BIG-IP® System and SafeNet Luna SA HSM: Implementation

Version 13.1

Table of Contents

Implementing the SafeNet Luna HSM with BIG-IP Systems

Overview: Setting up the SafeNet Luna SA HSM with BIG-IP systems, using a script

The SafeNet Luna SA HSM is an external hardware security module that is available for use with BIG-IP® systems. Because it is network-based, you can use the SafeNet solution with all BIG-IP platforms, including VIPRION® Series chassis and appliances and BIG-IP Virtual Edition (VE). You can also configure multiple HSMs as an HA (high availability) group to use with BIG-IP systems.

Note: *The BIG-IP system, when in appliance mode, does not support the SafeNet SA HSM installation/uninstallation.*

Only RSA-based cipher suites use the network HSM. After installation on the BIG-IP system, the SafeNet Luna SA HSM is compatible with Access Policy Manager® and Application Security Manager™, without additional configuration steps.

For information about using the iControl® interface to configure the Luna SA HSM with BIG-IP systems, consult the F5 DevCentral site (`https://devcentral.f5.com/icontrol/`).

For additional information about using the Luna SA HSM, contact SafeNet Technical Support (`http://www.safenet-inc.com/technical-support/`).

Prerequisites for setting up SafeNet Luna SA HSM with BIG-IP systems

Before you can use SafeNet Luna SA HSM with the BIG-IP® system, you must make sure that:

- The SafeNet device is installed on your network.
- The SafeNet device and the BIG-IP system can communicate with each other.
- The SafeNet device has a virtual HSM (HSM Partition) defined before you install the client software on the BIG-IP system.
- The BIG-IP system is licensed for external interface and network HSM.

Additionally, before you begin the installation process, make sure that you have access to:

- The Luna SA Client software. See the *Interoperability Matrix for BIG-IP TMOS with SafeNet Clients and HSM* supplemental document available on AskF5 for supported SafeNet client and HSM versions with BIG-IP TMOS versions information.
- The Luna SA Customer Documentation.

Note: *If you install the Luna SA HSM (external HSM) on a system with a FIPS card (internal HSM) installed, the Luna SA HSM takes precedence. You cannot use the SafeNet Luna SA HSM on a BIG-IP system that is running another external HSM.*

Note: *BIG-IP TMOS with SafeNet Luna SA HSM only supports IPv4.*

Task summary

The implementation process involves preparation of the SafeNet device and the BIG-IP® system, followed by key/certificate management and creation of a client SSL profile to use the key and certificate. You can generate SafeNet HSM protected keys and corresponding CSR and certificate using either `tmsh` (recommended) or the `fipskey.nethsm` utility (deprecated).

Task list

Preparing to install the Luna SA client on the BIG-IP system

Before you can set up the SafeNet Luna SA client software on a BIG-IP® system, you must obtain a valid SafeNet Luna SA client license.

To use the Luna SA HSM, you need to obtain the software tarball from SafeNet, and install the Luna SA client software onto the BIG-IP system.

1. Log in to the SafeNet Support portal.
   `https://serviceportal.safenet-inc.com`
2. Download the appropriate document, using the download password `F5Clientdownload!`.

   Note: *For supported SafeNet client and HSM versions with BIG-IP TMOS versions information, see the Interoperability Matrix for BIG-IP TMOS with SafeNet Clients and HSM supplemental document available on AskF5.*
3. Log in to the command-line interface of the BIG-IP system using an account with administrator privileges.
4. Create a directory under `/shared` named `safenet_install`.
   ```
   mkdir /shared/safenet_install
   ```
5. Copy the software tarball to `/shared/safenet_install`

Installing and registering the Luna SA client

You install and register the Luna SA client so that you can use the Luna SA device with the BIG-IP® system. You provide the passwords for your Luna SA device during the installation process. If you are setting up the Luna SA client on a VIPRION® system, you run the configuration script only on the primary blade, and then the system propagates the configuration to the additional active blades.

1. Log in to the command-line interface of the system using administrator privileges.
2. If you are installing the Luna SA client on a VIPRION system, and you are using the management network to connect to the HSM, disable `ip check` on the HSM. If you are not installing on a VIPRION system, or you are using a self IP address to communicate with the HSM, skip this step.
   ```
   tls ipcheck disable
   service restart ntls
   ```
   This step allows the same certificate to be used from multiple IP addresses, identifying multiple blades.
3. Install and register the Luna SA client on the BIG-IP system, using the parameters indicated.
   `nethsm-safenet-install.sh`
   - Parameters for a typical installation or on the primary blade of a VIPRION system.

```
--hsm_ip_addr=<luna_sa_device_IP_address>
[--image=<Luna_x.x_Client_Software.tar>]
```

The following example sets up the version 6.2 client where the Luna SA device has an IP address of `172.27.13.59`:

```
nethsm-safenet-install.sh --hsm_ip_addr=172.27.13.59 --
image=Luna_6.2_Client_Software.tar
```

Note: *The VIPRION system propagates the configuration to additional active blades, but you need to reload the PATH environment variable on any blades with already-open sessions:* `source ~/.bash_profile`

- Parameters when multiple HSMs are configured as an HA group.

```
--hsm_ip_addr="<SafeNet HSM1_IP_address> <SafeNet HSM2_IP_address>"
--hsm_ha_group=<Label name for the SafeNet HSM HA group>]
[--image=<Luna_x.x_Client_Software.tar>]
```

The following example sets up the version 6.2 client for an HA group named `luna_ha_test` where the Luna SA devices in the group have IP addresses of `10.10.10.100` and `10.10.10.101`:

```
nethsm-safenet-install.sh --hsm_ip_addr="10.10.10.100 10.10.10.101" --
hsm_ha_group=luna_ha_test --image=Luna_6.2_Client_Software.tar
```

Install all components when prompted. During the installation, you will register your client IP address with the SafeNet device and assign the Luna SA client to a previously defined HSM partition. For an HA configuration, this must be the first slot.

Note: *By default, the script sets up the SafeNet Luna SA client software to use 20 threads. To adjust this number, run this command before you restart the* `pkcs11d` *service:* `tmsh sys crypto fips external-hsm num-threads <integer>`*. Changing the number of threads affects performance.*

Setting up the Luna SA client on a newly added or activated blade

After you set up the Luna SA client on the primary blade of a VIPRION® system, the system propagates the configuration to the additional active blades. If you subsequently add a secondary blade, activate a disabled blade, or power-on a powered-off blade, you need to run a script on the new secondary blade.

1. Log in to the command-line interface of the system using an account with administrator privileges.
2. Run this script on any new or re-activated secondary blade:

   ```
   safenet-sync.sh <HSM partition password> -v
   ```
3. If you make the new blade a primary blade before running the synchronization script, you need to run the regular client installation and registration procedure on the new primary blade only.

   ```
   nethsm-safenet-install.sh
   ```

Generating a key/certificate using tmsh

You can use the Traffic Management Shell (`tmsh`) to generate a key and certificate.

1. Log in to the command-line interface of the system using an account with administrator privileges.
2. Open the TMOS Shell (`tmsh`).

   ```
   tmsh
   ```
3. Generate the key.

   ```
   create sys crypto key <key_name> gen-certificate common-name <cert_name>
   security-type nethsm
   ```

This example generates an external HSM key named `test_key` and a certificate named `test_safenet.com` with the security type of `nethsm`:

```
create sys crypto key test_key gen-certificate common-name test_safenet.com
security-type nethsm
```

4. Verify that the key was created.
   `list sys crypto key test_key.key`
   Information about the key displays:

```
sys crypto key test_key.key {
key-id <32-digit string>
key-size 2048
key-type rsa-private
security-type nethsm
}
```

When you generate a key/certificate using `tmsh`, the system creates a HSM private key. It also creates a local key, which points to the HSM key, residing in the HSM.

Creating a self-signed digital certificate

If you are configuring the BIG-IP® system to manage client-side HTTP traffic, you perform this task to create a self-signed certificate to authenticate and secure the client-side HTTP traffic. If you are also configuring the system to manage server-side HTTP traffic, you must repeat this task to create a second self-signed certificate to authenticate and secure the server-side HTTP traffic.

1. On the Main tab, click **System** > **Certificate Management** > **Traffic Certificate Management**. The Traffic Certificate Management screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique name for the SSL certificate.
4. From the **Issuer** list, select **Self**.
5. In the **Common Name** field, type a name.
   This is typically the name of a web site, such as `www.siterequest.com`.
6. In the **Division** field, type your department name.
7. In the **Organization** field, type your company name.
8. In the **Locality** field, type your city name.
9. In the or **State or Province** field, type your state or province name.
10. From the **Country** list, select the name of your country.
11. In the **E-mail Address** field, type your email address.
12. In the **Lifetime** field, type a number of days, or retain the default, **365**.
13. In the **Subject Alternative Name** field, type a name.
    This name is embedded in the certificate for X509 extension purposes.
    By assigning this name, you can protect multiple host names with a single SSL certificate.
14. From the **Security Type** list, select **NetHSM**.
15. From the **Key Type** list, **RSA** is selected as the default key type.
16. From the **Size** list, select a size, in bits.
17. Click **Finished**.

Requesting a certificate from a certificate authority

You perform this task to generate a certificate signing request (CSR) that can then be submitted to a third-party trusted certificate authority (CA).

Note: *F5 Networks recommends that you consult the CA to determine the specific information required for each step in this task.*

1. On the Main tab, click **System** > **Certificate Management** > **Traffic Certificate Management**.
   The Traffic Certificate Management screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique name for the SSL certificate.
4. From the **Issuer** list, select **Certificate Authority**.
5. In the **Common Name** field, type a name.
   This is typically the name of a web site, such as `www.siterequest.com`.
6. In the **Division** field, type your department name.
7. In the **Organization** field, type your company name.
8. In the **Locality** field, type your city name.
9. In the or **State or Province** field, type your state or province name.
10. From the **Country** list, select the name of your country.
11. In the **E-mail Address** field, type your email address.
12. In the **Lifetime** field, type a number of days, or retain the default, **365**.
13. In the **Subject Alternative Name** field, type a name.
    This name is embedded in the certificate for X509 extension purposes.
    By assigning this name, you can protect multiple host names with a single SSL certificate.
14. In the **Challenge Password** field, type a password.
15. In the **Confirm Password** field, re-type the password you typed in the **Challenge Password** field.
16. From the **Security Type** list, select **NetHSM**.
17. From the **Key Type** list, **RSA** is selected as the default key type.
18. From the **Size** list, select a size, in bits.
19. Click **Finished**.
    The Certificate Signing Request screen displays.
20. Do one of the following to download the request into a file on your system.
    - In the **Request Text** field, copy the certificate.
    - For **Request File**, click the button.
21. Follow the instructions on the relevant certificate authority web site for either pasting the copied request or attaching the generated request file.
22. Click **Finished**.
    The Certificate Signing Request screen displays.

The generated certificate signing request is submitted to a trusted certificate authority for signature.

Deleting a key from the BIG-IP

You perform this task to delete an existing key from the BIG-IP.

1. On the Main tab, click **System** > **Certificate Management** > **Traffic Certificate Management**.
   The Traffic Certificate Management screen opens.
2. From the **SSL Certificate List**, select the check box next to the key you wish to delete.
3. Click **Delete**.

The key you selected is deleted from BIG-IP.

Note: *The key stored in NetHSM is not deleted.*

Creating a client SSL profile to use an external HSM key and certificate

After you have added the external HSM key and certificate to the BIG-IP® system configuration, you can use the key and certificate as part of a client SSL profile. This task describes using the browser interface. Alternatively, you can use the Traffic Management Shell (`tmsh`) command-line utility.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a name for the profile.
4. From the **Parent Profile** list, select **clientssl**.
5. From the **Configuration** list, select **Advanced**.
   This selection makes it possible for you to modify additional default settings.
6. For the Configuration area, select the **Custom** check box.
   The settings in the Configuration area become available for modification.
7. Using the **Certificate Key Chain** setting, specify one or more certificate key chains:
   a) From the **Certificate** list, select the name of a certificate that you imported.
   b) From the **Key** list, select the name of the key that you imported.
   c) From the **Chain** list, select the chain that you want to include in the certificate key chain.
   d) Click **Add**.
8. Click **Finished**.

After you have created the client SSL profile, you must assign the profile to a virtual server, so that the virtual server can process SSL traffic according to the specified profile settings.

Additional Information

Upgrading the BIG-IP software when using the SafeNet Luna HSM

After a BIG-IP® system software or hotfix upgrade, you do not need to run the SafeNet Luna SA client setup script. Any local keys and certificates you added to the BIG-IP system configuration before upgrading (using the command `tmsh install sys crypto`) appear in the upgrade partition and can be used. Keys, certificates, and CSRs created using `tmsh` are already part of the BIG-IP system configuration and can be used.

Note: *If you will need keys, certificates, or CSRs that were not added to the BIG-IP system configuration, before you upgrade, copy the files into the `/shared` directory. After the upgrade, copy them back to their appropriate directories in the new partition: `/config/ssl/ssl.key/`, `/config/ssl/ssl.crt`, or `/config/ssl/ssl.csr`.*

---

1. Log in to the command-line interface of the BIG-IP system using an account with administrator privileges.
2. Reinstall the Luna SA client on the BIG-IP system, using the parameters you used when you initially installed and registered it.

   ```
   nethsm-safenet-install.sh
   ```

Uninstalling SafeNet Luna SA components from the BIG-IP system

If you no longer need to use the SafeNet Luna SA HSM on a BIG-IP® system, you should uninstall the files.

1. Log in to the command-line interface of the system using an account with administrator privileges.
2. Uninstall the SafeNet client software and clean up SafeNet directories.

   ```
   nethsm-safenet-install.sh -u [-v]
   ```

nethsm-safenet-install.sh utility options

The `nethsm-safenet-install.sh` utility includes these options:

Option	Description
`-f`	Reinstalls when a connect
`-h`	Displays help.
`-u`	Uninstalls SafeNet softwa
`-v`	Prints verbose output abo
`--hsm_ip_addr=<ip_addr>`	SafeNet Luna SA HSM I space-separated IP addres `hsm_ip_addr="10.10.`
`--hsm_partition_pwd=<password>`	SafeNet HSM partition pa in High Availability (HA)
`--hsm_username=<user_name>`	SafeNet Luna SA HSM u

Option	Description
`--hsm_ha_group=<group_name>`	Name for the SafeNet HS all HSMs in HA must use
`--image=<image_name>`	SafeNet Luna SA tarball t file must be stored on the
`--interface=<interface_name>`	Interface identifier of BIG (eth0). The default is the
`--ip_addr=<client_ip_addr>`	IP address of the BIG-IP
`--num_threads=<threads>`	Indicates the number of th
`--verbose=<level>`	Indicates message verbos indicate verbose output.

Legal Notices

Legal notices

Publication Date

This document was published on November 13, 2017.

Publication Number

MAN-0496-05

Copyright

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