



Network Hardware Security Module (HSM)

Feature Description

UPDATED: 09 January 2019



Copyright Notices

Copyright © 2002-2018 KEMP Technologies, Inc. All rights reserved. KEMP Technologies and the KEMP Technologies logo are registered trademarks of KEMP Technologies, Inc.

KEMP Technologies, Inc. reserves all ownership rights for the LoadMaster and KEMP 360 product line including software and documentation.

Used, under license, U.S. Patent Nos. 6,473,802, 6,374,300, 8,392,563, 8,103,770, 7,831,712, 7,606,912, 7,346,695, 7,287,084 and 6,970,933



Table of Contents

1 Introduction	4
1.1 Prerequisites	5
1.2 Document Purpose	6
1.3 Intended Audience	6
2 Configure the LoadMaster and the HSM	7
2.1 SafeNet HSM Steps	7
2.1.1 Download the CA Certificate from the HSM	7
2.1.2 Configure the LoadMaster	7
2.1.3 Configure the HSM	8
2.1.4 Enable HSM in the LoadMaster	9
2.2 Cavium HSM	10
2.2.1 Configure the LoadMaster	10
2.2.2 Configure the HSM	10
2.2.3 Enable HSM in the LoadMaster	11
2.3 Generate a Certificate Signing Request (CSR)	11
2.4 Import the CA Certificate and Assign it to a Virtual Service	12
3 Troubleshooting	13
3.1 Connection Lost Between the LoadMaster and the HSM	13
3.2 The LoadMaster Cannot Connect to the HSM	13
3.2.1 Ping the HSM	13
References	15
Last Updated Date	16

1 Introduction

A Hardware Security Module (HSM) is a physical device that provides a secure environment for the storage of cryptographic keys and for performing operations using these keys. The HSM provides physical protection using tamper evidence and tamper protection mechanisms and by providing a secure out-of-band management interface for key material.

HSMs act as trust anchors that protect the cryptographic infrastructure of some of the most security-conscious organizations in the world by securely managing, processing and storing cryptographic keys inside a hardened, tamper-resistant device.

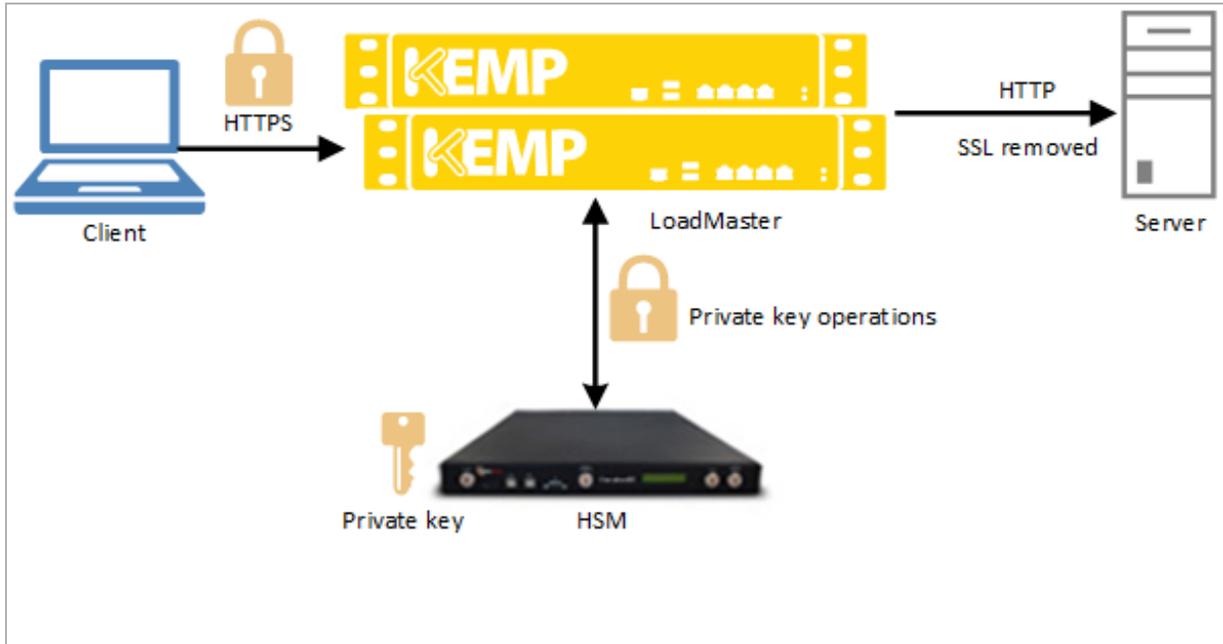
HSMs provide protection for transactions, identities and applications by securing cryptographic keys and provisioning encryption, decryption, authentication and digital signing services for a wide range of applications.

HSMs allow organisations to improve profitability and achieve compliance with solutions for paper-to-digital initiatives, Payment Card Industry (PCI) Data Security Standard (DSS), digital signatures, Domain Name System Security extensions (DNSSEC), hardware key storage, transactional acceleration, certificate signing, code/document signing, bulk key generation, data encryption and more.

The functions of a HSM are:

- On-board, secure cryptographic key generation
- On-board, secure cryptographic key storage and management
- Use of cryptographic and sensitive data material
- Offloading application servers for complete asymmetric and symmetric cryptography

A HSM is a third party product which works with the LoadMaster.



By default in the KEMP LoadMaster - all SSL handling is performed by the LoadMaster itself.

For more information about the default SSL handling, refer to the **SSL Accelerated Services, Feature Description**.

However, the LoadMaster can also be configured to connect to and work with an external network HSM device which will take care of the SSL transactions and certificate management and provides additional security.

The traffic flow as outlined in the diagram above, is as follows:

1. The client connects to the LoadMaster which presents a certificate as part of the SSL server “hello” handshake. This certificate contains the public key corresponding to the private key stored on the HSM.
2. The client provides the LoadMaster with the SSL “Pre-master Secret” which has been encrypted by the client using the public key from the certificate.
3. The LoadMaster passes the “Pre-master Secret” to the HSM for decryption.
4. Both client and server compute a new Transport Layer Security (TLS) session key using the “Pre-master Secret”. The HSM is not involved in this.

1.1 Prerequisites

The following prerequisites must be in place before the steps in this document should be attempted:

- The LoadMaster must be licensed and configured as needed.
- The HSM device and partition must be set up and configured as per the HSM vendor documentation.
- **Important:** Proximity to the LoadMaster is a key item that network architects should consider when designing their network to include the LoadMaster and HSM. Ideally, the LoadMaster and the HSM should be as close as possible to ensure the lowest latency and highest security.

1.2 Document Purpose

The purpose of this document is to outline how to configure the KEMP LoadMaster to effectively work with a HSM.

1.3 Intended Audience

This document is intended to be used by anyone who is interested in finding out how to configure the LoadMaster to work effectively with a HSM device. Knowledge of the HSM device is also required, particularly in relation to setup, configuration and administration.

2 Configure the LoadMaster and the HSM

The LoadMaster supports two network HSM devices:

- SafeNet HSM
- Cavium HSM (beta support)

The steps to configure the LoadMaster and HSM are similar, but some steps are not relevant for Cavium HSM. Refer to the relevant section below for steps on how to connect the HSM with the LoadMaster and configure the relevant settings as needed.

For further information on any of the HSM-specific steps, please refer to the relevant HSM vendor documentation.

2.1 SafeNet HSM Steps

Follow the steps in the sections below to configure the SafeNet HSM and the LoadMaster.

2.1.1 Download the CA Certificate from the HSM

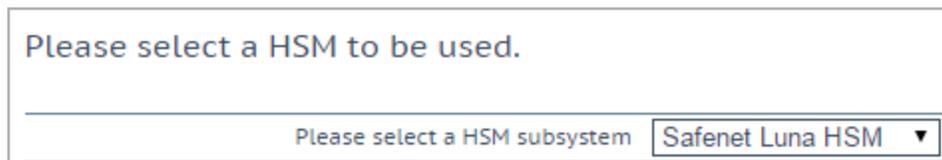
Before configuring the LoadMaster, the Certificate Authority (CA) certificate must be downloaded from the HSM. For instructions on how to do this, please refer to the HSM vendor documentation.

The CA certificate will later be uploaded to the LoadMaster to set up the secure connection between the HSM and the LoadMaster.

2.1.2 Configure the LoadMaster

To configure the LoadMaster, follow the steps below in the Web User Interface (WUI):

1. In the main menu, go to **Certificates & Security > HSM Configuration**.



Please select a HSM to be used.

Please select a HSM subsystem **Safenet Luna HSM** ▼

2. Select **Safenet Luna HSM**.

Safenet HSM Configuration

Address of the Safenet HSM	<input type="text" value="10.11.0.14"/>	<input type="button" value="Set Address"/>
Upload the CA certificate	<input type="button" value="Choose File"/> No file chosen	<input type="button" value="Upload CA certificate"/>
Generate the HSM Client Certificate	<input type="text" value="test1"/>	<input type="button" value="Generate Client Cert"/>
Password for the HSM partition	<input type="password" value="....."/>	<input type="button" value="Set the HSM Password"/>
Enable Safenet HSM	<input type="checkbox"/>	

3. Enter the IP address of the SafeNet HSM unit to be used and click **Set Address**.

4. To upload the CA certificate, click **Choose File**.

5. Browse to and select the relevant certificate that has been downloaded from the HSM in the **Download the CA Certificate from the HSM** section.

6. Enter the LoadMaster FQDN name in the **Generate the HSM Client Certificate** text box and click **Generate Client Cert**.

The client certificate (which will be downloaded) will be given the name which was entered in the Client Certificate text box, that is, **<HSMClientCertificateName>.pem** (test1.pem in our example).

This generates the client certificate that will be uploaded to the HSM. The name specified here should be used when setting up the connection on the HSM device, which is referred to in the **Configure the HSM** section.

7. Enter the Password for the HSM partition and click the Set the HSM Password button.

The HSM partition password would have been set on the HSM when originally configuring the partition. For further information, please consult the HSM vendor documentation.

If any of the fields are configured incorrectly, an error message is displayed such as "Configuration incorrect or network problems". The error message also lists the possible reason for the problem.

Before enabling HSM on the LoadMaster, the client certificate must be uploaded to the HSM and the LoadMaster must be registered as a client on the HSM, otherwise the LoadMaster will not be able to communicate with the HSM module. Follow the steps in the **Configure the HSM** section to do this.

2.1.3 Configure the HSM

To configure the HSM to work with the LoadMaster, follow the steps below:

These steps vary depending upon the type of HSM device. For step-by-step instructions on how to perform the steps below, please refer to the relevant vendor HSM documentation.

1. Upload the client certificate to the HSM.

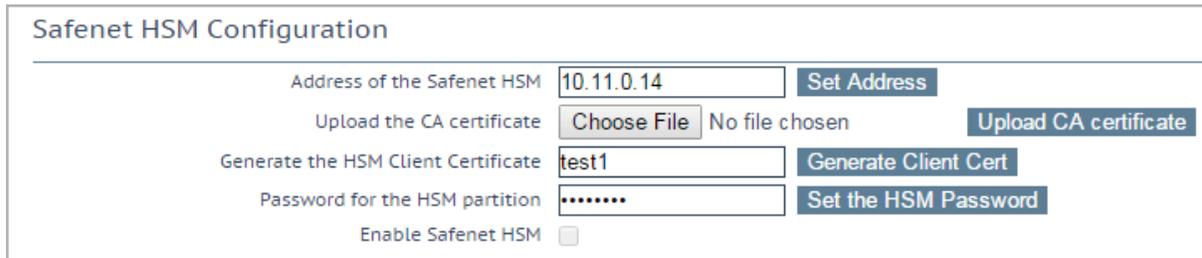
This is the client certificate that was generated in the LoadMaster in the **Configure the HSM** section.

2. Register the LoadMaster as a client on the HSM device.
3. Assign the partition where the private keys that the LoadMaster will use are located.
4. If the LoadMaster's IP address is not in DNS, an entry may be required to resolve the client name to the IP address.

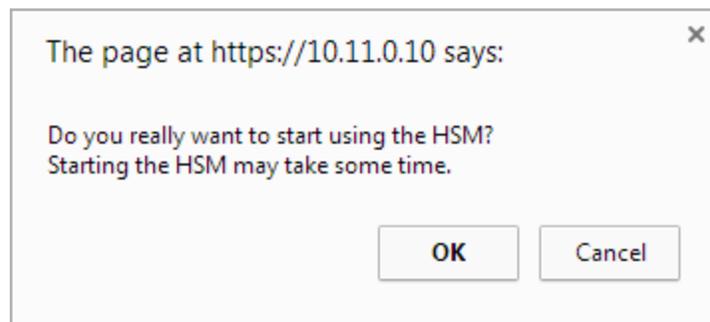
2.1.4 Enable HSM in the LoadMaster

To enable HSM in the LoadMaster, follow the steps below in the LoadMaster WUI:

1. In the main menu, go to **Certificates & Security > HSM Configuration**.



2. Select the **Enable Safenet HSM** check box.



3. Click **OK**.

If there are any problems with the connection an error will be displayed.

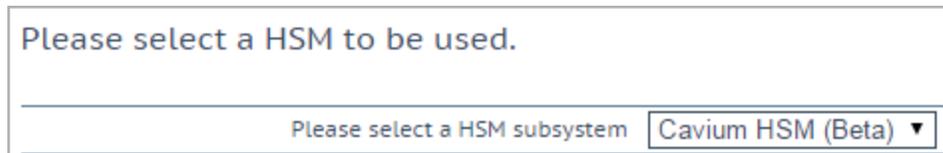
2.2 Cavium HSM

Follow the steps in the sections below to configure the Cavium HSM and the LoadMaster.

2.2.1 Configure the LoadMaster

To configure the LoadMaster, follow the steps below in the Web User Interface (WUI):

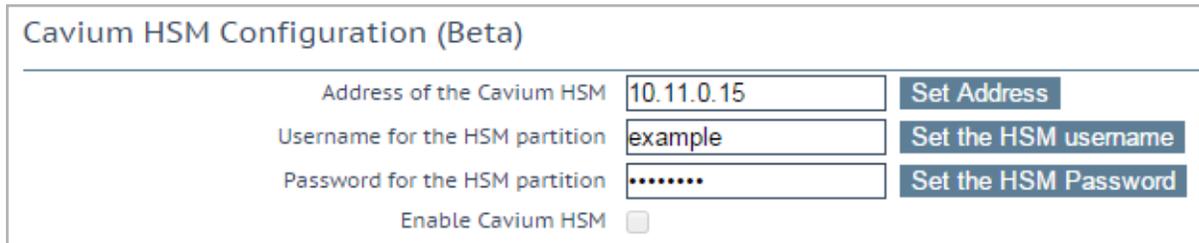
1. In the main menu, go to **Certificates & Security > HSM Configuration**.



Please select a HSM to be used.

Please select a HSM subsystem Cavium HSM (Beta) ▾

2. Select **Cavium HSM**.



Cavium HSM Configuration (Beta)

Address of the Cavium HSM	<input type="text" value="10.11.0.15"/>	Set Address
Username for the HSM partition	<input type="text" value="example"/>	Set the HSM username
Password for the HSM partition	<input type="password" value="....."/>	Set the HSM Password
Enable Cavium HSM	<input type="checkbox"/>	

3. Enter the IP address of the Cavium HSM unit to be used and click **Set Address**.
4. Enter the **Username** for the HSM partition and click **Set the HSM username**.
5. Enter the **Password** for the HSM partition and click the **Set the HSM Password** button.

The HSM partition password would have been set on the HSM when originally configuring the partition. For further information, please consult the HSM vendor documentation.

2.2.2 Configure the HSM

To configure the HSM to work with the LoadMaster, follow the steps below:

These steps vary depending upon the type of HSM device. For step-by-step instructions on how to perform the steps below, please refer to the relevant vendor HSM documentation.

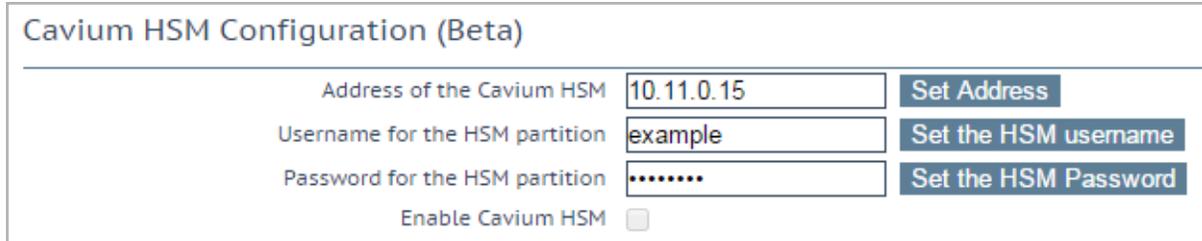
1. Register the LoadMaster as a client on the HSM device.
2. Assign the partition where the private keys that the LoadMaster will use are located.

3. If the LoadMaster's IP address is not in DNS, an entry may be required to resolve the client name to the IP address.

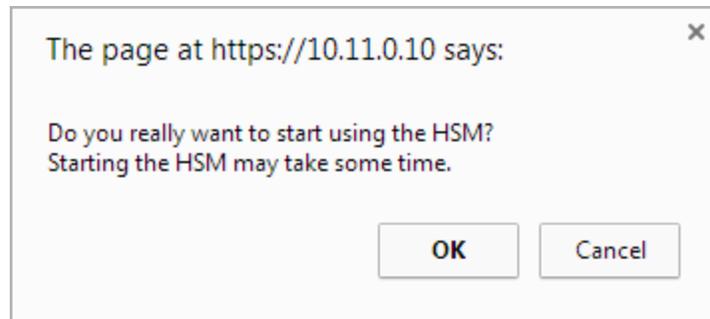
2.2.3 Enable HSM in the LoadMaster

To enable HSM in the LoadMaster, follow the steps below in the LoadMaster WUI:

1. In the main menu, go to **Certificates & Security > HSM Configuration**.



2. Select the **Enable Cavium HSM** check box.



3. Click **OK**.

If there are any problems with the connection an error will be displayed.

2.3 Generate a Certificate Signing Request (CSR)

Follow the steps below to generate a CSR:

In the main menu of the LoadMaster WUI, select **Certificates & Security > SSL Certificates**.

1. Enter a recognizable name in the **Private Key Identifier** text box.

2. Click **Generate CSR**.

2 Letter Country Code (ex. US)	<input type="text"/>
State/Province (Full Name - New York, not NY)	<input type="text"/>
City	<input type="text"/>
Company	<input type="text"/>
Organization (e.g., Marketing,Finance,Sales)	<input type="text"/>
Common Name (The FQDN of your web server)	<input type="text"/>
Email Address	<input type="text"/>
SAN/UCC Names	<input type="text"/>

3. Fill in the information and click **Create CSR**.

The CSR request will be generated from the HSM. As a result of this, the certificate issued by the CA can only be decrypted from the private key that sits in the HSM.

4. Copy the text and provide it to your Certificate Authority (CA) who will issue the certificate.

2.4 Import the CA Certificate and Assign it to a Virtual Service

When the CA provides the certificate, follow the steps below to import it into the LoadMaster and assign it to a Virtual Service:

1. In the main menu of the LoadMaster WUI go to **Certificates & Security > SSL Certificates**.
2. Click **Import Certificate**.
3. Click **Choose File**.
4. Browse to and select the relevant certificate file.
5. To assign the certificate to a Virtual Service, select the Virtual Service IP address in the **Available VSs** box in the **Assignment** section.
6. Click the right arrow.
7. Click **Save Changes**.

3 Troubleshooting

Refer to the sections below for some troubleshooting advice relating to common problems.

3.1 Connection Lost Between the LoadMaster and the HSM

A health check is performed every minute. If connection to the HSM is lost for any reason, an error message will be displayed on the home page of the LoadMaster WUI. This error message will say **ERROR: Connection to the HSM Lost. Please rectify and then restart the HSM.** Please be aware that the LoadMaster will not automatically re-enable the HSM connection. To re-enable the HSM connection, go to **Certificates & Security > HSM Configuration** and tick the enable HSM check box.

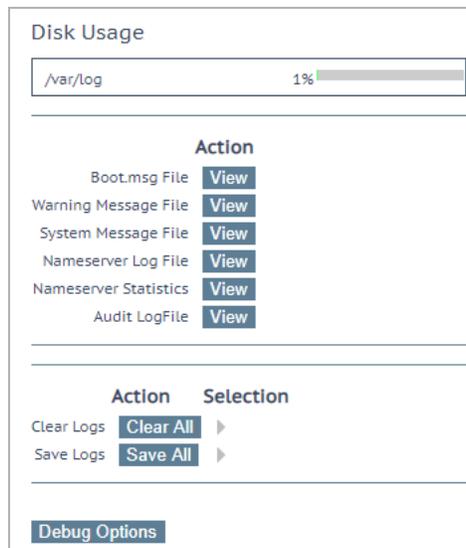
3.2 The LoadMaster Cannot Connect to the HSM

If the LoadMaster cannot connect to the HSM after all of the configuration steps in this document have been carried out, refer to the sections below for some troubleshooting steps.

3.2.1 Ping the HSM

To check if the LoadMaster can communicate with the HSM, try to ping the HSM from the LoadMaster. To do this, follow the steps below in the LoadMaster WUI:

1. Go to **System Configuration > Logging Options > System Log Files.**



2. Click **Debug Options.**

Debug Options

Disable All Transparency	Disable Transparency
Enable L7 Debug Traces	Enable Traces
Enable Extended L7 Debug	Enable Extended Debug
Perform an l7adm	l7adm
Enable WAF Debug Logging	Enable Logging
Enable IRQ Balance	Enable IRQ Balance
Enable TSO	Enable TSO
Enable Bind Debug Traces	Enable Bind Traces
Perform a PS	ps
Perform Top	top Iterations <input type="text" value="10"/> Interval <input type="text" value="1"/> sec <input type="checkbox"/> Show Threads <input type="checkbox"/> Sort by Memory usage
Include Top in Backups	<input type="checkbox"/>
Display Meminfo	Meminfo
Display Slabinfo	Slabinfo
Perform an Ifconfig	Ifconfig
Perform a Netstat	Netstat
Include Netstat in Backups	<input checked="" type="checkbox"/>
Reset Statistic Counters	Reset Statistics
Flush OCSPPD Cache	Flush Cache
Enable SSOMGR Debug Traces	Enable Traces
Flush SSO Authentication Cache	Flush SSO Cache
SSO LDAP server timeout	<input type="text" value="5"/> Set Timeout
Linear SSO Logfiles	<input type="checkbox"/>
Start IPsec IKE Daemon	Start IPsec IKE Daemon
Perform an IPsec Status	IPsec Status
Enable IKE Debug Level Logs	Enable Logs
Netconsole Host	<input type="text"/> Interface <input type="text" value="eth0"/> Set Netconsole Host
Ping Host	<input type="text"/> Interface <input type="text" value="eth0"/> Ping
Ping6 Host	<input type="text"/> Interface <input type="text" value="Automatic"/> Ping6
Traceroute Host	<input type="text"/> Traceroute
Kill LoadMaster (415805)	<input type="text"/> Kill LoadMaster

3. In the **Ping Host** text box, enter the IP address of the HSM.

4. Select the relevant **Interface**.

The **Automatic** option selects the correct interface to ping an address on a particular network.

5. Click **Ping**.

```
Results:
PING 10.154.11.70 (10.154.11.70) from 10.154.11.70 eth0: 56(84) bytes of data.
64 bytes from 10.154.11.70: icmp_seq=1 ttl=64 time=0.125 ms
64 bytes from 10.154.11.70: icmp_seq=2 ttl=64 time=0.097 ms
64 bytes from 10.154.11.70: icmp_seq=3 ttl=64 time=0.093 ms

--- 10.154.11.70 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.093/0.105/0.125/0.014 ms
```

The results of the ping will be displayed.



References

Unless otherwise specified, the following documents can be found at <http://kemptechnologies.com/documentation>.

SSL Accelerated Services, Feature Description



Last Updated Date

This document was last updated on 09 January 2019.