Secure Web Gateway
Version 11.7
Hardware Security Module
Setup and Integration Guide

Legal Notice

The most current version of this document may be obtained by contacting:

Trustwave Technical Support:
Phone: +1.800.363.1621
Email: **support@trustwave.com**

Trademarks

Revision History

Version	Date	Changes
1.0	April 2015	First release

Formatting Conventions

This manual uses the following formatting conventions to denote specific information.

Formats and Symbols	Meaning
Blue Underline	A blue underline indicates a Web site or email address.
Bold	Bold text denotes UI control and names such as commands, menu items, tab and field names, button and check box names, window and dialog box names, and areas of windows or dialog boxes.
`Code`	Text in `Courier New 9 pt in blue` indicates computer code or information at a command line.
Italics	Italics denotes the name of a published work, the current document, name of another document, text emphasis, to introduce a new term, and path names.
[Square brackets]	Square brackets indicate a placeholder for values and expressions.

Notes, Tips, and Cautions

	Note: This symbol indicates information that applies to the task at hand.
	Tip: This symbol denotes a suggestion for a better or more productive way to use the product.
	Caution: This symbol highlights a warning against using the software in an unintended manner.
	Question: This symbol indicates a question that the reader should consider.

Table of Contents

1 Overview

Trustwave SWG enables you to comply with Federal Information Processing Standards for cryptography modules (FIPS 140-2) for HTTPS services by integrating a certified Hardware Security Module (HSM) device into the security system topology.

An HSM is a physical device in the form of a plug-in card or external device attached directly to a computer or network server. The device safeguards and manages digital keys for strong authentication in compliance with the hardware and software protection requirements defined by FIPS 140-2. It provides cryptographic processing and is responsible for secure key generation, storage and use, while offloading application servers for complete symmetric and asymmetric cryptography.

Asymmetric cryptography, or public-key cryptography, is a class of cryptographic algorithms that require two separate keys, one secret (private) and one public. Although different, the two parts of this key pair are mathematically linked.

- The **private key** is used to decrypt cipher text or create a digital signature.
- The **public key** is used to encrypt plain text or verify a digital signature. Ownership of a public key is proved using an electronic document called a Digital Certificate.

The HSM device also enables performance improvements by offloading cryptographic operations, and accelerating SSL handshakes.

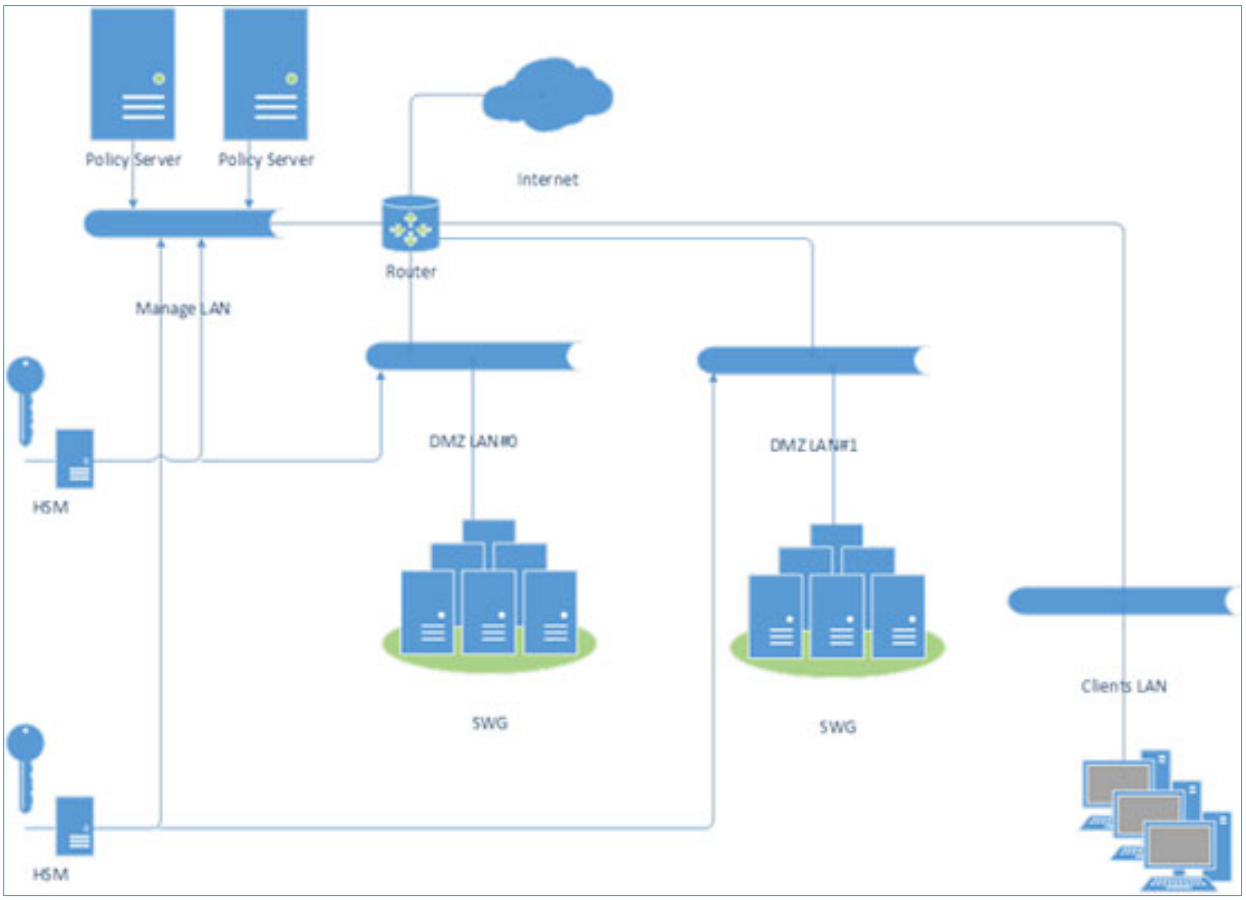
SWG uses a dedicated THALES netHSM device that isolates cryptographic processes and keys from applications and host operating systems, and is accessible only through tightly controlled cryptographic APIs.

Thales HSMs use a paradigm called **Security World** to provide a secure environment for all hardware security devices and key management operations. The Security World is scalable; you can add multiple hardware security devices to a server and share the Security World across multiple servers.

The Remote File System (**RFS)** contains master configuration information for the HSM, the Security World files, and key data. It can be configured on any computer available via the network.

Important Note: For more detailed information on configuring or managing a Thales netHSM hardware security device or an associated Security World, see the *nShield Connect and netHSM User Guide*. This document is provided on DVD with the device.

The supported HSM topology is illustrated as follows:



2 Setting up an HSM Device

Setting up an HSM Device comprises several steps:

- Setting up the Primary Network Interface, page 8
- (If required) Setting up a Secondary Network Interface, page 8
- Configuring the HSM Device in Trustwave SWG, page 8
- Setting up a Scanning Server HTTPS Service to use HSM, page 9
- Initializing the Thales License and Enabling Features, page 10

2.1 Setting up the Primary Network Interface

After the hardware is installed and connected, you can set up the primary interface as described in this section.

To set up the primary (default) Ethernet interface:

1. From the device front panel menu, select **System | System configuration | Network config | Set up interface #1**. The following screen is displayed:

   Network configuration

   Enter IP address for

   interface #1:

   0. 0. 0. 0

   Enter netmask:

   0. 0. 0. 0

   CANCEL NEXT

2. Enter the IP address and net mask for interface #1. Then press the **NEXT** navigation button on the right.

   The following screen is displayed:

   Network configuration

   Select desired link

   speed:

   auto / 1Gb

   BACK NEXT

3. Ensure **auto / 1Gb** is selected and press the **NEXT** navigation button on the right.
4. To accept the new interface, press the navigation button on the right when prompted.
5. To select a later reboot, press the left navigation button when prompted. Then press the navigation button on the right to continue the configuration.

Note: If you later change any of the IP addresses on the unit, you must update the configuration of all the clients that work with it to reflect the new IP addresses.

2.2 (If required) Setting up a Secondary Network Interface

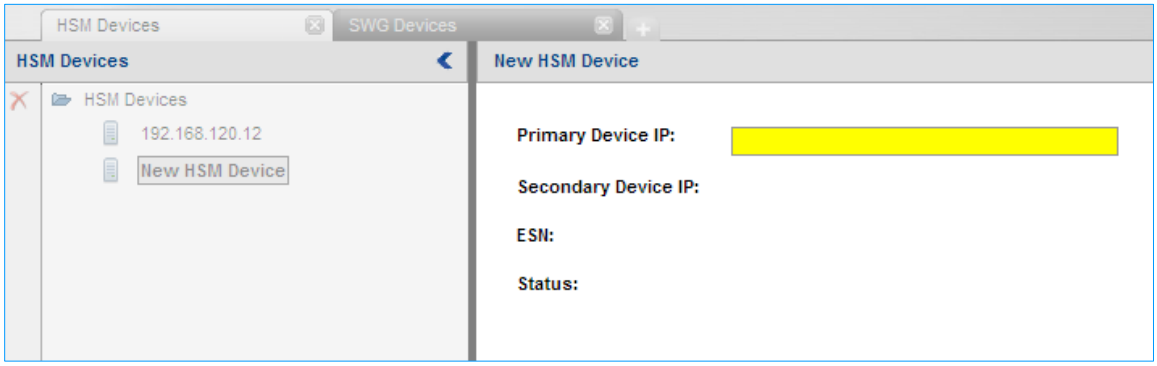
A second network interface (interface **#2**) can be set up in the same way as described in section 2.1.

2.3 Configuring the HSM Device in Trustwave SWG

To configure an HSM Device in Trustwave SWG:

1. In the SWG console, select **Administration | System Settings | HSM Devices**.
2. In the HSM Devices tree, right-click the **HSM Devices** root and choose **Add Device**. The New HSM Device screen is displayed in the main window.

3. Specify the **Primary Device IP**. This must be in the same subnet as the Policy server.

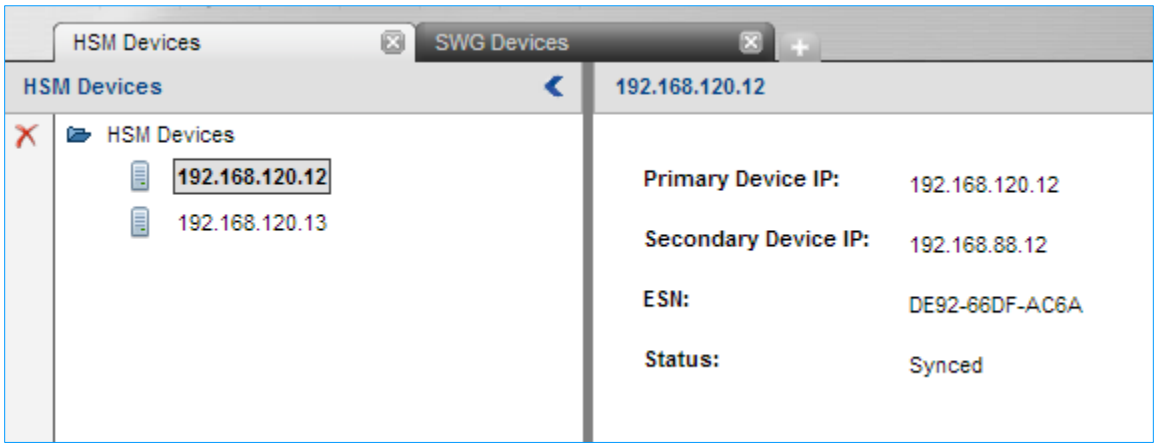


The following properties are also displayed:

- Secondary Device IP (If defined)
- **ESN** (Electronic Serial Number)
- **Status** (See the HSM Status Table on page 16)

4. Connect to the RFS, as described in **Configuring the Remote File System** on page **Error! Bookmark not defined.**.
5. Create the Security World, as described in **Creating a Security World** on page 11.

The status of HSM device should now be synced:



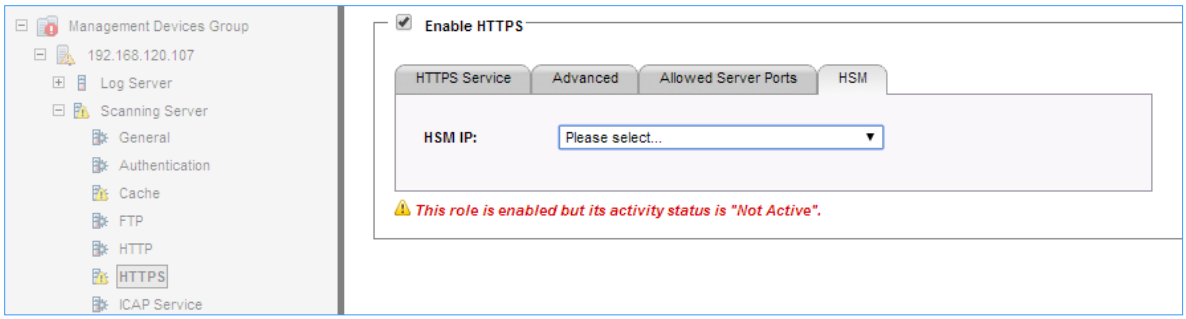
2.4 Setting up a Scanning Server HTTPS Service to use HSM

2.4.1 Prerequisites

- Initialize the Thales license using the "Features Enabled" card supplied with the device. See **Initializing the Thales License and Enabling Features** on page 10.
- The number of scanning services allowed to use the HSM appliance must be according to the Thales client license limit.
- The primary or secondary HSM IP must be in the same subnet as one of the scanning server network IPs.

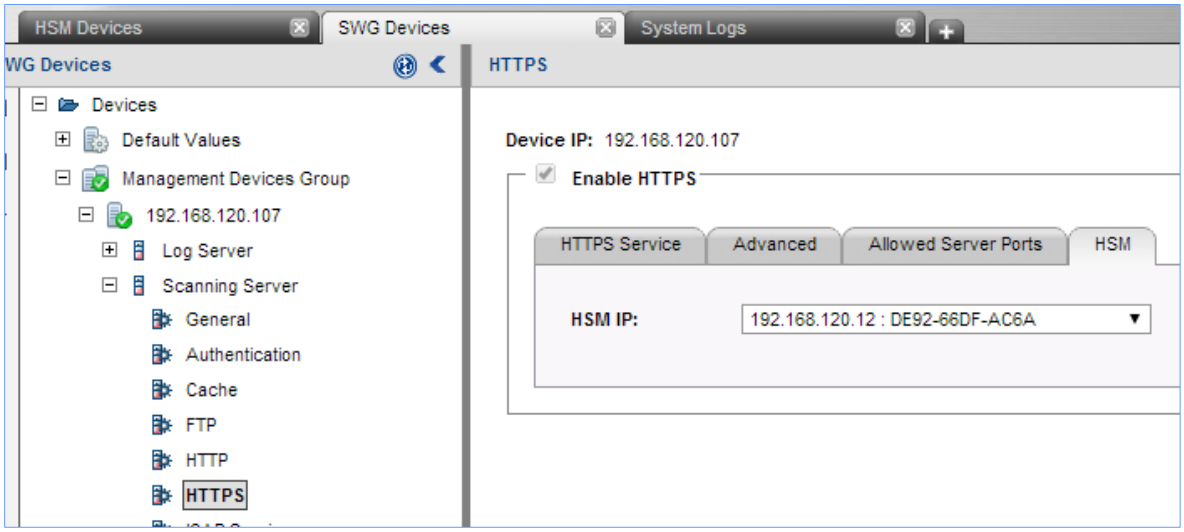
To set up a Scanning Server HTTPS Service to use HSM:

1. In the SWG console, select **Administration | System Settings | SWG Devices**.
2. In the Devices tree, select ***<device_group>*** **|** ***<device_ip>*** **| Scanning Server | HTTPS**.
3. In the main window, click **Edit**.



4. In the HSM tab, select the available **HSM IP** and click **Save**.

Important Note: SWG will produce a new certificate in the background.



5. Click the **Commit** button on the toolbar.

2.5 Initializing the Thales License and Enabling Features

You initialize the Thales License and enable new features using the Feature-Enabling smart card from Thales e-Security.

To initialize the Thales license and enable features:

1. Insert the Feature-Enabling smart card into the unit slot.
2. From the front panel, select **HSM | HSM feature enable | Read FEM from card**.

   A message is displayed if the features are enabled successfully.

3 Configuring the Remote File System (RFS)

The Remote File System contains the master copy of the unit Security World data for backup purposes. The RFS will be located on the Policy server where the Security World Software is installed.

The unit must be able to connect to TCP port 9004 of the RFS on the Policy Server. If necessary, modify the firewall configuration to allow this connection on either the RFS itself or on a router between the RFS and the unit.

To configure the RFS:

1. On the unit display screen, use the right-hand navigation button to select **System | System configuration | Remote file system**, and enter the IP address of the Policy Server.

   You must allow a configuration to be pushed automatically from the RFS to the unit. The **auto push** feature allows future unit configuration to be performed remotely (that is, without access to the front panel of the unit).
2. To enable auto push, use the right-hand navigation button to select **System | System configuration | Config file options | Allow auto push** and select **ON**.

4 Creating a Security World

You create a Security World with a single unit. If you have more than one module, select one module to create the Security World, and then add additional modules to the Security World after its creation.

Security World information is stored on the unit operating system's file system and the RFS computer's hard disk. The information is encrypted using the keys stored on the ACS.

Note that the process of creating a Security World:

- Erases the module
- Creates a new module key for this Security World
- Creates a new ACS (Administrator Card Set) to protect this module key

Notes:

- For Security World options, see **Appendix A: Security World Options**.
- For more detailed information on configuring or managing an associated Security World, see the *nShield Connect and netHSM User Guide*.

4.1 Prerequisites

Before configuring the Security World:

- You must know the security policy for the module and the number and quorum of Administrator Cards and Operator Cards to be used.
- You must have enough smart cards to form the Security World card sets.

4.2 Creating a Security World from the Unit Front Panel

To create a Security World from the unit front panel:

1. From the main menu, select **Security World mgmt | Module initialization | New Security World**.
2. Enter the default quorum for the ACS. This comprises:
   - The maximum number of cards from the ACS required by default for an operation. This number must be less than or equal to the total number of cards in the set.
   - The total number of cards to be used in the ACS. This must be a value in the range 1 – 64.
3. Respond to the question **Specify all quorums?**
   - Select **no** if you want to enable all operations and use the maximum number specified for all features
   - Select **yes** if you want to disable individual features or require a lower number of cards for an operation
4. Select the Cipher Suite for the Security World; that is, whether the Security World key is to be an AES key (original) or AES key (SP800-131 compliant).
5. Specify whether the Security World will conform to FIPS 140-2 requirements for roles and services at level 3. If not specified, the Security World complies with FIPS 140-2 requirements for level 2.
6. If you choose to disable individual features or require a lower number of cards required for an operation, specify these parameters now.

   You can select a different number of Administrator Cards (K) to be required for each operation. You can also disable recovery and replacement operations and choose to use K_{NSO} to authorize SEE (Secure Execution Engine) operations.
7. Specify whether the module is a valid target for remote shares (that is, whether it can import slots).
8. Format a card for the ACS as follows:
   a. Insert a card for the ACS and confirm that you want to use it.
   b. If the card is not blank, choose whether to overwrite it or to use a different card.
   c. Choose whether to specify a pass phrase for the card. If you choose to specify a pass phrase:
      i. Enter the pass phrase.
      ii. Enter the pass phrase again to confirm it.
      iii. If the two pass phrases do not match, you must enter the correct pass phrase twice.
   d. When prompted, remove the card.
9. Repeat the previous step to format additional cards for the ACS, setting their pass phrases as described until the ACS is complete.

   Each prompt screen shows how many cards are required and how many have been used.
10. On completion, a message confirms that the Security World has been created.

4.3 Displaying Information about your Security World

To display information about the status of your Security World:

1. Select **Security World mgmt | Display World info** from the main menu.
2. Run the `nfkminfo` command-line utility.

4.4 Adding an HSM to a Security World

After creating a Security World, you can add additional modules to it. You can restore modules that were previously removed from the same Security World in the same way.

You can also restore a module to a Security World to continue using existing keys and Operator Cards:

- After you upgrade the firmware
- If you replace the module

Note: The additional modules can be any nShield modules.

To add a module to a Security World, you must:

- Have installed the additional module hardware.
- Have a copy of the Security World data on the module's RFS in the Key Management Data directory.
- Possess a sufficient number of cards from the ACS and the appropriate pass phrases.

Adding or restoring a module to a Security World:

- Erases the Security World data on the module's internal file system.
- Reads the required number of cards (K) from the ACS so that it can recreate the key.
- Reads the Security World data from the RFS.
- Uses the key from the ACS to decrypt the Security World key.
- Stores the Security World key in the module's nonvolatile memory.

After adding a module to a Security World, you cannot access any keys that were protected by a previous Security World that contained that module.

Note: A module cannot use two separate Security Worlds simultaneously.

To add a module to a Security World:

1. If the module already belongs to a Security World, erase it from that Security World.
2. From the main menu, select **Security World mgmt | Module initialization | Load Security World**.
3. Specify whether the module can use the Remote Operator feature import slots.
4. At the prompt, insert an Administrator Card, and enter its pass phrase if required.
5. Continue to insert Administrator Cards when prompted until you have inserted the number required to authorize module reprogramming.

4.5 Erasing a Module from a Security World

Erasing a module from a Security World deletes from the module all the secret information that is used to protect your Security World. This returns the module to the factory state. Provided that you still have the ACS and the host data, you can restore the keys by adding the module to the Security World.

Erasing a module removes any data stored in its nonvolatile memory (for example, data for an SEE program or NVRAM-stored keys). To preserve this data, you must back it up before erasing the module. The nvram-backup utility is provided to enable data stored in nonvolatile memory to be backed up and restored.

Note: You do not need the ACS to erase a module. However, unless you have a valid ACS and the host data for this Security World, you cannot restore the Security World after you have erased it.

After you have erased a module, it is in the same state as when it left Thales e-Security (that is, it has a random module key and a known K_{NSO}).

To erase a module:

1. From the main menu, select **Security World mgmt | Module initialization | Erase Security World**.

   When you erase a Security World in this way, the Security World files remain on the RFS.
2. Delete these files if you wish to remove Security World completely.

   You should remove the files manually from the **/opt/nfast/kmdata/local** directory on the RFS and any client computers to which the Security World was copied.

5 Testing the Installation

To test the installation and configuration:

1. Log in on the client computer as a regular user, and open a command window.
2. Run the command: `opt/nfast/bin/enquiry`

   A successful `enquiry` command returns output in the following format:

```
server:
  enquiry reply flags none
  enquiry reply level Six
  serial number ####-####-####-####
  mode operational
  version #.#.#
  speed index ###
  rec. queue ##..##
  ...
  version serial #
  remote server port ####
```

```
Module #1:
  enquiry reply flags none
  enquiry reply level Six
  serial number ####-####-####-####
  mode operational
  version #.#.#
  speed index ###
  rec. queue ##..##
  ...
  Rec. LongJobs queue ##
  SEE machine type PowerPCSXF
```

If the mode is **operational**, the unit is installed correctly.

3. If the `enquiry` command returns that the unit is not found:
    a. Restart the client computer.
    b. Re-run the `enquiry` command.

6 Resetting the HSM Unit

6.1 Resetting to the Default Configuration

To reset the unit to its default configuration, select **System | System configuration | Default config** and confirm that you want to set the default configuration.

This removes the configuration of the module but does not change its $\mathbf{K_{NETI}}$.

6.2 Resetting to the Factory State

To reset the unit to its original (factory) state, select **Factory state** from the main menu and confirm that you want to return the unit to its factory state.

This gives a new $\mathbf{K_{NETI}}$ to the unit, which means that you must update the keyhash field of the unit's entry in the **nethsm_imports** section of the configuration file of all the clients that use it.

7 HSM Troubleshooting

This section includes descriptions for messages displayed on the SWG console.

Note: Backup and restore of HSM configuration is implemented as part of the policy server DB backup feature available in the SWG console (**Administration | Policy Server DB backup**).

7.1 HSM Add Failure

Error	Description
Device with IP: xxx.xxx.xxx.xxx already exists	Cannot add device – An HSM with the entered IP already exists.
The HSM Primary IP should be on the same network as the Policy Server	This requirement prevents degradation of performance.
Port CLOSED	The device is disconnected or an invalid HSM.
Error from AnonymousKnetiHash? command: InappropriateObject?	The device is not a valid HSM device.
Cannot add HSM	The device is not a valid HSM device. No ESN received.
Cannot make RFS Server	Failed to perform initial setup.

7.2 HSM Remove Failure

Error	Description
Cannot find HSM to remove	Policy Server local HSM files cannot be found. Restore from backup.
Cannot remove hsm-ESN	Failed to delete HSM data. Restore from backup.

7.3 HSM Status Table

Error	Description
Synced	The configuration is OK and the device is operational.
Unknown	The Policy Server is not the RFS server for this HSM. Check the HSM configuration via its console.
Unconfigured	No configuration received from the HSM. Check remote push settings.
No module found	No key file for the module found. Restore from backup or create a new Security World.
No Security World	No Security World found. Restore from backup or create a new one.
Configuration fail	The HSM is not configured for remote management, or failed to push configuration.

8 Appendix A: Security World Options

You must decide what kind of Security World you need before you create it. Depending on the kind of Security World you need, you can choose different options at the time of creation. For convenience, Security World options can be divided into the following groups:

- Security World Basic Options, which must be configured for all Security Worlds
- **OCS and Softcard Replacement**, which must be configured if the Security World, keys, or pass phrases are to be recoverable or replaceable
- **Security World SEE options**, which only need be configured if you are using the nCipher Secure Execution Engine (SEE)
- **Security World Replacement Options**, relating to the replacement of an existing Security World with a new Security World.

Security World options are highly configurable at the time of creation but, so that they remain secure, they are not configurable afterwards. For this reason we recommend that you familiarize yourself with Security World options, especially those required by your particular situation, before you begin to create a Security World.

8.1 Security World Basic Options

When you create a Security World, you must always configure the basic options described in this section.

8.1.1 Cipher Suite

You must decide whether to use a cipher suite that uses Triple DES, AES (standard), or AES (SP800-131 compliant) Security World keys. The Security World keys are generated during Security World creation and protect the application keys and OCSs.

Notes:

- Due to the additional primality checking required by SP800-131, Security World generation and key generation operations will take longer in SP800-131 compliant Security Worlds.
- To create a Triple DES Security World, you must use the `new-world` command-line utility.

8.1.2 K and N Values

You must decide the total number of cards (N) in a Security World's ACS and must have that many blank cards available before you start to create the Security World. You must also decide how many cards from the ACS must be present (K) when performing administrative functions on the Security World.

Note: We recommend that you do not create ACSs for which *K* is equal to *N*, because you cannot replace such an ACS if even 1 card is lost or damaged.

In many cases, it is desirable to make K greater than half the value of N (for example, if N is 7, to make K 4 or more). Such a policy makes it harder for a potential attacker to obtain enough cards to access the Security World. Choose values of K and N that are appropriate to your situation. The total number of cards used in the ACS must be in the range 1 to 64.

8.1.3 FIPS 140-2 Level 3 Compliance

By default, Security Worlds are created to comply with the roles and services, key management, and self-test sections of the FIPS 140-2 standard at level 2. However, you can choose to enable compliance with the FIPS 140-2 standard at level 3.

Note: This option provides compliance with the roles and services of the FIPS 140-2 level 3 standard. It is included for those customers who have a regulatory requirement for compliance.

If you enable compliance with FIPS 140-2 level 3 roles and services, authorization is required for the following actions:

- Generating a new OCS
- Generating or importing a key, including session keys
- Erasing or formatting smart cards (although you can obtain authorization from a card you are about to erase).

In addition, you cannot import or export private or symmetric keys in plain text.

8.1.4 UseStrongPrimes Security World Setting

When creating a Security World, the default setting for UseStrongPrimes depends on the FIPS level:

- *FIPS 140-2 level 3:* **UseStrongPrimes** is **on**, meaning that the Security World always generates RSA keys in a manner compliant with FIPS 186-3.
- *FIPS 140-2 level 2:* **UseStrongPrimes** is **off**, meaning that the Security World leaves the choice of RSA key generation algorithm to individual clients.

Enabling UseStrongPrimes increases the RSA key generation time by approximately 10 times. If you want to use a different UseStrongPrimes setting from its default setting, you must use the `new-world` command-line utility to create the Security World.

The `nfkminfo` utility shows the status of the Security World. Running the `enquiry` utility for a module shows the status of the world in relation to that module.

8.1.5 Remote Operator

To use a module without needing physical access to present Operator Cards, you must enable the Remote Operator feature on the module. For more information, see the *nShield Connect and netHSM User Guide*.

By default, modules are initialized into Security Worlds with remote card set reading enabled. If you add a module for which remote card reading is disabled to a Security World for which remote card reading is enabled, the module remains disabled.

8.2 OCS and Softcard Replacement Options

By default, Security Worlds are created with the ability to replace one OCS or softcard with another.

This feature enables you to transfer keys from the protection of the old OCS or softcard to a new OCS or softcard.

Note: You can replace an OCS with another OCS, or a softcard with another softcard, but you cannot replace an OCS with a softcard or a softcard with an OCS. Similarly, you can transfer keys from an OCS to another OCS, or from a softcard to another softcard, but you cannot transfer keys from an OCS to a softcard or from a softcard to an OCS.

You can choose to disable OCS and softcard replacement for a Security World when you create it.

However, in a Security World without this feature, you can never replace lost or damaged OCSs; therefore, you could never recover the keys protected by lost or damaged OCSs, even if the keys themselves were generated as recoverable (which is the default for key generation).

OCS and softcard replacement cannot be enabled after Security World creation without reinitializing the Security World and discarding all the existing keys within it.

For an overview of Security World robustness and OCS or softcard replacement, or for details about performing OCS and softcard replacement operations, see the *nShield Connect and netHSM User Guide*.

8.2.1 Pass Phrase Replacement

By default, Security Worlds are created so that you cannot replace the pass phrase of a card or softcard without knowing the existing pass phrase.

However, you can choose to enable pass phrase replacement at the time you create a Security World.

This option makes it possible to replace the pass phrase of a card or softcard even if you do not know the existing pass phrase. Performing such an operation requires authorization from the Security World's ACS.

For details about performing pass phrase replacement operations, see the *nShield Connect and netHSM User Guide*.

8.2.2 Nonvolatile Memory (NVRAM) Options

Enabling nonvolatile memory (NVRAM) options allows keys to be stored in the module's NVRAM instead of in the Key Management Data directory of the host computer. Files stored in the module's non-volatile memory have Access Control Lists (ACLs) that control who can access the file and what changes can be made to the file. NVRAM options are relevant only if your module's firmware supports them, and you can store keys in your module's NVRAM only if there is sufficient space.

Note: When the amount of information to be stored in the NVRAM exceeds the available capacity, you can instead store this data in a blob encrypted with a much smaller key that is itself then stored in the NVRAM. This functionality allows the amount of secure storage to be limited only by the capacity of the host computer.

8.3 Security World SEE Options

You must configure SEE options if you are using the nCipher Secure Execution Engine (SEE). If you do not have SEE installed, the SEE options are irrelevant.

8.3.1 SEE Debugging

SEE debugging is disabled by default, but you can choose whether to enable it for all users or whether to make it available only through use of an ACS. In many circumstances, it is useful to enable SEE debugging for all users in a development Security World but to disable SEE debugging in a production Security World. Choose the SEE debugging options that best suit your situation.

8.3.2 Real-time Clock (RTC) Options

Real-time clock (RTC) options are relevant only if you have purchased and installed the CodeSafe Developer kit. If so, by default, Security Worlds are created with access to RTC operations enabled.

However, you can choose to control access to RTC operations by means of an ACS.

8.4 Security World Replacement Options

Options relating to Security World replacement are relevant only if you are replacing a Security World.

If you replace an existing Security World, the **/opt/nfast/kmdata/local** directory is not overwritten but renamed **/opt/nfast/kmdata/local_N** (where N is an integer assigned depending on how many Security Worlds have been previously saved during overwrites). A new Key Management Data directory is created for the new Security World. If you do not wish to retain the **/opt/nfast/kmdata/local_N** directory from the old Security World, you must delete it manually.

About Trustwave

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide.

For more information, visit https://www.trustwave.com.