Luna HSM 6.0.0

UPGRADE INSTRUCTIONS

Issue date: 27 May 2015

Document part number: 007-012226-005 Rev.A

Contents

Overview

This document describes how to upgrade your Luna SA, Luna PCI-E, and Luna G5 devices, and their supporting components, to Luna HSM 6.0.0 Depending on your specific product and the supporting components it uses, you might have to upgrade your client software, appliance software, and possibly HSM firmware. Detailed instructions are included for upgrading all products and components supported in Luna HSM 6.0.0.

About Luna HSM 6.0.0

For more information regarding Luna HSM 6.6.0, refer to the customer release notes. The most up-to-date version of the Luna HSM 6.0.x Customer Release Notes document is at:

http://www.securedbysafenet.com/releasenotes/luna/crn_luna_hsm_6-0.pdf

Reasons for Upgrade

If you have any Luna HSM 5.x at 5.2.3 or newer, you can upgrade to version 6.0.0 to obtain the value of newer features and fixes.

Upgrade Paths

Upgrade to this version from Luna SA, Luna PCI-E or Luna G5 at versions 5.2.1 or 5.2.2 or 5.2.3 or 5.3.0 or 5.3.1 or 5.4.

Component	Directly from version	To version
Luna SA client software	Any [see Note 1]	6.0
Luna SA appliance software	5.2.3-1 , 5.2.4-2, 5.2.6-1, 5.3.0-11, 5.3.1-1, 5.3.3-2, 5.3.5-1, 5.3.6-1, 5.4.0-13, 5.4.1-2, 5.4.2-2, 5.4.3-1, 5.4.4-2, 5.4.6-1, 5.4.7-1 [see Note 2]	6.0
HSM firmware	6.2.1, 6.10.2, 6.20.0, 6.21.0 [see Note 3]	6.22.0

[NOTE 1: LunaClient software replaces earlier versions with no dependencies, so you can uninstall any earlier version and install the latest, without intermediate steps.]

[NOTE 2: If Luna appliance software is older than version 5.2.3-1, you must update to appliance software version 5.2.3-1 before updating to appliance software version 6.0. Refer to the earlier upgrade documentation provided by SafeNet Technical Support.]

[NOTE 3: If HSM firmware is older than version 6.2.1, you must update to firmware version 6.2.1 before updating to firmware 6.22.0. Refer to the earlier upgrade documentation provided by SafeNet Technical Support.

Luna Backup HSMs can remain at their current firmware version, if you wish, and will work to backup and restore newer-firmware HSMs. Backup HSMs do not perform cryptographic operations on the objects that they archive, so there is no urgent requirement to update. At this writing, Luna Backup HSMs ship from the factory with firmware 6.0.8.]

> **Note:** Firmware can be left as-is (at the sacrifice of many newer features that require newer firmware),
> or can be upgraded to version 6.10.4, which is the current, in-evaluation FIPS candidate version, but which does not support all the features of Luna HSM 6.0,
> or can be upgraded to version 6.22.0, which supports all the latest features and fixes, but which is

not FIPS validated and which will not be submitted as an evaluation candidate (however a 6.22.x firmware is currently being developed and tested in anticipation of submission for FIPS evaluation).

Note: When you install Luna SA software, you displace the firmware version that was previously in standby. So, if you need FIPS validation and do not have firmware 6.10.4 in your appliance when that version receives FIPS validation, simply contact SafeNet and download a stand-alone firmware 6.10.4 upgrade package.

Component Firmware Versions

The following table lists the supported firmware versions for the various components supported in Luna HSM 6.0.0.

Component	Version
Luna SA and Luna PCI-E HSM firmware	6.22.0 *
Luna [Remote] Backup HSM firmware	6.22.0 *
Luna G5 firmware	6.22.0 *
Luna PED 2	2.4.0-3
Luna PED 2 Remote (Remote PED - requires PED workstation s/w on PC) [optional]	2.4.0-3
*You can upgrade LunaClient and (for Luna SA) the appliance software to version 6.0.0 while leaving the HSM firmware at version 6.2.1 or 6.10.4, but several Luna HSM 6.0.0 features are not supported without the latest firmware. Refer to the Luna HSM 6.0 Customer Release Notes for the list of new features, which indicates which ones are software-only, and which ones require firmware 6.22.0.	

Preparing for the Upgrade

Before attempting to upgrade to Luna HSM 6.0.0, ensure that you have satisfied the following prerequisites:

• you have the upgrade software (downloaded from the SafeNet Service Portal).

• you have the authentication credentials required to perform the upgrade.

• you have prepared your HSMs for the upgrade.

Each of these prerequisites is discussed in detail in the following sections.

Obtaining the Upgrade Software

All of the software and firmware required to upgrade to Luna HSM 6.0.0 is available via download from the SafeNet Service Portal (formerly Customer Connection Center or C3).

Note: Authorization codes are required to install firmware. To obtain the authorization codes for your firmware, contact SafeNet Technical Support.

The following packages are included in the upgrade software:

• Luna HSM 6.0.0 Client software

- Luna SA 6.0.0 appliance software
- Luna HSM 6.22.0 firmware

PED firmware (Refer to the readme.txt file included in the Luna HSM 6.0.0 client software for more information)

Required Authentication Credentials

You must be able to login to the HSM as the security officer (SO) to perform the upgrade. On PED-authenticated HSMs, you need the blue PED key. On password-authenticated HSMs, you need the SO password. On Luna SA, you also need to be able to login to the appliance using an admin-level account before you can login to the HSM as the SO.

To install the Luna Client software on a computer, you must run the installer with root/super-user privileges (Linux/UNIX) or Administrator privileges (Windows), or be able to launch the installer from an "Administrator: Command Prompt" (Windows).

Preparing your HSMs for the Upgrade

Perform the following tasks to prepare your HSM for the upgrade:

1. Ensure that your client and appliance software, and firmware, are at a version listed in the "Upgrade Paths" section above.

2. Connect your HSM appliance or host computer to an uninterruptible power supply (UPS), if available. Although this is not a requirement, use of a UPS is strongly recommended to ensure a successful completion of all upgrade activities.

3. Ensure that your USB devices (Luna G5, Luna Remote Backup HSM) are connected, using a USB cable, to the computer on which you are installing the Luna software. If the USB devices are not connected to the host computer, the USB drivers do not install successfully. This issue applies to Windows 2008 only.

4. If the Secure Recovery Key (SRK) on the HSM is enabled, it must be disabled before you can upgrade the HSM firmware. The SRK is an external split of the HSM's Master Tamper Key (MTK) that is imprinted on the purple PED key. When you disable the SRK, the SRV (Secure Recovery Vector) portion of the MTK is returned to the HSM, so that the SRV is no longer external to the HSM. It is only in this state that you can upgrade the HSM firmware. After you upgrade the firmware, you can re-enable SRK, if desired, to re-imprint a purple PED key with the SRV.

5. Backup the content of your HSM or HSM partitions to Luna SA Backup HSMs (if you have the Backup option).

6. Copy the Luna HSM 6.0.0 upgrade software package (the downloaded tar file) to the client computer and use your favorite archiving program to untar the archive.

7. Stop all applications and services that are using the HSM.

Performing the Upgrade

Depending on the product you are upgrading you might need to upgrade the client software, appliance software, and/or the HSM firmware, as specified in the following table:

Product	Client software upgrade	Appliance software upgrade	HSM firmware upgrade
Luna SA	X	X	X
Luna PCI-E	X		X
Luna G5	X		X
Luna Backup HSM	X		X

Upgrade the software/firmware in the following order:

1. Client software
2. Appliance software (Luna SA only)
3. HSM firmware

Upgrading the Client Software

> 📝 **Note:** Upgrade the client software before upgrading the appliance software or HSM firmware.

Overview - upgrading your client software consists of the following main steps:

1. Ensure that all applications using the Luna library are stopped.
2. Uninstall your old client software. When you uninstall your old Luna HSM client software, backups of your existing configuration file (all Luna HSM types), and certificates (Luna SA only), are retained so that they may be restored. Any other custom files/directories found in the client installation directory/folder that are not part of the standard client installation are also retained.
3. Install the Luna HSM 6.0.0 client software. On Linux/Unix, your backup configuration file and certificates are automatically restored. On Windows, your configuration file and certificates are retained.

To upgrade the client software to Luna HSM 6.0.0

1. Uninstall the currently installed Luna client software. The method you use is platform specific, as follows:
   - **Windows** Use the Windows uninstaller (Start > Control Panel > Programs and Features) to uninstall SafeNet LunaClient, which removes all of the Luna client software components.
   - **AIX/Linux** Run the /usr/safenet/lunaclient/bin/uninstall.sh script.
   - **HP-UX/Solaris** Run the /opt/safenet/lunaclient/bin/uninstall.sh script.
2. Install the Luna HSM 6.0.0 software. The method you use is platform specific, as follows:
   - **Windows** Run the LunaClient.msi installation program and respond to the prompts as they appear.
   - **Linux/Unix** Run the install.sh installation script and respond to the prompts as they appear.

Upgrading the Luna SA Appliance Software

> 📝 **Note:** Upgrade the Luna SA appliance software before you upgrade the Luna SA HSM firmware. The appliance software can be applied only to the Luna SA appliance.

> 📝 **Note:** Appliance software upgrade is a one-way operation. There is currently no way to downgrade the appliance software once a new version is applied. This contrasts with
> - LunaClient software, which can can be replaced by any version, simply by uninstalling the current version and installing a desired version, and
> - Luna HSM firmware, which can be rolled back to the version that was installed before the currently-installed version (applies only to versions since firmware rollback was enabled).

To upgrade the Luna SA Appliance software to Luna HSM 6.0.0

1. Copy the Luna HSM 6.0.0 appliance package file (.spkg) to the Luna SA appliance you want to upgrade:
   – Windows pscp <path>\<partnum>.spkg admin@<LunaSA_hostname>
   – Unix/Linux scp <path>/<partnum>.spkg admin@<LunaSA_hostname>
2. Stop all client applications that are connected to the Luna SA.
3. At the console, log in to the Luna SA appliance using an admin-level account (the default account is admin).
4. Log in to the Luna SA HSM as the HSM Security Officer:

   lunash :> hsm login

   – For Luna SA with PED authentication, the blue PED Key is required.
   – For Luna SA with Password Authentication, you are prompted for the HSM Admin (SO) password.
5. Verify that the upgrade package file that you copied is present (optional):

   lunash :> package listfile
6. Verify the upgrade package (optional):

   lunash :> package verify <partnum>.spkg -authcode <authorization_code>

   The verification process requires approximately 90 seconds.
7. Install the upgrade package:

   lunash :> package update <partnum>.spkg -authcode <authorization_code>

The installation/upgrade process takes approximately 90 seconds. During that time, a series of messages are displayed that detail the progress of the upgrade. At the end of this process, a message "Software upgrade completed!" is displayed.

Upgrading the HSM Firmware

> **Note:** Upgrade the HSM firmware only after you have upgraded the client software (and – for Luna SA – the appliance software). This ensures that the correct version is ready to be installed.

On Luna SA, use lunash (the Luna Shell) to upgrade the firmware. On Luna PCI-E and Luna G5, use lunacm to upgrade the firmware.

HSM Firmware 6.22.0 and FIPS 140-2

Luna HSMs with HSM firmware version 6.10.4 (from Luna HSM 5.2.2 or 5.2.3 release) are in the evaluation process for FIPS validation.

Firmware 6.22.0 implements some of the features of release 6.0.0, but will NOT be a FIPS-validation candidate (however a 6.22.x firmware is currently being developed and tested in anticipation of submission for FIPS evaluation).

Until firmware version 6.10.4 achieves validation, the validated firmware for Luna PCI-E and Luna SA is f/w 6.2.1; the validated firmware for Luna G5 is f/w 6.2.3. If you currently require FIPS validation, your HSM firmware must remain at those versions. The Luna Backup HSM continues to ship with firmware 6.0.8 with the same possibility to upgrade to newer firmware.

For Luna SA, if you update to Luna 6.0.0 software on the appliance (which includes the option to update the HSM firmware to 6.22.0), that would displace the standby firmware update option 6.10.4. When firmware 6.10.4 achieves FIPS validation (expected mid-2015), you would not have that upgrade option available on your Luna SA – having displaced it with firmware 6.22.0 as the standby upgrade option. For this reason, we provide a stand-alone firmware 6.10.4 upgrade package that you can download; contact SafeNet.

To upgrade the Luna SA HSM firmware

1. Log in to the HSM as the HSM admin user if you are not already logged in.

   lunash :> hsm login

2. Run the firmware upgrade command. The HSM will reset when the upgrade is complete:

   lunash :> hsm update firmware

3. Use the hsm show command to verify that the firmware upgrade was successful:

   lunash :> hsm show

   If the upgrade was successful, the firmware version is displayed as 6.22.0.

   > **Note:** If you did not reboot the appliance before upgrading the firmware (remote PED case) the following error message is displayed:
   > Error: Unable to communicate with HSM.
   > Please run 'hsm supportInfo' and contact customer support.
   >
   > You can ignore the error message.

4. If you disabled the SRK prior to performing the firmware upgrade, re-enable it if desired. Refer to the Luna documentation for details. If you attempted to upgrade the firmware without disabling the SRK, the firmware upgrade fails with the following error:

   Error: 'hsm update firmware' failed. (10A0B : LUNA_RET_OPERATION_RESTRICTED)

5. If you logged into the HSM using a remote PED, ensure that all client connections are terminated and then enter the following command to reboot the appliance:

sysconf appliance reboot

To upgrade the Luna PCI-E or Luna G5 HSM firmware

To upgrade the firmware on a Luna PCI-E or Luna G5 HSM, you run a lunacm command on a Luna HSM 5.4 client computer

• that contains a copy of the firmware upgrade (.fuf) file with its associated firmware authentication code (.txt) file, and

• contains the Luna PCI-E HSM, or

• is connected to the Luna G5 HSM that you want to upgrade.

1. Ensure that your client computer is running the Luna HSM 5.4 client software.

2. Copy the firmware file (<fw_filename>.fuf) from the firmware folder on the software CD to the Luna HSM 5.4 client root directory:

   – Windows: C:\Program Files\SafeNet\LunaClient

   – Linux/AIX: /usr/safenet/lunaclient/bin

   – Solaris/HP-UX: /opt/safenet/lunaclient/bin

3. Obtain the firmware authorization code:

   a. Contact SafeNet Customer Support (support@safenet-inc.com). The firmware authorization code is provided as a .txt file.

   b. Copy the <fw_auth_code>.txt file to the Luna HSM 5.4 client root directory:

   – Windows: C:\Program Files\SafeNet\LunaClient

- Linux/AIX: /usr/safenet/lunaclient/bin

- Solaris/HP-UX: /opt/safenet/lunaclient/bin

4. Launch the lunacm utility:

Windows
Open a Command Prompt window

(Start > Programs > Accessories > Command Prompt).

Change to the Luna G5 client root directory:

cd C:\Program Files\SafeNet\LunaClient

Enter the following command

Lunacm

Linux/AIX
Open a terminal window and change to the Luna G5 client root directory:

/usr/safenet/lunaclient/bin

Enter the following command:

./lunacm

HP-UX/Solaris
Open a terminal window and change to the Luna G5 client root directory:

/opt/safenet/lunaclient/bin

Enter the following command:

./lunacm

5. Enter the following command to login to the HSM. Note that the password is not required on PED-based systems:

hsm login [-password <password>]

6. Enter the following command to upgrade the firmware on the attached Luna G5 HSM:

hsm –updateFirmware –fuf <fw_filename>.fuf –authcode <fw_authcode_filename>.txt

Additional Tasks for Java Users

You must copy the Java library (LunaAPI.dll) and jar file (LunaProvider.jar) from the client installation folder/directory to the jre/lib/ext folder/directory.

Returning the HSM to Operation

After performing the upgrade, you must reactivate the HSM partitions (if applicable) and re-register the Luna client, to return the HSM to operation.

To return the HSM to operation

1. Updating the HSM firmware separates Luna G5 and Luna PCI-E HSM administration partition and client application partitions, which causes client applications to see them as separate slots, a change from previous behavior. Make any necessary adjustment to your scripts and application settings.

2. Updating can change slot numbering, specifically the starting slot number in a slot listing. Refer to the "Slot Numbering and Behavior" section in the Luna HSM Product Overview document. Other than that adjustment, for Luna PCI-E or Luna G5 your HSM is ready as soon as the firmware update is done.

3. Reactivate all partitions that were activated before the upgrade (applies to Luna SA with PED Authentication).

Migration Notes

Luna HSM 6.0 introduces significant changes to way in which the product operates. This section describes the tasks you might need to perform to successfully migrate your HSMs to Luna HSM 6.0.

PCI-E or G5 HA groups

Firmware 6.22.0 changes how you see your Luna PCI-E and G5 HSMs. In previous releases, each slot represented a physical HSM. With 6.22.0 firmware, each physical HSM is divided into two distinct partitions, as follows:

- an Admin partition. The Admin partition is reserved for the HSM SO role, and uses the original (pre-6.22.0), HSM Serial Number.

- a User partition. The User partition is used by the Partition Owner/Crypto Officer for cryptography. It is assigned a new serial number, created by appending 3 digits to the original serial number.

Virtual slots, used to configure HA groups, are also viewed as user partitions, and are therefore also assigned new serial numbers.

If you are using PCI-E or G5 devices in HA mode, you must edit your **Chrystoki.conf** (Linux/Unix) or **Chrystoki.ini** (Windows) file to update the partition serial numbers for the HA group members.

Behavior with firmware older than 6.22.0

Before firmware version 6.22.0, LunaCM did not make Luna PCI-E and Luna G5 user partitions visible. The following example shows how LunaCM displays PCI-E, G5, and HA virtual slots with pre-6.22.0 firmware. Note that the HA group is shown at Slot Id 5.

Example

```
Available HSMs:

Slot Id ->              0
Tunnel Slot Id ->       1
HSM Label ->            pcie_hsm1
HSM Serial Number ->    155316
HSM Model ->            K6 Base
HSM Firmware Version -> 6.21.0
HSM Configuration ->    Luna PCI (PED) Signing With Cloning Mode
HSM Status ->           OK

Slot Id ->              1
Tunnel Slot Id ->       2
HSM Label ->            pcie_hsm2
HSM Serial Number ->    155317
HSM Model ->            K6 Base
HSM Firmware Version -> 6.21.0
HSM Configuration ->    Luna PCI (PED) Signing With Cloning Mode
HSM Status ->           OK

Slot Id ->              5
HSM Label ->            PCIHA
HSM Serial Number ->    1155316
HSM Model ->            LunaVirtual
HSM Firmware Version -> 6.21.0
HSM Configuration ->    Luna Virtual HSM (PED) Signing With Cloning Mode
HSM Status ->           N/A - HA Group
```

HA group definition in the Chrystoki.conf/Crystoki.ini file

The members of the HA group shown in slot 5 are defined in the **VirtualToken** section of the **Chrystoki.conf/Crystoki.ini** file, as illustrated below:

```
VirtualToken = {
VirtualToken00Label = PCIHA;
VirtualToken00SN = 1155316;
VirtualToken00Members = 155316,155317;
}
```

Behavior with 6.22.0 firmware

With firmware 6.22.0, LunaCM makes the user partition visible: it has its own serial number derived from the HSM's serial number. The following example shows the output of LunaCM for the same hardware after upgrading to the 6.22.0 firmware.

Note the user partition labeled **Cryptoki User** with serial number **155316014** is distinct from the HSM partition with label **pcie_hsm1** and serial number **155316**. Note also that LunaCM does not identify the HA group. This is because the serial number of the HSM user partition changed, and no longer matches the value in the HA members list in the **Chrystoki.conf** or **Crystoki.ini** file.

Example

```
Available HSMs:

Slot Id ->              0
Tunnel Slot Id ->       6
Label ->                Cryptoki User
Serial Number ->        155316014
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna User Partition, No SO (PED) Signing With Cloning Mode
Slot Description ->      User Token Slot

Slot Id ->              5
Tunnel Slot Id ->       6
Label ->                pcie_hsm1
Serial Number ->        155316
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description ->      Admin Token Slot
HSM Configuration ->    Luna HSM Admin Partition (PED)
HSM Status ->           OK

Slot Id ->              6
Tunnel Slot Id ->       12
Label ->                Cryptoki User
Serial Number ->        155317014
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna User Partition, No SO (PED) Signing With Cloning Mode
Slot Description ->      User Token Slot

Slot Id ->              11
Tunnel Slot Id ->       12
Label ->                pcie_hsm2
Serial Number ->        155317
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description ->      Admin Token Slot
```

```
HSM Configuration ->    Luna HSM Admin Partition (PED)
HSM Status ->           OK
```

Changes required to the Chrystoki.conf/Crystoki.ini file to restore the HA group definition

To restore the HA group configuration, you must edit the **Chrystoki.conf/Crystoki.ini** file to update the virtual token slot serial numbers to include the three extra digits added to the user slot serial numbers after upgrading to firmware 6.22.0 (in this example, the extra digits are **014**). You must add the three digits to the **VirtualToken**<nn>**SN** and **VirtualToken**<nn>**Members** entries, as shown in the following example:

Before upgrading to firmware 6.22.0

```
VirtualToken = {
VirtualToken00Label = PCIHA;
VirtualToken00SN = 1155316;
VirtualToken00Members = 155316,155317;
}
```

After upgrading to firmware 6.22.0

```
VirtualToken = {
VirtualToken00Label = PCIHA;
VirtualToken00SN = 1155316014;
VirtualToken00Members = 155316014,155317014;
}
```

Updating Your HA Group Configurations After Upgrading to Firmware 6.22.0

The following procedure describes, in detail, the steps you need to perform to reconfigure your HA group definitions in the **Chrystoki.conf/Crystoki.ini** file after upgrading to firmware 6.22.0.

To update your HA group definitions

1. Update all members of the HA group to firmware 6.22.0.

2. Ensure that you have write access to **/etc/Chrystoki.conf** (Linux/UNIX) or **chrystoki.ini** (Windows, in the Luna client installation directory).

3. Edit the **Chrystoki.conf/Crystoki.ini** file and navigate to the **VirtualToken** section. Each virtual token is defined by three entries, as follows:

   – **VirtualToken**<nn>**Label**. For example, `VirtualToken00Label`

   – **VirtualToken**<nn>**SN**. For example, `VirtualToken00SN`

   – **VirtualToken**<nn>**Members**. For example, `VirtualToken00Members`

   where <nn> starts at 00 and increments by one for each HA group

   You will need to modify the value of **VirtualToken**<nn>**Members** for each virtual token in the file to reflect its new serial number.

4. In LunaCM, enter the **partition list** command to determine the new serial numbers for the HA group members:

```
Available HSMs:
Slot Id ->            0
Tunnel Slot Id ->     6
Label ->              Cryptoki User
Serial Number ->      155316014
Model ->              K6 Base
Firmware Version ->   6.22.0
Configuration ->      Luna User Partition, No SO (PED) Signing With Cloning Mode
Slot Description ->   User Token Slot

Slot Id ->            5
```

```
Tunnel Slot Id ->        6
Label ->                 pcie_hsm1
Serial Number ->         155316
Model ->                 K6 Base
Firmware Version ->      6.22.0
Configuration ->         Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description ->      Admin Token Slot
HSM Configuration ->     Luna HSM Admin Partition (PED)
HSM Status ->            OK

Slot Id ->               6
Tunnel Slot Id ->        12
Label ->                 Cryptoki User
Serial Number ->         155317014
Model ->                 K6 Base
Firmware Version ->      6.22.0
Configuration ->         Luna User Partition, No SO (PED) Signing With Cloning Mode
Slot Description ->      User Token Slot

Slot Id ->               11
Tunnel Slot Id ->        12
Label ->                 pcie_hsm2
Serial Number ->         155317
Model ->                 K6 Base
Firmware Version ->      6.22.0
Configuration ->         Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description ->      Admin Token Slot
HSM Configuration ->     Luna HSM Admin Partition (PED)
HSM Status ->            OK
```

5. For each serial number in **VirtualToken**<nn>**Members** find the slot with the matching serial number prefix, and take note of the three additional digits. Look for this information in slots with `Slot Desciption ---> User Token Slot`.

   For example, for `VirtualToken00Members = 155316,155317,` the new serial numbers displayed in LunaCM are 155316**014** and 155317**014**.

6. Add the last portion (**014** in our example) to the serial number for each virtual token member. In our example the new values after the modifications are:

   `VirtualToken00Members = 155316014,155317014;`

7. Next adjust the value of **VirtualToken**<nn>**SN** in a similar manner. In our example, the adjusted value is 1155316014.

8. When you have updated the serial number for all virtual tokens and members, save the file.

9. If the HSMs are PED-AUTH, log in to each user partition slot (where Slot Description --> User Token Slot), one at the time, and enter the following LunaCM commands to activate the partition (the activation policy remains on after firmware update).

   slot set -slot <slot_id>
   role login -n "Crypto Officer"

   You will be prompted for the challenge in LunaCM, and for the black key at the attached PED device. Successful login will activate your partition.

10. You should now be able to see your virtual token (HA group). First, restart LunaCM in one of following two ways:

    – Exit from LunaCM by typing **exit** and launch LunaCM again

    – From the lunacm:> prompt, enter **clientconfig restart -force**

    LunaCM output for our example now shows:

```
Available HSMs:
Slot Id ->              0
Tunnel Slot Id ->       6
Label ->                Cryptoki User
Serial Number ->        155316014
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna User Partition, No SO (PED) Signing With Cloning Mode
Slot Description ->     User Token Slot

Slot Id ->              5
Tunnel Slot Id ->       6
Label ->                pcie_hsm1
Serial Number ->        155316
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description ->     Admin Token Slot
HSM Configuration ->    Luna HSM Admin Partition (PED)
HSM Status ->           OK

Slot Id ->              6
Tunnel Slot Id ->       12
Label ->                Cryptoki User
Serial Number ->        155317014
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna User Partition, No SO (PED) Signing With Cloning Mode
Slot Description ->     User Token Slot

Slot Id ->              11
Tunnel Slot Id ->       12
Label ->                pcie_hsm2
Serial Number ->        155317
Model ->                K6 Base
Firmware Version ->     6.22.0
Configuration ->        Luna HSM Admin Partition (PED) Signing With Cloning Mode
Slot Description ->     Admin Token Slot
HSM Configuration ->    Luna HSM Admin Partition (PED)
HSM Status ->           OK

Slot Id ->              8
HSM Label ->            PCIHA
HSM Serial Number ->    1155316014
HSM Model ->            LunaVirtual
HSM Firmware Version -> 6.22.0
HSM Configuration ->    Luna Virtual HSM (PED) Signing With Cloning Mode
HSM Status ->           N/A - HA Group
```

Support Contacts

If you encounter a problem while installing, registering or operating this product, please ensure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support. SafeNet support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact method	Contact	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	Global	+1 410-931-7520
	Australia	1800.020.183
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	000.800.100.4290
	Netherlands	0800.022.2996
	New Zealand	0800.440.359
	Portugal	800.1302.029
	Singapore	800.863.499
	Spain	900.938.717
	Sweden	020.791.028
	Switzerland	0800.564.849
	United Kingdom	0800.056.3158
	United States	(800) 545-6608
Web	www.safenet-inc.com	
Support and Downloads	www.safenet-inc.com/support Provides access to the SafeNet Knowledge Base and quick downloads for various products.	
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	