SafeNet Luna Network HSM 7.0

Key Migration Guide

gemalto
security to be free

Document Information

Product Version	7.0
Document Part Number	007-013576-002
Release Date	02 June 2017

Revision History

Revision	Date	Reason
Rev. A	02 June 2017	Initial release.

Trademarks, Copyrights, and Third-Party Software

Table 1: Third-party software used in this product

Software	License and copyright
editline	This product incorporates editline licensed under Apache v2.0 Open Software. Copyright 1992,1993 Simmule Turner and Rich Salz. All rights reserved. You can obtain the full text of the Apache v2.0 Open Software license at the following URL: https://www.apache.org/licenses/LICENSE-2.0
libFDT	Dual License Choice of BSD or GPL-2.0 Copyright (C) 2006 David Gibson, IBM Corporation.
libsodium	ISC License (ISCL) Copyright (C) 2013-2016
Linux Kernel	GPL-2.0
OpenSSH	This product uses a derived version of OpenSSH Copyright 1995 Tatu Ylonen , Espoo, Finland. All rights reserved . Copyright 1995, 1996 by David Mazieres . Copyright 1983, 1990, 1992, 1993, 1995 The Regents of the University of California. All rights reserved You can obtain the full text of the OpenSSH license at the following URL: https://www.openbsd.org/policy.html
OpenSSL	SSLeay License Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) OpenSSL license

Software	License and copyright
	Copyright (C) 1998-2002 The OpenSSL Project
Software implementation of SHA2	Proprietary license Copyright (C) 2002, Dr Brian Gladman, Worcester, UK.
Software implementation of AES	Proprietary license Copyright (C) 2001, Dr Brian Gladman <brg@gladman.uk.net>, Worcester, UK.

Disclaimer

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

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

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

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

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

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

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

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

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

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 Gemalto-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 Migration Guide

This document describes how to migrate your keys and configuration from a 5.x or 6.x SafeNet Luna HSM partition to a 7.x SafeNet Luna HSM partition. It contains the following chapters:

This preface also includes the following information about this document:

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

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

Document Conventions

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

Notes

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

Note: Take note. Contains important or helpful information.

Cautions

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

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

Warnings

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

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

Command Syntax and Typeface Conventions

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

Format	Convention
{**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

Contact method	Contact	
Phone (Subject to change. An up-to-date list is maintained on the Technical Support Customer Portal)	Global	+1 410-931-7520
	Australia	1800.020.183
	India	000.800.100.4290
	Netherlands	0800.022.2996
	New Zealand	0800.440.359
	Portugal	800.863.499
	Singapore	800.1302.029
	Spain	900.938.717
	Sweden	020.791.028
	Switzerland	0800.564.849
	United Kingdom	0800.056.3158
	United States	(800) 545-6608
Web	https://safenet.gemalto.com	
Technical Support Customer Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Knowledge Base. To create a new account, click the **Register** link at the top of the page. You will need your Customer Identifier number.	

1
Key Migration Overview

You can migrate key material from an older SafeNet Luna HSMs (5.x or 6.x) to a new (7.x) SafeNet Luna HSM by using one of three methods; backup and restore, cloning, or cloning using a temporarily HA group.

This document guides you through several migration scenarios consisting of older and newer SafeNet Luna HSMs, using each applicable migration method. Before migrating, preconditions are provided for each scenario that must be met. There are specific user roles that are identified for performing the migration. In addition, both authentication methods (password and PED-authenticated) are supported.

Supported SafeNet Luna HSMs

This document describes key migration for these SafeNet Luna HSMs:

- SafeNet Luna Network HSM, version 5.x or 6.x to 7.x
- SafeNet Luna USB HSM, version 5.x or 6.x to 7.x
- SafeNet Luna PCIe HSM, version 5.x or 6.x to 7.x

Migration methods

The three migration methods used in this guide are:

- Backup and restore

  The backup and restore method uses the LunaCM **partition archive backup** command to backup key material on an HSM (5.x or 6.x) partition and the Restore command to then restore this material to an HSM 7.x partition.

- Cloning

  The cloning method uses the LunaCM **partition clone** command to clone from an HSM (5.x or 6.x) partition to an HSM 7.x partition. It is also referred to as slot-to slot cloning.

- Cloning using an HA group

  The HA group method uses the LunaCM **ha synchronize** command on members of a temporary HA group consisting of a 5.x or 6.x HSM and a 7.x HSM, set up solely for the purpose of migration. After migration, this group should be removed since the members are not using the same software version.

Preconditions

Each migration procedure in this document is prefaced by a "Preconditions" section that specifies the hardware and software requirements along with any assumptions the procedure is using to perform the migration steps. Examples are a 5.x or 6.x HSM, a 7.x HSM, 5.x, 6.x or 7.x client software, user roles and the slot #s used in the procedure.

Roles required for migration

The following partition roles are needed to migrate key material:

- Partition Security Officer. The partition security officer role is needed to perform LunaCM HA operations and to create the Crypto Officer role.
- Partition Crypto Officer. The partition Crypto Officer role is needed to perform LunaCM backup/restore and cloning operations.

Note: When logging in to a partition, be mindful of whether you're working with pre-PPSO or PPSO firmware. Use the **partition login** command if your HSM has pre-PPSO firmware (version 6.21.2 and earlier). Use the **role login** command if your HSM has PPSO firmware (version 6.22.0 and later). Also, with PPSO firmware 6.22.0 and later (up to but not including firmware 7.x), be careful with user names; that is, type **Crypto Officer** in full (is case sensitive) and not the abbreviation **co**.

Note: In firmware version release 7.x, partition login name requirements allow for abbreviations. That is, you can log in using **po** for Partition Security Officer or **co** for Crypto Officer.

2

SafeNet Network HSM (5.x or 6.x) to SafeNet Luna Network HSM (7.x)

This chapter describes how to migrate your key material from a release 5.x or 6.x SafeNet Luna Network HSM partition to a release 7.x SafeNet Luna Network HSM partition. You can migrate your key material using one of the following three methods:

- "Backup and Restore" below
- "Cloning" on page 13
- "Cloning Using an HA Group" on page 15

Backup and Restore

Cryptographic key material can be backed up and then restored to a release 7.x SafeNet Luna Network HSM partition using a SafeNet Luna Backup HSM.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To backup and restore cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see "HSM Initialization" on page 1).

The 7.x client software should be installed, and the connection to both the source and destination partitions verified, before attempting this procedure (see "SafeNet Luna HSM Client Software Installation" on page 1 for details). The source and destination partitions must both be assigned to the client machine issuing the backup and restore commands (see "Enable the Client to Access a Partition" on page 1 for details). Use **slot list** to ensure both partitions are visible to the client.

Preconditions

The following instructions assume that:

- the 7.x client software has been installed
- an uninitialized partition has been created on the 7.x HSM
- the source and destination partitions are both registered with the client (visible)
- the source partition's security policy allows cloning of private and secret keys

In the following example:

- Slot 0: the source 5.x/6.x partition
- Slot 1: the destination 7.x partition
- Slot 2: the Backup HSM partition

Note: Partition login name requirements have changed with the hardware versions. With release 7.x , you can log in using the abbreviated **po** (Partition Security Officer) or **co** (Crypto Officer).

To migrate cryptographic keys from a 5.x/6.x partition to a 7.x partition using a Backup HSM

Follow these steps to back up all cryptographic material on a 5.x/6.x partition to a Backup HSM, and restore to a new 7.x partition.

1. Run LunaCM, set the current slot to the 7.x partition, and initialize the partition and the Partition SO role.

   slot set -slot 0

   partition init -label <7.x_partition_label>

   a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

   b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

   role login -name po

   role init -name co

   If you are backing up a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

   role createchallenge -name co -challengeSecret <password>

3. Connect your backup HSM and make sure it is visible to the client, along with the 5.x/6.x and 7.x HSMs.

4. Set the current slot to the source 5.x/6.x slot.

   slot list

   slot set -slot 0

5. Log in as the Crypto Officer.

   Note: Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the **partition login** or **role login** commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type **Crypto Officer** in full (is case sensitive) and not **co**.

   a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:

      partition login

   b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up) , use:

      role login -name Crypto Officer

6. Optional: To verify the objects in the 5.x/6.x partition to be cloned, issue the "partition contents" command.

   partition contents

7. Back up the 5.x/6.x partition contents to the Backup HSM.

   partition archive backup -slot 2 -partition <backup_label>

   a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

Optionally, verify that all objects were backed up successfully on the Backup HSM by checking the partition contents.

8. Set the current slot to the 7.x partition, log in as the Crypto Officer, and restore from backup.

slot set -slot 1

role login -name co

partition archive restore -slot 2 -partition <backup_label>

Afterwards, you can verify the partition contents on the 7.x partition:

partition contents

Cloning

The simplest method of migrating key material to a new 7.x partition is slot-to-slot cloning. This procedure copies all permitted cryptographic material from a 5.x/6.x Network HSM partition to a 7.x Network HSM partition.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see "HSM Initialization" on page 1).

The 7.x client software should be installed, and the connection to both the source and destination partitions verified, before attempting this procedure (see "SafeNet Luna HSM Client Software Installation" on page 1 for details). The source and destination partitions must both be assigned to the client machine issuing the cloning commands (see "Enable the Client to Access a Partition" on page 1 for details). Use **slot list** to ensure both partitions are visible to the client.

If the source partition contains asymmetric keys, its security policy must allow cloning of private and secret keys. Use the command **partition showpolicies** in LunaCM to ensure that your source partition's security template allows this (see "partition showpolicies" on page 1). If the 5.x/6.x HSM's security template does not allow cloning of private/secret keys, the HSM Admin may be able to turn this feature on using **partition changepolicy** (see "partition changepolicy" on page 1).

CAUTION: Check your source partition policies and adjust them to be sure you can clone private and symmetric keys. Depending on the configuration of your partition and HSM, these policies may be destructive.

Preconditions

The following instructions assume that:

- the 7.x client software has been installed
- an uninitialized partition has been created on the 7.x Network HSM
- the source and destination partitions must be registered with the client (visible)
- the source 5.x/6.x partition's security policy allows cloning of private and secret keys

In the following examples:

- Slot 0: the source 5.x/6.x partition
- Slot 1: the destination 7.x partition

> **Note:** Partition login name requirements have changed with the hardware versions. With release 7.x, you can log in using the abbreviated **PO** (Partition Security Officer) or **CO** (Crypto Officer).

To clone cryptographic keys from a 5.x/6.x partition to a 7.x partition

Follow these steps to clone all cryptographic material on a 5.x/6.x partition to a 7.x partition.

1. Run LunaCM, set the current slot to the 7.x partition, and initialize the Partition SO role.

   slot list

   slot set -slot 1

   partition init -label <7.x_partition_label>

   a. If you are cloning a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

   b. If you are cloning a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

   role login -name po

   role init -name co

   If you are cloning a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

   role createchallenge -name co -challengesecret <password>

3. Set the current slot to the source 5.x/6.x slot, log in as the Crypto Officer.

   slot set -slot 0

   > **Note:** Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the "partition login" or "role login" commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type "Crypto Officer" in full (is case sensitive) and not "co".

   a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:

   partition login

   b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up) , use:

   role login -name Crypto Officer

4. Optional: To verify the objects in the 5.x/6.x partition to be cloned, issue the "partition contents" command.

   partition contents

5. Clone the objects to the 7.x partition slot (see "partition clone" on page 1 for correct syntax).

   partition clone -objects 0 -slot 1

   Afterward, you can set the current slot to the 7.x partition and verify that all objects have cloned successfully.

slot set -slot 1

role login -name co -password <password>

partition contents

You should see the same number of objects that existed on the 5.x/6.x HSM. You can now decommission the old 5.x/6.x HSM.

Cloning Using an HA Group

High Availability (HA) groups duplicate key material between the HSMs in the group. This function can be used to copy all cryptographic key material from a 5.x/6.x Network HSM partition to a new 7.x Network HSM partition.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see "HSM Initialization" on page 1).

The 7.x client software should be installed, and the connection to both the source and destination HSM partitions verified, before attempting this procedure (see "SafeNet Luna HSM Client Software Installation" on page 1 for details). The source and destination partitions must both be assigned to the client machine issuing the cloning commands (see "Enable the Client to Access a Partition" on page 1 for details). Use **slot list** to ensure both partitions are visible to the client.

Note: It is not recommended to maintain an HA group with different versions of the SafeNet Luna Network HSM hardware.

Preconditions

The following instructions assume that:

- the 7.x client software has been installed
- an uninitialized partition has been created on the 7.x Network HSM
- the source and destination partitions are both registered with the client (visible)

In the following examples:

- Slot 0 = the source 5.x/6.x partition
- Slot 1 = the destination 7.x partition

Note: Partition login name requirements have changed between hardware versions. With release 7.x, you can log in using the abbreviated **po** (Partition Security Officer) or **co** (Crypto Officer).

To clone cryptographic keys from a 5.x/6.x partition to a 7.x partition using an HA group

Follow these steps to copy cryptographic material from an 5.x/6.x partition to a new 7.x partition by creating an HA group that includes both partitions.

1. Run LunaCM, set the current slot to the SA7 partition, and initialize the Partition SO role.

slot set -slot 1

partition init -label <7.x_partition_label>

a. If you are cloning a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

b. If you are cloning a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

role login -name po

role init -name co

If you are cloning a PED-authenticated 5.x/6.x partition, create a challenge secret for the Crypto Officer. This is required to set an HA activation policy.

role createchallenge -name co -challengesecret <password>

3. Set the current slot to the source 5.x/6.x slot, log in as the Crypto Officer.

slot set -slot 0

Note: Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the **partition login** or **role login** commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type **Crypto Officer** in full (is case sensitive) and not **co**.

---

a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:

partition login

b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up) , use:

role login -name Crypto Officer

4. Optional: To verify the objects in the 5.x/6.x partition to be cloned, use:

partition contents

5. Using LunaCM, create an HA group of the 5.x/6.x slot and the 7.x slot.

Note: HA requires that all members have an activation policy set. See "Activation and Auto-Activation on PED-Authenticated Partitions" on page 1 for details.

---

a. Via LunaSH, log in as Security Officer and set policy 22 on the 5.x/6.x partition:

partition changepolicy -partition <5.x_partition_label> **-policy 22 -value 1**

b. In LunaCM, log in to the 7.x partition as Partition Security Officer, and set the activation policy from the client machine:

slot set -slot 1

role login -name po

partition changepolicy -policy 22 -value 1

c. Create the HA group with the 5.x/6.x partition as the primary partition. Select the "copy" option to preserve objects.

hagroup creategroup -label <group_label> **-slot 0 -password** <password>

d. Add the 7.x partition slot to the HA group. Repeat this step to add multiple 7.x partitions to the group.

hagroup addmember -group <group_label> **-slot 1 -password** <password>

6. Synchronize the group to clone the objects to the 7.x member(s).

hagroup synchronize -group <group_label> **-password** <password>

7. Check synchronization status of the group.

hagroup listgroups

Notice the entry "`Needs sync: no`". This means that the objects have been successfully cloned among all members of the HA group. You can also log in to the 7.x slot as the Crypto Officer and check the partition contents.

SafeNet Luna USB HSM (5.x or 6.x) to SafeNet Luna Network HSM (7.x)

This chapter describes how to migrate your key material from a release 5.x or 6.x SafeNet Luna USB HSM partition to a release 7.x SafeNet Luna Network HSM partition. You can migrate your key material using one of the following methods:

- "Backup and Restore" below
- "Cloning" on page 20

Backup and Restore

Cryptographic key material can be backed up from a release 5.x or 6.x SafeNet Luna USB HSM partition and then restored to a release 7.x SafeNet Luna Network HSM partition using a SafeNet Luna Backup HSM. The following procedure performs a backup of a 5.x/6.x partition on an older operating system to a SafeNet Luna Backup HSM. The Backup HSM is then moved to a newer operating system where the 5.x/6.x key material is restored to a 7.x partition.

Consult the 5.x/6.x/7.x CRN for a list of compatible operating systems. For general information on how to backup and restore an HSM partition, refer to the "Backup and Restore in General" on page 1.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the 5.x/6.x partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see "HSM Initialization" on page 1).

HSM Client software must be installed before attempting this procedure (see "SafeNet Luna HSM Client Software Installation" on page 1 for details). The source and destination partitions must be assigned to the client machine issuing the backup or restore command (see "Enable the Client to Access a Partition" on page 1 for details). Use **slot list** to ensure both partitions are visible to the client.

Preconditions

On the older operating system, the following instructions assume that:

- 5.x/6.x HSM Client Software is installed
- the source 5.x/6.x partition is visible
- the source partition's security policy allows cloning of private and secret keys
- the destination Backup HSM partition is visible

On the new operating system, the following instructions assume that:

- 7.x HSM Client Software is installed
- you have created an uninitialized partition on the 7.x Network HSM
- the destination 7.x partition is registered with the client software (visible)

- the source Backup HSM partition's security policy allows cloning of private and secret keys

Slots used in the following instructions:

On the older operating system running 5.x/6.x client software:

- Slot 0: the source 5.x/6.x partition
- Slot 2: the destination SafeNet Luna Backup HSM partition

On the new operating system running 7.x client software:

- Slot 1: the destination 7.x partition
- Slot 2: the source SafeNet Luna Backup HSM partition (with the backup of the 5.x/6.x partition)

Note: Partition login name requirements have changed with the hardware versions. With release 7.x , you can log in using the abbreviated **PO** (Partition Security Officer) or **CO** (Crypto Officer).

To backup/restore cryptographic keys from a 5.x/6.x partition to a 7.x partition using a Backup HSM

Follow these steps to back up all cryptographic material on a 5.x/6.x partition to a SafeNet Luna Backup HSM, and restore to a new 7.x partition.

1. On the old operating system running 5.x/6.x client software, run LunaCM and set the current slot to the 5.x/6.x partition.

   slot list

   slot set -slot 0

2. Log in as the Crypto Officer.

   Note: Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the "partition login" or "role login" commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type "Crypto Officer" in full (is case sensitive) and not "co".

   a. If you are backing up a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:

      partition login

   b. If you are backing up a release 6.x PPSO partition (Firmware 6.22.0 and up), use:

      role login -name Crypto Officer

3. Optional: To verify the objects in the 5.x/6.x partition to be backed up, use:

   partition contents

4. Back up the 5.x/6.x partition contents to the SafeNet Luna Backup HSM.

   partition archive backup -slot 2 -partition <backup_label>

   a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

   b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

Optionally, verify that all objects were backed up successfully on the SafeNet Luna Backup HSM by issuing the **partition contents** command.

5. Move the SafeNet Luna Backup HSM (with the backup of the 5.x/6.x partition) to the new operating system running the 7.x client software, and make sure it is visible to the client along with the 7.x HSM.
6. On the new operating system running the 7.x client software, run LunaCM, set the current slot to the 7.x partition, and initialize the partition and the PPSO role.

   slot set -slot 1

   partition init -label <7.x_partition_label>

   a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

   b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.
7. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

   role login -name po

   role init -name co

   If you are backing up a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

   role createchallenge -name co -challengesecret <password>
8. Set the current slot to the 7.x partition, log in as the Crypto Officer, and restore from backup.

   slot set -slot 1

   role login -name co

   partition archive restore -slot 2 -partition <backup_label>

   Afterwards, you can verify the partition contents on the 7.x partition:

   partition contents

Cloning

The simplest method of migrating key material to a new 7.x partition is slot-to-slot cloning. This procedure copies all permitted cryptographic material from a 5.x/6.x USB HSM partition to a 7.x Network HSM partition.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see "HSM Initialization" on page 1).

The 7.x client software should be installed, and the connection to both the source and destination partitions verified, before attempting this procedure (see "SafeNet Luna HSM Client Software Installation" on page 1 for details). The source and destination partitions must both be assigned to the client machine issuing the cloning commands (see "Enable the Client to Access a Partition" on page 1 for details). Use **slot list** to ensure both partitions are visible to the client.

If the source partition contains asymmetric keys, its security policy must allow cloning of private and secret keys. Use the command **partition showpolicies** in LunaCM to ensure that your source partition's security template allows this

(see "partition showpolicies" on page 1). If the 5.x/6.x HSM's security template does not allow cloning of private/secret keys, the HSM Admin may be able to turn this feature on using **partition changepolicy** (see "partition changepolicy" on page 1).

> **CAUTION:** Check your source partition policies and adjust them to be sure you can clone private and symmetric keys. Depending on the configuration of your partition and HSM, these policies may be destructive.

Preconditions

The following instructions assume that:

- the 7.x client software has been installed
- an uninitialized partition has been created on the 7.x Network HSM
- the destination 7.x partition must be registered with the client (visible)
- the source 5.x/6.x partition's security policy allows cloning of private and secret keys

In the following examples:

- Slot 0: the source 5.x/6.x partition
- Slot 1: the destination 7.x partition

> **Note:** Partition login name requirements have changed with the hardware versions. With release 7.x, you can log in using the abbreviated **PO** (Partition Security Officer) or **CO** (Crypto Officer).

To clone cryptographic keys from a 5.x/6.x partition to a 7.x partition

Follow these steps to clone all cryptographic material on a 5.x/6.x partition to a 7.x partition.

1. Run LunaCM, set the current slot to the 7.x partition, and initialize the Partition SO role.

   slot list

   slot set -slot 1

   partition init -label <7.x_partition_label>

   a. If you are cloning a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

   b. If you are cloning a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

   role login -name po

   role init -name co

   If you are cloning a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

   role createchallenge -name co -challengesecret <password>

3. Set the current slot to the source 5.x/6.x slot, log in as the Crypto Officer.

   slot set -slot 0

Note: Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the "partition login" or "role login" commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type "Crypto Officer" in full (is case sensitive) and not "co".

a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:

partition login

b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up) , use:

role login -name Crypto Officer

4. Optional: To verify the objects in the 5.x/6.x partition to be cloned, issue the "partition contents" command.

partition contents

5. Clone the objects to the 7.x partition slot (see "partition clone" on page 1 for correct syntax).

partition clone -objects 0 -slot 1

Afterward, you can set the current slot to the 7.x partition and verify that all objects have cloned successfully.

slot set -slot 1

role login -name co -password <password>

partition contents

You should see the same number of objects that existed on the 5.x/6.x HSM. You can now decommission the old 5.x/6.x HSM.

4

SafeNet PCIe HSM (5.x or 6.x) to SafeNet Luna Network HSM (7.x)

This chapter describes how to migrate your key material from a release 5.x or 6.x SafeNet PCIe HSM partition to a release 7.x SafeNet Luna Network HSM partition. You can migrate your key material using one of the following methods:

- "Backup and Restore" below
- "Cloning" on page 25

Backup and Restore

Cryptographic key material can be backed up from a release 5.x or 6.SafeNet Luna PCIe HSM partition and then restored to a release 7.x SafeNet Luna Network HSM partition using a SafeNet Luna Backup HSM. The following procedure performs a backup of a 5.x/6.x partition on an older operating system to a SafeNet Luna Backup HSM. The Backup HSM is then moved to a newer operating system where the 5.x/6.x key material is restored to a 7.x partition.

Consult the 5.x/6.x/7.x CRN for a list of compatible operating systems. For general information on how to backup and restore an HSM partition, refer to the "Backup and Restore in General" on page 1.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the 5.x/6.x partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see "HSM Initialization" on page 1).

HSM Client software must be installed on both operating systems (older and new) before attempting this procedure (see "SafeNet Luna HSM Client Software Installation" on page 1 for details). The destination partition must be assigned to the client machine (see "Enable the Client to Access a Partition" on page 1 for details). Use **slot list** to ensure partitions are visible to the client.

Preconditions

On the older operating system, the following instructions assume that:

- 5.x/6.x HSM Client Software is installed with "SafeNet Luna Backup HSM" option selected.
- the source 5.x/6.x partition is visible
- the source partition's security policy allows cloning of private and secret keys
- the destination Backup HSM partition is visible

On the new operating system, the following instructions assume that:

- 7.x HSM Client Software is installed with "SafeNet Luna Backup HSM" option selected.
- you have created an uninitialized partition on the 7.x Network HSM
- the destination 7.x partition is registered with the client software (visible)

- the source Backup HSM partition's security policy allows cloning of private and secret keys

Slots used in the following instructions:

On the older operating system running 5.x/6.x client software:

- Slot 0: the source 5.x/6.x partition
- Slot 2: the destination SafeNet Luna Backup HSM partition

On the new operating system running 7.x client software:

- Slot 1: the destination 7.x partition
- Slot 2: the source Backup HSM partition (with the backup of the 5.x/6.x partition)

Note: Partition login name requirements have changed with the hardware versions. With release 7.x , you can log in using the abbreviated **po** (Partition Security Officer) or **co** (Crypto Officer).

To backup/restore cryptographic keys from a 5.x/6.x partition to a 7.x partition using a Backup HSM

Follow these steps to back up all cryptographic material on a 5.x/6.x partition to a SafeNet Luna Backup HSM, and restore to a new 7.x partition.

1. On the old operating system running 5.x/6.x client software, run LunaCM and set the current slot to the 5.x/6.x partition.

   slot list

   slot set -slot 0

2. Log in as the Crypto Officer.

   Note: Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the "partition login" or "role login" commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type "Crypto Officer" in full (is case sensitive) and not "co".

   a. If you are backing up a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:

      partition login

   b. If you are backing up a release 6.x PPSO partition (Firmware 6.22.0 and up), use:

      role login -name Crypto Officer

3. Optional: To verify the objects in the 5.x/6.x partition to be backed up, use:

   partition contents

4. Back up the 5.x/6.x partition contents to the SafeNet Luna Backup HSM.

   partition archive backup -slot 2 -partition <backup_label>

   a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

   b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

Optionally, verify that all objects were backed up successfully on the SafeNet Luna Backup HSM by issuing the **partition contents** command.

5. Move the SafeNet Luna Backup HSM (with the backup of the 5.x/6.x partition) to the new operating system running the 7.x client software, and make sure it is visible to the client along with the 7.x HSM.
6. On the new operating system running the 7.x client software, run LunaCM, set the current slot to the 7.x partition, and initialize the partition and the PPSO role.

   slot set -slot 1

   partition init -label <7.x_partition_label>

   a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

   b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.
7. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

   role login -name po

   role init -name co

   If you are backing up a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

   role createchallenge -name co -challengesecret <password>
8. Set the current slot to the 7.x partition, log in as the Crypto Officer, and restore from backup.

   slot set -slot 1

   role login -name co

   partition archive restore -slot 2 -partition <backup_label>

   Afterwards, you can verify the partition contents on the 7.x partition:

   partition contents

Cloning

The simplest method of migrating key material to a new 7.x partition is slot-to-slot cloning. This procedure copies all permitted cryptographic material from a 5.x/6.x PCIe HSM partition to a 7.x Network HSM partition.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized . For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see "HSM Initialization" on page 1).

The 7.x client software should be installed, and the connection to both the source and destination partitions verified, before attempting this procedure (see "SafeNet Luna HSM Client Software Installation" on page 1 for details). The destination partition must be assigned to the client machine issuing the cloning commands (see "Enable the Client to Access a Partition" on page 1 for details). Use the **slot list** command to ensure both partitions are visible to the client.

If the source partition contains asymmetric keys, its security policy must allow cloning of private and secret keys. Use the command **partition showpolicies** in LunaCM to ensure that your source partition's security template allows this (see "partition showpolicies" on page 1). If the 5.x/6.x HSM's security template does not allow cloning of private/secret

keys, the HSM Admin may be able to turn this feature on using **partition changepolicy** (see "partition changepolicy" on page 1).

CAUTION: Check your source partition policies and adjust them to be sure you can clone private and symmetric keys. Depending on the configuration of your partition and HSM, these policies may be destructive.

Preconditions

On the operating system running 5.x/6/x client software, verify:

- that the 5.x/6.x PCIe HSM partition's security policy allows cloning of private and secret keys
- all key material on the 5.x/6.x PCIe HSM partition to be cloned

Regarding the operating system running 7.x client software, the following instructions assume that:

- the 7.x client software has been installed with "SafeNet Luna PCIe HSM" option selected.
- an uninitialized partition has been created on the 7.x HSM
- the destination 7.x HSM partition must be registered with the client (visible)
- the SafeNet Luna PCIe HSM card (with 5.x/6.x key material) has been installed

Slots used in the following instructions:

- Slot 0: the source 5.x/6.x SafeNet Luna PCIe HSM partition
- Slot 1: the destination 7.x partition

Note: Partition login name requirements have changed with the hardware versions. With release 7.x, you can log in using the abbreviated **po** (Partition Security Officer) or **co** (Crypto Officer).

To clone cryptographic keys from a 5.x/6.x partition to a 7.x partition

Follow these steps to clone all cryptographic material on a 5.x/6.x partition to a 7.x partition.

1. Run LunaCM, set the current slot to the 7.x partition, and initialize the Partition SO role.

   slot list

   slot set -slot 1

   partition init -label <7.x_partition_label>

   a. If you are cloning a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

   b. If you are cloning a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

   role login -name po

   role init -name co

   If you are cloning a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

   role createchallenge -name co -challengesecret <password>

3. Set the current slot to the source 5.x/6.x slot, log in as the Crypto Officer.

slot set -slot 0

> **Note:** Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the "partition login" or "role login" commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type "Crypto Officer" in full (is case sensitive) and not "co".

a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:

partition login

b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up) , use:

role login -name Crypto Officer

4. Optional: To verify the objects in the 5.x/6.x partition to be cloned, issue the "partition contents" command.

partition contents

5. Clone the objects to the 7.x partition slot (see "partition clone" on page 1 for correct syntax).

partition clone -objects 0 -slot 1

Afterward, you can set the current slot to the 7.x partition and verify that all objects have cloned successfully.

slot set -slot 1

role login -name co -password <password>

partition contents

You should see the same number of objects that existed on the 5.x/6.x HSM. You can now decommission the old 5.x/6.x HSM.

5

SafeNet Luna PCIe HSM or USB HSM (5.x or 6.x) to SafeNet Luna PCIe HSM (7.x)

This chapter describes how to migrate your key material from release 5.x or 6.x of the SafeNet Luna PCIe HSM or SafeNet USB HSM partition to release 7.x of the SafeNet Luna PCIe HSM partition. You can migrate your key material using one of the following three methods:

- "Backup and Restore" below
- "Cloning" on page 30
- "Cloning Using an HA Group" on page 32

Backup and Restore

Cryptographic key material can be backed up and then restored to a release 7.x SafeNet Luna PCIe HSM partition using a SafeNet Luna Backup HSM.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To backup and restore cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized. For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see "HSM Initialization" on page 1).

The 7.x client software should be installed, and the connection to both the source and destination partitions verified, before attempting this procedure (see "SafeNet Luna HSM Client Software Installation" on page 1 for details). The source and destination partitions must both be assigned to the client machine issuing the cloning commands (see "Enable the Client to Access a Partition" on page 1 for details). Use **slot list** to ensure both partitions are visible to the client.

Preconditions

The following instructions assume that:

- the 7.x client software has been installed
- an uninitialized partition has been created on the 7.x HSM
- the source and destination partitions are both registered with the client (visible)
- the source partition's security policy allows cloning of private and secret keys

In the following example:

- Slot 0: the source 5.x/6.x partition
- Slot 1: the destination 7.x partition

- Slot 2: the Backup HSM partition

> **Note:** Partition login name requirements have changed with the hardware versions. With release 7.x , you can log in using the abbreviated **po** (Partition Security Officer) or **co** (Crypto Officer).

To migrate cryptographic keys from a 5.x/6.x partition to a 7.x partition using a Backup HSM

Follow these steps to back up all cryptographic material on a 5.x/6.x partition to a Backup HSM, and restore to a new 7.x partition.

1. Run LunaCM, set the current slot to the 7.x partition, and initialize the partition and the Partition SO role.

   slot set -slot 0

   partition init -label <7.x_partition_label>

   a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

   b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

   role login -name po

   role init -name co

   If you are backing up a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

   role createchallenge -name co -challengeSecret <password>

3. Connect your backup HSM and make sure it is visible to the client, along with the 5.x/6.x and 7.x HSMs.

4. Set the current slot to the source 5.x/6.x slot.

   slot list

   slot set -slot 0

5. Log in as the Crypto Officer.

   > **Note:** Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the **partition login** or **role login** commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type **Crypto Officer** in full (is case sensitive) and not **co**.

   a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:

   partition login

   b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up) , use:

   role login -name Crypto Officer

6. Optional: To verify the objects in the 5.x/6.x partition to be cloned, issue the "partition contents" command.

   partition contents

7. Back up the 5.x/6.x partition contents to the Backup HSM.

partition archive backup -slot 2 -partition <backup_label>

a. If you are backing up a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

b. If you are backing up a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

Optionally, verify that all objects were backed up successfully on the Backup HSM by checking the partition contents.

8. Set the current slot to the 7.x partition, log in as the Crypto Officer, and restore from backup.

slot set -slot 1

role login -name co

partition archive restore -slot 2 -partition <backup_label>

Afterwards, you can verify the partition contents on the 7.x partition:

partition contents

Cloning

The simplest method of migrating key material to a new 7.x partition is slot-to-slot cloning. This procedure copies all permitted cryptographic material from a 5.x/6.x PCIe or USB HSM partition to a 7.x PCIe HSM partition.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized . For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see "HSM Initialization" on page 1).

The 7.x client software should be installed, and the connection to both the source and destination partitions verified, before attempting this procedure (see "SafeNet Luna HSM Client Software Installation" on page 1 for details). The source and destination partitions must both be assigned to the client machine issuing the cloning commands (see "Enable the Client to Access a Partition" on page 1 for details). Use **slot list** to ensure both partitions are visible to the client.

If the source partition contains asymmetric keys, its security policy must allow cloning of private and secret keys. Use the command **partition showpolicies** in LunaCM to ensure that your source partition's security template allows this (see "partition showpolicies" on page 1). If the 5.x/6.x HSM's security template does not allow cloning of private/secret keys, the HSM Admin may be able to turn this feature on using **partition changepolicy** (see "partition changepolicy" on page 1).

CAUTION: Check your source partition policies and adjust them to be sure you can clone private and symmetric keys. Depending on the configuration of your partition and HSM, these policies may be destructive.

Preconditions

The following instructions assume that:

- the 7.x client software has been installed
- an uninitialized partition has been created on the 7.x Network HSM

- the destination 7.x partition must be registered with the client (visible)
- the source 5.x/6.x partition's security policy allows cloning of private and secret keys

In the following examples:

- Slot 0: the source 5.x/6.x partition
- Slot 1: the destination 7.x partition

> **Note:** Partition login name requirements have changed with the hardware versions. With release 7.x, you can log in using the abbreviated **PO** (Partition Security Officer) or **CO** (Crypto Officer).

To clone cryptographic keys from a 5.x/6.x partition to a 7.x partition

Follow these steps to clone all cryptographic material on a 5.x/6.x partition to a 7.x partition.

1. Run LunaCM, set the current slot to the 7.x partition, and initialize the Partition SO role.

   slot list

   slot set -slot 1

   partition init -label <7.x_partition_label>

   a. If you are cloning a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

   b. If you are cloning a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

   role login -name po

   role init -name co

   If you are cloning a PED-authenticated 5.x/6.x partition, you can create an optional challenge secret for the Crypto Officer.

   role createchallenge -name co -challengesecret <password>

3. Set the current slot to the source 5.x/6.x slot, log in as the Crypto Officer.

   slot set -slot 0

   > **Note:** Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the "partition login" or "role login" commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type "Crypto Officer" in full (is case sensitive) and not "co".

   a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:

   partition login

   b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up) , use:

   role login -name Crypto Officer

4. Optional: To verify the objects in the 5.x/6.x partition to be cloned, issue the "partition contents" command.

   partition contents

5. Clone the objects to the 7.x partition slot (see "partition clone" on page 1 for correct syntax).

partition clone -objects 0 -slot 1

Afterward, you can set the current slot to the 7.x partition and verify that all objects have cloned successfully.

slot set -slot 1

role login -name co -password <password>

partition contents

You should see the same number of objects that existed on the 5.x/6.x HSM. You can now decommission the old 5.x/6.x HSM.

Cloning Using an HA Group

High Availability (HA) groups duplicate key material between the HSMs in the group. This function can be used to copy all cryptographic key material from a 5.x/6.x PCIe or USB HSM partition to a new 7.x PCIe HSM partition.

The new configuration's operating system must be compatible with both the new 7.x and the old 5.x/6.x hardware. Consult the 5.x/6.x CRN for a list of compatible operating systems.

To clone cryptographic keys from one HSM to another, the HSMs must share the same cloning domain. For password-authenticated HSMs, this domain should have been specified when the partition was initialized . For PED-authenticated HSMs, the red key determines the cloning domain. You will need the same red key that was imprinted during 5.x/6.x partition creation to initialize the 7.x partition (see "HSM Initialization" on page 1).

The 7.x client software should be installed, and the connection to both the source and destination HSM partitions verified, before attempting this procedure (see "SafeNet Luna HSM Client Software Installation" on page 1 for details). The source and destination partitions must both be assigned to the client machine issuing the cloning commands (see "Enable the Client to Access a Partition" on page 1 for details). Use **slot list** to ensure both partitions are visible to the client.

Note: It is not recommended to maintain an HA group with different versions of the SafeNet Luna Network HSM hardware.

Preconditions

The following instructions assume that:

- the 7.x client software has been installed
- an uninitialized partition has been created on the 7.x Network HSM
- the source and destination partitions are both registered with the client (visible)

In the following examples:

- Slot 0 = the source 5.x/6.x partition
- Slot 1 = the destination 7.x partition

Note: Partition login name requirements have changed between hardware versions. With release 7.x, you can log in using the abbreviated **po** (Partition Security Officer) or **co** (Crypto Officer).

To clone cryptographic keys from a 5.x/6.x partition to a 7.x partition using an HA group

Follow these steps to copy cryptographic material from an 5.x/6.x partition to a new 7.x partition by creating an HA group that includes both partitions.

1. Run LunaCM, set the current slot to the SA7 partition, and initialize the Partition SO role.

   slot set -slot 1

   partition init -label <7.x_partition_label>

   a. If you are cloning a PED-authenticated 5.x/6.x partition, use the 5.x/6.x partition's red key when prompted.

   b. If you are cloning a password-authenticated 5.x/6.x partition, enter the same cloning domain when prompted.

2. Log in as the **po** (Partition Security Officer) and initialize the **co** (Crypto Officer) role.

   role login -name po

   role init -name co

   If you are cloning a PED-authenticated 5.x/6.x partition, create a challenge secret for the Crypto Officer. This is required to set an HA activation policy.

   role createchallenge -name co -challengesecret <password>

3. Set the current slot to the source 5.x/6.x slot, log in as the Crypto Officer.

   slot set -slot 0

   Note: Be mindful of whether you're working with pre-PPSO or PPSO firmware and use the **partition login** or **role login** commands as specified below. Also, with PPSO firmware 6.22.0 and up, be careful with user names, i.e., type **Crypto Officer** in full (is case sensitive) and not **co**.

   a. If you are cloning a release 5.x or 6.x pre-PPSO partition (up to and including Firmware 6.21.2), use:

      partition login

   b. If you are cloning a release 6.x PPSO partition (Firmware 6.22.0 and up) , use:

      role login -name Crypto Officer

4. Optional: To verify the objects in the 5.x/6.x partition to be cloned, use:

   partition contents

5. Using LunaCM, create an HA group of the 5.x/6.x slot and the 7.x slot.

   Note: HA requires that all members have an activation policy set. See "Activation and Auto-Activation on PED-Authenticated Partitions" on page 1 for details.

   a. Via LunaSH, log in as Security Officer and set policy 22 on the 5.x/6.x partition:

      partition changepolicy -partition <5.x_partition_label> **-policy 22 -value 1**

   b. In LunaCM, log in to the 7.x partition as Partition Security Officer, and set the activation policy from the client machine:

      slot set -slot 1

      role login -name po

partition changepolicy -policy 22 -value 1

c. Create the HA group with the 5.x/6.x partition as the primary partition. Select the "copy" option to preserve objects.

hagroup creategroup -label <group_label> **-slot 0 -password** <password>

d. Add the 7.x partition slot to the HA group. Repeat this step to add multiple 7.x partitions to the group.

hagroup addmember -group <group_label> **-slot 1 -password** <password>

6. Synchronize the group to clone the objects to the 7.x member(s).

hagroup synchronize -group <group_label> **-password** <password>

7. Check synchronization status of the group.

hagroup listgroups

Notice the entry "`Needs sync: no`". This means that the objects have been successfully cloned among all members of the HA group. You can also log in to the 7.x slot as the Crypto Officer and check the partition contents.