F5® Platforms: FIPS Administration

Version 13.1.0

Table of Contents

F5 FIPS Platform Introduction

About F5 HSM/FIPS implementations

F5 offers several Federal Information Processing Standard (FIPS) approaches. For specifics on the platforms, software versions, FIPS Certificates, and document for each approach, see *f5.com/about-us/certifications*.

These solutions are based on the add-on license that you use:

FIPS BIG-IP Platform Module

This is a FIPS 140-2 validated BIG-IP ®system. This system requires a Full-Box FIPS add-on license. Also referred to as Platform FIPS. This system provides FIPS validation without the performance impact of using an embedded HSM.

BIG-IP System with FIPS 140-2 Validated Network HSM

This is a BIG-IP system that uses an external FIPS 140-2 validated Network HSM. This system requires an External Interface and Network HSM add-on license. Also referred to as Network FIPS. This system provides the ability for any BIG-IP system to support validated FIPS traffic.

FIPS BIG-IP Software Module

This is a FIPS 140-2 validated virtual BIG-IP system. This system requires a FIPS 140-2 Level 1 Virtual add-on license. Also referred to as VE FIPS. This provides a validated platform with the flexibility of a virtual appliance.

These solutions are based on the appliance including an embedded FIPS-validated HSM:

FIPS BIG-IP with Embedded HSM

This is a BIG-IP system with an on-board FIPS-validated HSM. This system does not require any specific add-on licenses and requires only a BIG-IP software license that is valid for the specific platform. Also referred to as Embedded FIPS. This provides the increased FIPS level that are available with an embedded FIPS HSM.

FIPS BIG-IP Platform with Embedded HSM

This is an Embedded FIPS system that is licensed with the Platform FIPS license. It provides the performance of the Platform FIPS with the increased FIPS level of the Embedded HSM. This system requires a Full-Box FIPS add-on license. Also referred to as Dual FIPS.

Platform FIPS Overview

About the Platform FIPS installation kit

The Platform FIPS system includes the Full-Box FIPS add-on license, which includes tamper evidence seals that you must apply to the chassis for it to be FIPS-validated. For more information, see the *F5 Platforms: FIPS Kit Installation* guide at *support.f5.com*.

Platform FIPS self-test requirement

The NIST 140-2 FIPS standards require that the system must pass a series of self tests during operation and at initial startup. If any of these self-tests fail, the BIG-IP® system restarts and will not be able to boot into that volume at startup.

One of the self-tests that the system performs is a system integrity test. This test watches for unauthorized changes to the system. Making changes to the system using the F5® TMOS® Shell (`tmsh`), the Configuration utility, and the F5® APIs does not cause this test to fail. Making any changes to the underlying operating system or any BIG-IP files directly, however, might cause the test to fail.

Platform FIPS best practices

F5 recommends these best practices for working with your Platform FIPS system:

Backup partitions

To recover from a self-test failure, F5 recommends that you have at least two volumes configured and set up with the software version that you are using on the BIG-IP® system. If possible, you should avoid installing the Platform FIPS add-on license on the backup volume. This provides recovery options from a failed self-test.

***Note:** The BIG-IP system should have multiple volumes set up from the factory, but the software versions installed might not support the Platform FIPS license. Be sure to verify the versions before placing the BIG-IP system into production use.*

The `sys-eicheck` utility

Use the `sys-eicheck` utility to determine, without rebooting and locking the volume, if anything has happened that might cause the integrity test to fail. Run this utility before and after any administrative actions to identify anything that might cause a self-test failure by typing this command sequence on the command line: `/usr/libexec/sys-eicheck.py`.

FIPS Validated vCMP Guests

On certain BIG-IP platforms and VIPRION® platforms that are licensed with the Platform FIPS add-on license, any vCMP® guests are also considered vCMP validated. Unless the platform is also an Embedded FIPS platform, no additional administration is needed. For more information, see the *About FIPS multi-tenancy for vCMP guests* section under *Hardware HSM Setup and Administration*.

Platform and VE FIPS Module and Upgrade Notes

About using F5 modules

Only certain F5 modules are FIPS-validated. This means that to maintain FIPS validation for traffic, you can use only the validated modules. You can provision and set up other modules and use them for processing traffic, but traffic that uses any non-validated modules would not be considered FIPS-validated.

These modules are FIPS-validated:

- Local Traffic Manager™ (LTM)
- Advanced Firewall Manager™ (AFM)

About upgrading TMOS

Before you install any software updates or hot fixes, verify the FIPS validation status of that version on the F5 Certifications page (`f5.com/about-us/certifications`). The system allows you to apply all updates, but if the version has not been validated, your device will no longer be considered FIPS-validated.

Network HSM Overview

About the FIPS Network HSM

For information on setting up and managing keys for network hardware security modules (HSMs) that are supported with BIG-IP® systems, see the guide for your specific network HSM:

- *BIG-IP System and SafeNet Luna SA HSM: Implementation*
- *BIG-IP System and Thales HSM: Implementation*

About using with Platform FIPS, VE FIPS, or Embedded HSM systems

If the Network FIPS add-on license is combined with a Platform FIPS or VE FIPS add-on license, you need to decide which location to use to store your keys based on the certificate and SSL Policy. You would need to set up and administer the network HSM using the instructions for your specific network HSM. For keys not stored in the Network HSM, see the key information for the Platform FIPS or VE FIPS.

The Network FIPS add-on license should not be used on an Embedded FIPS system.

Hardware HSM Setup and Administration

About setting up embedded FIPS platforms in a device group

You can configure a device group using two platforms from the same series with a FIPS hardware security module (HSM) installed in each unit. When setting up an embedded 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.

About embedded HSM initialization and synchronization

After you have set up and configured your BIG-IP® systems, you create a FIPS security domain by initializing the embedded HSM and then synchronizing all applicable HSMs.

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 TMOS 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 TMOS 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). If you have a 10350v-FIPS platform provisioned for Virtual Clustered Multiprocessing (vCMP), you can also view information about any FIPS partitions on the HSM.

1. Log in to the command line of the system using an account with root access.
2. Open the TMOS 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
```

4. View information about FIPS partitions on the HSM.
   `run util fips-util ptninfo`

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 TMOS 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>
   ```

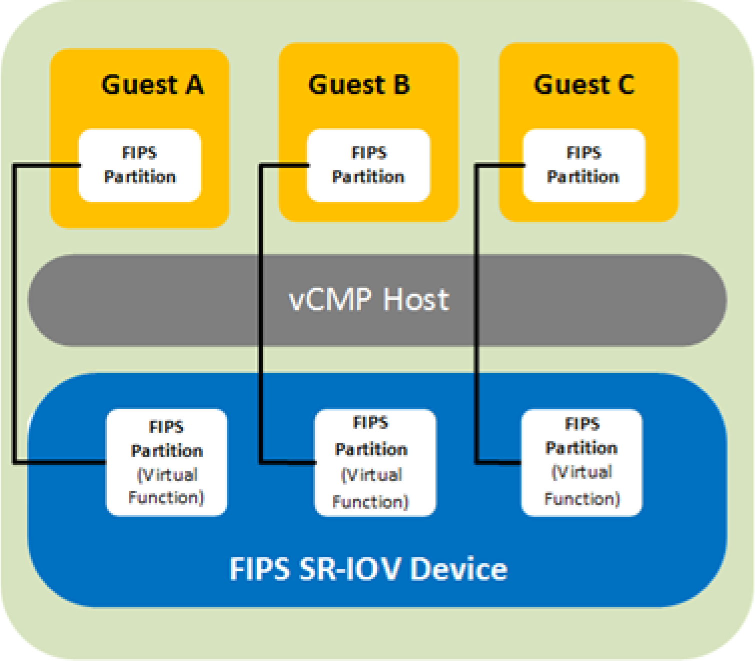
About FIPS multi-tenancy for vCMP guests

The BIG-IP® 10350v-FIPS platform model contains a FIPS-verified hardware security module (HSM) that supports Single Root I/O Virtualization (SR-IOV) mode on Virtual Clustered Multiprocessing (vCMP®)-enabled systems.

Benefit

The benefit of SR-IOV mode is that for a BIG-IP system on a 10350v-FIPS platform provisioned for Virtual Clustered Multiprocessing (vCMP®), you can create a virtual HSM (known as a FIPS partition) for each guest on the system. A *FIPS partition* is a portion of cores and private key slots on the HSM that a host administrator can dedicate to a guest for cryptographic functions.

This illustration shows a BIG-IP system where three guests each have their own FIPS partition for FIPS hardware-based processing.


Guest A
Guest B
Guest C
FIPS Partition
FIPS Partition
FIPS Partition
vCMP Host
FIPS Partition (Virtual Function)
FIPS Partition (Virtual Function)
FIPS Partition (Virtual Function)
FIPS SR-IOV Device

About core allocation

You can create up to 32 FIPS partitions on the HSM, with some number of cores allocated to each partition. The number of cores you allocate to a FIPS partition depends on the processing needs of the guest you assign the partition to. The only limit is that the combined number of cores for all partitions cannot exceed 63, the total number of cores that the HSM supports.

To determine how you want to deploy FIPS partitioning for your vCMP guests, you should:

- Identify the guests that need dedicated cores.
- Decide how many cores and private key slots you want to allocate to each guest's partition.

For example, to decide how many cores to dedicate to each guest, suppose guests `A` and `B` have equal core requirements, but guest `C` has twice the needs of both `A` and `B`. In this case, you could allocate 12 cores each to `A` and `B`, and 24 cores to `C`. This would mean a total core allocation of 48 HSM cores, leaving 15 cores unallocated and available for future guest needs.

About FIPS private keys

Once you have assigned a FIPS partition to a guest, the guest administrator can log in to the guest to create, convert, or import FIPS private SSL keys, which are stored on the HSM. The FIPS partition assigned to the guest dictates the amount of storage available for FIPS keys on the HSM for the guest.

Host administration tasks

Before vCMP® guest administrators can create and manage FIPS keys in their own secure partitions on the FIPS hardware security module (HSM), a host administrator must initialize the FIPS HSM, resize the default partition to free up cores for other FIPS partitions, and create those other partitions on the HSM. As host administrator, you'll create one unique partition for each guest.

Prerequisite tasks for managing FIPS partitions

Before you set up FIPS partitions for your Virtual Clustered Multiprocessing (vCMP®) guests, confirm that the vCMP host prerequisites have been met, on each device that hosts vCMP guests in your high availability configuration. Confirm all prerequisites by logging into the BIG-IP system using the management IP address of the vCMP host.

Important: *Your BIG-IP® user account must have a role of Administrator assigned to it.*

Prerequisites	Verification tool	Verification instructions
The BIG-IP system is provisioned for Virtual Clustered Multiprocessing (vCMP).	BIG-IP Configuration utility	On the Main tab, click **System** > **Resource Provisioning**. In the Module column, locate **Virtual CMP (vCMP)** and then view the Provisioning column.
You have created vCMP guests on the system.	BIG-IP Configuration utility	On the Main tab, click **vCMP** > **vCMP Guest List**. View the list of vCMP guests.
You have permission to use the TMSH (TMOS® Shell) command-line interface.	BIG-IP Configuration utility	On the Main tab, click **System** > **Users**. Then click your account name and view the **Terminal Access** list. This setting must be set to either **tmsh** or **Advanced shell**.
The license type is 10350v-FIPS.	An SSH application such as PuTTY	At the `tmsh` prompt, type `show sys hardware` and under `Platform`, look for a `Name` property of `10350F`.
The hardware security module (HSM) is initialized and the security label matches the label on all other devices hosting BIG-IP device group members (that is, vCMP guests).	An SSH application such as PuTTY	At the `tmsh` prompt, type `fips-util -v info`.
The HSMs on the appliances hosting the vCMP guests in the BIG-IP device group are synchronized.	An SSH application such as PuTTY	At the `tmsh` prompt, type `run util fips-card-sync` *`hostname`*.

Prerequisites	Verification tool	Verification instructions
You know the Security Officer password for managing the FIPS HSM.	Not applicable.	If you do not know the Security Officer password, see your security administrator.
The device has a Master Symmetric key.	An SSH application such as PuTTY	At the `tmsh` prompt, type `show sys crypto master-key`.
The BIG-IP configurations on all members of the BIG-IP device group (that is, vCMP guests) are synchronized.	BIG-IP Configuration utility	On the Main tab, click **Device Management** > **Overview**. Then verify that all device group members have a status of `In Sync`.

For more information, see the guide *BIG-IP Device Service Clustering: Administration*, on the F5 support site `support.f5.com`.

About resizing FIPS partitions

After all vCMP® guests are deployed with FIPS partitions assigned to them, you might decide later that you need to increase or decrease the number of cores for a specific guest.

When you resize a guest's partition, you use the TMSH (TMOS® Shell) command-line interface, and it's helpful to understand the output that TMSH displays during the resizing process. For example, suppose you initially resized `PARTITION_1` and created three other partitions, with these core allocations:

- `PARTITION_1`: 32 cores
- `PARTITION_2`: 8 cores
- `PARTITION_3`: 10 cores
- `PARTITION_4`: 4 cores

This shows that we have a total of 54 of the 63 cores on the HSM allocated, leaving 9 cores still unallocated.

Now suppose you decide to adjust the number of cores allocated to `PARTITION_2`, from 8 cores to 6. In this case, you'll need to use the `fips-util ptnresize` command within `tmsh`. For example, if you type:

```
   tmsh /util fips-util ptnresize
```

The system prompts you for a password and the relevant partition name and displays other fields showing their currently-configured values:

```
Enter Security Officer password: SO_password
Enter partition name: PARTITION_2
Enter max keys (1-82160, current 5000): 4000
Enter max accel devs (0 to 25, current 8):
```

In the `Enter max accel devs` field, the system shows that there are `0 to 25` cores available to `PARTITION_2` for resizing, with `8` cores currently allocated. The system calculates this `0 to 25` value using this formula:

```
(Total cores on the HSM - The sum of cores for the three other partitions) + (cores
currently assigned to PARTITION_2)
```

which translates to:

```
63 - (32 + 10 + 4) + 8 = 25
```

Important: *Notice that the displayed number of maximum cores available to* `PARTITION_2` *(25) includes the current allocation of 8 cores.*

For `Enter mac accel devs`, once you specify a new value of `6`, the number of unallocated cores on the HSM increases from 9 to 11.

Enabling vCMP after a BIG-IP software upgrade

If your BIG-IP® system was provisioned for vCMP® prior to upgrading to this BIG-IP version, you must enable a BigDB variable, `kernel.iommu`.

Important: *Be sure to do this before you manage the hardware security module (HSM) to create FIPS partitions for vCMP guests.*

1. Log in to the command line of the system using an account with root access.
2. Open the TMOS Shell (`tmsh`).
   ```
   tmsh
   ```
3. Enable the kernel.iommu DB variable.
   ```
   modify /sys db kernel.iommu value enable
   ```
4. Save your BIG-IP configuration.
   ```
   save /sys config
   ```
5. Reboot the system.
   ```
   sys reboot
   ```

Resizing the default FIPS partition

Whenever you initialize the FIPS hardware security module (HSM) on a vCMP® host, the process creates a FIPS partition named `PARTITION_1` that you can assign to one of your vCMP guests. By default, `PARTITION_1` contains all available FIPS cores on the HSM (63).

To free up cores for other guests, you'll need to reduce the number of cores assigned to `PARTITION_1`. You can then allocate those freed-up cores to other FIPS partitions that you create.

1. Log in to the command line of the system using an account with root access.
2. Open the TMOS Shell (`tmsh`).
   ```
   tmsh
   ```
3. Resize the default partition.
   ```
   fips-util ptnresize
   ```
4. Enter the Security Officer password.
5. At the `Partition name` prompt, enter the name of the default partition, `PARTITION_1`.
6. At the `Enter max keys` prompt, re-type or change the current value for the maximum number of SSL keys allocated to the default partition.
7. At the `Enter max accel devs` prompt, reduce the current value of `63`.

   The specified value represents the number of cores currently allocated to `PARTITION_1`.

   For example, if you intend to create three guests, and you know that for two of those guests, you'll want to create `PARTITION_2` and `PARTITION_3` and allocate 20 and 10 cores respectively, change the value for `PARTITION_1` from 63 to 33.
   Changing this value frees up the number of cores that you'll need for the other partitions.
8. Press Enter.

9. Save your BIG-IP configuration.
   `save /sys config`

After you complete this task, the HSM has available cores for you to allocate to other FIPS partitions that you create.

Creating FIPS partitions on the HSM

You can create a virtual hardware security module (HSM) for each vCMP® guest on the system that processes FIPS-related traffic. After creating FIPS partitions on the HSM, you can provide each guest with its own dedicated FIPS hardware resource to use for cryptographic functions.

***Note:** You only need to create a FIPS partition for a guest when the guest is processing FIPS-related traffic.*

1. Open the TMOS Shell (`tmsh`).
   `tmsh`
2. Create a FIPS partition.
   `fips-util ptncreate`

   ***Note:** If you receive an error message about acceleration, you'll need to resize the default FIPS partition before creating FIPS partitions.*

   The system then prompts you for Security Officer password.
3. Type the Security Officer password.
4. At the **Enter partition name** prompt, assign a name to the partition, such as `PARTITION_2`.

   ***Note:** Do not assign the name `PARTITION_1`. This is the name of the default FIPS partition.*
5. At the **Max key count** prompt, type the maximum number of private SSL keys that a guest administrator will be able to store in the guest's partition.
6. At the **Max accel devs** prompt, type a value for the number of FIPS hardware cores that you want to allocate to the partition.
7. Press Enter.
8. Save your BIG-IP configuration.
   `save /sys config`
9. Repeat for each additional partition that you want to create.

After you complete this task, the HSM has a unique FIPS partition for each guest that you want to assign FIPS hardware SSL resources to. You can then provide a guest with its own dedicated FIPS hardware SSL resource by assigning the FIPS partition to the guest.

Disabling a vCMP guest

Before performing this task, confirm that you are logged in to the BIG-IP® Configuration utility as a vCMP® host administrator.

Before you assign a FIPS partition to a guest, you must set the guest to the `Configured` state.

***Note:** This task is based on the assumption that the guest you want to disable is currently in a `Deployed` or `Provisioned` state.*

1. On the Main tab, click **vCMP** > **Guest List**.
   This displays a list of guests on the system.
2. In the Name column, find the name of the guest you want to assign a FIPS partition to, and in the left-most column, select the check box.

3. Click **Disable**.
   The guest state changes to `Configured`.
4. Repeat this task for each guest to which you plan on assigning a FIPS partition.

After performing this task, the guest can no longer process traffic, and you can now modify the guest to assign a FIPS partition.

Assigning a FIPS partition to a vCMP guest

Before performing this task, confirm that you are logged into the BIG-IP Configuration utility as a vCMP host administrator.

For BIG-IP® systems containing a FIPS hardware security module (HSM) on which you have created FIPS partitions, you can assign a separate FIPS partition to each vCMP® guest on the system. This provides each guest with its own virtual FIPS HSM to use for cryptographic functions when processing FIPS-related traffic.

It's worth noting that in addition to using FIPS partitions for FIPS-related traffic, you can configure the **SSL Mode** setting for non-FIPS related traffic. This controls the non-FIPS hardware SSL resources on the system.

1. On the Main tab, click **vCMP** > **Guest List**.
   This displays a list of guests on the system.
2. In the Name column, click the name of the guest that you want to modify.
   This displays the configured properties of the guest.
3. From the **FIPS Partition** list, select a FIPS partition name.
4. From the **Requested State** list, select **Deployed**.
5. Click **Update**.
   This action causes the guest to restart.
6. Repeat this task for each guest to which you want to assign a FIPS partition.

After you complete this task, each vCMP guest that you modified has a virtual FIPS HSM assigned to it to use for cryptographic functions.

Displaying the list of FIPS partitions on the HSM

When the FIPS hardware security module (HSM) in your BIG-IP® system contains FIPS partitions for multi-tenancy, you can display a list of the partitions at any time.

1. Open the TMOS Shell (`tmsh`).
   ```
   tmsh
   ```
2. View a list of partitions.
   ```
   fips-util ptninfo
   ```
3. Type the Security Officer password.
   The system displays a list of existing FIPS partitions on the HSM.

Deleting FIPS partitions on the HSM

When the FIPS hardware security module (HSM) in your BIG-IP® system contains FIPS partitions for multi-tenancy, you can delete one or more of those partitions from the HSM if for some reason you no longer need them.

1. Open the TMOS Shell (`tmsh`).
   ```
   tmsh
   ```
2. Delete a partition.
   ```
   fips-util ptndelete
   ```
   The system prompts you for the Security Officer password.

3. Type the Security Officer password.
4. At the `Enter partition name` prompt, type the name of the partition you want to delete.
5. Press Enter.
6. Save your BIG-IP configuration.
   ```
   save /sys config
   ```

Guest administration tasks

When a vCMP® guest has a FIPS partition assigned to it, the guest administrator can store private SSL keys on the FIPS hardware security module (HSM). Specifically, a guest administrator can use the BIG-IP® Configuration utility to:

- Create and store FIPS keys in the HSM.
- Import non-FIPS keys (`.exp` files) or FIPS keys to the HSM. Importing FIPS keys requires the BIG-IP system to use the same Master Symmetric key that was previously used to export the FIPS keys.
- Convert non-FIPS keys to FIPS keys, which are then stored in the HSM.

For information about managing your FIPS keys, see the Key Management section of this guide.

Before you log in to a vCMP guest and manage private SSL keys, confirm that you have met these prerequisites:

- You have a user role that allows you to log in to the system as a vCMP guest administrator.
- You have permission to use the TMSH (TMOS Shell) command-line interface.
- You have permission to manage private SSL keys.

For more information, see the *BIG-IP Digital Certificates: Administration* guide at `support.f5.com`.

About managing keys on embedded FIPS systems

You can use one of two tools to manage keys on your embedded FIPS system: the BIG-IP® Configuration utility or the F5® TMOS® Shell (`tmsh`).

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** > **Certificate Management** > **Traffic Certificate 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. From the **Key Type** list, select **FIPS**.
7. In the Key Properties area, select a key size from the **Size** list.
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** > **Certificate Management** > **Traffic Certificate 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** > **Certificate Management** > **Traffic Certificate 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 TMOS 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 TMOS 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 TMOS 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 TMOS 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 TMOS 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 TMOS 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 TMOS 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 TMOS 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 TMOS 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 TMOS 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 TMOS 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 TMOS 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 TMOS 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 hardware security module (HSM), 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 HSM only.

About recovery options

You can use one of these options for recovering your embedded FIPS system.

- Configure an additional unit for recovery
- Save the keys on a disk
- Configure a device group

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 hardware security module (HSM). For information about performing this initialization, see the appropriate HSM initialization procedure for your platform.

   Caution: *Be sure to run this FIPS HSM 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 HSM 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 HSM. 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 TMOS 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 December 28, 2017.

Publication Number

MAN-0659-01

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