F5 BIG-IP

nShield® HSM Integration Guide

2026-07-24

Table of Contents

Chapter 1. Introduction

The nShield Hardware Security Module (HSM) generates and stores a Root of Trust that protects the security objects used by F5 BIG-IP LTM to safeguard user keys and credentials. When operated in FIPS 140-2 Level 2 or Level 3 mode, the HSM meets compliance requirements.

More than one HSM can be enrolled on an F5 BIG-IP machine, provided all HSMs belong to the same Security World.

1.1. Product configurations

Entrust has successfully tested nShield HSM integration with F5 BIG-IP in the following configurations. Before using the latest versions tested by Entrust, confirm compatibility with the interoperability matrix.

Software	Version
BIG-IP - Virtual Edition	21.1.0-0.0.38

1.2. Supported nShield hardware and software versions

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

HSM	Security World Software	Firmware	Image	OCS	Softcard	Module	FIPS Level 3
nShield Connect	13.6.8	12.72.4 (FIPS 140-2 certified)	13.6.16	✓	✓	✓	✓
nShield 5c	13.6.8	13.4.5 (FIPS 140-3 certified)	13.6.16	✓	✓	✓	✓

Security World v13.6.8 is the last release that supports CentOS 7, the operating system used by the F5 BIG-IP software listed above. Because CentOS 7 has reached end of life (EOL), newer versions of Security World software cannot be used with F5 BIG-IP until F5 updates the underlying operating system shipped with its software.

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 *

* F5 BIG-IP SSL profiles that require TLS 1.2 are only supported with Entrust nShield firmware v12.50.11. Contact F5 or Entrust for details on TLS 1.3 support.

1.4. Requirements

The BIG-IP system must be licensed for *External Interface and Network HSM*.

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 used, a 1-of-N quorum must be used.
- Firewall configuration with usable ports:
  - 9004 for the HSM (hardserver).

The following design decisions also affect how the HSM is installed and configured:

- Whether your Security World must comply with FIPS 140-2 Level 3 standards.

- If using FIPS 140-2 Level 3, Entrust recommends creating 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* for the nShield HSM.

- Whether to instantiate the Security World as recoverable.

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

1.5. More information

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

Access to the Entrust nShield Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

Chapter 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 can be applied to other deployments.

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

2.2. Install the Security World software

The following steps describe 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
% mount -o loop SecWorld_Lin64-13.6.8.iso SecWorld
```

2. Untar the Security World files:

```
% cd /shared
% sudo tar -zxvf /shared/SecWorld/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 symbolic link from `/shared/nfast` to `/opt/nfast`:

```
% ln -s /shared/nfast /opt/nfast
```

6. Run the installation:

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

7. Run the `enquiry` utility to verify that 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 -p <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_OVERRIDE_SECURITY_ASSURANCES=wrapping_crypt
CKNFAST_FAKE_ACCELERATOR_LOGIN=1
```

   b. For OCS or Softcard protection:

```
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=wrapping_crypt
CKNFAST_LOADSHARING=1
CKNFAST_NO_ACCELERATOR_SLOTS=1
```

4. Restart the `pkcs11d` service to apply the new settings to the system:

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

Whenever you change the `cknfastrc` file, you must restart the `pkcs11d` service for the changes to take effect.

5. Append * to the `/shared/opt/nfast/kmdata/config/cardlist` file.

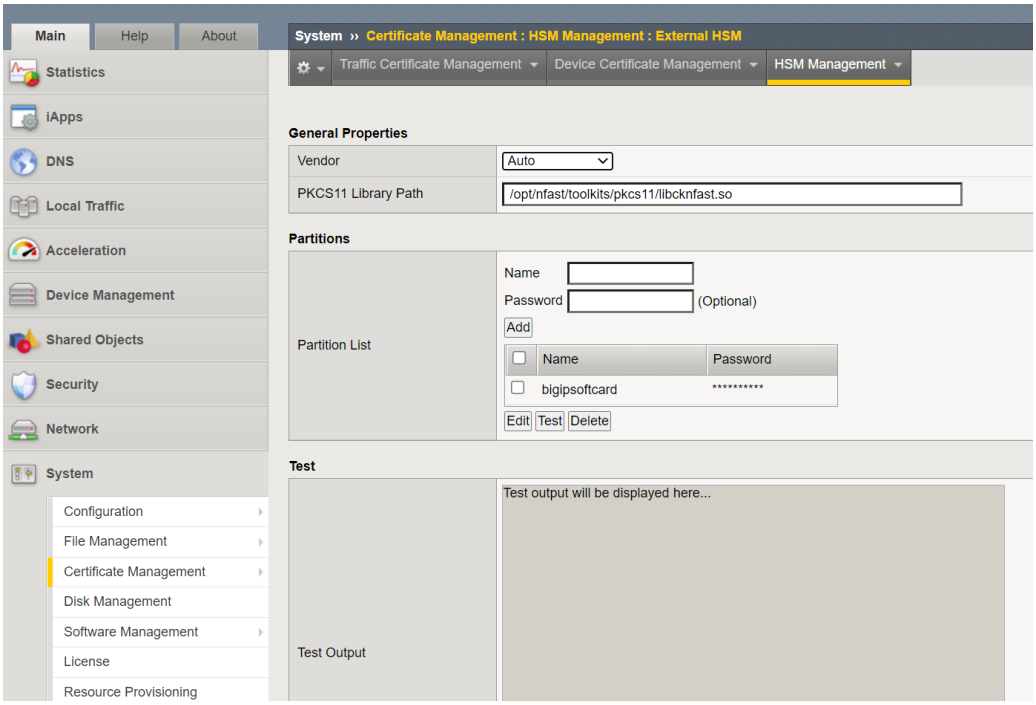
2.4. Configure HSM connectivity to BIG-IP

To configure HSM connectivity to BIG-IP:

1. Use the following F5 commands to verify the setup and to check the name of the partition to be used. For OCS or Softcard protection, this is typically the name of the card set.

```
% pkcs11d_test_suite
% pkcs11d_test_one
```

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:

```
% bigstart restart pkcs11d
```

8. Confirm that pkcs11d is running:

```
% bigstart status pkcs11d
```

2.5. Manage HSM keys for LTM

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. Under **General Properties:**
   a. For **Name**, enter a unique name for the SSL certificate.
5. Under **Certificate Properties:**
   a. For **Issuer**, select **Self**.
   b. For **Common Name**, enter a name. This is typically the name of a website, such as

`www.siterequest.com`.

c. Enter the other certificate details.

6. Under **Key Properties:**
   a. For **Security Type**, select **NetHSM**.
   b. For **NetHSM Partition**, select a partition to use.
   c. For **Key Type**, leave **RSA** selected as the default.
   d. For **Size**, select a size in bits.
7. Under **Certificate Order Properties:**
   a. For **Provider**, select the certificate provider.
   b. For **Certificate Manager Order**, select the **Manager**.
8. 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. Under **General Properties:**
   a. For **Name**, enter a unique name for the SSL certificate.
5. Under **Certificate Properties:**
   a. For **Issuer**, select **Certificate Authority**.
   b. Enter the other certificate details as appropriate.
6. Under **Certificate Signing Request Attributes:**
   a. For **Administrator E-mail Address**, enter the administrator's email address.
   b. For **Challenge Password**, type a password.
   c. Confirm the password.
7. Under **Key Properties:**
   a. For **Security Type**, select **NetHSM**.
   b. For **NetHSM Partition**, select a partition to use.

c. For **Key Type**, leave **RSA** selected as the default.
d. For **Size**, select a size in bits.

8. Under **Certificate Order Properties:**
   a. For **Provider**, select the certificate provider.
   b. For **Certificate Manager Order**, select the **Manager**.
9. Select **Finished**.

   The **Certificate Signing Request** page appears.

10. Do one of the following to download the request as a file on your system:
    a. For **Request Text**, copy the certificate.
    b. For **Request File**, select **Download**.
11. Submit the request to a certificate authority to be signed.
12. Select **Finished**.

    An option appears to import the signed certificate.

13. 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 delete it, find the key file in `/opt/nfast/kmdata/local` and remove 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 also be performed in the Configuration utility. See the F5 documentation for more information.

2.5.6. Configure BIG-IP High Availability (HA) Failover

SSL traffic failover can work with HSM keys and certificates.

1. Attach the HSM key and certificate to a client SSL profile.
2. Assign the profile to a virtual server so that the virtual server can process SSL traffic according to the specified profile settings.
3. Verify that the virtual server passes traffic correctly.
4. Perform a manual failover of the HA pair.

   The virtual server should still pass traffic correctly.

   When a new HSM key for F5 BIG-IP HA is created or imported on an HA machine, you must copy the `key_pkcs11` file from `/opt/nfast/kmdata/local` to the other machine in the HA setup. Entrust recommends using the `rfs-sync` feature for this. Other file transfer methods can also be used. Without this step, SSL traffic that uses this key fails when BIG-IP fails over to the peer machine that does not have the key file.

   For instructions on setting up two F5 BIG-IP machines in an HA pair, see https://techdocs.f5.com/en-us/bigip-14-0-0/big-ip-service-provider-sip-administration-14-0-0/high-availability-ha-failover.html.

   For instructions on manual failover, see https://my.f5.com/manage/s/article/K42061352.

Chapter 3. Additional resources and related products

3.1. nShield HSMs

3.2. nShield as a Service

3.3. Entrust products

3.4. nShield product documentation