Progress®
Kemp® LoadMaster®

Deployment Guide IIS

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

Document Purpose 4

Intended Audience 5

Chapter 2: Template 6

Chapter 3: Architecture 7

Chapter 4: Configure the LoadMaster 9

Enable Subnet Originating Requests Globally 9

Enable Check Persist Globally 10

Create the IIS Virtual Services 11

Create an IIS HTTP Virtual Service 12

Create an IIS HTTPS Virtual Service 13

Create an IIS HTTPS Offloaded Virtual Service 14

Create an IIS HTTPS Re-encrypt Virtual Service 16

Create the IIS and WAF Virtual Services 18

Create an IIS HTTP and WAF Virtual Service 18

Create an IIS HTTPS Offloaded and WAF Virtual Service 20

Create an IIS HTTPS Re-encrypt and WAF Virtual Service 22

Chapter 5: References 26

1

Introduction

Internet Information Services (IIS, formerly Internet Information Server) is an extensible web server created by Microsoft for use with Windows NT family. IIS supports HTTP, HTTPS, FTP, FTPS, SMTP and NNTP. It has been an integral part of the Windows NT family since Windows NT 4.0, though it may be absent from some editions (for example, Windows XP Home edition), and is not active by default.

The LoadMaster is used to load balance the IIS 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.

Related Links

For details, see the following topics:

- Document Purpose
- Intended Audience

Document Purpose

This document provides the recommended LoadMaster settings used when load balancing the IIS workload. The Progress Kemp Support Team is available to provide solutions for scenarios not explicitly defined. For further details, refer to the: LoadMaster Support and Learning Hub.

Intended Audience

This document is intended to be read by anyone who is interested in configuring the LoadMaster to optimize the IIS server.

2

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.

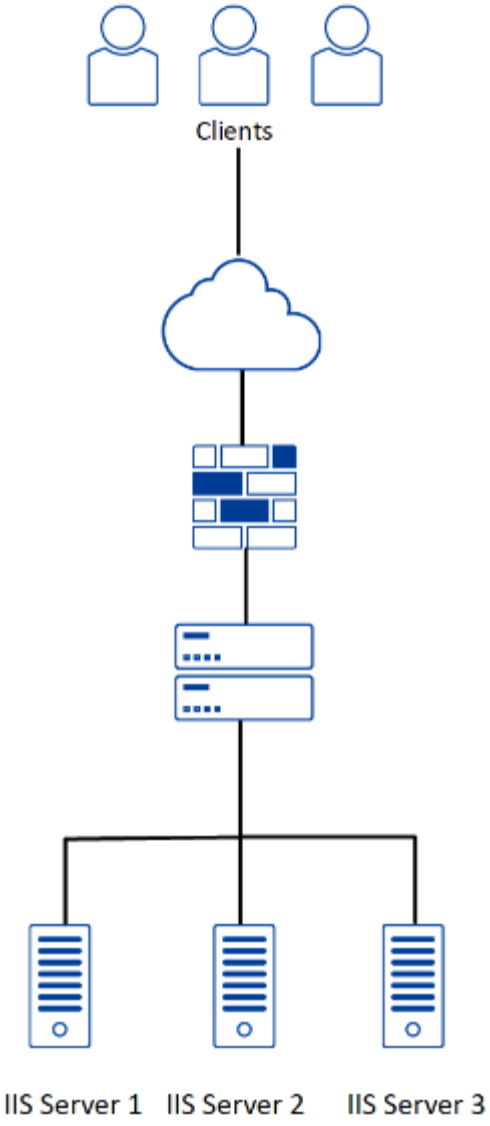
You can remove templates after use and this will not affect deployed services. If needed, you can make changes to any of the VS settings after using the template.

Download released templates from the following page: LoadMaster Templates.

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

3

Architecture


Clients
IIS Server 1
IIS Server 2
IIS Server 3

4

Configure the LoadMaster

The deployed IIS environment determines which of the following setups is used.

Related Links

For details, see the following topics:

- Enable Subnet Originating Requests Globally
- Enable Check Persist Globally
- Create the IIS Virtual Services
- Create the IIS and WAF Virtual Services

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.

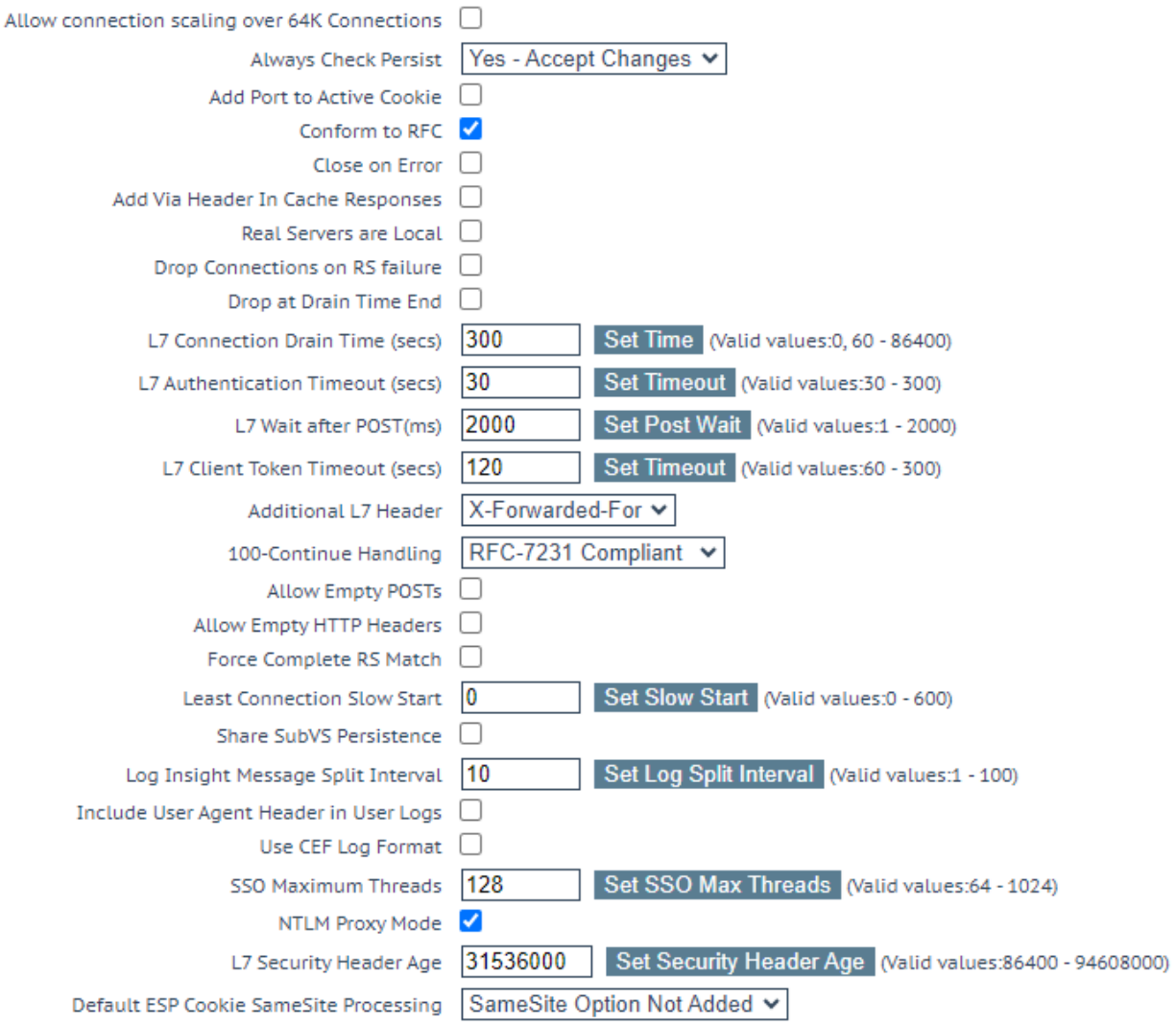
To enable **Subnet Originating Requests** globally, follow the steps below:

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: **Enable Check Persist** is not required if active cookie is enabled.

Create the IIS Virtual Services

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

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:

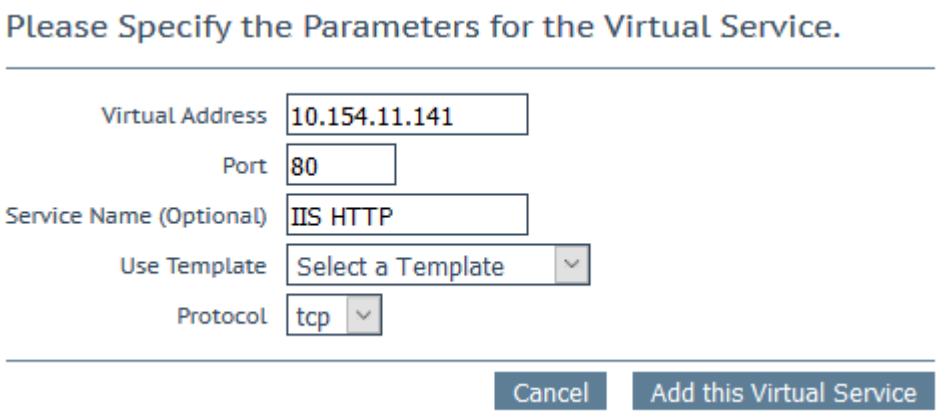
- One for HTTP traffic (normally port 80)

- One for HTTPS traffic (normally port 443)

Create an IIS HTTP Virtual Service

The following are the steps involved and the recommended settings to configure the IIS Virtual Service:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.



2. Type a valid **Virtual Address**.
3. Type **80** as the **Port**.
4. Enter a recognizable **Service Name**, such as **IIS HTTP Virtual Service**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value	Comment
Standard Options	Timeout	1 Hour	
	Cookie name	JSESSIONID	
	Scheduling Method	least connection	

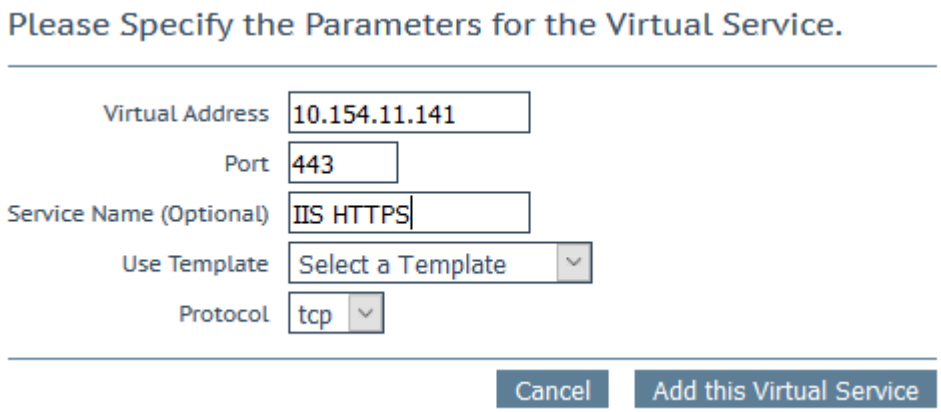
7. Add the Real Servers:
8. Expand the **Real Servers** section.
9. Click **Add New**.
   1. Enter the address of the relevant Real Server.
   2. Complete the other fields as required.

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 an IIS HTTPS Virtual Service

The following are the steps involved and the recommended settings to configure the IIS HTTPS 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 **IIS HTTPS Virtual Service**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value	Comment
Standard Options	Persistence Mode	Source IP Address	
	Timeout	1 Hour	
	Scheduling Method	least connection	
	Idle Connection Timeout	900	
Advanced Properties	Add a Port 80 Redirector	https://%h%s	Click **Add HTTP**

Section	Option	Value	Comment
	VS		**Redirector**. This automatically creates a redirect on port 80.
Real Servers	URL	/	

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.

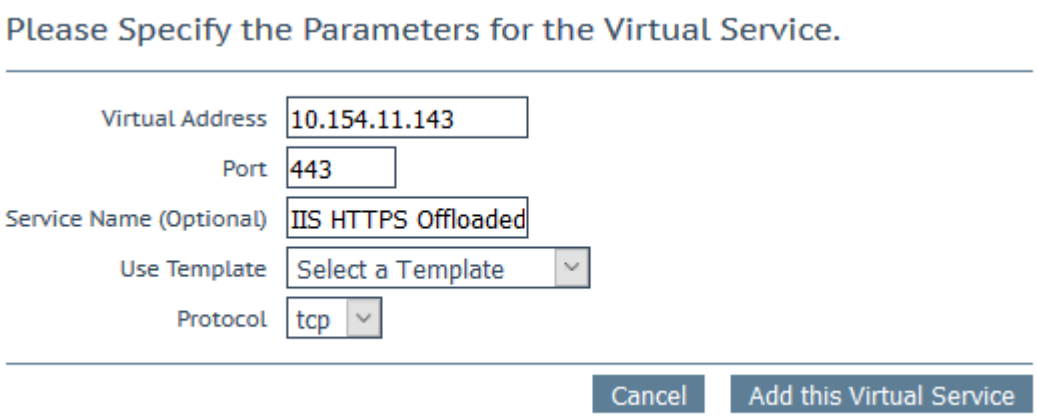
Create an IIS HTTPS Redirect Virtual Service

Clicking the **Add HTTP Redirector** button 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 **Real Server Check Method** and **Persistence Mode** to **None**.

Create an IIS HTTPS Offloaded Virtual Service

The following are the steps involved and the recommended settings to configure the IIS 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 **IIS HTTPS Offloaded HTTP** Virtual Service.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value	Comment
Standard Options	Persistence Mode	Active Cookie	SSL Acceleration must be enabled before you can select Active Cookie as a Persistence Mode.
	Timeout	1 Hour	
	Scheduling Method	least connection	
	Idle Connection Timeout	900	
SSL Properties	SSL Acceleration	Enabled	
	Cipher Set	BestPractices	
Advanced Properties	Add a Port 80 Redirector VS	https://%h%s	Click **Add HTTP Redirector**. This automatically creates a redirect on port 80.
Real Servers	Real Server Check Method	HTTPS Protocol	
	URL	/	

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.

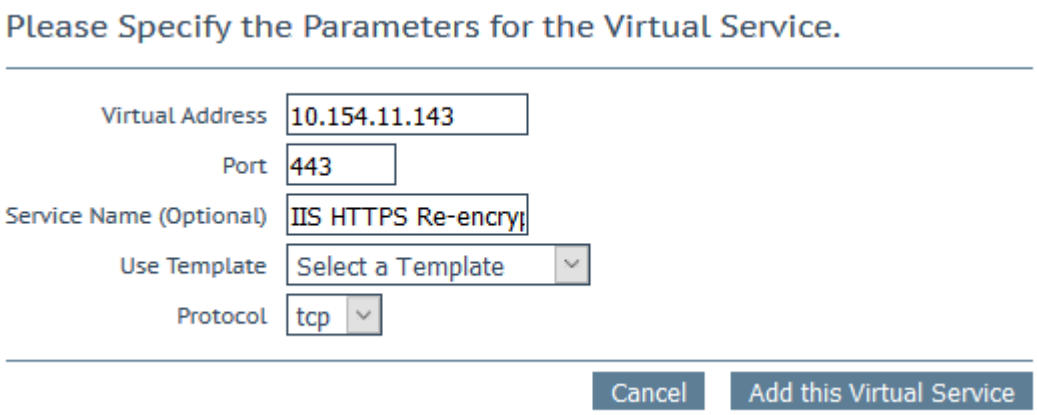
Create an IIS HTTPS Offloaded Redirect Virtual Service

Clicking the **Add HTTP Redirector** button 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 **Real Server Check Method** and **Persistence Mode** to **None**.

Create an IIS HTTPS Re-encrypt Virtual Service

The following are the steps involved and the recommended settings to configure the IIS 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 IIS HTTPS Re-encrypt Virtual Service.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value	Comment
Standard Options	Persistence Mode	Active Cookie	SSL Acceleration must be enabled before you can select Active Cookie as a Persistence Mode.

Section	Option	Value	Comment
	Timeout	1 Hour	
	Cookie name	JSESSSIONID	
	Scheduling Method	least connection	
	Idle Connection Timeout	900	
SSL Properties	SSL Acceleration	Enabled	
	Reencrypt	Enabled	
	Cipher Set	Best Practices	
Advanced Properties	Add a Port 80 Redirector VS	https://%h%s	Click **Add HTTP Redirector**. This automatically creates a redirect on port 80.
Real Servers	URL	/	

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 an IIS HTTPS Re-encrypt Redirect Virtual Service

Clicking the **Add HTTP Redirector** button 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 **Real Server Check Method** and **Persistence Mode** to **None**.

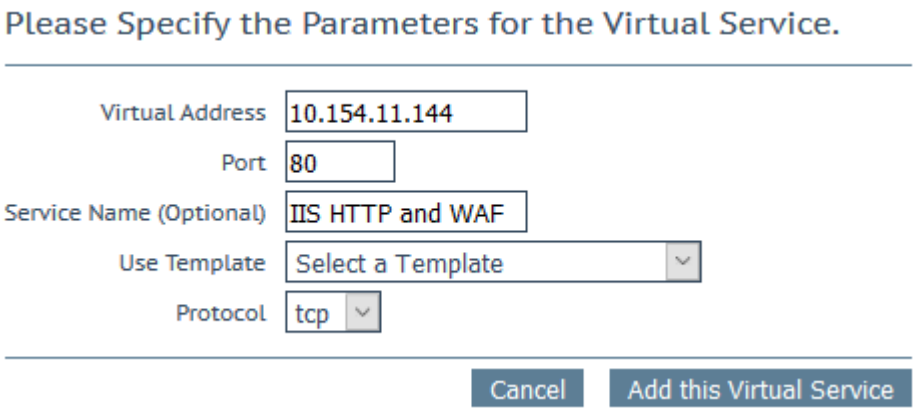
Create the IIS and WAF Virtual Services

The following sections describe the recommended settings for the IIS and WAF Virtual Services.

Create an IIS HTTP and WAF Virtual Service

The following are the steps involved and the recommended settings to configure the IIS HTTP WAF 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 **80** as the **Port**.
4. Enter a recognizable **Service Name**, such as IIS HTTP WAF Virtual Service.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value
Standard Options	Persistence Mode	Source IP Address
	Timeout	6 Minutes
	Scheduling Method	least connection
WAF Options	Enabled	Yes

Section	Option	Value
	Default Operation	Block Mode
	Audit mode	Audit Relevant
	Enabled Rules	owasp_protocol_violations
		owasp_protocol_anomalies
		owasp_request_limits
		owasp_bad_robots
		owasp_generic_attacks
		owasp_xss_attacks
		owasp trojans
		owasp_common_exceptions
	Application Specific	iis_attacks
Real Servers	Real Server Check Method	HTTPS Protocol
Real Servers	URL	/

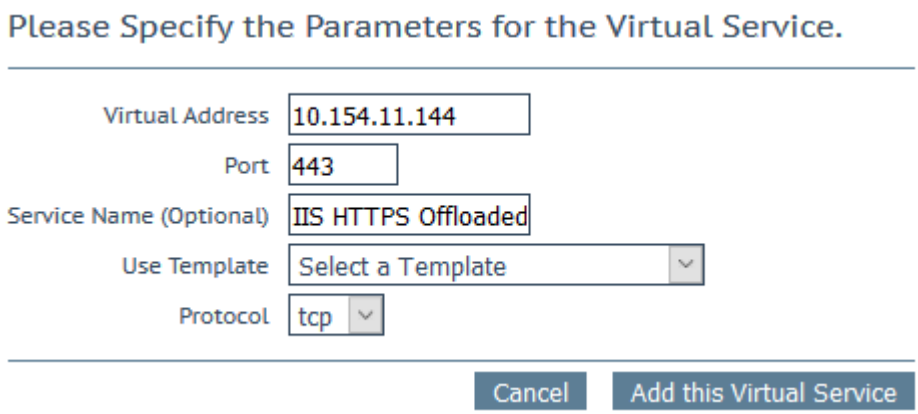
7. Add the Real Servers:
8. Expand the **Real Servers** section.
9. Click **Add New**.
    1. Enter the address of the relevant Real Server.

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 an IIS HTTPS Offloaded and WAF Virtual Service

The following are the steps involved and the recommended settings to configure the IIS HTTPS Offloaded and WAF 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 IIS HTTPS Offloaded WAF Virtual Service.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
Standard Options	Persistence Mode	Source IP Address	
	Timeout	6 Minutes	
	Scheduling Method	least connection	
	Idle Connection Timeout	900	

Section	Option	Value	Comments
SSL Properties	Enabled	Selected	
	Cipher Set	Best Practices	
Advanced Properties	Add a Port 80 Redirector VS	https://%h%s	Click **Add HTTP Redirector**. This automatically creates a redirect on port 80.
WAF Options	Enabled	Yes	
	Default Operation	Block Mode	
	Audit Mode	Audit Relevant	
	Enabled Rules	owasp_protocol_violations	
		owasp_protocol_anomalies	
		owasp_request_limits	
		owasp_bad_robots	
		owasp_generic_attacks	
		owasp_xss_attacks	
		owasp_trojans	

Section	Option	Value	Comments
		owasp_common_exceptions	
	Application Specific	iis_attacks	
Real Servers	Real Server Check Method	HTTPS Protocol	
Real Servers	URL	/	

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.

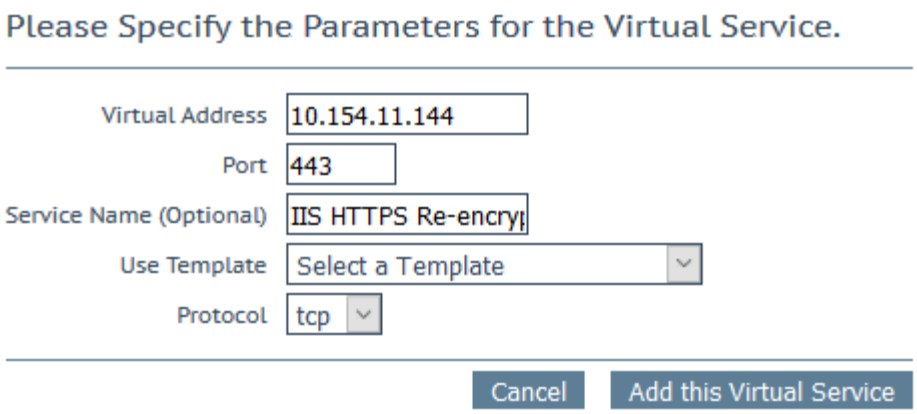
Create an IIS HTTPS Offloaded and WAF Redirect Virtual Service

Clicking the **Add HTTP Redirector** button 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 **Real Server Check Method** and **Persistence Mode** to **None**.

Create an IIS HTTPS Re-encrypt and WAF Virtual Service

The following are the steps involved and the recommended settings to configure the IIS HTTPS Re-encrypt and WAF 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 IIS HTTPS Re-encrypt and WAF Virtual Service.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
Standard Options	Persistence Mode	Source IP Address	
	Timeout	6 Minutes	
	Scheduling Method	least connection	
	Idle Connection Timeout	900	
SSL Properties	Enabled	Selected	
	Reencrypt	Selected	
	Cipher Set	Best Practices	
Advanced Properties	Add a Port 80 Redirector	https://%h%s	Click **Add HTTP**

Section	Option	Value	Comments
	VS		**Redirector**. This automatically creates a redirect on port 80.
WAF Options	Enabled	Yes	
	Default Operation	Block Mode	
	Audit mode	Audit Relevant	
	Enabled Rules	owasp_protocol_violations	
		owasp_protocol_anomolies	
		owasp_request_limits	
		owasp_bad_robots	
		owasp_generic_attacks	
		owasp_xss_attacks	
		owasp_trojans	
		owasp_common_exceptions	
	Application Specific	iis_attacks	

Section	Option	Value	Comments
Real Servers	Real Server Check Method	HTTPS Protocol	
Real Servers	URL	/	

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 an IIS HTTPS Re-encrypt and WAF Redirect Virtual Service

Clicking the **Add HTTP Redirector** button 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 **Real Server Check Method** and **Persistence Mode** to **None**.

5

References

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

Virtual Services and Templates, Feature Description