F5® Platforms: FIPS Administration

Version 13.0.0

Table of Contents

FIPS Platform Setup

About setting up FIPS platforms in a device group

You can configure a device group using two platforms from the same series with a FIPS card installed in each unit. When setting up a FIPS solution on a device group, you install the two systems and can connect to a serial console to remotely manage the systems. In the event that network access is impaired or not yet configured, the serial console might be the only way to access your system.

After you have set up and configured the systems, you can create the FIPS security domain by initializing the HSM and creating a security officer (SO) password. You must configure the same security domain name on all HSMs in the group.

Initializing the HSM in 5000/7000/10200 platforms

You must initialize the hardware security module (HSM) installed in each unit before you can use it. When you are creating a device group using more than one FIPS platform, you initialize the HSM on one unit, and then initialize the HSM on a peer unit using the same security domain label that you used on the first unit.

***Note:** You can initialize the HSM and create the security domain before you license the system and create a traffic management configuration.*

1. Log in to the command line of the system using an account with root access.
2. Open the Traffic Management Shell (`tmsh`).

   ```
   tmsh
   ```

3. Initialize the HSM and set a security officer (SO) password.

   ```
   run util fips-util -f init
   ```

   ***Important:** Running the `fipsutil init` command deletes all keys in the HSM and makes any previously exported keys unusable.*

   ***Note:** The initialization process takes a few minutes to complete.*

   The initialization process begins. When prompted, type an SO password.

   ***Note:** F5 recommends that you choose a strong value for the SO password. You cannot use the keyword `default` as the SO password.*

```
WARNING: This erases all keys from the FIPS 140 device.
Any configuration objects dependent on FIPS keys will cause
the configuration fail to load.

==================== WARNING ================================
The FIPS device will be reset to factory default state.
All keys and user identities currently stored in the device
will be erased.
Any configuration objects dependent on FIPS keys will cause
the configuration fail to load.

Press <ENTER> to continue or Ctrl-C to cancel
```

```
Resetting the device ...

The FIPS device is now in factory default state.
Enter new Security Officer password (min. 7, max. 14 characters):
Re-enter Security Officer password:
```

4. When this message displays, type a security domain label.

```
NOTE: security domain label must be identical on peer
FIPS devices in order to be able to synchronize with them.
Enter security domain label (max. 50 chars, default: F5FIPS):
```

   Be sure to keep the security domain label and password in a secure location. You need the domain label and password when you initialize the HSM on a peer unit. You can use the same password or choose a new one. This information is also required when replacing a unit (for RMA or other reasons). Since keys are synchronized from the working unit to a new unit, the domain label and password are required.

```
Initializing new security domain (F5FIPS)...
Creating crypto user and crypto officer identities
Waiting for the device to re-initialize ...
Creating key encryption key (KEK)
The FIPS device has been initialized.
```

5. Enable the HSM device using one of these options:
   - Reboot the unit.
   - Restart all services: `restart sys service all`.

   Note: Restarting services disrupts load-balanced traffic and might terminate remote login sessions to the system.

After you complete the initialization process on the first unit, you can initialize a peer system and add it to the security domain of the first unit. You must use the same SO password that you used on the first unit.

Initializing the HSM in 10350 platforms

You must initialize the hardware security module (HSM) installed in each unit before you can use it. When you are creating a device group using more than one FIPS platform, you initialize the HSM on one unit, and then initialize the HSM on a peer unit using the same security domain label that you used on the first unit. You can choose to use a different password on the peer unit.

***Note:** You can initialize the HSM and create the security domain, before you license the system and create a traffic management configuration.*

1. Log in to the command line of the system using an account with root access.
2. Open the Traffic Management Shell (`tmsh`).
   `tmsh`
3. Initialize the HSM and set a security officer (SO) password.
   `run util fips-util init`

   ***Important:** Running the `fipsutil init` command deletes all keys in the HSM and makes any previously exported keys unusable.*

***Note:** The initialization process takes a few minutes to complete.*

The initialization process begins. When prompted, type an SO password. You cannot use the keyword `default` as the SO password.

***Note:** F5® recommends that you choose a strong value for the SO password.*

```
WARNING: This erases all keys from the FIPS 140 device.
Any configuration objects dependent on FIPS keys will cause
the configuration fail to load.

==================== WARNING ================================
The FIPS device will be reset to factory default state.
All keys and user identities currently stored in the device
will be erased.
Any configuration objects dependent on FIPS keys will cause
the configuration fail to load.

Press <ENTER> to continue or Ctrl-C to cancel

Resetting the device ...

The FIPS device is now in factory default state.
Enter new Security Officer password (min. 7, max. 14 characters):
Re-enter Security Officer password:
```

4. When this message displays, type a security domain label.

```
NOTE: security domain label must be identical on peer
FIPS devices in order to be able to synchronize with them.
Enter security domain label (max. 50 chars, default: F5FIPS):
```

Be sure to keep the security domain label and password in a secure location. You need the domain label and password when you initialize the HSM on a peer unit. You can use the same password or choose a new one. This information is also required when replacing a unit (for RMA or other reasons). Since keys are synchronized from the working unit to a new unit, the domain label and password are required.

```
Initializing new security domain (F5FIPS)...
Creating crypto user and crypto officer identities
Waiting for the device to re-initialize ...
Creating key encryption key (KEK)
The FIPS device has been initialized.
```

5. Enable the HSM device using one of these options:
   - Reboot the unit.
   - Restart all services: `restart sys service all`.

   ***Note:** Restarting services disrupts load-balanced traffic and might terminate remote login sessions to the system.*

After you complete the initialization process on the first unit, you can initialize a peer system and add it to the security domain of the first unit. You can choose to use the same SO password that you used on the first unit.

Viewing HSM information using tmsh

You can use the Traffic Management Shell (`tmsh`) to view information about the hardware security module (HSM).

1. Log in to the command line of the system using an account with root access.
2. Open the Traffic Management Shell (`tmsh`).

   ```
   tmsh
   ```
3. View information about the HSM.

   ```
   run util fips-util info
   ```

   Depending on the HSM installed in your system, a summary similar to this example (from a 10350 platform) displays.

```
Label:              F5FIPS
Model:              NITROX-III CNN35XX-NFBE

Serial Number:      3.0G1501-ICM000059
FIPS state:         2

MaxSessionCount:    2048
SessionCount:       13

MaxPinLen:          14
MinPinLen:          7
TotalPublicMemory:  557540
FreePublicMemory:   234552
TotalUserKeys:      10075
AvailableUserKeys:  10075

Loging failures:
    user:    0
    officer: 0

Temperature:        72 C
HW version:         0.0
Firmware version:   CNN35XX-NFBE-FW-1.0-27
```

Before you synchronize the HSMs

Before you can synchronize the FIPS hardware security modules (HSMs), you must ensure that the target HSM:

- Is already initialized
- Has an identical security domain name
- Does not contain existing keys
- Is the same hardware model
- Contains the same firmware version

Before you run the `fips-card-sync` command, ensure that you have this information:

- The SO password for the source F5® device
- The SO password for the target F5 device
- The root password for the target F5 device

The target device must also be reachable using SSH from the source device.

Synchronizing the HSMs using tmsh

Be sure that you meet all prerequisites before synchronizing the hardware security modules (HSMs) in your devices.

Synchronizing the HSMs enables you to copy keys from one HSM to another. This is also required to synchronize the software configuration in a device group.

Note: *You only need to perform the synchronization process during the initial configuration of a pair of devices. After the two devices are in sync, they remain in sync.*

---

1. Log on to the command line of the source F5® device using an account with root access.
2. Open the Traffic Management Shell (`tmsh`).

   ```
   tmsh
   ```
3. Synchronize the Master Symmetric key from the HSM on the source F5 device to the HSM on the target F5 device, where <*`hostname`*> is the IP address or hostname of the target F5 device.

   ```
   run util fips-card-sync <hostname>
   ```

   Note: *Be sure to run this command on a device that contains a valid Master Symmetric key. Otherwise, you might invalidate all keys loaded in the HSM.*

   Note: *A Master Symmetric key is shared between the HSMs on each F5 device. This shared master key is used to encrypt the SSL private keys when the keys leave the cryptographic boundary of the HSM.*

   ---

   a) When prompted, type the security officer (SO) password for the local device.

   b) When prompted, type the SO password for the remote device or press Enter if the password is the same as for the local device.
   A message similar to this example displays:

```
Connecting to 172.27.76.255 as user root ...
```

   c) When prompted, type the root password.
   When the synchronization operation completes, a message similar to this example displays:

```
FIPS devices have been synchronized.
```

4. Confirm that all devices have the Master Symmetric key.

   ```
   tmsh show sys crypto master-key
   ```

   A summary similar to this example displays:

```
-------------------------------------------
Sys::Master-Key
-------------------------------------------
master-key hash  <hJqPIjC72OJOP90CfD9WHw==>
previous hash    <>
```

5. Synchronize the software configuration in the device group.

   Important: *You must run `fips-card-sync` before running `config-sync`. Otherwise, the FIPS keys will not load on the remote device.*

   ```
   run cm config-sync [ to-group | from-group ] <device_group_name>
   ```

Key Management

About managing FIPS keys using the BIG-IP Configuration utility

You can use the BIG-IP® Configuration utility to create FIPS keys, import existing FIPS keys into a hardware security module (HSM), and convert existing keys into FIPS keys.

Existing FIPS keys (.exp files) can only be imported into an HSM that possesses the same Master Symmetric key used when the FIPS keys were exported. The Symmetric Master Key is used to encrypt SSL private keys as they are exported from an HSM. Therefore, only the same Master Symmetric key can be used to decrypt the SSL private keys as they are imported into the HSM.

Note: *Import of FIPS keys is supported if the F5® system uses the same Master Symmetric key that was used to export the FIPS keys.*

Creating FIPS keys using the BIG-IP Configuration utility

You can use the BIG-IP® Configuration utility to create FIPS keys.

1. On the Main tab, click **System** > **File Management** > **SSL Certificate List**.
   This displays the list of certificates installed on the system.
2. Click **Create**.
   The New SSL Certificate screen opens.
3. In the **Name** field, type a unique name for the certificate.
4. From the **Issuer** list, specify the type of certificate that you want to use.
   - To request a certificate from a CA, select **Certificate Authority**.
   - For a self-signed certificate, select **Self**.
5. Configure the **Common Name** setting and any other settings as needed.
6. In the Key Properties area, select a key size from the **Size** list.
7. From the **Security Type** list, select **FIPS**.
8. Click **Finished**.

Importing keys using the BIG-IP Configuration utility

You can use the BIG-IP® Configuration utility to import existing keys into the system.

1. On the Main tab, click **System** > **File Management** > **SSL Certificate List**.
   This displays the list of certificates installed on the system.
2. Click **Import**.
3. From the **Import Type** list, select **Key**.
4. For the **Key Name** setting, click **Create New**.
5. In the **Key Name** field, type a name for the key.
6. From the **Key Source** setting, click either **Upload File** or **Paste Text**.
   - If you click **Upload File**, type a file name or click **Browse** and select a file.
   - If you click **Paste Text**, copy the text from another source and paste the text into the Key Source screen.
7. Click **Import**.

After you import the key, you can convert it to a FIPS key.

Converting a key to FIPS using the BIG-IP Configuration utility

You can use the BIG-IP® Configuration utility to convert an existing key to a FIPS key.

1. On the Main tab, click **System** > **File Management** > **SSL Certificate List**.
   This displays the list of certificates installed on the system.
2. Click a certificate name.
   This displays the properties of that certificate.
3. On the menu bar, click **Key**.
   This displays the type and size of the key associated with the certificate.
4. Click **Convert to FIPS** to convert the key to a FIPS key.
   The key is converted and appears in the list as a FIPS key. After the key is converted, this process cannot be reversed.

About managing FIPS keys using tmsh

You can use the Traffic Management Shell (`tmsh`) to create FIPS keys, import existing keys into an F5® system, and convert existing keys to FIPS keys.

Creating FIPS keys using tmsh

You can use the Traffic Management Shell (`tmsh`) to create FIPS keys.

1. Log in to the command line of the system using an account with root access.
2. Open the Traffic Management Shell (`tmsh`).
   ```
   tmsh
   ```
3. Create a basic key.
   ```
   create sys crypto key <key_object_name> security-type fips
   ```
   For information about additional options for this command, view the `sys crypto key` man page:
   ```
   help sys crypto key
   ```

   Note: *The key creation process takes a few minutes to complete.*

   ---
4. (Optional) View information about the generated key.
   ```
   list sys crypto key <key_object_name>
   ```

Importing FIPS keys using tmsh

You can use the Traffic Management Shell (`tmsh`) to import existing keys into the system.

1. Log in to the command line of the system using an account with root access.
2. Open the Traffic Management Shell (`tmsh`).
   ```
   tmsh
   ```
3. Import a key.
   ```
   install sys crypto key <key_object_name> from-local-file <path_to_key_file>
   security-type fips
   ```
   This example imports a FIPS key named `mykey` from a local key file stored in the `/shared/tmp` directory: `install sys crypto key mykey from-local-file /shared/tmp/mykey.exp security-type fips`

Converting a key to FIPS using tmsh

You can use the Traffic Management Shell (`tmsh`) to convert a key to a FIPS key.

1. Log in to the command line of the system using an account with root access.
2. Open the Traffic Management Shell (`tmsh`).
   ```
   tmsh
   ```
3. Convert an existing key to FIPS.
   ```
   install sys crypto key <key_object_name> from-local-file <key_file_path>
   security-type fips
   ```

Listing FIPS keys in the HSM using tmsh

You can use the Traffic Management Shell (`tmsh`) to list the FIPS keys in the hardware security module (HSM).

1. Log in to the command line of the system using an account with root access.
2. Open the Traffic Management Shell (`tmsh`).
   ```
   tmsh
   ```
3. List the keys in the HSM.
   ```
   tmsh show sys crypto fips key
   ```
   A summary similar to this example displays:

```
-------------------------------------------
FIPS 140 Hardware Device
-------------------------------------------
=== private keys (2)
ID                                      MOD.LEN(bits)
dd83774207ea554ba1192439de75e1c1        2048
        /Common/testkey1.key
d750c989e6afeb5ac8ca8aec2b93461b        1024
        /Common/testkey2.key
```

Listing FIPS keys in the F5 software configuration using tmsh

You can use the Traffic Management Shell (`tmsh`) to list the FIPS keys in the F5® software configuration.

1. Log in to the command line of the system using an account with root access.
2. Open the Traffic Management Shell (`tmsh`).
   ```
   tmsh
   ```
3. List the keys in the hardware security module (HSM).
   ```
   tmsh list sys crypto key
   ```
   A summary similar to this example displays:

```
sys crypto key default.key {
    key-size 1024
    key-type rsa-private
    security-type normal
}
sys crypto key testkey2.key {
    key-id d750c989e6afeb5ac8ca8aec2b93461b
    key-size 1024
    key-type rsa-private
    security-type fips
}
sys crypto key testkey1.key {
```

```
    key-id dd83774207ea554ba1192439de75e1c1
    key-size 2048
    key-type rsa-private
    security-type fips
}
```

Deleting a key from the F5 software configuration and HSM using tmsh

You can use the Traffic Management Shell (`tmsh`) to delete a key from the F5® software configuration and the hardware security module (HSM).

1. Log in to the command line of the system using an account with root access.
2. Open the Traffic Management Shell (`tmsh`).
   `tmsh`
3. Delete a specified key.
   `delete sys crypto key <key_object_name>`

Supported FIPS key sizes

These are the supported key sizes for F5® FIPS platforms.

FIPS platform	Supported key sizes (bits)
5000	1024, 2048, 4096
7000	1024/2048, 4096
10200	1024, 2048, 4096
10350	2048

Additional FIPS platform management tmsh commands

This table lists additional `tmsh` commands that you can use to manage your FIPS platform.

Command	Description
`show sys crypto fips key`	Lists information about FIPS keys stored in the FIPS card, including FIPS key ID, length, type, and key objects.
`list sys crypto key`	Lists keys in the F5® software configuration.
`delete sys crypto fips key <key-id>`	Deletes a FIPS key from the FIPS card only.

Recovery Options

FIPS system recovery options

This table describes configuration options for FIPS system recovery.

Option	Description
Configure a device group	Configure the F5® devices in a device group with the FIPS HSMs synchronized. In the event of a system failure, the standby unit becomes active and handles incoming traffic. Contact F5 to arrange a Return Material Authorization (RMA) for the failed F5 device and then follow the steps for implementing a replacement unit to recover the failed device.
Configure an additional unit for recovery	Fully configure a third unit, add it to the security domain, and synchronize the configurations. Remove the unit from the network and store it in a secure location. If the F5 system in production is damaged or destroyed, you can use the backup unit to reconstitute the security domain.
Save the keys on a disk	Generate the private keys outside of the FIPS HSM. Copy the non-FIPS protected keys to a secure external location as a backup. Then convert the non-FIPS into FIPS keys on the F5 system. The keys on the F5 system are now protected by the FIPS HSM. If there is a catastrophic system failure, use the non-FIPS protected backup keys to repopulate the FIPS HSM. ***Caution:*** *This method for backup is not FIPS-compliant.*

Implementing a replacement unit in a device group after a system failure

Before you recover hardware security module (HSM) information, ensure that the F5® software is configured and then install your saved UCS file on the new replacement system. For information about backup and recovery of a BIG-IP® system UCS file, see *BIG-IP® System: Essentials*.

If one unit of a device group fails, the failover unit becomes active and maintains the HSM information. After you replace the failed unit in a device group, you need to restore the HSM information on the replacement unit.

1. Connect the currently active unit to the replacement unit.
2. On the replacement unit, initialize the FIPS card. For information about performing this initialization, see the appropriate HSM initialization procedure for your platform.

   Caution: *Be sure to run this FIPS card initialization command sequence on the replacement unit. If you run it on the currently active unit, you will lose all of your existing keys.*

   Note: *Be sure to use the same security domain that you specified when you initially set up the currently active unit.*

3. On the currently active unit, copy information from the currently active unit to the replacement unit.

   ```
   fipscardsync peer
   ```

Caution: *Be sure to run this FIPS card initialization command from the currently active unit. If you run this command from the replacement unit, you will lose your original FIPS information.*

4. On the currently active unit, synchronize the full software configuration to the replacement unit using `tmsh`.

   ```
   tmsh run config-sync to-group /Common/<devicegroupname>
   ```

   Important: *Synchronizing the software configuration using this command sequence also synchronizes the keys stored in the HSM.*

The replacement unit is now ready to function as the failover unit in a device group.

Implementing a replacement standalone device after a system failure

You must have a backup of your non-FIPS protected keys before you can restore the hardware security module (HSM) information on a standalone replacement device.

After you replace a failed standalone unit, you need to restore the HSM information on the replacement unit.

1. Copy the full software configuration to the replacement unit using `tmsh`.

   ```
   tmsh load ucs <ucsfilename>
   ```

   Important: *Synchronizing the configuration does not synchronize the keys stored in the HSM.*

2. On the replacement unit, initialize the FIPS card. For information about performing this initialization, see the appropriate HSM initialization procedure for your platform.
3. Log in to the command line of the system using an account with root access.
4. Open the Traffic Management Shell (`tmsh`).

   ```
   tmsh
   ```

5. Convert an existing key to FIPS.

   ```
   install sys crypto key <key_object_name> from-local-file <key_file_path>
   security-type fips
   ```

   This example converts an SSL private key named `mykey` from a local key file stored in the `/shared/tmp` directory: `install sys crypto key mykey from-local-file /shared/tmp/mykey.key security-type fips`

Legal Notices

Legal Notices

Publication Date

This document was published on February 3, 2017.

Publication Number

MAN-0659-00

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks*.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

VCCI Class A Compliance

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take corrective actions. VCCI-A

この製置は、クラス A 情報技術製置です。この製置を家庭環境で使用す ると電波妨害を引き起こすことがあります。　この場合には使用者が適切 な対策を講ずるよう要求されることがあります。 VCCI-A

Index