Hardware Security Module (HSM)
Feature Description

VERSION: 1.3
UPDATED: APRIL 2015
Copyright Notices

Copyright © 2002-2015 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 product line including software and documentation. The use of the LoadMaster Exchange appliance is subject to the license agreement. Information in this guide may be modified at any time without prior notice.

Microsoft Windows is a registered trademark of Microsoft Corporation in the United States and other countries. All other trademarks and service marks are the property of their respective owners.

Limitations: This document and all of its contents are provided as-is. KEMP Technologies has made efforts to ensure that the information presented herein are correct, but makes no warranty, express or implied, about the accuracy of this information. If any material errors or inaccuracies should occur in this document, KEMP Technologies will, if feasible, furnish appropriate correctional notices which Users will accept as the sole and exclusive remedy at law or in equity. Users of the information in this document acknowledge that KEMP Technologies cannot be held liable for any loss, injury or damage of any kind, present or prospective, including without limitation any direct, special, incidental or consequential damages (including without limitation lost profits and loss of damage to goodwill) whether suffered by recipient or third party or from any action or inaction whether or not negligent, in the compiling or in delivering or communicating or publishing this document.

Any Internet Protocol (IP) addresses, phone numbers or other data that may resemble actual contact information used in this document are not intended to be actual addresses, phone numbers or contact information. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual addressing or contact information in illustrative content is unintentional and coincidental.

Portions of this software are; copyright (c) 2004-2006 Frank Denis. All rights reserved; copyright (c) 2002 Michael Shalayeff. All rights reserved; copyright (c) 2003 Ryan McBride. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE ABOVE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the above copyright holders..

Portions of the LoadMaster software are copyright (C) 1989, 1991 Free Software Foundation, Inc. -51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA- and KEMP Technologies Inc. is in full compliance of the GNU license requirements, Version 2, June 1991. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Portions of this software are Copyright (C) 1988, Regents of the University of California. All rights reserved.
Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions of this software are Copyright (C) 1995-2004, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Portions of this software are Copyright (C) 2003, Internet Systems Consortium

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

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 ............................................................................................................................... 5
  1.1 Prerequisites ......................................................................................................................... 6
  1.2 Document Purpose ............................................................................................................... 6
  1.3 Intended Audience .............................................................................................................. 6
2 Configure the LoadMaster and the HSM .................................................................................. 7
  2.1 Download the CA Certificate from the HSM ......................................................................... 7
  2.2 Configure the LoadMaster .................................................................................................... 7
  2.3 Configure the HSM .............................................................................................................. 8
  2.4 Enable HSM in the LoadMaster ........................................................................................... 8
  2.5 Generate a Certificate Signing Request (CSR) ....................................................................... 9
  2.6 Import the CA Certificate and Assign it to a Virtual Service ........................................... 10
3 Troubleshooting ....................................................................................................................... 11
  3.1 Connection Lost Between the LoadMaster and the HSM .................................................... 11
  3.2 The LoadMaster Cannot Connect to the HSM ..................................................................... 11
    3.2.1 Ping the HSM .............................................................................................................. 11
References ...................................................................................................................................... 13
Document History ......................................................................................................................... 14
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 via 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.
Hardware Security Module (HSM)

Feature Description

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 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.

The additional CPU load (which is caused by the work of encrypting and decrypting data and can be quite significant) is taken off of the server and is dealt with by the HSM instead.

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

Follow the steps in the sections below to connect the HSM with the LoadMaster and configure the relevant settings as needed.

### 2.1 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.

### 2.2 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 > HSM Configuration**.

   ![Select HSM Subsystem](Image)

   **Figure 2-1: Select the HSM subsystem**

2. Select the relevant HSM subsystem to use.

   ![SafeNet HSM Configuration](Image)

   **Figure 2-2: SafeNet HSM Configuration**

3. Enter the IP address of the 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 Section 2.1.
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, i.e. `<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 Section 2.3.
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.

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 **Section 2.3** to do this.

### 2.3 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 **Section 2.3**.

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.

### 2.4 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 > HSM Configuration**.

   ![Figure 2-3: Enable HSM](image)

2. Select the **Enable Safenet HSM** check box.
3. Click **OK**.

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

### 2.5 Generate a Certificate Signing Request (CSR)

Follow the steps below to generate a CSR:

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

![Generate CSR](image)

1. Enter a recognizable name in the **Private Key Identifier** text box.
2. Click **Generate CSR**.
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.
2.6 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 > SSL Certificates.

![Figure 2-7: Import Certificate](image)

2. Click Import Certificate.

![Figure 2-8: Choose File](image)

3. Click Choose File.

4. Browse to and select the relevant certificate file.

![Figure 2-9: Assignment](image)

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

![Figure 3-1: Error](image)

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. Please be aware that the LoadMaster will not automatically re-enable the HSM connection. To re-enable the HSM connection, go to Certificates > 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.

   ![Figure 3-2: Debug Options](image)

   - Click Debug Options.

2. Click Debug Options.
<table>
<thead>
<tr>
<th>Feature Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable All Transparency</td>
<td>Disable Transparency</td>
</tr>
<tr>
<td>Enable L7 Debug Traces</td>
<td>Enable Traces</td>
</tr>
<tr>
<td>Perform an i7adm</td>
<td>i7adm</td>
</tr>
<tr>
<td>Enable IRQ Balance</td>
<td>Enable IRQ Balance</td>
</tr>
<tr>
<td>Disable TSO</td>
<td>Disable TSO</td>
</tr>
<tr>
<td>Enable Bind Debug Traces</td>
<td>Enable Bind Traces</td>
</tr>
<tr>
<td>Perform a PS</td>
<td>ps</td>
</tr>
<tr>
<td>Display Meminfo</td>
<td>Meminfo</td>
</tr>
<tr>
<td>Display Slabinfo</td>
<td>Slabinfo</td>
</tr>
<tr>
<td>Perform an Ifconfig</td>
<td>Ifconfig</td>
</tr>
<tr>
<td>Perform a Netstat</td>
<td>Netstat</td>
</tr>
<tr>
<td>Reset Statistic Counters</td>
<td>Reset Statistics</td>
</tr>
<tr>
<td>Flush OCSPD Cache</td>
<td>Flush Cache</td>
</tr>
<tr>
<td>Flush SSO Authentication</td>
<td>Flush SSO Cache</td>
</tr>
<tr>
<td>Cache Logfiles</td>
<td></td>
</tr>
<tr>
<td>Stop IPsec IKE Daemon</td>
<td>Stop IPsec IKE Daemon</td>
</tr>
<tr>
<td>Perform an IPsec Status</td>
<td>IPsec Status</td>
</tr>
<tr>
<td>Enable IKE Debug Level Logs</td>
<td>Enable Logs</td>
</tr>
<tr>
<td>Netconsole Host</td>
<td></td>
</tr>
<tr>
<td>Ping Host</td>
<td></td>
</tr>
<tr>
<td>Traceroute Host</td>
<td></td>
</tr>
<tr>
<td>Kill LoadMaster (134382)</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 3-3: Ping Host**

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**.

**Figure 3-4: Ping Results**

The results of the ping will be displayed.
References

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

SSL Accelerated Services, Feature Description
## Document History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Version</th>
<th>Resp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 2015</td>
<td>Initial draft</td>
<td>First draft of document</td>
<td>1.0</td>
<td>LB</td>
</tr>
<tr>
<td>Jan 2015</td>
<td>Minor changes</td>
<td>Enhancements made</td>
<td>1.1</td>
<td>LB</td>
</tr>
<tr>
<td>Feb 2015</td>
<td>Minor changes</td>
<td>Screenshot updated</td>
<td>1.2</td>
<td>LB</td>
</tr>
<tr>
<td>Apr 2015</td>
<td>Release updates</td>
<td>Updates for 7.1-26</td>
<td>1.3</td>
<td>LB</td>
</tr>
</tbody>
</table>