EDGE NEXUS

ALB-X User Guide
Software Version
4.2.1 (Build 1734)

App Store 7
What is the App Store? 7
What can I get in the App Store? 7
Health Checks 7
jetPACKs 7
flightPATHs 8
Add-Ons 8
Software Updates 8
How do I Buy an App? 9
Buying a New Health Check: 9
IP Services 10
Virtual Services 10
Copy Service 13
Filtering and Sorting: 13
Search IP Services: 13
Real Servers 16
..... 17
Basic 18
Advanced 23
flightPATH 26
Add-Ons 27
User Guides for Add-Ons 27
Application Firewall Add On 27
Global Server Load Balancer Add On 27
What's an Add-On? 27
Purchasing an Add-On 27
Application Firewall Add On 29
Buying an Application Firewall Add-On 29
Running your Application Firewall 31
Example Architecture 33
Firewall Using External IP Address: 33
Firewall Using Internal IP Address: 34
Accessing your Firewall Add-On 34
Apps 38
What's an App? 38
Work Flow 38
Access App Store within ALB-X 38
Access App Store directly https://appstore.edgenexus.io 39
Purchasing an App 40
Buying a flightPATH App: 40
Authentication 44
Work Flow 44
Authentication Servers 44
Authentication Rules 45
Single Sign On: 46
Forms 46
Creating your own form 46
Adding a custom form 47

Preview a custom form 48
flightPATH 48
Cache 50
Cache Settings 50
Apply Cache Rule 51
Create Cache Rule 51
flightPATH 53
Details 53
Condition 54
Evaluation 56
..... 57
Action 58
Common Uses: 59
Pre-Built Rules: 60
Real Server Monitoring 66
Details 66
Upload Monitor 68
Custom Monitors 68
Creating a Custom Monitor Perl Script 68
Custom Health Checks have two outcomes 69
SSL Certificates 71
What can edgeNEXUS do with SSL? 71
Create Certificate 71
Manage Certificates 72
Import Certificate 75
Single Certificate: 75
Multiple Certificates: 76
Export Certificate 76
Widgets 78
Configured Widgets 78
Available Widgets 78
Events: 78
System Graphs: 80
Interface: 81
Status: 83
Traffic Graphs: 85
Dashboard 88
Adding a Widget 88
Customising the Dashboard 88
View History 91
How do I see some graphs? 91
3. 92
View Logs 94
Download W3C Log 94
Download System Log 94
Statistics 96
Total Input/Output 96
Compression 96

Hits and Connections 97
Caching 97
Hardware 98
Status 100
Virtual Service Details 100
VIP Status: 100
VS Status: 100
Name: 101
Virtual Service: 101
Hit/Sec: 101
Cache%: 101
Compression%: 101
RS Status: 101
Real Server: 102
Notes: 102
Conns: 102
Data: 102
Req/Sec: 102
Clustering 103
Notes on High Availability 103
Role 103
Cluster Role 103
Failure of Cluster Owner 104
Manual Role 105
Stand-Alone Role 106
Settings 106
Management 106
Date & Time 111
Date & Time 111
Time Server 111
Email Events 113
Email Address 113
Mail Sever [SMTP] 113
Notifications and Alerts 114
Warnings 115
System History 116
Enable Historical logging 116
Maintenance 116
Backup 117
Delete 117
..... 117
Restore 117
Licence 118
Licence Details 118
Facilities 118
Install Licence 120
Licence Support Information 121
System Logging 122

W3C Logging Details 122
Remote Syslog Server 123
Remote W3C Log Storage 124
Field Summary 125
Clear Log Files 126
Network 127
Basic Setup 127
Basic Setup: 127
Adapter Details 127
Interfaces 128
Bonding 129
Adapter Status 130
IP Addressing 130
Static Route 130
Static Route Details 131
Advanced Network Settings 131
Power 132
Restart 132
Reboot 132
Power Off 132
Security 134
SSH 134
Webconsole 134
REST API 134
SNMP 136
SNMP Settings 136
SNMP MIB 136
Historical Graphing 138
Users 139
Users 139
Adding a User 139
User Type 140
Removing Users 141
Editing Users 141
Audit Log 141
Configuration 142
Configuration 142
Global Settings 143
Global Settings 143
HTTP 144
Server Too Busy 144
Forwarded For 145
HTTP Compression Settings 147
Global Compression Exclusions 148
Software 149
ALB Software Upgrade Details 149
Download from Cloud 149
Upload software to ALB 150

Upload Apps and Software 150
Apply Software stored on ALB 151
Troubleshooting 152
Support Files 152
Ping 152
Trace 153
Capture 154
About Us 156
Who is jetNEXUS? 156
Contact information 156
EMEA 156
jetPACK 157
Download a jetPACK 157
Microsoft Exchange 157
..... 158
Microsoft Lync 2010/2013 158
Web Services 158
Microsoft Remote Desktop 158
DICOM – Digital Imaging and Communications in Medicine 159
Oracle – E-Business Suite 159
VMware Horizon View 159
Global Settings 159
Cipher Options 159
flightPATHs 160
Apply a jetPACK 160
Create a jetPACK 160
Section 0: 161
Section1: 161
Section 2: 161
Section 3: 162
Section 4: 162

App Store

The **Services — App Store** page will allow you to see https://appstore.edgenexus.io from within your ALB-X.

What is the App Store?

The edgeNEXUS App Store is a marketplace dedicated to the latest application networking solutions and services including Software Defined Networking (SDN), Application Delivery Controller (ADC), Security, Containerisation, Network Function Virtualisation (NFV), Big Data and the IoT.

What can I get in the App Store?

An **App** is the generic name for all the different products you can buy at the **App Store**. Some of these **Apps** can run independently of the ALB-X whilst others will integrate and enhance your current load balancer deployment.

Health Checks

Check that your applications are healthy with custom built real server **Health Check Monitors or Health Checks** for short.

jetPACKs

Download application templates called **jetPACKs** to automatically configure your ALB-X load balancer.

flightPATHs

The ALB-X has the ability to download **flightPATH** rules which allow you to shape and secure your traffic with an easy-to-use, drag and drop rules-based engine.

Add-Ons

Docker based Add-Ons that can run in isolation on your ALB-X load balancer. Examples include an Application Firewall and even another jetNEXUS ALB-X for true multitenancy.

Software Updates

Get the latest software for your ALB-X.

How do I Buy an App?

Buying a New Health Check:

- Click on the **Health Check** icon.
- Click on the specific health check that you are interested in.
- You will see more information about the health check.
- You can then choose how many you would like to download. If you are accessing the App Store from within your ALB-X please choose only 1 health check.
- Click **Add to Cart**. These are often free.
- **Proceed to Checkout**.
- Here you will be asked to login if you are a returning customer.
- Alternatively you can fill out your billing details and tick the box to create an account.
- Click **Place Order.**
- You should now be presented with a screen that allows you download your product manually by entering the Machine ID and clicking download.
- If the download is blanked out then you have already tied a purchase to another ALB-X.
- If you have purchased from within an **ALB-X** via the **Services — App** store page then you can now see your purchased app in the **Library — Apps** page.
- Here you can deploy your **App**, in this case a real server health monitor.
- Once you click deploy your monitor will be deployed as a new **Real Server Monitor** method in the **Library — Real Sever Monitors** page.

IP Services

The **Services —> IP Services** page allows you to add, delete and configure IP Services. The settings are organised into the following sections

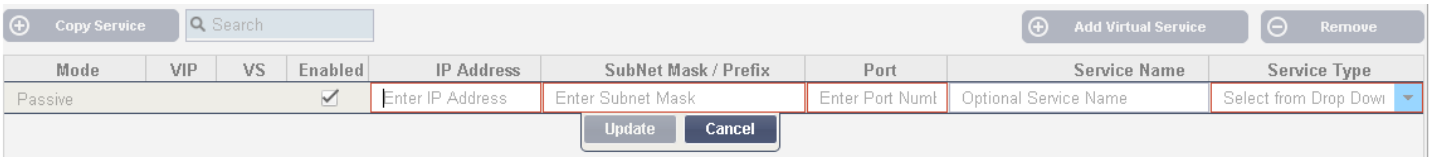
Virtual Services

A **Virtual Service** is a combination of a **Virtual IP (VIP)** and a **TCP/UDP** port that the **jetNEXUS ALB-X** will listen on:

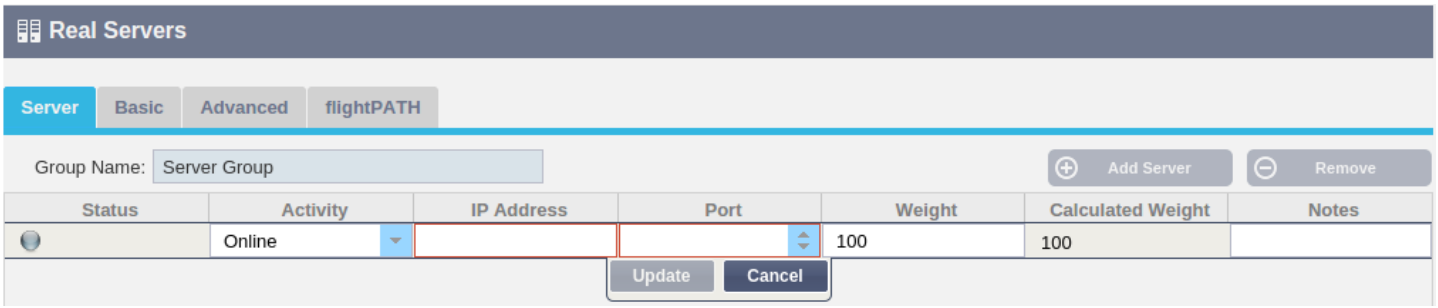
- Traffic arriving at the **Virtual Service** is directed to one of the **Real Servers** that are associated with that service
- The **Virtual Service** IP address cannot be the same as the management address of the jetNEXUS ALB-X. i.e. eth0, eth1 etc...
- The **jetNEXUS ALB-X** determines how the traffic is distributed to the **Real Servers** based on a load balancing policy set within the **Basic** tab

Create a new Virtual Service using a new VIP

- Click **Add Virtual Service**. You will then enter row edit mode. The 4 boxes highlighted in red must be completed before you can update



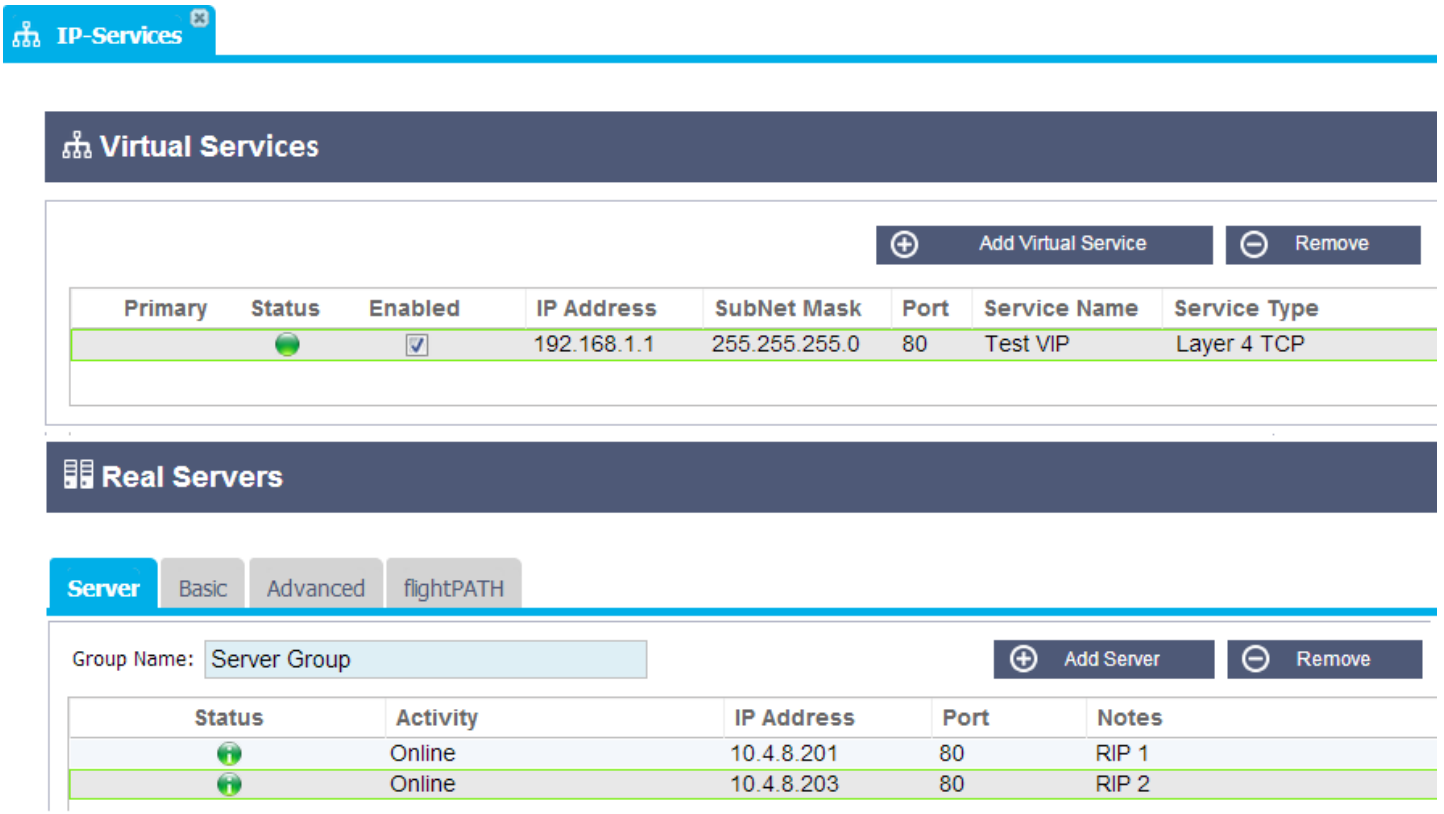
- The **IP Address** box should contain a blinking cursor so just start typing your **Virtual IP** address and then **TAB** to the next box
- Enter the **Subnet Mask** and **TAB** to the next box
- Enter the **Port Number** for your service and **TAB** to the next box
- Enter an optional **Service Name** and **TAB** to the next box
- Use the down arrows on your keyboard or select a **Service Type** using your mouse
- You can now press the **Update** button to save this section and jump automatically to the **Real Server** section below



- Leave the server in the **Online Activity –** this means it will be load balanced if it passes the default health monitor of **TCP Connect**
- Enter an **IP address** for the real server and **TAB** to the next box
- Enter a **Port Number** for the real server and **TAB** to the next box
- Enter an optional name for the **Real Server**

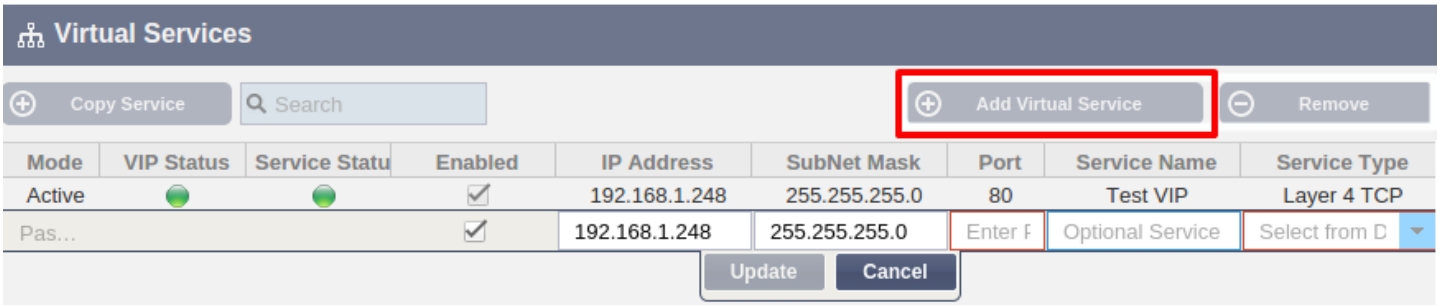
- Click **Update** or press **Enter** to save your changes
- The **Status** light will first turn Grey then it will turn green if the **Server Health Check** succeeds. It will turn **Red** if the **Real Server Monitor** fails
- A server that has a **Red Status** light will not be load balanced

Example of a completed Virtual Service with 2 Real Servers:

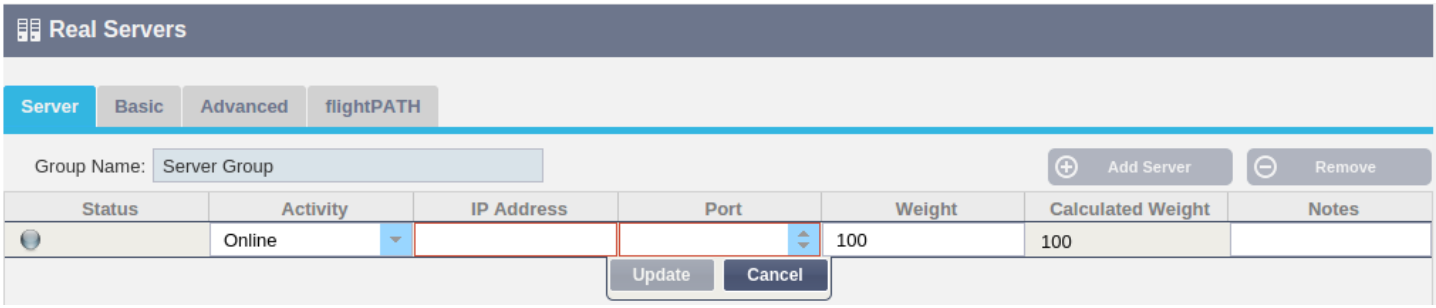


Create a new Virtual Service using the same VIP

- Highlight a **Virtual Service** with the IP address you wish to copy
- Click **Add Virtual Service** to enter row edit mode



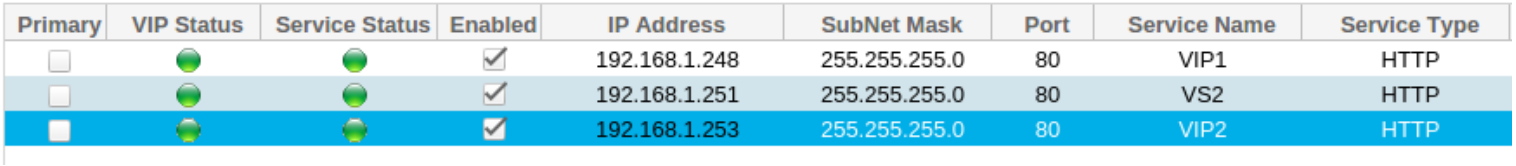
- The **IP Address** and **Subnet Mask** will be copied automatically
- Enter the **Port Number** for your service and **TAB** to the next box
- Enter an optional **Service Name** and **TAB** to the next box
- Use the down arrows on your keyboard or select a **Service Type** using your mouse
- You can now press the **Update** button to save this section and jump automatically to the **Real Server** section below



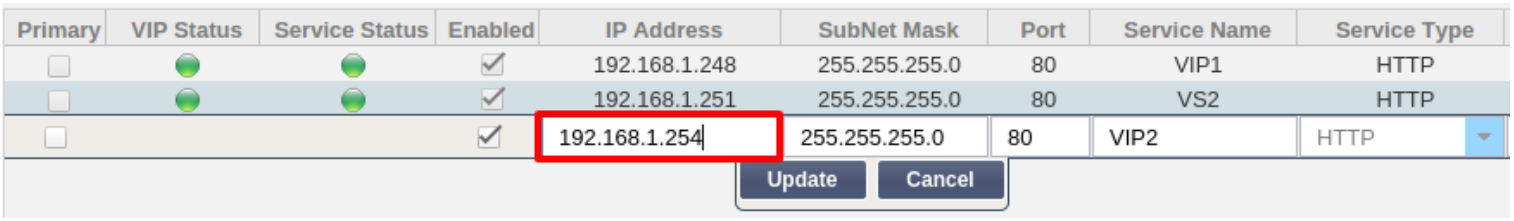
- Leave the server in the **Online Activity –** this means it will be load balanced if it passes the default health monitor of **TCP Connect** which can be changed later
- Enter an **IP address** of the real server and **TAB** to the next box
- Enter a **Port Number** for the real server and **TAB** to the next box
- Enter an optional name for the **Real Server**
- Click **Update** to save your changes
- The **Status** light will first turn grey then green if the **Server Health Check** succeeds. It will turn **Red** if the **Real Server Monitor** fails
- A server that has a **Red Status** light will not be load balanced

Changing the IP Address your Virtual Services

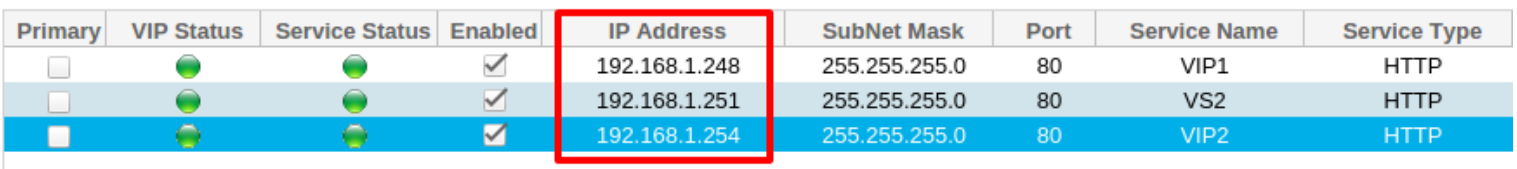
- Highlight a service with the IP address you would like to change



- Double Click into the **IP address** column
- Change the **IP address** and click **Update**



- This will change the IP address of ALL **Virtual Services** associated with this VIP



Copy Service

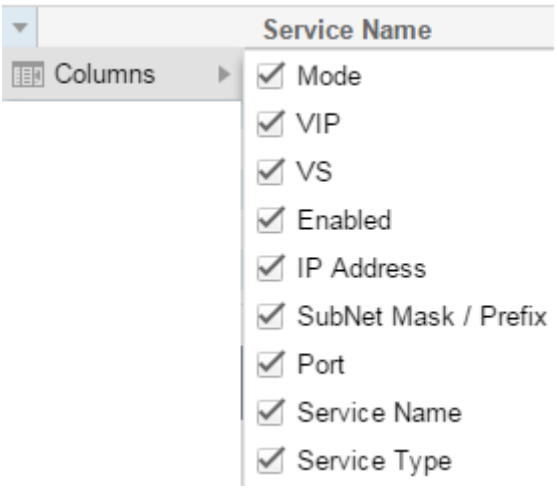
Create a new Virtual Service using the Copy Service button:

- The new **Copy** button will copy an entire service including all of the real servers, basic settings, advanced settings and flightPATH rules associated with it
- Highlight the service you wish to duplicate and click **Copy**
- The row editor will appear with the blinking cursor on the IP Address column
- You must change either the IP address to be unique or if you wish to keep the IP address the port must be unique to that IP address
- Don't forget to edit each tab if you wish to change a setting such as the load balancing policy the real server monitor or remove a flightPATH rule

Filtering and Sorting:

Filter Columns:

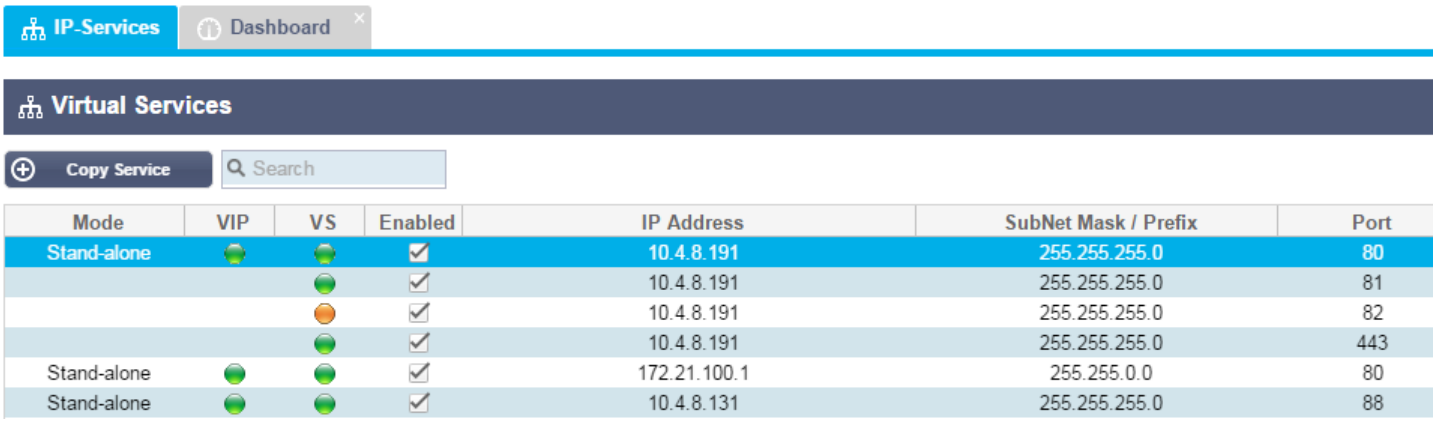
To the far right of each column is small down arrow (see the red box below). Clicking on this will reveal an extra submenu that allows you to "Sort Ascending", "Sort Descending" and "Columns". Add and remove the tick to show/hide the columns listed below.



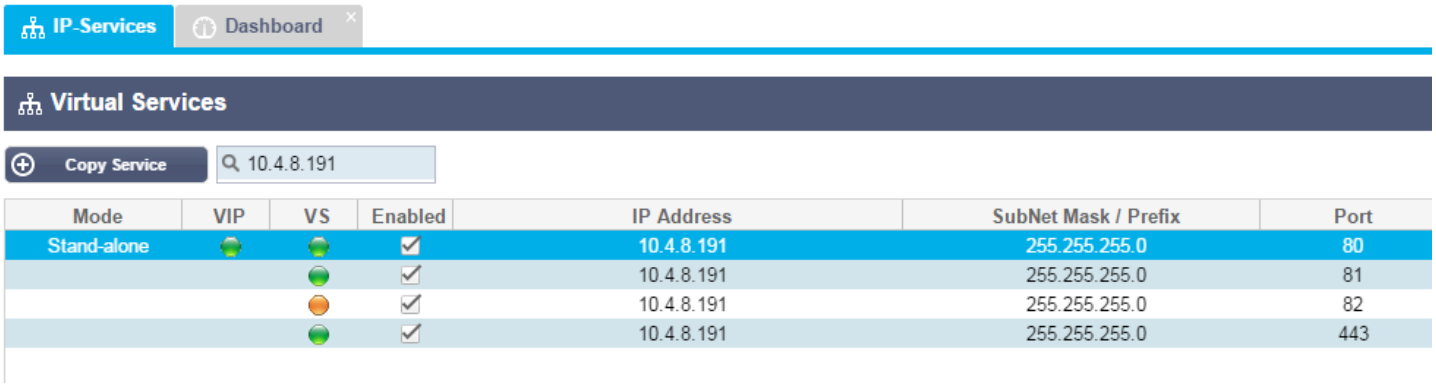
Search IP Services:

The Search box allows you to type in a term that will restrict the view to any services containing that term

You can search for whole or part terms such as three octets of a virtual IP address. The service name column allows you to freely write anything you want. So if you have named these by customer for example you will be able to search for every service associated with that customer. Example before search term entered:



Example screen shot after search term “10.4.8.191”



Primary/Mode

The **Primary/Mode** column contains different information depending on the high availability role that has been selected from the **Cluster** page High Availability Role:

1. **Cluster**
   - This is the default role for a new **ALB-X** and as such the **Primary/Mode** column will indicate whether the **ALB-X** is either **Active** or **Passive**
2. **Manual**
   - In this role the **ALB-X** can be **Active Active** for different **Virtual IP addresses** and as such the **Primary** column will contain a box next to each unique **Virtual IP** that can be ticked for **Active** or left un-ticked for **Passive**
3. **Stand-Alone**
   - The **ALB-X** is acting alone and is not in **High Availability** mode and as such the **Primary column** will say **Stand-alone**

VIP Status – This will provide visual feedback for the status of the Virtual IP address and all associated virtual services

- Online
- Failover-Standby. This virtual service is hot-standby
- Indicates a “secondary” is holding off for a “primary”
- Offline. Content servers are unreachable or no content servers enabled
- Finding status
- Not licenced or licenced Virtual IPs exceeded

Service Status – This will provide visual feedback for the status of each individual virtual service

- Online
- Failover-Standby. This virtual service is hot-standby
- Indicates a “secondary” is holding off for a “primary”
- Service Needs attention. This may be the result of a real server failing a health monitor or has been changed manually to Offline. Traffic will continue to flow but with reduced real server capacity
- Offline. Content servers are unreachable or no content servers enabled
- Finding status
- Not licenced or licenced Virtual IPs exceeded

Enabled

By default the box is ticked to enable the **Virtual Service**. Double click on the row to edit and remove the tick to disable the **Virtual Service**

IP Address

Add in your IPv4 address in decimal dotted notation or an IPv6 address. This is the Virtual IP address for your service. Example IPv4 “192.168.1.100”. Example IPv6 "2001:0db8:85a3:0000:0000:8a2e:0370:7334"

Subnet Mask / Prefix

Add in your subnet mask in decimal dotted notation. Example “255.255.255.0". Or for IPv6 add in your Prefix. For more information about IPv6 please see https://en.wikipedia.org/wiki/IPv6_address

Port

Add in the port number associated with your service. This may be TCP or UDP port number. Example “80” for Web Traffic

Service Name

Add in a friendly name to identify your service. Example “Production Web Servers”.

Service Type

Please note that with all “Layer 4” service types, edgeNEXUS will not interact or modify the data stream so flightPATH will not work with these service types. It will simply load balance the traffic according to the load balancing policy:

Layer 4 TCP:
Any TCP port (Layer 4). edgeNEXUS will not alter any information in the data stream and will simply load balance the traffic according to the load balancing policy

Layer 4 UDP:
Any UDP port (Layer 4)
Layer TCP/UDP:
Any TCP or UDP port (Layer 4) This is ideal if your service has a primary protocol such as UDP but will fall back to TCP
HTTP:
HTTP(s) Protocol (Layer 7)**.** jetNEXUS ALB-X has the ability to interact, manipulate and modify the data stream using flightPATH
FTP:

File Transfer Protocol Protocol (Layer 7). Using separate control and data connections between client and server

SMTP:

Simple Mail Transfer Protocol (Layer 4)

POP3:

Post Office Protocol (Layer 4)

IMAP:

Internet Message Access Protocol (Layer 4)

RDP:

Remote Desktop Protocol (Layer 4)

RPC:

Remote Procedure Call (Layer 4)

RPC/ADS:

Exchange 2010 Static RPC for Address Book Service (Layer 4)

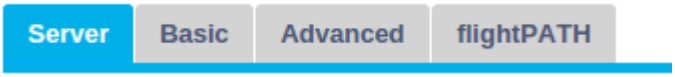
RPC/CA/PF:

Exchange 2010 Static RPC for Client Access & Public Folders (Layer 4)

DICOM:

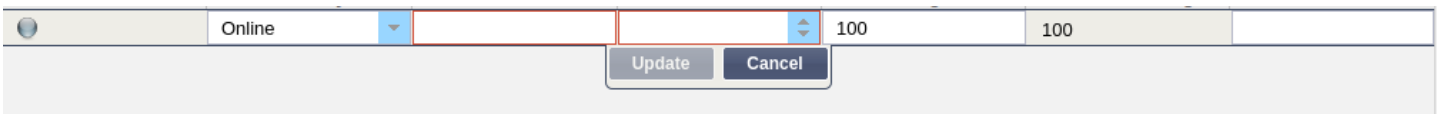
Digital Imaging and Communications in Medicine (Layer 4)

Real Servers

The **Server** tab contains the **Real Server** details associated with the highlighted **Virtual Service**. You will be prompted to add at least one **Real Server** when setting up a **Virtual Service**. 

Add a new Real Server to a Virtual Service

1. Click **Add Server**
2. A new row will appear with the cursor blinking on the IP Address column



1. Enter the IPv4 address of your server in dotted decimal notation. The **Real Server** can be on the same network as your **Virtual Service**, any directly attached local network or any network that your edgeNEXUS can route to. Example “10.1.1.1”.
2. Tab to the **Port** column and enter the TCP/UDP port number for your server. This can be the same as the **Virtual Service** port number or another port number for Reverse Proxy Connectivity. The jetNEXUS ALB-X will automatically translate to this number.
3. Tab to the **Notes** section to add in any relevant detail for the server. Example: “IIS Web Server 1”

Real Server Details

Group Name:

- This is the name you can associate with a particular group of servers. For Example “Exchange 2010 CAS Array”

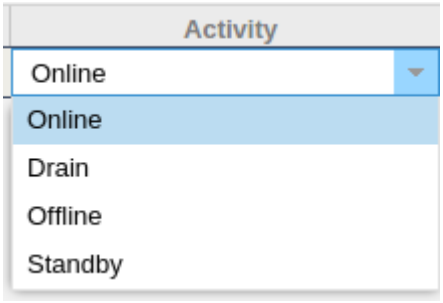
- This name will be automatically saved once edited
- In this version of software there is no additional functionality, however in future releases we will include the ability to add or link server groups once they have been configured

Real Server Status Lights

- Connected
- Not monitored
- Draining
- Offline
- Standby
- Not connected
- Finding status
- Not licenced or licenced real servers exceeded

Activity

If you wish to change the **Activity** of a **Real Sever**, click on a row to highlight then click again to enter row edit mode. You can now select an **Activity** from the drop down menu.



Online:
All **Real Servers** assigned as **Online** will receive traffic according to the load balancing policy set within the **Basic** tab

Drain:
All **Real Servers** assigned as **Drain** will continue to serve existing connections but will not accept any new connections. The **Status** light will flash green / blue whilst draining. Once the existing connections have closed naturally the **Real Servers** will be taken offline and the **Status** light will be solid blue. You can also view these connections on the **Navigation-Monitor-Status** page

Offline:
All **Real Servers** assigned as **Offline** will immediately be taken offline and will not receive any traffic

Standby:
All **Real Servers** assigned as **Standby** will remain offline until **ALL** of the **Online** group fail their **Server Health Montior**, at which point members of the **Standby** group will be sent traffic according to the load balancing policy. If one of the **Online** group passes the **Server Health Monitor** this **Online** server will receive all of the traffic and the **Standby** group will be no longer receive traffic.

IP Address

This is the IP address for your **Real Server**. Example “192.168.1.200”.

Port

This is a TCP or UDP port number that the **Real Server** is listening on for a particular service. Example “80” for Web Traffic.

Weight

This column will become editable when an appropriate Load Balancing Policy has been selected in the **Basic** tab. Appropriate policy are **Least Connections**, **Round Robin**, **Fastest**. The default weight for a real server is 100 and you can enter values from 1-100. 100 means maximum load and 1 means minimum load.

- Example 1 with 3 servers
- Server 1 Weight = 100
- Server 2 Weight = 50
- Server 3 Weight = 50

If we consider the load balancing policy is least connections and there are 200 total client connections

- Server 1 will get 100 current connections
- Server 2 will get 50 current connections
- Server 3 will get 50 current connections

If we consider Round Robin which servers in turn, altering the weights affect how often servers are chosen. If we consider Fastest which uses the time taken to get a response, altering the weights alters the bias in a similar way to least connections.

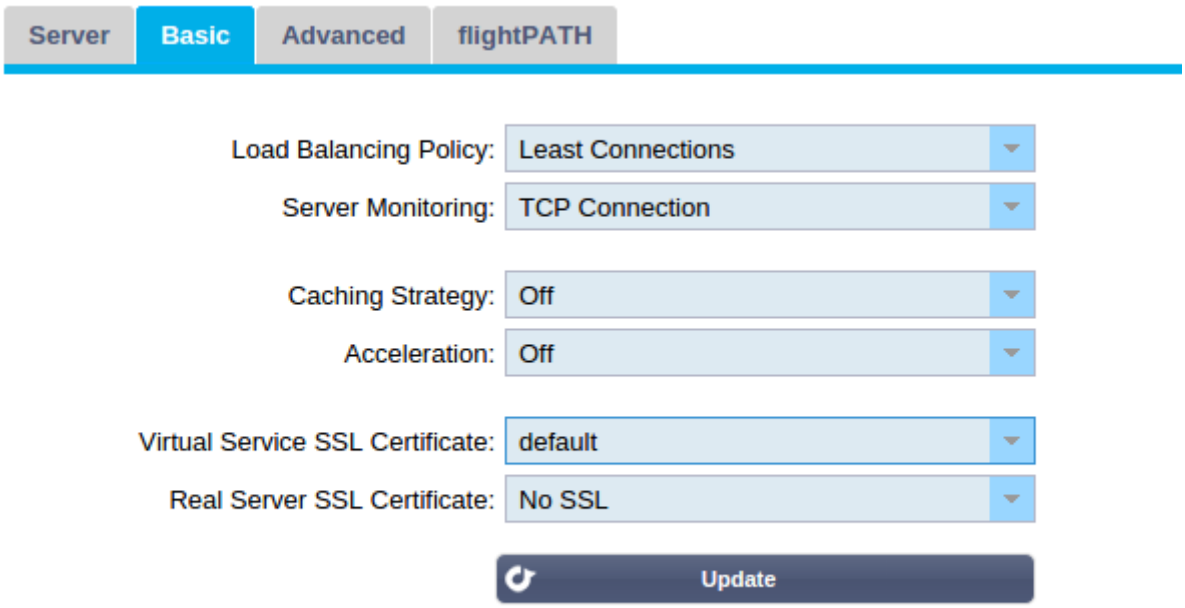
Calculated Weight

The calculated weight of each server can be viewed dynamically and is shown alongside the weight. This column is calculated automatically and cannot be edited by a user. This shows the actual weighting that ALB-X is using when considering manual weighting and load balancing policy.

Notes

Add in some useful notes about the particular server. Example “IIS Server1 – London DC”.

Basic



Load Balancing Policy

Select from the drop down list how you would like the traffic to be load balanced.

Fastest:

This load balancing policy will automatically calculates the response time for all request per server smoothed over time. The effects of this filtering can be viewed in the **Calculated Weight** column. A weighting can be entered manually when using this load balancing policy

Round Robin:

This is the simplest method. Each **Real Server** receives a new request in sequence. This method is useful to load balance evenly however it does not take in to account how busy each server is and can add to the burden of busy servers.

Least Connections:

The load balancer will keep track of the number of current connections to each **Real Server**. The **Real Server** with the least amount of connections will be sent the next new request.

Layer 3 Session Affinity/Persistence:

IP Bound:

In this situation the client's IP address is used to select which back end server will receive the request. This provides persistence. It can be used with HTTP or layer 4 protocols. This method is useful for internal networks where the network topology is known and you can be confident that there are no "super proxies" upstream. With layer 4 and proxies, all the requests can look as if they are coming from one client, and as such the load would not be even. With HTTP, X-Forwarded-For information is used, if present, to cope with proxies.

IP List Based:

The initial connection to the **Real Server** is made using "Least connections" then session affinity is achieved based on Clients IP. A list is maintained for 2 hours by default but this can be changed using a jetPACK

Layer 7 Session Affinity/Persistence:

ALB Session Cookie:

This is the one of the most popular persistence method for HTTP. In this situation, IP list based load balancing is used for each first request. A cookie is inserted into the headers of the first http response. Thereafter, jetNEXUS ALB-X uses the

client cookie to route traffic to the same back end server. Again this is used for persistence, when the client must go to the same back end server each time. The cookie will expire after the session is closed.**ALB Persistent Cookie:**In this situation, IP list based load balancing is used for each first request. A cookie is inserted into the headers of the first http response. Thereafter, jetNEXUS ALB-X uses the client cookie to route traffic to the same back end server. Again this is used for persistence, when the client must go to the same back end server each time. The cookie will expire after 2 hours and the connection will be load balanced according to IP List Based algorithm This is a configurable time that can be changed using a jetPACK.

Session Cookie:

Classic ASP Session Cookie:

Active Server Pages (ASP) is a Microsoft server-side technology. With this option selected the ALB-X will maintain session persistence to the same server if an ASP cookie is detected and is found in its list of known cookies. If a new ASP cookie is detected then it will be load balanced using the least connections algorithm.

ASP.NET Session Cookie: ASP.NET is a Microsoft server-side technology. With this option selected the ALB-X will maintain session persistence to the same server if an ASP.NET cookie is detected and is found in its list of known cookies. If a new ASP.NET cookie is detected then it will be load balanced using the least connections algorithm.

JSP Session Cookie: Java Server Pages (JSP) is an Oracle server-side technology. With this option selected the ALB-X will maintain session persistence to the same server if a JSP cookie is detected and is found in its list of known cookies. If a new JSP cookie is detected then it will be load balanced using the least connections algorithm.

JAX-WS Session Cookie: Java web services (JAX-WS) is an Oracle server-side technology. With this ption selected the ALB-X will maintain session persistence to the same server if a JAX-WS cookie is detected and is found in its list of known cookies. If a new JAX-WS cookie is detected then it will be load balanced using the least connections algorithm.

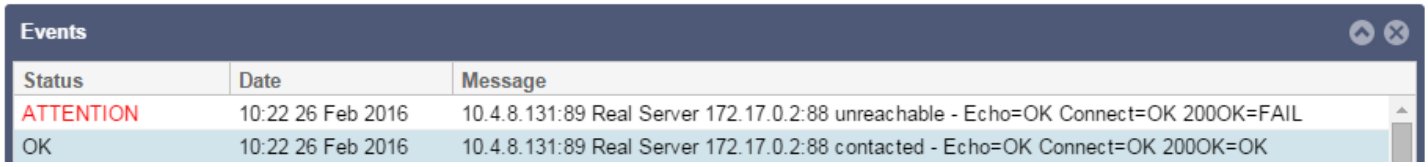
PHP Session Cookie: Personal Home Page (PHP) is an open source server-side technology. With this option selected the ALB-X will maintain session persistence to the same server if a PHP cookie is detected.

RDP Cookie Persistence:

This load balancing method uses the Microsoft created RDP Cookie based on user-name/domain to provide persistence to a server. The advantage of this is to maintain a connection to a server even if the IP address of the client changes.

Server Monitoring

Your jetNEXUS ALB-X contains six standard **Real Server Monitoring** methods listed below. Choose one to apply to the **Virtual Service**. Please make sure that you apply a relevant monitor to the **Virtual Service**. If the **Real Server** is an RDP server then a 200 OK monitor is not relevant. If you are unsure which monitor to choose, the default **TCP Connect** is a good place to start. New in version 4.2.0 is the ability to select multiple monitors. Simply cick each monitor you wish to apply to the service in turn. They will be executed in the order you select them so it best to start with monitors of the lower layers first. Example Select Ping/ICMP Echo, TCP Connection, 200OK. You can see the results of this monitor in the Dashboard Events and it will look similar to the image below:



If we look at the top line we can see that layer 3 **Ping** and layer 4 **TCP Connect** has succeeded and layer 7 **200OK** has failed so this provides enough information to indicate that routing is fine and there is a service running on the relevant port but the web site is not responding properly for the page requested. It's now time to look at the web server and the **Library — Real Server Monitor** section to see the details of the failing monitor.

None:

In this mode, the content server is not monitored at all and is assumed to be always up and running correctly. This is useful for situations where monitoring upsets a server and for services that should not join in the fail-over action of ALB-X. It can be viewed as a way of hosting unreliable or legacy systems that are not core to H/A operation. This monitoring method can be used with any service type.

Ping/ICMP Echo:

In this mode, ALB-X sends an ICMP echo request to the IP of the content server. If a valid echo response is received, the content server is deemed to be up and running and traffic will be sent to it. It will also then keep the service available on an H/A pair. This monitoring method can be used with any service type

TCP Connection:

In this mode, a TCP connection is made to the content server and immediately broken without sending any data. If the connection succeeds, the content server is deemed to be up and running. This monitoring method can be used with any TCP service type. UDP services are the only ones currently not appropriate for TCP Connection monitoring

ICMP Unreachable:

The ALB-X will send a UDP health check to the server and will mark the server down if it receives an ICMP port unreachable message. This can be useful when you need to check if for a UDP service port is available on a server such as DNS port 53

RDP:

In this mode, a TCP connection is made as above, but after the connection is made a layer 7 RDP connection is requested. If the connection is confirmed the content server is deemed to be up and running. This monitoring method can be used with Microsoft terminal servers

200 OK:

In this mode, a TCP connection is made to the content server as above, but after connection is made, a brief HTTP request is made to the content server. A HTTP response is waited for and it is checked for the “200 OK” response code. If the “200 OK” response code is received, the content server is deemed to be up and running. If, for any reason, the “200 OK” response code is not received, including timeouts, failure to connect, etc, then the content server is regarded as down. This monitoring method can only really be used with HTTP and Accelerate HTTP service types, although if a Layer 4 Service Type is in use for an HTTP server, it could still be used if SSL is not in use on the content server, or is handled appropriately by the “Content SSL” facility

DICOM:

In this mode, a TCP connection is made to the content server as above, but after a connection is made, an Echoscu “Associate Request” is made to the content server. A conversation that includes an “Associate Accept” from the content server, a transfer of a small amount of data followed by a “Release Request” then “Release Response” successfully concludes the monitor. If for any reason the monitor does not complete successfully then the content server is regarded as down

User Defined:

Any monitor configured in the Real Server Monitoring section will appear in the list

Caching Strategy

By default the caching strategy is set to Off. If your service type is HTTP then you can apply two types of caching strategy. Please refer to the Configure Cache page to configure detailed cache settings. Note that when caching is applied to a service with service type “Accelerate HTTP”, objects that are compressed will not be cached.

By Host:

Caching is applied on a per host name basis. A separate Cache will exist for each domain/host name. Ideal for web servers that can serve multiple websites depending on the domain.

By Virtual Service:

Caching is applied per virtual service. Only one Cache will exist for all domain/host names that pass through the virtual service. This is a specialist setting for use with multiple clones of a single site.

Acceleration

Off:

Turn compression off for the Virtual Service

Compression:

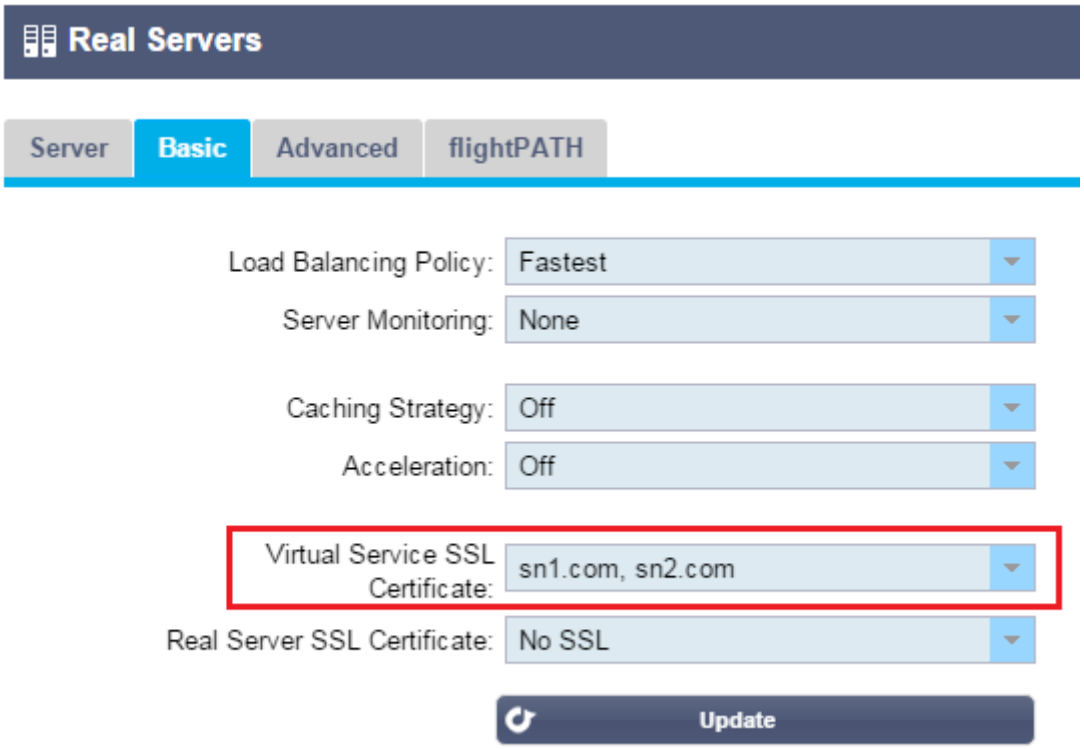
Turn compression on for the Virtual Service. Traffic from the ALB-X to the client will be dynamically compressed upon request. This only applies to objects that contain the content-encoding: gzip header. Example html css or javascript. You can also exclude certain content types from the Global Exclusions section. Note: If the object is cachable we will store a compressed version and serve this statically (from memory) until the content expires and it is revalidated.

Virtual Service SSL Certificate (Encryption between Client and ALB-X)

By default this is set to No SSL. If your service type is “HTTP” or “Layer4 TCP” you can select a certificate from the drop down box to apply to the Virtual Service. Certificates that have been created or imported will appear in this list. You may now highlight multiple certificates to apply to a service. This will automatically enable the SNI extension to allow the presentation of a certificate based on the "Domain Name" requested by the client.

Server Name Indication:

This is an extension to the TLS networking protocol by which the client indicates which hostname it is attempting to connect to at the start of the handshaking process. This allows the ALB-X to present multiple certificates on the same virtual IP address and TCP port.



No SSL:

Traffic from the browser to the ALB-X will not be encrypted

Default:

A locally created certificate called “Default” is applied to the browser side of the channel. This can be used to test SSL when one hasn’t been created or imported

UserCertificate1:

A locally created, imported or signed certificate is applied to the client side of the Virtual Service

Real Server SSL Certificate (Encryption between ALB-X and Real Server)

By default this is set to No SSL. If your server requires an encrypted connection then this must be set to anything other than No SSL. Certificates that have been created or imported will appear in this list.

No SSL:

Traffic from the ALB-X to the content server will not be encrypted. If a certificate has been selected – on the browser side, “No SSL” can be selected client-side to provide what is known as “SSL Offload”.

UserCertificate1:

Traffic from the ALB-X to the content server will be encrypted provided the named certificate is presented by the real server. If a certificate has been selected – on the Virtual Service side, “UserCertificate1” can be selected to provide what is known as “SSL Bridging” or “SSL Re-Encryption”.

UserCertificate2:

A 2nd locally created, imported or signed certificate is applied to the client side of the Virtual Service. If you select more than one certificate here then SNI will be enabled automatically.

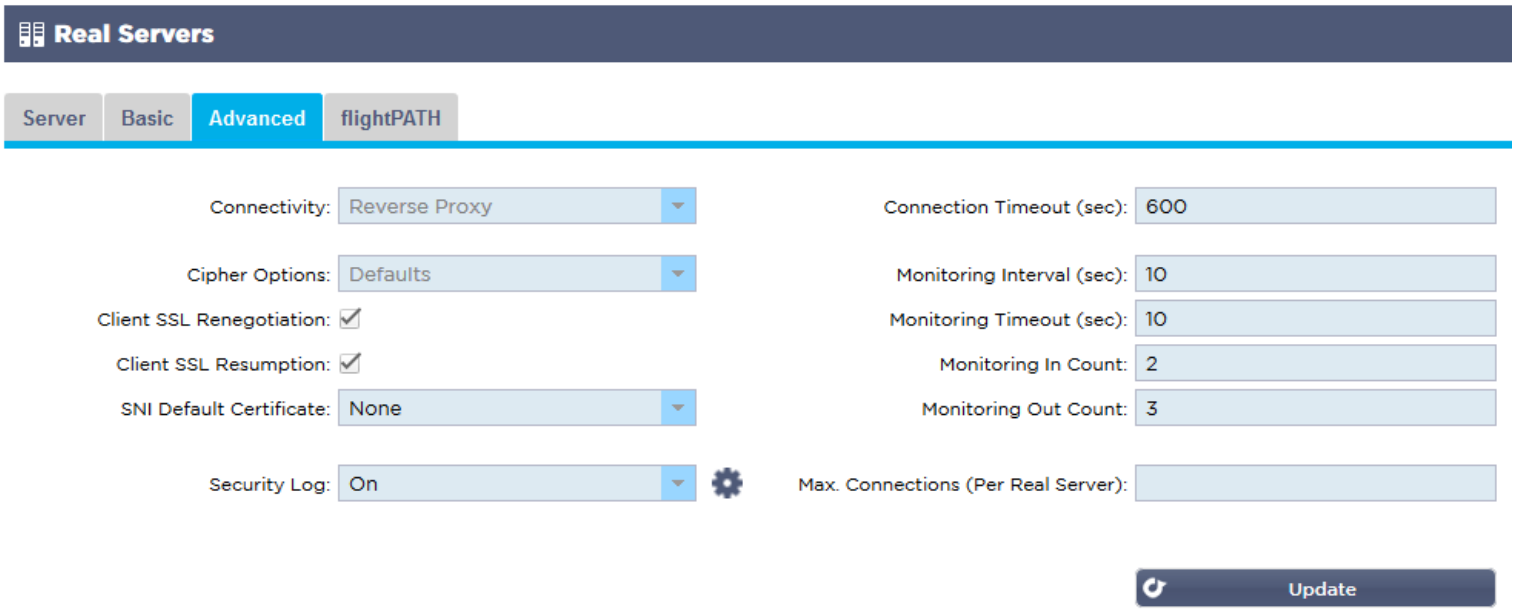
Any:

The ALB-X acts as a client and will accept any certificate the content server presents. Traffic from the ALB-X to the content server will be encrypted if this is selected. If a certificate has been selected – on the Virtual Service side, “Any” can be selected to provide what is known as “SSL Bridging” or “SSL Re-Encryption”.

SNI:

Choose this option to enable SNI on the server side.

Advanced



Connectivity

Your Virtual Service can be configured with four different types of connectivity. Please select one to apply to the service.

Reverse Proxy:

This is the default setting for jetNEXUS ALB-X and works at layer7 with compression and caching and also at layer4 without caching and compression. In this mode your jetNEXUS ALB-X acts as a reverse proxy and becomes the source address seen on the content servers.

Direct Server Return:

Direct Server Return or DSR as it's widely known (DR – Direct Routing in some circles) allows the server behind the load balancer to respond directly to the client bypassing the edgeNEXUS on the response. DSR is suitable for using with Layer 4 load balancing only. Therefore Caching and Compression are not available when enabled.
Layer 7 load balancing with this method will not work therefore there is no persistence support other than IP List Based.
SSL/TLS load balancing with this method is not ideal as there is only source IP persistence support. This method requires content server changes. Please refer to the real server changes section.

Gateway:

Gateway mode allows you to route all traffic through the jetNEXUS, this allows traffic from the content servers to be routed via the edgeNEXUS to other networks via the interfaces on the edgeNEXUS unit. Using the device as a gateway device for content servers should be used when running in multi interface mode. Layer 7 load balancing with this method will not work therefore there is no persistence support other than IP List Based. This method requires that the content server sets its default gateway to the local interface address (eth0, eth1, etc….) of the jetNEXUS ALB-X. Please refer to the real server changes section.

Cipher Options

As of software version 4.1.1 you can now set the ciphers per service. This is only relevant for services with SSL/TLS enabled. The default cipher will be chosen automatically. You can add different ciphers using jetPACKS available at the following URL Once the jetPACK's have been added you will be able to set the Cipher options per service. The benefit of this is that you can create a number of services with varying levels of security. Be aware that older clients are not compatible with newer ciphers and so you will be reducing the number of clients the more secure the service.

Client SSL Renegotiation:

Tick this box if you wish to allow client initiated SSL renegotiation. To prevent possible Dos attack against the SSL layer it is advisable to un-tick this box to disable client SSL renegotiation.

Client SSL Resumption:

Tick this box if you wish to enable SSL Resumption Server sessions are added to the session cache. When a client proposes a session to be reused, if the session is found, the server will try to reuse the session. If Resumption not checked, no session caching for client or server takes place.

SNI Default Certificate:

During an SSL connection with Client side SNI enabled if the requested domain does not match any of the certificates assign to

the service then it will present the SNI Default Certificate. The default setting for this is **None** which would effectively drop the connection should there be no exact match, Choose any of the certificates installed from the drop down box to present should an exact match fail.

Security Log:

This setting is turned on by default on a per service basis which means that the service is capable of logging authentication information to the W3C logs. Clicking the Cog icon will take you to the **System — Logging** page where you can check if W3C logging is set to anything other than **None** with the security information turned on.

Connection Timeout

The default setting for this is 600 seconds or 10 minutes. This setting will adjust the time for the connection to timeout out upon no activity. Reduce this for short lived stateless web traffic which is typically 90s or less. Increase this figure for stateful connections such as RDP to something like 7200 seconds (2 hours) or more depending on your infrastructure. This means that if a user has a period of inactivity of 2 hours or less the connections will still remain open.

Monitoring Settings

These settings are tied to the Real Server Monitors in the Basic tab. There are global entries in the configuration to count the number of successful or failed monitors before a server is allowed online or marked as failed.

Interval

The interval is the time in seconds between monitors. The default interval is 1s. Whilst 1s is acceptable for most applications it may be beneficial to increase this for other applications or during to testing.

Monitoring Timeout

The timeout value is the amount of time the ALB-X will wait for a server to respond to a connection request. The default value is 2s. This value may need to be increased for busy servers.

Monitoring In Count

The default value for this setting is 2. This means that the real server has to pass two successful health monitors before it will be brought online. Increasing this figure will increase the probability the server is capable of serving traffic but will take longer to come into service depending on the **Interval**. Decreasing this value will bring your server into service sooner.

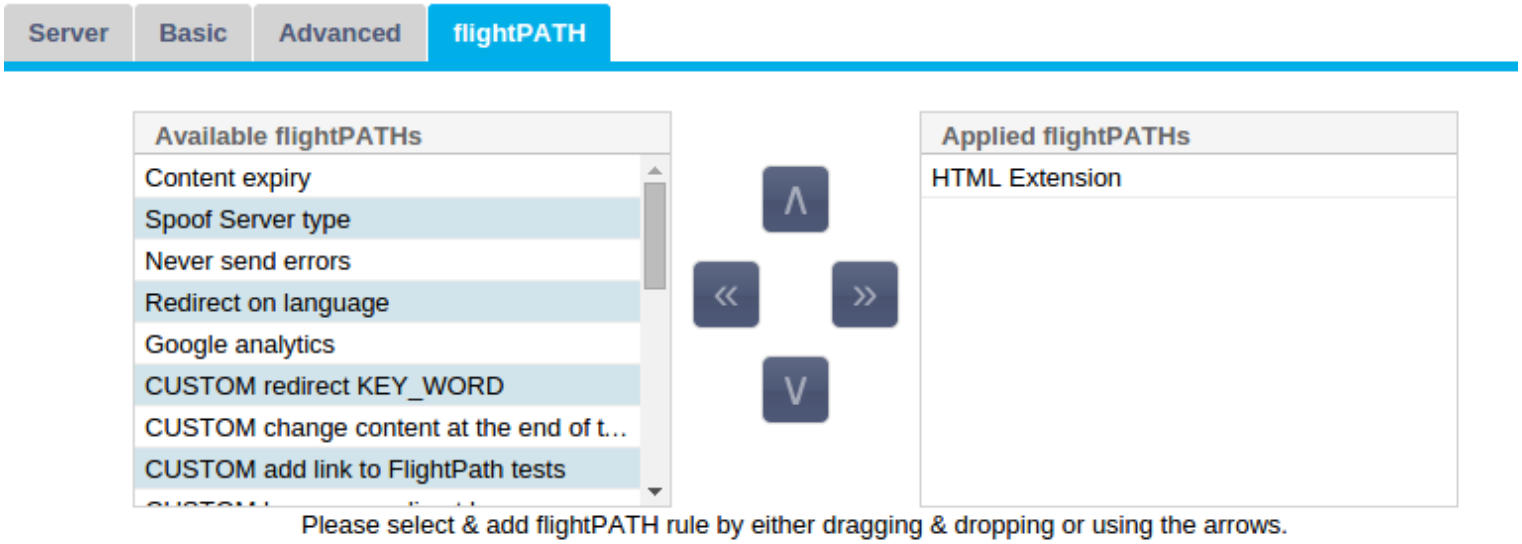
Monitoring Out Count

The default value for this setting is 3. This means that the real server monitor has to fail 3 times before the ALB-X will stop sending traffic to the server and it is marked RED and “Unreachable”. Increase this figure will result is a more reliable service at the expense of the time it takes the ALB-X to stop sending traffic to this server.

Max. Connections

This limits the number of simultaneous real server connections and can be set per service. For example if you set this to 1000 and have two real servers then the jetNEXUS ALB-X will limit EACH real server to 1000 concurrent connections. You may also choose to present a “Server too busy” page, once this limit is reached on all servers, helping users in this case. Leave this blank for unlimited connections. This will depend on your system resources.

flightPATH



- flightPATH rules are designed to manipulate HTTP(s) traffic. As such, the option for flightPATH is only visible if for Service Type “HTTP”
- The list of available rules is on the left and the current rules applied to the virtual service are on the right
- To add a new rule drag and drop the rule into position or highlight a rule and click the right arrow
- The order for execution is important and will start with the top rule being executed fist. To change the order highlight a rule and use the arrows to move up or down the list.
- To remove a rule simply drag and drop it back to the rule inventory or highlight the rule and click the left arrow
- You can add, remove and edit flightPATH rules in the Configure flightPATH section.

Add-Ons

The **Library — Add-Ons** page is the location of all of your deployed **Add-Ons**. If this page is blank it means that you have not deployed any **Add-Ons** yet. You can view your available **Apps** in the **Library — Apps** page. Here you will need to first **Download** the **App** and then the **Deploy** button will become available. You may **Deploy** more than one type of **Add-On**. For example you may want to deploy two instances of a Firewall **Add-On** for different services.

User Guides for Add-Ons

Application Firewall Add On

Global Server Load Balancer Add On

What’s an Add-On?

Add-Ons are Docker based Containers that can run in isolation on your ALB-X load balancer. Examples of these include an application firewall and a micro instance of a jetNEXUS ALB-X.

Purchasing an Add-On

- Click on the edgeNEXUS Add-On icon you require.
- You will see more information about the Add-On.
- You can then choose how many you would like to download. If you are accessing the App Store from within your ALB-X please choose only 1.
- If you are accessing direct from the website you may choose multiple and you can assign the correct MachineID to the App later in the process.
- Click Add to Cart. (These are often free)

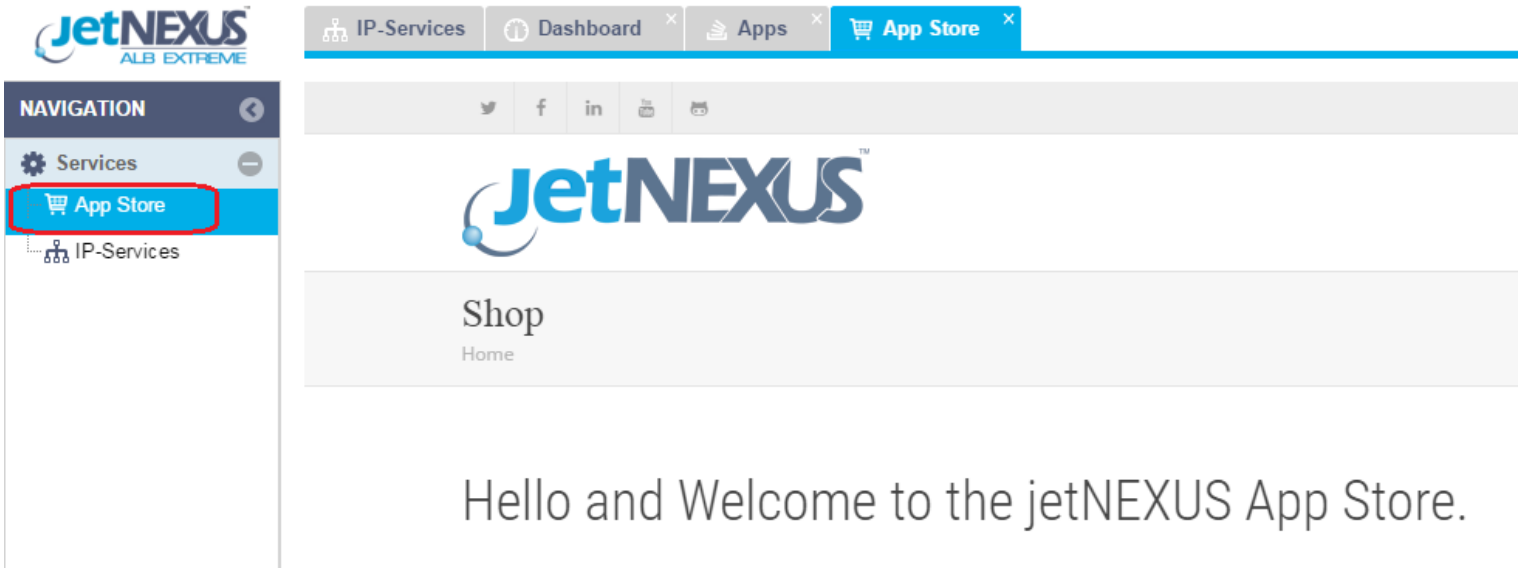
- Proceed to Checkout.
- Here you will be asked to login if you are a returning customer.
- Alternatively you can fill out your billing details and tick the box to create an account. You will not be charged for products that are free.
- Click Place Order.
- You should now be presented with a screen that allows you download your product manually by entering the MachineID and clicking Download.
- If the download is blanked out then you have already tied a purchase to another ALB-X.
- If you have purchased from within an ALB-X via the Services — App Store page then you can now see your purchased Apps in the Library — Apps page.
- Once you have purchased your Add-On, the first step is to find it in the Library–Apps page and click the green Download button

Application Firewall Add On

The **Library — Add-Ons** page is the location of all of your deployed **Add-Ons**. If this page is blank it means that you have not deployed any **Add-Ons** yet. You can view your available **Apps** in the **Library — Apps** page. Here you will need to first **Download** the **App** and then the **Deploy** button will become available. You may **Deploy** more than one type of **Add-On**. For example you may want to deploy two instances of a Firewall **Add-On** for different services.

Buying an Application Firewall Add-On

- You can access the **App Store** direct at https://appstore.edgenexus.io or open the **Services — App Store** page from within your **ALB-X**

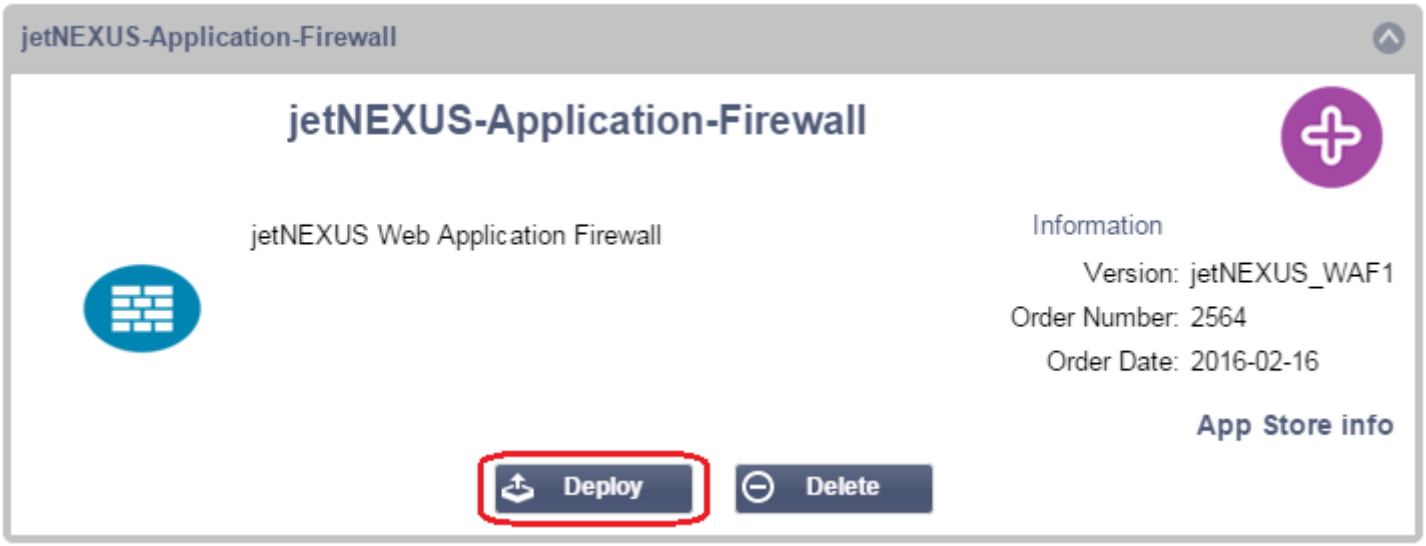


- Click on the **Add-On** icon

- Click on the **edgeNEXUS Application Firewall** icon

- You will see more information about the Application Firewall
- You can then choose how many you would like to download. If you are accessing the **App Store** from within your **ALB-X** please choose only 1
- If you are accessing direct from the website you may choose multiple and you can assign the correct **MachineID** to the App later in the process
- Click **Add to Cart**. (These are often free)
- **Proceed to Checkout**.
- Here you will be asked to login if you are a returning customer
- Alternatively you can fill out your billing details and tick the box to create an account. You will not be charged for products that are free
- Click **Place Order**
- You should now be presented with a screen that allows you download your product manually by entering the **MachineID** and clicking **Download**
- If the download is blanked out then you have already tied a purchase to another ALB-X
- If you have purchased from within an **ALB-X** via the **Services — App Store** page then you can now see your purchased Apps in the **Library — Apps** page
- Once you have purchased your Firewall App, the first step is to find it in the **Library–Apps** page and click the green **Download** button

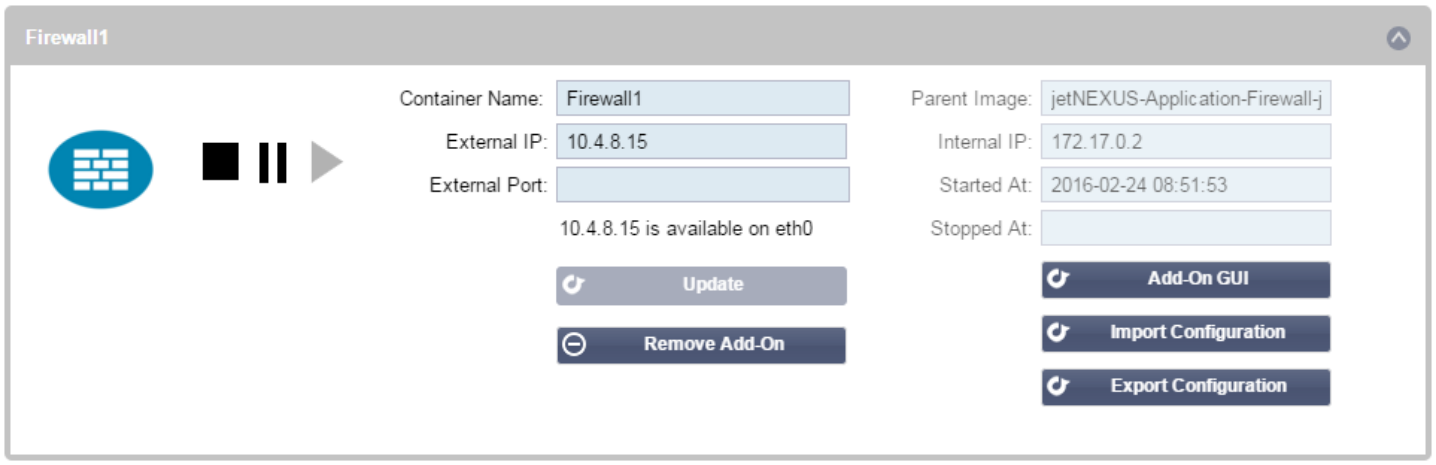
- Once your Firewall has been downloaded you will be able to click the **Deploy** button (it will be greyed out if the Firewall has not been downloaded)



- Once you click **Deploy** your Firewall will be deployed in the **Library — Add-Ons** page

Running your Application Firewall

All **Add-Ons** run in a Docker Container and therefore have some networking constraints. Once you have deployed your **Add-On** you will be able to set some parameters and start it



Stop:

This will be greyed out until an Add-On instance is started. Press this button to Stop the Docker instance

Pause:

This button will pause the Add-On

Play:

This will start the Add-On with the current settings

Container name:

Give your container a name to identify it from the other containers. This must be unique. You may use this as the name for a Real Server if you wish and it will resolve automatically to the **Internal IP** address of the instance

External IP:

Here you can set an **External IP** to access your **Add-On**. This may be to access the GUI of the **Add-On** as well as the service that runs via the **Add-On**.
In the case of the Firewall **Add-On** this is the IP address of your HTTP service. The Firewall can then be configured to access a server or an ALB-X VIP that contains multiple servers for load balancing.

External Port:

If you leave this blank then all ports will be forwarded to your Firewall. To restrict this then simple add in the comma separated port list. Example 80, 443, 88. Note the Firewall GUI address will be **http://[External IP]:88/waf** So either leave the **External Port** setting blank or add in port 88.to access the GUI if you are restricting the port list.

Update:

You can only update the settings of an **Add-On** once it has been stopped. Once your instance has stopped you can change the **Container name**, **External IP** and **External Port** settings.

Remove Add-On:

This will completely remove the **Add-On** from the **Add-On** page. You will need to go to the **Library–Apps** page to deploy the

Add-On again.

Parent Image:

This indicates the Docker image that the **Add-On** is built from. There might be several versions of a Firewall or indeed another type of **Add-On** completely so this will help to distinguish between them. This section is for informational purposes only and therefore is greyed out.

Internal IP:

The internal IP address is automatically created by Docker and therefore cannot be edited. If you stop the Docker instance and restart, a new internal IP address will be issued. It is for this reason that you should either use an **External IP** address for you service or you use the **Container Name** for the Real Server Address of your service.

Started At:

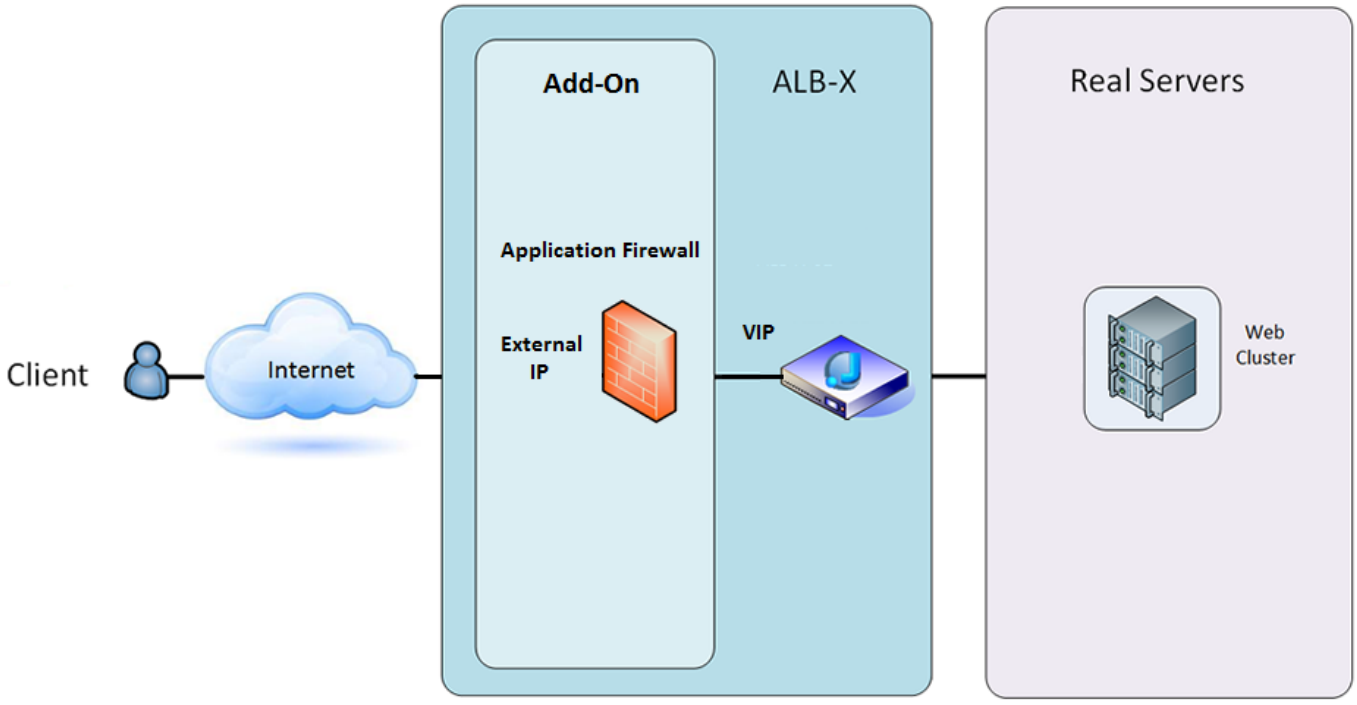
This will state the date and time the **Add-On** was started. Example 2016-02-16 15:57:21

Stopped At:

The will state the date and time the **Add-On** was stopped. Example 2016-02-24 09:58:39

Example Architecture

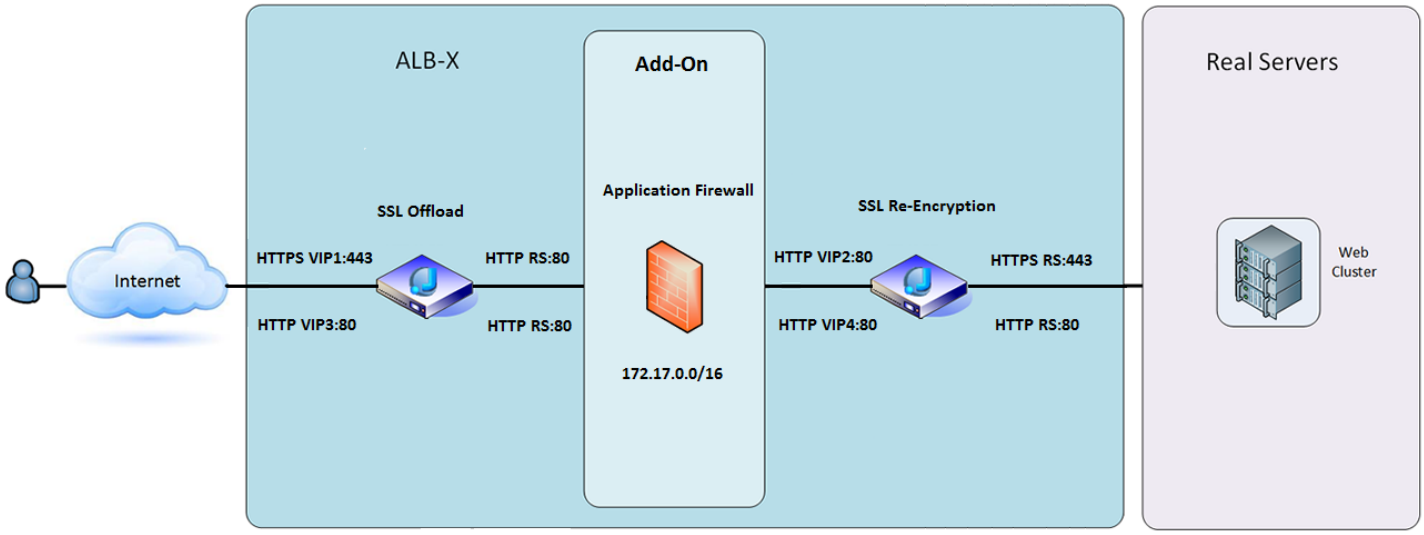
Firewall Using External IP Address:



- In this architecture only HTTP can be used for your service as the Firewall cannot inspect HTTPS traffic.
- The Firewall will need to be configured to send traffic on to the ALB-X VIP.

- The ALB-X VIP in turn will be configured to load balance traffic to your web cluster.

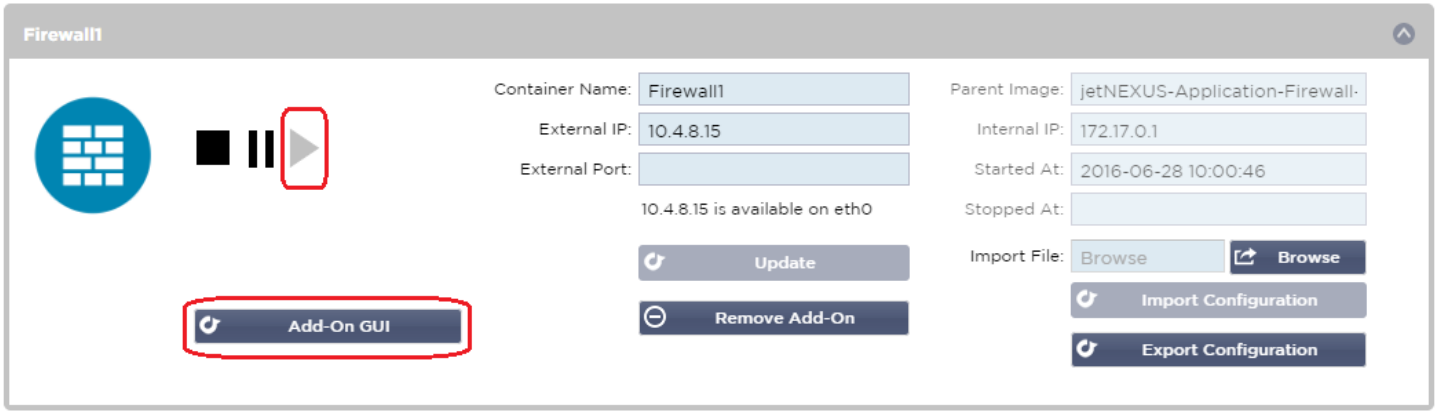
Firewall Using Internal IP Address:



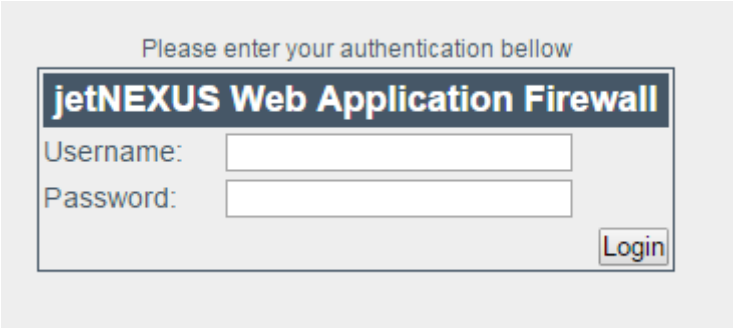
- In this architecture you can specify HTTP and HTTPS.
- HTTPS can be end to end where the connections from the Client to ALB-X are encrypted and also from the ALB-X to the Real Servers.
- The traffic from the ALB-X to the internal IP address of the firewall needs to be un-encrypted so that it can be inspected.
- Once the traffic has passed through the Firewall it is then forwarded on to another VIP which can then either re-encrypt the traffic and load balance to secure servers or simply load balance to insecure servers over HTTP.

Accessing your Firewall Add-On

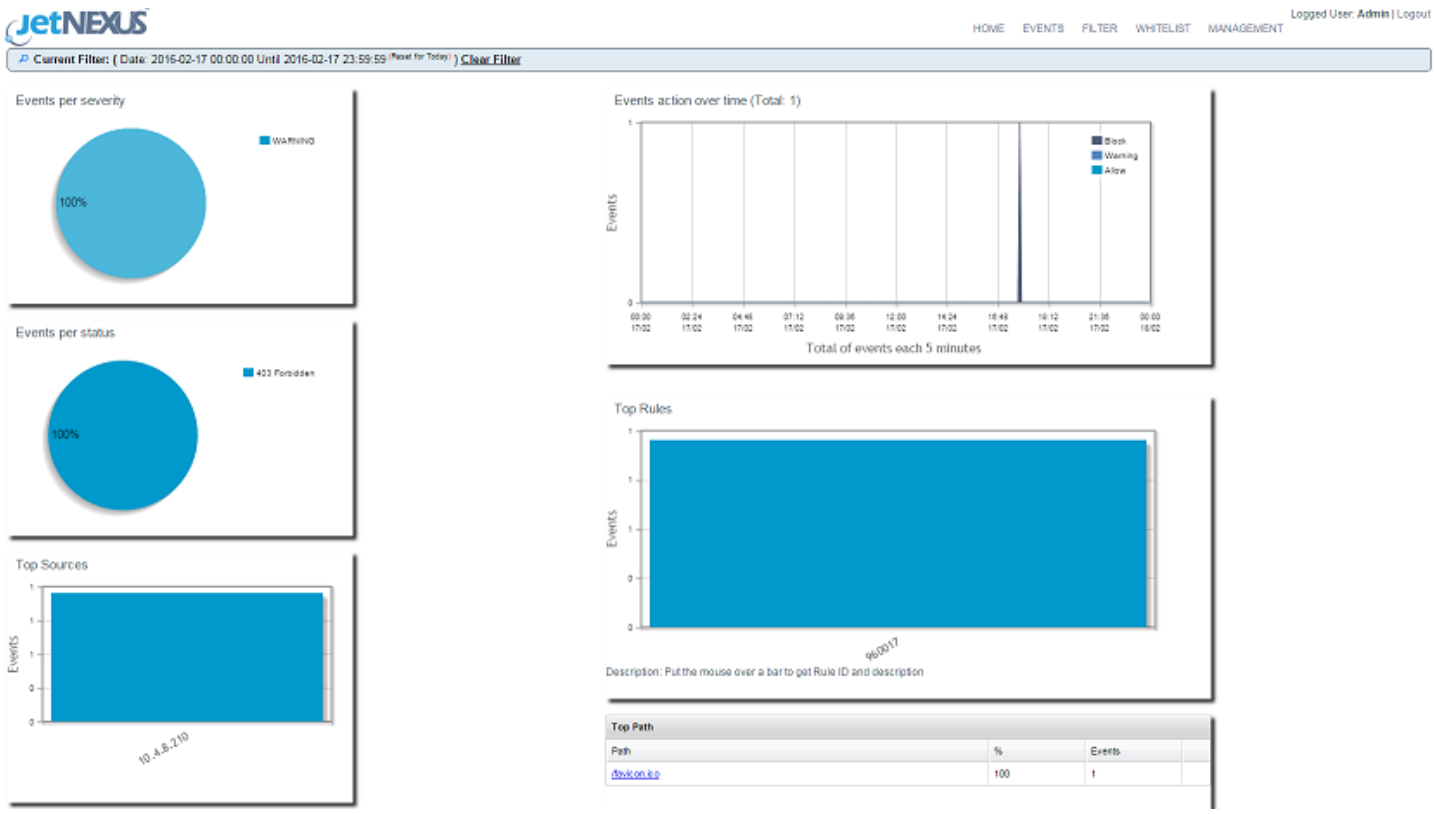
- Fill out the details for your Firewall
- You can either restrict your Ports to what you need or leave it blank to allow all ports
- Click the Play button
- An Add-On GUI button will appear



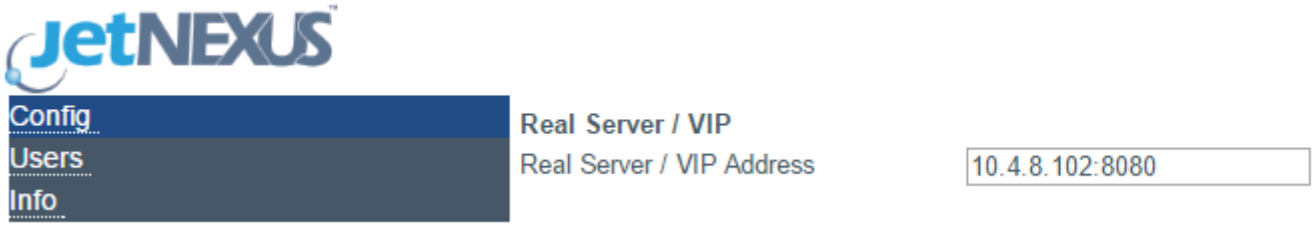
- Click on this button and it will open up a browser on **http://[External IP]:88/waf** in this example it will be **http://10.4.8.15:88/waf**



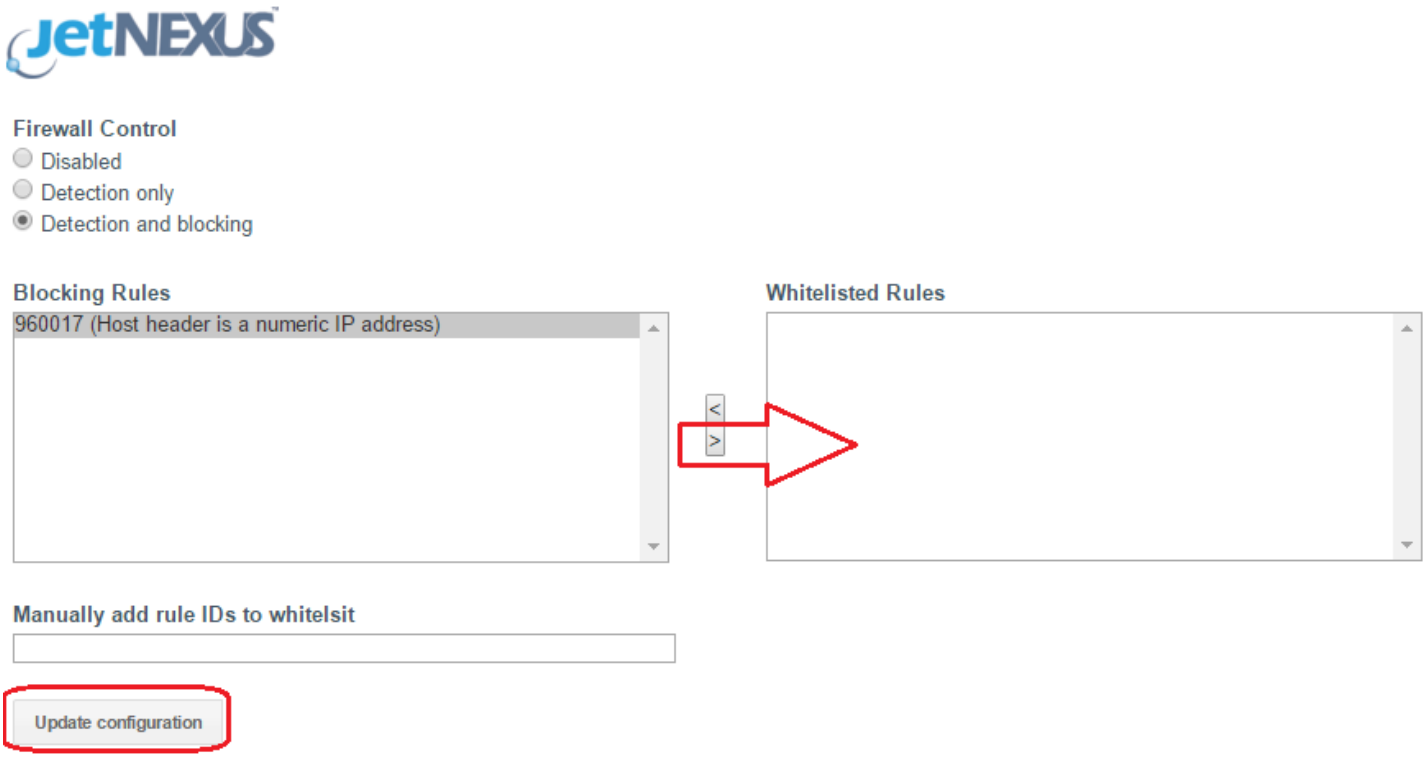
- Username: admin
- Password: jetnexus
- It is recommended to change the default password in the **Management-Users** section
- After logging in you will see the home page of the Application Firewall



- The home page displays a graphical overview of the events, i.e. filtering actions performed by the Application Firewall.
- The graphs will most likely be blank when you first open the page as there will be no access attempts through the firewall.
- You can configure the IP address or the domain name of the web site you will like to send the traffic to after it has been filtered by the firewall.
- This is changed in the **Management—>Config** section



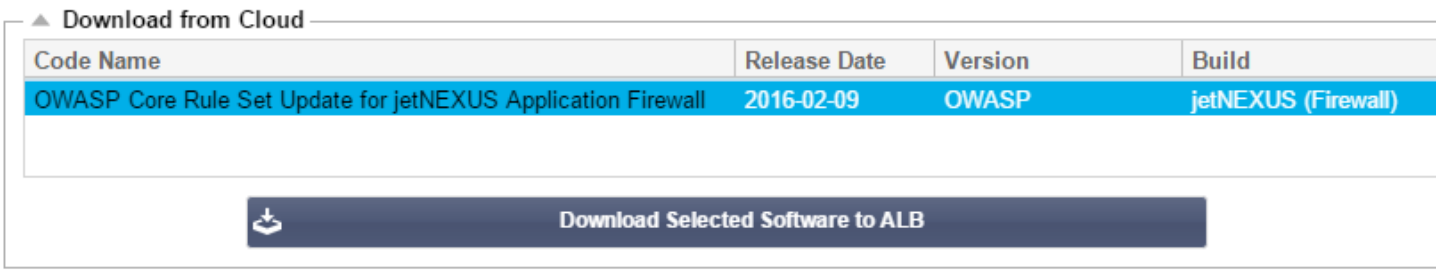
- The Firewall will inspect the traffic and then send it on to the Real Sever IP or VIP address here. You may also enter a port along with your IP address. If you just enter an IP address on its own the port will be assumed to be port 80. Click the "Update Configuration" button so save this new setting.
- When the Firewall blocks an application resource, the rule that is blocking traffic will appear in the **Blocking Rules** list on the **Whitelist** page.
- In order to prevent the firewall from blocking the valid application resource, please move the blocking rule to the **Whitelist Rules** section.



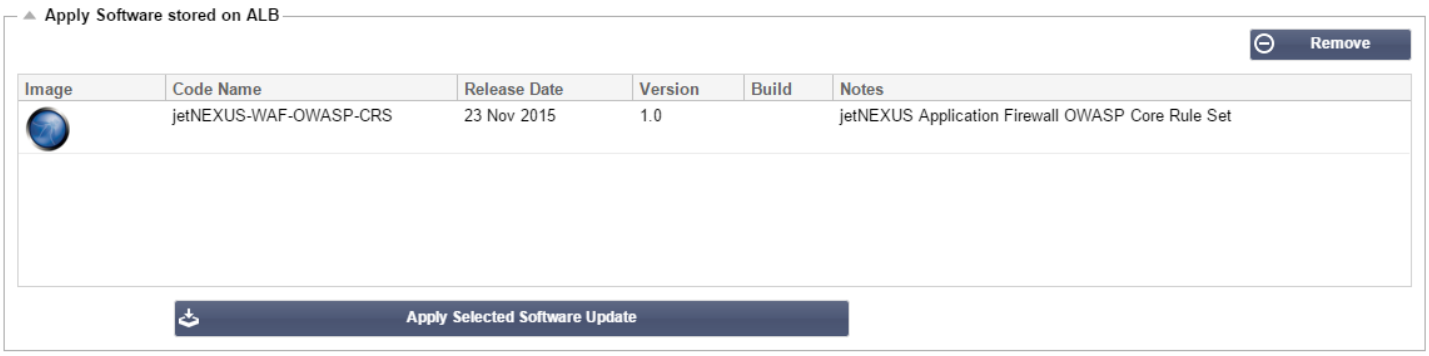
- Press Update Configuration when you have transferred all the rules from the Blocking section to the Whitelist section.

Updating Rules

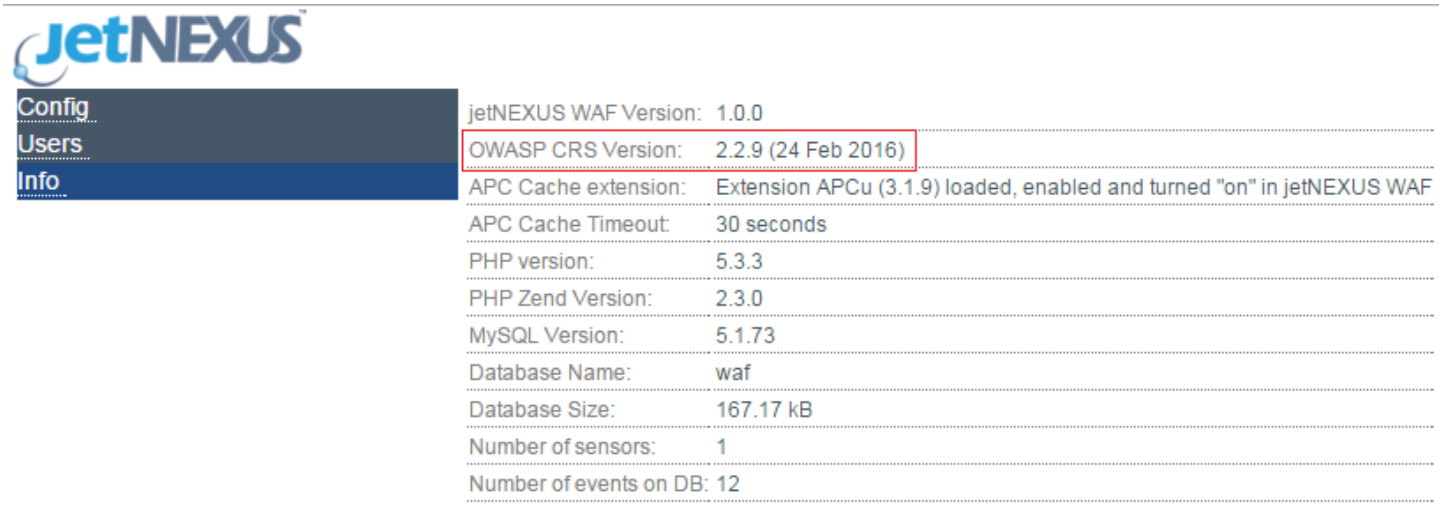
- edgeNEXUS Application Firewall rules can be updated by accessing the **Advanced — Software**
- Click the **Refresh to view available software** button in the **Software Upgrade Details** section
- This will reveal an additional box called **Download from Cloud**
- Check to see if you there is an OWASP Core Rule set available



- If so you can highlight and click **Download Selected Software to ALB-X**
- This will then download the smart file to the **Apply Software stored on ALB**



- Highlight the **jetNEXUS-WAF-OWASP-CRS** and click **Apply Selected Software Update** and click **Apply**
- The Firewall will automatically detect updated rule set, load and apply it.
- The IDs of Whitelisted rules will be kept, however new rules may start blocking valid application resources.
- Please check the Blocking Rules list on the Whitelist page in this case.
- You can also check the **Management Info** section of the Firewall GUI for the OWASP CRS Version



Apps

The **Library — Apps** page is the place to see all of the **Apps** that you have bought via the **edgeNEXUS App Store**. If this page is blank it means you have not bought any **Apps** yet, please visit the App Store.

What’s an App?

An **App** is anything bought on the **App Store**. There are different categories of **App** that can be installed on your ALB-X and a description of each can be found on the on the App Store page.

Click on an icon to show or hide an App. Hide flightPATHs

Show flightPATHs

Work Flow

Access App Store within ALB-X

- Purchase an App from the **Services — App Store** page
- Download the App from the **Purchased App** section of the **Library — Apps** page
- Deploy the App from the **Downloaded Apps** section of the **Library — Apps** page
- Apply your App depending on the kind of App deployed

    - **flightPATH**
        - **View or Edit Rule in the Library — flightPATH page**
        - **Apply the rule to a Virtual Service in the Services — IP-Service — flightPATH section**
- **Server Monitor**

- View or Edit the Monitor in the **Library — Real Sever Monitors** section
- Apply the rule to a **Virtual Service** in the **Services — IP-Service — Basic — Server Monitoring** section
- **jetPACK**

- A **jetPACK** is group of configuration changes that may or may not include **flightPATHs** and **Monitors**
- A **jetPACK** will generally add Virtual Services which can be viewed in the **Service — IP-Service** section
- **Add-Ons**
    - View, Edit or Start your **Add-Ons** in the **Library — Add-Ons** page
- **Feature Pack**
    - This will add a new feature so the first place to look would be the **System – Licence** page
    - If the **Feature Pack** contained **flightPATH** then you should now be able to see the **Library – flightPATH** section

Access App Store directly https://appstore.edgenexus.io

- Purchase an App from the App Store
- Add in the **MachineID** of your ALB-X then you will be able to download the App
- The App will take the form of an encrypted file <appname>.<apptype>.alb
- Upload the App from the **Advanced — Software** page
- Navigate to the **Upload Software to ALB** and click **Browse**
- Click **Upload Apps and Software**
- Deploy the App from the **Downloaded Apps** section of the **Library — Apps** page
- Apply your App depending on the kind of App deployed
    - **flightPATH**
        - **View or Edit Rule in the Library — flightPATH page**
        - **Apply the rule to a Virtual Service in the Services — IP-Service — flightPATH section**
- **Server Monitor**

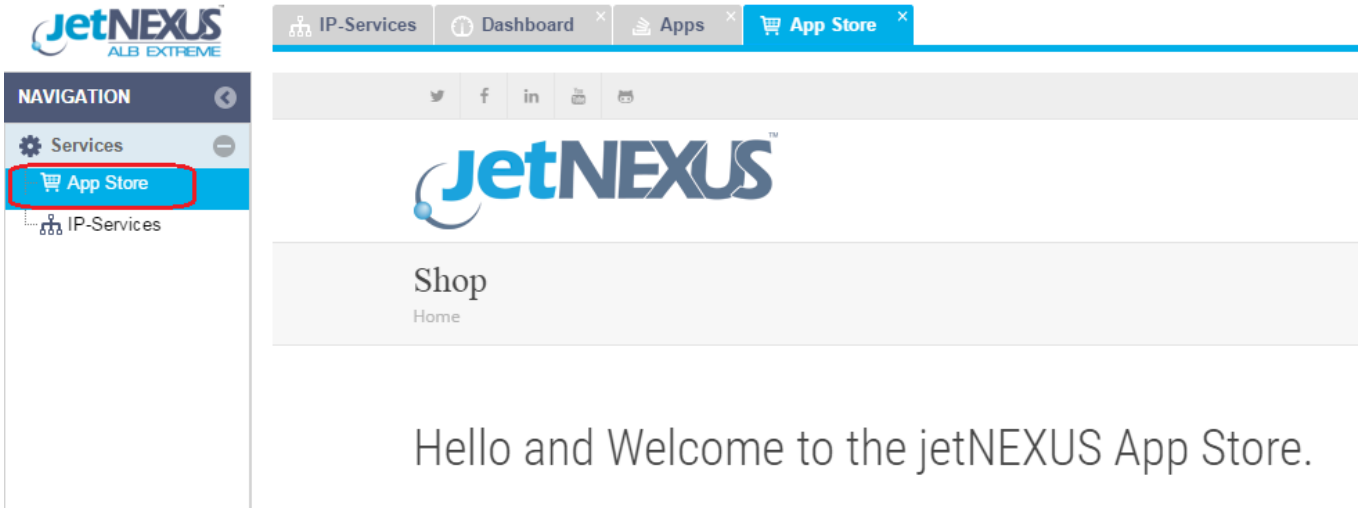
- View or Edit the Monitor in the **Library — Real Sever Monitors** section
- Apply the rule to a **Virtual Service** in the **Services — IP-Service — Basic — Server Monitoring** section
- **jetPACK**

- A jetPACK is group of configuration changes that may or may not include flightPATHs and Monitors
- A jetPACK will generally add Virtual Services which can be viewed in the **Service — IP-Service** section
- **Add-Ons**
    - View, Edit or Start your **Add-Ons** in the **Library — Add-Ons** page
- **Feature Pack**
    - This will add a new feature so the first place to look would be the **System – Licence** page
    - If the **Feature Pack** contained **flightPATH** then you should now be able to see the **Library – flightPATH** section

Purchasing an App

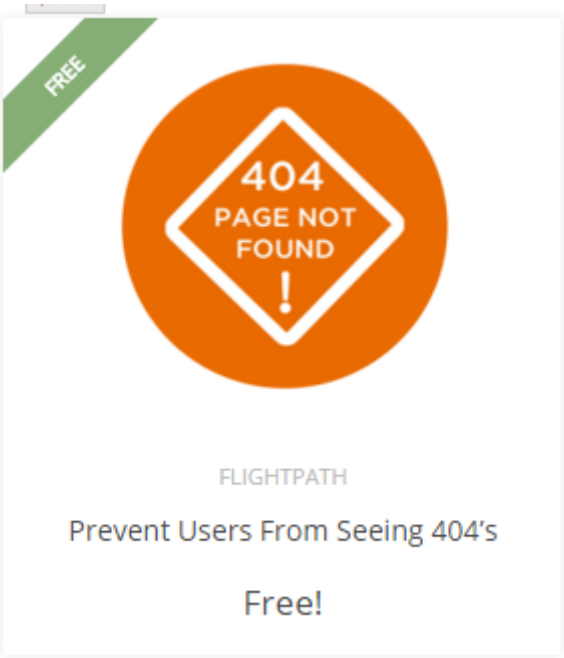
Buying a flightPATH App:

- You can access the**App Store** direct at https://appstore.edgenexus.io or open the **Services — App Store** page from within your **ALB-X**

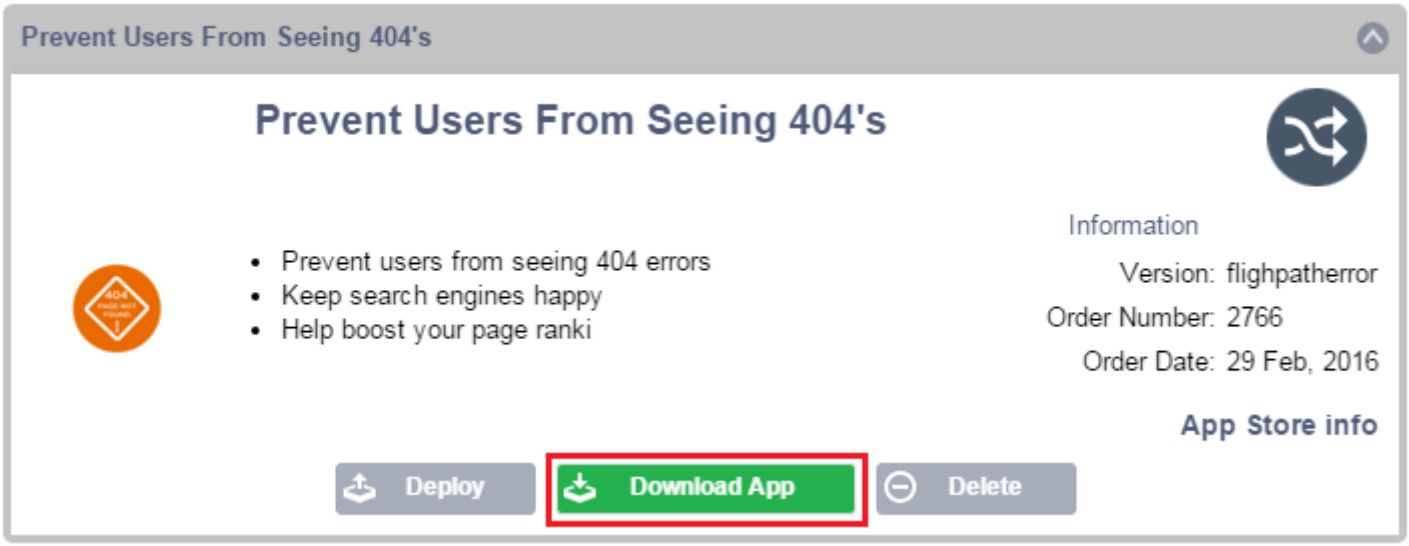


- Click on the **flightPATH** icon

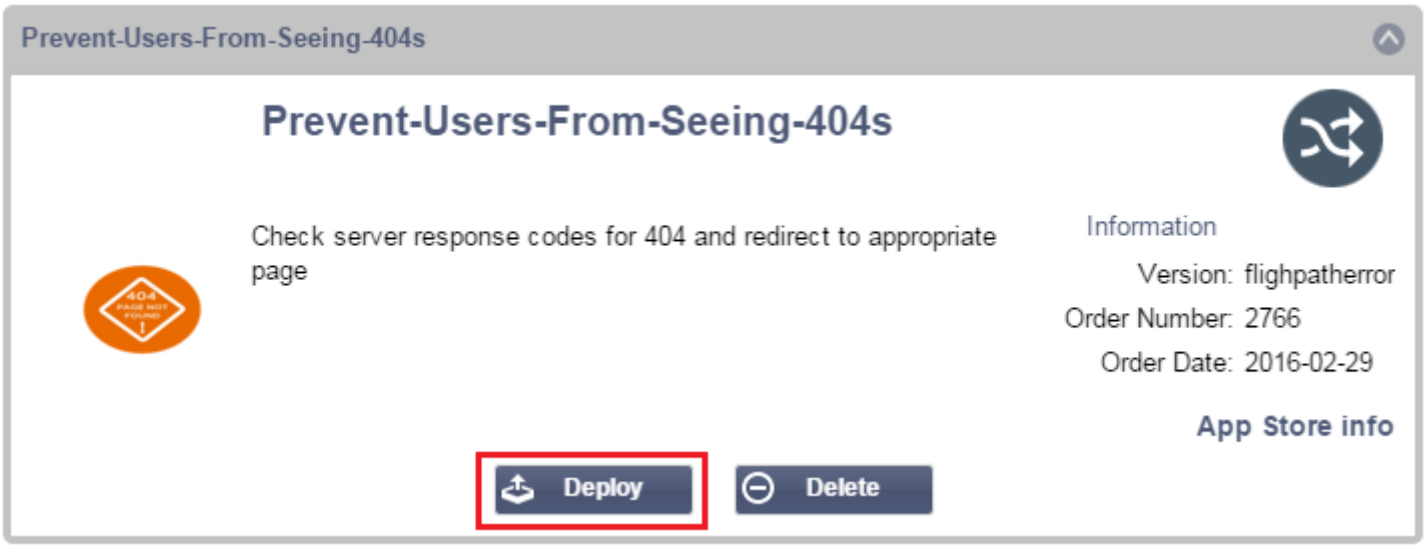
- Click on the **Prevent User From Seeing 404's** icon.



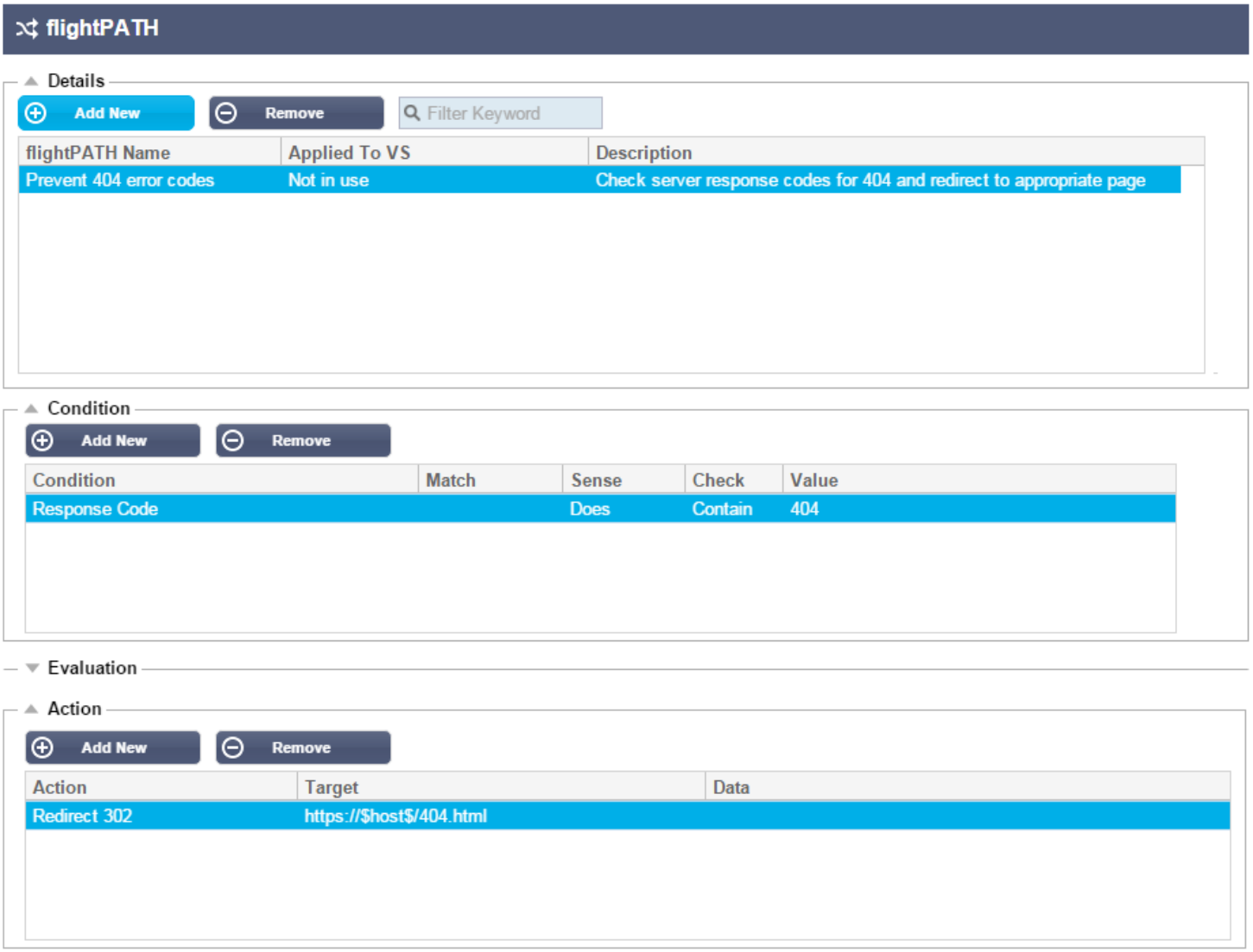
- You will see more information about the **flightPATH** rule
- You can then choose how many you would like to download. If you are accessing the **App Store** from within your **ALB-X** please choose only 1
- If you are accessing direct from the website you may choose multiple and you can assign the correct **MachineID** to the **App** once you have purchased
- Click **Add to Cart**. (These are often free)
- **Proceed to Checkout**
- Here you will be asked to login if you are a returningcustomer.
- Alternatively you can fill out your billing details and tick the box to create an account. You will not be charged for products that are free
- If the App is not free you will be presented with your order and the ability to pay by credit card or PayPal
- Once you have selected your payment type click **Place Order** or **Proceed to PayPal**
- If you have chosen **PayPal** a box will pop-up to enable you to sign in and pay with **PayPal** (please check your browser allows pop-ups)**.**
- After you have paid the **PayPal** pop-up will automatically close and you should be returned to the ALB-X
- You should now be presented with a screen that allows you to download your **App** manually by entering the **MachineID** and clicking **Download**
- This will download a smart-file that is locked by **MachineID** to an ALB-X. This smart-file can be uploaded via the **Advanced — Software** page, using the **Upload Apps and Software** button
- If the download is blanked out then you have already tied a purchase to another **ALB-X**
- If you have purchased from within an **ALB-X** via the **Services — App Store** page then you can now see your purchased **Apps** in the **Library — Apps** page
- The first step once you have purchased your **flightPATH App** is to find it in the **Library — Apps** page and click the green **Download** button



- Once your **flightPATH** has been downloaded it will move to the **Downloaded Apps** section and you will be able to click the **Deploy** button (it will be greyed out if the flightPATH has not been downloaded)



- Once you click **Deploy** your **flightPATH** rule will be deployed in the **Library — flightPATH** page



- Apply your flightPATH rule to a **Virtual Service** as normal from the **Services — IP-Services - flightPATH** page

Authentication

The **Library — Authentication** page allows you to setup authentication servers and create authentication rules with options for client side Basic or Forms and for server side NTLM or BASIC. The page is organised into the section below.

Work Flow

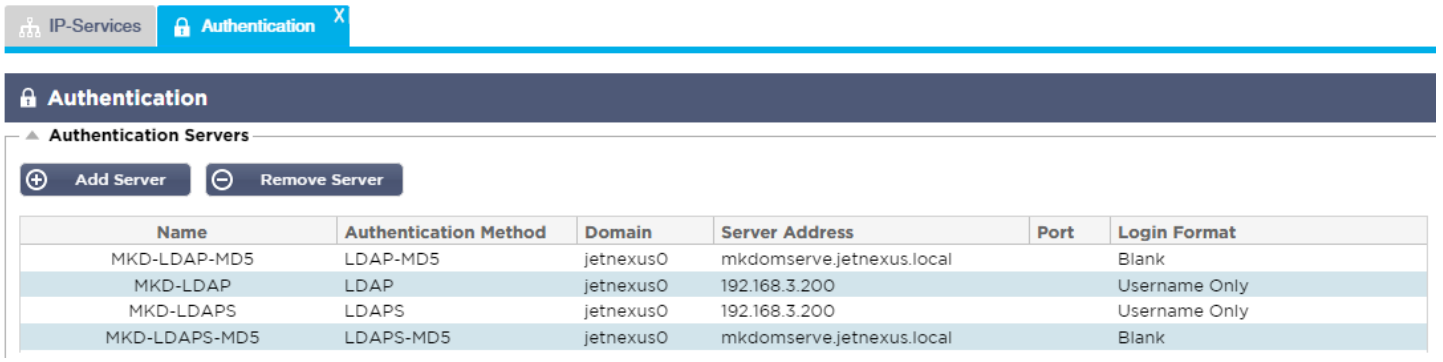
Please carry out the following steps as a minimum to apply Authentication to your service.

1. Create an Authentication Server.
2. Create an Authentication Rule that uses an Authentication Server.
3. Create a flightPATH rule that uses an Authentication Rule.
4. Apply the flightPATH rule to a Service.

Authentication Servers

First we must create a server to authenticate against.

- Click **Add Server**

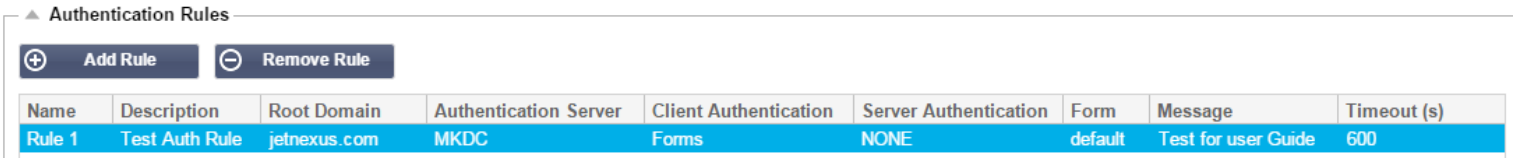


- This will produce a blank row ready for completion.
- **Name** – give your server a name for identification purposes – this name will be used in the rules below.
- **Description** – add a description.
- **Authentication Method** – choose an authentication method.
    - **LDAP** – basic LDAP with usernames and passwords sent in the clear to the LDAP server.
    - **LDAP-MD5** basic LDAP with username in the clear but password MD5 hashed for increased security.
    - **LDAPS** – LDAP over SSL. The password is sent in the clear but within an encrypted tunnel between the ALB-X and the LDAP server.
    - **LDAPS-MD5** – LDAP over SSL. The password is MD5 hashed for added security within an encrypted tunnel between the ALB-X and the LDAP server.
- **Domain –** add in the domain name for the LDAP server.
- **Server Address:**
    - **LDAP** – IPv4 address or hostname.
    - **LDAP-MD5** – hostname only (IPv4 address will not work).
    - **LDAPS – IPv4** address or hostname.

    - **LDAPS-MD5** – hostname only (IPv4 address will not work).
- **Port –** this will use port 389 for LDAP and port 636 for LDAPS by default. No need to add the port number for LDAP and LDAPS. When other methods become available you will be able to configure it here.
- **Search Conditions –** these search conditions must conform to RFC 4515. Example: (MemberOf=CN=Phone-VPN,CN=Users,DC=jetnexus,DC=local).
- **Search Base –** Starting point for the search in LDAP database. Example dc=jetnexus,dc=local.
- **Login Format:**
    - **Username –** when this format has been chosen you need only enter the username. Any user domain information entered by the user will be deleted and the domain information from the server will be used.
    - **Username and Domain –** The user must enter the full domain and username syntax. Example: jetnexus\gchristie OR gchristie@jetnexus. The domain information entered at the server level will be ignored.
    - **Blank –** we will accept anything the user inputs and send on to the authentication server. This must be used when using MD5.
- **Passphrase –** Not used in this version.
- **Dead Time –** Not used in this version.

Authentication Rules

Now we can create a rule that will use the server we created above.



- **Name:** add a suitable name for your authentication rule.
- **Description:** add suitable description.
- **Root Domain**: This must be left blank unless you need single-sign-on across sub-domains.
- **Authentication Server:** this is a drop down box that will contain any servers taht you have configured.
- **Client Authentication:**
    - **Forms** – this will present the edgeNEXUS default form to the user. Within the form you can add a message. You can select any other form that you have uploaded using the section below.
    - own pop-up to allow a user logon to your service. Note that the timeout value will be ignored for Basic Client Authentication.
- **Server Authentication Basic (401) – the browser will present its:**
    - **None** – if your server does not have any existing authentication select this setting. This means that you can now add authentication to a server that previously had none.
    - **Basic** – if your server has basic authentication enabled then select BASIC.
    - **NTLM** – if your server has NTLM authentication enabled then select NTLM.
- **Form:**
    - **Default –** this is the default edgeNEXUS form.
    - **Custom –** you can add your own form with your own name and select it here.
- **Message:** add a message to the form.
- **Timeout:** add a timeout to the rule after which the user will be required to authenticate again. Note this is only valid for Forms based authentication.

Single Sign On:

If you wish to provide a single sign on for users simply complete the Root Domain column with your domain. In this example we have used jetnexus.com. We can now have multiple services that will use the jetnexus.com as the root domain and you will only have to login once. If we consider the following services:

- sharepoint,jetnexus.com
- usercentral.jetnexus.com
- appstore.jetnexus.com

These services can reside on one VIP or can be distributed across 3 VIPs. A user accessing usercentral.jetnexus.com for the first time will be presented with a form asking them to log in depending on the authentication rule used. The same user then access appstore.jetnexus.com and will be authenticated automatically by the ALB-X. You can set the timeout which will force authentication once this period of in-activity has been reached.

Forms

This section will enable you to upload a custom form.

Creating your own form

In you wish to create your own custom form please use the following details within your htm or html form.

- Name of your form:
    - form name = loginform
    - action = %JNURL%
    - Method = POST
- Username:
    - name = “JNUSER”
- Password:
    - name=”JNPASS”
- Optional Message1:
    - %JNMESSAGE%
- Optional Message2:
    - %JNAUTHMESSAGE%
- Images
    - If you wish to add an image then please add it in-line using Base64 encoding.

Example html of simple form

```
<HTML>
        <HEAD>
        <TITLE>SAMPLE AUTH FORM</TITLE>
        </HEAD>
        <BODY>
        %JNMESSAGE%<br>
```

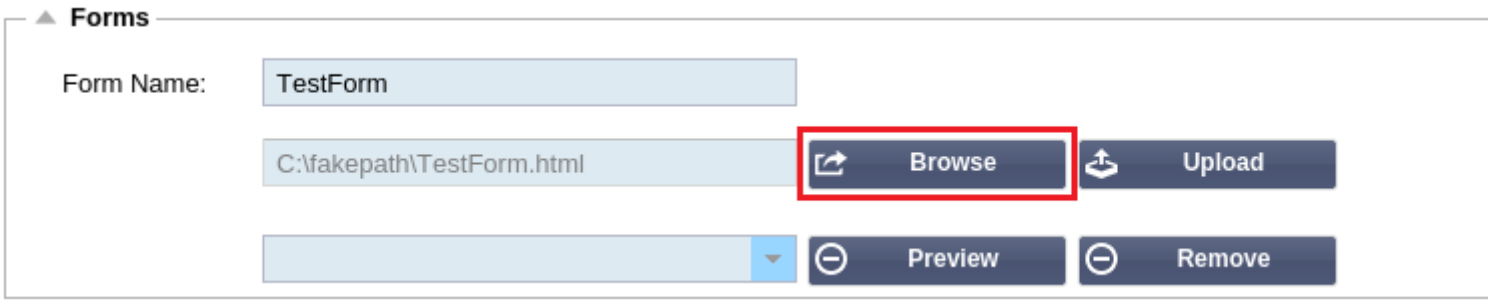
```
<form name="loginform" action="%JNURL%" method="post">
USER: <input type="text" name="JNUSER" size="20" value=""></br>
PASS: <input type="password" name="JNPASS" size="20" value=""></br>
<input type="submit" name="submit" value="OK">
</form>
</BODY>
```

Example screen shot of default form

Adding a custom form

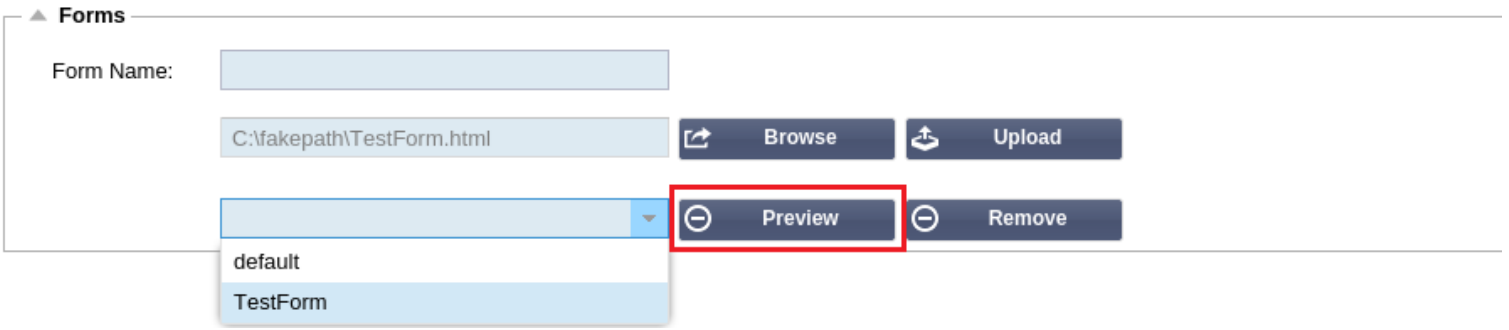
Once you have created a custom form you can add it using the Forms section.

- Choose a name for your form
- **Browse** locally for your form
- Click **Upload**



Preview a custom form

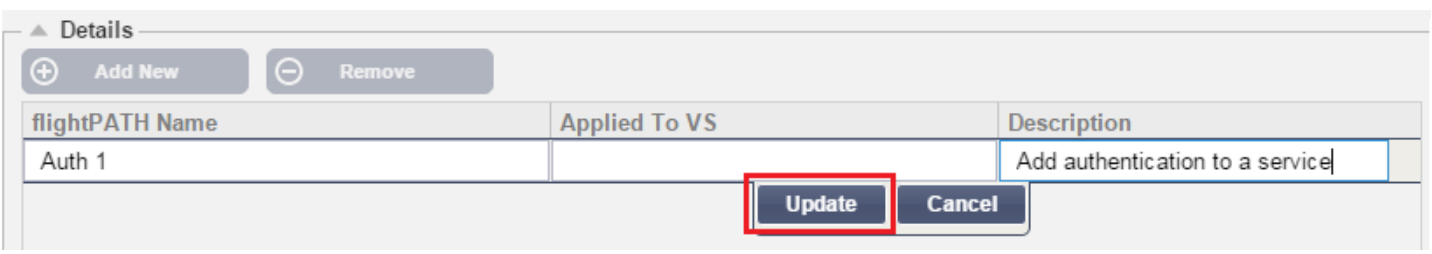
To view the custom form you have just added simply select it and click preview. You may also use this section to delete forms that are no longer required



flightPATH

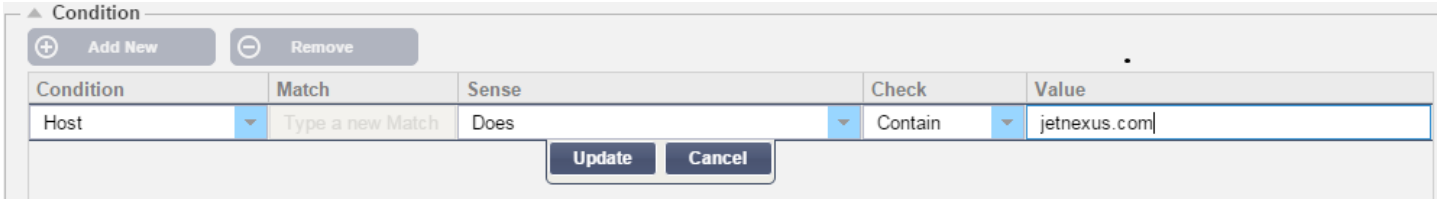
The final bit to tie everything together is to create a flightPATH rule and apply it to a Virtual Service

- Navigate to **Library-flightPATH**
- In the details section click **Add New**
- Enter a name for your rule. Example **Auth2**
- Enter a description of your rule
- Once the rule has been applied to a service you will see the Applied To column auto populate with an IP address:Port
- Don't forget to hit update to save your changes or if you make a mistake just hit cancel to remove all changes

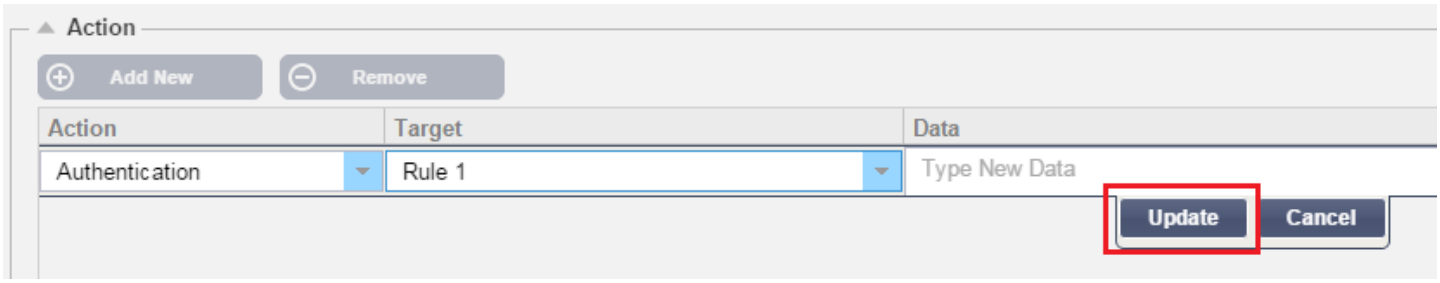


- Next we need to **Add New Condition**
- Choose a condition from the drop down box. Example **Host**
- Choose a **Sense**. Example **Does**
- Choose a **Check**. Example **Contain**

- Choose a **Value.** Example **jetnexus.com**



- Now we need to add an action to our rule
- Click **Add New**
- Choose **Authentication** from the drop down
- Choose the rule created within the **Authentication** page. Example **Rule 1**
- Click **Update**



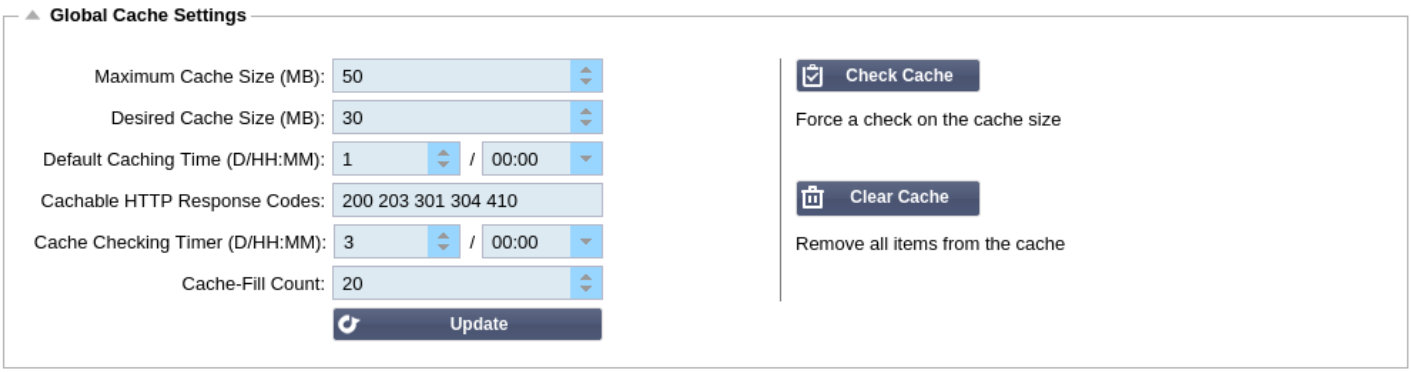
Finally we need to apply this flightPATH rule to a virtual service

- Navigate to **Services-IP Services**
- Highlight the desired **Virtual Service**
- Click on the **flightPATH** tab
- Select the rule from the **Available flightPATHs.** Example **Auth1**
- Click the **right arrow** or drag the rule to the **Applied flightPATHs**

Cache

The **Library — Cache** page allows you to configure the cache settings for the ALB-X. The page is organised is in the sections below:

Cache Settings



Maximum Cache Size (MB):

Maximum RAM that the Cache can consume. The edgeNEXUS Cache is an in-memory cache that is also periodically backed onto hard disk to maintain cache persistence after restarts, reboots and shutdowns. This means that the maximum cache size must fit within the memory footprint of the appliance (rather than disk space) and should be no more than half of available memory.

Desired Cache Size (MB):

Optimum RAM that the Cache will be trimmed to. While the maximum cache size represents the absolute upper boundary of the cache, the desired cache size is intended as the optimum size that the cache should attempt to attain whenever an automatic or manual check on the cache size is made. The gap between the maximum and desired cache size exists to accommodate the arrival and overlap of new content between periodic checks on cache size for the purpose of trimming expired content. Once again, it may be more effective to accept the default value (30 MB) and periodically review the size of the cache under "**Monitor -> Statistics**" for appropriate sizing.

Default Cache Time (D/HH:MM):

Life of content without an explicit expiry value. The default caching time is the period content will be stored in the cache for items that don't have a "no-store" directive, but also have no explicit expiry time in the traffic header. The field entry takes the form "D/HH:MM" – so an entry of "1/00:00" (the default) means to store the item for one day, "01:00" for one hour and "00:01" for one minute.

Cachable HTTP Response Codes:

HTTP responses that will be cached:

200 – Standard response for successful HTTP requests

203 – Headers are not definitive, but are gathered from a local or a 3rd party copy **301** – The requested resource has been assigned a new permanent URL **304** – Not modified since the last request & locally cached copy should be used instead **410** – Resource is no longer available at the server and no forwarding address is known

This field should be edited with caution as the most common cacheable response codes are already listed

Cache Checking Time (D/HH:MM):

Interval between cache trim operation

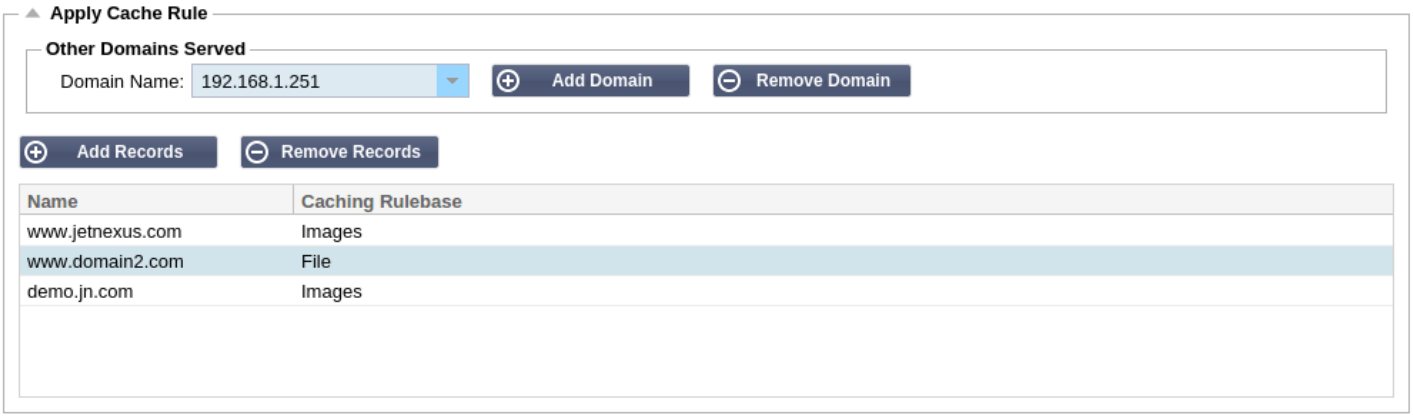
Cache-Fill Count:

This is a helper facility to help fill the cache when a certain number of 304's have been detected

Apply Cache Rule

This section allows you to apply a cache rule to a domain:

- Add domain manually with the **Add Records** button. This maybe a fully qualified domain name or an IP address in dotted decimal notation. Example www.jetnexus.com or 192.168.3.1:80
- Click the dropdown arrow and choose your domain from the list
- The list will be populated so long as traffic has passed through a virtual service and a caching strategy has been applied to the virtual service
- Choose your cache rule by double clicking on the **Caching Rulebase** column and selecting from the list



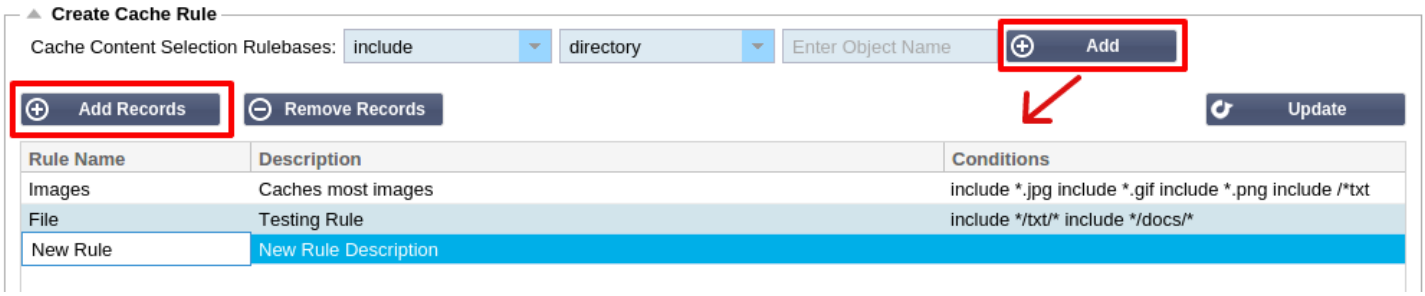
Create Cache Rule

This section allows you to create a number of different caching rules that can then be applied to a domain:

- Click **Add Records** and give your rule a name and description
- You can either type you conditions in manually or use the Add Condition

To add a condition using the **Selection Rulebase**:

- Choose Include or Exclude
- Choose **All JPEG Images**
- Click on the **+ Add** symbol
- You will see that **include *.jpg** has now been added to the conditions
- You can add more conditions. If you choose to do this manually you need to add each condition on a NEW line. Please note that your rules will display on the same line until you click in the Conditions box then they will show on a separate line


Create Cache Rule
Cache Content Selection Rulebases:
include
directory
Enter Object Name
Add
Add Records
Remove Records
Update
Rule Name
Description
Conditions
Images
Caches most images
include *.jpg include *.gif include *.png include /*txt
File
Testing Rule
include */txt/* include */docs/*
New Rule
New Rule Description

flightPATH

The **Library — flightPATH** page allows you to view and update the flightPATH rules on the jetNEXUS ALB-X. The settings are organised in the following sections: Although some components of flightPATH are IP objects, such as Source IP flightpath, they can only be applied to a Service Type.

What is flightPATH?

flightPATH is a rule engine developed by edgeNEXUS to intelligently manipulate and route HTTP and HTTPS traffic. It is highly configurable, very powerful and yet very easy to use. Although some components of flightPATH are IP objects such as Source IP flightPATH can only be applied to a **Service Type** equal to HTTP. If you choose any other service type then the flightPATH tab in IP Services will be blank. A flightPATH rule has three components:

Condition:
Set multiple criteria to trigger the rule.

Evaluation:
Variables that can be used in the Action.

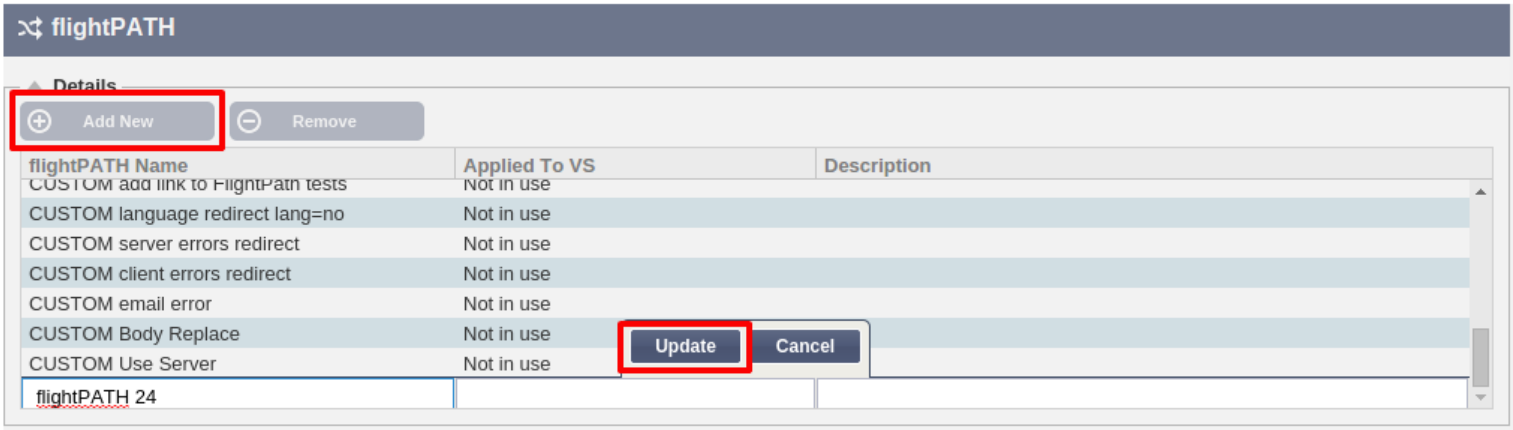
Action:
The behaviour once the rule has triggered.

What can flightPATH do?

- flightPATH can be used to modify **Incoming** and **Outgoing** HTTP(s) content and requests.
- As well as using simple string matches such as “Starts with”, “Ends With” etc. For more complete control powerful Perl Compatible Regular Expressions can be implemented.
- For more on Regular Expressions please see this useful site https://www.regexbuddy.com/regex.html
- In addition, custom variables can be created and used in the **Action** enabling many different possibilities.

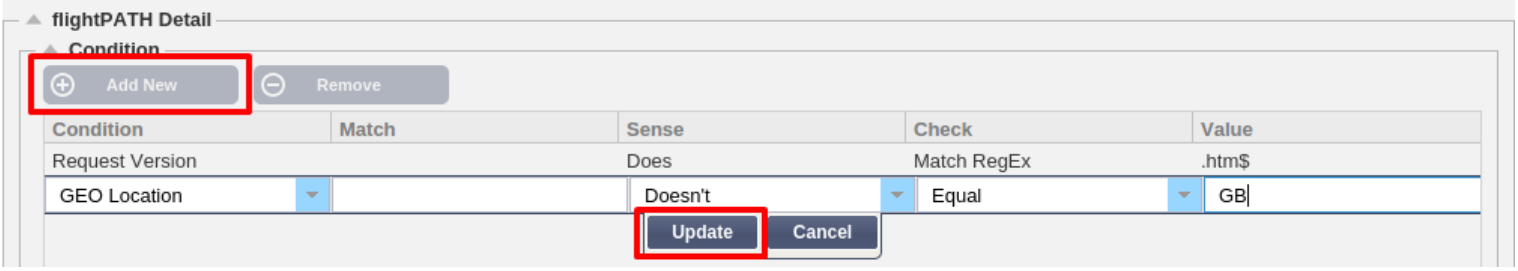
Details

The details section contains the name and description of all of the flightPATH rules configured on the ALB-X. As you click on a rule the details of the rule will show in the section below. To add a new flightPATH rule click **Add New** and give your rule a **Name** and **Description** then click **Update** to save this section.



Condition

- New conditions can be added by clicking, **Add New** button.
- Multiple conditions can be used but **ALL** must be met for the rule to execute.
- To use an **OR** you would need to create an additional flightPATH rule and apply this in IP Services.
- Each condition contains three elements and a value or not depending on the condition.



Condition:
Select from the drop down list. You can start typing and the option will auto-show, you can now select with arrow keys and tab to the next column
Match:
Select from the drop down list or type your match. Depending on the Condition, the Match maybe blank. For example if the **Condition** is **Request Header** the match might be **User-Agent**
Sense:
Select from the drop down list. There are only two option **Does** and **Doesn't**
Check:
Select from the drop down list. For a simple check use something like **Start**, **End** or **Contain**. If you wish to have more than one **Check** in the same line then please use **Match Regex**. Example Check = Match RegEx, Value = item1|intem2|item3Note: Match Regex uses Perl Compatible Regular Expression (PCRE). More information can be found at https://www.regexbuddy.com/
Value:
Manually type the value. This may be a text string or a regular expression.

<form>	HTML forms are used to pass data to a server	Example "form doesn't have length 0"
GEO Location	This compares the source IP address to the ISO 3166 Country Code	GEO Location does equal GB OR GEO Location does equal Germany
Host	This is the host extracted from the URL	www.mywebsite.com or 192.168.1.1
Language	This is the Language extracted from the language HTTP header	This condition will produce a dropdown with a list of Languages
Method	This is a drop down of HTTP methods	This is a drop down that includes GET, POST etc
Origin IP	If upstream proxy supports X-Forwarded-for (XFF) it will use the true Origin address	Client IP. Can also use multiple IP's or subnets. 10\.1\.2\.* is 10.1.2.0 /24 subnet 10\.1\.2\.3|10\.1\.2\.4 Use | for multiple IP's
Path	This is the path of the website	/mywebsite/index.asp
POST	POST request method	Check data being uploaded to a website
Query	This is the name and Value of a Query as such it can either accept the query name or a value also	"Best=jetNEXUS" Where the Match is Best and the Value is edgeNEXUS
Query String	The whole query string after the ? character	
Request Cookie	This is the name of a cookie requested by a client	MS-WSMAN=afYfn1CDqqCDqUD::

Request Header	This can be any HTTP Header	Referrer, User-Agent, From, Date
Request Version	This is the HTTP version	HTTP/1.0 OR HTTP/1.1
Response Body	A user defined string in the response body	Server UP
Response Code	The http code for the response	200 OK, 304 Not Modified
Response Cookie	This is the name of a cookie sent by the server	MS-WSMAN=afYfn1CDqqCDqUD::
Response Header	This can be any HTTP Header	Referrer, User-Agent, From, Date
Response Version	The HTTP version sent by the server	HTTP/1.0 OR HTTP/1.1
Source IP	This is either the origin IP, proxy server IP or some other aggregated IP address	Client IP, Proxy IP, Firewall IP. Can also use multiple IP's and subnets. You must escape the dots as these are RegEX. Example 10\.1\.2\.3 is 10.1.2.3

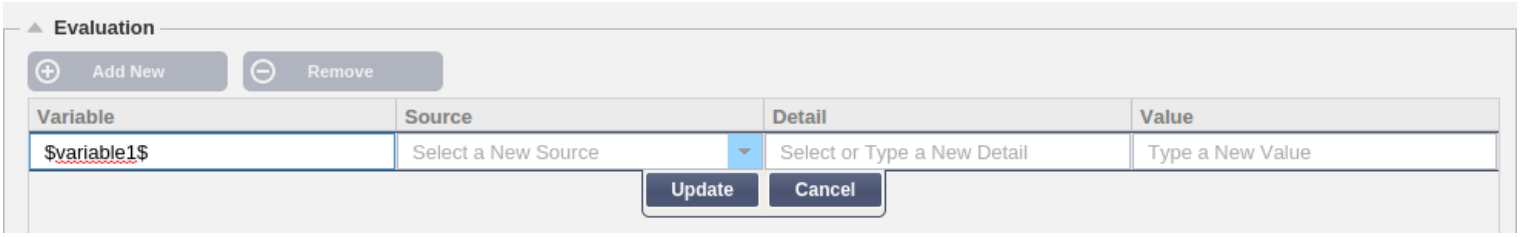
Accept	Content-Types that are acceptable	Accept: text/plain
Accept-Encoding	Acceptable encodings	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Acceptable languages for response	Accept-Language: en-US
Accept-Ranges	What partial content range types this server supports	Accept-Ranges: bytes
Authorization	Authentication credentials for HTTP authentication	Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Charge-To	Contains account information for the costs of the application of the method requested	
Content-Encoding	The type of encoding used on the data.	Content-Encoding: gzip
Content-Length	The length of the response body in Octets (8-bit bytes)	Content-Length: 348
Content-Type	The mime type of the body of the request (used with POST and PUT requests)	Content-Type: application/x-www-form-urlencoded
Cookie	A HTTP cookie previously sent by the server with Set-Cookie (below)	Cookie: $Version=1; Skin=new;
Date	Date and time at message was originated	Date = "Date" ":" HTTP-date
ETag	An identifier for a specific version of a resource, often a message digest	ETag: "aed6bdb8e090cd1:0"
From	The email address of the user making the request	From: user@example.com
If-Modified-Since	Allows a 304 Not Modified to be returned if content is unchanged	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Last-Modified	The last modified date for the requested object, in RFC 2822 format	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Implementation-specific headers that may have various effects anywhere along the request-response chain.	Pragma: no-cache
Referrer	This is the address of the previous web page from which a link to the currently requested page was followed	Referrer: http://www.edgenexus.io
Server	A name for the server	Server: Apache/2.4.1 (Unix)
Set-Cookie	A HTTP cookie	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
User-Agent	The user agent string of the user agent	User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Vary	Tells downstream proxies how to match future request headers to decide whether the cached response can be used rather than requesting a fresh one from the origin server	Vary: User-Agent
X-Powered-By	Specifies the technology (e.g. ASP.NET, PHP, JBoss) supporting the web application	X-Powered-By: PHP/5.4.0

Exist	This does not care for the detail of the condition just that it does/doesn't exist	Host — Does — Exist
Start	The string starts with the Value	Path — Does — Start — /secure
End	The string ends with the Value	Path — Does — End — .jpg
Contain	The string does contain the Value	Request Header — Accept — Does — Contain — image
Equal	The string does Equal the Value	Host — Does — Equal — www.jetnexus.com
Have Length	The string does have length of the value	Host — Does — Have Length — 16 www.jetnexus.com = TRUE www.jetnexus.co.uk = FALSE
Match RegEx	This enables you to enter a full Perl compatible regular expression	Origin IP — Does — Match Regex — 10\..* | 11\..*

Example:

- The example below has two conditions and BOTH must be met to carry out the action
- The first is checking that the requested object is an image
- The second is checking for a specific hostname

Evaluation



Adding a Variable is a very powerful feature that will allow you to extract data from the request and include this in the actions. For example you could log a user username or send an email if there is a security problem.

- **Variable:** This must start and end with a $ symbol
- **Source:** Select from the drop down box the source of the variable
- **Detail:** Select from the list when relevant. If the Source=Request Header the Details could be User-Agent
- **Value:** Enter the text or regular expression to fine tune the variable.

Built-in Variables:

- Built-In variables have already been hard coded so you do not need to create an evaluation entry for these.
- You can use any of the variable listed below in your action
- The explanation for each variable is located in the "Condition" table above
    1. Method = $method$

2. Path = $path$
3. Querystring = $querystring$
4. Sourceip = $sourceip$
5. Response code (text also included "200 OK") = $resp$
6. Host = $host$
7. Version = $version$
8. Clientport = $clientport$
9. Clientip = $clientip$
10. Geolocation = $geolocation$"

Example Action:

1. Action = Redirect 302
    - Target = https://$host$/404.html
2. Action = Log
    1. Target = A client from $sourceip$:$sourceport$ has just made a request $path$ page

Explanation:

- A client accessing page that does not exist would ordinarily be presented with a browsers 404 page
- In this instance the user is redirected to the original hostname they used but the wrong path is replaced with 404.html
- An entry is added to the syslog saying "A client from 154.3.22.14:3454 has just made a request to wrong.html page"

Cookie	This is the name and value of the cookie header	MS-WSMAN=afYfn1CDqqCDqUD::Where the name is MS-WSMAN and the value is afYfn1CDqqCDqUD::
Host	This is the hostname extracted from the URL	www.mywebsite.com or 192.168.1.1
Language	This is the language extracted from the Language HTTP header	This condition will produce a dropdown with a list of languages.
Method	This is a drop down of HTTP methods	The dropdown will include GET, POST
Path	This is the path of the website	/mywebsite/index.html
POST	POST request method	Check data being uploaded to a website
Query Item	This is the name and value of a query. As such it can either accept the query name or a value also	“Best=jetNEXUS” Where the Match is Best and the Value is edgeNEXUS
Query String	This is the whole string after the ? character	http://server/path/program?**query_string**
Request Header	This can be any header sent by the client	Referrer, User-Agent, From, Date…
Response Header	This can be any header sent by the server	Referrer, User-Agent, From, Date…
Version	This is the HTTP version	HTTP/1.0 or HTTP/1.1

Accept	Content-Types that are acceptable	Accept: text/plain
Accept-Encoding	Acceptable encodings	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Acceptable languages for response	Accept-Language: en-US
Accept-Ranges	What partial content range types this server supports	Accept-Ranges: bytes
Authorization	Authentication credentials for HTTP authentication	Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Charge-To	Contains account information for the costs of the application of the method requested	
Content-Encoding	The type of encoding used on the data.	Content-Encoding: gzip
Content-Length	The length of the response body in Octets (8-bit bytes)	Content-Length: 348

Content-Type	The mime type of the body of the request (used with POST and PUT requests)	Content-Type: application/x-www-form-urlencoded
Cookie	a HTTP cookie previously sent by the server with Set-Cookie (below)	Cookie: $Version=1; Skin=new;
Date	Date and time at which the message was originated	Date = “Date” “:” HTTP-date
ETag	An identifier for a specific version of a resource, often a message digest	ETag: “aed6bdb8e090cd1:0”
From	The email address of the user making the request	From: user@example.com
If-Modified-Since	Allows a 304 Not Modified to be returned if content is unchanged	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Last-Modified	The last modified date for the requested object, in RFC 2822 format	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Implementation-specific headers that may have various effects anywhere along the request-response chain.	Pragma: no-cache
Referrer	This is the address of the previous web page from which a link to the currently requested page was followed	Referrer: http://www.edgenexus.io
Server	A name for the server	Server: Apache/2.4.1 (Unix)
Set-Cookie	an HTTP cookie	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
User-Agent	The user agent string of the user agent	User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Vary	Tells downstream proxies how to match future request headers to decide whether the cached response can be used rather than requesting a fresh one from the origin server	Vary: User-Agent
X-Powered-By	Specifies the technology (e.g. ASP.NET, PHP, JBoss) supporting the web application	X-Powered-By: PHP/5.4.0

Action

The action is the task or tasks that are enabled once the condition or conditions have been met. **Action:**
Double click on the Action column to view drop down list.

Target:

Double click on the Target column to view the drop down list. The list will change depending on the Action. You may also type manually with some actions.

Data:

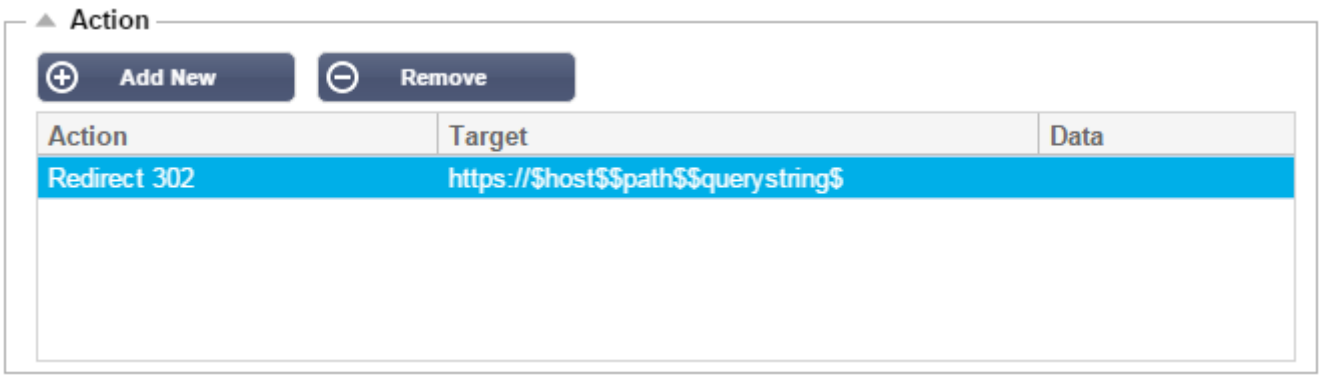
Double click on the Data column to manually add your data that you wish to add or replace.
The list of all the actions are detailed below:

Add Request Cookie	Add request cookie detailed in the Target section with value in Data section	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Add Request Header	Add a request header of Target type with value in Data section	Target= Accept Data= image/png
Add Response Cookie	Add Response Cookie detailed in the Target section with value in Data section	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Add Response Header	Add request header detailed in the Target section with value in the Data section	Target= Cache-Control Data= max-age=8888888
Body Replace All	Search the Response Body and replace all instances	Target= http:// (Search string) Data= https:// (Replacement string)

Body Replace First	Search the Response Body and replace first instance only	Target= http:// (Search string) Data= https:// (Replacement string)
Body Replace Last	Search the Response Body and replace last instance only	Target= http:// (Search string) Data= https:// (Replacement string)
Drop	This will drop the connection	Target= N/A Data= N/A
e-Mail	Will send an email to the address configured in Email Events. You can use a variable as the address or the message	Target= “flightPATH has emailed this event” Data= N/A
Log Event	This will log an event to the System log	Target= “flightPATH has logged this in syslog” Data= N/A
Redirect 301	This will issue a permanent redirect	Target= http://www.edgenexus.io Data= N/A
Redirect 302	This will issue a temporary redirect	Target= http://www.edgenexus.io Data= N/A
Remove Request Cookie	Remove request cookie detailed in the Target section	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Remove Request Header	Remove request header detailed in the Target section	Target=Server Data=N/A
Remove Response Cookie	Remove response cookie detailed in the Target section	Target=jnAccel
Remove Response Header	Remove the response header detailed in Target section	Target= Etag Data= N/A
Replace Request Cookie	Replace request cookie detailed in the Target section with value in the Data section	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Replace Request Header	Replace request header in the Target with Data value	Target= Connection Data= keep-alive
Replace Response Cookie	Replace the response cookie detailed in Target section with value in Data section	Target=jnAccel=afYfn1CDqqCDqCVii Date=MS-WSMAN=afYfn1CDqqCDqCVii
Replace Response Header	Replace the response header detailed in Target section with value in Data section	Target= Server Data= Withheld for Security
Rewrite Path	This will allow you to redirect the request to new URL based on the condition	Target= /test/path/index.html$querystring$ Data= N/A
Use Secure Server	Select which secure server or virtual service to use	Target=192.168.101:443 Data=N/A
Use Server	Select which server or virtual service to use	Target= 192.168.101:80 Data= N/A
Encrypt Cookie	This will 3DES Encrypt cookies and then base64 encode them	Target= Enter the cookie name to be encrypted, you may use the * as a wild card at the end Data= Enter a pass phrase for the encryption

Example:

The action below will issue a temporary redirect to the browser to a secure HTTPS Virtual Service. It will use the same hostname, path and querystring as the request.



Common Uses:

Application Firewall and Security:

- Block unwanted IPs
- Force user to HTTPS for specific (or all) content
- Block or redirect spiders
- Prevent and alert cross site scripting
- Prevent and alert SQL injection
- Hide internal directory structure
- Rewrite cookies
- Secure directory for particular users

Features:

- Redirect users based on path
- Provide Single sign on across multiple systems
- Segment users based on User ID or Cookie
- Add headers for SSL offload
- Language detection
- Rewrite user request
- Fix broken URLs
- Log and Email Alert 404 response codes
- Prevent directory access/ browsing
- Send spiders different content

Pre-Built Rules:

1. HTML Extension:
Changes all .htm requests to .html
Condition:

- Condition = Path
- Sense = Does
- Check = Match RegEx
- Value = \.htm$

Evaluation:

- Blank

Action:

- Action = Rewrite Path
- Target = $path$l

2. Index.html:
Force to use index.html in requests to folders.

Condition: this condition is a general condition that will match most objects

- Condition = Host
- Sense = Does
- Check = Exist

Evaluation:

- Blank

Action:

- Action = Redirect 302
- Target = http://$host$$path$index.html$querystring$

3. Close Folders:
Deny requests to folders.

Condition: this condition is a general condition that will match most objects

- Condition = this need proper thought
- Sense =
- Check =

Evaluation:

- Blank

Action:

- Action =
- Target =

4. Hide CGI-BBIN:
Hides cgi-bin catalogue in requests to CGI scripts.

Condition: this condition is a general condition that will match most objects

- Condition = Host
- Sense = Does
- Check = Match RegEX
- Value = \.cgi$

Evaluation:

- Blank

Action:

- Action = Rewrite Path
- Target = /cgi-bin$path$

5. Log Spider:
Log spider requests of popular search engines.

Condition: this condition is a general condition that will match most objects

- Condition = Request Header
- Match = User-Agent
- Sense = Does
- Check = Match RegEX
- Value = Googlebot|Slurp|bingbot|ia_archiver

Evaluation:

- Variable = $crawler$
- Source = Request Header
- Detail = User-Agent

Action:

- Action = Log Event
- Target = [$crawler$] $host$$path$$querystring$

6. Force HTTPS:

Force to use HTTPS for certain directory. In this case if a client is accessing anything containing the /secure/ directory then they will be redirected to the https version of the URL requested.

Condition:

- Condition = Path
- Sense = Does
- Check = Contain
- Value = /secure/

Evaluation:

- Blank

Action:

- Action = Redirect 302
- Target = https://$host$$path$$querystring$

7. Media Stream:

Redirects Flash Media Stream to appropriate service.

Condition:

- Condition = Path
- Sense = Does
- Check = End
- Value = .flv

Evaluation:

- Blank

Action:

- Action = Redirect 302
- Target = http://$host$:8080/$path$

8. Swap HTTP to HTTPS:

Change any hardcoded HTTP:// to HTTPS://

Condition:

- Condition = Response Code
- Sense = Does
- Check = Equal
- Value = 200 OK

Evaluation:

- Blank

Action:

- Action = Body Replace All
- Target = http://
- Data = https://

9. Blank out Credit Cards:
Check that there are no credit cards in the response and if one is found, blank it out.

Condition:

- Condition = Response Code
- Sense = Does
- Check = Equal
- Value = 200 OK

Evaluation:

- Blank

Action:

- Action = Body Replace All
- Target = [0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+
- Data = xxxx-xxxx-xxxx-xxxx

10. Content Expiry:
Add a sensible content expiry date to the page to reduce the number of requests and 304s.

Condition: this is a generic condition as a catch all. It is recommended to focus this condition on your

- Condition = Response Code
- Sense = Does
- Check = Equal
- Value = 200 OK

Evaluation:

- Blank

Action:

- Action = Add Response Header
- Target = Cache-Control
- Data = max-age=3600

11. Spoof Server Type:
Get the Server type and change it to something else.

Condition: this is a generic condition as a catch all. It is recommended to focus this condition on your

- Condition = Response Code
- Sense = Does
- Check = Equal
- Value = 200 OK

Evaluation:

- Blank

Action:

- Action = Replace Response Header
- Target = Server
- Data = Secret

12. Never Send Errors:
Client never gets any errors from your site.

Condition:

- Condition = Response Code
- Sense = Does
- Check = Contain
- Value = 404

Evaluation:

- Blank

Action:

- Action = Redirect 302
- Target = http://$host$/

13. Redirect on Language:

Find the language code and redirect to the related country domain.

Condition:

- Condition = Language
- Sense = Does
- Check = Contain
- Value = German (Standard)

Evaluation:

- Variable = $host_template$
- Source = Host
- Value = .*\.

Action:

- Action = Redirect 302
- Target = http://$host_template$de$path$$querystring$

14. Google Analytics:

Insert the code required by Google for the analytics – Please change the value MYGOOGLECODE to your Google UA ID.

Condition:

- Condition = Response Code
- Sense = Does
- Check = Equal
- Value = 200 OK

Evaluation:

- blank

Action:

- Action = Body Replace Last
- Target = </body>
- Data = <script type='text/javascript'> var _gaq = _gaq || []; _gaq.push(['_setAccount', 'MY GOOGLE CODE']); _gaq.push(['_trackPageview']); (function() { var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true; ga.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google-analytics.com/ga.js'; var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(ga, s); })(); </script> </body>

15. IPv6 Gateway:

Adjust Host Header for IIS IPv4 Servers on IPv6 Services. IIS IPv4 servers do not like to see an IPV6 address in the host client request so this rule replaces this with a generic name.

Condition:

- blank

Evaluation:

- blank

Action:

- Action = Replace Request Header
- Target = Host
- Data =ipv4.host.header

Real Server Monitoring

The **Library — Real Server Monitors** page allows you to add, view and edit custom monitoring. These are layer 7 server "Health-Checks" and once configured will appear in the drop-down list for Server Monitoring. This page is split in to three sections

Details

Name:
Double click on the column to manually add in a name for your monitor.

Description:
Double click on the column to manually add in a description for your monitor.

Monitoring Method:
Double click on the column to choose the monitoring method from the dropdown list.

Page Location:
Double click on the column to manually add in a page location for an HTTP monitor. This can be a relative link such as /folder1/folder2/page1.html. You can also use an absolute link where the web site is bound to the hostname.

Required Content:
Double click on the column to manually add in the required content. This will change depending on the monitoring method.

Applied to VS:
This column will be populated automatically with the service IP:Port that the monitor is applied to. You will not be able to delete any Monitor that has been applied to a virtual service.

User:
Some custom monitors can use this value along with the password column to log into a real server.

Password:
Some custom monitors can use this value along with the user column to log into a real server.

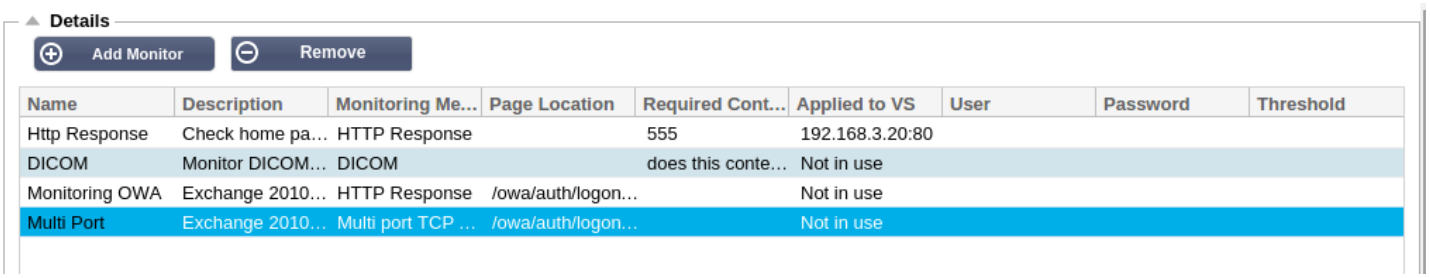
Threshold:
This is a general integer to be used in custom monitors where a threshold like CPU level is required.

NOTE: Please ensure the response back from the Application server is not a "Chunked" response

Monitoring Method	Description	Example

HTTP 200 OK	In this mode, a TCP connection is made to the content server as above, but after connection is made, a brief HTTP request is made to the content server.A HTTP response is waited for and it is checked for the "200 OK" response code. If the "200 OK" response code is received, the content server is deemed to be up and running. If, for any reason, the "200 OK" response code is not received, including timeouts, failure to connect, etc. then the content server is regarded as down.This monitoring method can only really be used with HTTP and Accelerate HTTP service types, although if a Layer 4 Service Type is in use for an HTTP server, it could still be used if SSL is not in use on the content server, or is handled appropriately by the "Content SSL" facility.	**Name:** 200OK **Description** Check production web site **Monitoring Method:** HTTP 200 OK **Page Location:** /main/index.html ORhttp://www.edgenexus.io/main/index.html **Required Content:** N/A
HTTP Response	In this mode, a connection and HTTP request/response are made/checked for as above, but instead of the "200 OK" response code being checked for, a custom text is searched for in both the HTTP headers, and the body of the HTTP response.The text can be a whole header, part of a header, a line from part of a page, or just one word. If the text is found, the content server is deemed to be up and running.This monitoring method can only really be used with HTTP and Accelerate HTTP service types, although if a Layer 4 Service Type is in use for an HTTP server, it could still be used if SSL is not in use on the content server, or is handled appropriately by the "Content SSL" facility.	**Name:** Server Up **Description** Check content of page for "Server Up" **Monitoring Method:** HTTP Response **Page Location:** /main/index.html OR http://www.edgenexus.io/main/index.html **Required Content:** Server Up
DICOM	In this mode we send a DICOM echo using the "Source Calling" AE Title value in the required content column. You can also set the "Destination Called" AE Title value in the Notes section of each server. You can find the Notes column withing the IP Services--Virtual Services--Server page	**Name:** DICOM **Description** L7 health check for DICOM service **Monitoring Method:** DICOM **Page Location:** N/A **Required Content:** AET Value
TCP Out of Band	This is similar to a TCP Connect except that you can specify the port you wish to monitor in the required content column. This port is typically not the same as the traffic port and is used when you want to tie services together.	**Name:** TCP Out of Band **Description:** Monitor Out of Band/Traffic port **Page Location:** N/A **Required Content:** 555
Multi-Port TCP monitor	This is similar to above except that you can have a number of different ports. The monitor is deemed successful only if all ports specified in the required content section respond correctly.	**Name:** Multi Port Monitor **Description:** Monitor multiple ports for success **Page Location:** N/A **Required Content:** 135,59534,59535

Example



Upload Monitor

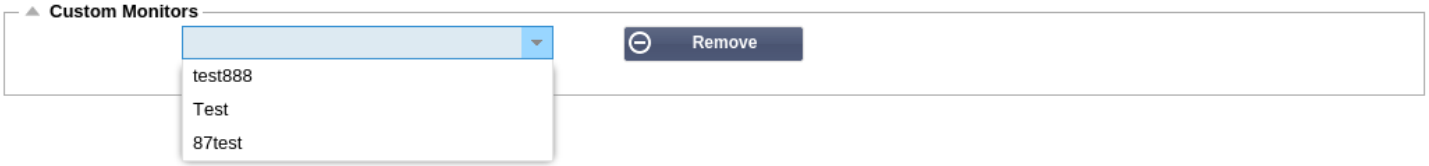
In this section you can upload a custom monitor that you have created or that has been created for you by our support team. It will take the form of a Perl script file. Example DNS.pl

- Give you monitor a name so that you can identify it in the **Monitoring Method** list
- Browse for the .pl file
- Click **Upload**
- Your file will be uploaded to the correct location and will be visible as a new **Monitoring Method.**

Custom Monitors

In this section you can view custom monitors that have been uploaded and remove them if they are no longer needed.

- Click the drop down box
- Select the name of the custom monitor
- Click **Remove**
- Your custom monitor will no longer be visible in the **Monitoring Method** list



Creating a Custom Monitor Perl Script

You should be familiar with Perl. The following show you what can be included in your script with an image of a working example at the bottom for reference. The #Monitor-Name: is the name used for the Perl Script stored on the ALB-X. If you do not include this line then your script will not be found!
The following are mandatory

- **#Monitor-Name:**

- **use strict;**
- **use warning;**

The perl scripts are run in a chrooted environment. They often call another application such as wget or curl Sometimes these need to be updated for a certain feature such as SNI

Dynamic Values

- **my $host = $_[0];**
  - This uses the "**Address**" from **IP Services--Real Server** section
- **my $port = $_[1];**
  - This uses the "**Port**" from **IP Services--Real Server** section
- **my $content = $_[2];**
  - This uses the "**Required Content**" value from the **Library--Real Server Monitoring** section
- **my $notes = $_[3];**
  - This uses the "**Notes**" column in **Real Server section of IP Services**
- **my $page = $_[4];**
  - This uses the "**Page Location**" values from **Library--Real Server Monitor** section
- **my $user = $_[5];**
  - This uses the "**User**" value from the **Library--Real Server Monitor** section
- **my $password = $_[6];**
  - This uses the "**Password**" value from the **Library--Real Server Monitor** section

Custom Health Checks have two outcomes

1. **Successful**
   - Return Value 1
   - Print a success message to Syslog
   - Mark the Real Server Online (provided IN COUNT match)
2. **Unsuccessful**
   - Return Value 2
   - Print a message saying Unsuccessful to Syslog
   - Mark the Real Server Offline (provided OUT Count match)

Example:

Example of working Custom Monitor:

```
#Monitor-Name:HTTPS_SNI
use strict;
use warnings;
#################################################################################################
# jetNEXUS custom health checking Copyright jetNEXUS 2016
#################################################################################################
# This is a Perl script for jetNEXUS customer health checking
# The monitor name as above is displayed in the dropdown of Available health checks
# There are 6 value passed to this script (see below)
## The script will return the following values
# 1 is the test is successful
# 2 if the test is unsuccessful
# Please see JNALB-7487 and JNALB-7493 for details.
sub monitor
{
   my $host      = $_[0];    ### Host IP or name
   my $port      = $_[1];    ### Host Port
   my $content   = $_[2];    ### Content to look for (in the web page and HTTP headers)
   my $notes     = $_[3];    ### Virtual host name
   my $page      = $_[4];    ### The part of the URL after the host address
   my $user      = $_[5];    ### domain/username (optional)
   my $password  = $_[6];    ### password (optional)
   my $resolve;
   my $auth      = '';

   if ($port)
   {
      $resolve = "$notes:$port:$host";
   }
   else {
      $resolve = "$notes:$host";
   }
   if ($user && $password) {
      $auth = "-u $user:$password";
   }
   my @lines = `curl -s -i --retry 1 --max-time 1 -k -H "Host:$notes" --resolve $resolve $auth https://${notes}${page} 2>&1`;
   if (join("",@lines) =~ /$content/)
   {
      print "https://${notes}${page} looking for - $content - Healhcheck check successful\n";
      return(1);
   }
   else
   {
      print "https://${notes}${page} looking for - $content - Healhcheck check failed.\n";
      return(2)
   }
}
monitor(@ARGV);
```

NOTE@ Custom Monitoring – Use of global variables is not possible. Use local variables only – variables defined inside function

SSL Certificates

The **Configure-SSL Certificates** tab contains four sub-pages. They are organised below.

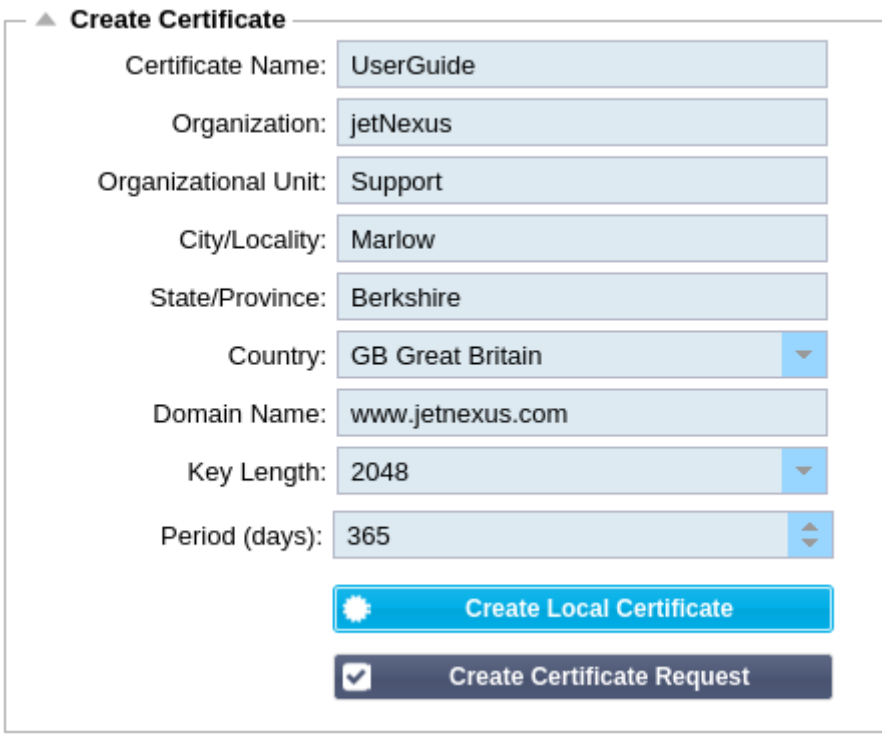
What can edgeNEXUS do with SSL?

The jetNEXUS ALB-X has the ability to offload the SSL encryption and decryption work load from your real servers and also becomes the termination point for your SSL certificates. The jetNEXUS ALB-X also has the ability to re-encrypt traffic to the real servers for more secure environments.

Create Certificate

To create a local certificate:

- Fill in all the details like the example below
- Click on **Create Local Certificate**
- Once you have clicked this you can apply the certificate to a Virtual Service.



To create a Certificate Request:

- Fill in all the details like the example below except for the Period

- Click on the bottom button called “Create Certificate Request”

- Once you have clicked this, a certificate request will pop-up. Please ensure your browser allows pop-ups
- Copy this information from —-Begin Certificate Request—– to —–End Certificate Request—– and paste into a text file
- This information can now be pasted into the CSR required by your Certificate Authority

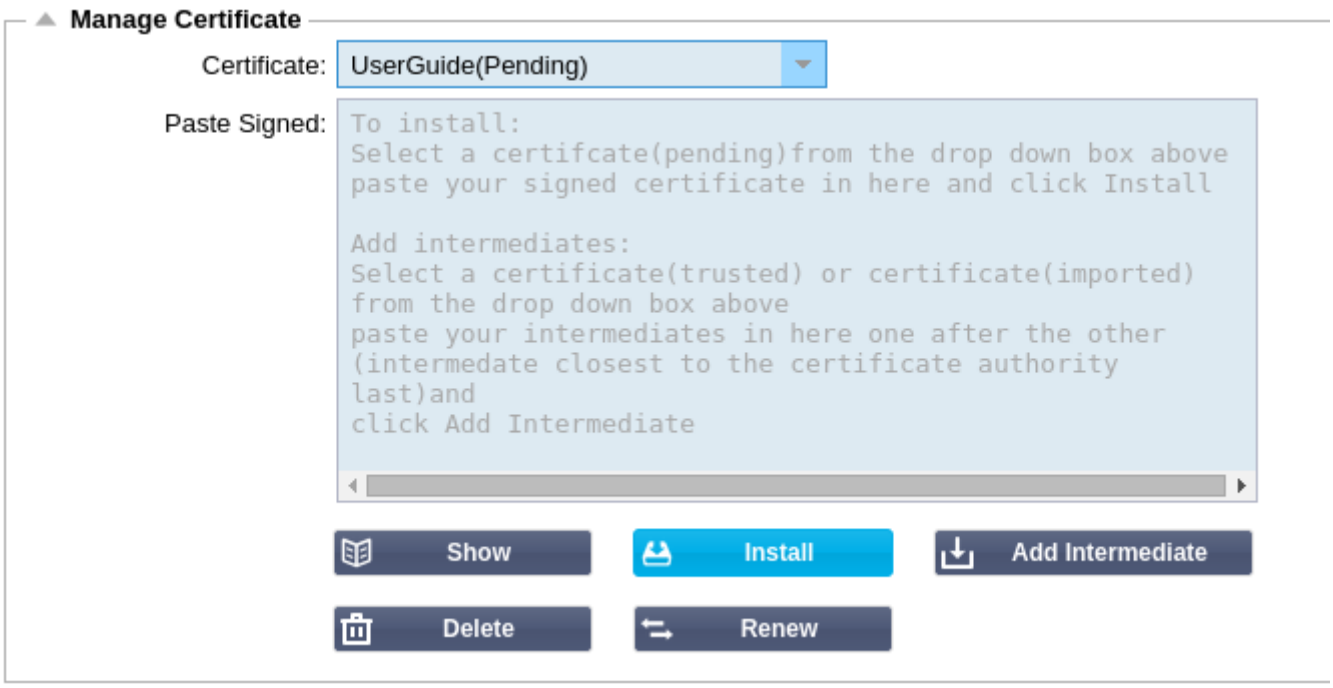
Refer to Installing a certificate to complete the process.

Manage Certificates

Install a certificate:

This will allow you to install a certificate from a CSR:

- Select a certificate from the drop-down list that has (pending) tagged on the end
- Paste your signed certificate that you received back from the Certificate Authority at the top



- You may also paste in the Intermediates below this taking care to follow the correct order:

    1. (TOP)————————————-Your Signed Certificate
    2. (2nd From Top)————————Intermediate 1
    3. (3rd from Top)————————–Intermediate 2
    4. (Bottom)————————————-Intermediate 3
    5. Root Certificate Authority———No need to add this as they exist on the client machines. (ALB-X also contains a root bundle for re-encryption where it acts as a client to a real server)

- Click **Install**
- Once you have installed you should see (Trusted) next to your certificate
- If you have made a mistake or entered the wrong intermediate order then simply select the Certificate (Trusted) and add the certificates (including the signed certificate) again in the correct order and click Install

Add Intermediate:

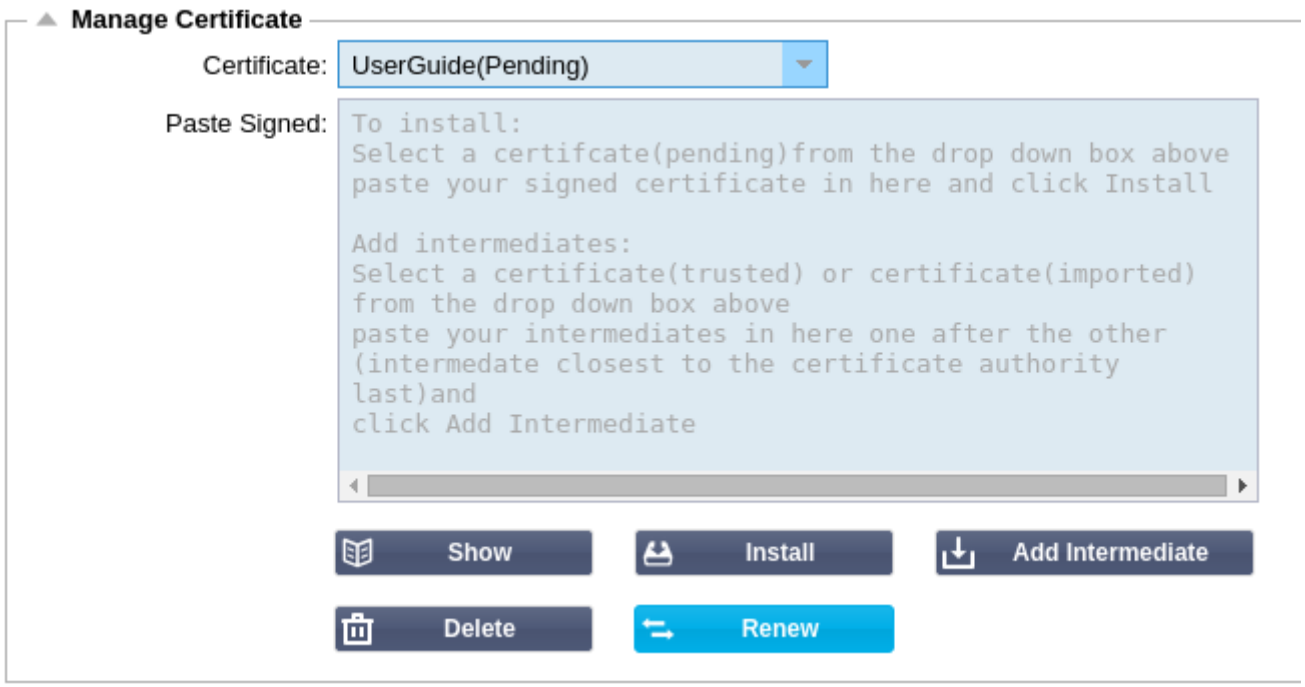
It is useful on occasion to add in the intermediates separately. For example if you have imported a certificate that does not have intermediates.

- Highlight a Certificate (trusted) or certificate (imported)
- Paste the intermediates one below the other taking care that the intermediate closest to the Certificate authority is last
- Click **Add Intermediate.**
- If you make a mistake with the order you can repeat the process and add the intermediates again. This will overwrite the previous intermediates only**.**

Renew a certificate:

This will allow you to obtain a new Certificate Signing Request.

- Select a certificate from the drop-down list, you may choose any certificate (Pending), (Trusted) or (Imported)

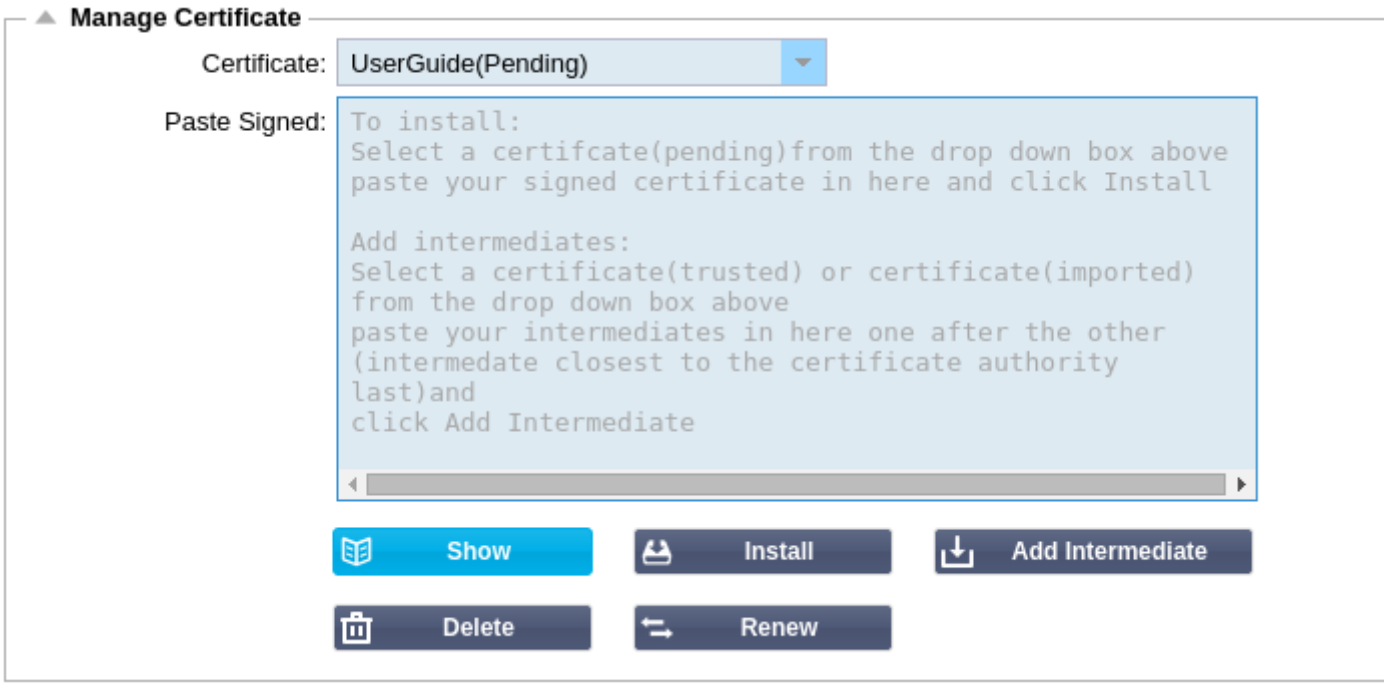


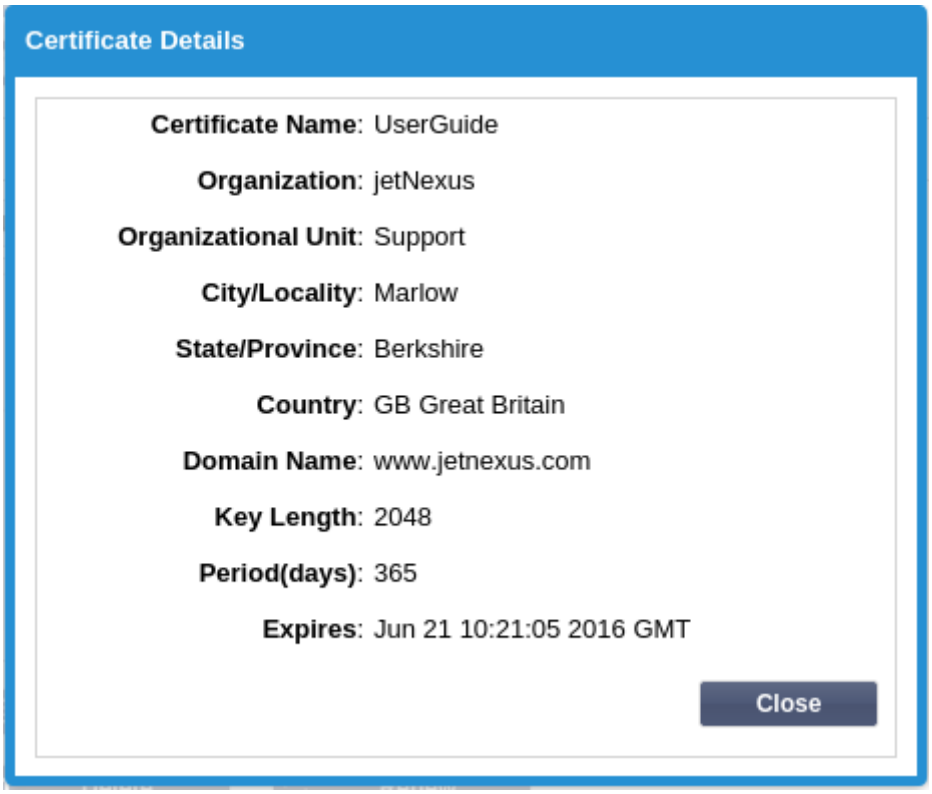
- Click **Renew**
- This will provide a new certificate request as above

Show the details of a certificate:

This will enable you to view the details of the certificate selected:

- Select a certificate from the drop-down list
- Click **Show**
- A pop-up will provide the details of the certificate like the example below

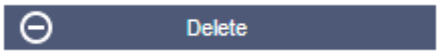




Delete a Certificate:

This will allow you to delete the selected certificate from the ALB-X

- Select a certificate from the drop-down list
- Click “Delete” at the bottom of the page



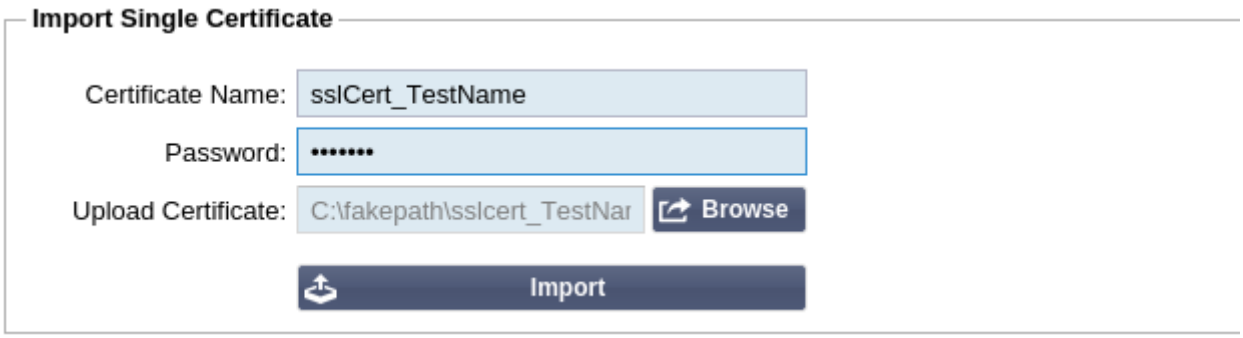
- The certificate is no longer installed on the jetNEXUS ALB-X

Import Certificate

Single Certificate:

This section allows you to import a signed certificate from a trusted Certificate Authority (CA). The signed certificate must be in PKCS#12 format. This container format can contain multiple embedded objects, such as multiple certificates and is usually

protected with a password.



To import your certificate:

- Give your certificate a friendly name, this is to identify it in the drop down list. It does not need to be the same as the certificate domain name and must be alphanumeric only with no spaces
- Type the password you used to create the PKCS#12 container
- Browse for the certificate.pfx
- Click **Import.**
- Your certificate will now be in the SSL drop down box for your channel

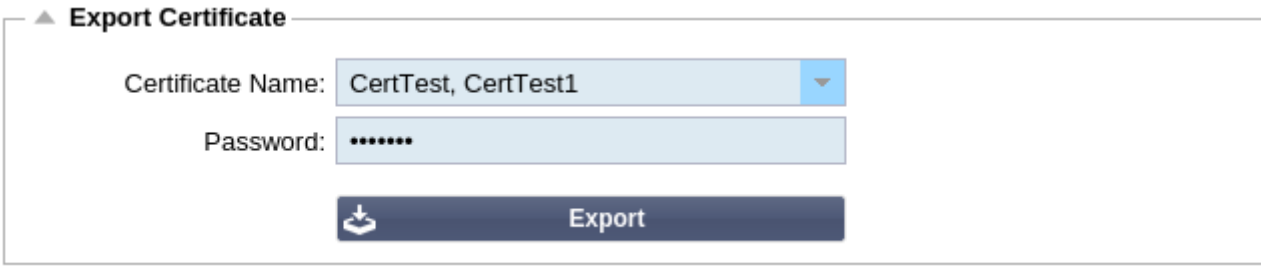
Multiple Certificates:

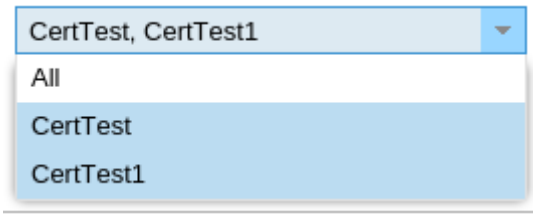
This section allows you to import a JNBK file that contains multiple certificates. A JNBK is an encrypted file produced by jetNEXUS ALB-X when exporting multiple certificates.

- Browse for your filename.jnbk file – you can create one of these by exporting multiple certificates
- Type the password you used to create the jnbk file
- Click **Import.**
- Your certificates will now be in the SSL drop down box for your service

Export Certificate

This section allows you to export any certificates that are installed on the jetNEXUS ALB-X. The certificate will be exported in PKCS#12 container format which will include the private key and intermediate certificates.





- Tick the certificate or certificates you wish to install. You may all tick All to automatically tick all certificates
- Type a password to protect your certificates. This must be at least 6 characters in length. Letters, numbers and certain symbols can be used
- The following characters cannot be accepted < > ” ‘ ( ) ; \ | \A3 % &
- Click **Export**
- Single Certificate: Your certificate will be saved as sslcert_<certificatename>.pfx – Example **sslcert_Test1Cert.pfx**
- Multiple Certificates: Your certificates will we saved as **sslcert_pack.jnbk**

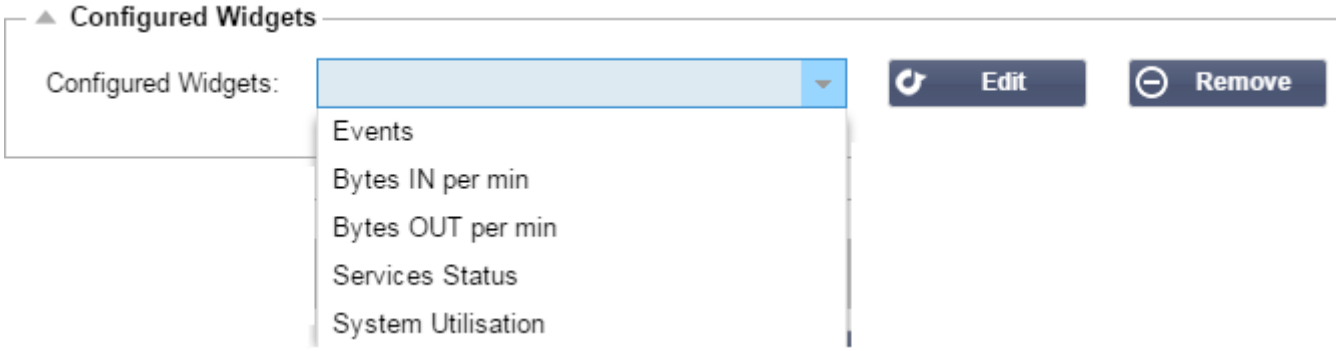
Note: A jnbk file is an encrypted container file produced by the jetNEXUS ALB-X. These types of files can only be imported by the jetNEXUS ALB-X

Widgets

The **Library — Widgets** page allows you to configure various lightweight visual components that can be displayed in your custom dashboard.

Configured Widgets

In this section you will be able to view, edit or remove any widgets that you have created from the available widgets section

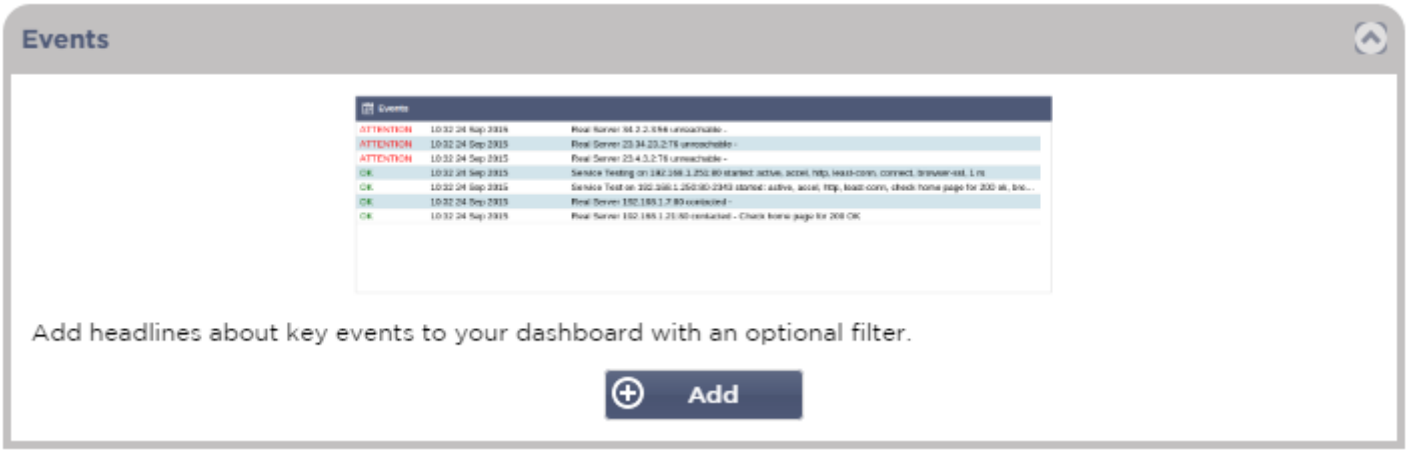


Available Widgets

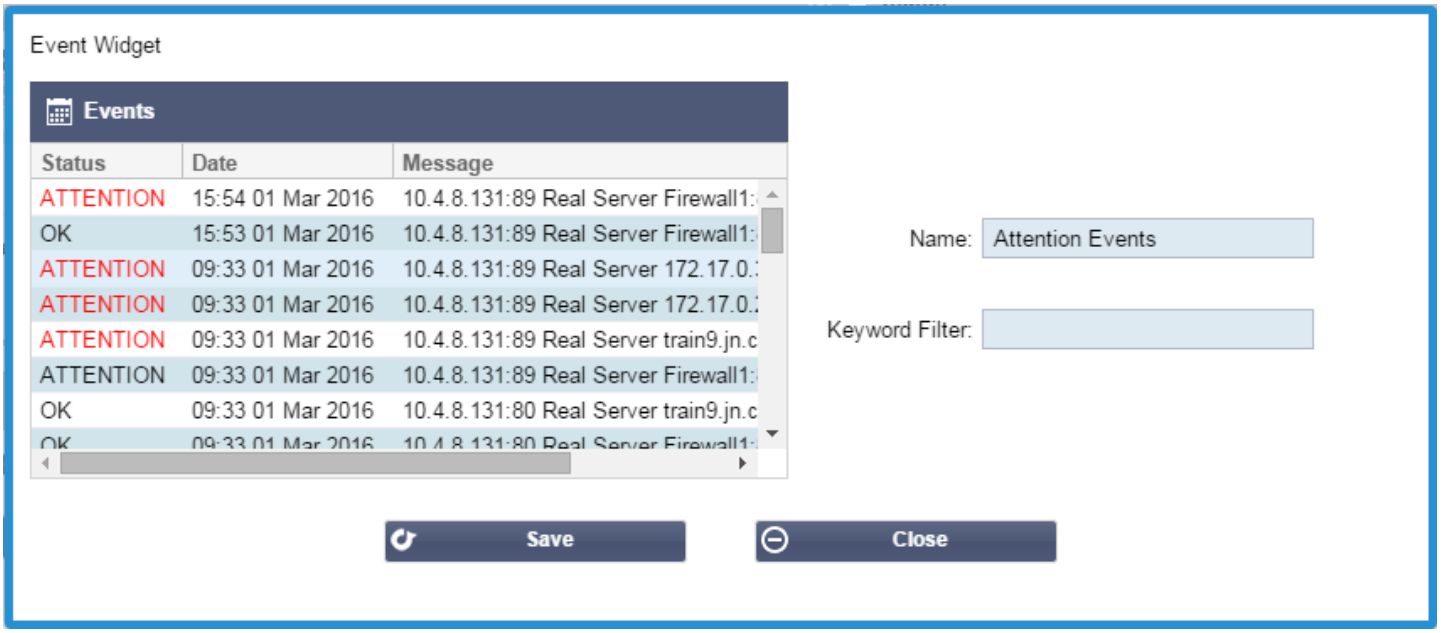
Choose from 5 types of Widgets that you can customize:

Events:

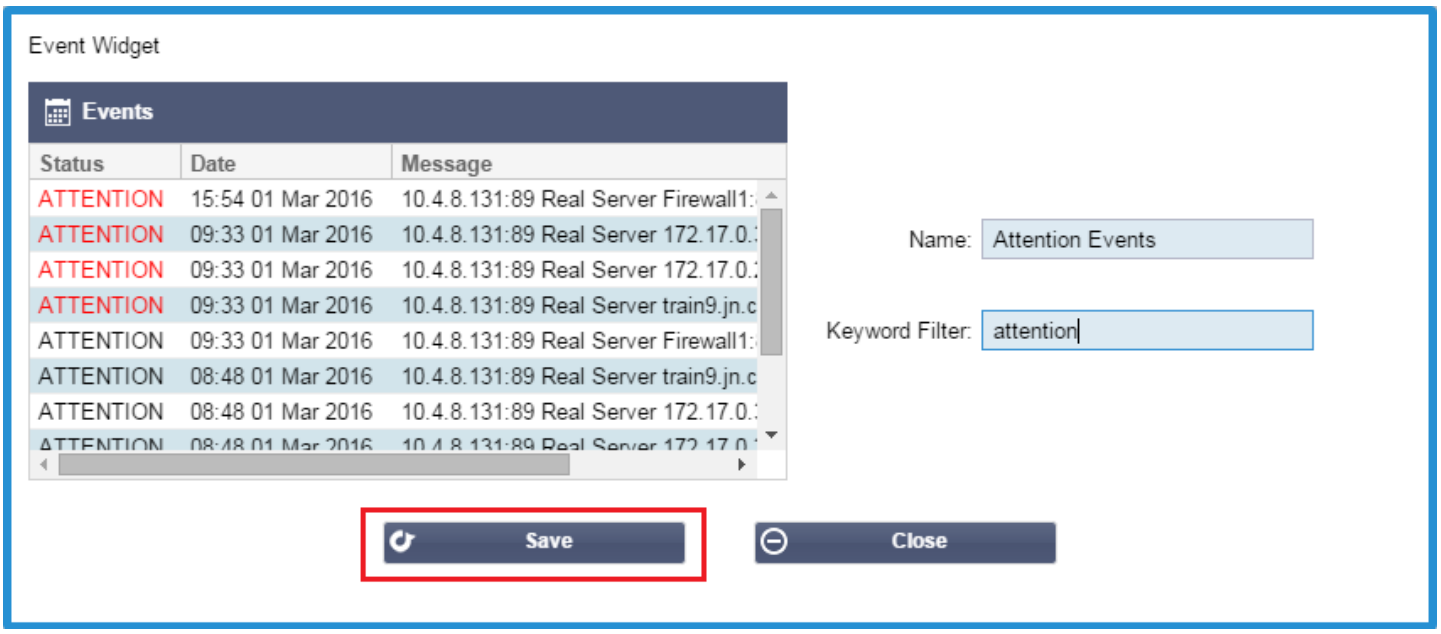
- Click **Add.**



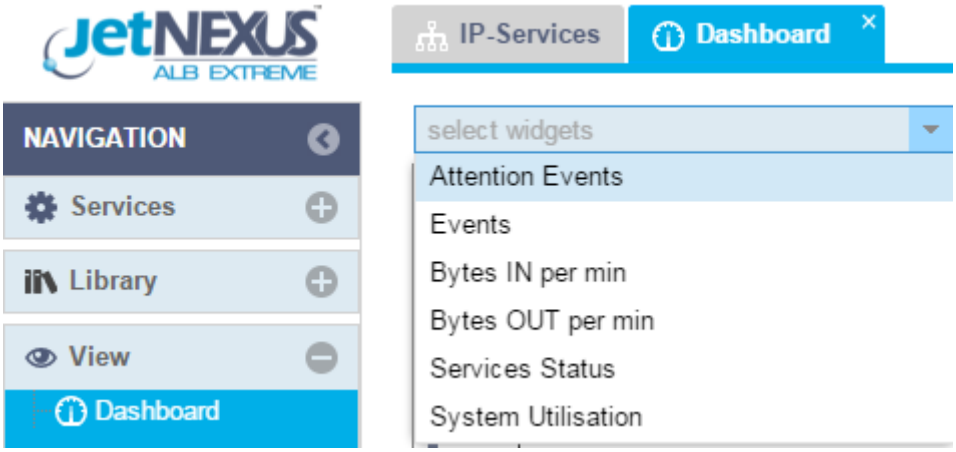
- Name your **Event.**



- Add a keyword filter then click **Save** then **Close.**



- You will now see an additional Widget called **Attention Events** in the Configured Widgets drop down.
- You can now add this **Attention Events** in the **View — Dashboard.**
- Select **Attention Events** to add this widget to the **View — Dashboard** page.

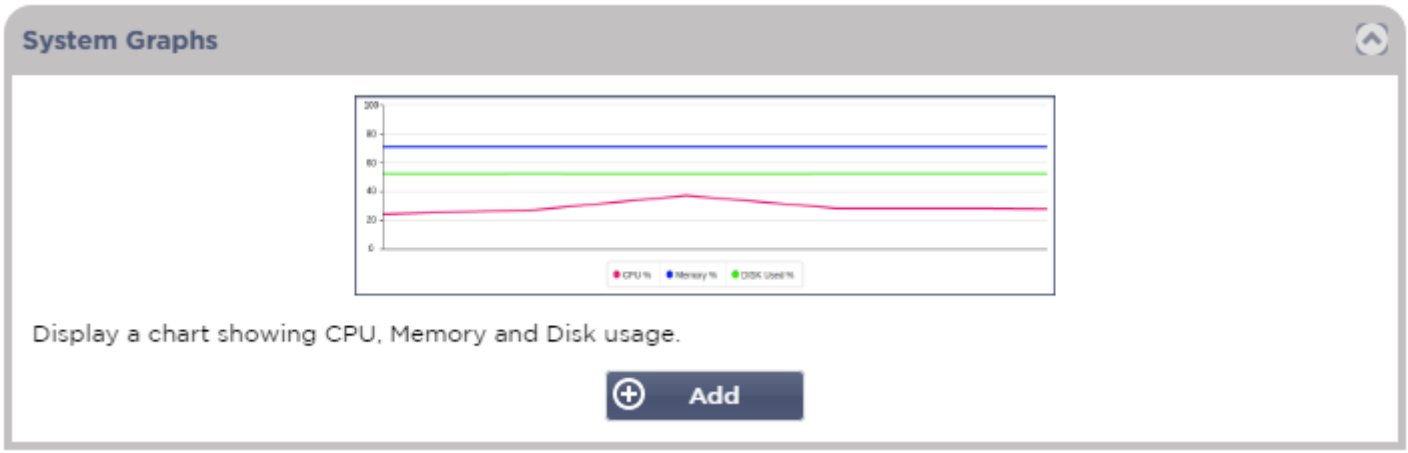


- You can move your widgets up and down and resize them
- If you have a lot of widgets with many live graphs then it is advisable to **Pause Live Data** and minimise the widgets before re-ordering.

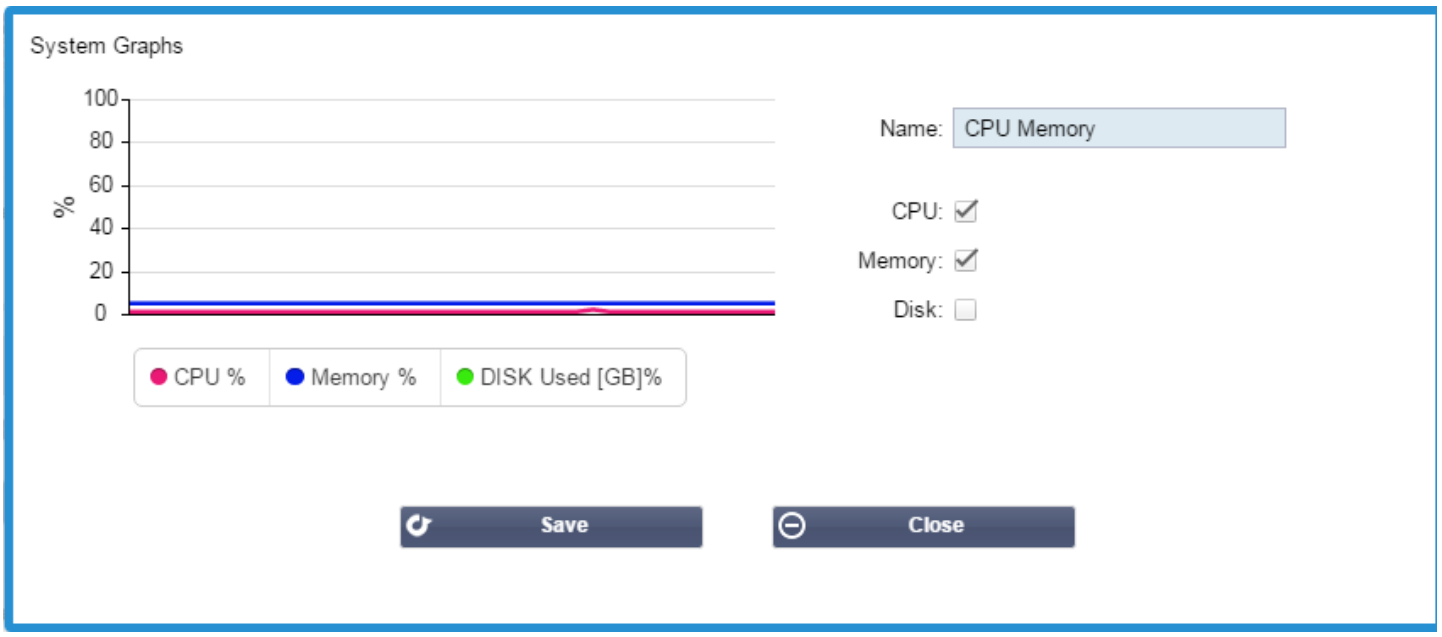
- Once you have re-arranged your dashboard you can click **Play Live Data** to start receiving live information

System Graphs:

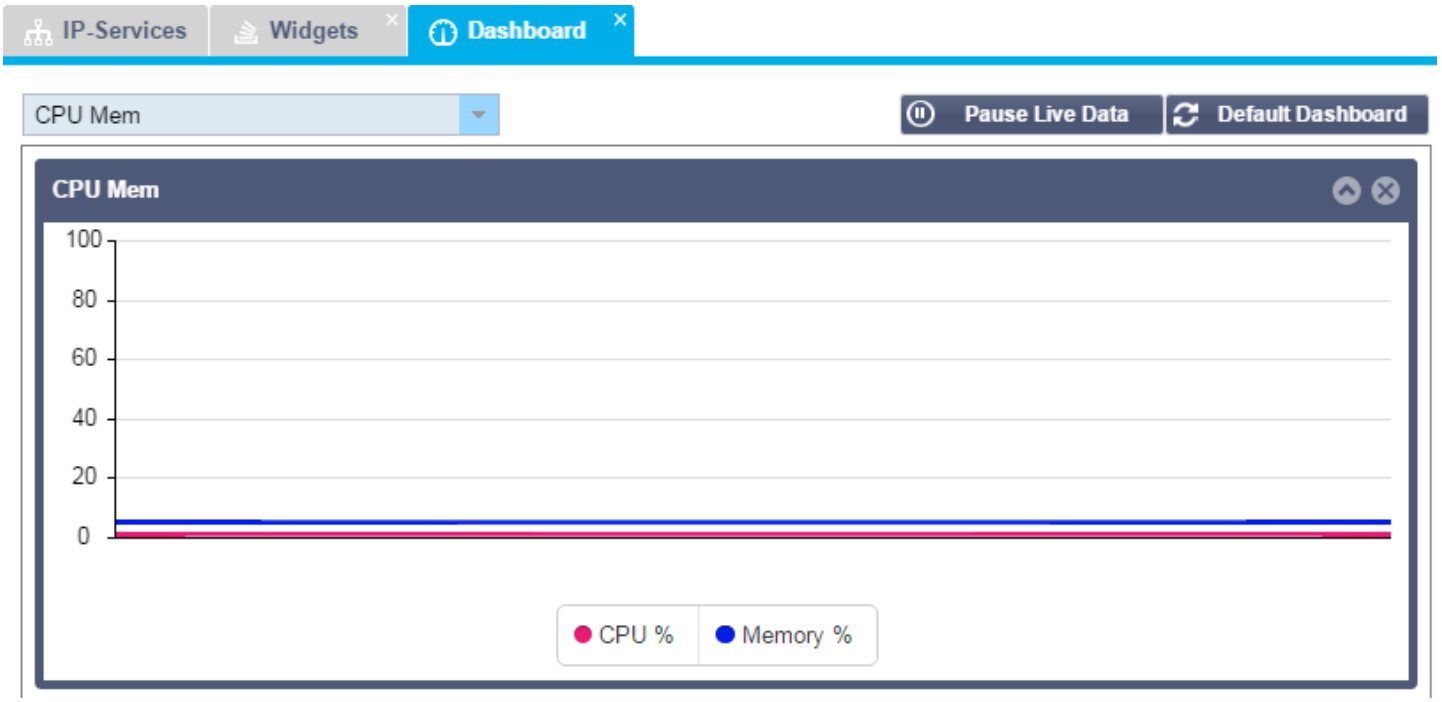
- Click **Add**



- Name your **System Graph**



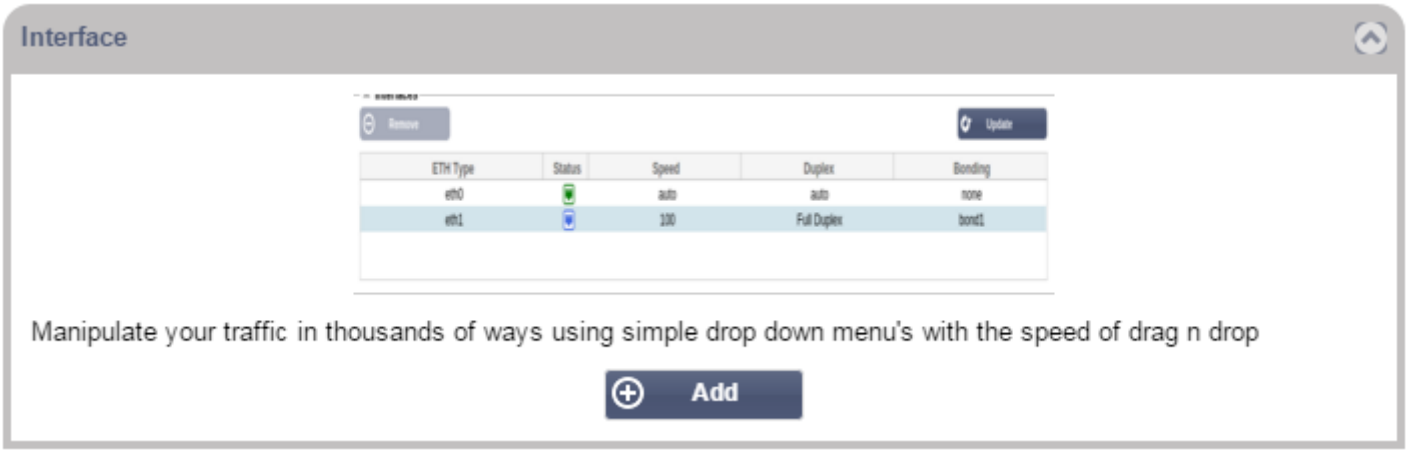
- You have three options for this graph. Tick the boxes that you wish to show in the graph
- Click **Save** then **Close**
- You can now add your **CPU Mem** widget to the **View — Dashboard** page.



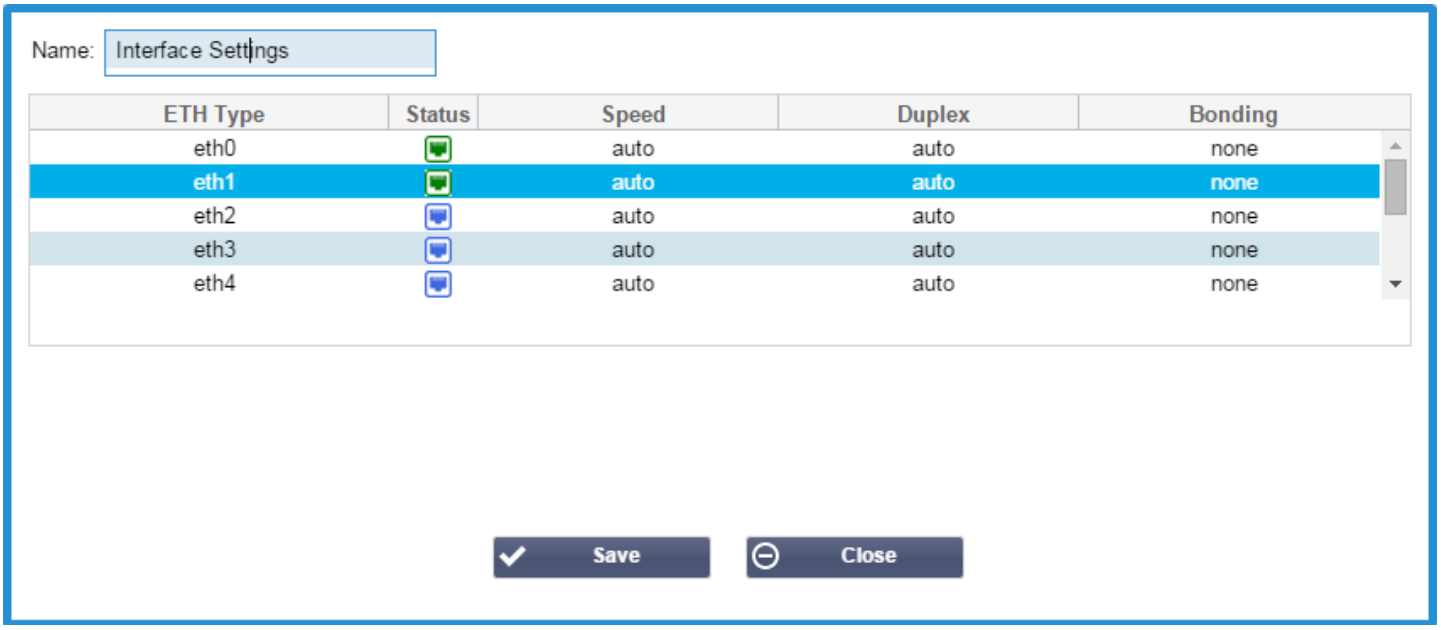
Interface:

This widget will show you the interface settings including status of each interface. It will show you all interfaces available on your ALB-X.

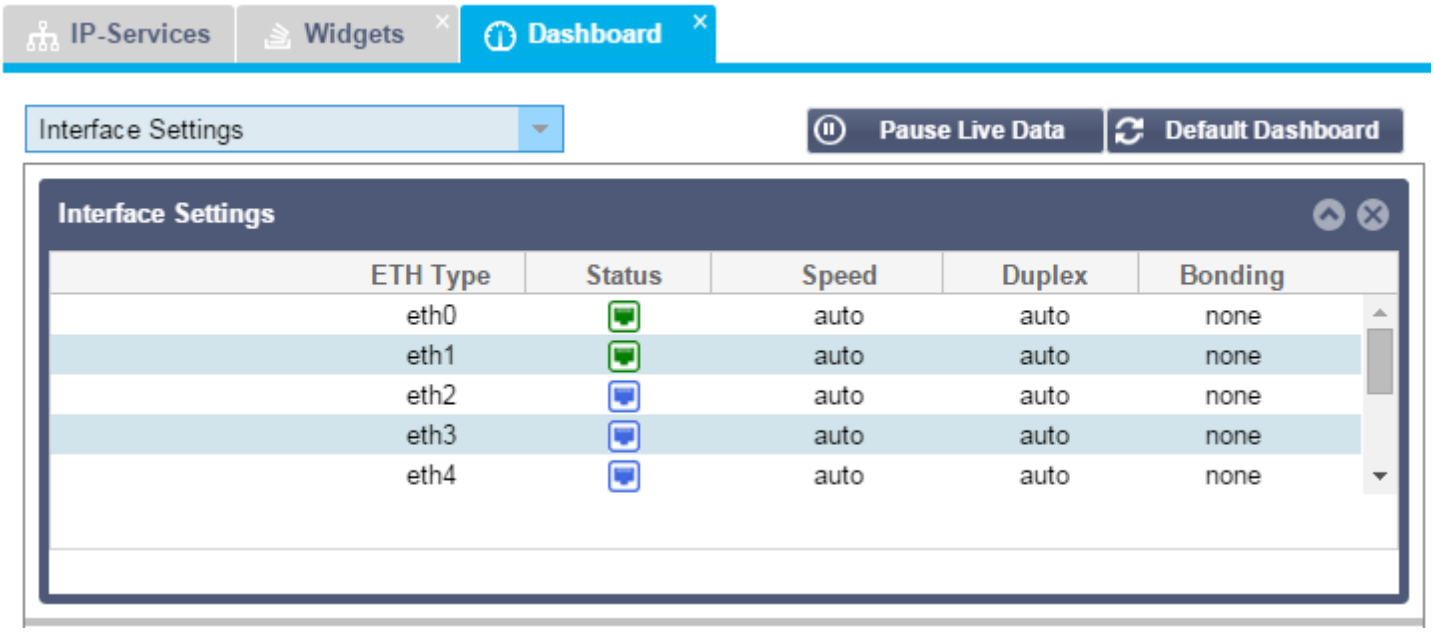
- Click **Add**



- Name your **Interface** widget



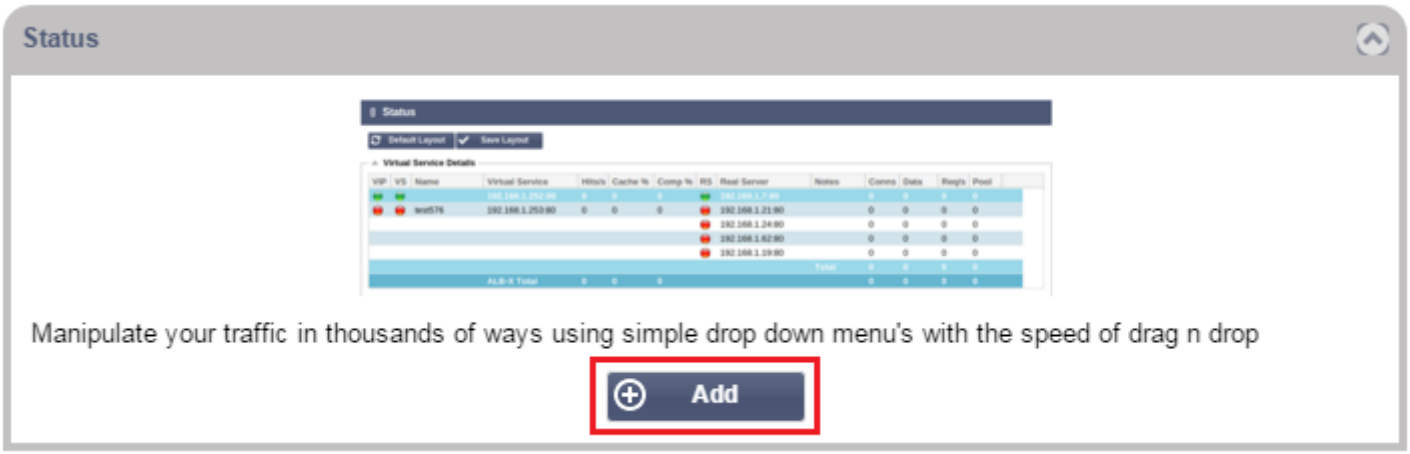
- Click **Save** and **Close**
- You can now add this widget to the **View — Dashboard** page.



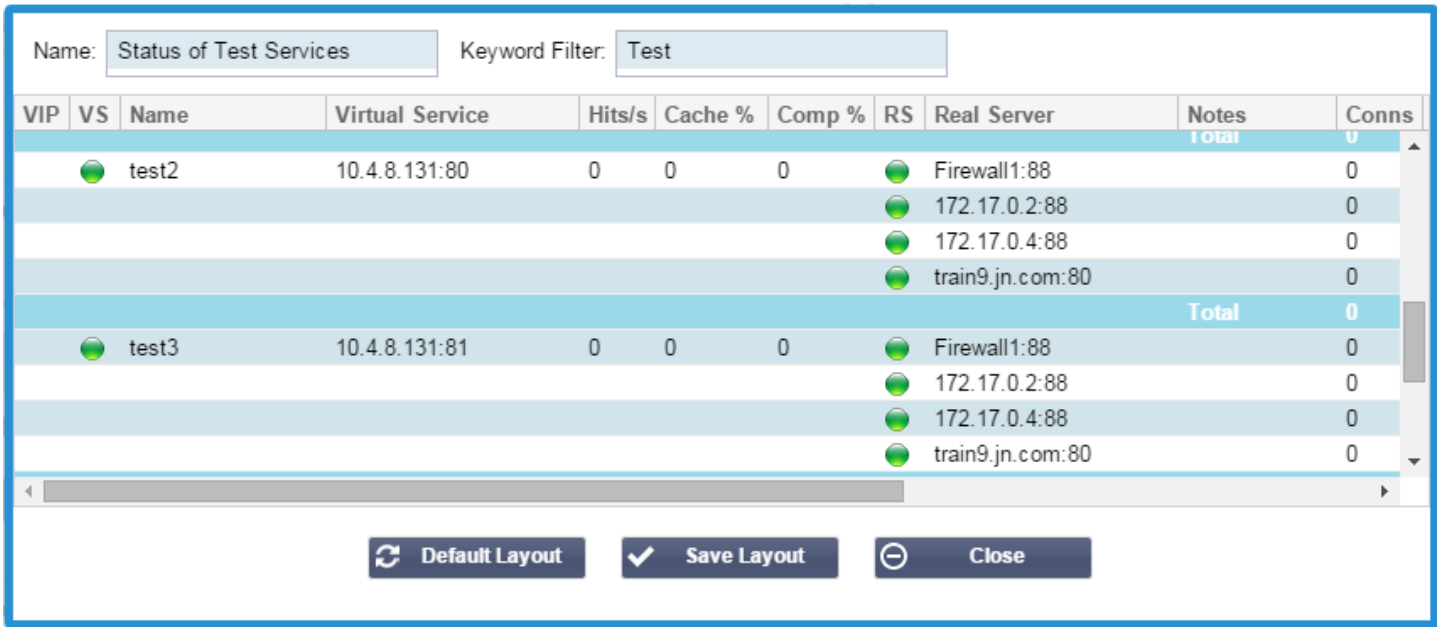
Status:

The Status widget allows you to see load balancing in action. You can also filter the view to show specific information.

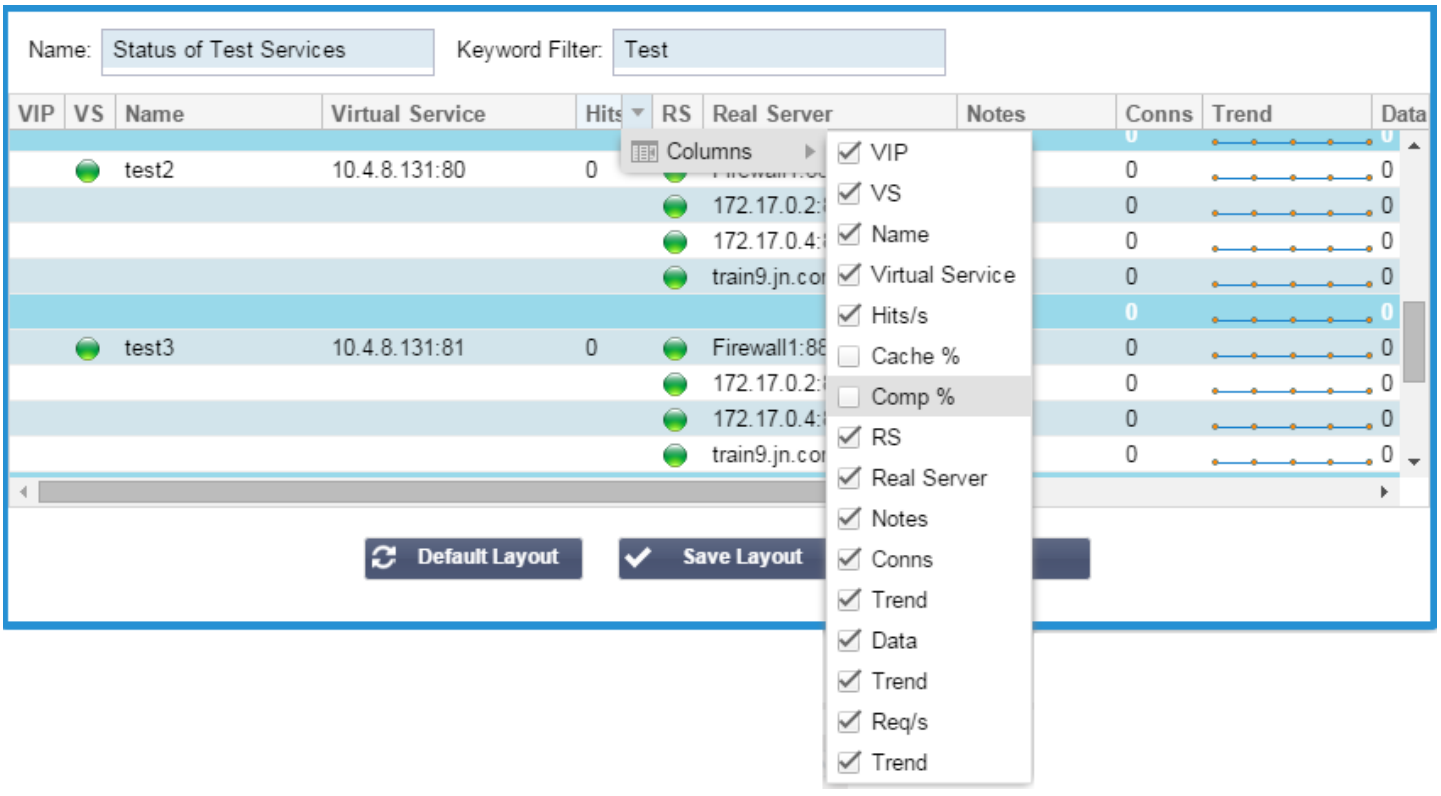
- Click **Add.**



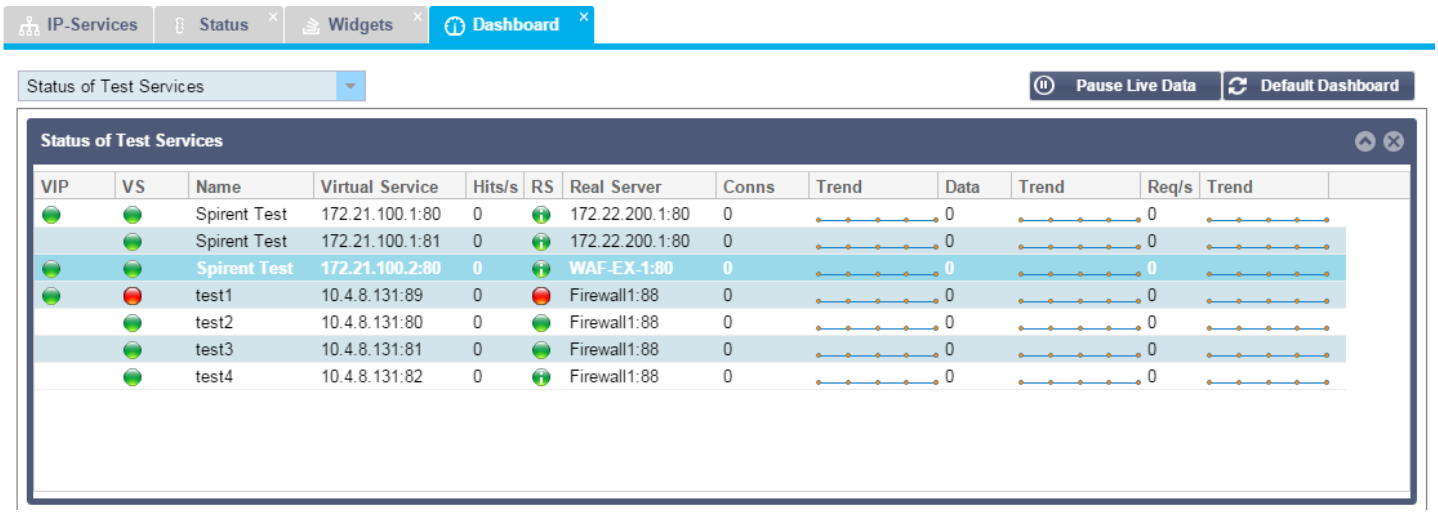
- Name your **Status** widget and add a filter if you wish to.



- You can also choose to tick which columns to show



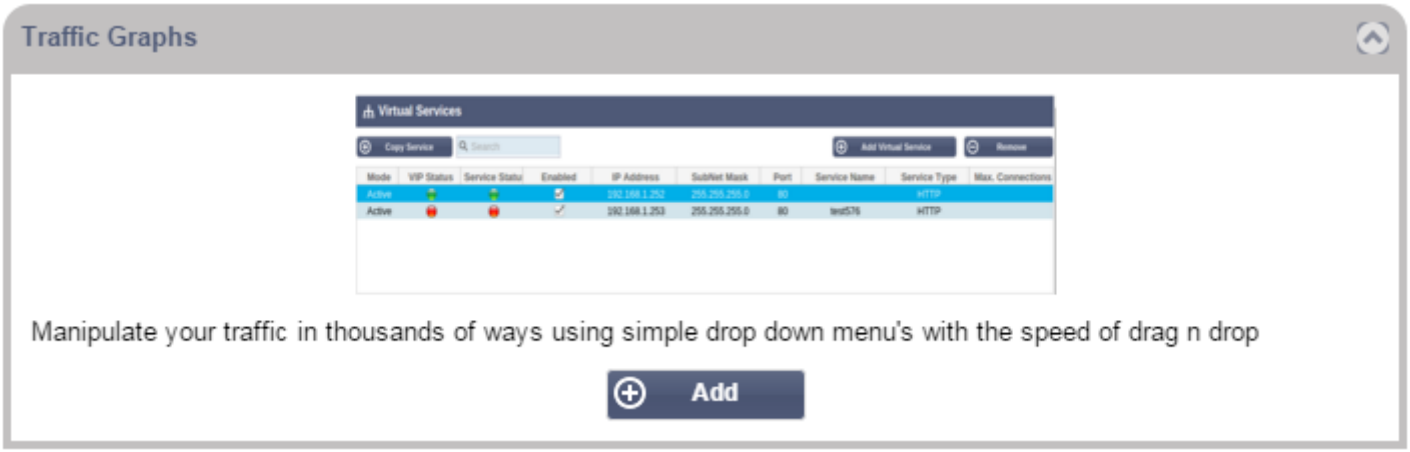
- Click **Save Layout** then **Close.**
- You can now add your **Status of Test Services** widget to the **View — Dashboard** page.



Traffic Graphs:

This widget can be configured to show current and historic traffic data per Virtual Services and Real Servers. In addition you can see overall current and historic data for global traffic

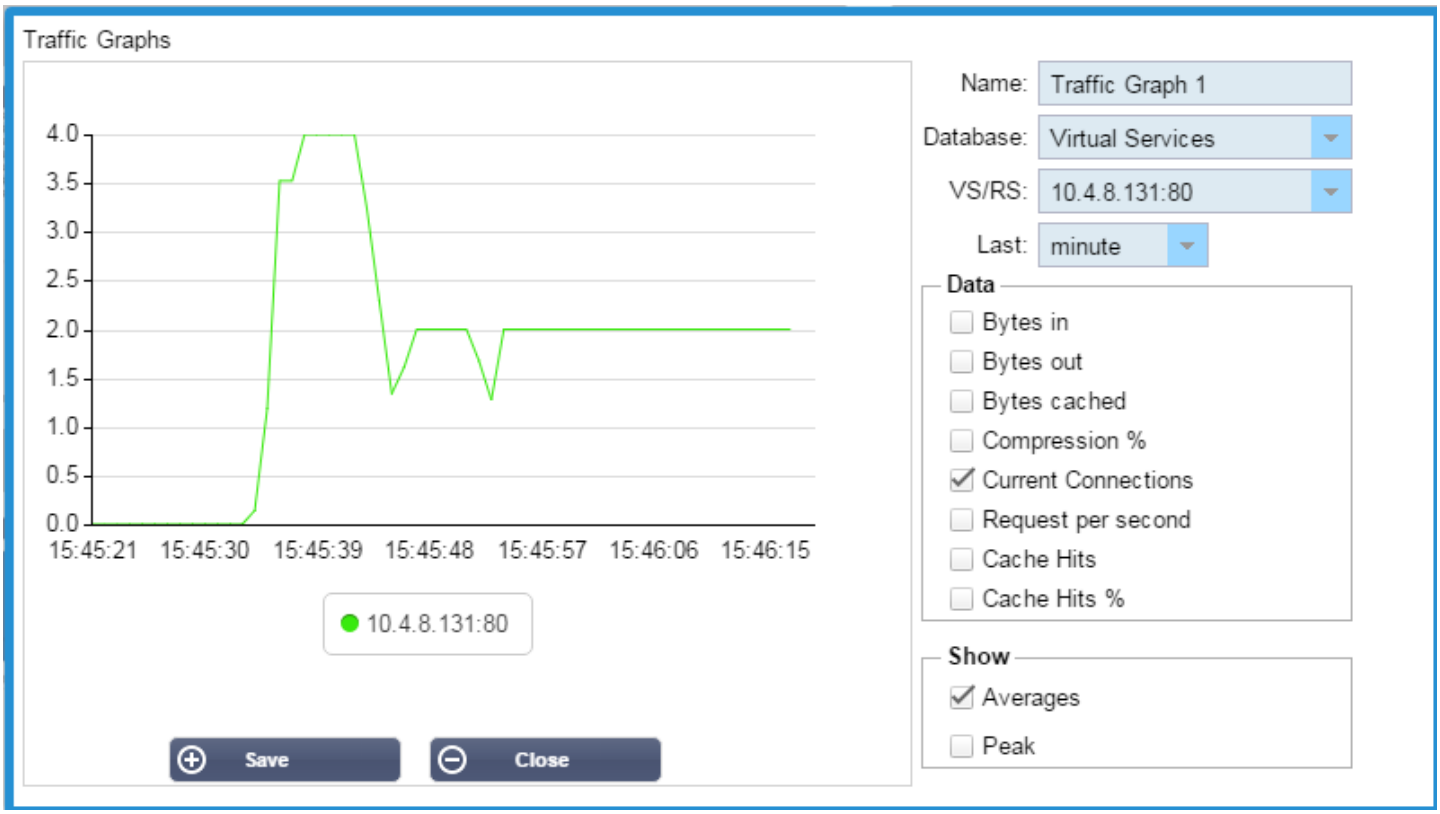
- Click **Add**



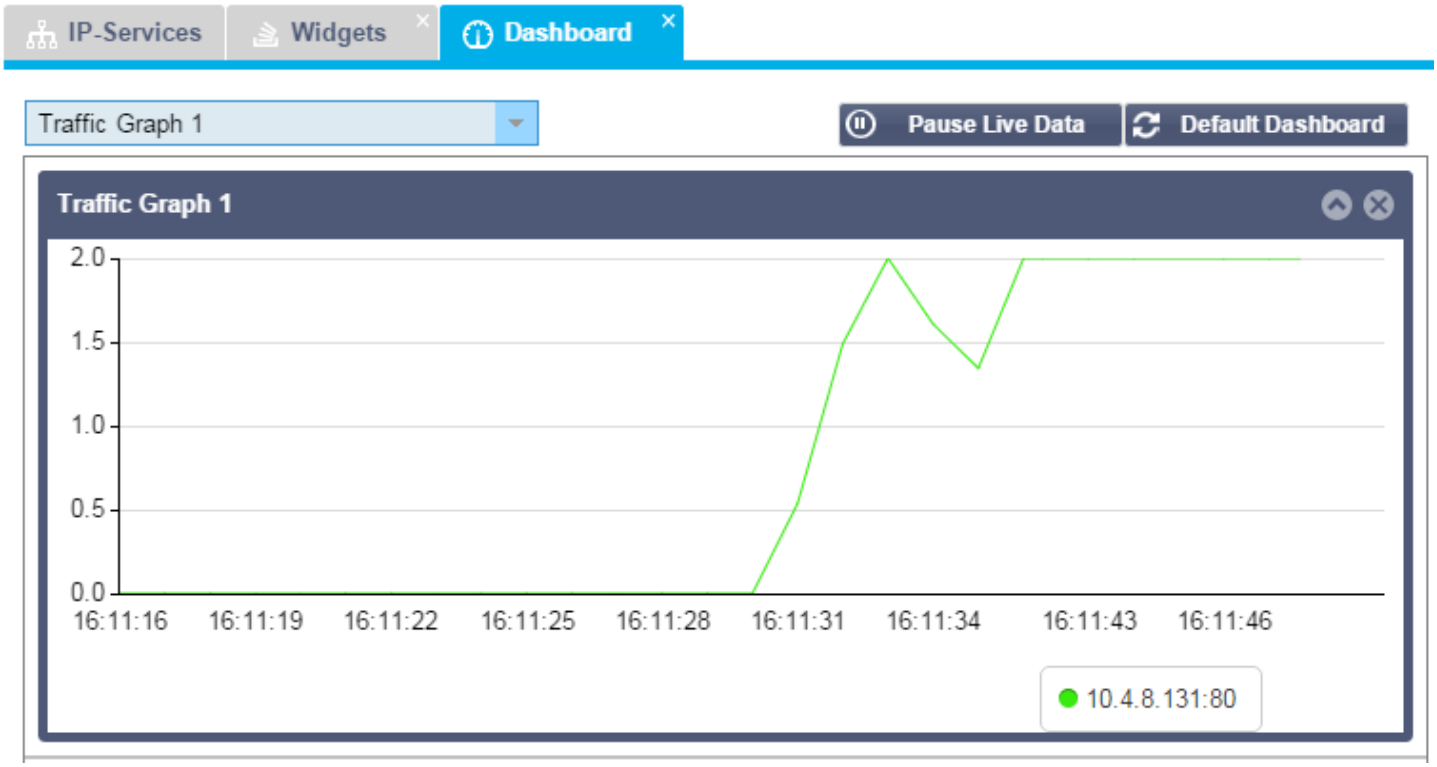
- Name your widget.
- Choose a Database from **Virtual Services, Real Servers** or **System.**
- If you choose **Virtual Services** then you can choose a virtual service from the **VS/RS** drop down.
- Choose a time frame from the **Last** drop down.
    - **Minute** – last 60s
    - **Hour –** aggregated data from each minute for the last 60 minutes
    - **Day –** aggregated data from from each hour for the last 24 hours
    - **Week –** aggregated data from each day for the last 7 days
    - **Month** – aggregated data from each week for the last 7 days
    - **Year** – aggregated data from the each month for the last 12 months
- Choose the **Data** available depending on the database you have chosen
    - **Virtual Services Database**
        - **Bytes in**
        - **Bytes out**
        - **Bytes cached**

        - **Compression %**
        - **Current Connections**
        - **Requests per second**
        - **Cache Hits**
        - **Cache Hits %**
    - **Real Servers**
        - **Bytes in**
        - **Bytes out**
        - **Current Connections**
        - **Request per second**
        - **Response time**
    - **System**
        - **CPU %**
        - **Services CPU**
        - **Memory %**
        - **Disk Free %**
        - **Bytes in**
        - **Bytes out**
- Chose to show either **Average** or **Peak values**
- Once you have chosen all the options click **Save** and **Close**

Example Traffic Graph:



- You can now add your **Traffic Graph 1** widget to the **View — Dashboard** page.

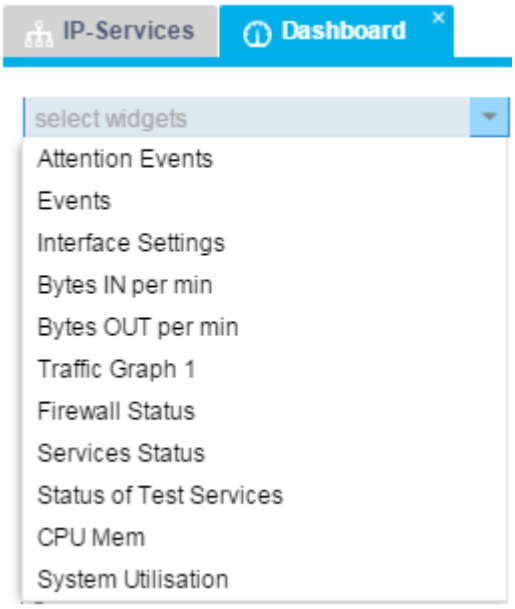

IP-Services
Widgets
Dashboard
Traffic Graph 1
Pause Live Data
Default Dashboard
Traffic Graph 1
2.0
1.5
1.0
0.5
0.0
16:11:16
16:11:19
16:11:22
16:11:25
16:11:28
16:11:31
16:11:34
16:11:43
16:11:46
10.4.8.131:80

Dashboard

The **View — Dashboard** page shows a number of default widgets that can be customised in the **Library — Widgets** page. You can also resize each widget and drag and drop them to create a custom Dashboard. The standard default dashboard comes with 5 pre-configured full width widgets

Adding a Widget

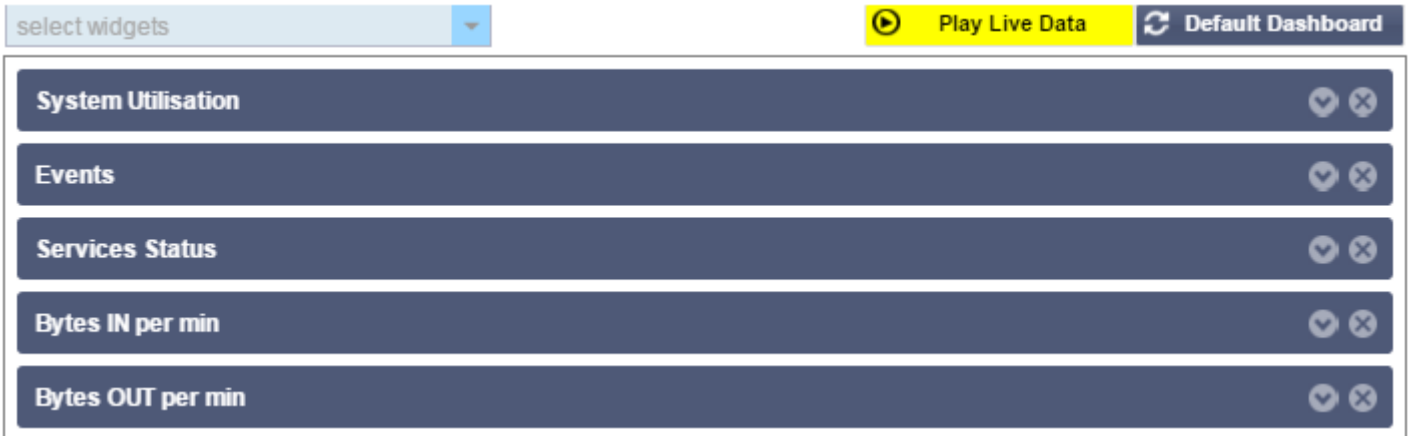
- At the top left of the page you will find a drop down of all the widgets that have been created in the **Library — Widgets** page.
- Simply select the widget name and it will automatically be added to the bottom of the page
- You can add 4 widgets for each type of widget to a maximum of 20 widgets displayed



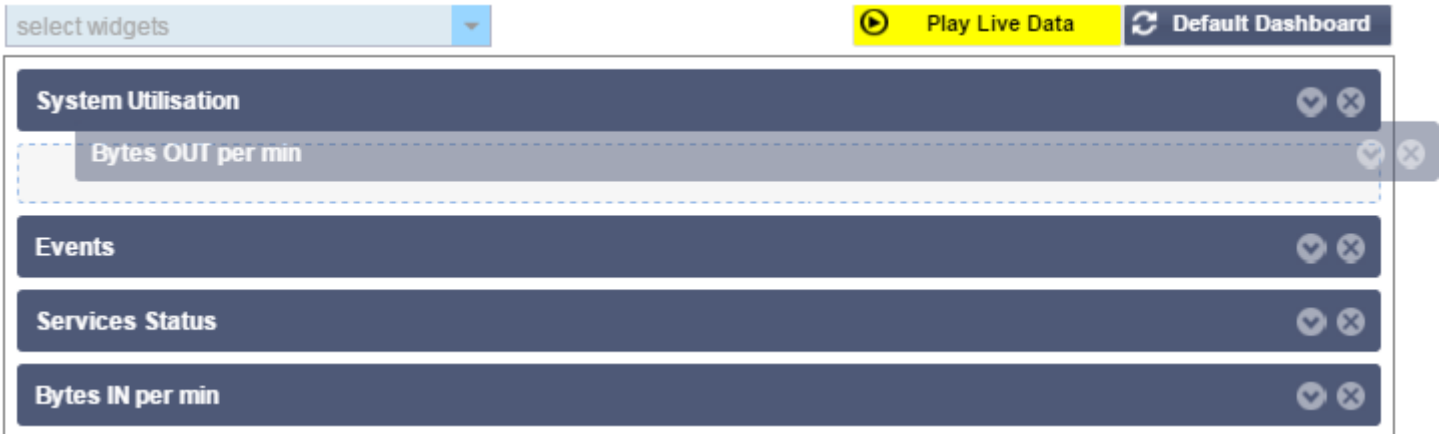
Customising the Dashboard

- The most efficient way to customise the **Dashboard** is to **Pause Live Date** then minimise each widget.

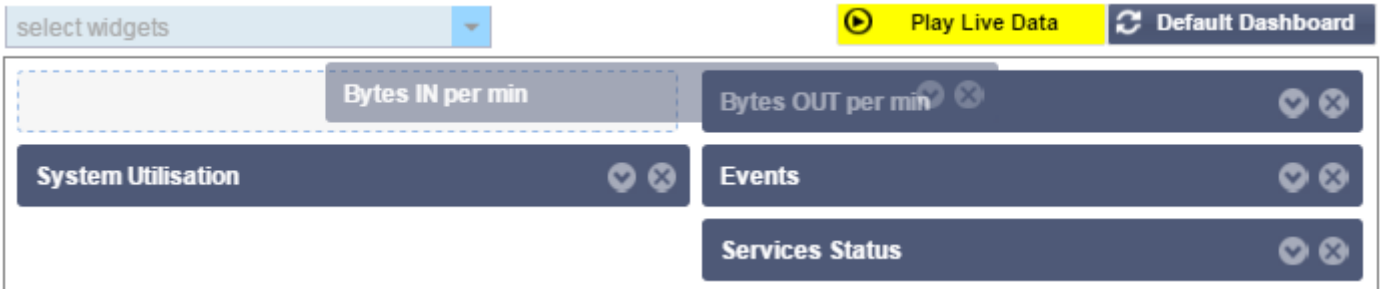
- The pause button will change colour to yellow and display **Play Live Data**



- Drag and drop a widget to change the order. Here we have selected the **Bytes OUT per min** and dragged it to position number two in the list. You will can use the dotted line as a guide to where your widget will move to.



- You can also resize a widget by dragging it to the position you want and dragging the mouse sideways. Watch for the dotted line to indicate what will happen when you drop it.

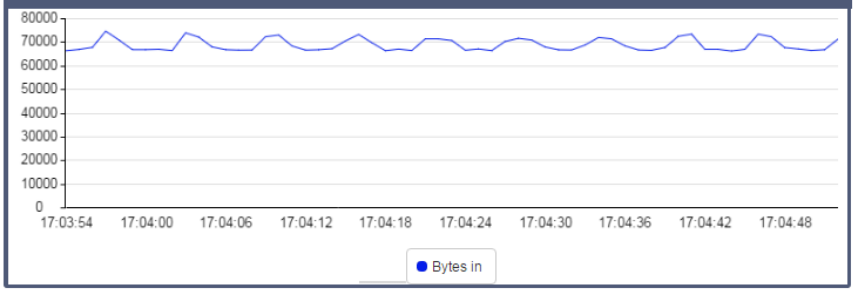


- Now it is time to expand all of the widgets and click **Play Live Data**

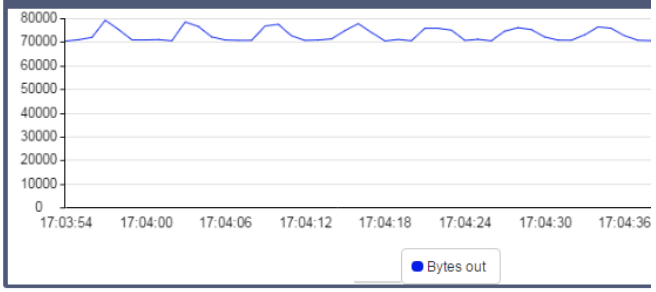
select widgets

Play Live

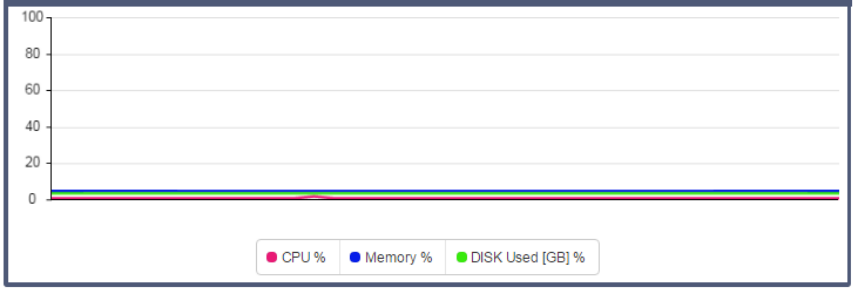
Bytes IN per min



Bytes OUT per min



System Utilisation



Events

Status	Date	Message
OK	16:48 02 Mar 2016	Service on 10.4.8.131:89 started: s/a, accel, http, least-conn, n
OK	16:48 02 Mar 2016	Service on 10.4.8.131:89 updated: s/a, accel, http, least-conn,
OK	15:45 02 Mar 2016	10.4.8.131:80 Real Server 10.4.8.201:80 contacted - Echo=Ok
ATTENTION	08:52 02 Mar 2016	10.4.8.131:89 Real Server train9.jn.com:80 unreachable - Con
ATTENTION	08:52 02 Mar 2016	10.4.8.131:89 Real Server 172.17.0.2:88 unreachable - Conne
ATTENTION	08:51 02 Mar 2016	10.4.8.131:89 Real Server Firewall1:88 unreachable - Connec
ATTENTION	08:51 02 Mar 2016	10.4.8.131:89 Real Server 172.17.0.3:88 unreachable - Conne
OK	08:51 02 Mar 2016	10.4.8.131:80 Real Server train9.jn.com:80 contacted - Echo=
OK	08:51 02 Mar 2016	10.4.8.131:80 Real Server 172.17.0.2:88 contacted - Echo=Ok
OK	08:51 02 Mar 2016	10.4.8.131:80 Real Server 172.17.0.4:88 contacted - Echo=Ok

Services Status

VIP	VS	Name	Virtual Service	Hits/s	Cache %	Comp %	RS	Real Server	Notes	Conns	Trend	Data	Trend	Req/s	Trend
		Spirent Test	172.21.100.1:80	0	0	0		172.22.200.1:80		0		0		0	
								172.22.200.2:80		0		0		0	
								172.22.200.3:80	gary	0		0		0	
								172.22.200.4:80		0		0		0	

View History

The **View — History** page displays the historical traffic for your system, virtual services and real services. It is a great way to see load balancing in action and view any errors or patterns over time. Note that you must enable historical logging from the **System — History** page.

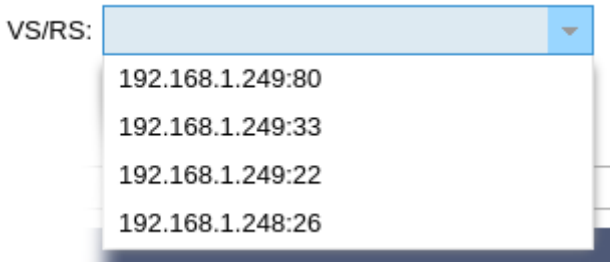
How do I see some graphs?

1. Choose a Database:

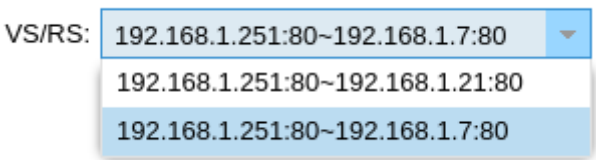
System:
Selecting this database will allow you to see CPU, memory and disk drive space over time
Virtual Services:
Selecting this database will allow you to choose all of the virtual services in the database from the time that you started logging data
Real Services:
Selecting this database will allow you to choose all the real servers in the database from the time that you started logging the data.

2. Choose VS/RS: Virtual Service or Real Server: Note this will be blank if you choose the system database as it is not relevant

If Virtual Services Database chosen from above. You should now see a list of virtual services. Click those that you wish to view, each one you click will be highlighted



If Real Servers Database chosen from above. You should now see a list of real servers. Click those that you wish to view, each one you click will be highlighted



3.

Last Minute:
The graph will contain 60 data points, one for each second
Last Hour:
The graph will contain 60 data points, one for each minute
Last Week:
The graph will contain 24 data points, one for each hour
Last Month:
The graph will contain 32 data points one for each day
Last Year:
The graph will contain 24 data points, two for each month

4. Choose a metric

System:
CPU % – This will show the maximum/average CPU % over the time period selected Memory % – This will show the maximum/average Memory % over the time period selected Compression % – This will show the maximum/average Compression % over the time period selected
Virtual Services:
Bytes in – This will show the maximum/average traffic flow in from the server in Bytes over the time period selected Bytes out – This will show the maximum/average traffic flow out to the client in Bytes over the time period selected Bytes cached – This will show the maximum/average size of the cached objects in Bytes over the time period selected Compression % Current Connections Request per second Cache HIts Cache Hits%
Real Servers:
Bytes in Current Connections: Pool Size Request per second

5. Choose what to Show

Averages:
This will show the average values over the period of time selected
Maximum:
This will show the maximum data values over the period of time selected

Data Set

Database: Virtual Services

VS/RS: 192.168.1.248:80, 192.168.1.251:80

Update

Last: minute

Globals

Metrics

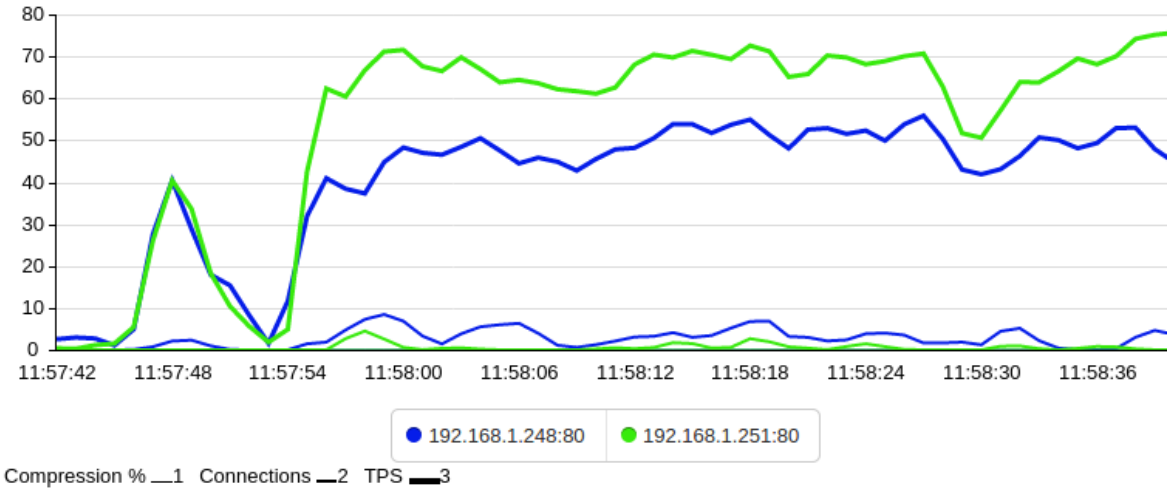
Data

- [ ] Bytes in
- [ ] Bytes out
- [ ] Bytes cached
- [x] Compression %
- [x] Current Connections
- [x] Request per second
- [ ] Cache Hits
- [ ] Cache Hits %

Show

- [x] Averages
- [ ] Peak

Graph



192.168.1.248:80 192.168.1.251:80

Compression % 1 Connections 2 TPS 3

View Logs

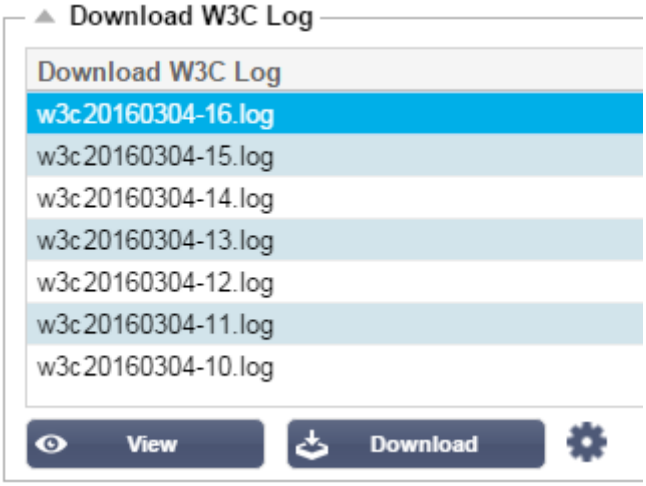
The **View — Logs** page allows you to view the **W3C logs** and the **System logs**. The page is organised into the two sections below.

Download W3C Log

Once you have configured your W3C logging level you can view or download the log in this section. The format for each log is:

- Name – w3c
- Year
- Month
- Day
- Hour

1. Highlight the required log.
2. Click **View** for a browser pop-up and the option to open with a text editor.
3. Click **Download** to automatically download to your browser download folder.
4. The downloaded file will append the name of the ALB to the file name. Example: w3c20160624-14_TR-E4-2.log
5. Click the **Cog** to open the **System Logging** page. Here you can configured the W3C levels and options.

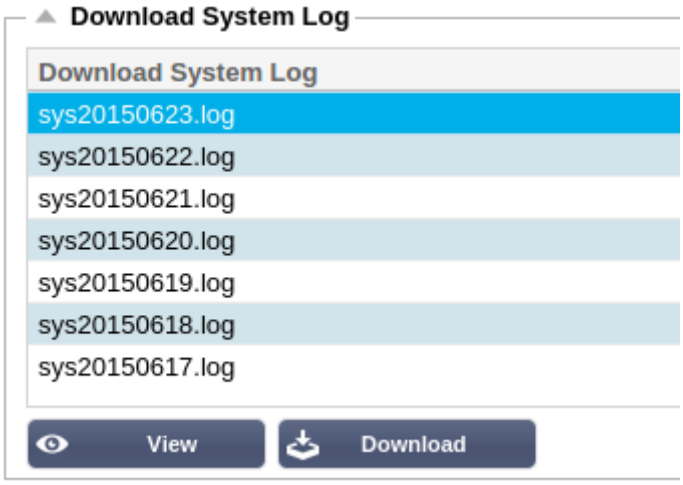


Download System Log

The format for each log is:

- Name – sys
- Year
- Month
- Day

1. Highlight the required log.
2. Click **View** for a browser pop-up and the option to open with a text editor.
3. Click **Download** to automatically download to your browser download folder.
4. The downloaded file will append the name of the ALB to the file name. Example: sys20160624_TR-E4-2.log



Statistics

The **Monitor-Statistics** pageimg allows you to view information about the traffic flowing through your jetNEXUS ALB-X. The page is split into four sections and organised below.

Total Input/Output

This statistic reports the raw data in and out of the ALB-X. The unit of measurement will change as the size grows from kbps to Mbps to Gbps

Total Input	= 2.13 GB	Input/s	= 9.10 Mbps
Total Output	= 2.18 GB	Output/s	= 9.24 Mbps

Compression

Content Compression to Date

This statistic reports how much compression the jetNEXUS ALB-X has achieved on **compressible** content. A typical percentage for this lies between 60-80%.

Overall Compression to Date

This statistic reports how much compression the jetNEXUS ALB-X has achieved on **all** content. A typical percentage for this depends how many pre-compressed images are contained on your services. The more images the smaller the overall compression percentage is likely to be.

Compression Statistic

Content Compression to Date

Compression	= 0%
Throughput Before Compression	= 0
Throughput After Compression	= 0

Overall Compression to Date		**Current Values**
Compression	= 0%	= 0%
Throughput Before Compression	= 1.93 GB	= 7.32 Mbps (data)
Throughput After Compression	= 1.93 GB	= 7.32 Mbps (data)
Throughput From Cache	= 0	= 0.00 Mbps (data)
	Total	= 14.64 Mbps (data)

Hits and Connections

This section contains the overall statistics for hits and transactions.
Hit:
A hit is defined as a layer 7 transaction. Typically for web servers this is a GET for an object such as an image.

Connection:
A connection is defined as a layer 4 TCP connection. Many transactions can occur over 1 TCP connection.

Overall Hits Counted

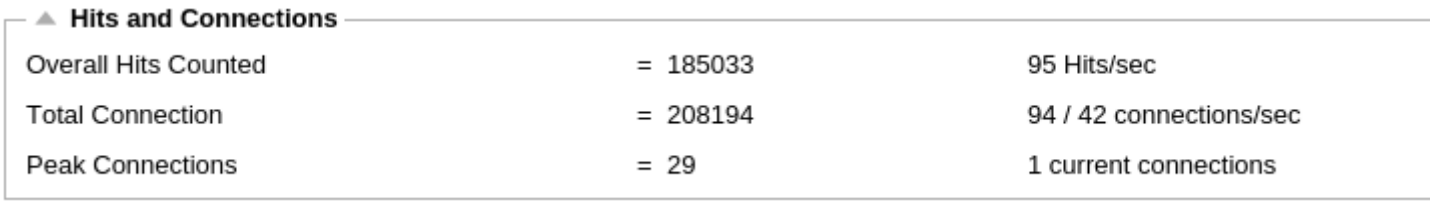
This is the cumulative number of non-cached hits since last reset. On the right hand side the figure will show the current number of hits per second.

Total Connections

This is the cumulative number of TCP connections since last reset. The first figure on the right hand side you can see the number of TCP connections per second to the ALB-X. The second number is the number of TCP connections per second to the content servers. Example 6/8 connections/sec – This means we have 6 TCP connections per second to the Virtual Service and 6 TCP connections per second to the real servers.

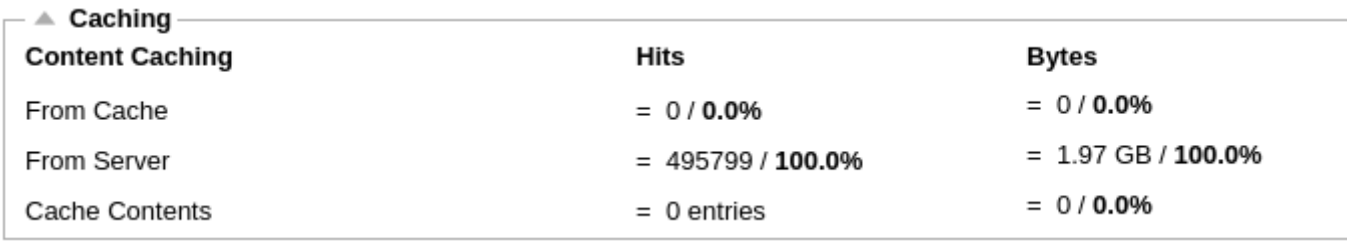
Peak Connections

This is the maximum number of TCP connections to the jetNEXUS ALB-X. The number on the right hand side gives the current number of active TCP connections.



Caching

This section will show the overall statistics in relation to caching when it has been applied to a channel. If caching has not been applied to a channel and configured correctly you will see 0 cache contents.



From Cache

Hits:
The first number gives the total number of transactions served from the jetNEXUS ALB-X cache since last reset. A percentage of total transactions is also provided.

Bytes:
The first number gives the total amount of data in Kilobytes served from the jetNEXUS ALB-X cache. A percentage of total data is also provided.

From Server

Hits:
The first number gives the total number of transactions served from the content servers since last reset. A percentage of total transactions is also provided.

Bytes:
The first number gives the total amount of data in Kilobytes served from the content servers. A percentage of total data is also provided.

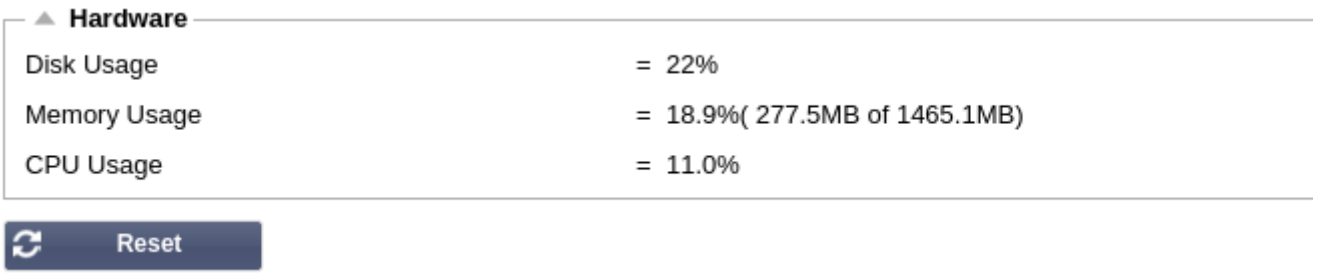
Cache Contents

Hits:
This number gives the total number of objects contained in the jetNEXUS ALB-X cache.

Bytes:
The first number gives the overall size in Megabytes of the jetNEXUS ALB-X cached objects. A percentage of the maximum cache size is also provided.

Hardware

This section provides the overall usage stats for the jetNEXUS ALB-X.



Disk Usage

This number gives the percentage of disk space currently used and includes such things as the log files and the cache which is periodically stored on the hard drive.

Memory Usage

This number gives the percentage of memory currently used. The larger number in brackets is the total amount of memory allocated to the ALB-X. It is recommended that this is a minimum of 2GB.

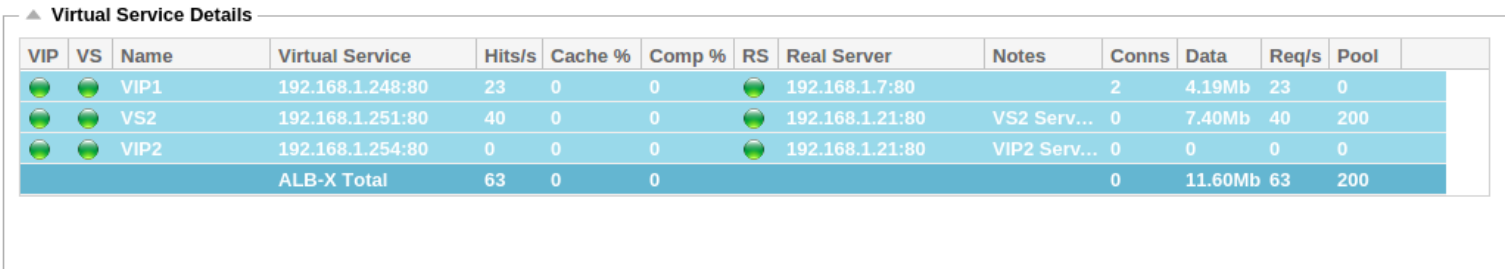
CPU Usage

This number gives the percentage of CPU currently used by jetNEXUS ALB-X. It is natural for this to fluctuate.

Status

The **View — Status** page displays the live traffic for your Virtual Services. It also shows the number of connections and data to each real server so you can see the load balancing in action.

Virtual Service Details



VIP Status:

The colour of the light indicates the state of the Virtual IP address associated with one or many virtual services.

- Online
- Failover-Standby. This virtual service is hot-standby
- Indicates a “passive” is holding off for an “active”
- Offline. Real servers are unreachable or no real servers are enabled
- Finding status
- Not licenced or licenced Virtual IPs exceeded

VS Status:

The colour of the light indicates the state of the Virtual Service:

- Online
- Failover-Standby This virtual service is hot-standby
- Indicates a “passive” is holding off for an “active”
- Service Needs attention. This may be the result of a real server failing a health monitor or has been changed manually to

Offline Traffic will continue to flow but with reduced real server capacity.

Offline. Real servers are unreachable or no real servers are enabled

Finding status

Not licenced or licenced Virtual IPs exceeded

Name:

Virtual Service name.

Virtual Service:

The virtual IP address and port for the service.

Hit/Sec:

Layer 7 transactions per second on the client side.

Cache%:

The percentage of objects that have been served from the ALB-X RAM Cache.

Compression%:

The percentage of objects that have been compressed between the client and ALB-X.

RS Status:

Connected

Not monitored

Draining

Offline

Standby

Not connected

Finding status

- Not licenced or licenced real servers exceeded

Real Server:

The real server IP address and port.

Notes:

Usually the name of the real server or helpful notes about the real server.

Conns:

The number of connections to each real server. Here you can see load balancing in action. Very helpful to verify that your load balancing policy is working correctly.

Data:

The amount of data being sent to each real server.

Req/Sec:

The number of requests per second sent to each real server.

Clustering

The **System — Clustering** page is the home of high availability for your jetNEXUS ALB-X. This page is organised into four sections

Notes on High Availability

- There is **no** requirement for a dedicated cable to maintain high availability heartbeat
- The heartbeat takes place on the same network as the **Virtual Service** that requires high availability
- There is **no** stateful fail-over between ALB-X appliances
- When high availability is enabled on two or more appliances each box will broadcast via UDP the **Virtual Services** it is configured to provide
- High availability fail-over uses unicast messaging and Gratuitous ARP to inform the switches of the new **Active** load balancer

Role

jetNEXUS ALB-X can be assigned into three separate roles with regards to high availability

Cluster Role

- By default a new ALB-X will power-on into the **Cluster** role. In this role each member of the cluster will have exactly the same “working configuration” and as such only one ALB-X in the **Cluster** will be **Active** at any one time
- A “working configuration” means all configuration except items that need to be unique such as the management IP address, ALB Name, network settings, interface details etc.
- The ALB-X in priority 1, top position, of the **Cluster Members** box is said to be the cluster **Owner** and is the **Active** load balancer, all other ALB-X’s are members and therefore **Passive**

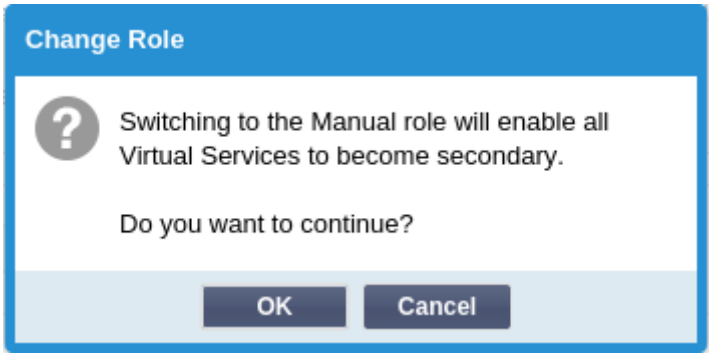
- You can edit any ALB-X in the **Cluster** and those changes will be synchronised to all members of the **Cluster**
- When you remove an ALB-X from the **Cluster,** all **Virtual Services** will be deleted from that ALB-X
- You cannot remove the last member of the **Cluster** to **Unclaimed Devices,** to remove the last member then please change roles to **Manual** or **Stand-alone**
- The following objects are not synchronised**:**
    - **Manual Date & Time section – (NTP Section is synchronised)**
    - **Failover Latency (ms)**
    - **Hardware section**
    - **Appliance section**
    - **Network section**

Failure of Cluster Owner

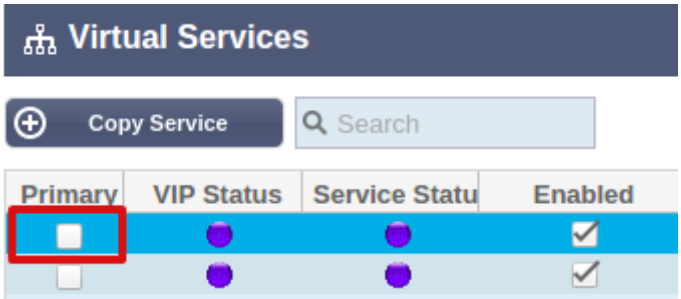
- When a cluster owner fails one of the remaining members will automatically load balancer traffic
- When the cluster owner returns it will resume load balancing traffic
- If you would like the member load balancing traffic to become the new owner simply highlight the member and click the up arrow so it moves to Priority 1 position
    - If you edit a remaining cluster member and the owner is down it will automatically promote itself to owner without loss of traffic

Changing role from Cluster to Manual

- If you wish to change from **Cluster** to **Manual** after you click on the radio button you will be prompted with the following message



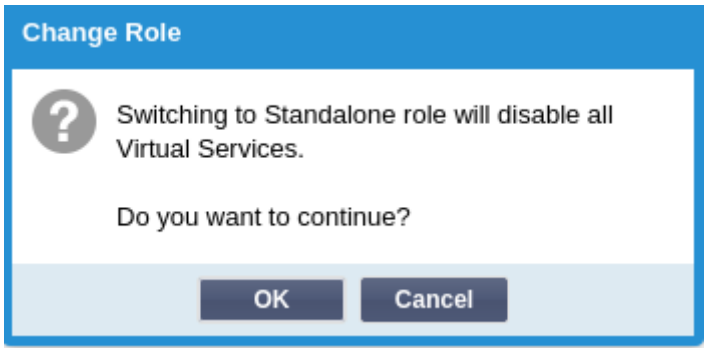
- Click **OK** to change roles
- Please then check your **Virtual Services** and you will see that the **Primary** column now shows an un-ticked box



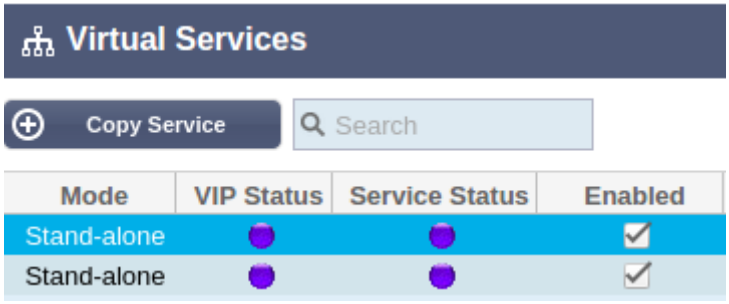
- This is a safety feature and means that if you have another ALB-X with the same **Virtual Services** then there will be no interruption to traffic flow

Changing role from Cluster to Stand-alone

- If you wish to change from **Cluster** to **Stand-alone,** after you click on the corresponding radio button you will be prompted with the following message



- Click **OK** to change roles
- Please then check your **Virtual Services** where you should see the **Primary** column change name to **Stand-alone**
- You should also see that all of the **Virtual Services** are disabled (un-ticked) for safety
- Once you are certain that no other ALB-X on the same network has duplicate **Virtual Services** you can enable each one in turn



Manual Role

An ALB-X in the **Manual** role will work with other ALB-X's in the **Manual** role to provide high availability. The main advantage over the **Cluster** role is the ability to set which ALB-X is **Active** for a particular Virtual IP. The disadvantage is that there is no configuration synchronisation between each ALB-X. Any changes must be replicated manually on each box via the GUI or for lots of changes you can create a jetPACK from one box and send this to another box.

- To make a Virtual IP address "Active" tick the check-box in the primary column (IP Services page)
- To make a Virtual IP address "Passive" leave the check-box blank in the primary column (IP Services page)
- In the event that an **Active** service fails over to the **Passive**:
    - If both Primary Columns are ticked then an election process takes place and the lowest MAC address will be **Active**
    - If both are un-ticked then the same election process takes place. In addition if both are un-ticked there is no automatic fail-back to the original **Active** ALB-X

Stand-Alone Role

An ALB-X in the **Stand-alone** role will not communicate with another ALB-X about its services and therefore all Virtual Services will remain status Green and connected. You must ensure that all Virtual Services have unique IP addresses or there will be a clash on your network.

Settings

In this section you can set the **Failover Latency** in milliseconds that a **Passive** ALB-X will wait before taking over the **Virtual Services** after the **Active** ALB-X has failed.

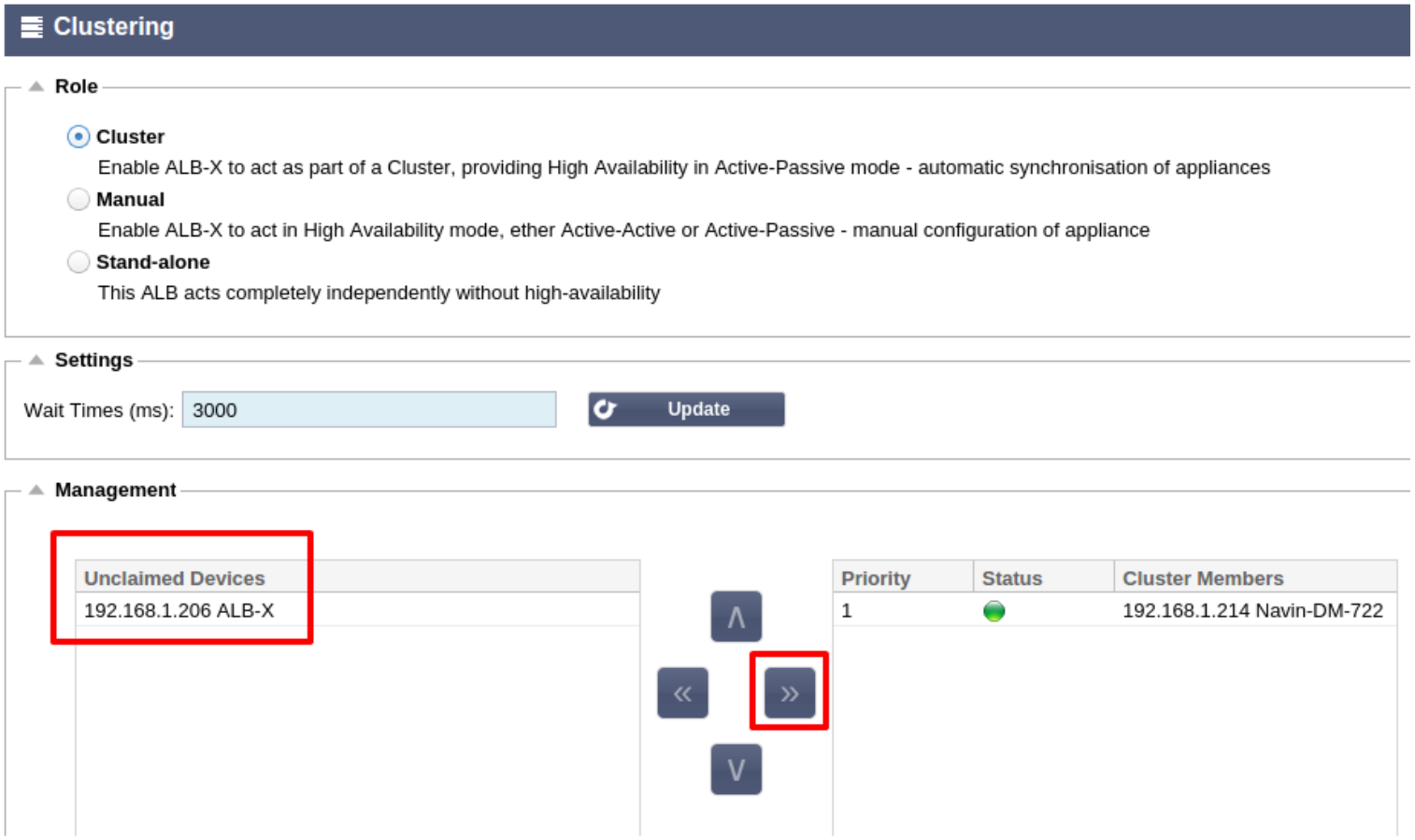
We recommend setting this to 10000ms or 10 seconds but you may decrease or increase this value to suit your network. Acceptable values fall between 1500ms and 20000ms. If you experience instability in the cluster at a lower latency please increase this value.

Management

In this section you can add and remove cluster members. You can also change the priority of an ALB-X in the cluster

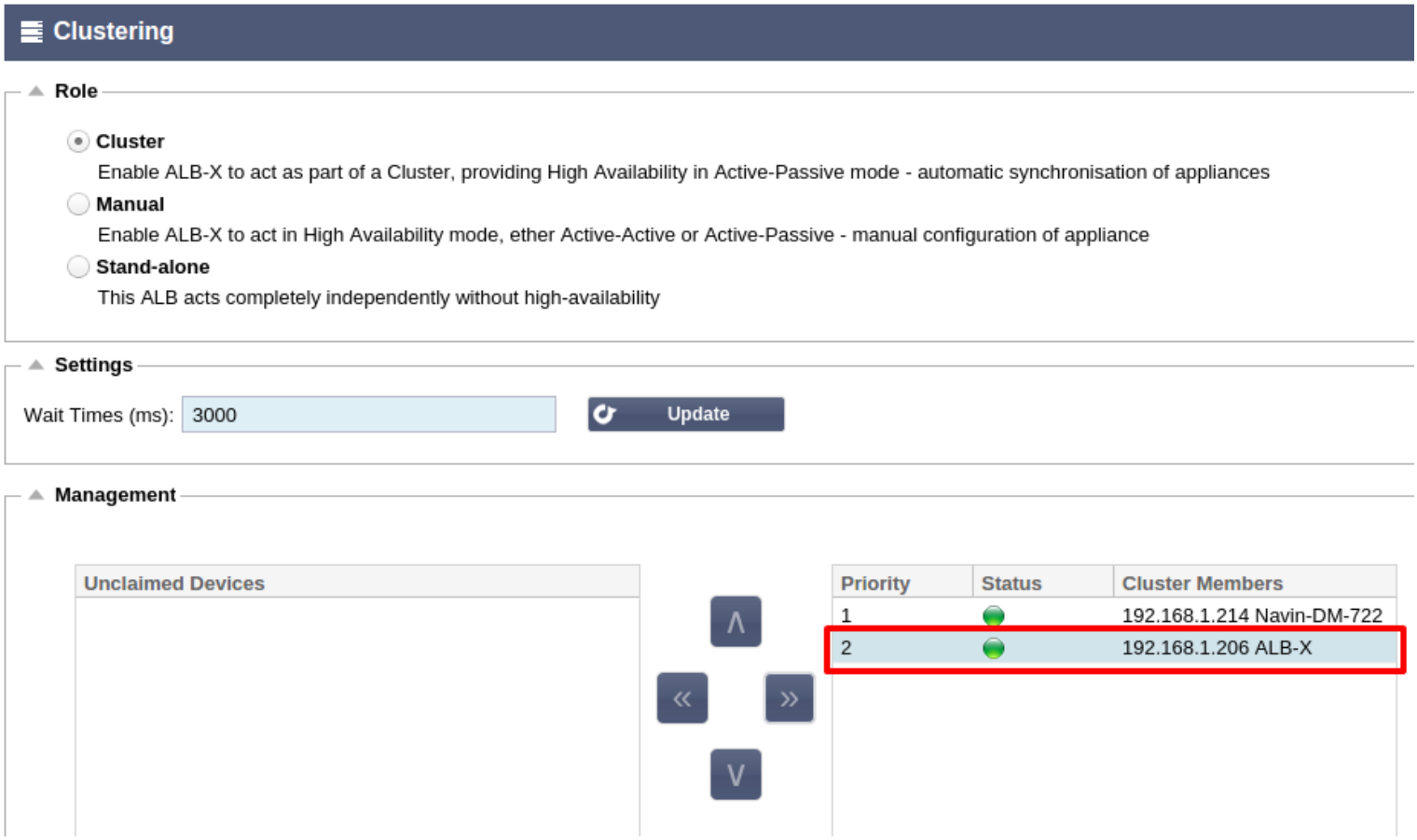
Add another ALB-X to the cluster

- Before adding an ALB-X to the cluster ensure that all ALB-X have the desired name which can be set in the appliance section
- In the management section you should see your ALB-X as **Priority 1** with **Status** green and its name under the **Cluster Members** column
- All available ALB-X will show up in the **Unclaimed Devices** window within the management section. An **Unclaimed Device** is an ALB-X that has been assigned in the **Cluster Role** but has no **Virtual Services** configured
- Highlight an ALB-X from the left hand **Unclaimed Devices** box and click the right arrow



- Click **OK** to promote your ALB-X to be a member of the cluster

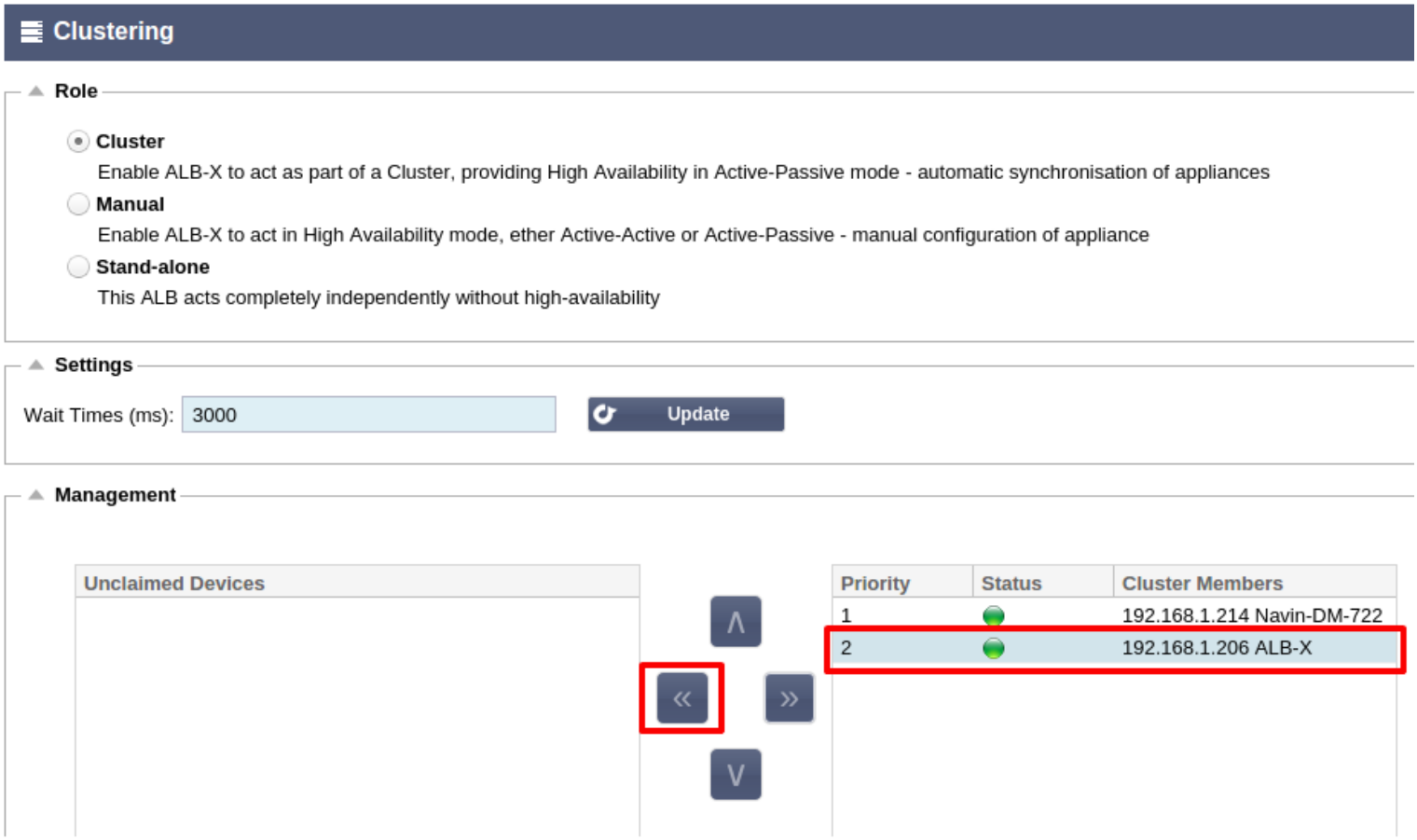
- Your ALB-X should now show as **Priority 2** in the cluster members list



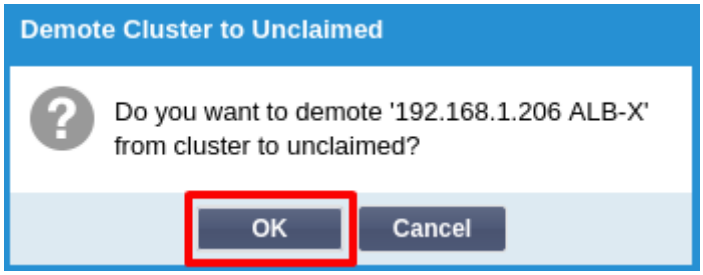
- You can now view the IP Services page on the second box and see the **Virtual Services** have been replicated and the configuration has been synchronised

Removing a Cluster Member

- Highlight the Cluster Member you wish to remove from the cluster
- Click the left arrow



- You will be presented with a confirmation message



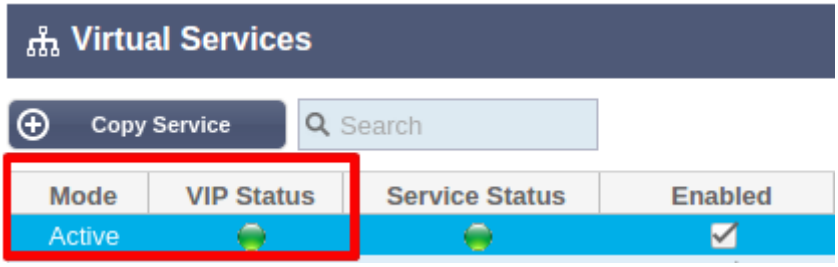
- Click **OK** to confirm
- The ALB-X that has been removed will now show up as an **Unclaimed Device** on the remaining cluster member(s)

- You should see on the removed cluster member that it is now the only cluster member

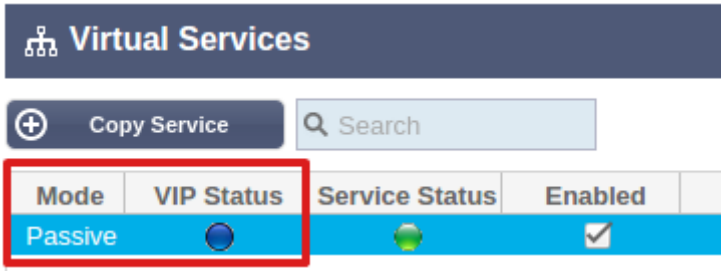
- Please check the **Virtual Services** have been deleted on the removed cluster member

Changing the priority of an ALB-X

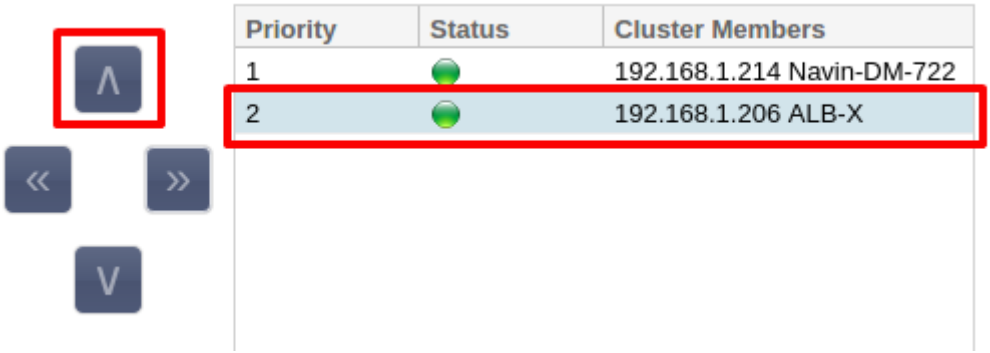
- The ALB-X at the top of the **Cluster Members** list is given **Priority 1** and is the **Active** ALB-X for all **Virtual Services**



- The ALB-X that is second in the list is given **Priority 2** and is the **Passive** ALB-X for all **Virtual Services**



- To change which ALB-X is Active simply highlight your ALB-X and click the up arrow until it is at the top of the list



Date & Time

The **System — Date & Time** page allows you to manually set the Date and Time on your jetNEXUS ALB-X. You can also configure a network time server to synchronise the time on your appliance. The page is organised into the two sections below.

Date & Time

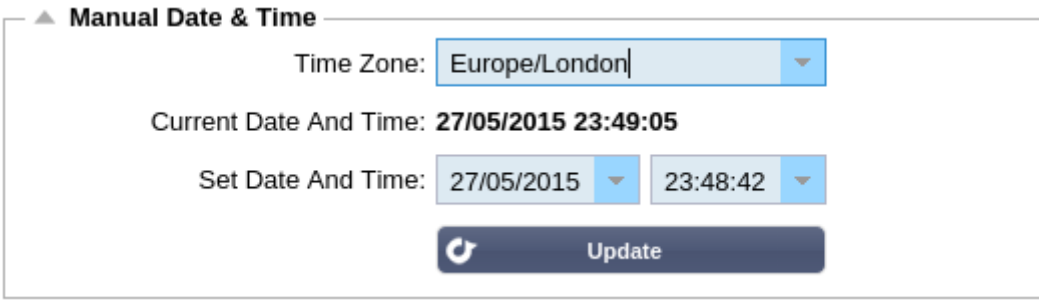
In this section you can view the current Date and Time. This is usually set for Universal Time Zone or UTC but you may change this to your local time zone.

Time Zone:

- Click on the drop down box for the Time Zone and start typing your location.
- Example London
- Start typing L – All location containing the letter L will be displayed
- Continue typing Lon – the above locations will be narrowed down to around 4 locations
- Choose Europe/London to set your location

Set Date and Time: If the Date and Time is still incorrect after the above change please change the date manually

- Choose the correct date from the first drop down or alternatively you can type the date in the following format DD/MM/YYYY
- Add in the time in the following format hh:mm:ss
- Once you have set this please click Update to apply.
- You should then see the new Date and Time in bold



Time Server

In this section you can configure a time server to keep the jetNEXUS ALB-X synchronised. Network Time Protocol (NTP) is a networking protocol for clock synchronisation between computer systems over variable-latency networks.

Time Server URL:

Choose the IP address or fully qualified domain name or the NTP server.

Update at [hh:mm]

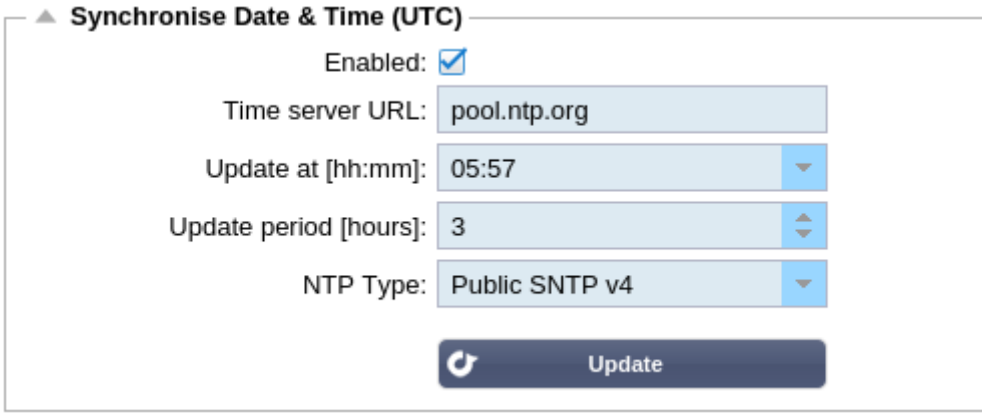
Select the time that you would like to first access the time server to synchronise.

Update Period [hours]:

Select how often you would like synchronisation to occur.

NTP Type:

Public SNTP V4 – This is the current and preferred method when synchronising with an NTP server. RFC 5905 NTP v1 Over TCP – Legacy NTP version over TCP. RFC 1059 NTP v1 Over UDP – Legacy NTP version over UDP. RFC 1059



The example above would synchronise every hour at 7 minutes past the hour with pool.ntp.org. Please not that synchronisation is in UTC only. If you wish to set local time this can only be done manually. This will be changed in later versions to enable the ability to select a time zone.

Email Events

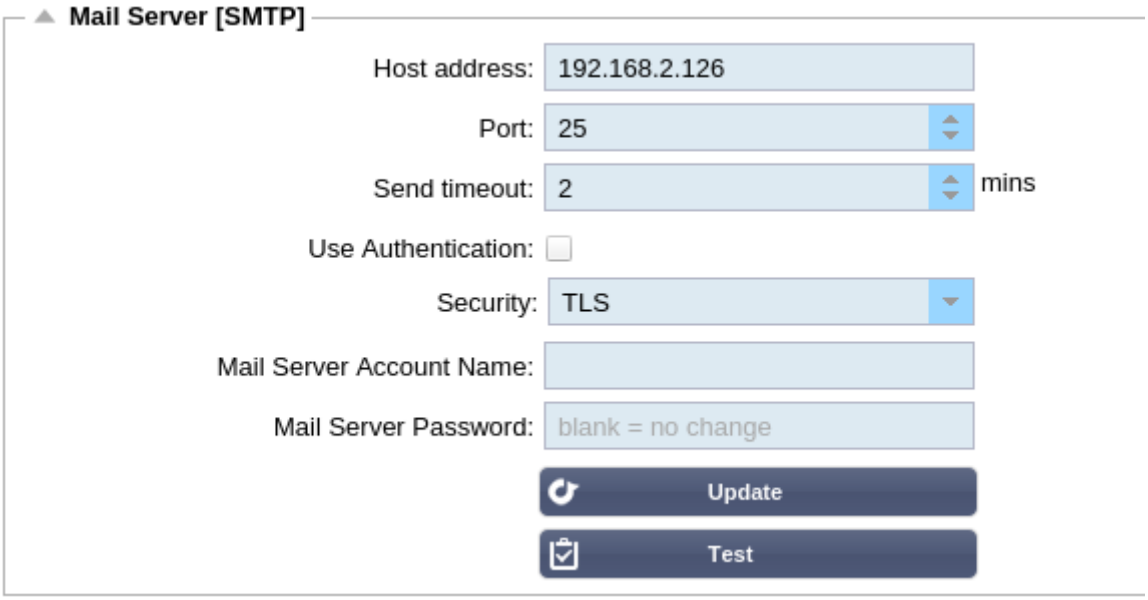
The **System — Email Events** page allows you to configure an email server and send notifications about your jetNEXUS ALB-X. The page is organised into the sections below.

Email Address

Send to Email Address:
Add in a valid email address to send the alerts, notifications and events to. Example support@domain.com.
Return Email Address:
Add in an email address that will appear in the inbox. Example ALB1@domain.com.

Mail Sever [SMTP]

Here you can add in the details of the SMTP server to be used to send the emails.
Host address:
Add in the IP address of your SMTP server.
Port:
Add in the Port of your SMTP server. Default Port for SMTP is 25.
Send Timeout:
Add in an SMTP timeout. The default is set to 2 minutes.
Use Authentication:
Tick the box if your SMTP server requires authentication.
Security:
None:
Default setting is none.
SSL:
Use this setting if your SMTP server requires Secure Sockets Layer authentication.
TLS:
Use this setting if your SMTP server requires Transport Layer Security authentication.
Main Server Account Name:
Add in the username required for authentication.
Mail Server Password:
Add in the password required for authentication.



Notifications and Alerts

Tick the various boxes to enable notifications and events. Notifications occur when servers are contacted or channels are started. Alerts occur when Servers cannot be contacted or channels stop.

IP Service:
This will inform you when a Virtual IP address is online or stopped. This will include all Virtual Services that belong to that Virtual IP

Virtual Service:
This will inform you when a particular Virtual Service is online or stopped.

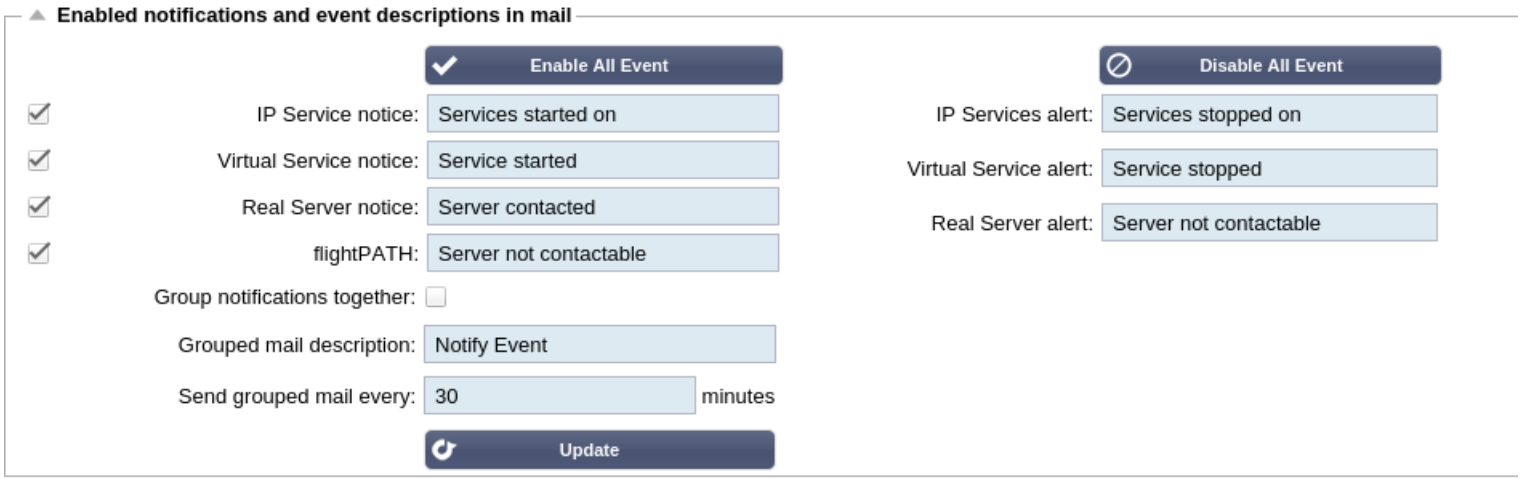
Real Server:
This will inform you when a Real Sever and Port is connected or not contactable.

flightPATH
This will email when a condition has been met and the action instructs to email the event**.**

Group Notifications:
Tick to group notifications together. With this ticked all of the notifications and alerts will be aggregated into one email.

Group Mail Description:
Add in a relevant subject name.

Group Send interval:
Stipulate the amount of time you wish to wait before sending one group email. Minimum time is 2 minutes.



Warnings

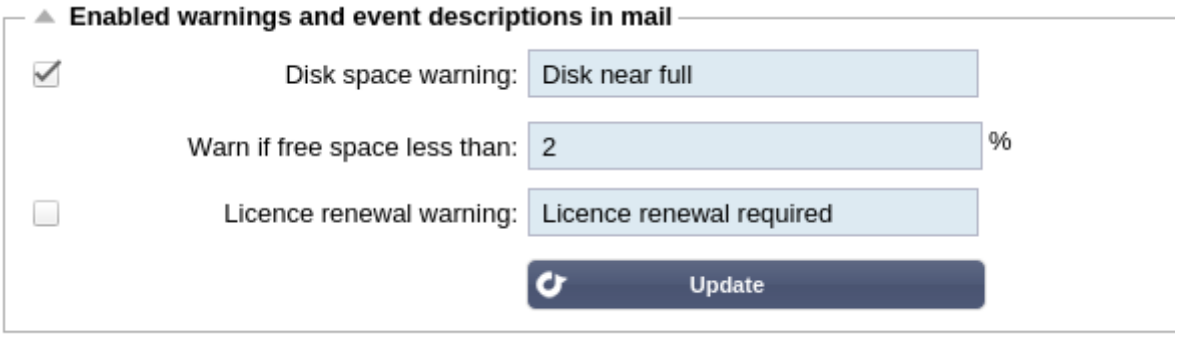
There are two warning emails.

Disk Space:

Set the percentage of free disk space. When this is reached you will be emailed.

Licence Expiry:

The default time remaining before your temporary licence will expire is 7 days. When this is reached you will be emailed.

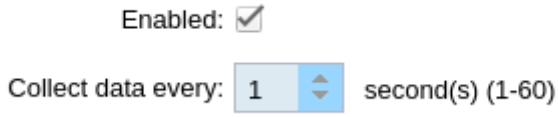


System History

The **System — History** page allows you enable historical data logging for such things as **CPU, Used Memory, Requests per Second** and so on**.** Once you have enabled this you can view the results in graphical form via the **View — History** page. This page will also allow you to backup or restore your history files to the local ALB-X.

Enable Historical logging

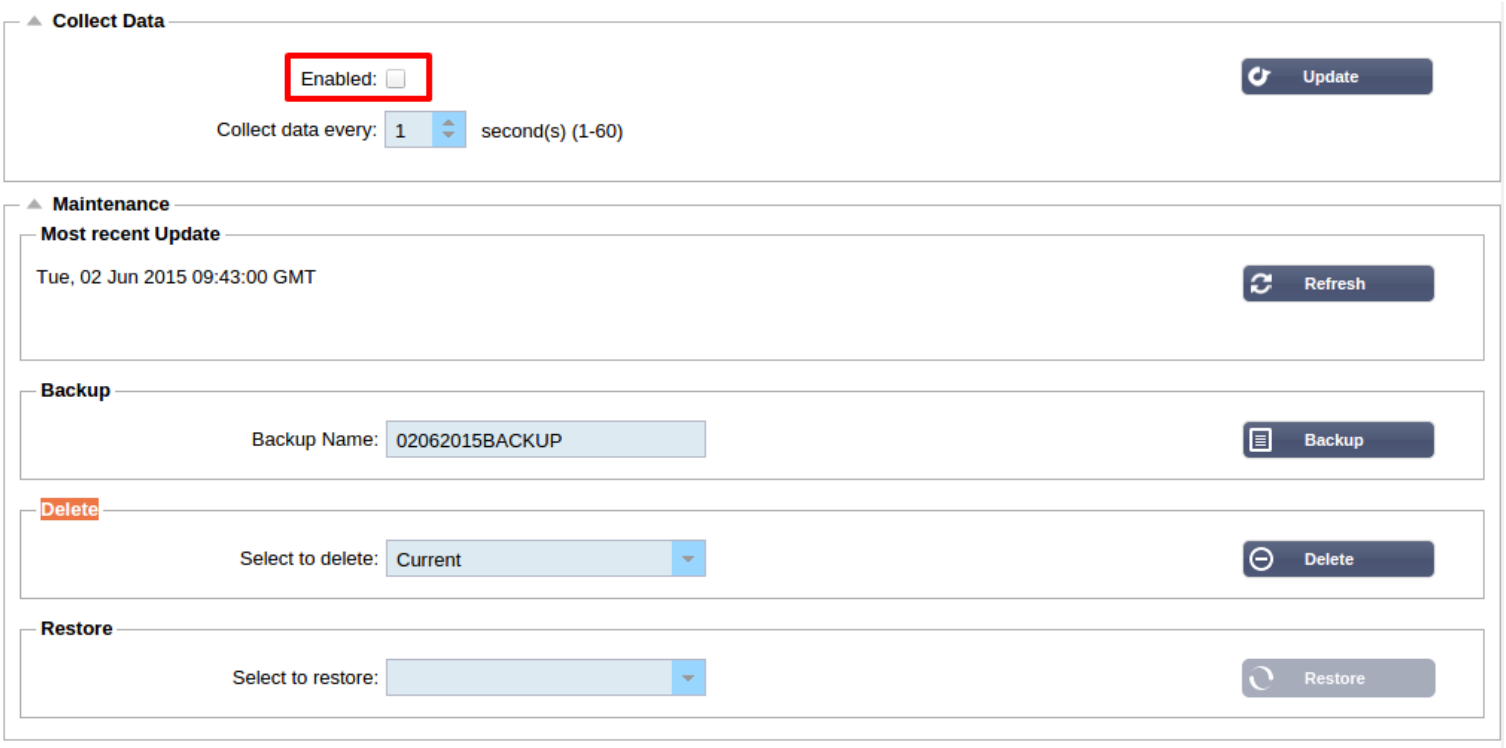
1. Tick the box at the top of the page to enable historical logging.



2. Choose the interval at which data will be logged. This value should be between 1s and 60s
3. Click Update to save these settings
4. Go to View-History to create the graphs from these data points

Maintenance

This section will be greyed out if you have enabled historical logging. To allow the maintenance of the historical logs please untick the Enabled Box and click Update.



Backup

Give your backup a descriptive name. Click **Backup** to store all files to the jetNEXUS ALB-X

Delete

Select a backup file from the drop down list. Click **Delete** to remove the backup file from your ALB-X

Restore

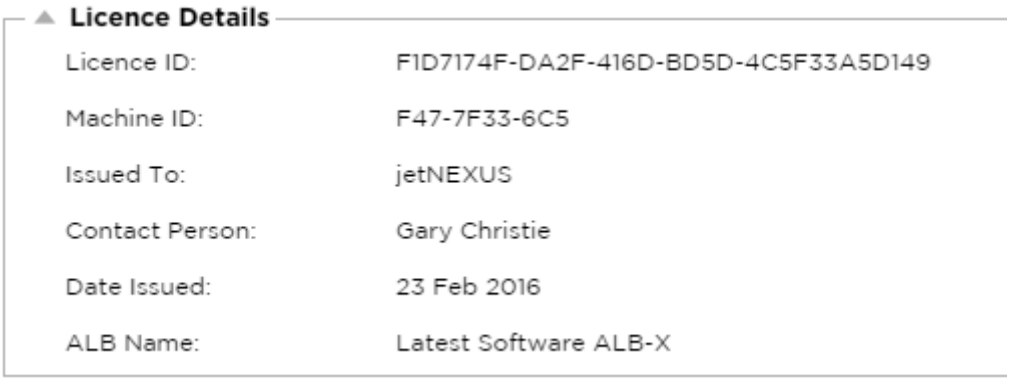
Select a previously stored backup file. Click **Restore** to populate the data from this backup file

Licence

The **System — Licence** page shows the facilities you are able to use. It also provides you with the ability to install a licence. The page is split into three sections.

Licence Details

Licence ID:
Unique licence ID stored against this machine and customer in our licence database.
Machine ID:
created from the IP address of eth0 for your Virtual Appliance and the MAC address of eth0 for a hardware appliance. Should you change the IP address of eth0 for a Virtual Appliance you licence will become invalid and you will need to contact support@edgenexus.io.
Issue To:
Company name associated with this machine ID.
Contact Person:
Administrative contact for this machine ID.
Date Issued:
Date the licence was issued.
ALB Name:
Descriptive name for the ALB-X.



Facilities

ALB:
The core functionality of the ALB-X. This can be “Permanent” or contain a number to indicate how many days the facility has remaining. This facility will only be displayed if you have a licence issue before version 4.2.0.
Layer 4:
Licence your ALB for Layer 4 services
Layer 7:
Licence your ALB for Layer 7 services
SSL:
The ability to decrypt/encrypt traffic. This can be “Permanent” or contain a number to indicate how many days the facility has

remaining.

Cache:

The ability to use the jetNEXUS intelligent caching engine for web traffic. This can be “Permanent” or contain a number to indicate how many days the facility has remaining.

flightPATH:

The ability to use the jetNEXUS intelligent traffic manipulation engine. This can be “Permanent” or contain a number to indicate how many days the facility has remaining.

Interfaces:

The maximum number of Virtual IP addresses. This can be “Permanent” or contain a number to indicate how many days the facility has remaining.

Real Servers:

The maximum number of real server IP addresses. This can be “Permanent” or contain a number to indicate how many days the facility has remaining.

Example:

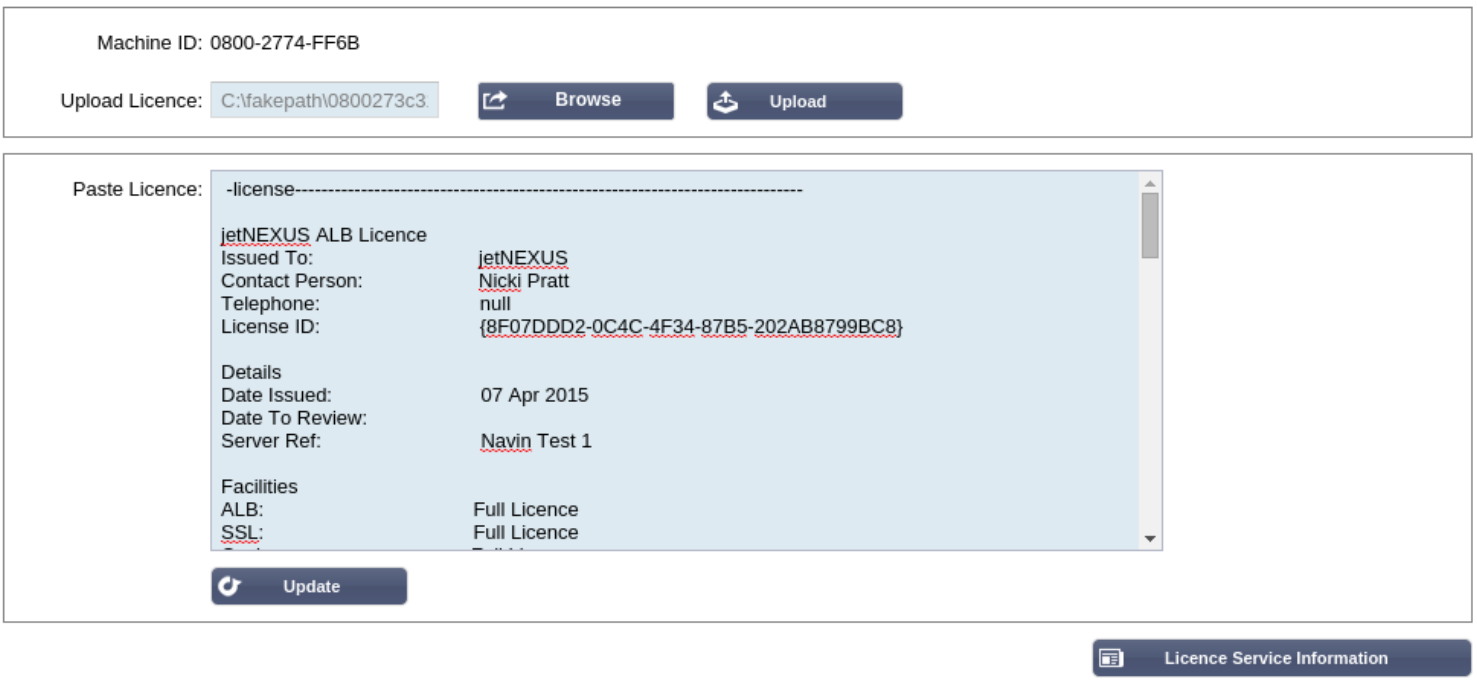
Install Licence

Machine ID:
The machine ID is needed to create your licence certificate. The machine ID is tied to the MAC address of Eth0 for a physical appliance. The Machine ID is tied to the IP address if Eth0 for a virtual appliance. Note, if you change the IP address of Eth0 on a virtual appliance the existing licence will be invalid and your services will stop working. You will still be able to access the web console on https://x.x.x.x:27376.

Upload Certificate:
Once you receive your licence from support@edgenexus.io you can **Browse** for the file. Click **Upload** to apply. You should then see your facilities have updated, please check they are correct. Note you will only be able to upload a licence with the correct Machine ID.

Paste Licence: From software version 4.1.1 you can now paste your licence.

1. Open up your licence in a text editor
2. Copy everything
3. Paste into the box
4. Click update to apply
5. The status bar along the bottom should go Green informing you that the licence is uploading
6. In some circumstances you might need to restart the ALB-X to apply



Licence Support Information

This page contains vital information that will help the jetNEXUS support team in assisting you if you have an issue. Please click on the

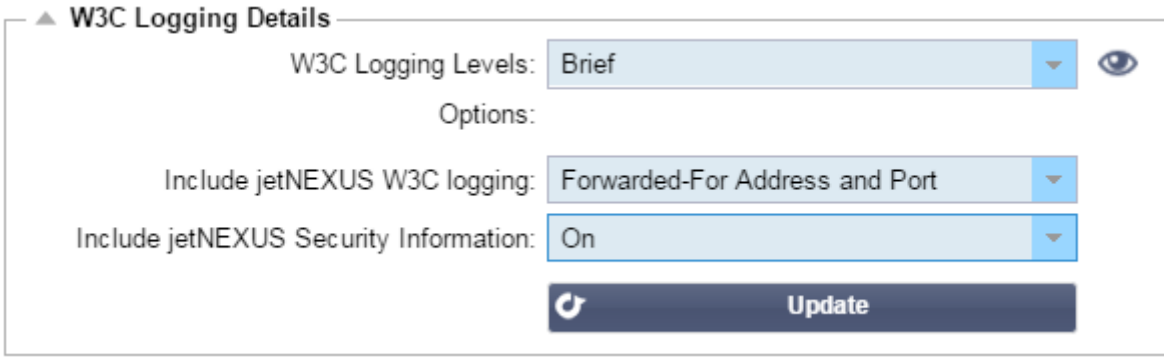
to retrieve your Support information similar to below. You can then send these details with the button on the bottom right hand side

System Logging

The **System — Logging** page allows you to set the **W3C logging levels** and specify the remote server export the logs automatically. The page is organised into the four sections below.

W3C Logging Details

Enabling W3C logging mode will start jetNEXUS ALB-X recording a W3C compatible log file. A W3C log is an access log for Web servers in which text files are generated containing data about each access request, including the source Internet Protocol (IP) address, the HTTP version, the browser type, the referrer page, and the time stamp. The format was developed by the World Wide Web Consortium (W3C), an organization that promotes standards for the evolution of the Web. The file is in ASCII text, with space-delimited columns. The file holds comment lines beginning with the # character. One of these comment lines is a line naming field (providing column names) so that data can be mined. There are separate files for HTTP and FTP protocols.



HTTP W3C Logging:

None:
W3C logging is off.
Brief:
The fields present are:
#Fields: time c-ip c-port s-ip method uri x-c-version x-r-version sc-status cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round-trip-time cs(User-Agent) x-sc(Content-Type).
Full:
This is a more processor-compatible format with separate date and time fields. See the fields summary below for information on what the fields mean. The fields present are: #Fields: date time c-ip c-port cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round-trip-time x-sc(Content-Type).
Site:
This format is very similar to “Full” but has an additional field. See the fields summary below for information on what the fields mean. The fields present are: #Fields: date time x-mil c-ip c-port cs-username s-ip s-port cs-host cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round-trip-time x-sc(Content-Type).
Diagnostic:
This format is filled with all sorts of information relevant to development and support staff. See the fields summary below for information on what the fields mean. The fields present are: #Fields: date time c-ip c-port cs-username s-ip s-port x-xff x-

xffcustom cs-host x-r-ip x-r-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round-trip-time x-trip-times(new,rcon,rqf,rql,tqf,tql,rsf,rsl,tsf,tsl,dis,log) x-closed-by x-compress-action x-sc(Content-Type) x-cache-action X-finish

FTP W3C Logging:

Brief:
#Fields: date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param sc-status sc-param sr-method sr-param rs-status rs-param
Full:
#Fields: date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param cs-bytes sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes
Diagnostic:
#Fields: date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param cs-bytes sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes

edgeNEXUS w3c Logging:

Client's Network Address and Port:
This will show the true client IP address along with the port.
Client's Network Address:
This will show the true client IP address only.
Forwarded-For Address and Port:
This will show the details held in the XFF header including the address and port.
Forwarded-For Address:
This will show the details held in the XFF header including the address only.

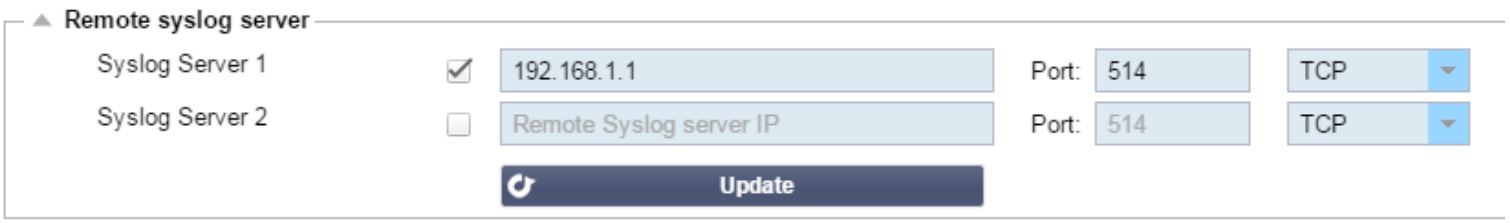
Include edgeNEXUS Security Information:

On:
This is a global setting. When this is set to on this will allow any virtual service that also has this setting turned on and is using Authentication to append the username to the W3C log.
Off:
This will turn off the ability to log the username to the W3C log on a global scale.

Remote Syslog Server

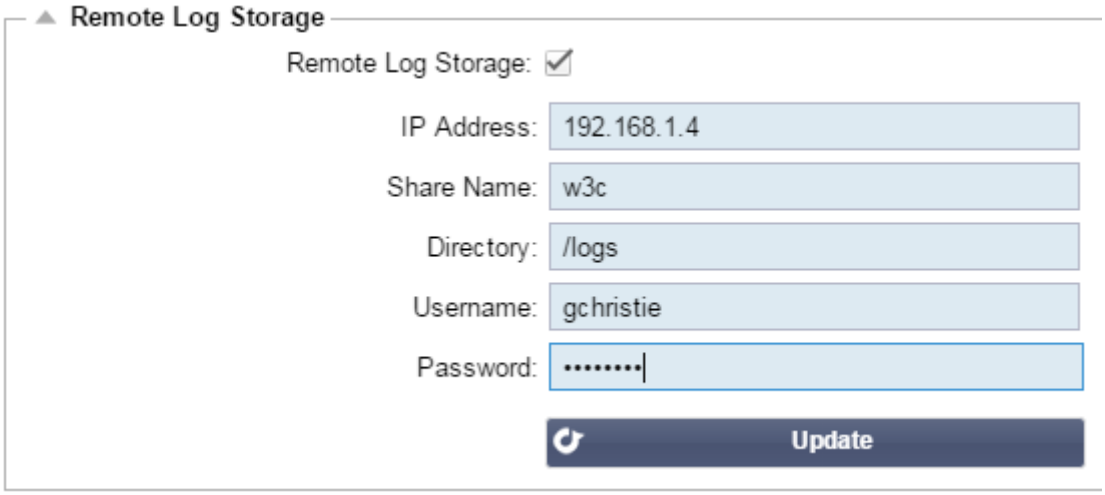
In this section you can configure two external syslog servers to send all system logs.

- Add the **IP** address of your syslog server
- Add the **Port**
- Choose **TCP** or **UDP**
- Tick the box
- Click **Update**



Remote W3C Log Storage

All W3C logs are stored compressed on the jetNEXUS ALB-X every hour. The oldest files will only be deleted when 30% of disk space is remaining. Should you wish to export these to a remote server for safekeeping you can configure that below using an SMB share. Please note that the W3C log will not transfer to the remote location until after the file has been completed and compressed. As the logs are written every hour this could take up to 2 hours for a Virtual Machine and will be 5 hours behind for a hardware appliance. We will include a test button in future releases to provide some feedback that your settings are correct.



Remote Log Storage:
Tick the box to enable remote log storage.

IP Address:
Add in the IP address of your SMB server. This should be in dotted decimal notation. Example: 10.1.1.23

Share Name:
Add in the share name on the SMB server. Example: w3c.

Directory:
Add in the directory on the SMB server. Example: /log.

Username:
Add in the username for the SMB share.

Password:
Add in the password for the SMB share.

Field Summary

HTTP

Condition	Description
Date	Not localised = always YYYY-MM-DD (GMT/UTC)
Time	Not localised = HH:MM:SS or HH:MM:SS.ZZZ (GMT/UTC) * Note-unfortunately this has two formats (Site has no .ZZZ milliseconds)
x-mil	Site format only = millisecond of time-stamp
c-ip	Client IP as best can be derived from network or X-Forwarded-For header
c-port	Client port as best can be derived from network or X-Forwarded-For header
cs-username	Client's user-name request field
s-ip	ALB's listening port
s-port	ALB's listening VIP
x-xff	Value of X-Forwarded-For header
x-xffcustom	Value of configured-named X-Forwarded-For type request header
cs-host	Host name in the request
x-r-ip	IP address of content server used
x-r-port	Port of content server used
cs-method	HTTP request method * except Brief format
method	* Only brief format uses this name for cs-method
cs-uri-stem	Path of the requested resource * except Brief format
cs-uri-query	Query for the requested resource * except Brief format
uri	* brief format logs a combined path and query-string
sc-status	HTTP response code
cs(User-Agent)	Browser's User-Agent string (as sent by client)
referer	Referring page (as sent by client)
x-c-version	Client's request HTTP version
x-r-version	Content-Server's response HTTP version
cs-bytes	Bytes from client, in the request
sr-bytes	Bytes forwarded to content server, in the request
rs-bytes	Bytes from real-server, in the response
sc-bytes	Bytes sent to client, in the response
x-percent	Compression percentage * = 100 * (1 – output / input) including headers
time-taken	How long the real-server took in seconds
x-trip-times	
new	millisecond from connect to posting in "newbie list"
pcon	millisecond from connect to placing the connection to the real-server
acon	millisecond from connect to finishing placing the connection to the real-server
rcon	millisecond from connect to establishing real-server connection
rqf	millisecond from connect to receiving the first byte of request from the client
rql	millisecond from connect to receiving the last byte of request from the client
tqf	millisecond from connect to sending the first byte of request to the real-server
tql	millisecond from connect to sending the last byte of request to the real-server
rsf	millisecond from connect to receiving the first byte of response from the real-server
rsl	millisecond from connect to receiving the last byte of response from the real-server

tsf	millisecond from connect to sending the first byte of response to the client
tsl	millisecond from connect to sending the last byte of response to the client
dis	millisecond from connect to disconnect (both sides – last one to disconnect)
log	millisecond from connect to this log record usually followed by (Load-balance policy and reasoning)
x-round-trip-time	How long ALB took in seconds
x-closed-by	What action caused the connection to be closed (or kept open)
x-compress-action	How compression was carried out, or prevented
x-sc(Content-Type)	Content-Type of response
x-cache-action	How caching responded, or was prevented
x-finish	Trigger that caused this log row

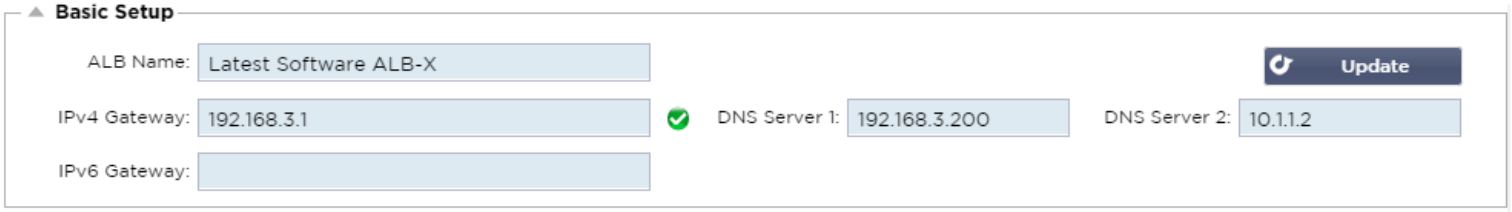
Clear Log Files

- Choose the log file you wish to clear
- Log Type
  - W3C log
  - System log
  - ACC – Access log
  - APP – Apps log
  - ADD – Add-Ons log
  - STT – System State log
- Click **Clear**

Network

The **Library—>Network** configuration page allows you to view and update the routing information on the jetNEXUS ALB-X. The settings are organised in the following sections:

Basic Setup

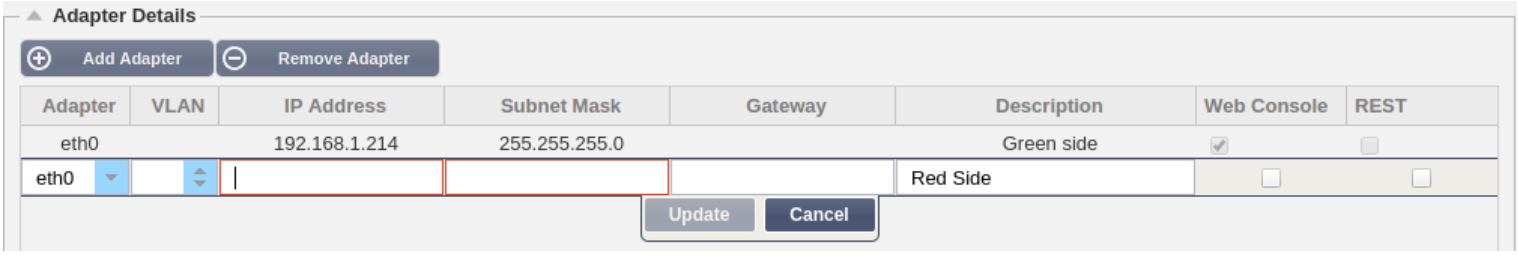


Basic Setup:

ALB Name:
Add in a name for your jetNEXUS ALB-X appliance. Please note that this cannot be changed if there is more than 1 member in the Cluster. Please see Clustering
IPv4 Gateway:
Add in the IPv4 Gateway address. This will need to be in the same subnet as an existing adapter. If you add in Gateway incorrectly you will see a White Cross in a red circle. When you add in a correct gateway you will see a green success banner at the bottom of the page and a white tick in a green circle next to the IP address.
IPv6 Gateway:
Add in the IPv6 Gateway address. This will need to be in the same subnet as an existing adapter. If you add in Gateway incorrectly you will see a White Cross in a red circle. When you add in a correct gateway you will see a green success banner at the bottom of the page and a white tick in a green circle next to the IP address.
DNS Server 1:
Add in the IPv4 address of your first DNS server.
DNS Server 2:
Add in the IPv4 address of your second DNS server

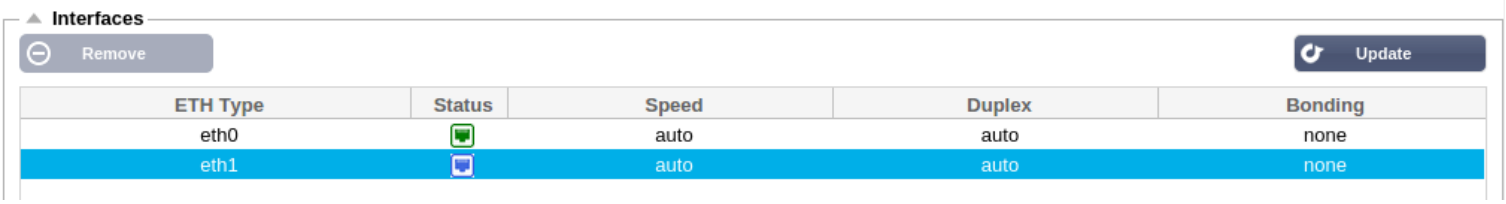
Adapter Details

Here you can add, remove and update the adapter settings.



Adapter:
Double click to see the physical adapters installed on your appliance. Choose an adapter from the list
VLAN:
Double click to add the VLAN ID for the adapter. A VLAN is a Virtual Local Area Network which creates a distinct broadcast domain. A VLAN has the same attributes as physical LAN but it allows for end stations to be grouped together more easily if they are not on the same network switch
IP Address:
Double click to add the IP address associated with the adapter interface. You can add multiple IP addresses to the same interface. This should be an IPv4 32-bit number in quad dotted decimal notation. Example: 192.168.101.2
Subnet Mask:
Double click to add the subnet mask assigned to the adapter interface. This should be an IPv4 32-bit number in quad dotted decimal notation. Example: 255.255.255.0
Gateway:
Add a gateway for the interface. When this is added the ALB-X will set-up a simple policy that will allow connections initiated from this interface to be returned via this interface to the gateway router specified. This allows the ALB-X to be installed in more complex networking environments without the hassle of manually configuring complex policy based routing.
Description:
Double click to add a description for your adapter. Example: Public Interface. Note: The ALB-X will automatically name the first interface **Green Side**, the second interface **Red Side** and the third interface **Side 3** etc. Please feel free to change these naming conventions to your own choice.
Web Console:
Double click the column then tick the box to assign the interface as the management address for the Graphical User Interface Web Console. Please be very careful when changing the interface that Web Console will listen on. You will need to have the correct routing set up or be in the same subnet as the new interface in order to reach the Web Console after the change. The only way to change this back is to access the command line and issue the **set greenside** command. This will delete all interfaces except for eth0.

Interfaces



- The settings on this screen control the network access. The defaults are to fix speed at 100 Mbps and full duplex. This avoids any issue with certain networking devices that have auto-negotiation which re-negotiates too frequently.

- The appliance can support speeds from 10 to 1000; for 1000 this should set to auto/auto. If this does not work, set the exact network hardware values.
- The speed and duplex setting should only be changed for hardware appliance.
    - Virtual appliances will take their configuration from the underlying hypervisor.
- In this section you can add and remove interfaces to a Bond once the bond has been configured in the section below.

Bonding

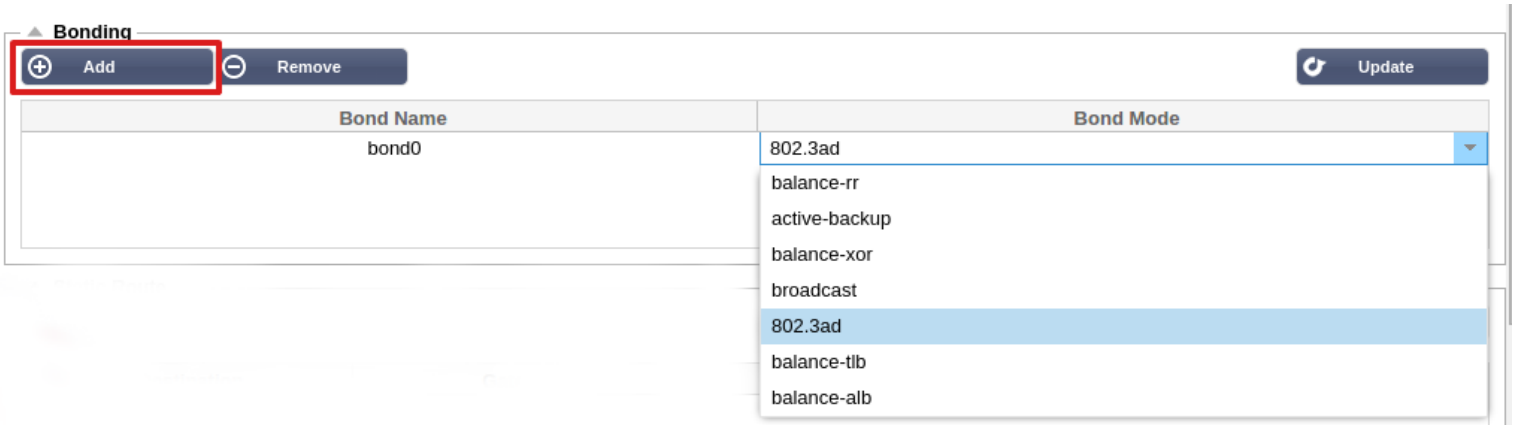
Bonding allows you to aggregate multiple ports into a single group, effectively combining the bandwidth into a single connection. Bonding also allows you to create multi-gigabit pipes to transport traffic through the highest traffic areas of your network. Note: this is only relevant for your hardware version of ALB-X. Do not use bonding for the Virtual Appliance.

Bonding Modes

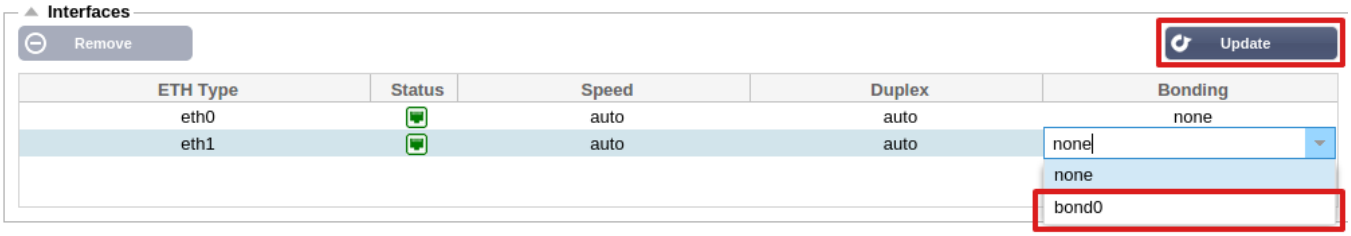
balance-rr:
Transmits packets in sequential order from the first available slave to the last.
active-backup:
Has one interface which will be active and the second interface will be in standby. This secondary interface only becomes active if the active connection on the first interface fails.
balance-xor:
Transmits based on source MAC address XOR'd with destination MAC address. This selects the same slave for each destination Mac address.
broadcast:
Transmits everything on all slave interfaces.
802.3ad:
Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification.
balance-tlb:
The Adaptive transmit load balancing bonding mode: Provides channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.
balance-alb:
The Adaptive load balancing bonding mode: also includes balance-tlb plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond, such that different peers use different hardware addresses for the server.

Configure Bonding

- Click on **Add** button on the bonding section and choose which bonding mode you wish to use



- Assign which interfaces are to be bonded in the interface section. In the example below eth0, eth1 and eth2 are now part of bond0. Whilst Eth0 remains on its own as the management interface



Adapter Status

Adapter Up

Adapter Down

Adapter Unplugged

Adapter missing

IP Addressing

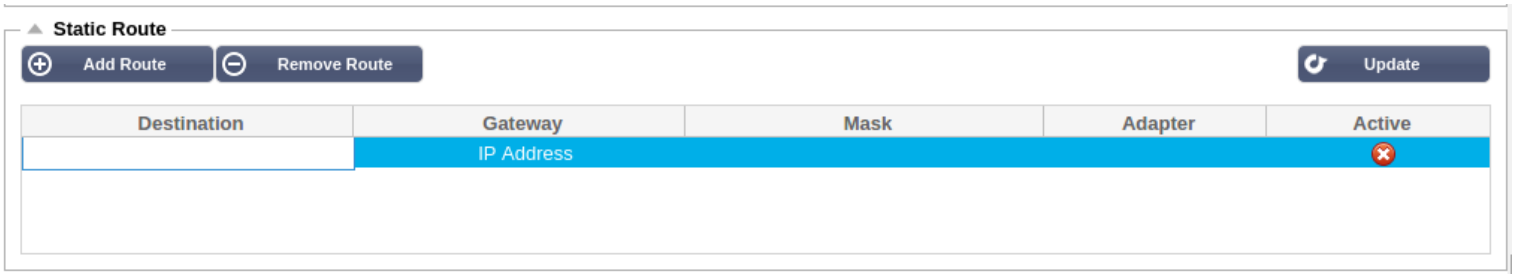
Now that you have added your bond you can go to the Adapter Details section to add the IP address and policy routing details

Static Route

You can manually add routes for specific subnets in this section.

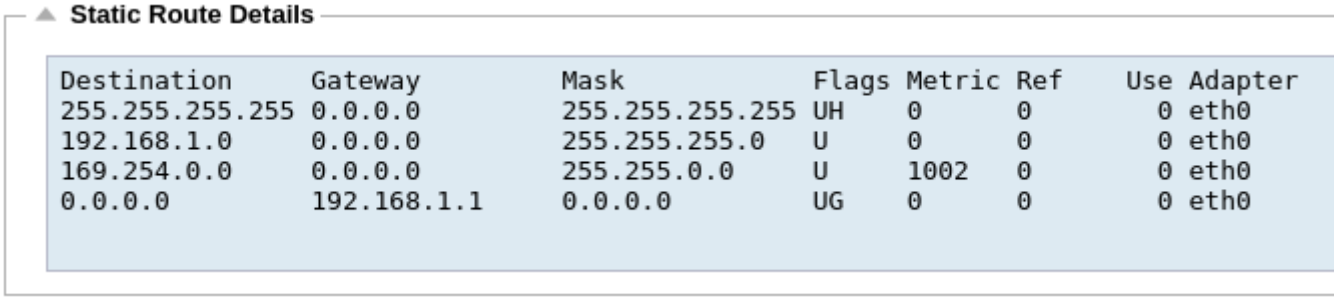
Destination:
Enter the destination network address in decimal dotted notation. Example 123.123.123.5

Gateway:
Enter the gateway IPv4 address in decimal dotted notation. Example 10.4.8.1
Mask:
Enter the destination subnet mask in decimal dotted notation. Example 255.255.255.0
Adapter:
Enter the adapter that the gateway can be reached on. Example eth1.
Active:
A green tick box will indicate that the gateway can be reached. A red cross will indicate that the gateway cannot be reach on that interface. Please make sure you have set up an interface and IP address on the same network as the gateway



Static Route Details

This section will provide information about all of the routes configured on your ALB-X.



Advanced Network Settings

Server Nagle:
Tick this box to enable. This is a means to improve efficiency of TCP/IP networks by reducing the number of packets that need to be sent over the network. This is applied to the Server side of the transaction. Care must be taken with the server settings as nagle and delayed ack may severely impact performance.

Client Nagle:
Tick the box to enable. As above but applied to the Client side of the transaction.

Power

The **Services — Power** page allows you to shut down the jetNEXUS ALB-X. The page is organised into the section below.

Restart

This is a global restart of all services. This will break all connections. All Services will resume after a short period automatically but the timing will depend on how many services you have configured. A pop-up will need to be confirmed in order to initialise a Reboot.

Reboot

Clicking **Reboot** will shut down you r ALB-X and automatically bring it back up again. A pop-up will need to be confirmed in order to initialise a Reboot.

Power Off

Clicking **Power Off** will shut down your ALB-X. If this is a hardware appliance you will need physical access to the appliance to Power it back on. A pop-up will need to be confirmed in order to initialise a Reboot.

Power Off

Click the Power off button to completely halt jetNEXUS ALB

Warning - This will suspend your web site and require a hardware power on

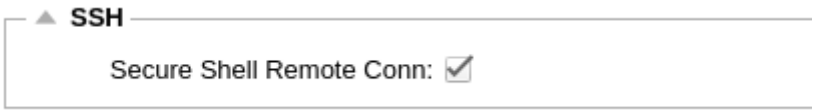
Power Off

Security

The **Configure—>Security** page allows you to change the web console password and enable or disable Secure Shell. The section is organised below:

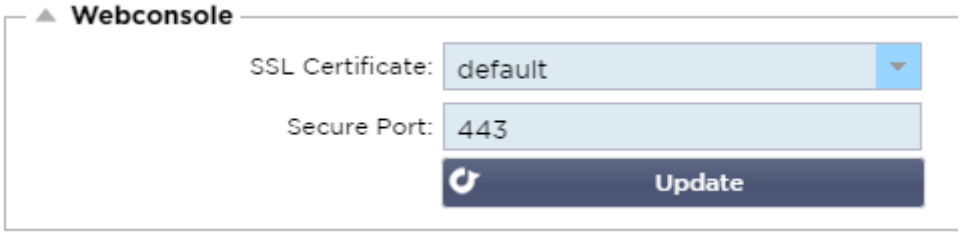
SSH

Secure Shell Conn:
Please tick the box if you wish to gain access to the ALB-X using SSH."Putty" is a great application for this.



Webconsole

SSL Certificate:
Choose a certificate from the drop down list. This is the certifcate used to secure your connection to the ALB-X. You can create your own self-signed certificate or import one from the Library -- SSL Certificates section.
Secure Port:
The default port is the Webconsole is 443. Use this box to use another port.



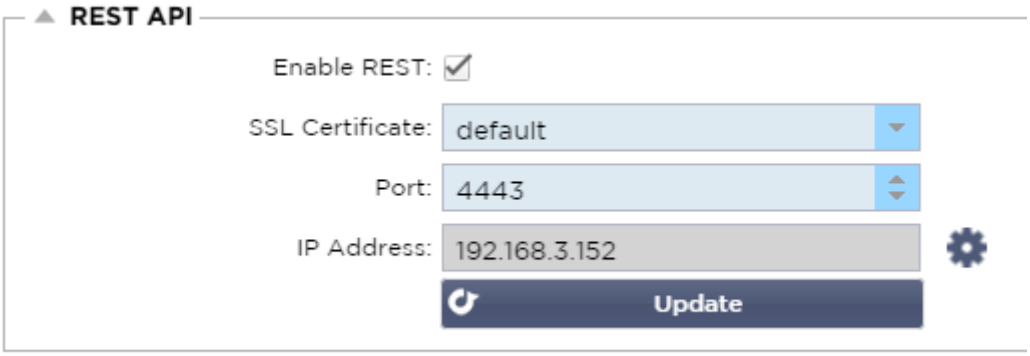
REST API

Enable REST:
Tick this box to enable REST. Note that you will also have to configure which adapter REST is enabled on. See the note on the Cog link below.
SSL Certificate:
Choose a certificate for the REST service. The drop down will show all of the certificates installed on your ALB-X.
Port:
Set the Port for the REST service. It is a good idea to use a port other than 443.
IP Address:
This will display the IP address that the REST service is tied to. You can click the Cog link to access the Network page to change

which adapter the REST service is enabled on.

Cog Link:

Clicking on this link will take you to the Network page where you can configure an adapter for the REST.



Documentation for REST API:

https://app.swaggerhub.com/apis/jetNEXUS/jetAPI/4.2.3

- Note:
  - If you get errors on the Swagger page this is because they have an issue supporting query strings
  - Scroll past the errors to edgeNEXUS REST API

Examples:

GUID using CURL:

- Command
  - curl -k https://<rest ip>/POST/32 -H "Content-Type: application/json" -X POST -d '{"<rest username>":"<password>"}'
- will return
  - {"Loginstatus":"OK","Username":"<rest username>","GUID":"<guid>"}
- Validity
  - GUID is valid for 24 hours

Licence Details:

- Command
  - curl -k https://<rest ip>/GET/39 -GET -b 'GUID=<guid;>

SNMP

The **Services->SNMP** page allows you to enable the jetNEXUS ALB-X for SNMP agent.
The page is organised into the section below.

SNMP Settings

Simple Network Management Protocol (SNMP) exposes management date in the form of variables on the jetNEXUS ALB-X. These variables can then be queried by third party SNMP managing applications.

SNMP v1:
RFC-1157

SNMP V2c:
RFC-1901-1908

SNMP v3:
RFC-3411-3418. The username for v3 is **admin**. Example:- snmpwalk -v3 -u admin -A jetnexus -l authNoPriv 192.168.1.11 1.3.6.1.4.1.38370

Community String:
This is the read-only string set on the agent and used by the manager to retrieve the SNMP information. The default community string is jetnexus

PassPhrase:
This is the password needed when SNMP v3 is enabled and must be at least 8 characters or more and contain letters Aa-Zz and numbers 0-9 only. The default passphrase is **jetnexus**

SNMP MIB

The information viewable over SNMP is defined by the Management Information Base (MIB). MIB's describe the structure of the management data and use hierarchical object identifiers (OID). Each OID can be read via an SNMP management application.

JETNEXUS-MIB

Download

JETNEXUS OID

ROOT OID:
iso.org.dod.internet.private.enterprise = .1.3.6.1.4.1

Our OIDS:

.38370 **jetnexusMIB**

.1 **jetnexusData** (1.3.6.1.4.1.38370.1)

.1 **jetnexusGlobal** (1.3.6.1.4.1.38370.1.1)

.2 **jetnexusVirtualServices** (1.3.6.1.4.1.38370.1.2)

.3 **jetnexusServers** (1.3.6.1.4.1.38370.1.3)

.1 **jetnexusGlobal** (1.3.6.1.4.1.38370.1.1)

.1 **jetnexusOverallInputBytes** (1.3.6.1.4.1.38370.1.1.1.0)

.2 **jetnexusOverallOutputBytes** (1.3.6.1.4.1.38370.1.1.2.0)

.3 **jetnexusCompressedInputBytes** (1.3.6.1.4.1.38370.1.1.3.0)

.4 **jetnexusCompressedOutputBytes** (1.3.6.1.4.1.38370.1.1.4.0)

.5 **jetnexusVersionInfo** (1.3.6.1.4.1.38370.1.1.5.0)

.6 **jetnexusTotalClientConnections** (1.3.6.1.4.1.38370.1.1.6.0)

.7 **jetnexusCpuPercent** (1.3.6.1.4.1.38370.1.1.7.0)

.8 **jetnexusDiskFreePercent** (1.3.6.1.4.1.38370.1.1.8.0)

.9 **jetnexusMemoryPercent** (1.3.6.1.4.1.38370.1.1.9.0)

.10 **jetnexusCurrentConnections** (1.3.6.1.4.1.38370.1.1.10.0)

.2 **jetnexusVirtualServices** (1.3.6.1.4.1.38370.1.2)

.1 **jnvirtualserviceEntry** (1.3.6.1.4.1.38370.1.2.1)

.1 **jnvirtualserviceIndexvirtualservice** (1.3.6.1.4.1.38370.1.2.1.**1**)

.2 **jnvirtualserviceVSAddrPort** (1.3.6.1.4.1.38370.1.2.1.**2**)

.3 **jnvirtualserviceOverallInputBytes** (1.3.6.1.4.1.38370.1.2.1.**3**)

.4 **jnvirtualserviceOverallOutputBytes** (1.3.6.1.4.1.38370.1.2.1.**4**)

.5 **jnvirtualserviceCacheBytes** (1.3.6.1.4.1.38370.1.2.1.**5**)

.6 **jnvirtualserviceCompressionPercent** (1.3.6.1.4.1.38370.1.2.1.**6**)

.7 **jnvirtualservicePresentClientConnections** (1.3.6.1.4.1.38370.1.2.1.**7**)

.8 **jnvirtualserviceHitCount** (1.3.6.1.4.1.38370.1.2.1.**8**)

.9 **jnvirtualserviceCacheHits** (1.3.6.1.4.1.38370.1.2.1.**9**)

.10 **jnvirtualserviceCacheHitsPercent** (1.3.6.1.4.1.38370.1.2.1.**10**)

.11 **jnvirtualserviceVSStatus** (1.3.6.1.4.1.38370.1.2.1.**11**)

.3 **jetnexusRealServers** (1.3.6.1.4.1.38370.1.3)

.1 **jnrealserverEntry** (1.3.6.1.4.1.38370.1.3.**1**)

.1 **jnrealserverIndexVirtualService** (1.3.6.1.4.1.38370.1.3.1.**1**)

.2 **jnrealserverIndexRealServer** (1.3.6.1.4.1.38370.1.3.1.**2**)

.3 **jnrealserverChAddrPort** (1.3.6.1.4.1.38370.1.3.1.**3**)

.4 **jnrealserverCSAddrPort** (1.3.6.1.4.1.38370.1.3.1.**4**)

.5 **jnrealserverOverallInputBytes** (1.3.6.1.4.1.38370.1.3.1.**5**)

.6 **jnrealserverOverallOutputBytes** (1.3.6.1.4.1.38370.1.3.1.**6**)

.7 **jnrealserverCompressionPercent** (1.3.6.1.4.1.38370.1.3.1.**7**)

.8 **jnrealserverPresentClientConnections** (1.3.6.1.4.1.38370.1.3.1.**8**)

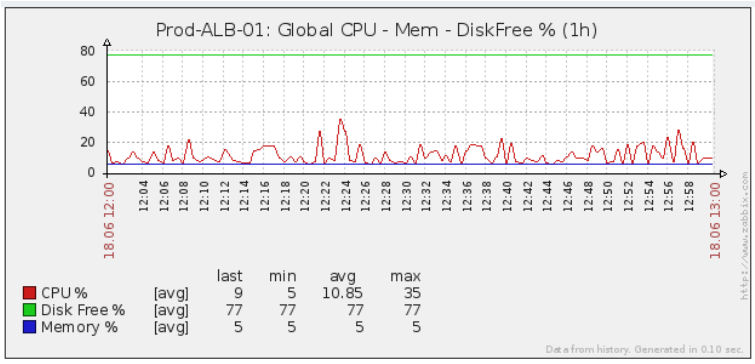
.9 **jnrealserverPoolUsage** (1.3.6.1.4.1.38370.1.3.1.**9**)

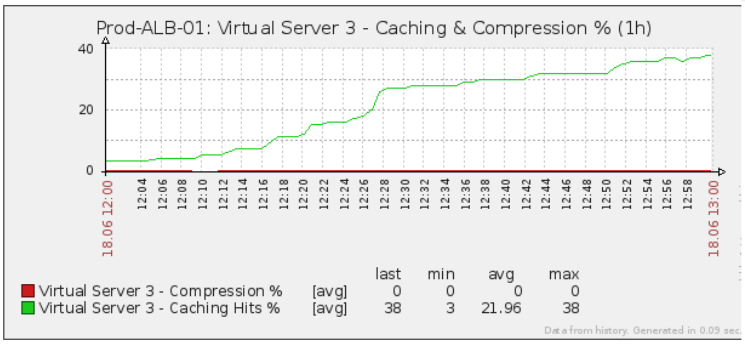
.10 **jnrealserverHitCount** (1.3.6.1.4.1.38370.1.3.1.**10**)
.11 **jnrealserverRSStatus** (1.3.6.1.4.1.38370.1.3.1.**11**)

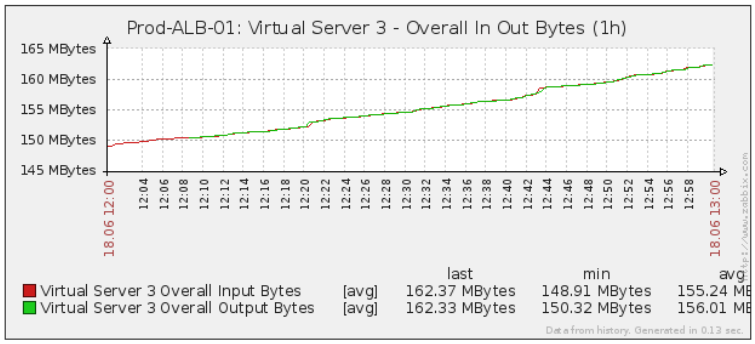
Historical Graphing

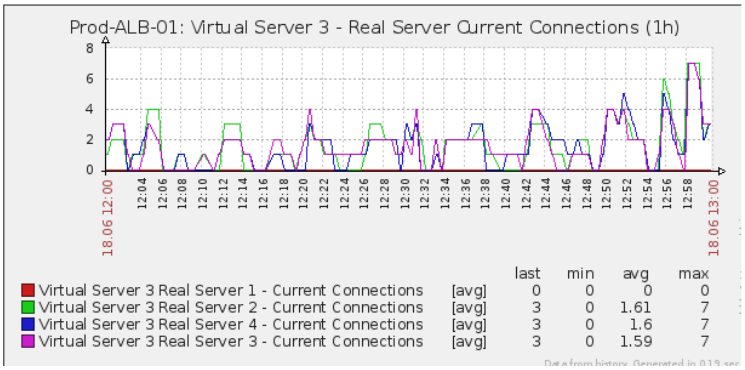
The best use of the edgeNEXUS Custom SNMP MIB is the ability to offload the historical graphing to a management console.

Below are some examples from Zabbix that polls a jetNEXUS ALB-X for various OID values listed above.









Users

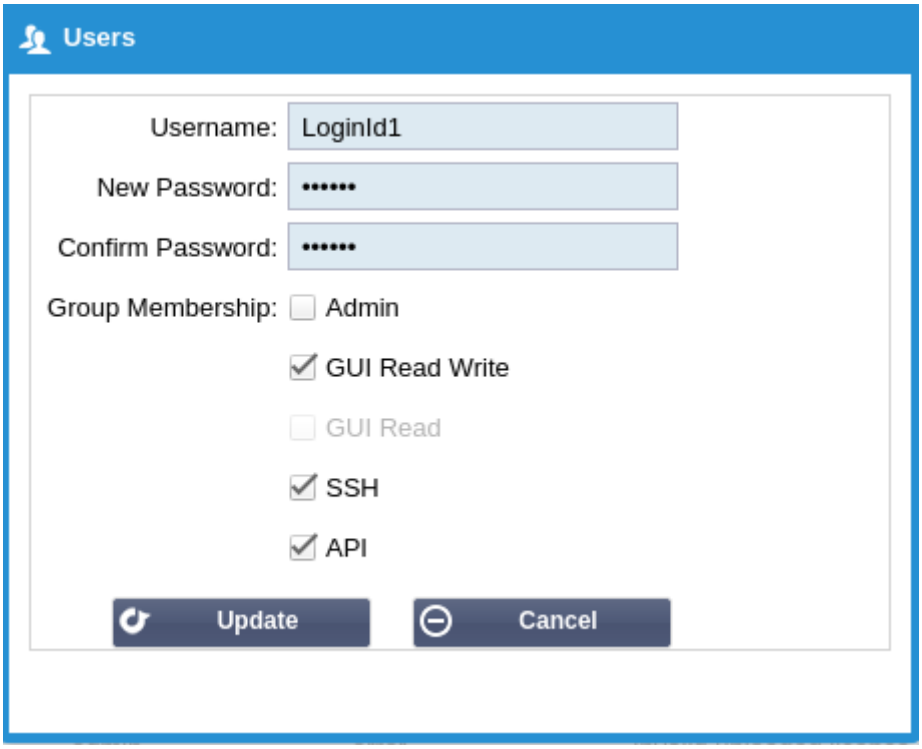
The **System — Users** page allows you to configure multiple users and assign different roles to each user. It also shows the audit log where you can see changes made by each user.

Users

Adding a User

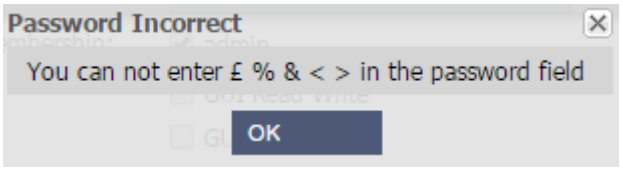
- Click

and the screen below will pop up



- Enter a suitable **User Name**:
  - Minimum number of characters 1
  - Maximum number of characters 32
  - Letters can be upper and lower case
  - Numbers may be used
  - Symbols are not permitted
- Enter a suitable strong password
  - Minimum number of characters 6
  - Maximum number of characters 32
  - Must use at least a combination of letters and numbers
  - Letters can be upper or lower case

- Symbols are permitted with the exception of those in the screen shot below



- Re-enter your strong password
- Tick one or more groups you would like the user to be a member of:
  - Admin
    - This group can do everything
  - GUI Read Write
    - Users in this group can access the GUI and make changes via the GUI
  - GUI Read
    - Users in this group can access the GUI to view information only. No changes can be made
  - SSH
    - Users in this group can access the ALB-X via Secure Shell. This will give access to the command line which has a very limited set of commands available
  - API
    - Users in this group will have access to SOAP and REST programmable interface. REST will be available from Software Version 4.2.1

User Type

Local User

- ALB-X in Stand-Alone or Manual H/A role will create Local Users only
- By default there is a local user called “admin” that is a member of the admin group. For backwards compatibility this user can never be deleted
- You may change the password of this user or delete it but you cannot delete the last local admin

Cluster User

- ALB-X in Cluster role will create Cluster Users only
- Cluster Users are synchronised across all of the ALB-X in the Cluster
- Any change to a cluster user will change on all members of the cluster
- If you are logged on as a cluster user then you will not be able to change roles from cluster to manual or stand-alone

Cluster and Local User

- Any users created whilst in Stand-Alone or Manual role will be copied to the Cluster
- If the ALB-X subsequently leave the Cluster then only Local Users will remain
- The last configured password for the user will be valid

Removing Users

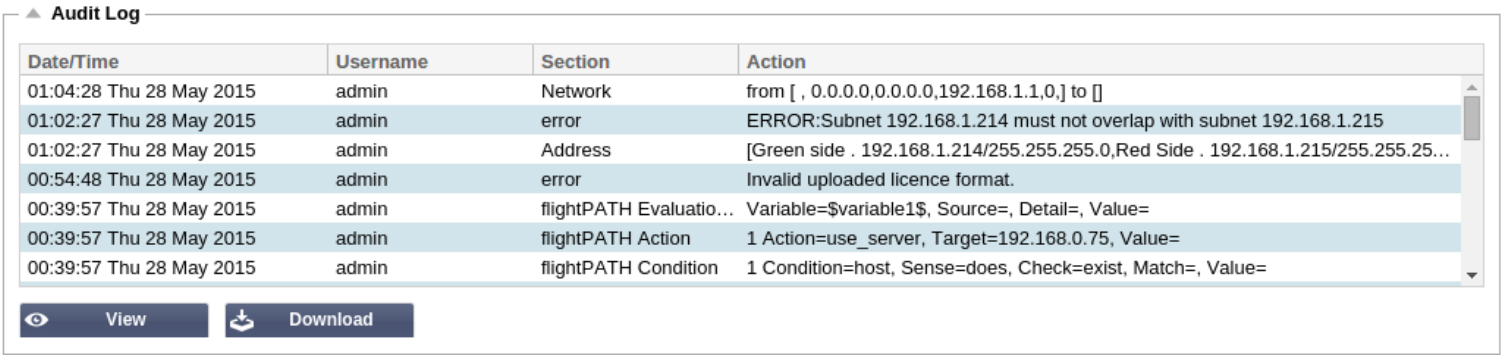
- Highlight an existing user
- Click **Remove**
- You will not be able to delete the user that is currently signed in
- You will not be able to remove the last local user in the admin group
- You will not be able to remove the last cluster user in the admin group
- You will not be able to delete the admin user for backwards compatibility
- If you remove an ALB-X from the cluster all users except local users will be deleted

Editing Users

- Highlight an existing user
- Click **Edit**
- You may change the user's group membership by ticking the appropriate boxes and updating
- You may also change the password of a user provided you have admin rights

Audit Log

As of software version 4.1.1 jetNEXUS ALB-X logs each change made by individual users. The audit log will provide the last 50 actions carried out by all users. You may also see ALL entries in the System Log Example:



Configuration

The **Advanced -- Configuration** page allows you to download your configuration, upload a new configuration or upload a jetPACK application template.

Configuration

Download or save a configuration file

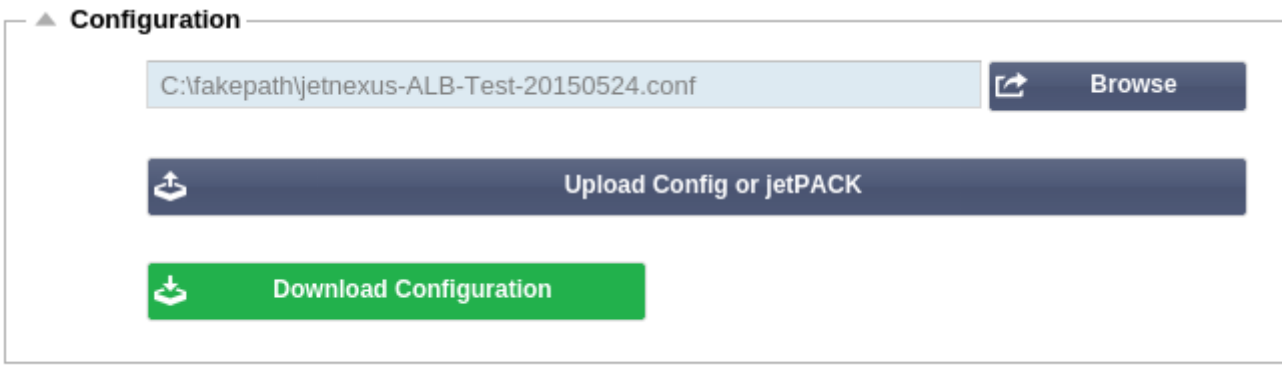
1. To download the current configuration of the jetNEXUS ALB-X simply press the Click Here icon.
2. A pop-up will appear asking you to open or save the .conf file.
3. Save to a convenient location.
4. You can open this with any text editor such as Notepad.

Upload a new configuration from a saved .conf file

1. You may upload a saved configuration file by browsing for the saved .conf file.
2. Click Upload.
3. The jetNEXUS ALB-X will apply the config and refresh the browser. If it does not, please click refresh.
4. You will be redirected to the Dashboard page upon completion.

Upload a new jetPACK

1. A jetPACK is a set of updates to the existing configuration.
2. A jetPACK can be as small as changing the TCPTimeout value to a complete application specific deployment such as Microsoft Exchange or Microsoft Lync.
3. You can obtain a jetPACK from support@edgenexus.io.
4. Browse for the jetPACK.txt file.
5. Click upload.
6. The browser will refresh automatically after upload.
7. You will be redirected to the Dashboard page upon completion. This may take longer for more complex deployments such as Lync.

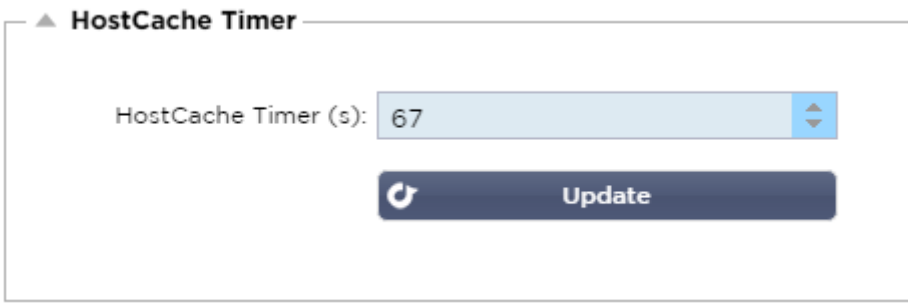


Global Settings

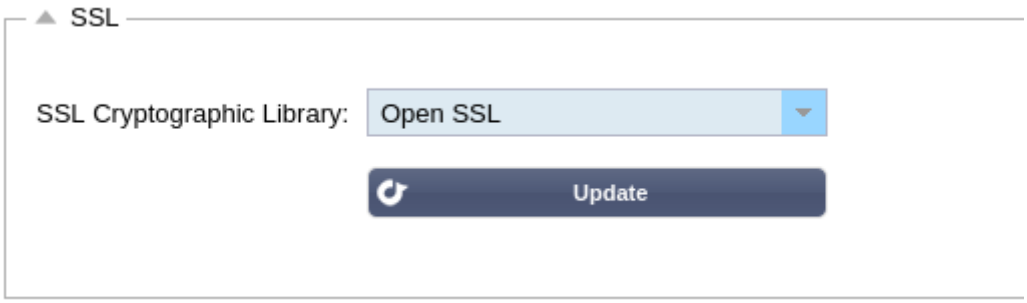
The **Services-->Global Settings** page allows you to change the SSL cryptographic library The page is organised into the section below.

Global Settings

The Host Cache Timer stores the IP Address of a real server when the domain name has been used instead of an IP Address. The cache is flushed upon a real server failure. Setting this value to zero will never flush. There is no max value for this setting.



This global setting will change the SSL library used for client side services. Open SSL is the default setting. There is an option to change this to WolfSSL. More information can be found here about Wolf SSL.



HTTP

The **Advanced->Protocol->HTTP** page allows you to set advanced settings for HTTP. The page is organised into the section below.

Server Too Busy

If you have limited the maximum connections to your real servers you can choose to present a friendly web page once this limit has been reached.

1. Create a simple web page with your message. You may include external links to objects on another web server. Alternatively if you want to include images on your web page then use inline base64 encoded images
2. **Browse** for your newly created web page
3. Click **Upload**
4. If you wish to preview the page you can do so with the **Click Here** link

Example of Server Too Busy page

Sorry for the inconvenience but the server is busy

please try again soon

Forwarded For

Forwarded for is the de facto standard for identifying the originating IP address of a client connecting to a web server through layer-7 load balancers and proxy-servers.

Forwarded-For Output:

Off:

jetNEXUS ALB-X does not alter the Forwarded-For header.

Add Address and Port:

This will append the IP address and port, of the device or client connected to the jetNEXUS ALB-X, to the Forwarded-For header.

Add Address:

This will append the IP address, of the device or client connected to the jetNEXUS ALB-X, to the Forwarded-For header.

Replace Address and Port:

This will replace the value of the Forwarded-For header with the IP address and port of the device or client connected to

jetNEXUS ALB-X.

Replace Address:

This will replace the value of the Forwarded-For header with the IP address of the device or client connected to jetNEXUS ALB-X.

Forwarded-For Header:

This is the name given to the Forwarded-For header. Typically this is “X-Forwarded-For” but may be changed for particular environments.

Advanced Logging for IIS – Custom Logging

You can obtain the X-Forwarded-For information by installing the IIS Advanced logging 64 bit app. Once downloaded, create a Custom Logging Field called X-Forwarded-For with the settings below
From the Category list, select Default From the Source Type list, select Request Header In the Source Name box, type X-Forwarded-For
http://www.iis.net/learn/extensions/advanced-logging-module/advanced-logging-for-iis-custom-logging

Apache httpd.conf changes

There are several changes you are going to want to make to the default format in order to log the X-Forwarded-For client ip address or the real client ip address if the X-Forwarded-For header does not exist.
Those changes are below:

- LogFormat: “%h %l %u %t \”%r\” %>s %b \”%{Referer}i\” \”%{User-Agent}i\”” combined
- LogFormat: “%{X-Forwarded-For}i %l %u %t \”%r\” %>s %b \”%{Referer}i\” \”%{User-Agent}i\”” proxy SetEnvIf X-Forwarded-For “^.*\..*\..*\..*” forwarded
- CustomLog: “logs/access_log” combined env=!forwarded
- CustomLog: “logs/access_log” proxy env=forwarded

This format takes advantage of apache’s built-in support for conditional logging based upon environment variable.

- The first line is the standard combined log formatted string from the default.
- The second line replaces the %h (remote host) field with the value(s) pulled from the X-Forwarded-For header and sets the name of this log file pattern to “proxy”.
- Line 3 is a setting for environment variable “forwarded” that contains a loose regular expression matching an ip address, which is ok in this case since we really care more whether an ip address exists in the X-Forwarded-For

header. Explained another way, line 3 could be read as: “If there is an X-Forwarded-For value, use it.”
- Lines 4 and 5 tell apache which log pattern to use. If and X-Forwarded-For value exists, use the “proxy” pattern, else use the “combined” pattern for that request. For readability, lines 4 and 5 do not take advantage of Apache’s rotatelogs (piped) logging feature but I assume that it is in use by most everyone.

These changes should result in logging an IP address for every request.

HTTP Compression Settings

Compression is an acceleration feature and is enabled for each Service on the IP Services page.

WARNING – Take extreme care when adjusting these settings as inappropriate settings can adversely affect the performance of jetNEXUS ALB-X

Initial Thread Memory [KB]:

This is the amount of memory each request received by jetNEXUS ALB-X may initially allocate. For most efficient performance, this value should be set at a value just in excess of the largest uncompressed HTML file that the web servers are likely to send.

Maximum Thread Memory [KB]:

This is the maximum amount of memory that the jetNEXUS ALB-X will allocate on one request. For maximum performance, jetNEXUS ALB-X normally stores and compresses all content in memory. IF an exceptionally large content file exceeding this amount is processed, jetNEXUS ALB-X will write to disk and compress the data there.

Increment Memory [KB]:

This sets the amount of memory added to the *Initial Thread Memory Allocation* when more is required. The default setting is zero. This means jetNEXUS ALB-X will double the allocation when the data exceeds the current allocation (e.g. 128Kb, then 256Kb, then 512Kb, etc) up to the limit set by *Maximum Memory Usage per Thread*. This is efficient where the majority of pages are of a consistent size but there are occasional larger files. (e.g. Majority of pages are 128Kb or less, but occasional responses are 1Mb in size.) In the scenario where there are large variable sized files, it is more efficient to set a linear increment of a ignificant size (e.g.Responses are 2Mb to 10Mb in size, an initial setting of 1Mb with increments of 1Mb would be more efficient.).

Minimum Compression Size [Bytes]:

This is the size, in bytes, under which the jetNEXUS ALB-X will not attempt to compress. This is useful because anything much under 200-bytes does not compress well and may even grow in size due to the overheads of compression headers.

Safe Mode:

Tick this option to prevent jetNEXUS ALB-X from applying compression to style sheets of JavaScript. The reason for this is that even though jetNEXUS ALB-X is aware of which individual browsers can handle compressed content, some other proxy servers, even though they claim to be HTTP/1.1 compliant are unable to transport compressed style sheets and JavaScript correctly. If problems are occurring with style sheets or JavaScript through a proxy server, then use this option to disable compression of these types. However, this will reduce the overall amount of compression of content.

Disable Compression:

Tick this to stop jetNEXUS ALB-X from compressing any response.

Compress As You Go:

On:

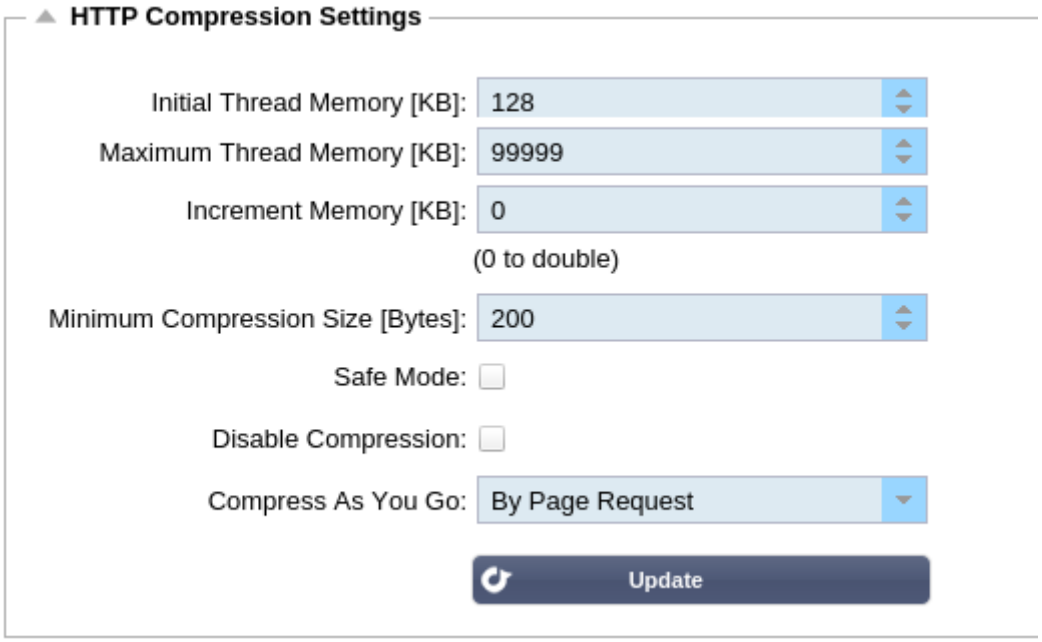
Use Compress as You Go on this page. This compresses each block of data received from the server in a discrete chunk that is fully de-compressible.

Off:

Do not use Compress As you Go on this page.

By Page Request:

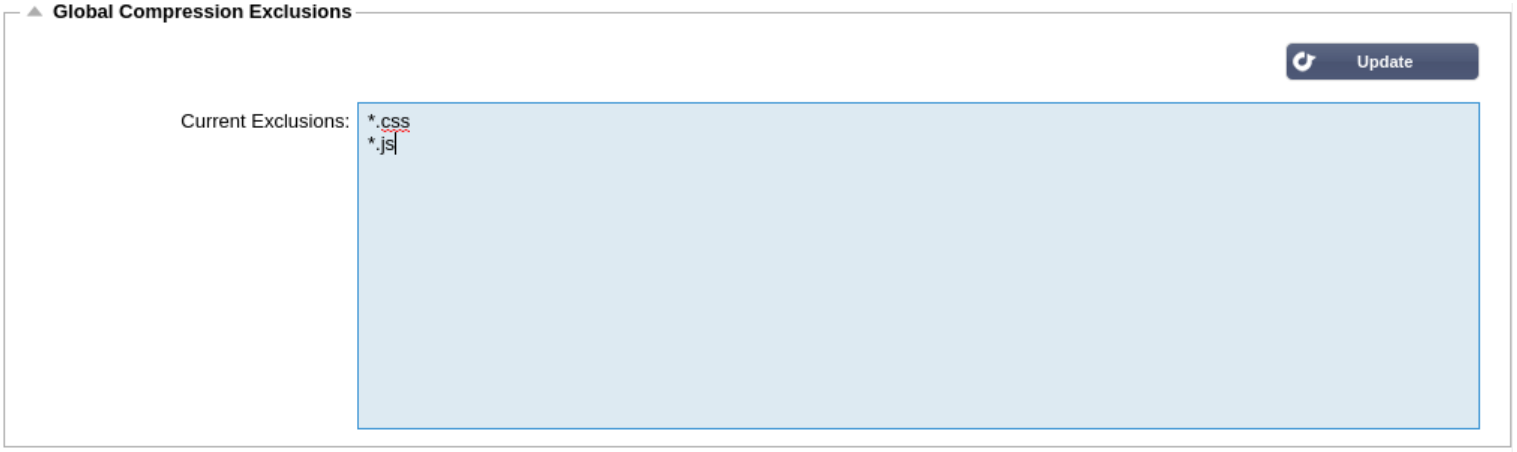
Use Compress as You Go by page request.



Global Compression Exclusions

Anything added to the current exclusion list will not be compressed.

1. Type in the individual file name.
2. Click update.
3. If you wish to add a file type simply type “*.css” for all cascading style sheets to be excluded.
4. Each file or file type should be added on a new line.



Software

The **Advanced->Software** page allows you to update the configuration and the firmware of your jetNEXUS ALB-X. The page is organised into the section below.

ALB Software Upgrade Details

The information in this section will be populated if you have a working Internet connection. If your browser does not have a connection to the Internet this section will be blank. Once you receive the banner message below

This section will be populated with the information similar to the screen shot below. Of particular interest is the support Type and Support Expiry date.

Note: We use your browsers internet connection to view what is available from the Cloud. You will only be able to download software updates if the ALB-X itself has an internet connection.

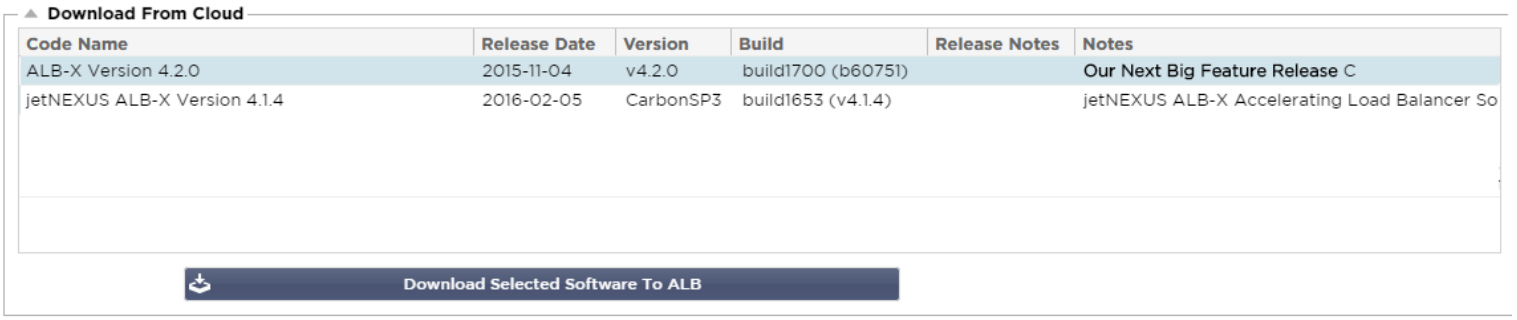
To check this:

- Advanced--Troubleshooting--Ping
- IP Address - www.jetnexuscloud.com
- Click Ping
- Result - "ping: unknown host www.jetnexuscloud.com"
- Your ALB-X will NOT be able to download anything from the cloud

Download from Cloud

If your browser is connected to the Internet you will be able to see details of software available in the cloud.

- Highlight the row you are interested in and click “Download Selected Software to ALB”
- This will download the selected software to your ALB where is can be applied in the “Apply Software Stored on ALB” section below.



Note: If your ALB-X does not have internet access directly you will receive an error like below:

Download error, ALB not able to access edgeNEXUS Cloud Services for file build1734-3236-v4.2.1-Sprint2-update-64.software.alb

Upload software to ALB

This section will allow you to manually upload a software build from your computer.

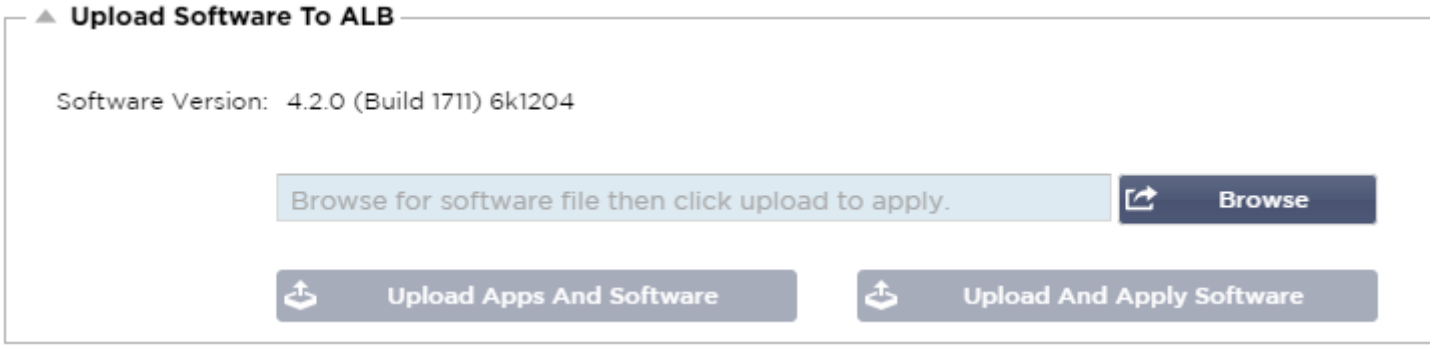
Upload Apps and Software

Apps

- If you have an App file which will end <apptype>.alb you can use this button to upload it.
- There are five types of App
  - <appname>flightpath.alb
  - <appname>.monitor.alb
  - <appname>.jetpack.alb
  - <appname>.addons.alb
  - <appname>.featurepack.alb
- Once uploaded each app will be found in the Library-Apps section
- You must then deploy each App in this section.

Software

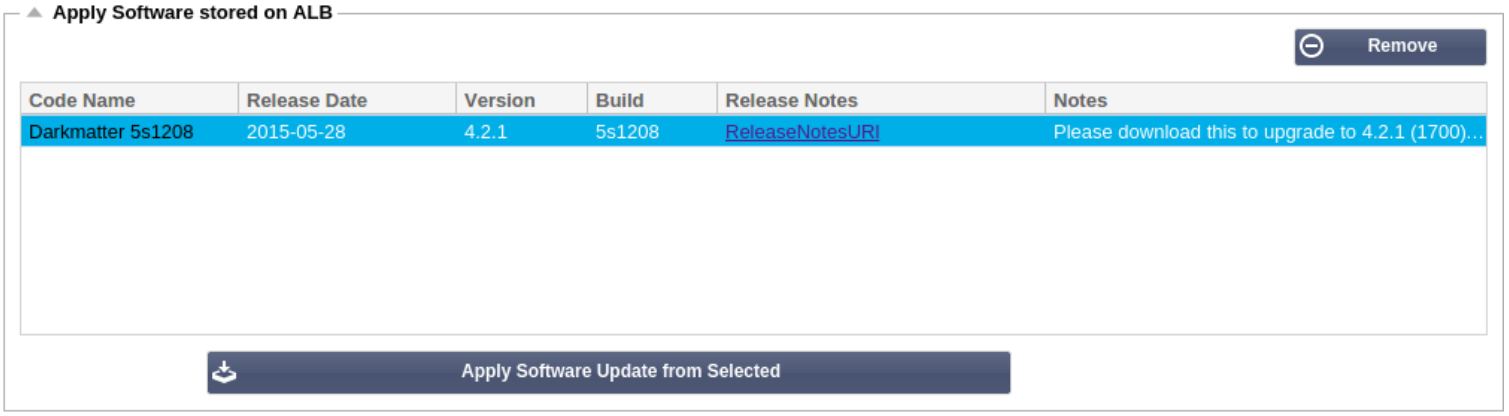
- If you wish to upload software without applying it then use this button.
- The Software File is <softwarename>.software.alb.
- It will then show in the “Software Stored on ALB” section where you can apply it at your convenience.



Apply Software stored on ALB

This section will show all Software files stored on the ALB itself. This will include updated Web Application Firewall signatures.

- Highlight the Software row you are interested in.
- Click “Apply Software from Selected”.
- If this is a Software Update for the ALB then please be aware that it will upload and then reboot to apply.
- If this is an OWASP signature update it will apply automatically without rebooting.



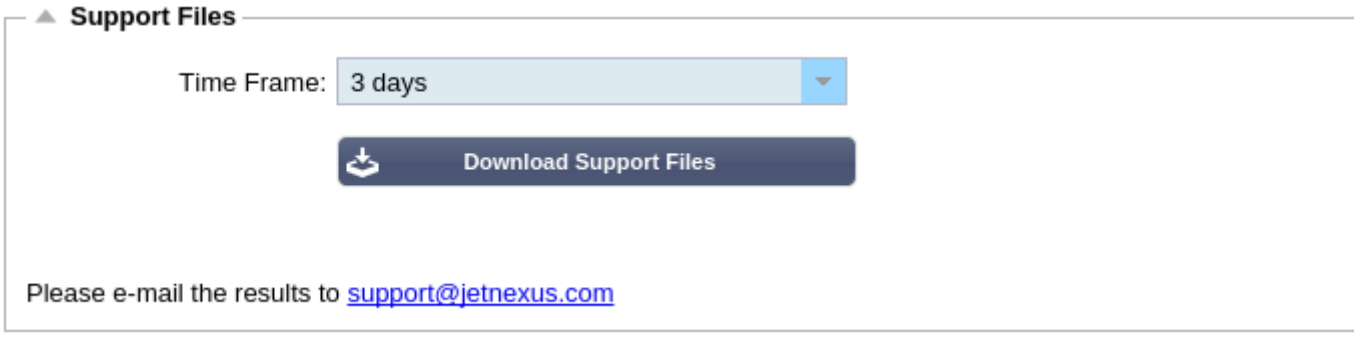
Troubleshooting

The **Advanced — Troubleshooting** page contains various sections that will allow you to investigate any issue you are having with your services. The page is organised into the 4 sections below:

Support Files

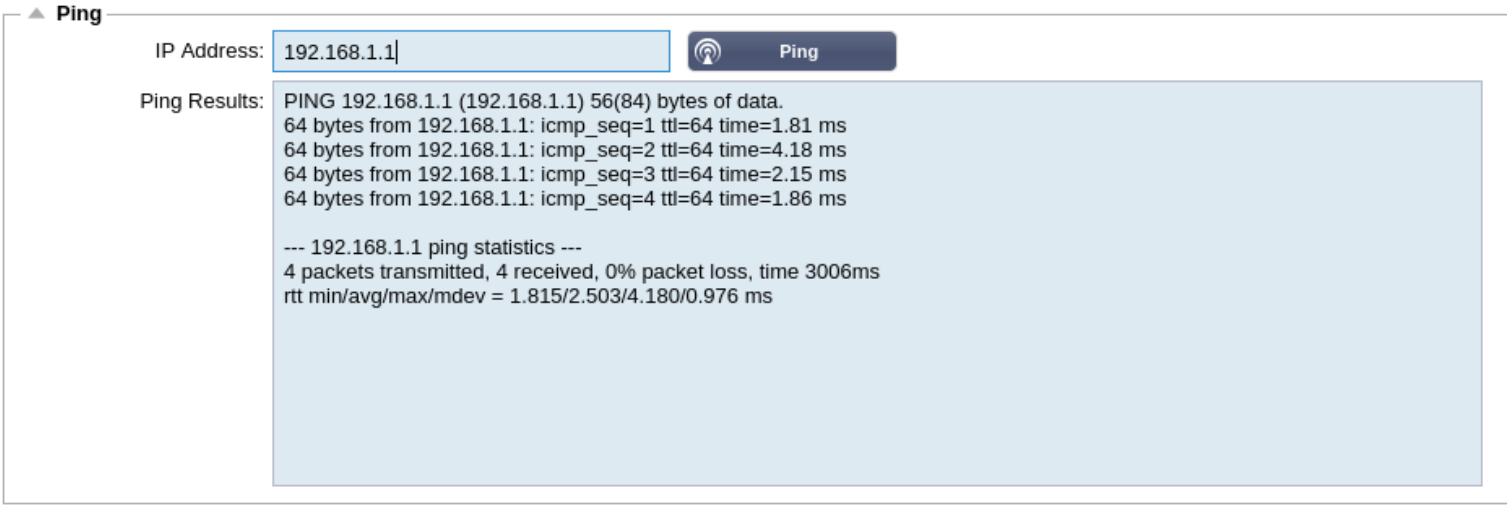
If you have an issue with your **ALB-X** and you need to open a support ticket they will often request a number of different files from your ALB-X appliance. These files have now been aggregated into one .dat file that can be downloaded via this section.

- Select a time frame from the drop down
    - 3 days
    - 7 days
    - 14 days
    - All
- Click “Download Support Files”
- A file will be downloaded in the format **Support-jetNEXUS-yyymmddhh-NAME.dat**

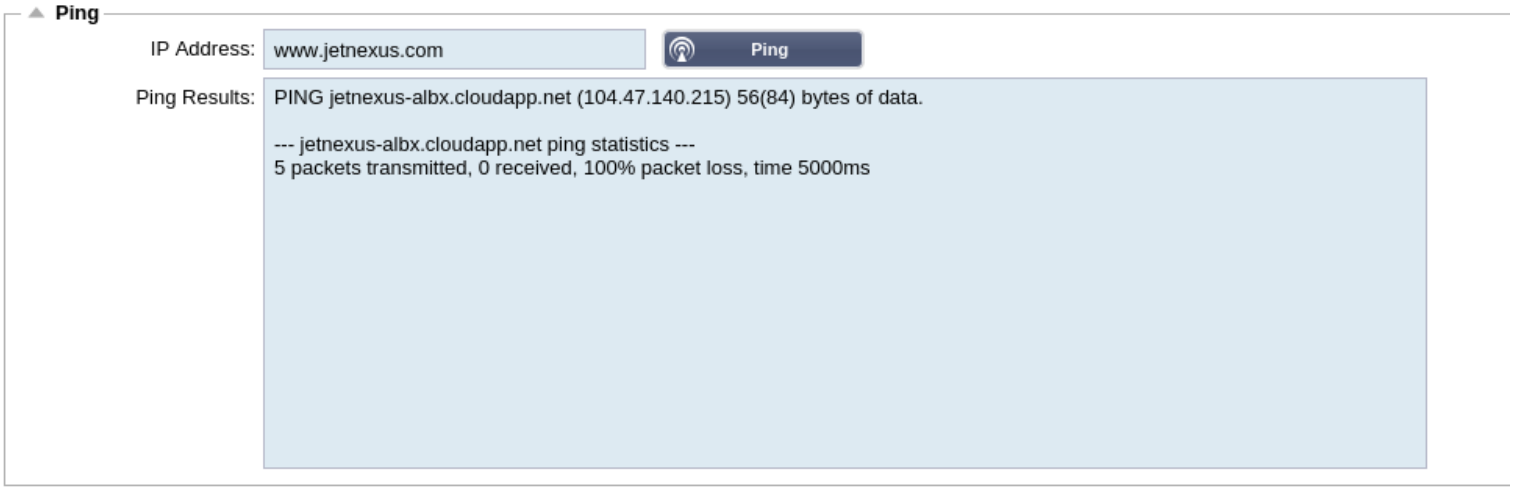


Ping

Type in the IP address of the host you wish to test, for example the default gateway using dotted decimal notation or an IPv6 address. You may have to wait a few seconds for the result but to feedback that you have pressed the “Ping” button it will go grey after pressing.



If you have configured a DNS server then you can type in the fully qualified domain name. You can configure a DNS server on the Appliance page. You may have to wait a few seconds for the result but to feedback that you have pressed the “Ping” button it will go grey after pressing.

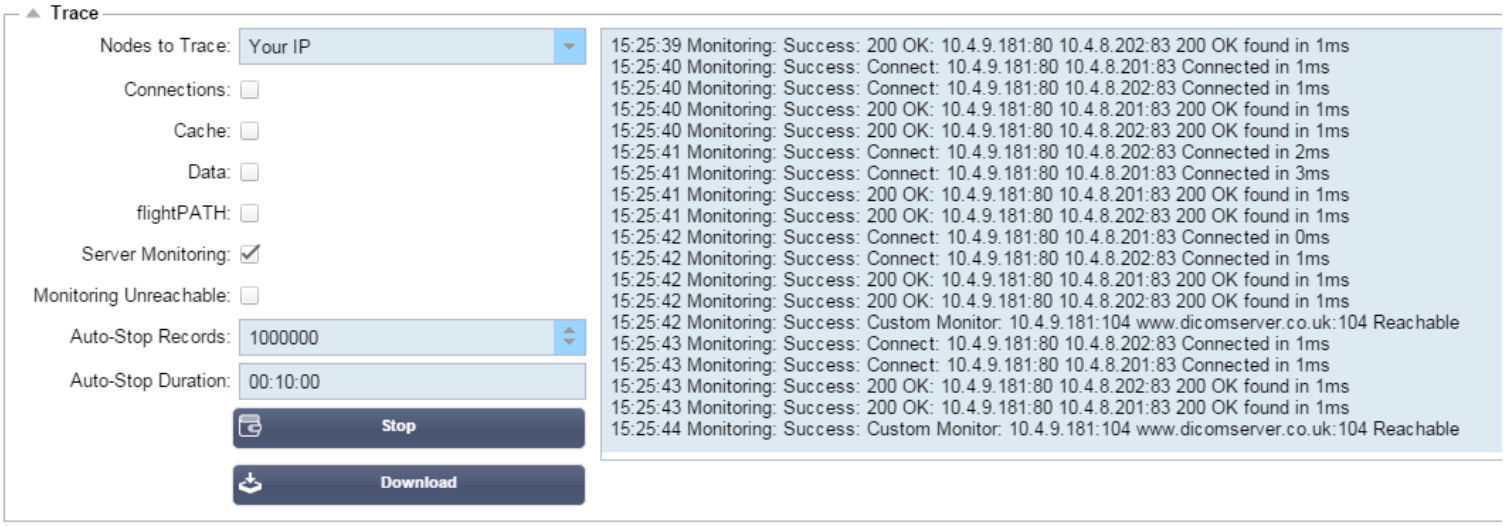


Trace

The Trace section will allow you to see debug information depending on the options you choose from the drop downs and the tick boxes.

- **Nodes to Trace:**
  - **Your IP: This will filter the output to use the IP address you are accessing the GUI from (Note do not choose this option for Monitoring as Monitoring will use the ALB-X interface address)**
  - **All IP: No filter will be applied. It should be noted that on a busy box this will adversely affect performance.**
- **Connections:**
  - This will show you information about the client and server side connections**.**
- **Cache:**

    - This will show you information with regards to cached objects.
- **Data:**
    - Shows the raw data bytes handled in and out by ALB-X**.**
- **flightPATH:**
    - This will show you detailed information about the flightPATH rules active on your box including if your rules is matching the condition and evaluation**.**
- **Server Monitoring:**
    - This will show the server health monitors active on your ALB-X and their respective result**.**
- **Monitoring Unreachable:**
    - This is similar to above except it will only show the failed monitors and so acts like a filter for these messages only.
- **Auto-Stop Records:**
    - The default value is 1,000,000 records after which the Trace facility will automatically stop. This is a safety precaution to prevent Trace accidentally being left on and affecting the performance of your ALB-X**.**
- **Auto-Stop Duration:**
    - The default time is set to 10 minutes after which the Trace facility will automatically stop. This is a safety precaution to prevent Trace accidentally being left on and affecting the performance of your ALB-X.
- **Start:**
    - **Click to manually Start the Trace facility.**
- **Stop:**
    - **Click to manually stop the Trace facility before the automatic record or time is reached.**
- **Download:**
    - Although you can see the live viewer on the right hand side the information may be displayed too quickly. You can download the Trace.log to view all the information gathered during the various traces that day. This is basically a filtered list of trace information. If you wish to view previous days trace information then you can download syslog for that day but will have to filter manually**.**

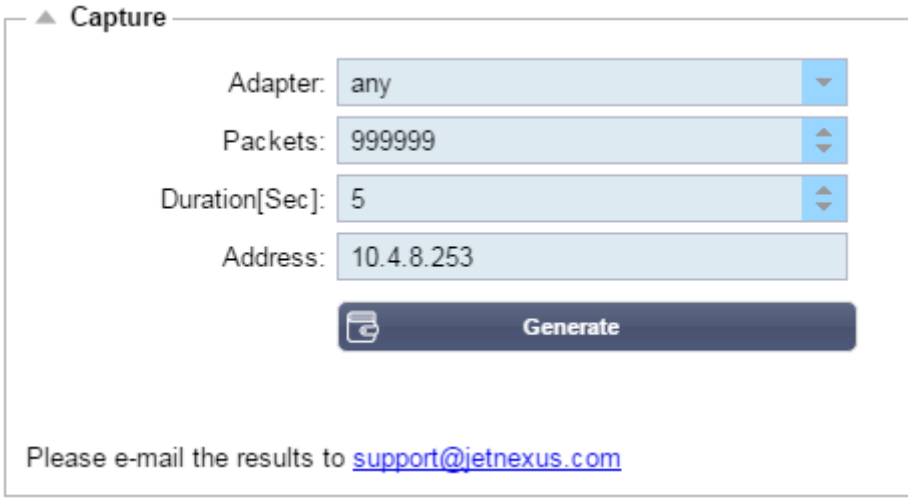


Capture

1. Complete each box

2. Click **Generate**
3. Once the capture has run your browser will pop-up and ask you where to save the file. It will be in the format "jetNEXUS.cap.gz"
4. Email this file to support@edgenexus.io
5. You can view the contents using Wireshark

Adapter:
Choose your adapter from the drop-down, typically **eth0** or **eth1**. You can also capture all interfaces with "**any**"
Packets:
This is the maximum amount of packets to capture. Typically 99999
Duration:
Choose a maximum time that the capture will run for. A typical time is 15 seconds for high traffic sites. The GUI will be inaccessible during the capture period
Address:
This will filter on any IP address entered in the box. Leave this blank for no filter.



To maintain performance we have limited the download file to 10MB. If you find that this is not enough to capture all the data you require we can increase this figure. This will have an impact on performance of live sites. To increase the available capture size please apply a global setting jetPACK to increase the capture size.

About Us

The **Help->About Us** page will provide the version of software and contact information for edgeNEXUS Solutions Ltd

Who is jetNEXUS?

- edgeNEXUS provide innovative, market leading solutions for application acceleration, load balancing and application delivery technology
- edgeNEXUS is a successful, profitable and privately owned company with over 10 years' industry experience
- Our product portfolio is accessible to a wide and varied client base, ranging from simple, cost effective point solutions to Enterprise-grade application delivery gateways
- We understand that this technology is mission critical and as such, maintain a tenacious focus on the quality of our products and technical support
    - Via a network of head offices in London, United States and Malaysia, edgeNEXUS continually strives to deliver outstanding support to our partners and customers regardless of location. Our approach to this international presence is: *Global Voice, Local Accent.*
- With a pragmatic attitude to product development, edgeNEXUS aims to include the features that deliver the biggest difference to the end user experience.
    - These features are packaged in a format that is flexible, intuitive and easy to configure.
    - We want to ensure that every interaction we have with our customers and partners is positive
- We love our business and we want this passion to be reflected in our product quality, innovative features and attitude towards support

Contact information

- EMEA

    edgeNEXUS EMEA Head Office, Suite 2, Anglers Court, 33-44 Spittal Street, Marlow, Buckinghamshire, SL7 1DB, UK.

    Tel: +44 (0) 870 382 5050 Email: info@edgenexus.io

jetPACK

jetPACKs are a unique method of instantly configuring your edgeNEXUS Accelerating Load Balancer for specific applications. These easy-to-use templates come pre-configured and fully-tuned with all of the application-specific settings that you need in order to enjoy optimised service delivery from your Load Balancer. . Some of the jetPACKs use flightPATH to manipulate the traffic, you must have a flightPATH license for this particular element to work. To find out if you have a license for flightPATH please refer to the Licence page. This page is split in to the following sections

Download a jetPACK

Each jetPACK below has been created with a unique Virtual IP address that is contained in the title of the jetPACK. For example the first jetPACK below has a Virtual IP Address of 1.1.1.1

You can either upload this jetPACK as is and change the IP address in the GUI or edit the jetPACK with a text editor such as Notepad++ and search and replace 1.1.1.1 with your own Virtual IP address.

In addition each jetPACK has been created with 2 real servers which have the IP address of 127.1.1.1 and 127.2.2.2 Again you can change these in the GUI after upload or beforehand using Notepad++ Right click on a jetPACK link below and **Save Link as...** a **jetPACK-VIP-Application.txt** file in your chosen location

Microsoft Exchange

Application	Download link	What does it do?	What's included?
Exchange 2010	jetPACK-1.1.1.1-Exchange-2010	This jetPACK will add the basic settings to load balance Microsoft Exchange 2010.There is a flightPATH rule included to redirect traffic on the http service to https but it there as an option. If you don't have a licence for flightPATH this jetPACK will still work.	• **Global settings:** Service timeout 2 hours • **Monitors:** Layer 7 monitor for outlook web app. Layer 4 out of band monitor for client access service • **Virtual Service IP:** 1.1.1.1 • **Virtual Service Ports:** 80, 443, 135, 59534, 59535 • **Real Servers:** 127.1.1.1 127.2.2.2 • **flightPATH:** Adds redirect from http to https
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	Same as above but it will add an SMTP service on port 25 in reverse proxy connectivity. The SMTP server will see the ALB-X interface address as the source IP.	• **Global settings:** Service timeout 2 hours • **Monitors:** Layer 7 monitor for outlook web app. Layer 4 out of band monitor for client access service • **Virtual Service IP:** 1.1.1.1 • **Virtual Service Ports:** 80, 443, 135, 59534, 59535, 25 (reverse proxy) • **Real Servers:** 127.1.1.1 127.2.2.2 • **flightPATH:** Adds redirect from http to https
	jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR	Same as above except this jetPACK will configure the SMTP service to use Direct Server Return connectivity. This is needed if your SMTP server needs to see the real ip address of the client.	• **Global settings:** Service timeout 2 hours • **Monitors:** Layer 7 monitor for outlook web app. Layer 4 out of band monitor for client access service • **Virtual Service IP:** 1.1.1.1 • **Virtual Service Ports:** 80, 443, 135, 59534, 59535, 25 (direct server return) • **Real Servers:** 127.1.1.1 127.2.2.2 • **flightPATH:** Adds redirect from http to https

Exchange 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	This setup adds 1 VIP and two services for both HTTP and HTTPS traffic and requires the least amount of CPU. It is possible to add multiple healtchecks to the VIP in order to check each of the individual services is up	• **Global settings:** • **Monitors:** Layer 7 monitor for OWA, EWS, OA, EAS, ECP, OAB and ADS • **Virtual Service IP:** 2.2.2.1 • **Virtual Service Ports:** 80, 443 • **Real Servers:** 127.1.1.1 127.2.2.2 • **flightPATH:** Adds redirect from http to https
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	This setup uses a unique IP address for each service and therefore uses more resource than above. You must configure each service as a unique DNS entry Example owa.jetnexus.com, ews.jetnexus.com etc. A monitor for each service will be added and applied to the relevant service	• **Global settings:** • **Monitors:** Layer 7 monitor for OWA, EWS, OA, EAS, ECP, OAB,ADS, MAPI and Powershell • **Virtual Service IP:** 2.2.3.1, 2.2.3.2, 2.2.3.3, 2.2.3.4, 2.2.3.5, 2.2.3.6, 2.2.3.7, 2.2.3.8, 2.2.3.9, 2.2.3.10 • **Virtual Service Ports:** 80, 443 • **Real Servers:** 127.1.1.1 127.2.2.2 • **flightPATH:** Adds redirect from http to https
	jetPACK-2.2.2.3-Exchange2013-HIgh-Resource	This jetPACK will add one unique IP address and several virtual services on different ports. flightPATH will then context switch based on the destination path to the correct Virtual Service. This requires the most amount of CPU to carry out the context switching	• **Global settings:** • **Monitors:** Layer 7 monitor for OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI and Powershell • **Virtual Service IP:** 2.2.2.3 • **Virtual Service Ports:** 80, 443, 1, 2, 3, 4, 5, 6, 7 • **Real Servers:** 127.1.1.1 127.2.2.2 • **flightPATH:** Adds redirect from http to https

Microsoft Lync 2010/2013

Reverse Proxy

-
  - jetPACK-3.3.3.1-Lync-Reverse-Proxy

Front End

- jetPACK-3.3.3.2-Lync-Front -End

Edge Internal

- jetPACK-3.3.3.3-Lync-Edge-Internal

Edge External

- jetPACK-3.3.3.4-Lync-Edge-External

Web Services

Normal HTTP

- jetPACK-4.4.4.1-Web-HTTP

SSL Offload

- jetPACK-4.4.4.2-Web-SSL Offload

SSL Re-Encryption

- jetPACK-4.4.4.3-Web-SSL-Re-Encryption

SSL Passthrough

- jetPACK-4.4.4.4-Web-SSL Passthrough

Microsoft Remote Desktop

- jetPACK-5.5.5.1-Remote-Desktop

DICOM – Digital Imaging and Communications in Medicine

- jetPACK-6.6.6.1-DICOM

Oracle – E-Business Suite

SSL Offload

- jetPACK-7.7.7..1-Oracle-EBS

VMware Horizon View

Connection Servers – SSL Offload

- jetPACK-8.8.8.1-View-SSL-Offload

Security Servers – SSL Re-Encryption

- jetPACK-8.8.8.2-View-SSL-Re-encryption

Global Settings

- GUI Secure Port 443 – this jetPACK will change you secure GUI port from 27376 to 443. https://x.x.x.x
- GUI Timeout 1 day – the GUI will request you to input your password every 20 minutes. This will increase that request to 1 day
- ARP Refresh 10 – during a failover between HA appliances this will increase the number of **Gratuitous ARP's** to assist the switches during the transition
- Capture Size 16MB – the default capture size is 2MB. This will increase the size to a maximum of 16MB

Cipher Options

- Strong Ciphers – This will add the ability to choose "Strong Ciphers" from the Cipher options list:
  - Cipher = ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5
- Anti-Beast – This will add the ability to choose "Anti Beast" from the Cipher Options list:
  - Cipher = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
- No SSLv3 – This will add the ability to choose "No SSLv3" from the Cipher Options list:
  - Cipher = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- No SSLv3 no TLSv1 No RC4 – This will add the ability to choose "No-TLSv1 No-SSLv3 No-RC4" from the Cipher Options list:
  - Cipher = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- NO_TLSv1.1 –This will add the ability to choose "NO_TLSv1.1" from the Cipher Options list: Cipher= ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128: DH+AES:RSA+AESGCM:RSA+AES:HIGH:!3DES:!aNULL:!MD5:!DSS:!MD5:!aNULL:!EDH:!RC4

flightPATHs

- X-Content-Type-Options – add this header if it doesn't exist and set it to "nosniff" – prevents the browser from automatically "MIME-Sniffing".
- X-Frame-Options – add this header if it doesn't exist and set it to "SAMEORIGIN" – pages on your website can be included in Frames, but only on other pages within the same website.
- X-XSS-Protection – add this header if it doesn't exist and set it to "1; mode=block" – enable browser cross site scripting protections
- Strict-Transport-Security – add header if it doesn't exist and set it to "max-age=31536000 ; includeSubdomains" – ensures client should honor that all links should be https:// for the max-age

Apply a jetPACK

You can apply any jetPACK in any order but be careful not to apply a jetPACK with the same Virtual IP address. This will cause a duplicate IP address in the configuration. If you do this by mistake you can change this in the GUI. Navigate to **Advanced->Update Software**

- Configuration Section
- Upload New Configuration or jetPACK
- Browse for jetPACK
- Click Upload
- Once the browser screen turns white please click refresh and wait for the Dashboard page to appear

Create a jetPACK

One of the great things about jetPACKs is that you can create your own. It may be that you have created the perfect config for an application and want to blast this to several other boxes independently.

- Start by copying the current configuration from your existing ALB-X
    - Advanced
    - Update Software
    - Download Current Configuration

    - **Click Hear** to download the ALB-X.conf file
- Edit this file with Notepad++
- Open up a new txt document and call it “yourname-jetPACK1.txt”
- Copy all the relevant sections from the config file to “yourname-jetPACK1.txt”
- Save once complete

IMPORTANT: Each jetPACK is split into different sections but all jetPACKs **must** have #!jetpack at the top of the page. The sections that are recommended for editing/copying are listed below.

Section 0:

#!jetpack

This needs to be at the top of the jetPACK or your current configuration will be over written.

Section1:

[jetnexusdaemon]

This section contains global settings that once changed will apply to all services. Some of these settings can be changed from the web console but others are only available here.

Examples:

ConnectionTimeout=600000

This is the tcp timeout value in milliseconds. This particular setting means that a tcp connection will be closed after 10 minutes of inactivity

ContentServerCustomTimer=20000

This is delay in milliseconds between content server health checks for custom monitors such as DICOM

jnCookieHeader=”MS-WSMAN”

This will change the name of the cookie header used in persistent load balancing from the default “jnAccel” to “MS-WSMAN”. This particular change is needed for Lync 2010/2013 reverse proxy.

Section 2:

[jetnexusdaemon-Csm-Rules]

This section contains the custom server monitoring rules that are normally configured from the web console here.

Example:

[jetnexusdaemon-Csm-Rules-0]
Content=”Server Up”
Desc=”Monitor 1″
Method=”CheckResponse”
Name=”Health Check- Is Server Up”
Url=”http://demo.jetneus.com/healthcheck/healthcheck.html”

Section 3:

[jetnexusdaemon-LocalInterface]

This section contains all of the details in the IP Services section. Each interface is numbered and contains subinterfaces for each channel. If your channel has a flightPATH rule applied then it will also contain a Path section too.

Example:

[jetnexusdaemon-LocalInterface1]
1.1=”443″
1.2=”104″
1.3=”80″
1.4=”81″
Enabled=1
Netmask=”255.255.255.0″
PrimaryV2=”{A28B2C99-1FFC-4A7C-AAD9-A55C32A9E913}”
[jetnexusdaemon-LocalInterface1.1]
1=”>,””Secure Group””,2000,”
2=”192.168.101.11:80,Y,””IIS WWW Server 1″””
3=”192.168.101.12:80,Y,””IIS WWW Server 2″””
AddressResolution=0
CachePort=0
CertificateName=”default”
ClientCertificateName=”No SSL”
Compress=1
ConnectionLimiting=0
DSR=0
DSRProto=”tcp”
Enabled=1
LoadBalancePolicy=”CookieBased”
MaxConnections=10000
MonitoringPolicy=”1″
PassThrough=0
Protocol=”Accelerate HTTP”
ServiceDesc=”Secure Servers VIP”
SNAT=0
SSL=1
SSLClient=0
SSLInternalPort=27400
[jetnexusdaemon-LocalInterface1.1-Path]
1=”6″

Section 4:

[jetnexusdaemon-Path]

This section contains all of the flightPATH rules. It is important that the numbers match what has been applied to the interface. In the example above we see that flightPATH rule “6” has been applied to the channel so we will include this as an

example below.

Example:

[jetnexusdaemon-Path-6]
Desc=”Force to use HTTPS for certain directory”
Name=”Gary – Force HTTPS”
[jetnexusdaemon-Path-6-Condition-1]
Check=”contain”
Condition=”path”
Match=
Sense=”does”
Value=”/secure/”
[jetnexusdaemon-Path-6-Evaluate-1]
Detail=
Source=”host”
Value=
Variable=”$host$”[jetnexusdaemon-Path-6-Function-1]
Action=”redirect”
Target=”https://$host$$path$$querystring$”
Value=