. One option is to have the Administrator perform the installation for you.

Another approach might be possible. If you have sufficient elevated permissions, you might be able to right-click and open a Command Prompt window as Administrator.
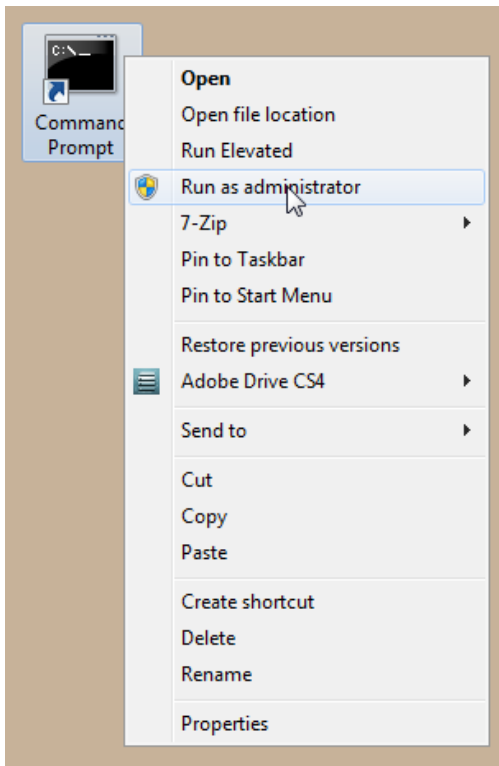
If that option is available, then you can use the command line to move to the location of the
LunaHSMClient.exe file and launch it there, which permits the needed services to load for PEDclient. See
"Scripted/Unattended Windows Installation/Uninstallation" on the next page for instructions on how to install
the client software from the command line.

Scripted/Unattended Windows Installation/Uninstallation

This section describes how to perform unattended or scripted installations on Windows platforms. The following procedures are described:

> "Command line options overview" below

> "Installing the SafeNet Luna HSM Client for the SafeNet Luna Network HSM" on page 84

> "Installing the SafeNet Luna HSM Client for the SafeNet Luna PCIe HSM" on page 84

> "Installing the SafeNet Luna HSM Client for the SafeNet Luna USB HSM" on page 84

> "Installing the SafeNet Luna HSM Client for the SafeNet Luna Backup HSM" on page 85

> "Installing the SafeNet Luna HSM Client for Remote PED" on page 85

> "Installation Location " on page 85

> "Logging" on page 86

> "Uninstalling the SafeNet Luna HSM Client" on page 86

If you want to perform an interactive installation, using the graphical, interactive installer, see "Windows SafeNet Luna HSM Client Installation" on page 71

> **NOTE**   Unattended installation stores the root certificate in the certificate store and marks the publisher (in this case, SafeNet, Inc.) as trusted for future installations. You are not prompted to trust SafeNet Inc. as a driver publisher during unattended installation.

Command line options overview

The following command-line options are available:

Option	Values	Description
addlocal=	Various (see below)	Takes one-or-more device values, and one-or-more feature values, as a comma-separated list. Case insensitive. Values may be quoted or not.
installdir=	A fully qualified folder path to install the client software	Case insensitive. Default value is "c:\program files\safenet\lunaclient". Enclose paths containing spaces in "".
/install	N/A	Install the product and features.
/uninstall	N/A	Remove the product and features.
/quiet	N/A	Performs a silent installation; no prompts or messages.(See Note below this table)
/norestart	N/A	Prevents a reboot, post-installation. Any reboots must be performed manually.

Option	Values	Description
/log	The name of a log file	Generates a highly detailed series of logs of the installation progress. This is equired only for product support.

> **NOTE** Windows defaults to launching the interactive graphical installer, unless you specify **/quiet** at the command line. Always include the **/quiet** option for scripted/unattended SafeNet Luna HSM Client installation.

The following devices or components are available for use with the addlocal= option:

Device identifier value	Can be used with these installable features
NETWORK	CSP_KSP, JSP, SDK, JCProv (*)
PCI	CSP_KSP, JSP, SDK, JCProv, SNMP
USB	CSP_KSP, JSP, SDK, JCProv, SNMP
BACKUP	SNMP (this device performs backup and restore operations and is not enabled for cryptographic applications)
PED	N/A (Used for remotely authenticating to PED-authenticated HSMs; not used by cryptographic applications - use of this device requires hands-on presence)

The device names are not case-sensitive.

(* The Network HSM appliance contains its own SNMP support; therefore the SNMP feature is not installed on clients where the Network HSM is the only HSM to be used.)

The following features are available for use with the addlocal= option :

Feature identifier value	Can be installed with these Luna devices	Description
CSP_KSP	NETWORK, PCI, USB	Microsoft CSP and KSP
FMSDK	NETWORK, PCIe *	Functionality Modules Software Development Kit
FMTOOLS	NETWORK, PCIe *	Tools for use when preparing Functionality Modules
JCProv	NETWORK, PCIe, USB	JCPROV PKCS#11
JSP	NETWORK, PCIe, USB	Java Provider component
SDK	NETWORK, PCIe, USB	Software SDK – Java / C++ samples
SNMP	PCIe, USB, Backup	SNMP subagent

The features can be installed together with the listed device(s) only - they cannot be installed separately - and need to be included only once in the command line. For example, if you are installing the NETWORK and PCI devices and you wish to install the CSP / KSP feature, specify CSP_KSP one time. The feature names are not case-sensitive.

> **NOTE** * If you install FMTOOLS for NETWORK only, then just **mkfm** and the **library** are installed.
>
> If you install FMTOOLS for PCI, then **mkfm** and the **library** along with **ctfm** and **fmrecover** are installed.
>
> If you install FMTOOLS for both NETWORK and PCIe devices, then all four elements are installed.
>
> If you install the FM SDK, the Luna SDK is installed as well, to satisfy dependencies.
>
> Options for **addlocal=** are separated by spaces. Device and feature values are separated by commas, with no spaces, unless the whole list is enclosed between quotation marks. If a space is encountered, outside of paired quotation marks, the next item found is treated as a command option.

Installing all components and features

Subsequent sections detail how to install the SafeNet Luna HSM Client software, drivers (if necessary), and optional features (like Java support and the SDK), for individual HSMs. This section describes how to install everything at once, so that all SafeNet Luna HSMs and Remote PED are supported and all the optional features are available.

Use the **ADDLOCAL=** option together with the value **all** to install the base client software and the drivers for all SafeNet Luna devices, along with all the features.

To install the SafeNet Luna HSM Client software and drivers for *all* SafeNet Luna devices and *all* features

From the location of **LunaHSMClient.exe** run the following command:

> Install the full SafeNet Luna HSM Client software with drivers for all SafeNet Luna HSMs (Network HSM (no driver), PCIe HSM, Backup HSM, Remote PED), as well as all the features (CSP/KSP, JSP, JCProv, C++ SDK, SNMP Subagent)

LunaHSMClient.exe /install /quiet ADDLOCAL=all

> **NOTE** You can omit the **/quiet** option to see all options in the GUI dialog.

> [Optional logging] Install the full SafeNet Luna HSM Client software with drivers for all SafeNet Luna HSMs (Network HSM (no driver), PCIe HSM, Backup HSM, Remote PED), as well as all the features (CSP/KSP, JSP, JCProv, C++ SDK, SNMP Subagent), and log the process.

LunaHSMClient.exe /install /log install.log /quiet ADDLOCAL=all

> **NOTE** The setting **/log** is optional and saves the installation logs to the file named **install.log** in the example. The **install.log** file (whatever name you give it) is required only if troubleshooting an issue with Technical Support.

Installing the SafeNet Luna HSM Client for the SafeNet Luna Network HSM

Use the **ADDLOCAL=NETWORK** option to install the base client software for the SafeNet Luna Network HSM. Include the values for any optional, individual software components you desire. The base software must be installed first.

To install the SafeNet Luna HSM Client for the SafeNet Luna Network HSM

From the location of **LunaHSMClient.exe** run one of the following commands:

> Install the base SafeNet Luna HSM Client software necessary to communicate with SafeNet Luna Network HSM

  LunaHSMClient.exe /install /quiet ADDLOCAL=NETWORK

> [Optional] Install the base SafeNet Luna HSM Client software and any of the optional components for the SafeNet Luna Network HSM that you desire:

  For example, the following command installs the base software and all of the optional components:

  LunaHSMClient.exe /install /quiet ADDLOCAL=NETWORK,CSP_KSP,JSP,SDK,JCProv

  If you wish to install only some of the components, just specify the ones you want after the product name (NETWORK in this example).

Installing the SafeNet Luna HSM Client for the SafeNet Luna PCIe HSM

Use the **ADDLOCAL=PCI** option to install the base client software for the SafeNet Luna PCIe HSM. Include any features you desire. The base software must be installed first.

To install the SafeNet Luna HSM Client for the SafeNet Luna PCIe HSM

From the location of **LunaHSMClient.exe** run one of the following commands:

> Install the base SafeNet Luna HSM Client software for SafeNet Luna PCIe HSM

  LunaHSMClient.exe /install /quiet ADDLOCAL=PCI

> Install the base SafeNet Luna HSM Client software and any of the optional features for the SafeNet Luna PCIe HSM that you desire:

  For example, the following command installs the base software and all of the optional components:

  LunaHSMClient.exe /install /quiet ADDLOCAL=PCI,CSP_KSP,JSP,SDK,JCProv,SNMP

  If you wish to install only some of the components, just specify the ones you want after the product name (PCI in this example).

Installing the SafeNet Luna HSM Client for the SafeNet Luna USB HSM

Use the **ADDLOCAL=USB** option to install the base client software for the SafeNet Luna USB HSM. Include any features you desire. The base software must be installed first.

To install the SafeNet Luna HSM Client for the SafeNet Luna USB HSM

From the location of **LunaHSMClient.exe** run one of the following commands:

> Install for SafeNet Luna USB HSM

LunaHSMClient.exe /install /quiet ADDLOCAL=USB

> Install the base SafeNet Luna HSM Client software and any of the optional features for the SafeNet Luna USB HSM that you desire:

For example, the following command installs the base software and all of the optional components:

LunaHSMClient.exe /install /quiet ADDLOCAL=USB,CSP_KSP,JSP,SDK,JCProv,SNMP

If you wish to install only some of the components, just specify the ones you want after the product name (USB in this example).

Installing the SafeNet Luna HSM Client for the SafeNet Luna Backup HSM

Use the **ADDLOCAL=BACKUP** option to install the base client software for the SafeNet Luna Backup HSM, and the optional feature, if desired. For the Backup HSM, which performs backup and restore operations and is not enabled for use with cryptographic applications, the feature you might add is SNMP, if applicable in your environment.

To install the SafeNet Luna HSM Client for the SafeNet Luna Backup HSM

From the location of **LunaHSMClient.exe** run one of the following commands:

> Install the base SafeNet Luna HSM Client software for SafeNet Luna Backup HSM

LunaHSMClient.exe /install /quiet /norestart ADDLOCAL=BACKUP

> Install the base SafeNet Luna HSM Client software and an optional component for the SafeNet Luna Backup HSM:

For example, the following command installs the base software and the optional component:

LunaHSMClient.exe /install /quiet /norestart ADDLOCAL=backup,snmp

Installing the SafeNet Luna HSM Client for Remote PED

Use the **ADDLOCAL=** option with component value **PED** to install the client software for the SafeNet Luna Backup HSM.

To install the SafeNet Luna HSM Client for the SafeNet Luna Backup HSM

> From the location of **LunaHSMClient.exe** run the following command:

LunaHSMClient.exe /install /quiet addlocal=ped

Installation Location

Specify the installation location, if the default location is not suitable for your situation.

This applies to installation of any Luna Device. Provide the **INSTALLDIR=** option, along with a fully qualified path to the desired target location. For example:

LunaHSMClient.exe /install /quiet addlocal=all installdir=c:\lunaclient

That command silently installs all of the SafeNet Luna device software and features to the folder c:\lunaclient (in this example). The software is installed into the same subdirectories per component and feature, under that named folder, as would be the case if **INSTALLDIR** was not provided. That is, **INSTALLDIR** changes the prefix or primary client installation folder to the one you specify, and the libraries, devices, tools, certificate folders, etc. are installed in their predetermined relationship, but under the new main folder location.

Logging

If problems are encountered during installation or uninstallation of the software and you wish to determine the reason, or if Gemalto Technical Support has requested you to do so, detailed logs can be generated and captured by specifying the /log option and providing a filename to capture the log output. Two logs are generated – one according to the name given and the other similarly named, with a number appended. Both log files must be sent to Gemalto support if assistance is required.

Example commands that include logging are:

LunaHSMClient.exe /install /quiet /log install.log /norestart ADDLOCAL=backup,snmp

LunaHSMClient.exe /uninstall /quiet /log uninstall.log

Uninstalling the SafeNet Luna HSM Client

You can also perform scripted/unattended uninstallation.

To uninstall the SafeNet Luna HSM Client

> From the location of **LunaHSMClient.exe** run the following command:

  LunaHSMClient.exe /uninstall /quiet

> To log the uninstallation process, run the following command:

  LunaHSMClient.exe /uninstall /quiet /log uninstall.log

Adding a DPoD HSM on Demand Service

SafeNet Luna HSM Client allows you to use both Luna partitions and Data Protection on Demand's HSM on Demand services. Using a single client workstation, you can back up or migrate your keys between Luna and HSMoD, or combine partitions and services into an HA group.

The standard SafeNet Luna HSM Client configuration file requires some special editing to add an HSMoD service. This procedure will allow you to add an HSMoD service to your existing SafeNet Luna HSM Client.

> **NOTE** This feature has software and/or firmware dependencies. See Version Dependencies by Feature for more information.

Prerequisites

> DPoD supports Windows and Linux operating systems only. This procedure presumes that you have already set up SafeNet Luna HSM Client on your Windows or Linux workstation:

  • "Windows SafeNet Luna HSM Client Installation" on page 71

  • "Linux SafeNet Luna HSM Client Installation" on page 44

> You must be using SafeNet Luna HSM Client software version 10.1 or higher (see Updating the SafeNet Luna HSM Client).

> HSMoD services are only compatible with password-authenticated SafeNet Luna Network HSM partitions. For more information on Luna/DPoD compatibility, refer to Cloning Keys Between Luna 6, Luna 7, and HSM on Demand. You can still use HSMoD and PED-authenticated Luna partitions from the same client workstation, but they cannot clone cryptographic objects between them.

> You must purchase an HSMoD service from SafeNet Data Protection on Demand:

  https://safenet.gemalto.com/data-protection-on-demand/

To add a DPoD HSM on Demand service to an existing SafeNet Luna HSM Client

1. After purchasing an HSMoD service, refer to the DPoD documentation for instructions on downloading the DPoD client package. Transfer the .zip file to your SafeNet Luna HSM Client workstation using **scp**, **pscp**, or other secure means (see SCP and PSCP).

2. Extract the .zip file into a directory on your client workstation.

3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the DPoD client install directory. The other client package can be safely deleted.

   • [Windows] **cvclient-min.zip**

   • [Linux] **cvclient-min.tar**

     # tar -xvf cvclient-min.tar

4. Run the provided script to create a new configuration file containing information required by the HSMoD service.

   • [Windows] Right-click **setenv.cmd** and select **Run as Administrator**.

   • [Linux] Source the **setenv** script.

     # source ./setenv

5. Copy the following certificates from the DPoD client directory to your existing client certificates directory:

   • [Windows default] **C:\Program Files\Safenet\Lunaclient\cert**

   • [Linux default] **/usr/safenet/lunaclient/cert/**

   partition-ca-certificate.pem

   partition-certificate.pem

   server-certificate.pem

6. Open the configuration file in the DPoD client directory.

   • [Windows] **crystoki.ini**

   • [Linux] **Chrystoki.conf**

7. Copy the following sections from the DPoD configuration file to the existing version in the SafeNet Luna HSM Client install directory. Edit the entries to use the correct filepath to the certificates you copied in step 5:

```
[XTC]
Enabled=1
PartitionCAPath=<client_cert_directory>\partition-ca-certificate.pem
PartitionCertPath00=<client_cert_directory>\partition-certificate.pem
```

```
TimeoutSec=600

[REST]
ClientConnectIntervalMs=1000
ClientConnectRetryCount=900
ClientEofRetryCount=15
ClientPoolSize=32
ClientTimeoutSec=120
CVAppSpecificData=90vNGg10a8uVBmO8zmEVRA==
RestClient=1
ServerName=na.hsm.dpod.live
ServerPort=443
SSLClientSideVerifyFile=<client_cert_directory>\server-certificate.pem
```

Also copy the following entry from the **Misc** section and edit to use the correct filepath to the **plugins** directory:

```
[Misc]
PluginModuleDir=<client_plugins_directory>
```

- [Windows default] **C:\Program Files\Safenet\Lunaclient\plugins**

- [Linux default] **/usr/safenet/lunaclient/plugins/**

> **NOTE**   The above example is taken from a Windows **crystoki.ini** file; for a Linux client platform, the **Chrystoki.conf** file uses the same entries in Linux syntax (**Misc = {** instead of **[Misc]**, etc).

Save the configuration file. If you wish, you can now safely delete the extracted DPoD client directory.

8. Manually reset the **ChrystokiConfigurationPath** environment variable back to the location of the original configuration file.

   - [Windows] In the Control Panel, search for "environment" and select **Edit the system environment variables**. Click **Environment Variables**. In both the list boxes for the current user and system variables, edit **ChrystokiConfigurationPath** to point to the **crystoki.ini** file in the original client install directory.

   - [Linux] Either open a new shell session, or reset the environment variable for the current session to the location of the original **Chrystoki.conf** file:

     # **export ChrystokiConfigurationPath=/etc/**

9. Launch or relaunch LunaCM to verify that both your Luna partitions and HSMoD service are available.

You can now initialize the HSM on Demand service just as you would a password-authenticated Luna application partition. The cloning domain you set on the HSMoD service must match the partition(s) from which you will migrate keys. Refer to the Data Protection on Demand documentation for instructions and information on the capabilities of your HSMoD service.

> Initializing an Application Partition

> Initializing the Crypto Officer and Crypto User Roles

Refer to Cloning Keys Between Luna 6, Luna 7, and HSM on Demand before migrating keys or using the HSMoD service in an HA group. You can migrate keys to your new HSMoD service using direct slot-to-slot cloning, a SafeNet Luna Backup HSM, or by setting up an HA group.

> Cloning Objects to Another Application Partition

> Backup and Restore Using a G5-Based Backup HSM

> Backup and Restore Using a G7-Based Backup HSM

> Setting Up an HA Group