Progress®
Kemp® LoadMaster®

Technical Note LoadMaster Hardening

Generated on: 18 December 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 5

Chapter 2: Choosing a Management Interface 6

Chapter 3: General Guidance 7

Chapter 4: User Accounts 8

Chapter 5: Configure UI Authorization 10

Chapter 6: Configure Remote Access 12

Chapter 7: Configure UI Access Options 13

Chapter 8: WUI Session Management 14

Chapter 9: Enable an NTP Service 16

Chapter 10: Packet Routing Filter 17

Chapter 11: Configure Syslog Hosts 20

Chapter 12: Enable a Minimum of Two Ethernet Interfaces 22

Chapter 13: Set an Alternate Interface for Management. 23

Chapter 14: Enable Alternate Gateway Support 25

Chapter 15: Enable DNSSEC Capabilities 27

Chapter 16: Configure OCSP. 30

Chapter 17: Currently Active Users 32

Chapter 18: Configure Security Event and Incident Management (SIEM) 33

1

Introduction

The 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 LoadMaster appliance has two approved means of access. The first method (Console Access) is typically used to set up 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 LoadMaster.

2

Choosing a Management Interface

Best practice when selecting a management interface is to use the first physical or virtual interface (for example, eth0) as a *dedicated* management interface. By *dedicated* we mean that only management traffic is permitted -- no production application server traffic is sent across this network. This is often described as Out-of-Band Management.

This best practice is common across the industry and recommended by US government standards, as well as by many vendors. US government best practices are described in the document Network Management Security At-a-Glance (Section 2.2).

A similar document is also available from Dell that discusses Management Networks for Dell EMC Networking.

Access to this network as well as access to the ‘bal’ user credentials (and any user logins configured with all permissions) should be restricted to trusted administrative personnel only.

3

General Guidance

This section outlines some general hardening guidance to consider:

- It is strongly recommended that you ensure that you are running at least the latest Long Term Support Feature (LTSF) firmware (7.2.54.x), which has the latest security fixes and updates. Refer to the following knowledge base article for help with selecting a release: Guidance for Selecting LoadMaster Releases.
- Sign up to receive security alerts and announcements from the Progress Alert & Notifications Service.
- 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.

4

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.

Use the following industry-standard guidelines to construct secure passwords for logins, which are based on the advice found in the Cybersecurity and Information Security Agency's (CISA's) strong password guidelines.

- Longer passwords are stronger; use 16 characters or more.
- Use random strings of mixed-case letters, numbers and symbols.
- Use a memorable phrase of 5 - 7 unrelated words; longer words result in a stronger password.
- Use creative spelling, numbers, and symbols.
- Use a different strong password for every account.

Some examples of strong passwords from the CISA document:

- cXmnZK65rf*&DaaD
- Yuc8$RikA34%ZoPPao98t
- Strong: HorsePurpleHatRunBaconShoes
- Stronger: HorsPerpleHatRunBayconShoos

- Strongest: HorsPerpleHat#1RunBayconShoos

We recommend 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**.

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

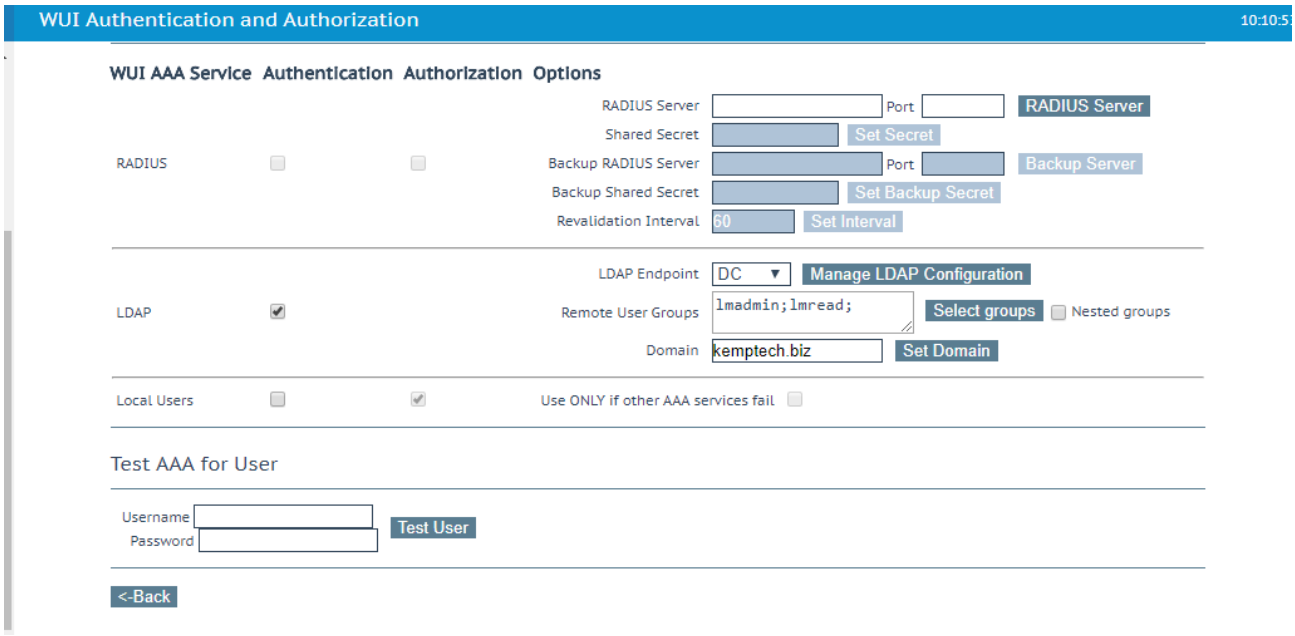
Local user accounts are also configured under **System Configuration > System Administration > User Management**.

Note: If the unit will be placed in High Availability (HA) mode, you should set the **bal** user password identically on both devices in the HA pair to prevent lockouts after fail over.

5

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 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** checkboxes are not selected.

6

Configure Remote Access

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

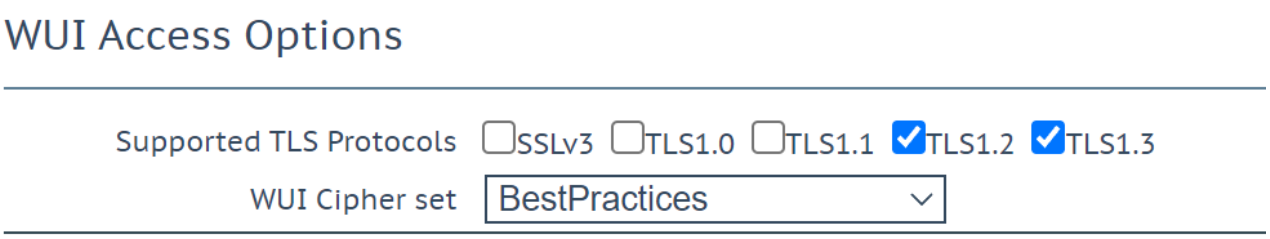
1. Disable **Allow Remote SSH Access**.
2. Enable **Allow Web Administrative Access**. Select the network interface to manage the LoadMaster from the **Using** drop-down list. It is critical to the security of your appliance that you use a dedicated network interface for management traffic; refer to the section Choosing a Management Interface for help making a selection.
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.
6. If you are using High Availability (HA), LoadMaster clustering, or GEO partner functionality - ensure to set the **Partner Shared Secret**.

Note: When an incoming shared secret does not match the local **Partner Shared Secret** (including if only one side is providing a shared secret), a warn-level log message is recorded that says **Unauthorized Remote Machine connection from <ClientIPAddress>** and the connection fails.
This secret must have a minimum of 8 and a maximum of 127 characters. The following characters are supported:

- Numeric: 0-9
- Uppercase alphabetic: A-Z
- Lowercase alphabetic: a-z
- Special characters: !"#$%&()*+,-./:;<=>?[\~]^_@`{|}

7

Configure UI Access Options



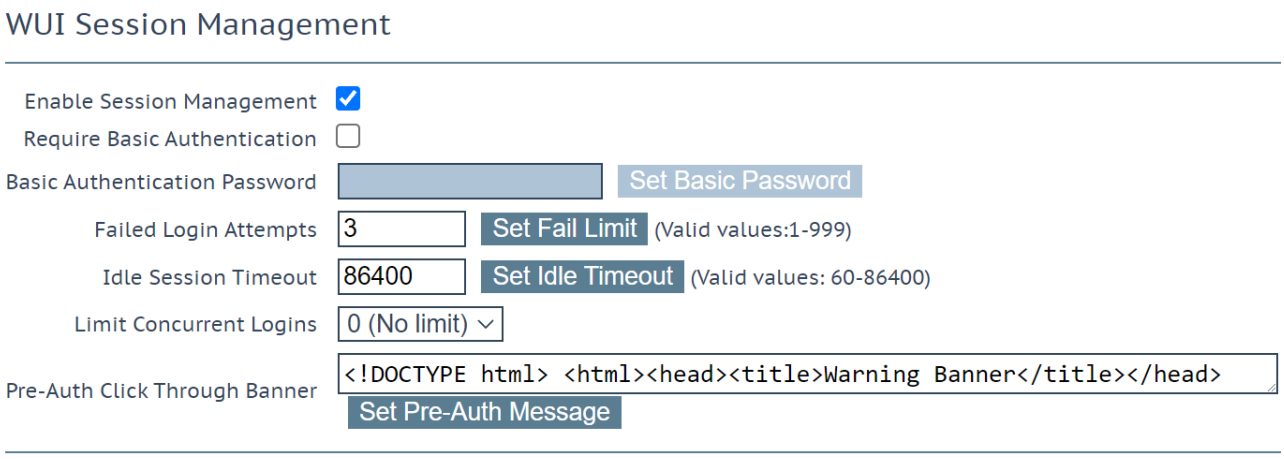
Using the **Certificates & Security > Admin WUI Access** menu, under **WUI Access Options**, ensure **SSLv3**, **TLS1.1**, and **TLS1.0** are not selected. Ensure the **WUI Cipher set** is set to **Best Practices**.

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

8

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**.



We recommend 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. we recommend 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. We recommend setting the number of concurrent logins to be in line with any organizational requirements.

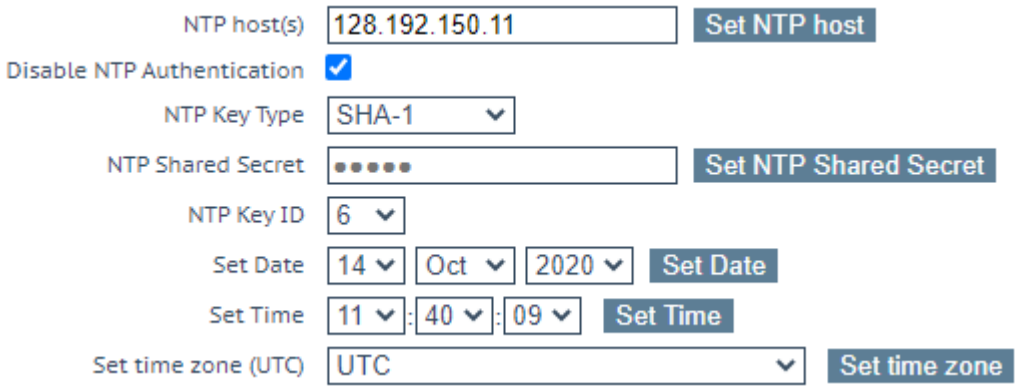
Set the **Pre-Auth Click Through Banner** that is displayed before the LoadMaster WUI login page. Users are not permitted to log in until they click **Accept**. This field can contain plain text or HTML code. The field cannot contain JavaScript. For security purposes, you cannot use the '‘ (single quote)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

9

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**.

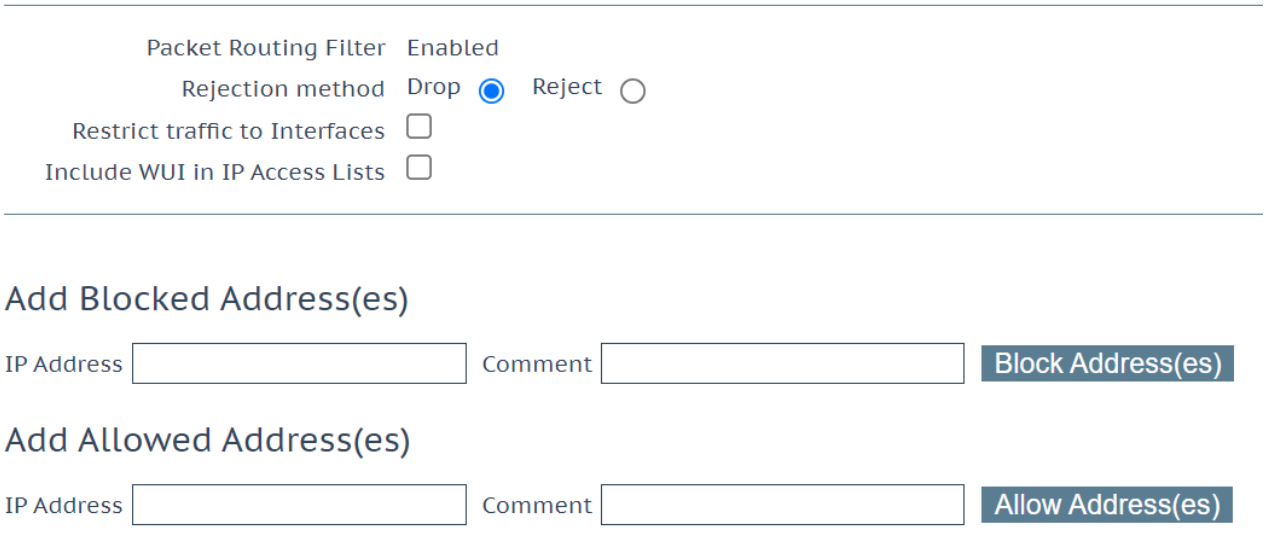


2. To enable NTPv3, select the **Show NTP Authentication Parameters** check box.
3. Ensure the **NTP Key Type** is set to **SHA-1**.
4. Set the **NTP Shared Secret** and **NTP Key ID** to the appropriate value(s) on the NTP Server.
5. In the **NTP host(s)** text box, specify the host(s) from which the 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.

10

Packet Routing Filter



Packet Routing Filter

If the packet routing 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.

Note: 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

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. Progress Kemp has this option disabled by default.

Include WUI in IP Access lists

By default, the access control lists on the **Packet Routing Filter** page control access to the Virtual Services on the LoadMaster but not WUI access. If the **Include WUI in IP Access Lists** option is enabled, access to the WUI is also controlled by the access control lists. Enabling the **Include WUI in IP Access Lists** option allows the WUI to be accessed only from the IP address that enabled the check box - a message appears next to the check box saying **Access allowed from <IPAddress>**. This protects you from locking yourself out of the WUI. Attempts to log in from other IP addresses will be denied. If access to the WUI is needed from other IP addresses, you must add them to the allowed list.

The **Include WUI in IP Access Lists** option is only designed to work with one IP address.

Enabling the **Include WUI in IP Access lists** option does not affect any current access to Virtual Services. For example:

- If you enable the **Include WUI in IP Access lists** option from an IP address that is not in either the allowed or blocked lists, that IP address has access to the WUI and all the Virtual Services.
- Other IP addresses not in either the allowed or blocked list do not have access to the WUI but they do have access to all Virtual Services.

If you add IP addresses using the **Add Allowed Address(es)** fields, the connectivity for all other IP addresses will be blocked to the Virtual Services.

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

If you need to, you can disable the access control lists using the console interface.

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.

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

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

11

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.

Note: 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**.

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

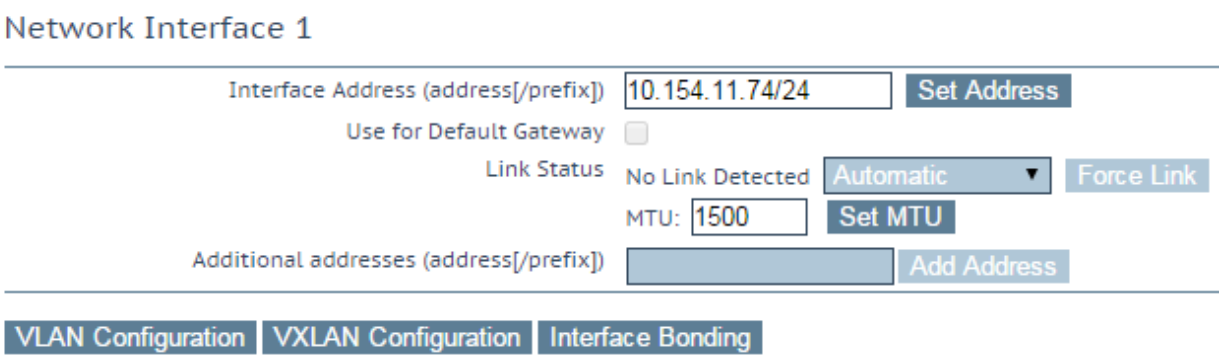
Server Certificate Validation is disabled by default.

12

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 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**.

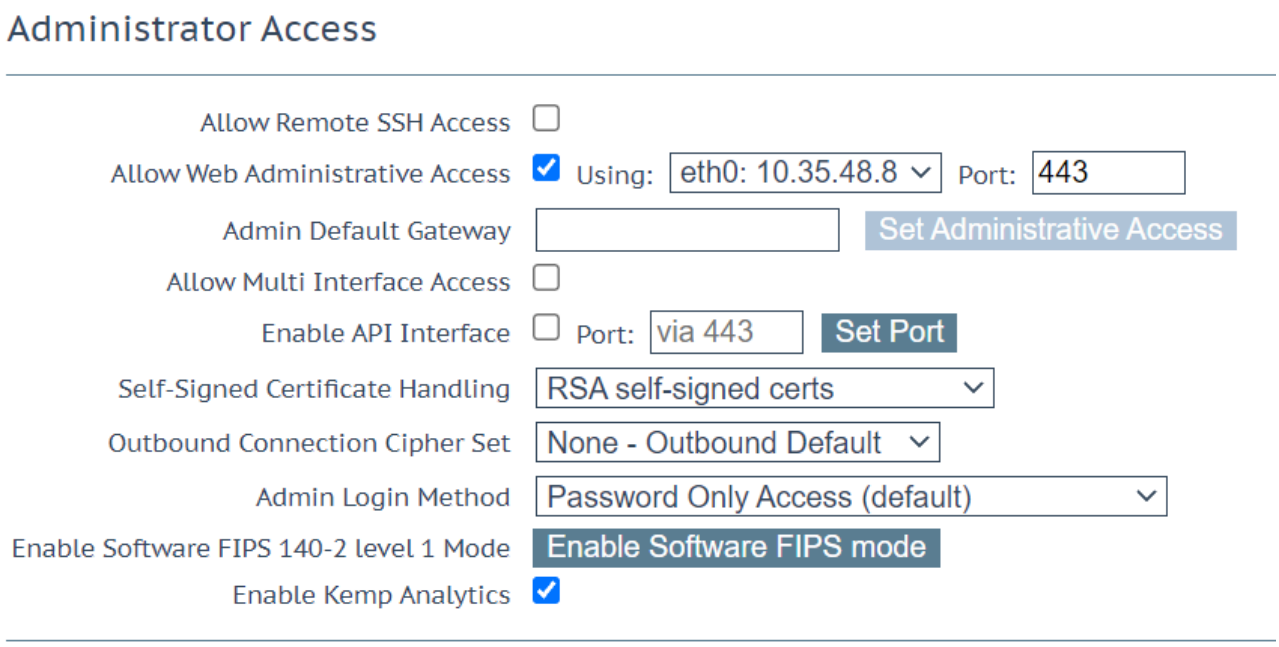


2. Enter the interface address (address[/CIDR notation]).
3. Click **Set Address**.
4. Configure any other settings as needed.
5. Repeat these steps for all other interfaces.

13

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.

Note: It is critical to the security of your appliance that you use a dedicated network interface for management traffic; refer to the section Choosing a Management Interface for help making a selection.

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

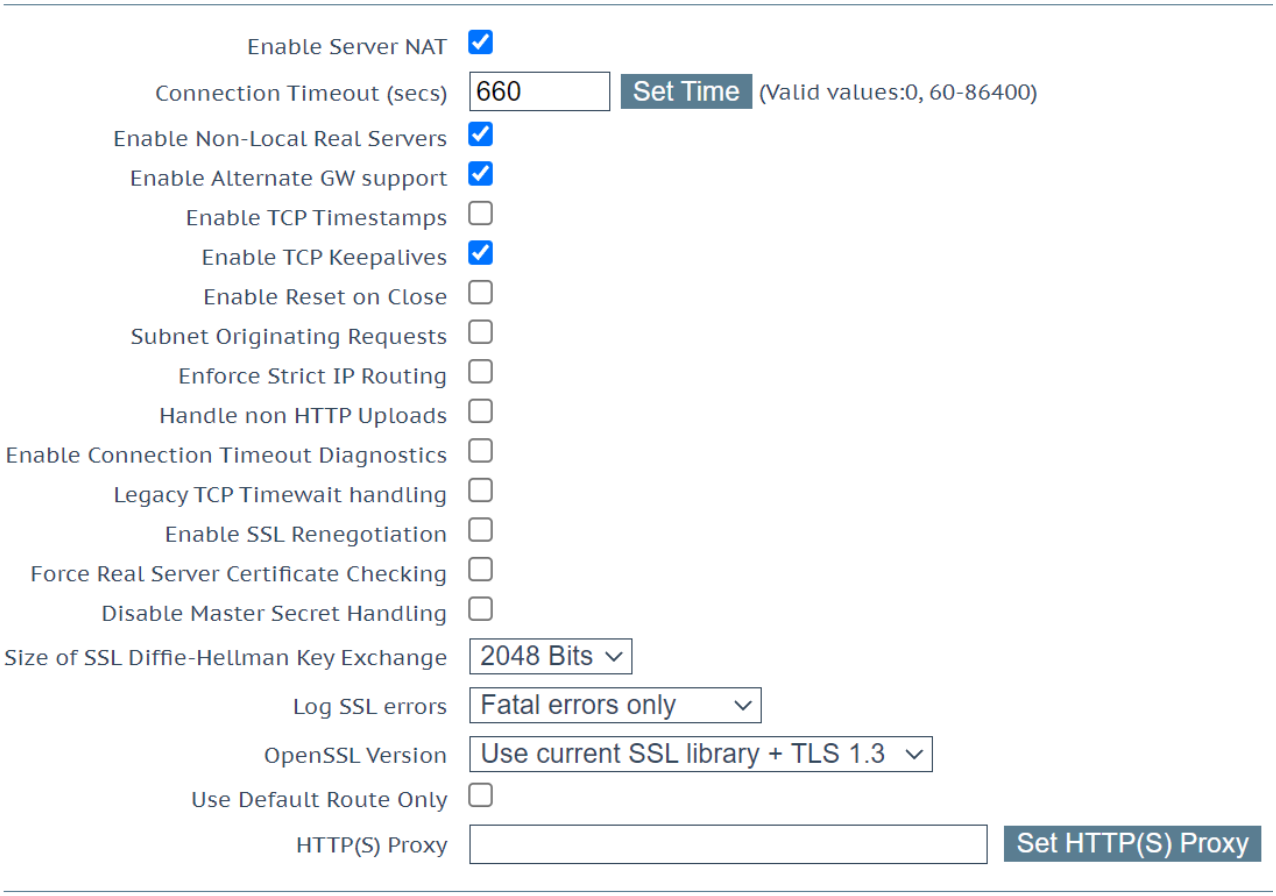
Note: These settings are not applied until **Set Administrative Access** is clicked.

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

14

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.

15

Enable DNSSEC Capabilities

By 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.

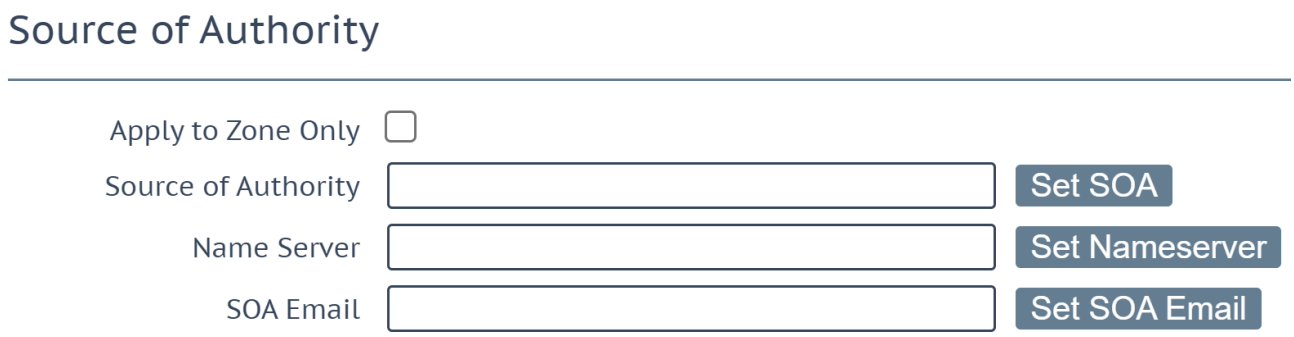
There are also two new DNS header flags, which are:

- 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.



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.



Note: 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).

Note:

If you have GEO partners and want to use DNSSEC, you must generate the KSK files outside of the LoadMaster using the BIND **dnssec-keygen** command and import them onto each GEO partner separately, for example:

```
dnssec-keygen -a RSASHA256 -f KSK -b 2048 -n ZONE <zone_name>
```

Then, import the generated KSK files onto each GEO LoadMaster separately.

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



4. The KSK details are displayed.



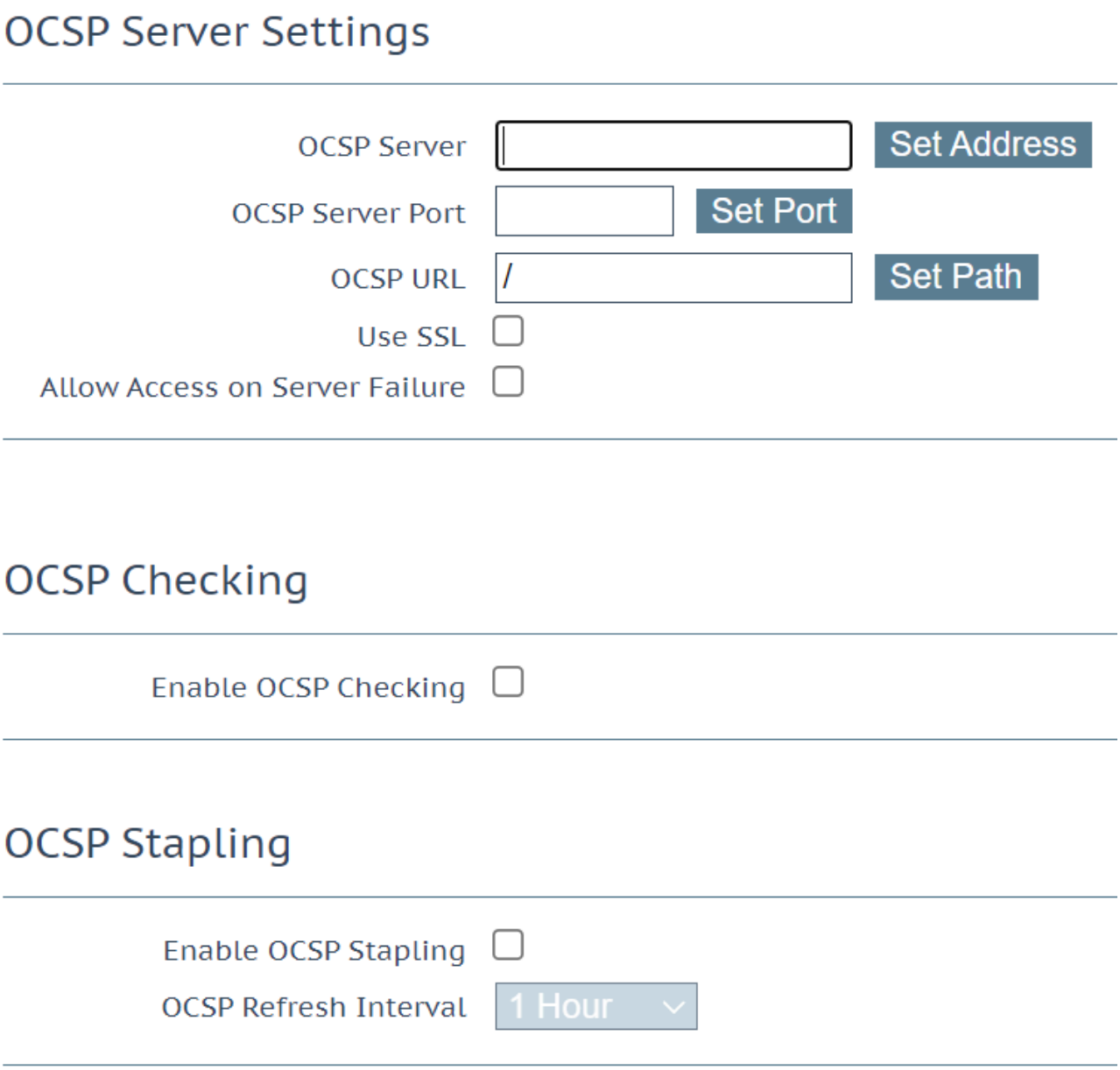
5. Select the **Enable DNSSEC** check box.

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.

16

Configure OCSP

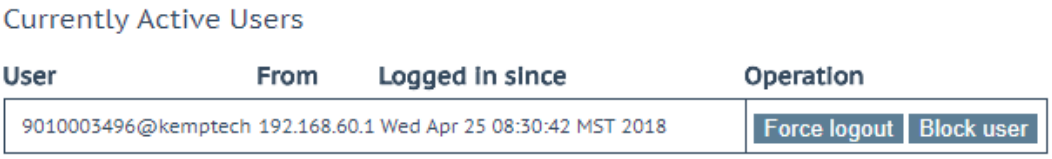
Facilitate the connection to an Online Certificate Status Protocol (OCSP) service for certificate validation. Enabling OCSP increases the security of your system by requiring the LoadMaster to periodically check the revocation status of the SSL certificates being used by Virtual Services.



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.

17

Currently Active Users



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

18

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 Manager. For further information on how to configure SEIM, refer to the relevant third-party product documentation.