FIPS Multi-Tenancy for vCMP Appliance Models

Version 13.1

Table of Contents

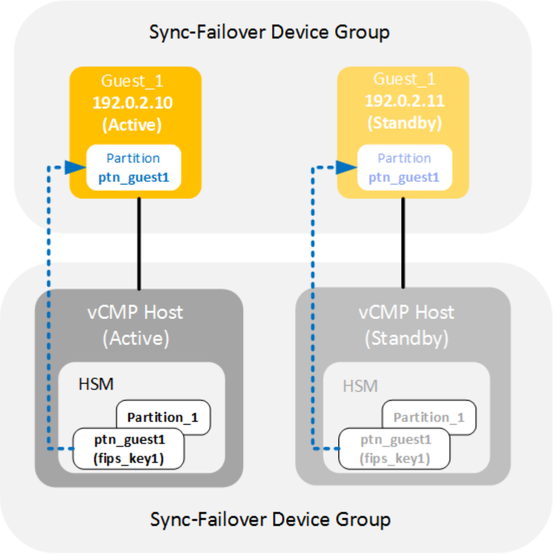
Overview: FIPS Multi-Tenancy for vCMP Systems

Overview: FIPS multi-tenancy for vCMP systems

Some F5 platform models contain a hardware security module (HSM) that supports FIPS multi-tenancy on Virtual Clustered Multiprocessing (vCMP)-enabled systems.

The benefit of an HSM that supports FIPS multi-tenancy is that you can create a virtual HSM (known as a FIPS partition) for each vCMP guest that processes FIPS-related traffic. A *FIPS partition* is a portion of SSL cores and private key slots on the HSM that a host administrator can dedicate to a vCMP guest for SSL acceleration and storage of FIPS keys.

This illustration shows a sample multi-tenant configuration on two vCMP hosts in a high-availability configuration.



In this example, two systems are configured as vCMP hosts and are members of a BIG-IP Sync-Failover device group (one member is active and the other standby), and each system hosts a guest named `Guest_1`. Each system also contains a hardware security module (HSM) with two FIPS partitions - the default partition, named `PARTITION_1`, and a second partition named `ptn_guest1`.

The guests, too, reside in a Sync-Failover device group and are configured identically except for their cluster management IP addresses, `192.0.2.10` and `192.0.2.11`. When creating each guest, the host administrator assigned the FIPS partition `ptn_guest1` to the guest. The two partitions are identical with respect to name, the amount of key storage allowed for the guest, and the maximum number of FIPS cores available to the guest.

Each instance of partition `ptn_guest1` on its respective HSM stores an SSL key named `fips_key1`.

With this setup, if failover occurs, both the active vCMP host configuration and its active guest configuration will fail over to their respective high availability peers, and the new FIPS partition and SSL key will be preserved.

vCMP Host Administration Tasks

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 perform some configuration tasks.

Prerequisite tasks

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

Important: *For you to confirm these prerequisites, your BIG-IP system user account must have a role of Administrator assigned to it.*

Prerequisites	Verification tool	Verification instructions
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**. For more information, see the guide *BIG-IP System: User Account Administration* on the F5 support site `support.f5.com`.
The license type on each BIG-IP device is correct.	An SSH application such as PuTTY	At the `tmsh` prompt, type `show sys hardware`. Under `Platform`, look at the `Name` property, and confirm that the platform model number includes an `F`. For more information, see the guide *BIG-IP System: Essentials* on the F5 support site `support.f5.com`.
The BIG-IP devices that are to operate as vCMP hosts are in a Sync-Failover device group for high availability.	The BIG-IP Configuration utility or the TMOS Shell (TMSH)	For more information, see the guide *BIG-IP Device Service Clustering: Administration* on the F5 support site `support.f5.com`.
The hardware security module in each BIG-IP device is in the factory default state.	The TMOS Shell (TMSH)	To reset an HSM to its factory default state, see the command `tmsh fips-util -f reset`.

Initializing the HSMs on vCMP hosts

On each physical device that you intend to configure as a vCMP host, you must initialize the installed hardware security module (HSM). In our sample configuration, two BIG-IP devices function as vCMP hosts.

During HSM initialization, the system creates a default FIPS partition named `PARTITION_1`. By default, all FIPS cores and key storage are allocated to this partition.

1. Using an SSH application such as `PuTTY`, log in to the command line of a BIG-IP system using an account with `root` access.
2. Open the TMOS Shell (TMSH) and type `tmsh`.
3. Start the process of initializing the HSM by typing this TMSH command:
   `run util fips-util init`

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

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

   After typing this command, the initialization process begins. When prompted, type an SO password. The password does not appear on the screen as you type it. Also, 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:
Initializing device...
The FIPS device has been initialized.
```

4. Enable the HSM 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.*
5. To view information about the HSM after initialization, type `fips-util -v info` at the TMSH prompt.
6. Repeat these steps on the other device that you intend to configure as a vCMP host.

After you complete this task, both HSMs on the BIG-IP devices are initialized. Also, each HSM contains the default FIPS partition, `PARTITION_1`.

Later in the configuration process, you will resize the default partition to free up FIPS resources to assign to a new FIPS partition.

Synchronizing the HSMs

Before you synchronize the HSMs on the peer devices, verify that the HSMs:

- Are already initialized
- Have identical security domain labels
- Do not contain existing keys
- Are the same hardware model
- Contain the same firmware version

Also, check that, for each device, you know the security officer (SO) password for the HSM and the password for an account with `root` access.

Synchronizing the HSMs between peer devices enables you to copy keys from one HSM to another. HSM synchronization is also required before you can synchronize the BIG-IP software configuration in a Sync-Failover device group later.

1. Log on to the command line of the source F5 device, using an account with `root` access.
2. Open the TMOS Shell (tmsh) by typing `tmsh` at the system prompt.
3. Confirm that the HSM on the device has a Master Symmetric key by typing the command `show sys crypto master-key`.
4. Synchronize the Master Symmetric key from the HSM on the source device to the HSM on the target device, where <*`ip_address`*> is the IP address of the target device: `run util fips-card-sync` *`<ip_address>`*.

   Note: *Be sure to run this command on a device that contains a valid Master Symmetric key. 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.*

   In our example, this command is `run util fips-card-sync 192.0.2.11`

   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 192.0.2.11 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.
```

5. On the source and target devices, confirm that the devices have the same 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    <>
```

After you perform this task, the Symmetric Master key of the source and target devices are synchronized.

Provisioning the vCMP feature

Before performing this task, ensure that the amount of reserve disk space that the provisioning process creates is sufficient on each BIG-IP system. Attempting to adjust the reserve disk space after you have provisioned the vCMP feature produces unwanted results.

Performing this task creates a vCMP host (the hypervisor) and dedicates most of the system resources to running vCMP. Performing this task also enables the BigDB variable `kernel.iommu`, which is a requirement for vCMP. You must perform this task on each BIG-IP device that you want to function as a vCMP host in the configuration.

***Warning:** If the system currently contains any BIG-IP module configuration data, this data is deleted when you provision the vCMP feature.*

1. On the Main tab, click **System** > **Resource Provisioning**.
2. Verify that all BIG-IP modules are set to **None**.
3. From the **Virtual CMP (vCMP)** list, select **Dedicated**.
4. Click **Update**.
5. Repeat this task on the other BIG-IP device that you want to function as a vCMP host.

After provisioning the vCMP feature, the system reboots TMOS and prompts you to log in again. This action logs you in to the vCMP host, thereby allowing you to create guests and perform other host configuration tasks.

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`. By default, this partition contains all available FIPS cores on the HSM, as well as all key storage. In our sample configuration, the default partition isn't used; therefore, you can reduce the amount of FIPS resource allocated to it. This frees up resources to allocate to a new partition that you create.

You must perform this task on each vCMP host in the configuration.

1. Log in to the command line of the system using an account with `root` access.
2. At the system prompt, open the TMOS Shell (tmsh) by typing `tmsh`.
3. Type the command `run util fips-util ptnresize`.
4. Enter the security officer (SO) password.
5. At the `Partition name` prompt, note the name of the default partition, `PARTITION_1`.
6. At the `Enter max keys` prompt, reduce the current value to the lowest value possible, `1`.
7. At the `Enter max accel devs` prompt, reduce the current value to the lowest value possible, `1`.
8. Press Enter.
9. Save your BIG-IP configuration by typing `save /sys config`.
10. Log on to the other vCMP host in the configuration and repeat this task.

After you complete this task, the HSM has available FIPS cores and key storage for you to allocate to a new FIPS partition that you will create.

Creating a FIPS partition on the HSMs

You can create a FIPS partition for a vCMP guest that processes FIPS-related traffic. A *FIPS partition* functions like a virtual HSM, dedicating some amount of FIPS cores and key storage from the physical HSM to the guest. Although the HSM initialization process created a default partition, named `PARTITION_1`, you can create a new FIPS partition to assign to each guest instead.

You must perform this task on each vCMP host in the configuration.

1. Log in to the command line of the system using an account with `root` access.
2. At the system prompt, open the TMOS Shell (TMSH) by typing `tmsh`.
3. Type the TMSH command `run util fips-util -v info` to see how many FIPS cores are available for a new partitions that you create.
4. Create a FIPS partition by typing `run util 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.*

5. Type a security officer password.

   This password can be the same as, or different from, the same FIPS partition that you create on the device that will be part of the guest's high-availability configuration.
6. At the **Enter partition name** prompt, assign a name to the partition.

   ***Note:** Do not assign the name `PARTITION_1`. This is the name of the default FIPS partition.*

   In our sample configuration, this name is `ptn_guest1`.
7. 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.

   ***Important:** This value must match the **Max key count** value that you will specify for an equivalent FIPS partition that you will create later on the other host device in the high availability configuration.*

8. At the **Max accel devs** prompt, type a value for the number of FIPS hardware cores that you want to allocate to the partition.

   ***Important:** This value must match the **Max accel devs** value that you will specify for an equivalent FIPS partition that you will create later on the other host device in the high availability configuration.*

9. Press Enter.
10. Save your BIG-IP configuration by typing `save /sys config`.
11. Verify that partition you created exists on the system by typing `run util fips-util ptninfo` at the TMSH prompt.

    You should see output similar to this:

```
    11:10.0 PARTITION_1
    11:10.2 ptn_guest1
```

12. Log on to the other vCMP host in the configuration and repeat this task to create an identical partition with the same name and the same storage and FIPS core values.

After you complete this task, the HSM on each vCMP host device has a FIPS partition that you can assign to a guest that you create.

Creating vCMP guests

Before you create a vCMP guest, verify that you have configured the base network on the system to create any necessary trunks or VLANs for guests to use when processing application traffic.

You create a vCMP guest when you want to create an instance of the BIG-IP software for the purpose of running one or more BIG-IP modules to process application traffic. When creating a guest, you specify the number of cores that you want the vCMP host to allocate to each guest, as well as the FIPS partition that the guest should use.

You must perform this task on each vCMP host in the Sync-Failover device group.

***Note:** When creating a guest, if you see an error message such as `Insufficient disk space on /shared/vmdisks. Need 24354M additional space.`, you must delete existing unattached virtual disks until you have freed up that amount of disk space.*

1. Log in to the BIG-IP system using a management IP address of the vCMP host.
2. On the Main tab, click **vCMP** > **Guest List**.
3. Click **Create**.
4. From the **Properties** list, select **Advanced**.
5. Type a **Name** for the guest.
   In our sample configuration, this name is `Guest_1`.
6. In the **Host Name** field, type a unique, fully-qualified domain name (FQDN) name for the guest.

   If you leave this field blank, the system assigns the name `localhost.localdomain`.
7. From the **Cores Per Guest** list, select the number of vCPU cores that you want the host to allocate to the guest.
   In our sample configuration, this value is `2`.
8. From the **Management Network** list, select **Bridged**.
9. For the **Management Port** setting, fill in the required information:
   a) In the **IP Address** field, type a unique management IP address that you want to assign to the guest.

      You use this IP address to access the guest when you want to manage the BIG-IP modules running within the guest.
   b) In the **Network Mask** field, type the network mask for the management IP address.
   c) In the **Management Route** field, type a gateway address for the management IP address.

   ***Important:** Assigning an IP address that is on the same network as the host management port has security implications that you should carefully consider.*
10. From the **Initial Image** list, select the ISO image file for creating the guest's virtual disk that matches the other guests in the cluster.
11. From the **FIPS Partition** list, select a FIPS partition name.
    In our sample configuration, this name is `ptn_guest1`.
12. In the **Virtual Disk** list, retain the default value of **None**.

    Note that if an unattached virtual disk file with that default name already exists, the system displays a message, and you must manually attach the virtual disk. You can do this using the `tmsh` command line interface, or use the Configuration utility to view and select from a list of available unattached virtual disks.

The BIG-IP system creates a virtual disk with a default name (the guest name plus the string `.img`, such as `Guest_1.img`).

13. For the **VLAN List** setting, subscribe to host-based VLANs:
    a) Select the external and internal VLANs from the **Available** list.
    b) Use the Move button to move the VLANs to the **Selected** list.

    After you create the guest, the guest uses the selected VLANs to process application traffic. As an option, the guest administrator can create additional VLANs later from within the guest.
14. Confirm that the **Appliance Mode** check box is cleared.
15. From the **Guest Traffic Profile** list:
    - Select **None** if you do not want to meter network traffic using a Single Rate Three Color Marker (srTCM) policer.
    - Select the name of an existing srTCM policer if you want the BIG-IP system to classify network traffic as green, yellow, or red using the srTCM standard.
16. From the **SSL Mode** list, select **Shared**.
17. From the **Requested State** list, select **Deployed**.
18. Click **Finished.**
    After you complete this task, the BIG-IP system begins to deploy the guest.
19. Repeat this task on the other vCMP host in the configuration assigning the same guest name, the same number of vCPU cores, and the same FIPS partition name to the guest. Only the host name of the guest must be different.

After you complete this task on each vCMP host in the configuration, each host device hosts a guest that is configured to use a portion of FIPS cores and key storage on the local HSM.

vCMP Guest Administration Tasks

Guest administration tasks

There are a few tasks that a guest administrator must perform in order to store private SSL keys on a FIPS hardware security module (HSM).

***Note:** Before performing guest administration tasks, make sure that your BIG-IP user account has assigned you the Administrator user role and that it grants you permission to access the TMOS Shell (TMSH).*

Initializing the HSMs within vCMP guests

Within each vCMP guest, you must initialize the hardware security module (HSM) in a similar way to the way you initialized the HSM on each vCMP host. Our sample configuration includes two guests, each named `Guest_1`.

***Important:** During HSM initialization on the first guest, you must create a security domain label. It's critical that you specify this same label during initialization of the HSM on the other device so that both HSMs are members of the same security domain.*

1. Using an SSH application such as PuTTY, log in to the command line of a BIG-IP system using an account with `root` access.
2. Open the TMOS Shell (`tmsh`) and type `tmsh`.
3. Start the process of initializing the HSM by typing this `tmsh` command:
   `run util fips-util init`

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

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

   After typing this command, the initialization process begins. When prompted, type an SO password. The password does not appear on the screen as you type it. Also, you cannot use the keyword `default` as the SO password.

   ***Note:** F5 recommends that you choose a strong value for the SO password. This password can be unique on each guest in the configuration.*

```
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 will specify the same domain label later, when you initialize the HSM on the other device.

```
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 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.*

6. To verify that the HSM is initialized with a security domain label, type `fips-util -v info` at the TMSH prompt.
7. Repeat these steps on the other vCMP guest.

   > ***Important:*** *Be sure to specify the same security domain label on each device so that both HSMs are members of the same security domain. The SO password, however, can be unique on each device.*

After you complete this task, both HSMs on the BIG-IP devices are initialized and members of the same security domain. Also, each HSM contains the default FIPS partition, `PARTITION_1`.

Later in the configuration process, you will resize the default partition to free up FIPS resources to assign to a new partition.

Synchronizing the FIPS partitions

Before you perform this task, make sure that you have the security officer (SO) passwords for both the local and remote vCMP guests, as well as an account with `root` access.

You must use the `fips-card-sync`command within the TMOS Shell (TMSH) to ensure that the FIPS partitions that the host administrator created on each hardware security module (HSM) are synchronized between the guests.

1. Log on to the command line of the source F5 vCMP guest, using an account with `root` access.
2. Open the TMOS Shell (`tmsh`) by typing `tmsh` at the system prompt.
3. Synchronize the FIPS partition from the local vCMP guest (`Guest_1`) to the remote guest (also `Guest_1`), where <*`hostname`*> is either the cluster management IP address or the fully-qualified domain name (FQDN) of the remote guest.

In our sample configuration, a guest administrator logged into `192.0.2.10` would type this command: `run util fips-card-sync -u root 192.0.2.11`.

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 192.0.2.11 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.
```

After you perform this task, the FIPS partitions on the vCMP guests are synchronized. Each FIPS partition has the same configuration with respect to key storage size and available FIPS cores for its associated guest.

Setting up the BIG-IP software within vCMP guests

Before you perform this task, make sure that you know the cluster IP management address assigned to each vCMP guest. Also, confirm that your BIG-IP user account has the Administrator user role assigned to it.

Use this task to run the Setup utility on the vCMP guest that resides on each vCMP host. In our sample configuration, the guest on each host is named `Guest_1`. The Setup utility automatically opens when you log in to a guest for the first time.

You run the Setup utility to perform tasks such as licensing the guest, assigning passwords to the `root` and `admin` user accounts, provisioning BIG-IP modules, and putting the guests into a high availability configuration.

1. From a browser window, log in to one of the vCMP guests by typing a URL that contains its cluster management IP address: `https://`*`cluster_management_IP_address`*.
   In our sample configuration, this IP address is either `192.0.2.10` or `192.0.2.11`.
   This action displays the Setup utility.
2. Run the Setup utility, making sure to enable high availability during the process.

   When setting up high availability during setup, make sure to enable both configuration synchronization and failover at a minimum. Enabling connection mirroring is optional.
3. Repeat these steps on the other vCMP guest.

After you perform this task, you have two guests that are ready to process application traffic and are configured for high availability in an active-standy configuration.

Creating FIPS keys

You can use the BIG-IP Configuration utility to create a FIPS key on each guest in the high-availability configuration. In our example, both guests in the guests' Sync-Failover device group are named `Guest_1`, and the FIPS key name for each guest is `fips_key1`.

1. On the Main tab of the BIG-IP Configuration utility, click **System** > **Certificate Management** > **Traffic Certificate Management** > **SSL Certificate List**.
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:
   - For a self-signed certificate, select **Self**.
   - To request a certificate from a CA, select **Certificate Authority**.
5. Do one of the following:
   - If you chose **Self** in the previous step, then in the Certificate Properties area of the screen, configure the settings as needed.
   - If you chose **Certificate Authority** in the previous step, then in the Certificate Properties and Certificate Signing Request Attributes areas of the screen, configure the settings as needed.
6. From the **Security Type** list, select **FIPS**.
7. From the **Key Type** list, select **FIPS**.
8. Select a key size from the **Size** list.
9. Click **Finished**.

After you complete this task, you must sync the BIG-IP system configuration on this guest to the other guest in the Sync-Failover device group, or confirm that automatic synchronization is enabled.

Confirming synchronization of FIPS partitions and keys

Before you perform this task, confirm that:

- You have permission to access the TMOS Shell (TMSH).
- You have performed a config sync from one guest to the other in the Sync-Failover device group.

When you have vCMP guests in a Sync-Failover device group, you can check to make sure that the FIPS partition and key for a guest are synced to the other guest.

1. Using an SSH program such as PuTTY, log in to the console of a guest, using the guest's cluster management IP address.
   In our sample configuration, this IP address is either `192.0.2.10` or `192.0.2.11`, depending on which instance of the guest you are logging in to.
2. At the `tmsh` prompt, display the configuration of the local guest's FIPS partition by typing `run util fips-util info`.
   In our sample configuration, the FIPS partition is named `ptn_guest1`.
3. At the prompt, type `list sys crypto` *`key_name`*.
   In our sample configuration, the key name is `fips_key1`.
   The system displays information about the key `fips_key1`.
4. Log in to the guest on the remote vCMP host and type the same commands.

After you perform this task, you can see that the FIPS partition and the FIPS key on one guest are synced to the other guest in the guest device group.

Legal Notices

Legal notices

Publication Date

This document was published on January 11, 2019.

Publication Number

MAN-0755-00

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*.

Link Controller Availability

This product is not currently available in the U.S.

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.

Index