Fortanix®

Integration Guide

USING FORTANIX DATA SECURITY MANAGER WITH F5 BIG-IP VIRTUAL EDITION

Fortanix, Inc. | 800 West El Camino Real | Suite 180 | Mountain View, CA 94040 | United States of America |
+1 (650) 943-2484 | info@fortanix.com | www.fortanix.com

1.0 INTRODUCTION

This article describes how to integrate **Fortanix Data Security Manager (DSM) with F5 Networks Big IP Virtual Edition (VE) version 15.1.2.1 or later**. It also contains the information that a user requires to:

- Set inbound traffic rules if using Azure Marketplace platform
- Set admin password for BIG-IP VE

2.0 PREREQUISITES

NOTE: The minimum supported BIG IP Version is 15.1.2.1.

2.1 F5 BIG-IP LOCAL TRAFFIC MANAGER (LTM) 15.1.2.1 OR LATER

Virtual Edition (VE) is utilized for this article. Both hardware and virtual edition platforms support network Hardware Security Module (HSM) integration. Additionally, you will need to provide a license covering the network HSM module.

2.2 CREATE INBOUND TRAFFIC RULES IF USING AZURE MARKETPLACE PLATFORM

In order to access the BIG-IP Configuration utility, you must open port `8443`. To connect to BIG-IP VE using SSH, use the open port `22`. To connect to your application through BIG-IP VE, use the open port `443` (in this example).

1. In the Azure portal, click **All Services -> Network security groups**.
2. Filter the list to find your group and click it.
3. In the left menu, under **Settings**, click **Inbound security rules**.
4. Click **Add**.

NAME	VALUE
SOURCE PORT RANGES	An IP range on your network.
DESTINATION PORT RANGES	22
PROTOCOL	TCP
NAME	A description, like `SSH access`.

5. Click **Add again.**

6. Repeat *Steps 4* and *5*, using `8443` as the **Destination port range**. This allows management traffic for the port `8443` to reach BIG-IP VE.

7. Repeat *Steps 4* and *5*, using `443` as the **Destination port range**. This allows traffic for your application (in this example).

2.3 SET ADMIN PASSWORD FOR BIG-IP VE

Give BIG-IP VE six to ten minutes to finish deploying before you attempt to connect.

The first time you boot BIG-IP VE, you must connect to the instance and create a strong admin password. You will use the admin account and password to access the BIG-IP Configuration utility.

This management interface may be accessible to the Internet, so ensure the password is secure.

1. Connect to BIG-IP VE.
2. To change to the `tmsh` prompt, type:

```
tmsh
```

3. Modify the admin password.

```
modify auth password admin
```

   The terminal screen displays the message:

```
changing password for admin
new password:
```

4. Type the new password and press Enter.

   The terminal screen displays the message:

```
confirm password
```

5. Re-type the new password, and then press Enter.
6. Ensure that the system retains the password change, and press Enter.
7. Save the system configuration.

```
save sys config
```

8. Now, open a web browser and go to the BIG-IP Configuration utility, for example: https://<external-ip-address>:8443

3.0 INTEGRATION WITH F5 BIG-IP VE

3.1 CREATE FORTANIX DATA SECURITY MANAGER APPLICATION

Create an application in Fortanix DSM. For more details refer to the Fortanix DSM Getting Started Guide. The application can access certificates, keys, and secrets that will be used by your application (delivered using the BIG-IP).

1. Log in to the Fortanix DSM UI. Select the **Apps** icon from the left panel and then click the '**+**' icon to open a new application form.
2. Enter the name of the application and select **API Key** as the authentication method.
3. Create a group and assign the application to the group. The group represents a collection of security objects, (applications, keys, certificates, and so on.) that are available to the members of the group.
4. Click **Save** to create the application.

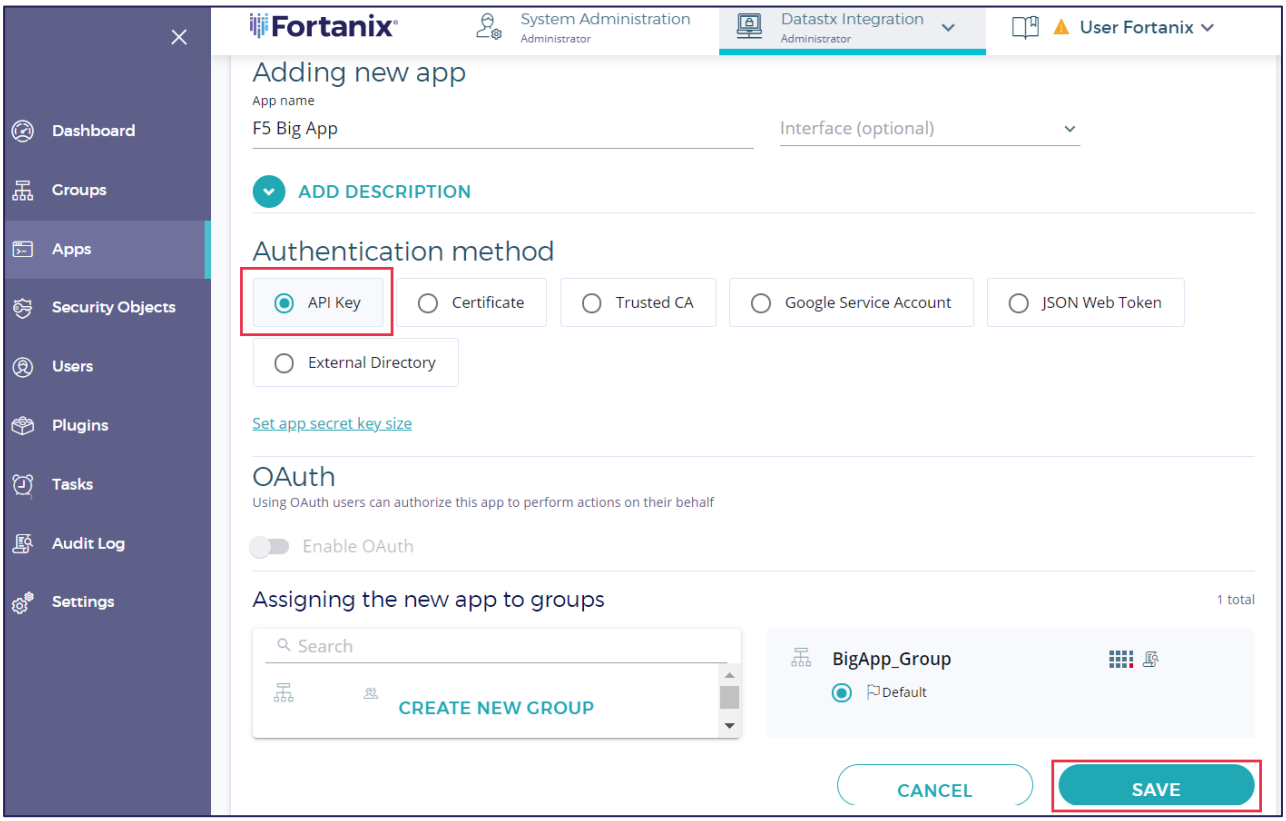

FIGURE 1: CREATE AN APP

With the application created, click **COPY API KEY** from the detailed view of the application or from the application table to capture the API key and store it for later use. The key will be used by the BIG-IP to authenticate calls to Fortanix DSM.

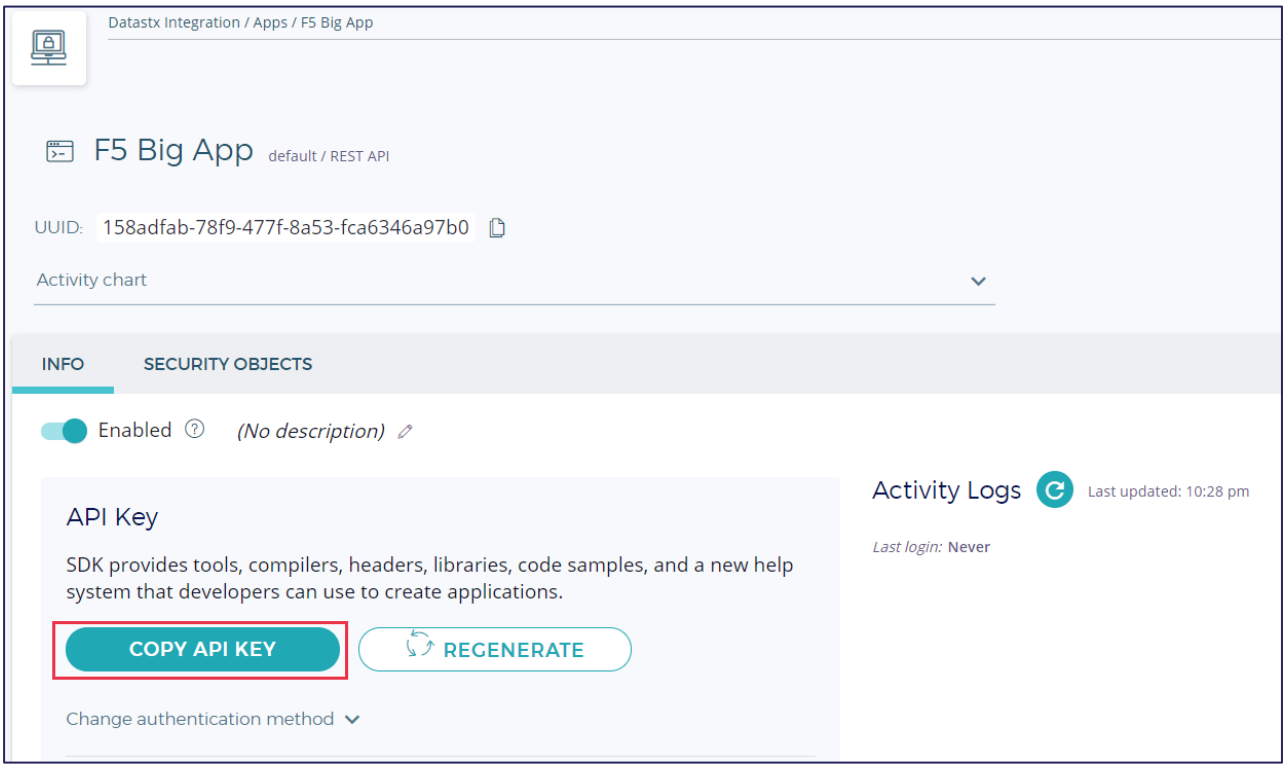

FIGURE 2: COPY API KEY

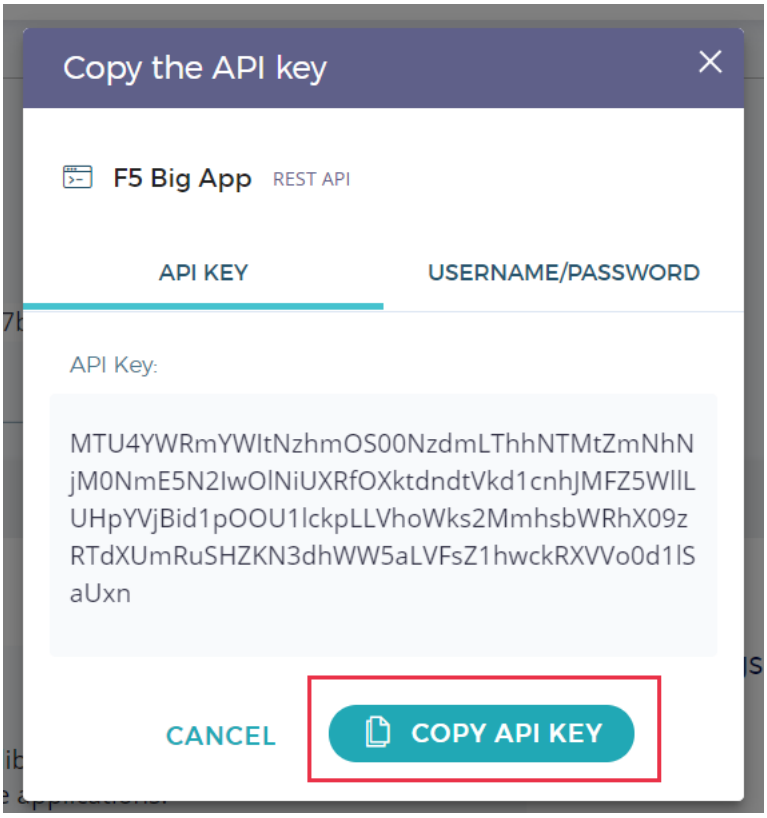

FIGURE 3: COPY API KEY

3.2 INSTALL FORTANIX PLUGIN

In this step, use the ssh client to log in to the BIG-IP as root. From there use the following commands to download and install the Fortanix plugin onto the BIG-IP. The plugin, (RPM) is available for download from here.

```
cd /shared/
mkdir nethsm
cd nethsm

curl -O https://d2bzqwib4mjc49.cloudfront.net/3.11.1281/fortanix-
pkcs11-3.11.1281-0.x86_64.rpm
rpm -ivh ./fortanix-pkcs11-3.11.1281-0.x86_64.rpm
```

3.3 CONFIGURE BIG-IP NETHSM INTEGRATION

1. Add the Fortanix HSM library to the BIG-IP.

```
tmsh create sys crypto fips external-hsm vendor auto pkcs11-lib-
path /opt/fortanix/pkcs11/fortanix_pkcs11.so
```

2. Create the `/config/fortanix.cfg` file.

```
vi /config/fortanix.cfg
```

   Add the following lines and save the file:

```
### sample fortanix config file
# cat /config/fortanix.cfg
api_endpoint="https://sdkms.fortanix.com"
api_key=""
# specify if endpoint uses self-signed certificate
ca_certs_file = ""
[log]
file = "/var/log/fortanix.log"
```

3. Configure the netHSM partition.

```
tmsh create sys crypto fips nethsm-partition auto password
"file:///config/fortanix.cfg"
```

4. Restart the ***pkcs11d*** service.

```
bigstart restart pkcs11d tmm
```

5. Test the connectivity - use the BIG-IP management GUI to test the connectivity between the BIG-IP and Fortanix DSM. After logging into the BIG-IP GUI navigate to **System** --> **Certificate Management** --> **HSM Management** --> **External HSM**. Under the *'Partitions'* section select the checkbox in the Partition List and click **Test**. Following is an example output of a successful connectivity test.

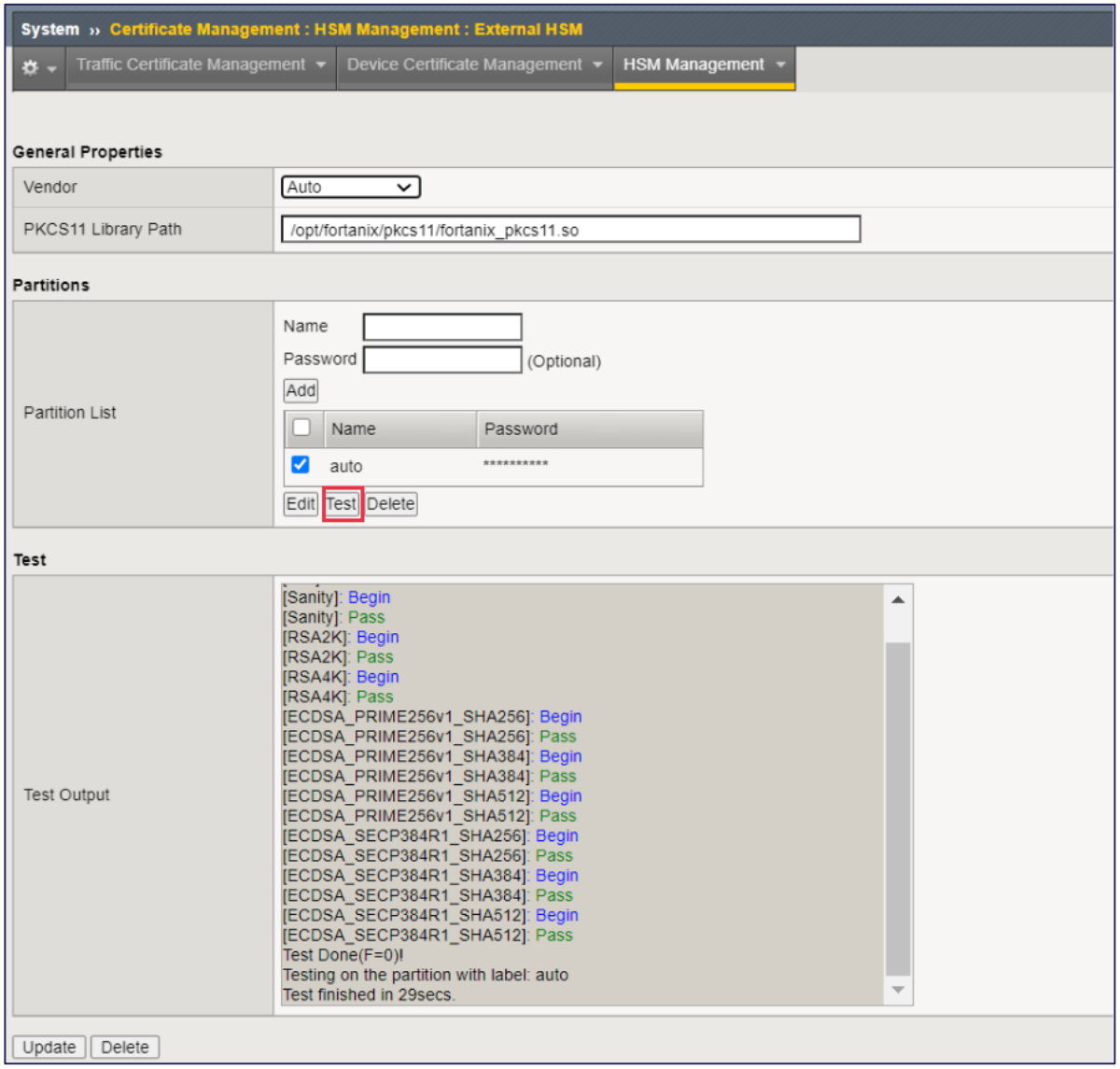

FIGURE 4: TEST CONNECTIVITY

3.4 IMPORT SSL CERTIFICATE/KEY TO BIG-IP AND FORTANIX DATA SECURITY MANAGER

1. **Import Private key into Fortanix DSM**: Now that we have our external HSM, (Fortanix), https://fortanix.aserracorp.com integrated with our BIG-IP let us put it to use. To start with, import a private key into Fortanix DSM.
   a. Log in to the Fortanix DSM UI and select the **Security Objects** icon from the left panel and then click the **+** button to create a new security object.
   b. Enter the name for the key and select the **Import** option to import a new key.
   c. Select **RSA** as the security object type.
   d. Select **Base64** and upload the private key.
   e. Associate the key to a previously created group.
   f. Click **Import** to create the security object.

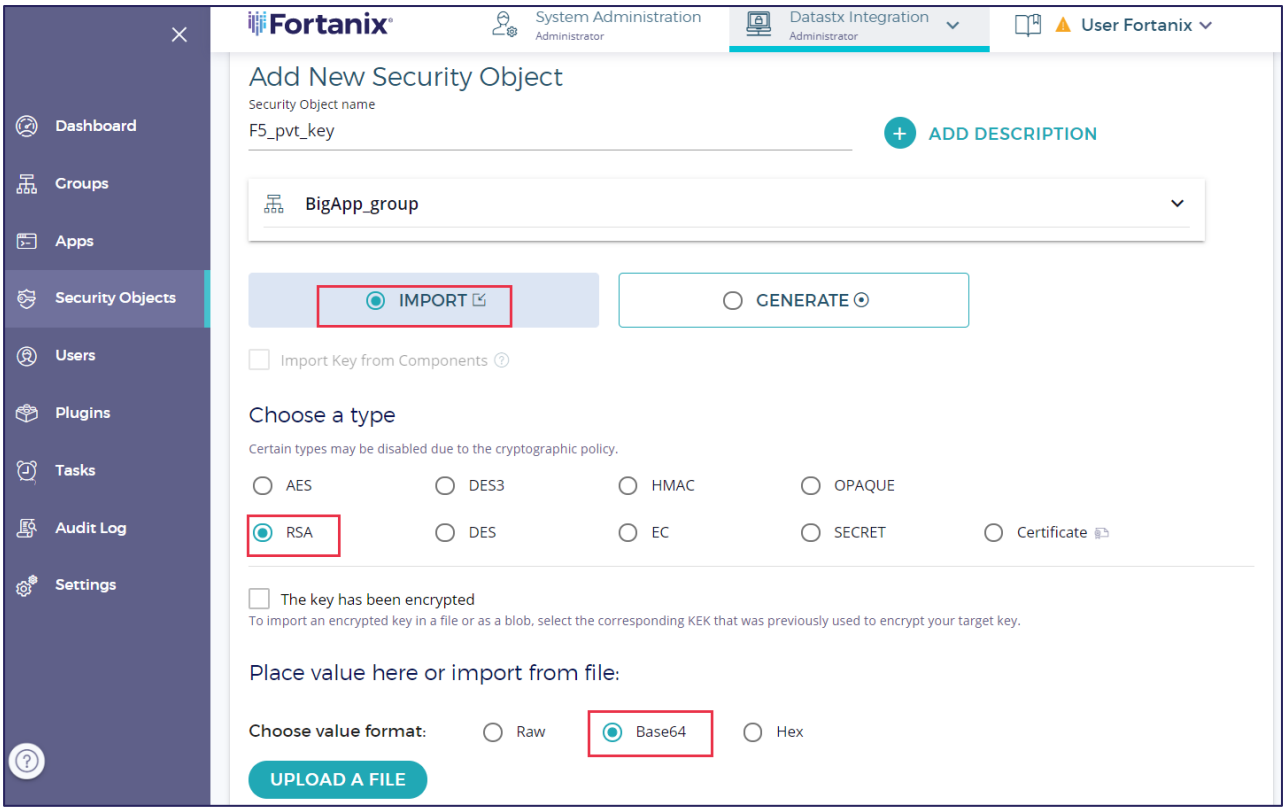

FIGURE 5: CREATE SECURITY OBJECT

2. **Import SSL Certificate and netHSM Key Pointer into BIG-IP:** With Fortanix DSM now hosting the private key, import the corresponding certificate into the BIG-IP. Additionally, create a key resource pointing to the Fortanix DSM-hosted key.
   a. Log in to the BIG-IP management GUI and navigate to **System** --> **Certificate Management** --> **SSL Certificate List** --> **Import**.
   b. Select **Certificate** as Import Type and enter a name.

c. Browse and upload the certificate, click **Import**.

d. Restart ***pkcs11d*** service using the following command:

```
bigstart restart pkcs11d tmm
```

e. Next, navigate to **System** --> **Certificate Management** --> **SSL Certificate List** --> **Import**.

f. Select **Key** as Impo`rt Type and enter a name. The name must match the security object name of the Fortanix DSM-stored key.

g. Select **Key Source** as **From NetHSM**, and click **Import**.

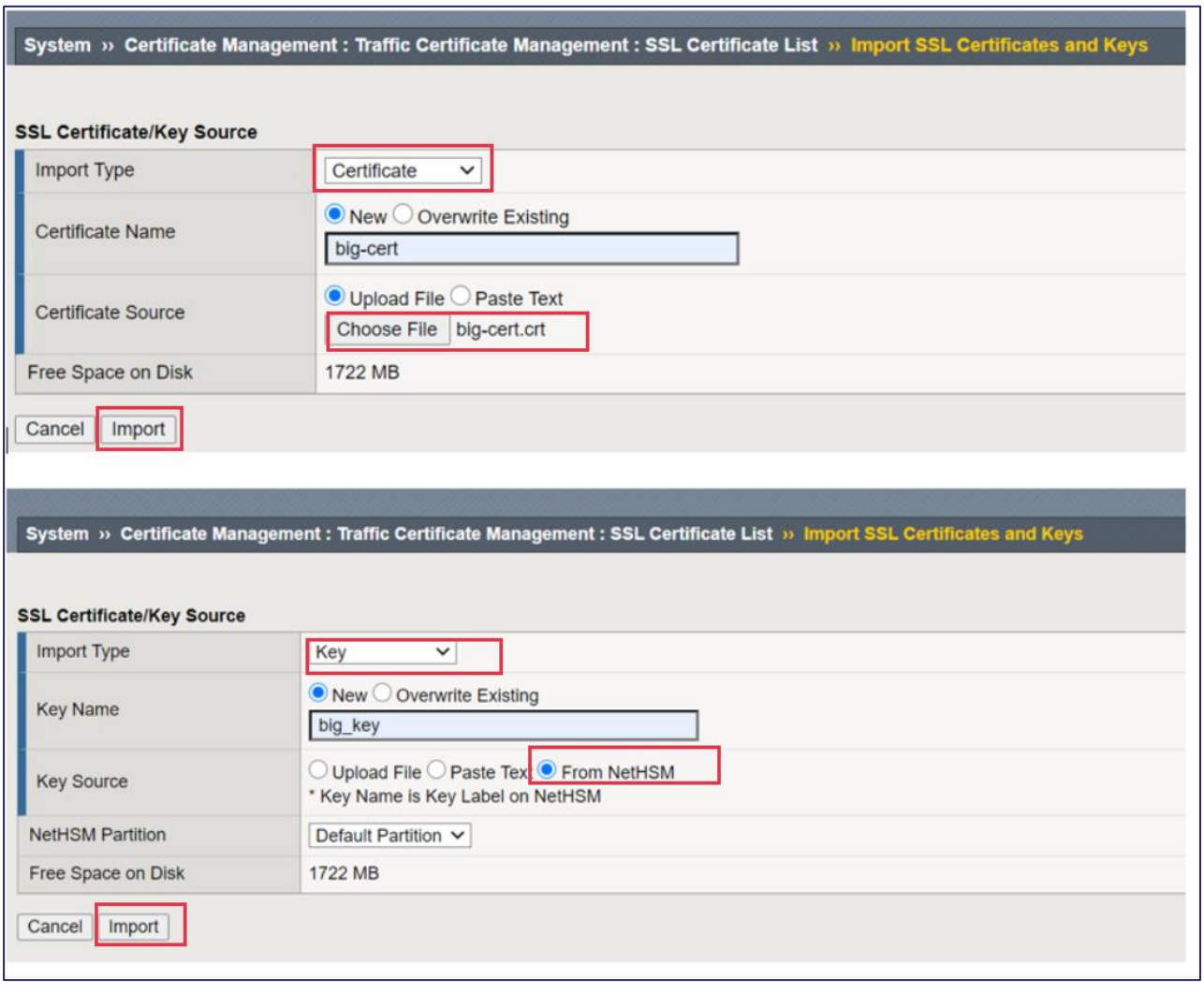

FIGURE 6: IMPORT SSL CERTIFICATE

3. **Create SSL Profile and Attach to Virtual Server:** Finally, create a Client SSL profile and associate it with the virtual server.

a. Log in to the BIG-IP management GUI and navigate to **Local Traffic** --> **Profiles** --> **SSL** --> **CLIENT** --> **+**.

b. Enter a name and select the **Custom** checkbox.

c. In the *Certificate Key Chain* section click **Add**.

d. Select the previously imported certificate and key from the drop-down menus

e. Click **Finished** to create the profile.

f. Navigate to **Local Traffic** --> **Virtual Servers** and select the appropriate virtual server.

g. Under the *SSLProfile (Client)* section select the previously create SSL profile.

h. Click **Update** to save the modified virtual server.

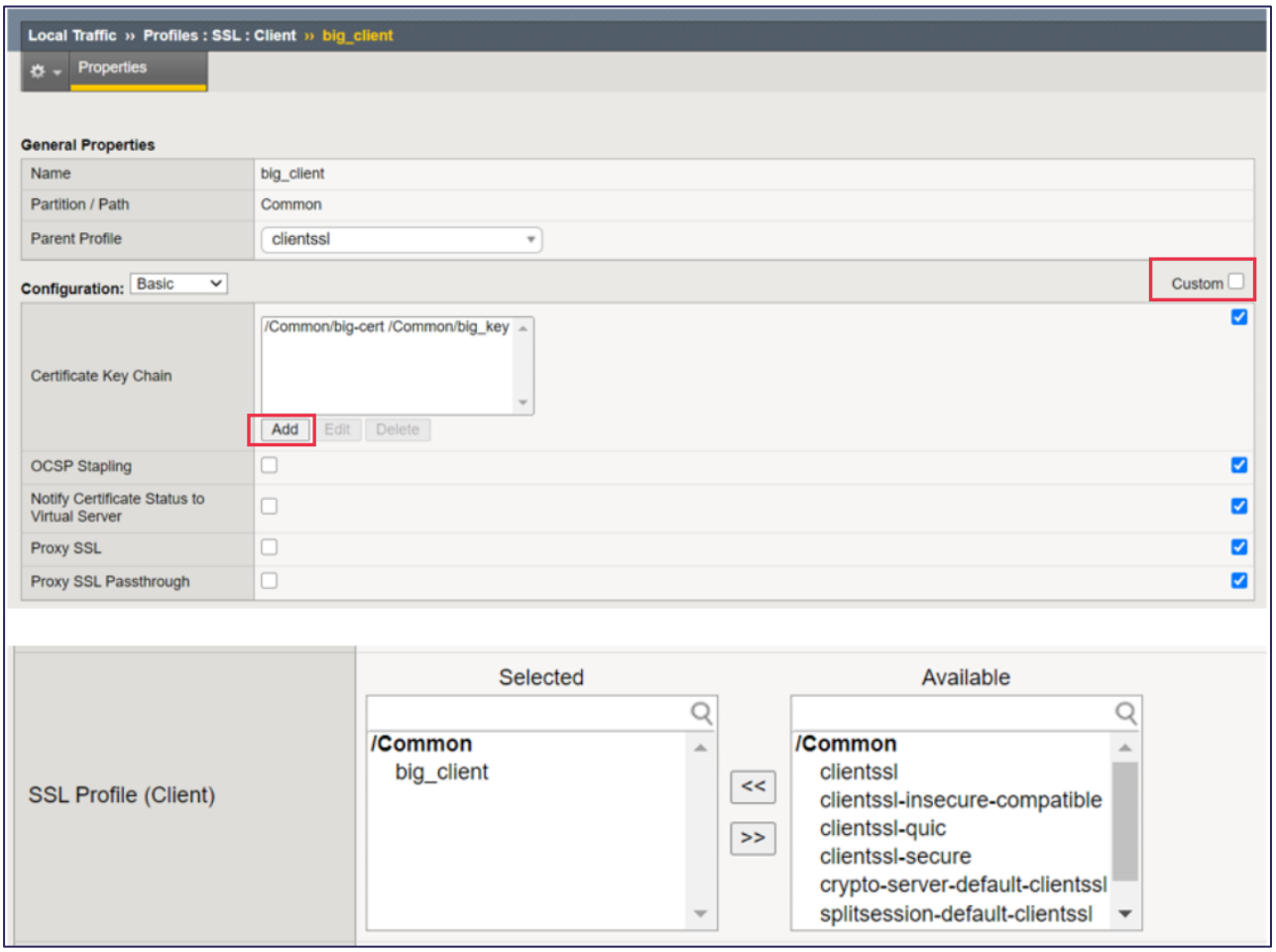

FIGURE 7: CREATE SSL PROFILE

The application is now secured with the BIG-IP offloading the crypto workload to Fortanix DSM.

4.0 DOCUMENT INFORMATION

4.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/360054219072-Using-Fortanix-Self-Defending-KMS-with-F5-BIG-IP-Virtual-Edition

4.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com