

Feature Description

UPDATED: 07 December 2020



Copyright Notices

Copyright © 2002-2020 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	. 6
	1.1 Document Purpose	. 6
	1.2 Intended Audience	. 6
	1.3 Related Firmware Version	. 6
2	Create an SSL Accelerated Virtual Service	. 7
	2.1 Adding an SSL Virtual Service	. 7
	2.2 Adding an SSL Certificate	.11
	2.3 Checking Certificate Installations	15
	2.4 Intermediate Certificates	.15
	2.5 Importing Intermediate Certificates	.16
	2.5.1 Invalid Certificate Formats	. 17
	2.6 IIS Certificates	. 17
	2.7 Re-encrypt SSL	. 18
	2.8 Assigning a Client Certificate for Re-encryption	. 18
	2.9 Certificate Signing Request (CSR)	.20
	2.10 Backup/Restore Certificates	.20
	2.11 SSL Ciphers	.21
	2.11.1 Cipher Set Management	. 24
	2.11.2 Certificate Considerations for Various Cipher Suites	25
	2.11.2.1 DH-RSA- and DHE-RSA- Cipher Suites	.25
	2.11.2.2 DH-DSS- and DHE-DSS- Cipher Suites	. 25



	2.11.2.3 ECDH-ECDSA- and ECDHE-ECDSA- Cipher Suites
	2.12 WUI Root Certificate Installation
	2.13 OCSP Configuration
	2.13.1 OCSP Server Settings
	2.14 Setting the Diffie-Hellman Key Exchange Size
3	WUI Options
	3.1 SSL Properties
	3.2 Certificates & Security
	3.2.1 SSL Certificates
	3.2.2 Intermediate Certificates
	3.2.3 Generate CSR (Certificate Signing Request)
	3.2.4 Backup/Restore Certs
	3.2.5 Cipher Sets
	3.2.6 Remote Access
	3.2.7 OCSP Configuration
4	Appendix A
	4.1 Default Cipher Set
	4.2 Default_NoRc4 Cipher Set
	4.3 Best Practices Cipher Set
	4.4 Intermediate_compatibility Cipher Set
	4.5 Backward_compatibility Cipher Set
	4.6 WUI Cipher Set



La	ast Updated Date	.66
Re	eferences	65
	4.11 ECDSA_BestPractices Cipher Set	.64
	4.10 ECDSA_Default Cipher Set	63
	4.9 Null_Ciphers Cipher Set	.63
	4.8 Legacy Cipher Set	.62
	4.7 FIPS Cipher Set	.62

1 Introduction



1 Introduction

Kemp 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 products optimize web and application infrastructure as defined by high-availability, highperformance, flexible scalability, security and ease of management. They maximize the total cost-ofownership 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.

1.3 Related Firmware Version

Published with LMOS version 7.2.48.3 LTS. This document has not required changes since 7.2.48.3 LTS. However, the content is in sync with the latest LoadMaster LTS firmware.



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		
Port 80		
Service Name (Optional)		
Protocol tcp		
	Cancel	Add this Virtual Service

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 CTLS1.1 CTLS1.2 TLS1.3		
Require SNI hostname			
Certificates	Self Signed Certificates Assigned Certificates Available Certificates Assigned Certificates None Available > Manage Certificates Set Certificates		
Cipher Set Default Assigned Ciphers ECDHE-ECDSA-AES256-GCM-SHA384 Ciphers Ciphers DHE-DSS-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-RSA-CHACHA20-POLY1305			
Client Certificates	ertificates No Client Certificates required		
Strict Transport Security Header	trict Transport Security Header Don't add the Strict Transport Security Header 🔹		

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 check boxes in the **Supported Protocols** section allow you to specify which protocols should be supported by the Virtual Service. By default, TLS1.1, TLS1.2, and TLS1.3 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.





Server connections are only restricted by the configuration of the Real Servers, regardless of the TLS version selected on the client side. Each Real Server can be configured independently of the others. The LoadMaster negotiates connections according to the requirements of each Real Server.

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, <u>www.kemptechnologies.com</u> 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.

There is a limit of 8171 characters when assigning certificates to a Virtual Service using the WUI.

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.

Please Specify the Parameters for the Real Server	
Real Server Address	
Port	80
Forwarding method	nat 🔻
Weight	1000
Connection Limit	
	<-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

If you have a Certificate Authority (CA)-signed certificate to use with an SSL-enabled Virtual Service, 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	
Certificates	Self Signed Certificate in use. Available Certificates None Available Set Certificates Manage Certificates
Ciphers	Cipher Set Default Assigned Ciphers CDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES256-SHA384 ECDHE-ECDSA-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.

L	ayer	Certificate Installed
	L7	Add New
	L7	Add New

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



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



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

Please specify the name of the file that contains the certificate. The file can also hold the private key. If the file does not contain the private key, then the file containing the private key must also be specified. The certificate can be in either .PEM or .PFX (IIS) format.		
Certificate File	Choose File	No file chosen
Key File (optional)	Choose File	No file chosen
Pass Phrase		
Certificate Identifier		

The certificate and key file can be added from this screen. The Passphrase (password) that the certificate was created with will need to be entered. The certificate can be given a name in the **Certificate Identifier** text box.

To import a certificate, follow the steps below:

1. Click the **Choose File** button next **Certificate File** and select the required certificate file.

The certificate file cannot have the following in the filename: **ident, cfile, kfile, ffile, replace, password**. If it does, an **Invalid Certificate Identifier** error message appears.

- 2. Click the **Choose File** button next to **Key File** and select the relevant key file, if required.
- 3. Enter the relevant pass phrase in the **Pass Phrase** text box (if required).
- 4. Enter a recognisable name in the **Certificate Identifier** text box.
- 5. Click **Save**.



Transactions Per Second (TPS) Performance will vary based on key length. Larger keys will reduce performance.

Certificate Configuration					
Identifier	Common Virtual Name(s) Services	Assignment			
ExampleCertificate	: james [Expires: Jul 27 15:51:48 2016 GMT]	Available VSs 10.154.11.61:80	_ > 1(<	Assigned VSs 0.154.11.62:80	Save Changes

6. 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**.

SSL Acceleration	Enabled: 🗹 Reencrypt: 🗆
Supported Protocols	SSLv3 @TLS1.0 @TLS1.1 @TLS1.2
Require SNI hostname	
Certificates	Self Signed Certificate in use. Available Certificates ExampleCertificate [Example] Set Certificates Set Certificates
Ciphers	Manage Certificates Cipher Set Default Modify Cipher Set Assigned Ciphers ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES256-SHA384 ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA ECDHE-ECDSA-AES256-SHA
Client Certificates	No Client Certificates required

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

If you add a certificate to the LoadMaster in version 7.2.51 or later (or in 7.2.48.3 LTS or a later LTS version) and then downgrade to 7.2.50 or an earlier version (or 7.2.48.2 LTS or an earlier version) - the certificate will not work. To work around this, create a backup of all SSL certificates before downgrading and then restore the certificates after downgrading (**Certificates & Security > Backup/Restore Certs**). If you forget to take the backup before downgrading: upgrade the firmware again, take the certificate backup, downgrade, and then restore the certificate backup.



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).

Certificate						
Ge	eneral Details Certification Path					
	Certificate Information					
	This certificate is intended for the following purpose(s):					
	•Ensures the identity of a remote computer					
	Issued to:					
	Issued by:					
	Valid from 12/17/2009 to 12/18/2011					
	Install Certificate					
	ОК					

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. 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. If you have questions on whether or not you should have received an intermediate certificate from your CA vendor, contact your CA vendor.

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 Importing 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.

Your CA vendor may have provided the required intermediate certificates in the same bundle as the certificate itself, and so these would be installed together. The method documented in this section should be used when you are installing one or more intermediate certificates alone.

The intermediate certificate formats that are officially supported by the LoadMaster are: .PEM, .CER, and .CRT.

A CER file can only be encoded and exported in Base-64 format for it to be uploaded to the LoadMaster. A CER file exported in a DER binary format is not supported on the LoadMaster and the LoadMaster is unable to upload this format.

This section provides steps on how to apply and upload intermediate certificates and how to resolve any invalid certificate formats.

To import an intermediate certificate to the LoadMaster complete the following steps:

1. Navigate to **Certificates & Security > Intermediate Certs** in the main menu.

Add a new Intermediate Certificate	
Intermediate Certificate	Choose File No file chosen
Certificate Name	Example Intermediate Certific Add Certificate



- 2. Click Choose File.
- 3. Browse to and select the required intermediate certificate file.

4. Enter the **Certificate Name**. This name is used on the LoadMaster to help you manage your certificates.

- 5. Click Add Certificate.
- 6. Click **OK**.

These intermediate certificates do not need to be associated with any Virtual Service certificates. The LoadMaster automatically builds 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.

2.5.1 Invalid Certificate Formats

If you follow the steps to upload an intermediate certificate to the LoadMaster and receive a **Certificate Format Invalid** error, it means the certificate file you are trying to upload is unsupported or is not in one of the formats required by LoadMaster (PEM, CER, CRT).

The standard PEM file format can be uploaded to the LoadMaster.

For details on how to convert other certificate formats to a PEM format using OpenSSL commands, refer to the following article: Using OpenSSL To Convert Certificate Formats.

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** 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 Acceleration	Enabled: 🗹 Reencrypt: 🗹
Supported Protocols	SSLv3 @TLS1.0 @TLS1.1 @TLS1.2
Require SNI hostname	
Certificates	Self Signed Certificate in use. Available Certificates ExampleCertificate [Example] Manage Certificates Manage Certificates
Ciphers	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-ECDSA-AES256-SHA ECDHE-ECDSA-AES256-SHA
Client Certificates	No Client Certificates required
Reencryption Client Certificate	None required
Reencryption SNI Hostname	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**.



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]		Available VSs 10.154.11.61:80 10.154.11.62:80	* > < *	Assigned VSs None Assigned	+	Save Changes
VSs using Example	Certificate for Re	encryption	Available VSs None Assigned	× ×	Assigned V5s 10.154.11.61:80	+	Save Changes

- 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: 🗹 Reencrypt: 🗹
Supported Protocols	□SSLV3 ✔TLS1.0 ✔TLS1.1 ✔TLS1.2 ✔TLS1.3
Require SNI hostname	
Certificates	Self Signed Certificate in use. Available Certificates None Available Set Certificates Manage Certificates
Ciphers	Cipher Set Default Assigned Ciphers ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 DHE-DSS-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-RSA-CHACHA20-POLY1305
Client Certificates	No Client Certificates required
Reencryption Client Certificate	None required
Reencryption SNI Hostname	Set SNI Hostname
Strict Transport Security Header	Don't add the Strict Transport Security Header
Intermediate Certificates	Using all installed Intermediate certificates Show Intermediate Certificates

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

2.9 Certificate Signing Request (CSR)

You can create a CSR for submission to your signing authority of choice. Using the WUI, navigate to **Certificates & Security > Generate CSR**. Fill in the information and click **Create CSR**. CSRs generated by the LoadMaster use SHA256.

Caution

Store the private key in a vault. The private key will be required once the authority creates the certificate.

2.10 Backup/Restore Certificates

The LoadMaster supports exporting of all certificate information. This includes private key, host and intermediate certificates. The export file is designed to be used for import into another LoadMaster and is encrypted. You can import and export certificates using the WUI at **Certificates & Security > Backup/Restore Certs.** Ensure to note the passphrase used to create the export - it is required to complete the import.





There are options to restore only Virtual Service certificates including private keys, intermediate certificates, or both.

2.11 SSL Ciphers

The LoadMaster supports SSLv3, TLS1.0, TLS1.1, TLS1.2, and TLS1.3.

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

 SSL Properties 			
SSL Acceleration	Enabled: 🗹 Reencrypt: 🗆		
Supported Protocols	□SSLv3 □TLS1.0 @TLS1.1 @TLS1.2 @TLS1.3		
Require SNI hostname			
Certificates	Self Signed Certificates Assigned Certificates Available Certificates Assigned Certificates None Available > > Manage Certificates Set Certificates		
Ciphers	Cipher Set Default Assigned Ciphers ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 DHE-DSS-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305 CDHE-RSA-CHACHA20-POLY1305		
Client Certificates	No Client Certificates required		
Strict Transport Security Header	Don't add the Strict Transport Security Header		

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**.

CHACHA20-POLY1305 ciphers are given special preference when they appear in both the client and LoadMaster cipher lists. If these ciphers appear at the top of the client preference list, the LoadMaster will prioritize using CHACHA20-POLY1305 ciphers for the connection, regardless of the position of these ciphers in the LoadMaster's cipher list.

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.
- 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.
- Null_Ciphers: Direct Access uses IP-HTTPS, which applies its own layer of encryption.
- **ECDSA_Default:** This is a non-RSA version of the default cipher set.
- **ECSDA_BestPractices:** This is a non-RSA version of the best practices cipher set.

Refer to **Appendix A** 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 reserves the right to change the contents of these cipher sets as required.

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.

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.

kemp.ax





Server connections are only restricted by the configuration of the Real Servers, regardless of the TLS version selected on the client side. Each Real Server can be configured independently of the others. The LoadMaster negotiates connections according to the requirements of each Real Server.



2.11.1 Cipher Set Management

ipher Set Default	¥			
vailable Ciphers Filter:			Assigned Ciphers Filter:	
Name	Strength	<u> </u>	Name	Strength
ECDHE-RSA-AES256-GCM-SHA384	High		ECDHE-RSA-AES256-GCM-SHA384	High
ECDHE-ECDSA-AES256-GCM-SHA384	High		ECDHE-ECDSA-AES256-GCM-SHA384	High
ECDHE-RSA-AES256-SHA384	High		ECDHE-RSA-AES256-SHA384	High
ECDHE-ECDSA-AES256-SHA384	High		ECDHE-ECDSA-AES256-SHA384	High
ECDHE-RSA-AES256-SHA	High		ECDHE-RSA-AES256-SHA	High
ECDHE-ECDSA-AES256-SHA	High		ECDHE-ECDSA-AES256-SHA	High
DH-DSS-AES256-GCM-SHA384	High		DH-DSS-AES256-GCM-SHA384	High
DHE-DSS-AES256-GCM-SHA384	High		DHE-DSS-AES256-GCM-SHA384	High
DH-RSA-AES256-GCM-SHA384	High		DH-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-GCM-SHA384	High		DHE-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-SHA256	High		DHE-RSA-AES256-SHA256	High
DHE-DSS-AES256-SHA256	High		DHE-DSS-AES256-SHA256	High
DH-RSA-AES256-SHA256	High		DH-RSA-AES256-SHA256	High
DH-DSS-AES256-SHA256	High	-	DH-DSS-AES256-SHA256	High

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-MND5 SSLv3 and RC4-MND5 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.

2.11.2 Certificate Considerations for Various Cipher Suites

When you create or request SSL certificates to be used in combination with a particular cipher suite, you must be aware of the following:

- Different cipher suites require different signing algorithms to be used when creating server and client certificates.
- Some cipher suites are designed to reject self-signed certificates, as an added level of security.

The following sections outline specific requirements for various cipher suites supported by the LoadMaster.

This information is not specific to the LoadMaster, but to the design of the cipher suites themselves.

2.11.2.1 DH-RSA- and DHE-RSA- Cipher Suites

This section applies to all ciphers with names beginning:

- DH-RSA-
- DHE-RSA-

As indicated in the names, these ciphers require RSA signing to be used in certificates. Additionally, the certificate cannot be a self-signed certificate. Therefore, when creating a Certificate Signing Request (CSR) for a certificate to be used with this cipher, ensure to specify an RSA-signed certificate.

2.11.2.2 DH-DSS- and DHE-DSS- Cipher Suites

This section applies to all ciphers with names beginning:



- DH-DSS-
- DHE-DSS-

As indicated in the names, these ciphers require DSS (also known as DSA) signing to be used in certificates. Additionally, the certificate cannot be a self-signed certificate. Therefore, when creating a CSR for a certificate to be used with this cipher, ensure to specify a DSS-signed certificate.

2.11.2.3 ECDH-ECDSA- and ECDHE-ECDSA- Cipher Suites

This section applies to all ciphers with names beginning:

- ECDH-ECDSA-
- ECDHE-ECDSA-

As implied by the names, these ciphers require an ECDSA certificate, but it can be self-signed.

For these ciphers, the following openssl command line example from a Linux system creates a selfsigned certificate for testing with the proper SSL options. The second command concatenates the key and certificate into a single file for input into the LoadMaster WUI.

openssl ecparam -name secp521r1 -param_enc named_curve -genkey -out privatekey.pem openssl req -new -x509 -key private-key.pem -out server-pub.pem -days 730

```
cat private-key.pem server-pub.pem > server.pem
```

The **-param_enc explicit** option must not be used in the command line above, or the resulting certificate will be rejected when used to negotiate a secure connection.

If you plan to use a certificate signed by a Certificate Authority (CA), ensure to specify an ECDSAsigned certificate when creating a CSR for a certificate to be used with this cipher.

2.12 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.

2.13 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.

2.13.1 OCSP Server Settings

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

OCSP Server Settings		
OCSP Server	10.11.0.35	Set Address
OCSP Server Port	443 Set Port	
OCSP URL	/	Set Path
Use SSL		
Allow Access on Server Failure		

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 Checking	
Enable OCSP Checking	

OCSP Checking

Select the **Enable OCSP Checking** check box to enable the LoadMaster to perform OCSP checks on certain outbound connections. This is disabled by default.

OCSP Stapling	
Enable OCSP Stapling	☐
OCSP Refresh Interval	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 24 hours.



2.14 Setting the Diffie-Hellman Key Exchange Size

The Diffie-Helman 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	
Connection Timeout (secs)	660 Set Time (Valid values:0, 60-86400)
Enable Non-Local Real Servers	
Enable Alternate GW support	
Enable TCP Timestamps	
Enable TCP Keepalives	
Enable Reset on Close	
Subnet Originating Requests	
Enforce Strict IP Routing	
Handle non HTTP Uploads	
Enable Connection Timeout Diagnostics	
Legacy TCP Timewait handling	
Enable SSL Renegotiation	
Force Real Server Certificate Checking	
Size of SSL Diffie-Hellman Key Exchange	1024 Bits 🗸
Log SSL errors	Fatal errors only
Openssl version	Use current SSL library + TLS 1.3 🗸
Use Default Route Only	
HTTP(S) Proxy	10.154.11.180 Set HTTP(S) Proxy

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**.



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

3.1 SSL Properties

 SSL Properties 			
SSL Acceleration Supported Protocols Require SNI hostname	Enabled: 🗹 Reencrypt: 🗌 SSLv3 OTLS1.0 🗹 TLS1.1 🗹 TLS1.2 🗹 TLS1.3		
Certificates	Self Signed Certificates In use. Available Certificates None Available Set Certificates Manage Certificates		
Ciphers	Cipher Set Default Assigned Ciphers ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-RSA-CHACHA20-POLY1305		
Client Certificates	No Client Certificates required		
Strict Transport Security Header	Don't add the Strict Transport Security Header		
Intermediate Certificates	Using all installed Intermediate certificates Available Certificates None Available		

SSL Acceleration

This check box appears when the criteria for SSL Acceleration have been met. Select this check box 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. You can add a certificate by clicking **Manage Certificates** and importing or adding a certificate.

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

You cannot use Extra Ports or Transparency with SSL reencryption.



Reversed: Selecting this check box means that the data from the LoadMaster to the Real Server is re-encrypted. The input stream must not be encrypted, for example, the client sends HTTP port 80 traffic to the LoadMaster and the LoadMaster sends HTTPS port 443 traffic to the Real Server. 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

The check boxes in the **Supported Protocols** section enable you to specify which protocols are supported by the Virtual Service. By default, TLS1.1, TLS1.2, and TLS1.3 are enabled and SSLv3 and TLS1.0 are disabled.

The **TLS1.3** check box will not be visible if the **OpenSSL Version** setting in **System Configuration > Miscellaneous Options > Network Options** is set to **Use older SSL library - no TLS 1.3**. For further details, refer to the **Network Options** section for further details.

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.





Server connections are only restricted by the configuration of the Real Servers, regardless of the TLS version selected on the client side. Each Real Server can be configured independently of the others. The LoadMaster negotiates connections according to the requirements of each Real Server.

Add Received Cipher Name

In LoadMaster version 7.2.52 and above, when this option is enabled, the LoadMaster adds X-SSL headers containing client SSL information such as TLS version, TLS cipher, client certificate serial number, and SNI host. For further details, refer to the following article: <u>SSL Information in Client</u> <u>Request Headers</u>.

Require SNI hostname

If require Server Name Indication (SNI) is selected, the hostname is always 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 note that the root domain name is not 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, <u>www.kemptechnologies.com</u> is matched until a wildcard of *.kemptechnologies.com. Kemptechnologies.com is not matched.

To send SNI host information in HTTPS health checks, 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.

Pass through SNI hostname



In LoadMaster firmware version 7.2.52 and above, when this option is enabled and when reencrypting, the received SNI hostname is passed through as the SNI to be used to connect to the Real Server. For further details, refer to the following article: <u>Ability To Use SNI In SubVS In Addition</u> <u>To SNI Hostname Pass Through</u>.

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.

There is a limit of 8171 characters when assigning certificates to a Virtual Service using the WUI.

A Virtual Service can be configured using both RSA and ECC certificates. However, if an RSA and an ECC certificate have the same common name, for example, kemp.com, the first certificate is preferred. If the ECC certificate is first in the list, and a client does not have an ECC cipher, the connection fails. Conversely, if the RSA certificate is first in the list, and a client does not have an RSA cipher, the connection fails.

The total number of certificates that you can add to a Virtual Service is 256, but this number may be further limited by the size of the certificate file names used. In LMOS Version 7.2.47 and later releases, the number of characters in each certificate file name and extension (not counting the period between them), plus all spaces used to separate multiple file names, must add up to 8176 characters or less (in earlier releases, the limitation is 1023 characters.)

Clicking Manage Certificates brings you to the SSL Certificates screen.

If you add a certificate to the LoadMaster in version 7.2.51 or later (or in 7.2.48.3 LTS or a later LTS version) and then downgrade to 7.2.50 or an earlier version (or 7.2.48.2 LTS or an earlier version) - the certificate will not work. To work around this, create a backup of all SSL certificates before downgrading and then restore the certificates after downgrading (**Certificates & Security** >



Backup/Restore Certs). If you forget to take the backup before downgrading: upgrade the firmware again, take the certificate backup, downgrade, and then restore the certificate backup.

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 preauthenticated certificate in the LoadMaster.

Reencryption SNI Hostname

Specify the Server Name Indication (SNI) hostname to use 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 one of the system-defined cipher sets or a user-customized cipher set. You can select system-defined cipher sets to quickly and easily select and apply the relevant ciphers. You can create and modify custom cipher sets by clicking **Modify Cipher Set**.

Ciphers

The **Ciphers** list is read only and displays a list of the currently assigned ciphers. Clicking **Modify Cipher Set** brings 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 accepts HTTPS requests from any client. Selecting any of the other values below requires all clients to present a valid client certificate. In addition, the LoadMaster also passes information about the certificate to the application.

You should not change this option 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.

Strict Transport Security Header

Enable this option to add the Strict-Transport-Security header to all LoadMaster-generated messages (ESP and error messages). The options in this drop-down list are as follows:

- Don't add the Strict Transport Security Header
- Add the Strict Transport Security Header no subdomains
- Add the Strict Transport Security Header include subdomains

Intermediate Certificates

Prior to the **Intermediate Certificates** field being added to the **SSL Properties** section, there was no ability to assign intermediate or root certificates to a Virtual Service. The Certificate Authority (CA) for client certificates was kept in the global certificate store, so the following could occur:

- Client certificates from two different CAs are installed on the LoadMaster
- Client A presents a certificate issued from CA 1 and as a network administrator, you only want them to be able to access Virtual Service 1.



- Client B presents a certificate issued from CA 2 and as a network administrator, you only want them to be able to access Virtual Service 2.
- Because both client certificates are validated against the global LoadMaster trust store, client A is also allowed access to Virtual Service 2 and client B is also allowed access to Virtual Service 1.

The **Intermediate Certificates** field allows you to assign intermediate and root certificates to specific Virtual Services. This provides the ability to restrict access. For example, when this is configured correctly for the scenario above - Client A will only have access to Virtual Service 1 and Client B will only have access to Virtual Service 2.

It is not possible to unassign all certificates from the Virtual Service. If you do not want client certificates to be required - select **No Client Certificates required** in the **Client Certificates** drop-down list.

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

Certificate 0	onfiguration	Import Certificate Add Intermediate
Identifier	Common Virtual Name(s) Services	Operation
ExampleCertifica	e james Available VSs Assigned VSs ID. 154.11.61:80 ASSIGNED VSs Save Changes	New CSR Replace Certificate Delete Certificate Reencryption Usage
Administrative Certificates		

Shown above is the **Manage Certificates** screen. Details about the various options on this screen are below:

Import Certificate – to import the certificate with a chosen filename.

Add Intermediate – refer to the Intermediate Certificates section for further information.

Identifier – is the name given to the certificate at the time it was created.

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

Virtual Services – the Virtual Service with which the certificate is associated.

Assignment – lists of available and assigned Virtual Services

3 WUI Options



Operations –

• New CSR – generates a new Certificate Signing Request (CSR) based on the current certificate.

If the certificate has Subject Alternative Names (SANs), generating a CSR in this way will not add the SANs. Instead, generate the CSR manually. For further information on this, refer to the **Generate CSR (Certificate Signing Request)** section.

- **Replace Certificate** updates or replaces the certificate stored in this file.
- **Delete Certificate** deletes the relevant certificate.
- **Reencryption Usage** display the Virtual Services that are using this certificate as a client certificate when re-encrypting.

Administrative Certificates – the certificate you want to use, if any, for the administrative interface.

TPS Performance will vary based on key length. Larger keys reduce performance.

3.2.2 Intermediate Certificates

Currently installed Intermediate Certific	cates	
Name		Operation
VeriSignCert.pem		Delete
Add a new Intermediate Certificate		
Intermediate Certificate	Choose File No file chosen	
Certificate Name	A	dd 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	ExampleIntermediateCertific 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)

If you do not have a certificate, you may complete the Certificate Signing Request (CSR) form and click the **Create CSR** button. CSRs generated by the LoadMaster use SHA256.

If **Self-Signed Certificate Handling** is set to **EC certs with an EC signature** (in **Certificates & Security > Remote Access**), CSR generation is restricted to the administrative (**bal**) user only. If **Self-Signed Certificate Handling** is set to a different value, all users (regardless of their permissions) can generate CSRs.

All Fields are optional except "Common Name"	
2 Letter Country Code (ex. US) State/Province (Full Name - New York, not NY) City Company Organization (e.g., Marketing,Finance,Sales) Common Name (The FQDN of your web server) Email Address	
Generate Elliptic Curve Request	Reset Create CSR

2 Letter Country Code (ex. US)

The 2 letter country code that should be included in the certificate, for example **US** should be entered for the United States.

kemp.ax

3 WUI Options



State/Province (Entire Name - New York, not NY)

The state which should be included in the certificate. Enter the full name here, for example **New York**, not NY.

City

The name of the city that should be included in the certificate.

Company

The name of the company which should be included in the certificate.

Organization (e.g., Marketing, Finance, Sales)

The department or organizational unit that should be included in the certificate.

Common Name

The Fully Qualified Domain Name (FQDN) for your web server.

Email Address

The email address of the responsible person or organization that should be contacted regarding this certificate.

SAN/UCC Names

A space-separated list of alternate names.

Generate Elliptical Curve Request

Select this check box to generate an Elliptical Curve (EC) request instead of an RSA request.

Display Private Key

This new option (introduced in LoadMaster firmware version 7.2.52 and LTS version 7.2.48.3) appears only when the **Certificates & Security > Remote Access > Self-Signed Certificate Handling** option is set to **EC certs with an EC signature** which means that an elliptical curve cipher is used for both the certificate and the digital signature.

Once the above option is selected, a **Display Private Key** check box appears on the **Certificates & Security > Generate CSR** WUI page.

• When **Display Private Key** is disabled (the default), the private key is not displayed in the WUI after the CSR is created. The unsigned CSR is downloaded by the user as in previous releases. Once it is signed by a Certificate Authority, the user uploads the signed certificate to



the LoadMaster - the difference from previous releases being that the user does not have to also upload the private key, since LoadMaster maintains it internally when **Display Private Key** is disabled. If the saved private key matches the new certificate, the certificate gets imported and the saved private key is deleted. The stored private key is not encrypted but there is no access to it from the outside and it cannot be seen or displayed.

• When **Display Private Key** is enabled, the LoadMaster behaves as in previous releases: the private key is displayed to the user and must be uploaded to LoadMaster along with the private key.

There is only one private key per machine and it is not shared between High Availability (HA) pairs. This means the newly-generated certificate must be installed on the machine that the CSR was generated on.

Alter clicking the **Create CSR** button, the following screen appears:





The top part of the screen should be copied and pasted into a plain text file and sent to the Certificate Authority of your choice. They will validate the information and return a validated certificate.



The lower part of the screen is your private key and should be kept in a safe place. This key should not be disseminated as you will need it to use the certificate. Copy and paste the private key into a plain text file (do not use an application such as Microsoft Word) and keep the file safe.

3.2.4 Backup/Restore Certs

Certificate Backup	
Backup all VIP and Intermediate Certificates	
Passphrase	Create Baskup File
Retype Passphrase	Create Backup File
Restore Certificates	
Backup File	Choose File No file chosen
Which Certificates	What to restore
Passphrase	Restore Certificates

Backup all VIP and Intermediate Certificates: When backing up certificates, you are prompted to enter a mandatory passphrase (password) twice. The parameters of the passphrase are that it must be alpha-numeric and it is case sensitive with a maximum of 64 characters.

Caution: This passphrase is a mandatory requirement to restore a certificate. You cannot restore a certificate without the passphrase. If you forget it, there is no way to restore the certificate.

Backup File: select the certificate backup file

Which Certificates: select which certificates you wish to restore

Passphrase: enter the passphrase associated with the certificate backup file



3.2.5 Cipher Sets

ipher Set Default	•			
vailable Ciphers Filter:			Assigned Ciphers Filter:	
Name	Strength	-	Name	Strength
ECDHE-RSA-AES256-GCM-SHA384	High		ECDHE-RSA-AES256-GCM-SHA384	High
ECDHE-ECDSA-AES256-GCM-SHA384	High		ECDHE-ECDSA-AES256-GCM-SHA384	High
ECDHE-RSA-AES256-SHA384	High		ECDHE-RSA-AES256-SHA384	High
ECDHE-ECDSA-AES256-SHA384	High		ECDHE-ECDSA-AES256-SHA384	High
ECDHE-RSA-AES256-SHA	High		ECDHE-RSA-AES256-SHA	High
ECDHE-ECDSA-AES256-SHA	High		ECDHE-ECDSA-AES256-SHA	High
DH-DSS-AES256-GCM-SHA384	High		DH-DSS-AES256-GCM-SHA384	High
DHE-DSS-AES256-GCM-SHA384	High		DHE-DSS-AES256-GCM-SHA384	High
DH-RSA-AES256-GCM-SHA384	High		DH-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-GCM-SHA384	High		DHE-RSA-AES256-GCM-SHA384	High
DHE-RSA-AES256-SHA256	High		DHE-RSA-AES256-SHA256	High
DHE-DSS-AES256-SHA256	High		DHE-DSS-AES256-SHA256	High
DH-RSA-AES256-SHA256	High		DH-RSA-AES256-SHA256	High
DH-DSS-AES256-SHA256	High	-	DH-DSS-AES256-SHA256	High

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.

The ciphers in the **Best Practices** cipher set were updated in LoadMaster firmware version 7.2.52. For further details, including a list of the ciphers, refer to the following article: <u>Best</u> <u>Practices Cipher Set Updated</u>.

- **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.
- Null_Ciphers: Direct Access uses IP-HTTPS which applies its own layer of encryption.
- ECDSA_Default: This is a non-RSA version of the default cipher set.
- ECSDA_BestPractices: This is a non-RSA version of the best practices cipher set.

Refer to <u>Appendix A of the SSL Accelerated Services Feature Description</u> 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 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. iThe **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 Remote Access

There are some SSL-related fields on the **Remote Access** screen. These are described below.

Administrator Access	
Allow Remote SSH Access	Using: All Networks V Port: 22 Set Port
SSH Pre-Auth Banner	Set Pre-Auth Message
Allow Web Administrative Access	✓ Using: eth0: 10.35.48.17 ▼ Port: 443
Admin Default Gateway	Set Administrative Access
Allow Multi Interface Access	
Enable API Interface	Port: via 443 Set Port
Self-Signed Certificate Handling	EC certs with a RSA signature 🔻
Outbound Connection Cipher Set	BestPractices v
Admin Login Method	Password Only Access (default) • Only Password mode is available if no Pre-Auth Banner is specified
Enable Software FIPS 140-2 level 1 Mode	Enable Software FIPS mode
Enable Kemp Analytics	

Self-Signed Certificate Handling

Select the type of self-signed certificates that the system will use. The options are described below:

- **RSA self-signed certs:** By default, these are RSA certificates that are signed with the Kemp RSA root certificate
- **EC certs with a RSA signature:** The LoadMaster can generate an EC certificate also signed by the original RSA Kemp root certificate.
- EC certs with an EC signature: The LoadMaster can generate an EC certificate signed by the Kemp EC root certificate. I this mode, any CSRs generated will also be EC.

If **Self-Signed Certificate Handling** is set to **EC certs with an EC signature**, CSR generation is restricted to the administrative (**bal**) user only. If **Self-Signed Certificate Handling** is set to a

3 WUI Options



different value, all users (regardless of their permissions) can generate CSRs.

You should not switch from **RSA self-signed certs** to **EC certs with an EC signature** directly. If you do this, connections will fail because there is no EC Kemp Certificate Authority (CA) certificate. To workaround this, you must first switch from **RSA self-signed certs** to **EC certs with a RSA signature**.





Then, download the new EC Kemp CA certificate by clicking **Download ECC Root Cert** in the bottom-right of the WUI under the main menu after refreshing the page. When this certificate has been downloaded, you can switch to **EC certs with an EC signature** with no loss of connection.



Outbound Connection Cipher Set

Select the cipher set to use on outbound connections (OCSP, email, LDAP, and so on). This is global for all outbound connections. For information on each of the cipher sets available, refer to the **Cipher Sets** section.

Re-encrypt connections are not affected by this.

3.2.7 OCSP Configuration

OCSP Server Settings		
OCSP Server	10.11.0.35	Set Address
OCSP Server Port	443 Set Port	
OCSP URL	/	Set Path
Use SSL		
Allow Access on Server Failure		

OCSP Server

The address of the OCSP server. This can either be in IP address or Fully Qualified Domain Name (FQDN) format.

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 Checking

Select the **Enable OCSP Checking** check box to enable the LoadMaster to perform OCSP checks on certain outbound connections. This is disabled by default.

OCSP Stapling	
Enable OCSP Stapling OCSP Refresh Interval	1 Hour V

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 24 hours.

4 Appendix A



4 Appendix A

Each of the following sub-sections provides a list of ciphers in each of the system-defined cipher sets that exist in the LoadMaster.

4.1 Default Cipher Set

Following is a full list of the ciphers supported by the LoadMaster. These are the ciphers that are in the **Default** system-defined cipher set:

AES128-GCM-SHA256 AES128-SHA AES128-SHA256 AES256-GCM-SHA384 AES256-SHA AES256-SHA256 CAMELLIA128-SHA CAMELLIA256-SHA DES-CBC3-SHA DH-DSS-AES128-GCM-SHA256 DH-DSS-AES128-SHA DH-DSS-AES128-SHA256 DH-DSS-AES256-GCM-SHA384 DH-DSS-AES256-SHA DH-DSS-AES256-SHA256 DH-DSS-CAMELLIA128-SHA DH-DSS-CAMELLIA256-SHA DH-DSS-DES-CBC3-SHA DHE-DSS-AES128-GCM-SHA256 DHE-DSS-AES128-SHA DHE-DSS-AES128-SHA256 DHE-DSS-AES256-GCM-SHA384 DHE-DSS-AES256-SHA DHE-DSS-AES256-SHA256 DHE-DSS-CAMELLIA128-SHA DHE-DSS-CAMELLIA256-SHA

4 Appendix A



DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-SHA DHE-RSA-AES128-SHA256 DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA256 DHE-RSA-CAMELLIA128-SHA DHE-RSA-CAMELLIA256-SHA DH-RSA-AES128-GCM-SHA256 DH-RSA-AES128-SHA DH-RSA-AES128-SHA256 DH-RSA-AES256-GCM-SHA384 DH-RSA-AES256-SHA DH-RSA-AES256-SHA256 DH-RSA-CAMELLIA128-SHA DH-RSA-CAMELLIA256-SHA DH-RSA-DES-CBC3-SHA ECDH-ECDSA-AES128-GCM-SHA256 ECDH-ECDSA-AES128-SHA ECDH-ECDSA-AES128-SHA256 ECDH-ECDSA-AES256-GCM-SHA384 ECDH-ECDSA-AES256-SHA ECDH-ECDSA-AES256-SHA384 ECDH-ECDSA-DES-CBC3-SHA ECDH-ECDSA-RC4-SHA ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES256-SHA384 ECDHE-ECDSA-DES-CBC3-SHA ECDHE-ECDSA-RC4-SHA ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA256

ECDHE-RSA-AES256-GCM-SHA384

4 Appendix A



ECDHE-RSA-AES256-SHA ECDHE-RSA-AES256-SHA384 ECDHE-RSA-DES-CBC3-SHA ECDHE-RSA-RC4-SHA ECDH-RSA-AES128-GCM-SHA256 ECDH-RSA-AES128-SHA ECDH-RSA-AES128-SHA256 ECDH-RSA-AES256-GCM-SHA384 ECDH-RSA-AES256-SHA ECDH-RSA-AES256-SHA384 ECDH-RSA-DES-CBC3-SHA ECDH-RSA-RC4-SHA EDH-DSS-DES-CBC3-SHA EDH-RSA-DES-CBC3-SHA RC4-MD5 RC4-SHA

4.2 Default_NoRc4 Cipher Set

These are the ciphers that are in the **Default_NoRc4** system-defined cipher set:

AES128-GCM-SHA256 AES128-SHA AES128-SHA256 AES256-GCM-SHA384 AES256-SHA AES256-SHA256 CAMELLIA128-SHA CAMELLIA256-SHA DES-CBC3-SHA DH-DSS-AES128-GCM-SHA256 DH-DSS-AES128-SHA DH-DSS-AES128-SHA256 DH-DSS-AES256-GCM-SHA384 DH-DSS-AES256-SHA DH-DSS-AES256-SHA256 DH-DSS-CAMELLIA128-SHA DH-DSS-CAMELLIA256-SHA

4 Appendix A



DH-DSS-DES-CBC3-SHA DHE-DSS-AES128-GCM-SHA256 DHE-DSS-AES128-SHA DHE-DSS-AES128-SHA256 DHE-DSS-AES256-GCM-SHA384 DHE-DSS-AES256-SHA DHE-DSS-AES256-SHA256 DHE-DSS-CAMELLIA128-SHA DHE-DSS-CAMELLIA256-SHA DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-SHA DHE-RSA-AES128-SHA256 DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA256 DHE-RSA-CAMELLIA128-SHA DHE-RSA-CAMELLIA256-SHA DH-RSA-AES128-GCM-SHA256 DH-RSA-AES128-SHA DH-RSA-AES128-SHA256 DH-RSA-AES256-GCM-SHA384 DH-RSA-AES256-SHA DH-RSA-AES256-SHA256 DH-RSA-CAMELLIA128-SHA DH-RSA-CAMELLIA256-SHA DH-RSA-DES-CBC3-SHA ECDH-ECDSA-AES128-GCM-SHA256 ECDH-ECDSA-AES128-SHA ECDH-ECDSA-AES128-SHA256 ECDH-ECDSA-AES256-GCM-SHA384 ECDH-ECDSA-AES256-SHA ECDH-ECDSA-AES256-SHA384 ECDH-ECDSA-DES-CBC3-SHA ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES128-SHA256

ECDHE-ECDSA-AES256-GCM-SHA384

4 Appendix A



ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES256-SHA384 ECDHE-ECDSA-DES-CBC3-SHA ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES256-SHA384 ECDHE-RSA-DES-CBC3-SHA ECDH-RSA-AES128-GCM-SHA256 ECDH-RSA-AES128-SHA ECDH-RSA-AES128-SHA256 ECDH-RSA-AES256-GCM-SHA384 ECDH-RSA-AES256-SHA ECDH-RSA-AES256-SHA384 ECDH-RSA-DES-CBC3-SHA EDH-DSS-DES-CBC3-SHA EDH-RSA-DES-CBC3-SHA

4.3 Best Practices Cipher Set

The list of ciphers below is based on the LoadMaster Long Term Support (LTS) firmware version. The ciphers in the **Best Practices** cipher set were updated in LoadMaster firmware version 7.2.52. For further details, including a list of the ciphers, refer to the following article: <u>Best Practices Cipher Set</u> <u>Updated</u>.

These are the ciphers that are in the **Best Practices** system-defined cipher set:

DHE-DSS-AES128-GCM-SHA256 DHE-DSS-AES128-SHA256 DHE-DSS-AES256-GCM-SHA384 DHE-DSS-AES256-SHA DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-SHA DHE-RSA-AES128-SHA256

4 Appendix A



DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384

4.4 Intermediate_compatibility Cipher Set

These are the ciphers that are in the **Intermediate_compatibility** system-defined cipher set:

AES128-GCM-SHA256 AES128-SHA AES128-SHA256 AES256-GCM-SHA384 AES256-SHA AES256-SHA256 CAMELLIA128-SHA CAMELLIA256-SHA DES-CBC3-SHA DH-DSS-AES128-GCM-SHA256 DH-DSS-AES128-SHA DH-DSS-AES128-SHA256 DH-DSS-AES256-GCM-SHA384 DH-DSS-AES256-SHA DH-DSS-AES256-SHA256 DH-DSS-CAMELLIA128-SHA DH-DSS-CAMELLIA256-SHA DHE-DSS-AES128-GCM-SHA256

4 Appendix A



DHE-DSS-AES128-SHA DHE-DSS-AES128-SHA256 DHE-DSS-AES256-GCM-SHA384 DHE-DSS-AES256-SHA DHE-DSS-AES256-SHA256 DHE-DSS-CAMELLIA128-SHA DHE-DSS-CAMELLIA256-SHA DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-SHA DHE-RSA-AES128-SHA256 DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA256 DHE-RSA-CAMELLIA128-SHA DHE-RSA-CAMELLIA256-SHA DH-RSA-AES128-GCM-SHA256 DH-RSA-AES128-SHA DH-RSA-AES128-SHA256 DH-RSA-AES256-GCM-SHA384 DH-RSA-AES256-SHA DH-RSA-AES256-SHA256 DH-RSA-CAMELLIA128-SHA DH-RSA-CAMELLIA256-SHA ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES256-SHA384 SRP-AES-128-CBC-SHA SRP-AES-256-CBC-SHA

4 Appendix A



SRP-DSS-AES-128-CBC-SHA SRP-DSS-AES-256-CBC-SHA SRP-RSA-AES-128-CBC-SHA SRP-RSA-AES-256-CBC-SHA

4.5 Backward_compatibility Cipher Set

These are the ciphers that are in the **Backward_compatibility** system-defined cipher set:

AES128-GCM-SHA256 AES128-SHA AES128-SHA256 AES256-GCM-SHA384 AES256-SHA AES256-SHA256 CAMELLIA128-SHA CAMELLIA256-SHA DES-CBC3-SHA DH-DSS-AES128-GCM-SHA256 DH-DSS-AES128-SHA DH-DSS-AES128-SHA256 DH-DSS-AES256-GCM-SHA384 DH-DSS-AES256-SHA DH-DSS-AES256-SHA256 DH-DSS-CAMELLIA128-SHA DH-DSS-CAMELLIA256-SHA DH-DSS-DES-CBC3-SHA DHE-DSS-AES128-GCM-SHA256 DHE-DSS-AES128-SHA DHE-DSS-AES128-SHA256 DHE-DSS-AES256-GCM-SHA384 DHE-DSS-AES256-SHA DHE-DSS-AES256-SHA256 DHE-DSS-CAMELLIA128-SHA DHE-DSS-CAMELLIA256-SHA DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-SHA DHE-RSA-AES128-SHA256

4 Appendix A



DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA256 DHE-RSA-CAMELLIA128-SHA DHE-RSA-CAMELLIA256-SHA DH-RSA-AES128-GCM-SHA256 DH-RSA-AES128-SHA DH-RSA-AES128-SHA256 DH-RSA-AES256-GCM-SHA384 DH-RSA-AES256-SHA DH-RSA-AES256-SHA256 DH-RSA-CAMELLIA128-SHA DH-RSA-CAMELLIA256-SHA DH-RSA-DES-CBC3-SHA ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES256-SHA384 ECDHE-ECDSA-DES-CBC3-SHA ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES256-SHA384 ECDHE-RSA-DES-CBC3-SHA SRP-3DES-EDE-CBC-SHA SRP-AES-128-CBC-SHA SRP-AES-256-CBC-SHA SRP-DSS-3DES-EDE-CBC-SHA SRP-DSS-AES-128-CBC-SHA SRP-DSS-AES-256-CBC-SHA SRP-RSA-3DES-EDE-CBC-SHA SRP-RSA-AES-128-CBC-SHA SRP-RSA-AES-256-CBC-SHA

4 Appendix A



4.6 WUI Cipher Set

These are the ciphers that are in the **WUI** system-defined cipher set:

AES128-GCM-SHA256 AES128-SHA AES128-SHA256 AES256-GCM-SHA384 AES256-SHA AES256-SHA256 CAMELLIA128-SHA CAMELLIA256-SHA DES-CBC3-SHA DH-DSS-AES128-GCM-SHA256 DH-DSS-AES128-SHA DH-DSS-AES128-SHA256 DH-DSS-AES256-GCM-SHA384 DH-DSS-AES256-SHA DH-DSS-AES256-SHA256 DH-DSS-CAMELLIA128-SHA DH-DSS-CAMELLIA256-SHA DH-DSS-DES-CBC3-SHA DHE-DSS-AES128-GCM-SHA256 DHE-DSS-AES128-SHA DHE-DSS-AES128-SHA256 DHE-DSS-AES256-GCM-SHA384 DHE-DSS-AES256-SHA DHE-DSS-AES256-SHA256 DHE-DSS-CAMELLIA128-SHA DHE-DSS-CAMELLIA256-SHA DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-SHA DHE-RSA-AES128-SHA256 DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA256 DHE-RSA-CAMELLIA128-SHA

4 Appendix A



DHE-RSA-CAMELLIA256-SHA DH-RSA-AES128-GCM-SHA256 DH-RSA-AES128-SHA DH-RSA-AES128-SHA256 DH-RSA-AES256-GCM-SHA384 DH-RSA-AES256-SHA DH-RSA-AES256-SHA256 DH-RSA-CAMELLIA128-SHA DH-RSA-CAMELLIA256-SHA DH-RSA-DES-CBC3-SHA ECDH-ECDSA-AES128-GCM-SHA256 ECDH-ECDSA-AES128-SHA ECDH-ECDSA-AES128-SHA256 ECDH-ECDSA-AES256-GCM-SHA384 ECDH-ECDSA-AES256-SHA ECDH-ECDSA-AES256-SHA384 ECDH-ECDSA-DES-CBC3-SHA ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES256-SHA384 ECDHE-ECDSA-DES-CBC3-SHA ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES256-SHA384 ECDHE-RSA-DES-CBC3-SHA ECDH-RSA-AES128-GCM-SHA256 ECDH-RSA-AES128-SHA ECDH-RSA-AES128-SHA256 ECDH-RSA-AES256-GCM-SHA384 ECDH-RSA-AES256-SHA ECDH-RSA-AES256-SHA384

4 Appendix A



ECDH-RSA-DES-CBC3-SHA EDH-DSS-DES-CBC3-SHA EDH-RSA-DES-CBC3-SHA

4.7 FIPS Cipher Set

These are the ciphers that are in the **FIPS** system-defined cipher set:

AES128-SHA AES128-SHA256 AES256-SHA AES256-SHA256 DES-CBC3-SHA DH-DSS-AES128-SHA256 DH-DSS-AES256-SHA256 DHE-DSS-AES128-SHA256 DHE-DSS-AES256-SHA256 DHE-RSA-AES128-SHA256 DHE-RSA-AES256-SHA256 DH-RSA-AES128-SHA256 DH-RSA-AES256-SHA256 ECDH-ECDSA-AES128-SHA256 ECDH-ECDSA-AES256-SHA384 ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-SHA384 ECDH-RSA-AES128-SHA256 ECDH-RSA-AES256-SHA384

4.8 Legacy Cipher Set

These are the ciphers that are in the **Legacy** system-defined cipher set:

ADH-AES128-SHA ADH-DES-CBC3-SHA ADH-RC4-MD5 AES128-SHA AES256-SHA

4 Appendix A



DES-CBC3-SHA DHE-DSS-AES128-SHA DHE-DSS-AES256-SHA DHE-RSA-AES128-SHA DHE-RSA-AES256-SHA EDH-DSS-DES-CBC3-SHA EDH-RSA-DES-CBC3-SHA IDEA-CBC-SHA RC4-MD5 RC4-SHA

4.9 Null_Ciphers Cipher Set

These are the ciphers in the **Null_Ciphers** cipher set: NULL-SHA NULL-SHA256

4.10 ECDSA_Default Cipher Set

These are the ciphers that are in the ECDSA_Default system-defined cipher set:

ECDHE-ECDSA-AES256-GCM-SHA384 DHE-DSS-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-ECDSA-AES256-CCM8 ECDHE-ECDSA-AES256-CCM ECDHE-ECDSA-ARIA256-GCM-SHA384 DHE-DSS-ARIA256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA384 DHE-DSS-AES256-SHA256 ECDHE-ECDSA-CAMELLIA256-SHA384 DHE-DSS-CAMELLIA256-SHA256 ECDHE-ECDSA-AES256-SHA DHE-DSS-AES256-SHA DHE-DSS-CAMELLIA256-SHA ECDHE-ECDSA-AES128-GCM-SHA256 DHE-DSS-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-CCM8

4 Appendix A



ECDHE-ECDSA-AES128-CCM ECDHE-ECDSA-ARIA128-GCM-SHA256 DHE-DSS-ARIA128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256 DHE-DSS-AES128-SHA256 ECDHE-ECDSA-CAMELLIA128-SHA256 ECDHE-ECDSA-AES128-SHA DHE-DSS-AES128-SHA DHE-DSS-CAMELLIA128-SHA ECDHE-ECDSA-RC4-SHA

4.11 ECDSA_BestPractices Cipher Set

These are the ciphers that are in the **ECDSA_BestPractices** system-defined cipher set:

ECDHE-ECDSA-AES256-GCM-SHA384 DHE-DSS-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA384 DHE-DSS-AES256-SHA DHE-DSS-AES256-SHA ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA256 References



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 FIPS, Feature Description



Last Updated Date

This document was last updated on 07 December 2020.