F5 BIG-IP

nShield® HSM Integration Guide

11 Apr 2023

Contents

1. Introduction

The nShield Hardware Security Module (HSM) can generate and store a Root of Trust that protects security objects used by F5 Big-IP LTM to safeguard users' keys and credentials. The HSM in FIPS 140-2 Level 2 or Level 3 mode meets compliance requirements.

More than one HSM can enroll to a F5 BIG-IP machine if all HSMs are in the same Security World.

1.1. Product configurations

Entrust has successfully tested nShield HSM integration with F5 BIG-IP in the following configurations:

Software	Version
Operating System	CentOS 7.3
BIG-IP	16.0.1, 17.0.0.1

1.2. Supported nShield hardware and software versions

Entrust has successfully tested with the following nShield hardware and software versions:

1.2.1. Connect XC

Security World Software	Firmware	Image	OCS	Softcard	Module
12.60.11	12.50.11 (FIPS Certified)	12.60.10	✓	✓	✓
12.80.4	12.50.11 (FIPS Certified)	12.80.4	✓	✓	✓
12.80.4	12.72.1 (FIPS Certified)	12.80.5	✓	✓	✓

1.2.2. Connect +

Security World Software	Firmware	Image	OCS	Softcard	Module
12.60.11	12.50.8 (FIPS Certified)	12.60.10	✓	✓	✓
12.80.4	12.50.8 (FIPS Certified)	12.80.4	✓	✓	✓
12.80.4	12.72.0 (FIPS Certified)	12.80.5	✓	✓	✓

1.2.3. nShield 5c

Security World Software	Firmware	Image	OCS	Softcard	Module
13.2.2	13.2.2 (FIPS Pending)	13.2.2	✓	✓	✓

Hotfix TAC_955 is required for the nShield 5 configuration. An unrestricted world may be used without the need for a hotfix.

1.3. Supported nShield HSM functionality

Feature	Support
Module-Only key	Yes
OCS cards	Yes
Softcards	Yes
nSaaS	Yes
FIPS 140-2 Level 3	Yes

1.4. Requirements

Before installing these products, read the associated documentation:

- For the nShield HSM: *Installation Guide* and *User Guide*.
- If nShield Remote Administration is to be used: *nShield Remote Administration User Guide*.

- F5 BIG-IP documentation (https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-system-and-ncipher-hsm-implementation.html).

In addition, the integration between nShield HSMs and F5 BIG-IP requires:

- PKCS #11 support in the HSM.
- A correct quorum for the Administrator Card Set (ACS).
- Operator Card Set (OCS), Softcard, or Module-Only protection.
    - If OCS protection is to be used, a 1-of-N quorum must be used.
- Firewall configuration with usable ports:
    - 9004 for the HSM (hardserver).

Furthermore, the following design decisions have an impact on how the HSM is installed and configured:

- Whether your Security World must comply with FIPS 140-2 Level 3 standards.
    - If using FIPS Restricted mode, it is advisable to create an OCS for FIPS authorization. The OCS can also provide key protection for the Vault master key. For information about limitations on FIPS authorization, see the *Installation Guide* of the nShield HSM.
- Whether to instantiate the Security World as recoverable or not.

1.5. More information

For more information about OS support, contact your F5 sales representative or Entrust nShield Support, https://nshieldsupport.entrust.com.

2. Procedures

2.1. Prerequisites

1. A Big-IP system must be deployed before following the steps in this guide.

Big-IP Virtual Edition was used for this guide, but the procedures in this guide can be applied to other deployments.

2. The BIG-IP system must be licensed for *External Interface and Network HSM*.
3. Access is required to the command-line interface of the Big-IP machine and the Configuration utility web interface.
4. A Security World ISO file is required for installing the nShield Security World software.

2.2. Install the Security World software

The following steps will be a manual installation of Security World on the BIG-IP machine. Automatic installation steps exist for older versions of Security World software. See the F5 documentation for more information.

1. Mount the Security World ISO file:

```
% cd /shared
% mkdir SecWorld-12.60.11
% mount -o loop SecWorld_Lin64-12.60.11.iso SecWorld-12.60.11
```

2. Untar the Security World files:

```
% cd /shared
% sudo tar -zxvf /shared/SecWorld-12.60.11/linux/amd64/ctd.tar.gz
```

3. Repeat for all `tar.gz` files in the `amd64` directory.
4. Fix installation directory paths:

```
% mv /shared/opt/nfast/ /shared
% rmdir /shared/opt
```

5. Create a link from `/opt/nfast` to `/shared/nfast`:

```
% cd /opt
% ln -s /shared/nfast
% ls -al
```

6. Run the installation:

```
% /opt/nfast/sbin/install
```

7. Run the `enquiry` utility to see if the hardserver is up and running:

```
% /opt/nfast/bin/enquiry
```

2.3. Configure the Security World

To configure the Security World:

1. Enroll the HSM onto the Big-IP machine. The machine must be a client of the HSM. For more information, see the *User Guide* for the HSM.

```
% /opt/nfast/bin/nethsmenroll <HSM_IP_Address>
% /opt/nfast/bin/enquiry
```

2. Create or import the Security World. For more information, see the *User Guide* for the HSM.
3. Edit `cknfastrc` in `/opt/nfast` and update it to contain one of the following configurations:
   a. For Module-Only protection:

```
CKNFAST_FAKE_ACCELERATOR_LOGIN=1
```

   b. For OCS or Softcard protection:

```
CKNFAST_LOADSHARING=1
CKNFAST_NO_ACCELERATOR_SLOTS=1
```

4. Add * to the end of the `/shared/opt/nfast/kmdata/config/cardlist` file.

2.4. Configure HSM connectivity to Big-IP

To configure HSM connectivity to Big-IP:

1. Use the following command to check the name of the partition to be used. For OCS or Softcard protection, this is typically the name of the card set.

```
% /opt/nfast/bin/cklist
```

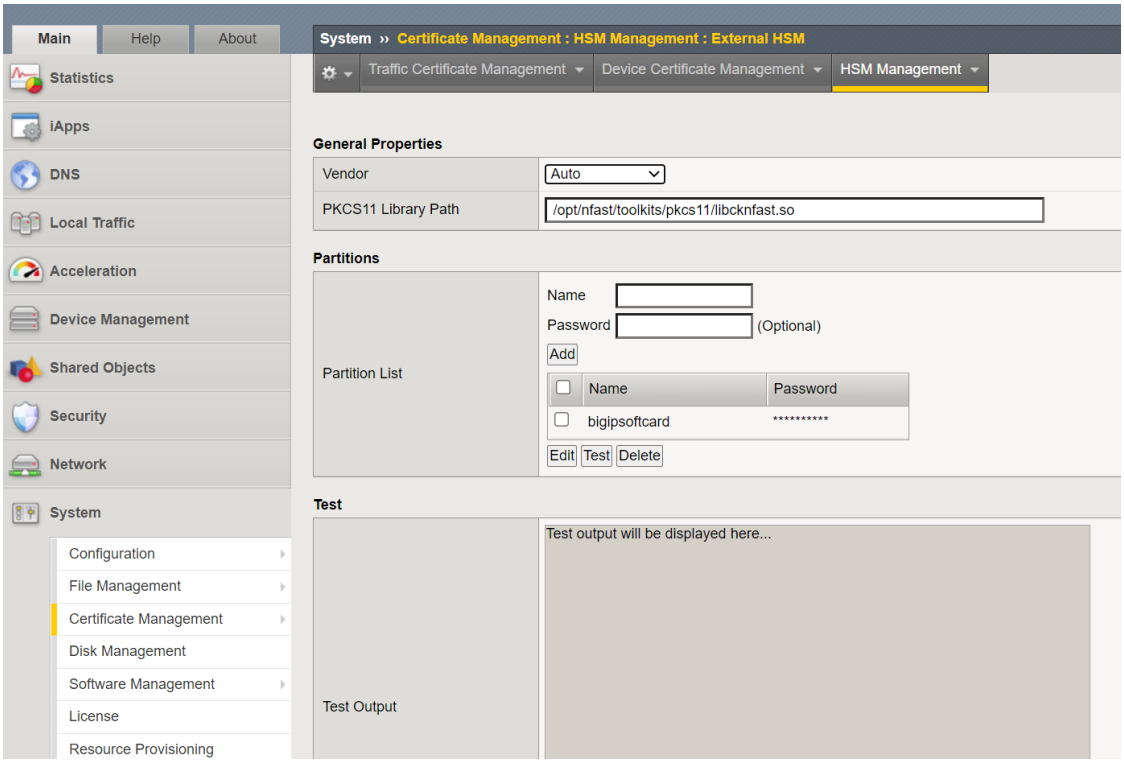
2. Take note of the partition name. This integration uses Module-Only protection, so the partition name was `accelerator`.
3. Log in to the Configuration utility using an account with the administrator role.
4. Add the following information under **System > Certificate Management > HSM Management > External HSM**.

    a. For **Vendor**, select **Auto**.

    b. For **PKCS11 Library Path**, enter **/opt/nfast/toolkits/pkcs11/libcknfast.so**.

    c. For **Partition**, enter the partition name.

    d. For **Password**, enter the card set passphrase.



5. Select **Add** to add the partition.
6. Select **Update**.
7. Restart the `pkcs11d` service to apply the new settings to the system:

```
% tmsh restart sys service pkcs11d
% tmsh restart sys service tmm
```

8. Confirm that `pkcs11d` is running:

```
% bigstart status pkcs11d
```

2.5. Manage HSM keys for LTM

Use the following procedures to manage HSM keys:

- Generate an HSM key.
- Generate a self-signed digital certificate.
- Request a certificate from a Certificate Authority.
- Delete a key from the BIG-IP system.
- Import a pre-existing NetHSM key to the BIG-IP system.

2.5.1. Generate an HSM key

The Traffic Management Shell `tmsh` can be used to generate a key or certificate on the HSM.

1. Generate the key:

```
% tmsh create sys crypto key <key_name> gen-certificate common-name <cert_name> security-type nethsm
```

2. Verify that the key was created:

```
% tmsh list sys crypto key test_key
```

2.5.2. Generate a self-signed digital certificate

To generate a self-signed digital certificate:

1. Log in to the Configuration utility using an account with the administrator role.
2. On the main page, select **System > Certificate Management > Traffic Certificate Management**.

   The **Traffic Certificate Management** page appears.
3. Select **Create**.
4. For **Name**, enter a unique name for the SSL certificate.
5. For **Issuer**, select **Self**.
6. For **Common Name**, enter a name. This is typically the name of a web site, such as www.siterequest.com.
7. Enter the other certificate details.
8. For **Security Type**, select **NetHSM**.
9. For **NetHSM Partition**, select a partition to use.

10. For **Key Type**, RSA is selected as the default key type.
11. For **Size**, select a size, in bits.
12. Select **Finished**.

2.5.3. Request a certificate from a Certificate Authority

To request a certificate from a Certificate Authority, you must generate a certificate signing request (CSR) and then submit the CSR to a third-party trusted certificate authority (CA):

1. Log in to the Configuration utility using an account with the administrator role.
2. On the main page, select **System > Certificate Management > Traffic Certificate Management**.

   The **Traffic Certificate Management** page appears.
3. Select **Create**.
4. For **Name**, enter a unique name for the SSL certificate.
5. For **Issuer** list, select **Certificate Authority**.
6. Enter the other certificate details.
7. Select **Finished**.
8. The **Certificate Signing Request** page appears.
9. Do one of the following to download the request into a file on your system.
   a. For **Request Text**, copy the certificate.
   b. For **Request File**, select the **Download** button.
10. Submit the request to a certificate authority to be signed.
11. Select **Finished**.

    An option appears to import the signed certificate.
12. Import the certificate.

2.5.4. Delete a key from the BIG-IP system

To delete a key from the BIG-IP system:

1. Log in to the Configuration utility using an account with the administrator role.
2. On the main page, select **System > Certificate Management > Traffic Certificate Management**.

   The **Traffic Certificate Management** page appears.

3. For **SSL Certificate List**, select the key to delete.
4. Select **Delete**.

   The key you selected is deleted from BIG-IP.

   The key stored in NetHSM is not deleted. To do this, find the key file in `/opt/nfast/kmdata/local` and delete it.

2.5.5. Import a pre-existing NetHSM key to the BIG-IP system

To import a pre-existing NetHSM key to the BIG-IP system:

1. Log in to the command-line interface of the system using an account with administrator privileges.
2. Import the NetHSM key:

```
% tmsh install sys crypto key <nethsm_key_label> from-nethsm security-type nethsm
```

This step can be completed on the Configuration utility. See the F5 documentation for more information.