

LoadMaster Hardening

Technical Note

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 4

2 General Guidance 5

3 User Accounts 6

4 Configure UI Authorization 7

5 Configure Remote Access 8

6 Configure UI Access Options 9

7 WUI Session Management 10

8 Enable an NTP Service 11

9 Packet Routing Filter 12

10 Configure Syslog Hosts 15

11 Enable a Minimum of Two Ethernet Interfaces 17

12 Set an Alternate Interface for Management 18

13 Enable Alternate Gateway Support 19

14 Enable DNSSEC Capabilities 20

15 Configure OCSP 24

16 Currently Active Users 26

17 Configure Security Event and Incident Management (SIEM) 27

Last Updated Date 28

© 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 optimizes the performance and availability of servers delivering important content to end-users, delivering requests to the best network servers as quickly and efficiently as possible and continually checking the performance and security of the workload.

The Kemp LoadMaster appliance has two approved means of access. The first method (Console Access) is typically used to setup the initial IP address for the management interface. The second access method, 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. The Console 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 the initial configuration is completed, all administrative tasks are performed using a web browser using HTTPS.

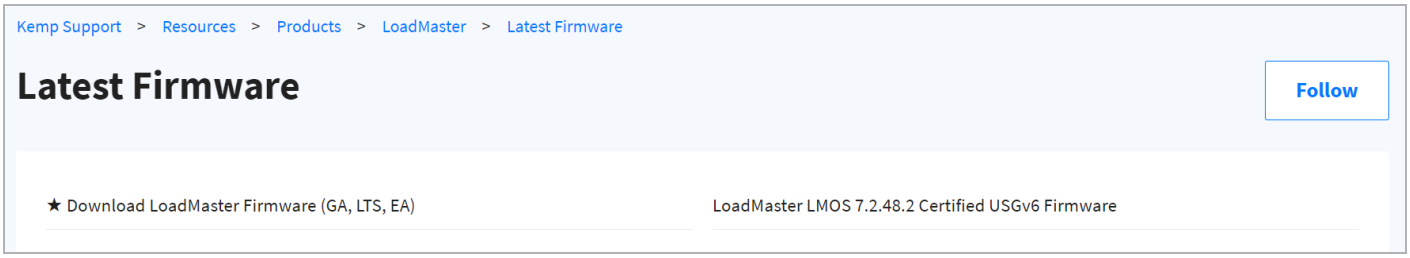
This document describes how to enhance the security of the LoadMaster and your applications by configuring the various features of the Kemp LoadMaster.

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

2 General Guidance

This section outlines some general hardening guidance to consider:

- Always ensure that you are running the Long Term Support (LTS) firmware which has the latest security fixes and updates.



- Sign up to receive security alerts and announcements from support.kemptechnologies.com by going to the Announcements page and clicking **Follow**.
- Under **System Configuration > Miscellaneous Options > Network Options** in the LoadMaster User Interface (UI) menu, ensure that **Enforce Strict IP Routing** is enabled. When set, the LoadMaster only accepts IP frames from a host over the interface where the routing algorithm would route frames to the host (strict source route validation).
- Under **System Configuration > Miscellaneous Options > Network Options**, ensure that **Enable TCP Timestamps** is disabled.
- Under **System Configuration > Miscellaneous Options > L7 Configuration**, ensure that **Allow Empty POSTs** is disabled.
- Under **System Configuration > Miscellaneous Options > L7 Configuration**, ensure that **Allow Empty HTTP Headers** is disabled.
- When performing re-encrypt Virtual Services, it is recommended to enable **Force Real Server Certificate Checking** under **System Configuration > Miscellaneous Options > Network Options**. This option forces the LoadMaster to verify that the certificate (including the intermediate certificate) on the Real Server is valid, that is, the certificate authority and expiration are OK.

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

3 User Accounts

This section outlines the configuration of a local password policy for user accounts on LoadMaster .

The Bal user is the default administrative user. The bal user should exist locally. Follow standard safekeeping practices for treating the bal user as an emergency account.

By default, there are no other local users. Local user accounts should be created for day-to-day operations.

Passwords should not be dictionary words and contain at least three of the following character types:

- Uppercase (26 letters A - Z)
- Lowercase (26 letters a - z)
- Numbers (10 numbers 0 - 9)
- Special characters (32 printable characters, such as !, $, and *)

Kemp recommends that any password is secure and in line with any organizational requirements.

Follow the steps below to set a password for the bal user:

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

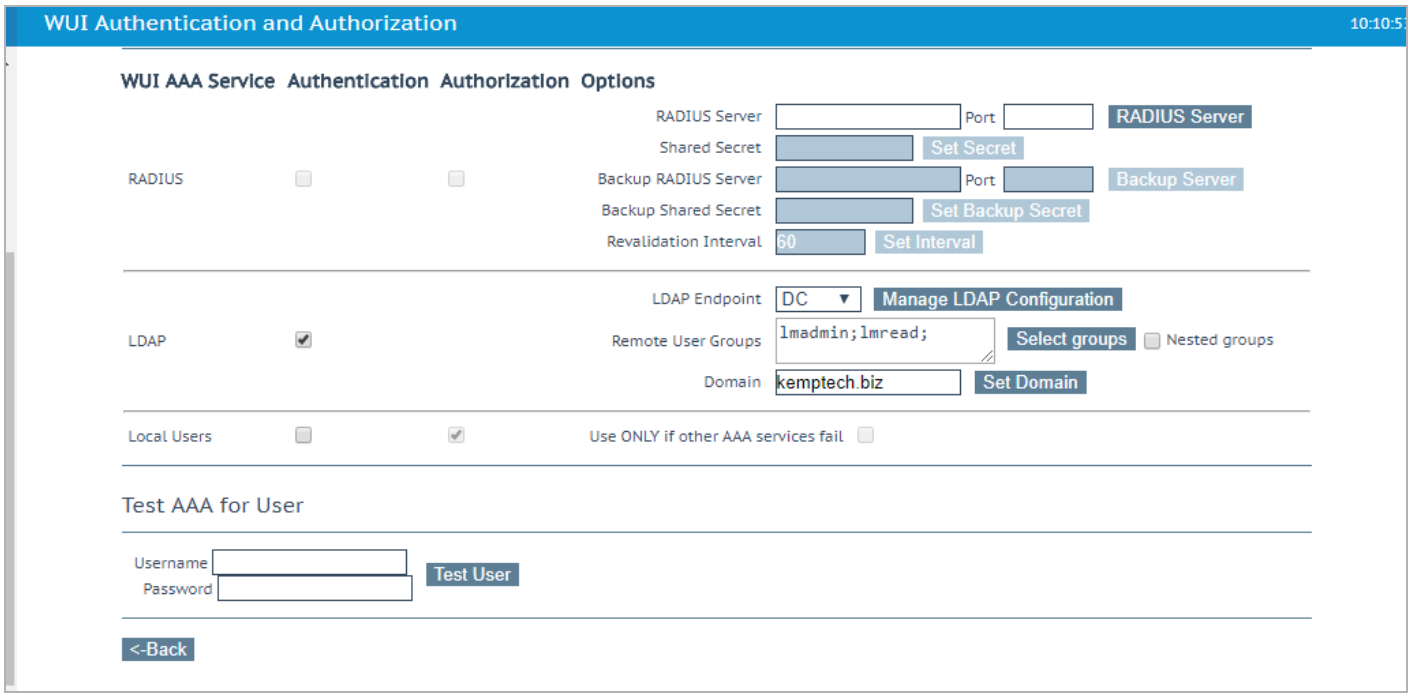
> The **bal** user password is initially configured on first installation of the LoadMaster. You can subsequently change and update it.

Local user accounts are also configured under **System Configuration > System Administration > User Management**.

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

4 Configure UI Authorization

In the **Certificates & Security > Remote Access** menu, click **WUI Authorization Options.**



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 group**s 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.

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

5 Configure Remote Access

In the LoadMaster UI, go to **Certificates & Security > Remote Access** and follow the steps below:

1. Disable **Allow Remote SSH Access**.

2. Enable **Allow Web Administrative Access**. Select the network interface to manage the LoadMaster from the **Using** drop-down list. Depending on your network architecture, this could be a dedicated management network/VLAN.

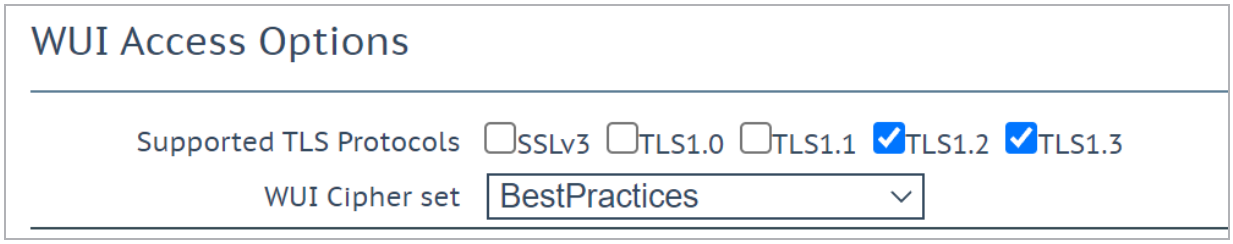
3. Enter the **Admin Default Gateway** (if the management interface is not on the same interface as your default gateway's network) and click **Set Administrative Access**.

4. The **Allow Multi Interface Access** check box should normally be disabled to force management traffic to only the management network.

5. Disable the **Enable API Interface** check box.

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

6 Configure UI Access Options



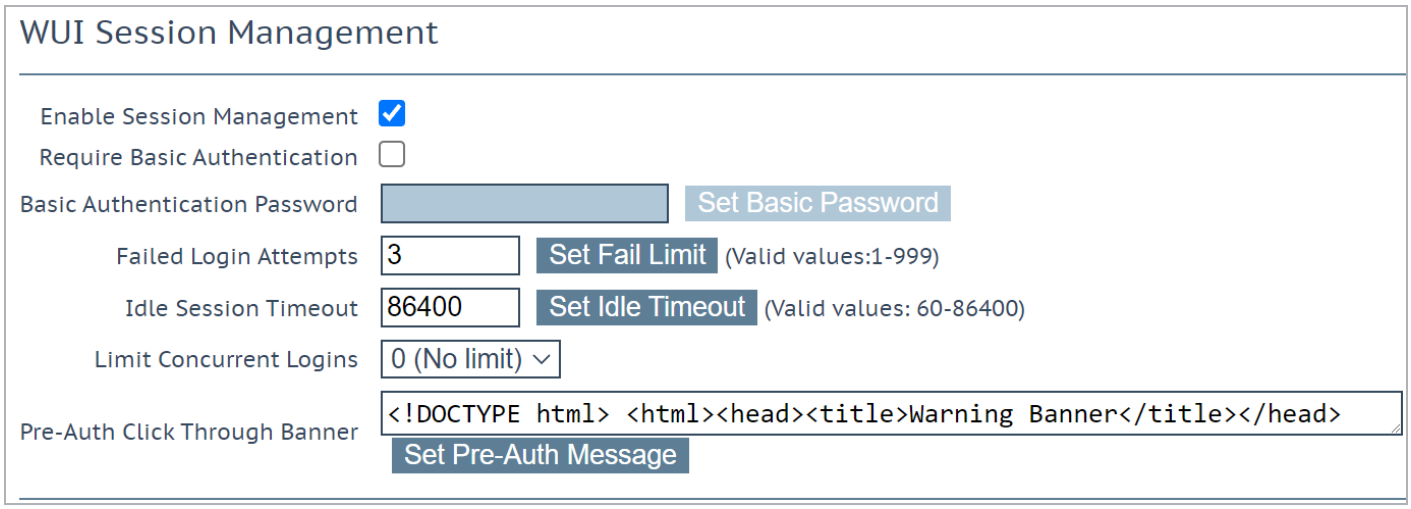
Using the **Certificates & Security > Admin WUI Access** menu, under **WUI Access Options**, ensure **SSLv3**, **TLS1.1**, and **TLS1.0** are not selected. Ensure the **WUI Cipher set** is set to **Best Practices**.

Under **SSL Certificates**, import a certificate that can be used for access to the UI.

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

7 WUI Session Management

The settings referred to in the sections below are available under the **Certificates & Security > Admin WUI Access** menu, under **WUI Session Management**.



Kemp recommends leaving **Failed Login Attempts** at **3** and setting the **Idle Session Timeout** (seconds) to the value your organization requires.

Idle Session Timeout is the length of time (in seconds) a user can be idle (no activity recorded) before they are logged out of the session. Kemp recommends setting the **Idle Session Timeout** (seconds) to the value your organization requires.

Limit Concurrent Logins provides the ability to limit the number of concurrent users of the management UI. It is currently not possible to restrict the number of concurrent command-line users. Kemp recommends setting the number of concurrent logins to be in line with any organizational requirements.

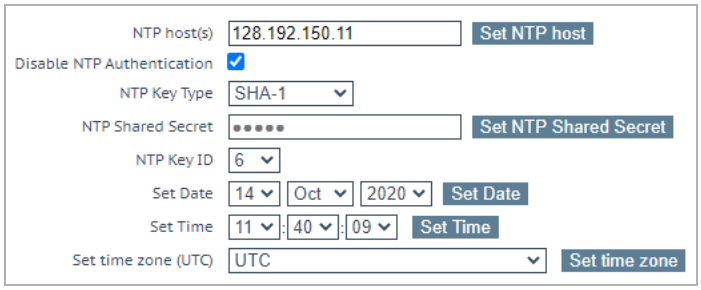
Set the **Pre-Auth Click Through Banner** that is displayed before the LoadMaster WUI login page. Users are not permitted to log in until they click **Accept**. This field can contain plain text or HTML code. The field cannot contain JavaScript. For security purposes, you cannot use the '‘ (single quote)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

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

8 Enable an NTP Service

Follow the steps below to configure an NTP service:

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



2. To enable NTPv3, select the **Show NTP Authentication Parameters** check box.

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

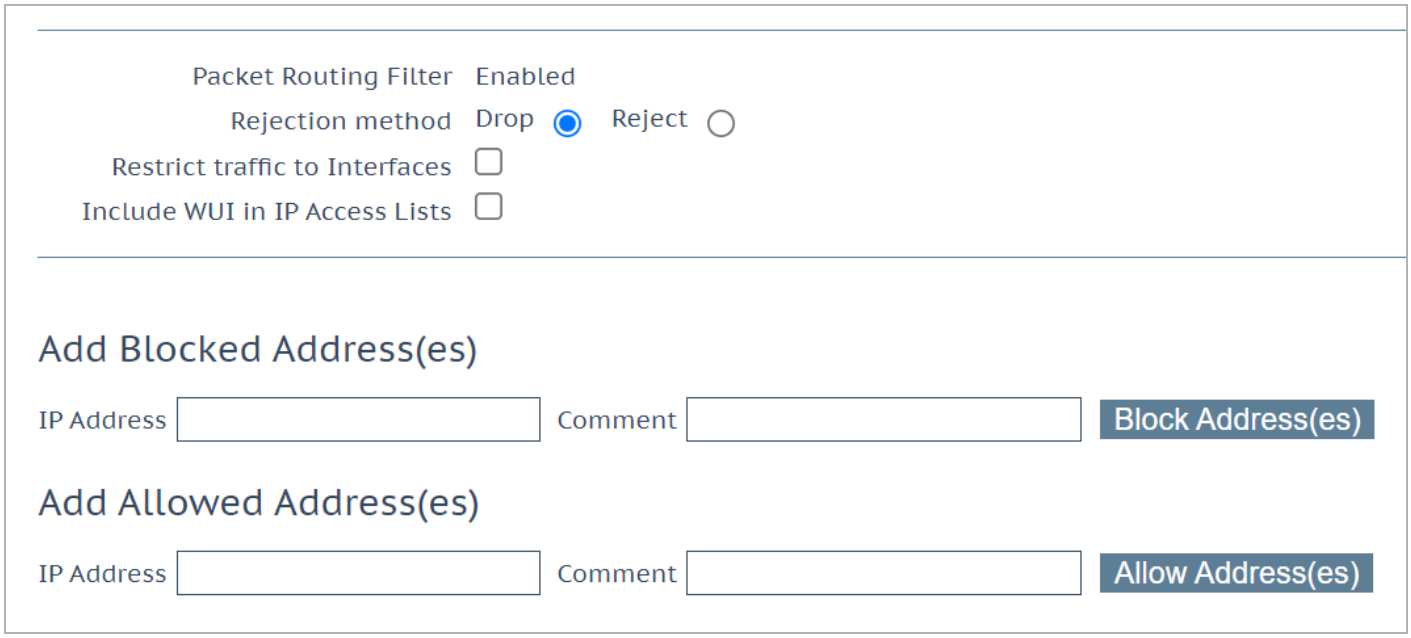
4. Set the **NTP Shared Secret** and **NTP Key ID** to the appropriate value(s) on the NTP Server.

5. In the **NTP host(s)** text box, specify the host(s) from which the LoadMaster 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.

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

9 Packet Routing Filter



Packet Routing Filter

If the filter is not activated, the LoadMaster also acts as a simple IP-forwarder.

When the packet routing filter is activated, it restricts traffic to the LoadMaster but client access to services running on the interface addresses (SSH 22, HTTPS 443, SNMP 161, and DNS 53) is unaffected. Enabling SNAT prevents you from blocking traffic to a Virtual Service that has the same IP address as the LoadMaster's default gateway interface. This can affect Azure or any cloud platforms that use a single IP address.

If the packet routing filter is not activated, the LoadMaster also acts as a simple IP-forwarder.

> The **Reject/Drop blocked packets** and **Restrict traffic to Interfaces** fields will not be displayed if the **Packet Routing Filter** is disabled.

Reject/Drop blocked packets

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

When an IP packet is received from a host, which is blocked using the Access Control Lists (ACLs), the request is normally ignored (dropped). The LoadMaster may be configured to return an ICMP reject packet, but for security reasons it is recommended to drop any blocked packets silently.

Restrict traffic to Interfaces

This setting enforces restrictions upon routing between attached subnets. Kemp has this option disabled by default.

Include WUI in IP Access lists

If this option is enabled, access to the WUI is also controlled by the packet filter. The IP address of the client that enables the **Include WUI in IP Access list**option to the packet filter will still have access (and be on the whitelist internally) - a message appears next to the check box saying **Access allowed from <IPAddress>**. This protects you from locking yourself out of the WUI.

Enabling the **Include WUI in IP Access lists** option does not affect Virtual Service connectivity.

With the**Include WUI in IP Access lists**option disabled, access to the WUI is not affected by the packet filter.

Add Blocked Address(es)

The LoadMaster supports a “blacklist” Access Control List (ACL) system. Any host or network entered into the ACL will be blocked from accessing any service provided by the LoadMaster.

The ACL is only enabled when the Packet Filter is enabled. The whitelist allows a specific IP address or address range access. If the address or range is part of a larger range in the blacklist, the whitelist will take precedence for the specified addresses.

If a user does not have any addresses listed in their blacklist and only has addresses listed in their whitelist, then only connections from addresses listed on the whitelist are allowed and connections from all other addresses are blocked.

This option allows a user to add or delete a host or network IP address to the Access Control List. In addition to IPv4 addresses - IPv6 addresses are allowed in the lists if the system is configured with an IPv6 address family. Using a network specifier specifies a network.

For example, specifying the address **192.168.200.0/24** in the blacklist will block all hosts on the 192.168.200 network.

> A static port Virtual Service, with an access list defined to block particular traffic, will not work correctly if you also have a wildcard Virtual Service on the same IP address. The wildcard

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

Virtual Service will accept the traffic after the static port Virtual Service denies it.

It is recommended to use a separate IP address in this case to avoid unexpected behavior resulting from this interaction.

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

10 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.

Using the **System Configuration > Logging Options > Syslog Options** menu, enter an IP address, or addresses, and select the severity level. The syslog server receiving port and protocol for communication (UDP, TCP, TLS) can optionally be configured.

When the TLS protocol is selected, the LoadMaster can use OCSP to check the validity of the server certificates supplied by configured syslog servers. If these checks fail, connections to the server are not permitted.

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

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.

Server Certificate Validation

This check box only appears when **TLS** is selected as the **Remote Syslog Protocol**.

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

When **Server Certificate Validation** is enabled, it ensures that the host name or IP address that was used to initiate the secure connection resides in the Certificate Subject or Subject Alternative Names (SAN) of the certificate.

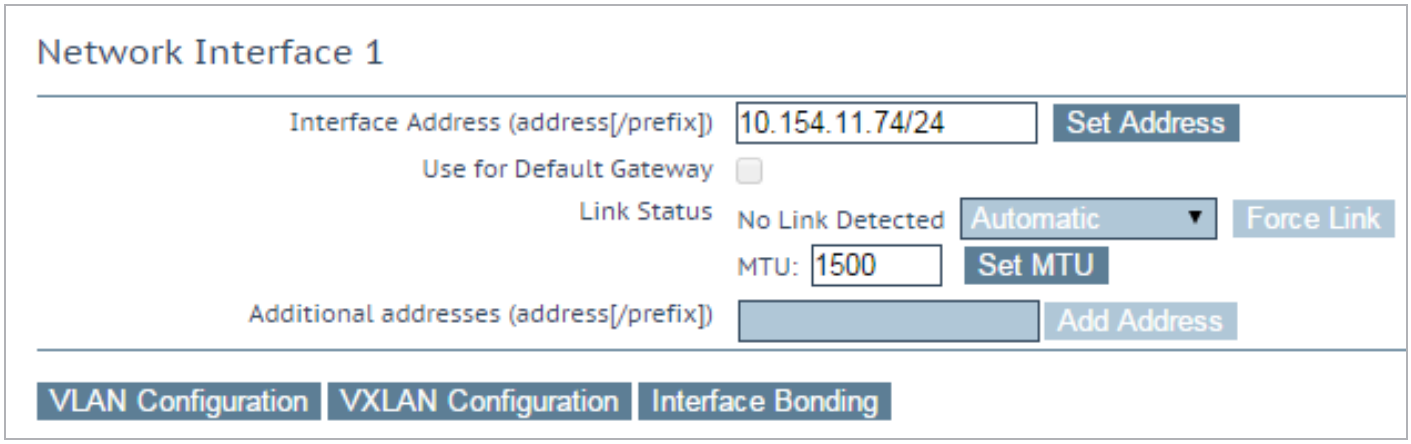
Server Certificate Validation is disabled by default.

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

11 Enable a Minimum of Two Ethernet Interfaces

To meet requirements related to management traffic restrictions to only dedicated management networks, it is necessary to configure at least two network interfaces and dedicate a network or VLAN to management. 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. Using the **System Configuration > Network Setup** menu, follow the steps below:

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

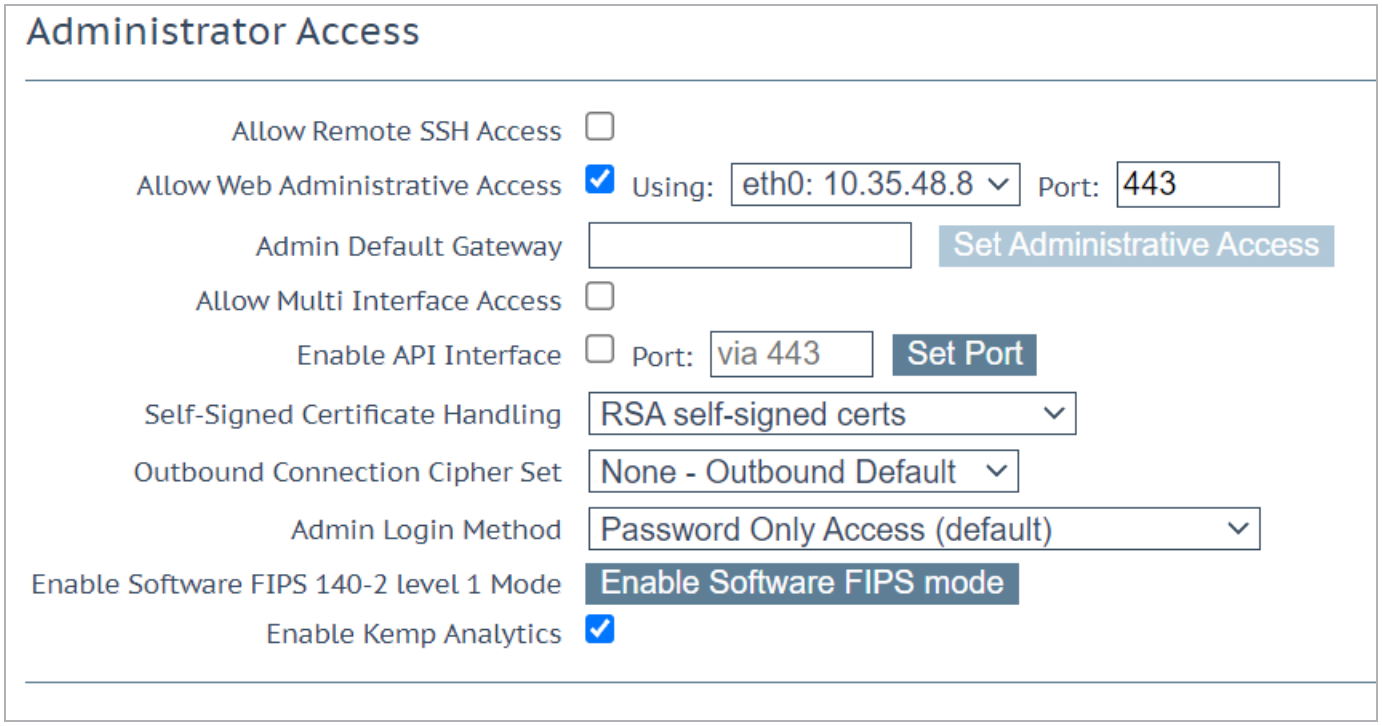


2. Enter the **Interface Address (address[/prefix])**.
3. Click **Set Address**.
4. Configure any other settings as needed.
5. Repeat these steps for all other interfaces.

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

12 Set an Alternate Interface for Management

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



1. Using the **Certificates & Security > Remote Access** menu, select the relevant interface, for example **eth1**, in the **Allow Web Administrative Access** drop-down list.

2. Enter the IP address of the desired default gateway in the **Admin Default Gateway** text box. **Click Set Administrative Access**.

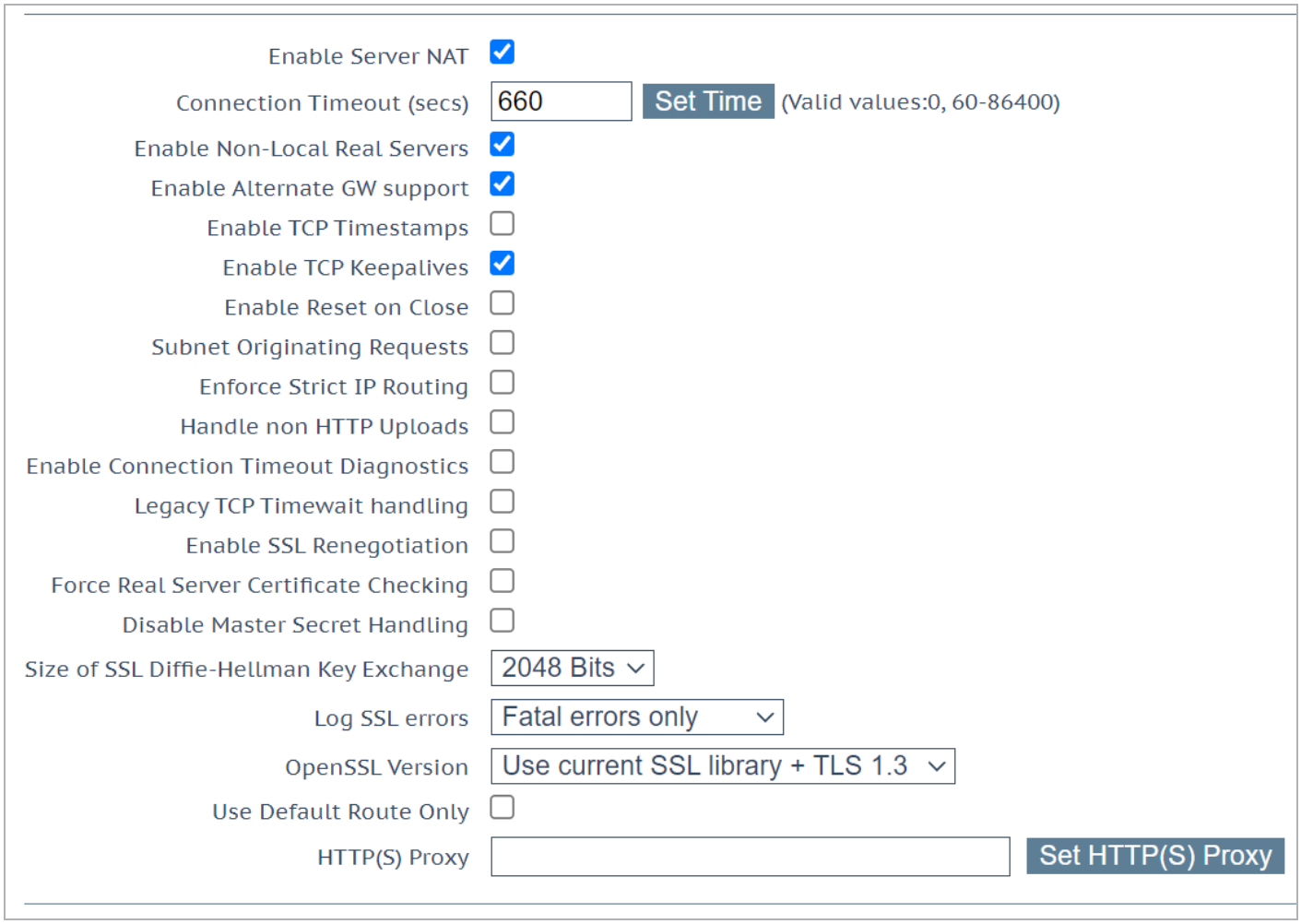
> These settings are not applied until **Set Administrative Access** is clicked.

3. When this is done, you must reconnect your web browser to the new IP address enabled as the management interface for the VLM.

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

13 Enable Alternate Gateway Support

The management interface should be connected to a closed Management VLAN.



To enable alternate gateway support, using the **System Configuration > Miscellaneous Options > Network Options** menu, ensure that the **Enable Alternate GW** support check box is selected.

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

14 Enable DNSSEC Capabilities

Be default, the LoadMaster DNSSEC client is disabled. This option should only be enabled if required and the DNS infrastructure supports DNSSEC capabilities.

DNSSEC helps protect against cache poisoning using a set of extensions that provide origin authentication of DNS data, data integrity and authenticated denial of existence. DNSSEC provides a mechanism to sign requests and prove the validity of records in a given zone and does this through a process called zone signing.

DNSSEC adds four new resource record types:

- Resource Record Signature (RRSIG)
- DNS Public Key (DNSKEY)
- Delegation Signer (DS)
- Next Secure (NSEC)

These resource record types are described in RFC 4034.

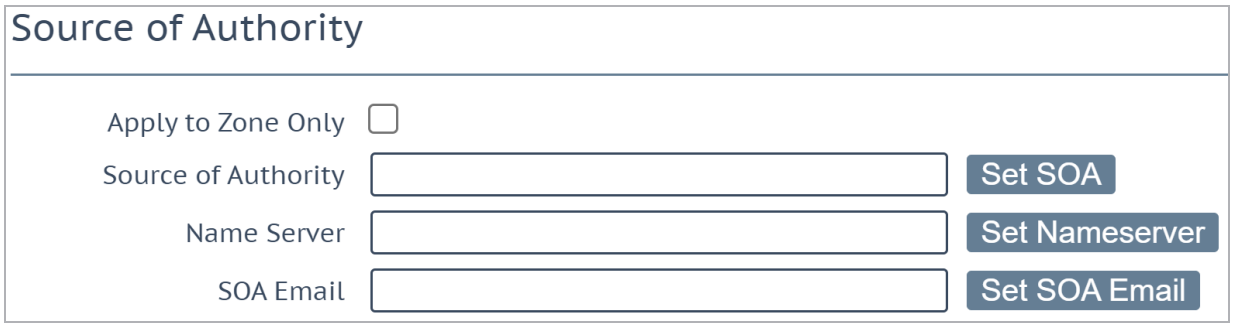
There are also two new DNS header flags, which are:

- Checking Disabled (CD)
- Authenticated Data (AD)

Before configuring DNSSEC, a zone must be defined. You can configure the zone settings in the **Global Balancing > Miscellaneous Params** screen of the WUI. A zone is a single unique part of a DNS namespace hierarchy that serves as the authoritative source for information about a select set of DNS domain names.

To group FQDNs within a zone, the FQDN must be the sub-domain of the zone. Otherwise, each FQDN defines a zone.

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



To define a zone, go to **Global Balancing > Miscellaneous Params** and specify a **Zone Name**.

To enable DNSSEC in the LoadMaster, follow the steps below:

1. Go to **Global Balancing > Configure DNSSEC** to configure the DNSSEC options.



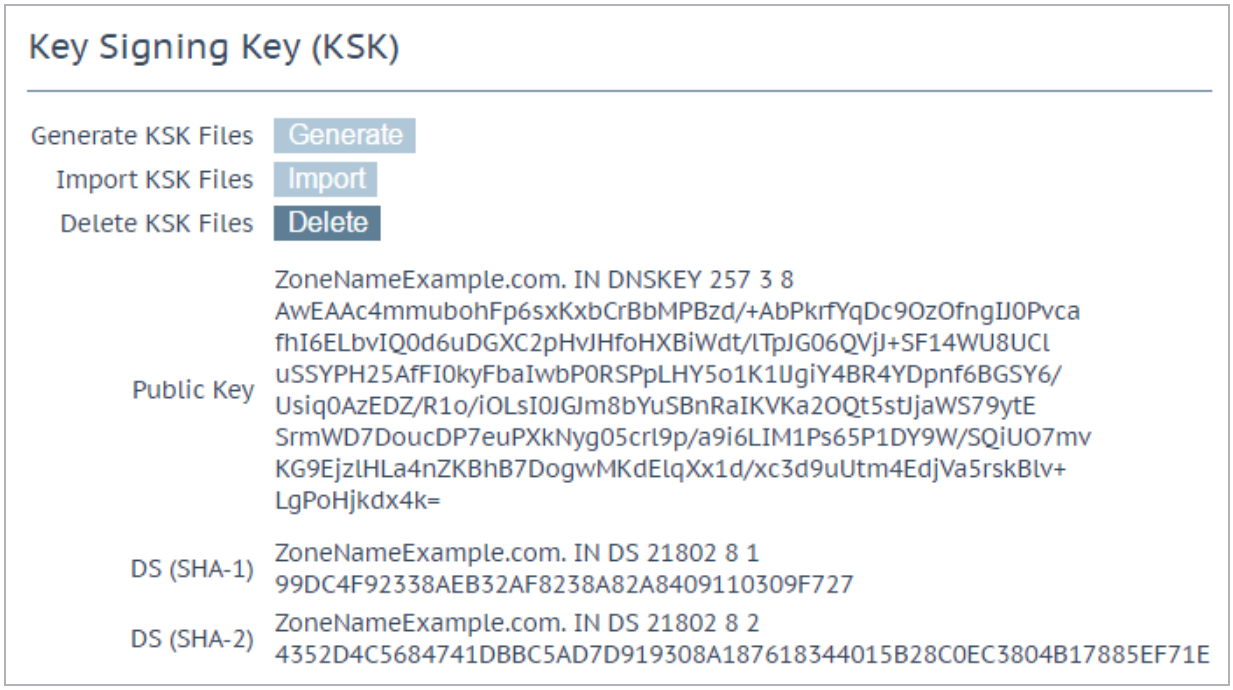
2. You can either import the Key Signing Keys (KSKs), or generate them. To import them, click **Import** and browse to and select the files. If generating, go to the next step.

> A KSK is a type of DNSKEY that is used to sign the keys contained within a DNS zone and are leveraged to validate resolvers. The KSK also signs the Zone Signing Key (ZSK).

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



3. If generating the KSKs, click **Generate**. Select the **Algorithm** and **Key Size** and click **Generate**.



4. The KSK details are displayed.



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

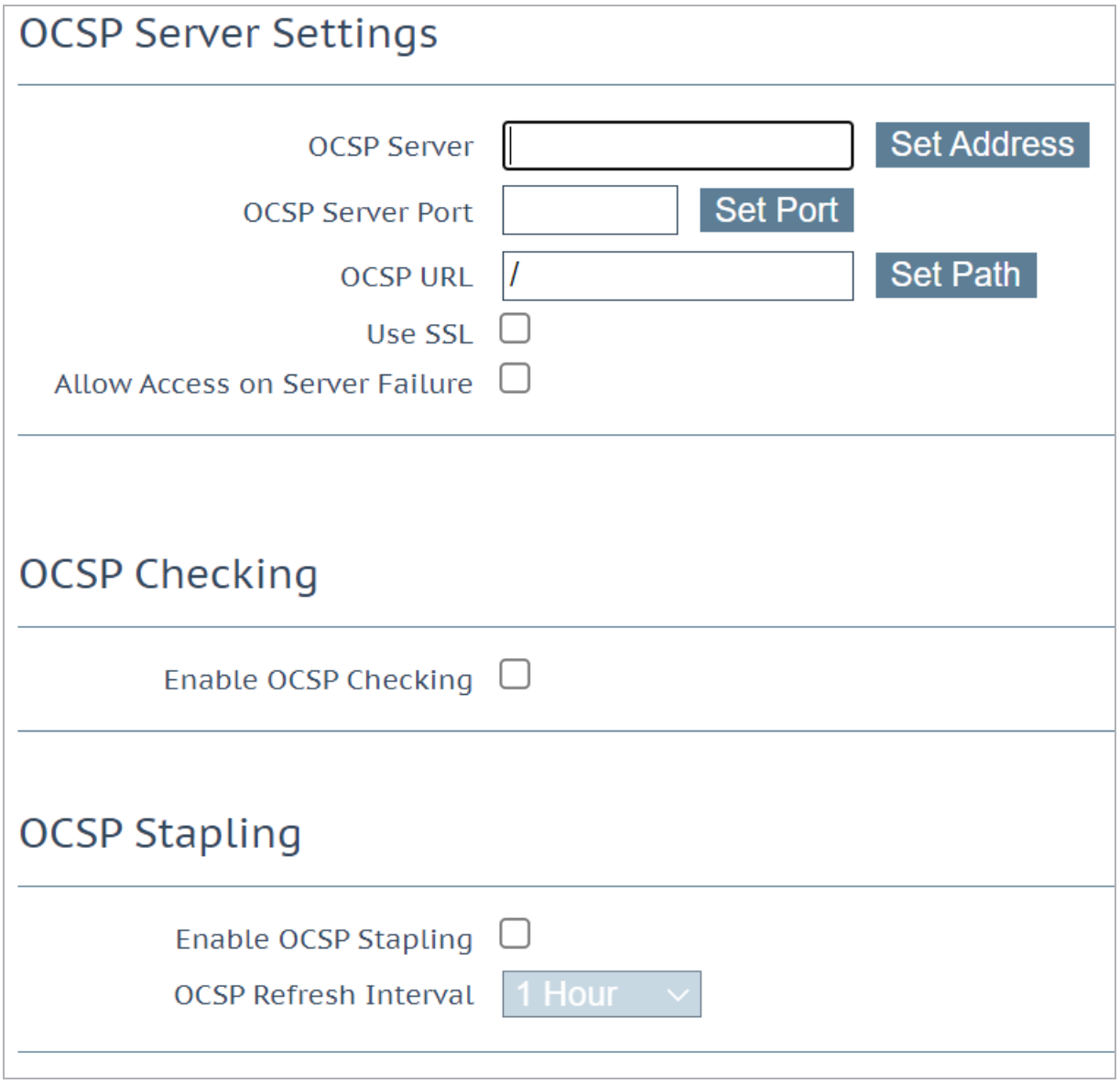
5. Select the **Enable DNSSEC** check box.

There is no user interface for ZSK files. A ZSK is used to generate Resource Record Signatures (RRSIG) for each set of resource records in a zone and sign these records. GEO creates the ZSK files automatically when DNSSEC is enabled. The same algorithm is used as specified for the KSK files. A key size of 1024 is used. If DNSSEC is disabled, the KSK files are deleted.

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

15 Configure OCSP

Facilitate the connection to an Online Certificate Status Protocol (OCSP) service for certificate validation. Enabling OCSP increases the security of your system by requiring the LoadMaster to periodically check the revocation status of the SSL certificates being used by Virtual Services.

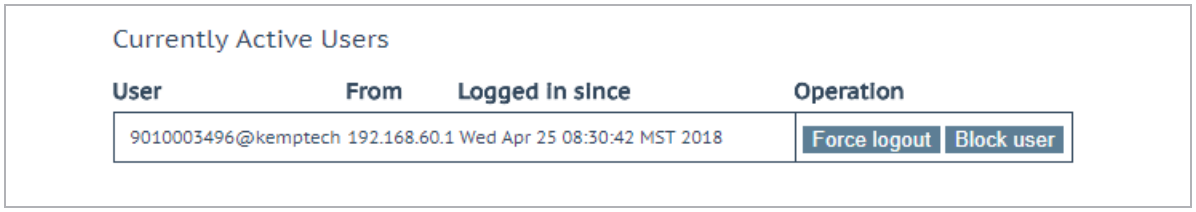


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Using the **Certificates & Security > OCSP Configuration** menu, enter the IP address (or multiple addresses using spaces to separate each entry) of the OCSP service associated with the certificates you are going to use to log in to the LoadMaster. Ensure you click **Set Address**, **Set Port**, and **Set Path** (if needed) to apply the settings.

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

16 Currently Active Users



Using the **Certificates & Security > Admin WUI Access** menu, under **Currently Active Users**, all currently logged in users and logged in times are displayed. An administrator can Block or Force logout of users as required.

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

17 Configure Security Event and Incident Management (SIEM)

SIEM systems are designed to provide a holistic view of network and application security. Once implemented, a SIEM system can help identify attacks and breaches in real time. This has obvious benefits for network security, compliance, and protection of an organization's reputation. It is better for an organization to respond quickly to any attack than to discover after the fact when the damage is done, and data has been compromised.

One aspect of a SIEM system is the deployment of tools to analyze network device logs in real-time. In this way, suspicious activity and known threats that leave well-known signatures in logs can be spotted, and system administrators alerted quickly. Automated responses can often be triggered to counter attacks in real-time.

Tune the SIEM to:

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

You should configure the SEIM, 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.

© 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.