SafeNet USB HSM

Configuration Guide

gemalto
security to be free

Document Information

Product Version	6.2.2
Document Part Number	007-011302-014
Release Date	01 December 2016

Revision History

Revision	Date	Reason
A	01 December 2016	Initial release.
B	03 February 2017	Reinstate "Technology Preview"

Trademarks

Acknowledgements

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software developed by the University of California, Berkeley and its contributors.

This product uses Brian Gladman's AES implementation.

Refer to the End User License Agreement for more information.

Regulatory Compliance

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

USA, FCC

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a "Class B" digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Changes or modifications not expressly approved by SafeNet could void the user's authority to operate the equipment.

Canada

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

Europe

This product is in conformity with the protection requirements of EC Council Directive 2004/108/EC. Conformity is declared to the following applicable standards for electro-magnetic compatibility immunity and susceptibility; CISPR22and IEC801. This product satisfies the CLASS B limits of EN 55022.

Disclaimer

Gemalto 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, Gemalto reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon Gemalto 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.

Gemalto 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	Gemalto 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 11
- "Configuring a PED-Authenticated HSM" on page 23
- "Optional Configuration Tasks" on page 45

This preface also includes the following information about this document:

- "Customer Release Notes" below
- "Gemalto Rebranding" below
- "Audience" on the next page
- "Document Conventions" on the next page
- "Support Contacts" on page 8

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_6-2-2.pdf

Gemalto Rebranding

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

Old product name	New product name
Luna SA HSM	SafeNet Network HSM
Luna PCI-E HSM	SafeNet PCIe HSM
Luna G5 HSM	SafeNet USB HSM
Luna PED	SafeNet PED

Old product name	New product name
Luna Client	SafeNet HSM Client
Luna Dock	SafeNet Dock
Luna Backup HSM	SafeNet Backup HSM
Luna CSP	SafeNet CSP
Luna JSP	SafeNet JSP
Luna KSP	SafeNet KSP

Note: These branding changes apply to the documentation only. The SafeNet HSM software and utilities continue to use the old names.

Audience

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

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

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

Document Conventions

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

Notes

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

Note: Take note. Contains important or helpful information.

Cautions

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

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

Warnings

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

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

Command syntax and typeface conventions

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

Support Contacts

Contact method	Contact
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA

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

Introduction

After your SafeNet HSM has been unpacked and installed, and the associated SafeNet HSM Client software is installed on the host computer, a few configuration steps remain, to prepare the HSM for use with your client application (s). Some are required, before you can place the HSM in operation; others are optional. Some decisions are required at each stage.

The first task is to initialize the HSM, assigning a Security Officer role, to oversee and administer the HSM. Then you can apply some optional, global settings.

- "Configuring a Password-Authenticated HSM" on page 1

  or

- "Configuring a PED-Authenticated HSM" on page 1

  and optionally

- "HSM Capabilities and Policies" on page 1.

The second task declares a special area within the HSM called an application partition, that your application accesses, to create, store, and use keys, certificates, and other crypto objects. Part of the task is to choose a style of interaction,

- either one that we have termed "legacy", where the HSM SO retains ownership and oversight of the application partition, and the HSM SO creates a Crypto Officer to handle access-control by applications,
- or the newer Per-Partition Security Officer (PPSO) style, where a Partition SO is created to oversee the application partition, and the HSM SO has no further interaction, and no ability to see, inside the partition; the Partition SO sets policies and performs other administration within the application partition, and creates a Crypto Officer to handle access-control by applications.

The HSM must be initialized (above) before the HSM SO can create an application partition of any style. See

"Creating a Legacy Application Partition on SafeNet PCIe HSM" on page 1 or "Overview - Configure a PED-Authenticated Application Partition" on page 1

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 SafeNet PED. A Password Authenticated version will prompt you for the password. You cannot change the authentication type of a SafeNet 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 SafeNet USB HSM" on the next page.
2. Change the HSM policies, if desired, as described in "Setting SafeNet USB HSM Policies [Optional]" on the next page. 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 SafeNet USB HSM" on page 17.
4. Change the partition policies, if desired, as described in "Setting SafeNet USB HSM Partition Policies [Optional] " on page 19

Initializing a Password-Authenticated SafeNet USB HSM

Initialization assigns a meaningful label and a Security Officer password, and places the HSM in a state ready to use.

Use the instructions on this page if you have a SafeNet USB HSM with Password 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.

First, Login as Security Officer

To perform HSM operations, you must login as the Security Officer (SO). For a new SafeNet USB HSM module, the HSM Security Officer password is “default”. Type:

```
lunacm:> hsm login -password default
Command Result : No Error
lunacm:>
```

The SafeNet USB HSM arrives in a default, ready-to-initialize state. Before you can make use of it, the HSM must be initialized (assigned a name/label and an SO password). This establishes your ownership for current and future HSM administration.

Second, Initialize the HSM

```
lunacm:> hsm init -label mylunaG5 -password Fu22y!00
     You
 are about to initialize the HSM.
The User will be deleted and all data will be erased.
Are you sure you wish to continue?
Type 'proceed' to continue, or 'quit' to quit now -> proceed
Command Result : No Error
```

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, of course, be displayed.

The next step is to "Creating a Partition on SafeNet USB HSM" on page 17 on the HSM.

Setting SafeNet USB 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.

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.

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

   ```
   lunacm:> hsm showinfo
   ```



```
        HSM
 Label -> myLunaG5
HSM Manufacturer -> SafeNet, Inc.
HSM Model -> K4Base
HSM Serial Number -> 8000001
Token Flags ->
CKF_RNG
CKF_LOGIN_REQUIRED
CKF_RESTORE_KEY_NOT_NEEDED
CKF_PROTECTED_AUTHENTICATION_PATH
CKF_TOKEN_INITIALIZED
Firmware Version -> 4.5.2
Slot Id -> 1
Session State -> CKS_RW_PUBLIC_SESSION
SO Status: Not Logged In
*** The HSM is NOT in FIPS 140-2 approved operation mode. ***
Command Result : No Error
lunacm:>
```

Note the message at 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 : 9
3: Enable MofN : 0
4: Enable domestic mechanisms & key sizes : 1
6: Enable masking : 1
7: Enable cloning : 0
8: Enable special cloning certificate : 0
9: Enable full (non-backup) functionality : 1
11: Enable ECC mechanisms : 0
12: Enable non-FIPS algorithms : 1
13: Enable MofN auto-activation : 0
15: Enable SO reset of partition PIN : 1
16: Enable network replication : 0
17: Enable Korean Algorithms : 0
18: FIPS evaluated : 0
19: Manufacturing Token : 0
20: Enable Remote Authentication : 1
21: Enable forcing user PIN change : 0
22: Enable offboard storage : 1
23: Enable partition groups : 0
      HSM Policies
0: PIN-based authentication : 0
1: PED-based authentication : 1
3: Require MofN : 0
6: Allow masking : 0
7: Allow cloning : 0
12: Allow non-FIPS algorithms :  1
13: Allow MofN auto-activation : 0
15: SO can reset partition PIN : 1
16: Allow network replication : 0
20: Allow Remote Authentication : 1
```



```
21: Force user PIN change after set/reset : 0
22: Allow offboard storage : 1
23: Allow partition groups : 0
        SO Capabilities
0: Enable private key cloning : 0
1: Enable private key wrapping : 0
2: Enable private key unwrapping : 1
3: Enable private key masking : 1
4: Enable secret key cloning : 0
5: Enable secret key wrapping : 1
6: Enable secret key unwrapping : 1
7: Enable secret key masking : 1
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 : 3
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
        SO Policies
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 : 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
Command Result : No Error
lunacm:>
```


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 the SafeNet PED if this is a PED-authenticated HSM (SafeNet PED must be connected and ready before you login) - 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 SafeNet PED screen.

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

lunacm:> hsm showpolicies
        HSM Capabilities
0: Enable PIN-based authentication : 0
1: Enable PED-based authentication : 1
2: Performance level : 9
3: Enable MofN : 0
4: Enable domestic mechanisms & key sizes : 1
6: Enable masking : 0
7: Enable cloning : 0
8: Enable special cloning certificate : 0
9: Enable full (non-backup) functionality : 1
11: Enable ECC mechanisms : 0
12: Enable non-FIPS algorithms : 1
13: Enable MofN auto-activation : 0
15: Enable SO reset of partition PIN : 1
16: Enable network replication : 0
17: Enable Korean Algorithms : 0
18: FIPS evaluated : 0
19: Manufacturing Token : 0
20: Enable Remote Authentication : 1
21: Enable forcing user PIN change : 0
         HSM Policies
0: PIN-based authentication : 1
1: PED-based authentication : 0
3: Require MofN : 0
6: Allow masking : 0
7: Allow cloning : 0
12: Allow non-FIPS algorithms :  0      <--
13: Allow MofN auto-activation : 0
15: SO can reset partition PIN : 1
16: Allow network replication : 0
20: Allow Remote Authentication : 1
21: Force user PIN change after set/reset : 0
        SO 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 : 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
        SO Policies
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 : 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
Command Result : No Error
lunacm:>
lunacm:> hsm showinfo
        HSM Label -> myLunaG5
HSM Manufacturer -> SafeNet, Inc.
HSM Model -> K4Base
HSM Serial Number -> 8000001
Token Flags ->
CKF_RNG
CKF_LOGIN_REQUIRED
CKF_RESTORE_KEY_NOT_NEEDED
CKF_PROTECTED_AUTHENTICATION_PATH
CKF_TOKEN_INITIALIZED
Firmware Version -> 4.5.2
Slot Id -> 1
```



```
Session State -> CKS_RW_PUBLIC_SESSION
SO Status: Not Logged In
*** The HSM is in FIPS 140-2 approved operation mode. ***
Command Result : No Error
lunacm:>
```

Note: 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 at the top 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.

Creating a Partition on SafeNet USB HSM

This section is HSM Partition setup for SafeNet USB HSM with Password Authentication. The activities in this section are required in two circumstances.

- if you just prepared an HSM on the SafeNet USB HSM 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, the SafeNet USB HSM 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 the SafeNet USB HSM 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.

Note: 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. Please note that the SafeNet 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 login, the counter is reset to zero.

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

Second, Create the Partition

At the lunacm:> prompt, type:

```
lunacm:> partition create -password <a_partition_password>
```

SafeNet USB HSM replies "Command Result : No Error"

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.

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.

For more detail, see "Setting SafeNet USB HSM Partition Policies [Optional]" below.

Where to go next?

Having set up your SafeNet USB HSM, 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 SafeNet USB HSM.

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

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

Setting SafeNet USB HSM 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.

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 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
        MofN Status ->
MofN Not Generated
 *** The HSM is NOT in FIPS 140-2 approved operation mode. ***
        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
27: Enable RA-type wrapping : 0
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
27: Allow RA-type wrapping : 0
28: Allow Key Management Functions : 1
29: Perform RSA signing without confirmation : 1
30: Allow Remote Authentication : 0
Command Result : No Error
lunacm:>
lunacm:> hsm login -password mySOpa55word!
Command Result : No Error
lunacm:> partition changePolicy -policy 20 -value 9

Command Result : No Error
lunacm:>
```

Note: 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.

```
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
        MofN Status ->
MofN Not Generated
 ***
 The HSM is NOT in FIPS 140-2 approved operation mode. ***
        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
27: Enable RA-type wrapping : 0
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 : 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
27: Allow RA-type wrapping : 0
28: Allow Key Management Functions : 1
29: Perform RSA signing without confirmation : 1
30: Allow Remote Authentication : 0
Command Result : No Error
lunacm:>
```

Note: 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.

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 SafeNet PED. A Password Authenticated version will prompt you for the password. You cannot change the authentication type of a SafeNet 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 SafeNet 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. If the HSM has been shipped in Secure Transport Mode, you must recover the MTK by providing the external split of the Secure Recovery Vector (SRV) that is carried on the Secure Recovery Key (SRK), together with the internal split, combines to recreate the MTK, as described in "Recovering the SRK" on the next page.
2. Initialize the HSM, as described in "Initializing a PED-Authenticated SafeNet USB HSM " on the next page.
3. Change the HSM policies, if desired, as described in "Setting SafeNet USB 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.
4. Create a partition on the HSM, as described in "Creating a Partition on SafeNet USB HSM" on page 35.

5. Change the partition policies, if desired, as described in "Setting SafeNet USB HSM Partition Policies [Optional] " on page 41

Recovering the SRK

PED-authenticated SafeNet USB HSMs might have been shipped from the factory in Secure Transport Mode (an extra-cost shipping and handling treatment). Alternatively, you might have elected to set Secure Transport mode before shipping the HSM to another of your organization's locations, or before shipping to a customer of yours. In this mode, and similar to the state following a system or HSM tamper event, the Master Tamper Key (MTK) is invalidated. Almost all objects on the HSM are encrypted by the MTK, so when that is not available inside the HSM, the HSM is not usable.

Before you can begin configuring or using the HSM, you must recover the MTK by providing the external split of the Secure Recovery Vector (SRV) that is carried on the Secure Recovery Key (SRK), together with the internal split, combines to recreate the MTK.

The SRK secret is held on the purple SRK PED Key(s), shipped to you separately from the HSM.

1. With the SafeNet USB HSM powered and connected to a SafeNet PED, and also connected to a computer with the Lung G5 software and driver installed, open a command-prompt window and start the lunacm utility.
2. Verify that the HSM is in "Hardware tamper zeroize" or "User requested zeroize" (transport) mode.

```
lunacm:> srk show
     SRK State Flags ->
         SRK Regeneration Required:   0
         Hardware (tamper) Zeroize: 0
         User Requested Zeroize:    1
         Locked:                    1
Command Result : No Error
lunacm:>
```

3. Recover the srk with the command

```
lunacm:> srk recover
```

   Refer to the SafeNet PED and follow the prompts to insert the purple PED Key, enter responses on the PED keypad, etc.
4. During the process, a validation string is shown. You should have received your HSM's validation string by separate mail. Compare that to the string that you see during SRK recovery. They should match. If so, acknowledge the match when requested, and the recovery process concludes with the SRK recreated on the HSM.

When the SRV has been retrieved from the SRK, onto the HSM, and combined with the internally-stored split to regenerate the MTK on the HSM, the HSM is still in zeroized state. However, with the MTK restored you can now resume using the HSM, if it was previously operational, or for a new HSM you can continue to the next configuration step, initializing the HSM.

Go to "Initializing a PED-Authenticated SafeNet USB HSM " below.

Initializing a PED-Authenticated SafeNet USB HSM

The SafeNet USB HSM arrives in a default, pre-initialized state. 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 a SafeNet USB HSM with Trusted Path authentication.

Initialize the HSM(required before you can create Partitions or Groups and use the HSM) to set up the necessary identities, ownership and authentication at the HSM Server level. To initialize a SafeNet HSM with Trusted Path Authentication, you must have the SafeNet PED connected and switched on, and in the “Awaiting command..”(when you power on the SafeNet PED, the screen displays the PED's firmware version while it goes through its self-test routine; it is not ready to accept commands from the SafeNet HSM until it completes that process (a few seconds), switches to "SCP mode..." or "Local" mode, and displays "Awaiting command..") state, and you must have a set of PED Keys.

A minimum set of PED Keys consists of:

- one Security Officer key (represented by the blue label),

- one Partition User key (represented by the black label)

- one Domain key (represented by the red label).

If you invoke MofN shared-secret authentication for any of those, you will need additional blanks of the same color to achieve quantity "N" of those PED Keys ["N" and "M" are values that you declare via SafeNet PED, during initialization, so you control how many imprintable PED Keys you will need]. For example if the SafeNet PED is imprinting blue SO PED Keys and asks for the N value and you select 1, then MofN is not invoked and you need to provide only a single blue key. However, if you select an N value greater than 1, then MofN is invoked and you will need to provide quantity N of blue keys for imprinting with portions of the SO secret. Note that this number is separate and distinct from any Duplicate PED Keys that you may choose to imprint.

If you invoke MofN and also choose to duplicate PED Keys [for backup or other purpose] then you must have enough of the current color of keys to duplicate the complete MofN set -- thus if you set MofN to 1 of 3, and choose to duplicate, then you would need three blue keys to complete the original secret shares, and additional groups of three [different] blue keys to form each duplicate set.) The above applies to the red Domain keys, as well - however, your choice to invoke, or not invoke, MofN for the blue keys does not affect your choice to invoke (or not) MofN for the red keys, and vice-versa.

You do not make these choices at the command line. They are made via the SafeNet PED, once the 'hsm init' command is received from the lunacm command line.

In addition, you might have orange RPV (Remote PED Vector) keys for use with the remote PED option, but these are not needed during initialization. See "Remote PED and pedclient and pedserver " on page 1 in the *Administration Guide*.

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.

Initializing the HSM

You should have ready a sufficient number of blue-labeled PED Keys for HSM authentication secret and its backups/duplicates, and a sufficient number of red-labeled PED Keys for the Domain secret and its backups/duplicates. If the blank keys are not already labelled, do so before you invoke the initialization - otherwise you might not have time to finish the task before timeout occurs.

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

Start the Initialization Process

SafeNet PED operation is required several times throughout the procedure. If, for any reason, the SafeNet HSM is allowed to timeout during a PED operation, you can switch the PED off, then switch it on again, or press and hold the [Clear] button and wait for "Awaiting command..." before re-starting the command that timed out.

What does "a sufficient number" of PED Keys mean? It means at least one of each for the absolute minimum setup, as you might prepare in a lab. For a production environment, you might prefer to have one or more backups of each type of PED Key for disaster recovery and for operational reasons - the number is, of course, up to you and your security rules.

Additionally, if you expect to use the MofN option (splitting the Security Officer, User, or Domain secrets among sets of keys that must be recombined for access) then you will need quantity N of each set, and then as many sets as your security rules require.

The first time you initialize, the system uses the default login (the default login requires no PED Key, because the HSM has not been initialized, and thus does not yet contain anything that needs protection - the default login occurs only on a zeroized hsm; thus if you ever see the words "Default login..." on the SafeNet PED, you must be attempting to login or to initialize an empty HSM) on the SafeNet PED. Subsequently, you login with the blue SO PED Key.

1. Have the SafeNet PED connected and ready (in SCP mode [or Local PED mode] and "Awaiting command...").
2. Insert a blank PED Key into the USB connector at the top of the PED.
3. Start the lunacm utility:

```
C:\Program Files\SafeNet\LunaClient>lunacm
.
LunaCM V2.3 - Copyright (c) 2009 SafeNet, Inc.
        Available HSM's:
Slot Id ->              1
HSM Label ->            no label
HSM Serial Number ->    8000001
HSM Model ->            K5Base
HSM Firmware Version -> 4.7
HSM Configuration ->    SafeNet USB HSM Undefined 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
4. Begin HSM initialization. At the lunacm prompt, type:

```
lunacm:> hsm init -label myLunaHSM
```

   The following warning appears only if you are re-initializing an HSM:


```
WARNING !!  This command will delete all HSM partitions and data.
If you are sure that you wish to proceed, then enter 'proceed',
otherwise this command will abort.
>
```

Type:

proceed

The system responds:

```
Luna PED operation required to initialize HSM - use blue PED key.
```

5. At this time, the SafeNet PED becomes active and begins prompting you for PED Keys and other responses. For security reasons, this sequence has a time-out, which is the maximum permitted duration, after which an error is generated and the process stops. If you allow the process to time-out, you must re-issue the initialization command.

   If the operation has timed out, leaving the SafeNet PED waiting for an action that is no longer needed, press and hold the the [Clear] key to reset the PED, and wait for "Awaiting command...", before you (re-)issue a `lunacm` command that invokes the PED. The SafeNet PED generally must be in the “Awaiting command..” state before it is invoked by the SafeNet HSM.

   If you make a mistake (perhaps an inadvertent choice with the PED), and wish to re-do the command, simply [Clear] the PED and let the `lunacm` command time-out. Then re-issue the `lunacm` command.

6. SafeNet PED asks preliminary setup questions, prior to imprinting the first blue (SO) PED Key.

   ```
   Token found at 01
   SO login...
   Default SO login...
   Writing SO PIN...
   Would you like to reuse an existing
   keyset? (y/n)
   ```

7. If data is encountered on the PED Key that you provide, the system can treat it in one of two ways:
   - It can act on the premise that you have another HSM for which the existing authentication secret is valid, and you wish the current HSM to be provided with that same secret. Therefore, you want to preserve the secret that is found on the PED Key and imprint that same secret onto the new HSM. You will be able to use this SO PED Key to unlock both HSMs. If that is the case, answer "Yes" (press the YES button on the PED keypad).
   - It can act on the premise that any data or secret that is found on the PED Key is invalid and not to be used. In that case, a new secret is created, overwriting whatever was on the PED Key before, and that same secret is imprinted onto the HSM. The PED Key can then unlock only the new HSM - any previous authentication secret that it might have held is gone. If that is the case, answer "No" (press the NO button on the PED keypad).

8. Answer the question (press the appropriate button on the PED keypad). The next prompt to appear on the PED is:

   ```
   Slot 01:
   Prompt for numeric...

   M value? (1-16)
   >00
   ```

9. If you do not wish to invoke MofN , then press "1" and press "ENTER" on the PED keypad.

10. SafeNet PED wants to know if you wish to invoke MofN. This splits the SO authentication across quantity "N" blue keys (up to 16) and requires that quantity "M" of them be presented whenever SO access is desired. This is an extra security measure that prevents any one person from gaining access without the co-operation of additional key-holders. It is required only in very-high-security regimes with exceptionally rigorous procedures.

This prompt is asking you to decide the "M" the minimum number of key-holders who will be required to unlock the HSM in future. "M" is normally chosen less than "N".

These MofN prompts appear only if you have chosen to create a new SO authentication secret (that is, if you answered "NO" to the earlier question "Would you like to reuse an existing keyset?")

```
Slot 01:
Prompt for numeric...

N value? (M-16)
>00
```

SafeNet PED is now asking for the other value in the MofN definition (N is the size of the full MofN set, therefore a number between M and 16 - usually, you would make "N" larger than "M", so that your HSM could by accessed while some trusted key-holders were not available). Again, if you are not invoking MofN, then press "1" and "ENTER".

11. SafeNet PED demands the first blue PED Key.

```
Slot 01:
Setting SO PIN...

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

Insert a blue PED Key

Insert the blue SO (Security Officer) PED Key and press ENTER. A unique SO PIN is to be imprinted on both the PED Key and the HSM. You might see the following message, depending upon your earlier response to the "reuse" question.

```
Slot 01:
Setting SO PIN...
*WARNING***
This PED Key is for
SO / HSM Admin.
Overwrite? YES/NO>
```

SafeNet PED is reminding you that whatever is written on this PED Key will now be overwritten by a new SO authentication secret. If this is a new PED Key, the message is of no importance. If this PED Key has been used before, and possibly has an authentication secret to unlock another SafeNet HSM, then this is your last chance to preserve that authentication data and use another blue key instead. If you said YES to the question "Would you like to reuse an existing keyset?", above, then this message about overwriting does not appear.

Just to be sure that you were paying attention, it asks you again:

```
               Slot
 01:
Setting SO PIN...
   *WARNING***
   Are you sure you
   want to overwrite
   this PED Key? YES/NO>
```

Provide a PED PIN (optional)

Next, you are asked to provide a PED PIN that must be typed on the PED keypad at the time a PED Key is presented – can be 4-to-48 digits, or can be set to no digits if a PED PIN is not desired; if you wish to have a PED PIN incorporated as part of the SO authentication hereafter, then type a series of numbers on the PED keypad [at this prompt] and press ENTER.

Note: do not begin your PED PIN with a zero.
(When the leading digit is zero, the PED ignores any digits following the exact PED PIN. Thus an an attacker attempting to guess the PED PIN must get the first digits correct, but does not need to know the exact length of the PED PIN. If the PED PIN is started with any digit other than zero, extra digits are detected as an incorrect attempt. This is not considered a serious vulnerability since any attacker must
a) have physical possession of the PED KEY,
b) have physical access to the HSM and PED, and
c) gets only three tries to guess correctly, before the HSM is zeroized.) .

```
Slot 01:
Setting SO PIN...
Enter new PED PIN
Password::
```

Enter a PIN if you wish, and press ENTER to inform SafeNet PED that you are finished entering PED PIN digits, or that you have decided not to use a PED PIN (no digits entered).

```
            Slot 01:

Setting SO PIN...
Confirm new PED PIN
Password:
```

Confirm(When you provide a PED PIN – even if it is the null PIN (by just pressing ENT with no digits) – SafeNet PED asks for it a second time, to ensure that you entered it correctly.) , by entering the same PED PIN(or nothing if you did not enter a PIN the first time) , and pressing ENTER again.

```
Setting SO PIN
Please wait..
```

It is only at this point that the key is actually imprinted.

Duplicating Your PED Key

You are prompted

```
Slot 01:
Prompt for YES/NO...
Are you duplicating
this keyset Y/N?
```

If you respond “NO”, SafeNet PED goes on to the next step in initialization of the HSM (creating/imprinting a domain). The PED behaves differently for "first" and "duplicate" PED Keys, depending on how you answered the question about reusing an existing keyset.

If you chose to generate new authentication data (you chose "NO" to "reuse an existing keyset"), then the PED must ask you about MofN and about the PED PIN option when creating the primary PED Key, and must ask again about the PED PIN when creating the duplicate(s).] .

If you respond “YES”, SafeNet PED asks for more blue PED Keys, until you have imprinted (duplicated) as many as you require. The PED behaves differently for "first" and "duplicate" PED Keys, depending on how you answered the question about reusing an existing keyset.
If you are re-using the authentication data, then the PED just accepts the blue key (or keyset), as-is, and gives the authentication data to the HSM to become the HSM's new authentication secret. Therefore, the PED does not ask you about MofN or about PED PINs. The assumption is that this PED Key is from another SafeNet HSM and must remain unchanged, so that it can continue to unlock that other HSM.
When the time comes to create duplicates, the PED can see whether the secret is split (MofN) or not and prompts accordingly, but it always asks the PED PIN question because the PED PIN is an optional overlay for any key.] .

This is your opportunity to make additional copies. The prompt is worded "keyset" in case you chose to invoke MofN. If no MofN, then the single SO key is duplicated until you run out of blank blue keys or decide to stop. If you invoked MofN earlier for the SO key, then the entire set of N blue keys must be duplicated; therefore you must have enough blanks to make complete additional sets.) of the imprinted SO PED Key, for backup or other operational purpose.

It is recommended to have at least one backup set of imprinted PED Keys, stored in a safe place, in case of loss or damage to the primary keys.

When you have finished with blue SO keys, SafeNet PED prompts for an imprinted blue SO key(If you had invoked MofN, then you will be prompted to insert quantity M of the imprinted blue SO keys, enough to reconstruct the split SO secret.) , because you now must use that key to login to the HSM (At this point, the new authentication data has been imprinted onto the HSM, but the HSM, being freshly initialized, is not yet in the login state using that new authentication data. The HSM demands a login now, before going ahead with the next step.) as SO, to perform the next step.

Setting SafeNet USB 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.

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.

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

```
lunacm:> hsm showinfo
        HSM
 Label -> myLunaG5
HSM Manufacturer -> SafeNet, Inc.
HSM Model -> K4Base
HSM Serial Number -> 8000001
Token Flags ->
CKF_RNG
CKF_LOGIN_REQUIRED
CKF_RESTORE_KEY_NOT_NEEDED
CKF_PROTECTED_AUTHENTICATION_PATH
CKF_TOKEN_INITIALIZED
Firmware Version -> 4.5.2
Slot Id -> 1
Session State -> CKS_RW_PUBLIC_SESSION
```



```
SO Status: Not Logged In
*** The HSM is NOT in FIPS 140-2 approved operation mode. ***
Command Result : No Error
lunacm:>
```

Note the message at 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 : 9
3: Enable MofN : 0
4: Enable domestic mechanisms & key sizes : 1
6: Enable masking : 1
7: Enable cloning : 0
8: Enable special cloning certificate : 0
9: Enable full (non-backup) functionality : 1
11: Enable ECC mechanisms : 0
12: Enable non-FIPS algorithms : 1
13: Enable MofN auto-activation : 0
15: Enable SO reset of partition PIN : 1
16: Enable network replication : 0
17: Enable Korean Algorithms : 0
18: FIPS evaluated : 0
19: Manufacturing Token : 0
20: Enable Remote Authentication : 1
21: Enable forcing user PIN change : 0
22: Enable offboard storage : 1
23: Enable partition groups : 0
      HSM Policies
0: PIN-based authentication : 0
1: PED-based authentication : 1
3: Require MofN : 0
6: Allow masking : 0
7: Allow cloning : 0
12: Allow non-FIPS algorithms :  1
13: Allow MofN auto-activation : 0
15: SO can reset partition PIN : 1
16: Allow network replication : 0
20: Allow Remote Authentication : 1
21: Force user PIN change after set/reset : 0
22: Allow offboard storage : 1
23: Allow partition groups : 0
      SO Capabilities
0: Enable private key cloning : 0
1: Enable private key wrapping : 0
2: Enable private key unwrapping : 1
3: Enable private key masking : 1
4: Enable secret key cloning : 0
5: Enable secret key wrapping : 1
6: Enable secret key unwrapping : 1
7: Enable secret key masking : 1
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 : 3
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
        SO Policies
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 : 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
Command Result : No Error
lunacm:>
```

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 the SafeNet PED if this is a PED-authenticated HSM (SafeNet PED must be connected and ready before you login) - 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 SafeNet PED screen.

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



```
 command Result : No error

lunacm:> hsm showpolicies
        HSM Capabilities
0: Enable PIN-based authentication : 0
1: Enable PED-based authentication : 1
2: Performance level : 9
3: Enable MofN : 0
4: Enable domestic mechanisms & key sizes : 1
6: Enable masking : 0
7: Enable cloning : 0
8: Enable special cloning certificate : 0
9: Enable full (non-backup) functionality : 1
11: Enable ECC mechanisms : 0
12: Enable non-FIPS algorithms : 1
13: Enable MofN auto-activation : 0
15: Enable SO reset of partition PIN : 1
16: Enable network replication : 0
17: Enable Korean Algorithms : 0
18: FIPS evaluated : 0
19: Manufacturing Token : 0
20: Enable Remote Authentication : 1
21: Enable forcing user PIN change : 0
         HSM Policies
0: PIN-based authentication : 1
1: PED-based authentication : 0
3: Require MofN : 0
6: Allow masking : 0
7: Allow cloning : 0
12: Allow non-FIPS algorithms :  0      <--
13: Allow MofN auto-activation : 0
15: SO can reset partition PIN : 1
16: Allow network replication : 0
20: Allow Remote Authentication : 1
21: Force user PIN change after set/reset : 0
        SO 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 : 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
        SO Policies
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 : 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
Command Result : No Error
lunacm:>
lunacm:> hsm showinfo
        HSM Label -> myLunaG5
HSM Manufacturer -> SafeNet, Inc.
HSM Model -> K4Base
HSM Serial Number -> 8000001
Token Flags ->
CKF_RNG
CKF_LOGIN_REQUIRED
CKF_RESTORE_KEY_NOT_NEEDED
CKF_PROTECTED_AUTHENTICATION_PATH
CKF_TOKEN_INITIALIZED
Firmware Version -> 4.5.2
Slot Id -> 1
Session State -> CKS_RW_PUBLIC_SESSION
SO Status: Not Logged In
*** The HSM is in FIPS 140-2 approved operation mode. ***
Command Result : No Error
lunacm:>
```

Note: 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 at the top 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.

Creating a Partition on SafeNet USB HSM

This section is HSM Partition setup for SafeNet USB HSM with Trusted Path Authentication. The activities in this section are required in two circumstances.

- if you just prepared an HSM on the SafeNet USB HSM 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, the SafeNet USB HSM 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 [the infrastructure of the partition]
- Set HSM Partition Policies (Optional)
- Create a challenge secret [generated by the PED and later presented/typed at the command line by the Crypto Officer when the CO needs to administer the partition]
- Create a Crypto User [and another secret generated by the PED and later presented programmatically or typed at the command line by the Crypto User when the user or client software needs to use the HSM Partition for cryptographic functions]

The above structure ensures the separation of roles between the end-users of the HSM and those who administer the partition.

First, Login as Security Officer

To create HSM Partitions, you must login to the SafeNet USB HSM as Security Officer. At the lunacm:> prompt, type:

```
lunacm:> hsm login
```

You are directed to the SafeNet PED.
Authenticate as Security Officer by supplying the appropriate SO PED Key (that was imprinted during the HSM initialization step. The PED prompts you for the numeric password to unlock the SO PED Key, which in turn provides the SO authentication secret to the SafeNet USB 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. When you successfully login, the counter is reset to zero.

Note: If you present the wrong type of PED Key - a black or red key when a blue key is called for, for example - the PED merely tells you to try again, and no bad login attempt is reported. However, if you present the wrong PED Key of the correct type, OR you present the correct PED Key but the wrong PED PIN (the [optional] multi-digit number that is input from the PED keypad) then that IS recorded as a bad login attempt and the counter is incremented.

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

Second, Create the Partition

1. Have the SafeNet PED connected and ready (in SCP or Local mode and "Awaiting command...").
2. In a terminal window (DOS command-line window in Windows), go to the LunaG5 directory and start the lunacm utility:
   ```
   lunacm:>
   ```
3. Log in as SO (the blue PED Key) with the lunacm command:
   ```
   lunacm:> hsm login
   ```
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
   Please attend to the PED.
   ```

   SafeNet PED asks preliminary setup questions, prior to imprinting the first SO PED Key.

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

5. If you say "NO" SafeNet PED needs to know if you wish to invoke MofN split-knowlege authentication for your partition, and if so, how many black PED Keys will be required to construct the partition authentication. Otherwise, proceed to the next step.

   ```
   Slot 01
   Setting user PIN...
   M value? (1-16)
   >00
   ```

   a. Select "1" if you prefer to use a single black PED Key to access the without MofN. Otherwise, enter the number of black-key holders who must always be present (with their PED Keys) to authenticate to the partition.

   b. Next SafeNet PED needs to know how big the set of "splits" should be.

   ```
   Slot 01
   Setting user PIN...
   N value? (1-16)
   >00
   ```

   c. Select "1" for the "N" number if you prefer to use a single black PED Key without MofN - no splitting of the secret takes place. Otherwise, enter the number of splits into which the secret will be broken. This number must be at least "M" and is usually larger so that some of your black key holders can be away on business,

vacation, illness, etc. while still leaving enough available to reconstruct the black-key secret when needed.

d. The PED now instructs you to insert a black PED Key for the operation of imprinting authentication secrets.

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

e. Next, you might present a factory-fresh black PED Key

```
Slot 01
Setting user PIN...
**WARNING**
This PED Key is blank
Overwrite   YES/NO
```

Or a previously-used black PED Key - which could be one that you now want to overwrite with a new authentication secret, or one that is in current use for another HSM and has been mistakenly inserted.

```
Slot 01
Setting user PIN...
**WARNING**
This PED Key is for
USER/Partition Owner.
Overwrite ?  YES/NO
```

f. Answer yes or no as follows (press the appropriate button on the PED keypad):

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 the SafeNet USB HSM during this initialization).

g. The PED wants to make very sure you are intentionally overwriting whatever was found on the currently inserted black PED Key.

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

h. Say yes.

```
Slot 01
Setting user PIN...

Enter new PED PIN
```



```
*
Confirm new PED PIN
```

i. Once the black key has been imprinted with a new partition authentication secret from the HSM (or the HSM has accepted an existing secret that was already on the black key and applied it to the new partition), the PED inquires...

```
Slot 01
Setting user PIN...
Are you duplicating
this keyset> (Y/N)
```

j. At this point you can say [No] and have only as many copies of that black key secret as already exist (just the one if this is a newly generated secret), or you can say [Yes] and be prompted to make as many copies of the current black PED Key as you wish - most organizations' security policies would demand that you have at least one backup for safekeeping.

k. If you say [Yes], the process is much more concise, as there are almost no choices to make.

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

and then ... .

```
Slot 01
Setting user PIN...
Are you duplicating
this keyset> (Y/N)
```

l. As in the other option (expandable above), if you already have enough copies of this black PED Key, say [No] and continue the partition creation sequence. Otherwise say [Yes] for as long as you wish to keep making additional copies, then say [No] when you are done with copying.

m. Log in for the next part of the process...

```
Slot 01
User login...
Insert a USER /
Partition Owner
PED Key
```

and begin the final part of this sequence, which is assigning a Cloning Domain to the newly created HSM partition (so its contents can be securely copied to another SafeNet HSM partition, perhaps for backup, or perhaps for HA, or perhaps for both uses)...

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

n. You could use an existing Cloning Domain for this partition - perhaps one that is shared by a partition on

another SafeNet USB HSM, or perhaps the one that is used by the current HSM (causing the HSM and its Partition to share the same domain). If you prefer to not share an existing Domain, then you get to sort through all the same options and prompts as for the black PED Key, above.

We will assume for this example that your new HSM partition is joining an existing Cloning domain, so the PED prompts.

```
Slot 01
Setting Domain...
Insert a Domain
PED Key
Press ENTER
```

o. The PED goes back to "Awaiting command...". and lunacm says:

```
Command Result : No Error
```

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 show
```

For an example of the output, click here.

```
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 SafeNet USB HSM, 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 SafeNet USB HSM.

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

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

Setting SafeNet USB HSM 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.

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 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
        MofN Status ->
MofN Not Generated
 *** The HSM is NOT in FIPS 140-2 approved operation mode. ***
        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
27: Enable RA-type wrapping : 0
```



```
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
27: Allow RA-type wrapping : 0
28: Allow Key Management Functions : 1
29: Perform RSA signing without confirmation : 1
30: Allow Remote Authentication : 0
Command Result : No Error
lunacm:>
lunacm:> hsm login -password mySOpa55word!
Command Result : No Error
lunacm:> partition changePolicy -policy 20 -value 9

Command Result : No Error
lunacm:>
```

Note: 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.

```
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
        MofN Status ->
MofN Not Generated
```



```
 ***
 The HSM is NOT in FIPS 140-2 approved operation mode. ***
        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
27: Enable RA-type wrapping : 0
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 : 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
27: Allow RA-type wrapping : 0
28: Allow Key Management Functions : 1
29: Perform RSA signing without confirmation : 1
30: Allow Remote Authentication : 0
Command Result : No Error
lunacm:>
```


Note: 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.

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) Configuration and Operation" on page 1 in the *Administration Guide*.

Configure SNMP

You can use the SafeNet 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*.

Appendix A - USB HSM Front-panel LEDs

In general, you should expect fault-free operation of your SafeNet USB HSM. The system is designed to run smoothly and handle gracefully a wide range of events and conditions. To display operational conditions, and also in the event that we have not anticipated everything, the SafeNet USB HSM has three LEDs on the front panel. They indicate as follows:

- ACTIVE - HSM crypto usage – this LED glows green when the HSM is performing cryptographic operations, off otherwise (similar to hard disk access LED on desktop PCs).
- TAMPER - HSM tamper – this LED glows red (latched) when a tamper condition is detected; the LED is off when the tamper condition is cleared.
- ERROR - HSM device driver error – this LED glows red (latched) for any unrecoverable device errors. The red LED is off whenever the error condition is cleared.

Tamper LED

The tamper LED glows only when actual physical tampering is detected and the SRK is invalidated.

Transport mode and battery removal - both of which also clear the SRK - do not trigger the tamper LED.

Any tamper event should be taken seriously. Your physical and operational security measures should allow you to discover the source/reason for any such event - why it happened, when it happened, and who was responsible.

Error LED

The error LED glows red when any of the following conditions has occurred, and has not been cleared:

- Error during power on/reset initialization
- Error in USB read/write
- Error processing an encrypt/decrypt command
- General internal hardware read/write errors
- General internal software errors

What To Do

Any of the above error types indicates that something serious has occurred. As soon as possible, do the following:

1. Run Lunadiag.
2. Select option 16.
3. Get the resulting trace and contact Gemalto Technical Support.

In most cases, you can clear the error by power-cycling the SafeNet USB HSM - unplug the power cord, wait 30 seconds, plug in the power cord again.

If the condition does not clear, contact Customer Support immediately.

If the condition does clear and does not return, you can resume using the SafeNet USB HSM, but we would still appreciate receiving the log of the event so that we can analyze what occurred and improve the product. None of your proprietary data of any kind is involved.

In either case, the Gemalto engineers will want to know what you were doing (or what your software was doing) around the time that the error condition occurred. If you clear the error and it recurs, we really want to know if it seems to recur during the same general circumstances - a fault that can be readily reproduced is on its way to being fixed.