

Military Unique Deployment Guide

LoadMaster Operating System (LMOS)
Software Release 7.2
Tracking Number 2118101

VERSION: 7.0

UPDATED: 27 July 2023

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Table of Contents

1 Introduction **5**

1.1 Document Purpose 6

1.2 Intended Audience 6

1.3 Document Feedback 6

2 Conditions of Fielding **7**

3 Installation **8**

3.1 Minimum Requirements for the LoadMaster 8

3.2 Install and License the LoadMaster 8

4 Configuration **9**

4.1 Disable Kemp Analytics 9

4.2 Configure TLS and FIPS 140-2 9

4.3 Configure DoD Warning Banner 10

4.4 Disable SSH 10

4.5 Disable SSL Renegotiation 10

4.6 Network Time Service (NTP) v3 11

4.7 Host Name and DNS Configuration 11

4.8 SNMP v3 13

4.9 Configure Syslog Hosts 13

4.10 Enable a Minimum of Two Ethernet Interfaces 15

4.11 Request and Install an Administrative SSL Certificate 15

4.12 Install Intermediate Certificates 16

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4.13 Enable Administrative Certificate 16
4.14 Configure WUI Access Options 16
4.15 Configure OCSP 18
4.16 Enable LDAP Endpoint 18
4.17 Configure Groups 19
4.18 Configure WUI Authorization 20
4.19 Configure Certificate Login 21
4.20 Configure Strict FIPS Mode 22
References **23**
Last Updated Date **24**
Document History **25**

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

1 Introduction

The Kemp LoadMaster is an Application Delivery Controller (ADC) that provides load balancing and Secure Sockets Layer (SSL) offloading. LoadMaster is certified under the Department of Defense (DoD) Information Network Approved Products List (DoDIN APL) program in the Cyber Security Tools (CST) area. LoadMaster is available as a hardware appliance or a virtual appliance supporting all common hypervisor and cloud computing environments. All Kemp LoadMasters operate using the same LoadMaster Operating System (LMOS) and this guide is relevant for securing all LoadMaster platforms.

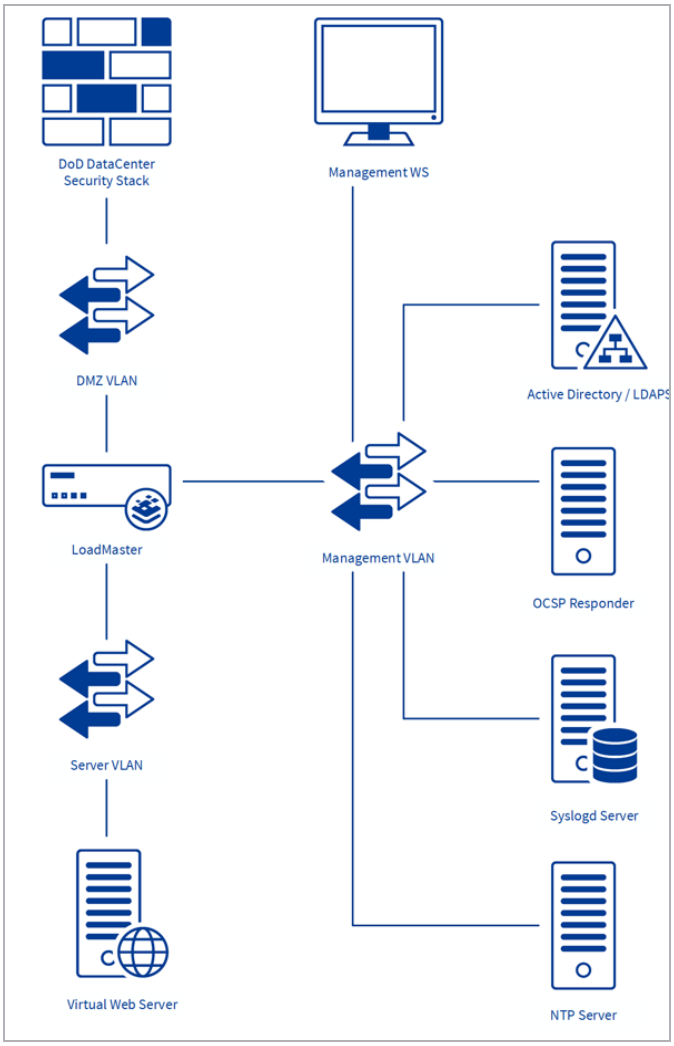


Figure 1. Typical LoadMaster Deployment Architecture

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

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

1.1 Document Purpose

Kemp provides this document to meet the Conditions of Fielding (CoF) as depicted within the “CYBERSECURITY ASSESSMENT REPORT FOR Kemp Technologies LoadMaster OS Software Release 7.2.48.4 Tracking Number 2118101”; specifically, this document is the required "Military Unique Deployment Guide" and updated based on addition of CAC/PIV/LDAPS/OCSP login functionality. This document provides instructions on how to configure and set various options in the LoadMaster to meet the DoDIN APL requirements.

For detailed, step-by-step instructions on some of the LoadMaster 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 need to configure a LoadMaster to meet DoDIN APL requirements.

1.3 Document Feedback

If you have any comments about this document, forward them to kemp.knowledgemanagementteam@progress.com.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2 Conditions of Fielding

Users must reference and follow the Conditions of Fielding (COF) found in the Cybersecurity Assessment Report (CAR).

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

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3 Installation

3.1 Minimum Requirements for the LoadMaster

The LMOS version must be version 7.2.48.4 or newer.

Virtual LoadMaster(s) 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 LoadMaster.

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

3.2 Install and License the LoadMaster

Instructions on installing, initially configuring, and licensing the LoadMaster are available in the Kemp Installation Guides which can be found on the LoadMaster Documentation web page.

For detailed licensing instructions, refer to the **Licensing, Feature Description** document which is also located on the LoadMaster Documentation web page.

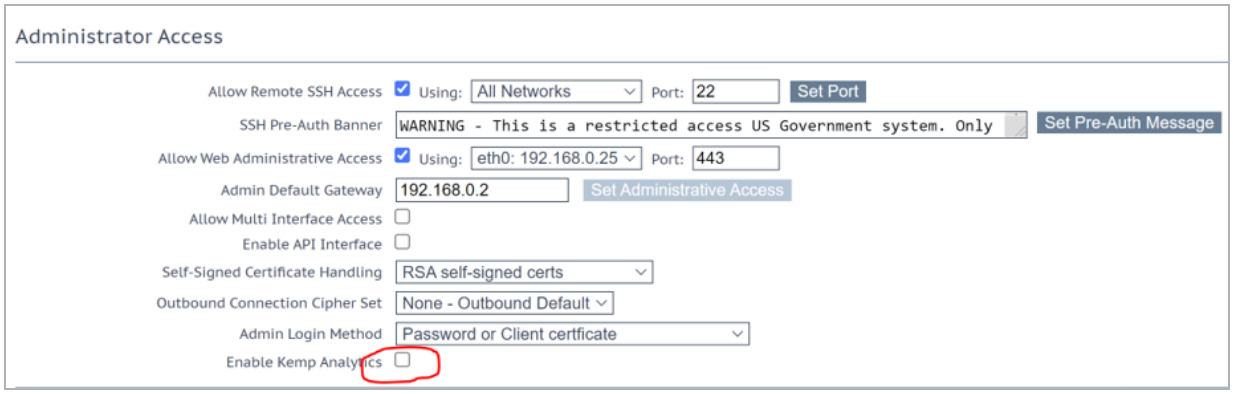
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4 Configuration

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

4.1 Disable Kemp Analytics

Using the **Certificates & Security > Remote Access** menu, unselect the **Enable Kemp Analytics** check box.



4.2 Configure TLS and FIPS 140-2



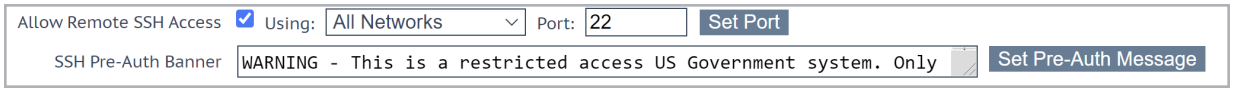
Using the **Certificates & Security > Remote Access** menu, select the **FIPS** option for the **Outbound Connection Cipher Set**.



Using the **Certificates & Security > Admin WUI Access** menu, disable **SSLv3** and **TLS1.0** in **Supported TLS Protocols** and select **FIPS** option for the **WUI Cipher set**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4.3 Configure DoD Warning Banner



Using the **Certificates & Security > Remote Access** menu, enter the warning message you want to display for console access in the **SSH Pre-Auth Banner** window and click **Set Pre-Auth Message**. This warning message is displayed for all console login methods.



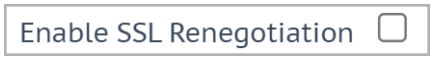
Using the **Certificates & Security > Admin WUI Access** menu, enter the DoD warning banner in the **Pre Auth Click Through Banner** text box and click **Set Pre-Auth Message**. This warning message is displayed for the WUI.

4.4 Disable SSH



Using the **Certificates & Security > Remote Access** menu, uncheck **Allow Remote SSH Access**.

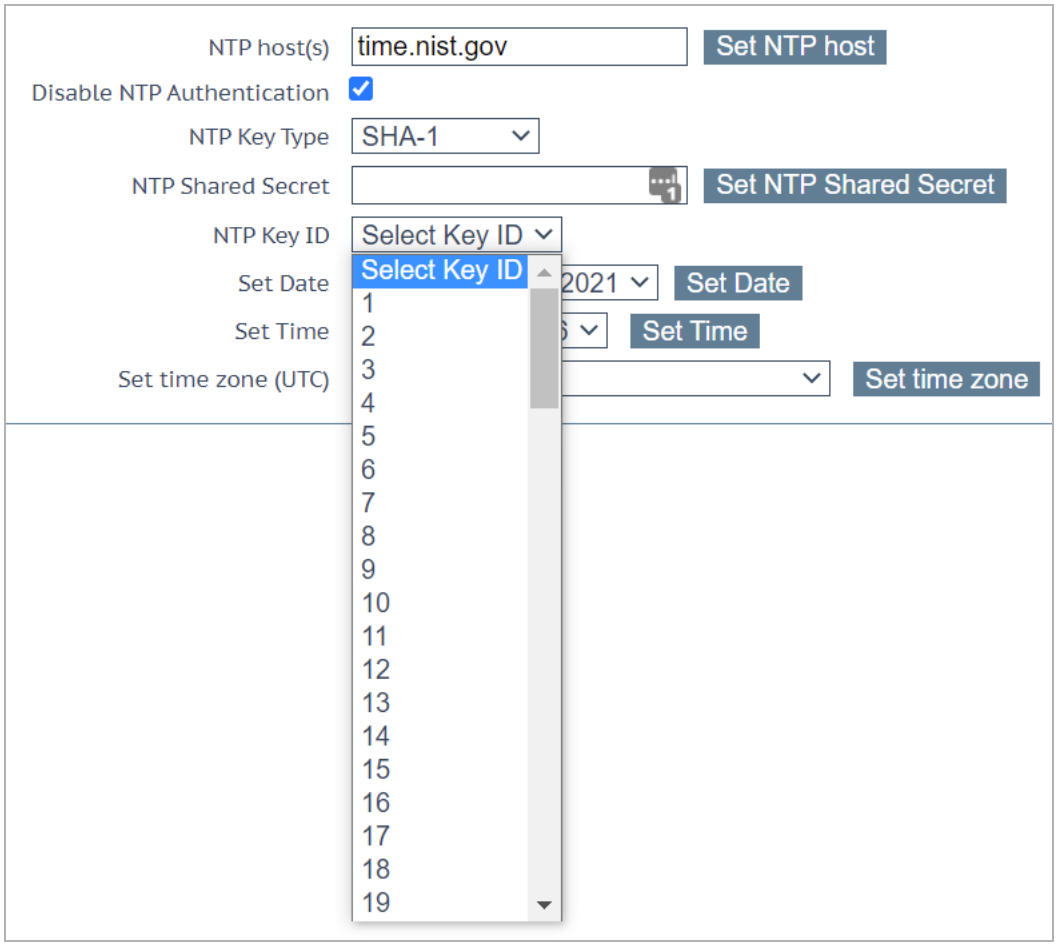
4.5 Disable SSL Renegotiation



Using the **System Configuration > Miscellaneous Options > Network Options** menu, disable the check box for **Enable SSL Renegotiation**. [As of LMOS version 7.2.55.0, this option is disabled by default.]

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4.6 Network Time Service (NTP) v3



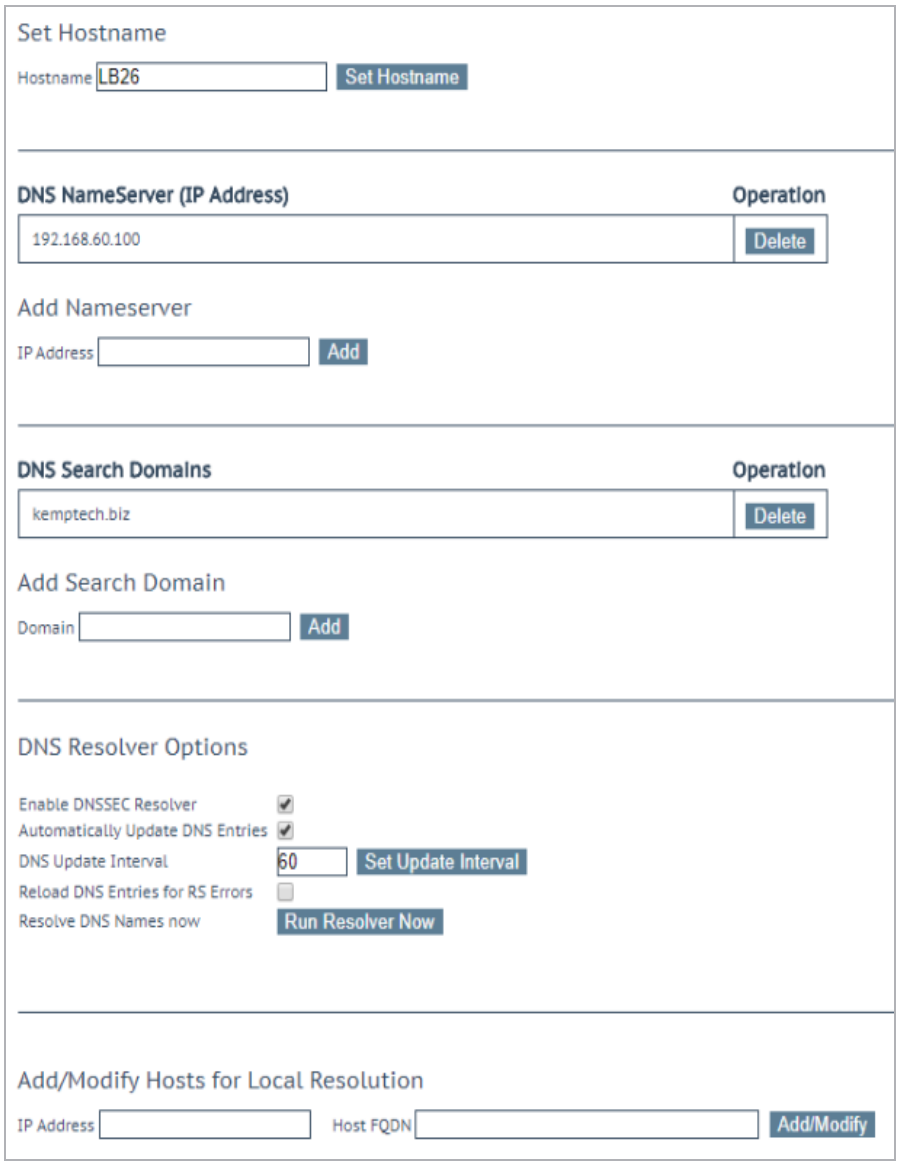
Using the **System Configuration > System Administration > Date/Time** menu in the WUI, configure NTP services. To enable NTPv3, select the **Show NTP Authentication Parameters** check box.

Ensure the **NTP Key Type** is set to **SHA-1**.

4.7 Host Name and DNS Configuration

Using the **System Configuration > Network Setup > Host & DNS Configuration** menu, set up the host name for the LoadMaster and various DNS settings. This screen is also where you enable the DNSSEC client on the LoadMaster:

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



1. Enter the **Hostname** (for example, **LB26**) and click **Set Hostname**.

2. Enter a space-separated list of **IP Address**(es) for your DNS Server(s) (up to three IP addresses can be entered).

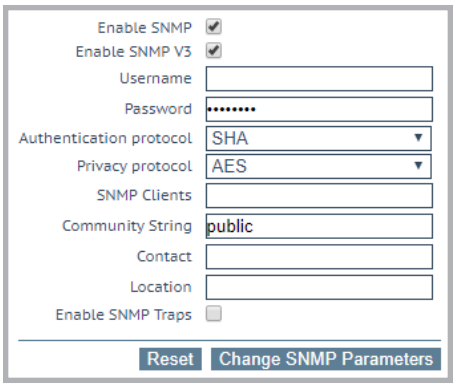
3. Enter the DNS Search **Domain** (minimum of your domain name (for example, **kempptech.biz**)).

4. Select the **Enable DNSSEC Resolver** check box.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

5. You can also add IP addresses and a **Host FQDN** for local DNS resolution. Entries here take precedence over entries in your DNS server.

4.8 SNMP v3

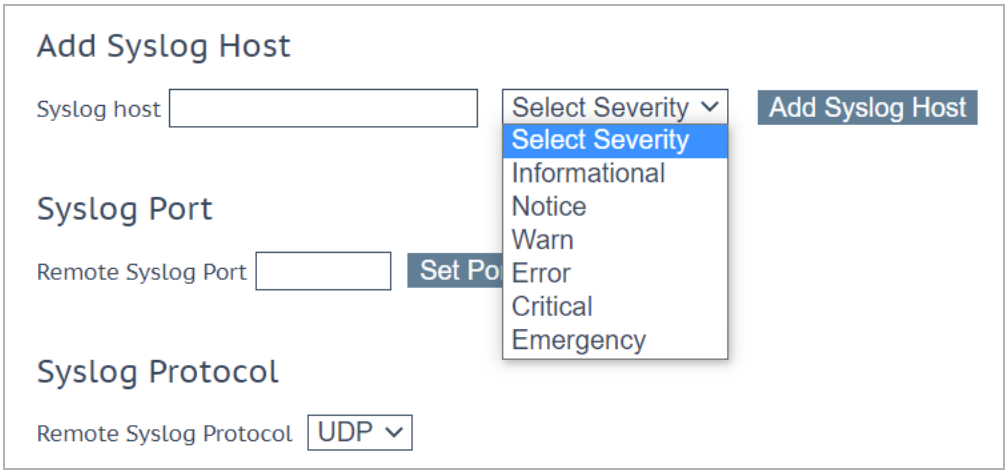


If SNMP is used, select the **Enable SNMP V3** check box and configure the options. This is available in the **System Configuration > Logging Options > SNMP Options** menu in the WUI.

Ensure **SHA** and **AES** are selected as the **Authentication protocol** and the **Privacy protocol**.

4.9 Configure Syslog Hosts

To meet requirements for persistent log storage and integration with Security Event and Incident Management (SEIM) systems, it is important to configure a syslog connection to a log collector.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Using the **System Configuration > Logging Options > Syslog Options** menu, enter an IP address, or addresses, and select the severity level. 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 ten 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 you may see 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 cascade in an upwards direction. Therefore, if a host is set to receive **Warn** messages, the message file includes message 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 LoadMaster, the syslog must be started with the "-r" flag.

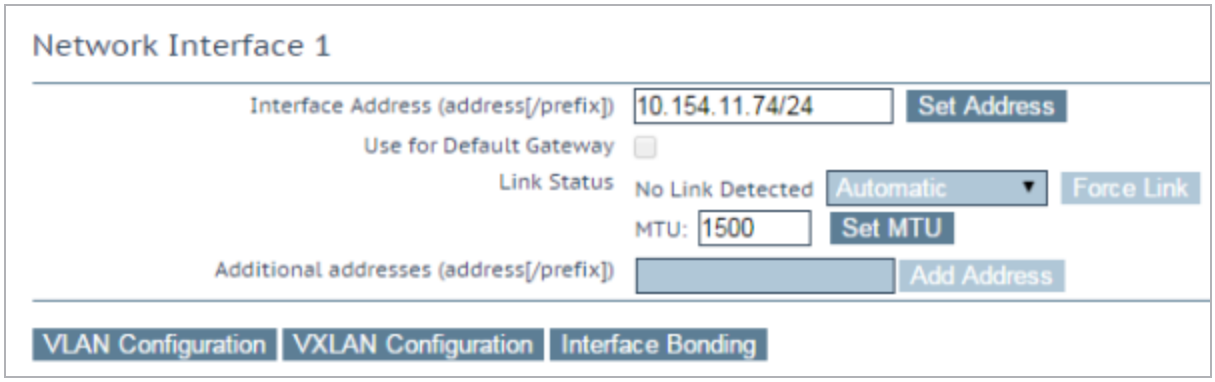
For organizations that require syslog over TLS, this option is also available for selection.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4.10 Enable a Minimum of Two Ethernet Interfaces

To enable a dedicated management network interface, it is necessary to configure at least two network interfaces.

Using the **System Configuration > Network Setup** menu, follow the steps below:



1. In the **Interfaces** section, click **eth1**.
2. Enter the **Interface Address (address[/prefix])** and click **Set Address**.
3. Configure any other settings as needed.

4.11 Request and Install an Administrative SSL Certificate

Follow the steps below to request and install an administrative SSL certificate. From an authorized Certificate Authority (CA), request a Web Server (SSL) certificate and install it on the LoadMaster.

1. Using the **Certificates & Security > Generate CSR** menu, generate the Certificate Service Request (CSR).

   > It is strongly recommended that you enter the LoadMaster management IP address into the SAN attributes field for the certificate request.

2. Copy the Certificate Request into a text file (use a basic editor like Notepad).
3. Copy the Private Key into another text file.
4. Send the CSR to your certificate authority and they will return the certificate (public) part of your server certificate to you.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

5. Using the **Certificates & Security > SSL Certificates** menu, select the certificate file from your CA and the key file which you had previously saved, type a **Certificate Identifier** (friendly name) and click **Save**.

4.12 Install Intermediate Certificates

Using the **Certificates & Security > Intermediate Certs** menu, install the root and intermediate certificate authority certificates for the CA that issued you the administrative certificate. Also, install the root and intermediate certificates for the CA that issued your Active Directory-based LDAP server its certificate.

On the management workstation, install the same root and intermediate certificates.

4.13 Enable Administrative Certificate

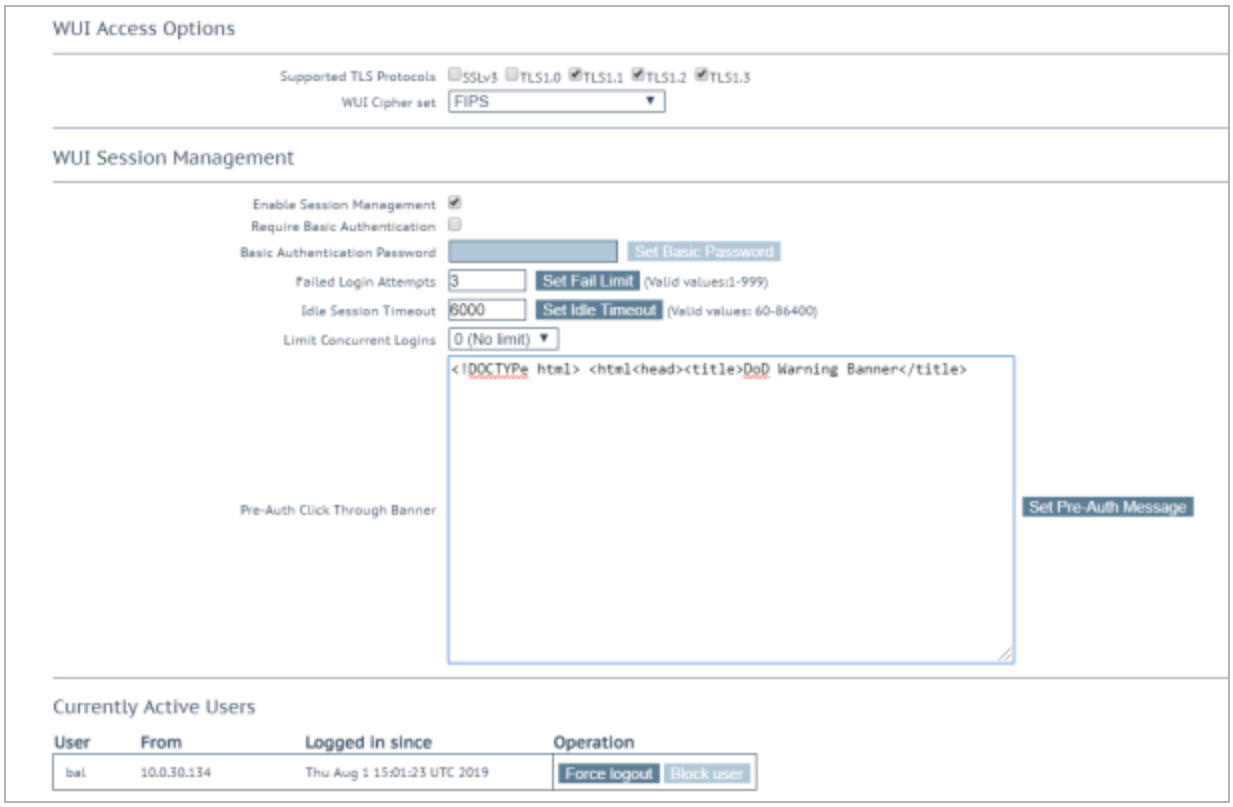
Using the **Certificates & Security > SSL Certificates** menu, under the **Administrative Certificates** section, select the new administrative certificate and click **Use Certificate**.

> Ensure the FQDN for the LoadMaster is registered in your DNS service (for example, **lb26.kemptech.biz**). This must match the Administrative SSL Certificate you requested above.

4.14 Configure WUI Access Options

Using the **Certificates & Security > Admin WUI Access** menu:

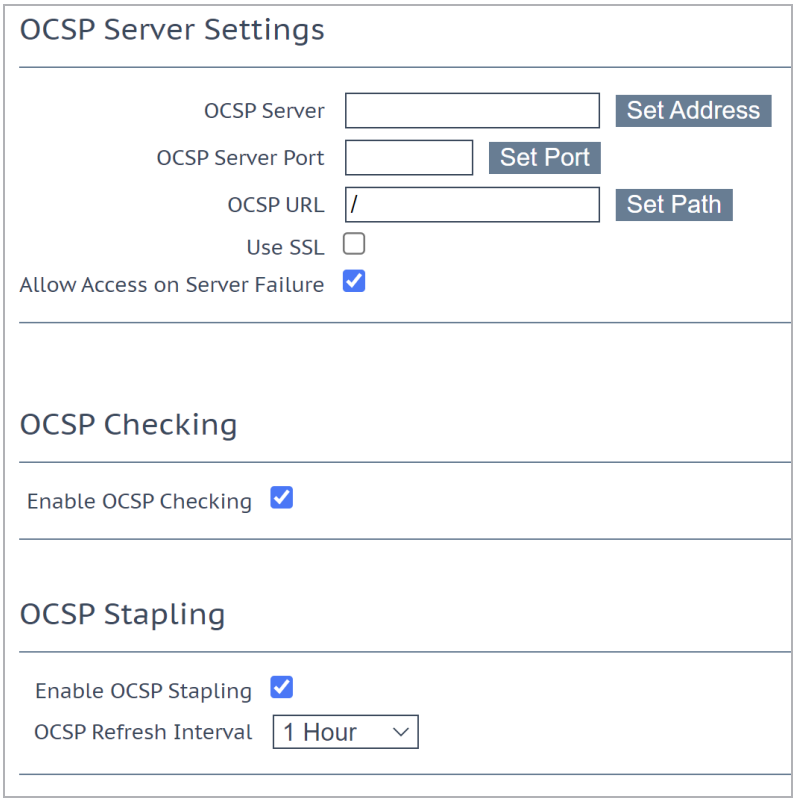
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



1. Ensure **Enable Session Management** is enabled.
2. Ensure **Require Basic Authentication** is disabled.
3. Set **Failed Login Attempts** to what your organization requires and click **Set Fail Limit**.
4. Set **Idle Session Timeout** (seconds) to the value your organization requires and click **Set Idle Timeout**.
5. Set **Limit Concurrent Logins** to the value your organization requires (Kemp recommends a minimum of 2).

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4.15 Configure OCSP



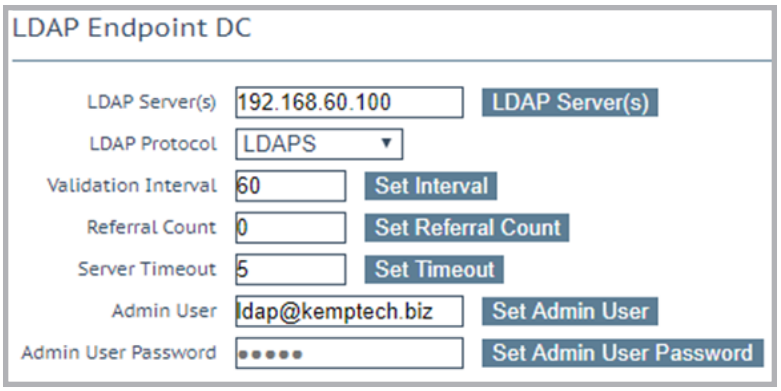
Using the **Certificates & Security > OCSP Configuration** menu, set the values as shown above. You can also configure a secondary OCSP Server, which is used when the OCSP server identified in the AIA field of the certificate is unavailable or the AIA field does not have an OCSP service defined.

4.16 Enable LDAP Endpoint

To meet the Conditions of Fielding, it is necessary to delete local accounts and use LDAPS to connect to an external user account database, often this is an Active Directory server.

To configure LDAP, follow the steps below:

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



1. Using the **Certificates & Security > LDAP Configuration** menu, enter a name in the **Add new LDAP Endpoint** text box and click **Add**. This opens the LDAP Endpoint configuration menu.

2. Enter the IP address (or addresses) for the LDAPS server (or servers) in the **LDAP Server(s)** text box and click **Set LDAP Server(s)**.

3. In the **LDAPS Protocol** drop-down list, select **LDAPS**.

4. If necessary, modify the **Validation Interval**, **Referral Count**, and **Server Timeout** values from the default values. Ensure you press the button to the right of the text boxes in which you make a change.

5. In the **Admin User** text box, enter an LDAP account in the format *account@domain* and click **Set Admin User**. This account does not need elevated rights; a Domain User is acceptable.

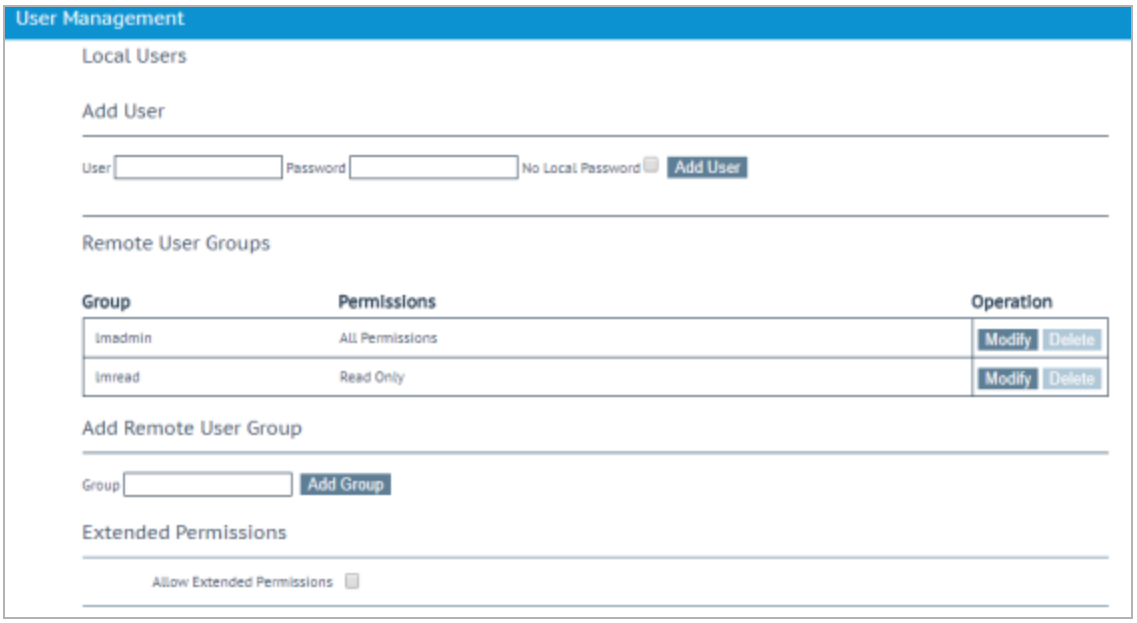
6. In the **Admin User Password** text box, enter the password for that user and click **Set Admin User Password**. Normally, you would create a service account for this **Admin User** account and you would use a very long random password for the account to minimize risk.

4.17 Configure Groups

LoadMaster supports two methods to assign rights to an LDAP login. Shadow accounts (local account without a password) and local Groups. LDAP is used to authenticate the user and pull associated group memberships. LoadMaster attempts to match these group memberships to local Groups or local shadow accounts. If there is a match, the user login is completed and the user is assigned the rights of the associated local Group or local shadow account.

Using the **System Configuration > System Administration > User Management** menu, create **Remote User Groups** and assign rights to these groups.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



The group names you use above must exactly match the LDAP group names you will use to map rights.

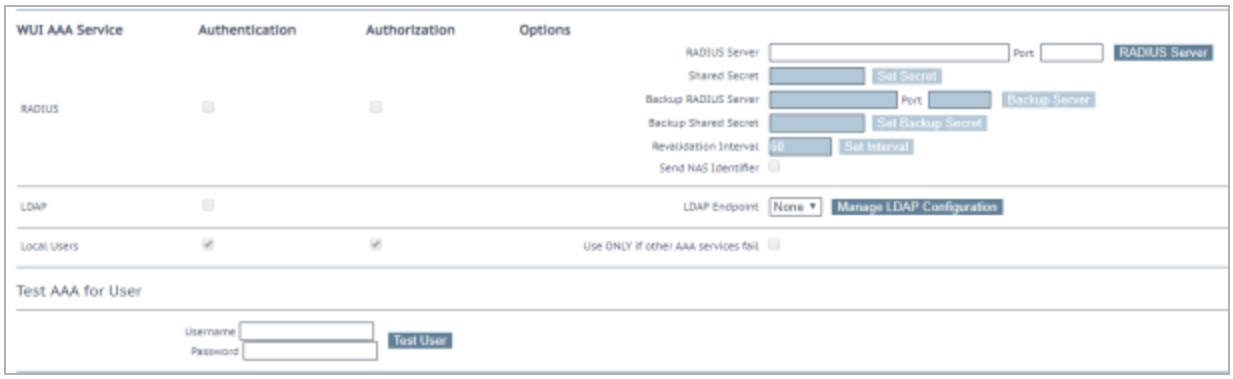
> The following characters are permitted in the group name: alphanumeric characters, spaces, or the following special symbols: **=~^._+#,@/-.**

Once you have created the Remote User Groups and assigned them rights on the LoadMaster, go to your LDAP system and ensure these groups are available (or create them).

4.18 Configure WUI Authorization

Using the **Certificates & Security > Remote Access** menu, click **WUI Authorization Options** and follow these steps:

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



1. Ensure **Local Users, Use ONLY if other AAA Services fail** is not selected.
2. Ensure the **Local Users Authentication** check box is not selected.
3. Add an **LDAP Endpoint** from the drop-down list.
4. Add **Remote User Groups** using the **Select groups** button.
5. Enter the full **Domain** name and click **Set Domain**.
6. Ensure the **LDAP Authentication** check box is selected.
7. Ensure the **RADIUS Authentication** and **Authorization** check boxes are not selected.

4.19 Configure Certificate Login

Ensure accounts are created in LDAP (Active Directory) where the **Principal Name** on the certificate matches the User Principal Name. Add these users to the appropriate groups. Once users are assigned to groups in LDAP and these users match the **Principal Name** on the certificates you will use to manage the LoadMaster, you are ready to enable Certificate login to the LoadMaster.

Using the **Certificates & Security > Remote Access** menu, set **Admin Login Method** to **Password or Client Certificate**.

Test certificate login. If certificate login works as expected you can further restrict user login methods to **Client Certificate Required (verify via OCSP)**.

If you end up with a broken WUI (for example, certificate login fails), you can reset the WUI using the console interface. Select **Local Administration**, **Web Address**, and you can **Restore Admin WUI Access to Default Mode** and optionally regenerate the SSL certificate. This lets you use the "bal" account and sign into the WUI.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4.20 Configure Strict FIPS Mode

LMOS includes an embedded FIPS 140-2 Level 1 certified encryption module. To enable strict FIPS mode on a LoadMaster it is first necessary to enable Session Management (**Certificates & Security > Admin WUI Access > Enable Session Management**). Once FIPS mode is enabled, it cannot be disabled. It is recommended that you verify all workloads you are planning to load balance supports FIPS algorithms before enabling strict FIPS mode. You can select FIPS options separately for each management function in addition to each Virtual Service (if you chose not to enable strict FIPS mode).



To enable strict FIPS mode, use the **Certificates & Security > Remote Access** menu and click **Enable Software FIPS mode**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

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

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Last Updated Date

This document was last updated on 27 July 2023.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Document History

Date	Change	Reason for Change	Version	Resp.
Sep 2018	Update	Corrected version number	1.0	LB
Jan 2019	Release updates	Updates for 7.2.45 release	2.0	LB
Feb 2019	Release updates	Updates for 7.2.46 release	3.0	LB
Dec 2019	Release updates	Updates for 7.2.49 release	4.0	LB
Feb 2020	Release updates	Updates for 7.2.49.1 release	5.0	CMC
Dec 2020	Release updates	Updates for 7.2.48.3 LTS release	6.0	LB
Nov 2021	Major update	Re-certification	7.0	MB
Feb 2022	Minor update	Re-branding updates	7.0	LB

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.