SafeNet HSM 6.2

UPGRADE INSTRUCTIONS

Issue date: 18 December 2015

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

Contents

Overview

This document describes how to upgrade your SafeNet Network HSM, SafeNet PCI-E HSM, and SafeNet USB HSM devices, and their supporting components, to SafeNet HSM 6.2.0. 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 SafeNet HSM 6.2.0.

About SafeNet HSM 6.2.0

For more information regarding SafeNet HSM 6.2.0, refer to the customer release notes. The most up-to-date version of the Luna HSM 6.2.x Customer Release Notes document is at:

http://www.securedbysafenet.com/releasenotes/luna/crn_luna_hsm_6-2.pdf

Product Rebranding

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

Old product name	New product name
Luna SA HSM	SafeNet Network HSM
Luna PCI-E HSM	SafeNet PCI-E HSM
Luna G5 HSM	SafeNet USB HSM
Luna PED	SafeNet PED
Luna Client	SafeNet HSM Client
Luna Backup HSM	SafeNet Backup HSM
Luna CSP	SafeNet CSP
Luna JSP	SafeNet JSP
Luna KSP	SafeNet KSP

Note: The Luna name is retained for some SafeNet HSM software tools, such as LunaCM, LunaSH, LunaProvider, and Lunadiag. The device names displayed by these tools will also use the old names.

Reasons for Upgrade

If you have any SafeNet HSM at 5.4.7 or newer, you can upgrade to version 6.2.0 to obtain the value of newer features and fixes.

Upgrade Paths

Upgrade to this version from SafeNet Network HSM, SafeNet PCI-E HSM or SafeNet USB HSM at versions 5.4.7 or 6.0.0 or 6.1.0.

Component	Directly from version	To version
Safenet HSM Client software	Any [see Note 1]	6.2
SafeNet Network HSM appliance software	5.4.7-1, 6.0.0, 6.1.0 [see Note 2]	6.2
HSM firmware	6.2.x, 6.10.x, 6.20.x, 6.21.x, 6.22.x, 6.23.x [see Note 3]	6.24.0
[NOTE 1: SafeNet HSM Client software replaces earlier versions with no dependencies, so you can uninstall any earlier version and install the latest without intermediate steps.]		
[NOTE 2: If your SafeNet Network HSM appliance software is not listed, contact SafeNet Technical Support to upgrade.]		
[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 6.24.0. Refer to the earlier upgrade documentation provided by SafeNet Technical Support.		

Note: When you install SafeNet Network HSM software, you displace the firmware version that was previously in standby. So, if you need FIPS validation and do not have firmware 6.10.9 in your appliance, simply contact SafeNet and download a stand-alone firmware 6.10.9 upgrade package.

Component Firmware Versions

The following table lists the supported firmware versions for the various components supported in SafeNet HSM 6.2.0.

Component	Version
SafeNet Network HSM and SafeNet PCI-E HSM firmware	6.24.0 *
SafeNet Remote Backup HSM firmware	6.10.9 *
SafeNet USB HSM firmware	6.24.0 *
SafeNet PED 2	2.4.0-3 through 2.6.0
SafeNet PED 2 Remote (Remote PED - requires PED workstation s/w on PC) [optional]	2.4.0-3 through 2.6.0
*You can upgrade SafeNet HSM Client and (for SafeNet Network HSM) the appliance software to version 6.2.0 while leaving the HSM firmware at lower firmware versions, but several SafeNet HSM 6.2.0 features are not supported without the latest firmware. Refer to the SafeNet HSM 6.2 Customer Release Notes for the list of new features, which indicates which ones are software-only, and which ones require firmware 6.24.0. We recommend that you upgrade SafeNet Remote Backup HSM to 6.10.9, which is a FIPS-validated version. Follow the same upgrade procedure as for a SafeNet USB HSM. It is not necessary to upgrade SafeNet Remote Backup HSMs beyond 6.10.9, as they work to backup and restore newer-firmware HSMs.	

Preparing for the Upgrade

Before attempting to upgrade to SafeNet HSM 6.2.0, ensure that you have satisfied the following prerequisites:

- you have the upgrade software (downloaded from the Gemalto 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 SafeNet HSM 6.2.0 is available via download from the Gemalto 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:

- SafeNet HSM 6.2.0 client software
- SafeNet Network HSM 6.2.0 appliance software
- SafeNet HSM 6.24.0 firmware
- PED firmware (Refer to the readme.txt file included in the SafeNet HSM 6.2.0 client software for more information)

Required Authentication Credentials

You must be able to log in 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 SafeNet Network HSM, you also need to be able to log in to the appliance using an admin-level account before you can log in to the HSM as the SO.

To install the SafeNet HSM 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 software, appliance software, and firmware are at a starting 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 successful completion of all upgrade activities.
3. Ensure that your USB devices (SafeNet USB HSM, SafeNet 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 SafeNet Network HSM Backup HSMs (if you have the Backup option).
6. Copy the SafeNet HSM 6.2.0 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.
8. Disable HSM policy 39 (Allow Secure Trusted Channel). You can re-enable this policy after upgrade.

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
SafeNet Network HSM	X	X	X
SafeNet PCI-E HSM	X		X
SafeNet USB HSM	X		X
SafeNet Backup HSM	X		X

Upgrade the software/firmware in the following order:

1. Client software
2. Appliance software (SafeNet Network HSM 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 SafeNet HSM software libraries are stopped.
2. Uninstall your old client software. When you uninstall your old SafeNet HSM client software, backups of your existing configuration file (all SafeNet HSM types), and certificates (SafeNet Network HSM 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 SafeNet HSM 6.2.0 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 SafeNet HSM 6.2.0

1. Uninstall the currently installed SafeNet HSM 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 HSM Client, which removes all of the SafeNet HSM 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 SafeNet HSM 6.2.0 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 SafeNet Network HSM Appliance Software

Note: Upgrade the SafeNet Network HSM appliance software before you upgrade the SafeNet Network HSM firmware. The appliance software can be applied only to the SafeNet Network HSM 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
- SafeNet HSM Client software, which can be replaced by any version, simply by uninstalling the current version and installing a desired version, and
- SafeNet HSM firmware, which can be rolled back to the version that was installed before the currently-installed version. This applies only to versions since firmware rollback was enabled.

To upgrade the SafeNet Network HSM Appliance software to Luna HSM 6.2.0

1. Copy the SafeNet HSM 6.2.0 appliance package file (.spkg) to the SafeNet Network HSM 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 SafeNet Network HSM.
3. At the console, log in to the SafeNet Network HSM appliance using an admin-level account. The default account is admin.
4. Log in to the SafeNet Network HSM as the HSM Security Officer:

   lunash :> hsm login
   - For SafeNet Network HSM with PED authentication, the blue PED Key is required.
   - For SafeNet Network HSM with Password Authentication, you are prompted for the HSM Admin (SO) password.
5. (Optional) Verify that the upgrade package file that you copied is present:

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

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

   Verification 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, the 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 SafeNet Network HSM – the appliance software). This ensures that the correct version is ready to be installed.

On SafeNet Network HSM, use LunaSH (the Luna Shell) to upgrade the firmware. On SafeNet PCI-E HSM, SafeNet USB HSM and SafeNet Remote Backup HSM, use LunaCM to upgrade the firmware.

HSM Firmware 6.24.0 and FIPS 140-2

Firmware 6.24.0 implements some of the features of release 6.2.0, but is not currently FIPS-validated. We plan to seek validation for 6.24.0 in the near future.

For SafeNet Network HSM, when you update to SafeNet HSM 6.2.0 software on the appliance, you have the option to also immediately update the firmware to 6.24.0, or to place 6.24.0 firmware on standby, available to be installed later. If you decide not to update the firmware to 6.24.0 because you wish to use FIPS validated firmware, we strongly recommend upgrading to 6.10.9. You can obtain a stand-alone 6.10.9 upgrade package from Gemalto's service portal. It is possible to upgrade to higher firmware versions to obtain desired features, but doing so loses the appliance's FIPS validated status.

> **Note:** If you have a PKI bundle including a SafeNet Network HSM and an attached SafeNet USB HSM running in PKI mode, often the SafeNet USB HSM has earlier firmware than the SafeNet Network HSM. Upgrade the SafeNet Network HSM first, following the above upgrade paths. Then, when you upgrade the firmware on the associated SafeNet USB HSM, the SafeNet USB HSM upgrades to the same firmware version as is installed on the SafeNet Network HSM.

Upgrading SafeNet Network HSM firmware

On SafeNet Network HSM, use LunaSH (the Luna Shell) to upgrade the 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 6.24.0.

> **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 SafeNet HSM 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

Upgrading the SafeNet PCI-E HSM or SafeNet USB HSM/SafeNet Backup HSM firmware

To upgrade the firmware on a SafeNet PCI-E HSM or SafeNet USB HSM/SafeNet Backup HSM, run a LunaCM command on a SafeNet HSM client computer

- that contains a copy of the firmware upgrade (.fuf) file with its associated firmware authentication code (.txt) file, and
- contains the SafeNet PCI-E HSM, or
- is connected to the SafeNet USB HSM/SafeNet Backup HSM that you want to upgrade.

1. Copy the firmware file (<fw_filename>.fuf) from the firmware folder on the software CD to the SafeNet HSM client root directory:
   - Windows: C:\Program Files\SafeNet\LunaClient
   - Linux/AIX: /usr/safenet/lunaclient/bin
   - Solaris/HP-UX: /opt/safenet/lunaclient/bin
2. 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 SafeNet HSM client root directory:
   - Windows: C:\Program Files\SafeNet\LunaClient
   - Linux/AIX: /usr/safenet/lunaclient/bin
   - Solaris/HP-UX: /opt/safenet/lunaclient/bin
3. Launch the LunaCM utility:

   Windows

   a. Open a Command Prompt window

      (Start > Programs > Accessories > Command Prompt).

   b. Change to the SafeNet HSM client root directory:

      cd C:\Program Files\SafeNet\LunaClient

   c. Enter the following command

      Lunacm

   Linux/AIX

   a. Open a terminal window and change to the SafeNet HSM client root directory:

      /usr/safenet/lunaclient/bin

   b. Enter the following command:

      ./lunacm

   HP-UX/Solaris

   a. Open a terminal window and change to the SafeNet HSM client root directory:

/opt/safenet/lunaclient/bin

b. Enter the following command:

./lunacm

4. Enter the following command to log in to the HSM. Note that the password is not required on PED-based systems:

hsm login [-password <password>]

5. Enter the following command to upgrade the firmware on an attached SafeNet USB 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 to the jre/lib/ext folder.

Returning the HSM to Operation

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

To return the HSM to operation

1. If updating from firmware below 6.22.0, upgrade separates SafeNet USB HSM and SafeNet PCI-E HSM administration partition and client application partitions, which causes client applications to see them as separate slots. This is a change from previous behavior. Make any necessary adjustments to your scripts and application settings.
2. If updating from firmware below 6.22.0, upgrading can change slot numbering, specifically the starting slot number in a slot listing. Refer to the "Slot Numbering and Behavior" section in the *HSM Administration Guide*. Other than that adjustment, for SafeNet PCI-E HSM or SafeNet USB HSM your HSM is ready as soon as the firmware update is done.
3. Reactivate all partitions that were activated before the upgrade (applies to SafeNet Network HSM with PED Authentication).

Migration Notes

SafeNet HSM 6.2 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 SafeNet HSM 6.2, if you are starting from a firmware version lower than 6.22.0.

PCI-E or G5 HA groups

> **Note:** This section only applies if you are upgrading from a firmware version lower than 6.22.0 to a firmware version that is 6.22.0 or higher.

Firmware 6.22.0 and above changes how you see your SafeNet PCI-E HSM and G5 HSMs. In previous releases, each slot represented a physical HSM. With 6.22.0 or higher 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 SafeNet PCI-E HSM and SafeNet USB HSM 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 or higher firmware

With firmware 6.22.0 or higher, 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 or above (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 or above

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

```
}
```

After upgrading to firmware 6.22.0 or above

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

Updating Your HA Group Configurations After Upgrading to Firmware 6.22.0 or above

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 or above.

To update your HA group definitions

1. Update all members of the HA group to firmware 6.22.0 or above.
2. Ensure that you have write access to **/etc/Chrystoki.conf** (Linux/UNIX) or **chrystoki.ini** (Windows, in the SafeNet HSM 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 Gemalto support. Gemalto 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 Gemalto 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

Contact method	Contact	
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.	