Luna PCI-E

Configuration Guide

SafeNet

THE DATA PROTECTION COMPANY

Document Information

Product Version	5.4.1
Document Part Number	007-011329-006
Release Date	04 July 2014

Revision History

Revision	Date	Reason
A	26 February 2014	Initial release.
B	17 April 2014	Updates to the SFF Backup feature.
C	04 July 2014	Solaris client support.

Trademarks

Disclaimer

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

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

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

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA
Email	techpubs@safenet-inc.com

CONTENTS

PREFACE

About the Configuration Guide

This document describes how to configure your HSM to get it ready to operate in your environment. It contains the following chapters:

- "Configuring a Password-Authenticated HSM" on page 7
- "Configuring a PED-Authenticated HSM" on page 23
- "Optional Configuration Tasks" on page 48

This preface also includes the following information about this document:

- "Customer Release Notes" on page 4
- "Audience" on page 4
- "Document Conventions" on page 4
- "Support Contacts" on page 6

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 for this release at the following location:

- http://www.securedbysafenet.com/releasenotes/luna/crn_luna_hsm_5-4.pdf

Audience

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

All products manufactured and distributed by SafeNet, Inc. 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

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.

Table 1: Technical support contacts

Contact method	Contact	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	(800) 545-6608, (410) 931-7520
	Australia and New Zealand	+1 410-931-7520
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	+1 410-931-7520
	United Kingdom	0870 7529200, +1 410-931-7520
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.	
Customer Technical Support Portal	https://serviceportal.safenet-inc.com Existing customers with a Customer Connection Center account, or a Service Portal account, can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	

CHAPTER 1

Configuring a Password-Authenticated HSM

This chapter describes how to configure a password-authenticated HSM to get it ready to operate in your environment. It contains the following sections:

Overview

The HSM is available in PED-authenticated or password-authenticated versions. Use the configuration steps in this chapter to configure a password-authenticated HSM.

There is no externally visible difference between a password-authenticated or PED-authenticated HSM. For an installed HSM, you can determine its mode of authentication by attempting to log in. A Trusted Path version will direct you to the Luna PED. A Password Authenticated version will prompt you for the password. You cannot change the authentication type of a Luna HSM. It is a manufacturing configuration, set at the factory. If you have a PED-authenticated (Trusted Path) version, you cannot access the HSM and partitions by means of passwords.

For password-authenticated HSMs, you authenticate to the HSM as Security Officer, or User, etc., by typing a password on your computer keyboard. This has the advantage of not requiring any additional hardware - you just have to remember the appropriate password. On the other hand, any password you type on a computer is vulnerable to being seen by someone watching, or by mal-ware that logs your keystrokes or otherwise records what you type. Also, if the password is strong enough to be secure, it might be complicated enough that personnel are tempted to write it down - another avenue of possible exposure.

High-Level Configuration Steps

1. Initialize the HSM, as described in "Initializing a Password-Authenticated Luna PCI-E HSM" on page 8.
2. Change the HSM policies, if desired, as described in "Setting Luna PCI-E HSM Policies [Optional]" on page 9. If any of the policies you set are destructive, you must re-initialize the HSM after setting the polices.
3. Create a partition on the HSM, as described in "Creating a Partition on Luna PCI-E HSM" on page 15.
4. Change the partition policies, if desired, as described in "Setting Luna PCI-E Partition Policies [Optional]" on page 19

Initializing a Password-Authenticated Luna PCI-E HSM

Initialization assigns a meaningful label and a Security Officer password, and places the HSM in a state ready to use. You cannot log into the HSM until it has been initialized with an authentication secret (a password).

Use these instructions if you have Luna PCI-E with Password authentication.

> **Note:** Some HSM Policy changes are destructive. A destructive policy change is one that requires the HSM to be initialized again, before it can be used. However, you must log in before you can perform such a policy change. Thus if you intend to perform a destructive HSM Policy change, you might need to perform this initialization step again, after the Policy change.

To initialize the HSM

1. This example shows the dialog for a Luna PCI-E 5.x HSM with Cloning. To perform HSM operations, you must be addressing the correct slot. If you have just one Luna PCI-E HSM installed, then by default it is slot 1. Run lunacm and begin the initialization process:

```
C:\Program Files\SafeNet\LunaClient>lunacm
LunaCM V2.3.3 - Copyright (c) 2006-2010 SafeNet, Inc.
Available HSMs:
Slot Id ->              1
Tunnel Slot Id ->       2
HSM Label ->            no label
HSM Serial Number ->    150051
HSM Model ->            K6Base
HSM Firmware Version -> 6.0.8
HSM Configuration ->    Luna PCI (PW) Undefined Mode / Uninitialized
Current Slot Id: 1
lunacm:> hsm init -label myluna1 -domain hard_to_gue$$
You are about to initialize the HSM that is in the
factory reset (zeroized) state.
Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now -> proceed
Option -password was not supplied.  It is required.
Enter the password: *********
Re-enter the password: *********
Command Result : No Error
lunacm:> hsm login
Option -password was not supplied.
It is required.
Enter the password: *********
Command Result : No Error
lunacm:>
```

   If you were to exit and restart the lunacm utility, you would see the new label that you have just applied to the HSM. The password would not be displayed.

2. The next step is to create a partition on the HSM. See "Creating a Partition on Luna PCI-E HSM" on page 15.

About the Domain

Always specify a cloning domain when you initialize a Password Authenticated Luna PCI-E HSM in a production environment. The HSM allows you to omit a specific domain at initialization, and instead uses the 'factory-default' domain. This is insecure. Anyone could clone objects to or from such an HSM. The default domain is useful in a lab or

integration/development setting. However, when you prepare a Luna HSM to go into service in a real "production" environment, always specify a proper, secure domain string when you initialize.

```
lunacm:> hsm init -label myluna1
You are about to initialize the HSM that is in the
factory reset (zeroized) state.
Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now -> proceed
Option -password was not supplied.  It is required.
Enter the password: *********
Re-enter the password: *********
Option -domain not specified.
If you proceed, the default domain will be used.
You will not be creating a new domain.
Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now -> proceed
Command Result : No Error
lunacm:>
```

Setting Luna PCI-E HSM Policies [Optional]

HSM Capabilities represent the underlying factory configurations of the HSM. HSM Policies are the settings based on those configuration elements, and can be modified by the HSM Security Officer (SO). If a Capability is turned off (disabled), then it cannot be switched on with a Policy setting. Only re-manufacturing or the application of a Secure Capability Update can change a Capability from off to on (disabled to enabled). If a Capability is enabled, then the SO may be able to alter it with a Policy change, but only to make it more restrictive. The SO cannot make a Capability less restrictive.

In most cases, Configurations and Policies are either off or on (disabled or enabled, where 0 [zero] equals off/disabled and 1 [one] equals on/enabled), but some involve a range of values.

Example policy change procedure

In this example, we show the initial values of the HSM Capabilities and their corresponding Policies, then we change one Policy, and show the values again.The settings you would see for a Password-Authenticated HSM and a PED-Authenticated HSM might differ slightly, but the general principle and the operation of policy change are the same.

1. First, for this example, display the basic HSM information.

```
lunacm:> hsm showinfo

        HSM Label -> no label
        HSM Manufacturer -> Safenet, Inc.
        HSM Model -> K6 Base
        HSM Serial Number -> 456278
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
        Firmware Version -> 6.1.3
        Rollback Firmware Version -> 6.1.0
        Slot Id -> 1
        Tunnel Slot Id -> 2
        Session State -> CKS_RW_PUBLIC_SESSION

        SO Status->        Not Logged In
```



```
        SO information is not available (HSM has not been initialized)

        HSM Storage:
                Total Storage Space:  2097152
                Used Storage Space:   0
                Free Storage Space:   2097152
                Allowed Partitions:   20
                Number of Partitions: 0

        SO Storage:
                Total Storage Space:  262144
                Used Storage Space:   0
                Free Storage Space:   262144
                Object Count:         0

        *** The HSM is NOT in FIPS 140-2 approved operation mode. ***


        License Count -> 7
                1. 621000026-000 621-000026-000 K6 BASE CONFIGURATION FILE,HSM UNMASKING
                2. 620127-000 ECC
                3. 620114-001 Cloning
                4. 620127-000 Test K3 ECC Update - 620127
                5. 621010358-001 621-010358-001 External MTK - STM disabled
                6. 621010089-001 621-010089-001 Remote Ped
                7. 621000021-001 SCU K5/K6 Performance 15

Command Result : No Error
lunacm:>
```

Note the message near the end, stating that the HSM is not in FIPS 140-2 approved operation mode. This is a condition that we are about to change for the purpose of providing an example; you do not need to make this particular change unless your organization's security policy calls for it.

2. Now display the controlling policies as they currently exist on the HSM.

```
lunacm:> hsm showpolicies

        HSM Capabilities
                0: Enable PIN-based authentication : 0
                1: Enable PED-based authentication : 1
                2: Performance level : 5
                4: Enable domestic mechanisms & key sizes : 1
                6: Enable masking : 1
                7: Enable cloning : 1
                8: Enable special cloning certificate : 0
                9: Enable full (non-backup) functionality : 1
                11: Enable ECC mechanisms : 1
                12: Enable non-FIPS algorithms : 1
                15: Enable SO reset of partition PIN : 1
                16: Enable network replication : 1
                17: Enable Korean Algorithms : 0
                18: FIPS evaluated : 0
                19: Manufacturing Token : 0
                20: Enable Remote Authentication : 1
                21: Enable forcing user PIN change : 1
                22: Enable offboard storage : 1
                23: Enable partition groups : 0
```



```
        25: Enable remote PED usage : 1
        26: Enable External Storage of MTK Split : 1
        27: HSM non-volatile storage space : 2097152
        28: Enable HA mode CGX : 0
        29: Enable Acceleration : 1
        30: Enable unmasking : 1

HSM Policies
        0: PIN-based authentication : 0
        1: PED-based authentication : 1
        6: Allow masking : 1
        7: Allow cloning : 1
        12: Allow non-FIPS algorithms : 1
        15: SO can reset partition PIN : 1
        16: Allow network replication : 1
        20: Allow Remote Authentication : 1
        21: Force user PIN change after set/reset : 0
        22: Allow offboard storage : 1
        23: Allow partition groups : 0
        25: Allow remote PED usage : 1
        26: Store MTK Split Externally : 1
        29: Allow Acceleration : 1
        30: Allow unmasking : 1

SO Capabilities
        0: Enable private key cloning : 1
        1: Enable private key wrapping : 0
        2: Enable private key unwrapping : 1
        3: Enable private key masking : 0
        4: Enable secret key cloning : 1
        5: Enable secret key wrapping : 1
        6: Enable secret key unwrapping : 1
        7: Enable secret key masking : 0
        10: Enable multipurpose keys : 1
        11: Enable changing key attributes : 1
        14: Enable PED use without challenge : 1
        15: Allow failed challenge responses : 1
        16: Enable operation without RSA blinding : 1
        17: Enable signing with non-local keys : 1
        18: Enable raw RSA operations : 1
        20: Max failed user logins allowed : 3
        21: Enable high availability recovery : 1
        22: Enable activation : 0
        23: Enable auto-activation : 0
        25: Minimum pin length (inverted: 255 - min) : 248
        26: Maximum pin length : 255
        28: Enable Key Management Functions : 1
        29: Enable RSA signing without confirmation : 1
        30: Enable Remote Authentication : 1
        31: Enable private key unmasking : 1
        32: Enable secret key unmasking : 1

SO Policies
        0: Allow private key cloning : 1
        1: Allow private key wrapping : 0
        2: Allow private key unwrapping : 1
        3: Allow private key masking : 0
```



```
        4: Allow secret key cloning : 1
        5: Allow secret key wrapping : 1
        6: Allow secret key unwrapping : 1
        7: Allow secret key masking : 0
        10: Allow multipurpose keys : 1
        11: Allow changing key attributes : 1
        14: Challenge for authentication not needed : 1
        15: Ignore failed challenge responses : 1
        16: Operate without RSA blinding : 1
        17: Allow signing with non-local keys : 1
        18: Allow raw RSA operations : 1
        20: Max failed user logins allowed : 3
        21: Allow high availability recovery : 1
        22: Allow activation : 0
        23: Allow auto-activation : 0
        25: Minimum pin length (inverted: 255 - min) : 248
        26: Maximum pin length : 255
        28: Allow Key Management Functions : 1
        29: Perform RSA signing without confirmation : 1
        30: Allow Remote Authentication : 1
        31: Allow private key unmasking : 1
        32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
```

3. For this example, to change an HSM Policy setting, you must provide the number that identifies the Policy and then the value for the desired state. First login to the HSM using Luna PED (Luna PED must be connected and ready before you login). For a password-authenticated HSM the password is needed, and no PED is involved), then type the `hsm changeHSMPolicy` or the `hsm changeSOPolicy` command:

```
lunacm:> hsm login
Please attend to the PED
```

> **Note:** At this time, you must respond to the prompts on the Luna PED screen.

```
command Result : No error
lunacm:>
hsm changeHSMPolicy -policy 12 -value 0
command Result : No error

lunacm:>
lunacm:> hsm showpolicies

        HSM Capabilities
                0: Enable PIN-based authentication : 0
                1: Enable PED-based authentication : 1
                2: Performance level : 5
                4: Enable domestic mechanisms & key sizes : 1
                6: Enable masking : 1
                7: Enable cloning : 1
                8: Enable special cloning certificate : 0
                9: Enable full (non-backup) functionality : 1
                11: Enable ECC mechanisms : 1
                12: Enable non-FIPS algorithms : 1
```



```
        15: Enable SO reset of partition PIN : 1
        16: Enable network replication : 1
        17: Enable Korean Algorithms : 0
        18: FIPS evaluated : 0
        19: Manufacturing Token : 0
        20: Enable Remote Authentication : 1
        21: Enable forcing user PIN change : 1
        22: Enable offboard storage : 1
        23: Enable partition groups : 0
        25: Enable remote PED usage : 1
        26: Enable External Storage of MTK Split : 1
        27: HSM non-volatile storage space : 2097152
        28: Enable HA mode CGX : 0
        29: Enable Acceleration : 1
        30: Enable unmasking : 1

HSM Policies
        0: PIN-based authentication : 0
        1: PED-based authentication : 1
        6: Allow masking : 1
        7: Allow cloning : 1
        12: Allow non-FIPS algorithms : 0
        15: SO can reset partition PIN : 1
        16: Allow network replication : 1
        20: Allow Remote Authentication : 1
        21: Force user PIN change after set/reset : 0
        22: Allow offboard storage : 1
        23: Allow partition groups : 0
        25: Allow remote PED usage : 1
        26: Store MTK Split Externally : 1
        29: Allow Acceleration : 1
        30: Allow unmasking : 1

SO Capabilities
        0: Enable private key cloning : 1
        1: Enable private key wrapping : 0
        2: Enable private key unwrapping : 1
        3: Enable private key masking : 0
        4: Enable secret key cloning : 1
        5: Enable secret key wrapping : 1
        6: Enable secret key unwrapping : 1
        7: Enable secret key masking : 0
        10: Enable multipurpose keys : 1
        11: Enable changing key attributes : 1
        14: Enable PED use without challenge : 1
        15: Allow failed challenge responses : 1
        16: Enable operation without RSA blinding : 1
        17: Enable signing with non-local keys : 1
        18: Enable raw RSA operations : 1
        20: Max failed user logins allowed : 3
        21: Enable high availability recovery : 1
        22: Enable activation : 0
        23: Enable auto-activation : 0
        25: Minimum pin length (inverted: 255 - min) : 248
        26: Maximum pin length : 255
        28: Enable Key Management Functions : 1
        29: Enable RSA signing without confirmation : 1
```



```
                30: Enable Remote Authentication : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 1

        SO Policies
                0: Allow private key cloning : 1
                1: Allow private key wrapping : 0
                2: Allow private key unwrapping : 1
                3: Allow private key masking : 0
                4: Allow secret key cloning : 1
                5: Allow secret key wrapping : 1
                6: Allow secret key unwrapping : 1
                7: Allow secret key masking : 0
                10: Allow multipurpose keys : 1
                11: Allow changing key attributes : 1
                14: Challenge for authentication not needed : 1
                15: Ignore failed challenge responses : 1
                16: Operate without RSA blinding : 1
                17: Allow signing with non-local keys : 1
                18: Allow raw RSA operations : 1
                20: Max failed user logins allowed : 3
                21: Allow high availability recovery : 1
                22: Allow activation : 0
                23: Allow auto-activation : 0
                25: Minimum pin length (inverted: 255 - min) : 248
                26: Maximum pin length : 255
                28: Allow Key Management Functions : 1
                29: Perform RSA signing without confirmation : 1
                30: Allow Remote Authentication : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
lunacm:> hsm showinfo

        HSM Label -> no label
        HSM Manufacturer -> Safenet, Inc.
        HSM Model -> K6 Base
        HSM Serial Number -> 456278
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
        Firmware Version -> 6.1.3
        Rollback Firmware Version -> 6.1.0
        Slot Id -> 1
        Tunnel Slot Id -> 2
        Session State -> CKS_RW_PUBLIC_SESSION

        SO Status->        Not Logged In
        SO information is not available (HSM has not been initialized)

        HSM Storage:
                Total Storage Space:  2097152
```



```
                Used Storage Space:   0
                Free Storage Space:   2097152
                Allowed Partitions:   20
                Number of Partitions: 0

        SO Storage:
                Total Storage Space:  262144
                Used Storage Space:   0
                Free Storage Space:   262144
                Object Count:         0

        *** The HSM is in FIPS 140-2 approved operation mode. ***


        License Count -> 7
                1. 621000026-000 621-000026-000 K6 BASE CONFIGURATION FILE,HSM UNMASKING
                2. 620127-000 ECC
                3. 620114-001 Cloning
                4. 620127-000 Test K3 ECC Update - 620127
                5. 621010358-001 621-010358-001 External MTK - STM disabled
                6. 621010089-001 621-010089-001 Remote Ped
                7. 621000021-001 SCU K5/K6 Performance 15

Command Result : No Error
lunacm:>
```

Note in the above example that HSM Capability "12: Enable non-FIPS algorithms : 1" still has a value of 1 (meaning that it remains enabled), but the associated Policy "12: Allow non-FIPS algorithms : **0** " now has a value of 0 (meaning that it has been disallowed by the SO).

Note also that the message in the middle of the "show" information now says "*** The HSM is in FIPS 140-2 approved operation mode. *** " because the HSM is now restricted to using only FIPS-approved algorithms.

Second Example – Destructive Change of HSM Policy

```
lunacm:> hsm -changeHSMPolicy -policy 15 -value 0
```

That command assigns a value of zero (0) to the “Enable SO reset of partition PIN” policy, turning it off.

The above example is a change to a destructive policy, meaning that, if you apply this policy, the HSM is zeroized and all contents are lost. For this reason, you are prompted to confirm if that is what you really wish to do. You must now re-initialize the HSM.

While this is not an issue when you have just initialized an HSM, it may be a very important consideration if your Luna HSM has been in a “live” or “production” environment and contains useful or important data, keys, certificates.

The work-around is to backup any important HSM or partition contents before making any destructive policy change, and then restore from backup after the HSM is re-initialized and the partition re-created.

Creating a Partition on Luna PCI-E HSM

This section is HSM Partition setup for Luna PCI-E with Password Authentication. The activities in this section are required in two circumstances.

- if you just prepared an HSM on the Luna PCI-E for the first time and must now create your first HSM Partition, or

- if you have deleted or zeroized an HSM Partition and wish to create a new one to replace it.

About HSM Partitions on the Initialized HSM

At this point, Luna PCI-E should already have its Security Officer assigned by Initializing an HSM.

Within the HSM, a separate cryptographic workspaces must be created. A workspace, or Partition, and all its contents are protected by encryption derived (in part) from its authentication. Only a User who presents the proper authentication is allowed to see the Partition and to work with its contents. That User and authentication can be separate from the Security Officer identity.

In this section, you will:

- Create an HSM Partition
- Set HSM Partition Policies (Optional)

First, Login as Security Officer

To create HSM Partitions, you must login to Luna PCI-E as Security Officer. At the lunacm:> prompt, type:

```
lunacm:> hsm login -password <your_password>
```

Authenticate as Security Officer by supplying the appropriate SO password. The password must be exactly as the HSM expects it, including proper use of uppercase/lowercase.

If you fail three consecutive login attempts as Security Officer, the HSM is zeroized and cannot be used — it must be re-initialized. Zeroizing renders all key material unrecoverable. Please note that the Luna HSM must actually receive some information before it logs a failed attempt, so if you just press [Enter] without typing a password, that is not logged as a failed attempt. Also, when you successfully log in, the counter is reset to zero.

If you are not sure that you are currently logged in as Security Officer, perform an '`hsm logout`'.

Second, Create the Partition

At the lunacm:> prompt, type:

```
lunacm:> partition create -domain $ecureDomain$tring

Option -password was not supplied. It is required.

Enter the password: *********
Re-enter the password: *********

Command Result : No Error

lunacm:>
```

If an error occurs, perhaps you have requested a too-short password. The password must be at least eight characters in length unless the SO sets a different minimum.

About the Domain

Always specify a cloning domain when you create a partition on a Password Authenticated Luna PCI-E HSM in a production environment. The HSM allows you to omit a specific domain at partition creation, and instead uses the 'factory-default' domain.
This is insecure.
Anyone could clone objects to or from such an HSM partition. The default domain is useful in a lab or integration/development setting. However, when you prepare a Luna HSM to go into service in a real "production" environment, always specify a proper, secure domain string when you create your partition.

```
lunacm:> partition create

Option -password was not supplied. It is required.
Enter the password: *********
Re-enter the password: *********

Option -domain not specified.
If you proceed, the default domain will be used.
You will not be creating a new domain.

Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now -> proceed

Command Result : No Error

lunacm:>
```

Alternate partition dialog

When you first create a partition on a newly initialized HSM, the HSM goes immediately to the partition setup, as requested.

However, if you have previously created a partition on this HSM - and not initialized since then - the HSM detects that a valid partition is present and warns you that 'partition create' operation is about to destroy/overwrite that existing partition. It gives you the opportunity to back out of the operation and investigate, in case you are unsure of the status.

```
lunacm:> partition create -domain $ecureDomain$tring

The existing partition will be destroyed.

Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now -> proceed

Option -password was not supplied. It is required.
Enter the password: *********
Re-enter the password: *********

Command Result : No Error

lunacm:>
```

Third, Set/Change Partition Policies [Optional]

View the partition information, including Capabilities and Policies, to see if you need to change anything. Type:

```
lunacm:> partition showpolicies
        Partition Capabilities
0: Enable private key cloning : 0
1: Enable private key wrapping : 0
2: Enable private key unwrapping : 1
3: Enable private key masking : 0
4: Enable secret key cloning : 0
5: Enable secret key wrapping : 1
6: Enable secret key unwrapping : 1
7: Enable secret key masking : 0
10: Enable multipurpose keys : 1
11: Enable changing key attributes : 1
14: Enable PED use without challenge : 1
15: Allow failed challenge responses : 1
16: Enable operation without RSA blinding : 1
17: Enable signing with non-local keys : 1
18: Enable raw RSA operations : 1
```



```
19: Max non-volatile storage space : 3
20: Max failed user logins allowed : 10
21: Enable high availability recovery : 1
22: Enable activation : 0
23: Enable auto-activation : 0
25: Minimum pin length (inverted: 255 - min) : 248
26: Maximum pin length : 255
28: Enable Key Management Functions : 1
29: Enable RSA signing without confirmation : 1
30: Enable Remote Authentication : 1
        Partition Policies
0: Allow private key cloning : 0
1: Allow private key wrapping : 0
2: Allow private key unwrapping : 1
3: Allow private key masking : 0
4: Allow secret key cloning : 0
5: Allow secret key wrapping : 1
6: Allow secret key unwrapping : 1
7: Allow secret key masking : 0
10: Allow multipurpose keys : 1
11: Allow changing key attributes : 1
14: Challenge for authentication not needed : 1
15: Ignore failed challenge responses : 1
16: Operate without RSA blinding : 1
17: Allow signing with non-local keys : 1
18: Allow raw RSA operations : 1
19: Max non-volatile storage space : 3
20: Max failed user logins allowed : 10
21: Allow high availability recovery : 1
22: Allow activation : 0
23: Allow auto-activation : 0
25: Minimum pin length (inverted: 255 - min) : 248
26: Maximum pin length : 255
28: Allow Key Management Functions : 1
29: Perform RSA signing without confirmation : 1
30: Allow Remote Authentication : 0
Command Result : No Error
lunacm:>
```

As an example of a change, you could type:

```
lunacm:> partition changePolicy -policy 16 -value 0
```

This would have the effect of switching off RSA blinding.

Where to go next?

Having set up your Luna PCI-E, you want to use it.

Either you have created an application of your own that can make use of an HSM, or you are using an existing third-party software. Examples might be Microsoft server applications like Certificate Services, IIS, ISA, RMS or others, which can perform their cryptographic functions in software, using local computer resources (CPU, memory, and hard disk) with their inherent security issues, or which can be configured to make use of an HSM like the Luna PCI.

If you are using one of the indicated Microsoft products, you will need to install the Luna CSP software and then install the server application, or else re-configure an existing installation to make use of Luna CSP (which provides the bridge between the application and the Luna HSM).

On 64-bit Windows systems, you have the option to use Microsoft's CNG (replaces CAPI), and to use our KSP provider instead of CSP.

Another option is a Java-based application, in which case you should install the Luna JSP, which comes with Javadocs and sample code.

Setting Luna PCI-E Partition Policies [Optional]

Partition Capabilities represent the underlying factory configurations that are in force when a Partition is created. Partition Policies are the settings based on those configuration elements, and can be modified by the HSM Security Officer (SO). If a Capability is turned off (disabled), then it cannot be switched on with a Policy setting. Only re-manufacturing or the application of a Secure Capability Update can change a Capability from off to on (disabled to enabled). If a Capability is enabled, then the SO may be able to alter it with a Policy change, but only to make it more restrictive. The SO cannot make a Capability less restrictive.

For example, if a Capability setting requires that the minimum length of a Partition Password must be (say) seven characters, then the SO can use a Policy change to require a minimum password length of eight, nine, ten, or more characters (up to 255). A requirement for a longer password is considered to be a more restrictive security setting. The SO cannot use a Policy change to set the minimum password length to six or fewer characters, because that would be less restrictive than the original Capability which demands at least seven characters.

In most cases, Configurations and Policies are either off or on (disabled or enabled, where 0 [zero] equals off/disabled and 1 [one] equals on/enabled), but some involve a range of values, as in the example below.

Example policy change procedure

In this example, we show the initial values of the Partition Capabilities and their corresponding Policies, then we change one Policy, and show the values again.

```
lunacm:> partition showinfo

        HSM Serial Number -> 456278
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
                CKF_USER_PIN_INITIALIZED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
                CKF_TOKEN_INITIALIZED
        Slot Id -> 1
        Tunnel Slot Id -> 2
        Session State -> CKS_RW_PUBLIC_SESSION

        User Status->                   Not Logged In
        Crypto Officer Failed Logins-> 0
        Crypto User Failed Logins->    0
        User Flags ->
                CONTAINER_KCV_CREATED
        User OUID: 6e000000e400000056f60600

        User Storage:
                Total Storage Space:  2094996
                Used Storage Space:   0
                Free Storage Space:   2094996
                Object Count:         0
```



```
        *** The HSM is NOT in FIPS 140-2 approved operation mode. ***


        License Count -> 9
                1. 0009-020 Test K6 Base Config - 9-20
                2. 620109-000 Test K3 FIPS3 Update - 620109
                3. 0009-030 Test K3 HSM Cloning Update - 000009-030
                4. 620127-000 Test K3 ECC Update - 620127
                5. 0009-025 Test K3 External MTK Update 2 - 000009-025
                6. 620111-000 Test K3 Performance 600 Update - 620111
                7. 0009-015 Test K3 Remote Ped Update - 000009-015
                8. 620124-000 Test K3 Partitions 20 Update - 620124
                9. 620114-000 Test K3 Cloning Update - 620114

Command Result : No Error
lunacm:>


lunacm:> partition showpolicies

        Partition Capabilities
                0: Enable private key cloning : 1
                1: Enable private key wrapping : 0
                2: Enable private key unwrapping : 1
                3: Enable private key masking : 0
                4: Enable secret key cloning : 1
                5: Enable secret key wrapping : 1
                6: Enable secret key unwrapping : 1
                7: Enable secret key masking : 0
                10: Enable multipurpose keys : 1
                11: Enable changing key attributes : 1
                14: Enable PED use without challenge : 1
                15: Allow failed challenge responses : 1
                16: Enable operation without RSA blinding : 1
                17: Enable signing with non-local keys : 1
                18: Enable raw RSA operations : 1
                20: Max failed user logins allowed : 10
                21: Enable high availability recovery : 1
                22: Enable activation : 1
                23: Enable auto-activation : 1
                25: Minimum pin length (inverted: 255 - min) : 248
                26: Maximum pin length : 255
                28: Enable Key Management Functions : 1
                29: Enable RSA signing without confirmation : 1
                30: Enable Remote Authentication : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 1

        Partition Policies
                0: Allow private key cloning : 1
                1: Allow private key wrapping : 0
                2: Allow private key unwrapping : 1
                3: Allow private key masking : 0
                4: Allow secret key cloning : 1
                5: Allow secret key wrapping : 1
                6: Allow secret key unwrapping : 1
                7: Allow secret key masking : 0
                10: Allow multipurpose keys : 1
```



```
                11: Allow changing key attributes : 1
                14: Challenge for authentication not needed : 1
                15: Ignore failed challenge responses : 1
                16: Operate without RSA blinding : 1
                17: Allow signing with non-local keys : 1
                18: Allow raw RSA operations : 1
                20: Max failed user logins allowed :10   <--
                21: Allow high availability recovery : 1
                22: Allow activation : 0
                23: Allow auto-activation : 0
                25: Minimum pin length (inverted: 255 - min) : 248
                26: Maximum pin length : 255
                28: Allow Key Management Functions : 1
                29: Perform RSA signing without confirmation : 1
                30: Allow Remote Authentication : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
```

In the example above, we change the maximum number of consecutive failed login attempts that is permitted on the Partition.
The default maximum is 10. You can change the maximum to less than 10, but not more than 10.
Setting to less than ten would make the partition more secure than the default, and is allowed.
Setting to more than ten would make the partition less secure than the default, and is not allowed.

```
lunacm:> partition showpolicies

        Partition Capabilities
                0: Enable private key cloning : 1
                1: Enable private key wrapping : 0
                2: Enable private key unwrapping : 1
                3: Enable private key masking : 0
                4: Enable secret key cloning : 1
                5: Enable secret key wrapping : 1
                6: Enable secret key unwrapping : 1
                7: Enable secret key masking : 0
                10: Enable multipurpose keys : 1
                11: Enable changing key attributes : 1
                14: Enable PED use without challenge : 1
                15: Allow failed challenge responses : 1
                16: Enable operation without RSA blinding : 1
                17: Enable signing with non-local keys : 1
                18: Enable raw RSA operations : 1
                20: Max failed user logins allowed : 10
                21: Enable high availability recovery : 1
                22: Enable activation : 1
                23: Enable auto-activation : 1
                25: Minimum pin length (inverted: 255 - min) : 248
                26: Maximum pin length : 255
                28: Enable Key Management Functions : 1
                29: Enable RSA signing without confirmation : 1
                30: Enable Remote Authentication : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 1
```

```
        Partition Policies
                0: Allow private key cloning : 1
                1: Allow private key wrapping : 0
                2: Allow private key unwrapping : 1
                3: Allow private key masking : 0
                4: Allow secret key cloning : 1
                5: Allow secret key wrapping : 1
                6: Allow secret key unwrapping : 1
                7: Allow secret key masking : 0
                10: Allow multipurpose keys : 1
                11: Allow changing key attributes : 1
                14: Challenge for authentication not needed : 1
                15: Ignore failed challenge responses : 1
                16: Operate without RSA blinding : 1
                17: Allow signing with non-local keys : 1
                18: Allow raw RSA operations : 1
                20: Max failed user logins allowed :9    <--
                21: Allow high availability recovery : 1
                22: Allow activation : 0
                23: Allow auto-activation : 0
                25: Minimum pin length (inverted: 255 - min) : 248
                26: Maximum pin length : 255
                28: Allow Key Management Functions : 1
                29: Perform RSA signing without confirmation : 1
                30: Allow Remote Authentication : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
```

Note in the above example that HSM Capability "20: Max failed user logins allowed : 10" still has a value of 10 (meaning that 10 is as many failed Partition login attempts as can be permitted), but the associated Policy "20: Max failed user logins allowed : **9**" now has a value of 9 - meaning that the SO has decided that 10 bad login attempts on the Partition was too many. The SO has used the Policy to impose greater restriction than the Capability required; that is, the SO has increased the security on the partition.

CHAPTER 2

Configuring a PED-Authenticated HSM

This chapter describes how to configure a PED-authenticated HSM to get it ready to operate in your environment. It contains the following sections:

Overview

The HSM is available in PED-authenticated or password-authenticated versions. Use the configuration steps in this chapter to configure a PED-authenticated HSM.

There is no externally visible difference between a password-authenticated or PED-authenticated HSM. For an installed HSM, you can determine its mode of authentication by attempting to log in. A Trusted Path version will direct you to the Luna PED. A Password Authenticated version will prompt you for the password. You cannot change the authentication type of a Luna HSM. It is a manufacturing configuration, set at the factory. If you have a PED-authenticated (Trusted Path) version, you cannot access the HSM and partitions by means of passwords.

For PED-authenticated HSMs, you authenticate to the HSM as Security Officer, or User, etc., by presenting an iKey PED Key device that contains the authentication. This method has the advantage that you don't need to remember (or write down) passwords, and when the PED Key is presented, the authentication is never exposed on a computer screen, never typed on a keyboard, and never exists on the computer bus or memory - thus the authentication data is never vulnerable to eavesdropping or software attacks. On the other hand, you need additional hardware (the Luna PED and cable, and the PED Keys), and you must enact procedures to track and keep secure those physical PED Keys.

High-Level Configuration Steps

1. Initialize the HSM, as described in "Initializing a Luna PED-Authenticated PCI-E HSM" on page 24.
2. Change the HSM policies, if desired, as described in "Setting Luna PCI-E HSM Policies [Optional]" on page 30. If any of the policies you set are destructive, you must re-initialize the HSM after setting the polices.
3. Create a partition on the HSM, as described in "Creating a Partition on a Luna PCI-E HSM" on page 36.
4. Change the partition policies, if desired, as described in "Setting Luna PCI-E Partition Policies [Optional]" on page 44

Initializing a Luna PED-Authenticated PCI-E HSM

Your Luna PCI-E 5 HSM arrives in "Zeroized" state, and in a default, pre-initialized condition (see below). It might also be in Secure Transport Mode, if you selected that option at purchase time.

To determine the state of the HSM

The LunaCM utility presents status information for connected HSMs when lunacm is launched.

```
bash-3.00# ./lunacm
LunaCM V2.3.3 - Copyright (c) 2006-2010 SafeNet, Inc.
Available HSMs:
Slot Id ->              1
Tunnel Slot Id ->       3
HSM Label ->            no label
HSM Serial Number ->    151433
HSM Model ->            K6 Base
HSM Firmware Version -> 6.2.1
HSM Configuration ->    Luna PCI (PED) Undefined Mode / Uninitialized
HSM Status ->           Transport Mode, Zeroized
Slot Id ->              2
Tunnel Slot Id ->       4
HSM Label ->            no label
HSM Serial Number ->    151446
HSM Model ->            K6 Base
HSM Firmware Version -> 6.2.1
HSM Configuration ->    Luna PCI (PED) Undefined Mode / Uninitialized
HSM Status ->           Transport Mode, Zeroized
Current Slot Id: 1
lunacm:>
```

“Transport Mode” refers to a user-invoked tamper event.

“Zeroized” state results from the battery being disengaged and the Real Time Clock and the battery-backed memory left un-powered. This renders any HSM contents unrecoverable (at the factory, we would have created only unimportant test objects on the HSM - if you have previously had the HSM in service, and then either "decommissioned" it or performed `hsm factoryreset` your valid objects and keys are similarly rendered permanently unrecoverable and the HSM is completely safe to store or ship).

The HSM card had to be removed from our manufacturing test computer in order to ship it to you. Removal of the HSM card from a computer slot is detected as a tamper event. This is a security feature.

Upon removing the HSM card from a computer we slide the battery switch to the “storage/travel” position. This removes battery power from the Real-time Clock and battery-backed memory which effectively places the HSM card in “Decommissioned” state. This is a security feature, and preserves the life of the battery.

The above two states are addressed by configuring and initializing your Luna PCI-E 5 HSM. Instructions start on this page.

If you requested Secure Transport Mode shipment from SafeNet, then a couple of additional steps are required (also included in these instructions).

Why Initialize?

Before you can make use of it, the HSM must be initialized. This establishes your ownership for current and future HSM administration. Initialization assigns a meaningful label, as well as Security Officer authentication (PED Key) and Domain (another PED Key), and places the HSM in a state ready to use.

Use the instructions on this page if you have Luna PCI-E with PED (Trusted Path) authentication.

Some HSM Policy changes are destructive. A destructive policy change is one that requires the HSM to be initialized again, before it can be used. Thus if you intend to perform a destructive HSM Policy change, you might need to perform this initialization step again, after the Policy change.

Start the lunacm Utility

```
C:\Program Files\LunaPCI>lunacm
LunaCM V2.3 - Copyright (c) 2006-2010 SafeNet, Inc.
Available HSMs:
Slot Id ->              1
Tunnel Slot Id ->       2
HSM Label ->            no label
HSM Serial Number ->    8000001
HSM Model ->            K6Base
HSM Firmware Version -> 6.1.3
HSM Configuration ->    Luna PCI (PED) Signing with Cloning Mode
Current Slot Id: 1
lunacm:>
```

Notice that the HSM does not yet have a label, indicating that it has not been initialized since manufacture.

Initialize the HSM

1. Have the Luna PED connected and ready (in local mode and "Awaiting command...").
2. Insert a blank PED Key into the USB connector at the top of the PED.
3. In a terminal window (DOS command-line window in Windows), go to the LunaPCI directory and start the lunacm utility:
   lunacm:>
4. Run the "hsm init" command, giving a label for your Luna PCI-E HSM. If Secure Transport Mode was set, you must unlock the HSM with the purple PED Key before you can proceed.

   The following is an example of initialization dialog, with PED interactions inserted to show the sequence of events.

   ```
   lunacm:> hsm init -label myPCI
   You are about to initialize the HSM.
   All contents of the HSM will be destroyed.
   Are you sure you wish to continue?
   Type 'proceed' to continue, or 'quit' to quit now -> proceed
   Please attend to the PED.
   ```

5. Luna PED asks preliminary setup questions [The simplest scenario is your first-ever HSM and new PED Keys. However, you might have previously initialized this HSM and be starting over. Or you might have other HSMs already initialized and need to share the authentication or the domain with your new HSM.] the HSM and PED need to know, prior to imprinting the first SO PED Key.

   ```
   Slot 01
   SETTING SO PIN...
   Would you like to
   reuse an existing
   keyset? (Y/N)
   ```

6. If you say [NO] (on the PED keypad), then you are indicating there is nothing of value on your PED Keys to preserve. On the assumption that you will now be writing onto a new blank PED Key, or onto one that contains old

unwanted authentication, Luna PED asks you to set M of N values.

```
Slot 01
SETTING SO PIN...
M value? (1-16)
>01
```

and

```
Slot 01
SETTING SO PIN...
N value? (M-16)
>01
```

Setting M and N equal to "1" means that the authentication is not to be split, and only a single PED Key will be necessary when the authentication is called for in future.

Setting M and N larger than "1" means that the authentication is split into N different "splits", of which quantity M of them must be presented each time you are required to authenticate. M of N allows you to enforce multi-person access control - no single person can access the HSM without cooperation of other holders.

7. If you say [YES], you indicate that you have a PED Key (or set of PED Keys) from another HSM and you wish your current/new HSM to share the authentication with that other HSM. Authentication will be read from the PED Key that you present and imprinted onto the current HSM.

   Luna PED now asks you to provide the appropriate PED Key - a fresh blank key, or a previously used key that you intend to overwrite, or a previously used key that you intend to preserve and share with this HSM.

   ```
   SLOT 01
   SETTING SO PIN...
   Insert a SO /
   HSM Admin
   PED Key.
   Press ENTER.

   Slot 01
   SETTING SO PIN...
   **WARNING**
   This PED Key is
   blank.
   Overwrite?   YES/NO
   ```

   OR

   ```
   Slot 01
   Initialize HSM
   **WARNING**
   This PED Key is for
   SO / HSM Admin.
   Overwrite?   YES/NO
   ```

8. Answer (press the appropriate button on the PED keypad)
   - "**NO**" if the PED key that you provided carries SO authentication data that must be preserved. In that case, you must have made a mistake so the PED goes back to asking you to insert a suitable key.
   - "**YES**" if the PED should overwrite (if you overwrite a never-used PED Key, nothing is lost; if you overwrite a PED Key that contains authentication secret for another HSM, then this PED Key will no longer be able to access the other HSM, only the new HSM that you are currently initializing with a new, unique authentication

secret - therefore "YES" means 'yes, destroy the contents on the key and create new authentication information in its place' - be sure that this is what you wish to do) the PED Key with a new SO authentication. (This will be matched on the Luna PCI-E HSM during this initialization).

9. Luna PED makes very sure that you wish to overwrite, by asking again.

```
SLOT 01
SETTING SO PIN...
***WARNING **
Are you sure you
want to overwrite
this PED Key? YES/NO
```

10. For any situation other than reusing a keyset, Luna PED now prompts for you to set a PED PIN. For multi-factor authentication security, the PED Key is "something you have". You can choose to associate that with "something you know", in the form of a multi-digit PIN code that must always be supplied along with the PED Key for all future HSM access attempts.

```
SLOT 01
SETTING SO PIN...
Enter new PED PIN:

Confirm new PED PIN:
```

11. Type a numeric password on the PED keypad, if you wish. Otherwise, just press [Enter] twice to indicate that no PED PIN is desired.

    Luna PED imprints the PED Key, or the HSM, or both, as appropriate, and then prompts the final question for this key:

```
SLOT 01
SETTING SO PIN...
Are you duplicating
this keyset? (Y/N)
```

12. You can respond [YES] and present one or more blank keys, all of which will be imprinted with exact copies of the current PED Key's authentication, or you can say [NO], telling the PED to move on to the next part of the initialization sequence. (You should always have backups of your imprinted PED Keys, to guard against loss or damage.)
13. To begin imprinting a Cloning Domain (red PED Key), you must first log into the HSM, so you can simply leave the blue PED Key in place.

```
SLOT 01
SO LOGIN...
Insert a SO /
HSM Admin
PED Key.
Press ENTER.
```

14. Luna PED passes the authentication along to the HSM and then asks the first question toward imprinting a cloning domain:

```
SLOT 01
SO SETTING DOMAIN...
Would you like to
reuse an existing
keyset? (Y/N)
```

If this is your first Luna HSM, or if this HSM will not be cloning objects with other HSMs that are already initialized, then answer [NO]. Luna PED prompts for values of M and N.

If you have another HSM and wish that HSM and the current HSM to share their cloning Domain, then you must answer [YES]. In that case, Luna PED does not prompt for M and N.

```
SLOT 01
SO SETTING DOMAIN...
M value? (1-16)

>01
SLOT 01
SO SETTING DOMAIN...
M value? (1-16)

>01
```

Luna PED goes through the same sequence that occurred for the blue SO PED Key, except it is now dealing with a red Domain PED Key.

```
SLOT 01
SO SETTING DOMAIN...
Insert a
Domain
PED Key
Press ENTER.

Slot 01
SO SETTING DOMAIN...
**WARNING**
This PED Key is
blank.
Overwrite?   YES/NO
```

OR

```
Slot 01
SO SETTING DOMAIN...
**WARNING**
This PED Key is for
Domain.
Overwrite?   YES/NO
```

Just as with the blue SO PED Key, the next message is:

```
Slot 01
SO SETTING DOMAIN...
**WARNING**
Are you sure you
want to overwrite
this PED Key?   YES/NO
```

15. When you confirm that you do wish to overwrite whatever is (or is not) on the currently inserted key, with a Cloning Domain generated by the PED, the PED asks:

```
Slot 01
SO SETTING DOMAIN...
Enter new PED PIN:

Confirm new PED PIN:
```


And finally:

```
SLOT 01
SO SETTING DOMAIN...
Are you duplicating
this keyset? (Y/N)
```

16. Once you stop duplicating the Domain key, or you indicate that you do not wish to make any duplicates (you should have backups of all your imprinted PED Keys...), Luna PED goes back to "Awaiting command...".

    Lunacm says:

```
Command Result : No Error
lunacm:>
lunacm:> hsm showinfo
       HSM
 Label -> myLuna
       HSM Manufacturer -> Safenet, Inc.
       HSM Model -> K6 Base
       HSM Serial Number -> 150022
       HSM Status -> OK
       Token Flags ->
            CKF_RNG
            CKF_LOGIN_REQUIRED
            CKF_USER_PIN_INITIALIZED
            CKF_RESTORE_KEY_NOT_NEEDED
            CKF_TOKEN_INITIALIZED
       Firmware Version -> 6.2.1
       Rollback Firmware Version -> Not Available
       Slot Id -> 1
       Tunnel Slot Id -> 2
       Session State -> CKS_RW_PUBLIC_SESSION
       SO Status->        Not Logged In
       SO Failed Logins-> 0
       SO Flags ->
            CONTAINER_KCV_CREATED
       HSM Storage:
            Total Storage Space:  2097152
            Used Storage Space:   2097152
            Free Storage Space:   0
            Allowed Partitions:   1
            Number of Partitions: 1
       SO Storage:
            Total Storage Space:  262144
            Used Storage Space:   0
            Free Storage Space:   262144
            Object Count:         0
*** The HSM is NOT in FIPS 140-2 approved operation mode. ***
License Count -> 7
            1. 621000026-000 621-000026-000 K6 BASE CONFIGURATION FILE,HSM UNMASKING
            2. 620127-000 ECC
            3. 620114-001 Cloning
            4. 620109-000 FIPS3
            5. 621010358-001 621-010358-001 External MTK - STM disabled
            6. 621010089-001 621-010089-001 Remote Ped
            7. 621000021-001 SCU K5/K6 Performance 15
Command Result : No Error
lunacm:>
```


Notice that the HSM now has a label. If you were to exit and restart the lunacm utility, you would see the new label that you have just applied to the HSM.

17. The next step is to create a partition on the HSM. See "Creating a Partition on a Luna PCI-E HSM" on page 36.

Setting Luna PCI-E HSM Policies [Optional]

HSM Capabilities represent the underlying factory configurations of the HSM. HSM Policies are the settings based on those configuration elements, and can be modified by the HSM Security Officer (SO). If a Capability is turned off (disabled), then it cannot be switched on with a Policy setting. Only re-manufacturing or the application of a Secure Capability Update can change a Capability from off to on (disabled to enabled). If a Capability is enabled, then the SO may be able to alter it with a Policy change, but only to make it more restrictive. The SO cannot make a Capability less restrictive.

In most cases, Configurations and Policies are either off or on (disabled or enabled, where 0 [zero] equals off/disabled and 1 [one] equals on/enabled), but some involve a range of values.

Example policy change procedure

In this example, we show the initial values of the HSM Capabilities and their corresponding Policies, then we change one Policy, and show the values again.The settings you would see for a Password-Authenticated HSM and a PED-Authenticated HSM might differ slightly, but the general principle and the operation of policy change are the same.

1. First, for this example, display the basic HSM information.

```
lunacm:> hsm showinfo

        HSM Label -> no label
        HSM Manufacturer -> Safenet, Inc.
        HSM Model -> K6 Base
        HSM Serial Number -> 456278
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
        Firmware Version -> 6.1.3
        Rollback Firmware Version -> 6.1.0
        Slot Id -> 1
        Tunnel Slot Id -> 2
        Session State -> CKS_RW_PUBLIC_SESSION

        SO Status->        Not Logged In
        SO information is not available (HSM has not been initialized)

        HSM Storage:
                Total Storage Space:  2097152
                Used Storage Space:   0
                Free Storage Space:   2097152
                Allowed Partitions:   20
                Number of Partitions: 0

        SO Storage:
                Total Storage Space:  262144
                Used Storage Space:   0
                Free Storage Space:   262144
```



```
        Object Count:         0

    *** The HSM is NOT in FIPS 140-2 approved operation mode. ***


    License Count -> 7
        1. 621000026-000 621-000026-000 K6 BASE CONFIGURATION FILE,HSM UNMASKING
        2. 620127-000 ECC
        3. 620114-001 Cloning
        4. 620127-000 Test K3 ECC Update - 620127
        5. 621010358-001 621-010358-001 External MTK - STM disabled
        6. 621010089-001 621-010089-001 Remote Ped
        7. 621000021-001 SCU K5/K6 Performance 15

Command Result : No Error
lunacm:>
```

Note the message near the end, stating that the HSM is not in FIPS 140-2 approved operation mode. This is a condition that we are about to change for the purpose of providing an example; you do not need to make this particular change unless your organization's security policy calls for it.

2. Now display the controlling policies as they currently exist on the HSM.

```
lunacm:> hsm showpolicies

    HSM Capabilities
        0: Enable PIN-based authentication : 0
        1: Enable PED-based authentication : 1
        2: Performance level : 5
        4: Enable domestic mechanisms & key sizes : 1
        6: Enable masking : 1
        7: Enable cloning : 1
        8: Enable special cloning certificate : 0
        9: Enable full (non-backup) functionality : 1
        11: Enable ECC mechanisms : 1
        12: Enable non-FIPS algorithms : 1
        15: Enable SO reset of partition PIN : 1
        16: Enable network replication : 1
        17: Enable Korean Algorithms : 0
        18: FIPS evaluated : 0
        19: Manufacturing Token : 0
        20: Enable Remote Authentication : 1
        21: Enable forcing user PIN change : 1
        22: Enable offboard storage : 1
        23: Enable partition groups : 0
        25: Enable remote PED usage : 1
        26: Enable External Storage of MTK Split : 1
        27: HSM non-volatile storage space : 2097152
        28: Enable HA mode CGX : 0
        29: Enable Acceleration : 1
        30: Enable unmasking : 1

    HSM Policies
        0: PIN-based authentication : 0
        1: PED-based authentication : 1
        6: Allow masking : 1
        7: Allow cloning : 1
        12: Allow non-FIPS algorithms : 1
```



```
        15: SO can reset partition PIN : 1
        16: Allow network replication : 1
        20: Allow Remote Authentication : 1
        21: Force user PIN change after set/reset : 0
        22: Allow offboard storage : 1
        23: Allow partition groups : 0
        25: Allow remote PED usage : 1
        26: Store MTK Split Externally : 1
        29: Allow Acceleration : 1
        30: Allow unmasking : 1

SO Capabilities
        0: Enable private key cloning : 1
        1: Enable private key wrapping : 0
        2: Enable private key unwrapping : 1
        3: Enable private key masking : 0
        4: Enable secret key cloning : 1
        5: Enable secret key wrapping : 1
        6: Enable secret key unwrapping : 1
        7: Enable secret key masking : 0
        10: Enable multipurpose keys : 1
        11: Enable changing key attributes : 1
        14: Enable PED use without challenge : 1
        15: Allow failed challenge responses : 1
        16: Enable operation without RSA blinding : 1
        17: Enable signing with non-local keys : 1
        18: Enable raw RSA operations : 1
        20: Max failed user logins allowed : 3
        21: Enable high availability recovery : 1
        22: Enable activation : 0
        23: Enable auto-activation : 0
        25: Minimum pin length (inverted: 255 - min) : 248
        26: Maximum pin length : 255
        28: Enable Key Management Functions : 1
        29: Enable RSA signing without confirmation : 1
        30: Enable Remote Authentication : 1
        31: Enable private key unmasking : 1
        32: Enable secret key unmasking : 1

SO Policies
        0: Allow private key cloning : 1
        1: Allow private key wrapping : 0
        2: Allow private key unwrapping : 1
        3: Allow private key masking : 0
        4: Allow secret key cloning : 1
        5: Allow secret key wrapping : 1
        6: Allow secret key unwrapping : 1
        7: Allow secret key masking : 0
        10: Allow multipurpose keys : 1
        11: Allow changing key attributes : 1
        14: Challenge for authentication not needed : 1
        15: Ignore failed challenge responses : 1
        16: Operate without RSA blinding : 1
        17: Allow signing with non-local keys : 1
        18: Allow raw RSA operations : 1
        20: Max failed user logins allowed : 3
        21: Allow high availability recovery : 1
```

```
                22: Allow activation : 0
                23: Allow auto-activation : 0
                25: Minimum pin length (inverted: 255 - min) : 248
                26: Maximum pin length : 255
                28: Allow Key Management Functions : 1
                29: Perform RSA signing without confirmation : 1
                30: Allow Remote Authentication : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
```

3. For this example, to change an HSM Policy setting, you must provide the number that identifies the Policy and then the value for the desired state. First login to the HSM using Luna PED (Luna PED must be connected and ready before you login). For a password-authenticated HSM the password is needed, and no PED is involved), then type the `hsm changeHSMPolicy` or the `hsm changeSOPolicy` command:

```
lunacm:> hsm login
Please attend to the PED
```

Note: At this time, you must respond to the prompts on the Luna PED screen.

```
command Result : No error
lunacm:>
hsm changeHSMPolicy -policy 12 -value 0
command Result : No error

lunacm:>
lunacm:> hsm showpolicies

        HSM Capabilities
                0: Enable PIN-based authentication : 0
                1: Enable PED-based authentication : 1
                2: Performance level : 5
                4: Enable domestic mechanisms & key sizes : 1
                6: Enable masking : 1
                7: Enable cloning : 1
                8: Enable special cloning certificate : 0
                9: Enable full (non-backup) functionality : 1
                11: Enable ECC mechanisms : 1
                12: Enable non-FIPS algorithms : 1
                15: Enable SO reset of partition PIN : 1
                16: Enable network replication : 1
                17: Enable Korean Algorithms : 0
                18: FIPS evaluated : 0
                19: Manufacturing Token : 0
                20: Enable Remote Authentication : 1
                21: Enable forcing user PIN change : 1
                22: Enable offboard storage : 1
                23: Enable partition groups : 0
                25: Enable remote PED usage : 1
                26: Enable External Storage of MTK Split : 1
                27: HSM non-volatile storage space : 2097152
                28: Enable HA mode CGX : 0
```



```
        29: Enable Acceleration : 1
        30: Enable unmasking : 1

HSM Policies
        0: PIN-based authentication : 0
        1: PED-based authentication : 1
        6: Allow masking : 1
        7: Allow cloning : 1
        12: Allow non-FIPS algorithms : 0
        15: SO can reset partition PIN : 1
        16: Allow network replication : 1
        20: Allow Remote Authentication : 1
        21: Force user PIN change after set/reset : 0
        22: Allow offboard storage : 1
        23: Allow partition groups : 0
        25: Allow remote PED usage : 1
        26: Store MTK Split Externally : 1
        29: Allow Acceleration : 1
        30: Allow unmasking : 1

SO Capabilities
        0: Enable private key cloning : 1
        1: Enable private key wrapping : 0
        2: Enable private key unwrapping : 1
        3: Enable private key masking : 0
        4: Enable secret key cloning : 1
        5: Enable secret key wrapping : 1
        6: Enable secret key unwrapping : 1
        7: Enable secret key masking : 0
        10: Enable multipurpose keys : 1
        11: Enable changing key attributes : 1
        14: Enable PED use without challenge : 1
        15: Allow failed challenge responses : 1
        16: Enable operation without RSA blinding : 1
        17: Enable signing with non-local keys : 1
        18: Enable raw RSA operations : 1
        20: Max failed user logins allowed : 3
        21: Enable high availability recovery : 1
        22: Enable activation : 0
        23: Enable auto-activation : 0
        25: Minimum pin length (inverted: 255 - min) : 248
        26: Maximum pin length : 255
        28: Enable Key Management Functions : 1
        29: Enable RSA signing without confirmation : 1
        30: Enable Remote Authentication : 1
        31: Enable private key unmasking : 1
        32: Enable secret key unmasking : 1

SO Policies
        0: Allow private key cloning : 1
        1: Allow private key wrapping : 0
        2: Allow private key unwrapping : 1
        3: Allow private key masking : 0
        4: Allow secret key cloning : 1
        5: Allow secret key wrapping : 1
        6: Allow secret key unwrapping : 1
        7: Allow secret key masking : 0
```



```
                10: Allow multipurpose keys : 1
                11: Allow changing key attributes : 1
                14: Challenge for authentication not needed : 1
                15: Ignore failed challenge responses : 1
                16: Operate without RSA blinding : 1
                17: Allow signing with non-local keys : 1
                18: Allow raw RSA operations : 1
                20: Max failed user logins allowed : 3
                21: Allow high availability recovery : 1
                22: Allow activation : 0
                23: Allow auto-activation : 0
                25: Minimum pin length (inverted: 255 - min) : 248
                26: Maximum pin length : 255
                28: Allow Key Management Functions : 1
                29: Perform RSA signing without confirmation : 1
                30: Allow Remote Authentication : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
lunacm:> hsm showinfo

        HSM Label -> no label
        HSM Manufacturer -> Safenet, Inc.
        HSM Model -> K6 Base
        HSM Serial Number -> 456278
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
        Firmware Version -> 6.1.3
        Rollback Firmware Version -> 6.1.0
        Slot Id -> 1
        Tunnel Slot Id -> 2
        Session State -> CKS_RW_PUBLIC_SESSION

        SO Status->        Not Logged In
        SO information is not available (HSM has not been initialized)

        HSM Storage:
                Total Storage Space:  2097152
                Used Storage Space:   0
                Free Storage Space:   2097152
                Allowed Partitions:   20
                Number of Partitions: 0

        SO Storage:
                Total Storage Space:  262144
                Used Storage Space:   0
                Free Storage Space:   262144
                Object Count:         0

        *** The HSM is in FIPS 140-2 approved operation mode. ***
```

```
        License Count -> 7
                1. 621000026-000 621-000026-000 K6 BASE CONFIGURATION FILE,HSM UNMASKING
                2. 620127-000 ECC
                3. 620114-001 Cloning
                4. 620127-000 Test K3 ECC Update - 620127
                5. 621010358-001 621-010358-001 External MTK - STM disabled
                6. 621010089-001 621-010089-001 Remote Ped
                7. 621000021-001 SCU K5/K6 Performance 15

Command Result : No Error
lunacm:>
```

Note in the above example that HSM Capability "12: Enable non-FIPS algorithms : 1" still has a value of 1 (meaning that it remains enabled), but the associated Policy "12: Allow non-FIPS algorithms : **0** " now has a value of 0 (meaning that it has been disallowed by the SO).

Note also that the message in the middle of the "show" information now says "*** The HSM is in FIPS 140-2 approved operation mode. *** " because the HSM is now restricted to using only FIPS-approved algorithms.

Second Example – Destructive Change of HSM Policy

```
lunacm:> hsm -changeHSMPolicy -policy 15 -value 0
```

That command assigns a value of zero (0) to the “Enable SO reset of partition PIN” policy, turning it off.

The above example is a change to a destructive policy, meaning that, if you apply this policy, the HSM is zeroized and all contents are lost. For this reason, you are prompted to confirm if that is what you really wish to do. You must now re-initialize the HSM.

While this is not an issue when you have just initialized an HSM, it may be a very important consideration if your Luna HSM has been in a “live” or “production” environment and contains useful or important data, keys, certificates.

The work-around is to backup any important HSM or partition contents before making any destructive policy change, and then restore from backup after the HSM is re-initialized and the partition re-created.

Creating a Partition on a Luna PCI-E HSM

This section is HSM Partition setup for Luna PCI-E with PED (Trusted Path) Authentication. The activities in this section are required in two circumstances.

- if you just prepared an HSM on the Luna PCI-E for the first time and must now create your first HSM Partition, or
- if you have deleted or zeroized an HSM Partition and wish to create a new one to replace it.

About HSM Partitions on the Initialized HSM

At this point, Luna PCI-E should already have its Security Officer assigned by Initializing an HSM.

Within the HSM, a separate cryptographic workspaces must be created. A workspace, or Partition, and all its contents are protected by encryption derived (in part) from its authentication. Only a User who presents the proper authentication is allowed to see the Partition and to work with its contents. That User and authentication can be separate from the Security Officer identity.

In this section, you will:

- Create an HSM Partition
- Set HSM Partition Policies (Optional)

First, Login as Security Officer

To create HSM Partitions, you must login to Luna PCI-E as Security Officer. At the lunacm:> prompt, type:

lunacm:> hsm login

You are directed to Luna PED.
Authenticate as Security Officer by supplying the appropriate SO PED Key (that was imprinted during the HSM initialization step. The PED might prompts you for the numeric password PED PIN that might optionally have been assigned to the SO PED Key. Luna PED provides the SO authentication secret to the Luna PCI-E HSM.

If you fail three consecutive login attempts as Security Officer, the HSM is zeroized and cannot be used — it must be re-initialized. Zeroizing destroys all key material.

Actions that might be flagged as bad login attempts are:

- offering a PED Key that has the correct color, but that carries a wrong authentication secret for the current HSM,

- offering a PED Key that contains the correct secret, but just pressing [Enter] on the PED keypad, with no digits, when a PED PIN was expected, that is considered a bad login attempt

- offering a PED Key that contains the correct secret, but typing any numbers when no PED PIN had previously been set).

Please note that the Luna HSM must actually receive some information before it logs a failed attempt, so actions that would not trigger the bad-login counter might include:

-if you just press [Enter] on the PED keypad without a PED Key inserted, or

- if you insert a wrong-color* PED Key and press [Enter],

those are not logged as failed attempts.

When you successfully login, the counter is reset to zero.

(*Wrong color means that the PED Key that you present has been imprinted with an authentication secret for a different function than is currently requested - so inserting a cloning domain (red) key when a blue key is requested is not a bad login attempt.)

If you are not sure that you are currently logged in as Security Officer, perform an '`hsm logout`'.

Second, Create the Partition

1. Have Luna PED connected and ready (in Local mode and "Awaiting command...").
2. Insert a blank PED Key into the USB connector at the top of the PED.
3. In a terminal window (DOS command-line window in Windows), go to the LunaPCI directory and start the lunacm utility:
   lunacm:>

   This sequence assumes that you are already logged in as the HSM Security Officer (SO) or HSM Admin (another

name for the same role) as directed in the preceding section.

4. Run the "partition create" command.

```
The following is an example of initialization
 dialog, with PED interactions inserted to show the sequence of events.
lunacm:> partition create
The existing Partition will be destroyed.
Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now -> proceed
Please attend to the PED.
Command Result : No Error
        Please attend to the PED.
```

5. Luna PED asks preliminary setup questions, prior to imprinting the first Partition User/Owner PED Key (could also be called the Crypto Officer PED Key if you are using that model).

```
Slot 01
SETTING USER PIN...
Would you like to
reuse an existing
keyset? YES/NO
```

"Yes" if you have a black PED Key containing authentication for another partition (on another HSM), and you wish to preserve that authentication (so it continues to be valid for the other HSM) and imprint that value from the PED Key onto the HSM (so it becomes valid for the new partition being created).

"No" If the black PED Key that you are about to use is blank, or if it contains old authentication that is no longer needed.

Below, we show an example where the key has previous authentication on it. If you present a fresh, empty PED Key, the prompts are slightly different.

```
Slot 01
SETTING USER PIN...

M value? (1-16):

>00:
```

If you wish to split the User/Owner secret across multiple keys, such that quantity M different persons must be present with their portions in order to unlock the partition (multi-person access control), then provide a number M greater than 1. If you do not need multi-person access control and do not wish the extra administrative burden, then just type "1" and press [Enter]]

```
Slot 01
SETTING USER PIN...

N value? (M-16):

>00:
```

If you chose not to invoke multi-person access control for the new partition (you typed just "1" for the M value, then type "1" for the N value as well. If you do wish to invoke multi-person access control and you did provide an M value - for how many persons must be present to unlock the partition, then type a quantity N that is greater than M and press [Enter]. This sets the size of the pool of splits of the User/Owner secret. It should be greater than M so that

you can still achieve a quorum (M key holders) when some holders are unavailable due to business travel, vacation, sickness, etc.]

```
Slot 01
SETTING USER PIN...
Insert a USER /
Partition Owner
 PED Key
 Press ENTER.
```

6. Insert either a fresh, blank PED Key (with a black label on it,or a previously used black PED Key, as appropriate.]

```
Slot 01
SETTING USER PIN...
**WARNING**
This PED Key is
blank.
Overwrite?   YES/NO
```

OR

```
Slot 01
SETTING USER PIN...
**WARNING**
This PED Key is for
USER/PartitionOwner.
Overwrite?   YES/NO
```

- "**NO**" if the PED key that you provided carries any authentication data that must be preserved. In that case, the partition being created will be imprinted to recognize the existing Partition User authentication (that is, once this initialization is complete, this Partition User PED Key will be able to unlock the current Partition and the previous Partition(s) for which it carries the authentication secret - the secret that is already on the key will be preserved) .
- "**YES**" if the PED should overwrite (if you overwrite a never-used PED Key, nothing is lost; if you overwrite a PED Key that contains authentication secret for another Partition, then this PED Key will no longer be able to access the other Partition, only the new Partition that you are currently initializing with a new, unique authentication secret - therefore "YES" means 'do not reuse; instead overwrite the key now' - therefore, be sure that this is what you wish to do) the PED Key with a new Partition authentication. (This will be matched on Luna PCI-E during this initialization).

```
Slot 01
SETTING USER PIN...
***WARNING***
Are you sure you
want to overwrite
 this PED Key? YES/NO
```

7. This is serious business, so Luna PED asks one more time if you truly intend to overwrite the key's content.

```
Slot 01
SETTING USER PIN...

Enter new PED PIN:

Confirm new PED PIN:
```

8. Type a numeric password of at least 4 digits on the PED keypad, if you wish the additional security of a PED-

mediated numeric password - something you know - along with the physical authentication of the PED Key itself - something you have. If you do not need to invoke a PED PIN and the necessity to remember it while keeping it secret, then just press [Enter] twice, with no digits.

9. The PED prompts:

```
Slot 01
SETTING USER PIN...
Are you duplicating
this keyset? YES/NO
```

You should probably make at least one copy of this key as a backup. Some security regimes would have a working copy for on-site storage and another copy for off-site backup. As long as you continue to say "Yes" and present more keys to be imprinted, Luna PED continues to make copies of the current PED Key.

When you are done, say "No", and Luna PED goes to the next step in the sequence, creating a cloning domain for the Partition. This requires that the Partition User / Owner must be logged in.

```
Slot 01
USER LOGIN...
 Insert a USER /
 Partition Owner
PED Key
Press ENTER.
```

10. Leave the black key inserted and press [Enter]. The Partition User/Owner credentials on that key are presented to the HSM allow you to log into the partition.

Now the HSM and the PED can proceed to create a cloning domain for the new partition, and imprint that domain on both the HSM and a red PED Key. Alternatively, if you have an existing cloning domain that you would like shared with the new HSM partition, you can present a red PED Key containing that domain and have that domain imprinted onto the current HSM for the newly created partition.

```
Slot 01
SETTING DOMAIN...
Would you like to
reuse an existing
keyset? YES/NO
```

11. This is a critical choice. If this is your first Luna HSM, or if you are starting a new group of HSMs that have no connection to any others that you might own, then you should be using a blank key and writing a new Domain secret from the current HSM onto this blank PED Key. Say "No" on the PED keypad.

12. If you have existing HSMs and wish to be able to clone their partition contents to this one, or to back up their contents onto a backup HSM and then restore from there onto this HSM and partition, then this new partition MUST share the same cloning domain as those other HSMs' partitions. That means you must preserve the cloning domain secret on an existing red PED Key and imprint that secret onto the current HSM for the new partition. Say "Yes" to this "reuse" question.

```
Slot 01
SETTING DOMAIN...

M value? (1-16):

>00:
```

For a new red PED Key, this is exactly the same option (multi-person access control) as you encountered above, for the black PED Key. Type "1" and press enter if you do **not** wish to split the Domain secret and require multiple

persons when the domain is needed. Type a larger number if you **do** wish to invoke multi-person access control (splitting the Domain secret) for cloning or backup.]

```
Slot 01
SETTING DOMAIN...

N value? (M-16):

>00:
```

Again, if you chose not to invoke multi-person access control for the new partition (you typed just "1" for the M value, then type "1" for the N value as well. If you chose a larger "M", then choose a suitable "N" (up to 16) to allow some substitutions.

```
Slot 01
SETTING DOMAIN...
Insert a
Domain
 PED Key
 Press ENTER.
```

Insert either a fresh, blank PED Key (with a red label on it,or a previously used red PED Key, as appropriate.]

Depending on the condition of the key that you insert (a fresh, blank one or a used one that contains no-longer-useful data, or previously imprinted key containing a valid Domain secret, Luna PED shows one or the other of these prompts:

```
Slot 01
SETTING DOMAIN...
**WARNING**
This PED Key is
blank.
Overwrite?   YES/NO
```

OR

```
Slot 01
SETTING DOMAIN...
**WARNING**
This PED Key is for
Domain.
Overwrite?   YES/NO
```

- "**NO**" if the PED key that you provided carries any authentication data that must be preserved. In that case, the partition being created will be imprinted to recognize the existing Cloning secret (that is, once this initialization is complete, this Partition will have a cloning domain identical to the domain on current red key, and matching the domain on other HSMs- the secret that is already on the key will be preserved) .
- "**YES**" if the PED should overwrite (if you overwrite a never-used PED Key, nothing is lost; if you overwrite a PED Key that contains the cloning secret for another Partition, then this PED Key will get a new cloning domain secret from this HSM - therefore "YES" means 'do not reuse; instead overwrite the key now' - therefore, be sure that this is what you wish to do) the PED Key with a new Partition cloning domain. (This will be matched on the Luna PCI-E HSM during this initialization).

```
Slot 01
SETTING DOMAIN...
***WARNING***
Are you sure you
```



```
want to overwrite
 this PED Key? YES/NO
```

This is serious business, so Luna PED asks one more time if you truly intend to overwrite the key's content.

```
Slot 01
SETTING DOMAIN...

Enter new PED PIN:

Confirm new PED PIN:
```

As discussed for the black PED Key, earlier, type a numeric password of at least 4 digits on the PED keypad, if you wish the additional security of a PED-mediated numeric password - something you know - along with the physical authentication of the PED Key itself - something you have. If the physical PED Key (without additional secrets) is sufficient for your security scheme, if you do not need to invoke a PED PIN and the necessity to remember it while keeping it secret, then just press [Enter] twice, with no digits.

```
The PED prompts:
Slot 01
SETTING DOMAIN...
Are you duplicating
this keyset? YES/NO
```

Again, as discussed for the black keys, earlier, you should probably make at least one copy of this key as a backup. Your organization's security policies dictate how many copies you need, or are allowed to make. As long as you continue to say "Yes" and present more keys to be imprinted, Luna PED continues to make copies of the current PED Key.

When you are done, say "No", and Luna PED goes back to "Awaiting command...".

Lunacm says:

```
Command Result : No Error
lunacm:>
```

Third, Set/Change Partition Policies [Optional]

View the partition information, including Capabilities and Policies, to see if you need to change anything. Type:

```
lunacm:> partition showpolicies


        HSM Serial Number -> 65130
        Token Flags ->
CKF_RNG
CKF_LOGIN_REQUIRED
CKF_USER_PIN_INITIALIZED
CKF_RESTORE_KEY_NOT_NEEDED
CKF_EXCLUSIVE_EXISTS
        Slot Id -> 3
Session State -> CKS_RW_PUBLIC_SESSION
        Partition Capabilities
0: Enable private key cloning : 0
1: Enable private key wrapping : 0
2: Enable private key unwrapping : 1
3: Enable private key masking : 0
4: Enable secret key cloning : 0
5: Enable secret key wrapping : 1
6: Enable secret key unwrapping : 1
7: Enable secret key masking : 0
```



```
10: Enable multipurpose keys : 1
11: Enable changing key attributes : 1
14: Enable PED use without challenge : 1
15: Allow failed challenge responses : 1
16: Enable operation without RSA blinding : 1
17: Enable signing with non-local keys : 1
18: Enable raw RSA operations : 1
19: Max non-volatile storage space : 3
20: Max failed user logins allowed : 10
21: Enable high availability recovery : 1
22: Enable activation : 0
23: Enable auto-activation : 0
25: Minimum pin length (inverted: 255 - min) : 248
26: Maximum pin length : 255
28: Enable Key Management Functions : 1
29: Enable RSA signing without confirmation : 1
30: Enable Remote Authentication : 1
        Partition Policies
0: Allow private key cloning : 0
1: Allow private key wrapping : 0
2: Allow private key unwrapping : 1
3: Allow private key masking : 0
4: Allow secret key cloning : 0
5: Allow secret key wrapping : 1
6: Allow secret key unwrapping : 1
7: Allow secret key masking : 0
10: Allow multipurpose keys : 1
11: Allow changing key attributes : 1
14: Challenge for authentication not needed : 1
15: Ignore failed challenge responses : 1
16: Operate without RSA blinding : 1
17: Allow signing with non-local keys : 1
18: Allow raw RSA operations : 1
19: Max non-volatile storage space : 3
20: Max failed user logins allowed : 10
21: Allow high availability recovery : 1
22: Allow activation : 0
23: Allow auto-activation : 0
25: Minimum pin length (inverted: 255 - min) : 248
26: Maximum pin length : 255
28: Allow Key Management Functions : 1
29: Perform RSA signing without confirmation : 1
30: Allow Remote Authentication : 0
Command Result : No Error
lunacm:>
```

As an example of a change, you could type:

```
lunacm:> partition changePolicy -policy 16 -value 0
```

This would have the effect of switching off RSA blinding.

Where to go next?

Having set up your Luna PCI-E, you want to use it.

Either you have created an application of your own that can make use of an HSM, or you are using an existing third-party software. Examples might be Microsoft server applications like Certificate Services, IIS, ISA, RMS or other applications from other vendors. Normally, such applications can perform their cryptographic functions in software, using local computer resources (CPU, memory, and hard disk) with their inherent security issues, or they can be configured to make use of an HSM like Luna PCI-E.

If you are using one of the indicated Microsoft products, you will need to install the Luna CSP software and then install the server application, or else re-configure an existing installation to make use of Luna CSP (which provides the bridge between the application and the Luna HSM).

Another option is a Java-based application, in which case you should install the Luna JSP, which comes with Javadocs and sample code.

Setting Luna PCI-E Partition Policies [Optional]

Partition Capabilities represent the underlying factory configurations that are in force when a Partition is created. Partition Policies are the settings based on those configuration elements, and can be modified by the HSM Security Officer (SO). If a Capability is turned off (disabled), then it cannot be switched on with a Policy setting. Only re-manufacturing or the application of a Secure Capability Update can change a Capability from off to on (disabled to enabled). If a Capability is enabled, then the SO may be able to alter it with a Policy change, but only to make it more restrictive. The SO cannot make a Capability less restrictive.

For example, if a Capability setting requires that the minimum length of a Partition Password must be (say) seven characters, then the SO can use a Policy change to require a minimum password length of eight, nine, ten, or more characters (up to 255). A requirement for a longer password is considered to be a more restrictive security setting. The SO cannot use a Policy change to set the minimum password length to six or fewer characters, because that would be less restrictive than the original Capability which demands at least seven characters.

In most cases, Configurations and Policies are either off or on (disabled or enabled, where 0 [zero] equals off/disabled and 1 [one] equals on/enabled), but some involve a range of values, as in the example below.

Example policy change procedure

In this example, we show the initial values of the Partition Capabilities and their corresponding Policies, then we change one Policy, and show the values again.

```
lunacm:> partition showinfo

        HSM Serial Number -> 456278
        Token Flags ->
                CKF_RNG
                CKF_LOGIN_REQUIRED
                CKF_USER_PIN_INITIALIZED
                CKF_RESTORE_KEY_NOT_NEEDED
                CKF_PROTECTED_AUTHENTICATION_PATH
                CKF_TOKEN_INITIALIZED
        Slot Id -> 1
        Tunnel Slot Id -> 2
        Session State -> CKS_RW_PUBLIC_SESSION

        User Status->                   Not Logged In
        Crypto Officer Failed Logins-> 0
        Crypto User Failed Logins->    0
        User Flags ->
                CONTAINER_KCV_CREATED
        User OUID: 6e000000e400000056f60600
```



```
        User Storage:
                Total Storage Space:  2094996
                Used Storage Space:   0
                Free Storage Space:   2094996
                Object Count:         0

        *** The HSM is NOT in FIPS 140-2 approved operation mode. ***


        License Count -> 9
                1. 0009-020 Test K6 Base Config - 9-20
                2. 620109-000 Test K3 FIPS3 Update - 620109
                3. 0009-030 Test K3 HSM Cloning Update - 000009-030
                4. 620127-000 Test K3 ECC Update - 620127
                5. 0009-025 Test K3 External MTK Update 2 - 000009-025
                6. 620111-000 Test K3 Performance 600 Update - 620111
                7. 0009-015 Test K3 Remote Ped Update - 000009-015
                8. 620124-000 Test K3 Partitions 20 Update - 620124
                9. 620114-000 Test K3 Cloning Update - 620114

Command Result : No Error
lunacm:>


lunacm:> partition showpolicies

        Partition Capabilities
                0: Enable private key cloning : 1
                1: Enable private key wrapping : 0
                2: Enable private key unwrapping : 1
                3: Enable private key masking : 0
                4: Enable secret key cloning : 1
                5: Enable secret key wrapping : 1
                6: Enable secret key unwrapping : 1
                7: Enable secret key masking : 0
                10: Enable multipurpose keys : 1
                11: Enable changing key attributes : 1
                14: Enable PED use without challenge : 1
                15: Allow failed challenge responses : 1
                16: Enable operation without RSA blinding : 1
                17: Enable signing with non-local keys : 1
                18: Enable raw RSA operations : 1
                20: Max failed user logins allowed : 10
                21: Enable high availability recovery : 1
                22: Enable activation : 1
                23: Enable auto-activation : 1
                25: Minimum pin length (inverted: 255 - min) : 248
                26: Maximum pin length : 255
                28: Enable Key Management Functions : 1
                29: Enable RSA signing without confirmation : 1
                30: Enable Remote Authentication : 1
                31: Enable private key unmasking : 1
                32: Enable secret key unmasking : 1

        Partition Policies
                0: Allow private key cloning : 1
                1: Allow private key wrapping : 0
```



```
                2: Allow private key unwrapping : 1
                3: Allow private key masking : 0
                4: Allow secret key cloning : 1
                5: Allow secret key wrapping : 1
                6: Allow secret key unwrapping : 1
                7: Allow secret key masking : 0
                10: Allow multipurpose keys : 1
                11: Allow changing key attributes : 1
                14: Challenge for authentication not needed : 1
                15: Ignore failed challenge responses : 1
                16: Operate without RSA blinding : 1
                17: Allow signing with non-local keys : 1
                18: Allow raw RSA operations : 1
                20: Max failed user logins allowed :10    <--
                21: Allow high availability recovery : 1
                22: Allow activation : 0
                23: Allow auto-activation : 0
                25: Minimum pin length (inverted: 255 - min) : 248
                26: Maximum pin length : 255
                28: Allow Key Management Functions : 1
                29: Perform RSA signing without confirmation : 1
                30: Allow Remote Authentication : 1
                31: Allow private key unmasking : 1
                32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
```

In the example above, we change the maximum number of consecutive failed login attempts that is permitted on the Partition.
The default maximum is 10. You can change the maximum to less than 10, but not more than 10.
Setting to less than ten would make the partition more secure than the default, and is allowed.
Setting to more than ten would make the partition less secure than the default, and is not allowed.

```
lunacm:> partition showpolicies

        Partition Capabilities
                0: Enable private key cloning : 1
                1: Enable private key wrapping : 0
                2: Enable private key unwrapping : 1
                3: Enable private key masking : 0
                4: Enable secret key cloning : 1
                5: Enable secret key wrapping : 1
                6: Enable secret key unwrapping : 1
                7: Enable secret key masking : 0
                10: Enable multipurpose keys : 1
                11: Enable changing key attributes : 1
                14: Enable PED use without challenge : 1
                15: Allow failed challenge responses : 1
                16: Enable operation without RSA blinding : 1
                17: Enable signing with non-local keys : 1
                18: Enable raw RSA operations : 1
                20: Max failed user logins allowed : 10
                21: Enable high availability recovery : 1
                22: Enable activation : 1
                23: Enable auto-activation : 1
```



```
            25: Minimum pin length (inverted: 255 - min) : 248
            26: Maximum pin length : 255
            28: Enable Key Management Functions : 1
            29: Enable RSA signing without confirmation : 1
            30: Enable Remote Authentication : 1
            31: Enable private key unmasking : 1
            32: Enable secret key unmasking : 1

        Partition Policies
            0: Allow private key cloning : 1
            1: Allow private key wrapping : 0
            2: Allow private key unwrapping : 1
            3: Allow private key masking : 0
            4: Allow secret key cloning : 1
            5: Allow secret key wrapping : 1
            6: Allow secret key unwrapping : 1
            7: Allow secret key masking : 0
            10: Allow multipurpose keys : 1
            11: Allow changing key attributes : 1
            14: Challenge for authentication not needed : 1
            15: Ignore failed challenge responses : 1
            16: Operate without RSA blinding : 1
            17: Allow signing with non-local keys : 1
            18: Allow raw RSA operations : 1
            20: Max failed user logins allowed :9    <--
            21: Allow high availability recovery : 1
            22: Allow activation : 0
            23: Allow auto-activation : 0
            25: Minimum pin length (inverted: 255 - min) : 248
            26: Maximum pin length : 255
            28: Allow Key Management Functions : 1
            29: Perform RSA signing without confirmation : 1
            30: Allow Remote Authentication : 1
            31: Allow private key unmasking : 1
            32: Allow secret key unmasking : 1


Command Result : No Error
lunacm:>
```

Note in the above example that HSM Capability "20: Max failed user logins allowed : 10" still has a value of 10 (meaning that 10 is as many failed Partition login attempts as can be permitted), but the associated Policy "20: Max failed user logins allowed : **9**" now has a value of 9 - meaning that the SO has decided that 10 bad login attempts on the Partition was too many. The SO has used the Policy to impose greater restriction than the Capability required; that is, the SO has increased the security on the partition.

CHAPTER 3
Optional Configuration Tasks

After completing the base configuration, you can also perform any of the following optional configuration tasks:

Configure multiple HSMs to operate in high-availability (HA) mode

High Availability (HA) mode allows you to automatically replicate the data on a HSM/partition over two or more physical HSMs to provide redundancy and load balancing. Applications using an HA HSM/partition do not access it directly. Instead, the HA software creates a virtual slot for the partition and manages which physical HSM is actually used when responding to an application request. See "High Availability (HA) Mode" on page 1 in the *Administration Guide*.

Configure SNMP

You can use the Luna SNMP MIB to monitor the performance of your HSMs. See "SNMP Monitoring" on page 1 in the *Administration Guide*.

Configure a remote PED

If you are configuring a PED-authenticated HSM, you can configure it to use a remote PED, which allows you to authenticate to the HSM from a remote location. See "Remote PED" on page 1 in the *Administration Guide*.