



# **SSL Accelerated Services for the LM-5305**

## **Feature Description**

*VERSION: 9.0*

*UPDATED: March 2017*

## Copyright Notices

Copyright © 2002-2017 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 trademarks 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) 1998, Massachusetts Institute of Technology

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.

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

---

<b>1 Introduction</b>	<b>7</b>
1.1 Document Purpose	7
1.2 Intended Audience	7
<b>2 Create an SSL Accelerated Virtual Service</b>	<b>8</b>
2.1 Adding an SSL Virtual Service	8
2.2 Adding an SSL Certificate	12
2.3 Checking Certificate Installations	15
2.4 Intermediate Certificates	16
2.5 Installing Intermediate Certificates	17
2.6 IIS Certificates	17
2.7 Re-encrypt SSL	18
2.8 Assigning a Client Certificate for Re-encryption	18
2.9 Backup/Restore Certificates	20
2.10 SSL Ciphers	20
2.10.1 Cipher Set Management	22
2.11 WUI Root Certificate Installation	23
2.12 OCSP Configuration	24
2.12.1 OCSP Server Settings	24
2.13 Setting the Diffie-Hellman Key Exchange Size	25
<b>3 WUI Options</b>	<b>27</b>
3.1 SSL Properties	27
3.2 Certificates & Security	31
3.2.1 SSL Certificates	31
3.2.2 Intermediate Certificates	32
3.2.3 Generate CSR (Certificate Signing Request)	32

---



---

3.2.4 Backup/Restore Certs .....	34
3.2.5 Cipher Sets .....	35
3.2.6 OCSP Configuration .....	37
<b>4 Appendix A - Cipher List .....</b>	<b>39</b>
<b>References .....</b>	<b>40</b>
<b>Document History .....</b>	<b>41</b>

## 1 Introduction

KEMP Technologies leads the industry in driving the price/performance value proposition for application delivery and load balancing to levels that our customers can afford. Our products' versatile and powerful architecture provide the highest value, while enabling our customers to optimize their businesses that rely on Internet-based infrastructure to conduct business with their customers, employees and partners.

KEMP Technologies products optimize web and application infrastructure as defined by high-availability, high-performance, flexible scalability, security and ease of management. They maximize the total cost-of-ownership for web infrastructure, while enabling flexible and comprehensive deployment options.

### 1.1 Document Purpose

This document describes various aspects of SSL Accelerated Services using the KEMP LoadMaster. It describes in detail how to configure SSL Accelerated Services using the LoadMaster Web User Interface (WUI).

### 1.2 Intended Audience

This document is intended to help anyone who wishes to learn about or implement the SSL Accelerated Services within the KEMP LoadMaster.

## 2 Create an SSL Accelerated Virtual Service

This section will explain how to create a Virtual Service with SSL Acceleration activated.

SSL Acceleration transfers the processing of SSL from the Real Servers to the LoadMaster, meaning that only one certificate is required per Virtual Service.

When SSL Acceleration is enabled, communication from the LoadMaster to the Real Servers is unencrypted.

### 2.1 Adding an SSL Virtual Service

The process for adding an SSL-enabled Virtual Service is the same for a regular Virtual Service. First, add the Virtual Service. In the main menu of the LoadMaster WUI, select **Virtual Services** and **Add New**. A screen will appear asking to enter the **Virtual Address**, **Port**, **Service Name** and **Protocol**.



Please Specify the Parameters for the Virtual Service.

Virtual Address	<input type="text"/>
Port	<input type="text" value="80"/>
Service Name (Optional)	<input type="text"/>
Protocol	<input type="text" value="tcp"/>

The port defaults to port **80**, which is the standard HTTP port. If an SSL-enabled Virtual Service is being created, change the port to **443**, which is the default HTTPS port. Keep the protocol as **tcp**, and click **Add this Virtual Service**.

The Virtual Service properties screen will appear. Among the various sections in this screen is **SSL Properties**.



## 2 Create an SSL Accelerated Virtual Service

SSL Properties

SSL Acceleration

Enabled: ☒ Reencrypt: ☐

Supported Protocols

☐ SSLv3 ☒ TLS1.0 ☒ TLS1.1 ☒ TLS1.2

Require SNI hostname

☐

Self Signed Certificate in use.

Available Certificates

None Available

Assigned Certificates

None Assigned

Set Certificates

Manage Certificates

Cipher Set

Default

Modify Cipher Set

Assigned Ciphers

ECDHE-RSA-AES256-GCM-SHA384

ECDHE-ECDSA-AES256-GCM-SHA384

ECDHE-RSA-AES256-SHA384

ECDHE-ECDSA-AES256-SHA384

ECDHE-RSA-AES256-SHA

ECDHE-ECDSA-AES256-SHA

Client Certificates

No Client Certificates required

To enable SSL for this Virtual Service, select the **Enabled** check box.

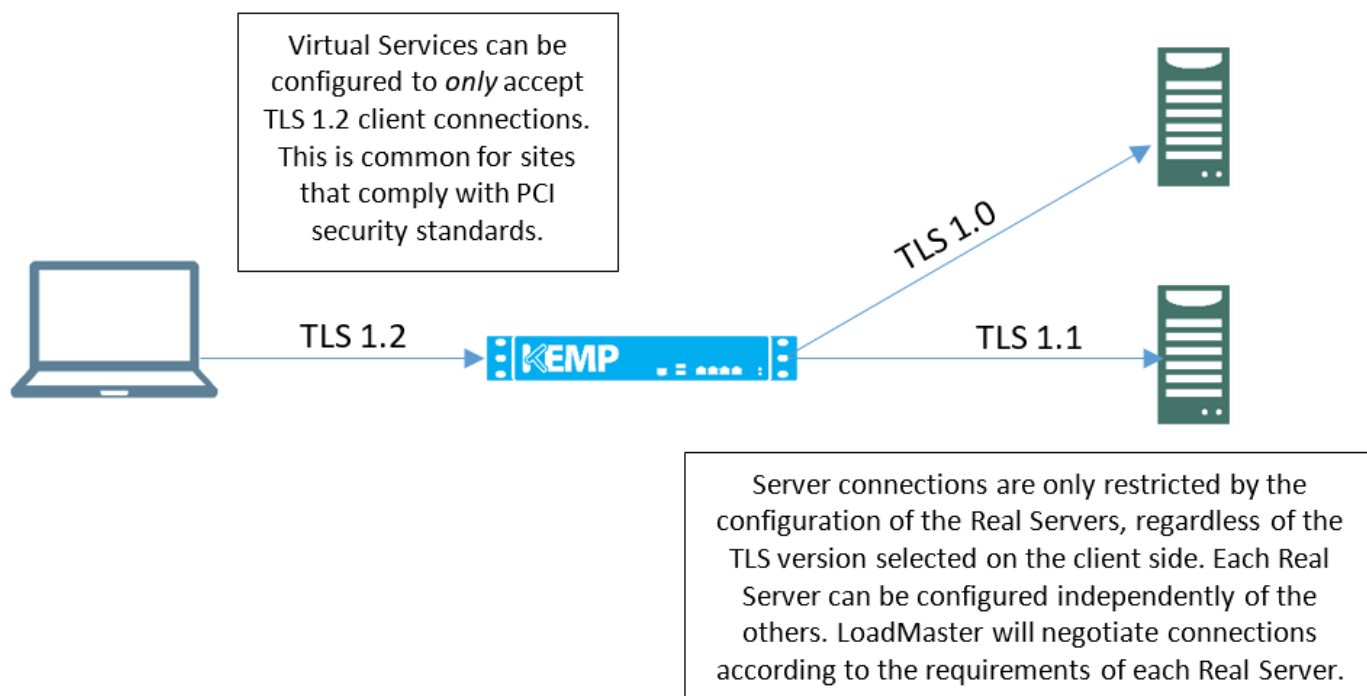
A warning will appear saying that a temporary certificate will be used for the service. Click **OK**.

As soon as SSL is enabled, the LoadMaster will install a self-signed certificate for the Virtual Service.

The checkboxes in the **Supported Protocols** section allow you to specify which protocols should be supported by the Virtual Service. By default, TLS1.1 and TLS 1.2 protocols are enabled and SSLv3 and TLS1.0 are disabled.

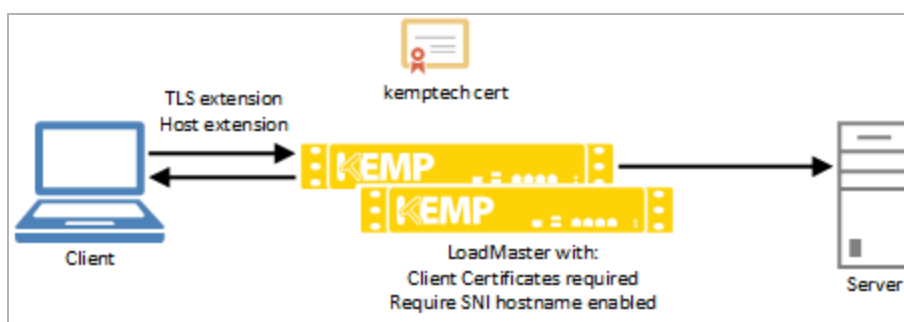
Starting with version 7.2.37, when re-encryption is enabled, the TLS version that can be negotiated between the LoadMaster and the Real Servers behind it are no longer constrained by the TLS version settings configured on the client side. All TLS versions and ciphers that are supported on the LoadMaster can be negotiated without restriction by Real Servers. In this way, the LoadMaster can, for example, provide strict security for client-side application access and still support server-side connections to legacy servers that only support specific, less secure, TLS versions and ciphers. This is illustrated in the example below.

## 2 Create an SSL Accelerated Virtual Service



Selecting the require Server Name Identifier (SNI) hostname check box means that the hostname will always be required to be sent in the TLS client hello message.

When **Require SNI hostname** is disabled, the first certificate in the list of **Assigned Certificates** as a host header match is not found.



When **Require SNI hostname** is enabled, a certificate with a matching host name must be found, otherwise the connection is dropped. This also supports wildcard certificates.

Multiple certificates are supported. Wildcard certificates work regardless of what position they are in. SNI can find certificates by Subject Alternative Name (SAN) when the certificate is not in the first position. SNI will choose the first matching certificate in a list if multiple certificates contain the same name in either the Common Name or SAN name.

When using a Subject Alternative Name (SAN) certificate, alternate source names are not matched against the host header.

Wildcard certificates are supported but please note that the root domain name will not be matched as per RFC 2459. Only anything to the left of the dot will be matched. Additional certificates must be added to match the root domain names. For example, [www.kemptechnologies.com](http://www.kemptechnologies.com) will be matched until a wildcard of \*.kemptechnologies.com. Kemptechnologies.com will not be matched.

After you have added certificates to the LoadMaster (see the **Adding an SSL Certificate** section) you can assign one or more certificates to the Virtual Service by selecting them in the **Available Certificates** list, clicking the right arrow and clicking the **Set Certificates** button. Both internal and external certificates can be assigned to the same Virtual Service.

A description of each of the options in the **Client Certificates** drop-down is provided below:

- **No Client Certificates required:** enables the LoadMaster to accept HTTPS requests from any client. This is the recommended option.

By default the LoadMaster will accept HTTPS requests from any client. Selecting any of the other values below will require all clients to present a valid client certificate. In addition, the LoadMaster can also pass information about the certificate to the application.

This option should not be changed from the default of **No Client Certificates required**. Only change from the default option if you are sure that all clients that access this service have valid client certificates.

- **Client Certificates required:** requires that all clients forwarding a HTTPS request must present a valid client certificate.
- **Client Certificates and add Headers:** requires that all clients forwarding a HTTPS request must present a valid client certificate. The LoadMaster also passes information about the certificate to the application by adding headers.
- The below options send the certificate in its original raw form. The different options let you specify the format that you want to send the certificate in:
  - Client Certificates and pass DER through as SSL-CLIENT-CERT
  - Client Certificates and pass DER through as X-CLIENT-CERT
  - Client Certificates and pass PEM through as SSL-CLIENT-CERT
  - Client Certificates and pass PEM through as X-CLIENT-CERT

Real Servers can be added to this SSL Virtual Service by clicking **Add New** in the **Real Servers** section.

## 2 Create an SSL Accelerated Virtual Service

Please Specify the Parameters for the Real Server

Real Server Address	<input type="text"/>
Port	<input type="text" value="80"/>
Forwarding method	<input type="text" value="nat"/>
Weight	<input type="text" value="1000"/>
Connection Limit	<input type="text"/>

[< Back](#) [Add This Real Server](#)

When adding Real Servers, ensure to add them on port **80** (or whatever port that the non-SSL service is running on), and not port 443.

## 2.2 Adding an SSL Certificate

To add an SSL Certificate, first generate a CSR. A CSR can be created, for submission directly to the signing authority of choice, by using the WUI.

In the main menu of the LoadMaster WUI, go to **Certificates > SSL Certificates**. Enter a Private Key Identifier and click **Generate CSR**.

Create a CSR for private key Example  
All Fields are optional except "Common Name"

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"/>

Fill out the form and create the CSR and private key by clicking the **Create CSR** button.

If you have the CA certificate generated using the step above, or have a custom self-signed certificate, this can be added to the Virtual Service through the WUI.

## 2 Create an SSL Accelerated Virtual Service

SSL Properties

SSL Acceleration Enabled: ☒ Reencrypt: ☐

Supported Protocols ☐SSLv3 ☒TLS1.0 ☒TLS1.1 ☒TLS1.2

Require SNI hostname ☐

Self Signed Certificate In use.

Certificates

Available Certificates

None Available

Assigned Certificates

None Assigned

Set Certificates

Manage Certificates

Cipher Set

Default

Modify Cipher Set

Assigned Ciphers

ECDHE-RSA-AES256-GCM-SHA384  
ECDHE-ECDSA-AES256-GCM-SHA384  
ECDHE-RSA-AES256-SHA384  
ECDHE-ECDSA-AES256-SHA384  
ECDHE-RSA-AES256-SHA  
ECDHE-ECDSA-AES256-SHA

Client Certificates

No Client Certificates required

There is a button called **Manage Certificates** that you can click to add an (RSA or EC) SSL certificate.

Layer	Certificate Installed
L7	<div>Add New</div>
L7	<div>Add New</div>

There is also an **Add New** button in the **View/Modify Services** screen in the **Certificates Installed** column.

Private Key Identifier: 

Generate CSR

Private Key	Common Name(s)	Virtual Services	Assignment	Operation
ExampleCert	Example.com (Expires: Sep 1 12:20:38 2020 GMT)	172.21.11.11:443	<div>Available VSS</div> <div>None Assigned</div> <div>Save Changes</div>	<div>Import Certificate</div> <div>Delete Key</div> <div>Show Reencrypt Certs</div>

Either route opens the same screen; the screen to input the certificate information.

At this point there are two options; **Add Intermediate** and **Import Certificate**.

### Add Intermediate

## 2 Create an SSL Accelerated Virtual Service

### Add a new Intermediate Certificate

Intermediate Certificate

Choose File

No file chosen

Certificate Name

Add Certificate

Clicking this button will allow you to add an intermediate certificate as a temporary measure. Browse to where the file is stored, enter the desired name in the **Desired File Name** field and click the **Add Certificate** button.

### Import Certificate

When using FIPS in HA mode, ensure to only import certificates when both nodes are up.

Private Key	Common Name(s)	Virtual Services	Assignment	Operation
Example	CSR generated	Available VSs 172.21.11.11:443	Assigned VSs None Assigned	<div>Import Certificate</div> <div>Delete Key</div> <div>Show Reencrypt Certs</div>

Save Changes

An entry for the CSR previously generated will be available with the status **CSR generated** in red font under the **Virtual Services** column. Click **Import Certificate** on the right.

### Please supply the file containing the Signed Certificate for Example

Signed Public Certificate File

Choose File

No file chosen

Cancel

Submit

Click **Choose File** to select the signed certificate and click **Submit**.

A dialog informing you that the certificate installed successfully should appear.

Private Key	Common Name(s)	Virtual Services	Assignment
ExampleCert	Example.com [Expires: Sep 1 12:20:38 2020 GMT]	Available VSs None Assigned	Assigned VSs 172.21.11.11:443

Save Changes

The certificate can then be assigned to a Virtual Service(s) by selecting the relevant IP address(s) in the **Available VSs** list, clicking the right arrow and clicking **Save Changes**.

## 2 Create an SSL Accelerated Virtual Service

SSL Properties

SSL Acceleration

Enabled: ☒ Reencrypt: ☐

Self Signed Certificate in use.

Available Certificates

Example []

Assigned Certificates

None Assigned

>

<

Set Certificates

Manage Certificates

Cipher Set

Default

Modify Cipher Set

Assigned Ciphers

ECDHE-RSA-AES256-SHA384

ECDHE-ECDSA-AES256-SHA384

DHE-RSA-AES256-SHA256

DHE-DSS-AES256-SHA256

ECDH-RSA-AES256-SHA384

ECDH-ECDSA-AES256-SHA384

Ciphers

Client Certificates

No Client Certificates required

Certificates can also be assigned to a Virtual Service within the **Modify Virtual Service** screen.

### 2.3 Checking Certificate Installations

Some browsers have functionality that allows a check of the nature of the certificate installed on the website being connecting to. This can be useful when troubleshooting a certificate problem.

When browsing an SSL site, HTTPS should be displayed in the address and there may be an icon signifying a secure link (a padlock icon).



The icon can be clicked to see information about the certificate that is used with that SSL site.

## 2.4 Intermediate Certificates

Some certificates issued by Certificate Authorities require a third certificate, often referred to as an intermediate certificate, or third-party certificate. This additional certificate provides a chain path from the CA to the certificate issued to your site.

While some CAs use intermediate certificates, others do not. Check with your CA to determine if one is needed.

If a CA certificate has been installed, and an SSL error appears when browsing the Virtual Service, it is likely that an intermediate certificate needs to be installed.

Uploading several consecutive intermediate certificates within a single piece of text, as practiced by some certificate vendors such as GoDaddy, is allowed. The uploaded file is split into individual certificates.

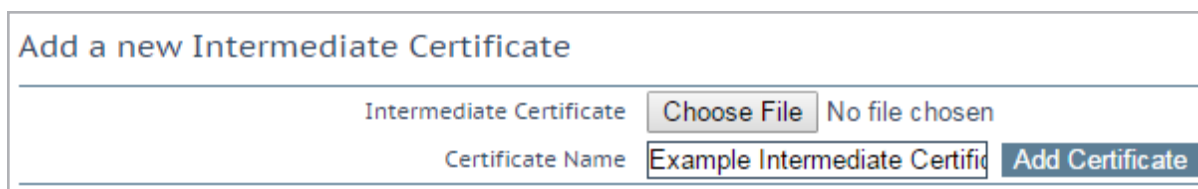


### 2.5 Installing Intermediate Certificates

Installing an intermediate certificate is simple to do through the WUI. First, obtain the intermediate certificate from the CA. This can usually be found on their web site, and is usually in a text window to make it easier to cut and paste.

To install an intermediate certificate please complete the following steps:

1. Navigate to **Certificates & Security > Intermediate Certs** in the main menu.
2. Click **Add New**.



Add a new Intermediate Certificate	
Intermediate Certificate	<input type="button" value="Choose File"/> No file chosen
Certificate Name	<input type="text" value="Example Intermediate Certificate"/> <input type="button" value="Add Certificate"/>

3. Click **Choose File**.
4. Browse to and select the required certificate file.
5. Enter the **Desired File Name**.
6. Click **Add Certificate**.
7. Click **OK**.

These third party/intermediate certificates do not need to be associated with any Virtual Service certificates. The LoadMaster will automatically build the required certificate chain.

Also, only one intermediate certificate is required per CA. If several certificates have been installed from VeriSign, for instance, you only need to install the VeriSign intermediate certificate once.

### 2.6 IIS Certificates

This section outlines how to migrate SSL from Microsoft Internet Information Services (IIS) to the LoadMaster.

When putting a LoadMaster in a situation where a Microsoft IIS server was previously performing SSL, there is an option to import the IIS certificate into the LoadMaster. This SSL certificate can be migrated from Microsoft IIS to the LoadMaster by completing two simple tasks. The first task is to export the SSL certificate from the IIS using Microsoft export tools; ensure to export the certificate and private key as a Personal Information Exchange File (PFX). The second step is to import the PFX file into the LoadMaster using the LoadMaster WUI. To start the import process on the LoadMaster simply click the **Add New**

## 2 Create an SSL Accelerated Virtual Service

button in the SSL enabled Virtual Service and install the certificate as per the instructions in the **Adding an SSL Certificate** section.

### 2.7 Re-encrypt SSL

With SSL acceleration, the SSL session is terminated at the LoadMaster, and sent to the Real Servers unencrypted. In some security situations, it may be necessary to encrypt the connection between the LoadMaster and Real Servers. This can be done with reencrypt SSL.

With reencrypt SSL, the SSL session is first terminated at the LoadMaster. Persistence and other Layer 7 functionality can then be performed. After that, the traffic is re-encrypted in a new SSL session between the LoadMaster and the Real Server.

SSL Properties	
SSL Acceleration	Enabled: <input checked="" type="checkbox"/> Reencrypt: <input checked="" type="checkbox"/>
Supported Protocols	<input type="checkbox"/> SSLv3 <input checked="" type="checkbox"/> TLS1.0 <input checked="" type="checkbox"/> TLS1.1 <input checked="" type="checkbox"/> TLS1.2
Require SNI hostname	<input type="checkbox"/>
Certificates	<div> <div>Self Signed Certificate in use.</div> <div>Available Certificates</div> <div>ExampleCertificate [Example]</div> <div>Assigned Certificates</div> <div>None Assigned</div> <div>Set Certificates</div> </div>
Ciphers	<div> <div>Cipher Set</div> <div>Default</div> <div>Modify Cipher Set</div> <div>Assigned Ciphers</div> <div>           ECDHE-RSA-AES256-GCM-SHA384            ECDHE-ECDSA-AES256-GCM-SHA384            ECDHE-RSA-AES256-SHA384            ECDHE-ECDSA-AES256-SHA384            ECDHE-RSA-AES256-SHA            ECDHE-ECDSA-AES256-SHA         </div> </div>
Client Certificates	No Client Certificates required
Reencryption Client Certificate	None required
Reencryption SNI Hostname	<input type="text"/> Set SNI Hostname

This is turned on by a single option in the properties screen of a Virtual Service in the SSL section.

### 2.8 Assigning a Client Certificate for Re-encryption

It is possible to require client certificates when SSL re-encryption is enabled. To assign a client certificate for re-encryption, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **Certificates & Security > SSL Certificates**.

## 2 Create an SSL Accelerated Virtual Service

Operation	
	New CSR
	Replace Certificate
	Delete Certificate
	Reencryption Usage

2. Click **Reencryption Usage** on the relevant certificate.

Identifier	Common Name(s)	Virtual Services	Assignment
ExampleCertificate	Example [Expires: Aug 24 09:11:21 2016 GMT]		<div>Available VSs</div> <div>10.154.11.61:80 10.154.11.62:80</div> <div>Assigned VSs</div> <div>None Assigned</div> <div>&gt; &lt;</div> <div>Save Changes</div>
VSs using ExampleCertificate for Reencryption		<div>Available VSs</div> <div>None Assigned</div>	<div>Assigned VSs</div> <div>10.154.11.61:80</div> <div>&gt; &lt;</div> <div>Save Changes</div>

3. Select the relevant IP address from the **Available VSs** box.
4. Click the right arrow.
5. Click **Save Changes**.

## 2 Create an SSL Accelerated Virtual Service

SSL Properties	
SSL Acceleration	Enabled: <input checked="" type="checkbox"/> Reencrypt: <input checked="" type="checkbox"/>
Supported Protocols	<input type="checkbox"/> SSLv3 <input checked="" type="checkbox"/> TLS1.0 <input checked="" type="checkbox"/> TLS1.1 <input checked="" type="checkbox"/> TLS1.2
Require SNI hostname	<input type="checkbox"/>
Certificates	<div> <div>Self Signed Certificate in use.</div> <div>Available Certificates</div> <div>ExampleCertificate [Example]</div> <div>Assigned Certificates</div> <div>None Assigned</div> <div>Set Certificates</div> </div> <div>Manage Certificates</div>
Ciphers	<div> <div>Cipher Set</div> <div>Default</div> <div>Modify Cipher Set</div> </div> <div>Assigned Ciphers</div> <div> ECDHE-RSA-AES256-GCM-SHA384  ECDHE-ECDSA-AES256-GCM-SHA384  ECDHE-RSA-AES256-SHA384  ECDHE-ECDSA-AES256-SHA384  ECDHE-RSA-AES256-SHA  ECDHE-ECDSA-AES256-SHA </div>
Client Certificates	No Client Certificates required
Reencryption Client Certificate	ExampleCertificate [Example] Expires: Aug 24 09:11:21 2016 GMT
Reencryption SNI Hostname	<input type="text"/> Set SNI Hostname

The **Reencryption Client Certificate** is displayed in the **SSL Properties** section of the relevant Virtual Service.

## 2.9 Backup/Restore Certificates

The LM-5305 supports exporting of intermediate certificates. The export file is designed to be used for import into the same LM-5305 and is encrypted. Export and import can be completed using the WUI at **Certificates > Backup/Restore Certs**. Please make sure to note the passphrase used to create the export because it will be required to complete the import.

## 2.10 SSL Ciphers

The LoadMaster supports SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2.

Ciphers define how the data stream is encrypted. The LoadMaster supports ciphers supporting perfect forward secrecy and Elliptic Curve.

## 2 Create an SSL Accelerated Virtual Service

SSL Properties

SSL Acceleration

Enabled: ☒ Reencrypt: ☐

Supported Protocols

☐ SSLv3 ☒ TLS1.0 ☒ TLS1.1 ☒ TLS1.2

Require SNI hostname

☐

Self Signed Certificate in use.

Available Certificates

ExampleCertificate [Example]

Assigned Certificates

None Assigned

Set Certificates

Manage Certificates

Cipher Set

Default

Modify Cipher Set

Assigned Ciphers

ECDHE-RSA-AES256-GCM-SHA384  
ECDHE-ECDSA-AES256-GCM-SHA384  
ECDHE-RSA-AES256-SHA384  
ECDHE-ECDSA-AES256-SHA384  
ECDHE-RSA-AES256-SHA  
ECDHE-ECDSA-AES256-SHA

Client Certificates

No Client Certificates required

Each Virtual Service (which has **SSL Acceleration** enabled) has a cipher set assigned to it. This can either be one of the system-defined cipher sets or a user-customized cipher set. The system-defined cipher sets can be selected to quickly and easily select and apply the relevant ciphers.

A cipher set also needs to be assigned to the LoadMaster WUI. To set the WUI cipher set, go to **Certificates & Security > Admin WUI Access**.

Each Virtual Service (which has **SSL Acceleration** enabled) has a cipher set assigned to it. This can either be a system-defined cipher set or a user-customized cipher set. A system-defined cipher set can be selected to quickly and easily select and apply the relevant ciphers.

In the FIPS LoadMaster, there are three system-defined cipher sets; **WUI**, **Default** and **BestPractices**. Each of these cipher sets only contain ciphers that are supported by FIPS.

The list of ciphers which are assigned to a Virtual Service can be edited by clicking the **Modify Cipher Set** button. If changes are made to a preconfigured cipher set, a new custom cipher set will be created. Custom cipher sets can be named and can be used across different Virtual Services.

By default, the name for the custom cipher set will be **Custom\_<VirtualServiceID>**. KEMP recommends changing the name of custom cipher sets because if another system-defined cipher set is modified, the name will again default to **Custom\_<VirtualServiceID>** and will overwrite any existing cipher sets with that name.

It is not possible to modify the list of ciphers in a system-defined cipher set. Instead, a new custom cipher set will be created when changes are made to the ciphers list.

### 2.10.1 Cipher Set Management

Cipher Set Management

Cipher Set Default

Available Ciphers

Filter:

Name	Strength
ECDHE-RSA-AES256-GCM-SHA384	High
ECDHE-ECDSA-AES256-GCM-SHA384	High
ECDHE-RSA-AES256-SHA384	High
ECDHE-ECDSA-AES256-SHA384	High
ECDHE-RSA-AES256-SHA	High
ECDHE-ECDSA-AES256-SHA	High
DH-DSS-AES256-GCM-SHA384	High
DHE-DSS-AES256-GCM-SHA384	High
DH-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-SHA256	High
DHE-DSS-AES256-SHA256	High
DH-RSA-AES256-SHA256	High
DH-DSS-AES256-SHA256	High

Assigned Ciphers

Filter:

Name	Strength
ECDHE-RSA-AES256-GCM-SHA384	High
ECDHE-ECDSA-AES256-GCM-SHA384	High
ECDHE-RSA-AES256-SHA384	High
ECDHE-ECDSA-AES256-SHA384	High
ECDHE-RSA-AES256-SHA	High
ECDHE-ECDSA-AES256-SHA	High
DH-DSS-AES256-GCM-SHA384	High
DHE-DSS-AES256-GCM-SHA384	High
DH-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-SHA256	High
DHE-DSS-AES256-SHA256	High
DH-RSA-AES256-SHA256	High
DH-DSS-AES256-SHA256	High

Save as: Default

Save

Two lists are displayed – **Available Ciphers** and **Assigned Ciphers**. These lists can be filtered by typing some text into the **Filter** text boxes provided. The **Filter** text boxes will only allow you to enter valid text which is contained in the cipher names, for example **ECDHE**. If invalid text is entered, the text box will turn red and the invalid text is deleted.

Ciphers can be dragged and dropped to/from the **Available** and **Assigned** lists as needed. Ciphers which are already assigned will appear greyed out in the **Available Ciphers** list.

Changes cannot be made to a preconfigured cipher set. However, you can start with a preconfigured cipher set – make any changes as needed and then save the cipher set with a new custom name. Enter the new name in the **Save as** text box and click the **Save** button. Custom cipher sets can be used across different Virtual Services and can be assigned as the WUI cipher set.

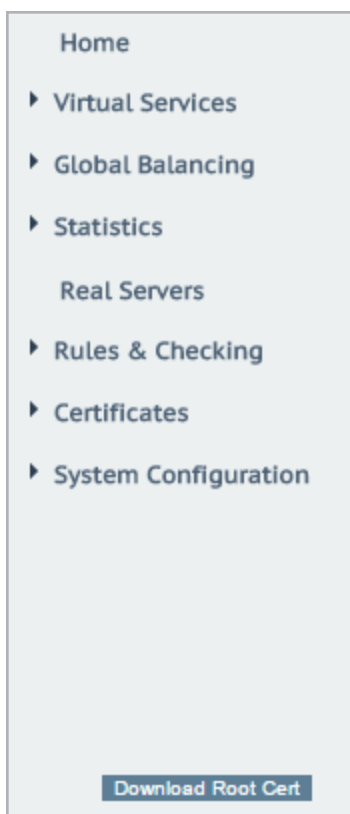
It is not possible to delete preconfigured cipher sets. However, custom cipher sets can be deleted by selecting the relevant custom cipher set and clicking the **Delete Cipher set** button.

The RC4-MD5 SSLv3 and RC4-MD5 SSLv3 ciphers are not supported for WUI connections (this is to improve security).

The RC4 ciphers are supported with (and can be assigned to) Virtual Services if needed.

### 2.11 WUI Root Certificate Installation

By default the LoadMaster uses a self-signed certificate to ensure secure administrative access to the WUI. However, most modern browsers will display a warning when such a certificate is used.



In order to eliminate this warning, the LoadMaster certificate can be installed by clicking the **Download Root Cert** button in the main menu on the **Home** page, when you first access the WUI in a browser.

If this button is not visible, go to the WUI **Home** and refresh the page.

This will download the certificate file that can be installed on the browser so that the security warning can be avoided.

### 2.12 OCSP Configuration

A Common Access Card (CAC) is a smart card used for identification of active-duty military personnel, selected reserve, US Department of Defence (DoD) civilian employees and eligible contractor personnel. In addition to providing physical access to buildings and protected areas, it also allows access to DoD computer networks and systems satisfying two-factor authentication, digital security and data encryption. It leverages a Public Key Infrastructure (PKI) Security Certificate to verify a cardholder's identity prior to allowing access to protected resources.

The Edge Security Pack (ESP) feature of the KEMP LoadMaster supports integration with DoD environments, leveraging CAC authentication and Active Directory application infrastructures. The LoadMaster acts on behalf of clients presenting X.509 certificates using CAC and becomes the authenticated Kerberos client for services.

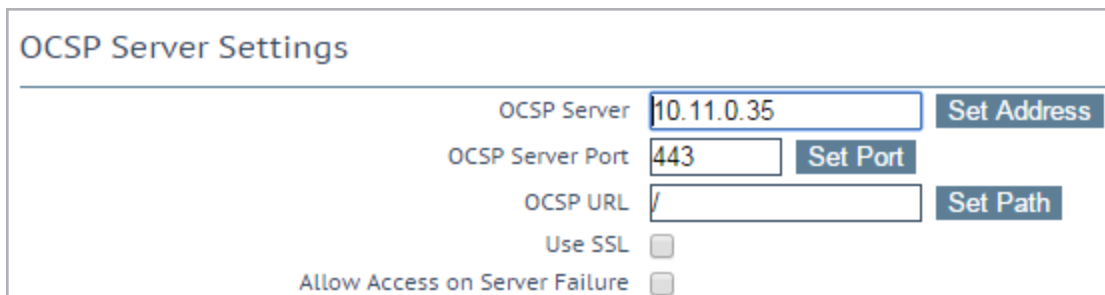
The request for and presentation of the client certificate happens during initial SSL session establishment. There are two core elements to the process of a user gaining access to an application with CAC:

- Authentication – occurs during SSL session establishment and entails:
  - Verifying the certificate date
  - Verifying revocation status using Online Certificate Status Protocol (OCSP)
  - Verifying the full chain to the Certificate Authority (CA)
- Authorization – occurs after SSL session establishment and the matching of the certificate Subject Alternative Name (SAN) against the User Principal Name (UPN) of the appropriate principal in Active Directory.

For more information, refer to the **DoD Common Access Card (CAC) Authentication, Feature Description** document.

#### 2.12.1 OCSP Server Settings

The OCSP server settings can be set in the LoadMaster WUI in **Certificates & Security > OCSP Configuration**.





## 2 Create an SSL Accelerated Virtual Service

---

### OCSP Server

The address of the OCSP server.

### OCSP Server Port

The port of the OCSP server.

### OCSP URL

The URL to access on the OCSP server.

### Use SSL

Select this to use SSL to connect to the OCSP server.

### Allow Access on Server Failure

Treat an OCSP server connection failure or timeout as if the OCSP server had returned a valid response, that is, treat the client certificate as valid.

## 2.13 Setting the Diffie-Hellman Key Exchange Size

The Diffie-Hellman Key Exchange Size is set to **2048 Bits** by default in the LoadMaster. This can be changed if needed. To change the Diffie-Hellman Key Exchange Size, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to System Configuration > Miscellaneous Options > Network Options.

Enable Server NAT	<input checked="" type="checkbox"/>
Connection Timeout (secs)	<input type="text" value="660"/> <a href="#">Set Time</a> (Valid values:0, 60-86400)
Enable Non-Local Real Servers	<input type="checkbox"/>
Enable Alternate GW support	<input type="checkbox"/>
Enable TCP Timestamps	<input type="checkbox"/>
Enable TCP Keepalives	<input checked="" type="checkbox"/>
Enable Reset on Close	<input type="checkbox"/>
Subnet Originating Requests	<input checked="" type="checkbox"/>
Enforce Strict IP Routing	<input type="checkbox"/>
Handle non HTTP Uploads	<input type="checkbox"/>
Enable Connection Timeout Diagnostics	<input type="checkbox"/>
Enable SSL Renegotiation	<input checked="" type="checkbox"/>
Size of SSL Diffie-Hellman Key Exchange	<input type="text" value="1024 Bits"/>
Use Default Route Only	<input type="checkbox"/>
HTTP(S) Proxy	<input type="text" value="10.154.11.80"/> <a href="#">Set HTTP(S) Proxy</a>

## 2 Create an SSL Accelerated Virtual Service

---

2. Select the relevant option in the **Size of Diffie-Helman Key Exchange** drop-down list.  
Available values are:

- 512 Bits
- 1024 Bits
- 2048 Bits

3. A reboot is required to apply the change. To reboot the LoadMaster, go to **System Configuration > System Administration > System Reboot** and click **Reboot**.

### 3 WUI Options

This section provides a description for each of the WUI options relating to SSL.

#### 3.1 SSL Properties

SSL Properties

SSL Acceleration

Enabled: ☒ Reencrypt: ☐

Supported Protocols

☐ SSLv3 ☒ TLS1.0 ☒ TLS1.1 ☒ TLS1.2

Require SNI hostname

☐

Self Signed Certificate in use.

Available Certificates

None Available

Assigned Certificates

None Assigned

Manage Certificates

Set Certificates

Cipher Set

Default

Modify Cipher Set

Assigned Ciphers

ECDHE-RSA-AES256-GCM-SHA384

ECDHE-ECDSA-AES256-GCM-SHA384

ECDHE-RSA-AES256-SHA384

ECDHE-ECDSA-AES256-SHA384

ECDHE-RSA-AES256-SHA

ECDHE-ECDSA-AES256-SHA

Client Certificates

No Client Certificates required

#### SSL Acceleration

This checkbox appears when the criteria for SSL Acceleration have been met, and serves to activate SSL Acceleration.

**Enabled:** If the **Enabled** check box is selected, and there is no certificate for the Virtual Service, you are prompted to install a certificate. A certificate can be added by clicking the **Manage Certificates** button and importing or adding a certificate.

**Reencrypt:** Selecting the **Reencrypt** checkbox re-encrypts the SSL data stream before sending it to the Real Server.

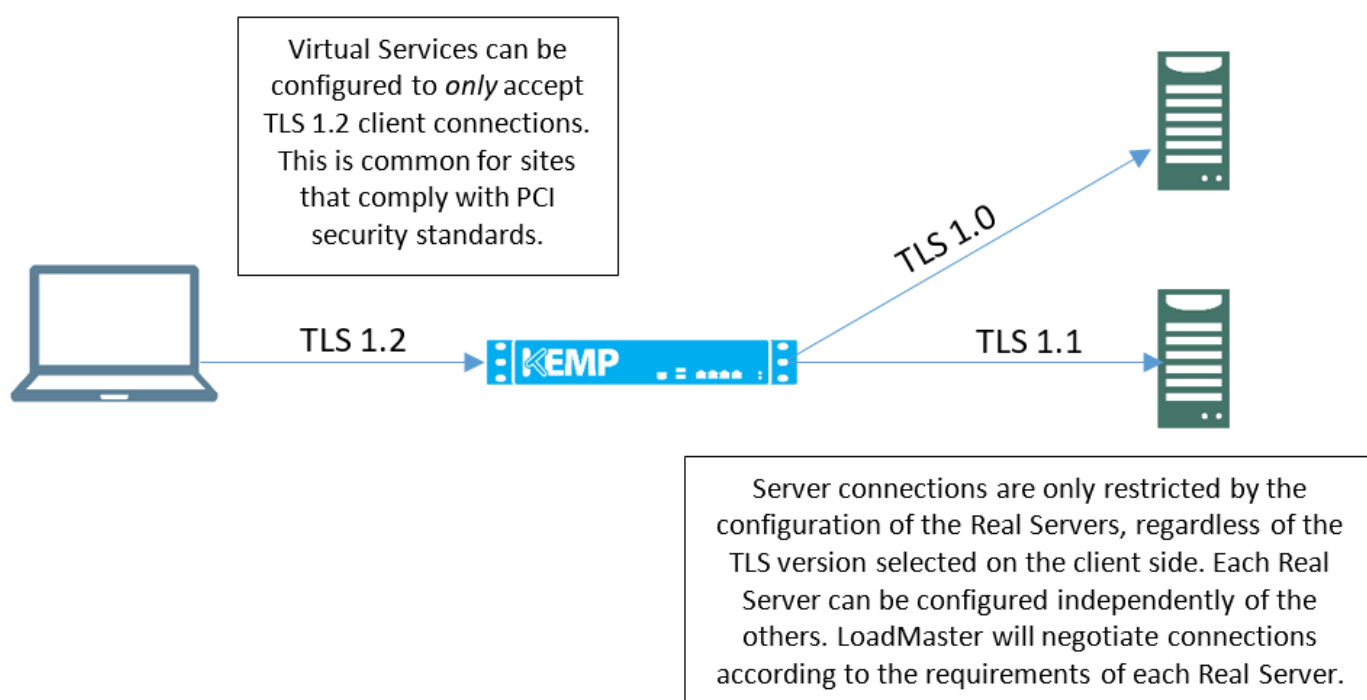
**Reversed:** Selecting this checkbox will mean that the data from the LoadMaster to the Real Server is re-encrypted. The input stream must not be encrypted. This is only useful in connection with a separate Virtual Service which decrypts SSL traffic then uses this Virtual Service as a Real Service and loops data back to it. In this way, the client to real server data path is always encrypted on the wire.

#### Supported Protocols

## 3 WUI Options

The checkboxes in the **Supported Protocols** section enables you to specify which protocols should be supported by the Virtual Service. By default, TLS1.1 and TLS 1.2 are enabled and SSLv3 and TLS1.0 are disabled.

Starting with version 7.2.37, when re-encryption is enabled, the TLS version that can be negotiated between the LoadMaster and the Real Servers behind it are no longer constrained by the TLS version settings configured on the client side. All TLS versions and ciphers that are supported on the LoadMaster can be negotiated without restriction by Real Servers. In this way, the LoadMaster can, for example, provide strict security for client-side application access and still support server-side connections to legacy servers that only support specific, less secure, TLS versions and ciphers. This is illustrated in the example below.



### Require SNI hostname

If require Server Name Indication (SNI) is selected, the hostname will always be required to be sent in the TLS client hello message.

When **Require SNI hostname** is disabled, the first certificate is used if a host header match is not found.

When **Require SNI hostname** is enabled, a certificate with a matching common name must be found, otherwise an SSL error is yielded. Wildcard certificates are also supported with SNI.

When using a Subject Alternative Name (SAN) certificate, alternate source names are not matched

against the host header.

Wildcard certificates are supported but please note that the root domain name will not be matched as per RFC 2459. Only anything to the left of the dot is matched. Additional certificates must be added to match the root domain names. For example, [www.kemptechnologies.com](http://www.kemptechnologies.com) is matched until a wildcard of \*.kemptechnologies.com. Kemptechnologies.com will not be matched.

To send SNI host information in HTTPS health checks, please enable **Use HTTP/1.1** in the **Real Servers** section of the relevant Virtual Service(s) and specify a host header. If this is not set, the IP address of the Real Server is used.

### Certificates

Available certificates are listed in the **Available Certificates** select list on the left. To assign or unassign a certificate, select it and click the right or left arrow button. Then click **Set Certificates**. Multiple certificates can be selected by holding **Ctrl** on your keyboard and clicking each required certificate.

Clicking the **Manage Certificates** button brings you to the SSL Certificates screen.

### Reencryption Client Certificate

With SSL connections, the LoadMaster gets a certificate from the client and also gets a certificate from the server. The LoadMaster transcribes the client certificate in a header and sends the data to the server. The server still expects a certificate. This is why it is preferable to install a pre-authenticated certificate in the LoadMaster.

### Reencryption SNI Hostname

Specify the Server Name Indication (SNI) hostname that should be used when connecting to the Real Servers.

This field is only visible when SSL re-encryption is enabled.

### Cipher Set

A cipher is an algorithm for performing encryption or decryption.

Each Virtual Service (which has **SSL Acceleration** enabled) has a cipher set assigned to it. This can either be the system-defined cipher set or a user-customized cipher set. The system-defined cipher set can be selected to quickly and easily select and apply the relevant ciphers.

In the FIPS LoadMaster, there are three system-defined cipher sets; **WUI**, **Default** and **BestPractices**. Each of these cipher sets only contain ciphers that are supported by FIPS.

Refer to the **SSL Accelerated Services for the LM-5305 FIPS, Feature Description** on the [KEMP Documentation Page](#) for a full list of the ciphers supported by the FIPS LoadMaster.

The list of ciphers which are assigned to a Virtual Service can be edited by clicking the **Modify Cipher Set** button. If changes are made to a preconfigured cipher set, a new custom cipher set will be created. Custom cipher sets can be named and can be used across different Virtual Services.

By default, the name for the custom cipher set will be **Custom\_<VirtualServiceID>**. KEMP recommends changing the name of custom cipher sets because if another system-defined cipher set is modified, the name will again default to **Custom\_<VirtualServiceID>** and will overwrite any existing cipher sets with that name.

It is not possible to modify the list of ciphers in a system-defined cipher set. Instead, a new custom cipher set will be created when changes are made to the ciphers list.

### Ciphers

The **Ciphers** list is read only and displays a list of the currently assigned ciphers. Clicking the **Modify Cipher Set** button will bring you to the **Cipher Set Management** screen. This screen allows you to create new and modify existing custom cipher sets.

### Client Certificates

- **No Client Certificates required:** enables the LoadMaster to accept HTTPS requests from any client. This is the recommended option.

By default the LoadMaster will accept HTTPS requests from any client. Selecting any of the other values below will require all clients to present a valid client certificate. In addition, the LoadMaster can also pass information about the certificate to the application.

This option should not be changed from the default of **No Client Certificates required**. Only change from the default option if you are sure that all clients that access this service have valid client certificates.

- **Client Certificates required:** requires that all clients forwarding a HTTPS request must present a valid client certificate.
- **Client Certificates and add Headers:** requires that all clients forwarding a HTTPS request must present a valid client certificate. The LoadMaster also passes information about the certificate to the application by adding headers.
- The below options send the certificate in its original raw form. The different options let you specify the format that you want to send the certificate in:
  - Client Certificates and pass DER through as SSL-CLIENT-CERT
  - Client Certificates and pass DER through as X-CLIENT-CERT
  - Client Certificates and pass PEM through as SSL-CLIENT-CERT

- Client Certificates and pass PEM through as X-CLIENT-CERT

### Verify Client using OCSP

Verify (using Online Certificate Status Protocol (OCSP)) that the client certificate is valid.

This option is only visible when ESP is enabled.

## 3.2 Certificates & Security

The sections below describe the various screens in the **Certificates & Security** section of the LoadMaster WUI.

### 3.2.1 SSL Certificates



Shown above is the **Manage Certificates** screen. The options on this screen are described below.

**Private Key Identifier** - to generate a new private key which will be stored on the LoadMaster, enter a name for the private key and click **Generate CSR**.

**Add Intermediate** – adds an intermediate certificate.

**Private Key** – is the private key identifier given to the certificate at the time it was created.

**Common Name(s)** – is the FQDN (Fully Qualified Domain Name) for the site.

**Assignment** – the **Available VSs** box lists all of the SSL Virtual Services which are configured on the LoadMaster. The **Assigned VSs** box lists the Virtual Services which the certificate has been assigned to. The Virtual Services can be assigned/unassigned by selecting them and clicking the right/left arrow buttons and clicking **Save Changes**.

**Operations** –

- **Import Certificate** – imports the signed certificate.

When using FIPS in HA mode, ensure to only import certificates when both nodes are up.

- **Delete Key** - deletes the relevant private key and/or certificate

- **Show Reencrypt Certs** - display the re-encrypt certificates

### Administrative Certificates

This section contains two drop-down lists:

- **Administrative Certificate** - select the certificate to be used for the administrative interface. Click Use Certificate to apply the changes.
- **Local Machine Certificate** - select the certificate to be used on the local machine interface. Click Use Certificate to apply the changes.

### 3.2.2 Intermediate Certificates

#### Currently installed Intermediate Certificates

Name	Operation
VeriSignCert.pem	<button>Delete</button>

#### Add a new Intermediate Certificate

Intermediate Certificate

Choose File No file chosen

Certificate Name

Add Certificate

This screen shows a list of the installed intermediate certificates and the name assigned to them.

#### Add a new Intermediate Certificate

Intermediate Certificate

Choose File No file chosen

Certificate Name

Add Certificate

If you already have a certificate, or you have received one from a CSR, you can install the certificate by clicking the **Choose File** button. Navigate to and select the certificate and then enter the desired **Certificate Name**. The name can only contain alpha characters with a maximum of 32 characters.

Uploading several consecutive intermediate certificates within a single piece of text, as practiced by some certificate vendors such as GoDaddy, is allowed. The uploaded file is split into the individual certificates.

### 3.2.3 Generate CSR (Certificate Signing Request)

To create a CSR please complete the following steps:

1. In the main menu, go to **Certificates > SSL Certificates**.



## 3 WUI Options

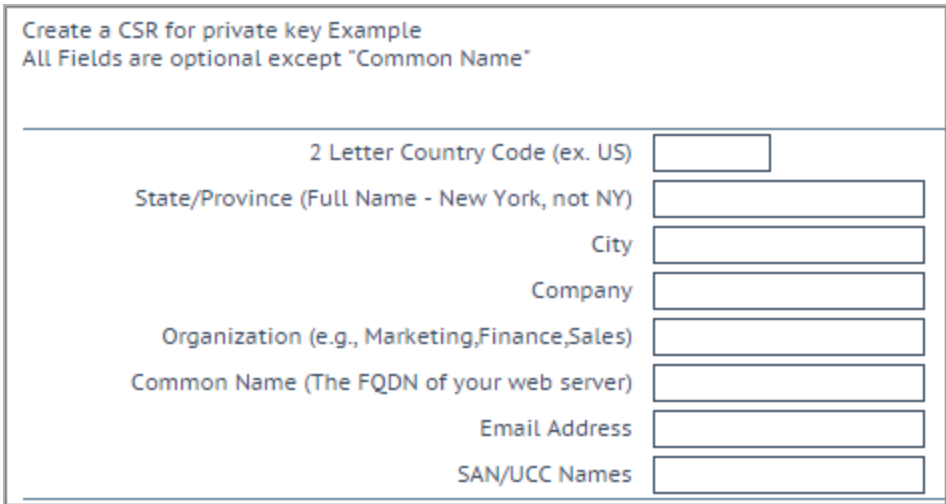
The Manage Certificates screen will appear.



2. Enter a unique name in the **Private Key Identifier** field for the RSA 2048 key you intend to store on the HSM.

The Private Key Identifier is the password. Make a note of it because you will need it.

3. Click **Generate CSR**.



4. Fill in the details in the resulting screen. The **Common Name** field is mandatory, all other fields are optional.

5. Click **Create CSR**.

The resulting key size will be 2048 bits.

The following is your 2048 bit *unsigned* certificate request. Copy the following, in its entirety, and send it to your trusted certificate authority

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC9zCCAd8CAQAwBgExCzAJBgNVBAYTA1VTMREwDwYDVQQIEwh0ZXcgW9yazER
MA8GA1UEBxMlTmV3IFlvcmsxGjAYBgNVBAoTFTVAgVGvjaG5vbG9naWZMR0w
GwYDVQQLExRlbm93bGVkZ2UgTWFuYXd1bWVudDEUMBIGA1UEAxMLRXhhbXBsZS5j
b20xKzApBgkqhkiG9w0BCQEWHGpibG9nZ3NAa2VtcHRlY2hub2xvZ211cy5jb20w
ggEiMA0GCSqGSIb3DQEBQUAA4IBDwAwggEKAoIBAQC+fCQ6Dx6VAHofGbqH01Ew
7j+DIpYXYt62I4NakrMzkFhkHEI6ond29p4s5Ntw0b2burBjUhw7HGV8kAkdMEx
VTZCSTvtF0k2mow6hk6+koF1K8kFcJomYcz5ZU0LICy2oGK8C34RBfes5DAYV7uv
Ks5SvWPhyC/10LZp/+g1sRtf7Nj0KvzIkIGdzSuFumCj1z+BvdSxf+gV2tqW81Nh
eMsuXbrhCyVhaohmz+Df03aubLOpFulyXpHopfOTCbc8mGn3y/xA0gKbdRAMjdZ
VMe6fzt6D1jKYr5W/PZa8UBr9RipVhr6TabluB9xsFVP5MrM5SvbHYDxAXWv9rw7
AgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEAZpDqjy+nt6rjuxI10JXUC31qJwY
sikrVVSr4dU31gWI8CJIU+YASecvtzSpU0yZKumdHeDSJH3CmYI81vn79xzbtT6b
3fDn0070NI+Tj07KWLfGszTIIo6/yvUOgcIvLaiHHbrXGJ1TLRLYGZMwMtoFE8+3
S1a5Z8ZxJZFp8Jho5iWjE5z0eRXa6Ah3wya/O3nM0i6W71/m1zfesQFkTy19+I5g
T7bm9z+pUrIhmQQkcoeJ4Y2FaZz8flt8pRuLLldivV8tCsa/qdX8mCiAnikQMDrN
a4e348uEH9j28WHS140EPNfM3KoAig5iBI6IbKAF3WmUkrBekQNg4MPeA==
-----END CERTIFICATE REQUEST-----
    
```

[<-Back](#)

6. The CSR is displayed.

7. Copy the CSR into a file and send it to your Certificate Authority for signing. The Certificate Authority will provide you with the certificate which will be put on the server.

Unlike a non-FIPS certificate operation, the private key is never displayed or available during this process. It is stored inside the HSM, and is completely inaccessible to the user.

### 3.2.4 Backup/Restore Certs

#### Certificate Backup

##### Backup Intermediate Certificates

Passphrase

Retype Passphrase

Create Backup File

##### Restore Intermediate Certificates

Intermediate Certificate Backup File  No file selected.

Passphrase

Restore Intermediate Certificates

**Backup Intermediate Certificates:** Create a backup of all intermediate certificates. The backup will be encrypted with the given passphrase.

### Caution

When backing up certificates, a mandatory passphrase (password) needs to be entered twice. The parameters of the passphrase are that it must be alpha-numeric and it is case sensitive with a maximum of 64 characters. This passphrase is a mandatory requirement to restore a certificate. A certificate cannot be restored without the passphrase. If it is forgotten, there is no way to restore the certificate.

**Intermediate Certificate Backup File:** browse to and select the intermediate certificate backup file

**Passphrase:** enter the passphrase associated with the certificate backup file

### 3.2.5 Cipher Sets

#### Cipher Set Management

Cipher Set Default

Available Ciphers

Filter:

Name	Strength
ECDHE-RSA-AES256-GCM-SHA384	High
ECDHE-ECDSA-AES256-GCM-SHA384	High
ECDHE-RSA-AES256-SHA384	High
ECDHE-ECDSA-AES256-SHA384	High
ECDHE-RSA-AES256-SHA	High
ECDHE-ECDSA-AES256-SHA	High
DH-DSS-AES256-GCM-SHA384	High
DHE-DSS-AES256-GCM-SHA384	High
DH-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-SHA256	High
DHE-DSS-AES256-SHA256	High
DH-RSA-AES256-SHA256	High
DH-DSS-AES256-SHA256	High

Assigned Ciphers

Filter:

Name	Strength
ECDHE-RSA-AES256-GCM-SHA384	High
ECDHE-ECDSA-AES256-GCM-SHA384	High
ECDHE-RSA-AES256-SHA384	High
ECDHE-ECDSA-AES256-SHA384	High
ECDHE-RSA-AES256-SHA	High
ECDHE-ECDSA-AES256-SHA	High
DH-DSS-AES256-GCM-SHA384	High
DHE-DSS-AES256-GCM-SHA384	High
DH-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-SHA256	High
DHE-DSS-AES256-SHA256	High
DH-RSA-AES256-SHA256	High
DH-DSS-AES256-SHA256	High

Save as: Default Save

### Cipher Set

Select the cipher set to view/modify.

The system-defined cipher sets are as follows:

- **Default:** The current default set of ciphers in the LoadMaster.
- **Default\_NoRc4:** The Default\_NoRc4 cipher set contains the same ciphers as the default cipher set, except without the RC4 ciphers (which are considered to be insecure).
- **BestPractices:** This is the recommended cipher set to use. This cipher set is for services that do not need backward compatibility - the ciphers provide a higher level of security. The configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7.
- **Intermediate\_compatibility:** For services that do not need compatibility with legacy clients (mostly Windows XP), but still need to support a wide range of clients, this configuration is recommended. It is compatible with Firefox 1, Chrome 1, IE 7, Opera 5 and Safari 1.
- **Backward\_compatibility:** This is the old cipher suite that works with clients back to Windows XP/IE6. This should be used as a last resort only.
- **WUI:** This is the cipher set recommended to be used as the WUI cipher set. The WUI cipher set can be selected in the **Admin WUI Access** screen. For further information, refer to the **Admin WUI Access** section.
- **FIPS:** Ciphers which conform to FIPS (Federal Information Processing Standards).
- **Legacy:** This is the set of ciphers that were available on the old LoadMaster firmware (v7.0-10) before OpenSSL was updated.

Refer to the **SSL Accelerated Services, Feature Description** on the [KEMP Documentation Page](#) for a full list of the ciphers supported by the LoadMaster, and a breakdown of what ciphers are in each of the system-defined cipher sets.

KEMP Technologies can change the contents of these cipher sets as required based on the best available information.

Two lists are displayed – **Available Ciphers** and **Assigned Ciphers**. These lists can be filtered by typing some text into the **Filter** text boxes provided. The **Filter** text boxes will only allow you to enter valid text which is contained in the cipher names, for example **ECDHE**. If invalid text is entered, the text box will turn red and the invalid text is deleted.

Ciphers can be dragged and dropped to/from the **Available** and **Assigned** lists as needed. Ciphers which are already assigned will appear greyed out in the **Available Ciphers** list.

Changes cannot be made to a preconfigured cipher set. However, you can start with a preconfigured cipher set – make any changes as needed and then save the cipher set with a new custom name. Enter the new name in the **Save as** text box and click the **Save** button. Custom cipher sets can be used across different Virtual Services and can be assigned as the WUI cipher set.

It is not possible to delete preconfigured cipher sets. However, custom cipher sets can be deleted by selecting the relevant custom cipher set and clicking the **Delete Cipher set** button.

### 3.2.6 OCSP Configuration

#### OCSP Server Settings

OCSP Server	<input type="text" value="10.11.0.35"/>	<b>Set Address</b>
OCSP Server Port	<input type="text" value="443"/>	<b>Set Port</b>
OCSP URL	<input type="text" value="/"/>	<b>Set Path</b>
Use SSL	<input type="checkbox"/>	
Allow Access on Server Failure	<input type="checkbox"/>	

#### OCSP Server

The address of the OCSP server.

#### OCSP Server Port

The port of the OCSP server.

#### OCSP URL

The URL to access on the OCSP server.

#### Use SSL

Select this to use SSL to connect to the OCSP server.

#### Allow Access on Server Failure

Treat an OCSP server connection failure or timeout as if the OCSP server had returned a valid response, that is, treat the client certificate as valid.

#### OCSP Stapling

Enable OCSP Stapling	<input type="checkbox"/>
OCSP Refresh Interval	<input type="text" value="1 Hour"/>

#### Enable OCSP Stapling

Select this check box to enable the LoadMaster to respond to OCSP stapling requests. If a client connects using SSL and asks for an OCSP response, this is returned. Only Virtual Service certificates are validated. The system holds a cache of OCSP responses that are sent back to the client. This cache is maintained by the OCSP daemon. When the OCSP daemon sends a request to the server, it uses the name specified in the certificate (in the **Authority Information Access** field). If it cannot resolve this name, then it uses the default OCSP server specified in the **OCSP Server** text box.

### **OCSP Refresh Interval**

Specify how often the LoadMaster should refresh the OCSP stapling information. The OCSP daemon caches the entry for up to the amount of time specified here, after which it is refreshed. Valid values range from 1 hour (default) to 7 days.

### 4 Appendix A - Cipher List

Delete all of the content and replace it with the below:

1. ECDHE-RSA-AES256-SHA384
2. ECDHE-ECDSA-AES256-SHA384
3. DHE-RSA-AES256-SHA256
4. DHE-DSS-AES256-SHA256
5. DH-RSA-AES256-SHA256
6. DH-DSS-AES256-SHA256
7. ECDH-RSA-AES256-SHA384
8. ECDH-ECDSA-AES256-SHA384
9. AES256-SHA256
10. AES256-SHA
11. ECDHE-RSA-AES128-SHA256
12. ECDHE-ECDSA-AES128-SHA256
13. DHE-RSA-AES128-SHA256
14. DHE-DSS-AES128-SHA256
15. DH-RSA-AES128-SHA256
16. DH-DSS-AES128-SHA256
17. ECDH-RSA-AES128-SHA256
18. ECDH-ECDSA-AES128-SHA256
19. AES128-SHA256
20. AES128-SHA
21. DES-CBC3-SHA

## References

Unless otherwise specified, the following documents can be found at:

<http://kemptechnologies.com/documentation>.

**Web User Interface (WUI), Configuration Guide**

**KEMP LoadMaster, Product Overview**

**DoD Common Access Card (CAC) Authentication, Feature Description**

**RESTful API, Interface Description**

**SSL Accelerated Services for the LM-5305 FIPS, Feature Description**



### Document History

Date	Change	Reason for Change	Ver.	Resp.
Nov 2014	Minor changes	Defects resolved	1.10	LB
Jan 2015	Release updates	Updates for 7.1-24	1.11	LB
Sep 2015	Release updates	Updates for 7.1-30	3.0	LB
Nov 2015	Minor updates	Enhancements made	4.0	LB
Jan 2016	Minor updates	Updated Copyright Notices	5.0	LB
Mar 2016	Release updates	Updates for 7.1-34	6.0	LB
July 2016	Release updates	Updates for 7.1.35	7.0	LB
Jan 2017	Release updates	Updates for 7.2.37	8.0	LB
Mar 2017	Release updates	Updates for 7.2.38	9.0	LB