Removing Sensitive Data from BIG-IP® 6900/8900 FIPS Platforms

Removing sensitive data from the internal hardware security module (HSM)

You can remove the sensitive customer data from the hardware security module (HSM) installed in the system before returning it to F5® Networks.

Note: *The HSM cannot be removed from the platform.*

1. Use the Configuration utility to delete all key/certificate pairs.
   a) On the Main tab, click **System** > **File Management** > **SSL Certificate List**.
   This displays the list of certificates installed on the system.
   b) Select the certificates that you want to delete and click **Delete**.

   This removes all `.crt`, `.exp`, and `.key` files from the system.
2. Log on to the command line of the system using an account with root access.
3. Initialize the HSM and reconfigure it using fictitious data.
   `run util fips-util -f init`

   Important: *This deletes all keys and makes any previously exported keys unusable.*

   a) When prompted, type a security officer (SO) password.

```
NFB Initialization Process

WARNING - all private keys in NFB will be erased after SO password is
entered!
Any configuration objects dependent on FIPS keys will cause the
configuration fail to load.
Passwords must be at least 7 characters in length.
Enter no password if you instead wish to cancel.

New SO Password:
Re-enter new SO Password:
```

   b) When this message displays, type a security domain name.

```
Initializing NFB...
The security domain name must be the same on all FIPS machines.
Please enter your security domain name:
```

   When the initialization process completes successfully, this message displays: `The FIPS device has been initialized.`