Forum Systems Sentry™ HSM Quick Start Guide

Forum Systems Sentry™ HSM Quick Start Guide, published July 2020.

D-ASF-SE-417833

Table of Contents

INTRODUCTION

Audience

The *Forum Systems Sentry™ HSM Quick Start Guide* provides a step-by-step guide for System Administrators to:

- Initialize HSM on the CLI for the first time for HSM-enabled systems.
- Review concepts of a Security World within the context of the system.
- Manage Security World Keys.

Note: This entire document applies to HSM-enabled systems only.

Conventions Used

A red asterisk (*) aligned with a field term means that this field is required.

In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum XML Security Appliance™ is referred to as the 'device', 'product' or 'system'.

In this document, all commands and parameters that must be entered are displayed in italicized boldface.

Instructions for the CLI user are displayed in italicized boldface text inside brackets. Press the ***<enter>*** key or ↵ after each command.

Example:

```
login as: admin1 ↵
[Enter your User Name, then press <enter>.]
```

HSM CONCEPTS

What is a Security World

Every Hardware Security Module (HSM) operates within a context known as a "Security World." Each Security World has a unique secret key that encrypts all application keys created (or imported) by an administrator on the system. Only an HSM which has been initialized with the same Security World can understand application key-data created by another HSM system in that Security World. Therefore, in order for multiple HSM-enabled systems to share key-data, each system's HSM must be initialized in the same Security World context.

Note: When an HSM-enabled is first installed, a new Security World must be created for the HSM. What follows is a brief description of the installation procedure focusing on the HSM initialization.

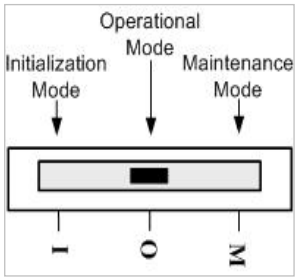
The Security World key is important in that different HSM-enabled systems can only share configurations if their HSM module is initialized with the same Security World key. For more information, refer to the GDM Full Configuration Imports and GDM Full Configuration Exports chapters of the *Forum Systems Sentry™ System Management Guide*.

Hardware Security Module (HSM)

Note: As part of the installation procedure, the HSM module must be initialized with the Security World key which will protect all of the application keys which are later generated for use within the system.

HSM Modes on the Product

The HSM operates in three modes, visible at the front of the system:



- Initialization mode is used exclusively when first initializing (or re-initializing) the HSM module for normal operation.
- Operational mode is used during normal operation.
- Maintenance mode is used exclusively for upgrading the module's firmware.

Figure 1: HSM Modes.

Note: The mode switch should always be left in this position by default. Should an operation in the CLI or WebAdmin require you to move the switch, it will prompt you to do so. If the switch is not in the "O" position when the product boots, the product will fail to initialize properly.

HSM Components
The HSM package contains the following components:

- HSM, the module itself (pre-installed hardware inside the HSM-enabled system).
- Smart Card reader.
- Administrator cards.
- Electro Magnetic Interference (EMI) filter adapter.

Hardware Schematic
The following diagram displays the Forum Systems HSM-enabled system:

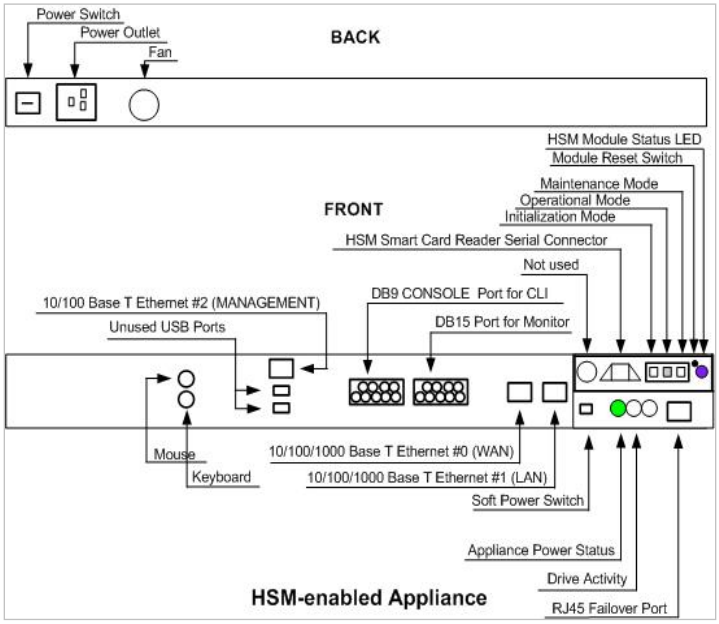


Figure 2: Product Schematic for HSM-enabled Systems.

Learn About the HSM-related Keys
HSM-enabled products use a hierarchical protection scheme for private keys stored on the product.

Application Keys
At the lowest level are the application keys. These are the keys that the user loads onto the product for such uses as encryption/decryption, signing/signature-verification, SSL initiation/SSL termination, etc. Once loaded onto the product through the standard means (i.e. through key generation, key import, or configuration import), these keys are protected by the HSM. The HSM encrypts these keys using the Security World Key and stores the encrypted values on the product's backing store. When these application keys are referenced by the system, if they are not already loaded onto the HSM, the HSM loads them, and then decrypts them (internally, on the FIPS 140-2 Level II certified module) using the security world key. The keys may then be used for cryptographic operations on the system.

Security World Key
The Security World Key is the key with which the HSM is originally initialized. It, too, has an encrypted backup version stored on the product's backing-store. When the HSM module is initialized, that encrypted version is loaded and decrypted (again, internally on the tamper proof module) so that it may be used to decrypt the application keys when they are loaded onto the module. This decrypted Security World Key will remain on the module until the next time the module is initialized. The encrypted, stored version of the Security World Key is encrypted with a key stored on an Administrator card at the time when the Security World Key is generated (usually, this is done as part of the HSM initialization process).

Administrator Cards
The keys stored on Administrator cards are encrypted using a passphrase which is set by the user when the Administrator card is first initialized. The Administrator cards are initialized as part of the process that creates a new Security World Key (a new Security World Key is usually created as part of the HSM module initialization process).

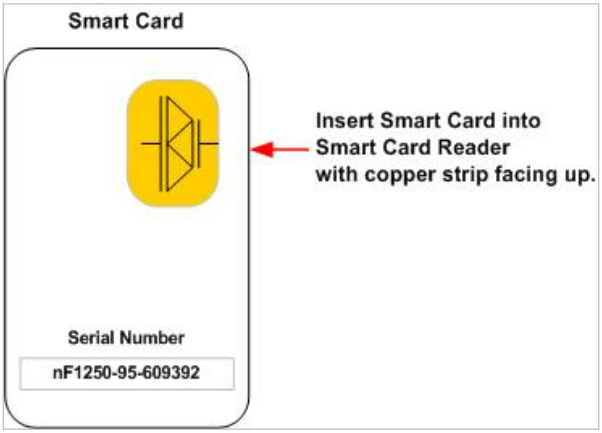


Figure 3: Example Smart Card.

If an HSM is to be initialized with an existing Security World Key (as opposed to with a newly generated Security World Key), the user must be prepared with the corresponding Administrator card and its passphrase in order to load the encrypted version of the existing Security World Key onto the module.

A summary of the types of keys follows:

TYPE OF KEY	DESCRIPTION
Application keys	These are the user's keys (including private/secret keys) used in encryption/decryption, signing/verification, and SSL policies on the product. They are stored, encrypted by the security world key, on the product's backing store and are loaded onto the module and decrypted when needed.
Security World Keys	Each HSM module is loaded with a Security World Key. The HSM uses this key to protect (encrypt) all application keys loaded onto a product. A version of this key is stored encrypted, by an Administrator card key, on the product's backing store.
Administrator card keys	Administrator card keys are generated at the same time as a new Security World Key. The Administrator card keys are used to encrypt the Security World Key stored on the product's backing store. The Administrator card keys are each encrypted with a user supplied passphrase and stored on an Administrator card.
Administrator card passphrases	HSM Administrator card passphrases must be unique, are case sensitive, and may be from 6 to 128 printable characters (i.e., #, $, %, &, etc. are valid). Spaces are allowed, but leading and trailing white space is ignored.

INITIALIZE HSM AND ADMINISTRATOR CARDS WITH A NEW SECURITY WORLD KEY

The Forum Systems Installation Wizard will prompt users to initialize the HSM and enter Administrator cards and passphrases to enable Hardware Key Management on the product with a new Security World Key. The following operation demonstrates initializing the HSM using a single Administrator card. However, users may initialize more Administrator cards if desired.

Note: Forum Systems strongly recommends initializing all Administrator cards for the devices which will be configured in the new Security World.

The Forum Systems Installation Wizard displays the following start-up screen and sequenced prompts:

```
*******************************************************
*   Welcome to the Forum Systems Installation Wizard  *
*                                                     *
* Before using the command line interface, some       *
* basic information will be needed to configure       *
* the management network interface and the hardware   *
* security module (HSM).  Type exit at                *
* the command prompt if you would like to defer       *
* this wizard until later.                            *
*                                                     *
* Once this information is collected, you will be     *
* able to use the command line interface or the       *
* the WebAdmin GUI.                                   *
*******************************************************

*******************************************************
*           HSM Settings for the System           *
*                                                     *
* This section will help you set up your Hardware     *
* Security Module.  You will need the card reader     *
* and smart cards that came with your system.      *
* NOTE: The system may take a few moments to complete *
* some of the operations necessary to initialize the  *
* HSM module.                                         *
*******************************************************

# The HSM module must be initialized with a security world key
# Would you like to initialize the module with:
  1. A newly generated security world key and Administrator
     Cards
  2. A security world key from a bootstrap file using a
     corresponding Administrator Card

> 1 ↵
[Select 1 to generate a new security world key, and then press <enter>]
```

Note: If you have previously initialized a system with an HSM, you may now take the opportunity to load another security world key from that system. To do so, export a bootstrap file from the other system (refer to the "management bootstrap export" command in the *Forum Systems Sentry™ Command Line Interface Reference*), have a corresponding Administrator Card ready, select 2 here, and follow the onscreen instructions.

```
# Please enter: number of Administrator Cards
# The number of Administrator Cards to create for this Security World.
> 1 ↵
[Enter the number of Administrator cards, and then press <enter>.]

# Please set the switch on the HSM module to "I" and press
# enter.
> ↵
[Physically switch the Mode of the HSM module to I (Initialization) at the front of the product, and
then press <enter>.]
```

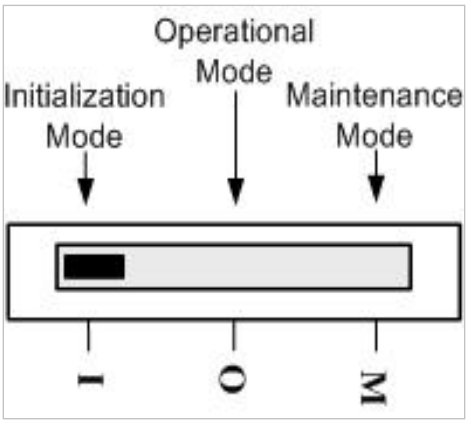


Figure 4: HSM Module Set to Initialization Mode.

```
# Please insert an Administrator Card (1/1) to be initialized
# and # press enter.
> ↵
[Insert the first Administrator Card into the Smart Card Reader, and then press <enter>.]
```

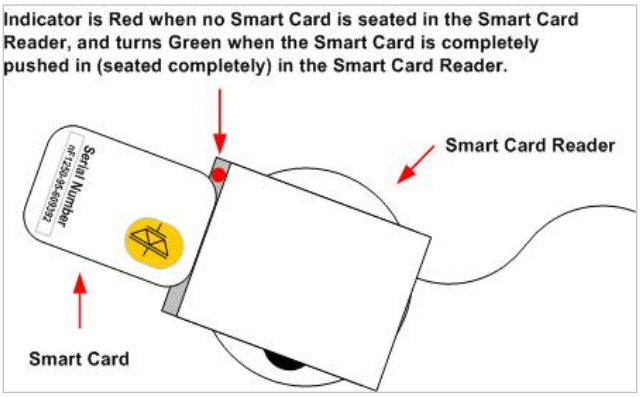


Figure 5: Smart Card Being Inserted into Smart Card Reader.

Note: Insert Administrator cards as far as possible into the smart card reader with the copper strip facing up (toward the ceiling). The LED status is now green, indicating that the smart card is properly seated in the smart card reader.

```
# Please enter: a passphrase
# A new passphrase for the current Administrator Card
# (The passphrase length should be between 6 and 128 characters.
# Leading and trailing whitespace will be ignored.)
> ******** ↵
[Enter Passphrase, and then press <enter>.]
```

Note: HSM Administrator card passphrases must be unique, are case sensitive, and may be from 6 to 128 printable characters (i.e., #, $, %, &, etc. are valid). Spaces are allowed, but leading and trailing white space is ignored.

```
# Please enter: a passphrase
# Please confirm the passphrase for the current Administrator
# Card.
> ******** ↵
[Re-enter Passphrase, and then press <enter>.]

# To complete HSM initialization, please set the switch on the # HSM module to "O" and press enter.
> ↵
[Physically switch the Mode of the HSM module to O (Operational) at the front of the product, and
then press <enter>.]
```

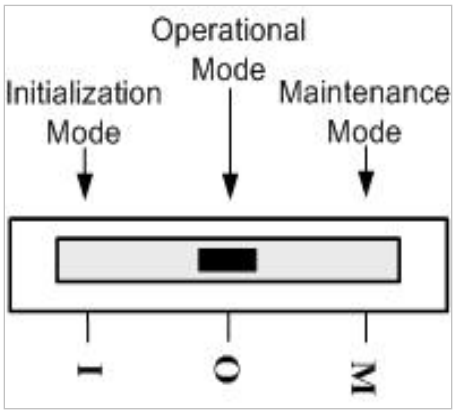


Figure 6: HSM Module Set to Operational Mode.

The HSM is now initialized. Return to the *Forum Systems Sentry™ Hardware Installation Guide* and continue with the Configure Network Interfaces for the Product chapter to continue with installation.

Caution: The HSM module should always be in the "O" mode except when initializing the module. After initialization of Administrator cards, you must switch the HSM module back in the "O" mode.

Note: The device does not reboot immediately after the HSM initialization portion of the installation procedure is complete. However, expect the device to reboot after completion of the install-wizard on a run which included initializing the HSM.

APPENDIX

Appendix A – Specifications of the CLI

ELEMENT	SPECIFICATIONS	CHAR COUNT
HSM Administrator Card Passpshrase	Unique & case sensitive. Accepts all printable characters (i.e. #, $, %, &, etc. are valid). Spaces are allowed, but leading and trailing white space is ignored.	6-128

INDEX