Progress®
Kemp® LoadMaster®

Technical Note Updating the LoadMaster Software

Generated on: 18 December 2024

Copyright

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

Table of Contents

Chapter 1: Introduction 4

Chapter 2: Gateway Releases 5

Chapter 3: Updating the LoadMaster Software 6

Download the Software Update 6

Back Up the LoadMaster Configuration 7

Back Up the System 7

Back Up the Certificates 7

Back Up Cipher Sets In Use 8

Update the Software 8

Set the Partner Shared Secret 11

Chapter 4: Restore the Software 13

Restore the Software – No Changes Made 13

Restore the Software – Changes Made 14

Restoring Certificates and Private Keys 14

Chapter 5: References 16

1

Introduction

As new LoadMaster software versions are released, you can apply these updates to get improvements, patch vulnerabilities, and maintain compatibility with the latest standards and protocols.

This document describes the steps to upgrade the LoadMaster software. We recommend performing a full backup of the system before updating the software.

To find out what is included in a LoadMaster software version, refer to the LoadMaster Release Notes.

You can download the latest software from the Progress Kemp website.

Prerequisites

If you plan on updating from a pre-LTS firmware version to a post-LTS firmware version, you must first upgrade to LTS. This is because the kernel was upgraded in the LTS version. You can follow the steps in this document to do this, but ensure to update to the LTS version before updating to a later version.

Before upgrading the LoadMaster firmware version, it is also a good idea to back up:

- The LoadMaster base configuration
- The LoadMaster's certificates
- Any cipher sets that are currently in use

Refer to the Back Up the LoadMaster section for instructions on how to do this.

2

Gateway Releases

7.2.60 is a Generally Available (GA) gateway release for the LoadMaster software. This means:

- You can upgrade from 7.2.60 to future LoadMaster versions
- You can upgrade from 7.2.54.7 (Long Term Support Feature (LTSF) release) or higher LTSF versions to 7.2.60
- To upgrade from any other LoadMaster versions (older than 7.2.60 GA or 7.2.54.7 LTSF) to a version above 7.2.60, you must first upgrade to 7.2.60

When downgrading, 7.2.61 is a gateway release. That means, if you want to downgrade from a version above 7.2.61 to a version below 7.2.61, you should downgrade to 7.2.61 first.

For an explanation of the difference between GA and LTSF releases, and approximate release dates of the GA and LTSF LoadMaster firmware versions, refer to the following article: Guidance for Selecting LoadMaster Releases.

3

Updating the LoadMaster Software

Follow the steps in the sub-sections below to back up and update the LoadMaster software.

Note: You will experience issues accessing the LoadMaster if all of the below conditions are met:

- You update the LoadMaster firmware from a version below LTS to 7.2.*XX*
- Any time after updating the firmware, you change the password to access the LoadMaster
- After changing the LoadMaster password, you downgrade to version 7.1.*XX*

This is because the hashing algorithm changed in version 7.2.36. LoadMasters with firmware version 7.2.36 and above can read old passwords, but LoadMasters with firmware version 7.1.*XX* cannot read new passwords.

Related Links

For details, see the following topics:

- Download the Software Update
- Back Up the LoadMaster Configuration
- Update the Software

Download the Software Update

To download the latest version of the LoadMaster software, go to the following page: Download LoadMaster

Firmware.

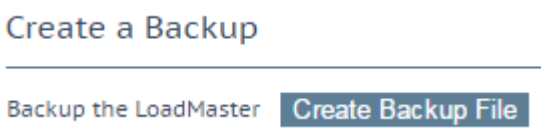
Back Up the LoadMaster Configuration

The sections below contain instructions on how to back up the LoadMaster system configuration, SSL certificates, and any cipher sets in use.

Back Up the System

Follow the steps below to create a backup file:

1. In the main menu of the LoadMaster Web User Interface (WUI), navigate to **System Configuration > System Administration > Backup/Restore**.



2. Click the **Create Backup File** button.

A download of the backup will start. The file name is set to **LMbackup** and the date and time.

If you rename the file, do not change the file extension.

Select a location to save the backup file to – this is browser-dependent as some browsers will automatically save the file to a location that was already pre-set.

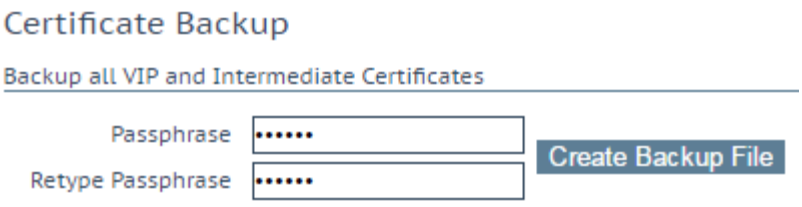
The backup file contains the LoadMaster base information such as system defaults and all information about each configured Virtual Service. LoadMaster accounts are not included in backups for security reasons.

For High Availability (HA) pairs, you only need to take a backup from one of the units (not both).

Back Up the Certificates

To back up certificates, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **Certificates & Security > Backup/Restore Certs**.



2. Enter a **Passphrase** in the text boxes provided.

Note: The passphrase is very important and should be safeguarded. The backup file cannot be opened without the passphrase as it is encrypted.

3. Click the **Create Backup File** button.
4. The filename is automatically set with **CertBackup** and the date and time. Select the location to save the backup file to – this is browser-dependent as some browsers will automatically save the file to a location that was already pre-set. It is a good idea to save this file with the system backup. The file can be renamed but do not change the file extension.

Note: The private keys are backed up as part of the certificate backup. Even though this file is password protected – it should be stored securely as it contains private key material.

Back Up Cipher Sets In Use

The built-in LoadMaster cipher sets may be automatically changed during a firmware upgrade. As a result, you may want to save a copy of the current cipher sets you have in use. The steps below provide instructions on how to do this for the **BestPractices** cipher set, as an example:

1. In the LoadMaster WUI, go to **Certificates & Security > Cipher Sets**.
2. Select **BestPractices** in the **Cipher Set** drop-down list.
3. In the **Save as** text box, enter a name for the cipher set to save, for example, **BestPractices-7.2.58**.

You can assign this cipher set to your Virtual Services as needed in the **SSL Properties** section of the Virtual Service modify screen.

Update the Software

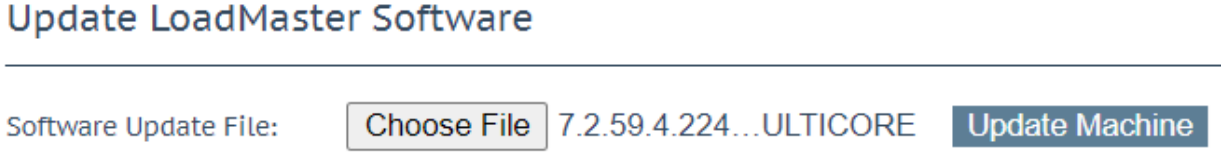
Note: As the update process requires a reboot, we recommend that the software update is performed during a maintenance window.

The following Knowledge Base articles provide some additional information about LoadMaster firmware upgrades:

- Progress LoadMaster Firmware Upgrade Path
- Firmware Upgrade Questions, Issues and Best Practices

To update the software, follow the steps below:

1. In the main menu of the LoadMaster WUI, navigate to **System Configuration > System Administration > Update Software**.



2. Click **Choose File** in the **Update LoadMaster Software** section and navigate to the software file that was downloaded from the Progress Kemp site.

   Note:

   When updating LoadMaster hardware, starting with 7.2.54.5, you can only update a hardware LoadMaster with an image that supports the boot method used by the hardware. The newer NG models (introduced in 2023) use the UEFI boot method, while earlier models use the BIOS boot method. If you attempt to update a hardware appliance with an updated image that doesn't support the boot method used by the appliance, the update process stops and the following message is displayed:

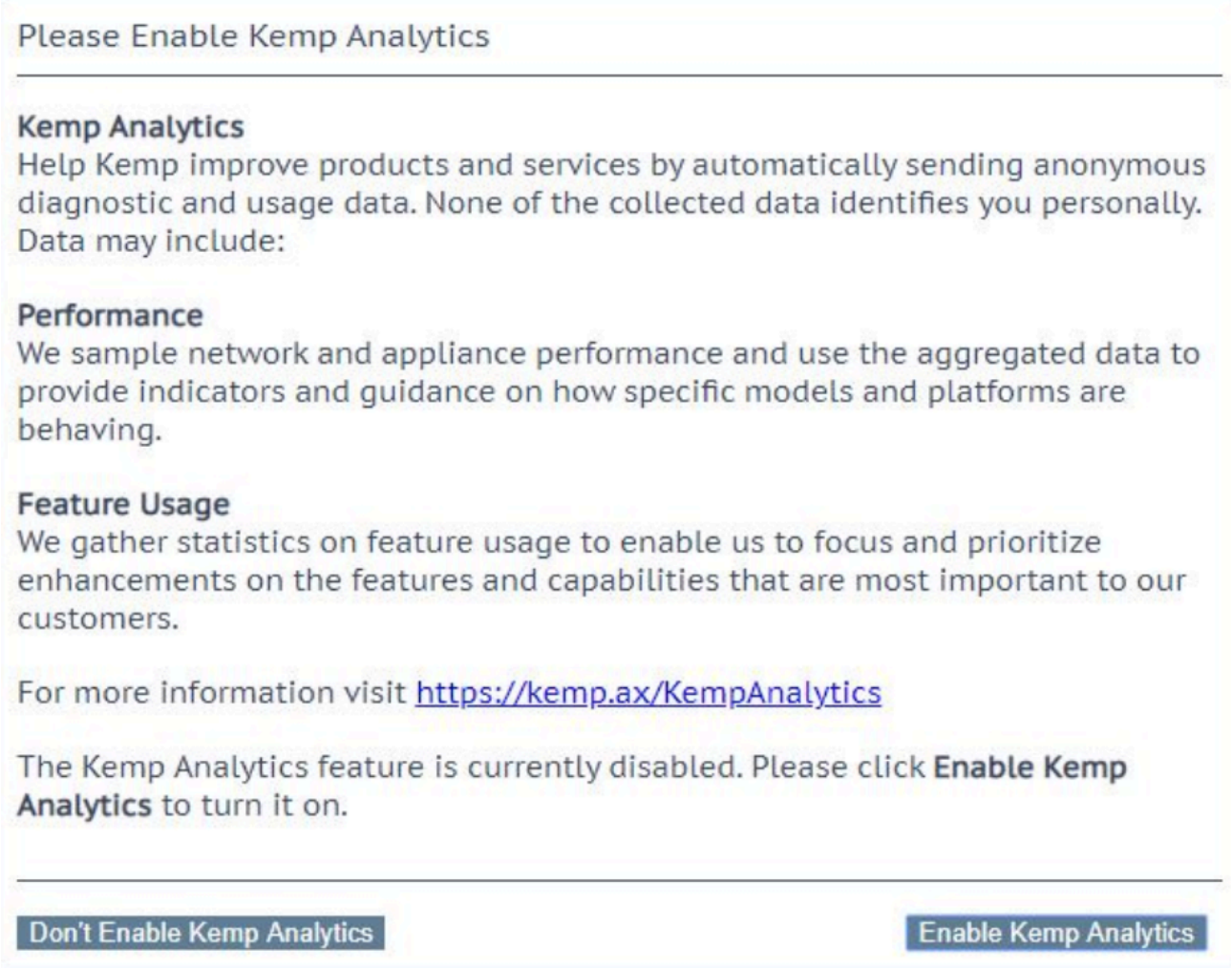
   The system cannot be updated with the provided image, which is not supported on the hardware platform on which you are attempting to install it.

   All LoadMaster -NG hardware models (introduced in 2023) require UEFI-capable patches, and so cannot be updated with any patch earlier than 7.2.54.6, or between 7.2.55.0 and 7.2.59.1 (inclusive).

   For more information, refer to the knowledge base article: LoadMaster Firmware Upgrade Path.

   Note: Do not install an ECS update image on a LoadMaster without the ECS add-on package already installed. Doing so invalidates your LoadMaster license.

3. Click **Update Machine**. The file is checked and validated.
4. Click **OK** to proceed and install the software after validation is complete. Once installed, the LoadMaster will need to be rebooted.
5. Click **Reboot**.
6. Click **Continue**.

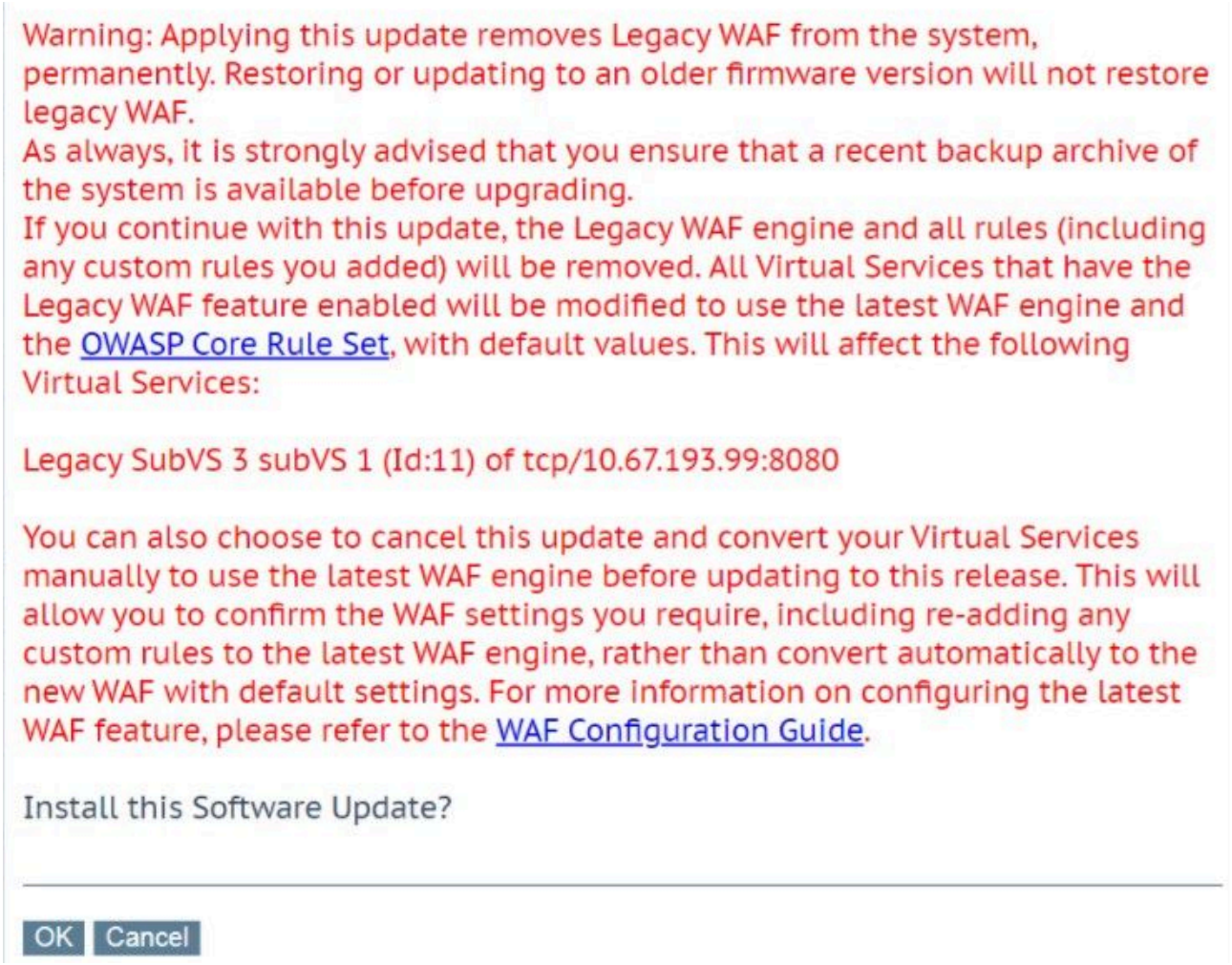


If you are updating the software to version 7.2.49.1 or higher, a screen appears to enable Kemp Analytics. To enable this feature, click **Enable Kemp Analytics**. To proceed without enabling this feature, click **Don't Enable Kemp Analytics**.

For further details, refer to the following pages:

- Call Home - Disclosure and Usage
- Kemp Analytics Disclosure and Usage

Upgrading to 7.2.61 or above (legacy WAF removal)



If you upgrade from a LoadMaster version prior to 7.2.61, during the upgrade any legacy WAF-enabled Virtual Services get converted to use the OWASP WAF with the default values configured. During upgrade, you get notified with a warning message that indicates the list of Virtual Services and SubVSs that have legacy WAF enabled. To continue to use the legacy WAF functionality, click **Cancel** (to remain on the previous version) or click **OK** to proceed with the LoadMaster firmware version upgrade. For more details, refer to the following section: Converting from Legacy WAF to OWASP WAF of WAF Feature description document.

When you upgrade to 7.2.61, legacy WAF functionality is removed from the LoadMaster. If you downgrade from 7.2.61 or above to a version below 7.2.61, legacy WAF will not be restored.

Set the Partner Shared Secret

If you update the LoadMaster software from a version prior to 7.2.54.10 (LTSF) or 7.2.59.4 (GA) and High Availability (HA), clustering, and/or GEO partners are configured, you will see a warning on the LoadMaster homepage that says: **Please set the Partner Shared Secret used to verify communications between High Availability, Clusters, and GEO partners. Click on Certificates & Security > Remote Access in the main menu. This secret must be set to the same string on all partners**.

Note: The Partner Shared Secret is in **Certificates & Security > Remote Access** in the regular/shared

Web User Interface (WUI). However, it is in **Local Administration > Remote Access** in the local WUI of a configured HA or cluster unit.

The **Partner Shared Secret** is required to secure communications between partner devices and must be enabled on all High Availability (HA) partners, all LoadMasters in a cluster, and all GEO partners. The **Partner Shared Secret** must be the same on:

- Both units in a HA setup
- All units in a LoadMaster cluster
- All GEO partners
- All remote GEO machines that retrieve Virtual Services from this device

When an incoming shared secret does not match the local **Partner Shared Secret** (including if only one side is providing a shared secret), a warn-level log message is recorded that says **Unauthorized Remote Machine connection from <ClientIPAddress>** and the connection fails.

This secret must have a minimum of 8 and a maximum of 127 characters. The following characters are supported:

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

4

Restore the Software

When performing a software update, the LoadMaster automatically creates a restore point of the current firmware and, provided no changes are made, the restore point can be used. Therefore, when restoring to a previous version there are two options;

- Restore to the previous version – no changes made
- Restore to the previous version – changes made

Refer to the relevant section below for restore instructions.

Related Links

For details, see the following topics:

- Restore the Software – No Changes Made
- Restore the Software – Changes Made
- Restoring Certificates and Private Keys

Restore the Software – No Changes Made

If there have been no further changes to the configuration since the software update, the software can be restored by following the steps below:

1. In the main menu of the LoadMaster WUI, go to **System Configuration > System Administration > Update Software**.



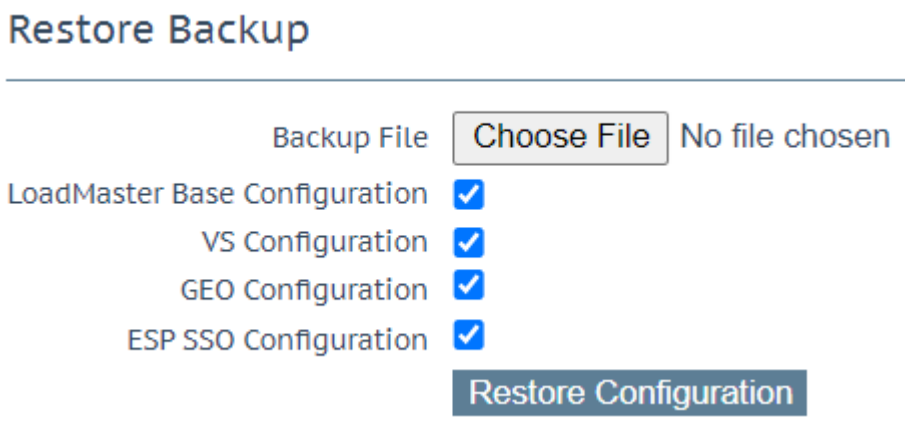
2. Click the **Restore Software** button and click **OK** to confirm.
3. Reboot the LoadMaster.

After the reboot, the LoadMaster is restored to the time before the software update and it is fully operational, as it was at that time.

Restore the Software – Changes Made

If changes have been made and you want to keep those changes, you will need to back up the system by following the steps in the Back Up the System section. Then, after restoring the software (steps in the Restore the Software – No Changes Made section), the backup can be restored by following the steps below:

1. In the main menu of the LoadMaster (WUI), navigate to **System Configuration > System Administration > Backup/Restore**.



2. Click the **Choose File** button.
3. Browse to and select the backup file.

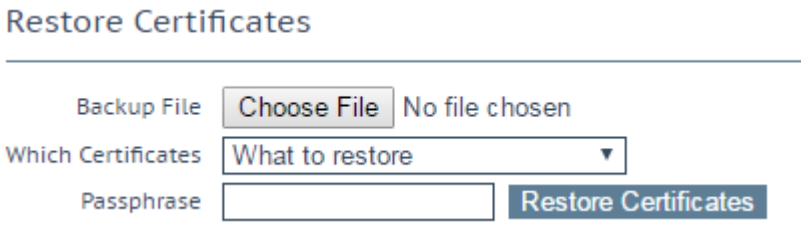
Note: We recommend restoring all settings (check all boxes).

4. Click the **Restore Configuration** button.
5. Click **Reboot**.
6. Click **Continue**.

Restoring Certificates and Private Keys

To restore certificates, follow the instructions below:

1. In the main menu of the LoadMaster WUI, navigate to **Certificates & Security > Backup/Restore Certs.**



2. Click the **Choose File** button. Locate and select the certificate backup file.
3. In the drop-down list select **All VS and Intermediate Certs**.
4. Enter the passphrase assigned to the certificate backup file.
5. Click **Restore Certificates** button.

5

References

Unless otherwise specified, the following documents can be found at https://docs.progress.com/.

LoadMaster Release Notes

Licensing, Feature Description