LoadMaster UC APL Compliant (7.1.35)

Deployment Guide

UPDATED: 29 January 2019

Copyright Notices

Table of Contents

1 Introduction 5

1.1 Document Purpose 6

1.2 Intended Audience 6

1.3 Document Feedback 6

2 Minimum Requirements 7

3 Installation 8

3.1 Minimum Requirements for the VLM 8

3.2 Install the VLM 8

4 Configuration 9

4.1 Ensure the LoadMaster Passwords are Encrypted Using SHA-2 9

4.2 Configure the WUI Access Options 9

4.2.1 Enable Client Certificate WUI Authentication 9

4.2.2 Add a Pre-Auth Click Through Banner 9

4.2.3 Delete and Disable Local Accounts 10

4.2.4 Set a Complex Password for the 'bal' User 10

4.3 Enable an NTP Service 11

4.4 Configure Syslog Hosts 12

4.5 Disable SNMP 13

4.6 Disable API Access 13

4.7 Disable SSH Access 13

4.8 Upload the DoD Certificate 14

4.9 Enable CAC Authentication for WUI Access 15

4.10 Enable a Minimum of Two Ethernet Interfaces 15

4.11 Set an Alternate Interface for Management 16

4.12 Enable Alternate Gateway Support 17

4.13 Enable DNSSEC Capabilities 17

4.14 Add a Firewall Block for alsi.kemptechnologies.com 18

4.15 Configure Security Event and Incident Management (SEIM) 19

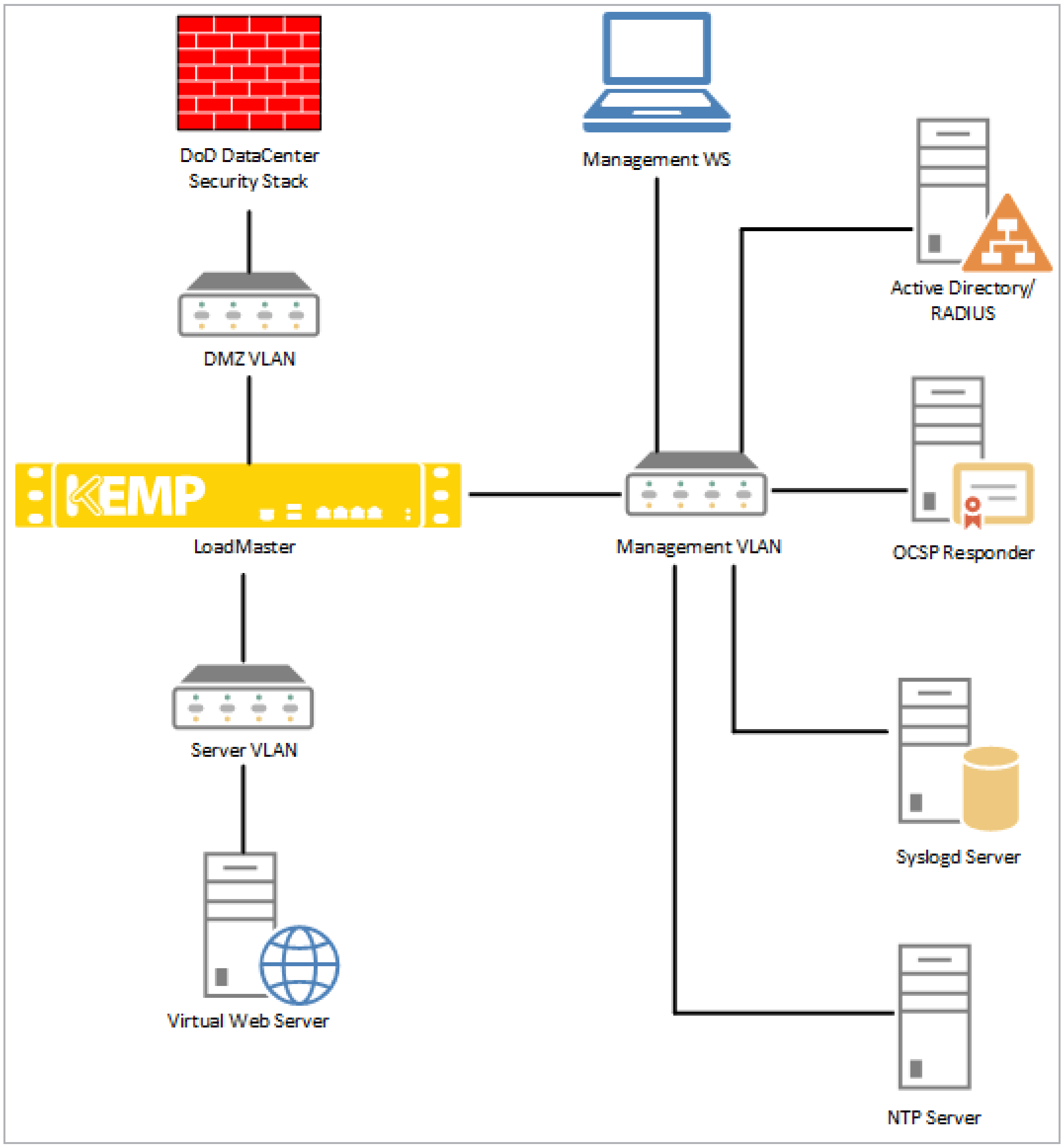
4.16 Conditions of Fielding from DoD IAAR 19

References 23

Last Updated Date 24

1 Introduction

The Kemp Virtual LoadMaster (VLM) is an Application Delivery Controller (ADC) that provides load balancing and Secure Sockets Layer (SSL) offloading. The VLM is certified under the Department of Defense (DoD) Unified Capabilities Approved Products List (UC APL) program as a Cyber Security Tool (CST).



In accordance with DoD security guidelines and the specific UC APL implementation guidelines, the Kemp VLM appliance has two approved means of access. The first access method (hypervisor virtual Console Access) is typically used to set up the initial IP address for the management interface on the VLM. The second access method, Web User Interface (WUI) is used to manage and configure the VLM. You can also use the Console Access method to restore the VLM to a default state. All VLM management should be originated from a Security Technical Implementation Guide (STIG)-compliant management workstation. The hypervisor virtual Console method is used to configure the VLM to communicate with other components and to be accessible using Internet Protocol (IP) addressing using Hypertext Transfer Protocol Secure (HTTPS). After the initial configuration is completed, the VMware client session is disconnected, and all administrative tasks are performed using a web browser using HTTPS.

1.1 Document Purpose

This document provides instructions on how to configure and set various options in the VLM to meet the UC APL requirements. This document meets the Conditions of Fielding (para 4.16 h.), specifically this document is the required "Kemp Virtual LoadMaster, Software Release 7.1.35, Tracking Number 1512701, Military Unique Features Deployment Guide".

For detailed, step-by-step instructions on some of the VLM features mentioned in this document, refer to the individual Feature Description documents, for example:

- **User Management, Feature Description**
- **DoD Common Access Card Authentication, Feature Description**
- **Kerberos Constrained Delegation, Feature Description**

1.2 Intended Audience

Network administrators who must configure a VLM to meet UC APL requirements.

1.3 Document Feedback

If you have any comments about this document, forward them to KM@kemptechnologies.com.

2 Minimum Requirements

The following security measures (at a minimum) must be in place to ensure an acceptable level of risk:

- The system uses a RADIUS server integrated with Active Directory (AD) to authenticate users.
- The system uses a Syslog device for auditing purposes.
- Role-based security must be used for user access and management of the vendor's device.
- All local user accounts must be deleted on the device after initial setup and configuration, with the exception of one emergency administrative account. The site also disables local authentication of administrative users.
- Ensure that the emergency administrative account's username and password are locked up in separate safes, both of which are not accessible by any one individual, and procedures are implemented to log all access and usage.
- Ensure the emergency administrative account meets all Department of Defence (DoD) user identification (ID) and password requirements.
- Ensure that all unused open ports are closed.
- The device has management access limited to an authorized Common Access Card (CAC)-enabled workstation which is located in a physically secured area and connected to the management Virtual Local Area Network (VLAN) behind a firewall.
- Ensure that Telnet, HTTP web service, and SNMPv1 and 2c are disabled.
- Ensure that Secure Shell (SSH) is disabled.

Instructions on how to meet these minimum requirements are provided throughout the remainder of this document.

3 Installation

3.1 Minimum Requirements for the VLM

Each Kemp VLM must be allocated a minimum of:

- 2 vCPUs
- 2 GB RAM
- 32 GB disk space

The Kemp license defines the throughput and SSL Transactions Per Second (TPS) performance levels for the VLM.

Kemp recommends that 2 vCPUs and 2 GB RAM is added to the VLM Virtual Machine for each additional Gbps throughput required.

3.2 Install the VLM

Instructions on installing, initially configuring and licensing the VLM are available in the Kemp Installation Guides which can be found on the Kemp Documentation page: http://kemptechnologies.com/documentation.

For detailed licensing instructions, refer to the **Licensing, Feature Description** document which is also located on the Kemp Documentation page: http://kemptechnologies.com/documentation.

4 Configuration

The sections below provide instructions on how to configure the VLM and guidance on any other configuration needed to meet the UC APL requirements.

> The LoadMaster supports security headers on WUI pages.

4.1 Ensure the LoadMaster Passwords are Encrypted Using SHA-2

As of LoadMaster firmware version 7.2.36, SHA-256 is used to encrypt all new LoadMaster passwords.

If your LoadMaster is running an older firmware version, you can update the firmware by following the steps in the **Updating the LoadMaster Software, Technical Note** on the Kemp Documentation Page. On upgrade from a previous version, the stored password hashes for users (including **bal**) are not changed. All users (including **bal**) must change their password for it to be stored using SHA-256.

4.2 Configure the WUI Access Options

Refer to the sections below to configure the various WUI access options.

4.2.1 Enable Client Certificate WUI Authentication

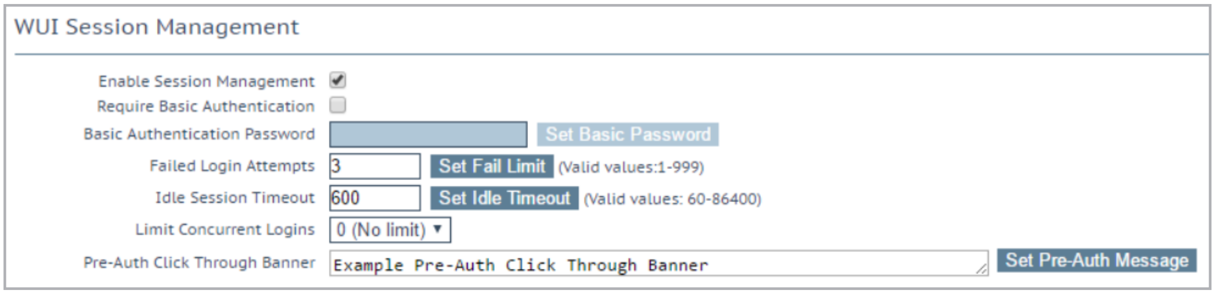
For detailed, step-by-step instructions on how to configure client certificate WUI authentication, refer to the **User Management, Feature Description** on the Kemp Documentation Page.

4.2.2 Add a Pre-Auth Click Through Banner

Set the pre-authentication click through banner that is displayed before the LoadMaster WUI login page. Users are not permitted to log in until they click **Accept**. This field can contain plain text or HTML code. The field cannot contain JavaScript. For security purposes, you cannot use the **‘** (single quote) and **“** (double-quote) characters. This field accepts up to 5,000 characters.

To set this, follow the steps below:

1. In the LoadMaster WUI, expand **Certificates & Security** and click **Admin WUI Access**.



WUI Session Management

Enable Session Management	☑
Require Basic Authentication	□
Basic Authentication Password	Set Basic Password
Failed Login Attempts	3 Set Fail Limit (Valid values:1-999)
Idle Session Timeout	600 Set Idle Timeout (Valid values: 60-86400)
Limit Concurrent Logins	0 (No limit) ▾
Pre-Auth Click Through Banner	Example Pre-Auth Click Through Banner Set Pre-Auth Message

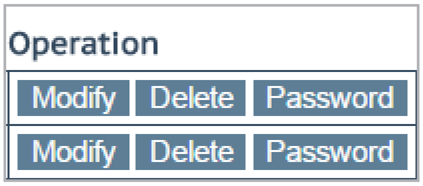
2. Type the appropriate text or HTML code into the **Pre-Auth Click Through Banner** text box.

3. Click **Set Pre-Auth Message**.

4.2.3 Delete and Disable Local Accounts

To delete and disable local accounts, follow the steps below in the VLM WUI:

1. In the main menu, go to **System Configuration > User Management**.



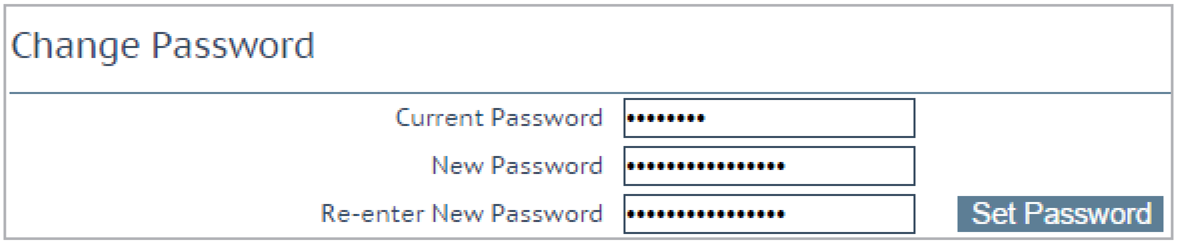
2. If any local users are listed, click **Delete** to remove them. Click **OK** to the confirmation message.

By default, there are no other local users. **Bal** is the default administrative user. The **bal** user should exist locally. Please follow DoD safekeeping practices for treating the **bal** user as an emergency account.

4.2.4 Set a Complex Password for the 'bal' User

As mentioned in the previous section, **bal** is the default administrative user. Follow the steps below to set a complex password for the **bal** user:

1. In the main menu of the VLM WUI, go to **System Configuration > System Administration > User Management**.



Change Password

Current Password •••••••••

New Password ••••••••••••••••

Re-enter New Password ••••••••••••••••

2. Enter the **Current Password** for the **bal** user.

3. Enter a new complex password.

4. Re-enter the new complex password.

5. Click **Set Password**.

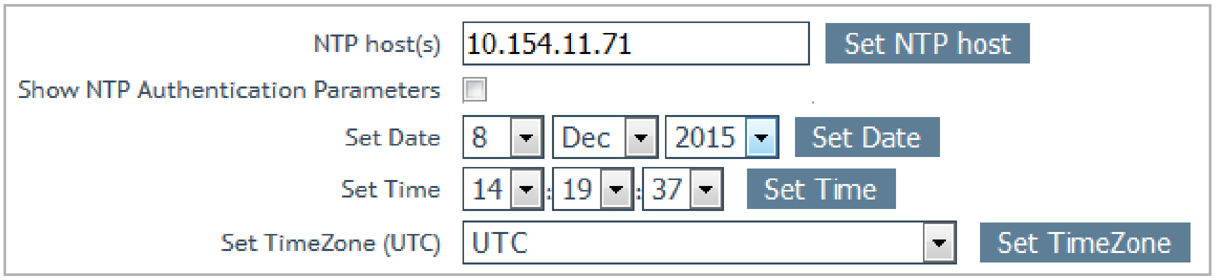
6. Seal the complex password into an envelope and store it in an approved security container.

> Follow DoD and local standards when setting and storing the complex password.

4.3 Enable an NTP Service

To enable a Network Time Protocol (NTP) Service, follow the steps below in the VLM WUI:

1. In the main menu, go to **System Configuration > System Administration > Date/Time**.



NTP host(s) 10.154.11.71

Show NTP Authentication Parameters □

Set Date 8 Dec 2015

Set Time 14 : 19 : 37

Set TimeZone (UTC) UTC

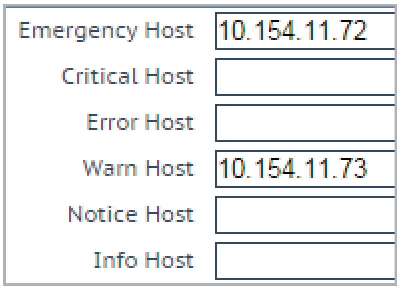
2. In the **NTP host(s)** text box, specify the host(s) from which the VLM will set its time. Click **Set NTP host**.

Multiple hosts can be specified in a space-separated list. The time is set from the first host that returns a valid answer.

4.4 Configure Syslog Hosts

The VLM can produce various warning and error messages using the syslog protocol. These messages are normally stored locally. It is also possible to configure the VLM to transmit these error messages to a remote syslog server. To configure this, follow the steps below in the VLM WUI:

1. In the main menu, go to **System Configuration > Logging Options > Syslog Options**.



Emergency Host	10.154.11.72
Critical Host	
Error Host	
Warn Host	10.154.11.73
Notice Host	
Info Host	

2. Enter the hosts to receive the events.

Six different error message levels are defined and each message level may be sent to a different server. **Notice** messages are sent for information only; **Emergency** messages normally require immediate user action.

> Up to 10 individual IP addresses can be specified for each of the Syslog fields. The IP addresses must be differentiated using a space-separated list.

Examples of the type of message that may be seen after setting up a **Syslog** server are below:

- **Emergency**: Kernel-critical error messages
- **Critical**: Unit one has failed and unit two is taking over as master (in a High Availability (HA) setup)
- **Error**: Authentication failure for root from 192.168.1.1
- **Warn**: Interface is up/down
- **Notice**: Time has been synced
- **Info**: Local advertised Ethernet address

> One point to note about syslog messages is they are cascading in an upwards direction. Therefore, if a host is set to receive WARN messages, the message file includes messages from all levels above WARN but none for levels below.

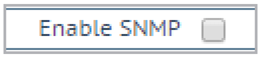
Kemp recommends not setting all six levels for the same host because multiple messages for the same error will be sent to the same host.

To enable a syslog process on a remote Linux server to receive syslog messages from the VLM, the syslog must be started with the "-r" flag.

4.5 Disable SNMP

To disable SNMP, follow the steps below in the VLM WUI:

1. In the main menu, go to **System Configuration > Logging Options > SNMP Options**.



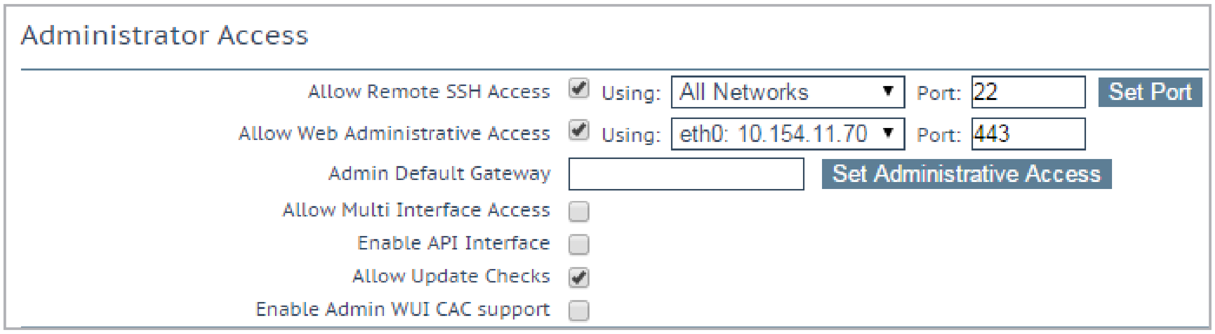
Enable SNMP ☐

2. Clear the **Enable SNMP** check box.

4.6 Disable API Access

To disable Application Program Interface (API) access to the VLM, follow the steps below in the VLM WUI:

1. In the main menu, go to **Certificates & Security > Remote Access**.



Administrator Access

Allow Remote SSH Access ☑ Using: All Networks ▼ Port: 22 Set Port

Allow Web Administrative Access ☑ Using: eth0: 10.154.11.70 ▼ Port: 443

Admin Default Gateway Set Administrative Access

Allow Multi Interface Access ☐

Enable API Interface ☐

Allow Update Checks ☑

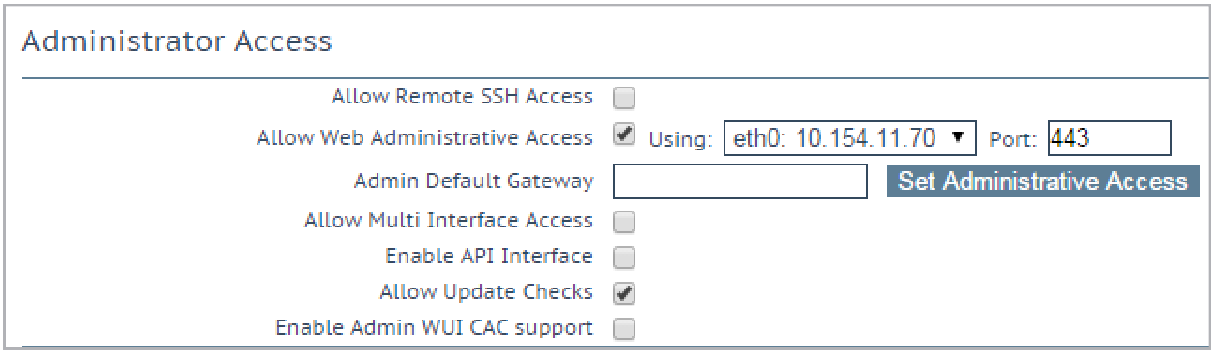
Enable Admin WUI CAC support ☐

2. Ensure that the **Enable API Interface** check box is not selected.

4.7 Disable SSH Access

To disable SSH access to the VML, follow the steps below in the VLM WUI:

1. In the main menu, go to **Certificates & Security > Remote Access**.



Administrator Access

Allow Remote SSH Access □

Allow Web Administrative Access ☑ Using: eth0: 10.154.11.70 Port: 443

Admin Default Gateway

Allow Multi Interface Access □

Enable API Interface □

Allow Update Checks ☑

Enable Admin WUI CAC support □

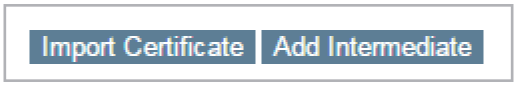
2. Clear the **Allow Remote SSH Access** check box.

3. Click **OK** to the warning message.

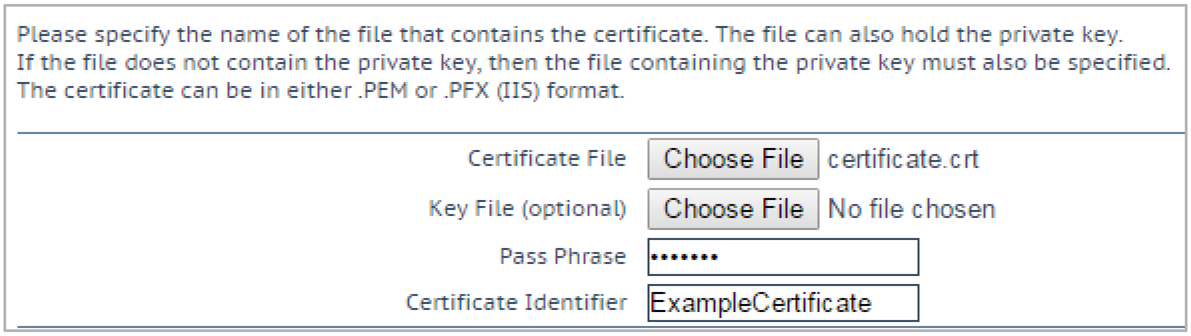
4.8 Upload the DoD Certificate

Kemp VLM appliances come with a self-signed certificate. This is not sufficient to meet DoD requirements and additional DoD Public Key Infrastructure (PKI) issued certificates must be loaded on the Kemp VLM for the purpose of managing the appliance as well as for the purpose of performing SSL acceleration (decryption) by the appliance. To upload the DoD certificates to the VLM, follow the steps below in the VLM WUI:

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



2. Click **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 certificate.crt

Key File (optional): Choose File No file chosen

Pass Phrase: •••••••

Certificate Identifier: ExampleCertificate

3. Click **Choose File** in the **Certificate File** section.

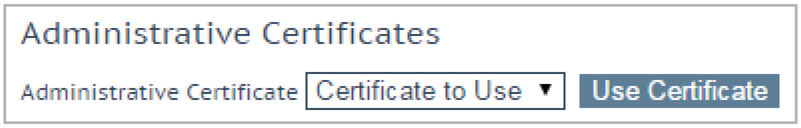
4. Browse to and select the relevant DoD certificate file.

5. Upload the **Key File**, if needed.

6. Enter the **Pass Phrase** for the certificate.

7. Enter a recognizable name for the certificate.

8. Click **Save**.



Administrative Certificates

Administrative Certificate: Certificate to Use ▼

9. After uploading the DoD certificate intended to manage the VLM, select this certificate as the **Administrative Certificate** to be used to manage the VLM.

Upload any additional DoD certificates as needed to support load-balanced SSL offloading.

4.9 Enable CAC Authentication for WUI Access

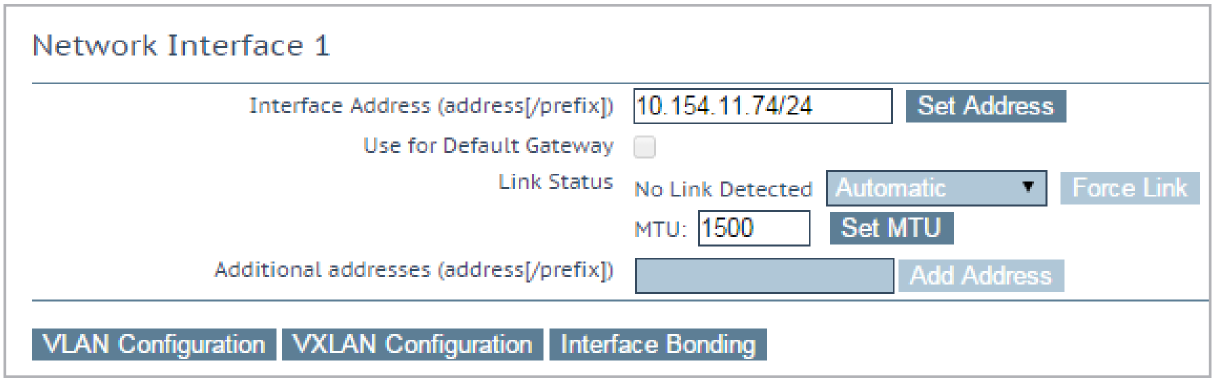
Kemp released CAC-enabled login functionality in the 7.1-30 software release of the VLM. A number of steps are involved in enabling CAC authentication for WUI access. For step-by-step instructions, refer to the **Using CAC Authentication For LoadMaster WUI Access** section of the **DoD Common Access Card Authentication, Feature Description** which is available on the Kemp Documentation Page.

4.10 Enable a Minimum of Two Ethernet Interfaces

To dedicate an interface for management and connection to the DoD Management VLAN, you must enable a minimum of two Ethernet interfaces. Ensure the hypervisor has allocated two virtual interfaces to the Virtual Machine created for the Kemp VLM and then follow the steps below using the VLM WUI to add the second interface:

1. In the main menu, go to **System Configuration > Network Setup**.

2. In the **Interfaces** section, click **eth1**.



Network Interface 1

Interface Address (address[/prefix]): 10.154.11.74/24

Use for Default Gateway: □

Link Status: No Link Detected; Automatic ▼

MTU: 1500

Additional addresses (address[/prefix]):

3. Enter the **Interface Address (address[/prefix])**.

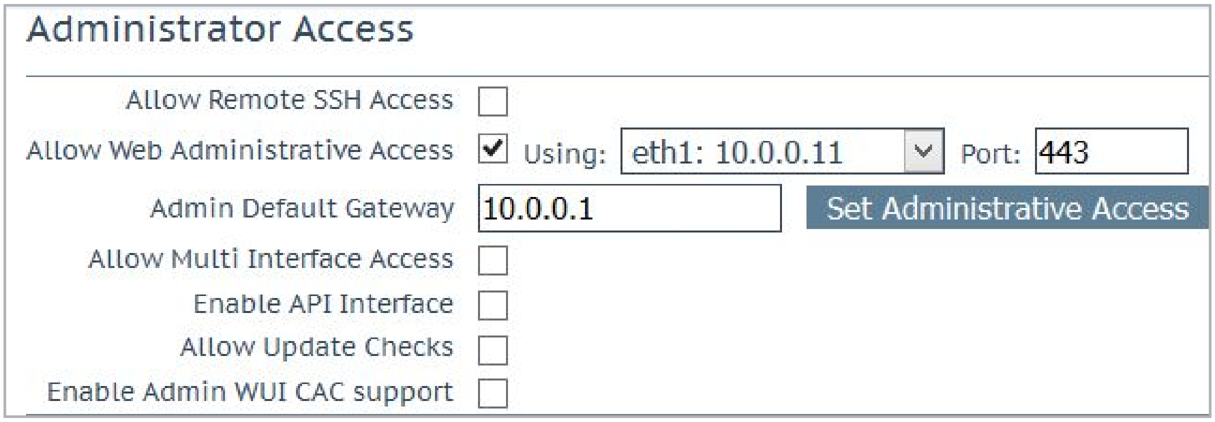
4. Click **Set Address**.

5. Configure any other settings as needed.

4.11 Set an Alternate Interface for Management

DoD requires all management be performed on a dedicated interface connected to a closed DoD management VLAN. To change the default eth port for management, follow the steps below in the VLM WUI:

1. In the main menu, go to **Certificates & Security > Remote Access**.



Administrator Access

Allow Remote SSH Access	□				
Allow Web Administrative Access	☑	Using:	eth1: 10.0.0.11	Port:	443
Admin Default Gateway	10.0.0.1		Set Administrative Access		
Allow Multi Interface Access	□				
Enable API Interface	□				
Allow Update Checks	□				
Enable Admin WUI CAC support	□				

2. Select the relevant interface, for example **eth1**, in the **Allow Web Administrative Access** drop-down list.

3. Enter the IP address of the desired default gateway in the **Admin Default Gateway** text box.

4. Click **Set Administrative Access**.

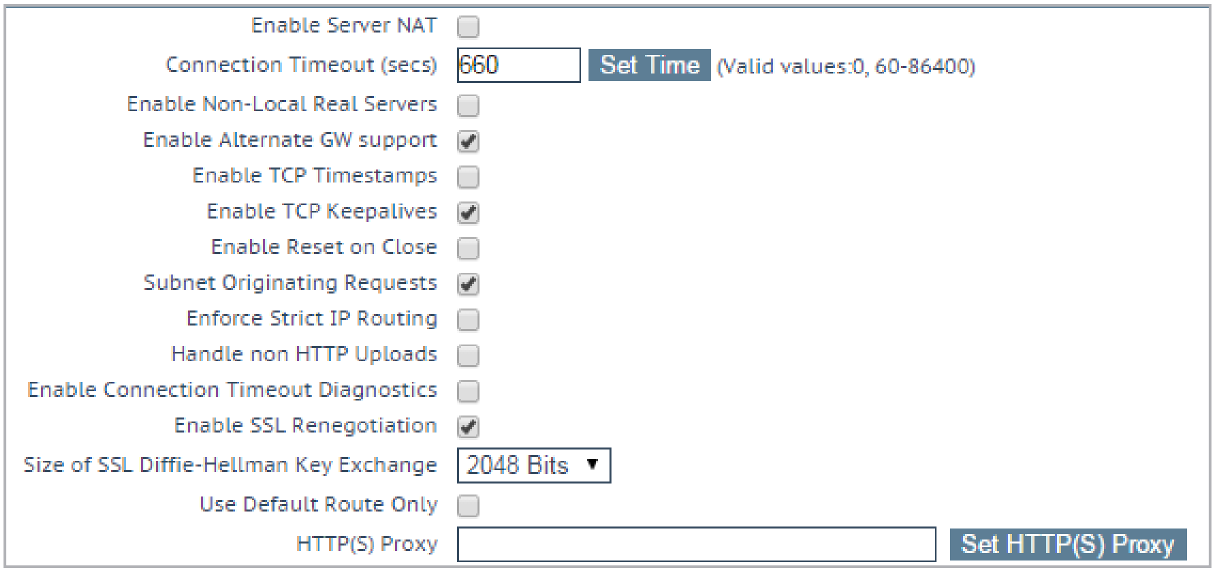
> These settings are not applied until **Set Administrative Access** is clicked.

5. Once this is done, you must reconnect your web browser to the new IP address established and enabled as the management interface for the VLM.

4.12 Enable Alternate Gateway Support

The management interface (possibly eth1) must be connected to the closed DoD Management VLAN. To enable alternate gateway support, follow the steps below in the VLM WUI:

1. In the main menu, 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	□
Enable SSL Renegotiation	☑
Size of SSL Diffie-Hellman Key Exchange	2048 Bits ▼
Use Default Route Only	□
HTTP(S) Proxy	Set HTTP(S) Proxy

2. Ensure that the **Enable Alternate GW support** check box is selected.

4.13 Enable DNSSEC Capabilities

DNSSEC works with the following utilities in the LoadMaster:

- Vipdump
- Ping and ping6
- Syslog
- SNMP
- Wget
- NTP
- SMTP

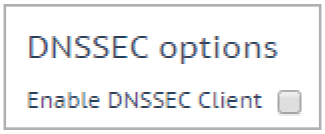
By default, the LoadMaster DNSSEC client is disabled. Only enable this option if needed. In some circumstances, the DNSSEC validation can take a significant amount of time to fail. This can cause the LoadMaster to appear to freeze or hang.

At least one **Nameserver** must be added before DNSSEC can be enabled. To enable DNSSEC capabilities on the LoadMaster, follow the steps below:

The LoadMaster must be rebooted to apply a change to the DNSSEC option.

When using HA – the DNSSEC option must be configured on both devices separately.

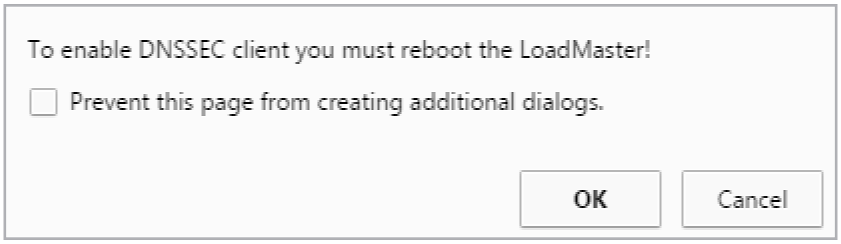
1. In the LoadMaster WUI, navigate to **System Configuration > Network Setup > Host & DNS Configuration**.



DNSSEC options

Enable DNSSEC Client □

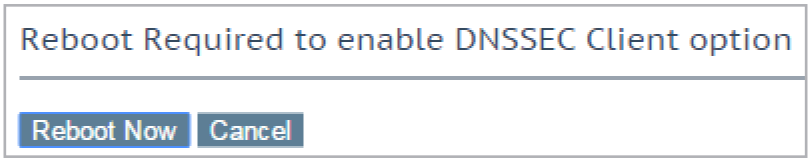
2. Select the **Enable DNSSEC Client** check box.



To enable DNSSEC client you must reboot the LoadMaster!

□ Prevent this page from creating additional dialogs.

3. Click **OK** to the pop-up message.



Reboot Required to enable DNSSEC Client option

4. Click **Reboot Now**.

4.14 Add a Firewall Block for alsi.kemptechnologies.com

Block **alsi.kemptechnologies.com** in the external firewall. Refer to the third party firewall documentation for instructions on how to do this.

4.15 Configure Security Event and Incident Management (SEIM)

The VLM does not have built in alerting capabilities. As a result of this, Kemp recommends that DoD utilize tools that analyse syslogd files, for example ArcSight, be tuned to:

- Look for successive logins without associated logout events to identify potential misuse in this area. ArcSight provides an alert for unsuccessful login attempts.
- Look for suspicious activity in audit logs to identify potential misuse.
- Send an alert when a new account is created on the VLM.
- Review log data from AD and VLM and generate alerts based on any account changes associated with VLM administrative accounts.
- Send an alert when a VLM account is deleted.

You should configure the SEIM, for example ArcSight, to use syslogd information and report the results to the Security Manger. For further information on how to configure SEIM, refer to the relevant third-party product documentation.

4.16 Conditions of Fielding from DoD IAAR

The following is provided as a direct quote from the “INFORMATION ASSURANCE ASSESSMENT REPORT FOR Kemp Virtual LoadMaster, Software Release 7.1.35 (Tracking Number 1512701)”.

CONDITIONS OF FIELDING. When the system is deployed into an operational environment, the following security measures (at a minimum) must be implemented to ensure an acceptable level of risk for the site's Designated Approving Authority:

a.The system will use a RADIUS server integrated with AD to authenticate users. Otherwise, the following findings are incorporated into the site's architecture:

.Application Security and Development STIG:

i.APP3320, CAT II, Virtual LoadMaster

.Network Device Management SRG:

i.SRG-APP-000023-NDM-000205, CAT II, Virtual LoadMaster

ii.SRG-APP-000025-NDM-000207, CAT II, Virtual LoadMaster

iii.SRG-APP-000026-NDM-000208, CAT II, Virtual LoadMaster

iv.SRG-APP-000027-NDM-000209, CAT II, Virtual LoadMaster

v.SRG-APP-000028-NDM-000210, CAT II, Virtual LoadMaster

vi.SRG-APP-000029-NDM-000211, CAT II, Virtual LoadMaster vii.SRG-APP-000091-NDM-000223, CAT II, Virtual LoadMaster

viii.SRG-APP-000148-NDM-000246, CAT II, Virtual LoadMaster

ix.SRG-APP-000163-NDM-000251, CAT II, Virtual LoadMaster

x.SRG-APP-000164-NDM-000252, CAT II, Virtual LoadMaster

xi.SRG-APP-000165-NDM-000253, CAT II, Virtual LoadMaster

xii.SRG-APP-000166-NDM-000254, CAT II, Virtual LoadMaster

xiii.SRG-APP-000167-NDM-000255, CAT II, Virtual LoadMaster

xiv.SRG-APP-000168-NDM-000256, CAT II, Virtual LoadMaster

xv.SRG-APP-000169-NDM-000257, CAT II, Virtual LoadMaster

xvi.SRG-APP-000170-NDM-000329, CAT II, Virtual LoadMaster

xvii. SRG-APP-000173-NDM-000260, CAT II, Virtual LoadMaster

xviii. SRG-APP-000174-NDM-000261, CAT II, Virtual LoadMaster

xix.SRG-APP-000389-NDM-000306, CAT II, Virtual LoadMaster

xx.SRG-APP-000495-NDM-000318, CAT II, Virtual LoadMaster

xxi.SRG-APP-000499-NDM-000319, CAT II, Virtual LoadMaster

b.The site will use a Syslog device for auditing purposes. Otherwise, the following findings are incorporated into the site's architecture:

.Application Security and Development STIG:

i.APP3650, CAT II, Virtual LoadMaster

.Network Device Management SRG:

i.SRG-APP-000118-NDM-000235, CAT II, Virtual LoadMaster

ii.SRG-APP-000125-NDM-000241, CAT II, Virtual LoadMaster

iii.SRG-APP-000126-NDM-000242, CAT II, Virtual LoadMaster

iv.SRG-APP-000359-NDM-000294, CAT II, Virtual LoadMaster

.Network Other Devices STIG:

i.NET0386, CAT III, Virtual LoadMaster

.Web Server SRG:

i.SRG-APP-000357-WSR-000150, CAT II, Virtual LoadMaster

ii.SRG-APP-000359-WSR-000065, CAT II, Virtual LoadMaster

c.The site must use role-based security for user access and management of the vendor's device.

d.The site must delete all local user accounts on the device after initial setup and configuration with the exception of one emergency administrative account. The site will also disable local authentication of administrative users.

e.The site will ensure that the emergency administrative account's userid and password are locked up in separate safes, both of which are not accessible by any one individual, and procedures are implemented to log all access and usage.

f.The site must ensure the emergency administrative account meets all DoD user identification (ID) and password requirements.

g.The site will ensure all unused open ports are closed.

h.The device will have management access limited to an authorized Common Access Card (CAC)-enabled workstation located in a physically secured area and connected to the management Virtual Local Area Network (VLAN) behind a firewall.

i.The site will ensure Telnet, http web service, and SNMPv1 and 2c are disabled. If SNMP is enabled, the following findings are incorporated into the site's architecture:

.Network Other Devices STIG:

i.NET1660, CAT II, Virtual LoadMaster (SNMP)

j.The site will ensure Secure Shell (SSH) is disabled. Otherwise, the following findings are incorporated into the site's architecture:

.Application Security and Development STIG:

i.APP3440, CAT II, Virtual LoadMaster

.Network Device Management SRG:

i.SRG-APP-000075-NDM-000217, CAT II, Virtual LoadMaster

ii.SRG-APP-000076-NDM-000218, CAT II, Virtual LoadMaster

iii.SRG-APP-000076-NDM-000219, CAT II, Virtual LoadMaster

iv.SRG-APP-000149-NDM-000247, CAT II, Virtual LoadMaster v.SRG-APP-000516-NDM-000332, CAT II, Virtual LoadMaster

vi.SRG-APP-000516-NDM-000344, CAT II, Virtual LoadMaster

.Network Other Devices STIG:

i.NET0340, CAT II, Virtual LoadMaster

ii.NET1645, CAT II, Virtual LoadMaster

iii.NET1646, CAT II, Virtual LoadMaster

k.The configuration must be in compliance with the "Kemp Virtual LoadMaster, Software Release 7.1.35, Tracking Number 1512701, Military Unique Features Deployment Guide".

l.The site must register the system in the Systems Networks Approval Process Database <https://snap.dod.mil/index.cfm> as directed by the Defense IA Security Accreditation Working Group and Program Management Office.

References

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

User Management, Feature Description

DoD Common Access Card Authentication, Feature Description

Kerberos Constrained Delegation, Feature Description

Licensing, Feature Description

Web User Interface (WUI), Configuration Guide

Updating the LoadMaster Software, Technical Note

Last Updated Date

This document was last updated on 29 January 2019.