Progress®
Kemp® LoadMaster®

Deployment Guide Progress ShareFile

Generated on: 12 January 2026

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: Configure the LoadMaster 6

Enable Subnet Originating Requests Globally 6

Enable Check Persist Globally 7

Create the ShareFile Virtual Services 8

Create a ShareFile HTTPS Offloaded Virtual Service 9

Create a ShareFile HTTPS Re-encrypt Virtual Service 11

ShareFile HTTPS Virtual Service Recommended API Settings (optional) 12

Content Switching and Rules 13

Template 14

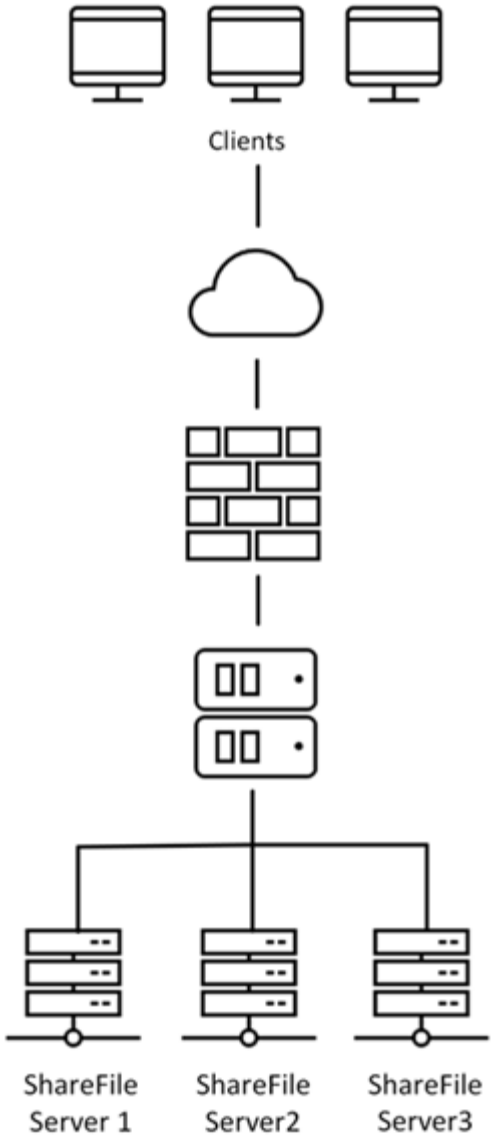
Chapter 3: References 15

1

Introduction

Progress ShareFile is a secure, extensible document collaboration and file-sharing platform developed by Progress Software. Designed for seamless integration with enterprise environments, ShareFile supports a wide range of protocols and services, including secure email, encrypted file transfers, and automated workflows.

The LoadMaster can load balance the ShareFile workload. The LoadMaster offers advanced Layer 4 and Layer 7 server load balancing, SSL Acceleration and a multitude of other advanced Application Delivery Controller (ADC) features. The LoadMaster intelligently and efficiently distributes user traffic among the application servers so that users get the best experience possible.


Clients
ShareFile Server 1
ShareFile Server2
ShareFile Server3

2

Configure the LoadMaster

Refer to the following sections for instructions on how to configure a LoadMaster to load balance the ShareFile workload.

Contents

- Enable Subnet Originating Requests Globally
- Enable Check Persist Globally
- Create the ShareFile Virtual Services
- Content Switching and Rules
- Template

Enable Subnet Originating Requests Globally

It is best practice to enable the **Subnet Originating Requests** option globally.

In a one-armed setup (where the Virtual Service and Real Servers are on the same network/subnet) **Subnet Originating Requests** is usually not needed. However, enabling **Subnet Originating Requests** should not affect the routing in a one-armed setup.

In a two-armed setup where the Virtual Service is on network/subnet A, for example, and the Real Servers are on network B, **Subnet Originating Requests** should be enabled on LoadMasters with firmware version 7.1-16 and above.



When **Subnet Originating Requests** is enabled, the Real Server sees traffic originating from 10.20.20.21 (LoadMaster eth1 address) and responds correctly in most scenarios.

With **Subnet Originating Requests** disabled, the Real Server sees traffic originating from 10.0.0.15 (LoadMaster Virtual Service address on **eth0**) and responds to **eth0** which could cause asymmetric routing.

When **Subnet Originating Requests** is enabled globally, it is automatically enabled on all Virtual Services. If the **Subnet Originating Requests** option is disabled globally, you can choose whether to enable **Subnet Originating Requests** on a per-Virtual Service basis.

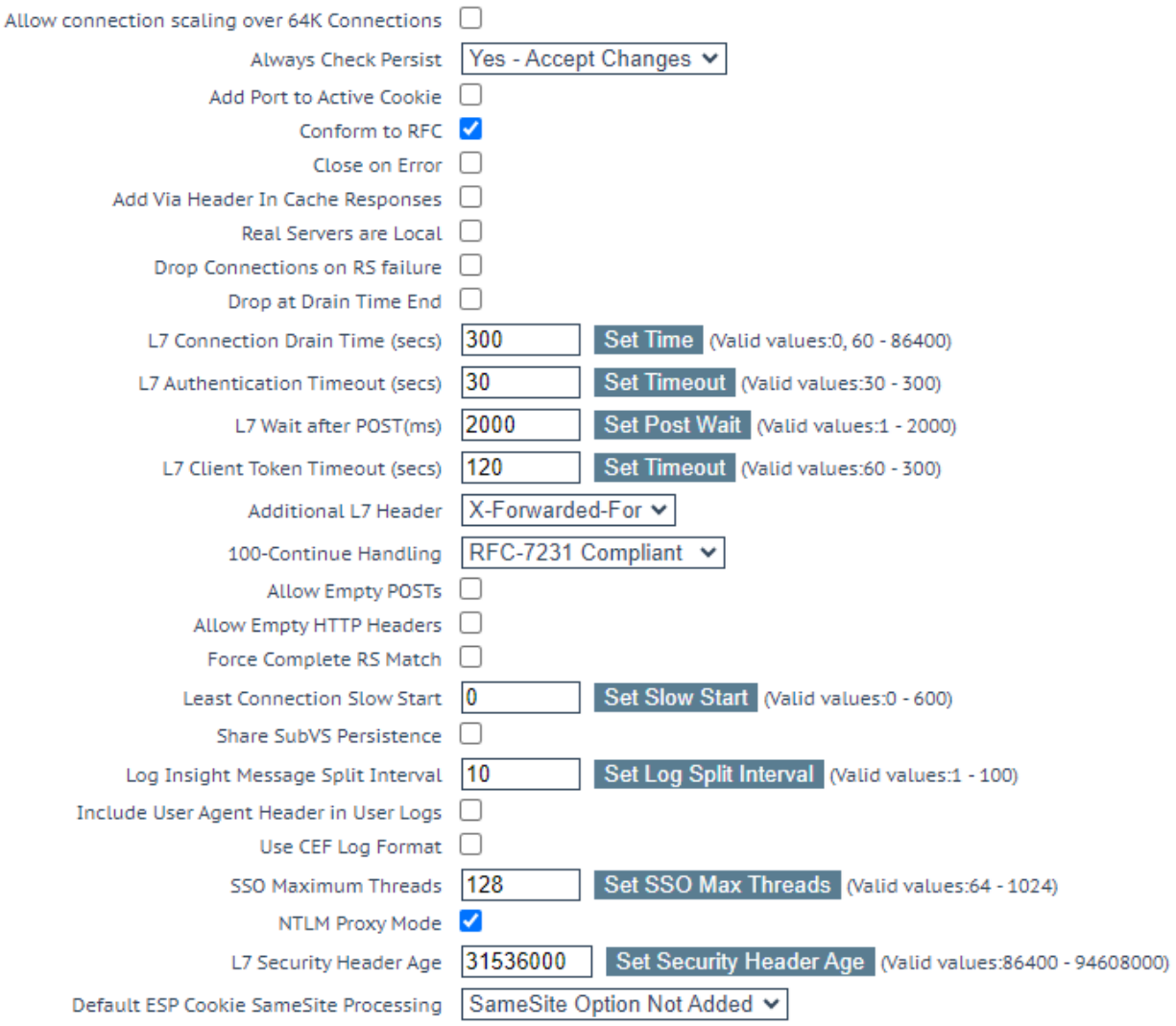
To enable **Subnet Originating Requests** globally, follow the steps below:

1. In the main menu of the LoadMaster User Interface (UI), go to **System Configuration > Miscellaneous Options > Network Options**.
2. Select the **Subnet Originating Requests** check box.

Enable Check Persist Globally

It is recommended that you change the **Always Check Persist** option to **Yes – Accept Changes**. Use the following steps:

1. Go to **System Configuration > Miscellaneous Options > L7 Configuration**.



2. Click the **Always Check Persist** drop-down arrow and select **Yes – Accept Changes**.

Note: The **Always Check Persist** option does not need to be set to **Yes - Accept Changes** if the **Persistence Mode** in the Virtual Service is set to **Active Cookie**.

Create the ShareFile Virtual Services

The following sections describe the recommended settings for the ShareFile Virtual Services.

Note: Progress Kemp developed a template containing our recommended settings for this workload. You can install this template to help create Virtual Services because it automatically populates the settings. You can use the template to easily create the required Virtual Services with the recommended settings. For further details, refer to the following section: Template.

Note: It is not possible to load balance HTTP and HTTPS traffic on the same Virtual Service. Using

---

additional ports is not a solution because these are different protocols. To load balance HTTP and HTTPS traffic, you must create two Virtual Services:

- One for HTTP traffic (normally port 80)
- One for HTTPS traffic (normally port 443)

Contents

- Create a ShareFile HTTPS Offloaded Virtual Service
- Create a ShareFile HTTPS Re-encrypt Virtual Service
- ShareFile HTTPS Virtual Service Recommended API Settings (optional)

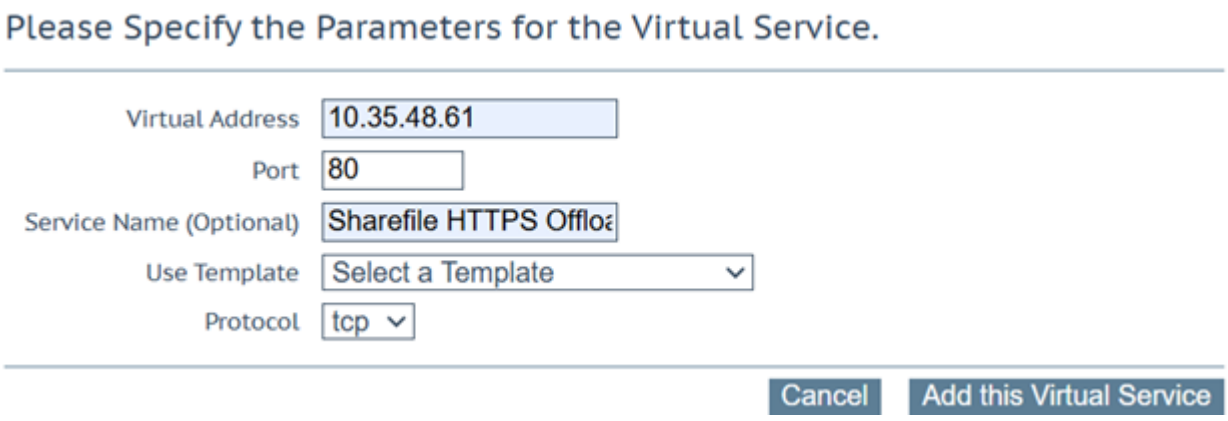
Create a ShareFile HTTPS Offloaded Virtual Service

The SSL offload feature transparently improves the performance of websites that conduct SSL transactions. By offloading CPU-intensive SSL encryption and decryption tasks from the local web server to the appliance, SSL offloading ensures secure delivery of web applications without the performance penalty incurred when the server processes the SSL data. Once the SSL traffic is decrypted, it can be processed by all standard services. The SSL protocol works seamlessly with various types of HTTP and TCP data and provides a secure channel for transactions using such data. To configure SSL, you must first enable it. Then, you configure HTTP or TCP services and an SSL Virtual Service on the LoadMaster, and bind the services to the Virtual Service. You must also add a certificate-key pair and bind it to the SSL Virtual Service. If you use Outlook Web Access servers, you must create an action to enable SSL support and a policy to apply the action. An SSL Virtual Service intercepts incoming encrypted traffic and decrypts it by using a negotiated algorithm. The SSL Virtual Service then forwards the decrypted data to the other entities on the appliance for appropriate processing. For further details on SSL offloading, refer to the SSL Accelerated Services Feature Description.

Intermediate certificates may be required. For further details, refer to the following page: Intermediate Certificates.

The following are the steps involved and the recommended settings to configure the ShareFile HTTPS Offloaded Virtual Service:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.



2. Type a valid **Virtual Address**.
3. Type **443** as the **Port**.
4. Enter a recognizable **Service Name**, such as **ShareFile HTTPS Offloaded**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

WUI Section	WUI Field Name	WUI Field Value
	Port	443
	Protocol	tcp
Basic Properties	Service Type	HTTP-HTTP/2-HTTPS
Standard Options	Transparency	Disabled
	Subnet Originating Requests	Enabled
	Persistence Options	None
	Scheduling Method	least connection
	Idle Connection Timeout	660 (Default)
SSL Properties	SSL Acceleration	Enabled
	Supported Protocols	TLS1.1, TLS1.2, and TLS1.3 (Enabled)
	Cipher Set	BestPractices
	TLS1.3 Ciphersets	TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, and TLS_AES_128_GCM_SHA256

Note: As of version 6 of ShareFile, TLS 1.3 is not in use.

7. Add the Real Servers:
8. Expand the **Real Servers** section.
9. Click **Add New**.
    1. Enter the address of the relevant Real Server.
    2. Complete the other fields as required.
    3. Click **Add this Real Server** then click **OK** to the pop-up message.
    4. Repeat the steps above to add more Real Servers as needed, based on your environment.

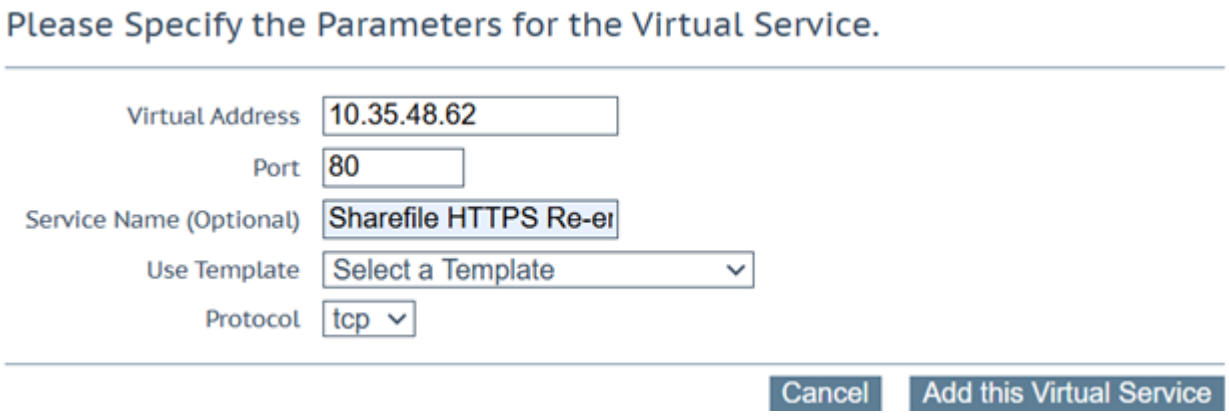
Create a ShareFile HTTPS Offloaded Redirect Virtual Service

Clicking **Add HTTP Redirector** (in **Advanced Properties**) automatically creates a port 80 redirect Virtual Service. This is optional, but the purpose of this Virtual Service is to redirect any clients who have connected using HTTP to the HTTPS Virtual Service. We also recommend changing the **Persistence Mode** to **None**.

Create a ShareFile HTTPS Re-encrypt Virtual Service

The following are the steps involved and the recommended settings to configure the ShareFile HTTPS Re-encrypt Virtual Service:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.



2. Type a valid **Virtual Address**.
3. Type **443** as the **Port**.
4. Enter a recognizable **Service Name**, such as **ShareFile HTTPS Re-encrypted**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

WUI Section	WUI Field Name	WUI Field Value
	Port	443
	Protocol	tcp
Basic Properties	Service Type	HTTP-HTTP/2-HTTPS
Standard Options	Transparency	Disabled
	Subnet Originating Requests	Enabled
	Persistence Options	None
	Scheduling Method	least connection
	Idle Connection Timeout	660 (Default)
SSL Properties	SSL Acceleration	Enabled
	Reencrypt	Enabled
	Supported Protocols	TLS1.1, TLS1.2, and TLS1.3 (Enabled)
	Cipher Set	BestPractices

WUI Section	WUI Field Name	WUI Field Value
	TLS1.3 Ciphersets	TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, and TLS_AES_128_GCM_SHA256

Note: As of version 6 of ShareFile, TLS 1.3 is not in use.

7. Add the Real Servers:
8. Expand the **Real Servers** section.
9. Click **Add New**.
    1. Enter the address of the relevant Real Server.
    2. Complete the other fields as required.
    3. Click **Add this Real Server** then click **OK** to the pop-up message.
    4. Repeat the steps above to add more Real Servers as needed, based on your environment.

Create a ShareFile HTTPS Re-encrypted Redirect Virtual Service

Clicking **Add HTTP Redirector** (in **Advanced Properties**) automatically creates a port 80 redirect Virtual Service. This is optional, but the purpose of this Virtual Service is to redirect any clients who have connected using HTTP to the HTTPS Virtual Service. We also recommend changing the **Persistence Mode** to **None**.

ShareFile HTTPS Virtual Service Recommended API Settings (optional)

These tables outline the Application Programming Interface (API) parameters and values set using the Progress Kemp application template. You can use these settings with scripts and automation tools.

HTTPS Offloaded Virtual Service

Recommended settings to configure the ShareFile HTTPS Offloaded Virtual Service using API:

API Parameter	API Value
port	443
prot	tcp
VStype	http
Transparent	0
SubnetOriginating	1
Persist	none
Schedule	lc
Idletime	660

API Parameter	API Value
SSLAcceleration	1
TLSType	2
CipherSet	BestPractices
Tls13CipherSet	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256

HTTPS Re-encrypt Virtual Service

Recommended settings to configure the ShareFile HTTPS Re-encrypt Virtual Service using API:

API Parameter	API Value
port	443
prot	tcp
VStype	http
Transparent	0
SubnetOriginating	1
Persist	none
Schedule	lc
Idletime	660
SSLAcceleration	1
SSLReencrypt	1
TLSType	2
CipherSet	BestPractices
Tls13CipherSet	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256

Content Switching and Rules

The LoadMaster supports content switching, which is sometimes referred to as URL switching. This enables the LoadMaster to direct specific requests to specific Real Servers based on the contents of the requested URL. For further details, refer to the Content Rules Feature Description.

Template

Progress Kemp has developed a template containing our recommended settings for this workload. You can install this template to help create Virtual Services (VSs) because it automatically populates the settings. You can use the template to easily create the required VSs with the recommended settings. For some workloads, additional manual steps may be required such as assigning a certificate or applying port following. These steps are covered in the document, if needed.

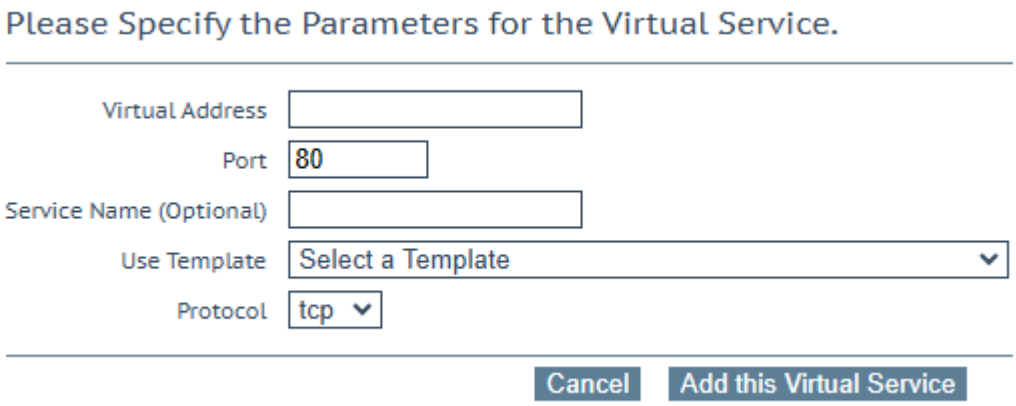
You can remove templates after use and this will not affect deployed services. If needed, you can make changes to any of the VS settings after using the template.

Download released templates from the following page: LoadMaster Templates.

You can import templates to the LoadMaster through the **Manage Templates** page under **Virtual Services** in the main menu of the LoadMaster User Interface (UI).

Click **Choose File**, select the template to install and click **Add New Template**. The template will then be available to select when you are adding a new Virtual Service.

To begin the process of creating a new Virtual Service, click **Virtual Services** and **Add New** in the main menu.



This opens the Virtual Service parameters page which prompts to enter the Virtual IP (VIP) address of the Virtual Service, the port, and the name to give the service and the protocol. You can select a previously-imported template in the **Use Template** drop-down list.

For more information and steps on how to use templates, refer to the Virtual Services and Templates, Feature Description.

3

References

For further details on Virtual Services and Templates, refer to the following document:

Virtual Services and Templates Feature Description