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

Version 11.6

Table of Contents

Legal Notices and Acknowledgments

Legal Notices

Publication Date

This document was published on October 21, 2016.

Publication Number

MAN-0496-01

Copyright

Trademarks

Patents

This product may be protected by one or more patents indicated at:
http://www.f5.com/about/guidelines-policies/patents

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, http://www.and.com.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler (bazsi@balabit.hu), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller (nisse@lysator.liu.se), which is protected under the GNU Public License.

In the following statement, "This software" refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with 386BSD and similar operating systems. "Similar operating systems" includes mainly non-profit oriented systems for research and education, including but not restricted to NetBSD, FreeBSD, Mach (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at http://www.perl.com.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (http://www.rrdtool.com/index.html) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (http://www.nominum.com).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

This product includes Intel QuickAssist kernel module, library, and headers software licensed under the GNU General Public License (GPL).

This product includes software licensed from Gerald Combs (gerald@wireshark.org) under the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or any later version. Copyright ©1998 Gerald Combs.

This product includes software developed by Thomas Williams and Colin Kelley. Copyright ©1986 - 1993, 1998, 2004, 2007

Permission to use, copy, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Permission to modify the software is granted, but not the right to distribute the complete modified source code. Modifications are to be distributed as patches to the released version. Permission to distribute binaries produced by compiling modified sources is granted, provided you

1. distribute the corresponding source modifications from the released version in the form of a patch file along with the binaries,

2. add special version identification to distinguish your version in addition to the base release version number,
3. provide your name and address as the primary contact for the support of your modified version, and
4. retain our contact information in regard to use of the base software.

Permission to distribute the released version of the source code along with corresponding source modifications in the form of a patch file is granted with same provisions 2 through 4 for binary distributions. This software is provided "as is" without express or implied warranty to the extent permitted by applicable law.

This product contains software developed by Google, Inc. Copyright ©2011 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product includes software developed by Jeremy Ashkenas and DocumentCloud, and distributed under the MIT license. Copyright © 2010-2013 Jeremy Ashkenas, DocumentCloud.

This product includes gson software, distributed under the Apache License version 2.0. Copyright © 2008-2011 Google Inc.

This product includes ec2-tools software, copyright © 2008, Amazon Web Services, and licensed under the Amazon Software License. A copy of the License is located at http://aws.amazon.com/asl/ .

This product includes jxrlib software, copyright ©2009 Microsoft Corp. All rights reserved. Distributed under the new BSD license.

This product includes node-uuid software, copyright © 2010-2012, Robert Kieffer, and distributed under the MIT license.

This product includes opencsv software, which is distributed under the Apache 2.0 license.

This product includes owasp-jave-encoder software, copyright © 2014, Jeff Ichnowski, and distributed under the New BSD license.

Setting Up 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 does not support the SafeNet Luna SA HSM in Appliance mode.*

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.

Note: *This implementation describes the steps for using an installation script. If the installation script does not support your network configuration, refer to the procedure for manual setup.*

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 (Version 5.1 or 5.2). For VIPRION® system support or configuring multiple HSMs as an HA group, you must use Version 5.2.
- 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.*

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.

Task list

Preparing to install the Luna SA client on the BIG-IP system
Installing and registering the Luna SA client
Setting up the Luna SA client on a newly added or activated blade
Generating a key/certificate using tmsh
Generating a key/certificate using the fipskey.nethsm utility
Creating a client SSL profile to use an external HSM key and certificate

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!`.
   - LunaSA Client v5.1 for F5, Document Id:DOW3519
   - LunaSA Client v5.2.1-6 for F5, Document Id:DOW3520

   Note: *For supporting the VIPRION® system or configuring multiple HSMs in an HA group, you must use version 5.2.x with this release.*
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 5.2 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_5.2_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 5.2 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_5.2_Client_Software.tar
     ```

   Install all components when prompted. During the installation, you register your client IP address with the SafeNet device and assign the Luna SA client to one previously-defined HSM partition. The BIG-IP system supports using keys only within the first HSM partition/slot assigned to the Luna SA client. Note that HSM partitions are not the same as BIG-IP partitions.

   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 -p <HSM partition password>
```

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 Traffic Management 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 siterequest.key
```

Information about the key displays:

```
sys crypto key siterequest.key {
key-size 2048
key-type rsa-private
security-type nethsm
}
```

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

Generating a key/certificate using the fipskey.nethsm utility

Before you generate a key/certificate, make sure that the SafeNet Luna SA client is running on the BIG-IP® system.

You can use the `fipskey.nethsm` utility to generate private keys and self-signed certificates on the BIG-IP system.

1. Display the available options.

```
fipskey.nethsm --help
```

2. Generate the key, using any options you need.

```
fipskey.nethsm --genkey -o <output_file>
```

This example generates the three files that follow:

```
fipskey.nethsm --genkey -o siterequest
```

- /config/ssl/ssl.key/siterequest.key
- /config/ssl/ssl.csr/siterequest.csr
- /config/ssl/ssl.crt/siterequest.crt

The key is saved in /config/ssl/ssl.key/<*output_file*>.key. The certificate request is saved in /config/ssl/ssl.csr/<*output_file*>.csr. The self-signed certificate is saved in /config/ssl/ssl.crt/<*output_file*>.crt.

After you generate keys and certificates, you need to add the local key to the BIG-IP configuration using tmsh. The local key points to the HSM key, which resides in the HSM.

Adding the SafeNet local key to the BIG-IP system configuration

You can use the Traffic Management Shell (tmsh) to add the SafeNet local key, which was created on the BIG-IP® system when you generated a key/certificate using the fipskey.nethsm utility. The local key points to the HSM key.

1. Log in to the command-line interface of the system using an account with administrator privileges.
2. Open the Traffic Management Shell (tmsh).
   ```
   tmsh
   ```
3. Add the key.
   ```
   install sys crypto key key_object_name>< from-local-file <keyname>
   ```
   This example adds a local key named my_key.key from a local key file stored in the /config/ssl/ssl.key/ directory: `install sys crypto key my_key.key from-local-file /config/ssl/ssl.key/my_key.key`

Adding certificates using tmsh

You can use the Traffic Management Shell (tmsh) to add existing certificates to the BIG-IP® system configuration.

1. Log in to the command-line interface of the system using an account with administrator privileges.
2. Open the Traffic Management Shell (tmsh).
   ```
   tmsh
   ```
3. Add the certificate.
   ```
   install sys crypto cert <cert_object_name> from-local-file <path_to_cert_file>
   ```
   This example loads the certificate named my_key.crt from a local certificate file stored in the /config/ssl/ssl.crt/ directory:
   ```
   install sys crypto cert my_key.crt from-local-file
   /config/ssl/ssl.crt/my_key.crt
   ```

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.

Manually Setting Up the SafeNet Luna HSM with BIG-IP Systems

Overview: Manually setting up the SafeNet Luna SA HSM with BIG-IP systems

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. Typically, you would use the script to set up the SafeNet Luna SA HSM. However, in cases where the installation script does not support your network configuration, you can install one or more HSMs manually. For a VIPRION Series chassis, this procedure would require manual setup on the additional blades.

Note: *The BIG-IP system does not support the SafeNet Luna SA HSM in Appliance mode.*

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 (Version 5.1 or 5.2). For VIPRION® system support or configuring multiple HSMs as an HA group, you must use Version 5.2.
- 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.*

Task summary

The implementation process for a manual installation 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. If you are setting up multiple HSMs configured as an HA group, you repeat a subset of the manual installation steps for each additional HSM, and then create an HA group. You can generate SafeNet HSM protected keys and corresponding CSR and certificate using either `tmsh` (recommended) or the `fipskey.nethsm` utility.

Task list

Preparing to manually 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!`.
   - LunaSA Client v5.1 for F5, Document Id:DOW3519
   - LunaSA Client v5.2.1-6 for F5, Document Id:DOW3520

   Note: *For supporting the VIPRION® system or configuring multiple HSMs as an HA group, you must use version 5.2.x with this release.*
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`.

Manually 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. You can use this procedure to install and register the Luna SA client on the BIG-IP system, either for a single HSM or multiple HSMs configured as an HA group.

1. 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.

2. Untar the image, and place the extracted files into appropriate directories, moving the extracted toolkit to the safenet path.

   ```
   tar -C /shared/safenet_install -xvr /shared/safenet_install/<lunasa tar file>


   mkdir -p /shared/safenet/toolkit
   mv /shared/safenet_install/toolkit/* /shared/safenet/toolkit
   chmod 755 /shared/safenet/toolkit/*
   ```

3. Set the write permission and create softlinks for the `/usr path`.

   ```
   mount -o remount,rw /usr   mkdir -p /shared/safenet/lunasa
   rm -rf /usr/lunasa
   ln -sf /shared/safenet/lunasa /usr/lunasa

   rm -rf /usr/safenet/
   mkdir -p /usr/safenet/
   ln -sf /shared/safenet/lunasa /usr/safenet/lunaclient
   ```

4. Install the SafeNet Luna SA package.

   ```
   sh /shared/safenet_install/linux/x86/64/install.sh
   ```

5. Adjust the location and permission of the `Chrystoki.conf` file

   ```
   mv /etc/Chrystoki.conf /shared/safenet/lunasa/Chrystoki.conf
   restorecon /shared/safenet/lunasa/Chrystoki.conf
   chmod 644 /shared/safenet/lunasa/Chrystoki.conf
   ```

6. Add these entries to the file `/shared/safenet/lunasa/Chrystoki.conf`, if the entries do not already exist:

   ```
   Misc = {
       Apache = 0;
       PE1746Enabled=1;
   }

   EngineLunaCA3 = {
       DisableCheckFinalize = 1;
       DisableEcdsa = 0;
       DisableDsa = 0;
       DisableRand = 0;
       EngineInit = 1:10:11;
       LibPath64 = /usr/lunasa/lib/libCryptoki2_64.so;
       LibPath = /usr/lunasa/lib/libCryptoki2.so;
   }
   ```

7. Set these softlinks:

```
ln -sf /shared/safenet/lunasa/Chrystoki.conf /etc/Chrystoki.conf
ln -sf /shared/safenet/lunasa/lib/libCryptoki2_64.so
/usr/lib/libCryptoki2_64.so
```

8. Fetch the server certificate from the SafeNet Luna SA HSM.

```
scp <hsm_username>@<hsm_ip_addr>:server.pem
/usr/lunasa/bin/server_<hsm_ip_addr>.pem
```

9. Create the client certificate.

```
/usr/lunasa/bin/vtl createCert -n <BIG-IP IP address>
```

10. Send the client certificate to the SafeNet Luna SA HSM.

```
scp /usr/lunasa/cert/client/<BIG-IP IP address>.pem
<hsm_username>@<hsm_ip_addr>:
```

11. Clean up the old server information (if any), and add the server information to the client.

```
/usr/lunasa/bin/vtl deleteServer -n <hsm_ip_addr>
rm -f /usr/lunasa/cert/server/CAFile.pem
rm -f /usr/lunasa/cert/server/<hsm_ip_addr>Cert.pem
```

12. Add the server to the list of servers.

```
/usr/lunasa/bin/vtl addServer -n <hsm_ip_addr> -c
/usr/lunasa/bin/server_<hsm_ip_addr>.pem
```

13. On the SafeNet Luna SA HSM device, register a client name that has the IP address of the BIG-IP system, and assign a partition for the client.

```
lunash:> client register -client <clientname> [-hostname <resolvable
hostname>] [-ip <client IP address>]
lunash:> client assignPartition -client <clientname> -partition
<partitionname>
```

For additional details, refer to the SafeNet documentation.

14. (HA only) If you are setting up multiple HSMs configured as an HA group, repeat these steps for each SafeNet Luna SA HSM device.
    a) Fetch the server certificate from the Safenet Luna SA HSM.

```
scp <hsm_username>@<hsm_ip_addr>:server.pem
/usr/lunasa/bin/server_<hsm_ip_addr>.pem
```

    b) Send the client certificate to the SafeNet Luna SA HSM.

```
scp /usr/lunasa/cert/client/<BIG-IP IP address>.pem
<hsm_username>@<hsm_ip_addr>:
```

c) Clean up the old server information (if any), and add the server information to the client.

```
/usr/lunasa/bin/vtl deleteServer -n <hsm_ip_addr>
rm -f /usr/lunasa/cert/server/<hsm_ip_addr>Cert.pem
```

d) Add the server to the list of servers.

```
/usr/lunasa/bin/vtl addServer -n <hsm_ip_addr> -c
/usr/lunasa/bin/server_<hsm_ip_addr>.pem
```

e) On the SafeNet Luna SA HSM device, register a client name that has the IP address of the BIG-IP system, and assign a partition for the client.

```
lunash:> client register -client <clientname> [-hostname <resolvable
hostname>] [-ip <client IP address>]
lunash:> client assignPartition -client <clientname> -partition
<partitionname>
```

For additional details, refer to the SafeNet documentation.
This example shows the list of slots after the BIG-IP system is securely connected to two SafeNet Luna SA HSMs.

```
[root@test:Active:Standalone] shared # vtl listSlots
Number of slots: 5

The following slots were found:

Slot #    Description          Label                            Serial #
  Status
========= ==================== ================================ ==========
 ============
slot #1   LunaNet Slot         test1                            153124004
  Present
slot #2   LunaNet Slot         test1                            153560010
  Present
slot #3    -                    -                                 -
  Not present
slot #4    -                    -                                 -
  Not present
slot #5    -                    -                                 -
  Not present
```

15. (HA only) If you are setting up multiple HSMs configured as an HA group, after you have securely connected all the SafeNet Luna SA HSMs, create an HA group, and add all the HSMs into the group. These commands use serial numbers from the previous example.

```
/usr/lunasa/bin/vtl haAdmin newGroup -serialNum 153124004 -label ha1

/usr/lunasa/bin/vtl haAdmin addMember -group ha1 -serialNum 153560010

/usr/lunasa/bin/vtl haAdmin HAOnly -enable
```

16. (HA only) Verify that the HA group configuration was successful.

```
/usr/lunasa/bin/vtl listSlots
```

17. Close and open the session for the SafeNet Luna SA HSM in slot #1.

```
/shared/safenet/toolkit/sautil -v -s 1 -i 10:11 -c
/shared/safenet/toolkit/sautil -v -s 1 -i 10:11 -o -p <hsm_partition_password>
```

18. Install the `pkcs11d` service on the BIG-IP system.

```
bigstart add pkcs11d
bigstart stop pkcs11d
bigstart add --default pkcs11d
```

19. Revert the read-write permission.
    `mount -o remount,ro /usr`
20. Set the vendor name to SafeNet.
    `fipskey.nethsm --hsm=Safenet`
21. Configure the vendor name and partition password in `tmsh`.

```
tmsh create sys crypto fips external-hsm vendor safenet password <Safenet
partition password>
```

22. To adjust the number of threads, you can modify the configuration, as shown.
    `tmsh modify sys crypto fips external-hsm num-threads <integer>`
    The default value for the number of threads is 20.
23. Restart the daemons.
    a) Restart the `pkcs11d` service.
       `bigstart restart pkcs11d`
    b) Restart `tmm`.
       `bigstart restart tmm`

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 Traffic Management 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 siterequest.key`

Information about the key displays:

```
sys crypto key siterequest.key {
key-size 2048
key-type rsa-private
security-type nethsm
}
```

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

Generating a key/certificate using the fipskey.nethsm utility

Before you generate a key/certificate, make sure that the SafeNet Luna SA client is running on the BIG-IP® system.

You can use the `fipskey.nethsm` utility to generate private keys and self-signed certificates on the BIG-IP system.

1. Display the available options.
   ```
   fipskey.nethsm --help
   ```
2. Generate the key, using any options you need.
   ```
   fipskey.nethsm --genkey -o <output_file>
   ```
   This example generates the three files that follow:
   ```
   fipskey.nethsm --genkey -o siterequest
   ```
   - `/config/ssl/ssl.key/siterequest.key`
   - `/config/ssl/ssl.csr/siterequest.csr`
   - `/config/ssl/ssl.crt/siterequest.crt`

   The key is saved in `/config/ssl/ssl.key/<output_file>.key`. The certificate request is saved in `/config/ssl/ssl.csr/<output_file>.csr`. The self-signed certificate is saved in `/config/ssl/ssl.crt/<output_file>.crt`.

After you generate keys and certificates, you need to add the local key to the BIG-IP configuration using `tmsh`. The local key points to the HSM key, which resides in the HSM.

Adding the SafeNet local key to the BIG-IP system configuration

You can use the Traffic Management Shell (`tmsh`) to add the SafeNet local key, which was created on the BIG-IP® system when you generated a key/certificate using the `fipskey.nethsm` utility. The local key points to the HSM key.

1. Log in to the command-line interface of the system using an account with administrator privileges.
2. Open the Traffic Management Shell (`tmsh`).
   ```
   tmsh
   ```
3. Add the key.
   ```
   install sys crypto key key_object_name>< from-local-file <keyname>
   ```

This example adds a local key named `my_key.key` from a local key file stored in the `/config/ssl/ssl.key/` directory: `install sys crypto key my_key.key from-local-file /config/ssl/ssl.key/my_key.key`

Adding certificates using tmsh

You can use the Traffic Management Shell (`tmsh`) to add existing certificates to the BIG-IP® system configuration.

1. Log in to the command-line interface of the system using an account with administrator privileges.
2. Open the Traffic Management Shell (`tmsh`).
   `tmsh`
3. Add the certificate.
   `install sys crypto cert <cert_object_name> from-local-file <path_to_cert_file>`

   This example loads the certificate named `my_key.crt` from a local certificate file stored in the `/config/ssl/ssl.crt/` directory:

   ```
   install sys crypto cert my_key.crt from-local-file
   /config/ssl/ssl.crt/my_key.crt
   ```

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 must run the SafeNet Luna SA client setup script to restore your default SafeNet configuration. 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, but they are usable only after you run the SafeNet Luna SA client setup script. Keys, certificates, and CSRs created using `tmsh` are already part of the BIG-IP system configuration, and can be used after running the SafeNet script. If you are restoring the Luna SA client on a VIPRION® system, you run the script only on the primary blade, and then the system propagates the configuration to the additional active blades.

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`	Force reinstall when a connection with the HSM already exists.
`-h`	Display help

Option	Description
-u	Uninstall the SafeNet client software and clean up SafeNet directories
-v	Verbose output
--hsm_ip_addr=<ip_addr>	SafeNet Luna SA HSM IP address(s). For multiple HSMs, use a double-quoted value with space-separated IP addresses.
--hsm_partition_pwd=<password>	SafeNet Luna SA HSM user name. Default is admin.
--hsm_username=<user_name>	SafeNet Luna SA HSM user name. Default is admin. For multiple HSMs with different user names, use a double-quoted value with space-separated user names in the same order as the corresponding HSM IP address list.
--hsm_ha_group=<group name>	Name for the SafeNet HSM HA group, when you are using multiple HSMs in an HA configuration. All HSMs in the HA group must use the same partition password.
--interface=<interface_name>	BIG-IP system interface used to communicate with the SafeNet Luna SA HSM. Default is the management interface.
--ip_addr=<client_ip_addr>	IP address of the BIG-IP system, as seen by the SafeNet Luna SA HSM
--image=<image_name>	SafeNet Luna SA tarball to be installed (for example, Luna_5.2_Client_Software.tar). This file must be stored on the BIG-IP system in /shared/safenet_install.

Index