F5 BIG-IP

nShield® HSM Integration Guide
## Contents

1. **Introduction** ........................................... 4  
   1.1. Product configurations ........................................ 4  
   1.2. Supported nShield hardware and software versions ................. 4  
   1.3. Supported nShield HSM functionality .............................. 5  
   1.4. Requirements .......................................... 5  
   1.5. More information ...................................... 6  

2. **Procedures** ............................................ 7  
   2.1. Prerequisites ........................................ 7  
   2.2. Install the Security World software .......................... 7  
   2.3. Configure the Security World .............................. 8  
   2.4. Configure HSM connectivity to Big-IP ........................ 8  
   2.5. Manage HSM keys for LTM ................................ 9  

**Contact Us** ............................................. 12
1. Introduction

The nShield Hardware Security Module (HSM) can generate and store a Root of Trust (RoT) 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

We have successfully tested nShield HSM integration with F5 BIG-IP in the following configurations:

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>CentOS 7.3</td>
</tr>
<tr>
<td>BIG-IP</td>
<td>16.0.1</td>
</tr>
</tbody>
</table>

1.2. Supported nShield hardware and software versions

We have successfully tested with the following nShield hardware and software versions:

1.2.1. Connect XC

<table>
<thead>
<tr>
<th>Security World Software</th>
<th>Firmware</th>
<th>Image</th>
<th>OCS</th>
<th>Softcard</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.60.11</td>
<td>12.50.11</td>
<td>12.60.10</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

1.2.2. Connect +

<table>
<thead>
<tr>
<th>Security World Software</th>
<th>Firmware</th>
<th>Image</th>
<th>OCS</th>
<th>Softcard</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.60.11</td>
<td>12.50.8</td>
<td>12.60.10</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
1.3. Supported nShield HSM functionality

<table>
<thead>
<tr>
<th>Feature</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module-only key</td>
<td>Yes</td>
</tr>
<tr>
<td>OCS cards</td>
<td>Yes</td>
</tr>
<tr>
<td>Softcards</td>
<td>Yes</td>
</tr>
<tr>
<td>nSaaS</td>
<td>Yes</td>
</tr>
<tr>
<td>FIPS 140-2 level 3</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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*.

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](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 tested 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 is required to the command line interface of the Big-IP machine and the Configuration utility web interface.


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.


   ```
   % 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
   Repeat for all tar.gz files in the amd64 directory.
   ```

3. Fix installation directory paths.

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

4. Create a link from /opt/nfast to /shared/nfast.

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

5. Run the installation.
6. Run the `enquiry` utility to see if the hardserver is up and running.

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

### 2.3. Configure the Security World

1. Enroll the HSM onto the Big-IP machine. The machine has to 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 protection:
     ```
     CKNFAST_FAKE_ACCELERATOR_LOGIN=1
     ```
   - b. For OCS or Softcard protection:
     ```
     CKNFAST_LOADSHARING=1
     CKNFAST_NO_ACCELERATOR_SLOTS=1
     ```

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

### 2.4. 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 cardset.

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

2. Take note of the partition name. This integration uses module 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**.
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

#### 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

1. Log in to the Configuration utility using an account with the administrator role.
3. Select Create.
4. In the Name field, enter a unique name for the SSL certificate.
5. From the Issuer list, select Self.
6. In the Common Name field, enter a name. This is typically the name of a web site, such as www.siterequest.com.
7. Enter the other certificate details.
8. From the Security Type list, select NetHSM.
9. From the NetHSM Partition list, select a partition to use.
10. From the Key Type list, RSA is selected as the default key type.
11. From the Size list, select a size, in bits.
12. Select Finished.

2.5.3. Request a certificate from a Certificate Authority

Generate a certificate signing request (CSR) that can then be submitted to a third-party trusted certificate authority (CA).

1. Log in to the Configuration utility using an account with the administrator role.
3. Select Create.
4. In the Name field, enter a unique name for the SSL certificate.
5. From the Issuer list, select Certificate Authority.
6. Enter the other certificate details.
7. Select Finished.
8. The **Certificate Signing Request** screen displays.

9. Do one of the following to download the request into a file on your system.
   a. In the **Request Text** field, 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**.

12. An option will be displayed to import the signed certificate.

### 2.5.4. Delete a key from the BIG-IP system


2. The **Traffic Certificate Management** screen opens.

3. From the **SSL Certificate List**, select the key to delete.

4. Select **Delete**.

5. The key you selected is deleted from BIG-IP.

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

### 2.5.5. 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.

   ```bash
   % 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.
# Contact Us

<table>
<thead>
<tr>
<th><strong>Web site</strong></th>
<th><a href="https://www.entrust.com">https://www.entrust.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Support</strong></td>
<td><a href="https://nshieldsupport.entrust.com">https://nshieldsupport.entrust.com</a></td>
</tr>
<tr>
<td><strong>Email Support</strong></td>
<td><a href="mailto:nShield.support@entrust.com">nShield.support@entrust.com</a></td>
</tr>
<tr>
<td><strong>Online documentation:</strong></td>
<td>Available from the Support site listed above.</td>
</tr>
</tbody>
</table>

You can also contact our Support teams by telephone, using the following numbers:

### Europe, Middle East, and Africa

**United Kingdom:**
+44 1223 622444  
One Station Square  
Cambridge, UK CB1 2GA

### Americas

**Toll Free:**
+1 833 425 1990

**Fort Lauderdale:**
+1 954 953 5229  
Sawgrass Commerce Center – A  
Suite 130  
13800 NW 14 Street  
Sunrise, FL 33323 USA

### Asia Pacific

**Australia:**
+61 8 9126 9070  
World Trade Centre Northbank Wharf  
Siddeley St  
Melbourne VIC 3005 Australia

**Japan:**
+81 50 3196 4994

**Hong Kong:**
+852 3008 3188  
31/F, Hysan Place,  
500 Hennessy Road,  
Causeway Bay
ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they’re crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it’s no wonder the world’s most entrusted organizations trust us.

To get help with Entrust nShield HSMs
nShield.support@entrust.com
nshieldsupport.entrust.com