PROGRESS LOADMASTER OS 7.2.54.18 COMMON CRITERIA CONFORMANCE GUIDE

VERSION 0.5

DOCUMENT PREPARED BY:

Intertek Acumen Security, LLC
2400 Research Blvd, Suite 395
Rockville, MD 20850
www.acumensecurity.net

TABLE OF CONTENTS

Revision History

VERSION	DATE	CHANGES
0.1	05/28/2025	Initial Release
0.2	06/09/2025	Formatted document
0.3	06/13/2025	Addressing internal lead comments
0.4	05/06/2026	Updates based on QA
0.5	06/18/2026	Updates based on ECR

COMMON CRITERIA CONFIGURATION INSTRUCTIONS

Follow the instructions in this document to install and license LoadMaster, and to make the configuration changes required after installation to bring the system into "Common Criteria mode".

This document is a guide to the Progress Software Corporation's Progress LoadMaster implementation of the collaborative Protection Profile for Network Devices, Version 3.0e, (CPP_ND_V3.0E).

1. TARGET RELEASE

These instructions have been prepared for **Progress Software Corporation's Progress LoadMaster OS Version 7.2.54.18**, which is the Common Criteria tested, evaluated, and certified release. This release can be downloaded directly from firmware download page of Progress website at: https://support.kemptechnologies.com/hc/en-us/sections/4405063394061-Latest-Firmware. If this firmware version is not available, please reach out to Progress Support at https://support.kemptechnologies.com/hc/en-us/articles/201870787.

2. TOE DELIVERY

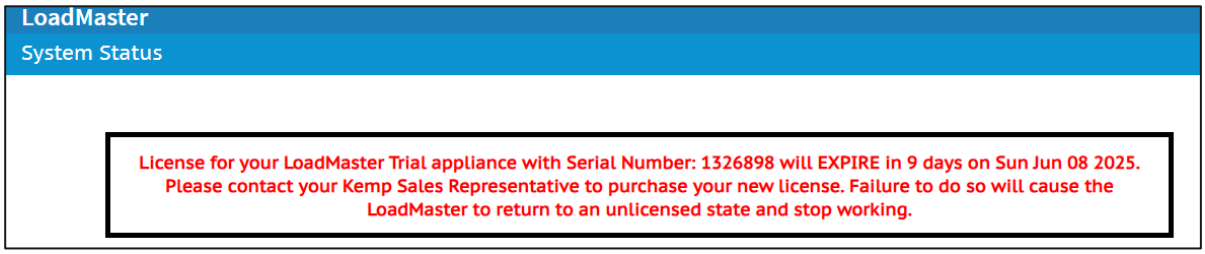
The TOE is delivered via commercial carrier (i.e. FedEx, UPS, Expeditors etc.). The TOE will contain a packing slip with the serial numbers of all shipped devices. The receiver must verify that the hardware serial numbers match the serial numbers listed in the packing slip. The TOE is shipped with the software pre-installed on it.

3. INSTALLATION PROCESS

The only prerequisite is the deployment, licensing, and initial configuration of LoadMaster. An additional VMware platform installation document is available from the Progress website to guide you through this process for Virtual LoadMaster. Please note the following:

- You need a console connected during the initial boot process.
- After boot, you will use the console to set the IP address data for the LoadMaster.
- You'll need to Register (https://sso.kemptechnologies.com/register/kemp) for license the unit online; it's a simple process that is confirmed via email.
- When you reach the point in the VMware platform installation document where LoadMaster is licensed, be sure to choose the **Online Licensing** option, specify the Progress ID and password you created, and accept the license provided by the licensing server.

Note: From 13 days prior to the license or subscription expiry date, a message is displayed on the **Home** screen that states the expiry date. To relicense the appliance or to renew your subscription, contact Progress. Failure to relicense may cause the LoadMaster to stop working.



Upgrade: Upgrade the LoadMaster by buying a license from the Progress purchase portal.

4. Operational Environment

The following environmental components are required to operate the TOE in the evaluated configuration:

- Management Workstation providing local console access to the TOE and a browser to connect to the Web User Interface (WUI) over TLSv1.2.
- Syslog server that receives audit logs from the TOE over TLSv1.2.
- ESXi v7.0 U3 acting as the hypervisor for Virtual LoadMaster.
- Authentication server supporting LDAP over TLSv1.2.
- NTP server supporting SHA-1 integrity verification with NTPv4.
- OCSP server that receives ocsp requests from TOE over HTTP.
- CA Server that provides signed certificates over HTTP.

5. Supported Platforms

The TOE boundary consists of one of the appliances listed below. The LoadMaster X25-NG, LoadMaster X40-NG, ECS CM H2 NG and ECS CM H3 NG are physical devices while the Virtual LoadMaster is a virtual machine which runs on ESXi. The virtual TOE is conformant with Case 1 as described in the NDcPP.

Table 1 – TOE Physical Boundary Components

Model	LoadMaster X25-NG	LoadMaster X40-NG	ECS CM H2 NG	ECS CM H3 NG	Virtual LoadMaster
Processor	Intel Xeon Silver 4316 (Ice Lake)	Intel Xeon Silver 4316 (Ice Lake)	Intel Xeon Silver 4316 (Ice Lake)	Intel Xeon Silver 4316 (Ice Lake)	Intel Xeon Gold 5222 (Cascade Lake)
RAM	64 GB RAM (evaluated)	64 GB RAM (evaluated)	128 GB RAM	128 GB RAM	4GB (evaluated)
Network	2 1Gb Ethernet 8 10Gb Ethernet Fiber	2 1Gb Ethernet 8 10Gb Ethernet Fiber	2 1Gb Ethernet 8 10Gb Ethernet Fiber 4 25Gb Ethernet Fiber 4 100Gb Ethernet Fiber	2 1Gb Ethernet 8 10Gb Ethernet Fiber 4 25Gb Ethernet Fiber 4 100Gb Ethernet Fiber	2 10Gb virtual NIC
Platform	LoadMaster OS 7.2.54.18	LoadMaster OS 7.2.54.18	LoadMaster OS 7.2.54.18	LoadMaster OS 7.2.54.18	LoadMaster OS 7.2.54.18 on ESXi v7.0 U3

6. CC CONFIGURATION PROCESS

Once you complete the steps in the above document, follow the steps in these sub-sections.

When administrators log in with role-based credentials, their access is limited to commands they have privileges and permissions to use based on the Common Criteria standards. No management functionality is available prior to successful identification and authentication of the users.

In an evaluated configuration, TOE supports only a trusted channel to an external audit server (a syslog server). That trusted channel must be configured to be protected by TLS.

Network management communication paths are protected against modification and disclosure by TLS.

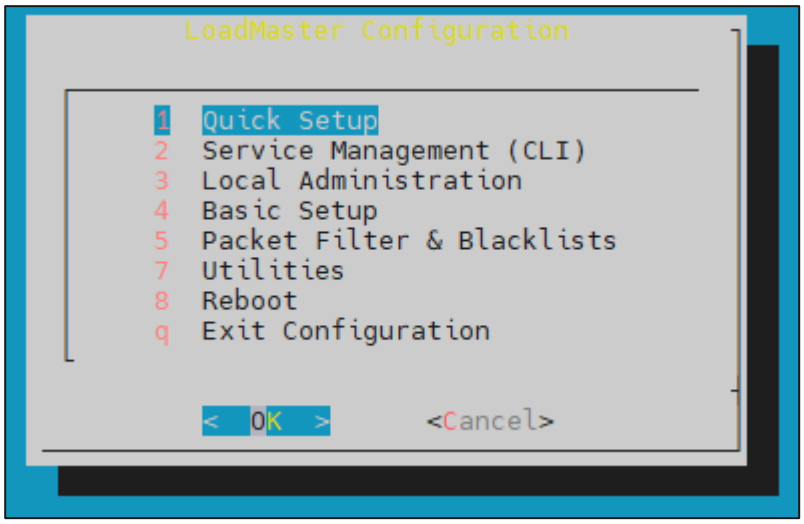
TOE has only one normal operational mode. The TOE implements a suite of self-tests at startup and halts or disables affected functionality if a self-test fails

6.1. LOGIN VIA CONSOLE

The Command Line Interface allows users to interface with the LoadMaster via a command line shell or a menu-based series of options.

1. You will need a PC to connect via COM+ (Console) port with a terminal emulation application, or a standard VGA and keyboard. Use a null modem cable (reversal) to connect the COM+ port to the LoadMaster COM port on the rear of the unit.
2. The COM+ settings should be 115200, 8, N,1.
3. After initially deploying and powering on a LoadMaster, ideally the IP address of the LoadMaster will be obtained via DHCP.
4. If the IP address has not been obtained via DHCP, or if the address details of the LoadMaster need to be changed, the console can be used to configure the IP address of the LoadMaster, the default gateway address and the name server addresses.
5. To go through this menu, simply log in to the console using the default username and password **(bal and 1fourall)**.

After successful login, the console displays the LoadMaster configuration menu as shown below:

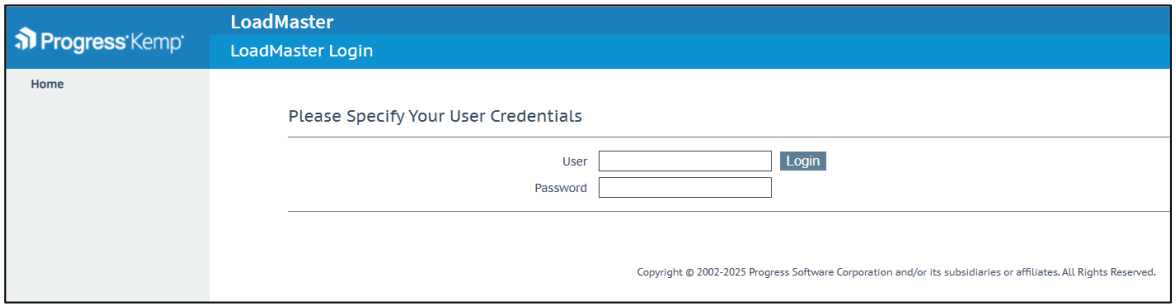


6.2. LOGIN VIA WUI

Prior to authentication, the TSF only permits users to access a warning banner (if configured) and to generate system keys automatically during first-time setup. The TOE does not expose any other interface or administrative access prior to successful login. All authenticated access requires a valid username and password.

The following steps describe the login process via the WUI:

1. Launch a web browser from a laptop that is connected to the device.
2. **Log in to the WUI** via HTTPS using the IP address assigned during installation, the 'bal' administrative login, and the password you specified during installation.

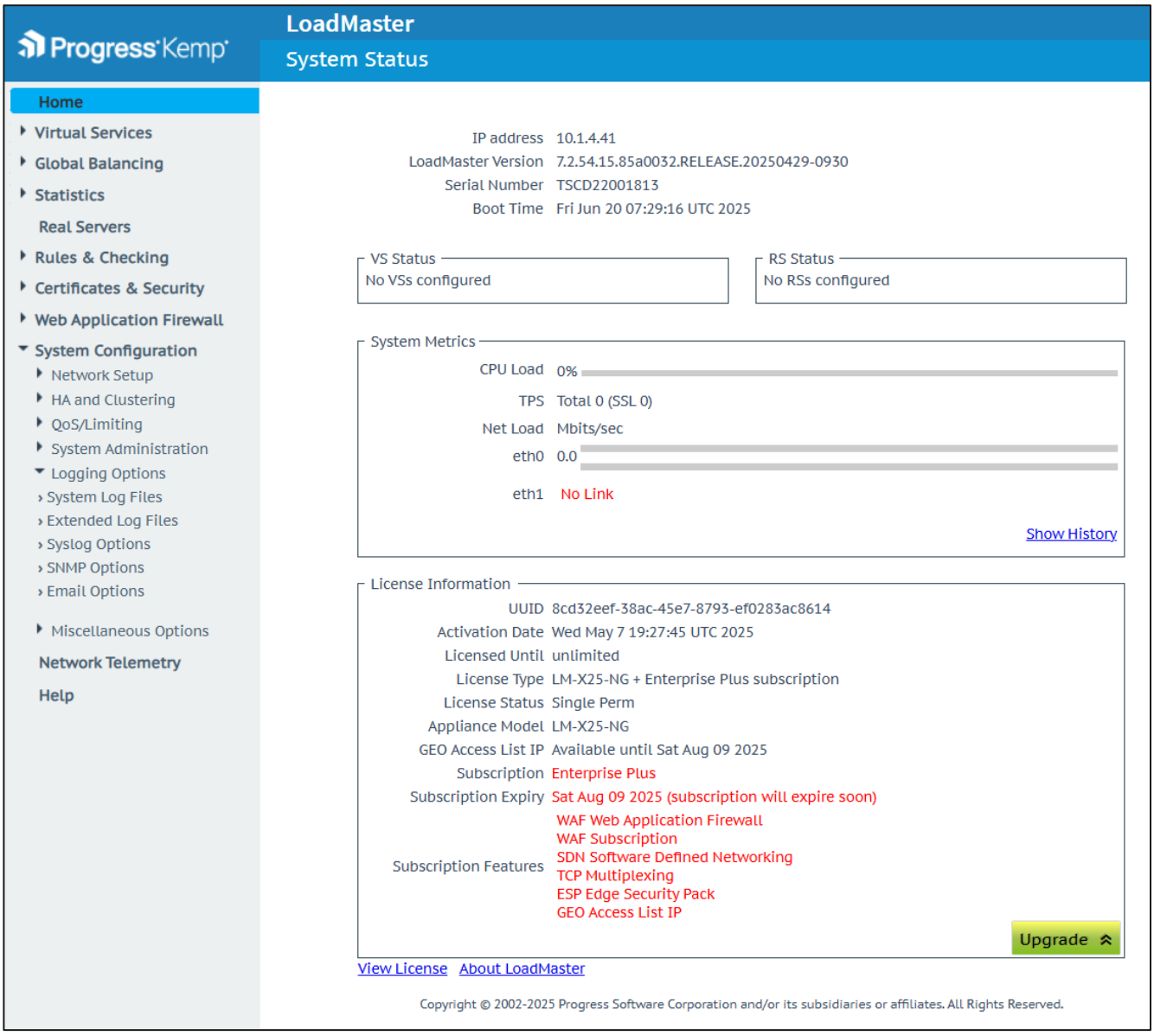


   a. Download the LoadMaster issuing CA ECDSA certificate and install it in the management workstation certificate store and/or the browser certificate store.

3. After initially logging in to the LoadMaster, if Session Management is enabled - some login information is displayed:
   a. The last login time and IP address of the current user
   b. The number of successful logins by the current user in the last 30 days
   c. The total number of failed logins attempts by any user (including unknown usernames) since the last successful login
   d. Audit Logs are generated for each action which is performed by a user; either using the API or the WUI.

4. The primary user (bal) always has full permissions. Secondary users may be restricted to certain functions.
5. Only the bal user is permitted to set the Basic Authentication password.
6. Users must be authenticated before logging on to the LoadMaster.

After successful login, the Web User Interface displays the Home page with system information, as shown below:



6.3. Authentication And Role-Based Access Control

No administrative or security-relevant functions are available until the user has successfully authenticated, and the feedback during authentication is obscured. Only authenticated users with the appropriate permissions can view or modify TSF data. Unauthorized users cannot perform any security-related actions.

Users must be authenticated before logging on to the LoadMaster.

Users with the 'All Permissions' permission set can view the **Enable Session Management**, **Require Basic Authentication,** and the **Basic Authentication Password** fields. However, users with the 'All Permissions' permission set can configure the **Failed Login Attempts** and **Idle Session Timeout values**.

Users with the 'User Administration' permissions set can view the screen but all buttons and input fields are greyed out.

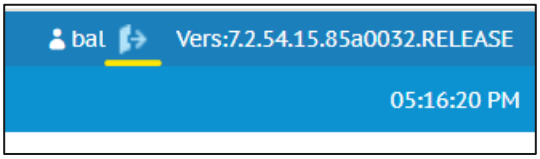
All other users cannot view the **WUI Session Management**, **Currently Active Users** or **Currently Blocked Users** sections of the **WUI Configuration** screen.

Note: Both the 'bal' and administrator accounts are assigned to the **Security Administrator role**, which grants permission to manage all TSF functions and configuration. All administrative access to the system must be authenticated through these accounts.

6.4. LOG OUT

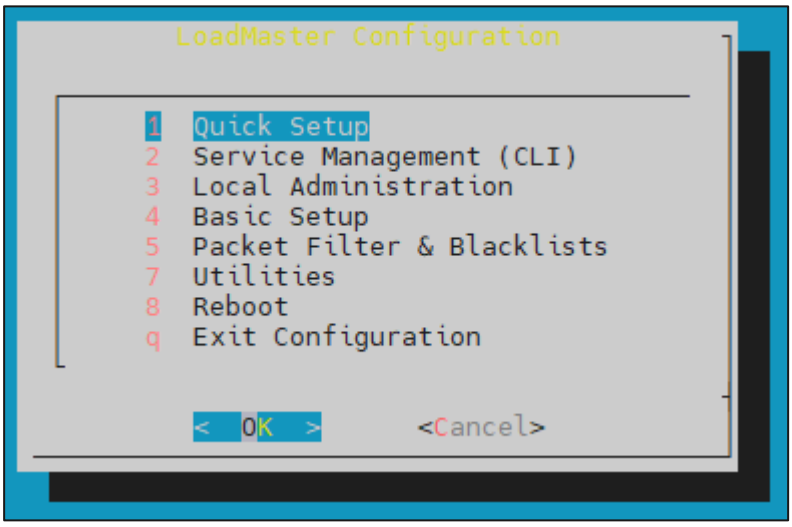
For WUI:

1. After logging in via the WUI, the user can log out by clicking the Logout button, located in the **top right-hand corner** of the screen.



For CLI:

1. When accessing the console, the main menu is displayed by default.



2. To log out of the console session, press **q** to **Quit** the session.

6.5. IDLE SESSION TIMEOUT

TOE allows administrators to configure an idle session timeout to automatically log out inactive sessions. This configured timeout applies to both remote WUI sessions and the Local console sessions.

To configure the idle timeout setting via WUI:

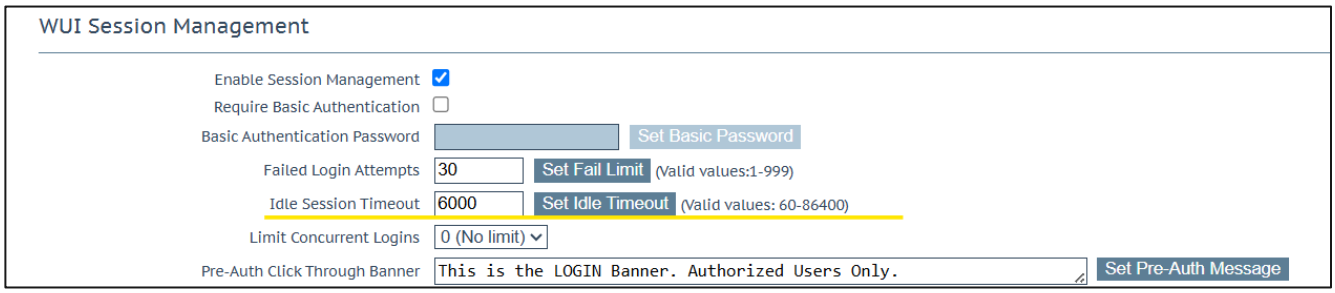
1. In the left frame menu in the WUI, navigate to:

   System Configuration > Certificate & Security > Admin WUI Access > Idle Session Timeout.

   The length of time (in seconds) a user can be idle (no activity recorded) before they are logged out of the session.

2. Enter the desired timeout value in seconds.

   - Valid values range from **60 seconds (1 minute)** to **86400 seconds (24 hours)**.
   - This setting determines how long a session can remain idle before it is automatically terminated by the TSF.



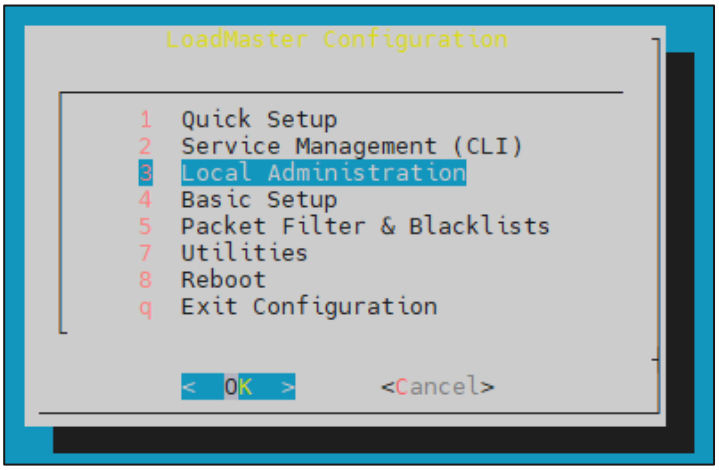
The TSF allows the administrator to terminate their own active local or remote interactive session through the session management options in the WUI.

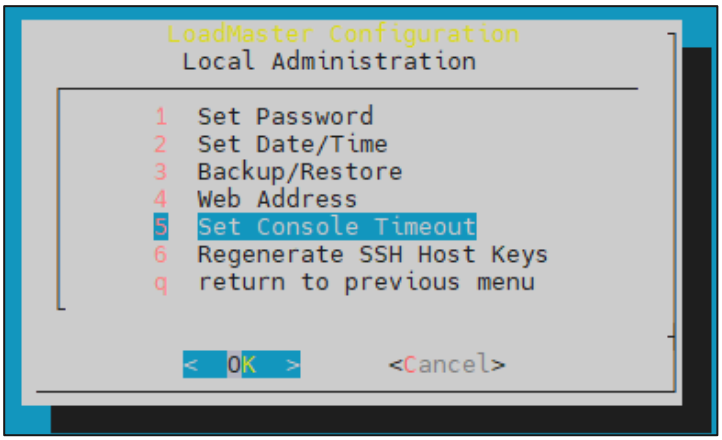
The TSF enforces an **administrator-configurable session inactivity timeout**, which can be set from **1 to 1440 minutes**. If an administrative session remains idle beyond the configured timeout, the TSF automatically terminates the session.

To configure the idle timeout setting via Console:

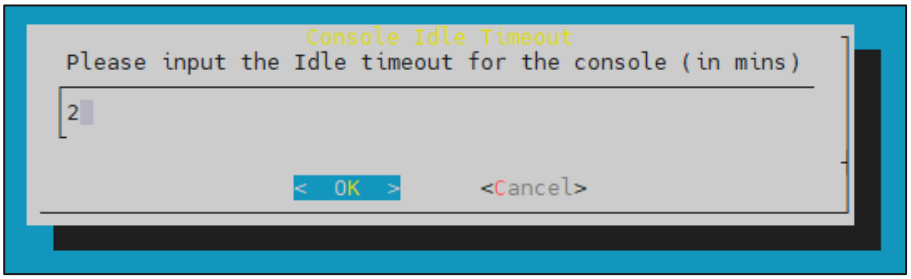
1. After logging in to the Console, Navigate to:

   Local Administration > Set Console Timeout





2. When prompted, input the desired idle timeout value.
    - Valid values range from **1 minute (60 seconds)** to **1440 minutes (24 hours)**.



    - This setting determines how long a CLI/console session can remain idle before it is automatically terminated by the TSF.

6.6. Set Minimum Password Length

1. In the left frame menu, click **System Configuration > System Administration > User Management** to set the desired **Minimum Password Length** (default is 8).
2. The TSF allows administrators passwords to be composed of any combination of upper and lower case letters, numbers and the following printable ASCII character (i.e. 0x20-0x7E inclusive):

    “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “ “, “‘”, “‘”, “+”, “,”, “-“, “.”, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “@”, “[“, “\”, “]”, “_”, “`”, “{“, “|”, “}”, “~”;

3. The Minimum Password Length should be configured between 8 and 16 characters.

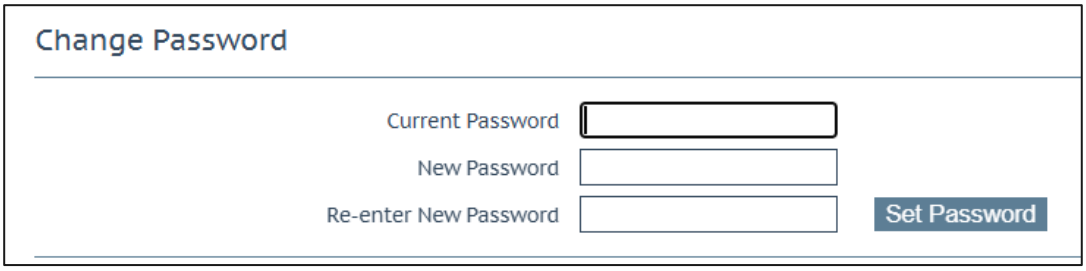
6.7. Change The Password

6.7.1. Changing The Password For Current User

To change the password for the currently logged-in user via the WUI:

1. Log in to the Web User Interface using valid credentials.
2. Navigate to **System Configuration** > **System Administration** > **User Management** > **Change Password**.

3. Enter the following details:
    - **Current Password**
    - **New Password**
    - **Re-enter New Password**
4. Click on **Set Password** to apply the changes.



Note: Ensure the new password meets any configured password policy requirements.

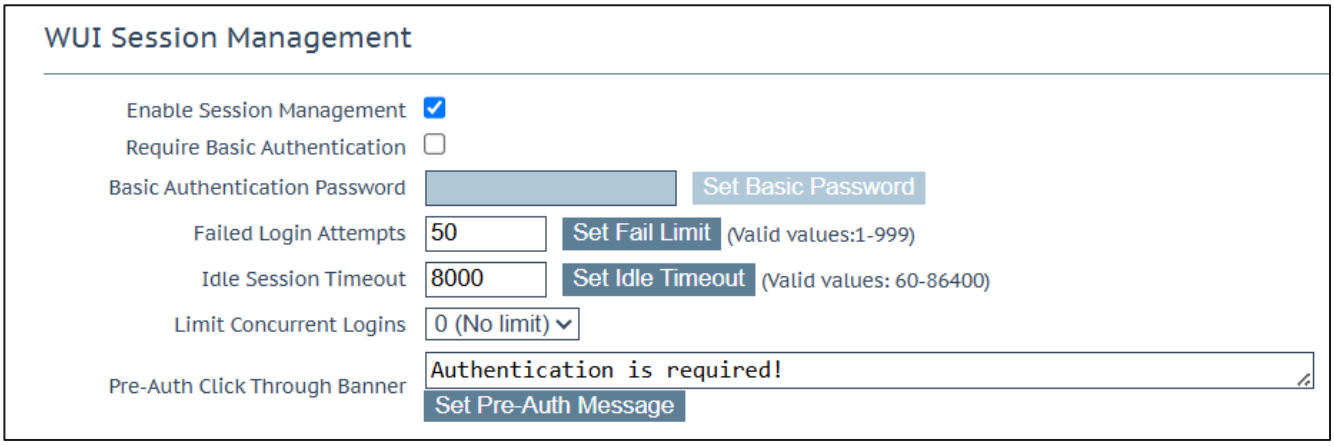
6.7.2. Changing The Password For Another User

To change the password of a different user (not the currently logged-in user):

1. Navigate to **System Configuration** > **System Administration** > **User Management** > **Local Users**.
2. Select the target user from the list.
3. Click on **Modify**.
4. Enter and confirm the new password, then save the changes.

Note: Only users with appropriate administrative privileges can modify other users' passwords.

6.8. FAILED LOGIN ATTEMPTS



The TSF blocks remote authentication attempts after a configurable number of consecutive failed login attempts. This policy is enforced for remote administrative access via the WUI (TLS-based).

To configure the maximum number of failed login attempts:

1. In the left frame menu of the Web User Interface (WUI), navigate to:

   System Configuration > Certificate & Security > Admin WUI Access > Failed Login Attempts

2. Set the desired value in the **Failed Login Attempts** field.
   - This specifies the number of times a user can fail to authenticate before their account is blocked.
   - Valid values range from **1 to 999.**
3. If a user account becomes blocked due to failed login attempts:
   - The account must be manually **unblocked** by the bal user or another user with **All Permissions** set.
   - If the bal user is blocked, there is an enforced **cool-down period of 10 minutes**, after which the bal user can log in again.

The TSF ensures that administration is always possible, even in the event of a lockout. **Local console access is never locked**, ensuring that a security administrator can always regain access to the system even if all remote interfaces are temporarily inaccessible.

This lockout policy applies to **all remote authentication channels**, for access over TLS (WUI).

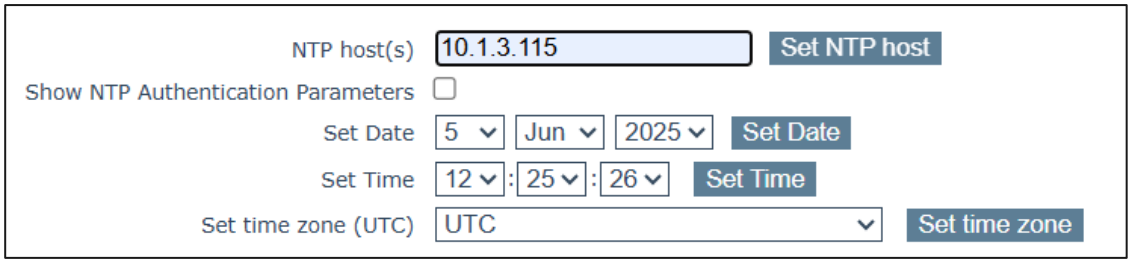
6.9. SETTING DATE/TIME

The current system date and time, maintained using the underlying hardware clock, is displayed. This timestamp is applied to all audit records and is used to track the inactivity of administrative sessions.

The date and time of LoadMaster can be configured in two ways:

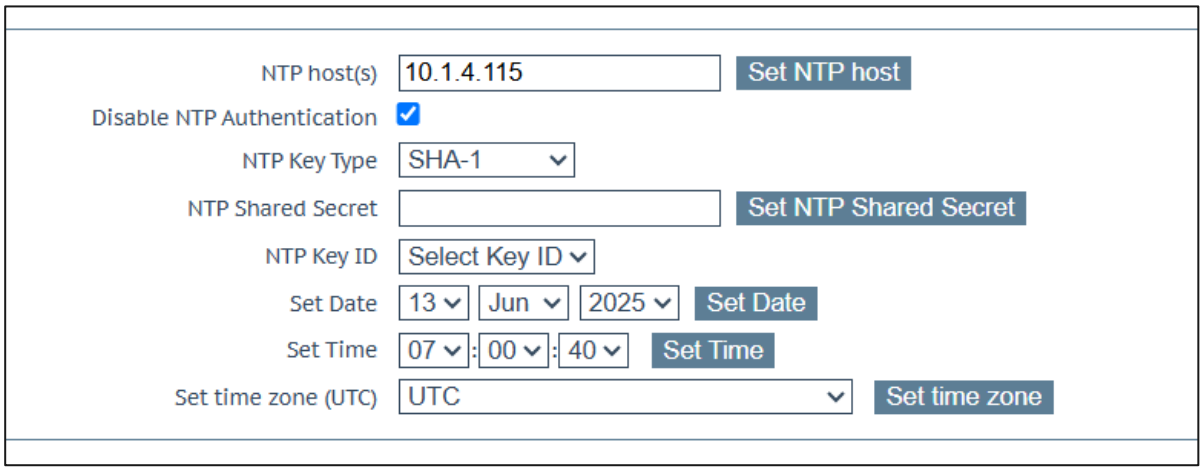
- **Automatic Synchronization via NTP**. for further details and configuration refer section 6.10.
- **Manual Configuration**: A Security Administrator can directly modify the date and time fields to set the correct system time.

1. In the left frame menu, click **System Configuration > System Administration > Date/Time:**
   - Set Date: Set the date on the LoadMaster.
   - Set Time: Set the time on the LoadMaster.
   - Set time zone: Set the time zone where the LoadMaster is located.



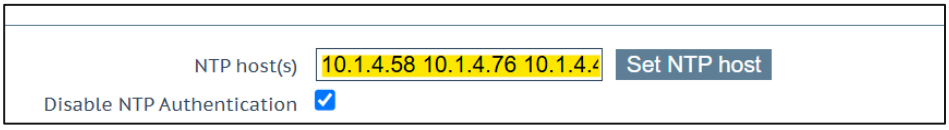
6.10. CONFIGURING NTP SERVER

You can manually configure the date and time of LoadMaster or leverage an NTP server. It supports time updates using NTPv4 only. The LoadMaster authentications updates using an administrator configured symmetric key and SHA-1. By default, the TOE rejects broadcast and multicast time updates. The TOE allows up to 10 NTP time sources to be configured.



In the left frame menu, click **System Configuration > System Administration > Date/Time:**

a. **NTP host(s)**: Specify the IP address of the NTP server to be used. You may configure multiple NTP servers by entering a space-separated list of hosts.



b. **Show NTP Authentication Parameters**: Enable the Show NTP Authentication Parameters check box to display the parameters that are needed to support NTP authenticated requests. Disable the Show NTP Authentication Parameters checkbox to hide.

c. **NTP Key Type**: Select **SHA-1** from the drop-down menu for the NTP key type to ensure the integrity and authenticity of the timestamp data exchanged between the TOE and the NTP server.

d. **NTP Shared Secret**: The NTP shared secret string. The NTP secret can be a maximum of 20 ASCII characters long or 40 hexadecimal characters long.

e. **NTP Key ID**: Select the NTP key ID. The values range from 1 to 99. Different key IDs can be used for different servers.

f. **Set Date**: Set the date on the LoadMaster.

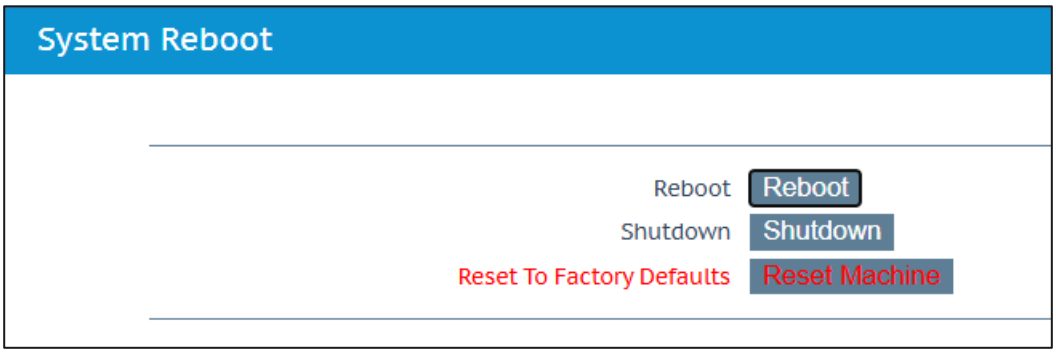
g. **Set Time**: Set the time on the LoadMaster.

h. **Set time zone**: Set the time zone where the LoadMaster is located.

6.11. SYSTEM REBOOT

The Progress LoadMaster appliance can be restarted from the Web Management interface. To restart the LoadMaster:

1. In the left frame menu, click **System Configuration > System Administration > System reboot > Reboot**

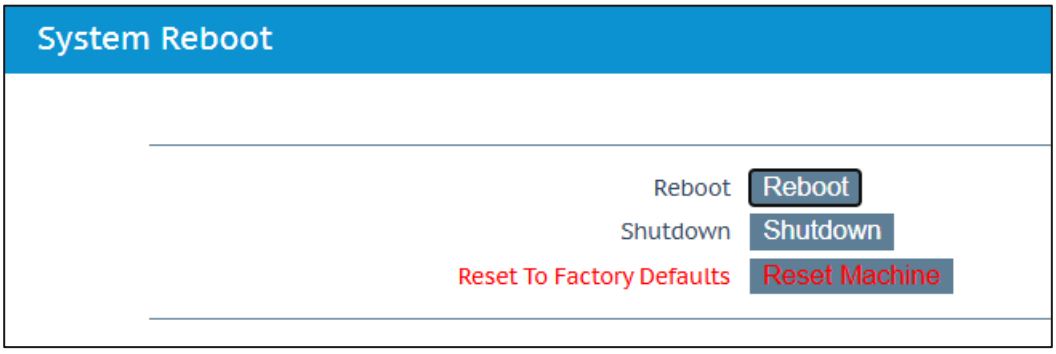


The LoadMaster takes approximately 60 seconds to restart. During the restart time, all interfaces are down.

6.12. SYSTEM SHUTDOWN

To shut down the system:

1. In the left frame menu, click **System Configuration > System Administration > System reboot > Shutdown**



Clicking this button attempts to power down the LoadMaster. If, for some reason, the power down fails, it will at a minimum halt the CPU.

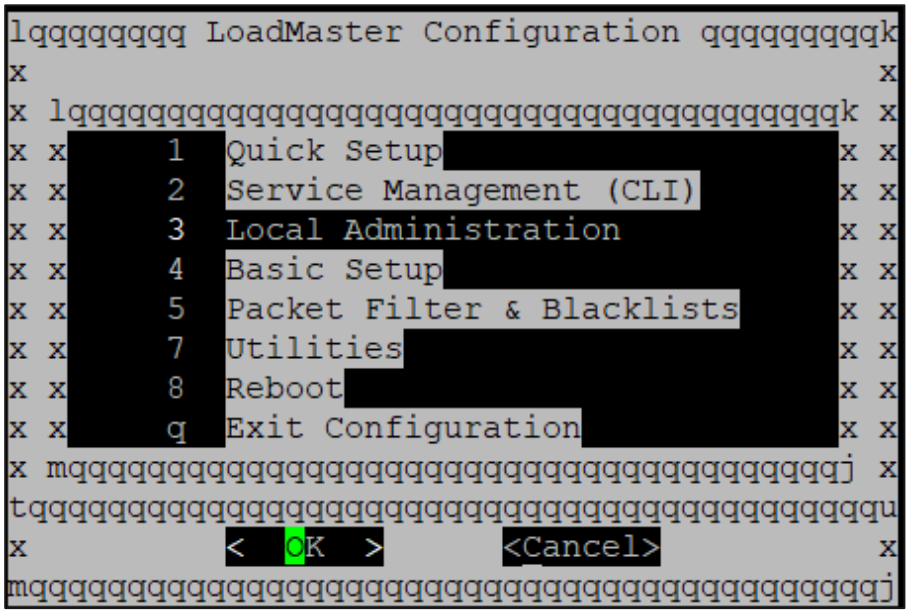
6.13. START/STOP WEBUI ACCESS

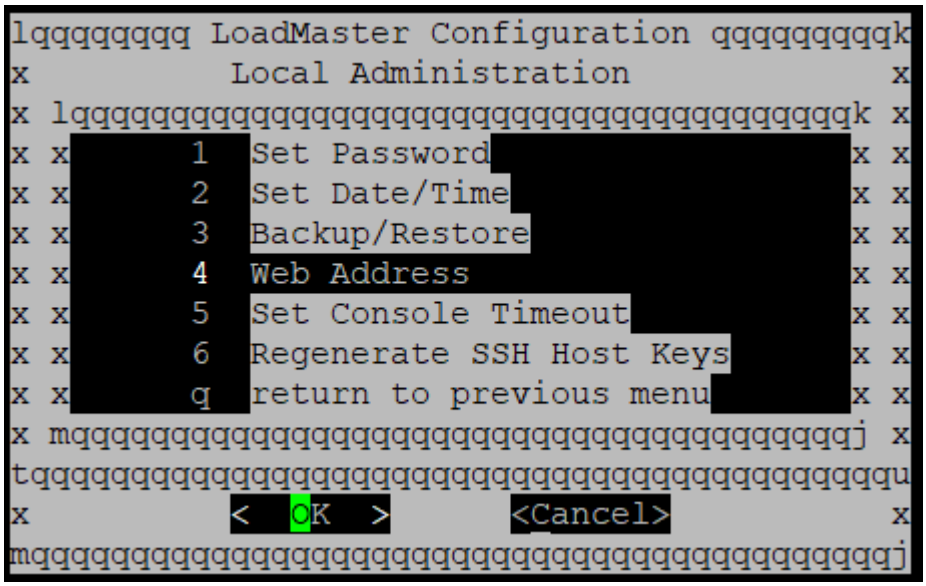
The TOE allows the security administrator to control access to the Web User Interface (WUI) either directly from the local console or partially through the WUI itself.

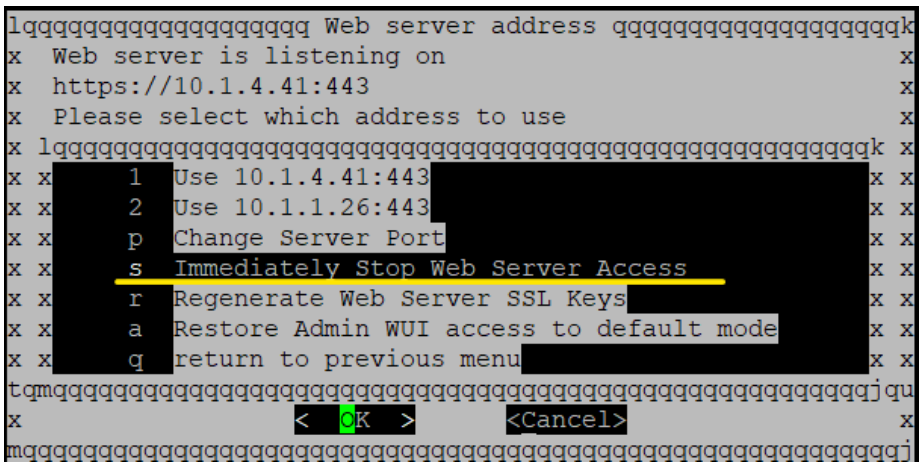
To perform this action via local console:

1. Access the TOE via **local console**.
2. Navigate to **Local Administration > Web Address > Immediately Stop/Start Web Server Access**.
3. Use this option to:
    - **Stop**: Immediately disable access to the WUI, blocking all remote browser-based administrative access.
    - **Start**: Re-enable access to the WUI over TLS, allowing remote administration.

The screenshot below shows the exact location of this option within the local console interface.

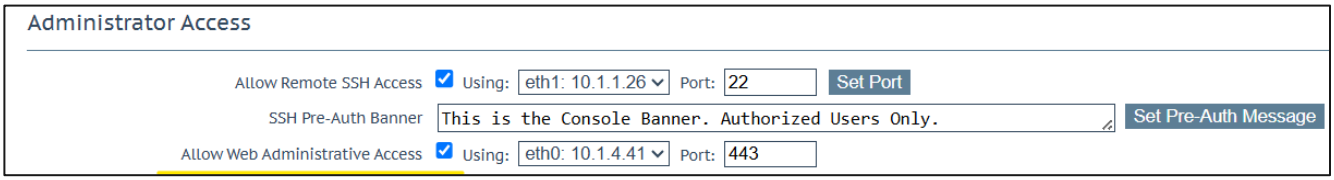






Alternatively, to disable WUI access via WUI:

1. Navigate to **Certificates & Security > Remote Access > Administrator Access**.
2. Uncheck the **Allow Web Administrative Access** checkbox.



Note: Through WUI, you can **only disable** WUI access. Once disabled, WUI access can **only be re-enabled via the local console** using the steps outlined above.

This functionality enables the administrator to manage the availability of the WUI as needed for security or maintenance purposes.

6.14. CONFIGURING SYSLOG SERVER

The configuration of a remote syslog server is described in the section 6.39. The administrator can configure the syslog host, port, severity level, protocol (TLS), and enable server certificate validation as required for secure log transmission.

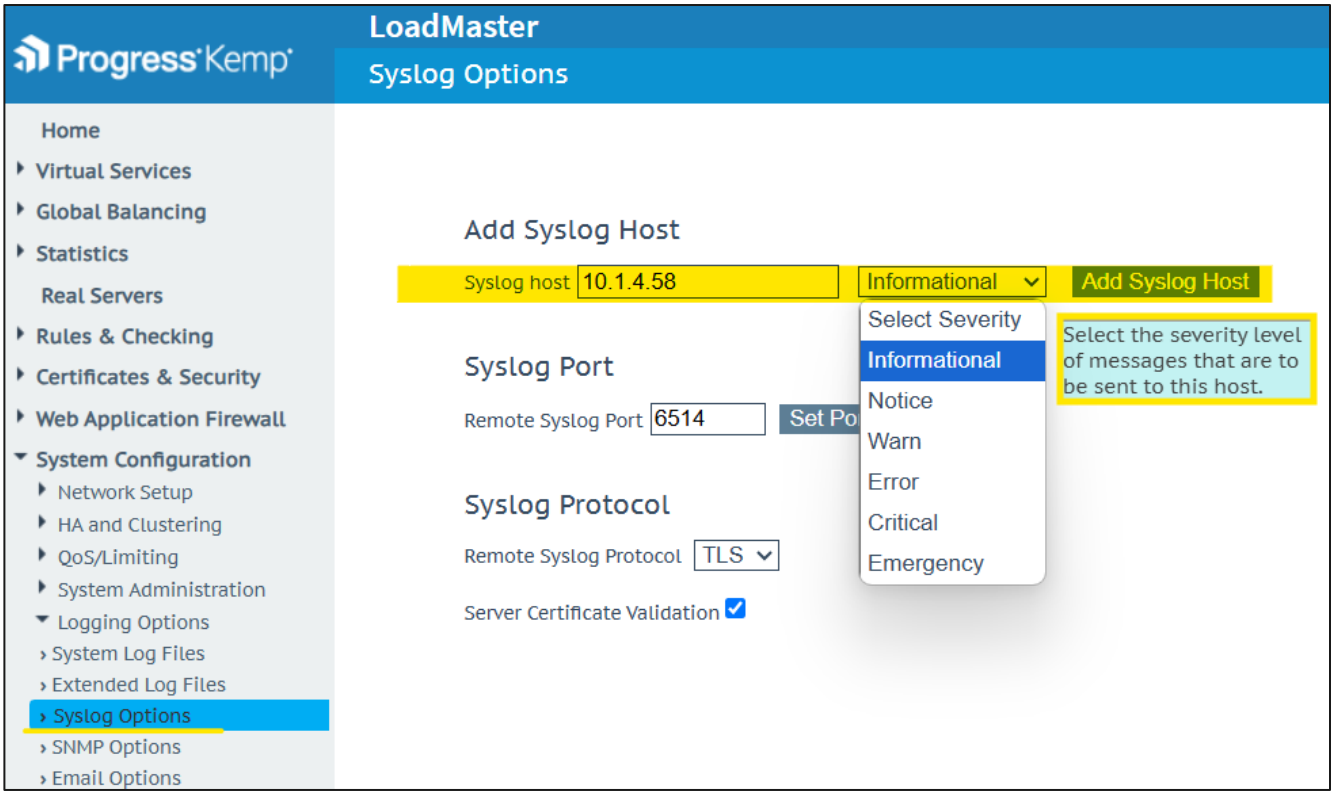
6.15. MANAGING SYSLOG SERVICE

Administrators can start or stop the syslog service from the Web User Interface (WUI) by configuring the syslog level setting.

6.14.1 STARTING THE SYSLOG SERVICE

To start or enable the syslog service:

1. Navigate to:
   System Administration > Logging Options > Syslog Options
2. Under the **Syslog Hosts** section, locate the **Syslog Level** dropdown menu.
3. From the dropdown, select **any level except None** (e.g., Alert, Critical, Error, etc.).

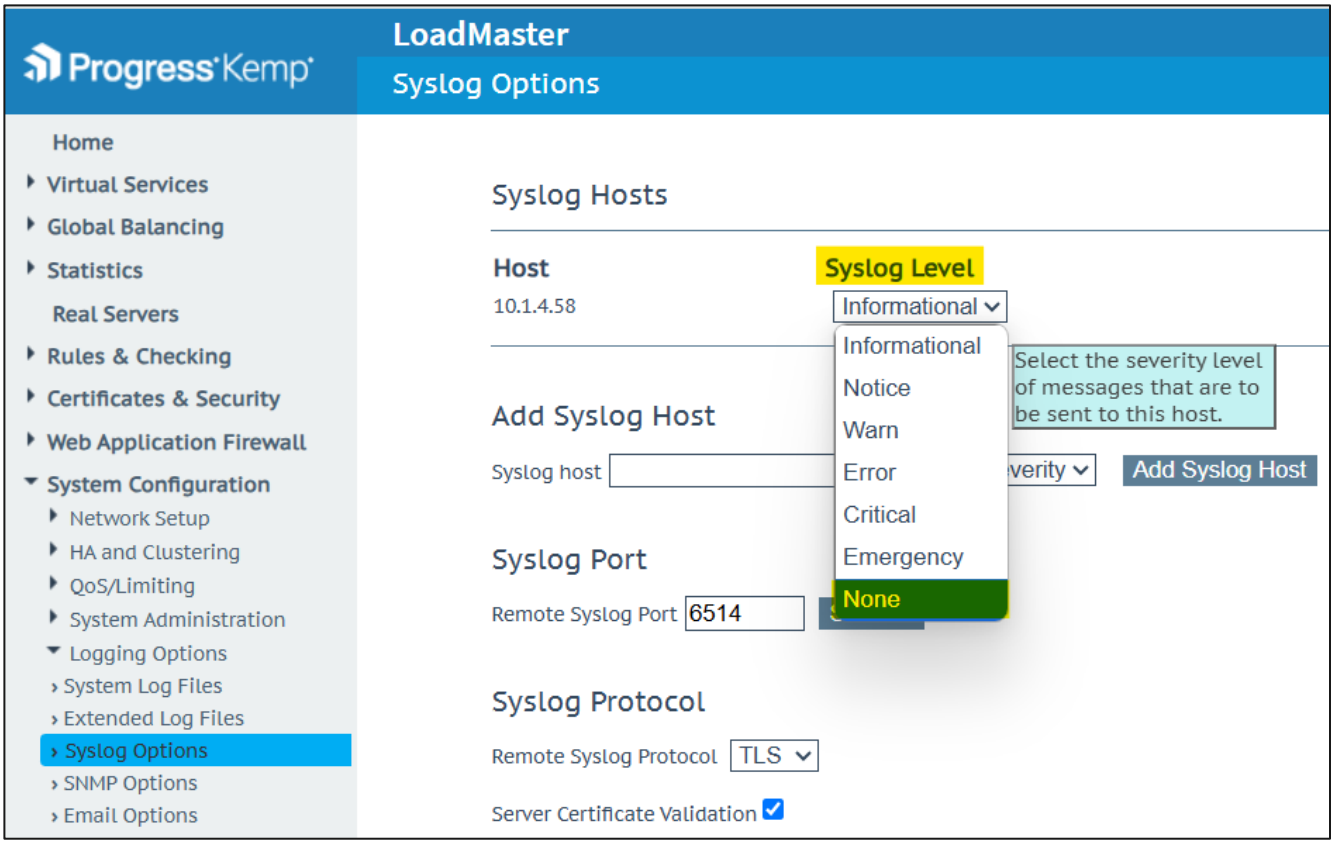


Selecting any valid syslog level will start the syslog service and enable log forwarding to the configured syslog hosts.

6.14.2 STOPPING THE SYSLOG SERVICE

To stop or disable the syslog service:

1. Navigate to:
   System Administration > Logging Options > Syslog Options
2. Under the **Syslog Hosts** section, locate the **Syslog Level** dropdown menu.
3. From the dropdown, select **None**.

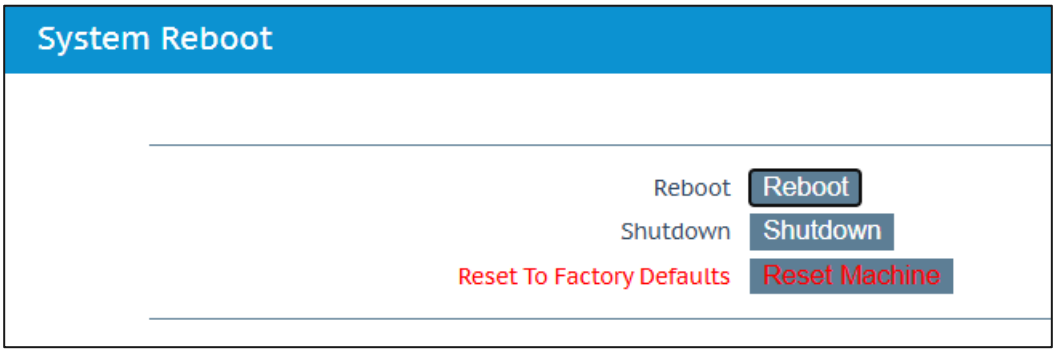


This will stop the syslog service and prevent the TOE from sending logs to the configured syslog servers.

6.16. RESET MACHINE

To reset the system to factory defaults:

1. In the left frame menu, click **System Configuration > System Administration > System reboot > Reset Machine**



Reset the configuration of the appliance with the exception of the license and username and password information. This only applies to the active appliance in a HA pair.

6.17. START-UP AND SELF-TEST

The TSF runs a suite of the following self-tests [during initial start-up (on power on)] to demonstrate the correct operation of the TSF:

- File systems checks (performed during initial start-up)

  During boot up the TSF checks file system by verifying the metadata and that it is mounted correctly.

- SHA-256 Software integrity checks (performed during initial start-up)

  The TSF generates a SHA-256 has of the firmware image and compares it with the stored value.

- Cryptographic algorithm known answer tests (performed prior to providing any cryptographic service)

  For each cryptographic algorithm, the TSF performs a sample cryptographic operation using know values and compares the output with the expected value.

- Cryptographic algorithm pairwise constancy test (performed prior to providing any cryptographic service)

  For each cryptographic algorithm with a key-pair, the TSF performs a sample operation using know value and compares the output with the corresponding key-pair.

- Health test of the noise source (performed continuously during runtime)

  This is a continuous health-test that checks the number of occurrences of 6 different bit patterns in each 256-bit output from the noise source. It checks if any of the pattern counts are outside of predetermined thresholds. If more than 128 of the most recent 256 256-bit samples fails, the Entropy Source ceases to output data.

Failure Handling:

If **any** of these tests fail:

- The affected functionality (e.g., cryptographic services) is disabled.
- If critical failures occur (e.g., in cryptographic algorithm KATs, consistency tests, or entropy source), the TSF **halts boot** or proceeds **with cryptographic services disabled**.

These self-tests ensure the TOE is operating securely and reliably, in such cases, the administrator may review the failure condition and proceed with rebooting the TOE.

Verification of Self-Test Failure:

If the **self-tests fail** during system startup, the following log message is generated:

“Crypto Self-Tests failed”

This indicates that the system has not passed the required cryptographic integrity checks and may not proceed with normal operation.

Verification of Self-Test Success:

Upon **successful completion of the self-tests**, the following log message is generated:

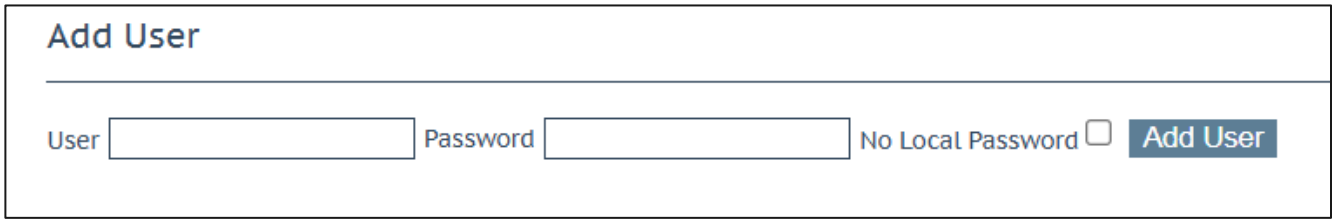
2026-02-17T13:26:12+00:00 lb100 logger: script Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: sha1 Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: sha160 Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: sha256 Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: sha384 Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: sha512 Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: hmacsha1 Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: hmacsha160 Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: hmacsha256 Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: hmacsha384 Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: hmacsha512 Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: aescbc128 Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: aescbc256 Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: aesecb128 Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: aesecb256 Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: rand Self-Test passed
2026-02-17T13:26:12+00:00 lb100 logger: RSA Sign and Verify Self-Test passed
2026-02-17T13:26:13+00:00 lb100 logger: EC Self-Test passed
2026-02-17T13:26:13+00:00 lb100 logger: Crypto Self-Tests passed

Administrators can check the system logs for these messages to confirm that the cryptographic self-tests and system initialization completed successfully during startup.

6.18. User Creation

For Local Users creation:

1. Navigate to **System Configuration (**in the left frame menu) **> System Administration > User Management > Add User**



2. Usernames can be a maximum of 64 characters long. Usernames can start with a digit and can contain alphanumeric characters, in addition to the following special characters: **=~^._+#@/-**
3. The minimum password length is defined by what is set in the Minimum password length field.

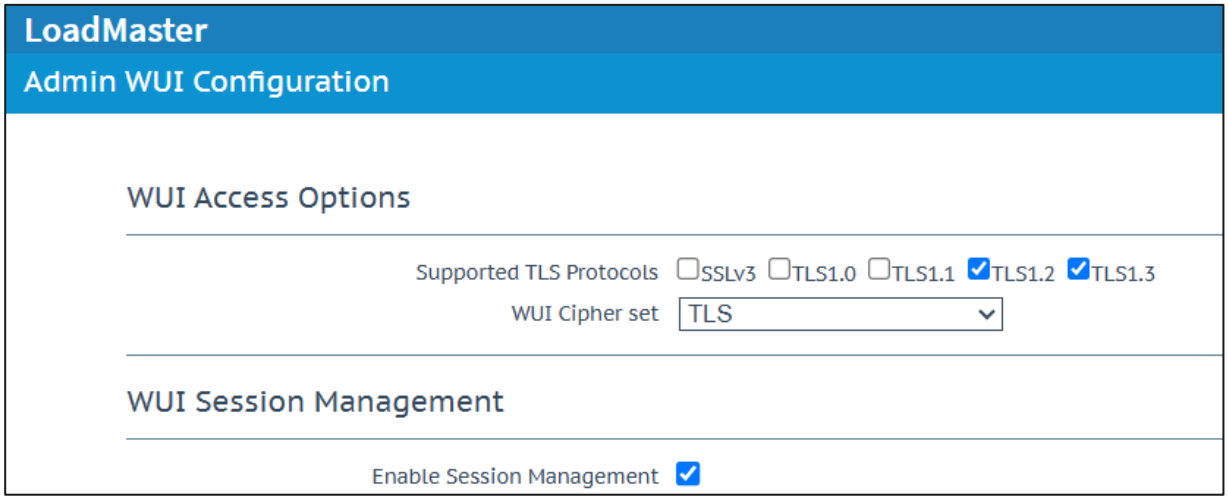
4. To modify or delete a Local User navigate to **System Configuration (**in the left frame menu) **> System Administration > User Management > Local User**

5. The **Local Users** section lists any existing local users. Two options are available for existing users:
   - **Modify:** Change details for an existing local user, such as their permissions and password. For further information, refer to the Modify User section.
   - **Delete**: Delete the relevant user.

6.19. ADMIN WUI ACCESS

Progress LoadMaster supports versions 1.0, 1.1, 1.2 and 1.3 of the Transport Layer Security (TLS) protocol.

In the evaluated configuration, the TLS1.2 must use.

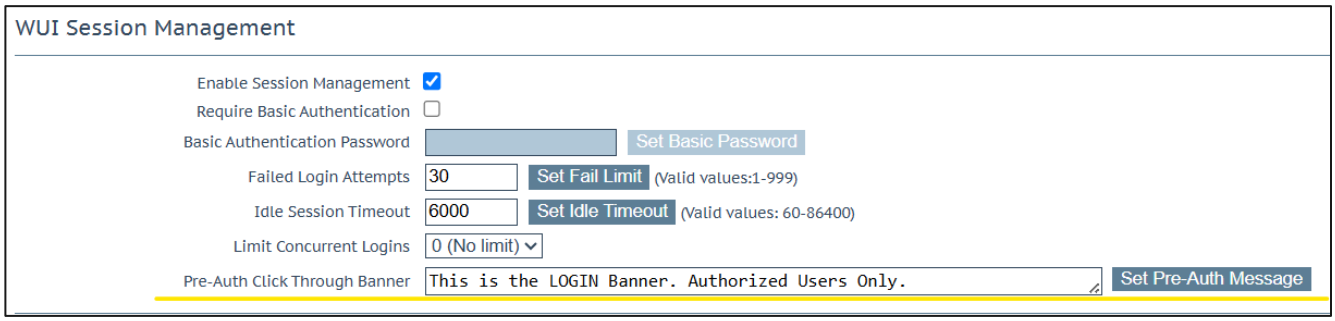


In the left frame menu, click **Certificates & Security > Admin WUI Access > Select TLS1.2**

6.20. SET THE WUI BANNER

The TSF displays a configurable pre-authentication banner before establishing Remote (HTTPS/WUI) administrative session.

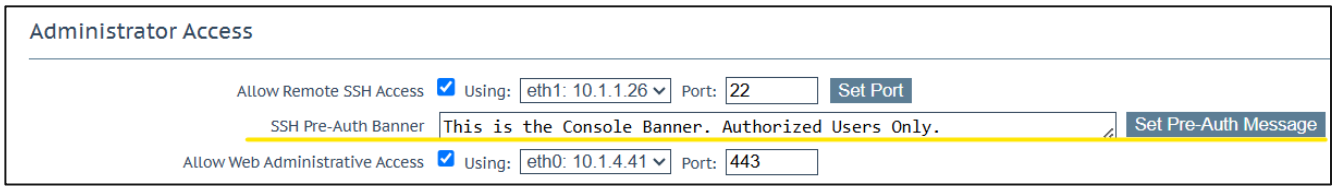
1. In the left frame menu, click **Certificates & Security > Admin WUI Access**
2. Type in a **Pre-Auth Click Through Banner** and click **Set Pre-Auth Message**



6.21. SET THE CLI BANNER

The TSF displays a configurable pre-authentication banner before establishing Local (Console/Serial) session.

1. In the left frame menu in WUI, click **Certificates & Security > Remote Access**.
2. Check the **Allow Remote SSH Access box**, type in an **SSH Pre-Auth Banner** and click **Set Pre-Auth Message**. This banner is also used for the CLI (even if SSH is disabled).



Note: To ensure the **SSH Pre-Auth Banner** applies only **to console access** and to effectively **disable remote SSH** access, set the "**Using**" option to the console interface IP instead of "All Networks," and configure the port as needed. This restricts SSH access to the specified interface, preventing remote access via other network interfaces.

6.22. INTERMEDIATE CERTIFICATE

The **Intermediate Certificates** field allows you to assign intermediate and root certificates. If you already have a certificate, or you have received one from a CSR, you can install the certificate by clicking the **Choose File** button. Navigate to and select the certificate and then enter the desired **Certificate Name**. The name can only contain alpha characters with a maximum of 32 characters.

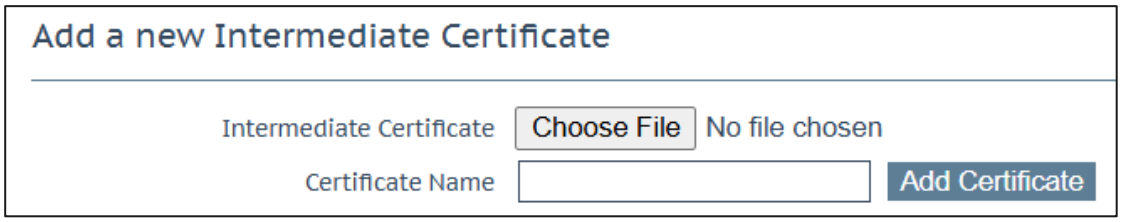
Uploading several consecutive intermediate certificates within a single piece of text, as practiced by some certificate vendors such as GoDaddy, is allowed. The uploaded file is split into the individual certificates.

You can also delete the certificates by clicking the '**Delete'** button shown in the first screenshot of this section.

If a connection is not possible because the validity of a certificate cannot be determined, there is no override option. A valid certificate must be presented. This may include installing required certificates in the trust store, i.e. uploading the certificates in the **Intermediate Certificate** field.

To upload **Root** and **Intermediate CA** Certificates, before enabling certificate-based admin WUI access:

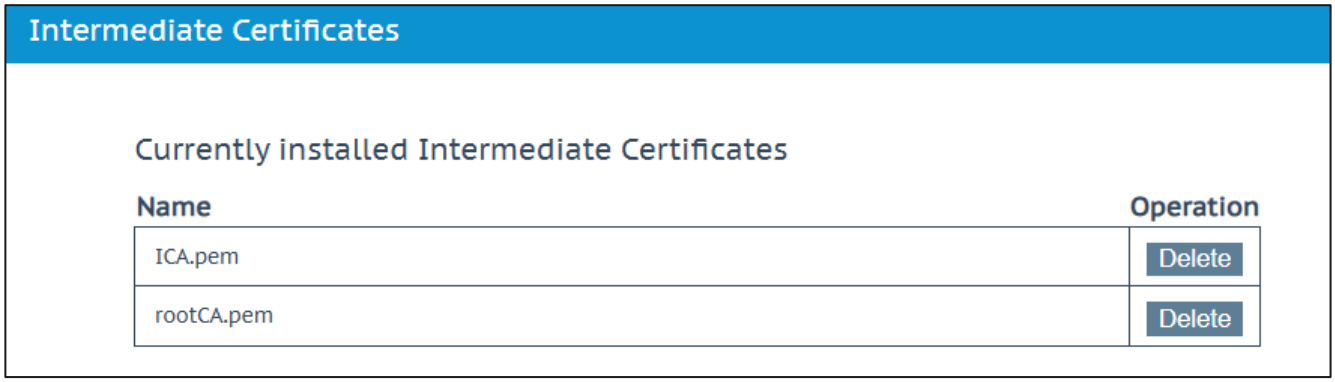
1. Navigate to **Certificates & Security → Intermediate Certificates.**
2. Upload the issuing CA and Root CA certificates required to validate administrator certificates for client authentication.



Note: Ensure that the server certificate is an X.509 certificate with an ECDSA public key using the secp256r1 (P-256) curve, as required by the evaluated configuration.

TSF allows the security administrator to generate cryptographic keys associated with TSF's self-signed web server certificate or Certificate Signing Requests.

The same screen as shown below displays the list of installed certificates along with their assigned names.



6.23. GENERATE CSR (CERTIFICATE SIGNING REQUEST)

The TOE is capable of generating a Certificate Signing Request (CSR) that includes the public key along with device-specific information such as email address, requested Subject Alternative Name (SAN), Common Name (CN), Organization (O), Organizational Unit (OU), and Country (C). The following instructions explain how to establish these fields before creating the CSR.

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

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

The following are the instructions for establishing the above fields in the CSR:

- **Letter Country Code (ex. US)**

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

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

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

- **City**

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

- **Company (Organization)**

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

- **Organization Unit (e.g., Marketing, Finance, Sales)**

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

- **Common Name**

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

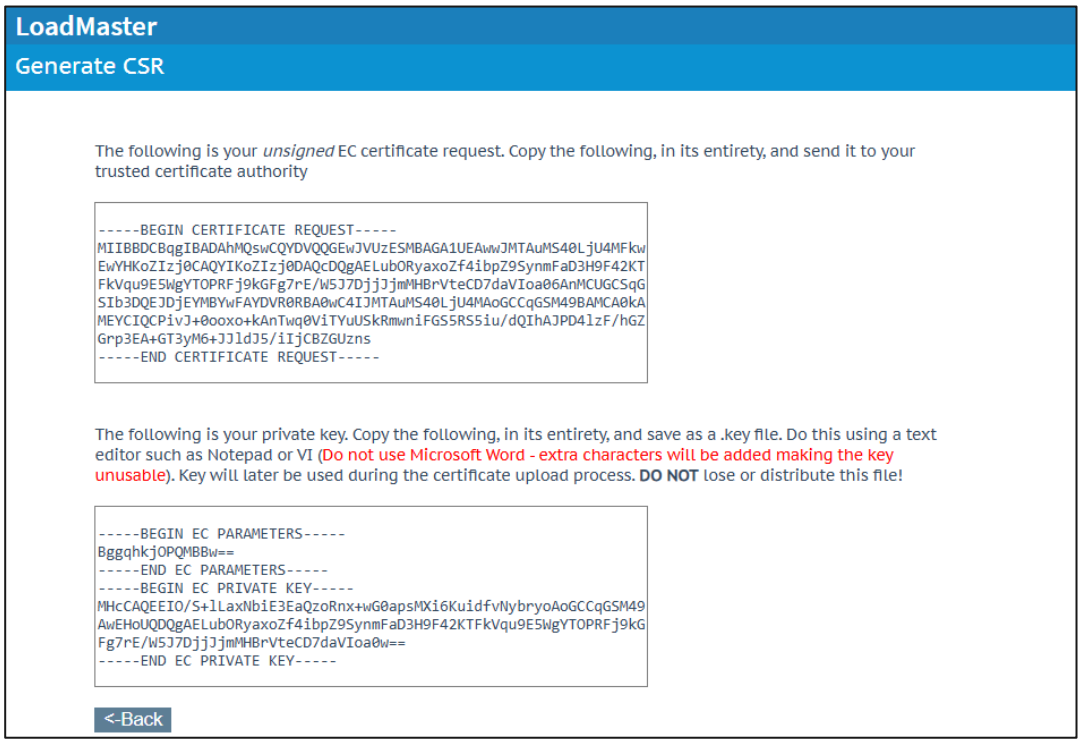
- **Email Address**

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

- **SAN/UCC Names**

A space-separated list of alternate names.

2. Fill in the details in the resulting screen. The **Common Name** field is mandatory, all other fields are optional.
3. Click **Create CSR**.
4. Alter clicking the **Create CSR** button, the following screen appears:

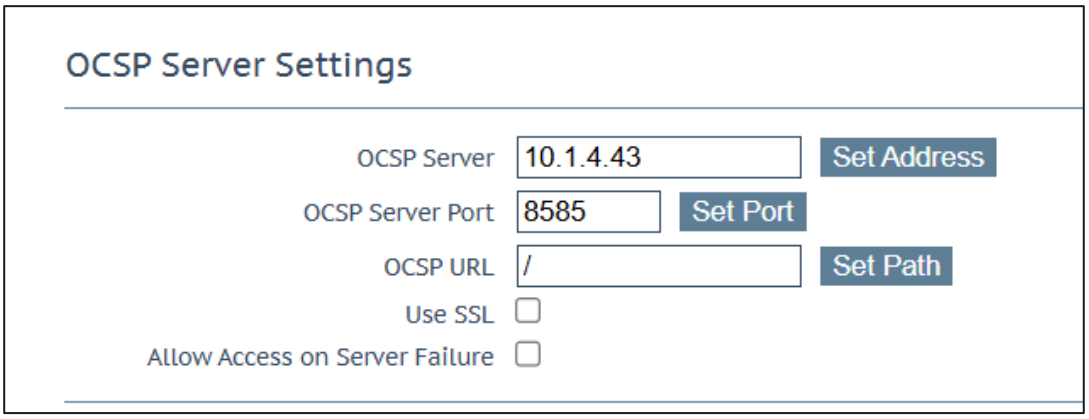


5. The top part of the screen should be copied and pasted into a plain text file and sent to the Certificate Authority of your choice. They will validate the information and return a validated certificate.
6. The lower part of the screen is your private key and should be kept in a safe place. This key should not be disseminated as you will need it to use the certificate. Copy and paste the private key into a plain text file (do not use an application such as Microsoft Word) and keep the file safe.
7. The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

6.24. Enable OCSP Checking

In the left frame menu, click **Certificates & Security > OCSP Configuration**:

1. Enter the **OCSP Server** IP address and click **Set Address**.
2. Enter the **OCSP Server Port** and click **Set Port**.
3. Enter the **OCSP URL** and click **Set URL**.
4. Enable the **Enable OCSP Checking** check box.



5. If the certificate cannot be validated because the server is unavailable, there is an option called **Allow Access on Server Failure** where you can decide if you want to pass the authentication or not. Enabling this check box treats an OCSP server connection failure or timeout as if the OCSP server has returned a valid response. That is, the client certificate is treated as valid.

Note: The AIA is given precedence and will be used based on its presence. If the AIA is not present or appears invalid, the **OCSP Server** configuration details will be used.

Please note the following:

- LDAPS: AIA information from the server certificate is honoured if **Certificates & Security > OCSP Configuration > OCSP Checking** is enabled.
- Syslog-NG: AIA information from the server certificate is honoured if **Certificates & Security > OCSP Configuration > OCSP Checking** is enabled.
- WUI Authentication: AIA information from the client certificate is honoured if the "Client certificate required (verify via OCSP)" is configured under **Certificates & Security > Remote Access > Administrator Access > Admin Login Method.**

The TOE treats a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE. Certificates that do not contain this extension or have the CA flag set to FALSE are not treated as CA certificates and will not be accepted for certificate chaining.

As a TLS Client, the TOE performs revocation checking using the Online Certificate Status Protocol (OCSP) to determine the revocation status of peer certificates.

If the TOE does not receive an OCSP response (e.g., due to a timeout or connectivity issue), it rejects the certificate by default. However, the Security Administrator can configure the TOE to accept the certificate when no OCSP response is received, effectively allowing revocation checking to be bypassed in such cases.

6.25. SAN EXTENSIONS

- The TOE supports the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN, IPv4 address in SAN.
- The TOE only checks the identifier in the CN if the SAN extension is not present. The TSF does not support SRV or URI identifiers.

- The TSF then parses the SAN (when present) or Common Name from the certificate. The TSF the matches the identifier against a list of defined users or by sending the identifier to an LDAP server.
- The TOE **does not permit out-of-band provisioning of pre-shared keys (PSKs)**.

6.26. REFERENCE IDENTIFIERS

- The reference identifier for external IT entities is configured by the administrator using the available administrative commands in the CLI. The reference identifiers must be an IPv4 address, or a hostname.
- When the reference identifier is a hostname, the TOE compares the hostname against all the DNS Name entries in the Subject Alternative Name (SAN) extension. If the hostname does not match any of the DNS Name entries, then the verification fails. If the certificate does not contain any DNS Name entries in SAN, the TOE will compare the hostname against the Common Name (CN). If the hostname does not match the CN, then the verification fails. For both DNS Name and CN matching, the hostname must be an exact match or wildcard match. In the case of a wildcard match, the wildcard must be the left-most component, wildcard matches a single component, and there are at least two non-wildcard components.
- When the reference identifier is an IP address, the TOE converts the IP address to a binary representation in network byte order. IPv4 addresses are converted directly from decimal to binary with period "." serving as the delineator. The TOE compares the binary IP address against all the IP Address entries in the Subject Alternative Name extension. If there is not an exact binary match, then the verification fails. If the SAN entry is missing, the TOE will compare the IPv4 address against the Common Name (CN). If the IPv4 address in CN is not an exact binary match, then the verification fails. For IPv4 address in SAN or CN matching, the IPv4 address must be an exact binary match.

  Note: SAN is prioritized over CN.

  Warning: The above-mentioned reference identifier matching rules should be taken into consideration while connecting to peers or IT entities using certificates that have DNS names or IP Addresses.

  Note: Usage of IP addresses as reference identifiers is discouraged due to their potential unreliability. As stated in RFC 6125, factors such as host mobility, NATs, and shared IPs can make IP addresses unsuitable for secure identity verification.
- The TLS channel is terminated if verification fails.
- The TOE does not enforce canonical format.

6.27. X509 CERTIFICATE

The TOE performs **X.509 certificate validation** at the following points:

- TOE TLS client authentication of server X.509 certificates;
- When certificates are loaded into the TOE, such as when importing CAs and certificate responses.

The TOE performs **certificate validation** according to the following rules:

- Certificates must not be expired. An expired certificate (where the notAfter date is in the past) is considered invalid.
- The certificate chain must end with a trusted CA (trust anchor) that is configured on the TOE.

- All non-trust-anchor certificates are validated for revocation status using OCSP (Online Certificate Status Protocol).
- All CA certificates (trust anchors and intermediates) must include the basicConstraints extension with the CA flag set to TRUE.
- TLS server certificates must include the serverAuthentication purpose in their extendedKeyUsage field.
- TLS client certificates must include the clientAuthentication purpose.
- Certificates used to sign OCSP responses must include the OCSP Signing purpose.

The TOE performs X.509v3 certificate validation for all TLS connections.

If certificate verification fails for any reason, the connection attempt fails, and the trusted channel is not established.

There are no fallback authentication mechanisms for failed certificate authentication.

The TOE provides a **trust store** to manage and store X.509v3 certificates used for authentication and trusted connections.

Only users with **Security Administrator** privileges (e.g., the bal account or users with "All Permissions") can:

- **Import certificates** into the trust store.
- **Delete certificates** from the trust store.

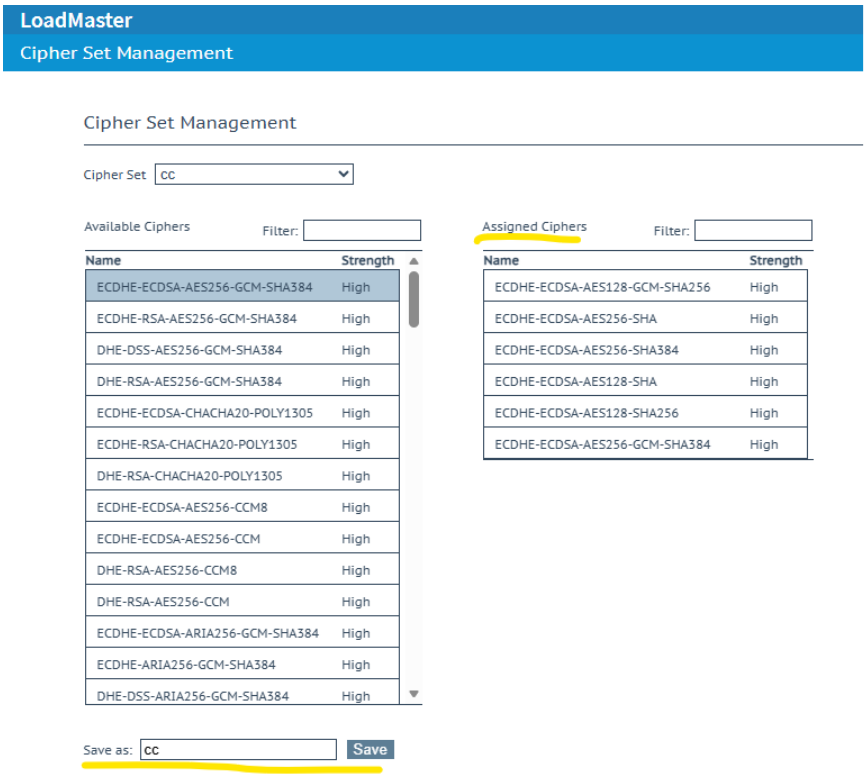
Note: Once uploaded, the TOE automatically treats the CA certificate as trust anchor—no further configuration is required.

6.28. TLS Cipher Suites and Role

6.28.1. Enabling and Configuring TLS Cipher Suites for Secure Communication

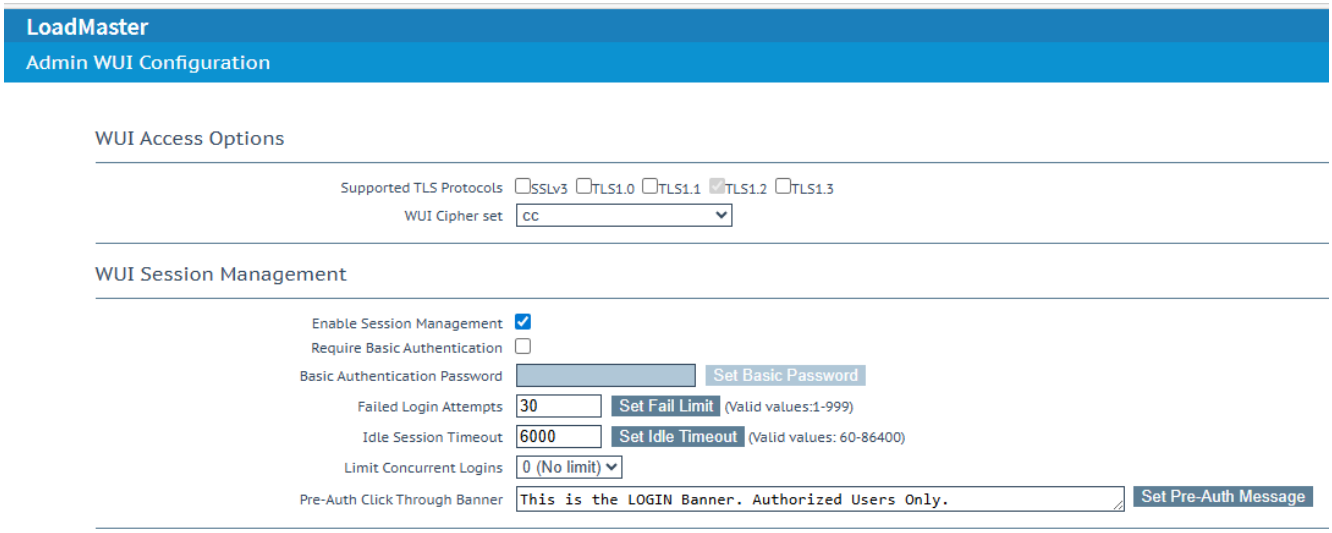
To configure the TLS cipher suites used by the TOE to secure WUI access, perform the following steps:

1. Navigate to **Certificates & Security → Cipher Sets**.
2. From the Cipher Set Management page:
    a. Select a Cipher Set (e.g., Default, TLS, or a custom ECC set).
    b. In the Available Ciphers list, select required cipher suites.
    c. Use the right arrow to assign selected ciphers to the Assigned Ciphers list.
    d. Click Save to store the changes.

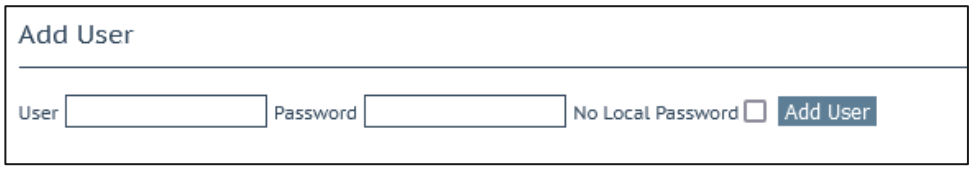


3. Apply Cipher Set to WUI Access
    a. Go to **Certificates & Security → Admin WUI Access**:
        - Under **WUI Access Options**, select supported TLS versions (TLS 1.2).
        - In the **WUI Cipher Set** dropdown, select the configured Cipher Set.
        - Configure a **Pre-Auth Click Through Banner**, required for certificate-based authentication.

Note: The configured cipher set is applied both for TLS server functionality (WUI access) and TLS client functionality (e.g., Syslog/LDAP).



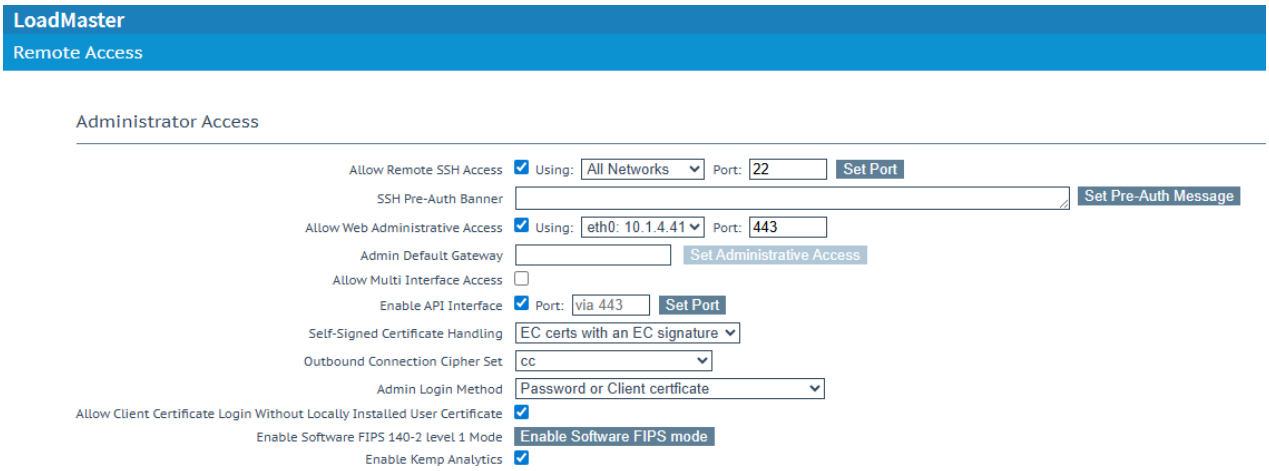
4. Configure Client Certificate-Based Authentication
    a. Go to **System Configuration → System Administration → User Management**:
        - Create a user with a name that exactly matches the certificate's Principal Name.
        - Do not set a password; select the "no password" option.
        - Assign appropriate privileges (e.g., “All Rights” for the first certificate user).



    b. Go to **Certificates & Security → Remote Access**:
        - Set the **Admin Login** field to “Password or Client Certificate”.
        - In the **Outbound Connection Cipher Set** dropdown, select the configured Cipher Set.

If login fails after configuration, try:

- Clearing cookies and restarting the browser.
- Bypassing certificate request and logging in using the default bal account.



6.28.2. TLS SERVER (WUI ACCESS)

The TOE acts as a TLS server to provide secure administrator access via the Web UI. It supports TLSv1.2 only.

The following cipher suites are supported for TLS server connections:

Cipher Suites:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (RFC 8422)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (RFC 8422)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (RFC 5289)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (RFC 5289)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (RFC 5289)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (RFC 5289)

Connections using TLS versions except 1.2 (e.g., TLS 1.1, TLS 1.3 or SSL) are rejected.

Note: Configuration steps for all supported algorithms (e.g., ECDSA certificate, TLS versions, and cipher suites) are detailed in Section 6.28.1.

Support for ECDSA over a NIST secp256r1 for authenticating itself to TLS clients and establishing keys is available by default and no additional configuration is required.

Elliptic Curve Support

- By default, TOE supports ECDHE curves: secp256r1, secp384r1, secp521r1.
- Connections proposing unsupported curves will fail.

Session Management

- Session resumption and session tickets are **not supported**.

The TOE's TLS implementation does **not support or negotiate the TLS early data extension.**

No configuration is required by the administrator to enable **reject all renegotiation attempts** behavior, as the TSF enforces the rejection of renegotiation attempts by default.

The TOE does not support the out-of-band provisioning of PSKs.

6.28.3. TLS CLIENT (OUTBOUND CONNECTIONS TO SYSLOG/LDAP)

TOE also acts as a TLS client for establishing outbound secure connections to trusted IT entities (e.g., Syslog or LDAP servers). These connections use the same configured cipher set as the server role.

Supported Protocols and Cipher Suites

Cipher Suites:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (RFC 8422)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (RFC 8422)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (RFC 5289)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (RFC 5289)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (RFC 5289)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (RFC 5289)

The TOE **does not support** other versions of TLS except TLS v1.2 for outbound connections.

Server Certificate Validation

- Enforces **strict certificate verification** using trusted root CA list.
- Verifies the **reference identifier** in the server certificate (e.g., Common Name or SAN).
- If validation fails, the connection is aborted.

Supported Groups Extension
By default, the TOE supports the following supported_groups extension:

- secp256r1
- secp384r1
- secp521r1

No other curves/groups are included in the extension.

TLS Signature Algorithms (ClientHello)

By default, the TOE supports the signature_algorithms extension with:

- ecdsa_secp256r1 with sha256
- ecdsa_secp384r1 with sha384
- ecdsa_secp521r1 with sha512

No other signature algorithms are offered by the TOE.

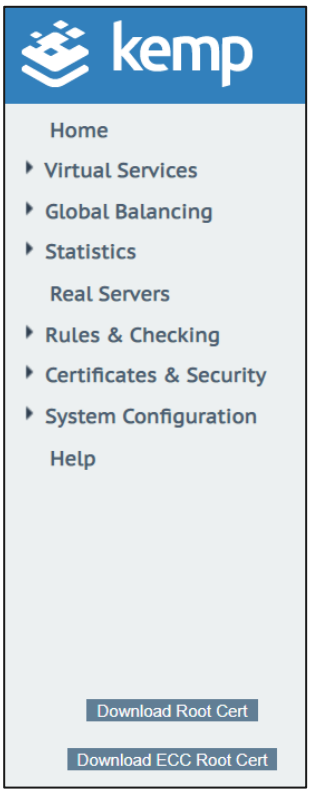
Also, Pre-Shared Keys (PSKs) out-of-band provisioning is not used.

6.28.4. SELF-SIGNED CERTIFICATE HANDLING (WUI)

To use ECC self-signed certificates for the WUI:

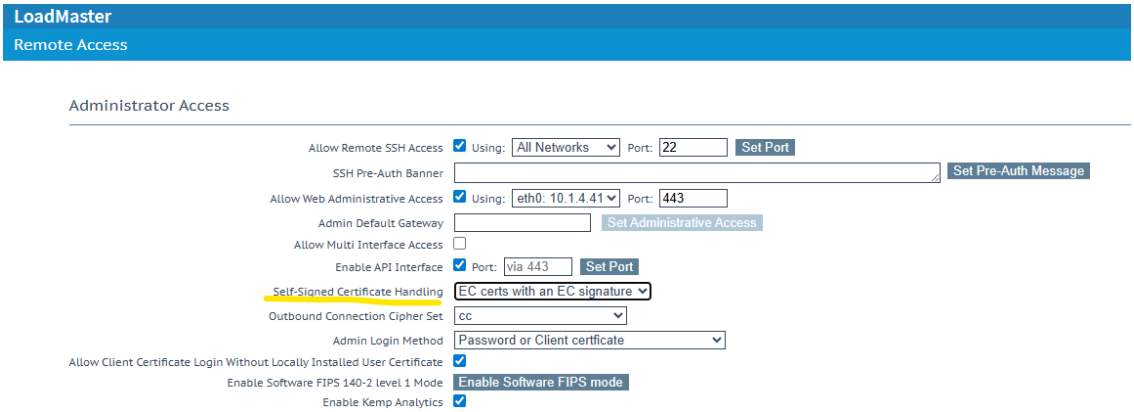
- Navigate to **Certificates & Security → Remote Access**.
- In **Self-Signed Certificate Handling**, choose:

- **EC Certs with RSA Signature** (generates a new ECC certificate with RSA sig).
  - Download and install the ECC Issuing CA certificate on the admin workstation.



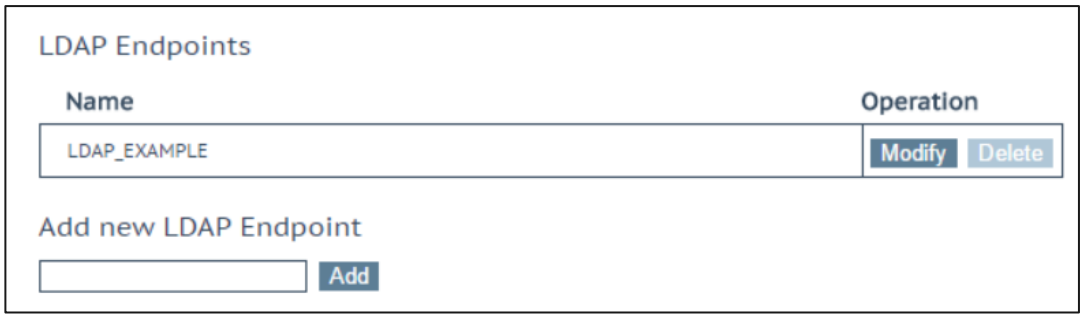
- **EC Certs with EC Signature** (fully ECC certificate).
  - **Important:** Before selecting this, ensure the ECC Issuing CA certificate is already trusted in the admin workstation/browser.
  - Failing to do this will lock out WUI access, requiring **console access and a factory reset** (note: bal account remains unchanged post-reset).

Note: Ensure that the server certificate is an X.509 certificate with an ECDSA public key using the secp256r1 (P-256) curve, as required by the evaluated configuration.



6.29. Setup Admin WUI Access via LDAP

To set up an LDAP domain, click **Certificates & Security > LDAP Configuration**.

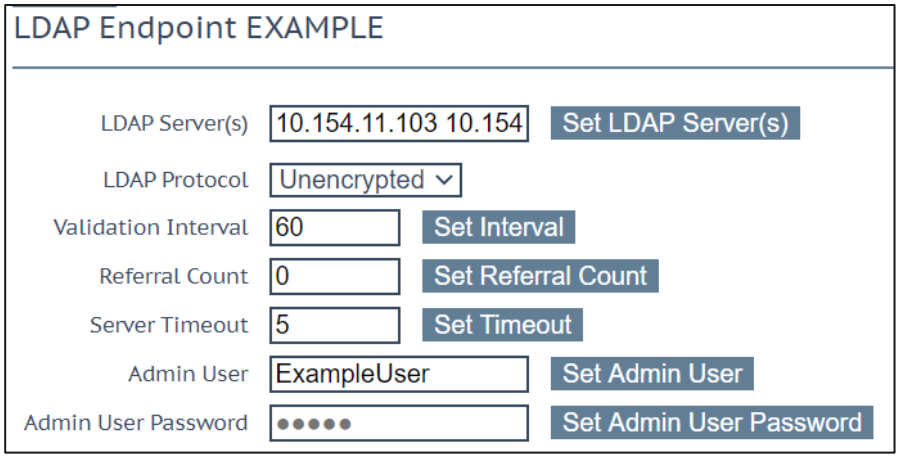


This screen provides a management interface for LDAP endpoints. These LDAP endpoints may be used in three different areas:

- Health checks
- SSO domains
- WUI authentication

Any existing **LDAP Endpoints** are listed here, with an option to **Modify** and **Delete**. If an LDAP endpoint is in use, it cannot be deleted.

There is also an option to add a new LDAP endpoint. Type a name for the endpoint and click **Add**. Spaces and special characters are not permitted in the LDAP endpoint name.



- **LDAP Server(s)**

  Specify a space-separated list of LDAP servers to be used. Port numbers can also be specified if required. If you have multiple domains and are using **Permitted Groups**, sometimes it is necessary to include the Global Catalog port number, otherwise the Permitted Groups will fail. The default port is **3628**. For example, **10.110.20.23:3268**.

  The LoadMaster uses OCSP to check the validity of the server certificates supplied by configured LDAPS servers. If these checks fail, connections to the server are not permitted.

- **LDAP Protocol**

  Select the transport protocol to use when communicating with the LDAP server.

  If you create an SSO domain with the **Authentication Protocol** set to **Certificates**, ensure to set the **LDAP Protocol** to **LDAPS** in the LDAP endpoint.

- **Validation Interval**

  Specify how often you should revalidate the user with the LDAP server.

- **Referral Count**

  The LoadMaster offers beta functionality to support LDAP referral replies from Active Directory Domain Controllers. If this is set to **0**, referral support is not enabled. Set this field to a value between **1** and **10** to enable referral chasing. The number specified will limit the number of hops (referrals chased).

- **Server Timeout**

  Specify the LDAP server timeout in seconds. The default value is **5**. Valid values range from **5** to **60**.

- **Admin User**

  Type the username of an administrator user.

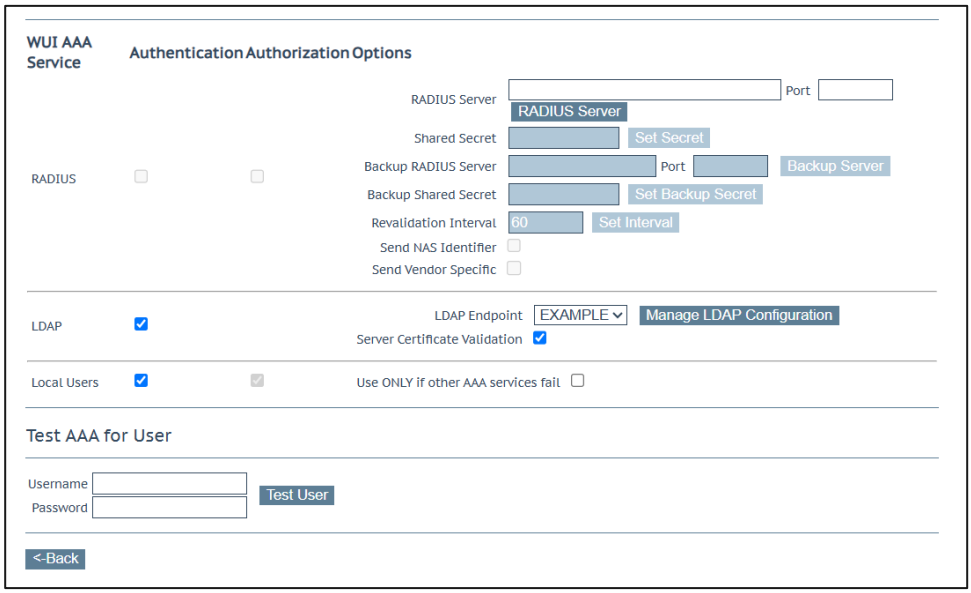
- **Admin User Password**

  Type the password for the specified administrator user.

To set up admin WUI (bal account) access via LDAP/AD:

a. In the left frame menu, click **Certificates & Security > Remote Access**.

b. In the page at right, click the **WUI Authorization Option** button.



c. Select the **LDAP** option.

d. Select the **LDAP Endpoint** that is created.

e. Add **Remote User Groups** if created.

f. Add the **Domain** and enable **Server Certificate Validation** option.

Note: LDAPS channel is restricted to TLSv1.2. If the TLS connection to the LDAP Server is unintentionally broken, the administrator should verify the connectivity to the LDAP server. Once connectivity is restored, the administrator must manually re-initiate the LDAP connection.

6.30. Disable CLI Virtual Service Administration

To disable CLI VS administration (to meet logging requirements):

1. In the left frame menu, click **System Configuration > Logging Options > System Logs** and then do the following:
2. In the page at right, click the **Debug Options** button.
3. Click **Disable CLI VS** Management. [Note that the button and label now read: Enable CLI VS Management.]

6.31. Keyed Hash Cryptographic Operation (Keyed Hash Algorithm)

The TOE supports keyed-hash message authentication in accordance with the HMAC algorithm using HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-384. The cryptographic key sizes are 160 bits, 256 bits, and 384 bits respectively, with corresponding output MAC lengths of 160, 256, and 384 bits, consistent with ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2.”

- The associated block sizes are as follows:
  - HMAC-SHA-1: 512-bit block size
  - HMAC-SHA-256: 512-bit block size
  - HMAC-SHA-384: 1024-bit block size

The TOE comes preconfigured for these algorithms, key sizes, block sizes, and MAC lengths. No additional configuration is required by the administrator.

6.32. Random Bit Generation

The TOE supports random bit generation services in accordance with ISO/IEC 18031:2011 using CTR_DRBG (AES-256).

The TOE comes preconfigured for these sizes and no additional configuration is required.

6.33. Use of Cryptographic Key Generation Schemes

No manual configuration by the administrator is required to select these schemes or key sizes.

- For HTTPS (administrative Web UI), the TSF generates **ECDSA P-256** keys.
- For TLS key establishment (ECDHE), the TSF supports **ECDH using P-256, P-384, and P-521** curves.

6.34. Hash Function

The TOE supports cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1, SHA-256, SHA-384, SHA-512 and message digest sizes 160, 256, 384, 512 bits that meet the following: ISO/IEC 10118-3:2004.

The TOE supports SHA-1, SHA-256, SHA-384, and SHA-512 hashing functions used in NTP, Digital Signature generation and verification, File integrity checking, Password hashing, and HMAC operations. The table below shows the hash algorithms used in the TOE and their specific usages:

Hash	Usage
SHA-1	Used for NTP message authentication, HMAC primitive, TLS hash function
SHA-256	Used for Digital Signature generation and verification, File integrity checking, HMAC primitive, TLS hash function
SHA-384	Supported for hashing functions, HMAC primitive, TLS hash function
SHA-512	Used for Password hashing

The TOE comes preconfigured for these sizes and no additional configuration is required.

6.35. DEFAULT CONFIGURATION

The following behaviours are enforced automatically without any additional configuration changes:

- The TOE supports AES encryption and decryption, in CBC and GCM modes using 128-bit and 256-bit keys during TLS communications and in CTR mode using 256-bit key during RNG functionality.
- The TOE supports digital signature generation and verification using:
    - **RSA Digital Signature Algorithm:**
      Supported schemes:
        - RSASSA-PSS (as specified in FIPS PUB 186-4, Section 5.5 and PKCS #1 v2.1)
        - RSASSA-PKCS1v1_5 (as specified in FIPS PUB 186-4, Section 5.5 and PKCS #1 v2.1)
        - ISO/IEC 9796-2 Digital Signature Scheme 2 and Scheme 3

      Supported key size:
        - **2048-bit modulus**
    - **Elliptic Curve Digital Signature Algorithm (ECDSA):**
      Supported schemes:
        - ECDSA with NIST curves P-256, P-384, and P-521 (as specified in FIPS PUB 186-4, Section 6 and Appendix D)
        - ISO/IEC 14888-3, Section 6.4-compliant ECDSA

      Supported key size:
        - **256-bit curve (P-256)**

All actions related to key management are done implicitly without the user's knowledge or involvement.

6.36. ZEROIZATION PROCESS

The TOE performs key destruction in accordance with the specifications in the Security Target. Keys stored in RAM are destroyed by overwriting them with zeroes.

Keys stored in non-volatile memory are destroyed by logically addressing the storage location, overwriting it with zeroes, and then deleting the file.

In the event of a power loss, key destruction may not complete for keys stored on disk. However, such keys are protected by restricted file system access.

- The TSF zeroizes the EC Diffie-Hellman session keys (P-256, P-384, or P-521) stored in RAM by overwriting them with zeros immediately after the TLS session is terminated.
- The TSF zeroizes the TLS Encryption Keys (AES-128 or AES-256) stored in RAM by overwriting them with zeros when the corresponding TLS session is closed.
- The TSF zeroizes the TLS Integrity Keys (HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384) stored in RAM by overwriting them with zeros after session termination.
- The TSF zeroizes the TLS Private Host Key (ECDSA P-256) stored in non-volatile memory by logically addressing the file system location and performing an overwrite with zeros. Once the overwrite is complete, the key file is deleted.
- The TSF zeroizes the User Passwords stored in non-volatile memory by performing an overwrite with zeros. Once the overwrite is complete, the key file is deleted.

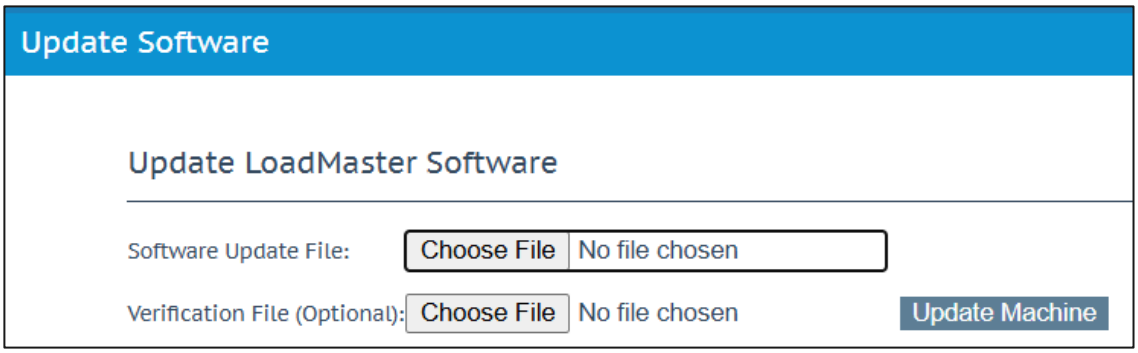
The only situation where the key destruction may be prevented would be if the TOE suffers a loss of power. This situation only impacts on the keys that are stored on the disk. Since the TOE is inaccessible in this situation, administrative zeroization cannot be performed. However, the keys on the disk are protected with restricted file system access.

6.37. Installing an Update Image

To install an update image on LoadMaster:

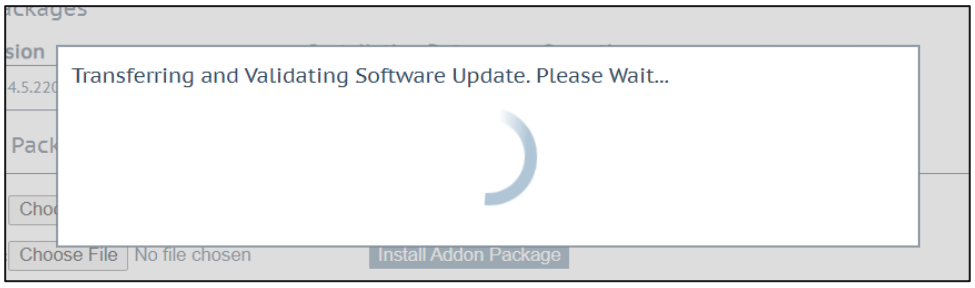
1. Unzip the archive received from Progress on a laptop or other device with a browser.
   - The archive contains the update image and an XML file.
2. Open the LoadMaster WUI and navigate to:

   System Configuration > System Administration > Update Software.

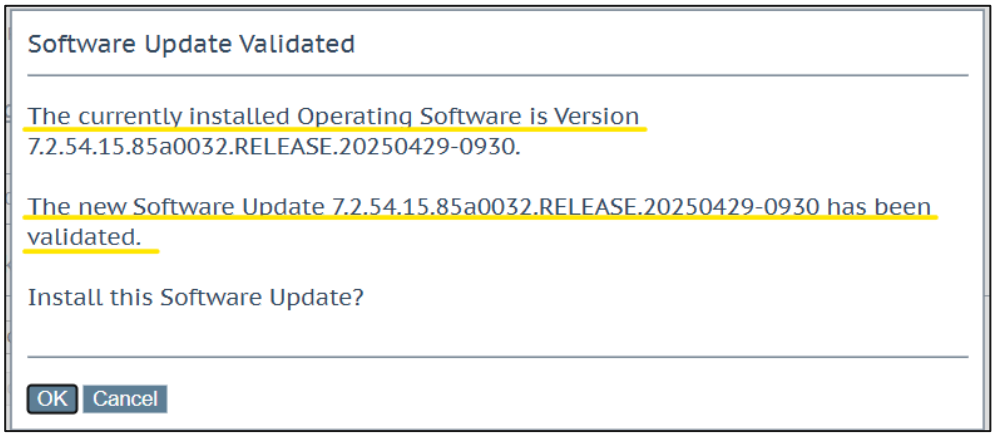


3. Click on the **Browse** button next to **Software Update File** and select the update image from Step 1.
4. Click on the **Browse** button next to **Verification File** and select the XML file from Step 1.
5. Click **Update Machine**.

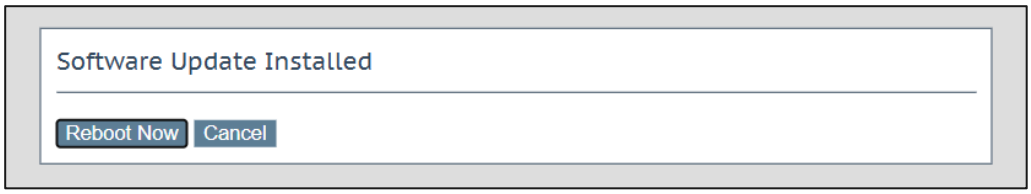
   A dialog appears showing: **"Transferring and Validating Software Update. Please Wait..."**



Once validation is successful, a confirmation window is displayed showing both the currently installed version and the validated new version.



6. Click **OK** to proceed or **Cancel** to abort the update process.
7. On After confirming the update, the system installs the software and then prompts the administrator with **Reboot Now** or **Cancel**.

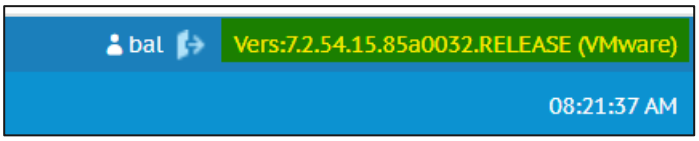


- Clicking **Reboot Now** reboots the TOE and activates the new version.
- Clicking **Cancel** aborts the update process. The TOE does not retain the uploaded version, and the system continues running the previously active version.

Note: The TOE does **not** support delayed activation. If the reboot is not performed immediately after installation, the update is discarded and must be re-uploaded and installed again.

8. The currently active version of the TOE is displayed in the top-right corner of the Home page screen.

The TSF allows the Security Administrator to query the currently running version of the software and initiate software updates via HTTPS WUI. The currently active software version is displayed on the Home page of the TOE, specifically in the top-right corner. To view this, the administrator must log in to the WUI using valid credentials. Upon successful authentication, the Home page is displayed by default, showing the active version information.



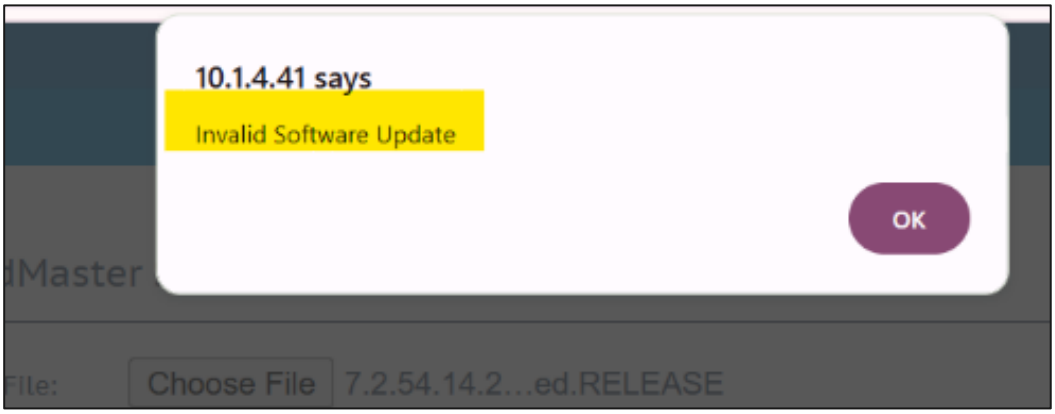
The WUI will display a warning message indicating that the device is rebooting, and all functions will cease to operate during the reboot. Once the reboot is complete and the WUI becomes accessible again, the administrator can log in to the TOE.

Integrity and Signature Verification:

The software image and the corresponding XML signature file must be downloaded by the Security Administrator from the official support website to a trusted administrative workstation uploaded to the TOE for the update process.

The TOE performs a mandatory **digital signature verification using RSA-2048 before installing the software update.**

- If the signature is **valid**, the update proceeds as described.
- If the digital signature verification **fails** (due to tampering, an invalid software image, missing XML signature file, or a mismatched XML signature file):
  - The TSF **discards the update**,
  - Displays an **error message**, and
  - Generates an **audit log** entry.



Note: The TOE does not support hash-based verification for update validation. The TOE rejects updates if an invalid software image or mismatched XML file is provided.

An audit log is generated in such cases.

Note: Only users with full administrative privileges (such as the 'bal' user) can initiate manual software updates.

Restore Software:

If an update of LoadMaster's firmware has been completed, the administrator can use this option to revert to the previous build.

6.38. AUDITING

Progress LoadMaster sends audit records to the external server as the audit records are generated. It transmits generated audit data to an external server using the TLS trusted channel. It does not retransmit audit logs that were generated while the connection to the audit server was down.

When local audit storage is exhausted, the TSF will not record new events locally until additional space is available. Records are still transmitted to the external server, and so the audit trail is preserved. Local audit records will be temporarily stored in a buffer until they can be stored. The TOE stores persistent audit records locally with a minimum storage size of [7GB], ensuring that audit records are preserved across reboots or power cycles. TSF allows all available space to be used to store audit records. For the Virtual Load Master that is up to 7GB. The HW Load Master models have up to 25GB of space.

Note: The audit log storage size is not configurable.

The TOE restricts the ability to determine and modify the behavior of transmission of audit data to an external IT entity to Security Administrators.

The TOE is a single standalone component that stores audit data locally.

The TSF protects audit data from unauthorized modification and deletion through the restrictive administrative interfaces. This protection is enforced by default and does not require any additional configuration.

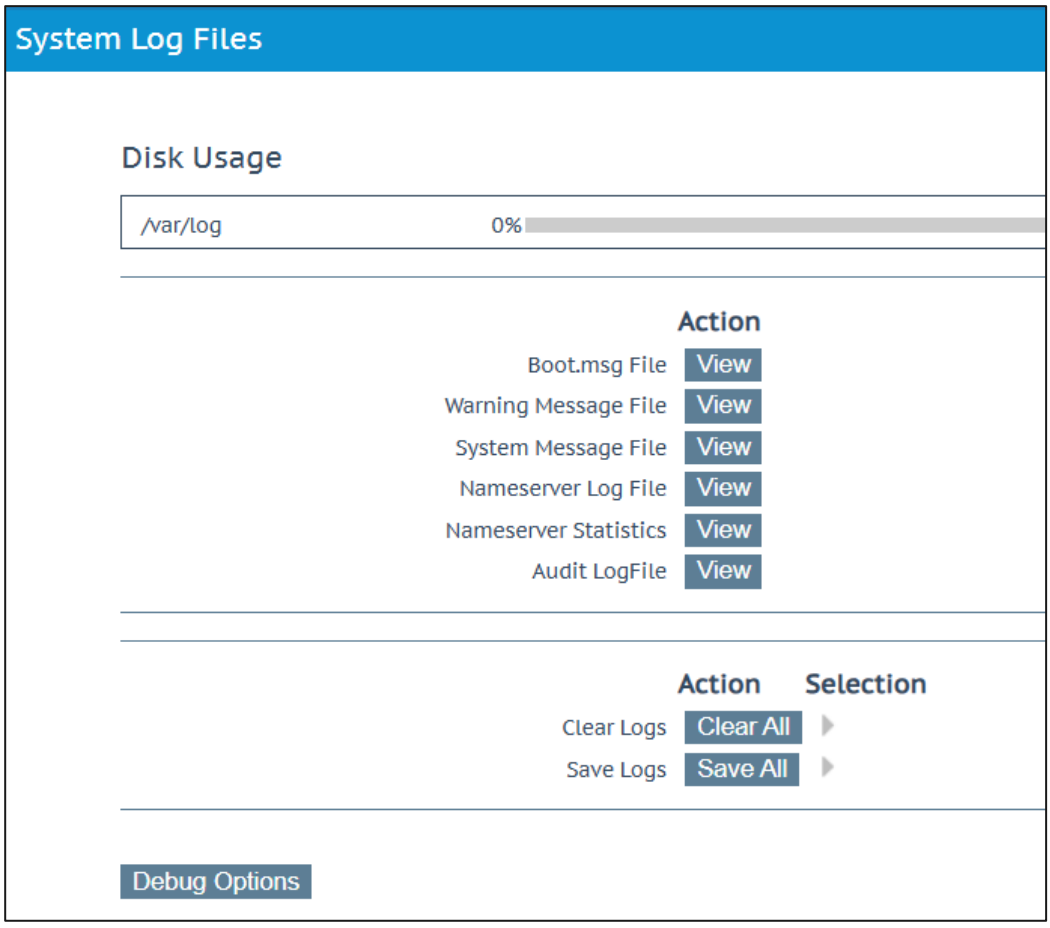
The Progress LoadMaster generates a warning log when audit storage reaches 85% of capacity to inform the administrator that audit storage is nearing capacity.

The **Disk Usage** under **System Configuration > Logging Options > System Log Files** provides a visual indication of the percentage used/free of the log partition. Color-coding is used to highlight different usage levels:

- 0% to 50%: green
- 50% to 90%: orange
- 90% to 100%: red

The screenshots below demonstrate this visual behavior at different usage levels:

The image below shows the /var/log partition at **0% usage**, indicating sufficient available space.

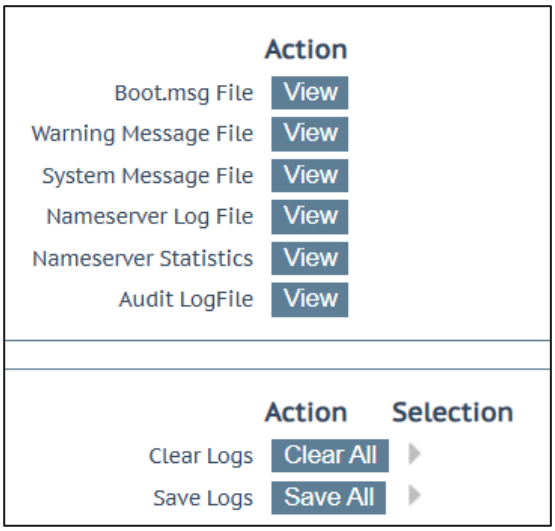


The image below shows the /var/log partition at **100% usage**, displayed in **red**, indicating that the log storage is full.

The administrator can view locally stored logs using the Web User Interface by navigating to: **System Configuration > Logging Options > System Log Files.**

In this section, the administrator can perform the following actions:

- **View individual log files** by clicking the **View** button next to each log file listed under the "Action" column. The available log files are:
    - Boot.msg File
    - Warning Message File
    - System Message File
    - Nameserver Log File
    - Nameserver Statistics
    - Audit LogFile
- **Manually export logs** by clicking the **Save All** button under the "Action" section. This option allows the administrator to download all log files, including the audit log, for external analysis or archival.

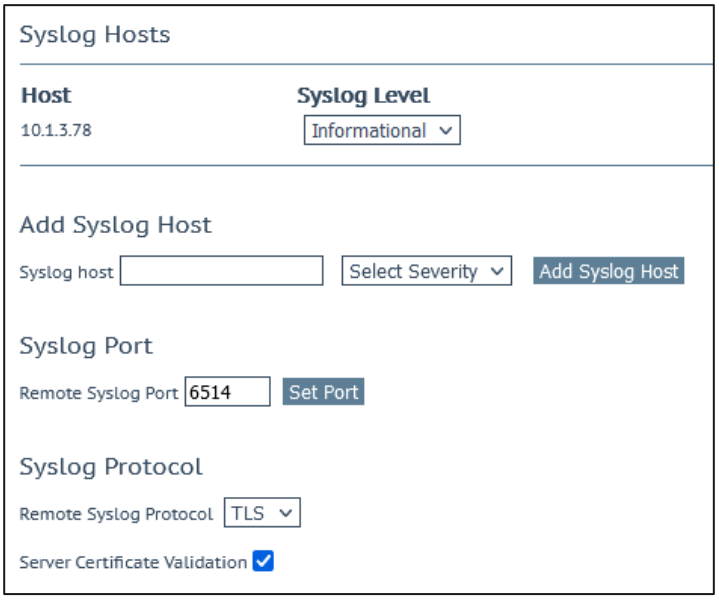


6.39. SECURE REMOTE LOGGING

The LoadMaster can produce various warning and error messages using the syslog protocol. These messages are normally stored locally. Syslog messages are transmitted securely using TLS to remote servers. The LoadMaster uses 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.

1. In the left frame menu, click **System Configuration > System Log Files > Syslog Options.**
2. By entering the relevant IP address in the **Syslog host** text box and select the severity and click **Add Syslog Host.**
3. Also enter the **Syslog Port** enter *any port other than 601* and click on **Set Port**.
4. Select the **Syslog Protocol** either TCP, UDP or TLS.
5. Enable the Server Certificate Validation.

Note: secure syslog channel is restricted to TLSv1.2.



NOTE: If the TLS connection to the syslog server is unintentionally broken, the administrator should verify the connectivity to the syslog server. Once connectivity is restored, the administrator must manually re-initiate the syslog connection.

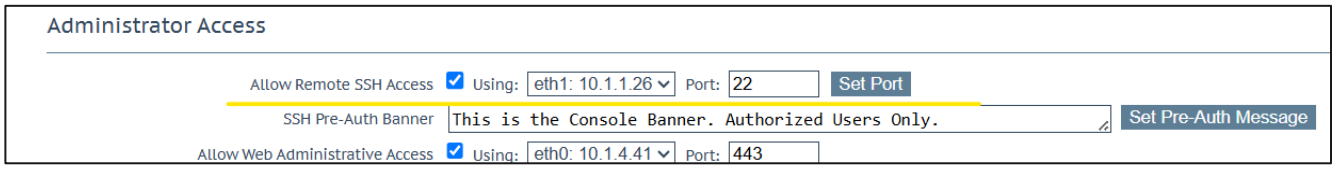
6.40. LOGGING FOR ADMIN WUI LOGON

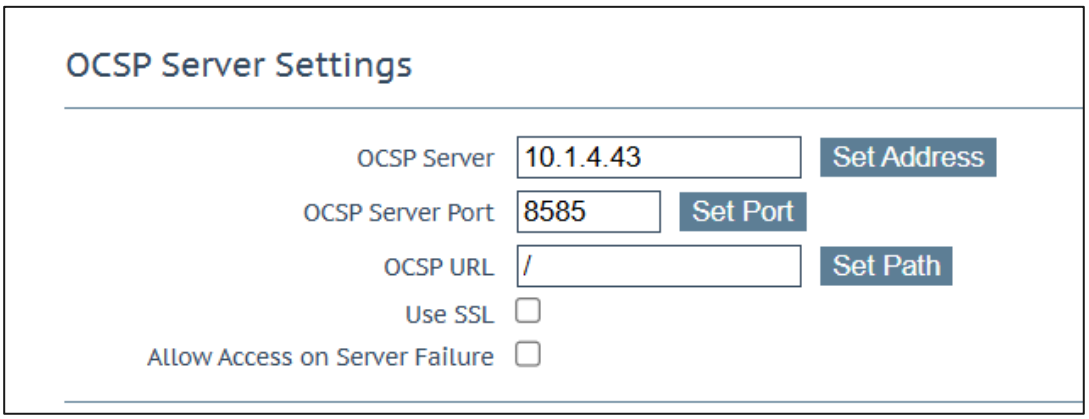
In the left frame menu, click **System Configuration -> Network Options**

a. Set the **Log SSL errors** to **"All errors"**

6.41. DISABLE SSH ACCESS

In the left frame menu, click **Certificates & Security > Remote Access**, and to disable remote SSH access, set the "**Using**" option under **Allow Remote SSH Access** to the **console interface IP** instead of "**All Networks**." This limits SSH access to the local console only.





6.42. SAMPLE AUDIT LOGS

6.42.1. FORMAT

The following is the general format of all syslog messages:

```
Timestamp Hostname process name: Message content
```

Field details are as follows:

Timestamp: The date and time when the message were generated, indicating when the event occurred.

Hostname: The name device that generated the message, identifying the source of the log.

Process name: The name of the process that generated the message, specifying which software component is logging into the message.

Message content: The actual log message detailing the event or condition being reported.

For example, a logged message looks like this:

```
2025-06-23T13:49:37+00:00 lb100 syslog-ng: syslog-ng starting up;
version='3.25.1'
```

6.42.2. AUDITABLE EVENTS:

The following events generate audit logs:

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence

FAU_GEN.1	•Start-up and shut-down of the audit functions
	
	•Auditable events for the not specified level of audit; and Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).
	
	•Changes to TSF data related to configuration changes
		None	• **Start-up of the audit functions**
			
			`2025-06-23T13:49:36+00:00 lb100 logger: User bal (192.168.254.147) set 'SYSLOG_INFO' to '10.1.4.58'`
			
			`2025-06-23T13:49:37+00:00 lb100 syslog-ng: syslog-ng starting up; version='3.25.1'`
			
			`2025-06-23T13:49:38+00:00 lb100 syslog-ng: System log started`
			
			• **Shut-down of the audit functions**
			
			`2025-06-23T13:47:44+00:00 lb100 kernel: Kernel logging (proc) stopped.`
			
			`2025-06-23T13:47:44+00:00 lb100 kernel: Kernel log daemon terminating.`
			
			`2025-06-23T13:47:44+00:00 lb100 syslog-ng: syslog-ng shutting down; version='3.25.1'`
			
			• **Administrative login and logout**
			Remote:
			Login:
			`2025-06-10T11:30:48+00:00 lb100 logger: User bal (192.168.254.239) Logged in (Session: teDHpUfAB6172OQH88ESbfYz)`
			
			Logout:

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
	(in addition to the information that a change occurred it shall be logged what has been changed). •Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged). •Resetting passwords (name of related user account shall be logged).		2025-06-10T11:34:27+00:00 lb100 logger: User bal (192.168.254.239) Logged out (Session: teDHpUfAB6172OQH88ESbfYz) **Console:** **Login:** 2025-06-16T02:00:23+00:00 lb100 bal: Isetup: User bal logged in to session 02456FB018B6 from /dev/ttyS0 **Logout:** 2025-06-10T11:26:52+00:00 lb100 bal: Isetup: User bal logged out from session 9FFEEC9780A4 • **Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).** **Time Change:** 2021-06-11T23:01:10+00:00 lb100 logger: User bal (192.168.254.239) Changed date from Wed Jun 11 23:01:10 UTC 2025 to Fri Jun 11 23:01:10 UTC 2021 2021-06-11T15:59:20+00:00 lb100 logger: User bal (192.168.254.239) Changed time from Fri Jun 11 23:01:10 UTC 2021 to Fri Jun 11 15:59:20 UTC 2021 **Addition of trust anchors:** 2025-06-13T10:05:58+00:00 lb100 logger: User bal (192.168.254.8) Installed an Intermediate/CA Certificate rootCA (/C=US/CN=rootCA) 2025-06-13T10:11:32+00:00 lb100 logger: User bal (192.168.254.8) Installed an Intermediate/CA Certificate ICA (/C=US/CN=ICA)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence

			• **Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).**
			Generating of Key:
			`2025-06-09T11:30:59+00:00 lb100 logger: User bal (192.168.254.239) Generated self signed certificate key for 10.1.4.41`
			
			• **Resetting passwords (name of related user account shall be logged).**
			`2025-07-23T10:58:28+00:00 lb100 logger: User bal (192.168.228.68) Set password for user testuser`

FAU_GEN.2	None	None	

FAU_STG_EXT.1	Configuration of local audit settings	Identity of account making changes to the audit configuration	• **Configuration of local audit settings**
			
			`2025-07-23T11:00:21+00:00 lb100 logger: User bal (192.168.228.68) set 'SYSLOG_PORT' to '65140'`
			`2025-07-23T11:00:30+00:00 lb100 logger: User bal (192.168.228.68) set 'SYSLOG_PORT' to '6514'`

FAU_STG_EXT.3	Low storage space for audit events.	None.	`2025-05-19T21:00:01+00:00 lb100 logger: /var/log partition usage exceeded 96%`
FCS_CKM.1	None	None	
FCS_CKM.2	None	None	
FCS_CKM.4	None	None	
FCS_COP.1/DataEncryption	None	None	
FCS_COP.1/SigGen	None	None	
FCS_COP.1/Hash	None	None	
FCS_COP.1/KeyedHash	None	None	
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure	This does not apply since TOE is a HTTPS server without mutual authentication. Refer to FCS_TLSS_EXT.1 for non-mutual authentication logs

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity if new/removed time server	**Configuration of a new time server** 2025-06-11T12:25:40+00:00 lb100 logger: User bal (192.168.254.8) Set Time from NTP server "10.1.4.76" to Wed Jun 11 12:25:40 UTC 2025 from Wed Jun 11 12:25:32 UTC 2025 2025-06-11T12:25:41+00:00 lb100 logger: User bal (192.168.254.8) set 'NTP_HOST' to '10.1.4.76' 2025-06-11T12:15:54+00:00 lb100 logger: User bal (192.168.254.8) set 'NTP_KEYTYPE' to 'SHA1' 2025-06-11T12:22:19+00:00 lb100 logger: User bal (192.168.254.8) set 'NTP_KEYVAL' to '11' 2025-06-11T12:22:25+00:00 lb100 pwmangle: User bal (192.168.228.8) Set Passphrase in 'NTP_KEYSTRING' **Removal of configured time server** 2025-06-30T12:24:55+00:00 lb100 logger: User bal (192.168.254.8) set 'NTP_KEYSTRING' to '' 2025-06-30T12:24:55+00:00 lb100 logger: User bal (192.168.254.8) set 'NTP_KEYVAL' to '' 2025-06-30T12:24:55+00:00 lb100 logger: User bal (192.168.254.8) set 'NTP_KEYTYPE' to '' 2025-06-30T12:24:59+00:00 lb100 logger: User bal (192.168.254.8) set 'NTP_HOST' to ''
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure	• **Failure to establish a TLS Session** **Unsupported Ciphersuite:** 2025-06-12T09:26:22+00:00 lb100 syslog-ng: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_hello:wrong cipher returned'

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
			• **Modify a byte in Server Finished handshake Message:** 2025-06-12T09:37:49+00:00 lb100 syslog-ng: SSL error while writing stream; tls_error='SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac' • **Unsupported Protocol Version:** 2025-06-12T08:21:11+00:00 lb100 sslproxy: Client 10.1.4.58 failed SSL negotiation (ssl/statem/statem_srvr.c/1661): error:142090FC:SSL routines:tls_early_post_process_client_hello:unknown protocol) • **Unsupported EC Curve:** 2025-10-07T15:01:59+00:00 lb100 syslog-ng: SSL error while writing stream; tls_error='SSL routines:ssl3_get_key_exchange:wrong curve'
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure	• **Failure to establish a TLS Session** **Unsupported Ciphersuite:** 2025-06-12T07:31:19+00:00 lb100 sslproxy: Client 10.1.4.58 failed SSL negotiation (ssl/statem/statem_srvr.c/2285): error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher) • **Modify a byte in client Finished handshake Message:** 2025-06-12T07:47:24+00:00 lb100 sslproxy: Client 10.1.4.58 failed SSL negotiation (ssl/record/ssl3_record.c/521): error:1408F119:SSL routines:ssl3_get_record:decryption failed or bad record mac)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
			• **Unsupported Protocol Version:** 2025-06-12T08:21:11+00:00 lb100 sslproxy: Client 10.1.4.58 failed SSL negotiation (ssl/statem/statem_srvr.c/1686): error:14209102:SSL routines:tls_early_post_process_client_hello:unsupported protocol) • **Unsupported EC Curve:** 2025-11-19T16:48:15+00:00 lb100 sslproxy: Client 10.1.4.42 failed SSL negotiation (ssl/statem/statem_srvr.c/2285): error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher)
FCS_RBG_EXT.1	None	None	
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address).	• **Unsuccessful login attempts limit is met or exceeded** 2025-06-15T23:46:20+00:00 lb100 logger: User acumensec (192.168.254.239) Login failed - Invalid user/password 2025-06-15T23:46:27+00:00 lb100 logger: User acumensec (192.168.254.239) Login failed - Invalid user/password 2025-06-15T23:47:05+00:00 lb100 logger: User acumensec (192.168.254.239) Login failed - Invalid user/password 2025-06-15T23:47:05+00:00 lb100 logger: Blocking User acumensec (192.168.254.239) - too many failed attempts
FMT_MOF.1/Functions	None	None	

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate •Any addition, replacement or removal of trust anchors in the TOE's trust store	•Reason for failure of certificate validation •Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	**• Unsuccessful attempt to validate a certificate** 2025-06-13T10:42:00+00:00 lb100 syslog-ng: Certificate validation failed; subject='CN=rootCA, C=US', issuer='CN=rootCA, C=US', error='self signed certificate in certificate chain' 2025-06-13T10:42:00+00:00 lb100 syslog-ng: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed' **• Any addition, replacement or removal of trust anchors in the TOE's trust store** **Addition of trust anchors** 2025-06-13T10:05:58+00:00 lb100 logger: User bal (192.168.254.8) Installed an Intermediate/CA Certificate rootCA (/C=US/CN=rootCA) 2025-06-13T10:11:32+00:00 lb100 logger: User bal (192.168.254.8) Installed an Intermediate/CA Certificate ICA (/C=US/CN=ICA) **Removal of trust anchors** 2025-06-13T10:35:40+00:00 lb100 logger: User bal (192.168.254.8) Deleted Intermediate/CA Certificate ICA (/C=US/CN=ICA) **•Expired server certificate:** 2025-06-13T10:58:30+00:00 lb100 syslog-ng: Certificate validation failed; subject='CN=10.1.4.58, C=US', issuer='CN=ICA, C=US', error='certificate has expired' 2025-06-13T10:58:30+00:00 lb100 syslog-ng: SSL error while writing stream;

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
			tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed' **•Revoked server certificate:** 2025-06-20T05:20:03+00:00 lb100 ocspd: Connected to OCSP server: 10.1.4.58 (/C=US/ST=MD/O=Intertek/OU=Acumen/CN=10.1.4.58) 2025-06-20T05:20:03+00:00 lb100 ocspd: Certificate /C=US/ST=MD/O=Intertek/OU=Acumen/CN=10.1.4.58 revoked (UNKNOWN) 2025-06-20T05:20:03+00:00 lb100 ocspd: OCSP server returned FAIL status for cert '/C=US/ST=MD/O=Intertek/OU=Acumen/CN=10.1.4.58' 2025-06-20T05:20:03+00:00 lb100 ocspd: Connected to OCSP server: 10.1.4.58 (/C=US/CN=ICA) 2025-06-20T05:20:03+00:00 lb100 ocspd: OCSP server returned OK status for cert '/C=US/CN=ICA' **•Revoked Intermediate CA Certificate:** 2025-06-20T03:52:45+00:00 lb100 ocspd: Certificate /C=US/CN=ICA revoked (UNKNOWN) 2025-06-20T03:52:45+00:00 lb100 ocspd: OCSP server returned FAIL status for cert '/C=US/CN=ICA **•Invalid ocsp response** 2025-06-22T12:43:53+00:00 lb100 ocspd: Failed to connect to OCSP server: 10.1.4.58

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
			(/C=US/ST=MD/O=Intertek/OU=Acumen/CN=10.1.4.58) 2025-06-22T12:43:53+00:00 lb100 ocspd: Failed to connect to OCSP server: 10.1.4.58 (/C=US/CN=ICA) 2025-06-22T12:43:53+00:00 lb100 ocspd: Failed to connect to OCSP server: 10.1.4.58 (/C=US/ST=MD/O=Intertek/OU=Acumen/CN=10.1.4.58) 2025-06-22T12:43:53+00:00 lb100 ocspd: Failed to connect to OCSP server: 10.1.4.58 (/C=US/CN=ICA) 2025-06-22T12:43:56+00:00 lb100 kernel: Kernel logging (proc) stopped. 2025-06-22T12:43:56+00:00 lb100 kernel: Kernel log daemon terminating. 2025-06-22T12:43:57+00:00 lb100 syslog-ng: OCSP server certificate check failure - Remote logging disabled for 10.1.4.58 • **Error due to modified certificate bytes:** 2025-06-13T11:04:51+00:00 lb100 syslog-ng: SSL error while writing stream; tls_error='asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag' • **Failure due to Modified byte in signature:** 2025-06-13T11:09:04+00:00 lb100 syslog-ng: Certificate validation failed; subject='CN=10.1.4.58, C=US', issuer='CN=ICA, C=US', error='certificate signature failure' 2025-06-13T11:09:04+00:00 lb100 syslog-ng: SSL error while writing stream; tls_error='asn1 encoding routines:ASN1_item_verify:EVP lib' • **Failure due to modified byte in the public key:** 2025-06-13T11:13:00+00:00 lb100 syslog-ng: Certificate validation failed;

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
			subject='CN=10.1.4.58, C=US', issuer='CN=ICA, C=US', error='certificate signature failure' 2025-06-13T11:13:00+00:00 lb100 syslog-ng: SSL error while writing stream; tls_error='elliptic curve routines:ec_GFp_simple_oct2point:point is not on curve' **•Basic constraint is not present in the CA certificate:** 2025-06-13T14:33:27+00:00 lb100 syslog-ng: Certificate validation failed; subject='CN=ICA, C=US', issuer='CN=rootCA, C=US', error='invalid CA certificate' 2025-06-13T14:33:27+00:00 lb100 syslog-ng: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed'
FIA_X509_EXT.2	None	None	
FIA_X509_EXT.3	None	None	
FIA_PMG_EXT.1	None	None	
FIA_UIA_EXT.1	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)	**All use of identification and authentication mechanism** • **Successful authentication of Console** 2025-06-16T02:00:23+00:00 lb100 bal: Isetup: User bal logged in to session 02456FB018B6 from /dev/ttyS0 • **Successful authentication of Remote (WUI Authentication)** 2025-06-16T02:04:48+00:00 lb100 logger: User bal (192.168.254.239) Logged in (Session: LMiy1DFqev115L0oG16awQQz) • **Successful authentication of Remote (LDAP Authentication)**

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
			2025-06-16T02:12:00+00:00 lb100 logger: User ldapuser@acumen.local (192.168.254.239) Logged in (Session: vGHuOXQgxyIibo6KT2uZzAQz)
FIA_UAU.7	None	None	
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None	• **Any attempt to initiate a manual update:** 2026-06-18T04:56:41+00:00 lb100 logger: User bal (192.168.253.72) Logged in (Session: MfPkQNoHmwYERlSP1nu09A8z) 2026-06-18T04:59:02+00:00 lb100 logger: User bal (192.168.253.72) Software update started 2026-06-18T04:59:57+00:00 lb100 logger: User bal (192.168.253.72) Installed new software version: 7.2.54.18.a5db575.RELEASE.20260513-1210 2026-06-18T05:00:34+00:00 lb100 logger: User bal (192.168.253.72) Performed a Reboot 2026-06-18T05:00:34+00:00 lb100 logger: Nosession: Rebooting machine 2026-06-18T05:01:46+00:00 lb100 logger: RSA Sign and Verify Self-Test passed 2026-06-18T05:01:46+00:00 lb100 logger: Nosession: Generated self signed certificate key for 10.1.4.41 2026-06-18T05:01:48+00:00 lb100 logger: Crypto Self-Tests passed 2026-06-18T05:01:48+00:00 lb100 logger: Nosession: UI service started 2026-06-18T05:02:17+00:00 lb100 logger: System Booted
FMT_MOF.1/Services	None.	None.	
FMT_MTD.1/CoreData	None	None	

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
FMT_MTD.1/CryptoKeys	None	None	

FMT_SMF.1	All management activities of TSF data	None	•**Ability to administer the TOE locally:**
			`2025-06-16T02:00:23+00:00 lb100 bal: Isetup: User bal logged in to session 02456FB018B6 from /dev/ttyS0`
			
			•**Ability to administer the TOE remotely:**
			`2025-06-16T02:04:48+00:00 lb100 logger: User bal (192.168.254.239) Logged in (Session: LMiy1DFqev115L0oG16awQQz)`
			
			•**Ability to configure the access banner.**
			`2025-06-10T11:52:00+00:00 lb100 logger: User bal (192.168.254.239) set 'INITIAL_AUTH' to 'This is the LOGIN Banner. Authorized Users Only.'`
			
			•**Ability to configure the local and remote session inactivity time before session termination.**
			Local session:
			`2025-06-24T19:20:57+00:00 lb100 bal: Isetup: set 'CONSOLE_IDLE' to '300'`
			
			Remote session:
			`2025-06-10T17:25:58+00:00 lb100 logger: User bal (192.168.254.239) set 'SESSION_IDLE' to '300'`
			
			•**Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates.**
			`2026-06-18T04:56:41+00:00 lb100 logger: User bal (192.168.253.72) Logged in (Session: MfPkQNoHmwYERlSP1nu09A8z)`
			`2026-06-18T04:59:02+00:00 lb100 logger: User bal (192.168.253.72) Software update started`

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
			2026-06-18T04:59:57+00:00 lb100 logger: User bal (192.168.253.72) Installed new software version: 7.2.54.18.a5db575.RELEASE.20260513-1210 2026-06-18T05:00:34+00:00 lb100 logger: User bal (192.168.253.72) Performed a Reboot 2026-06-18T05:00:34+00:00 lb100 logger: Nosession: Rebooting machine 2026-06-18T05:01:46+00:00 lb100 logger: RSA Sign and Verify Self-Test passed 2026-06-18T05:01:46+00:00 lb100 logger: Nosession: Generated self signed certificate key for 10.1.4.41 2026-06-18T05:01:48+00:00 lb100 logger: Crypto Self-Tests passed 2026-06-18T05:01:48+00:00 lb100 logger: Nosession: UI service started 2026-06-18T05:02:17+00:00 lb100 logger: System Booted • **Ability to start and stop services;** **Start WUI** 2025-11-12T12:40:01+00:00 lb100 bal: Isetup: set 'START_SSLPROXY' to 'yes' 2025-11-12T12:40:03+00:00 lb100 logger: Nosession: UI service started **Stop WUI** 2025-11-12T12:39:54+00:00 lb100 bal: Isetup: set 'START_SSLPROXY' to 'no' 2025-11-12T12:39:54+00:00 lb100 logger: Nosession: UI service stopped **Start Syslog** 2025-06-23T13:49:36+00:00 lb100 logger: User bal (192.168.254.147) set 'SYSLOG_INFO' to '10.1.4.58'

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
			2025-06-23T13:49:37+00:00 lb100 syslog-ng: syslog-ng starting up; version='3.25.1' 2025-06-23T13:49:38+00:00 lb100 syslog-ng: System log started **Stop Syslog** 2025-06-23T13:47:44+00:00 lb100 logger: User bal (192.168.254.147) set 'SYSLOG_INFO' to '' 2025-06-23T13:47:44+00:00 lb100 kernel: Kernel logging (proc) stopped. 2025-06-23T13:47:44+00:00 lb100 kernel: Kernel log daemon terminating. 2025-06-23T13:47:44+00:00 lb100 syslog-ng: syslog-ng shutting down; version='3.25.1' • **Ability to modify the behaviour of the transmission of audit data to an external IT entity** 2025-07-23T11:00:30+00:00 lb100 logger: User bal (192.168.228.68) set 'SYSLOG_PORT' to '6514' • **Ability to configure the cryptographic functionality.** 2025-06-22T23:41:19+00:00 lb100 logger: User bal (192.168.254.147) Generated a new CSR for /C=US/O=Intertek/OU=Acumen Security/emailAddress=test.user@intertek.com/CN=10.1.4.41/ • **Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;** 2026-01-29T11:33:45+00:00 lb100 logger: Nosession: Generated self signed certificate key for 10.1.4.41 • **Ability to configure the list of supported (D)TLS ciphers;** 2025-10-07T15:18:05+00:00 lb100 logger: User bal (192.168.228.76) Added cipher list cc: ECDHE-ECDSA-AES128-SHA:ECDHE-

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
			ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384 2025-10-07T15:18:05+00:00 lb100 logger: User bal (192.168.228.76) set 'WUI_CIPHERSET' to 'cc' **•Ability to re-enable an Administrator account;** 2025-06-16T00:14:15+00:00 lb100 logger: User bal (192.168.254.239) User acumensec unblocked **•Ability to set time which is used for time-stamps.** 2021-06-11T23:01:10+00:00 lb100 logger: User bal (192.168.254.239) Changed date from Wed Jun 11 23:01:10 UTC 2025 to Fri Jun 11 23:01:10 UTC 2021 2021-06-11T15:59:20+00:00 lb100 logger: User bal (192.168.254.239) Changed time from Fri Jun 11 23:01:10 UTC 2021 to Fri Jun 11 15:59:20 UTC 2021 2025-06-11T23:41:30+00:00 lb100 logger: User bal (192.168.254.239) Set Time from NTP server "10.1.4.76" to Wed Jun 11 23:41:30 UTC 2025 from Fri Jun 11 23:41:22 UTC 2021 **•Ability to configure NTP;** 2025-06-11T12:25:41+00:00 lb100 logger: User bal (192.168.254.8) set 'NTP_HOST' to '10.1.4.76' 2025-06-11T12:15:54+00:00 lb100 logger: User bal (192.168.254.8) set 'NTP_KEYTYPE' to 'SHA1' 2025-06-11T12:22:19+00:00 lb100 logger: User bal (192.168.254.8) set 'NTP_KEYVAL' to '11' 2025-06-11T12:22:25+00:00 lb100 pwmangle: User bal (192.168.228.8) Set Passphrase in 'NTP_KEYSTRING' **•Ability to configure the authentication failure parameters for FIA_AFL.**

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
			2025-06-15T23:41:15+00:00 lb100 logger: User bal (192.168.254.239) set 'SESSION_MAXBLOCK' to '3' • **Ability to manage the cryptographic keys.** 2025-06-09T11:30:59+00:00 lb100 logger: User bal (192.168.254.239) Generated self signed certificate key for 10.1.4.41 • **Ability to manage trust stores and designate X509.v3 certificates as trust anchors** 2025-06-13T10:05:58+00:00 lb100 logger: User bal (192.168.254.8) Installed an Intermediate/CA Certificate rootCA (/C=US/CN=rootCA) 2025-06-13T10:11:32+00:00 lb100 logger: User bal (192.168.254.8) Installed an Intermediate/CA Certificate ICA (/C=US/CN=ICA) • **Ability to generate Certificate Signing Request (CSR) and process CA certificate response** 2025-06-22T23:41:19+00:00 lb100 logger: User bal (192.168.254.147) Generated a new CSR for /C=US/O=Intertek/OU=Acumen Security/emailAddress=test.user@intertek.com/CN=10.1.4.41/
FMT_SMR.2	None	None	
FPT_APW_EXT.1	None	None	
FPT_SKP_EXT.1	None	None	
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to	For discontinuous changes to time: The old and new values for the time. Origin of the attempt	• **Discontinuous changes to time** **Manual** 2021-06-11T23:01:10+00:00 lb100 logger: User bal (192.168.254.239) Changed date from Wed Jun 11 23:01:10 UTC 2025 to Fri Jun 11 23:01:10 UTC 2021 2021-06-11T15:59:20+00:00 lb100 logger: User bal (192.168.254.239) Changed time from Fri Jun 11 23:01:10 UTC 2021 to Fri Jun 11 15:59:20 UTC 2021 **NTP**

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
	be logged. See also application note	to change time for success and failure (e.g., IP address	2025-06-11T23:41:30+00:00 lb100 logger: User bal (192.168.254.239) Set Time from NTP server "10.1.4.76" to Wed Jun 11 23:41:30 UTC 2025 from Fri Jun 11 23:41:22 UTC 2021
FPT_TST_EXT.1	None	None	
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None	• **Initiation of update; result of the update attempt (success or failure)** **Successful attempt** 2026-06-18T04:56:41+00:00 lb100 logger: User bal (192.168.253.72) Logged in (Session: MfPkQNoHmwYERlSP1nu09A8z) 2026-06-18T04:59:02+00:00 lb100 logger: User bal (192.168.253.72) Software update started 2026-06-18T04:59:57+00:00 lb100 logger: User bal (192.168.253.72) Installed new software version: 7.2.54.18.a5db575.RELEASE.20260513-1210 2026-06-18T05:00:34+00:00 lb100 logger: User bal (192.168.253.72) Performed a Reboot 2026-06-18T05:00:34+00:00 lb100 logger: Nosession: Rebooting machine 2026-06-18T05:01:46+00:00 lb100 logger: RSA Sign and Verify Self-Test passed 2026-06-18T05:01:46+00:00 lb100 logger: Nosession: Generated self signed certificate key for 10.1.4.41 2026-06-18T05:01:48+00:00 lb100 logger: Crypto Self-Tests passed 2026-06-18T05:01:48+00:00 lb100 logger: Nosession: UI service started 2026-06-18T05:02:17+00:00 lb100 logger: System Booted **unsuccessful attempt**

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
			2025-07-10T12:07:14+00:00 lb100 logger: User bal (192.168.254.8) Software update started 2025-07-10T12:07:23+00:00 lb100 logger: User bal (192.168.254.8) Software update failed: Invalid Update 2025-07-17T13:09:16+00:00 lb100 logger: User bal (192.168.254.8) Software update started 2025-07-17T13:09:25+00:00 lb100 logger: User bal (192.168.254.8) Software update failed: Verification file required 2025-07-10T13:05:17+00:00 lb100 logger: User bal (192.168.254.8) Software update started 2025-07-10T13:05:27+00:00 lb100 logger: User bal (192.168.254.8) Software update failed: Invalid Verification file
FTA_SSL_EXT.1 (if "terminate the session is selected)	The termination of a local session by the session lock	None	• **The termination of a local session by the session lock** 2025-11-12T12:26:06+00:00 lb100 logger: Isetup: User bal Logged out from session due to inactivity
FTA_SSL.3	The termination of a remote session by the session locking mechanism	None	• **The termination of a remote session by the session locking mechanism** 2025-06-10T17:46:08+00:00 lb100 logger: User bal Timed out (Session : sBblYJaiEsL3OAsN7Pj1Y24z)
FTA_SSL.4	The termination of an interactive session	None	• **The termination of an interactive session** **Local Console Logout** 2025-06-10T11:26:52+00:00 lb100 bal: Isetup: User bal logged out from session 9FFEEC9780A4

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence
			Remote Logout 2025-06-10T11:34:27+00:00 lb100 logger: User bal (192.168.254.239) Logged out (Session: teDHpUfAB6172OQH88ESbfYz)
FTA_TAB.1	None	None	
FTP_ITC.1	•Initiation of the trusted channel •Termination of the trusted channel •Failure of the trusted channel functions	•None •None •Reason for failure	•**Initiation of the trusted channel (LDAP)** 2026-02-17T19:07:55+00:00 lb100 logger: User cn=admin,dc=acumen,dc=local (192.168.253.113) Logged in (Session: VObMntIgviO8A1JqZXWeAfoz) 2026-02-17T19:07:54+00:00 lb100 validuser: LDAP connected to server 10.1.4.42. CC approved mode enabled •**Termination of the trusted channel (LDAP)** 2026-02-09T17:00:42+00:00 lb100 validuser: LDAP disconnected from server 10.1.4.42 •**Failure of the trusted channel functions (LDAP)** 2025-07-31T23:19:40+00:00 lb100 validuser: bind failed for user [cn=admin,dc=acumen,dc=local], rc:-1 server:ldaps://10.1.4.42 error:unspecified •**Initiation of the trusted channel (External audit server)** 2026-05-05T17:21:19-04:00 lb100 syslog-ng: syslog-ng starting up; version='3.25.1' 2026-05-05T17:21:19-04:00 lb100 syslog-ng: Syslog connection established; server='10.1.4.58' 2026-05-05T17:21:19-04:00 lb100 syslog-ng: Override sigalgs: 'ECDSA+SHA384:ECDSA+SHA256:ECDSA+SHA512' 2026-05-05T17:21:20-04:00 lb100 syslog-ng: System log started

Requirement	Auditable Events	Additional Audit Record Contents	Audit Logs evidence

			• **Termination of the trusted channel (External audit server)**
			`2026-05-05T17:21:19-04:00 lb100 syslog-ng: syslog-ng shutting down; version='3.25.1'`
			
			• **Failure of the trusted channel functions (External audit server)**
			`2026-02-04T11:48:56+00:00 lb100 syslog-ng: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_hello:wrong cipher returned'`

FTP_TRP.1/Admin	• Initiation of the trusted channel
	• Termination of the trusted channel
	• Failure of the trusted channel functions
		• None
		
		• None
		
		Reason for failure
			• **Initiation of the trusted channel**
			`2025-06-12T01:44:33+00:00 lb100 logger: User bal (192.168.254.239) Logged in (Session: HjPaKz90UHDxGz1Mqhc0FKwz)`
			
			• **Termination of the trusted channel**
			`2025-06-12T01:53:47+00:00 lb100 logger: User bal (192.168.254.239) Logged out (Session: HjPaKz90UHDxGz1Mqhc0FKwz)`
			
			• **Failure of the trusted channel functions**
			`2025-11-19T16:48:15+00:00 lb100 sslproxy: Client 10.1.4.42 failed SSL negotiation (ssl/statem/statem_srvr.c/2285): error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher)`

APPENDIX A: GAINING XROOT ACCESS TO THE LOADMASTER

Some testing (such as generating log data for capacity testing) will require gaining privileged access to the system, which is called 'xroot access' on LoadMaster. Credentials obtained for xroot access will last about 24 hours, or until the unit is rebooted. To obtain credentials requires interaction with a member of the Kemp Team. The procedure is as follows:

1. Open the LoadMaster system console in VMware. You should see a login prompt.
2. Log in as the user 'bal' with the same password used to log into the UI. (Unless it was changed afterwards, this is the password you set at installation.)
3. Press **7** and then **Enter**.
4. Press **9** and then **Enter**.
5. Press **6** and then **Enter**.
6. The Diagnostic Login screen displays a key (a string of digits). Send this key in an email to ***<email_address_provided_by_Kemp>***. You can now exit the console interface as follows:
    a. Press **Enter** at the **Diagnostic Login** screen.
    b. At the next 3 menus, press **q** and then **Enter** to return to the login prompt.
7. When you receive an email response, use the password provided to log into the LoadMaster via SSH, as in this Linux shell command example:

    $ssh xroot@192.168.1.24

    Substitute the **eth0** IP address of the LoadMaster for the one in the example above. After logging in successfully, you should see a login prompt like the following:

    lb100:~ #

APPENDIX B: GENERATING LOG DATA FOR FAU_STG_EXT.1 TEST #2

Steps for filling up the */var/log* partition and checking disk usage:

1. Follow the steps in Appendix A, above, to login to LoadMaster as xroot.
2. To check disk usage, enter: df -h
3. Enter: cd /var/log
4. Fill the */var/log/* partition up to 84% using the "dd" command":

   dd bs=1024 count=$((1024 * 1024 * 5)) if=/dev/zero of=bigfile

   Note: the value (1024 * 1024 * 5) is equivalent to 5GB. The first 1024 is a KB value equivalent to 1 MB. Second 1024 and 5 are just the multiplication factors to provide expected file size.
5. To update the cron job for log disk usage notification to be executed per minute, edit the file */etc/crontab* and find the following line:

   0 * * * * root /sbin/check_dskusage >/dev/null 2>&1

   Change the "0" to "*", so that it reads as follows:

   * * * * * root /sbin/check_dskusage >/dev/null 2>&1

   As a result of this change, no log will appear until disk usage is above 85%.
6. Now fill up the log partition to about 86% capacity and wait for more than a minute. The following log should appear in the system log file:

   2020-11-12T17:00:01+00:00 lb100 logger: /var/log partition usage exceeded 86%

APPENDIX C: CVE MITIGATION

CVE-2021-41823

The TOE (Progress LoadMaster) is **not directly affected** by CVE-2021-41823 when tested independently. By default, **real servers are not configured** on the appliance.

However, if the deployment involves routing **production traffic through LoadMaster to backend real servers**, and those real servers are **not patched**, then the vulnerability could still be **observed** via responses from the **unpatched backend systems**.

Mitigation Steps When Using Real Servers:

To mitigate this risk in such scenarios, a custom Web Application Firewall (WAF) rule can be applied on LoadMaster to block exploitation attempts:

SecRule REQUEST_URI "@detectXSS" \

"id:1000,\

phase:2,\

deny,\

capture,\

t:none,t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls,\

msg:'XSS Attack Detected via libinjection',\

logdata:'Matched Data: %{TX.0} found within %{MATCHED_VAR_NAME}: %{MATCHED_VAR}',\

tag:'application-multi',\

tag:'language-multi',\

tag:'platform-multi',\

tag:'attack-xss',\

tag:'OWASP_CRS',\

tag:'capec/1000/152/242',\

ctl:auditLogParts=+E,\

ver:'OWASP_CRS/3.3.2',\

severity:'CRITICAL'"

Please see this link for details on how to use custom WAF rules on LoadMaster:

https://docs.progress.com/bundle/loadmaster-technical-note-waf-rule-writing-guide-ltsf/page/Add-a-Custom-Rule.html [docs.progress.com]

REFERENCES

Link to WUI Guide:

https://support.kemptechnologies.com/hc/en-us/articles/213906303-Web-User-Interface-WUI-

Link to CLI guide:

https://support.kemptechnologies.com/hc/en-us/articles/203128129-Command-Line-Interface-CLI-

Link to Procuring the TOE:
Latest Firmware – Kemp Support (kemptechnologies.com)