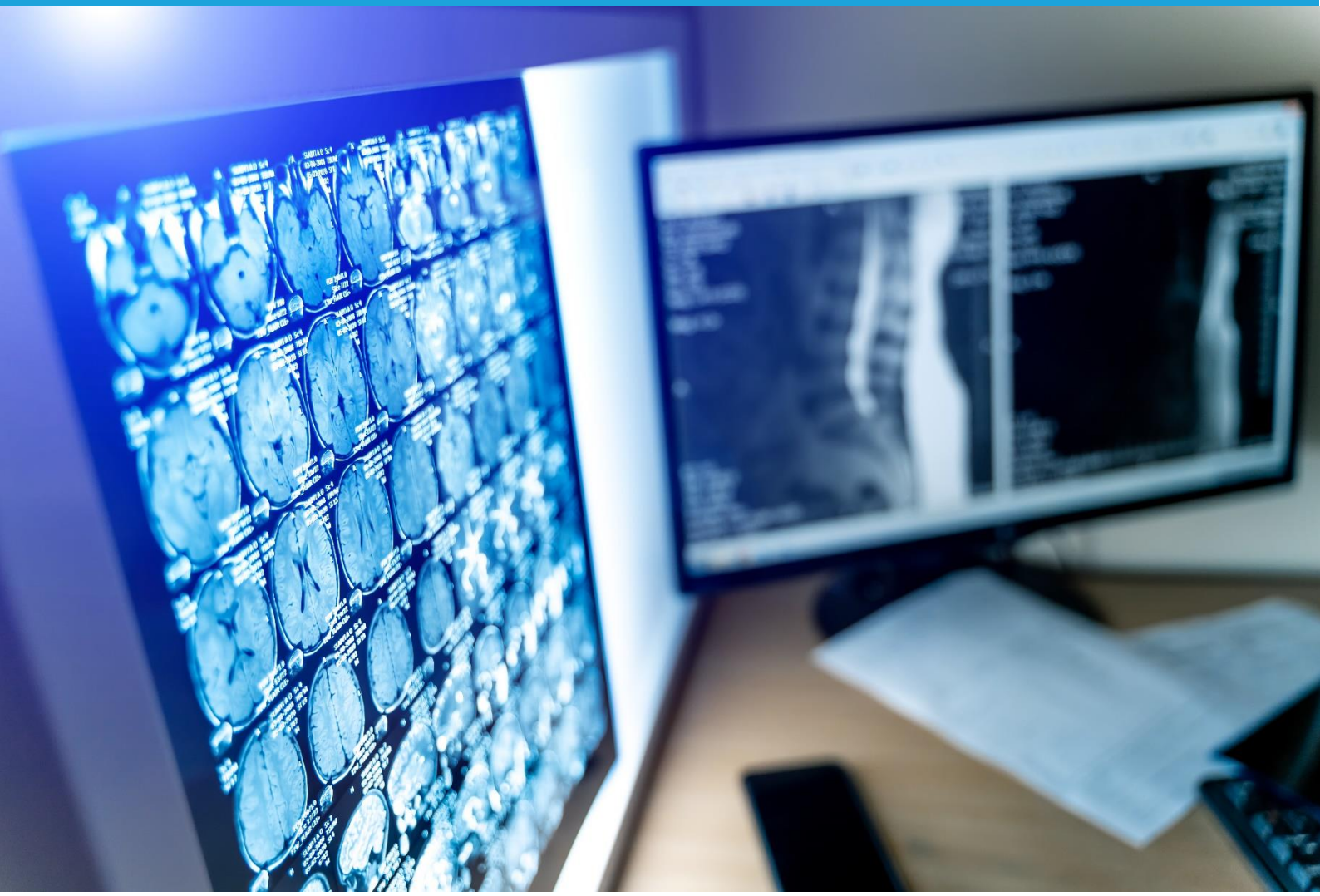


AGFA IMAGING EXCHANGE

AN EDGENEXUS ADC DEPLOYMENT GUIDE

EDGENEXUS

Contents

Document Properties

Document Number: 2.0.9.14.23.17.09

Document Creation Date: September 7, 2023

Document Last Edited: September 14, 2023

Document Author: Jay Savoor

Document Last Edited by:

Document Referral: EdgeADC - Version All Versions

Document Disclaimer

Screenshots and graphics in this manual may differ slightly from your product due to your product release version differences. Edgenexus ensures that they make every reasonable effort to ensure that the information in this document is complete and accurate. However, Edgenexus assumes no liability for any errors. Edgenexus makes changes and corrections to the information in this document in future releases when the need arises.

Copyrights

Trademarks

The Edgenexus logo, Edgenexus, EdgeADC, EdgWAF, EdgeGSLB, EdgeDNS are all trademarks or registered trademarks of Edgenexus Limited. All other trademarks are the properties of their respective owners and are acknowledged.

Edgenexus Support

If you have any technical questions regarding this product, please raise a support ticket at: support@edgenexus.io

Introduction

This EdgeADC (ADC) application deployment guide is intended for persons administering the Agfa Imaging Exchange and its load balancing. This document contains specific general suggestions and guidance, which may or may not be relevant for use within your organization.

Agfa HealthCare's Enterprise Imaging Exchange

Overview

The Enterprise Imaging Exchange is a platform designed to facilitate the secure sharing of medical images and associated data across different healthcare systems and institutions. It acts as a bridge between disparate PACS (Picture Archiving and Communication System) and other imaging systems to allow for a smoother transfer and consolidation of medical imaging data.

Key Features:

- **Secure Image Transfer:** The platform ensures that all image transfers are compliant with healthcare security standards, ensuring patient data protection during transmission.
- **Interoperability:** Agfa's Enterprise Imaging Exchange is built to be interoperable, working seamlessly with various PACS systems, EMRs (Electronic Medical Records), and other healthcare IT infrastructure. This interoperability is crucial for a more integrated and connected healthcare environment.
- **Web-based Access:** Clinicians and healthcare professionals can access the platform via web browsers, ensuring that critical patient imaging data is available when and where it is needed without requiring specialized software installations.
- **Workflow Integration:** The solution is not just about image sharing but also integrates with workflow solutions to help route images to the appropriate stakeholders, improving turnaround times and patient care.
- **Scalability:** The platform is designed to cater to both small healthcare setups and large multi-institutional networks, making it a flexible solution for various healthcare environments.

Recommendations

To successfully load balance using the EdgeADC, we recommend the following:

- The ADC is deployed as a pair of appliances in either a virtualization technology, installing it as a virtualized appliance or as a hardware appliance in approved server hardware.
- When external users access the network via the Internet, we recommend that the ADC pair is deployed in the DMZ and the traffic rerouted through the firewall to the LAN zone.
- The ADC's operate in a high-availability (HA) mode when placed in pairs and provide you the level of redundancy and resilience required for mission-critical systems.

The ADC is fully capable of load-balancing your Agfa Imaging Exchange, and this guide explains how to set this up.

Prerequisites for supporting Agfa Imaging Exchange

As usual, it is assumed that the person who is installing and configuring the ADC is familiar with the terminology used within this document and networking in general. We strongly suggest that both the network technician and Agfa Imaging Exchange administrator work in tandem when setting up the load balancing and that this is first done for a sandbox environment before replicating to the production environment.

Further, it is also recommended you follow the below requirements, which are regarded as the minimum:

- The latest ADC firmware should be used
- The Agfa Imaging Exchange should be installed and operational.
- The initial ADC configuration should be done against the Agfa Imaging Exchange sandbox deployment.
- DNS entries for both internal and external access should be configured and working.
- The ADC should be reachable using a web browser and the management IP.

Acronyms used

VIP – Virtual IP
RS – Real Server
ADC – Edgenexus EdgeADC
VS – Virtual Service
RSIP – Real Server IP

Sizing the EdgeADC

The ADC can operate in either physical or virtual deployments. The reverse proxy engine within the ADC is optimized for speed and efficiency. The ADC will use all available threads automatically.

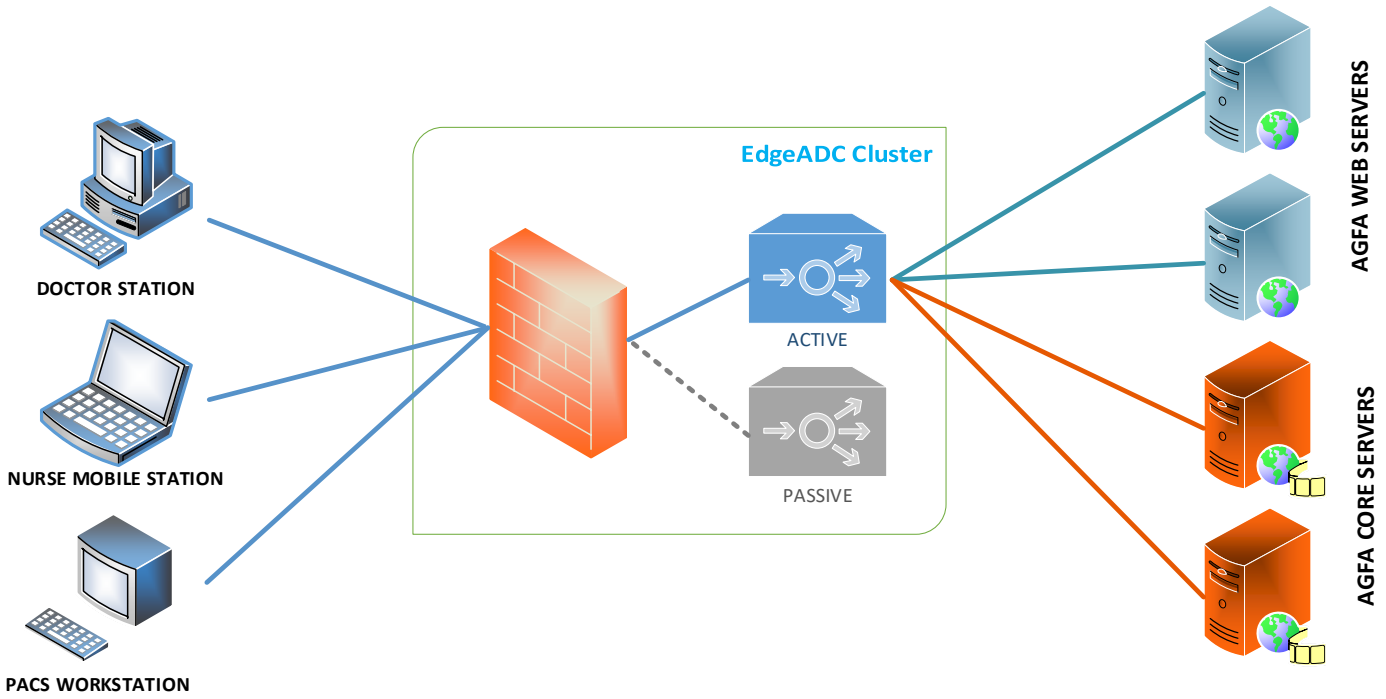
In virtualized environments, we recommend that you set the ADC to 4 vCPU with 8GB RAM, to begin with, and scale up when you need to.

We recommend that you utilize the hardware platforms from our partners in physical environments, with the base system being a quad-core Intel Xeon with 8GB RAM.

In both cases, 50GB of disk storage space should be sufficient.

Deployment Scenarios

Connections to the Agfa Imaging Exchange system occur by clients connecting to the VIP or Virtual IP service created on the ADC. The ADC then load-balances the connections to the nodes configured within the ADC and linked to the VIP. An example diagram is shown below.



Virtual Service Methodologies

There are several methods of configuring the ADC for use with Agfa Imaging Exchange.

Non-Encrypted Port 80 In this mode, the traffic will enter the ADC using an un-encrypted VIP using port 80. It will then be sent onto the nodes using the same means. Therefore, traffic will not be encrypted when using this mode and is not recommended for best practices. ADC service type Layer 4 TCP is used.

SSL Passthrough In this mode, the traffic enters the ADC on port 443 using SSL. Then, the traffic is sent onto the nodes without inspection. ADC service type Layer 4 TCP is used.

SSL Re-Encrypt In this mode, the SSL traffic is terminated in the ADC and then re-encrypted before passing to the nodes. When this mode is chosen, you will need to have the SSL certificate installed on the nodes and install it in the ADC. This mode is the recommended best practice method for security reasons. ADC service type HTTP is used.

SSL Termination This mode allows SSL traffic to be received by the ADC, which then terminates the SSL encryption internally before passing it to the nodes using unencrypted SSL. This mode may not be the desired choice for security reasons. ADC service type HTTP is used.

You will need to choose the one appropriate to your infrastructure.

Persistence Choices

The EdgeADC implementation for load balancing the Agfa Imaging Exchange requires session persistence to be used for certain virtual services.

JSESSION Persistence

JSESSIONID is a **cookie** used in Java web applications to track a user's session. It enables the server to associate data, like user authentication status, with a particular client.

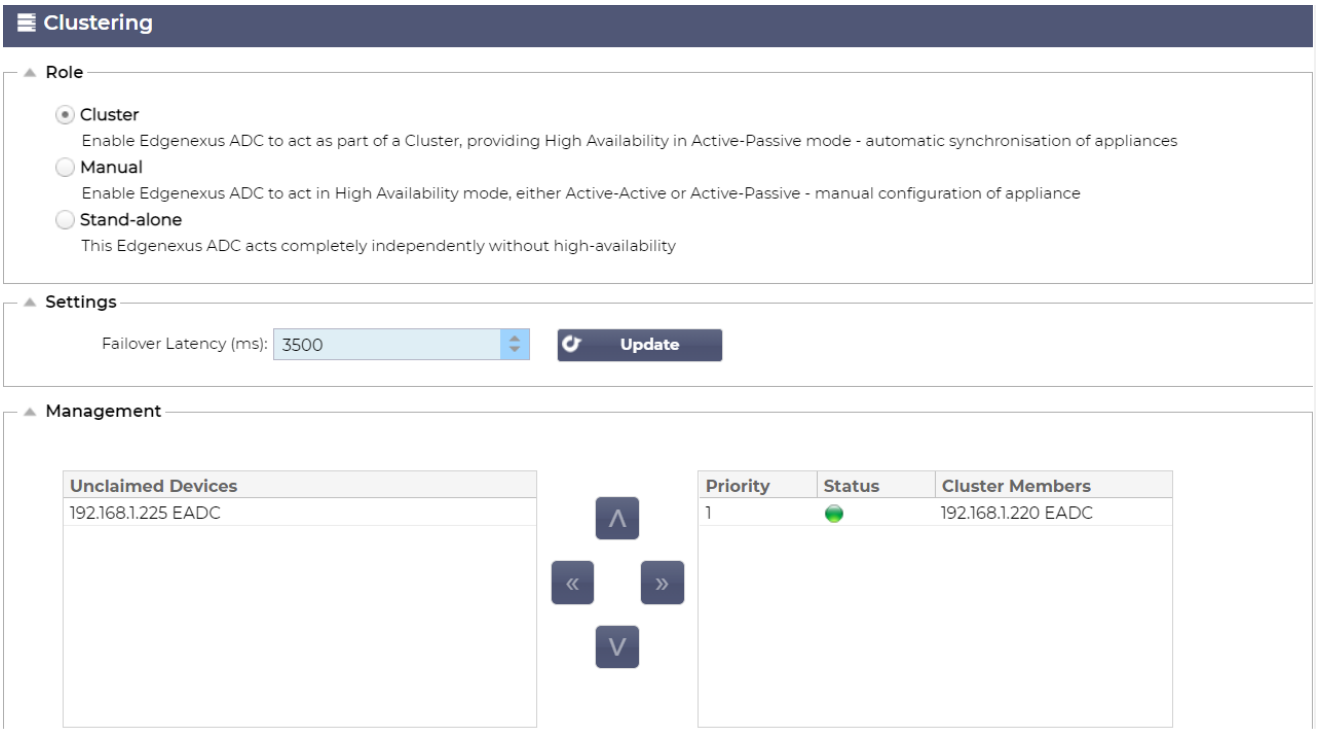
JSESSIONID Persistence refers to mechanisms that allow for the session information (not just the JSESSIONID cookie itself, but the actual session data on the server side) to be stored and retrieved across multiple server instances or server restarts.

The following pages will take you through the VIP configuration. Please take care to configure correctly to avoid issues in operations.

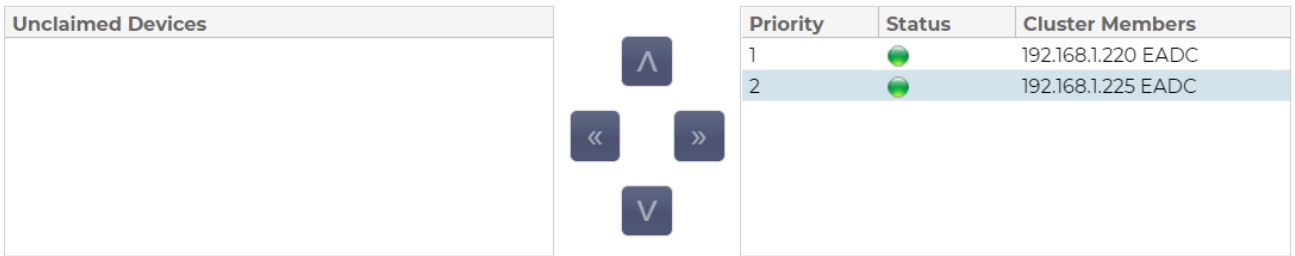
Clustering the EdgeADC

The EdgeADC can operate as a stand-alone appliance, and it is incredibly reliable. However, in terms of best practice, we must accept that it is as critical as the servers it is load balancing, and we would therefore recommend placing it in a cluster.

- First, stand up a second EdgeADC in the same subnet as the primary.
- Once you have licensed it logon to your Primary EdgeADC
- Proceed to System > Clustering
- You should see the page as below.



- You will notice that there are two panels within the Management panel. On the left is the Unclaimed panel. On the right is the Cluster showing the cluster members, their priority, and status.
- In between the two panels is a cluster of arrow buttons.
- Click on the EdgeADC that is in the Unclaimed Panel and click the RIGHT arrow button.
- This action moved the unclaimed EdgeADC into the cluster.
- Immediately it is moved across; the Primary will replicate its settings, including VIPs to the secondary. Note that any apps you have added to the Primary will not be replicated to the Secondary – examples are WAF, GSLB, etc.
- After clustering, the Management panel should look like the one below.



The Agfa Web Server flightPATH Rule

In this document, we will be showing the techniques used for load balancing three web servers. You may have more than three, or perhaps just two, but the principle is the same and can be used for any number of web servers being load balanced.

The first thing to note when load balancing the fronting web servers is that you will need to define some rules using flightPATH that will ensure that traffic is directed to the appropriate web server in a consistent manner.

For the purposes of this demo, we will assume there are three Real Servers, and they have each an allocated Hash Value of A101794, A101795, and A101796.

Defining the Agfa Health flightPATH Rule

FlightPATH is a traffic management technology developed by Edgenexus, and is intended to allow rules that are implemented without the need for any coding knowledge.

You will require **one** rule per Real Server (Agfa Web Server) being load balanced, and this will ensure that the requests are directed to the appropriate Real Server.

Each Agfa Web Server request uses a specific hash code specified within the URL being used to address it. For example, the URL could look something like this.

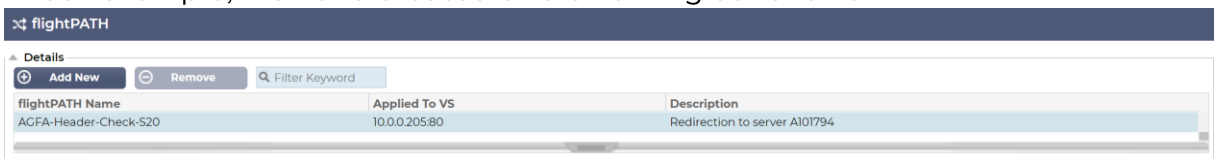
https://agfawebserver.myhospital.com/patient/A101794/surgical

This is a ficticious example, but the key element that determines what happens is the value A101794. This is the hash value and corresponds to a particular web server in the Agfa infrastructure.

Creating the Rule

The first step is to create the flightPATH rule.

- Navigate to Library > flightPATH > Details
- You will see the flightPATH page in the right panel
- Click Add New
- This will create a new flightPATH rule and place the cursor in the flightPATH Name field.
- Add an appropriate name, taking into account that there will be several rules, all doing a similar thing.
- Also, add an appropriate description entry. You can see that we have put an appropriate description so others can understand what the rule does.
- In our example, we have created a rule naming as follows:



- The Applied to VS will be automatically filled in once you apply to rule to a Virtual Service.
- Once you have finished, click the Update button.

Creating the Condition

The Conditions section, located below the Details section and allows the creation of conditions that are expressed as Boolean AND.

- Click the Add New button
- The cursor will be placed in the empty field for selection of the Condition. This is a dropdown menu of predefined conditions, as well as a text field for manual entry of applicable field values (see the admin guide).
- Select the value Path from the dropdown.
- Next, select the value Does from the dropdown in the Sense column.
- Select the value Contain from the Check column dropdown
- Type in the value provided to you by Agfa or your system administrator, but in our case we will use A101794.
- Click the Update button.

The condition is now added, and will check to see if the PATH CONTAIN A101794 = TRUE.

Creating the Evaluation Variables

The next and very important task is to create the variables that will be used to form the target path. The task is to essentially detect the Hash Value, and remove it from the PATH.

So, the original path:

https://agfawebserver.myhospital.com/patient/A101794**/surgical**

is sent onto the server as:

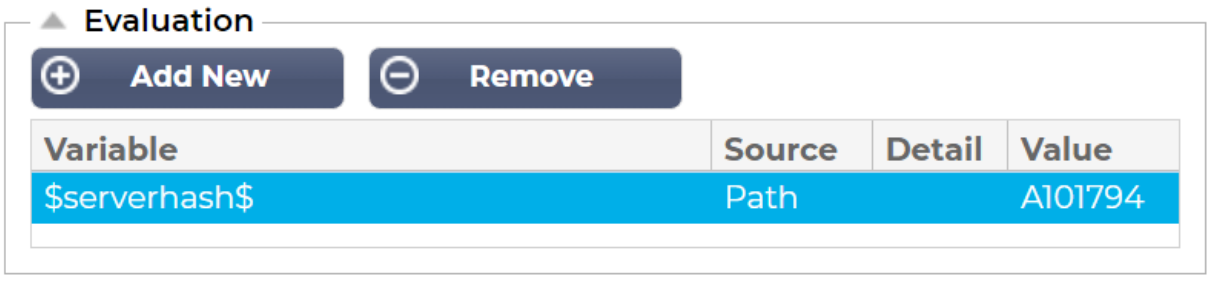
https://agfawebserver.myhospital.com/patient/surgical

We will use the Evaluation section located under Condition to define the variables.

$serverhash$

- Select Add New
- In the Variable column enter **$serverhash$**
- In the Source column select **Path**
- In the Value column enter the **Server Hash** value appropriate for Real Server 1.

In our example, shown below, the Server Hash value is A101794.

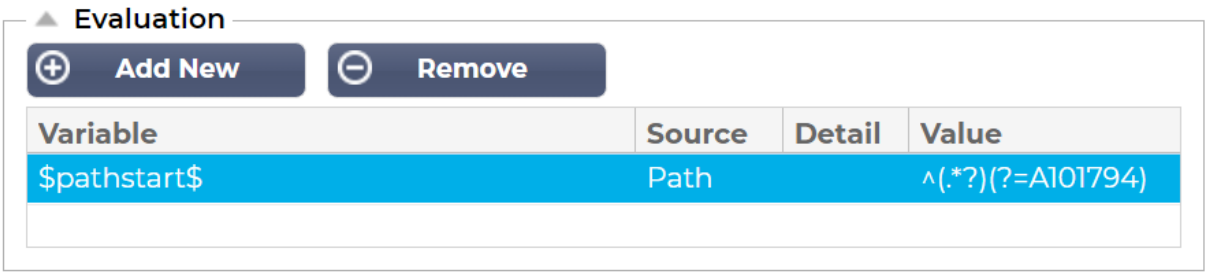


$pathstart$

- Select Add new
- In the Variable column enter **$pathstart$**
- In the Source column select **Path**

- In the Value column enter the following: ^(.*?)(?=<Server Hash>)
  where you will replace **<Server Hash>** with the appropriate Server Hash value for your server

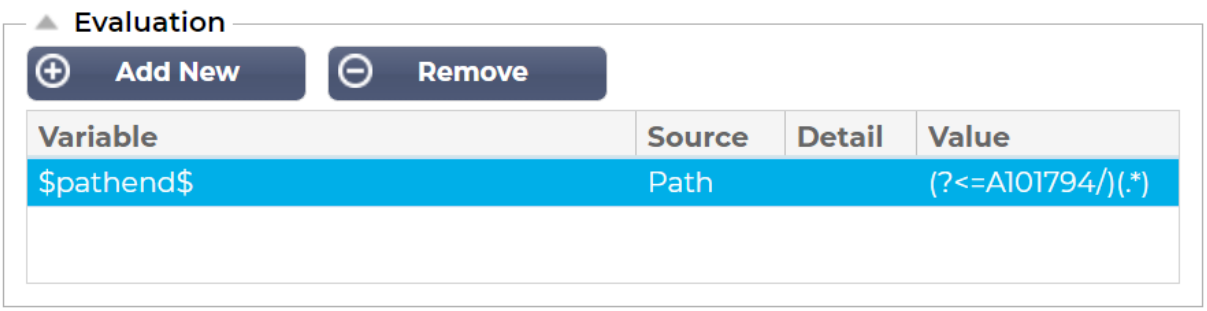
In our example below, we have used A101794 as the Server Hash value.



$pathend$

- Select Add new
- In the Variable column enter **$pathend$**
- In the Source column select **Path**
- In the Value column enter the following: (?<=<Server Hash>/)(.*)
  where you will replace **<Server Hash>** with the appropriate Server Hash value for your server

In our example below, we have used A101794 as the Server Hash value.



Creating the Action

The final stage in the flightPATH definition is to create the Action that will enact the traffic management sought after.

The Action section is located below Evaluation, and we will create two Actions for this flightPATH rule. Actions are configured in order of execution, so please plan this when you are making your own flightPATH rules.

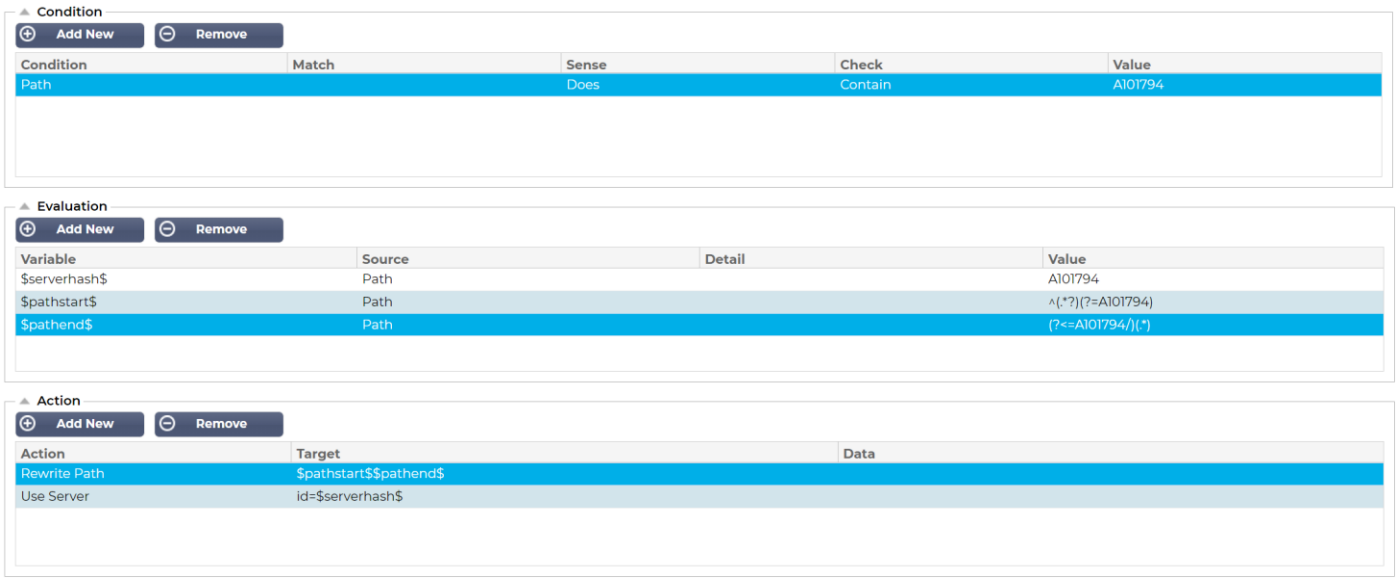
Rewrite Path

This Action essentially rewrites the path to the one that the evaluation variables have been defined as using the RegEx equations.

- Click Add New
- In the Action field, select Rewrite Path
- In the Target column enter: **$pathstart$$pathend$**
- Click Add New
- In the Action field select Use Server or Use Secure Server depending on whether you are performing an SSL Offload or SSL ReEncrypt.
- In the Target field, enter: **id=$serverhash$**

Repeat the above for each Real Server (Agfa Web) you will define.

The final flightPATH configuration should look like this.



Defining the Agfa Real Server Monitors

In order to maintain a healthy infrastructure, it is required to monitor the Real Servers for health and configure the load balancing if server requests are not being answered.

The Agfa Core servers require monitoring specified locations on specific ports with both HTTP and HTTPS. For this, we require a custom monitor written in PERL.

PERL Monitor Fields

The monitor has several field values it uses, with two of the fields that need filling in manually.

- IP Address – This is taken from the IP address of the Real Server entry
- Monitoring Method – The name of the monitor you specified when importing it.
- Page Location – this is a special field that needs to be filled in with "**Path, Port**". So the value will be for example: **/status , 80**
- Required Content: The expected response, in this case, 200OK

Below, you will find the PERL script for the monitor.

PERL Script Content

```
#Monitor-Name: Edgenexus-Agfa-Status-Health-Check
use strict;
use warnings;

##############################################################################################################
# Edgenexus custom health checking Copyright Edgenexus 2023
##############################################################################################################
#
#
# This is a Perl script for Edgenexus customer health checking
# The monitor name as above is displayed in the dropdown of Available health checks
# There are 3 value passed to this script
#
# _[0] IP address of the server to be health checked
# _[2] Required content - 200OK
# _[4] Page - Location and Port to use
#
# The script will return the following values
# 1 is the test is successful
# 2 if the test is unsuccessful
#

sub monitor
{
    my $host       = $_[0];### Host IP or name
    my $content    = $_[2];           ### Required Response
    my $cvar       = $_[4];### Path to be checked (Path, Port, prefix)

        my ($page, $port, $prefix) = split(/,\s*/, $cvar);

    $host = "$host:$port";

    my @lines      = `/usr/bin/wget -q -S --tries=1 --timeout=1 --no-check-certificate --output-document=- $prefix://$host$page 2>&1`;
    if (join("",@lines))
    {
        print "$prefix://$host$page looking for - $content - Healhcheck check successful\n";
        return(1);
```

```
    }
    else
    {
        print "$prefix://$host$page looking for - $content - Healhcheck check failed.\n";
        return(2)
    }

}

monitor(@ARGV);
```

Save using a suitable name such as Agfa-Status-80-Health-Check.pl, to your local file system.

You can download this script here:
https://www.edgenexus.io/docs/customhealthchecks/HTTPS-Agfa-Status-Check.pl

Importing the Monitor

To import the monitor is simple.

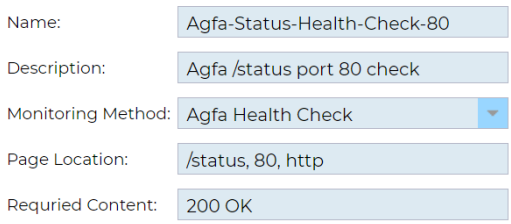
1. Navigate to Library > Real Server Monitors
2. Scroll down to Upload Monitor
3. Type **Agfa-Status-Health-Check** in the Name field
4. Browse and locate the .pl file you saved
5. Click Upload.

Creating the Monitor Definitions

Creating the STATUS Port 80 Monitor Definition

At the top of the Real Server Monitoring page you will find the Details section.

1. Click Add Monitor
2. In the fields section below the listing, you will see the fields that need to be filled in.
3. Fill in the Name field with, Agfa-Status-Health-Check-80
4. Add a Description. For example, Agfa /status port 80 check
5. Select the Monitoring Method, and select the **Agfa-Status-Health-Check option**.
6. In the Page Location field fill in: **/status, 80, http**
7. In the Required Content Field, fill in: **200OK** *(200 in numerals and OK in letters)*



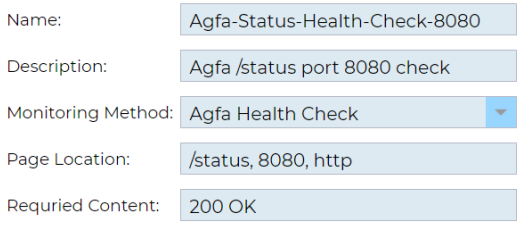
The monitor is defined and ready to use.

Creating the STATUS Port 8080 Monitor Definition

At the top of the Real Server Monitoring page you will find the Details section.

1. Click Add Monitor
2. In the fields section below the listing, you will see the fields that need to be filled in.

3. Fill in the Name field with, Agfa-Status-Health-Check-8080
4. Add a Description. For example, Agfa /status port 8080 check
5. Select the Monitoring Method, and select the **Agfa-Status-Health-Check option**.
6. In the Page Location field fill in: **/status, 8080, http**
7. In the Required Content Field, fill in: **200OK** *(200 in numerals and OK in letters)*

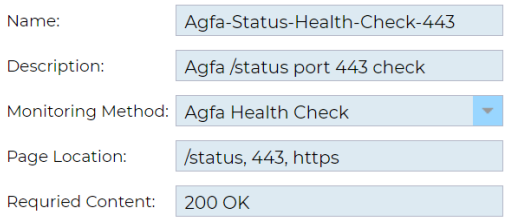


The monitor is defined and ready to use.

Creating the STATUS Port 443 Monitor Definition

At the top of the Real Server Monitoring page you will find the Details section.

1. Click Add Monitor
2. In the fields section below the listing, you will see the fields that need to be filled in.
3. Fill in the Name field with, Agfa-Status-Check-443
4. Add a Description. For example, Agfa /status port 443 check
5. Select the Monitoring Method, and select the **Agfa-Status-Health-Check option**.
6. In the Page Location field fill in: **/status, 443, https**
7. In the Required Content Field, fill in: **200OK** *(200 in numerals and OK in letters)*

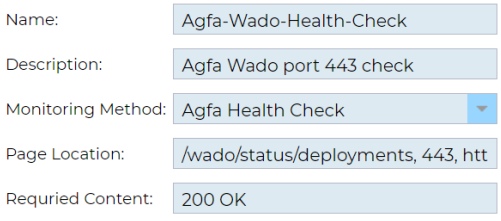


The monitor is defined and ready to use.

Creating the WADO Monitor Definition

At the top of the Real Server Monitoring page you will find the Details section.

1. Click Add Monitor
2. In the fields section below the listing, you will see the fields that need to be filled in.
3. Fill in the Name field with Agfa-Wado-443
4. Add a Description. For example, Agfa Wado port 443 check
5. Select the Monitoring Method, and select the **Agfa-Wado-Health-Check** option.
6. In the Page Location field fill in: **/wado/status/deployed, 443, https**
7. In the Required Content Field, fill in: **200OK** *(200 in numerals and OK in letters)*



The monitor is defined and ready to use.

VS Definition: Agfa Web with Xero Xtend

The following methodology outlines how to configure the VIP (Virtual IP) and VS (Virtual Service) for Agfa Web Servers with Xero Xtend.

To do this, navigate to the IP Services section under Services, or click on the IP Services tab on top of the right side of the page.

Adding the Virtual Service

1. Click Add Service
2. A new Virtual Service will be created with blank fields.
3. Enter the IP address (VIP) for the service.
4. Enter the Netmask
5. Enter the port value. Since we are configuring an HTTPS service, this will normally be 443.
6. Enter the Service Name. This is a description for understanding what the service does.
7. Select the Service Type. This will be HTTP in our case.
8. Click Update

A new entry will be created in the Server tab, within the Real Servers section below.

1. In the Address field, enter the IP address for the first server.
2. Enter the Port value. If you are using SSL Offload, this will be 80, and if you are using SSL Re-Encrypt, this will be 443.
3. Leave the Calcluated Weight column as is unless you have disparate hardware nodes.
4. Enter a note in the Notes column to identify the server
5. In the ID field, enter the first of the Server Hash values that you have for each of the web servers. In our case, it is A101794.
6. Click Update

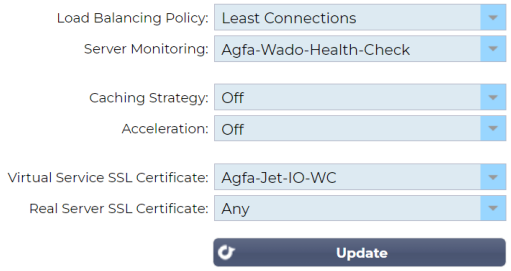
The ID field is used to define which server the flightPATH rule will send requests to. If you recall, we used the **Use Server / Use Secure Server** with **id=$serverhash$**.

Other Settings

Now that we have defined the basic rule, we have to configure other settings that can be found in the Basic and Advanced tabs.

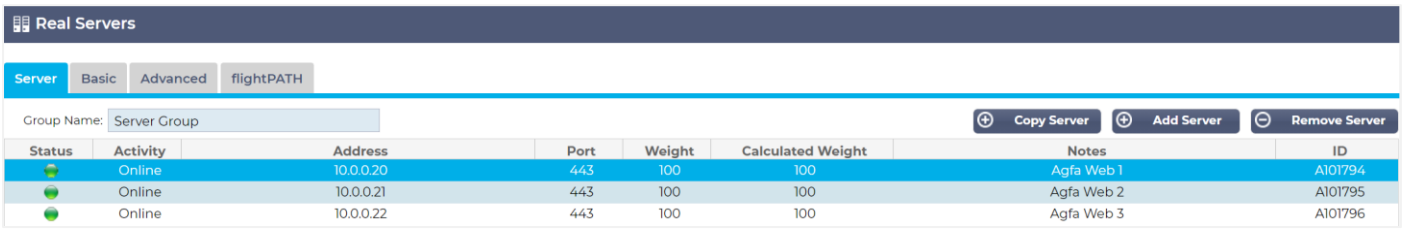
1. Click the Basic Tab
2. Load Balancing Policy: **Least Connections**
3. Server Monitoring: **Agfa-Wado-Health-Check**
4. Acceleration: Compression
5. Virtual Service SSL Certificate: **Choose your SSL certificate**
   For information on installing SSL Certificates, see the Administrator Guide
6. Real Server SSL Certificate: **Any**
   If you are using SSL Offload, then set to **No SSL**
7. Click Update

The Basic tab will look something like this:



Repeat steps 1-6 for each web server you are defining in the load balancing pool.

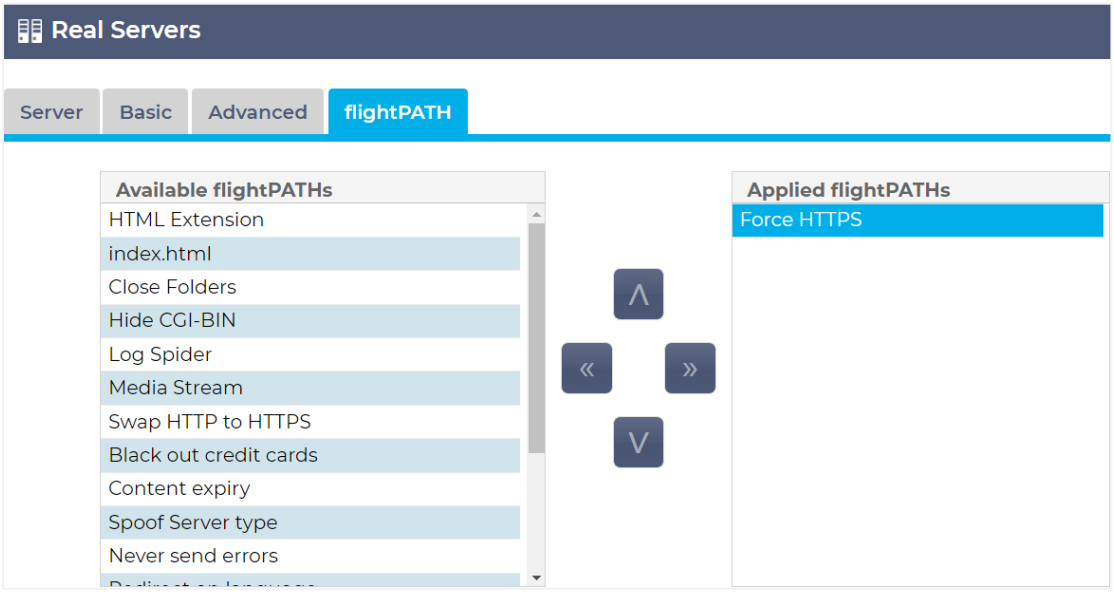
The final configuration should look something like the one below.



Adding a HTTPS Redirection Service

You will also need to add a HTTP redirection service as a sub-VS to the definition. This will ensure that any requests made to HTTP will automatically be sent to HTTPS.

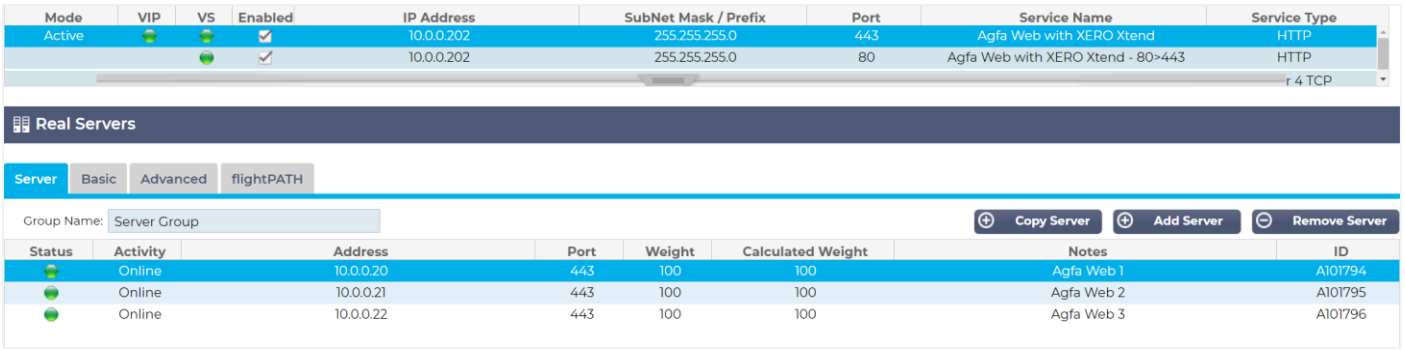
1. Make sure you have highlighted the Virtual Service you just created.
2. Click Add Service
3. A new Virtual service entry will be created with the IP address copied
4. Leave the IP address as is, making sure it matches the Virtual IP Service you had just created.
5. Add a Real Server – you only need one to configure the Virtual Service
6. Go to the flightPATH tab
7. Locate the flightPATH called **Force HTTPS** in the left side panel
8. Click on the flightPATH rule and click the right arrow in the central cluster.



9. The flightPATH rule will be moved to the activated section on the right
10. Click Update

Any requests entering the Virtual IP using HTTP, will now be redirected to HTTPS.

The complete definition will look something like this.



Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active			☑	10.0.0.202	255.255.255.0	443	Agfa Web with XERO Xtend	HTTP
			☑	10.0.0.202	255.255.255.0	80	Agfa Web with XERO Xtend - 80>443	HTTP

r 4 TCP

Real Servers

Server | Basic | Advanced | flightPATH

Group Name: Server Group

Copy Server | Add Server | Remove Server

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
	Online	10.0.0.20	443	100	100	Agfa Web 1	A101794
	Online	10.0.0.21	443	100	100	Agfa Web 2	A101795
	Online	10.0.0.22	443	100	100	Agfa Web 3	A101796

VS Definition: Agfa Web without Xero Xtend

The following methodology outlines how to configure the VIP (Virtual IP) and VS (Virtual Service) for Agfa Web Servers without Xero Xtend.

To do this, navigate to the IP Services section under Services, or click on the IP Services tab on top of the right side of the page.

Adding the Virtual Service

9. Click Add Service
10. A new Virtual Service will be created with blank fields.
11. Enter the IP address (VIP) for the service.
12. Enter the Netmask
13. Enter the port value. Since we are configuring an HTTPS service, this will normally be 443.
14. Enter the Service Name. This is a description for understanding what the service does.
15. Select the Service Type. This will be HTTP in our case.
16. Click Update

A new entry will be created in the Server tab, within the Real Servers section below.

7. In the Address field, enter the IP address for the first server.
8. Enter the Port value. If you are using SSL Offload, this will be 80, and if you are using SSL Re-Encrypt, this will be 443.
9. Leave the Calcluated Weight column as is unless you have disparate hardware nodes.
10. Enter a note in the Notes column to identify the server
11. In the ID field, enter the first of the Server Hash values that you have for each of the web servers. In our case, it is A101794.
12. Click Update

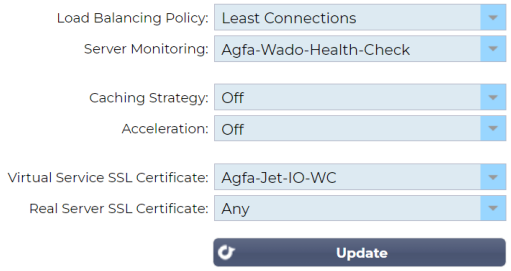
The ID field is used to define which server the flightPATH rule will send requests to. If you recall, we used the **Use Server / Use Secure Server** with **id=$serverhash$**.

Other Settings

Now that we have defined the basic rule, we have to configure other settings that can be found in the Basic and Advanced tabs.

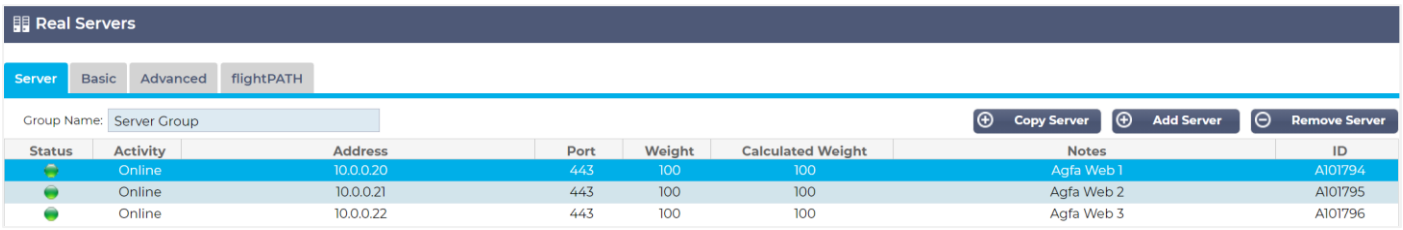
8. Click the Basic Tab
9. Load Balancing Policy: **JSP Session Cookie**
10. Server Monitoring: **Agfa HV WADO**
11. Acceleration: Compression
12. Virtual Service SSL Certificate: **Choose your SSL certificate**
    For information on installing SSL Certificates, see the Administrator Guide
13. Real Server SSL Certificate: **Any**
    If you are using SSL Offload, then set to **No SSL**
14. Click Update

The Basic tab will look something like this:



Repeat steps 1-6 for each web server you are defining in the load balancing pool.

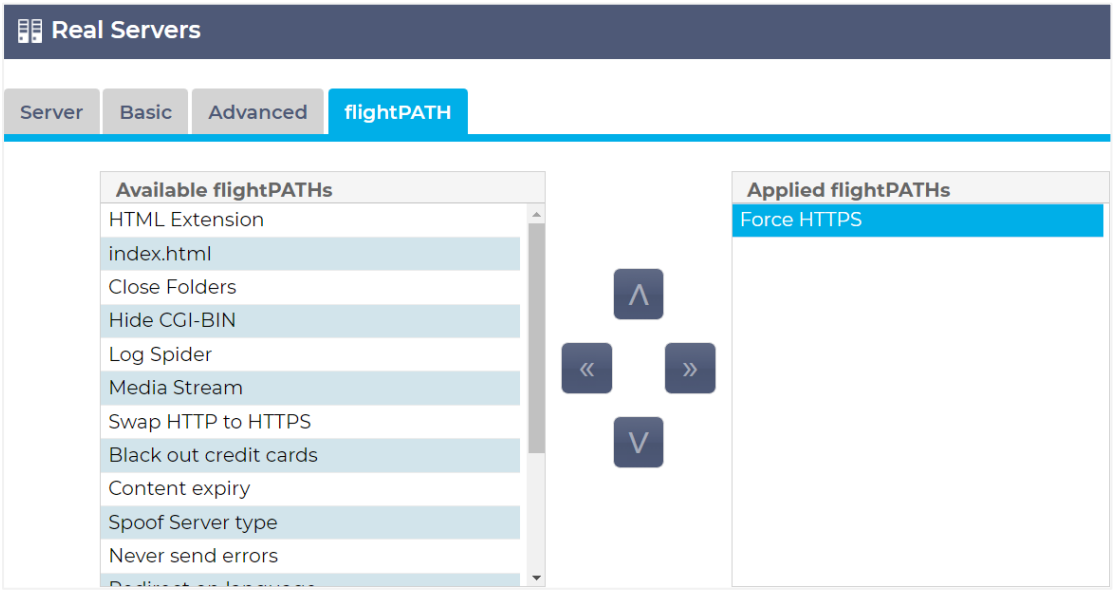
The final configuration should look something like the one below.



Adding a HTTPS Redirection Service

You will also need to add a HTTP redirection service as a sub-VS to the definition. This will ensure that any requests made to HTTP will automatically be sent to HTTPS.

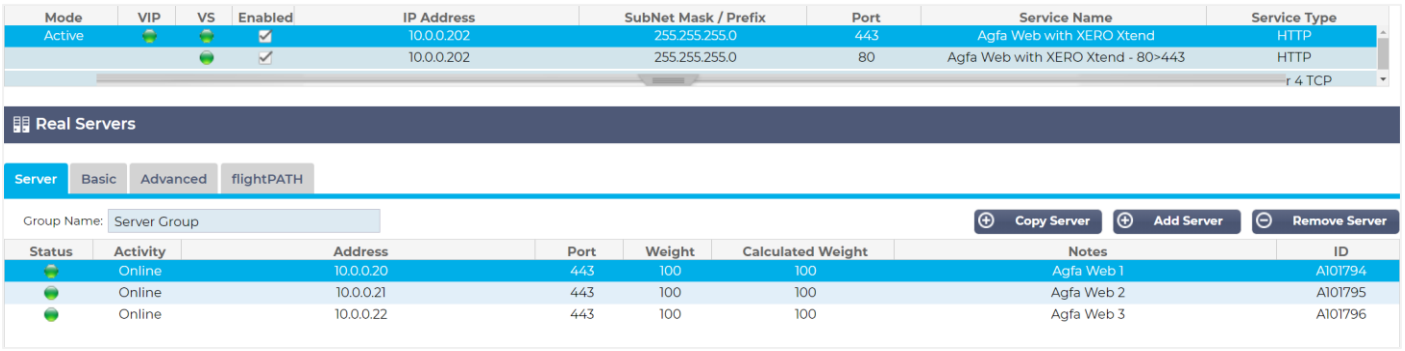
11. Make sure you have highlighted the Virtual Service you just created.
12. Click Add Service
13. A new Virtual service entry will be created with the IP address copied
14. Leave the IP address as is, making sure it matches the Virtual IP Service you had just created.
15. Add a Real Server – you only need one to configure the Virtual Service
16. Go to the flightPATH tab
17. Locate the flightPATH called **Force HTTPS** in the left side panel
18. Click on the flightPATH rule and click the right arrow in the central cluster.



19. The flightPATH rule will be moved to the activated section on the right
20. Click Update

Any requests entering the Virtual IP using HTTP, will now be redirected to HTTPS.

The complete definition will look something like this.



Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active			☑	10.0.0.202	255.255.255.0	443	Agfa Web with XERO Xtend	HTTP
			☑	10.0.0.202	255.255.255.0	80	Agfa Web with XERO Xtend - 80>443	HTTP

r 4 TCP

Real Servers

Server | Basic | Advanced | flightPATH

Group Name: Server Group

Copy Server | Add Server | Remove Server

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
	Online	10.0.0.20	443	100	100	Agfa Web 1	A101794
	Online	10.0.0.21	443	100	100	Agfa Web 2	A101795
	Online	10.0.0.22	443	100	100	Agfa Web 3	A101796

Agfa Core Client Services

The Agfa Core Client Services, together with the DICOM, HL7 and ARR services all work through the same Virtual Service.

VS Definition: Agfa Core Client Service 80

To add this Virtual Service, please follow the steps below.

1. Go to IP Services
2. Click Add Service
3. Fill out the IP Address field with a valid IP
4. Fill out the Netmask
5. Enter **80** into the Port field
6. Enter description, **Agfa Core Client 80**, into the Description field
7. Set the Service Type to **HTTP**

Now you will add the Real Servers.

8. The cursor will have been placed in the Address Field
9. Enter the IP address of the first Agfa Core Server
10. Enter a port value of **80**
11. Leave the Weight field untouched
12. Enter **Agfa Core Server 1**, into the Description field
13. Click Update once done
14. Add the next Real Server by clicking Copy Server
15. Change the IP Address as needed.
16. Click Update once done.
17. You can repeat steps 7-9 for additional Real Servers you wish to add.

Now we will enter the required settings into the Basic Tab.

18. Proceed to the Basic Tab
19. Change the Load Balancing Policy to: **JSP Session Cookie**
20. Choose the Server Monitor as: **Agfa-STATUS-Health-Check-80**
21. Click Update

The service is now configured.

VS Definition: Agfa Core Client Service 443

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **443** into the Port field
5. Enter **Agfa Core Client 443**, into the Description field
6. Set the Service Type as **HTTP**
7. Now we will enter the required settings into the Basic Tab.

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

8. Change the Port values of all the Real Servers to **443**
9. Proceed to the Basic Tab
10. Change the Load Balancing Policy to: **JSP Session Cookie**
11. Choose the Server Monitor as: **Agfa-Status-Health-Check-443**
12. Set the Acceleration option to **Compression**
13. Select your certificate in the Virtual Service SSL Certificate menu
14. Choose **Any** in the Real Server SSL Certificate
15. Click Update

The service is now configured.

VS Definition: Agfa Core Client Service 4447

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **4447** into the Port field
5. Enter **Agfa Core Client 4447**, into the Description field
6. Set the Service Type to **HTTP**
7. Change the Port values of all the Real Servers to **4447**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **Agfa-Status-Health-Check-80**
11. Set the Acceleration option to **Compression**
12. Click Update

The service is now configured.

VS Definition: Agfa Core Client Service 5222

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **5222** into the Port field
5. Enter **Agfa Core Client 5222**, into the Description field
6. Set the Service Type to **HTTP**
7. Change the Port values of all the Real Servers to **5222**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **TCP Connection**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa Core Client Service 5223

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **5223** into the Port field
5. Enter **Agfa Core Client 5223**, into the Description field
6. Set the Service Type to **HTTP**
7. Change the Port values of all the Real Servers to **5223**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **TCP Connection**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa Core Client Service 8080

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **8080** into the Port field
5. Enter **Agfa Core Client 8080**, into the Description field
6. Set the Service Type to **HTTP**
7. Change the Port values of all the Real Servers to **8080**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **Agfa-Status-Health-Check-8080**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa Core Client Service 7443

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **7443** into the Port field
5. Enter **Agfa Core Client 7443**, into the Description field
6. Set the Service Type to **HTTP**
7. Change the Port values of all the Real Servers to **7443**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **TCP Connection**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa Core Client Service 8443

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **8443** into the Port field
5. Enter **Agfa Core Client 8443**, into the Description field
6. Set the Service Type to **HTTP**
7. Change the Port values of all the Real Servers to **8443**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **Agfa-Status-Health-Check-443**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa Core Client Service 9080

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.

3. The IP Address and Netmask values are copied over
4. Enter **9080** into the Port field
5. Enter **Agfa Core Client 9080**, into the Description field
6. Set the Service Type as **HTTP**
7. Change the Port values of all the Real Servers to **9080**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **Agfa-Status-Health-Check-80**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa Core Client Service 9081

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **9081** into the Port field
5. Enter **Agfa Core Client 9081**, into the Description field
6. Set the Service Type as **HTTP**
7. Change the Port values of all the Real Servers to **9081**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **Agfa-Status-Health-Check-80**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa Core Client Service 10080

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **100080** into the Port field
5. Enter **Agfa Core Client 10080**, into the Description field
6. Set the Service Type as **HTTP**
7. Change the Port values of all the Real Servers to **10080**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **Agfa-Status-Health-Check-80**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa Core Installer Service 10123

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **10123** into the Port field
5. Enter **Agfa Core Installer 10123**, into the Description field
6. Set the Service Type as **HTTP**
7. Change the Port values of all the Real Servers to **10123**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **TCP Connection**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa Core Installer Service 10124

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **10124** into the Port field
5. Enter **Agfa Core Installer 10124**, into the Description field
6. Set the Service Type as **HTTP**
7. Change the Port values of all the Real Servers to **10124**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**

10. Choose the Server Monitor as: **TCP Connection**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa Dicom Service 104

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **104** into the Port field
5. Enter **Agfa Dicom 104**, into the Description field
6. Change the Service Type to **Dicom**
7. Change the Port values of all the Real Servers to **104**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **Dicom**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa Dicom Service 110

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **110** into the Port field
5. Enter **Agfa Dicom 110**, into the Description field
6. Change the Service Type to **Dicom**
7. Change the Port values of all the Real Servers to **110**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **Dicom**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa Dicom Service 2762

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **2762** into the Port field
5. Enter **Agfa Dicom 2762**, into the Description field
6. Change the Service Type to **Dicom**
7. Change the Port values of all the Real Servers to **2762**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **Dicom**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa HL7 Service 2310

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **2310** into the Port field
5. Enter **Agfa HL7 2310**, into the Description field
6. Set the Service Type to **HTTP**
7. Change the Port values of all the Real Servers to **2310**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **TCP Connection**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa HL7 Service 2311

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **2311** into the Port field
5. Enter **Agfa HL7 2311**, into the Description field

6. Set the Service Type to **HTTP**
7. Change the Port values of all the Real Servers to **2311**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **TCP Connection**
11. Set the Acceleration option to **Compression**
12. Click Update

VS Definition: Agfa ARR Service 6514

To add this Virtual Service, please follow the steps below.

1. Ensure that the previously configured Virtual Service is highlighted
2. Click Copy Service
   Note that we are not using Add Service as we will be defining sub-Virtual Services.
3. The IP Address and Netmask values are copied over
4. Enter **6514** into the Port field
5. Enter **Agfa ARR 6514**, into the Description field
6. Change the Service Type to **HTTP**
7. Change the Port values of all the Real Servers to **6514**

You will note that the Real Servers are maintained as this is a Sub-VS, however, we still need to change their Port values to match the Virtual Service changes we just made.

Now we will enter the required settings into the Basic Tab.

8. Proceed to the Basic Tab
9. Change the Load Balancing Policy to: **Least Connections**
10. Choose the Server Monitor as: **TCP Connection**
11. Set the Acceleration option to **Compression**
12. Click Update