

---

EDGE  
NEXUS

---

SOFTWARE VERSION  
5.0.0

# EdgeADC

EdgeADC Administration Guide

## Contents

Document Properties.....	12
Document Disclaimer.....	12
Copyrights.....	12
Trademarks.....	12
Edgenexus Support .....	12
Introduction.....	13
The purpose of this document.....	13
For whom is this document intended? .....	13
Load Balancing 101 .....	14
What is a Load Balancer or ADC? .....	15
VIPs and Virtual Services (VS) explained.....	16
What is a Load Balancing Service Type? .....	18
The Start of the Journey .....	20
Downloading the EdgeADC .....	21
Installation .....	22
Installing the EdgeADC.....	23
Installing onto VMware ESXi .....	23
Installing the VMXNET3 Interface.....	23
Installing on Microsoft Hyper-V .....	24
Installing on Citrix XenServer .....	25
Installing on KVM .....	26
Requirements and Versions .....	26
Installing on Nutanix AHV .....	29
Requirements and Versions .....	29
Installing on ProxMox.....	30
Uploading the OVA to ProxMox.....	30
First Boot Configuration.....	33
First Boot – Manual Network Details .....	33
First Boot – DHCP successful .....	33
First Boot – DHCP Fails .....	33
Changing the Management IP Address.....	34
Changing the Subnet Mask for eth0 .....	34
Assigning a Default Gateway .....	34
Checking the Default Gateway value .....	34
Accessing the web interface.....	34
Command Reference Table.....	35

The Web Console.....	36
Launching the ADC Web Console .....	37
Default Login Credentials.....	37
Using an External Authentication Service.....	37
The Main Dashboard.....	38
Services .....	39
IP Services .....	40
Virtual Services.....	40
Creating a new Virtual Service using a new VIP.....	40
Example of a completed Virtual service.....	41
How to use Monitor End Point .....	42
Creating Sub Virtual Services .....	42
Changing the IP Address of a Virtual Service.....	43
Creating a new Virtual Service using Copy Service.....	43
Filtering displayed data .....	44
Searching for a specific term .....	44
Selecting column visibility .....	44
Understanding the Virtual Services columns.....	44
Primary/Mode.....	44
VIP .....	44
Enabled .....	45
IP Address.....	45
Subnet Mask/Prefix .....	45
Port .....	45
Service Name.....	45
Service Type .....	45
Real Servers .....	46
Server.....	46
Basic .....	49
Advanced .....	54
flightPATH .....	58
Real Server Changes for Direct Server Return .....	60
Required Content Server Configuration .....	60
General .....	60
Windows.....	60
Linux.....	61
Real Server Changes – Gateway Mode.....	62
Required Content Server Configuration .....	62

Single Arm example .....	62
Dual Arm example .....	63
Library .....	64
Add-Ons .....	65
Apps .....	66
The Filter .....	66
Downloaded Apps .....	66
Purchased App .....	66
Deploy .....	67
Download App .....	67
Delete .....	67
Authentication .....	68
Setting up Authentication – A Workflow .....	68
Authentication Servers .....	68
Options for LDAP, LDAP-MD5, LSAPS, LDAPS-MD5, Radius and SAML .....	68
Options for SAML Authentication .....	69
KDC Realms .....	71
Authentication Rules .....	71
Forms .....	72
Cache .....	74
Global Cache Settings .....	74
Apply Cache Rule .....	75
Create Cache Rule .....	75
flightPATH .....	77
Details .....	77
Adding a new flightPATH rule .....	77
Condition .....	78
Evaluation .....	81
Action .....	82
A flightPATH rule scenario .....	84
Applying the flightPATH rule .....	85
Real Server Monitors .....	86
Types of Real Server Monitors .....	86
Details .....	89
Real Server Monitor examples .....	91
SSL Certificates .....	94
What does the ADC do with the SSL Certificate? .....	94
The SSL Configuration Manager .....	94

The Certificate Listing Area .....	94
The Action Buttons & Configuration Areas.....	95
Overview .....	96
Create Request .....	96
Rename.....	98
Delete.....	98
Install/Sign.....	99
Renew .....	99
Validate Certificate .....	100
Adding Intermediates.....	100
Reorder .....	101
Import/Export.....	102
Backup & Restore .....	103
Backup .....	103
Restore.....	103
Widgets .....	104
Configured Widgets .....	104
Available Widgets .....	104
The Events Widget .....	104
The System Graphs Widget.....	105
Interface Widget .....	106
Status Widget .....	106
Traffic Graphics Widget .....	106
View .....	109
Dashboard.....	110
Dashboard Usage .....	110
The Widgets Menu .....	110
Pause Live Data Button .....	110
Default Dashboard Button .....	110
Resizing, minimizing, re-ordering, and removing widgets .....	111
History .....	112
Viewing Graphical Data .....	112
Logs .....	114
W3C Logs .....	114
System Log .....	114
Statistics.....	115
Compression.....	115
Content Compression to Date .....	115

Overall Compression to Date.....	115
Total Input/Output.....	115
Hits and Connections.....	115
Overall Hits Counted .....	116
Total Connections.....	116
Peak Connections .....	116
Caching.....	116
From Cache.....	116
From Server .....	116
Cache Contents.....	116
Application Buffer.....	116
Session Persistence .....	117
Total current sessions .....	117
% Used (of max).....	117
New session this min.....	117
Revalidate this min .....	117
Expired sessions this min .....	117
Hardware .....	117
Disk Usage.....	117
Memory Usage.....	117
CPU Usage .....	118
Status.....	119
Virtual Service Details.....	119
VIP Column .....	119
VS Status Column .....	119
Name.....	119
Virtual Service (VIP) .....	120
Hit/Sec.....	120
Cache%.....	120
Compression% .....	120
RS Status (Remote Server) .....	120
Real Server .....	120
Notes.....	120
Conns (Connections).....	120
Data .....	120
Req/Sec (Requests per second).....	120
System .....	121
Clustering .....	122

Role .....	122
Cluster.....	122
Manual Role .....	124
Stand-alone Role.....	124
Settings.....	125
Failover Latency (ms) .....	125
Failover Messaging .....	125
Management.....	125
Adding an ADC to the cluster .....	126
Manually adding an ADC to the cluster.....	126
Removing a cluster member .....	127
Changing the priority of an ADC .....	127
Date and Time .....	129
Manual Date and Time.....	129
Time Zone .....	129
Set Date and Time.....	129
Synchronize Date and Time (UTC) .....	129
Time Server URL.....	130
Update at [hh:mm].....	130
Update Period [hours]:.....	130
NTP Type: .....	130
Email Events .....	131
Address.....	131
Send to Email Events to Email Addresses.....	131
Return Email Address:.....	131
Mail Server (SMTP) .....	131
Host address .....	131
Port .....	131
Send Timeout.....	131
Use Authentication .....	132
Security .....	132
Main Server Account Name.....	132
Mail Server Password.....	132
Notifications and Alerts .....	132
IP Service Notice.....	132
Virtual Service Notice .....	132
Real Server Notice .....	132
flightPATH.....	132

Group Notifications Together .....	132
Group Mail Description .....	133
Group Send interval.....	133
Enabled Warnings and Event Descriptions in Mail .....	133
Disk Space .....	133
Warn if Free Space Less Than .....	133
Licence Expiry .....	133
History .....	134
Collect Data .....	134
Enable .....	134
Collect Data Every.....	134
Maintenance .....	134
Most Recent Update.....	134
HP Enterprise Based ADCs .....	134
Backup .....	134
Delete.....	134
Restore.....	135
License .....	136
License Details.....	136
License ID .....	136
Machine ID .....	136
Issued To .....	136
Contact Person.....	136
Date Issued .....	136
Name.....	137
Facilities.....	137
Install License .....	137
License Service Information .....	138
Logging .....	139
W3C Logging Details .....	139
W3C Logging Levels .....	139
Include W3C Logging .....	140
Include Security Information .....	140
Syslog Server .....	140
Remote Syslog Server .....	141
Remote Log Storage.....	141
Field Summary .....	141
Clear Log Files.....	143



Network .....	144
Managing Virtual Network Interfaces in a Virtual Environment .....	144
Key Considerations .....	144
Recommended Steps for Host Configuration .....	144
Example Scenario .....	144
Avoiding Frequent vMotion for Critical Appliances .....	145
Why Frequent vMotion is Not Recommended .....	145
Recommendations for Managing Critical Appliances .....	145
Basic Setup .....	146
ALB Name .....	146
IPv4 Gateway .....	146
IPv6 Gateway .....	146
DNS Server 1 & DNS Server 2 .....	146
Adapter Details .....	146
Interfaces .....	147
Bonding .....	147
Creating a Bonding profile .....	148
Bonding Modes .....	148
Static Route .....	149
Adding a Static Route .....	149
Static Route Details .....	149
Advanced Network Settings .....	149
What is Nagle? .....	149
Server Nagle .....	150
Client Nagle .....	150
SNAT .....	150
Power .....	151
Restart .....	151
Reboot .....	151
Power Off .....	151
Security .....	152
SSH .....	152
Authentication Service .....	152
Web Console .....	152
REST API .....	153
Documentation for REST API .....	153
SNMP .....	154
SNMP Settings .....	154

SNMP MIB .....	154
MIB Download .....	154
ADC OID .....	154
Historical Graphing .....	155
Users and Audit Logs .....	156
Users .....	156
Add User .....	156
User Type.....	157
Removing a User.....	157
Editing a User.....	158
Audit Log.....	158
Advanced .....	159
Configuration .....	160
Downloading a configuration .....	160
Uploading a configuration .....	160
Upload a JetPACK.....	160
Global Settings .....	161
App Store Download Proxy .....	161
HTTP Proxy URL.....	161
HTTP Proxy Username.....	161
HTTP Proxy Password .....	161
Host Cache Timer .....	161
Drain .....	162
SSL.....	162
Authentication .....	163
Failover Setting .....	163
Protocol.....	164
Server too Busy .....	164
Forwarded For .....	164
Forwarded-For Output .....	164
Forwarded-For Header .....	164
Advanced Logging for IIS – Custom Logging.....	164
Apache HTTPd.conf changes.....	165
HTTP Compression Settings.....	165
Global Compression Exclusions.....	166
Persistence Cookies .....	167
UDP Timeout Reset .....	167
Software .....	168

Software Upgrade Details .....	168
Download from Cloud.....	168
Upload Software .....	169
Apps Upload.....	169
Software/Firmware Updates .....	169
Apply Software stored on ADC.....	169
Troubleshooting.....	171
Support Files.....	171
Trace .....	171
Ping .....	172
Capture.....	173
Help.....	174
About us.....	174
Reference .....	174
JetPACKs.....	175
Edgenexus jetPACKs .....	176
Downloading a jetPACK.....	176
Microsoft Exchange .....	176
Microsoft Lync 2010/2013.....	177
Web Services .....	177
Microsoft Remote Desktop .....	177
DICOM – Digital Imaging and Communication in Medicine.....	177
Oracle e-Business Suite .....	178
VMware Horizon View .....	178
Global settings .....	178
Ciphers and Cipher jetPACKs .....	178
Strong Ciphers .....	178
Anti-Beast.....	178
No SSLv3 .....	178
No SSLv3 no TLSv1 No RC4 .....	178
NO_TLSv1.1.....	178
Enable TLS-1.0-1.1 Ciphers .....	179
Example Cipher jetPACK .....	179
Applying a jetPACK.....	179
Creating a jetPACK .....	179
flightPATH.....	183
Introduction to flightPATH.....	184
What is flightPATH?.....	184

What can flightPATH do? .....	184
Condition.....	184
Match.....	185
Check .....	186
Example .....	187
Evaluation .....	187
Action.....	189
Action .....	189
Target.....	189
Data .....	190
Common Uses .....	191
Application Firewall and Security .....	191
Features .....	191
Pre-Built Rules.....	192
HTML Extension.....	192
Index.html.....	192
Close Folders .....	192
Hide CGI-BBIN:.....	193
Log Spider .....	193
Force HTTPS .....	193
Media Stream:.....	194
Swap HTTP to HTTPS .....	194
Blank out Credit Cards .....	194
Content Expiry.....	195
Spoof Server Type.....	195
SAML and Entra ID.....	198
Setting up the Entra ID Authentication Application in Microsoft Entra .....	199
Technical Support.....	202

## Document Properties

---

Document Number: 2.0.3.18.25.15.03

Document Creation Date: 18 March 2025

Document Last Edited: 18 March 2025

Document Author: Jay Savoor

Document Last Edited by:

Document: EdgeADC - Version 5.0.0

## Document Disclaimer

---

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

## Copyrights

---

© 2025 All rights reserved.

Information in this document is subject to change without prior notice and does not represent a commitment on the manufacturer's part. No part of this guide may be reproduced or transmitted in any form or means, electronic or mechanical, including photocopying and recording, for any purpose, without the express written permission of the manufacturer. Registered trademarks are properties of their respective owners. Every effort is made to make this guide as complete and as accurate as possible, but no warranty of fitness is implied. The authors and the publisher shall have neither responsibility nor liability to any person or entity for loss or damages arising from using the information contained in this guide.

## Trademarks

---

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

## Edgenexus Support

---

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

## Introduction

---

You are reading this guide because you intend to deploy the Edgenexus EdgeADC and load-balance your server-based applications efficiently and cost-effectively.

The EdgeADC is built around a highly secure engine that offers high scalability, security, high performance, and a very easy-to-use management interface. These factors ensure that what you deploy will deliver the best cost of ownership possible.

### The purpose of this document

---

This document has been written so that you can administer the EdgeADC using its easy web-based interface. Functions and their configurations are described in detail, and we hope that this will be enough for you to configure the EdgeADC for your requirements.

### For whom is this document intended?

---

This document is intended for persons with networking knowledge, particularly protocols, applications, and servers.

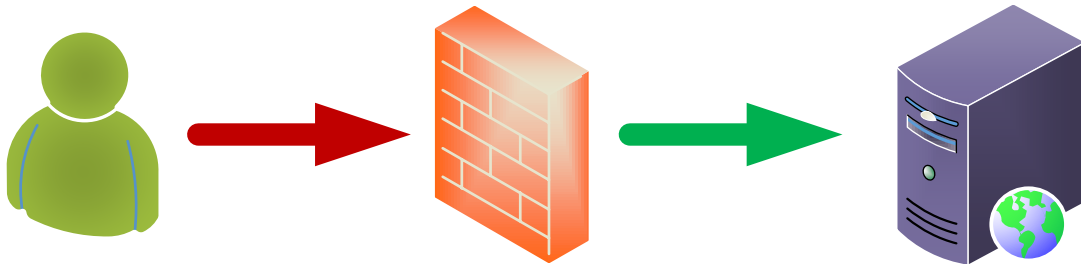
# Load Balancing 101

## What is a Load Balancer or ADC?

Load balancers have evolved massively and have much more intelligence built into their engines than earlier. They are often referred to as application delivery controllers or ADCs today.

Before we can understand what a load balancer or ADC is, we need to recognize the IT person and user's problems. So, let's take an example.

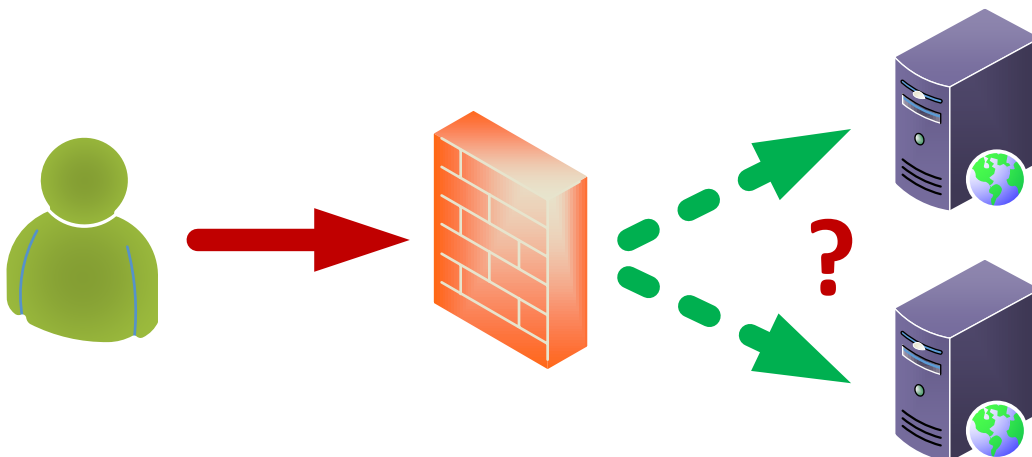
- A company has a web application that it is publishing to the Internet. The application is hosted on a single web server, with data residing on a separate database server.



**User Client**

**Application Servers**

- This server uses the IP address of 1.2.3.4 as an example.
- The number of clients accessing the application is regularly increasing, and some have pointed out that the application performance is decreasing.
- Analysis of the server shows that the traffic hitting the server has increased massively and continues to progress upward.
- So the decision is taken to add another server to host the application.
- The new second server uses the IP address of 1.2.3.5.
- The problem is how to direct the client to the new and current server to share the load and ensure that the user's session is maintained on the first logged-on server.



**User Client**

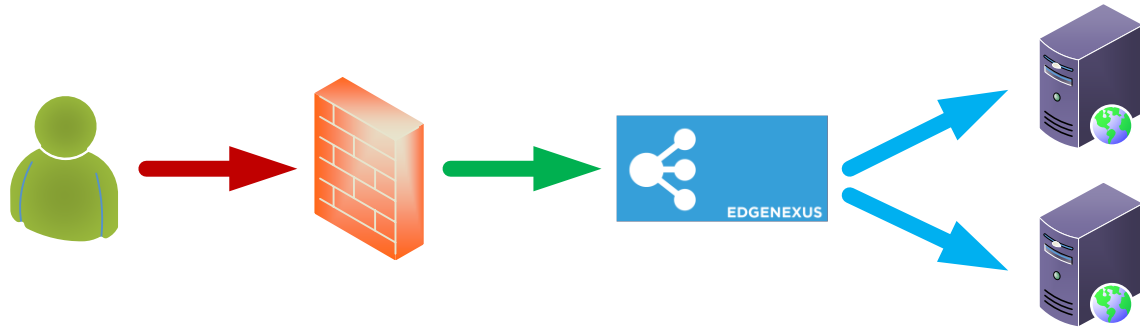
**Application Servers**

- The answer is a load balancer or ADC.

Now the solution.



- We place an ADC in front of the two application servers.



User Client

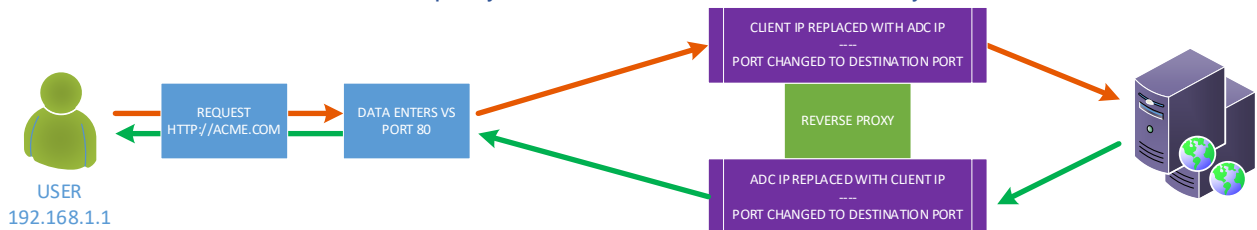
ADC

Application Servers

- The ADC will have an external-facing IP of 1.2.3.6, and the firewall will NAT redirect the requests to this address instead of the earlier 1.2.3.4
- The ADC's IP to receive the requests is called the VIP, and the configuration is called the Virtual Service.
- The ADC will receive the requests from the client users and reverse proxy them to the real servers using load balance policies while monitoring the health of the application servers to ensure efficiency.



- The ADC balances traffic to the servers based on the load balancing policy in use, the nature of the load together with the status of the application servers.
- Traffic from the servers will be sent back to the client through the ADC in the opposite direction.
- Because of the nature of the reverse proxy, the server and the client are anonymous to each other.



- The reverse proxy technology ensures the optimum level of security.

## VIPs and Virtual Services (VS) explained

A VIP is, in essence, an IP address defined for use on the EdgeADC and allows users to access the services tied to it. That is pretty much what a VIP is. Because of how the EdgeADC works, the VIP need not be in the same subnet as the Real Servers, and this network address translation methodology makes the technology very secure from hackers attempting to access the internal servers.

Note: The IP address of the VIP cannot be the same as the IP address used for the Management IP.

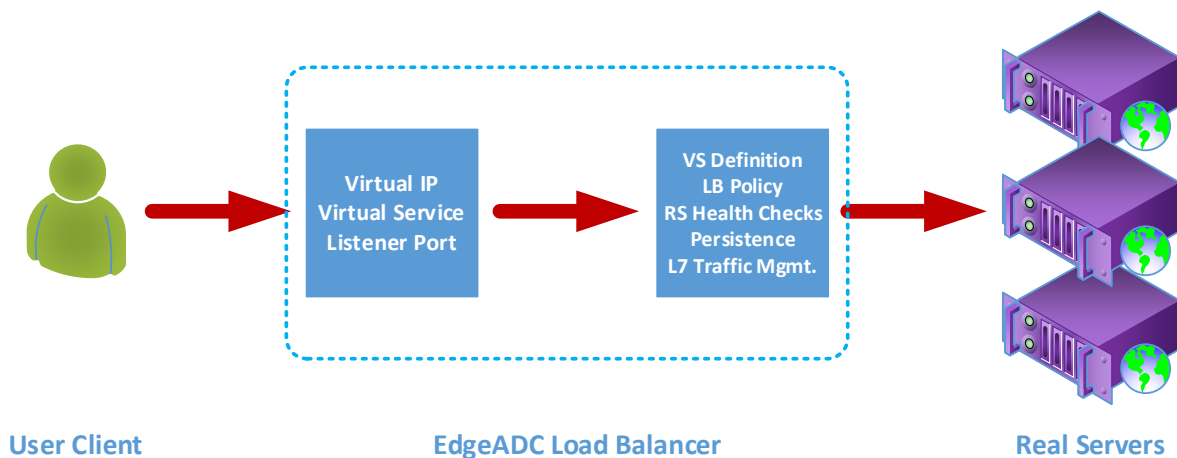
Virtual services form the core of the EdgeADC proxying and load-balancing technologies. The Virtual IP is the address through which the VS is advertised to the network and the world, listening for traffic and requests from clients who wish to use the applications it services.

When clients hit the VS, the VS will be configured to perform numerous actions on the traffic, including but not limited to:

- Proxy of the client's connection
- Specific functions are carried out such as compression, acceleration, load balancing, traffic inspection, etc.
- Forward the client's requests to destination servers defined within the load balancing policies of the virtual service.

You could think of the VS as married to an IP address (VIP) that the EdgeADC is listening on in preparation for data requests. When standard TCP or HTTP configurations are made, the client will connect to the VIP, and the EdgeADC will process the request as per the definition that makes up the VS. Once this is done, the EdgeADC will send the traffic onto the Real Servers specified.

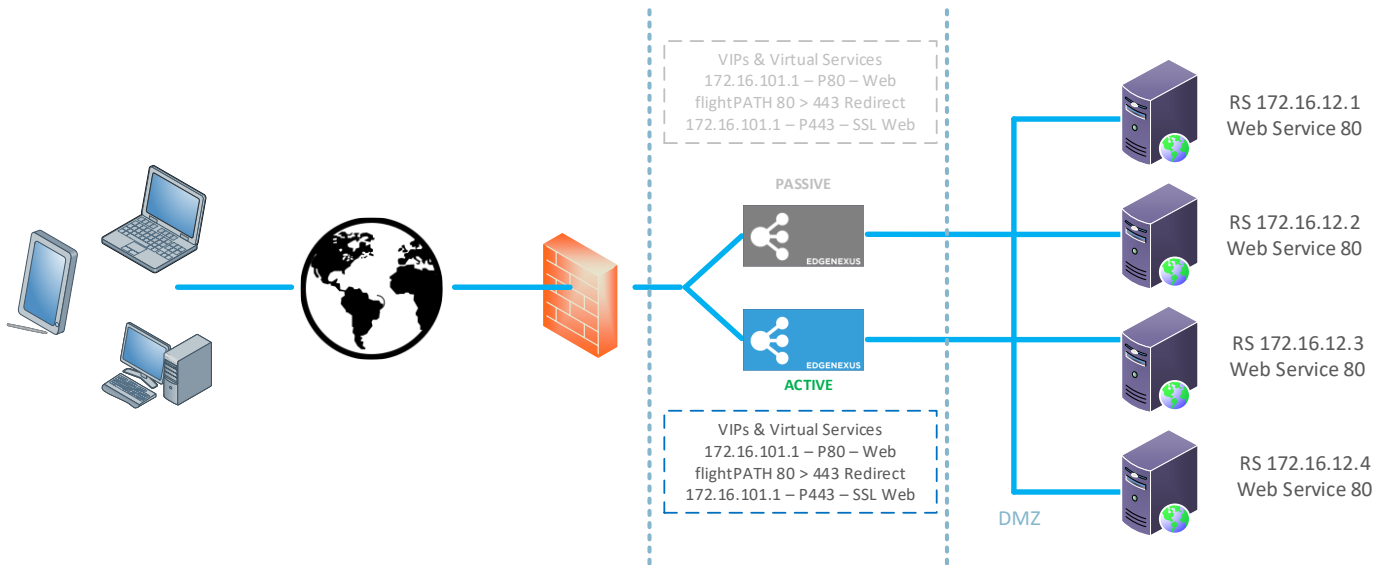
The VS receives the connection and data in a typical configuration and then terminates or proxies using the reverse proxy engine within the EdgeADC. The EdgeADC then proceeds to open a new connection to the Real Servers and sends the data onward. When the Real Servers respond to the request, the EdgeADC will then send the response to the client using a similar reverse path, this depending on the settings made in the Connectivity option within the Real Servers Load Balancing tab.



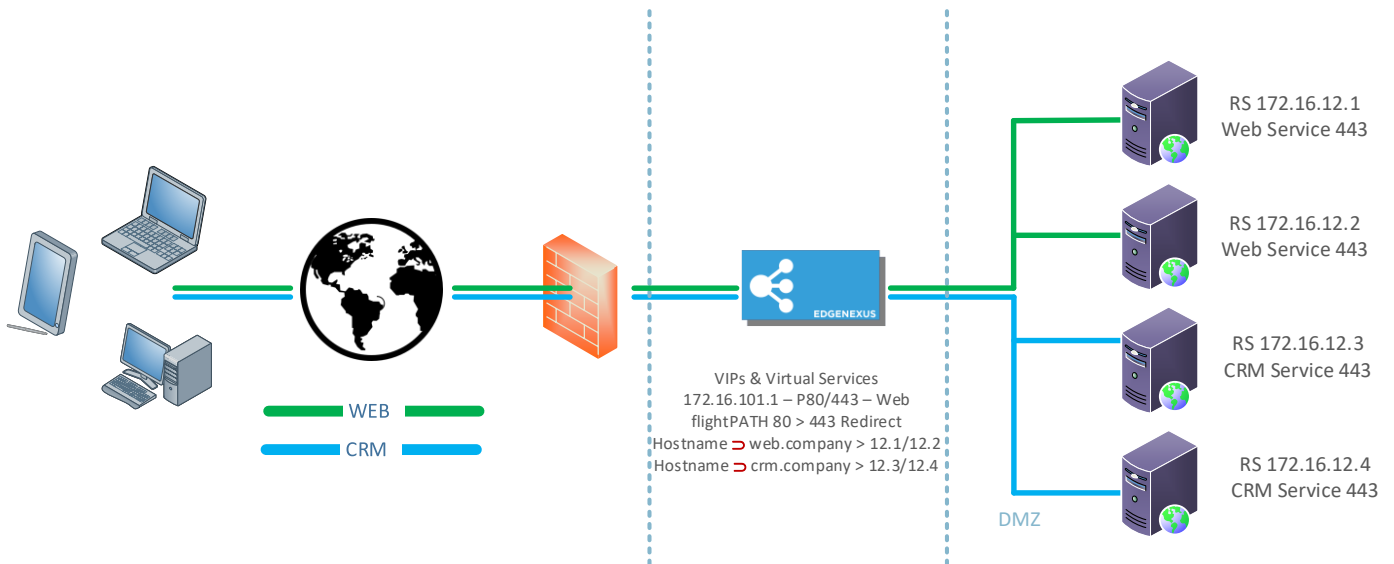
A Virtual Service definition comprises a single IP address (VIP) and a collection of ports that serve as ingress points to different services, using a variety of protocols.

For example, you need to load-balance a series of web servers to provide resilience. Now let us assume that these systems will be accessed using HTTPS secured communications using <https://myweb.company.com>.

Should one look at the definition of such a configuration, it will comprise of a single VIP with two entries, one for port 80 and the other for port 443. The port 80 VIP will have a flightPATH rule attached that will force-convert the traffic to HTTPS. The second entry for port 443 will then send the traffic onto the Real Servers defined under it. Similarly, you could have other services under the same VIP to load balance traffic to mail servers or other application servers.



With lesser functional ADCs, services that use the same ports would need different VIPs, but the ADC and its flightPATH system allow you to use a single VIP with multiple services that use the same ports. So, you could have two applications, both accessed using 443 with different hostnames, using a single VIP. An example is illustrated below.



The EdgeADC's systems are extremely flexible and allow for very complex and functional configurations to be defined.

### What is a Load Balancing Service Type?

Load balancing service types consist of algorithms and methodologies used to distribute intelligently or load balance the traffic across pools of servers. The method and algorithm that the ADC makes available will depend on the service type or application used on the servers being load-balanced, and it will also depend on the state of the network and servers in use. It should be noted that the load balancing service type that you select to use also depends on the level of traffic being sent through the ADC. So when the traffic throughput or load is low, the load balancing service types can be simple ones. But when the loads are greater, you may need to elect more complex types to attain the more efficient load distribution to the back-end servers.

The following load balancing service types are available within the EdgeADC.

DICOM	LAYER 4 UDP	RPC
FTP	LAYER 4 TCP/UDP	RPC/ADS
HTTP(S)	DNS	RPC/CA/PF
IMAP	POP3	SMTP
LAYER 4 TCP	RDP	GSLB

# The Start of the Journey

## Downloading the EdgeADC

Before installation, the first step is to download the EdgeADC that is suitable for your environment.

We provide editions for most virtualized environments and an ISO edition when installing directly on bare-metal hardware.

Step one is to fill out the evaluation form located on the Edgenexus website, located at <https://www.edgenexus.io/products/load-balancer/free-trial/>.

The screenshot shows the Edgenexus website's 'Request a Free Trial' form. The form is titled 'Request a Free Trial' and includes the subtext '(Downloaded or cloud provisioned)'. It contains the following fields: 'First name', 'Last name', 'Email\*', and 'Company name'. Below these fields is a reCAPTCHA widget with a 'protected by reCAPTCHA' label and a 'Submit' button. The background of the form area features a blue gradient with white paper airplanes and the text 'The Easy choice for Load balancing' and 'Fast, Scalable and Secure Applications'. A 'Why Edgenexus?' button is also visible. At the bottom of the page, there are logos for Exchange, SharePoint, Microsoft Dynamics, ORACLE, Skype for Business, and VMware Horizon View, along with the text 'Your Load Balancing Experts' and a chat icon.

The process is simple, and upon filling the form and submitting it, you will be taken to the download page, where you can select the correct image for your environment.

EdgeADC editions are available for the following virtualization systems:

- VMware ESX
- Microsoft Hyper-V
- Citrix XenServer
- Nutanix
- KVM

You can also opt to test-drive in the Cloud using Microsoft Azure or Amazon AWS marketplace editions.

If you choose to download the software for an on-premise installation, you will receive the EdgeADC with an in-built 14-day trial license. We would recommend that you contact [sales@edgenexus.io](mailto:sales@edgenexus.io) and request a 30-day licence key with all features enabled.

# Installation

## Installing the EdgeADC

The EdgeADC (ADC) is available for installation on a variety of platform targets, each requiring its installer, and these are made available to you once you have registered to download.

These are the various installation models available.

- VMware ESXi
- KVM
- Citrix Xen
- Nutanix AHV
- Microsoft Hyper-V
- Oracle VM
- Proxmox (Use OVA)
- ISO for BareMetal hardware

The sizing of the virtual machine you will use to host the ADC depends on the use case scenario and the data throughput.

### Installing onto VMware ESXi

The ADC is supported for installation on VMware ESXi are 5.x and above.

- Download the latest installation OVA package of ADC using the appropriate link provided with the download email.
- Once downloaded, please unzip in a suitable directory on your ESXi host or SAN.
- In your vSphere client, select File: Deploy OVA/OVF Template.
- Browse and select the location where you have saved your files; choose the OVF file and click **NEXT**
- The ESX server requests the appliance name. Type a suitable name and click **NEXT**
- Select the datastore from where your ADC appliance will run.
- Select a datastore with enough space and click **NEXT**
- You then will be told information about the product; click **NEXT**
- Click **NEXT**.
- Once you have copied the files to the datastore, you can install the virtual appliance.

Launch your vSphere client to see the new ADC virtual appliance.

- Right-click on the VA and go to Power > Power-On
- Your VA will then boot, and the ADC boot screen will show on the console.

```
Checking for management interface ..... [ OK ]  
  
Management interface: eth0  MAC: 00:0c:29:05:2e:1a  
  
1. Enter networking details manually  
2. Configure networking setting automatically via DHCP
```

### Installing the VMXNET3 Interface

The VMXnet3 driver is supported, but you will need to make changes to the NIC settings first.



**Note – Do NOT upgrade the VMware-tools**

### Enabling the VMXNET3 interface on a freshly imported VA (never started)

1. Delete both NICs from the VM
2. Upgrade the VM hardware – -Right-click on the VA in the list and select Upgrade Virtual Hardware (do not start a VMware tools installation or update, **only** perform the hardware upgrade)
3. Add two NICs and selected them to be VMXNET3
4. Start the VA using the standard method. It will work with the VMXNET3

### Enabling VMXNET3 interface on an already running VA

1. Stop the VM (CLI shutdown command or GUI power-off)
2. Get the MAC addresses of both NICs (**remember the order of the NICs in the list!**)
3. Delete both NICs from the VM
4. Upgrade the VM hardware (do not start a VMware tools installation or update, **only** perform the hardware upgrade)
5. Add two NICs and select them to be VMXNET3
6. Set the MAC addresses for the new NICs accordingly to step 2
7. Restart the VA

We support VMware ESXi as the production platform. For evaluation purposes, you can use VMware Workstation and Player.

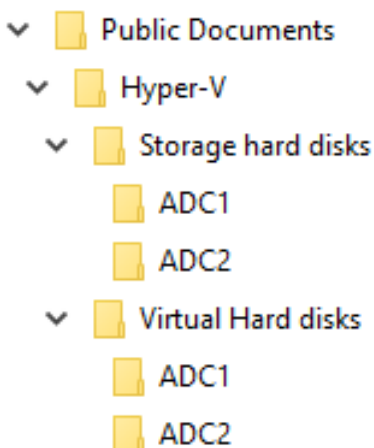
Please refer to the section **FIRST BOOT CONFIGURATION** to proceed further.

## Installing on Microsoft Hyper-V

The Edgenexus ADC Virtual appliance can be easily installed within a Microsoft Hyper-V virtualization framework. This guide assumes you have correctly specified and configured your Hyper-V system and system resources to accommodate the ADC and its load balancing architecture.

**Note each appliance requires a unique MAC address.**

- Extract the downloaded Hyper-V compatible ADC-VA file to your local machine or server.
- Open Hyper-V Manager.
- Create a new folder to contain the ADC VA 'Virtual hard disk' and another new folder to contain the 'Storage hard disk,' e.g., C:\Users\Public\Documents\Hyper-V\Virtual hard disks\ADC1 and C:\Users\Public\Documents\Hyper-V\Storage hard disks\ADC1
- **Note:** New ADC specific subfolders for the Virtual hard disks\ and Storage hard disks\ need to be created for each virtual ADC instance installation, as shown below:



- Copy the extracted EdgeADC .vhd file to the 'Storage hard disk' folder created above.
- In your Hyper-V Manager client, right-click on the server and select "Import Virtual Machine"
- Browse to the folder containing the downloaded ADC VA image file extracted earlier
- Select Virtual Machine - highlight the virtual machine to import and click Next
- Select Virtual Machine - highlight the virtual machine to import and click Next
- Choose Import Type - select "**Copy the virtual machine (create a new unique ID)**" click next
- Choose Folders for Virtual Machine Files - the Destination can be left as the Hyper-V default or you can choose to select a different location
- Locate Virtual Hard Disks – browse to and select the virtual hard disks folder created above and click next
- Choose Folders to Store Virtual Hard Disks – browse to and select the Storage hard disks folder created previously and click next
- Verify the details in the Completing Import Wizard Summary window are correct and click Finish
- Right-click on the newly imported **ADC** virtual machine and select Start

**NOTE: AS PER [HTTP://SUPPORT.MICROSOFT.COM/KB/2956569](http://support.microsoft.com/kb/2956569) YOU SHOULD IGNORE THE “DEGRADED (INTEGRATION SERVICES UPGRADE REQUIRED)” STATUS MESSAGE, WHICH MAY BE DISPLAYED AS BELOW AFTER THE VA IS STARTED. NO ACTION IS REQUIRED, AND THE SERVICE IS NOT DEGRADED**

- While the VM is initializing, you can right-click on the VM entry and select Connect...You will then be presented with the EdgeADC console.

```
Checking for management interface ..... [ OK ]  
  
Management interface: eth0   MAC: 88:8c:29:85:2e:1a  
  
1. Enter networking details manually  
2. Configure networking setting automatically via DHCP
```

- Once you configure the network properties, the VA will reboot and present the logon to the VA console.

Please refer to the section **FIRST BOOT CONFIGURATION** to proceed further.

## Installing on Citrix XenServer

The ADC Virtual appliance is installable on Citrix XenServer.

- Extract the ADC OVA ALB-VA file to your local machine or server.
- Open Citrix XenCenter Client.
- In your XenCenter client, select "**File: Import.**"
- Browse to, and select the **OVA** file, then click "**Open Next.**"
- Select the VM creation location when asked.
- Choose which XenServer you wish to install and click "**NEXT.**"
- Select the storage repository (SR) for virtual disk placement when asked.
- Select an SR with enough space and click "**NEXT.**"
- Map your virtual network interfaces. Both interfaces will say Eth0; however, note that the bottom interface is Eth1.
- Select the target network for each interface and click **NEXT**
- **DO NOT** tick the "Use Operating System Fixup."
- Click "**NEXT**"

- Choose the network interface to use for the temporary transfer VM.
- Choose the Management interface, usually Network 0, and leave the network settings on DHCP. Please be aware that you must assign static IP address details if you do not have a working DHCP server for the transfer. Failure to do this will result in the import saying Connecting continuously then failed. Click "**NEXT**"
- Review all the information and check the correct settings then. Click "**FINISH.**"
- Your VM will begin transferring virtual disk "ADC" and, once complete, will show under your XenServer.
- Within your XenCenter client, you will now be able to see the new virtual machine. Right-click on the VA and click "**START.**"
- Your VM will then boot, and the ADC boot screen will show.

```
Checking for management interface ..... [ OK ]  
  
Management interface: eth0  MAC: 00:0c:29:05:2e:1a  
  
1. Enter networking details manually  
2. Configure networking setting automatically via DHCP
```

- Once configured, the logon to the VA presents itself.

Please refer to the section **FIRST BOOT CONFIGURATION** to proceed further.

## Installing on KVM

The following section shows how to install the EdgeADC onto a KVM platform. The KVM platform used for this exercise ran on a CentOS v8 operating system with Cockpit and virtualization installed.

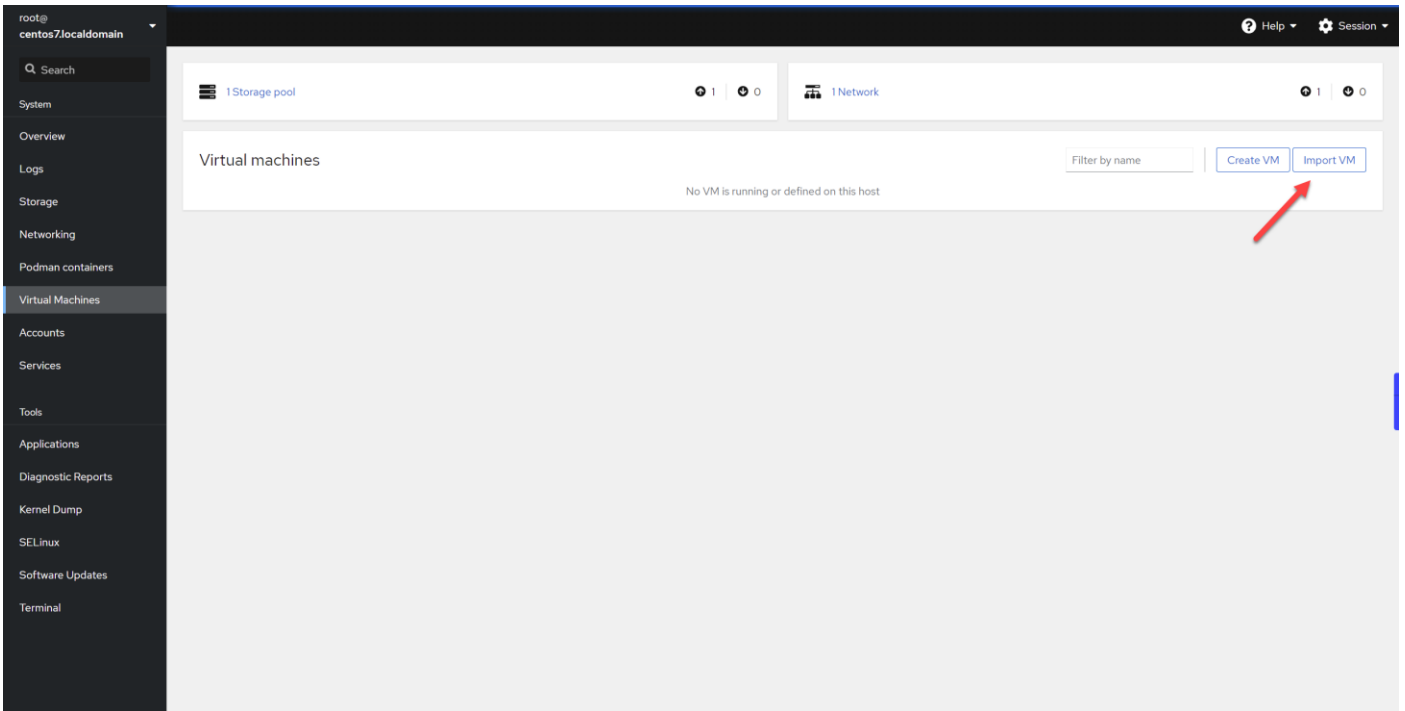
### Requirements and Versions

This guide is relevant for EdgeADC 4.2.6 and above.

The guidance below does not cover the installation of KVM or its networking.

We have assumed that you have downloaded the KVM virtual appliance and stored it on the host in an accessible location.

- The first step is to log into the Cockpit console.



- Click on Import VM
- The first dialog is where you will need to specify the details for the virtual appliance import. See the image below for the content of fields. You must specify Red Hat Enterprise 6.0 as the OS.

### Import a virtual machine ✕

**Name**

**Disk image**

**Operating system**

**Memory**

Up to 7.5 GiB available on the host

**Immediately start VM**

- Please ensure that you have the “Immediately Start VM” unchecked.
- Once you have filled in the details, please click the Import button.
- The next stage is to specify the vCPU and memory allocation you may wish to use.

## Overview

### General

State	Shut off
Memory	4 MiB <a href="#">edit</a>
vCPUs	1 <a href="#">edit</a>
CPU type	host <a href="#">edit</a>
Boot order	disk <a href="#">edit</a>
Autostart	<input type="checkbox"/> Run when host boots

### Hypervisor details

Emulated machine	pc-i440fx-rhel7.6.0
Firmware	BIOS

- To allocate the memory, you will see a dialog similar to the one below.

### EdgeADC memory adjustment

Current allocation 4 GiB

Maximum allocation 4 GiB

[Save](#) [Cancel](#)

- To allocate the vCPU, you will see a dialog similar to the one below.

### EdgeADC vCPU details

vCPU count 4

vCPU maximum 4

Sockets 1

Cores per socket 2

Threads per core 2

[Apply](#) [Cancel](#)

- The choices we have made are only examples but workable unless you are using heavy throughput with SSL re-encryption, in which case, you will need to adjust accordingly by using the Hardware section under View > Statistics.

▲ Hardware	
Disk Usage	40%
Memory Usage	11.6%( 894.7MB of 7689.6MB)
CPU Usage	16.0%

- You now have a working ADC installed in KVM. See image below.

The screenshot displays the KVM management interface for the EdgeADC. It is divided into several sections:

- Overview:** Shows the VM is in a 'Running' state. General settings include 4 vCPUs, 4 GiB of memory, and a custom CPU type (Cooperlake). Hypervisor details show an emulated machine of 'pc-i440fx-rhel7.6.0' and BIOS firmware.
- Usage:** A bar chart shows memory usage at 583.4 / 4096 MB and CPU usage at 6% of 4 vCPUs.
- Disks:** A table lists a single disk with 1.4 GiB used out of a 25 GiB capacity, connected via virtio bus. The source is a file path: /home/Edgenexus-ADC-6.8-64-KVM.1140-1909-7567-bam1727.qcow2.
- Networks:** A table lists a single network interface with a virtio model type, MAC address 52:54:00:60:83:65, and an unknown IP address.
- Console:** A VNC console window shows the EdgeADC boot process, including a login prompt for 'jetnexus'.

## Installing on Nutanix AHV

The following section shows how to install the EdgeADC onto a Nutanix AHV platform.

### Requirements and Versions

This guide is relevant for EdgeADC 4.2.6 and above.

All versions of the Nutanix hypervisor are compatible, but the certification has been performed on Nutanix version 5.10.9.

- The first step is to log into Nutanix Prism Central.

### Uploading the EdgeADC Image

- Navigate to Virtual Infrastructure > Images
- Click the Add Image button
- Select the EdgeADC image file you have downloaded and click the Open button to upload the image.
- Enter a name for the image in the Image Description field.
- Select an appropriate category
- Select the image and click the right-arrow key
- Select All Images and click Save.

## Creating the VM

- Navigate to Virtual Infrastructure > VMs
- Click the Create VM button
- Enter a name for the VM, the number of CPUs you wish to have, and the number of cores you want to allocate to the VM.
- Then scroll down in the dialog and enter the amount of memory you wish to allocate to the VM. You can start with 4GB and increase this depending on usage.

## Adding the Disk

- Next, click the Add New Disk link
- Select the Clone from Image Service option within the Operation drop-down.
- Select the EdgeADC image you have added and click the Add button.
- Select the disk to be the bootable disk.

## Adding the NIC, Network & Affinity

- Next, click the Add New NIC button. You will need to have two NICS.
- Select the Network and click the Add button
- Click the Set Affinity button
- Select the Nutanix hosts on which the VM is allowed to run, then click the Save button.
- Verify the settings you have made and click the Save button

## Powering on the VM

- From the list of VMs, click the VM name you just created
- Click the Power On button for the VM
- Once the VM has powered on, click the Launch Console button

## Configuring the EdgeADC Networking

- Follow the instructions in the section First Boot Environment.
- The EdgeADC is now ready for use, and you will be able to access its GUI using your browser and the Management IP address.

## Installing on ProxMox

Installation on ProxMox is simple but requires a couple of extra steps.

We will use the VMWare OVA version of installation. This is a multi-step process and requires knowledge of shell commands in ProxMox. However, we have made the instructions as easy as possible to follow. We are going to assume that you are conversant with ProxMox and so will not go into ProxMox features in depth.

### Uploading the OVA to ProxMox

Since we are using an OVA version, we will first need to upload the OVA to ProxMox.

- Log into the ProxMox console
- Create a folder called OVA\_Import.
- You will now need to use an SFTP client such as WinSCP (Windows) or CyberDuck (Mac) to transfer the OVA file.
- Once the file is transferred, you will see it in the folder you created.
- Type the following command to extract the contents of the OVA file.
- Tar xvf {filename}. See thee example below.

```
tar xvf Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
```

- Once extracted, you should see something like the below example.

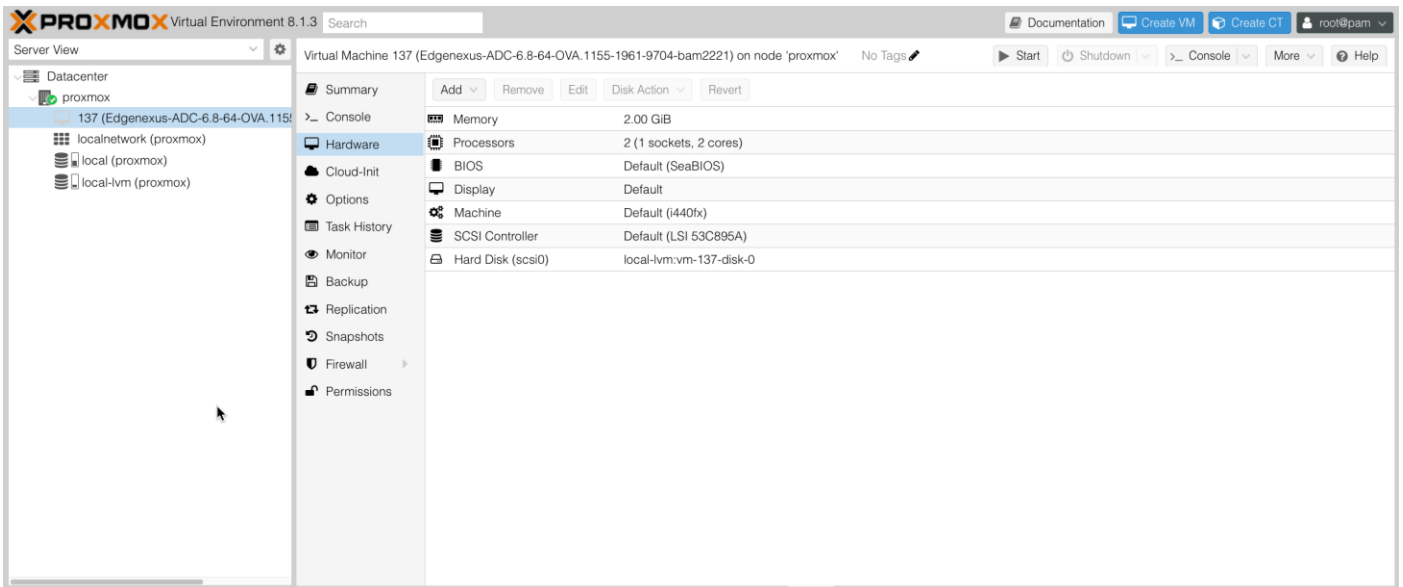
```

root@proxmox:~/OVA_Import# ls
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
root@proxmox:~/OVA_Import# tar xvf Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ovf
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.mf
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221-disk1.vmdk
root@proxmox:~/OVA_Import#
    
```

- There are three files. The .ovf and .mf are the configuration. The .vmdk is the virtual disk holding the ADC.
- The next step is to import the VMDK into ProxMox and create the virtual machine.
- Type the following command to create the virtual machine using the configuration files.

```
qm importovf 137 ./{filename.ovf} local-lvm --format qcow2
```

- In this example, we have given an ID of 100, but this may be different for your installation if you already have virtual machines created in ProxMox. You can determine the next ID by starting the process of VM creation in ProxMox, or by choosing a number higher than 100 that is safely out of reach.
- The VM has now been created.



- The next step is to add a network interface to the VM.
- Click on Hardware on the right panel.
- Click Add and choose a Network Interface.

**Add: Network Device** ✕

Bridge: <input type="text" value="vibr0"/>	Model: <input type="text" value="VMware vmxnet3"/>
VLAN Tag: <input type="text" value="no VLAN"/>	MAC address: <input type="text" value="auto"/>
Firewall: <input checked="" type="checkbox"/>	
Disconnect: <input type="checkbox"/>	Rate limit (MB/s): <input type="text" value="unlimited"/>
MTU: <input type="text" value="1500 (1 = bridge MTU)"/>	Multiqueue: <input type="text"/>

Advanced

- Configure it as the image above shows. It's important to choose the Model as VMware vmxnet3.
- Click Add once configured.



- You can add additional network adapters as your needs dictate.
- You can now start the VM and proceed to use the instructions in the First Boot Configuration chapter.

## First Boot Configuration

On the first boot, the ADC (also referred to as VA below) displays the following screen requesting configuration for production operations.

```
Checking for management interface ..... [ OK ]
Management interface: eth0  MAC: 00:0c:29:05:2e:1a

1. Enter networking details manually
2. Configure networking setting automatically via DHCP
```

### First Boot – Manual Network Details

On the first boot, you will have 10 seconds to interrupt the automatic assignment of IP details via DHCP.

To interrupt this process, click into the console window and press any key. You can then enter the following details manually.

- IP Address
- Subnet Mask
- Gateway
- DNS Server

These changes are persistent and will survive a reboot and don't need to be configured again on the VA.

### First Boot – DHCP successful

If you do not interrupt the network assignment process, your ADC will contact a DHCP server after a timeout to obtain its network details. If contact is successful, then your machine will be assigned the following information.

- IP Address
- Subnet Mask
- Default Gateway
- DNS Server

We advise that you only operate the ADC using a DHCP address if that IP address links permanently to the MAC address of the ADC within the DHCP server. We always advise using a **FIXED IP ADDRESS** when using the virtual appliances. Follow the steps in [CHANGING THE MANAGEMENT IP ADDRESS](#) and subsequent sections until you have completed the network configuration.

### First Boot – DHCP Fails

If you do not have a DHCP server or the connection fails, the IP Address 192.168.100.100 will be assigned. The IP address will increment by '1' until the VA finds a free IP address. Equally, the VA will check to see if the IP address is currently in use, and if so, will increment again and recheck.

## Changing the Management IP Address

You can change the IP address of the VA at any time using the command **set greenside=n.n.n.n**, as shown below.

```
set greenside={IP Address}
```

## Changing the Subnet Mask for eth0

The network interfaces use the prefix 'eth'; the base network address is called eth0. The subnet mask or netmask can be changed using the command **set mask [NIC] [MASK]**. You can see an example below.

```
set mask eth0 {mask}
```

## Assigning a Default Gateway

The VA needs a default gateway for its operations. To set the default gateway, use the command **route add default gw [GATEWAY IP]** as shown in the example below.

```
route add default gw {IP Address}
```

## Checking the Default Gateway value

To check if the default gateway is added and is correct, use the command **route**. This command will display the network routes and default gateway value. See the example below.

```
Command:route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
255.255.255.255 *                255.255.255.255 UH      0      0      0 eth0
192.168.101.0    *                255.255.255.0  U       0      0      0 eth0
default          192.168.101.254 0.0.0.0         UG      0      0      0 eth0
```

You can now access the Graphical User Interface (GUI) to configure the ADC for production or evaluation usage.

## Accessing the web interface

You can use any Internet browser with JavaScript to configure, monitor, and deploy the ADC into operational use.

In the browser URL field, type either **HTTPS://{IP ADDRESS}** or **HTTPS://{FQDN}**

The ADC, by default, uses a self-signed SSL certificate. You can change the ADC to use the SSL certificate of your own choice.

Once your browser reaches the ADC, it will show you the login screen. The factory default credentials for the ADC are:

**Username: admin / Pwd: jetnexus**

## Command Reference Table

Command	Parameter1	Parameter2	Description	Example
date			Shows the configured date and time currently configured	Tue Sept 3 13:00 UTC 2013
defaults			Assign the factory default settings for your appliance	
exit			Log out of the command line interface	
help			Displays all valid commands	
ifconfig	[blank]		View the interface configuration for all interfaces	ifconfig
	eth0		View the interface configuration of eth0 only	ifconfig eth0
machineid			This command will provide the machineid used to licence the ADC ADC	EF4-3A35-F79
quit			Log out of the command line interface	
reboot			Terminate all connections and reboot the ADC ADC	reboot
restart			Restart the ADC ADC virtual services	
route	[blank]		View the routing table	route
	add	default gw	Add the default gateway IP address	route add default gw 192.168.100.254
set	greenside		Set the management IP address for ADC	set greenside=192.168.101.1
	mask		Set the subnet mask for an interface. Interface names are eth0, eth1....	set mask eth0 255.255.255.0
show			Displays the global configuration settings	
shutdown			Terminate all connections and power-off the ADC ADC	
status			Displays the current data statistics	
top			View the process information such as CPU and Memory	
viewlog	messages		Displays the raw syslog messages	View log messages

Please note: Commands are not case sensitive. There is no command history.

# The Web Console

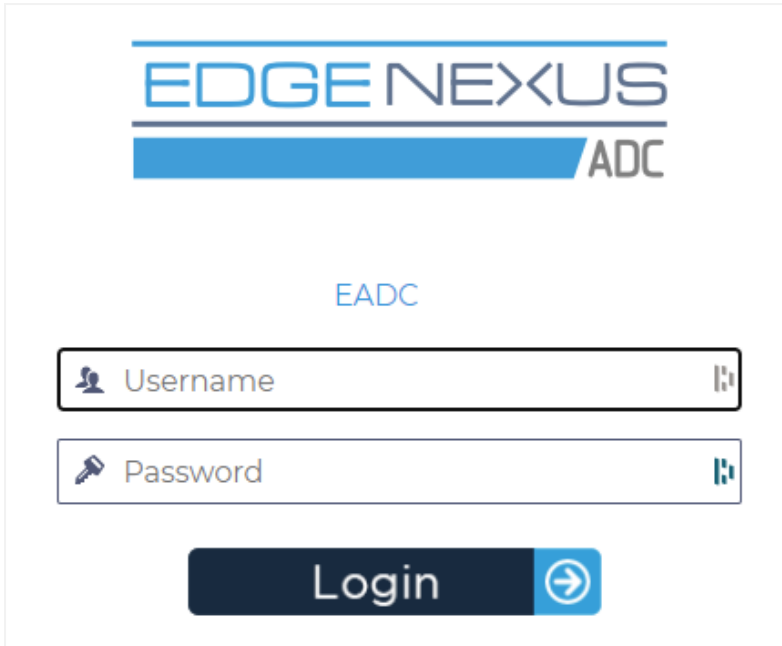
## Launching the ADC Web Console

All operations on the ADC are configured and performed using the web console. The web console is accessed using any browser with JavaScript.

To launch the ADC web console, enter the URL or IP address of the ADC into the URL field. We will use the example of `adc.company.com` as an example:

**`https://adc.company.com`**

When launched, the web console of the ADC is as shown below, allowing you to log in as the admin user.



The screenshot shows the login interface for the EdgeNexus ADC. At the top, the logo 'EDGE NEXUS' is displayed in blue, with 'ADC' in grey below it. Below the logo, the text 'EADC' is centered. There are two input fields: 'Username' with a person icon and 'Password' with a key icon. Both fields have a small 'i' icon on the right side. Below the input fields is a dark blue 'Login' button with a white right-pointing arrow icon.

### Default Login Credentials

The default login credentials are:

**Username: admin / Pwd: jetnexus**

You can change this at any time using user configuration located at *System > Users*.

Once you successfully log in, the main dashboard of the ADC is shown on screen.

### Using an External Authentication Service

Should you wish to use an external authentication service, you can do so by configuring an Authentication Server and Authentication Service.

Information on this can be found in [Authentication](#) and [Authentication Service](#).

## The Main Dashboard

The image below illustrates how the main dashboard or 'home page' of the ADC looks. We may occasionally make some changes for improvement, but all functions will remain.

The screenshot displays the EdgeADC main dashboard. At the top, there is a navigation bar with 'EDGE NEXUS' on the left, 'IP-Services' and 'Clustering' tabs in the center, and 'GUI Status', 'Home', 'Help', and 'admin' on the right. Below this is a 'NAVIGATION' sidebar on the left with options for 'Services', 'App Store', and 'IP-Services'. The main content area is divided into two sections: 'Virtual Services' and 'Real Servers'.

The 'Virtual Services' section features a search bar and three buttons: 'Copy Service', 'Add Service', and 'Remove Service'. It contains a table with the following data:

Mode	VIP	VS	Enab...	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active				10.0.0.190	255.255.255.0	80	Web Sites	HTTP(S)

The 'Real Servers' section has tabs for 'Server', 'Basic', 'Advanced', and 'flightPATH'. It includes a 'Group Name' field set to 'Server Group' and buttons for 'Copy Server', 'Add Server', and 'Remove Server'. The table below shows server details:

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
Online	Online	10.0.0.20	80	100	50		
Online	Online	10.0.0.21	80	100	100		
Online	Online	10.0.0.22	80	100	100		

At the bottom of the dashboard, a status bar indicates '[ Timed licence 14 days left ]'.

The Navigation section on the left side allows you to navigate the various areas of the ADC's functionalities. By default, the Services section is selected, and the IP Services sub-section is opened, indicated by the tab located above the Virtual Services section. This tab is fixed and is always shown.

When you click on a section within Navigation, that section is expanded, and its contents are revealed. Clicking on an option within a section will open the section content on the right side, and a tab will be placed at the top allowing for fast switching.

The different navigation sections are explained in detail in subsequent chapters.

# Services



## IP Services

The IP Services section of the ADC allows you to add, delete and configure the various virtual IP services you need for your particular use case. The settings and options fall into the sections below. These sections are on the right side of the application screen.

### Virtual Services

A Virtual Service combines a Virtual IP, or VIP, and a TCP/UDP port on which the ADC listens. Traffic arriving at the Virtual IP is redirected to one of the Real Servers associated with that service. The Virtual IP address cannot be the same as the management address of the ADC. i.e. eth0, eth1 etc...

The ADC determines how the traffic is re-distributed to the Servers based on a load-balancing policy set within the Basic tab in the Real Servers section.

### Creating a new Virtual Service using a new VIP

Mode	VIP	VS	Enab...	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	10.0.0.130	255.255.255.0	80	Web Sites	HTTP(S)

- Click the Add Virtual Service button as indicated above.

Virtual Services

Search

Copy Service Add Service Remove Service

Mode	VIP	VS	Enab...	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active			<input checked="" type="checkbox"/>	10.0.0.130	255.255.255.0	80	Web Sites	HTTP(S)

Update Cancel

You will then enter the **edit row** mode.

- Complete the four highlighted fields to proceed, and then click the update button.

Please use the TAB key to navigate through the fields.

Field	Description
IP Address	Enter a new Virtual IP address to be the target entry point for accessing the Real Server. This IP is where users or applications will point to access the load-balanced application.
Subnet Mask/Prefix	This field is for the subnet mask relevant to the network on which the ADC sits
Port	The entry port used when accessing the VIP. This value does not necessarily need to be the same as the Real Server if you are using Reverse Proxy.
Service Name	The service name is a textual representation of the VIP's purpose. It is optional, but we recommend you provide this for clarity. Note that this field is used for other specific purposes when using GSLB.
Service Type	There are many different Service Types available for you to select. Layer 4 service types cannot use flightPATH technology.

You can now press the Update button to save this section and jump automatically to the Real Server section detailed below:

Real Servers									
Server <span>Basic</span> <span>Advanced</span> <span>flightPATH</span>									
Group Name: <input type="text" value="Server Group"/>						<input type="button" value="Copy Server"/> <input type="button" value="Add Server"/> <input type="button" value="Remove Server"/>			
Status	Activity	Address	Port	Weight	Cal. Weight	Monitor End Point	Notes	ID	
	Online	10.0.0.20	80	100	100	Self		WEB1	
	Online	10.0.0.21	80	100	100	Self		WEB1	
	Online	10.0.0.22	80	100	100	Self		WEB1	

Field	Description
Activity	<p>The Activity field can be used to show and change the status of the load-balanced real server.</p> <p>Online – Denotes that the server is active and receiving load-balanced requests.</p> <p>Offline – The server is offline and is not receiving requests.</p> <p>Drain – The server has been placed in drain mode so that persistence can flush and the server moved to an offline state without affecting users.</p> <p>Standby – The server has been placed in a standby state</p>
IP Address	This value is the IP address of the Real Server. It must be accurate and should not be a DHCP address.
Port	The target Port of access on the Real Server. When using a reverse proxy, this can be different from the entry Port specified on the VIP.
Weighting	This setting usually is automatically configured by the ADC. You can change this if you wish to change the priority weighting.
Cal. Weight	If you leave the Weighting at its default value, the ADC will automatically calculate weighting based on response times.
Monitor End Point	The default value for this is 'Self'. However, you can change this to a Port value or an IP Address:Port. The field is used to monitor a different end point and determine whether traffic should be passed to the Virtual Service. See How to use Monitor End Point below.

- Click the Update button or press Enter to save your changes
- The Status light will first turn Grey, followed by Green should the Server Health Check succeed. 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

Virtual Services									
Search <input type="text"/>									
<input type="button" value="Copy Service"/> <input type="button" value="Add Service"/> <input type="button" value="Remove Service"/>									
Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type	
Active			<input checked="" type="checkbox"/>	10.0.0.142	255.255.255.0	443		HTTP(S)	
			<input checked="" type="checkbox"/>	10.0.0.142	255.255.255.0	80		HTTP(S)	
Active			<input checked="" type="checkbox"/>	10.0.0.143	255.255.255.0	443		HTTP(S)	

Real Servers									
Server <span>Basic</span> <span>Advanced</span> <span>flightPATH</span>									
Group Name: <input type="text" value="Server Group"/>						<input type="button" value="Copy Server"/> <input type="button" value="Add Server"/> <input type="button" value="Remove Server"/>			
Status	Activity	Address	Port	Weight	Cal. Weight	Monitor End Point	Notes	ID	
	Online	10.0.0.20	80	100	100	Self	Web1	web1	
	Online	10.0.0.21	80	100	100	Self	Web2	web2	
	Online	10.0.0.22	80	100	100	Self	Web3	web3	

## How to use Monitor End Point

### Example 1

Let's take an example of an infrastructure comprising two load balanced web servers that deliver a web application to the end user. The web application is connected to a database server in the back end. The access to the database server goes down, but the web application servers remain in operation. The users will be trying to use the web application and will be receiving errors.

The solution is to use Monitor End Point.

The screenshot shows the 'Virtual Services' configuration page. The 'Virtual Services' table has the following data:

Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	●	●	☑	10.0.0.142	255.255.255.0	443		HTTP(S)
Active	●	●	☑	10.0.0.142	255.255.255.0	80		HTTP(S)
Active	●	●	☑	10.0.0.143	255.255.255.0	443		HTTP(S)

Below this is the 'Real Servers' configuration page for the 'Server Group'. The 'Real Servers' table has the following data:

Status	Activity	Address	Port	Weight	Cal. Weight	Monitor End Point	Notes	ID
●	Online	10.0.0.20	80	100	100	10.0.0.111:4033	Web1	web1
●	Online	10.0.0.21	80	100	100	10.0.0.111:4033	Web2	web2
●	Standby	10.0.0.22	80	100	100	Self	Web3	web3

- The example shows two web servers, 10.0.0.20 and 10.0.0.21, together with a third web server 10.0.0.22. The 10.0.0.22 server has been placed in a Standby mode.
- The two active web servers have been configured with a Monitoring End Point value of 10.0.0.111:4033 which is the database server connection IP Address and Port.
- In the event that the database server connection was to drop, the two active servers will be placed into an Offline mode, and the Standby server will go online, serving a web page that may inform the customer that the systems are under maintenance.

### Example 2

Another example for the usage of Monitor End Point is when you are load balancing UDP protocol servers, such as Always-On-VPN. As you may know, UDP ports are not reliably monitored, and so there arises a need to monitor a TCP port.

Using Monitor End Point allows us to do just that. The main port being used by the Always-on-VPN servers will be 53/udp, but you will monitor say, 8433/tcp. In such a case, you just need to enter the port value in the Monitor End Point field.

## Creating Sub Virtual Services

You can also have sub-Virtual Services in cases where you need to load balance using different ports on the same VIP. For example, you may have servers being accessed using the same virtual IP on ports 80, 8088 and 443, so will need to create sub-virtual services in order to accommodate this.

- Highlight a Virtual Service you wish to copy.
- Click Add Virtual Service to enter row edit mode.

The screenshot shows the 'Virtual Services' configuration page. The 'Virtual Services' table has the following data:

Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	●	●	☑	10.0.0.130	255.255.255.0	80	Web Sites	HTTP(S)
		●	☑	10.0.0.130	255.255.255.0	443	Web Sites 443	HTTP(S)

- The IP Address and Subnet Mask copies across automatically.
- Enter the Port Number for your service.
- Enter an optional Service Name
- Select a Service Type.
- You can now press the Update button to save this section and jump automatically to the Real Server section below

Real Servers

Server Basic Advanced flightPATH

Group Name: Server Group + Add Server - Remove

Status	Activity	IP Address	Port	Weight	Calculated Weight	Notes
	Online			100	100	

Update Cancel

- Leave the server Activity option as Online – this means it will be load balanced if it passes the default health monitor of TCP Connect. This setting can be changed later if required.
- Enter an IP address for the Real Server
- Enter a Port Number for the Real Server
- Enter an optional name for the Real Server in the Notes field. Remember this notes field is used for other, specific purposes such as in flightPATH variables, etc.
- Click Update to save your changes.
- The Status light will first turn Grey, then Green if the Real Server Monitor 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 of a Virtual Service

You can change the IP address of an existing Virtual Service or VIP at any time.

- Highlight the Virtual Service whose IP address you wish to change.
- Click the IP address field for that service, to change it to an editable status.

Virtual Services

Search + Copy Service + Add Service - Remove Service

Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active			<input checked="" type="checkbox"/>	10.0.0.130		80	Web Sites	HTTP(S)
Active			<input checked="" type="checkbox"/>	10.0.0.130		443	Web Sites 443	HTTP(S)
Passive			<input checked="" type="checkbox"/>	10.0.0.131	255.255.255.0	Enter Port Num	Optional Service Name	HTTP(S)

Update Cancel

- Change the IP address to the one you wish to use
- Click the Update button to save the changes.

**Note:** Changing the IP address of a Virtual Service will change the IP address of all services associated with the VIP

## Creating a new Virtual Service using Copy Service

- The Copy Service button will copy an entire service, including all the Real Servers, basic settings, advanced settings, and flightPATH rules associated with it
- Highlight the service you wish to duplicate and click Copy Service
- The row editor will appear with the blinking cursor on the IP Address column

- You must change the IP address to be unique, or if you wish to keep the IP address, you must edit the Port so it is unique to that IP address

Remember to edit each tab if you change a setting such as a load balancing policy, the Real Server monitor, or remove a flightPATH rule.

## Filtering displayed data

### Searching for a specific term

The Search box allows you to search the table using any value, such as the octets of the IP address or name of the service.

### Selecting column visibility

You can also select the columns that you wish to display in the dashboard.

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
Online	Online	192.168.1.200	80	100	100	Site 1	
Online	Online	192.168.1.201				Site 2	

- Move the mouse over any one of the columns
- You will see a small arrow appear on the right side of the column
- Clicking the checkboxes selects the columns you wish to see in the dashboard.

## Understanding the Virtual Services columns

### Primary/Mode

The Mode column indicates the high availability role selected for the current VIP. For the modes, see System > Clustering>Roles.

Option	Description
Active	In Cluster mode, the value of this field is Active. When you have an HA pair of ADC appliances in your datacentre, one of them will show Active and the other Passive. If the current appliance
Passive	When the ADC is acting as a secondary member of a cluster, then Passive is shown in the Mode column.
Manual	The Manual role allows the ADC pair to run in Active-Active mode for different Virtual IP addresses. In such cases, the Primary column will contain a box next to each unique Virtual IP that is selectable for Active or left un-ticked for Passive.
Stand-Alone	The ADC is acting as a stand-alone device and is not in High Availability mode. As such, the Primary column will state Stand-alone.

### VIP

This column provides visual feedback on the status of each Virtual Service. The indicators are color-coded and are as follows:

LED	Meaning
●	Online
●	Failover-Standby. This virtual service is hot-standby

●	Indicates a "secondary" is holding off for a "primary."
●	Service Needs attention. This indication may result from a Real Server failing a health monitor check 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 licensed or licensed Virtual IPs exceeded

## Enabled

The default for this option is Enabled, and the checkbox shows as ticked. You can disable the Virtual Service by double-clicking the line, unchecking the checkbox, and then clicking the Update button.

## IP Address

Add your IPv4 address in decimal dotted notation or an IPv6 address. This value is the Virtual IP address (VIP) for your service. Example IPv4 "192.168.1.100". Example Ipv6 "2001:0db8:85a3:0000:0000:8a2e:0370:7334"

## Subnet Mask/Prefix

Add your subnet mask in decimal dotted notation. Example "255.255.255.0". You can also use the subnet value such as /24, or for IPv6, add in your Prefix. For more information about IPv6, please see [HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6\\_ADDRESS](https://en.wikipedia.org/wiki/IPv6_address)

## Port

Add the port number associated with your service. The port can be a TCP or UDP port number. Example TCP "80" for Web Traffic and TCP "443" for Secured Web Traffic. You can also specify a range of values such as 80-87.

Currently, it is not possible to use comma separated values to specify non-contiguous port values.

## Service Name

Add in a friendly name to identify your service. Example "Production Web Servers." This field is also used when using GSLB.

## Service Type

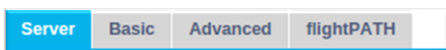
Please note that with all "Layer 4" service types, the ADC will not interact or modify the data stream, so flightPATH is unavailable with Layer 4 service types. Layer 4 services simply load balance the traffic according to the load balancing policy:

Service Type	Port/Protocol	Service Layer	Comment
Layer 4 TCP	Any TCP port	Layer 4	The ADC will not alter any information in the data stream and will perform standard load balancing the traffic according to the load balancing policy
Layer 4 UDP	Any UDP port	Layer 4	As with Layer 4 TCP, the ADC will not alter any information in the data stream and will perform standard load balancing the traffic according to the load balancing policy

Layer 4 TCP/UDP	Any TCP or UDP port	Layer 4	It is ideal if your service has a primary protocol such as UDP but will fall back to TCP. The ADC will not alter any information in the data stream and will perform standard load balancing the traffic according to the load balancing policy
DNS	TCP/UDP	Layer 4	Used to load balance DNS servers.
HTTP(S)	HTTP or HTTPS protocol	Layer 7	The ADC can interact, manipulate and modify the data stream using flightPATH.
FTP	File Transfer Protocol	Layer 7	Using separate control and data connections between client and server
SMTP	Simple Mail Transfer Protocol	Layer 4	Use when load balancing mail servers
POP3	Post Office Protocol	Layer 4	Use when load balancing mail servers
IMAP	Internet Message Access Protocol	Layer 4	Use when load balancing mail servers
RDP	Remote Desktop Protocol	Layer 4	Use when load balancing Terminal Services servers
RPC	Remote Procedure Call	Layer 4	Use when load balancing systems using RPC calls
RPC/ADS	Exchange 2010 Static RPC for Address Book Service	Layer 4	Use when load balancing Exchange servers
RPC/CA/PF	Exchange 2010 Static RPC for Client Access & Public Folders	Layer 4	Use when load balancing Exchange servers
DICOM	Digital Imaging and Communications in Medicine	Layer 4	Use when load balancing servers using DICOM protocols

## Real Servers

There are several tabs in the Real Servers section of the dashboard: Server, Basic, Advanced, and flightPATH.



### Server

The Server tab holds the definitions of the real back-end servers paired to the Virtual Service currently selected. You are required to add at least one server to the Real Servers section.

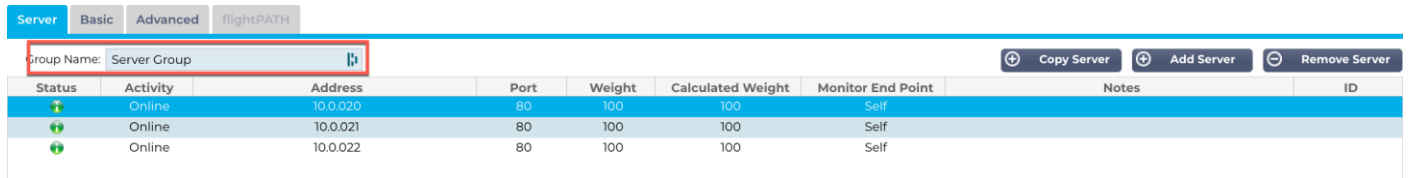
Status	Activity	Address	Port	Weight	Calculated Weight	Monitor End Point	Notes	ID
Online	Online	10.0.0.20	80	100	100	Self		
Online	Online	10.0.0.21	80	100	100	Self		
Online	Online	10.0.0.22	80	100	100	Self		

### Add Server

- Select the appropriate VIP that you have previously defined.
- Click Add Server
- A new row will appear with the cursor blinking on the IP Address column

- 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 ADC can route. Example "10.1.1.1".
- Tab to the Port column and enter the TCP/UDP port number for your server. The port number can be the same as the Virtual Service port number or another port number for Reverse Proxy Connectivity. The ADC will automatically translate to this number.
- Tab to the Notes section to add in any relevant detail for the server. Example: "IIS Web Server 1"

### Group Name



When you have added in the servers comprising the load-balanced set, you can also attach a Group Name. Once you have edited this field, the contents save without the need to press the Update button.

### Real Server Status Lights

You can see the status of a Real Server by the light color in the Status column. See below:

LED	Meaning
	Connected
	Not Monitored
	Draining
	Offline
	Standby
	Not Connected
	Finding Status
	Not licensed or licensed Real Servers exceeded

### Activity

You can change the Activity of a Real Server at any time by using the dropdown menu. To do this, double-click on a Real Server row to place it into edit mode.

Option	Description
Online	All Real Servers assigned 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 while the drain is in process. Once the existing



	connections have closed naturally, the Real Servers will go offline, and the Status light will be solid blue. You can also view these connections by navigating to the Navigation > Monitor > Status section. The Drain Behaviour can be changed in the Advanced setting tab.
Offline	All Real Servers set as Offline will immediately be taken offline and will not receive any traffic.
Standby	All Real Servers set as Standby will remain offline until <b>ALL</b> the Online group servers fail their Server Health Monitor checks. Traffic is received by the Standby group as per the load balancing policy when this happens. If one server in the Online group passes the Server Health Monitor check, this Online server will receive all the traffic, and the Standby group will stop receiving traffic.

### IP Address

This field is the IP address for your Real Server. Example "192.168.1.200".

### Port

TCP or UDP port number that the Real Server is listening on for the service. Example "80" for Web Traffic.

### Weight

This column will become editable when there is an appropriate Load Balancing Policy specified.

The default weight for a Real Server is 100, and you can enter values from 1-100. A value of 100 means maximum load, and 1 means minimum load.

An example for three servers may look something like this:

- Server 1 Weight = 100
- Server 2 Weight = 50
- Server 3 Weight = 50

If we consider the load balancing policy is set to Least Connections, and there are 200 total client connections;

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

If we were to use Round Robin as the load balancing method, which rotates requests through the load balanced server set, altering the weights affects how often the servers get chosen as the target.

If we believe the Fastest load balancing policy uses the shortest time taken to GET a response, adjusting the weights alters the bias similarly to Least Connections.

### Calculated Weight

The Calculated Weight of each server can be viewed dynamically and is calculated automatically and is not editable. The field shows the actual weighting that ADC is using when considering manual weighting and load balancing policy.

### Monitor End Point

This feature allows you to specify particular endpoints to monitor, and thereby determine the health status for the Real Server entry. You can leave it at the default value of "Self" where it will rely on the Real Server Monitors specified for the Virtual Service. Alternatively, you can also specify an IP address, Port or IP Address:Port allowing you to monitor another endpoint on your network. Examples of this could include, say, a database server on which the services are dependent on.

## Notes

Enter any particular notes helpful in describing the defined entry to the Notes field. Example "IIS Server1 – London DC". This field can be used for specific needs within flightPATH rules and GSLB.

## ID

This setting has a number of uses.

### Persistence

The value can be used in conjunction with the Cookie ID Based persistence method. This is very much like PHP Session Based persistence, but uses a new technique called Cookie ID Based and cookie RegEx `h=[^;]+`. The Cookie ID Based persistence based method will use the value in the ID field to generate a Cookie.

### flightPATH Usage

You can also use the value in this field to direct traffic etc.

## Basic

Server
Basic
Advanced
flightPATH

Load Balancing Policy: Least Connections ▼

Server Monitoring: TCP Connection ▼

Caching Strategy: Off ▼

Acceleration: Compression ▼

Virtual Service SSL Certificate: No SSL ▼

Real Server SSL Certificate: No SSL ▼

Update

## Load Balancing Policy

The dropdown list shows you the currently supported load balancing policies available for use. A list of load-balancing policies, together with an explanation, is below.

- Least Connections
- Fastest
- Persistent Cookie
- Round Robin
- IP-Bound
- IP List Based
- Shared IP List Based
- Classic ASP Session Cookie
- ASP.NET Session Cookie
- JSP Session Cookie
- JAX-WS Session Cookie
- PHP Session Cookie
- RDP Cookie Persistence
- Cookie ID Based

Option	Description
--------	-------------

Least Connections	The load balancer will keep track of the number of current connections to each Real Server. The Real Server with the least number of connections receives the subsequent new request.
Fastest	The Fastest load balancing policy automatically calculates the response time for all requests per server smoothed over time. The Calculated Weight column contains the automatically calculated value. Manual entry is only possible when using this load balancing policy.
Persistent Cookie	Layer 7 Session Affinity/Persistence The IP list-based load balancing mode is used for each first request. The ADC inserts a cookie into the headers of the first HTTP response. After that, the ADC uses the client cookie to route traffic to the same back-end server. This cookie 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 an IP List Based algorithm. This expiry time is configurable using a jetPACK.
Round Robin	Round Robin is commonly used in firewalls and basic load balancers and is the simplest method. Each Real Server receives a new request in sequence. This method is only proper when you need to load balance requests to servers evenly; an example would be look-up web servers. However, when you need to load balance based on application load or the server load, or even ensure that you use the same server for the session, the Round Robin method is inappropriate.
IP Bound	Layer 3 Session Affinity/Persistence Cookie. In this mode, the client's IP address forms the basis to select which Real Server will receive the request. This action provides persistence. HTTP and Layer 4 protocols can use this mode. This method is helpful 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, the header (X-Forwarder—For) information is used when present to cope with proxies.
IP List Based	The connection to the Real Server initiates using "Least connections" then, session affinity is achieved based on the client's IP address. A list is maintained for 2 hours by default, but this can be changed using a jetPACK.
Shared IP List Based	This service type is only available when the Connectivity Mode is set to Direct Server Return. It has been primarily added for support with VMware load balancing.
Persistent Cookie	Layer 7 Session Affinity/Persistence The IP list-based load balancing mode is used for each first request. The ADC inserts a cookie into the headers of the first HTTP response. After that, the ADC uses the client cookie to route traffic to the same back-end server. This cookie 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 an IP List Based algorithm. This expiry time is configurable using a jetPACK.
Classic ASP Session Cookie	Active Server Pages (ASP) is a Microsoft server-side technology. With this option selected, the ADC will maintain session persistence to the same server if an ASP cookie is detected and found in its known cookies list. On detection of a new ASP cookie, it will be load balanced using the Least Connections algorithm.
ASP.NET Session Cookie	This mode applies to <b>ASP.net</b> . With this mode selected, the ADC will maintain session persistence to the same server if an ASP.NET cookie is detected and found in its list of known cookies. On detection of a new ASP cookie, 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 mode selected, the ADC will maintain session persistence to the same server if a JSP cookie is detected and found in its known cookies list. On detection of a new JSP cookie, 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 mode selected, the ADC will maintain session persistence to the same server if a JAX-WS cookie is detected and found in its list of known cookies. On detection of a new JAX-WS cookie, it will load balanced using the Least Connections algorithm.
PHP Session Cookie	Personal Home Page (PHP) is an open-source server-side technology. With this mode selected, the ADC will maintain session persistence to the same server when a PHP cookie is detected.
RDP Cookie Persistence	This load balancing method uses the Microsoft-created RDP Cookie based on username/domain to provide persistence to a server. The advantage of this method means maintaining a connection to a server is possible even if the IP address of the client changes.
Cookie-ID Based	<p>A new method very much like "PhpCookieBased" and other load-balancing methods, but using CookieIDBased and cookie RegEx <code>h=[^;]+</code></p> <p>This method will use the value set in the Real Server's notes field "ID=X;" as the cookie value to identify the server. This, therefore, means it is a similar methodology as CookieListBased but uses a different cookie name and stores a unique cookie value, not the scrambled IP, but the ID from the Real Server (read in at load-time.)</p> <p>The Default value is <code>CookieIDName="h"</code>; however, if there is an override value in the virtual server's advanced settings configuration, use this instead. <b>NOTE:</b> We overwrite the cookie expression above to replace <code>h=</code> with the new value if this value is set.</p> <p>The last bit is that if an unknown cookie value arrives and matches one of the Real Server IDs, it should select that server; otherwise, use the next method (delegate.)</p>

## Server Monitoring

Your ADC contains several pre-defined Real Server Monitoring methods.

Choose the monitoring method you wish to apply to the Virtual Service (VIP).

It is essential to choose the right monitor for the service. For example, if the Real Server is an RDP server, a 200OK monitor is not relevant. Equally, choosing TCP Connection and 200OK also make no sense as you require a working TCP connection for 200OK to work. If you are unsure which monitor to choose, the default TCP Connection is an excellent place to start.

You can choose multiple monitors by clicking each monitor you wish to apply to the service in turn. The selected monitors execute in the order you select them; hence start with monitors of the lower layers first. For example, setting monitors Ping/ICMP Echo, TCP Connection, and 200OK will display in the Dashboard Events like the image below:



Status	Date	Message
ATTENTION	10:22 26 Feb 2016	10.4.8.131:89 Real Server 172.17.0.2:88 unreachable - Echo=OK Connect=OK 200OK=FAIL
OK	10:22 26 Feb 2016	10.4.8.131:89 Real Server 172.17.0.2:88 contacted - Echo=OK Connect=OK 200OK=OK

We can see that Layer 3 Ping and Layer 4 TCP Connect has succeeded if we look at the top line, but Layer 7 200OK has failed. These monitoring results provide enough information to indicate that routing is OK and there is a service running on the relevant port, but the website is not responding correctly to the page requested. It's now time to look at the webserver and the Library > Real Server Monitor section to see the details of the failing monitor.

Option	Description
--------	-------------

None	In this mode, the Real Server is not monitored and is always up and running correctly. The None setting is helpful for situations where monitoring upsets a server and for services that should not join in the fail-over action of the ADC. It is a route to host unreliable or legacy systems that are not primary to H/A operations. Use this monitoring method with any service type.
Ping/ICMP Echo	In this mode, the ADC sends an ICMP echo request to the IP of the content server. If a valid echo response is received, the ADC deems the Real Server up and running, and traffic throughput to the server continues. It will also keep the service available on a H/A pair. This monitoring method is usable with any service type.
TCP Connection	A TCP connection is made to the Real Server and immediately broken without sending any data in this mode. If the connection succeeds, the ADC deems the Real Server to be up and running. This monitoring method is usable with any service type, and UDP services are currently not appropriate for TCP Connection monitoring.
ICMP Unreachable	The ADC will send a UDP health check to the server and mark the Real Server as unavailable if it receives an ICMP port unreachable message. This method can be helpful when you need to check if a UDP service port is available on a server, such as DNS port 53.
RDP	In this mode, a TCP connection initializes as explained in the ICMP Unreachable method. After the connection initializes, a Layer 7 RDP connection is requested. If the link is confirmed, the ADC deems the Real Server to be up and running. This monitoring method is usable with any Microsoft terminal server.
200 OK	In this method, a TCP connection initializes to the Real Server. After the connection succeeds, the ADC sends the Real Server an HTTP request. An HTTP response is waited for and checked for the "200 OK" response code. The ADC deems the Real Server up and running if the "200 OK" response code is received. If the ADC does not receive a "200 OK" response code for any reason, including timeouts, failure to connect, and other reasons, the ADC marks the Real Server unavailable. This monitoring method is only valid for use with HTTP and accelerated HTTP service types. If a Layer 4 Service type is used for an HTTP server, it is useable if SSL is not in use on the Real Server or handled appropriately by the "Content SSL" facility.
DICOM	A TCP connection initializes to the Real Server in DICOM mode, and an Echoscu "Associate Request" is made to the Real Server on connection. 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 the monitor does not complete successfully, then the Real Server is regarded as down for any reason.
User Defined	Any monitor configured in the Real Server Monitoring section will appear in the list.

## Caching Strategy

By default, the Caching Strategy is disabled and set as 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 VIP with the Accelerated "HTTP" service type, compressed objects are not cached.

Option	Description
By Host	Caching per host is based on application per hostname. A separate Cache will exist for each domain/hostname. This mode is ideal for web servers that can serve multiple websites depending on the domain.
By Virtual Service	Caching per virtual service is available when you choose this option. Only one Cache will exist for all domain/hostnames that pass through the virtual service. This option is a specialist setting for use with multiple clones of a single site.

## Acceleration

Option	Description
Off	Turn compression off for the Virtual Service
Compression	When selected, this option turns on the compression for the selected Virtual Service. The ADC dynamically compresses the data stream to the client upon request. This process only applies to objects that contain the content-encoding: gzip header. Example content includes HTML, CSS, or JavaScript. You can also exclude certain content types using the Global Exclusions section.

Note: If the object is cacheable, the ADC will store a compressed version and serve this statically (from memory) until the content expires and is re-validated.

### Virtual Service SSL Certificate (Encryption between Client and the ADC)

By default, the setting is No SSL. If your service type is "HTTP", you can select a certificate from the dropdown to apply to the Virtual Service. Certificates that have been created or imported will appear in this list.

You can also highlight multiple certificates to apply to a service. This operation will automatically enable the SNI extension to allow a certificate based on the "Domain Name" requested by the client.

Virtual Service SSL Certificate:  ▼

No SSL
All
default
AnyUseCert

Option	Description
No SSL	Traffic from the source to the ADC is not encrypted.
All	Loads all available certificates for use
Default	This option results in applying a locally created certificate called "Default" to the browser side of the channel. Use this option to test SSL when one hasn't been created or imported.

### Real Server SSL Certificate (Encryption between the ADC and Real Server)

The default setting for this option is No SSL. If your server requires an encrypted connection, this value must be anything other than No SSL. Certificates that have been created or imported will appear in this list.

No SSL
Any
SNI
default

Option	Description
No SSL	Traffic from the ADC to the Real Server is not encrypted. The selection of a certificate on the browser side means "No SSL" can be chosen client-side to provide what is known as "SSL Offload."
Any	The ADC acts as a client and will accept any certificate the Real Server presents. Traffic from the ADC to the Real Server is encrypted when this option is selected. Use the "Any" option when a certificate is specified on the Virtual Service side, providing what is known as "SSL Bridging" or "SSL Re-Encryption."
SNI	SNI, or Server Name Indication is an extension to the TLS networking protocol using which the client indicates what hostname it is attempting to connect to at the start of the

	handshaking process. This setting allows the ADC to present multiple certificates on the same virtual IP address and TCP port.
Default	Any self-signed certificates that you have generated appear here.

### Advanced

Real Servers

Server
Basic
Advanced
flightPATH

Connectivity: Reverse Proxy

Cipher Options: Defaults

Client SSL Renegotiation:

Client SSL Resumption:

SNI Default Certificate: None

Client Proxy Header: None

Server Proxy Header: None

Real Server Source Address: Base IP

Security Log: On

Max. Connections (Per Real Server):

Connection Timeout (sec):

Persistence Timeout (sec):

Monitoring Interval (sec):

Monitoring Timeout (sec):

Monitoring In Count:

Monitoring Out Count:

Monitoring KCD Realm: None

Drain Behaviour: Persistence Driven

Switch To Offline On Failure:

Update

### Connectivity

Your Virtual Service is configurable with different types of connectivity. Please select the connectivity mode to apply to the service.

Option	Description
<b>Reverse Proxy</b>	Reverse Proxy is the default value and uses compression and caching when used with Layer 7. At Layer 4, reverse proxy works without caching or compression. In this mode, your ADC acts as a reverse proxy and becomes the source address seen by the Real Servers.
<b>Direct Server Return</b>	<p>Direct Server Return or DSR also known DR – Direct Routing, allows the server behind the load balancer to respond directly to the client bypassing the ADC on the response. DSR is only suitable for use with Layer 4 load balancing. Therefore, Caching and Compression are not available with this option chosen.</p> <p><b>This mode can only be used with TCP, UDP, and TCP/UDP service types.</b></p> <p>Load balancing persistence policies are also restricted to Least Connections, Shared IP List Based, Round Robin and IP List Based.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>Least Connection</p> <p>Shared IP List Based</p> <p style="background-color: #e0e0e0;">Round Robin</p> <p>IP List Based</p> </div> <p>Using DSR also requires Real Server changes to be done. Please refer to the Real Server Changes section.</p>
<b>NAT</b>	By default, the ADC uses the IP address of the ADC as the Source IP address, and the Real Servers then send the response back to the ADC for return to the Client. This is fine in almost all circumstances, but there are scenarios when the Real Server needs to see the Source IP address of the Client and not the ADC.

	<p>When NAT mode is applied, the ADC receives the incoming request, and then sends it to the Real Server after it changes the Source IP address back to that of the Virtual Service (VIP address).</p> <p><b>This mode can only be used with the following Load Balancing Policies:</b></p> <div data-bbox="384 304 810 421" style="border: 1px solid #ccc; padding: 5px;"> <p>Least Connection</p> <p>Round Robin</p> <p>IP List Based</p> </div>
<p><b>Gateway</b></p>	<p>Gateway mode allows you to route all traffic through the ADC, allowing the Real Servers to be routed via the ADC to other networks via the ADC virtual services or hardware interfaces. Using the device as a gateway device for Real Servers is ideal when running in multi-interface mode.</p> <p>Load balancing persistence policies are also restricted to Least Connections, Shared IP List Based, Round Robin and IP List Based.</p> <div data-bbox="384 651 754 781" style="border: 1px solid #ccc; padding: 5px;"> <p>Least Connection</p> <p>Shared IP List Based</p> <p style="background-color: #e0f0ff;">Round Robin</p> <p>IP List Based</p> </div> <p>This method requires that the Real Server sets its default gateway to the ADC's local interface address (eth0, eth1, etc.). Please refer to the Real Server Changes section.</p> <p><b><i>Please note that Gateway mode does not support failover in a cluster environment.</i></b></p>

## Cipher Options

Ciphers form the basis of SSL cryptography and are extremely important for successful and secure web content and application delivery.

The ADC contains a built-in set of default Ciphers, comprising the most up-to-date and secure ones available for use.

There are occasions when the user wishes to announce the availability of a particular set of Ciphers, and the ADC allows the creation of such Ciphers through user-authored jetPACKS. jetPACKS written by users can be imported into the ADC through Configuration > Software, then made available for choosing using the Cipher Options menu.

Cipher Options are specific to each VIP, delivering high flexibility and security.

For more information on Cipher Options, please see: *Cipher*

## Client SSL Renegotiation

Tick this box if you wish to allow client-initiated SSL renegotiation. Disable client SSL renegotiation to prevent any possible DDOS attacks against the SSL Layer by un-ticking this option.

## Client SSL Resumption

Tick this box if you wish to enable SSL Resumption Server sessions added to the session cache. When a client proposes re-use of a session, the server will try to reuse the session if found. If Resumption is unchecked, no session caching for the client or server takes place.

## SNI Default Certificate

During an SSL connection with the Client-side SNI enabled, if the requested domain does not match any of the certificates assigned to the service, the ADC 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 dropdown to present should an exact SSL certificate match fail.



## The Proxy Protocol

The Proxy Protocol is designed to allow network proxies to forward client connection information (such as the originating IP address and port number) to the receiving server. This protocol is particularly useful in scenarios where the actual end-user IP address needs to be preserved while traffic is routed through a load balancer or reverse proxy. It helps in maintaining the original client's source IP for logging, statistics, or security purposes, enhancing the capability to make informed decisions based on the true source of the traffic.

### Client Proxy Header

The Client Proxy Header, refers to a header added to the client's request by the ADC, encapsulating original connection information (such as the client's IP address and port). This is crucial in environments where the ADC acts as a proxy, and the server needs to know the original client details for purposes like logging, security assessments, and maintaining client-specific behaviour. The Client Proxy Header ensures that despite the ADC's intermediary role, the server can accurately identify and interact with the client's original connection details.

Options include:

Option	Description
None	When there is no Proxy header, or its not supported in the current Service type
Remove	Removes the Proxy header from the TCP packet
Forward	Forwards the Proxy header to the server

### Server Proxy Header

There are two versions of Server Proxy Headers: Version 1 and Version 2.

Option	Description
Version 1	<ul style="list-style-type: none"> <li>Text-based format, easy to implement and debug.</li> <li>Provides basic information about the client's connection, including source IP, destination IP, source port, and destination port.</li> <li>The protocol line is added to the start of the TCP connection, making it human-readable but slightly less efficient in terms of performance compared to binary formats.</li> </ul>
Version 2	<ul style="list-style-type: none"> <li>Binary format, designed for enhanced performance and efficiency.</li> <li>Extends the information that can be relayed about the connection, supporting additional data like address family and protocol-specific information.</li> <li>Ensures better compatibility with modern network protocols and features, including support for IPv6 and transport protocols beyond TCP.</li> </ul>

The Client Proxy Header and Server Proxy header options are only available for Layer 4 and Layer 7 HTTP service types.

### Real Server Source Address

This setting works together with Reverse Proxy and either Layer 4 TCP, Layer 4 UDP or HTTP(S) service. The setting provides three options that you can choose from.

Option	Description
--------	-------------

Base IP (Default)	Uses the eth0, or Base IP address of the ADC as the Source IP of the request.
Virtual IP	Uses the Virtual IP of the service.
<IP Address>	Allows you to specify an IP address that is part of the ADC. This could be a different network interface or a different VIP.

## Security Log

'On' is the default value and is on a per-service basis, enabling the service of logging authentication information to the W3C logs. Clicking the Cog icon will take you to the System > Logging page, where you can check the settings of the W3C logging.

## Max. Connections

Limits the number of simultaneous Real Server connections and is set per service. For example, if you configure this to 1000 and have two Real Servers, the ADC limits **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 understand why any non-response or delay has occurred. Leave this blank for unlimited connections. What you set here depends on your system resources.

## Connection Timeout

The default connection timeout 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. The RDP timeout example means that if a user has a period of inactivity of 2 hours or less, the connections will remain open.

## Persistence Timeout

The Persistence Timeout setting in load balancers specifies the duration for which a load balancer maintains the session information for a client. This ensures that subsequent requests from the same client are directed to the same backend server, promoting session consistency and stateful communication. Once the specified timeout period elapses without further client activity, the session information is discarded, and new requests may be routed to a different server.

## Monitoring Interval

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

## Monitoring Timeout

The timeout value is when the ADC will wait for a server to respond to a connection request. The default value is 2s. Increase this value for busy servers.

## Monitoring In Count

The default value for this setting is 2. The value of 2 indicates that the Real Server must pass two successful health monitor checks before it comes online. Increasing this figure will increase the probability that the server can serve 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, meaning that the Real Server monitor must fail three times before the ADC will stop sending traffic to the server, and it is marked RED and Unreachable. Increasing this figure

will result in better and more reliable service at the expense of the time it takes the ADC to stop sending traffic to this server.

## Monitoring KCD Realm

This setting allows you to enable monitoring of the Kerberos Constrained Delegation Realm that you have set up in Kerberos definitions. See Authentication > Kerberos.

## Drain Behaviour

Whenever any Real Server is placed into Drain mode, it is always better to be able to control the behaviour of traffic being sent to it. The Drain Behaviour menu allows the selection of traffic behaviour on a per Virtual Service basis. Options are:

Option	Description
Persistence Driven	This is the default selection. Whenever the user visits using the persistence session, it is extended. With 24-hour usage, it is possible that the drain would never happen. However, if the number of connections to the real server ever reaches 0, drain ends, persistence sessions are deleted, and all visitors get re-balanced on the next connection they make.
Migrate Visitors	Persistent session ignored on re-connect - (legacy behavior before 2022) New TCP connections (whether part of an existing session or not) are always made to an online real server. If the persistence session was to a draining real server, it is overwritten. The Virtual Service will effectively ignore persistence on any new connections, and they will be load balanced to a new server.
Retire Sessions	Persistent sessions not extended. Incoming user connections will be allocated to their desired server, but their persistence session is not extended. So, after the persistence session time is exceed, they will be treated as new connection and moved to a different server.

## Switch To Offline on Failure

When this is checked, the Real Servers that fail their health check are placed offline and can only be set online manually.

## flightPATH

flightPATH is a traffic management technology designed by Edgenexus and exclusively available within the ADC. Unlike other vendors' rules-based engines, flightPATH does not operate through a command line or script entry console. Instead, it uses a GUI to select the different parameters, conditions, and actions to perform to achieve what they need. These features make flightPATH extremely powerful and allow network administrators to manipulate HTTPS traffic in highly effective ways.

flightPATH is only available for use with HTTPS connections, and this section is not visible when the Virtual Service Type is not HTTP.

You can see from the image above; there are a list of available rules on the left and the rules applied to the virtual service on the right.

Apply an available rule by dragging and dropping the rule from the left side to the right, or highlighting a rule and clicking the right arrow to move it to the right side.

The order for execution is essential and starts with the top rule executed first. To change the order of execution, highlight the rule and move up and down using the arrows.

It is important to understand that flightPATH rules in this section of the ADC work on a Boolean **OR** basis, whereas the conditions and actions within the flightPATH definition area work on an **AND** basis.

To remove a rule, drag and drop it back to the rule inventory on the left or highlight the rule and click the left arrow.

You can add, remove, and edit flightPATH rules in the Configure flightPATH section of this guide.

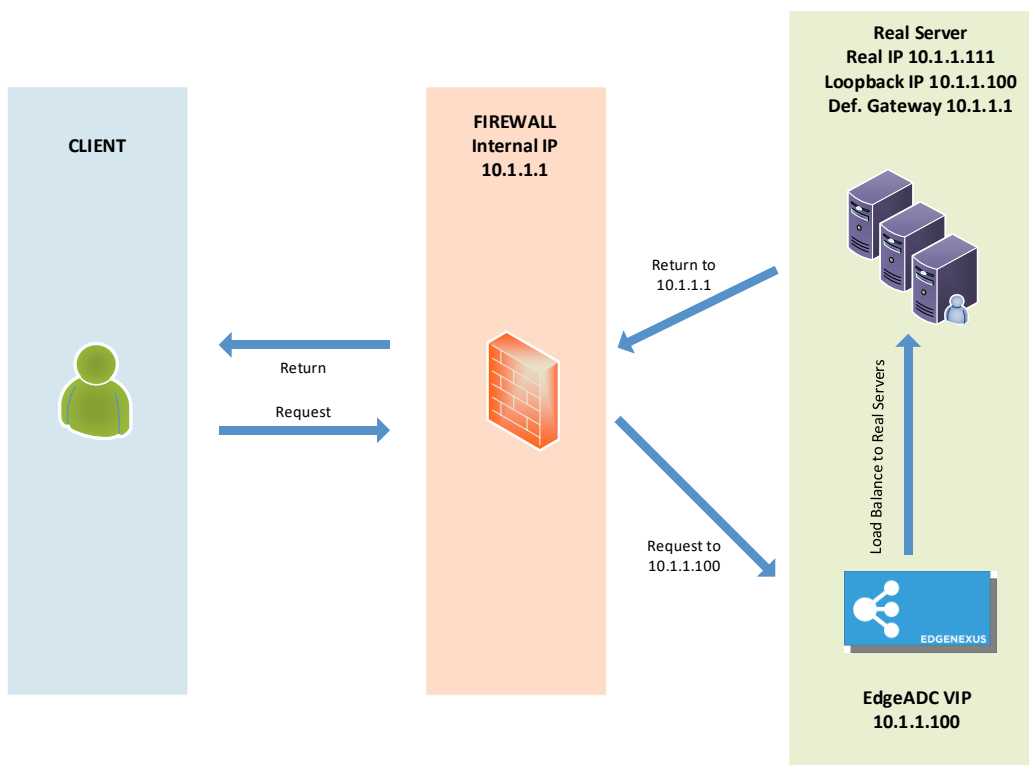
## Real Server Changes for Direct Server Return

Direct Server Return or DSR as it's widely known (DR – Direct Routing in some circles), allows the server behind the ADC to respond directly to the client, bypassing the ADC on the response. DSR is only suitable for use with Layer 4 load balancing. Caching and Compression are not available when enabled.

Layer 7 load balancing with this method will not work as there is no persistence support other than source IP. SSL/TLS load balancing with this method is not ideal as there is only source IP persistence support.

### How it Works

- The client sends a request to the EdgeADC VIP
- Request received by EdgeADC
- Request routed to content servers
- Response sent directly to the client without passing through EdgeADC



## Required Content Server Configuration

### General

- The content server default gateway should be configured as normal. (Not via the ADC)
- The content server and the load balancer must be in the same subnet

### Windows

- The content server needs to have a loopback or Alias configure with the IP address of the Channel or VIP
  - Network metric must be 254 to prevent response to ARP requests
  - Add a loopback adapter in Windows Server 2012 – [Click here](#)
  - Add a loopback adapter in Windows Server 2003/2008 – [Click here](#)
- Run the following in a command prompt for each network interface you have configured on the Windows Real Servers

*netsh interface ipv4 set interface "Windows network interface name" weakhostreceive=enable*

*netsh interface ipv4 set interface "Windows loopback interface name"  
weakhostreceive=enable*

*netsh interface ipv4 set interface "Windows loopback interface name" weakhostsend=enable*

## Linux

- Add a permanent loopback interface
- Edit "/etc/sysconfig/network-scripts"

*ifcfg-lo:1*

*DEVICE=lo:1*

*IPADDR=x.x.x.x*

*NETMASK=255.255.255.255*

*BROADCAST=x.x.x.x*

*ONBOOT=yes*

- Edit "/etc/sysctl.conf"

*net.ipv4.conf.all.arp\_ignore = 1*

*net.ipv4.conf.eth0.arp\_ignore = 1*

*net.ipv4.conf.eth1.arp\_ignore = 1*

*net.ipv4.conf.all.arp\_announce = 2*

*net.ipv4.conf.eth0.arp\_announce = 2*

*net.ipv4.conf.eth1.arp\_announce = 2*

- Run "sysctl -p"

## Real Server Changes – Gateway Mode

Gateway mode allows you to route all traffic through the ADC, and this allows traffic originating from the content servers to be routed via the ADC to other networks via the interfaces on the ADC unit. Using the device as a gateway device for content servers should be used when running in multi-interface mode.

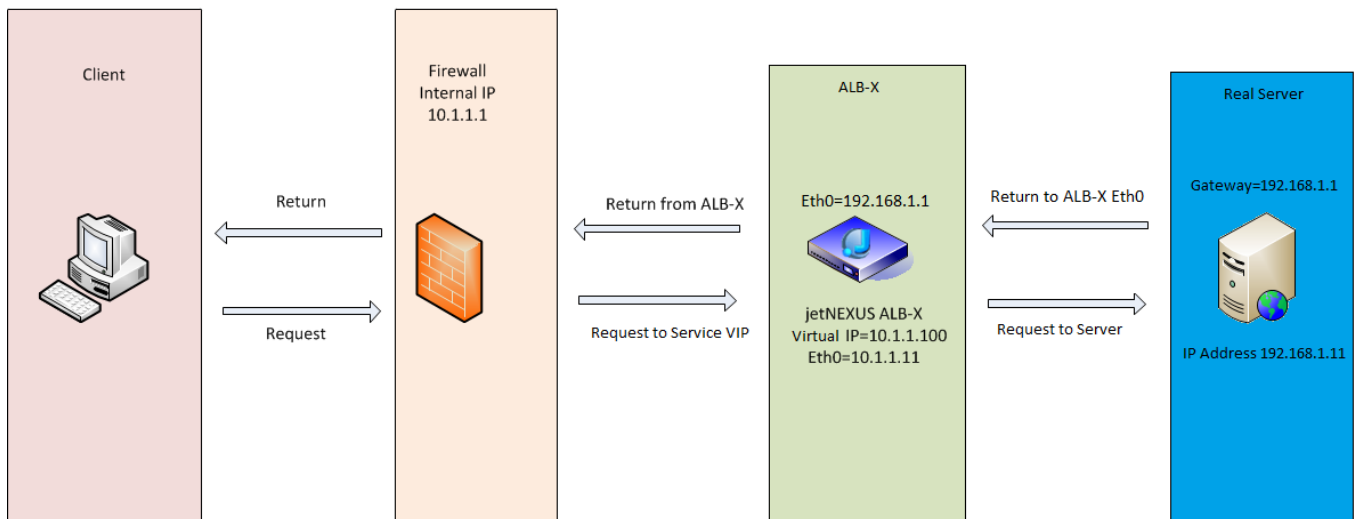
### How it works

- The client sends a request to the EdgeADC
- A request is received by EdgeADC
- Request sent to content servers
- Response sent to EdgeADC
- ADC routes the response to the client

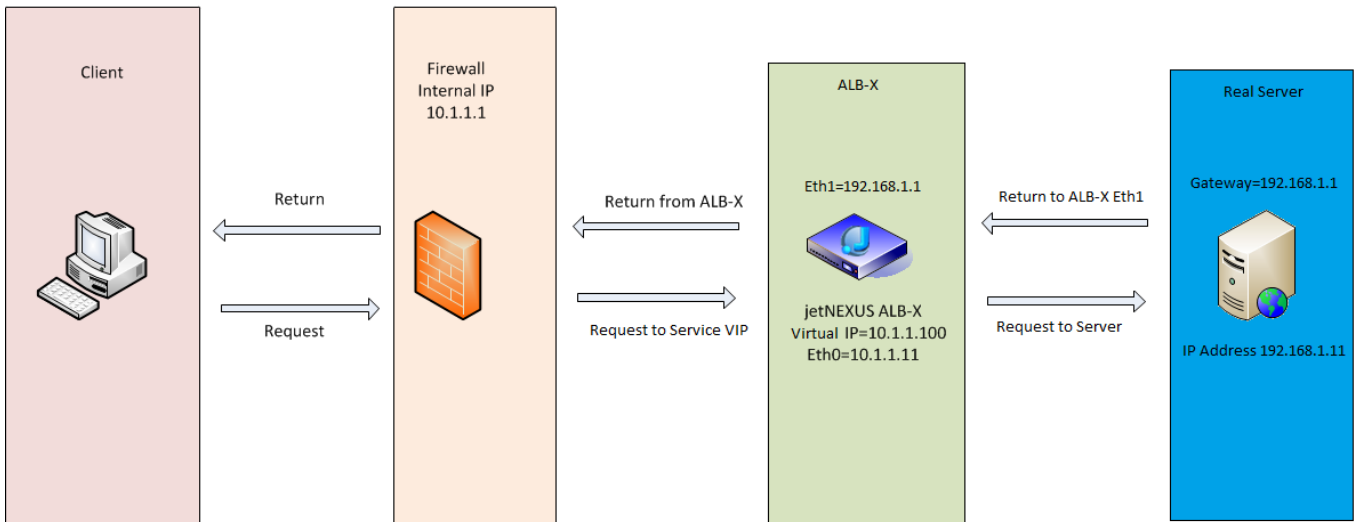
### Required Content Server Configuration

- Single Arm Mode – one interface is utilized, but the service VIP and the Real Servers must be on different subnets.
- Dual Arm Mode – two interfaces are utilized, but the service VIP and real servers must be on different subnets.
- In each case, Single and Dual Arm, the Real Servers need to configure their default gateway to the ADC interface address on the relevant subnet.

### Single Arm example



### Dual Arm example



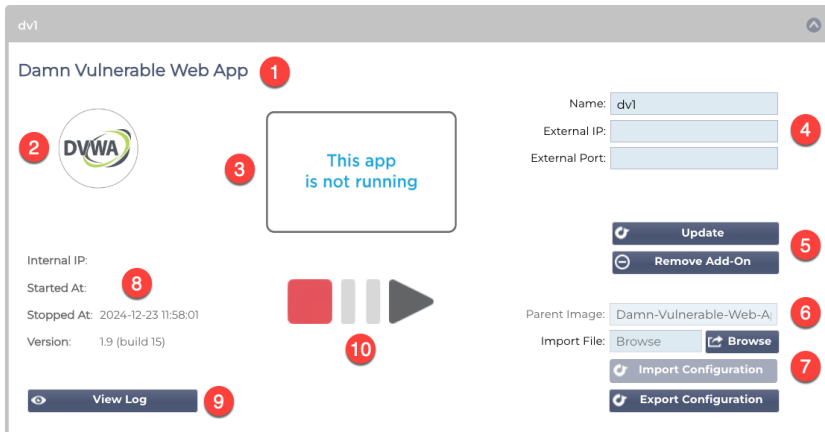


# Library

## Add-Ons

Add-ons are Apps that are loaded in as containers and run in an isolated mode within the ADC. Examples of Add-ons could be an application firewall or even a micro instance of the ADC itself.

An App is deployed to the Add-Ons section using the Apps page, as described in this guide. Once deployed an App appears like this.



As you can see from the image shown above, there are several elements that are highlighted.

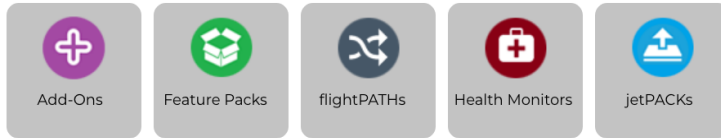
Item	Description
1	App Title
2	App Icon
3	App running display. If the App is running it will show a miniature of the screen.
4	Access details: <b>Name:</b> This is an internal name you use to refer to the App from within the Virtual Services section. It is not possible to reference an App using its IP address. Alphanumeric only, with no spaces. <b>External IP:</b> This is the IP address you must provide for the App. This will be part of your network subnet. <b>External Port:</b> <b>This is an important field.</b> You will need to specify the ports that will be used to access the App. When traffic external to the App is accessing it, you will need to specify it using the following notation: 53/tcp or 53/udp. In addition to this, you will need to specify the UI port for the App. These are shown in the field tooltip for each App.
5	Update button: Once you have filled in the details specified in 4, click this button to confirm the entries and configure the App. The Remove Add-On button is used to remove it from the Apps section. In order to remove an App, please ensure that all references to the App are also removed prior to attempting removal.
6	Parent Image is an informative field and is unused from a user perspective.
7	Importing and exporting a configuration is important to keep a backup of the settings. Use this to perform the Import and Export function.
8	Run details provide information on the Internal API IP address, start and stop time, and version number of the App.
9	This button allows you to download and view the log. This is primarily used when you need to open a support ticket.
10	Operation of the App is carried out using these buttons. Red=Stopped, Gold=Paused and Green=Running.

## Apps

The Apps section has several sub-sections that handle the Apps available for use on the ADC. These are the Filter, Downloaded Apps and Purchased Apps.

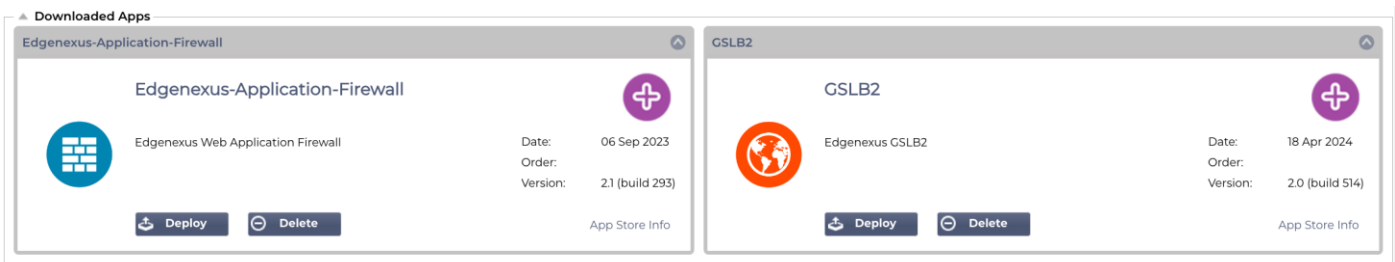
### The Filter

Click icons to toggle groups of apps



The Filter allows you to filter the Apps/tools by their type.

### Downloaded Apps

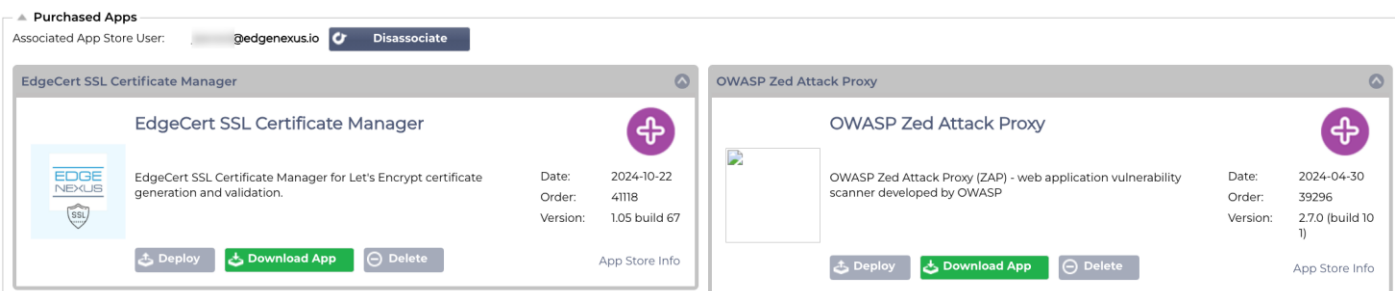


This section contains the Apps that have been downloaded onto the ADC. You may have downloaded them to your local desktop, and subsequently uploaded them to the ADC, or you may have downloaded them via the inbuilt App Store portal.

Each App is equipped with two buttons, as well as data that indicates their version number and date it was released.

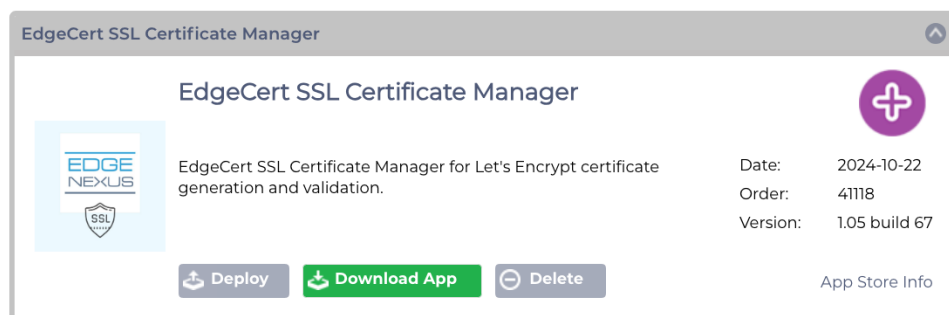
The Deploy button will deploy the App as a secured container, while the Delete button will delete the App from within the ADC.

### Purchased App



The first thing you will note is the Associated App Store User and its associated button. You will need to log in using your App Store credentials so that the ADC is associated with the App Store. Underneath this you will find the Apps associated with your account.

When you log into the App Store, either directly or via the inbuilt portal, you can purchase Apps. These are indicated within this section and can be uploaded to the ADC ready for deployment.



Each App has a number of buttons: Deploy, Download App and Delete. In addition to this, there is also an App Store Info link on the right side that will take you to the relevant App Store page and show information on the Addon.

### Deploy

The Apps section within Add-Ons details the Apps that you have purchased, downloaded, and deployed. Once deployed the App will appear in the Downloaded section.

### Download App

The App can be downloaded from the App Store by clicking this button.

### Delete

If you wish to delete an App that has been downloaded.

## Authentication

The Library > Authentication page allows you to set up authentication servers and create authentication rules.

### Setting up Authentication – A Workflow

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

To set up a working authentication method, we must first set up an authentication server.

The first stage is to select which authentication method you need.

- Click Add Server.
- Select the Method from the dropdown menu.

▲ Authentication Servers

⊕ Add Server ⊖ Remove Server

Method:  ←

⊕ Update ⊖ Cancel

Name	Description	Method	Domain	Server Address

The Authentication Server function is dynamic and displays only those fields that are required for the authentication method you choose.

- Fill out the fields accurately to ensure proper connection to the servers.

### Options for LDAP, LDAP-MD5, LSAPS, LDAPS-MD5, Radius and SAML

▲ Authentication Servers

⊕ Add Server ⊖ Remove Server

Method:

Name:

Server Address:

Port:

Domain:

Login Format:

Description:

Search Base:

Search Condition:

Search User:  ✖

Password:  ✖

⊕ Update ⊖ Cancel

Name	Description	Method	Domain	Server Address

Option	Description
Method	Choose an authentication method

	<p>LDAP – basic LDAP with usernames and passwords sent in clear text to the LDAP server.                  LDAP-MD5 – basic LDAP with username in clear text and password MD5 hashed for increased security.                  LDAPS – LDAP over SSL. Sends the password in clear text within an encrypted tunnel between the ADC and LDAP server.                  LDAPS-MD5 – LDAP over SSL. The password is MD5 hashed for added security within an encrypted tunnel between the ADC and the LDAP server</p>
Name	Give your server a name for identification purposes – this name is used in any rules.
Server Address	Add the IP address or hostname of the authentication server
Port	For LDAP and LDAPS the ports are set to 389 and 636 by default. For Radius the port is generally 1812. For SAML, the ports are set in the ADC.
Domain	Add in the domain name for the LDAP server.
Login Format	<p>Use the login format you need.</p> <p>Username – with this format chosen, you need only enter the username. Any user and domain information entered by the user is deleted, and the domain information from the server is used.</p> <p>Username and Domain – The user must enter the whole domain and username syntax. Example: <i>mycompany\jdoe</i> OR <i>jdoe@mycompany</i>. The domain information entered at the server level is ignored.</p> <p>Blank – the ADC will accept anything the user inputs and send it on to the authentication server. This option is used when using MD5.</p>
Description	Add a description
Search Base	This value is the starting point for the search in the LDAP database. Example <i>dc=mycompany,dc=local</i>
Search Condition	Search conditions must conform to RFC 4515. Example: (MemberOf=CN=Phone- VPN,CN=Users,DC=mycompany,DC=local).
Search User	Perform a search for a domain admin user within the directory server.
Password	Password for the domain admin user.
Dead Time	The amount of time after which an inactive server is marked as active again

### Options for SAML Authentication

**IMPORTANT: When setting up authentication via SAML, you are required to create an Enterprise App for Entra ID Authentication. The instructions for doing this are available in chapter, Setting up the Entra ID Authentication Application in Microsoft Entra**

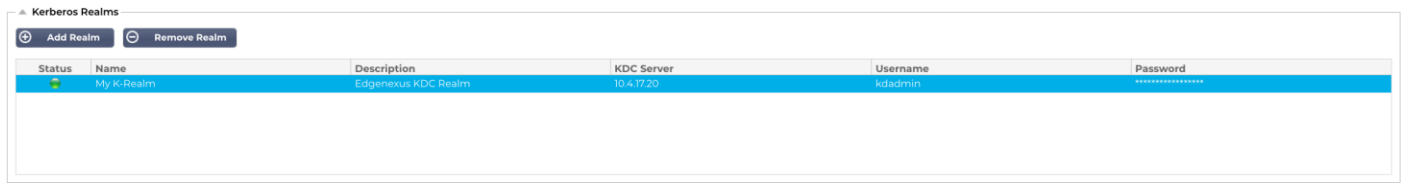
The screenshot shows the 'Authentication Servers' configuration page. At the top, there are 'Add Server' and 'Remove Server' buttons. The 'Method' is set to 'SAML'. Below this, there are two columns of fields: 'Identity Provider' and 'Server Provider'. The 'Identity Provider' fields include 'IdP Certificate match' (checkbox), 'IdP Entity ID', 'IdP SSO URL', 'IdP Logoff URL', and 'IdP Certificate'. The 'Server Provider' fields include 'Description', 'SP Entity ID', 'SP Signing Certificate' (dropdown), and 'SP Session Timeout' (set to 900). At the bottom of the form are 'Update' and 'Cancel' buttons. Below the form is a table with columns: Name, Description, Method, Domain, and Server Address. The table is currently empty.

Option	Description
Method	Choose an authentication method LDAP – basic LDAP with usernames and passwords sent in clear text to the LDAP server. LDAP-MD5 – basic LDAP with username in clear text and password MD5 hashed for increased security. LDAPS – LDAP over SSL. Sends the password in clear text within an encrypted tunnel between the ADC and LDAP server. LDAPS-MD5 – LDAP over SSL. The password is MD5 hashed for added security within an encrypted tunnel between the ADC and the LDAP server
Name	Give your server a name for identification purposes – this name is used in any rules.
<b>Identity Provider</b>	
IdP Certificate Match	IdP Certificate Match refers to the process of verifying that the digital certificate used by an Identity Provider (IdP) to sign SAML assertions matches the certificate that the Service Provider (SP) trusts. This validation ensures that the IdP is legitimate and that the assertions it sends are authentic and unaltered. The SP typically stores the IdP's certificate in its metadata, and it compares the certificate embedded in the SAML assertions against the stored one to determine a match.
IdP Entity ID	A SAML IdP Entity ID is a globally unique identifier that serves as the definitive address for an Identity Provider (IdP) within the Security Assertion Markup Language (SAML) ecosystem. This identifier is typically a URL or URI that uniquely distinguishes the IdP from other entities involved in SAML-based authentication and authorization processes. It plays a crucial role in establishing trust and facilitating secure communication between IdPs, Service Providers (SPs), and users.
IdP SSO URL	An IdP SSO URL, short for Single Sign-On URL, is a specific endpoint URL provided by an identity provider (IdP) that serves as the authentication gateway for initiating single sign-on (SSO) sessions. Upon redirecting a user to this URL, the IdP prompts them to authenticate using their credentials, and upon successful authentication, it redirects them back to the service provider (SP) with an assertion containing their identity information. This assertion is then validated by the SP, allowing the user to access the SP's resources without having to re-authenticate.
IdP Log off URL	The SAML IdP Log off URL is a specific endpoint on the Identity Provider (IdP) that initiates and manages the logout process for Single Sign-On (SSO) sessions. When a user clicks the logout button on an application, the application redirects the user to the IdP's Log off URL. The IdP then invalidates the user's session on all relying parties associated with the SSO authentication and sends a logout response back to the application, effectively logging the user out of all connected applications.
IdP Certificate	A SAML IdP Certificate is an X.509 digital certificate issued by a trusted authority to an identity provider (IdP) that participates in Security Assertion Markup Language (SAML) authentication protocols. This certificate serves as a secure means of verifying the identity of the IdP and authenticating the integrity and confidentiality of SAML messages exchanged between the IdP and service providers (SPs). You can select the IdP Certificate that you will have installed in the ADC using the drop-down menu.
Description	A description for the definition.
Search User	Perform a search for a domain admin user.
Password	For specifying the password for the admin user.
<b>Server Provider</b>	
SP Entity ID	An SP Entity ID is a unique identifier that serves as a global address for a specific Service Provider (SP) in the context of the SAML protocol. It is a standardized way to identify an SP and is typically a URL or other URI that pinpoints the SP's SAML metadata, which contains critical information like encryption certificates and authentication endpoints.

SP Signing Certificate	A SAML SP Signing Certificate is an X.509 certificate used by a Service Provider (SP) to sign SAML responses, ensuring the authenticity and integrity of the messages exchanged between the SP and Identity Provider (IdP) during Single Sign-On (SSO) authentication. The SP signs the response using its private key, and the IdP verifies the signature using the public key associated with the certificate, confirming the sender's identity and the message's contents have not been tampered with.
SP Session timeout	SP Session Timeout refers to the maximum duration for which a user's authentication session is considered valid on the Service Provider (SP) side after successful Single Sign-On (SSO) through an Identity Provider (IdP). After this specified time, the SP terminates the session and requires the user to reauthenticate to regain access to protected resources. This mechanism helps protect against unauthorized access and ensures that user sessions are not idle for extended periods.

## KDC Realms

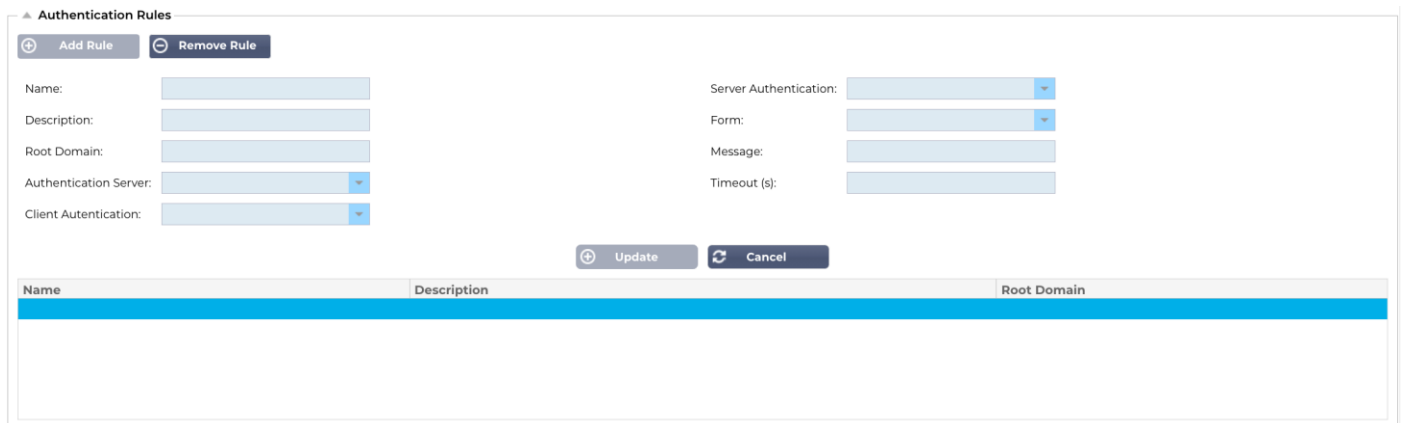
KDC Realms refer to configurations within the Kerberos authentication protocol, where each realm is essentially a domain or network that operates under a single Key Distribution Center (KDC). This setup delineates a group of systems that are managed under the same master KDC, facilitating secure authentication and ticket-granting mechanisms across the network. Realms can be hierarchical or non-hierarchical, with the possibility of establishing trust relationships between them for secure inter-realm authentication .



The user interface provided in the ADC, as shown in the image above, allows you to define your Kerberos realms. This information can then be used within Authentication rules.

## Authentication Rules

The next stage is to create the authentication rules for use with the server definition.



Field	Description
Name	Add a suitable name for your authentication rule.
Description	Add a suitable description.
Root Domain	This must be left blank unless you need single-sign-on across sub-domains.
Authentication Server	This is a dropdown box containing servers that you have configured.



Client Authentication:	Choose the value appropriate to your needs: Basic (401) – This method uses the standard 401 authentication method Forms – this will present the ADC default form to the user. Within the form, you can add a message. You can select a form that you have uploaded using the section below.
Server Authentication	Choose the appropriate value. None – if your server does not have any existing authentication, select this setting. This setting means that you can add authentication abilities to a server that previously had none. Basic – if your server has basic authentication (401) enabled, then select BASIC. NTLM – if your server has NTLM authentication enabled, then select NTLM.
Form	Choose the appropriate value Default – Selecting this option will result in the ADC using its built-in form. Custom – you can add a form that you have designed and select it here.
Message	Add a personal message to the form.
Timeout	Add a timeout to the rule, after which the user will be required to authenticate again. Note the Timeout setting is only valid for Forms-based authentication.

If you wish to provide a single sign-on for users, complete the Root Domain field with your domain. In this example, mycompany.com. We can now have multiple services that will use edgenexus.io as the root domain, and you will only have to log in once. If we consider the following services:

- [SharePoint.mycompany.com](#)
- [usercentral.mycompany.com](#)
- [App Store.mycompany.com](#)

These services can reside on one VIP or can be distributed across 3 VIPs. A user accessing usercentral.mycompany.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 can then connect to App Store.mycompany.com and will be authenticated automatically by the ADC. You can set the timeout, which will force authentication once this period of inactivity has been reached.

## Forms

The screenshot shows a web interface for managing forms. At the top, there is a section titled 'Forms' with an expand/collapse arrow. Below this, there is a 'Form Name' label followed by a text input field. To the right of the input field is a small icon. Below the input field are three more input fields: one for a file path, one for a file type dropdown, and one for a file size. To the right of these fields are four buttons: 'Browse' (with a folder icon), 'Upload' (with an upload icon), 'Preview' (with a magnifying glass icon), and 'Remove' (with a minus icon).

This section will enable you to upload a custom form.

### How to create your custom form

Although the basic form the ADC provides is sufficient for most purposes, there will be occasions where companies wish to present their own identity to the user. You can create your custom form that users will be presented with to fill in in such cases. This form must be in either HTM or HTML format.

Option	Description
Name	form name = loginform action = %JNURL% Method = POST
Username	Syntax: 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 code of a very basic and 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>
</HTML>
```

#### Adding a custom form

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

1. [Choose a name for your form](#)
2. [Browse locally for your form](#)
3. [Click Upload](#)

#### Previewing your custom form

The screenshot shows a web interface for managing forms. At the top, there is a section titled 'Forms'. Below this, there is a 'Form Name' label followed by an input field. To the right of the input field are four buttons: 'Browse', 'Upload', 'Preview', and 'Remove'. The 'Preview' and 'Remove' buttons have a minus sign icon. A dropdown menu is open below the 'Form Name' input field, showing the text 'default'.

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

Note: When using cookie filtering products such as AdGuard, you may get a 404-error message. Whitelist the ADC's IP address to prevent this.

# Cache

The ADC is capable of caching data within its internal memory and enhances the delivery of web services. The settings that manage this functionality are provided within this section.

**▲ Global Cache Settings**

Maximum Cache Size (MB):	<input type="text" value="50"/>	<input type="button" value="↑"/>	<input type="button" value="↓"/>	
Desired Cache Size (MB):	<input type="text" value="30"/>	<input type="button" value="↑"/>	<input type="button" value="↓"/>	
Default Caching Time (D/HH:MM):	<input type="text" value="1"/>	<input type="button" value="↑"/>	<input type="button" value="↓"/>	<input type="text" value="00:00"/>
Cacheable HTTP Response Codes:	<input type="text" value="200 203 301 304 410"/>			
Cache Checking Timer (D/HH:MM):	<input type="text" value="0"/>	<input type="button" value="↑"/>	<input type="button" value="↓"/>	<input type="text" value="03:00"/>
Cache-Fill Count:	<input type="text" value="20"/>	<input type="button" value="↑"/>	<input type="button" value="↓"/>	

Force a check on the cache size


Remove all items from the cache

## Global Cache Settings

### Maximum Cache Size (MB)

This value determines the maximum RAM that the Cache can consume. The ADC Cache is an in-memory cache that is also periodically flushed to the storage medium to maintain cache persistence after restarts, reboots, and shutdown operations. This functionality 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 the available memory.

### Desired Cache Size (MB)

This value denotes the optimum RAM to which the Cache will be trimmed. 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 to trim 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 Caching Time (D/HH:MM)

The value entered here represents the life of content without an explicit expiry value. The default caching time is the period for which content without a "no-store" directive or explicit expiry time in the traffic header is stored.

The field entry takes the form "D/HH:MM" – so an entry of "1/01:01" (default is 1/00:00) means to store the ADC will hold the content for one day, "01:00" for one hour, and "00:01" for one minute.

### Cacheable HTTP Response Codes

One of the cached data sets is HTTP responses. The HTTP response codes that are cached are:

- 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 Timer (D/HH:MM)

This setting determines the time interval between cache trim operations.

## Cache-Fill Count

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

## Apply Cache Rule

Apply Cache Rule

Other Domains Served

Domain Name:

Name	Caching Rulebase
jet.io	Images

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

- Add domain manually with the Add Records button. You must use a fully qualified domain name or an IP address in dotted-decimal notation. Example www.mycompany.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

Create Cache Rule

Cache Content Selection Rulebases:

Rule Name	Description	Conditions
Images	Caches most images	include *.jpg include *.gif include *.png

This section allows you to create several 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 your conditions in manually or use the Add Condition

To add a condition using the Selection Rulebase:

Create Cache Rule

Cache Content Selection Rulebases:

Rule Name	Description	Conditions
Images	Caches most images	include *.jpg include *.gif include *.png

[ Timed licence 10 days left ]

- Choose Include or Exclude.
- Choose a selection criterion, for example, 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.

## flightPATH

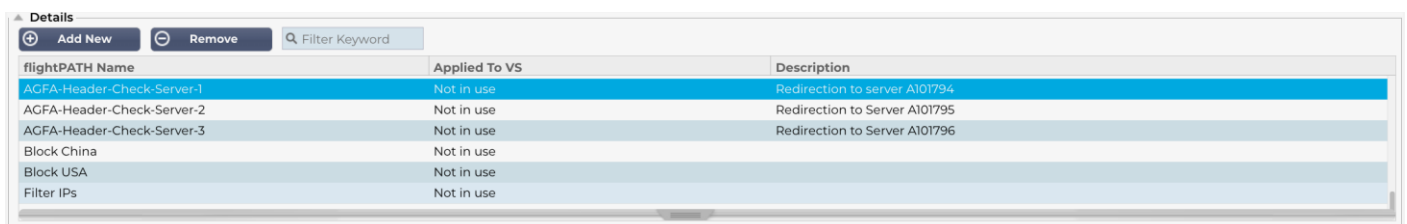
flightPATH is the traffic management technology built into the ADC and allows the inspection of HTTP and HTTPS traffic in real-time and perform actions based on conditions.

To use flightPATH rules, they must be applied to a Virtual Service using the flightPATH tab within the Real Servers section.

A flightpath rule consists of four elements:

1. Details, where you define the flightPATH Name and Service to which it is attached.
2. Condition(s) that can be defined that cause the rule to be triggered.
3. Evaluation that allows the definition of variables that can be used within Actions.
4. Actions that are used to manage what should happen when conditions are met.

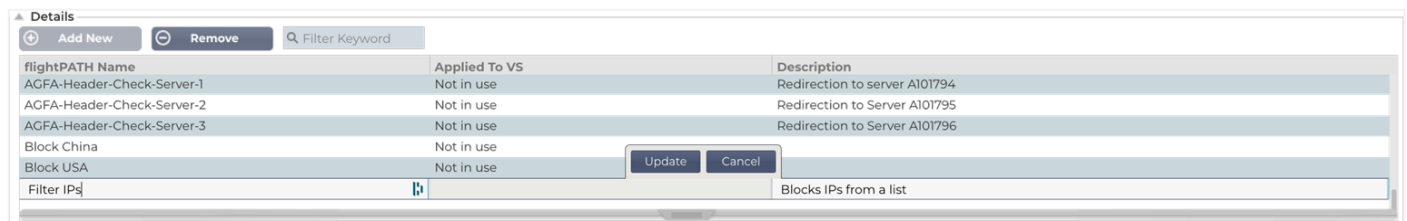
### Details



flightPATH Name	Applied To VS	Description
AGFA-Header-Check-Server-1	Not in use	Redirection to server A101794
AGFA-Header-Check-Server-2	Not in use	Redirection to Server A101795
AGFA-Header-Check-Server-3	Not in use	Redirection to Server A101796
Block China	Not in use	
Block USA	Not in use	
Filter IPs	Not in use	

The details section shows the available flightPATH rules. You can add new flightPATH rules and remove defined ones from this section.

### Adding a new flightPATH rule



flightPATH Name	Applied To VS	Description
AGFA-Header-Check-Server-1	Not in use	Redirection to server A101794
AGFA-Header-Check-Server-2	Not in use	Redirection to Server A101795
AGFA-Header-Check-Server-3	Not in use	Redirection to Server A101796
Block China	Not in use	
Block USA	Not in use	
Filter IPs		Blocks IPs from a list

Field	Description
FlightPATH Name	This field is for the name of the flightPATH rule. The name you provide here appears in and is referenced within other parts of the ADC.
Applied to VS	This column is read-only and shows the VIP to which the flightPATH rule is applied.
Description	Value representing a description provided for readability purposes.

#### Steps to add a flightPATH rule

1. First, click the Add New button located in the Details section.
2. Enter a name for your rule. Example Auth2
3. Enter a description of your rule
4. Once the rule has been applied to a service, you will see the Applied To column auto-populate with an IP address and port value
5. Don't forget to hit the Update button to save your changes or if you make a mistake, just hit cancel revert to the previous state.

## Condition

A flightPATH rule can have any number of conditions. The conditions work on an **AND** basis allow you to set the condition on which the action is triggered. If you want to use an **OR** condition, create additional flightPATH rules and apply it to the VIP in the correct order.

The screenshot shows a configuration window titled "Condition" with "Add New" and "Remove" buttons. Below is a table with the following data:

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

You can also use RegEx by selecting Match RegEx in the Check field and the RegEx value in the Value field. The inclusion of RegEx evaluation extends the capability of flightPATH tremendously.

### Creating a new flightPATH condition

The screenshot shows the "Condition" configuration window with two rows in the table. The second row is in an edit state:

Condition	Match	Sense	Check	Value
Path		Does	Match RegEx	\.htm\$
Host	Type a new Match	Does	Contain	mycompany.com

Below the table are "Update" and "Cancel" buttons.

You first have to select a value from the Condition column.

We provide several Conditions within the dropdown and cover all foreseen scenarios. When new Conditions are added, these will be available through Jetpack updates.

Choices available are:

CONDITION	DESCRIPTION	EXAMPLE
<form>	HTML forms are used to pass data to a server	Example "form doesn't have length 0"
GEO Location	Compares the source IP address to the ISO 3166 Country Codes	GEO Location does equal GB, OR GEO Location does equal Germany
Host	Host extracted from the URL	www.mywebsite.com or 192.168.1.1
Language	Language extracted from the language HTTP header	This condition will produce a dropdown with a list of Languages
Method	Dropdown of HTTP methods	Dropdown that includes GET, POST, etc
Origin IP	If upstream proxy supports X-Forwarded-for (XFF) it will use the true Origin address	Client IP. It can also use multiple IPs 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	Path of the website	/mywebsite/index.asp
POST	POST request method	Check data being uploaded to a website
Query	Name and value of a query, and 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	Name of a cookie requested by a client	MS-WSMAN=afYfn1CDqqCDqUD::

Request Header	Any HTTP Header	Referrer, User-Agent, From, Date
Request Version	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	The name of a cookie sent by the server	MS-WSMAN=afYfn1CDqqCDqUD::
Response Header	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	Either the origin IP, proxy server IP, or some other aggregated IP address	Client IP, Proxy IP, Firewall IP. Can also use multiple IP and subnets. You must escape the dots as these are RegEX. Example 10\.\1\.\2\.\3 is 10.1.2.3

## Match

The Match field can be either a drop-down or a text value and is definable depending on the value in the Condition field. For example, if the Condition is set to Host, the Match field is not available. If the Condition is set to <form>, the Match field is shown as a text field, and if the Condition is POST, the Match field is presented as a drop-down containing pertinent values.

Choices available are:

MATCH	DESCRIPTION	EXAMPLE
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 QWxhZGRpbjpvYVUHNlc2FtZQ==
Charge-To	Contains account information for the costs of the application of the method requested	
Content-Encoding	The type of encoding used	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 the 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	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

## Sense

The Sense field is a drop-down Boolean field and contains either Does or Doesn't choices.

## Check

The Check field allows the setting of check values against the Condition.

Choices available are: Contain, End, Equal, Exist, Have Length, Match RegEx, Match List, Start, Exceed Length

CHECK	DESCRIPTION	EXAMPLE
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.edgenexus.io
Have Length	The string does have a length of the value	Host >Does >Have Length >16 www.edgenexus.io = TRUE www.edgenexus.com = FALSE

Match RegEx	Enables you to enter a full Perl compatible regular expression	Origin IP > Does > Match Regex
Match List	Enables you to match the value against a list of values. This is useful when there are say, specific IP addresses that need matching against. Values are separated using commas (,) or pip ( ).	Source IP > Does > Match List > 10.10.10.1, 10.10.10.2, 10.10.10.3 etc
Exceed Length	Allows you to check if the value exceeds the length specified.	Path > Does > Exceed Length > 200

### Steps to add a Condition

Adding a new flightPATH Condition is very easy. An example is shown above.

1. Click the Add New button within the Condition area.
2. Choose a condition from the drop-down box. Let's take Host as an example. You can also type into the field, and the ADC will show the value in a drop-down.
3. Choose a Sense. For example, Does
4. Choose a Check. For example, Contain
5. Choose a value. For example, mycompany.com

Condition	Match	Sense	Check	Value
Request Header	Request Header	Does	Contain	image
Host	Host	Does	Equal	www.imagepool.com

The above example shows that there are two conditions that both have to be TRUE for the rule to complete

- The first is checking that the requested object is an image
- The second checks whether the host in the URL is www.imagepool.com

### Evaluation

The ability to add definable variables is a compelling capability. Other ADC's offer this capability using scripting or command-line options that are not ideal for anyone. The EdgeADC allows you to define any number of variables using an easy-to-use GUI, as shown and described below.

flightPATH variable definition comprises four entries that need to be made.

- Variable – this is the name of the variable
- Source – a drop-down list of possible source points
- Detail – select values from a drop-down or manually typed.
- Value – the value that the variable holds and can be an alphanumeric value or a RegEx for fine-tuning.

### Built-in Variables:

Built-In variables have already been hardcoded, so you do not need to create an evaluation entry for these.

You can use any of the variables listed below in the Action section.

- \$sourceip\$ - The source IP address of the request
- \$sourceport\$ - The source port that was used
- \$clientip\$ - The IP address of the client
- \$clientport\$ - The port used by the client
- \$host\$ - The host named in the request
- \$method\$ - The method used: GET, POST etc

- \$path\$ - The path specified in the request
- \$querystring\$ - The querystring used in the request
- \$version\$ - The version of the HTTP request in the REQUEST (only 1 and 1.1 allowed at present).
- \$resp\$ - The RESPONSE from the server. eg. 200OK, 404 etc.
- \$geolocation\$ - The GEO location from where the request originated.

ACTION	TARGET
Action = Redirect 302	Target = HTTPs://\$host\$/404.html
Action = Log	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 the browser’s 404 Error page
- Instead, the user is redirected to the original hostname they used, but the incorrect path is replaced with 404.html
- An entry is added to the Syslog saying, "A client from 154.3.22.14:3454 has just requested the wrong.html page."

**Action**

The next stage in the process is to add an action associated with the flightPATH rule and condition.



In this example, we want to rewrite the path portion of the URL to reflect the URL typed by the user.

- Click Add New
- Choose Rewrite Path from the Action drop-down menu
- In the Target field, type in \$path\$/myimages
- Click Update

This action will add /myimages to the path, so the final URL becomes [www.imagepool.com/myimages](http://www.imagepool.com/myimages)

Action	Description	Example
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	Remove response cookie detailed in the Target section Cookie	Target=jnAccel
Remove Response	Remove the response header detailed in Target section Header	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	Replace the response cookie detailed in Target section with value in Data section Cookie	Target=jnAccel=afYfn1CDqqCDqCVii Date=MSWSMAN=afYfn1CDqqCDqCVii
Replace Response	Replace the response header detailed in Target section with value in Data section Header	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

## A flightPATH rule scenario

A customer has an e-commerce site and is having issues with cookies being blocked by the latest versions of a browser.

The customer traces the issues and finds the root cause to be the lack of 'secure' and 'same-site' tagging for the cookies in question.

Let's look at how flightPATH can help.

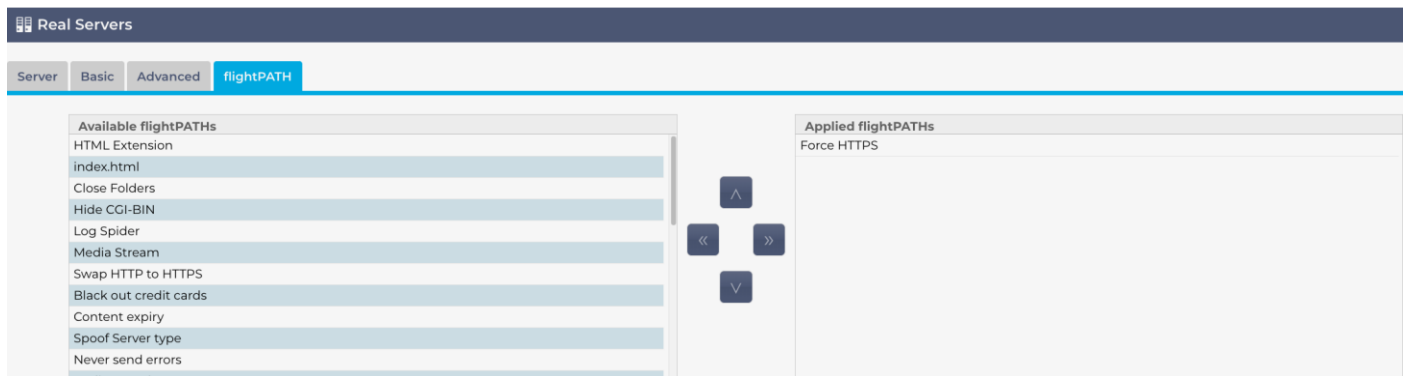
- We have a cookie by the name 'wp\_woocommerce\_session\_97929973749972642'
- The name of the cookie is 'wp\_woocommerce\_session\_' with a random unique ID value of '97929973749972642' generated by the e-commerce system.
- The tags for 'same-site' and 'secure' tags appear to be blank, hence the cookie is blocked by the browser's new security restrictions.
- To prevent this happening, we can create the following flightPATH rules.
- **flightPATH Rule for Session ID**
  - **Condition:**  
Leave blank
  - **Evaluation:**  
Variable = \$variable\_1\$  
Source = Response cookie  
Detail = wp\_woocommerce\_session\_\*
  - **Action:**  
Action = Replace Response Cookie  
Target = wp\_woocommerce\_session\_\*  
Data = \$variable\_1\$
- **flightPATH Rule for Tags**

- **Condition:**  
Condition = Response Cookie  
Match = woocommerce\_cart\_hash  
Sense = Does  
Check = Exist  
Value = Leave blank
- **Evaluation:**  
Variable = \$variable\_2\$  
Source = Response Cookie  
Detail = woocommerce\_cart\_hash  
Value = Leave blank
- **Action:**  
Action = Replace Response Cookie  
Target = woocommerce\_cart\_hash  
Data = \$variable\_2\$,SameSite=None,Secure

Now you apply the rules to the Virtual Service(s) that require them.

## Applying the flightPATH rule

The application of any flightPATH rule is made within the flightPATH tab of each VIP/VS.



- Navigate to Services > IP Services and choose the VIP to which you wish to assign the flightPATH rule.
- You will see the Real Server list shown below
- Click on the flightPATH tab
- Select the flightPATH rule you have configured or one of the pre-built ones supported. You can select multiple flightPATH rules if required.
- Drag and drop the selected set to the Applied flightPATHs section or click the >> arrow button.
- The rule will be moved to the right side and automatically applied.

# Real Server Monitors

Monitoring

▲ Details

⊕ Add Monitor   ⊖ Remove

Name	Description	Monitoring Method	Applied To VS
200OK	Check home page for 200 OK	HTTP 200 OK	Not in use
DICOM	Monitor DICOM server	DICOM	Not in use
Check Page Returns	Check a page returns Success	HTTP Response	Not in use

---

Name:       User Name:

Description:       Password:

Monitoring Method:       Threshold:

Page Location:       SSL/TLS:

Required Content:

⊕ Update   ⊖ Cancel

Monitoring real servers is important in a load balancing scenario to detect and respond to server issues, ensure balanced load distribution, optimize resource utilization, prioritize critical services, and identify and address software vulnerabilities.

The Library > Real Server Monitors page allows you to add, view and edit custom monitoring. These are Layer 7 server "Health Checks" and select them from the Server Monitoring field within the Basic tab of the Virtual service you define.

## Types of Real Server Monitors

There are several Real Server Monitors available, and the table below explains these. You can, of course, write additional monitors using PERL.

Monitoring Method	Description	Example
HTTP 200 OK	<p>A TCP connection is made to the Real Server. After the connection is made, a brief HTTP request is sent to the Real Server. When the response is received, it is checked for the '200 OK' string. If it is present, the server is considered operational. Please note that using this monitor fetches the entire page with contents.</p> <p>This monitoring method can only really be used with HTTP and Accelerated HTTP service types. However, 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 Real Server or handled appropriately by the "Content SSL" facility.</p>	<p><b>Request</b>  GET / HTTP/1.1  Host: 192.168.159.200  Accept: */*  Accept-Language: en-gb  User-Agent: Edgenexus-ADC/4.0  Connection: Keep-Alive  Cache-Control: no-cache</p> <p><b>Response</b>  HTTP/1.1 200 OK  Content-Type: text/html  Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT  Accept-Ranges: bytes  ETag: "0dd3253a59ad31:0"  Server: Microsoft-IIS/10.0  Date: Tue, 13 Jul 2021 15:55:47 GMT  Content-Length: 1364</p> <pre>&lt;!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"&gt; &lt;html xmlns="http://www.w3.org/1999/xhtml"&gt; &lt;head&gt;</pre>

		<pre>&lt;meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /&gt; &lt;title&gt;jetNEXUS&lt;/title&gt; &lt;style type="text/css"&gt; &lt;!-- body {     color:#FFFFFF;     ... }&lt;/body&gt; &lt;/html&gt;</pre>
HTTP 200 Head	<p>A TCP connection is made to the Real Server with the PATH field specifying the location to be checked.</p> <p>The head portion of the response is fetched from the server, with contents discarded. The response is checked for 200 OK. If it is present, the server is considered operational. Please note that using this monitor fetches only the head portion.</p> <p>This monitoring method can only really be used with HTTP and Accelerated HTTP service types. However, 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 Real Server or handled appropriately by the "Content SSL" facility.</p>	<p><b>Request</b>  HEAD / HTTP/1.1  Host: 192.168.159.200  Accept: */*  Accept-Language: en-gb  User-Agent: Edgenexus-ADC/4.0  Connection: Keep-Alive  Cache-Control: no-cache</p> <p><b>Response</b>  HTTP/1.1 200 OK  Content-Length: 1364  Content-Type: text/html  Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT  Accept-Ranges: bytes  ETag: "Odd3253a59ad31:0"  Server: Microsoft-IIS/10.0  Date: Tue, 13 Jul 2021 15:49:19 GMT</p>
HTTP 200 Options	<p>A TCP connection is made to the Real Server, and an Options request is made.</p> <p>The Options are returned and checked for 200 OK content.</p> <p>If the 200 OK content is found, then the server is deemed to be available.</p>	<p><b>Request</b>  OPTIONS / HTTP/1.1  Host: 192.168.159.200  Accept: */*  Accept-Language: en-gb  User-Agent: Edgenexus-ADC/4.0  Connection: Keep-Alive  Cache-Control: no-cache</p> <p><b>Response</b>  HTTP/1.1 200 OK  Allow: OPTIONS, TRACE, GET, HEAD, POST  Server: Microsoft-IIS/10.0  Public: OPTIONS, TRACE, GET, HEAD, POST  Date: Tue, 13 Jul 2021 16:23:39 GMT  Content-Length: 0</p>
HTTP Head	<p>The HTTP Head monitor allows us to check for a specific value in the Head portion of the HTTP stream. We can enter a Path and Required Response in the appropriate fields and then check for that value in the response. Should the Required Response value be found in the Head, the server is deemed to be up and available.</p> <p>We can also use this on specially protected pages that need a username and password. In this manner, the monitor's result can be deemed to be accurate.</p> <p>For example, providing <b>/ispagethere.html</b> and <b>200 OK</b> values in the Path and Required Response fields will return a successful result if the server is up, the page is available, and responds to the request.</p>	<p><b>Request</b>  HEAD /ispagethere.htm HTTP/1.1  Host: 192.168.159.200  Accept: */*  Accept-Language: en-gb  User-Agent: Edgenexus-ADC/4.0  Connection: Keep-Alive  Cache-Control: no-cache</p> <p><b>Response</b>  HTTP/1.1 200 OK  Content-Length: 1364  Content-Type: text/html  Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT  Accept-Ranges: bytes  ETag: "Odd3253a59ad31:0"  Server: Microsoft-IIS/10.0  Date: Wed, 14 Jul 2021 08:28:18 GMT</p>



	<p>This monitoring method can only really be used with HTTP and Accelerated HTTP service types. However, 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 Real Server or handled appropriately by the "Content SSL" facility.</p>	
HTTP Options	<p>The HTTP Options monitor allows you to check for a specific value within the returned Options data.</p> <p>We enter a Path and Required Response in the appropriate fields and then check the response.</p> <p>If the Required Response is found in the Options data, the server is available and running.</p> <p>The Required Response values can be any of the following: OPTIONS, TRACE, GET, HEAD, and POST.</p> <p>For example, providing <b>/ispagethere.html</b> and <b>GET</b> values in the Path and Required Response fields will return a successful result if the server is up, the page is available, and it responds to the request.</p> <p>This monitoring method can only really be used with HTTP and Accelerated HTTP service types. However, 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 Real Server or handled appropriately by the "Content SSL" facility.</p>	<p><b>Request</b>  OPTIONS /ispagethere.htm HTTP/1.1  Host: 192.168.159.200  Accept: */*  Accept-Language: en-gb  User-Agent: Edgenexus-ADC/4.0  Connection: Keep-Alive  Cache-Control: no-cache</p> <p><b>Response</b>  HTTP/1.1 200 OK  Allow: OPTIONS, TRACE, GET, HEAD, POST  Server: Microsoft-IIS/10.0  Public: OPTIONS, TRACE, GET, HEAD, POST  Date: Wed, 14 Jul 2021 09:47:27 GMT  Content-Length: 0</p>
HTTP Response	<p>A connection and HTTP request/response is made to the Real Server and checked as explained in the previous examples.</p> <p>But rather than check for a "200 OK" response code, the HTTP response's header is checked for custom text content. The text can be a full header, part of a header, a line from part of a page, or just one word.</p> <p>For instance, in the example shown to the right, we specified <b>/ispagethere.htm</b> as the Path and <b>Microsoft-IIS</b> as the Required Response.</p> <p>If the text is found, the Real Server is deemed to be up and running.</p> <p>This monitoring method can only really be used with HTTP and Accelerated HTTP service types.</p> <p>However, 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 Real Server or handled appropriately by the "Content SSL" facility.</p>	<p><b>Request</b>  GET /ispagethere.htm HTTP/1.1  Host: 192.168.159.200  Accept: */*  Accept-Language: en-gb  User-Agent: Edgenexus-ADC/4.0  Connection: Keep-Alive  Cache-Control: no-cache</p> <p><b>Response</b>  HTTP/1.1 200 OK  Content-Type: text/html  Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT  Accept-Ranges: bytes  ETag: "Odd3253a59ad31:0"  Server: Microsoft-IIS/10.0  Date: Wed, 14 Jul 2021 10:07:13 GMT  Content-Length: 1364</p> <pre>&lt;!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1- strict.dtd"&gt; &lt;html xmlns="http://www.w3.org/1999/xhtml"&gt; &lt;head&gt; &lt;meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /&gt; &lt;title&gt;jetNEXUS&lt;/title&gt; &lt;style type="text/css"&gt; &lt;!-- body {</pre>

		color:#FFFFFF; ...
Multi-Port TCP monitor	This method is like the above, except that you can have several 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
TCP Out of Band	The TCP Out of Band method is like 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
DICOM	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 within 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
LDAPS	This new health check is used to check the health and response of an LDAP/AD server.	Name: LDAPS Description: LDAP/AD Server health check Usage parameters are as follows: <b>Username:</b> cn=username,cn=users,dc=domainname,dc=local <b>Password:</b> DomainUserPassword <b>Content:</b> 200OK
SNMP v2	This monitoring method allows you to check for a server availability status using the server's SNMP MIB response. The Require Response value should contain the Community Name.	
DNS Server Check	When load balancing DNS Servers, it is helpful to see if the server responds to DNS queries. The monitor can be used as follows: <ul style="list-style-type: none"> <li>• The Path field is used for the FQDN that you are querying. For example, if you wished to query <a href="http://www.edgenexus.io">www.edgenexus.io</a>, then enter this in the Path field.</li> <li>• If you leave this blank, then the monitor will use its default lookup to make the query.</li> <li>• The Required Response field can be left blank, and the monitor will assume that any response is considered valid. Otherwise, you should enter the expected IP in the Required Response field. For example, this may be 101.10.10.100. If the query returns this value, the monitor flags a success; else, it will flag a failure.</li> </ul> A success result indicates that the DNS server you are load-balancing is operational.	

The Real Server Monitors page is split into three sections.

## Details

The Details section is used to add new monitors and to remove any that you do not need. You can also edit an existing monitor by double-clicking on it.

Name	Description	Monitoring Method	Applied To VS
200OK	Check home page for 200 OK	HTTP 200 OK	Not in use
DICOM	Monitor DICOM server	DICOM	Not in use

Name: 200OK  
 Description: Check home page for 200 OK  
 Monitoring Method: HTTP 200 OK  
 Page Location: /  
 Required Content: What must be seen within the page  
 User Name: User name if the page is a secured  
 Password: Password if the page is a secured p  
 Threshold: Passed to custom monitors where :

Update Cancel

## Name

Name of your choice for your monitor.

## Description

Textual description for this Monitor, and we recommend that it is best to make it as descriptive as possible.

## Monitoring Method

Choose the monitoring method from the drop-down list. Available choices are:

- HTTP 200 OK
- HTTP 200 Head
- HTTP 200 Options
- HTTP Head
- HTTP Options
- HTTP Response
- Multi-Port TCP Monitor
- TCP Out of Band
- DICOM
- SNMP v2
- DNS Server Check
- LDAPS

## Page Location

URL Page location for an HTTP monitor. This value can be a relative link such as /folder1/folder2/page1.html. You can also use an absolute link where the website is bound to the hostname.

## Required Content

This value contains any content that the monitor needs to detect and utilize. The value represented here will change depending on the monitoring method that is chosen.

## Applied to VS

This field is automatically populated with the IP/Port of the Virtual Service to which the monitor is applied. You will not be able to delete any Monitor that has been used with a Virtual Service.

## User

Some custom monitors can use this value along with the password field to log into a Real Server.

## Password

Some custom monitors can use this value along with the User field to log into a Real Server.

## Threshold

The Threshold field is a general integer used in custom monitors where a threshold such as the CPU level is required.

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

## SSL/TLS

This field allows you to force whether to use or not use SSL. The settings are as follows:

- On – This will force SSL
- Off – This will disable SSL
- Auto – This will leave in the current state

## Real Server Monitor examples

Name	Description	Monitoring Me...	Page Location	Required Cont...	Applied to VS	User	Password	Threshold
Http Response	Check home pa...	HTTP Response		555	192.168.3.20:80			
DICOM	Monitor DICOM...	DICOM		does this conte...	Not in use			
Monitoring OWA	Exchange 2010...	HTTP Response	/owa/auth/logon...		Not in use			
Multi Port	Exchange 2010...	Multi port TCP ...	/owa/auth/logon...		Not in use			

## Upload Monitor

There will be many occasions when users wish to create their own custom monitors and this section allows them to upload them to the ADC.

Custom monitors are written using PERL scripts and have a .pl file extension.

▲ Upload Monitor

Monitor Name:

- Give your monitor a name so that you can identify it in the Monitoring Method list
- Browse for the .pl file
- Click Upload New Monitor
- 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 uploaded and remove them if they are no longer needed.

▲ Upload Monitor

Monitor Name:

- 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

**CAUTION:** This section is intended for persons with experience in using and writing in Perl

This section shows you the commands you can use within your Perl script.

The #Monitor-Name: command is the name used for the Perl Script stored on the ADC. 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 specific features, such as SNI.

### Dynamic Values

- my \$host = \$\_[0]; ### Host IP or name (comes from RS details or OOB if used)
- my \$port = \$\_[1]; ### Host Port (comes from RS details or OOB if used)
- my \$content = \$\_[2]; ### Required content from the monitor settings (what must be seen in the response)
- my \$notes = \$\_[3]; ### notes from RS details in IP Services (use this to customise each RS monitor uniquely)
- my \$page = \$\_[4]; ### page location in the monitor settings
- my \$user = \$\_[5]; ### username from the monitor settings
- my \$password = \$\_[6]; ### password from the monitor settings
- my \$threshold = \$\_[7]; ### threshold parameter from the monitor settings
- my \$rsaddr = \$\_[8]; ### RS IP (different from \_[0] if out-of-band monitoring)
- my \$rsport = \$\_[9]; ### RS port (different from \_[1] if out-of-band monitoring)
- my \$timeout = \$\_[10]; ### monitor contact timeout in seconds from IP Services > Real Server > Advanced > Monitoring Timeout

### Custom Health Checks have two outcomes

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

### Example of a Custom Health Monitor

```
#Monitor-Name HTTPS_SNI
use strict;
use warnings;
# The monitor name as above is displayed in the drop-down 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 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 $auth HTTP://${notes}${page} 2>&1";
if(join("@"@lines)=~/content/)
{
    print "HTTP://${notes}${page} looking for - $content - Health check successful.\n";
    return(1);
}
else
{
    print "HTTP://${notes}${page} looking for - $content - Health check failed.\n";
    return(2)
}
}
monitor(@ARGV):

```

**NOTE:**

Custom Monitoring – Use of global variables is not possible. Use local variables only – variables defined inside functions

Use of RegEx - All regular expressions must use a Perl compatible statement syntax.

## SSL Certificates

To successfully use Layer 7 load-balancing with servers using encrypted connections using SSL, the ADC must be equipped with the SSL certificates used on the target servers. This requirement is so that the data stream can be decrypted, examined, managed, and then re-encrypted before sending to the target server.

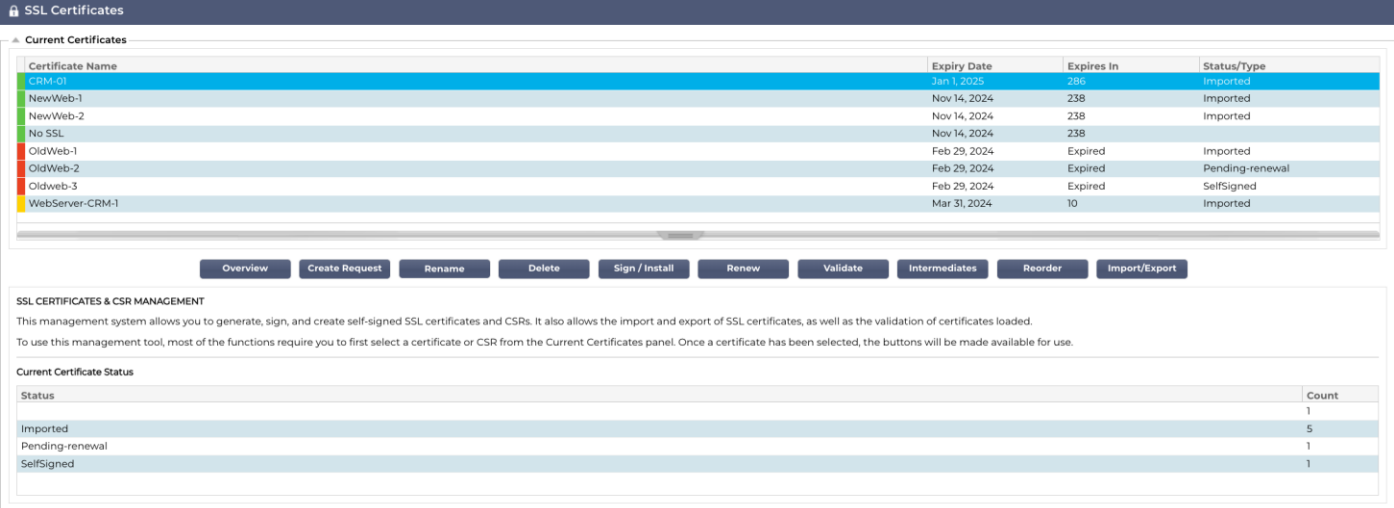
The SSL certificates can range from self-signed certificates that the ADC can generate to the traditional certificates (wildcard included) available from trusted providers. You can also use domain signed certificates that are generated from Active Directory.

### What does the ADC do with the SSL Certificate?

The ADC can perform traffic management rules (flightPATH) depending on what the data contains. This management cannot be performed on SSL encrypted data. When the ADC has to inspect the data, it needs first to decrypt it, and for that, it needs to have the SSL certificate used by the server. Once decrypted, the ADC will then be able to examine and perform the flightPATH rules. Following this, the data will be re-encrypted using the SSL certificate and sent onto the final Real Server.

### The SSL Configuration Manager

Version 196X onward features a new and more straightforward method of configuring and managing SSL certificates and Certificate Requests.



The screenshot displays the 'Current Certificates' section of the SSL Configuration Manager. It features a table with the following data:

Certificate Name	Expiry Date	Expires In	Status/Type
CRM-01	Jan 1, 2025	286	Imported
NewWeb-1	Nov 14, 2024	238	Imported
NewWeb-2	Nov 14, 2024	238	Imported
No SSL	Nov 14, 2024	238	
OldWeb-1	Feb 29, 2024	Expired	Imported
OldWeb-2	Feb 29, 2024	Expired	Pending-renewal
Oldweb-3	Feb 29, 2024	Expired	SelfSigned
WebServer-CRM-1	Mar 31, 2024	10	Imported

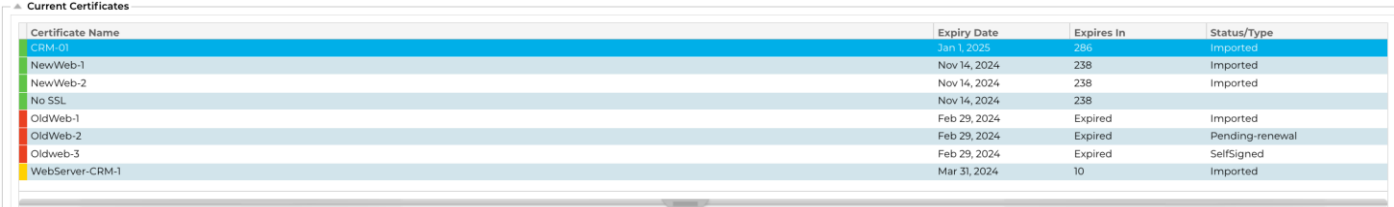
Below the table, there are several action buttons: Overview, Create Request, Rename, Delete, Sign / Install, Renew, Validate, Intermediates, Reorder, and Import/Export.

The 'SSL CERTIFICATES & CSR MANAGEMENT' section provides a brief description of the tool's capabilities and instructions on how to use it. Below this, the 'Current Certificate Status' table shows the following data:

Status	Count
Imported	5
Pending-renewal	1
SelfSigned	1

There are three main sections to the SSL Configuration Manager.

### The Certificate Listing Area



The screenshot shows the 'Current Certificates' section of the SSL Configuration Manager, displaying a table of certificates with the following data:

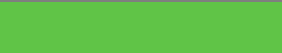




Certificate Name	Expiry Date	Expires In	Status/Type
CRM-01	Jan 1, 2025	286	Imported
NewWeb-1	Nov 14, 2024	238	Imported
NewWeb-2	Nov 14, 2024	238	Imported
No SSL	Nov 14, 2024	238	
OldWeb-1	Feb 29, 2024	Expired	Imported
OldWeb-2	Feb 29, 2024	Expired	Pending-renewal
Oldweb-3	Feb 29, 2024	Expired	SelfSigned
WebServer-CRM-1	Mar 31, 2024	10	Imported

The top side of the Manager shows the SSL certificates that are available for use or pending activation from a Trusted Authority.

The certificates are displayed in a four-column display, showing the Certificate Name, Expiry Date, Expires In (number of days to expiry) and the Status/Type of the certificate.

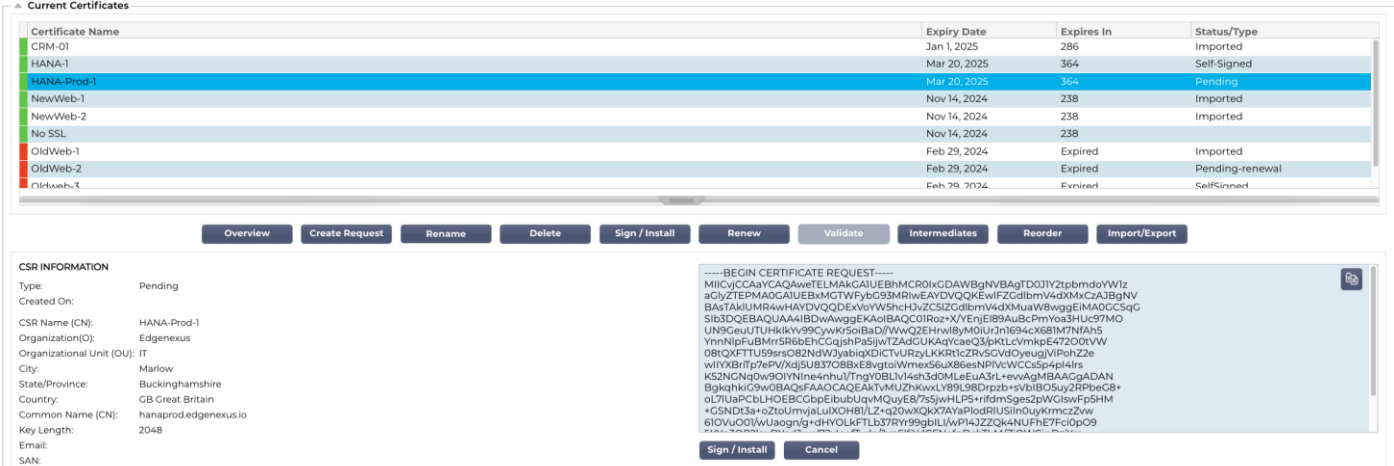
### Colour Codes

As you can see each line shows a certificate together with a colour coded block. Below is a table that shows the different colour coded blocks and their meaning.

Colour Code	Meaning
	Certificate is current and has more than 60 days before expiry
	Certificate will expire in less than 30 days
	Certificate has between 30 and 60 days left
	Certificate is about to expire with <1 day left
	Certificate has expired

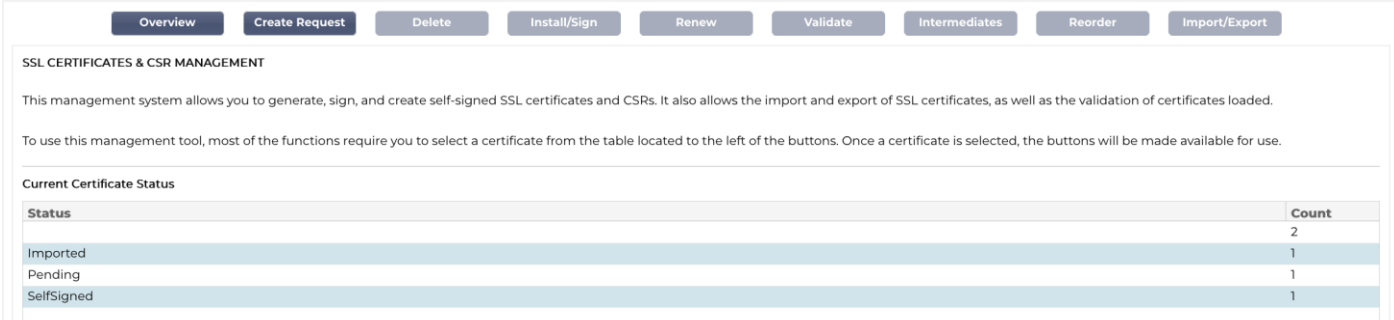
### Certificate/CSR Information Display

Clicking on a certificate or a CSR displays its information in the bottom panel. See image below.



The screenshot shows the 'Current Certificates' management interface. At the top, there is a table listing certificates with columns for Certificate Name, Expiry Date, Expires In, and Status/Type. The 'HANA-Prod-1' certificate is highlighted in blue. Below the table is a row of action buttons: Overview, Create Request, Rename, Delete, Sign / Install, Renew, Validate, Intermediates, Reorder, and Import/Export. The bottom panel displays the 'CSR INFORMATION' for the selected certificate, including fields like Type, Created On, CSR Name (CN), Organization (O), and a large text area containing the CSR request data. A 'Sign / Install' button is visible at the bottom of the CSR information panel.

### The Action Buttons & Configuration Areas



The screenshot shows the 'SSL CERTIFICATES & CSR MANAGEMENT' interface. At the top, there is a row of action buttons: Overview, Create Request, Delete, Install/Sign, Renew, Validate, Intermediates, Reorder, and Import/Export. Below the buttons is a text area explaining the management system's capabilities. Underneath, there is a 'Current Certificate Status' table showing the count of certificates in different states.

Status	Count
Imported	2
Pending	1
SelfSigned	1

There are number of action buttons that are available and come into play when a certificate is selected in the Listing are.



## Overview

Current Certificate Status	
Status	Count
Imported	5
Pending	1
Pending-renewal	1
Self-Signed	1
SelfSigned	1

The Overview button displays an overall situation on certificates in the bottom section. Unlike other actions, the Overview button is independent and does not require a certificate to be selected.

## Create Request

If you want to create a self-signed certificate or a CSR, you need to click on the Create Request button. This will bring up a common entry panel that allows you to provide all the details that are required.

**CREATE SELF-SIGNED CERTIFICATE / CSR**

AD Certificate Name (CN):

Organization (O):

Organizational Unit (OU):

City/Locality:

State/Province:

Country:

Common Name (FQDN):

Key Length:

Period (days):

Email:

Subject Alternative Names:

DNS:

### AD Certificate Name (CN)

This is a descriptive field that is used to display the name of the certificate in the ADC. The field entry should be specified as alphanumeric without spaces.

### Organization (O)

This field is used to specify the name of the organization that is going to use the certificate.

### Organizational Unit (OU)

Normally used to specify the department or organizational unit, this is an optional field.

### City/Locality

As the name suggests, users generally tend to specify where the organization is located.

## State/Province

Specify the state, county, or province in this field.

## Country

This is a mandatory field and must be completed by selecting the country in which the certificate will be used. Please ensure that the information provided here is accurate.

## Common Name (FQDN)

This is a critical field and is used to specify the fully qualified domain name (FQDN) of the server(s) that are to be protected using the certificate. This could be something like **www.edgenexus.io**, or **edgenexus.io**, or even a wildcard **\*.edgenexus.io**. You could also use an IP address should you wish to bind the certificate to it.

## Key Length

Used to specify the encryption key length for the SSL certificate.

## Period (Days)

The length of certificate validity in days. Once the period has elapsed, the certificate will become non-operational.

## Email

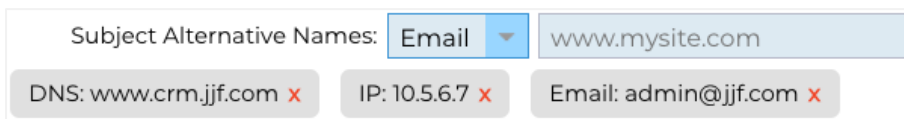
This is the administrative email ID used for the certificate.

## Subject Alternate Names (SAN)

Subject Alternative Name (SAN) is an extension within SSL certificates that allows multiple domain names to be protected under a single certificate. This feature is especially useful for securing websites with multiple subdomains or different domain names, enabling a more streamlined and cost-effective approach to SSL management. By including SANs, a single SSL certificate can cover a variety of domain names and subdomains, eliminating the need for individual certificates for each web address, thereby simplifying the process of securing web communications and ensuring data encryption across diverse domains.

This field comprises of two elements, a drop-down allowing the selection of the type of SAN, and a text field to specify the value.

The EdgeADC has the following SANs available for use: DNS, IP Address, Email Address and URI. You can select and specify multiple SANs for a certificate or CSR.



Subject Alternative Names: **Email**

DNS: www.crm.jjf.com **x**    IP: 10.5.6.7 **x**    Email: admin@jjf.com **x**

SANs that have been specified can be removed by clicking the red **x** located in each SAN value.

- **DNS** - The DNS Subject Alternate Name (SAN) allows you to specify additional domain names for which the certificate is valid. Unlike the Common Name (CN) field, which allows for only one domain, the SAN field can include multiple domain names, offering flexibility and scalability in certificate management. This is particularly useful for organizations hosting multiple services across different domains and subdomains, as it allows them to secure communications for all these entities under a single SSL/TLS certificate, simplifying administration and improving security.
- **IP Address** - The IP Subject Alternative Name (SAN) allows the inclusion of IP addresses alongside domain names as entities protected by the certificate. This feature is crucial for securing direct access to services via IP addresses, ensuring that encrypted connections can also be established when accessing a server not through its domain name, but directly via its IP address. By incorporating IP SANs, organizations can enhance

their network security by enabling SSL/TLS encryption for both domain-based and IP-based communications, making it versatile for environments where domain names may not be used or preferred for accessing internal resources or specific services.

- **Email Address** - The Email Address Subject Alternative Name (SAN) permits you to specify additional email addresses to be associated with the certificate, beyond the primary domain or entity it was issued for. This allows the certificate to validate the identity of the issuer for multiple email addresses, not just a single domain or Common Name (CN). It's particularly useful in scenarios where secure email communication is required for various email addresses under the same organization or entity, ensuring that encrypted email exchanges are authenticated and tied back to the issuer's identity verified by the certificate. This makes the Email Address SAN a key feature for enhancing the security and trustworthiness of email communications within an encrypted framework.
- **URI** - The URI (Uniform Resource Identifier) SAN is used to specify additional identities represented by URIs for a single entity secured by the certificate. Unlike traditional SAN entries that typically include domain names (DNS names) or IP addresses, a URI SAN enables the certificate to associate the entity with specific URIs, such as a URL to a specific resource or a service endpoint. This allows for more flexible and precise identification, enabling secure connections to be established with specific resources or services within a domain, rather than just securing the domain itself, thereby enhancing the granularity and scope of SSL/TLS certificates.

Once filled in correctly, you can choose to create a Certificate Signing Request (CSR) and send it for signing by a Certificate Authority or create a Self-Signed Certificate for immediate use.

The Cancel button will cancel the entire request, while the Reset button will reset all the fields.

## Rename

The Rename button allows you to rename certificates that are not in use on Virtual Services.

To use this function:

- Click on the certificate you wish to rename and click on the Rename button.
- The certificate line will change and you will be able to change its name.

Certificate Name	Expiry Date	Expires In	Status/Type
HANA-1	Mar 20, 2025	364	Self-Signed
HANA-Prod-1	Mar 20, 2025	364	Pending
NewWeb-1	Nov 14, 2024	238	Imported
NewWeb-2	Nov 14, 2024	238	Imported
No SSL	Nov 14, 2024	238	Imported
OldWeb-1	Feb 29, 2024	Expired	Imported
OldWeb-2	Feb 29, 2024	Expired	Pending-renewal
Oldweb-3	Feb 29, 2024	Expired	SelfSigned
WebServer-CRM-1	Mar 31, 2024	9	Imported

Buttons: Overview, Create Request, Rename, Delete, Sign / Install, Renew, Validate, Intermediates, Reorder, Import/Export

- Once you are done, click the Update button.
- You can also double click on the certificate to rename the certificate.

## Delete

The Delete button will only be available when a certificate is selected. When clicked, it will display the following content.

**CERTIFICATE/CSR DELETION**

You have elected to delete the following SSL certificate:

Certificate/CSR Name: **Web-Server-Certificate**

If you are sure you want to delete, click Delete or to prevent deletion, click Cancel.

Buttons: Cancel, Delete

The bottom pane will display the deletion request together with the name of the certificate to for which deletion has been requested.

Click the Delete button in the bottom right of the pane to proceed with the deletion.

## Install/Sign

**SIGN / INSTALL CERTIFICATE**

**Certificate Name:** Web-Server-Certificate  
 To sign a certificate, please upload the ZIP file provided by your certification authority. This must be an Apache-compliant file.

**Upload Certificate:**  Browse Sign

Alternatively, you can also copy and paste the certificate below. Please take care when doing this and do not miss out any information. Intermediates can also be added below the certificates, and terminated with Root CA.

**Certificate Text:**

Cancel Sign  
Apply

When you create a CSR and wish to have the request signed by a Certificate Authority (CA), you will send the CSR to the CA. In return, the CA will send the signed certificate together with the Private Key file, and any intermediates required to make the certificate function properly.

They may well send you a ZIP file containing all the required elements, and this can be uploaded using the upper part of the right pane.

Alternatively, you can also construct the certificate set in a text editor and paste the content into the Certificate Text field in the lower section of the pane.

Once you have used either method, click the Sign button and then the Apply button. The signed certificate will now be displayed in the left pane.

## Renew

**RENEW CERTIFICATE**

You have chosen to **renew** the certificate shown below.

If you'd like to revoke or cancel this request, please click the CSR on the left-side table and select Cancel CSR.

**Certificate Name** Web-Server-Certificate  
**(CN):**

**Important**  
 A new CSR has been created for signing, but the original SSL certificate for which renewal was requested is still active. Please ensure you allocate the newly signed certificate to the correct CSR when importing.

Cancel Create Renewal CSR

When a certificate is due to expire past its validity data, the Renew button allows you to extend and renew the certificate. There are two types of renewal.

### Self-Signed Certificates

Self-Signed certificates unlike trusted certificates cannot be renewed using a CSR. Instead, the self-signed certificate is renewed by presenting a new configuration using the existing data. The user is then allowed to specify a new name for the certificate together with a new expiry value for the certificate.

Once this is done, the new self-signed certificate will be created and saved in the certificate store. It is then the responsibility of the administrator to ensure that the virtual services that use the certificate are reconfigured in time.

### Trusted Signed Certificates

When it comes to certificates that are trusted, and signed by a Certification Authority the use of CSRs is adopted.

When you click on an expiring certificate in the top panel, and click Renew, you will be presented with a new CSR using the current certificate details. The CSR can then be downloaded and presented to the certification authority for signing, after which the signed certificate can be installed.

The certificate that you had asked to renew will have a new status, Renewing. Once the signed certificate is installed the certificate you will be asked to allocate a new name to the certificate. This will then show as Trusted. The original certificate will be retained and any services using it should be configured to use the new certificate as soon as possible.

## Validate Certificate

There are several parts that go together to make up an SSL certificate, and it is essential that these parts are not only present but are also in the correct order. The reasons for validating SSL certificates obtained from third party organizations are listed below.

- **Authentication:** Validation ensures that the certificate comes from a trusted authority and verifies the identity of the website or server. This helps in preventing man-in-the-middle attacks, where an attacker could intercept the communication between a client and a server.
- **Integrity:** By validating an SSL certificate, you can ensure that the certificate has not been tampered with or altered. This is crucial for maintaining the integrity of the secure connection.
- **Trust Chain Verification:** SSL certificates are issued by Certificate Authorities (CAs). Validating a certificate includes verifying that it chains back to a trusted root CA. This process ensures that the certificate is legitimate and can be trusted.
- **Revocation Status:** During validation, it's also important to check whether the SSL certificate has been revoked by the issuing CA. A certificate might be revoked if it was issued erroneously, the website's private key was compromised, or the site no longer needs the certificate. Importing a revoked certificate could lead to security vulnerabilities.
- **Expiration Check:** SSL certificates are valid for a specific period. Validating a certificate on import includes checking its expiration date to ensure that it is still valid. Using an expired certificate could lead to vulnerabilities and might cause browsers or clients to reject the secure connection.
- **Configuration and Compatibility:** Validation ensures that the certificate's configuration is compatible with the client's security policies and the technical requirements of the server or application. This includes checking the algorithms used, the certificate's purpose, and other technical details.
- **Compliance:** In certain industries, regulations may require the validation of SSL certificates to ensure the secure handling of sensitive information. This is especially important in sectors like finance, healthcare, and e-commerce.

The ADC's SSL management system allows the validation of an SSL certificate that has been imported.

- Select an SSL certificate that you have imported.
- Click the Validate button.
- The results are seen in the lower panel as represented by the image below.

VALIDATE CERTIFICATE		
The validation results are shown below:		
Certificate Name:	EdgeWild	
Test Name	Test Result	Test Status
Certificate file	/jetnexus/etc/sslcert_EdgeWild.pem: CN = *.edgenexus.io error 20 at 0 depth lookup:unable to get local issu	✓
Certificate expires	Certificate expired 114 days ago	✗
Private key check	OK	✓
Public key check	OK	✓

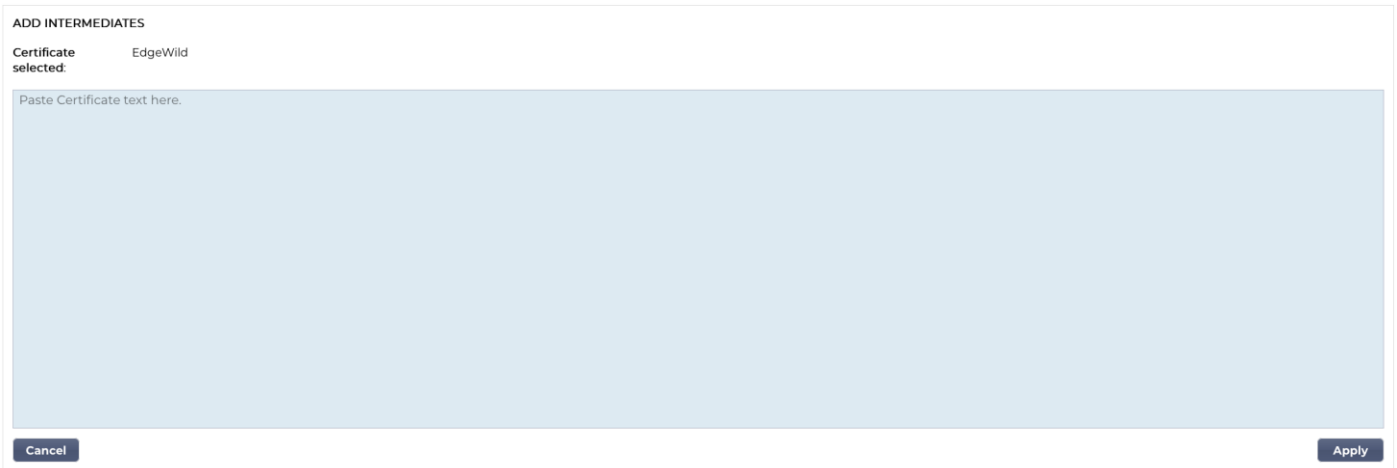
## Adding Intermediates

As said earlier, SSL certificates comprise of several parts, one of which are the intermediate certificates that go to make up the complete chain.

The SSL Manager in the ADC allows you to add any missing intermediate certificates.

- Click on the SSL to which you wish to add the Intermediate certificate.

- Click the Intermediates button.
- A panel is shown, much like the image below.



- Paste the content of the Intermediate certificate.
- Click Apply.

It may be the case that you need to change the order of the Intermediate certificates, so the SSL certificate validates correctly. This is done using the Reorder button.

## Reorder

For an SSL certificate to operate correctly, it must be in in the right order.

The golden rule is that the sender’s certificate must come first, with the final Root Certificate last in the chain. Generally, this looks somewhat like the below representation:

Original issuer > Intermediate 1 > Final Root.

The Final Root is a trusted root certificate provided by a certificate authority.

In some cases, there are several Intermediate certificates, and these should also be placed in the correct position. Essentially, each following certificate must certify the one preceding it. So, it could end up looking like this.

Original issuer > Intermediate 1 > Final Root

When you import say, Intermediate 2, this could be placed at the end of the chain, which would mean the certification failing validity. Hence, the need to reorder it and place Intermediate 2 into its correct position (shown in red).

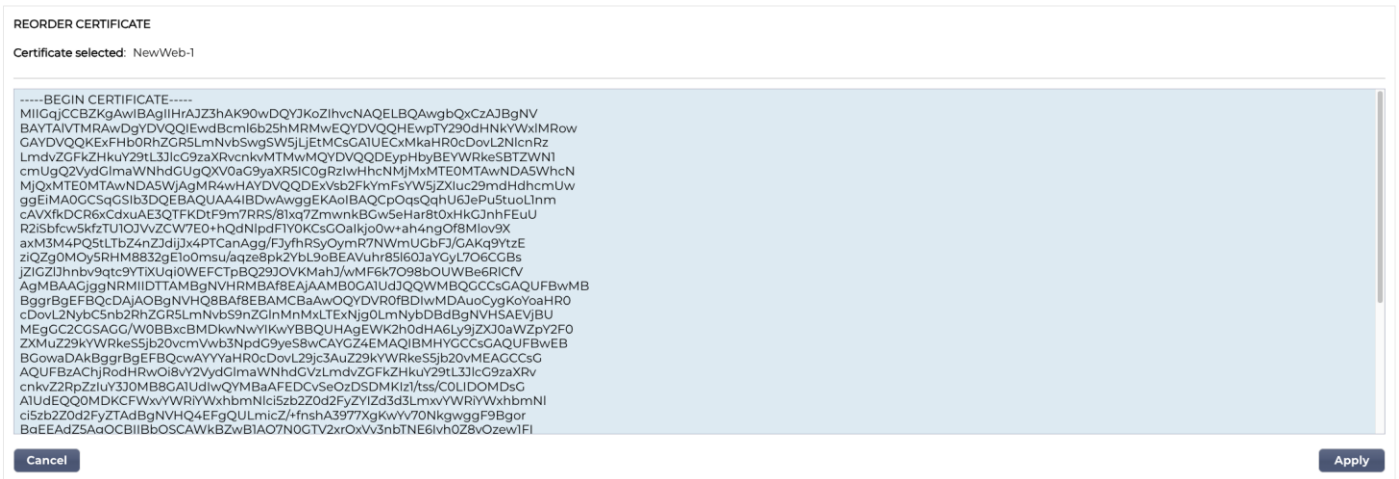
So, the final one would look like this:

Original issuer > Intermediate 1 > **Intermediate 2** > Final Root

```
-----BEGIN CERTIFICATE-----
MIIFKTCBBGgAwIBAgISA/UUyBjJ71fucZuvpiLsdfsfsdfsdfd
...
hoFWWJt3/SeBKn+ci03RRvZsdfsfsdfw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFfJCCAv6gAwIBAgIRAJErCERPDBinsdfsfsdfsdfsdfsdfsd
....
```

```
nLRbwHqsD7hHwg==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFYDCCBsdSDFSDVSDVzfsdffvqdsfgsT664ScbvsfGDGSDV
...
Dfvp700GAN6dEOM4+SDFSDZET+DFGDFQSD45Bddfghqsqf6Bssf
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFYDCCBsdSDFSDVSDVzfsdffvqdsfgsT664ScbvsfGDGSDV
...
Dfvp700GAN6dEOM4+SDFSDZET+DFGDFQSD45Bddfghqsqf6Bssf
-----END CERTIFICATE-----
```

The Reorder section looks like the image below once you select a certificate and press the Reorder button.



To reorder the certificate sections, you can copy the text within the box, edit and reorder the content within a text editor and then paste it back to replace the existing content. Once done, click the Apply button.

## Import/Export

**IMPORT CERTIFICATE**

Certificate Name:

Upload Certificate:  .pfx, .cer, .pem & .der supported

Upload Key File:  optional

Password:  required for .pfx

---

**EXPORT CERTIFICATE**

Certificate Name:

Password:

Whenever you receive a certificate from your SSL certificate provider, it will come as a ZIP file or a set of files. These will contain the SSL certificate, the key file and the root ca, as well as any intermediates.

You will need to import them into the ADC, and so, we have provided a method of importing them in.

There are a number of formats for SSL certificates such as CER, DER, PEM and PFX. Some formats require a KEY file to be added to the import procedure. PFX files require the password in order to import the PFX certificate.

We have also provided the means of export a certificate from the ADC if required. When exported, the file will be in PFX format, and it therefore requires a password for creating the export.

## Backup & Restore

### Backup

The screenshot displays the 'Backup & Restore' interface. It is divided into two main sections: 'BACKUP ALL SSL, CSR & INTERMEDIATE CERTIFICATES' and 'RESTORE CERTIFICATES, CSRs & INTERMEDIATES FROM BACKUP'. The 'Backup' section includes a 'Filename for Backup' field with the text 'jnbk extension will be added', a 'Certificate Name' dropdown menu with the option 'Choose one or more installed certificate', and a 'Password' field with the placeholder 'Enter password for backup'. Below these fields are 'Reset' and 'Create Backup' buttons. The 'Restore' section includes an 'Upload Certificate' field with the placeholder 'Select JNBK archive' and a 'Browse' button, and a 'Password' field with the placeholder 'Enter your backup password'. Below these fields are 'Reset' and 'Restore' buttons.

In order to back up the certificates in the Certificate Store of the ADC:

- Add a filename to be used for the backup.
- Use the drop-down menu to select a single certificate, or ALL for backing up all the certificates.
- Add a password
- Click the Create Backup button.
- The file created is a JNBK file which is encrypted.

#### IMPORTANT

The backup will only work with Trusted certificates that have been imported.

### Restore

When you wish to restore the backup, use the lower section of the Backup & Restore section.

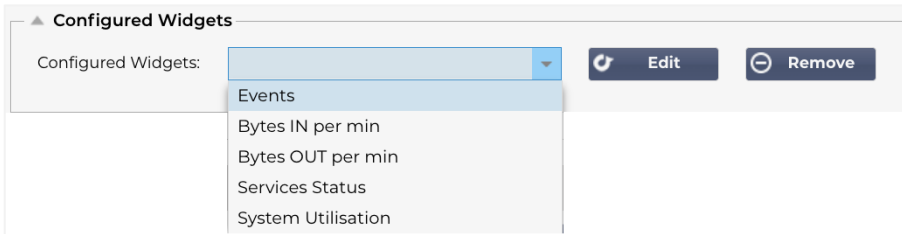
- Browse to and locate the backup file.
- Enter the password.
- Click the Restore button.
- The certificates within the backup file will be restored.



## Widgets

The Library > Widgets page allows you to configure various lightweight visual components displayed in your custom dashboard.

### Configured Widgets

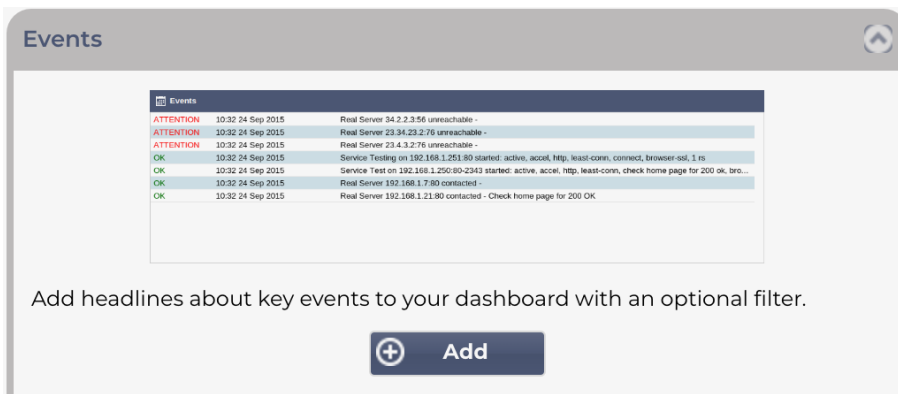


The Configured Widgets section allows you to view, edit or remove any widgets created from the available widgets section.

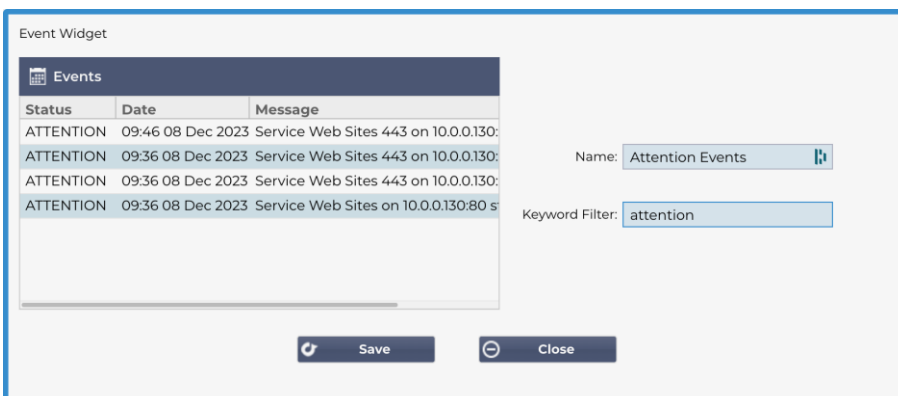
### Available Widgets

There are five different widgets provided within the ADC, and you may configure them to your requirements.

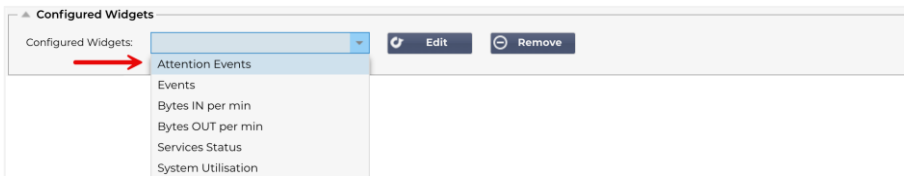
#### The Events Widget



- To add an event to the Events widget, click the Add button.
- Provide a name for your event. In our example, we have added Attention Events as the event name.
- Add a keyword filter. We have also added the filter value of Attention



- Click Save, then Close
- You will now see an additional Widget called Attention Events in the Configured Widgets dropdown.

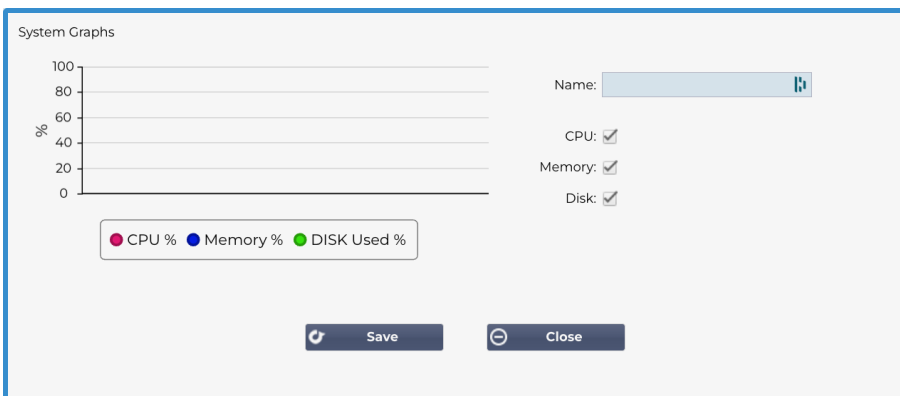


- You can see we have now added this widget in the View > Dashboard section.
- Select the Attention Events widget to display this within the Dashboard. See below.

Status	Date	Message
ATTENTION	14:49 08 Dec 2023	Service on 10.0.0.125:443 stopped: active, accel, http, jsp, 200ok, browser-ssl, 3 rs - stop interface deleted
ATTENTION	10:51 07 Dec 2023	Service on 10.0.0.125:80 stopped: active, accel, http, jsp, 200ok, browser-ssl, 3 rs - Stopping VS 10.0.0.125:80; update interface 10.0.0.125 updated
ATTENTION	10:51 07 Dec 2023	Service on 10.0.0.125:80 stopped: active, accel, http, least-conn, connect, 1 rs - Stopping VS 10.0.0.125:80; update interface 10.0.0.125 updated
ATTENTION	12:12 30 Nov 2023	10.0.0.120:80 Real server myWAF:80 unreachable - Connect=FAIL
ATTENTION	12:09 30 Nov 2023	10.0.0.120:80 Real server myWAF:80 unreachable - Connect=FAIL
ATTENTION	08:53 29 Nov 2023	Service on 10.0.0.125:443 stopped: active, accel, http, least-conn, connect, 3 rs - stop interface deleted
ATTENTION	10:39 23 Nov 2023	Service INGRESS on 10.0.0.120:80 stopped: active, http, least-conn, connect, 1 rs - Stopping VS 10.0.0.120:80; update interface 10.0.0.120 updated
ATTENTION	11:10 22 Nov 2023	Service on 10.0.0.125:443 stopped: active, accel, http, least-conn, connect, browser-ssl, 3 rs - Stopping VS 10.0.0.125:443; update interface 10.0.0.125 updated

You can also pause and restart the live data feed by clicking the Pause Live Data button. In addition, you can revert to the default dashboard at any time by clicking the Default Dashboard button.

## The System Graphs Widget

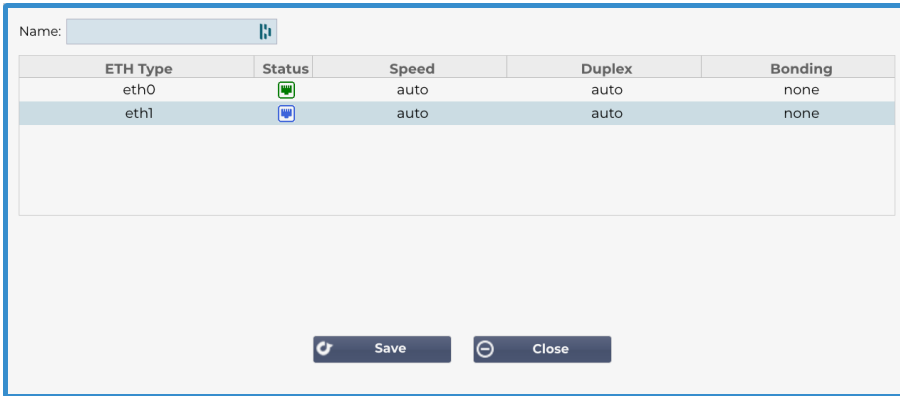


The ADC has a configurable System Graph widget. By clicking the Add button on the widget, you can add the following monitoring graphs to be displayed.

- CPU
- MEMORY
- DISK

Once you have added them, they will be individually available within the Dashboard's widget menu.

## Interface Widget



The Interface widget allows you to display the data for the chosen network interface, such as ETH0, ETH1, and so on. The number of available interfaces for addition depends on how many network interfaces you have defined for the virtual appliance or provisioned within the hardware appliance.

Once you have finished, click the Save button, then the Close button.

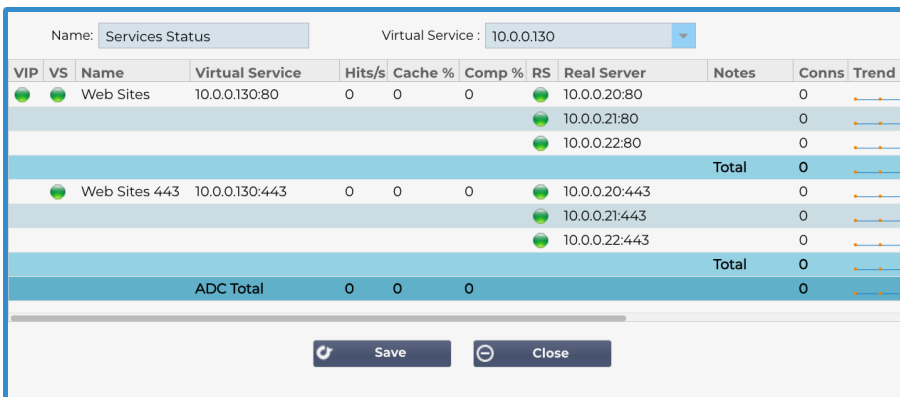
Select the Widget you just customized from the widget drop-down menu within the Dashboard. You will see a screen like the one below.



## Status Widget

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

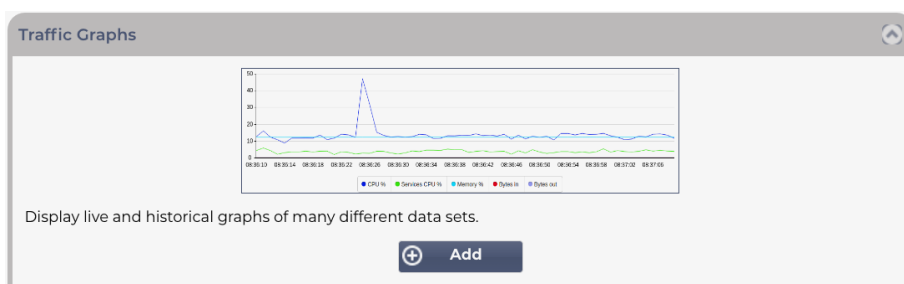
- Click Add.



- Enter a name for the service you wish to monitor
- You can also choose which columns you wish to display in the widget by clicking the column header.
- Once you are satisfied, click Save, followed by Close.
- The chosen Status widget will be available in the Dashboard section.

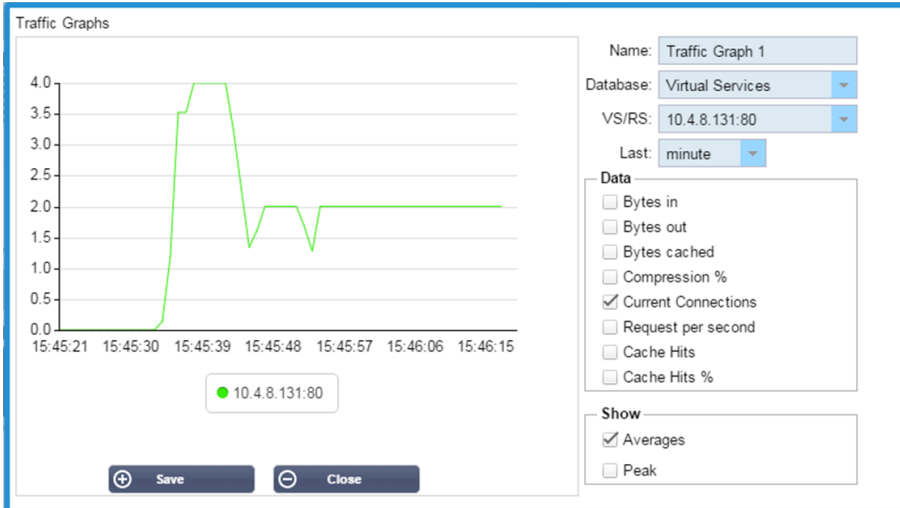
## Traffic Graphics Widget

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



- Click the Add button
- Name your widget.
- Choose a Database from Virtual Services, Real Servers, or System.
- If you choose Virtual Services, you can select 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 each hour for the previous 24 hours
  - Week – aggregated data from each day during the previous seven days
  - Month – aggregated data from each week for the last seven days
  - Year – aggregated data from each month during the previous 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



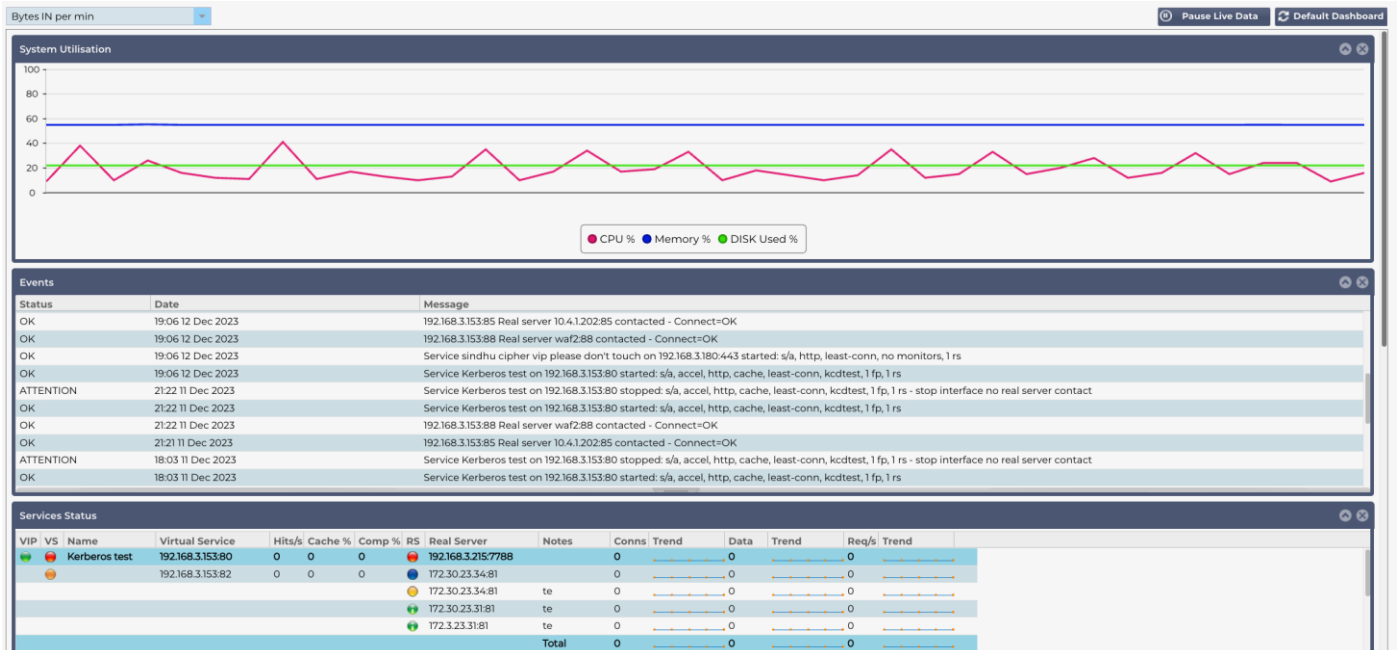
You can now add your Traffic Graph widget to the View > Dashboard.

**View**

## Dashboard

Like all IT systems management interfaces, there are many times when you need to look at performance metrics and data that the ADC is handling. We provide a customizable dashboard for you to do this in an easy and meaningful manner.

The Dashboard is reachable by using the View segment of the navigator panel. When selected, it shows several default widgets and allows you to choose any customized ones that you have defined.



## Dashboard Usage

There are four elements to the Dashboard UI: The Widgets Menu, the Pause/Play Button, and the Default Dashboard button.

### The Widgets Menu

The Widgets menu located at the top left of the dashboard allows you to select and add any standard or customized widgets you have defined. To use this, select the widget from the drop-down.

### Pause Live Data Button

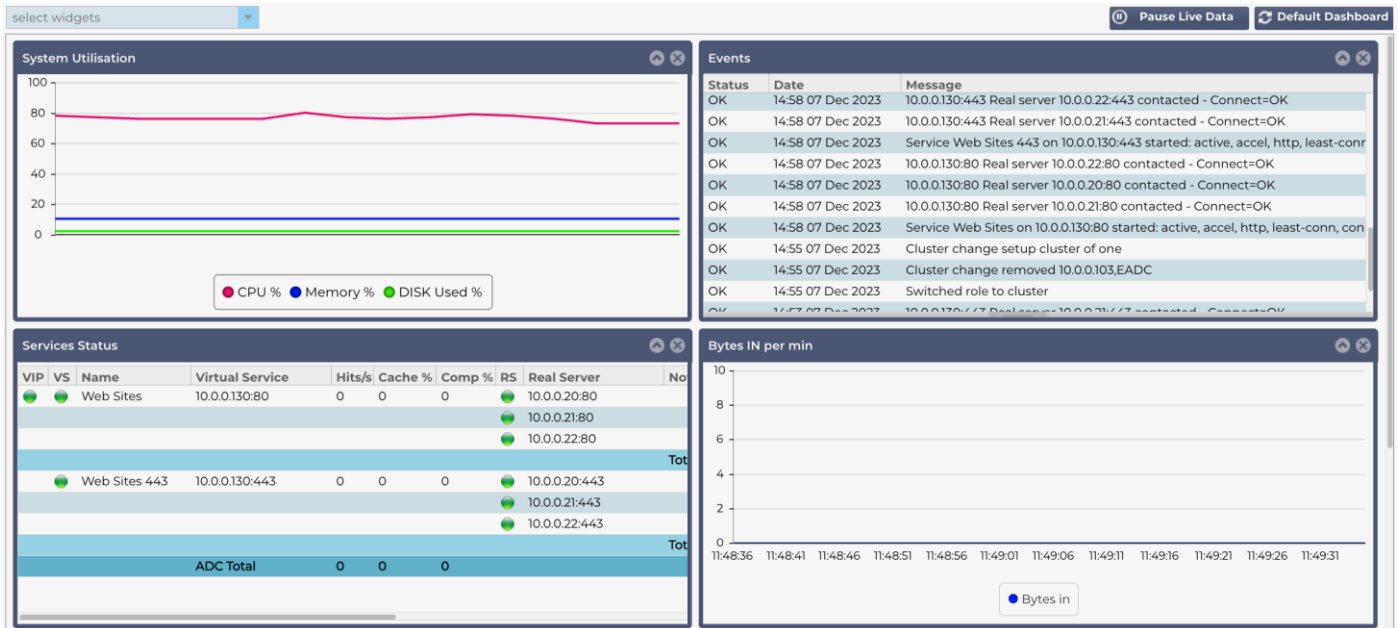
This button allows you to select whether the ADC should update the dashboard in real-time. Once paused, no dashboard widget will be updated, allowing you to examine the content at your leisure. The button changes state to display Play Live Data once a pause is initiated.

When you have finished, simply click the Play Live Data button to restart the data gathering and update the Dashboard.

### Default Dashboard Button

It may come to be that you wish to reset the Dashboard layout to the default. In such a case, press the Default Dashboard button. Once clicked, all changes made to the Dashboard will be lost.

## Resizing, minimizing, re-ordering, and removing widgets



### Resizing a Widget

You can resize a widget very easily. Click and hold on the widget's title bar and drag it to the left or right side of the Dashboard area. You will see a dotted rectangle that represents the new widget size. Drop the widget into the rectangle and let go of the mouse button. If you wish to drop a resized widget alongside a previously resized widget, you will see the rectangle appear adjacent to the widget you want to drop beside.


### Minimizing a Widget

You can minimize widgets at any time by clicking the title bar of the widget. This action will minimize the widget and display only the title bar.

### Moving Widget Order

To move a widget, you can drag and drop by click and hold down on the title bar and moving the mouse.

### Removing a Widget

You can remove a widget by clicking the  icon in the widget title bar.



# History



The History option, selectable from the navigator, allows the administrator to examine the historical performance of the ADC. Historical views can be generated for Virtual Services, Real Servers, and System. It also allows you to see load balancing in action and helps catch any errors or patterns that need investigating. Note that you must enable historical logging in System > History to make use of this feature.

## Viewing Graphical Data

### Data Set

To view the historical data in graphical format, please proceed as follows:

The first step is to choose the database and period relevant to the information you wish to view. The period that you can select from the Last drop-down is Minute, Hour, Day, Week, Month, and Year.

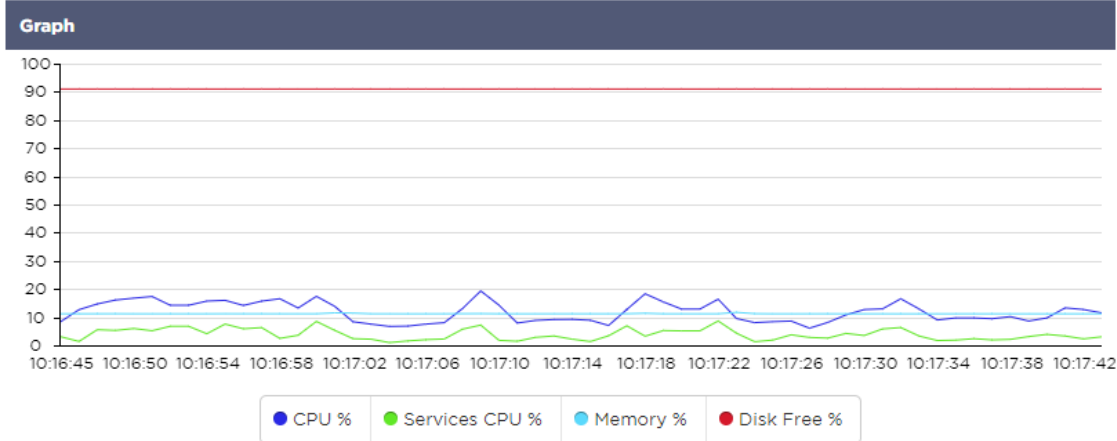
Database	Description
System	<p>Selecting this database will allow you to see CPU, memory, and disk drive space over time</p>
Virtual Services	<p>Selecting this database will allow you to choose all of the virtual services in the database from when you started logging data. You will see a list of Virtual Services from which you can select one.</p>
Real Services	<p>Selecting this database will allow you to choose all the Real Servers in the database from when you started logging the data. You will see a list of Real Servers from which you can select one.</p>

## Metrics

Once you have selected the Data Set that you will use, it is time to choose the Metrics you wish to display. The image below illustrates the metrics available for selection by the administrator: these selections correspond with System, Virtual services, and Real Servers (left to right).

SYSTEM	VIRTUAL SERVICES	REAL SERVERS
<p><b>Metrics</b></p> <p><b>Data</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> CPU %</li> <li><input checked="" type="checkbox"/> Services CPU %</li> <li><input checked="" type="checkbox"/> Memory %</li> <li><input checked="" type="checkbox"/> Disk Free %</li> </ul> <p><b>Show</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Averages</li> <li><input type="checkbox"/> Peak</li> </ul>	<p><b>Metrics</b></p> <p><b>Data</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Bytes In</li> <li><input type="checkbox"/> Bytes Out</li> <li><input type="checkbox"/> Bytes Cached</li> <li><input type="checkbox"/> Compression %</li> <li><input type="checkbox"/> Current Connections</li> <li><input type="checkbox"/> Request Per Second</li> <li><input type="checkbox"/> Cache Hits</li> <li><input type="checkbox"/> Cache Hits %</li> </ul> <p><b>Show</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Averages</li> <li><input type="checkbox"/> Peak</li> </ul>	<p><b>Metrics</b></p> <p><b>Data</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> CPU %</li> <li><input checked="" type="checkbox"/> Services CPU %</li> <li><input checked="" type="checkbox"/> Memory %</li> <li><input checked="" type="checkbox"/> Disk Free %</li> </ul> <p><b>Show</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Averages</li> <li><input type="checkbox"/> Peak</li> </ul>

## Sample Graph



## Logs

The Logs page within the View section allows you to preview and download the W3C and System logs. The page is organized into two sections, as detailed below.

### W3C Logs



W3C logging is enabled from the System > Logging section. 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 timestamp. W3C logs can become very large depending on the amount of data and the category of logging being recorded.

From the W3C section, you can select the log you need and then view or download it.

#### View Button

The View button allows you to view the chosen log within the text editor window, such as Notepad.

#### Download Button

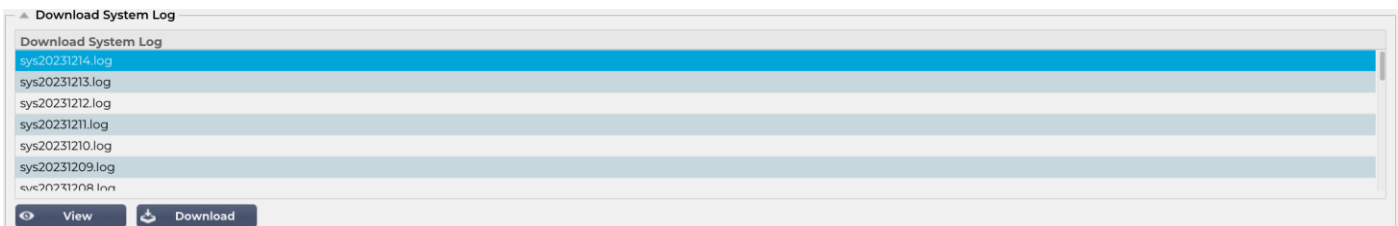
This button allows you to download the log to your local storage for viewing later.

#### The Cog Icon

Clicking this icon takes you to the W3C Log Settings section located in System > Logging. We will discuss this in detail in the Logging section of the guide.

### System Log

The system log is critical to debugging or examining what has been happening with the ADC. It is intended for quitably experienced persons within the IT department.



#### View Button

The View button allows you to view the chosen log within the text editor window, such as Notepad.

#### Download Button

This button allows you to download the log to your local storage for viewing later.

## Statistics

The Statistics section of the ADC is a much-used area by system administrators who want to ensure that the ADC performance is on par with their expectations.

### Compression

The whole purpose of the ADC is to monitor data and direct it to Real Servers configured to receive it. The compression feature is provided in the ADC to increase the ADC's performance. There will be times when administrators will wish to test and check the ADC's data compression information; this data provided by the Compression panel within Statistics.

#### Content Compression to Date

Content Compression To Date	
Compression	0%
Throughput Before Compression	0
Throughput After Compression	0

The data shown in this section details the level of compression achieved by the ADC on compressible content. A value of 60-80% is what we would term as typical

#### Overall Compression to Date

Overall Compression To Date		Current Values
Compression	0%	0%
Throughput Before Compression	0	0.00 Mbps (data)
Throughput After Compression	0	0.00 Mbps (data)
Throughput From Cache	0	0.00 Mbps (data)
<b>Total</b>		0.00 Mbps (data)

The values provided in this section report how much compression the ADC has achieved on all content. A typical percentage for this depends on how many pre-compressed images are contained in your services. The more the number of images, the smaller the overall compression percentage is likely to be.

#### Total Input/Output

Total Input	345.9 MB	Input/s	12.7 kbps
Total Output	296.8 MB	Output/s	25.7 kbps

The Total Input/Output figures represent the amount of raw data traversed into and out of the ADC. The unit of measurement will change as the size grows from kbps to Mbps to Gbps.

### Hits and Connections

Content Caching	Hits	Bytes
From Cache	0 / -	0 / -
From Server	0 / -	0 / -
Cache Contents	0 entries	0 / 0.0%

The Hits and Connections section contains the overall statistics for hits and transactions that pass through the ADC. So what do hits and connections mean?

- A Hit is defined as a Layer 7 transaction. Typically used for web servers, this is a GET request for an object such as an image.
- A Connection is defined as a Layer 4 TCP connection. Many transactions can occur over 1 TCP connection.

## Overall Hits Counted

The figures within this section show the cumulative number of non-cached hits since the last reset. On the right-hand side, the figure will show the current number of hits per second.

## Total Connections

The Total Connections value represents the cumulative number of TCP connections since the last reset. The figure in the second column indicates the TCP connections made per second to the ADC. The number in the right-side column is the number of TCP connections per second made to the Real Servers. Example 6/8 connections/sec. We have 6 TCP connections per second to the Virtual Service and 6 TCP connections per second to the Real Servers in the example shown.

## Peak Connections

The peak Connections value represents the maximum number of TCP connections made to the ADC. The number on the rightmost column indicates the current number of active TCP connections.

## Caching

As you will recall, the ADC is equipped with both compression and caching. This section shows the overall statistics related to caching when applied to a channel. If caching has not been applied to a channel and configured correctly, you will see 0 cache contents.

Content Caching	Hits	Bytes
From Cache	0 / -	0 / -
From Server	0 / -	0 / -
Cache Contents	0 entries	0 / 0.0%

## From Cache

**Hits:** The first column gives the total number of transactions served from the ADC cache since the last reset. A percentage of the total transactions is also provided.

**Bytes:** The second column gives the total amount of data in Kilobytes served from the ADC cache. A percentage of total data is also provided.

## From Server

**Hits:** Column 1 gives the total number of transactions served from the Real Servers since the last reset. A percentage of total transactions is also provided.

**Bytes:** The second column gives the total amount of data in Kilobytes served from the Real Servers. A percentage of total data is also provided.

## Cache Contents

**Hits:** This number gives the total number of objects contained in the ADC cache.

**Bytes:** The first number gives the overall size in Megabytes of the ADC cached objects. A percentage of the maximum cache size is also provided.

## Application Buffer

Buffer Type	Connections Used/Free	Memory Used/Free	Average Buffer Fill Size
Low	0/5k(0%)	0/655MB(0%)	0
Medium	0/5k(0%)	0/30MB(0%)	0
High	0/10k(0%)	0/20MB(0%)	0

The use of application buffers in ADC helps in optimizing performance, improving throughput, and ensuring the reliable and efficient flow of data between clients and servers. Buffer sizes, handling policies, and other parameters are optimised by ADC to fine-tune the load based on the specific requirements of the applications and the infrastructure.

In the EdgeADC, we do the hard work for you and adjust buffer parameters automatically as needs require.

## Session Persistence

Total current sessions	0
% used (of max)	0
New sessions this min	0
Revalidations this min	0
Expired sessions this min	0

The Session Persistence section delivers information for several parameters.

### Total current sessions

This shows how many persistence sessions are in progress - updated each minute

### % Used (of max)

This shows how much usage there is of the total space allowed for session information

### New session this min

This shows, within the last minute, how many new persistence sessions were added

### Revalidate this min

This shows, within the last minute, how many existing persistence sessions were revalidated by more traffic

### Expired sessions this min

This shows, within the last minute, how many existing persistence sessions expired due to no further traffic within the timeout

## Hardware

Whether you are using the ADC in a virtual environment or within hardware, this section will provide you with valuable information on the appliance's performance.

Disk Usage	2%
Memory Usage	10.1%( 185.4MB of 1832.7MB)
CPU Usage	76.0%

### Disk Usage

The value provided in column 2 gives the percentage of disk space currently used and includes information on log files and cache data, which is periodically stored on the storage.

### Memory Usage

The second column gives the percentage of memory currently used. The more significant number in brackets is the total amount of memory allocated to the ADC. It is recommended that the ADC be allocated a minimum of 2GB of RAM.

## CPU Usage

One of the critical values provided is the percentage of CPU currently used by ADC. It is natural for this to fluctuate.

## Status

The View > Status page displays the live traffic traversing through the ADC for the virtual Services you have defined. It also shows the number of connections and data to each Real Server so you can experience the load balancing in real-time.

Virtual Service Details		VIP	VS	Name	Virtual Service	Hits/s	Cache %	Comp %	RS	Real Server	Notes	Conns	Data	Req/s
●	●			Web Sites	10.0.0.130:80	0	0	0	●	10.0.0.20:80		0	0	0
									●	10.0.0.21:80		0	0	0
									●	10.0.0.22:80		0	0	0
											Total	0	0	0
●				Web Sites 443	10.0.0.130:443	0	0	0	●	10.0.0.20:443		0	0	0
									●	10.0.0.21:443		0	0	0
									●	10.0.0.22:443		0	0	0
											Total	0	0	0
					ADC Total	0	0	0				0	0	0

### Virtual Service Details

#### VIP Column

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

Status	Description
●	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 licensed or licensed Virtual IPs exceeded

#### VS Status Column

The color of the light indicates the state of the Virtual Service.

Status	Description
●	Online
●	Failover-Standby. This virtual service is hot-standby
●	Indicates a “passive” is holding off for an “active”
●	Service Needs attention. This status indication may result from 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 licensed or licensed Virtual IPs exceeded

#### Name

The name of the Virtual Service



## Virtual Service (VIP)

The Virtual IP address and port for the service and the address users or applications will use.

## Hit/Sec

Layer 7 transactions per second on the client-side.

## Cache%








The figure provided here represents the percentage of objects that have been served from the ADC's RAM Cache.

## Compression%

This figure represents the percentage of objects that have been compressed between the client and the ADC.

## RS Status (Remote Server)

The table below outlines the meaning of the status of Real Servers linked to the VIP.

Status	Description
	Connected
	Not monitored
	Drain or Offline
	Standby
	Not Connected
	Finding status
	Not licensed or licensed Virtual IPs exceeded

## Real Server

The Real Server IP address and port.

## Notes

This value can be any helpful notes to make others understand the purpose of the entry.

## Conns (Connections)

Representing the number of connections to each Real Server allows you to see the load balancing in action. Very helpful to verify that your load balancing policy is working correctly.

## Data

The value in this column shows the amount of data being sent to each Real Server.

## Req/Sec (Requests per second)

The number of requests per second sent to each Real Server.

# System

# Clustering

The ADC can be used as a single stand-alone device, and it will work perfectly well doing that. However, when one considers that the purpose of the ADC is to load balance sets of servers, the need to cluster the ADC itself becomes apparent. The ADC's easily navigable UI design makes the configuration of the clustering system straightforward.

The System > Clustering page is where you will configure the high availability of your ADC appliances. This section is organized into several sections.

## Important Note

- There is no requirement for a dedicated cable between the ADC pair to maintain a high availability heartbeat.
- The heartbeat takes place on the same network as the Virtual Service that requires high availability to be put in place.
- There is no stateful fail-over between the ADC appliances.
- When high availability is enabled on two or more ADC's, 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 new Active load balancer switches.

Clustering

**Role**

**Cluster**  
Enable Edgenexus ADC to act as part of a Cluster, providing High Availability in Active-Passive mode - automatic synchronisation of appliances

**Manual**  
Enable Edgenexus ADC to act in High Availability mode, either Active-Active or Active-Passive - manual configuration of appliance

**Stand-alone**  
This Edgenexus ADC acts completely independently without high-availability

---

**Settings**

Failover Latency (ms):

Failover Messaging:

---

**Management**

Unclaimed Devices

↑

←   →

↓

Priority	Status	Cluster Members
1	●	10.0.0.103 EADC-103-BETA

IP Address:

Machine Name:

## Role

There are three cluster roles available when you configure the ADC for high availability.

## Cluster

**Role**

**Cluster**  
Enable ALB-X to act as part of a Cluster, providing High Availability in Active-Passive mode - automatic synchronisation of appliances

**Manual**  
Enable ALB-X to act in High Availability mode, either Active-Active or Active-Passive - manual configuration of appliance

**Stand-alone**  
This ALB acts completely independently without high-availability

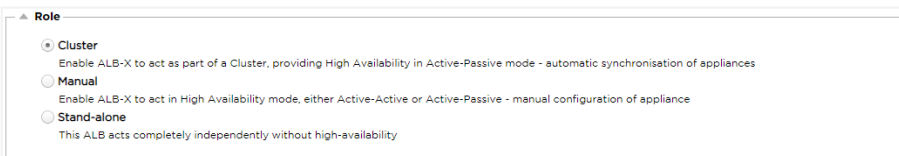
- By default, a new ADC will power on using the Cluster role. In this role, each cluster member will have the same “working configuration,” and as such, only one ADC in the Cluster will be Active at any one time.
- A “working configuration” means all configuration parameters, except items that need to be unique such as the management IP address, ALB Name, network settings, interface details, and so on.
- The ADC in priority 1, the topmost position, of the Cluster Members box is the Cluster Owner and the Active load balancer, while all other ADC’s are Passive members.
- You can edit any ADC in the Cluster, and the changes will be synchronized to all Cluster members.
- When you remove an ADC from the Cluster, all Virtual Services will be deleted from that ADC.
- You cannot remove the last member of the Cluster to Unclaimed Devices. To remove the last member, please change the role to Manual or Stand-alone.
- The following objects are not synchronized:
  - Manual Date & Time section – (NTP Section is synchronized)
  - Failover Latency (ms)
  - Hardware section
  - Appliance section
  - Network section

### Failure of the Cluster Owner

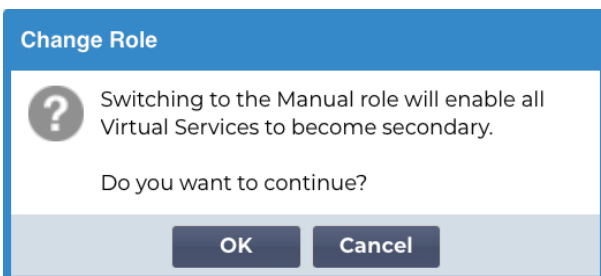
- When a cluster owner fails, one of the remaining members will automatically take over and carry on load balancing the traffic.
- When the cluster owner returns, it will resume load balancing traffic and take over the owner role.
- Let’s assume the Owner has failed, and a Member has taken over the load balancing. If you would like that Member that has taken over load balancing traffic to become the new owner, highlight the member and click the up arrow to move it to the Priority 1 position.
- If you edit one of the remaining cluster members and the owner is down, the edited member will automatically promote itself to the owner without loss of traffic

### Changing role from Cluster role to Manual role

- If you wish to change the role from Cluster to Manual, click the radio button next to the Manual role option



- After you click the radio button, you will see the following message:



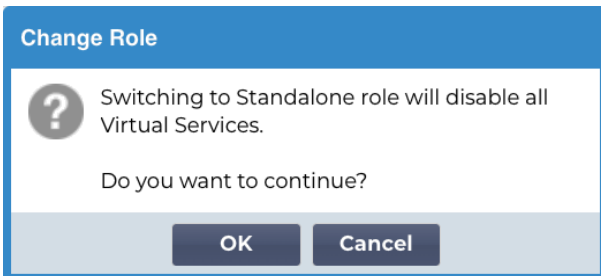
- Click the OK button
- Check the Virtual Services section. You will find that the Primary column now shows an unticked box.

Virtual Services			
Primary	VIP Status	Service Status	Enabled
<input type="checkbox"/>	<span style="color: purple;">●</span>	<span style="color: purple;">●</span>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<span style="color: purple;">●</span>	<span style="color: purple;">●</span>	<input checked="" type="checkbox"/>

- It is a safety feature and means that if you have another ADC 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 the role from Cluster to Stand-alone, click on the radio button next to the Standalone option.
- You will be prompted with the following message:



- Click OK to change roles.
- Check your Virtual Services. You will see that the Primary column change name to Stand-alone
- You will also see that all the Virtual Services are disabled (un-ticked) for safety reasons.
- Once you are confident that no other ADC on the same network has duplicate Virtual Services, you can enable each one in turn.

### Manual Role

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

- To make a Virtual IP address "Active", tick the checkbox 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, 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 fallback to the original Active ADC

### Stand-alone Role


An ADC in the Stand-alone role will not communicate with any other ADC regarding its services, and therefore all Virtual Services will remain in the Green status and connected. You must ensure that all Virtual Services have unique IP addresses, or there will be a clash on your network.

## Settings

▲ Settings

Failover Latency (ms):

Failover Messaging:

 **Update**

### Failover Latency (ms)

You can set the Failover Latency in milliseconds. This is the time that a Passive ADC will wait before taking over the Virtual Services after the Active ADC has failed.

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

### Failover Messaging

▲ Settings

Failover Latency (ms):

Failover Messaging:

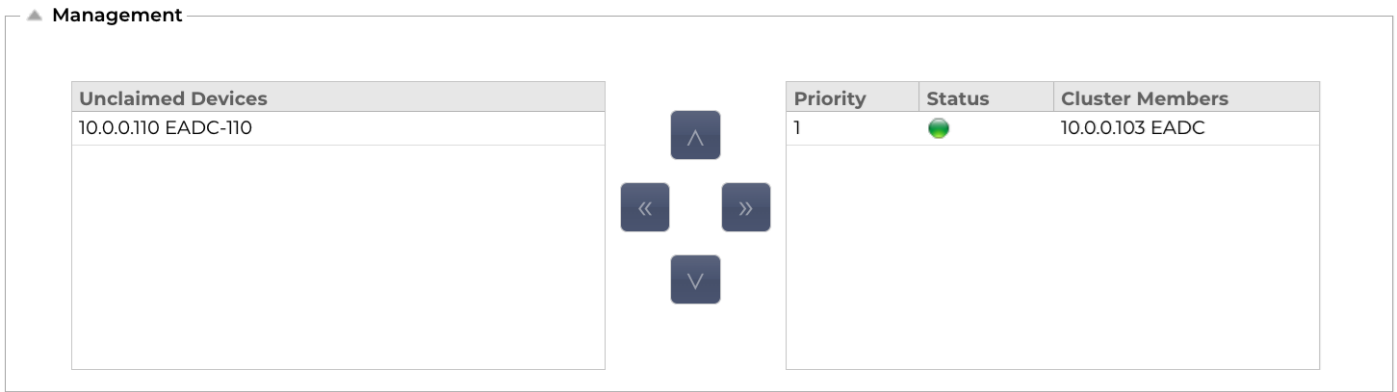
- Broadcast
- Unicast
- Hybrid

By default, the ADC uses Broadcast for its failover messaging. However, some networks block broadcast and so we have provided Unicast and Hybrid, a mix of Unicast and Broadcast.

When running in default Broadcast mode unclaimed devices will be automatically listed and broadcast messages will be used for failover. When running in Hybrid mode unclaimed devices will still advertise over Broadcast but failover communication will be over Unicast. Unicast mode will not broadcast as such you, and you may need to manually enter the cluster members.

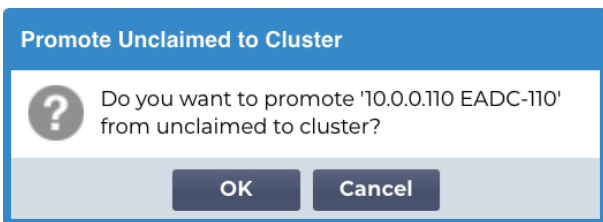
## Management

In this section, you can add and remove cluster members while also changing the priority of an ADC in the cluster. The section consists of two panels and a set of arrow keys in between. The area on the left is the Unclaimed Devices, while the rightmost area is the Cluster itself.

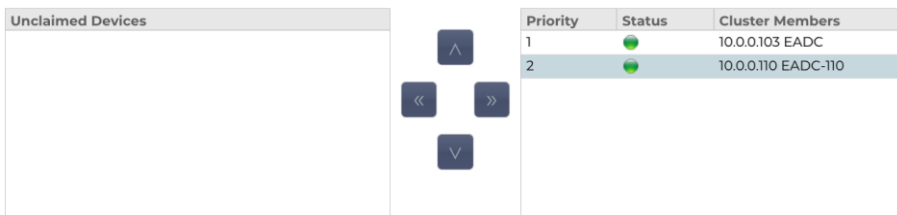


### Adding an ADC to the cluster

- Before adding the ADC to the cluster, you must ensure that all the ADC appliances have been provided with a unique name set in the System > Network section.
- You should see the ADC as Priority 1 with Status green and its name under the Cluster Members column in the management section. This ADC is the default primary appliance.
- All the other available ADC's will show up in the Unclaimed Devices window within the management section. An Unclaimed Device is the ADC that has been assigned in the Cluster Role but has no Virtual Services configured.
- Highlight the ADC from the Unclaimed Devices window and click the right arrow button.
- You will now see the following message:



- Click OK to promote the ADC to the cluster.
- Your ADC should now be showing as Priority 2 in the cluster members list.



### Manually adding an ADC to the cluster

In systems where Broadcast is blocked, you will need to choose Unicast or Hybrid mode in order to add an ADC to the cluster.

▲ Management

**Unclaimed Devices**

10.0.0.110 EADC-110
---------------------

▲

◀ ▶

▼

Priority	Status	Cluster Members
1	<span style="color: green;">●</span>	10.0.0.103 EADC-103-BETA

IP Address:

Machine Name:

**Add Server**

To add an ADC manually to the cluster:

1. Provide its IP address
2. Provide the Machine Name – this is available in the System > Networking section.

▲ Basic Setup

Name:

IPv4 Gateway:  ✓      DNS Server 1:       DNS Server 2:

IPv6 Gateway:  ✓  **Update**

3. Click Add Server

The ADC will then be added to the cluster.

If the ADC you are trying to add is already in a cluster, you will be notified via an error message.

### Removing a cluster member

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

**Unclaimed Devices**

▲

◀ ▶

▼

Priority	Status	Cluster Members
1	<span style="color: green;">●</span>	10.0.0.103 EADC
2	<span style="color: green;">●</span>	10.0.0.110 EADC-110

- You will be presented with a confirmation request.
- Click OK to confirm.
- Your ADC will be removed and be shown on the Unclaimed Devices side.

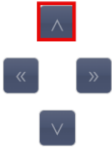
### Changing the priority of an ADC



There may be times when you wish to change the priority of an ADC within the members' list.

- The ADC at the top of the Cluster Members list is given Priority 1 and is the Active ADC for all Virtual Services
- The ADC that is second in the list is given Priority 2 and is the Passive ADC for all Virtual Services
- To change which the ADC is Active simply highlight the ADC and click the up arrow until it is at the top of the list



Unclaimed Devices



Priority	Status	Cluster Members
1		10.0.0.103 EADC
2		10.0.0.110 EADC-110

## Date and Time

The date and time section allows the setting of the ADC's date/time characteristics, including the timezone in which the ADC is located. Together with the timezone, the date and time play a vital part in the cryptographic processes associated with SSL encryption.

### Manual Date and Time

▲ Manual Date & Time

Time Zone: UTC

Current Date And Time: 14/12/2023 14:48:45

Set Date And Time: 14/12/2023 14:48:38

Update

### Time Zone

The value you set in this field represents the timezone in which the ADC is located.

- Click on the drop-down box for the Time Zone and start typing your location.
- For example London
- As you begin typing, the ADC will automatically display locations containing the letter L.
- Continue typing 'Lon,' and so on – the locations listed will be narrowed down to ones containing 'Lon.'
- If you are in, say, London, then choose Europe/London to set your location

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

### Set Date and Time

This setting represents the actual date and time.

- 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, for example, 06:00:10 for 6 am and 10 seconds.
- Once you have entered it correctly, please click Update to apply.
- You should then see the new Date and Time in bold characters.

### Synchronize Date and Time (UTC)

You can use NTP servers to synchronize your date and time accurately. The NTP servers are located globally, and you may also have your own internal NTP server when your infrastructure has limitations on external access.

▲ Synchronise Date & Time (UTC)


Enabled:

Time Server URL:

Update At [hh:mm]: 06:00 ▼

Update Period [hours]: 1 ▼

NTP Type: Public SNTP v4 ▼

 Update

### Time Server URL

Enter a valid IP address or fully qualified domain name (FQDN) for the NTP server. If the server is a globally located server on the Internet, we recommend using an FQDN.

### Update at [hh:mm]

Select the scheduled time at which you would like the ADC to synchronize with the NTP server.

### Update Period [hours]:

Select how often you would like synchronization to occur.

### NTP Type:

- Public SNTP V4 – This is the current and preferred method when synchronizing 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](#)

Note: Please note that synchronization is in UTC only. If you wish to set a local time, this can only be done manually. This limitation will be changed in later versions to enable the ability to select a time zone.

## Email Events

The ADC is a critical appliance, and like any essential system, it is equipped with the ability to inform the systems administrator of any issues that may require attention.

The System > Email Events page allows you to configure an email server connection and send notifications to system admins. The page is organized into the sections below.

### Address

▲ **Address**

Send E-Mail Events To E-Mail Address:

Return E-Mail Address:

### Send to Email Events to Email Addresses

Add a valid email address to send the alerts, notifications, and events to. Example [support@domain.com](mailto:support@domain.com). You can also add multiple email addresses using a comma separator.

### Return Email Address:

Add in an email address that will appear in the inbox. Example [adc@domain.com](mailto:adc@domain.com).

### Mail Server (SMTP)

In this section, you must add the SMTP server details to be used to send the emails. Please ensure that the email address you use for sending is authorized to do so.

▲ **Mail Server [SMTP]**

Host Address:

Port:

Send Timeout:  minutes

Use Authentication:

Security:

Mail Server Account Name:

Mail Server Password:

### Host address

Add in the FQDN or IP address of your SMTP server.

### Port

Add in the Port of your SMTP server. Default Port for SMTP is 25 or 587 if you use SSL.

### 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
- The 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

Enabled Notifications And Event Descriptions In Mail

Enable All Event  Disable All Event

IP Service Notice: Service started IP Services Alert: Service stopped

Virtual Service Notice: Virtual Service started Virtual Service Alert: Virtual Service stopped

Real Server Notice: Server contacted Real Server Alert: Server not contactable

flightPATH: flightPATH

Group Notifications Together:

Grouped Mail Description: Event notifications

Send Grouped Mail Every: 30 minutes

There are several types of event notifications that the ADC will send to persons configured to receive them. You can tick and enable the notifications and alerts that should be sent out. Notifications occur when Real Servers are contacted or channels started. Alerts occur when Real Servers cannot be contacted, or channels stop working.

## IP Service Notice

The IP Service notice will inform you when any Virtual IP address is online or has stopped working. This action is carried out for all Virtual services that belong to the VIP.

## Virtual Service Notice

Informs the recipient a Virtual Service is online or has stopped working.

## Real Server Notice

When a Real Server and Port is connected or is not contactable, the ADC will send the Real Server notice.

## flightPATH

This notice is an email sent out when a condition has been met, and there is an action configured instructing the ADC to email the event.

## Group Notifications Together

Tick to group notifications together. With this ticked, all the notifications and alerts will be aggregated into one email.

## Group Mail Description

Specify the relevant subject matter for the group notice email.

## Group Send interval

Stipulate the amount of time you wish to wait before sending a group notification email. The minimum time is 2 minutes. The default is set to 30 minutes.

## Enabled Warnings and Event Descriptions in Mail

▲ Enabled Warnings And Event Descriptions In Mail

Disk Space Warning:

Warn If Free Space Less Than:  %

Licence Renewal Warning:

There are two types of warning emails, and neither should be ignored.

### Disk Space

Set the percentage of free disk space before which the warning is sent. When this is reached, you will be emailed.

### Warn if Free Space Less Than

You can set a percentage value here so the ADC can send a warning email should the disk space fall below this threshold.

### Licence Expiry

This setting allows you to enable or disable the license expiration warning email sent to the system admin. When this is reached, you will be emailed.

## History

In the System section, there is the System History option, allowing the delivery of historical data for elements such as CPU, memory, requests per second, and other features. Once enabled, 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 ADC.

### Collect Data

▲ Collect Data

Enabled:

Collect Data Every: 1 Second(s) (1-60)

Update

#### Enable

To enable the collection of data, please tick the checkbox.

#### Collect Data Every

Next, set the time interval at which you wish the ADC to collect the data. This time value can range between 1-60 seconds.

### Maintenance

▲ Maintenance

**Most Recent Update**

Fri, 15 Dec 2023 14:45:42

Refresh

**Backup**

Backup Name:

Backup

**Delete**

Select To Delete:

Delete

**Restore**

Select To Restore:

Restore

#### Most Recent Update

This shows when the last history data was collected from the ADC.

This section will be greyed out if you have enabled historical logging. Please untick the Enabled checkbox in the Collect Data section and click Update to allow the maintenance of the historical logs.

### HP Enterprise Based ADCs

This section of features is only valid for ADCs that are installed on HPE ProLiant bare metal servers, and make use of ILO.

#### Backup

Give your backup a descriptive name. Click Backup to backup all the files to the ADC

#### Delete

Select a backup file from the drop-down list. Click Delete to remove the backup file from the ADC

## Restore

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



## License

The ADC is licensed for use either using one of the following models, which depends on your purchase parameters and customer type.

License Type	Description
Perpetual	You, the customer, have the right to use the ADC and other software in perpetuity. It does not preclude you from having to purchase support to receive assistance and updates.
SaaS	SaaS or Software-as-a-Service means you essentially rent the software on an ongoing or pay-as-you-go basis. In this model, you pay an annual rental for the software. You do not have perpetual rights to use the software.
MSP	Managed Service Providers can offer the ADC as a service and purchase the license on a per-VIP basis, charged and paid annually.

### License Details

Each license includes specific details pertinent to the person or organization purchasing it.

Licence Details	
Licence ID:	8090DD7C-DE8D6A1
Machine ID:	F F3
Issued To:	Edgenexus
Contact Person:	Jay Savor
Date Issued:	06 Dec 2023
Name:	

### License ID

The License ID is directly linked to the Machine ID and other details specific to your purchase and ADC appliance. This information is essential and is required when you wish to retrieve updates and other items from the App Store.

### Machine ID

The Machine ID is generated using the eth0 IP address of the ADC appliance. If you change the IP address of the ADC appliance, the license will no longer be valid. You will have to contact support for assistance. We recommend that your ADC appliance(s) have fixed IP addresses with instructions to your IT staff not to change them. Technical support is available by raising a ticket at <https://www.edgenexus.io/support>.

**Note:** You must not change the IP address of your ADC appliances. If you are in a virtualized framework, then please fix the MAC ID and use a static IP Address.

### Issued To

This value contains the purchaser's name associated with the ADC's Machine ID.

### Contact Person

This value contains the contact person to be contacted at the customer's company associated with the Machine ID

### Date Issued

The date on which the license was issued.

## Name

This value shows the descriptive name for the ADC Appliance that you have provided in System > Networking.

## Facilities

▲ Facilities	
Layer 4:	Permanent licence
Layer 7:	Permanent licence
SSL:	Permanent licence
Acceleration:	Permanent licence
flightPATH:	Permanent licence
Pre-Authentication:	Permanent licence
Global Server Load-Balancing:	Permanent licence
Firewall:	Permanent licence
Throughput:	3 Gbps permanent licence
Virtual Service IPs:	24 Virtual Service IPs permanent licence
Real Server IPs:	64 Real Server IPs permanent licence

The facilities section provides you with information on which functions within the ADC have been licensed for use and the license validity. Also displayed is the throughput that has been licensed for the ADC and the number of Real Servers. This information is dependent on the license you have purchased.

## Install License

▲ Install Licence

Upload Licence:

Paste Licence: Please paste licence in here or upload the licence file above

- Installing a new license is very simple. When you receive your new or replacement license from Edgenexus, it will be sent in the form of a text file. You can open the file and then copy and paste the content into the Paste License field.
- You can also upload it to the ADC if copy/paste is not an option for you.

- Once you have done this, please click the update button.
- The license is now installed.

## License Service Information

Clicking the License Service Information button will display all the information on the license. This function can be used for sending the details to support personnel.

MAC Address: 00:3C

Current Version: 4.3.0 (Build 1965) c50631

Server Ref: EADC

OS Version: Linux jetnexus 2.6.32-754.31.1.el6.x86\_64 #1 SMP

Licence Configuration: [jetnexusdaemon].001Licence="jetNEXUS ALB Licence".002Customer="Issued To,Edgenexus".003Contact="Contact Person,.".004Tel="Telephone,.".005LicenseID="License ID,(8090D[ DE8D6A1)".Customer="Edgenexus".100Details="Details"

System Configuration: [jetnexusdaemon]AdaptivePollingEnabled=1AddXForwardedFor=1AdvancedW3C="HTTP Layer4"AllowCompressedUploads=0AllowIdentity=0AlwaysChunk=0ApiSessionTimeout="525600"

System Log: 18 Dec 00:28:12 jetnexus software-monitoring: Stats|HitCount=0|InputBytes=0|OutputBytes=0|CompressedInputBytes=0|CompressedOutputBytes=0|TotalClientConnections=0|TotalServerConnections=0|CurrentConnections=0|MaximumConnections=0|RefusedConnections=0|UploadInputBytes=0|UploadOutputBytes=0|UploadCompressedInputBytes=0|UploadCompressedOutputBytes=0|TotalInputBytes=461,445,645|TotalOutputBytes=378,426,680|Memory=184,552,448|MemoryUsagePercent=10|DiskFreeSpace=19,308,112|DiskFree=98|CPUPercent=3|CPUHostPercent=0|EthernetErrors=0|Runnable=1|Processes=424|Sessions=0|NewSess=0|ExpiredSess=0|RevalidatedSess=0|BLCon=0|BLMax=5,000|BLFill=0|BLAlloc=0|BLRoom=655,360,000|BMCon=0|BMMax=5,000|BMFill=0|BMAlloc=0|BMRoom=30,000,000|BTCCon=0|BTMax=10,000|BTFill=0|BTAlloc=0|BTRoom=20,000,000|BSecure=0|CONNECTIONS=5|TIME-WAIT=0|ALLOCSOCK=134|ORPHANSOCK=0|SOCKMEM=0|ESTABLISHED=0|SYN=0|PORTS=21

## Logging

The System > Logging page allows you to set the W3C logging levels and specify the remote server to which logs will be automatically exported. The page is organized into the four sections below.

### W3C Logging Details

Enabling W3C logging will cause the ADC to start 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 indicating the fields (providing column names) so that data can be mined. There are separate files for HTTP and FTP protocols.

▲ W3C Logging Details

W3C Logging Levels: None

Include jetNEXUS W3C Logging: Forwarded-For Address and Port

Include jetNEXUS Security Information: On

Update

### W3C Logging Levels

There are different logging levels available, and depending on the service type, the data provided varies.

The table below describes logging levels for W3C HTTP.

Value	Description
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-ur- -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-roun-trip-time x-sc(Content-Type).
Site	This format is very similar to “Full” but has an additional field. See the summary of the fields 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-ur--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

The table below describes logging levels for W3C FTP.

Value	Description
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

### Include W3C Logging

This option allows you to set what ADC information should be included in the W3C logs.

Value	Description
Client's Network Address and Port	The value shown here displays the actual client IP address along with the port.
Client's Network Address	This option will include and only show the actual client IP address.
Forwarded-For Address and Port	This option will show the details held in the XFF header, including the address and port.
Forwarded-For Address	This option will show the details held in the XFF header, including the address only.

### Include Security Information

This menu consists of two options:

Value	Description
On	This setting is global. When set to on, the username will be appended to W3C log when any Virtual Service is using Authentication and has W3C logging enabled.
Off	This will turn off the ability to log the username to the W3C log on a global level.

### Syslog Server

▲ Syslog

Message Level: Warning

Update

This section allows you to set the level of message logging performed to the SYSLOG server. The options available are as follows.

Error

Warning

Notice

Info

## Remote Syslog Server

▲ Remote Syslog Server

Syslog Server 1:  Port:   Enabled:

Syslog Server 2:  Port:   Enabled:

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 whether you wish to use TCP or UDP
- Tick the Enabled checkbox to begin logging
- Click Update

## Remote Log Storage

▲ Remote Log Storage

Remote Log Storage:

IP Address:

Share Name:

Directory:

Username:

Password:

All W3C logs are stored in compressed form onto the ADC every hour. The oldest files will be deleted when 30% of disk space is remaining. Should you wish to export these to a remote server for safekeeping, you can configure this using an SMB share. Please note that the W3C log will not transfer to the remote location until the file has been completed and compressed. As the logs are written every hour, this could take up to two hours in a Virtual Machine appliance and five hours for a hardware appliance.

Col1	Col2
Remote Log Storage	Tick the box to enable remote log storage
IP Address	Specify the IP address of your SMB server. This should be in dotted decimal notation. Example: 10.1.1.23
Share Name	Specify the share name on the SMB server. Example: w3c.
Directory	Specify the directory on the SMB server. Example: /log.
Username	Specify the username for the SMB share.
Password	Specify the password for the SMB share

## Field Summary

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 Real Server used
x-r-port	Port of Real 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 Real 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 pcon	millisecond from connect to posting in "newbie list" 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

▲ Clear Log Files

Log Type:

This feature allows you to clear the log files from the ADC. You can select the type of log you wish to delete from the drop-down menu and then click the Clear button.



## Network

The Network section within the Library allows the configuration of the ADC's network interfaces and their behavior.

### IMPORTANT

### Managing Virtual Network Interfaces in a Virtual Environment

When deploying VMs within a virtualized environment such as ESXi, network interfaces (e.g., eth0, eth1) are automatically created and mapped to host configuration network adapters (e.g., Network Adapter 1, Network Adapter 2). However, these mappings may not always align consistently due to operating system rules that bind interfaces to specific MAC addresses. This section outlines steps to manage network interfaces on the host to prevent disruptions to services when the user cannot access the VM.

#### Key Considerations

- MAC Address Persistence:**
  - The operating system assigns interface names (e.g., eth0, eth1) based on rules that associate a name with a specific MAC address.
  - Deleting and recreating a VM network interface without reusing the original MAC address can result in an inconsistent or non-functional network configuration.
- Internal Mappings in ADC (EdgeOS):**
  - Virtual network interfaces are automatically recognized by the ADC (Application Delivery Controller) and mapped internally.
  - Removing a network interface from the VM host can leave stale mappings in the ADC, potentially disrupting management access or network services.

#### Recommended Steps for Host Configuration

- Before Removing a NIC:**
  - Record the MAC address of the interface you intend to remove. This can be viewed in the VM's settings in the ESXi host.
- When Adding a Replacement NIC:**
  - Assign the previously recorded MAC address to the new network adapter to ensure the VM's interface mappings remain consistent.
- Prevent Accidental Deletion of Critical NICs:**
  - Identify which NICs are mapped to critical ADC interfaces (e.g., ETH0 (Greenside) for management access). Avoid removing these NICs unless absolutely necessary.
- Verify MAC Address Consistency:**
  - Ensure that the MAC addresses assigned to the VM's network interfaces match the expected configuration within the ADC. Use ESXi host tools to confirm this mapping.
- Coordinate with VM Administrators:**
  - If changes are necessary that might affect the internal VM configuration, inform the VM administrators to prepare for potential disruptions and ensure proper mappings are maintained.

#### Example Scenario

- Initial Setup:**
  - ADC VM has two NICs: NIC1 (MAC: 00:11:22:33:44:55) and NIC2 (MAC: 00:11:22:33:44:66).
- Action:** Remove NIC1 and add a new NIC (NIC3).
  - Assign the original MAC address (00:11:22:33:44:55) to NIC3 during creation on the ESXi host.
- Impact Avoidance:**
  - By reusing the original MAC address, the ADC's internal mappings (e.g., ETH0) remain consistent, avoiding any disruption to management access or network services.

When managing network interfaces in a virtualized environment, it is crucial to maintain consistency in MAC address assignments. If access to the VM is unavailable, all necessary steps must be completed on the host side to ensure seamless operation and prevent service interruptions. Always coordinate with the relevant administrators to address potential impacts effectively.

## Avoiding Frequent vMotion for Critical Appliances

vMotion is a powerful VMware feature that enables live migration of virtual machines (VMs) between ESXi hosts without downtime. However, while vMotion is highly useful in maintaining infrastructure flexibility and availability, it is not recommended to frequently migrate critical appliances, such as load balancers, especially when they are actively managing a high volume of connections.

There may be other technologies that are similar and provided by other vendors, but for this section, we will work on the basis it is VMware.

### Why Frequent vMotion is Not Recommended

- 1. Session Disruptions:**
  - a. Load balancers manage active sessions between clients and backend servers. During a vMotion operation, there is a brief period where the network state is reinitialized, potentially disrupting these sessions.
  - b. The disruption may cause connection drops, requiring clients to re-establish their sessions, which could degrade user experience.
- 2. Latency and Packet Loss:**
  - a. The process of migrating a VM involves temporarily pausing and synchronizing its memory and state. For appliances handling real-time traffic, this pause can introduce latency or even packet loss.
  - b. Applications relying on low-latency responses may experience degraded performance or timeouts.
- 3. Increased Resource Utilization:**
  - a. vMotion requires CPU, memory, and network bandwidth resources for data synchronization between the source and destination hosts.
  - b. Frequent migrations can strain infrastructure resources, potentially impacting other VMs and services hosted on the same environment.
- 4. Impact on High-Availability Configurations:**
  - a. In environments with high-availability (HA) configurations, frequent vMotion may conflict with failover mechanisms, leading to unexpected behavior or delays in failover actions.
- 5. Operational Complexity:**
  - a. Constantly moving critical VMs increases the complexity of network configurations, including VLAN mappings and firewall rules, which can introduce configuration errors.

### Recommendations for Managing Critical Appliances

- 1. Plan vMotion Operations During Maintenance Windows:**
  - a. Schedule migrations during periods of low traffic to minimize the impact on active sessions.
- 2. Implement Load Balancer Clustering:**
  - a. Use clustering or high-availability configurations for load balancers to ensure redundancy. This allows traffic to be seamlessly redirected to another node during vMotion operations.
- 3. Monitor Infrastructure Resources:**
  - a. Ensure sufficient CPU, memory, and network bandwidth are available before initiating vMotion to prevent resource contention.
- 4. Minimize Migration Frequency:**
  - a. Limit vMotion of critical appliances to scenarios where it is absolutely necessary, such as host maintenance or failure recovery.
- 5. Test Before Production:**
  - a. Test vMotion operations in a staging environment to understand their impact on active sessions and ensure configurations are optimized.

While vMotion is an invaluable tool for VM management, it should be used judiciously for critical appliances like load balancers. Frequent migrations can disrupt services, increase latency, and strain resources. By

carefully planning vMotion operations and employing strategies like clustering and maintenance scheduling, you can ensure reliable service delivery and minimize the risk of disruptions.

## Basic Setup

Basic Setup

Name: EADC

IPv4 Gateway: 10.0.0.1 ✓ DNS Server 1: 8.8.8.8 DNS Server 2:

IPv6 Gateway: ✓ Update

## ALB Name

Specify a name for your ADC appliance. Please note that this cannot be changed if there is more than one member in the cluster. Please see the section on Clustering.

## IPv4 Gateway

Specify the IPv4 Gateway address. This address 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 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

Specify the IPv6 Gateway address. This address 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 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 & DNS Server 2

Add in the IPv4 address of your first and second (optional) DNS server.

## Adapter Details

This section of the Network panel shows the network interfaces that are installed in your ADC appliance. You can add and remove adapters as needed.

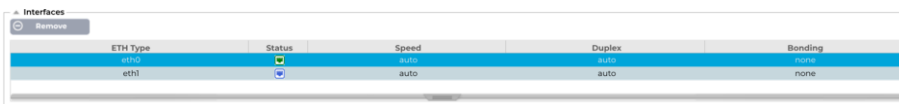
Adapter	VLAN	IP Address	Subnet Mask	Gateway	BP Filter	Description	Web Console	REST
emc		10.0.0.103	255.255.255.0			Green side		





Column	Description
Adapter	This column displays the physical adapters installed on your appliance. Choose an adapter from the list of available adapters by clicking on it – a double-click will place the listing line into edit mode.
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 ADC 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 ADC to be installed in more complex networking environments without the trouble of manually configuring complex policy based routing.
Description	Double click to add a description for your adapter. Example Public Interface.
	<p><b>Note: The ADC will automatically name the first interface Green Side, the second interface Red Side and the third interface Side 3 etc.</b></p>
	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 Interfaces section within the Network panel allows the configuration of certain elements pertaining to the network interface. You can also remove a network interface from the listing by clicking the Remove button. When using a virtual appliance, the interfaces you see here are limited by the underlying virtualization framework.



Column	Description
ETH Type	This value indicates the internal OS reference to the network interface. This field cannot be customized. Values begin with ETH0 and continue in sequence depending on the number of network interfaces.
Status	<p>This graphical indication shows the current status of the network interface. A Green status shows that the interface is connected and up. Other status indicators are shown below.</p> <ul style="list-style-type: none"> <li> <b>Adapter UP</b></li> <li> Adapter Down</li> <li> Adapter Unplugged</li> <li> Adapter Missing</li> </ul>
Speed	By default, this value is set to auto-negotiate the speed. But you can change the network speed of the interface to any value available in the drop-down (10/100/1000/AUTO).
Duplex	The value of this field is customizable, and you can choose between Auto (default), Full-Duplex, and Half-Duplex.
Bonding	You can choose one of the bonding types that you have defined. See the section on Bonding for more details.

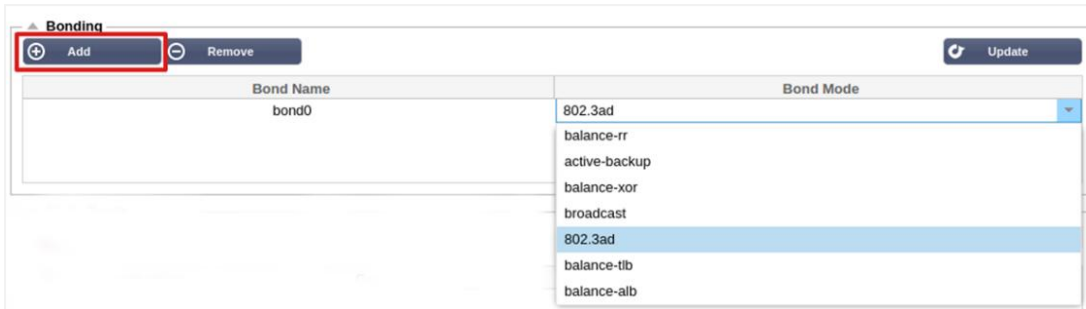
## Bonding

Many names are used to title network interface bonding: Port Trunking, Channel Bonding, Link Aggregation, NIC teaming, and others. Bonding combines or aggregates multiple network connections into

a single channel bonded interface. Bonding allows two or more network interfaces to act as one, increase throughput, and provide redundancy or failover.

The ADC’s kernel has a built-in Bonding driver for aggregating multiple physical network interfaces into a single logical interface (for example, aggregating eth0 and eth1 into bond0). For each bonded interface, you can define the mode and the link monitoring options. There are seven different mode options, each providing specific load balancing and fault tolerance characteristics. These are shown in the image below.

Note: Bonding can only be configured for hardware-based ADC appliances.

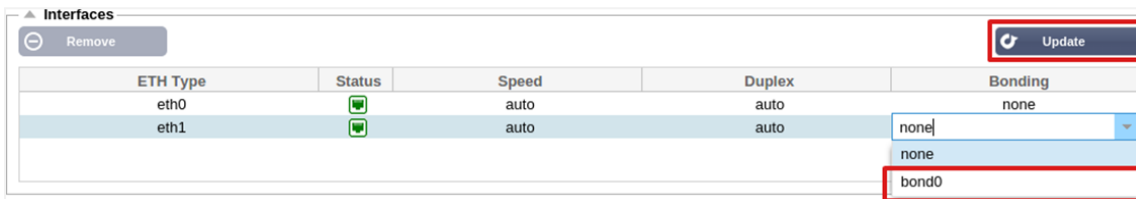


### Creating a Bonding profile

- Click on Add button to add a new Bond
- Provide a name for the bonding configuration
- Choose which bonding mode you wish to use

Then from the Interfaces section, select the Bonding mode you wish to use from the Bond drop-down field for the network interface.

In the example below, eth0, eth1, and eth2 are now part of bond0. While Eth0 remains on its own as the management interface.



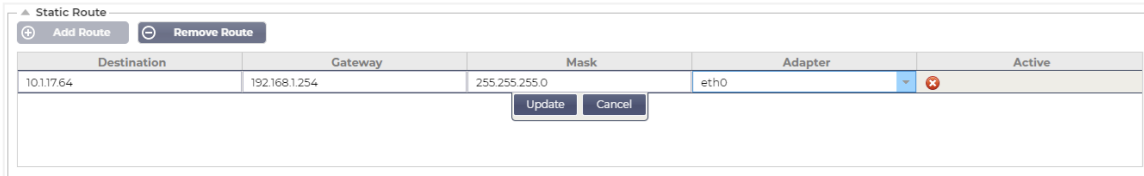
### Bonding Modes

Bonding Mode	Description
balance-rr:	Packets are sequentially transmitted/received through each interface one by one.
active-backup:	In this mode, one interface will be active, and the second interface will be on 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 option selects the same slave for each destination Mac address.
broadcast:	This mode will transmit all data on all slave interfaces.
802.3ad:	Creates aggregation groups that share the same speed and duplex settings and utilizes all the slaves in the active aggregator following 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. The current slave receives incoming traffic. 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.
--------------	---

## Static Route

There will be times when you need to create static routes for specific subnets within your network. The ADC provides you with the ability to do this using the Static Routes module.



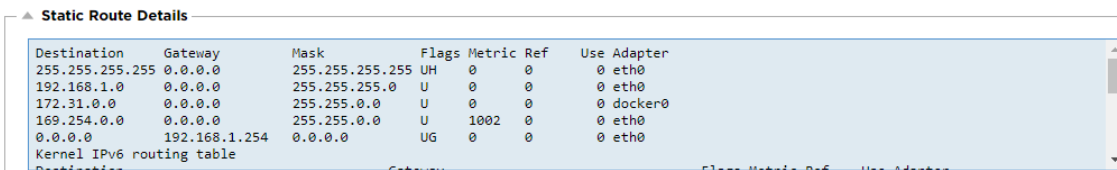
### Adding a Static Route

- Click the Add Route button
- Fill in the field using the details in the table below as guidance.
- Click the Update button when done.

Field	Description
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 reached 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 the routes configured on the ADC.



## Advanced Network Settings



### What is Nagle?

Nagle's Algorithm, also known as the TCP No Delay algorithm, is a technique used in network communication to reduce the number of retransmitted packets due to out-of-order data. It works by delaying the sending of small packets if no acknowledgment has been received for previous packets. This helps to ensure that data arrives in the correct order and reduces the load on the network.

See [WIKIPEDIA ARTICLE ON NAGLE](#)

## Server Nagle

Tick this box to enable the Server Nagle setting. The Server Nagle is a means of improving the efficiency of TCP/IP networks by reducing the number of packets that need to be sent over the network. This setting 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 the Client Nagle setting. As above but applied to the Client side of the transaction.

## SNAT



SNAT stands for Source Network Address Translation, and different vendors have slight variations in the implementation of SNAT. A simple explanation of the EdgeADC SNAT would be as follows.

Under normal circumstances, inbound requests would be directed to the VIP that would see the source IP of the request. So, for example, if a browser endpoint had an IP address of 81.71.61.51, this would be visible to the VIP.

When SNAT is in force, the original source IP of the request will be hidden from the VIP, and instead, it will see the IP address as provided in the SNAT rule. Thus, SNAT can be used in Layer 4 and Layer 7 load balancing modes.

Field	Description
Source IP	The Source IP address is optional, and it can be either a network IP address (with /mask) or a plain IP address. The mask can be either a network mask or a plain number, specifying the number of 1's at the left side of the network mask. Thus, a mask of /24 is equivalent to 255.255.255.0.
Destination IP	The Destination IP address is optional, and it can be either a network IP address (with /mask) or a plain IP address. The mask can be either a network mask or a plain number, specifying the number of 1's at the left side of the network mask. Thus, a mask of /24 is equivalent to 255.255.255.0.
Source Port	The source port is optional, it can be a single number, in which case it specifies only that port, or it can include a colon, which specifies a range of ports. Examples: 80 or 5900:5905.
Destination Port	The destination port is optional, it can be a single number, in which case it specifies only that port, or it can include a colon, which specifies a range of ports. Examples: 80 or 5900:5905.
Protocol	You can choose whether to use SNAT on a single protocol or all the protocols. We suggest being specific to be more precise.
SNAT to IP	SNAT to IP is a mandatory IP address or a range of IP addresses. Examples: 10.0.0.1 or 10.0.0.1-10.0.0.3.
SNAT to Port	The SNAT to Port is optional, it can be a single number, in which case it specifies only that port, or it can include a dash, which specifies a range of ports. Examples: 80 or 5900-5905.
Notes	Use this to put a friendly name to remind yourself why the rules exist. This is also useful for debugging in the Syslog.

# Power

This ADC system feature also allows you to conduct several power-related tasks on your ADC.


## Restart

▲ **Restart**

Click the Restart button to quickly stop and start essential jetNEXUS ALB services.

**Warning** - This will cause a brief break in current connections.

Software Version : 4.2.6 (Build 1831) 3j1329

 Restart


This setting initiates a global restart of all Services and consequently breaks all currently active connections. All the Services will automatically resume after a short period, but the timing will depend on how many Services are configured. A pop-up will be displayed requesting confirmation for the restart action.

## Reboot

▲ **Reboot**

Click the Reboot button to re-initialise all jetNEXUS ALB services.

**Warning** - This will suspend your Connections and Services for about 2 minutes.

 Reboot

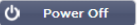
Clicking the Reboot button will power cycle the ADC and automatically bring it back to an active state. A pop-up will be displayed requesting confirmation for the reboot action.

## Power Off

▲ **Power Off**

Click the Power off button to completely halt jetNEXUS ALB.

**Warning** - This will suspend your Connections and Services and require a hardware power on.

 Power Off

Clicking the Power Off button will shut down the ADC. If this is a hardware appliance, you will need physical access to the device to power it back on. A pop-up will be displayed requesting confirmation for the shutdown action.



## Security

This section allows you to change the web console password and enable or disable the Secure Shell access. It also allows the enablement of the REST API capability.

### SSH

▲ SSH

Secure Shell Remote Conn:

Option	Description
Secure Shell Remote Conn	Please tick the box if you wish to gain access to the ADC using SSH. "Putty" is an excellent application for doing this.

### Authentication Service

▲ Authentication Service


Authentication Mode: Remote Then Local

Authentication Source:

ALB GUI Admin Groups:

ALB GUI Read/Write Groups:

ALB GUI Read-Only Groups:

 Update

In most organisations there will be a requirement that accessing the ADC's management interface must be done via the company's own authentication services.

For such scenarios, we have provided the Authentication Service feature described here. This feature operates with local directory services, as well as external services such as SAML.


Option	Description
Authentication Mode	Local Only : This is the default mode and uses the local database within the ADC, for example for the user, admin.  Remote then Local: The ADC will attempt to validate the user against the remote authentication server specified in the Authentication Source field. If it is not successful, it will then use the local database as the source for validation.
Authentication Source	This drop-down menu allows you to select one of the authentication servers you have defined in Library > Authentication.
ALB GUI Admin Groups	Specify the permitted admin groups allowed.
ALB GUI Read/Write Groups	Specify the Read/Write groups allowed
ALB GUI Read-Only Groups	Specify the Read-Only groups allowed.

### Web Console

▲ Webconsole

SSL Certificate: default

Secure Port: 443

 Update

SSL Certificate Choose a certificate from the drop-down list. The certificate you choose will be used to secure your connection to the ADC's web user interface. You can create a self-signed certificate within the ADC or import one from the [SSL CERTIFICATES](#) section.

Option	Description
Secure Port	The default port for the web console is TCP 443. If you wish to use a different port for security reasons, you can change it here.

## REST API

The REST API, also known as RESTful API, is an application programming interface that conforms to the REST architectural style and allows configuration of the ADC or data extraction from the ADC. The term REST stood for representational state transfer and was created by computer scientist Roy Fielding.

Option	Description
Enable REST	Tick this box to enable access using the REST API. Note that you will also have to configure which adapter on which REST is enabled. See the note on the Cog link below.
SSL Certificate	Choose a certificate for the REST service. The drop-down will show all the certificates installed on the ADC.
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

Documentation on how to use the REST API is available: [jetAPI | 4.2.3 | jetNEXUS | SwaggerHub](#)

*Note: If you get errors on the Swagger page this is because they have an issue supporting query strings  
Scroll past the errors to jetNEXUS 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 SNMP section allows the configuration of the SNMP MIB residing within the ADC. The MIB can then be queried by third-party software capable of communicating with devices equipped with SNMP.

### SNMP Settings

Option	Description
SNMP v1 / V2C	Tick the checkbox to enable the V1/V2C MIB. SNMP v1 conforms with RFC-1157. SNMP V2c conforms with RFC-1901-1908
SNMP v3	Tick the checkbox to enable the V3 MIB. 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 <b>jetnexus</b>

### 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.

#### MIB Download

The MIB can be downloaded [here](#):

#### ADC OID

#### ROOT OID

```
iso.org.dod.internet.private.enterprise = .1.3.6.1.4.1
```

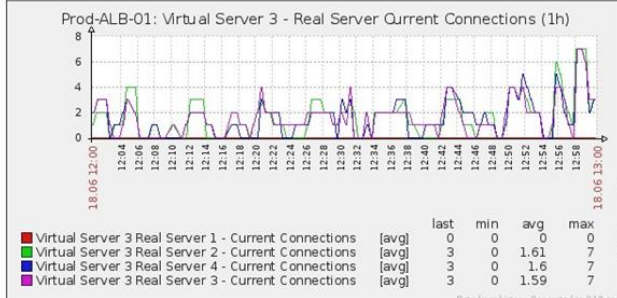
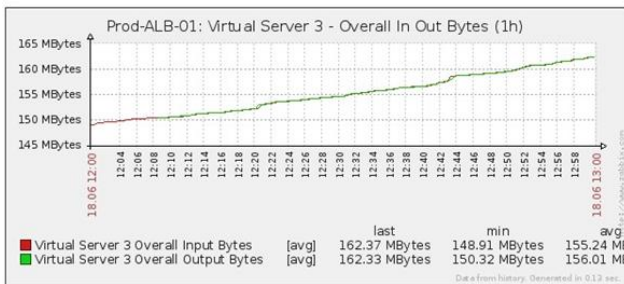
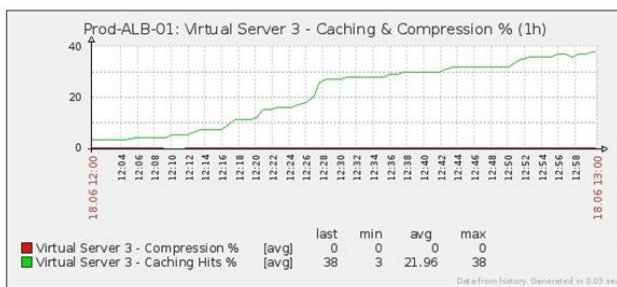
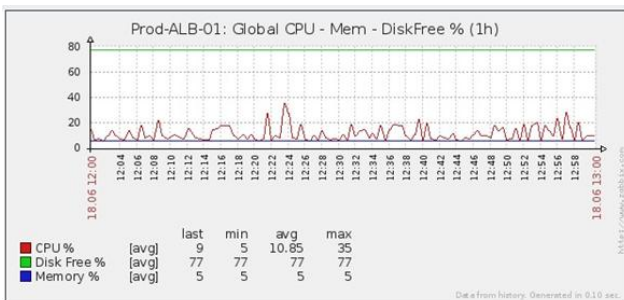
#### Our OIDs

```
.38370 jetnexusMIB
.1 jetnexusData (1.3.6.1.4.1.38370.1)
.1.1 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)
.1.1 jetnexusGlobal (1.3.6.1.4.1.38370.1.1)
.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 for the ADC's Custom SNMP MIB is the ability to offload the historical graphing to a management console of your choice. Below are some examples from Zabbix that polls an ADC for various OID values listed above.



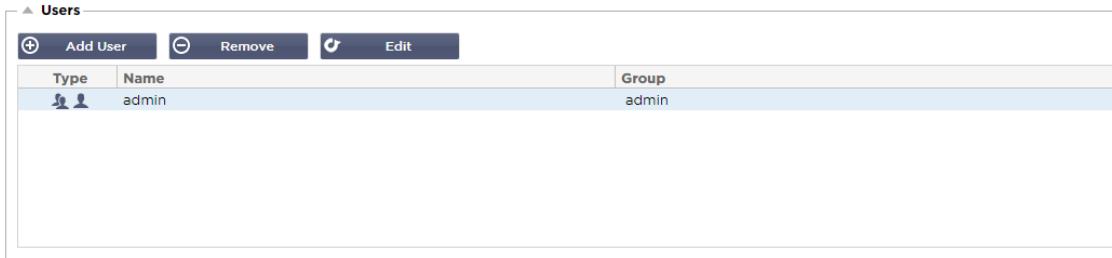
## Users and Audit Logs

The ADC provides the ability to have an internal set of users to configure and define what the ADC does. Users defined within the ADC can perform a variety of operations depending on the role attached to them.

There is a default user called **admin** that you use when first configuring the ADC. The default password for admin is **jetnexus**.

### Users

The Users section is provided for you to create, edit and remove users from the ADC.



### Add User

The screenshot shows the 'Add User' dialog box. It has a blue header with a person icon and the text 'Users'. The form contains the following fields and options:




- Username:** A text input field with a red border.
- New Password:** A text input field with a strength indicator showing '6 or more letters and num'.
- Confirm Password:** A text input field with a strength indicator showing '6 or more letters and num'.
- Group Membership:** A list of checkboxes:
  - Admin
  - GUI Read Write
  - GUI Read
  - SSH
  - API
  - Add-Ons

At the bottom of the dialog, there are two buttons: 'Update' (with a refresh icon) and 'Cancel' (with a minus icon).

Click the Add User button shown in the image above to bring up the Add User dialog.

Parameter	Description/Usage
Username	Enter a username of your choice. The username must comply with the following: <ul style="list-style-type: none"> <li>• Minimum number of characters 1</li> <li>• Maximum number of characters 32</li> <li>• Letters can be upper and lower case.</li> <li>• Numbers may be used.</li> <li>• Symbols are not permitted</li> </ul>
Password	Enter a <b>strong</b> password that conforms with the below requirements. <ul style="list-style-type: none"> <li>• Minimum number of characters 6</li> <li>• Maximum number of characters 32</li> <li>• Must use at least a combination of letters and numbers.</li> <li>• Letters can be upper or lower case.</li> <li>• Symbols are permitted except for those in the example below <b>£, %, &amp;, &lt;, &gt;</b></li> </ul>
Confirm Password	Confirm the password again to ensure it is correct
Group Membership	Tick the group that you would like the user to belong to. <ul style="list-style-type: none"> <li>• Admin - This group can do everything.</li> <li>• GUI Read Write - Users in this group can access the GUI and make changes via the GUI.</li> <li>• GUI Read - Users in this group can access the GUI to view information only. No changes can be made.</li> <li>• SSH - Users in this group can access the ADC via Secure Shell. This choice will give access to the command line, which has a minimal set of commands available.</li> <li>• API - Users in this group will have access to SOAP and REST programmable interface. REST will be available from Software Version 4.2.1</li> <li>• Add-Ons - Permission is granted to access Add-On configurations.</li> </ul>

## User Type

	<p><b>Local User</b></p> <p>The ADC in Stand-Alone or Manual H/A role will create Local Users only. By default, a local user called “admin” is a member of the admin group. For backward 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.</p>
	<p><b>Cluster User</b></p> <p>The ADC in Cluster role will create Cluster Users only. Cluster Users are synchronized across all the ADCs 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, you will not be able to switch roles from Cluster to Manual or Stand-Alone</p>
	<p><b>Cluster and Local User</b></p> <p>Any users created while in Stand-Alone or Manual role will be copied to the Cluster. If the ADC subsequently leave the Cluster, then only Local Users will remain. The last configured password for the user will be valid.</p>

## Removing a User

- 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 final remaining cluster user in the admin group.
- You will not be able to delete the admin user for backward compatibility.
- If you remove the ADC from the cluster, all users except local users will be deleted.



### Editing a User

- 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

The ADC logs changes made to the ADC configuration 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 **LOGS** section. For example:

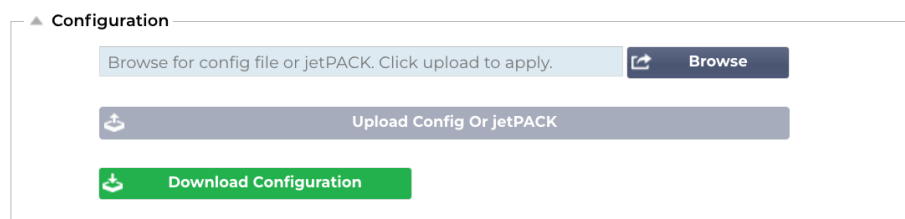
Date/Time	Username	Section	Action
09:49:01 Fri 15 Dec 2023	admin	warning	Passwords must have 6 or more characters
09:49:01 Fri 15 Dec 2023	admin	import certificate [Jet2]	
09:48:15 Fri 15 Dec 2023	admin	error	Failed to create local certificate
09:48:14 Fri 15 Dec 2023	admin	Cert	Create
15:17:44 Thu 14 Dec 2023	admin	IP Services	Deleted: virtual service: :
15:17:44 Thu 14 Dec 2023	admin	IP Services	Deleted: virtual service: (Web Sites 443)
15:17:40 Thu 14 Dec 2023	admin	IP Services	Deleted: virtual service: 10.0.0.130:80 (Web Sites)

 View  Download

# Advanced



## Configuration



It is always best practice to download and save the configuration of the ADC once it is fully set up and working as required. You can use the Configuration module to both download and upload a configuration.

Jetpacks are configuration files for standard applications and are provided by Edgenexus to simplify your job. These, too, can be uploaded to the ADC using the Configuration module.

A configuration file is essentially a text-based file, and as such, can be edited by you using a text editor such as Notepad++, Nano or VI. Once edited as required, the configuration file can be uploaded into the ADC.

### CAUTION:

Editing the configuration file of the EdgeADC is only intended for trained experts. Should you decide to edit the configuration file yourselves, and a technical issue ensues, Edgenexus Technical Support will no longer be able to support the product.

### Downloading a configuration

- To download the current configuration of the ADC, press the Download Configuration button.
- A pop-up will appear asking you to open or save the .conf file.
- Save to a convenient location.
- You can open this with any text editor, such as Notepad++.

### Uploading a configuration

- You may upload a saved configuration file by browsing for the saved .conf file.
- Click the 'Upload Config or Jetpack' button.
- The ADC will upload and apply the config and then refresh the browser. If it does not refresh the browser automatically, please click refresh on the browser.
- You will be redirected to the Dashboard page upon completion.

**Critical: It is critical that you do not attempt to copy the configuration from one ADC to another without prior consultation with Edgenexus Support. Doing so may render your ADC irrecoverable.**

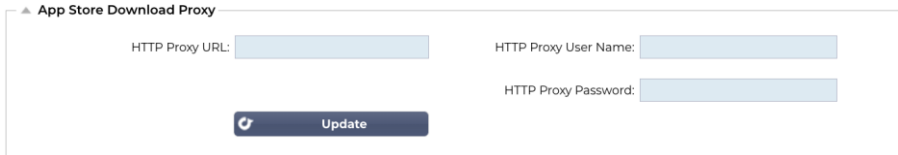
### Upload a JetPACK

- A JetPACK is a set of configuration updates to the existing configuration.
- A JetPACK can be as small as changing the TCP Timeout value right up to a complete application-specific configuration such as Microsoft Exchange or Microsoft Lync.
  - You can obtain a JetPACK from the support portal shown at the end of this guide.
- Browse for the jetPACK.txt file.
- Click upload.
- The browser will refresh automatically after upload.
- You will be redirected to the Dashboard page upon completion.
- The import may take longer for more complex deployments such as Microsoft Lync etc.

## Global Settings

The Global settings section allows you to change various elements, including the SSL cryptographic library.

### App Store Download Proxy



▲ App Store Download Proxy

HTTP Proxy URL:

HTTP Proxy User Name:

HTTP Proxy Password:

Secured networks generally do not allow access to the Internet unless data is sent via the organization's proxy servers. The EdgeADC is a perimeter device and needs to be able to access the Edgenexus servers in order to ascertain validity of support and also to access the App Store to download updates and applications.

#### HTTP Proxy URL

This field is used to specify the hostname or IP address of your proxy server.

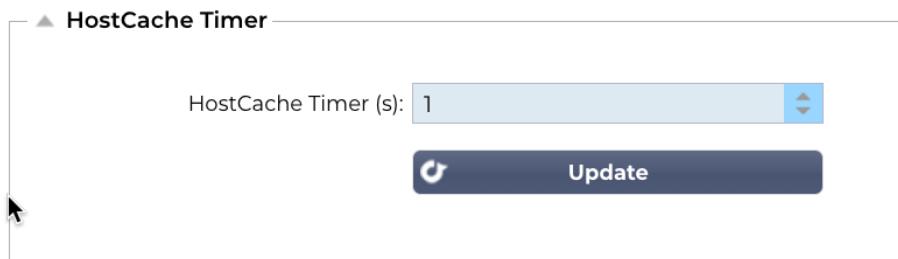
#### HTTP Proxy Username

Enter the username specifically used to authorize devices and users who use the proxy server.

#### HTTP Proxy Password

The username specified in HTTP Proxy Username will be a secured one. You will need to enter the associated password in this field.

### Host Cache Timer



▲ HostCache Timer

HostCache Timer (s):

The Host Cache Timer is a setting that stores the IP Address of a Real Server for a given period 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 prevent the cache from being flushed. There is no max value for this setting.

## Drain

▲ Drain

Default Drain Behaviour: Migrate Visitors ▼

Update

Whenever any Real Server is placed into Drain mode, it is always better to be able to control the behaviour of traffic being sent to it. The Drain Behaviour menu allows the selection of traffic behaviour on a per Virtual Service basis. Options are:

Option	Description
Persistence Driven	This is the default selection. Whenever the user visits using the persistence session, it is extended. With 24-hour usage, it is possible that the drain would never happen. However, if the number of connections to the real server ever reaches 0, drain ends, persistence sessions are deleted, and all visitors get re-balanced on the next connection they make.
Migrate Visitors	Persistent session ignored on re-connect - (legacy behavior before 2022) New TCP connections (whether part of an existing session or not) are always made to an online real server. If the persistence session was to a draining real server, it is overwritten. The Virtual Service will effectively ignore persistence on any new connections, and they will be load balanced to a new server.
Retire Sessions	Persistent sessions are not extended. Incoming user connections will be allocated to their desired server, but their persistence session is not extended. So, after the persistence session time is exceeded, they will be treated as a new connection and moved to a different server.

## SSL

▲ SSL

SSL Cryptographic Library: Open SSL ▼

Update

This global setting allows the SSL library to be changed as needed. The default SSL Cryptographic Library used by the ADC is from OpenSSL. If you wanted to use a different crypto library, this could be changed here.

## Authentication

▲ **Authentication**

Authentication Server Timeout (s):

**Update**

This value sets the timeout value for authentication, after which the authentication attempt will have been deemed as failed.

## Failover Setting

▲ **Failover Setting**

VIP Failover Behaviour :

**Update**

When a clustered set of ADCs is created there are now two methods of specifying how a Virtual Service will fail over.

Option	Description
Any Service	When this option is chosen, the failure of any Service within the VIP will cause the entire VIP with its Virtual Services to fail over to the cluster partner. For example, you may have a VIP 10.0.100.101, with Virtual Services each using port 443, 8080, 4399,2020, etc. Should any of these sub-Services fail, the entire VIP will fail over.
All Services	When this option is chosen, should one or more sub-Services fail, the VIP will remain on the current cluster member. The VIP will only fail over to the cluster partner if <b>all</b> the Services fail. This is useful when you wish to disable one particular Service, but not wish the VIP to fail over.

## Protocol

The Protocol section is used to set the many advanced settings for the HTTP protocol.

### Server too Busy

Suppose you have limited the Max Connections to your Real Servers; you can choose to present a friendly web page once this limit has been reached.

- Create a simple web page with your message. You may include external links to objects on another web servers and sites. Alternatively, if you want to have images on your web page, then use inline base64 encoded images.
- Browse for your newly created web page HTM(L) file.
- Click Upload
- If you wish to preview the page, you can do so with the Click Here link.

### 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

Option	Description
Off	ADC does not alter the Forwarded-For header.
Add Address and Port	This choice will append the IP address and port, of the device or client connected to the ADC, to the Forwarded-For header.
Add Address	This choice will append the IP address, of the device or client connected to the ADC, to the Forwarded-For header.
Replace Address and Port	This choice will replace the value of the Forwarded-For header with the IP address and port of the device or client connected to the ADC.
Replace Address	This choice will replace the value of the Forwarded-For header with the IP address of the device or client connected to ADC.

### Forwarded-For Header

This field allows you to specify the name given to the Forwarded-For header. Typically, this is “X-Forwarded-For” but may be changed for some 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.

Select Default from the Source Type list from the Category list, select Request Header In the Source Name box, and type X-Forwarded-For.

HTTP://www.iis.net/learn/extensions/advanced-logging-module/advanced-logging-for-iis-custom-logging

## Apache HTTPd.conf changes

You will want to make several changes to the default format to log the X-Forwarded-For client IP address or the actual client IP address if the X-Forwarded-For header does not exist.

Those changes are below:

Type	Value
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 environmental variables.

- Line 1 is the standard combined log formatted string from the default.
- Line 2 replaces the %h (remote host) field with the value(s) pulled from the X-Forwarded-For header and set the name of this log file pattern to "proxy".
- Line 3 is a setting for the environment variable "forwarded" that contains a loose regular expression matching an IP address, which is ok in this case since we care more whether an IP address exists in the X-Forwarded-For header.
- Also, 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 an X-Forwarded-For value exists, use the "proxy" pattern, else use the "combined" pattern for the request. For readability, lines 4 and 5 do not take advantage of Apache's rotate logs (piped) logging feature, but we assume that almost everyone uses it.

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

## HTTP Compression Settings

▲ HTTP Compression Settings

Initial Thread Memory [KB]:

Maximum Thread Memory [KB]:

Increment Memory [KB]:    
(0 to double)

Minimum Compression Size [Bytes]:

Safe Mode:

Disable Compression:

Compress As You Go:

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 ADC**

Option	Description
Initial Thread Memory [KB]	This value is the amount of memory each request received by ADC 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 value is the maximum amount of memory that the ADC will allocate on one request. For maximum performance, ADC normally stores and compresses all content in memory. IF an exceptionally large content file exceeding this amount is processed, ADC will write to disk and compress the data there.
Increment Memory [KB]	This value sets the amount of memory added to the Initial Thread Memory Allocation when more is required. The default setting is zero. This means ADC 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 significant 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 value is the size, in bytes, under which the ADC 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 ADC from applying compression to style sheets of JavaScript. The reason for this is that even though ADC 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 ADC 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

Any pages with the added extension in the exclusion list will not be compressed.

- Type in the individual file name.

- Click update.
- If you wish to add a file type, simply type “.css” for all cascading style sheets to be excluded.
- Each file or file type should be added to a new line.

## Persistence Cookies

▲ Persistence Cookies

Same Site Cookie Attribute: None

Secure:

Http Only:

↻ Update

This setting allows you to specify how Persistence Cookies are handled.

Field	Description
Same Site Cooke Attribute	<p><b>None:</b> All cookies are accessible to scripts</p> <p><b>Lax:</b> Prevents cookies being accessed across sites, but they are stored to become accessible and submitted to the owning site if it is visited</p> <p><b>Strict:</b> prevents any cookie for a different site from being accessed or stored</p> <p><b>Off:</b> returns to the browser’s default behavior</p>
Secure	This checkbox, when checked, applies the persistence to secure traffic
HTTP Only	When checked, this allows Persistent Cookies only on HTTP traffic

## UDP Timeout Reset

▲ UDP Timeout Reset

UDP Timeout Reset On: Both

↻ Update

UDP Timeout Reset is a mechanism used in network communications where the timeout relating to a UDP (User Datagram Protocol) session is restarted. The reset helps maintain the session as active, ensuring continuous data flow without interruption.

Option	Description
Both	Resets the UDP timeout on both server and client.
Server	Resets the UDP timeout on the server.
Client	Resets the UDP timeout on the client.



## Software

The Software section allows you to update the configuration and the firmware of your ADC.

### Software Upgrade Details

**Software Details**

User Name: admin	Location: Manchester, United Kingdom
Machine ID: FF-3F3	Support Expiry: None
Licence ID: (B090-EBD6A1)	Support Type: NFR
Licence Expiry: Permanent	Current Software Version: 4.3.0 (Build 1965) c50631

[Refresh To View Available Software](#)

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

We have successfully connected to Cloud Services Manager to retrieve your Software Update Details

The section Download from Cloud shown below will be populated with information showing updates available to you under your support plan. You should pay attention to the support Type and Support Expiry date.

*Note: We use your browser's internet connection to view what is available from the Edgenexus Cloud. You will only be able to download software updates if the ADC has an internet connection.*

To check this:

- Advanced--Troubleshooting--Ping
- IP Address – App Store.edgenexus.io
- Click Ping
- If the result shows "ping: unknown host App Store.edgenexus.io."
- The ADC will NOT be able to download anything from the cloud

### Download from Cloud

Code Name	Release Date	Version	Build	Release Notes	Notes
ALB-X Version 4.2.6	2020-Apr-15	4.2.6	1926	<a href="#">Click here</a> for release notes. This is our latest release 4.2.6. This APP will only w	
ALB-X Version 4.2.4 Safe Rollback	2022-Aug-05	4.2.4	1918XUS	Use this safe 1764 roll-back, not to use this safe 1764 roll-back, not software stored in	
OWASP Core Rule Set 3.1.4 Update for Edgenexus Ap	2023-Feb-09	3.1.4_20.01.2023	Edgenexus	The OWASP CRS is a set of web a The OWASP CRS is a set of web application firewa	
ADC Version 4.2.10 Software Update	2023-Oct-27	4.2.10	1961	<a href="#">Release notes</a>	EdgeADC version 4.2.10 software update <a href="#">Offline F</a>

[Download Selected Software](#)

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

- Highlight the row you are interested in and click the “Download Selected Software to ALB.” button
- The selected software will download to your ALB when clicked, which can be applied in the “Apply Software Stored on ALB” section below.

Note: If the ADC does not have direct internet access, you will receive an error like the below:

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

If your network is protected by a proxy server, please see App Store Download Proxy.

## Upload Software

▲ Upload Software

Software Version: 4.3.0 (Build 1965) c50631

Browse for software file then click upload to apply.

## Apps Upload

▲ Upload Software

Software Version: 4.3.0 (Build 1965) c50631

Browse for software file then click upload to apply.

If you have an App file which ends with <appname>.<apptype>.alb you can use this method 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 that section individually.

## Software/Firmware Updates

▲ Upload Software To ALB

Software Version: 4.2.6 (Build 1831) 3j1329

Browse for software file then click upload to apply.



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

## Apply Software stored on ADC

▲ Apply Software

Image	Code Name	Release Date	Version	Build	Notes
	jetNEXUS ALB v4.2.7	2021-04-28	4.2.7	(Build1890)	build1890-7054-v4.2.7-Sprint2-update-64
	jetNEXUS ALB v4.2.7	2021-03-30	4.2.7	(Build1889)	build1889-6977-v4.2.7-Sprint2-update-64
	jetNEXUS ALB v4.2.6	2020-09-03	4.2.6	(Build1860)	build1860-6247-v4.2.6-Sprint2-update-64

This section will show all Software files stored on the ALB and available for deployment. The listing will include updated Web Application Firewall (WAF) signatures.

- Highlight the Software row you are interested in using.
- Click “Apply Software from Selected”

- If this is an ALB Software Update, please be aware that it will upload and then reboot the ALB to apply.
- If the update you are applying is an OWASP signature update, it will apply automatically without rebooting.

## Troubleshooting

There are always issues that require troubleshooting to come to a root cause and solution. This section allows you to do that.

### Support Files

▲ Support Files

Time Frame: 7 days

Download Support Files

If you have an issue with the ADC and need to open a support ticket, Technical Support will often request several different files from the ADC appliance. These files have now been aggregated into one single .dat file that can be downloaded via this section.

- Select a time frame from the drop-down: A choice of 3, 7, 14, and All days are available to you.
- Click “Download Support Files”
- A file will be downloaded in the format Support-jetNEXUS-yyymmddhh-NAME.dat
- Raise a support ticket on the support portal, details of which are available at the end of this document.
- Make sure you describe the problem thoroughly and attach the .dat file to the ticket.

### Trace

▲ Trace

Nodes To Trace: Your IP

Connections:

Cache:

Data:

Authentication:

flightPATH: No flightPATH trace

Server Monitoring:

Monitoring Unreachable:

Auto-Stop Records: 1000000

Auto-Stop Duration: 00:10:00

Purpose:

Start

Download

Clear

Full results can be obtained using download.

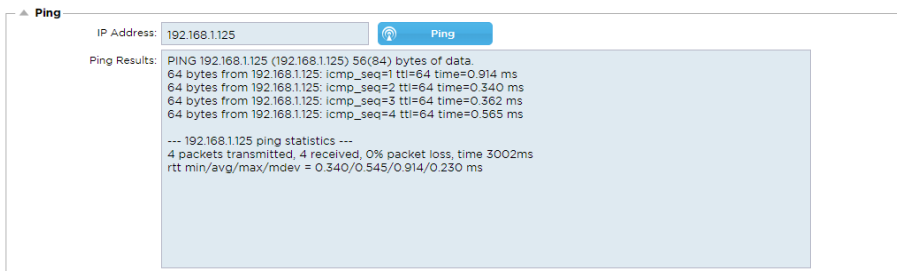
The Trace section will allow you to examine information enabling the debugging of the issue. The information delivered depends on the options you choose from the drop-downs and the tick boxes.

Option	Description
Nodes to Trace	<b>Your IP:</b> 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 ADC interface address) <b>All IP:</b> No filter will be applied. It should be noted that on a busy box this will adversely affect performance.
Connections	This checkbox, when ticked, will show you information about the client and server-side connections.
Cache	This checkbox ticked will show you information with regards to cached objects.

Data	When this checkbox is ticked, it will include the raw data bytes handled in and out by the ADC.
flightPATH	The flightPATH menu allows you to select a particular flightPATH rule to monitor or All flightPATH rules.
Server Monitoring	This checkbox, when ticked, will show the server health monitors active on the ADC and their respective results.
Monitoring Unreachable	When this option is selected, it's very much like Server monitoring in behavior, except it will only show the failed monitors and so acts as 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 setting is a safety precaution to prevent Trace from accidentally being left on and affecting your ADC performance.
Auto-Stop Duration	The default time is set to 10 minutes, after which the Trace facility will automatically stop. This feature is a safety precaution to prevent Trace from accidentally being left on and affecting the performance of the ADC.
Start	Click this to Start the Trace facility manually.
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. Instead, you can download the Trace.log to view all the information gathered during the various traces that day. This feature is a filtered list of trace information. If you wish to view previous days' trace information, you can download Syslog for that day but will have to filter manually.
Clear	Clears the trace log

## Ping

You can check for network connectivity to servers and other network objects in your infrastructure using the Ping tool.



Type in the host's IP address 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 to feedback once you have pressed the “Ping” button.

If you have configured a DNS server, then you can type in the fully qualified domain name. You can configure a DNS server in the [DNS SERVER 1 & DNS SERVER 2](#) section. You may have to wait a few seconds for the result to feedback once you have pressed the “Ping” button.

## Capture


▲ Capture

Adapter:  ▼

Packets:  ▲▼

Duration[Sec]:  ▲▼

Address:  🏠

 Generate

To capture network traffic, follow the simple instructions below.

- Complete the options in the form
- Click Generate
- Once the capture has run, your browser will pop up and ask you where you wish to save the file. It will be in the format “jetNEXUS.cap.gz”
- Raise a support ticket on the support portal, details of which are available at the end of this document.
- Make sure you describe the problem thoroughly and attach the file to the ticket.
- You can also view the contents using Wireshark

Option	Description
Adapter	Choose your adapter from the drop-down, typically eth0 or eth1. You can also capture all interfaces with “any”
Packets	This value is the maximum number 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 value 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 needed, we can increase this figure.

Note: This will have an impact on the performance of live sites. To increase the available capture size, please apply a global setting jetPACK to increase the capture size.


# Help

The Help section provides access to the information on Edgenexus and access to the user guides and other helpful information.

## About us

Clicking on the About Us option will display information on Edgenexus and its corporate office.

**About Us**



**Edgenexus ADC(TM)**  
4.3.0 (Build 1965) c50631  
Copyright © 2005-2020 Edgenexus Limited. All Rights Reserved.










Edgenexus Limited,  
Jubilee House,  
Third Avenue,  
Marlow  
SL7 1YW

[www.edgenexus.io/support/](http://www.edgenexus.io/support/)

Some elements of the SSL subsystem are open source.

## Reference

The reference option will open the webpage containing user guides and other helpful documents. The webpage can also be found using <https://www.edgenexus.io/documentation>.

 <b>EN</b> English WEB PDF	 <b>FR</b> French WEB PDF	 <b>DE</b> German WEB PDF
 <b>ES</b> Spanish WEB PDF	 <b>BP</b> Portugese WEB PDF	 <b>JP</b> Japanese WEB PDF
 <b>CN</b> Chinese WEB PDF	 <b>RU</b> Russian WEB PDF	 <b>IT</b> Italian WEB PDF

If you do not find what you are looking for, please contact [support@edgenexus.io](mailto:support@edgenexus.io).

# JetPACKs



## Edgenexus jetPACKs

jetPACKs are a unique method of instantly configuring your ADC for specific applications. These easy-to-use templates come pre-configured and fully tuned with all application-specific settings that you need to enjoy optimized service delivery from your ADC. Some of the jetPACKs use flightPATH to manipulate the traffic, and you must have a flightPATH license for this element to work. To find out if you have a license for flightPATH, please refer to the [LICENSE](#) page.

### Downloading a jetPACK

- Each jetPACK below has been created with a unique Virtual IP address 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 Virtual IP address.
- In addition, each jetPACK has been created with 2 Real Servers with IP addresses of 127.1.1.1 and 127.2.2.2. Again you can change these in the GUI after upload or beforehand using Notepad++.
- 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	<a href="#">jetPACK-1.1.1.1-Exchange-2010</a>	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 is an option. If you don't have a license for flightPATH, this jetPACK will still work.	Global settings: Service timeout 2 hours Monitors: Layer 7 monitor for the Outlook web app, and 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
	<a href="#">jetPACK-1.1.1.2-Exchange-2010-SMTP-RP</a>	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 the 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
	<a href="#">jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR</a>	Same as above, except this jetPACK will configure the SMTP service to use Direct Server Return connectivity. This jetPACK is needed if your SMTP server needs to see the actual IP address of the client.	Global settings: Service timeout 2 hours Monitors: Layer 7 monitor for the 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	<a href="#">jetPACK-2.2.2.1-Exchange-2013-Low-Resource</a>	This setup adds 1 VIP and two services for HTTP and HTTPS traffic and requires the least CPU. It is possible to add multiple health checks to the VIP 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
	<a href="#">jetPACK-2.2.3.1-Exchange-2013-Med-Resource</a>	This setup uses a unique IP address for each service and therefore uses more resources than above. You must configure each service as an individual DNS entry Example owa.edgenexus.com, ews.edgenexus.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
	<a href="#">jetPACK-2.2.2.3-Exchange2013-High-Resource</a>	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 jetPACK 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	Front End	Edge Internal	Edge External
<a href="#">jetPACK-3.3.3.1-Lync-Reverse-Proxy</a>	<a href="#">jetPACK-3.3.3.2-Lync-Front -End</a>	<a href="#">jetPACK-3.3.3.3-Lync-Edge-Internal</a>	<a href="#">jetPACK-3.3.3.4-Lync-Edge-External</a>

## Web Services

Normal HTTP	SSL Offload	SSL Re-Encryption	SSL Passthrough
<a href="#">jetPACK-4.4.4.1-Web-HTTP</a>	<a href="#">jetPACK-4.4.4.2-Web-SSL-Offload</a>	<a href="#">jetPACK-4.4.4.3-Web-SSL-Re-Encryption</a>	<a href="#">jetPACK-4.4.4.4-Web-SSL-Passthrough</a>

## Microsoft Remote Desktop

### Normal

[jetPACK-5.5.5.1-Remote-Desktop](#)

## DICOM – Digital Imaging and Communication in Medicine

### Normal HTTP

[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 your 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 setting will increase that request to 1 day
- ARP Refresh 10 – during a failover between HA appliances, this setting 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 value will increase the size to a maximum of 16MB

## Ciphers and Cipher jetPACKs

The EdgeADC has best practice Ciphers included as standard. These Ciphers are coupled with their respective TLS protocols, making it easier for users.

We have provided a set of additional Ciphers for you to use should you require them.

### Strong Ciphers

Adds the ability to choose “Strong Ciphers” from the Cipher options list:

```
ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5
```

### Anti-Beast

Adds the ability to choose “Anti Beast” from the Cipher Options list:

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
```

### No SSLv3

Adds the ability to choose “No SSLv3” from the Cipher Options list:

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
```

### No SSLv3 no TLSv1 No RC4

Adds the ability to choose “No-TLSv1 No-SSLv3 No-RC4” from the Cipher Options list:

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
```

### NO\_TLSv1.1

Adds the ability to choose “NO\_TLSv1.1” from the Cipher Options list:

```
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
```

## Enable TLS-1.0-1.1 Ciphers

In build 4.2.10 onwards, Cipher support for protocols TLS1.0 and TLS 1.1 has been deprecated. However, some customers continue to use these older, legacy protocols for their internal servers. The Cipher below adds the ability to enable TLS v1.0 and TLS v1.1.

```
AES128-SHA:AES256-SHA:DES-CBC-SHA:DES-CBC3-SHA:EXP-DES-CBC-SHA:RC4-SHA:RC4-MD5:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-SHA256:AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
```

## Example Cipher jetPACK

Ciphers are imported into the ADC using jetPACKs. A jetPACK is a simple text file that contains parameters that the ADC will recognize. The example below shows a jetPACK using the Enable TLS-1.0-1.1 Cipher.

```
#!update
[[jetnexusdaemon-cipher-TLS1-0-TLS-1-1]
Cipher="AES128-SHA:AES256-SHA:DES-CBC-SHA:DES-CBC3-SHA:EXP-DES-CBC-SHA:RC4-SHA:RC4-MD5:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-SHA256:AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM"
Cipher1=""
Cipher2=""
CipherOptions="-NO_TLSv1.0 -NO_TLSv1.1 -NO_TLSv1.2 -NO_TLSv1"
Description=" TLS v1.0 - v1.1 Enabled"
```

- [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

## Applying a jetPACK

You can apply any jetPACK in any order but be careful not to use a jetPACK with the same Virtual IP address. This action 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](#)

## Creating a jetPACK

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

- Start by copying the current configuration from your existing ALB-X
  - Advanced
  - Update Software
  - Download Current Configuration
- Edit this file with Notepad++
- Open 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 line needs to be at the top of the jetPACK, or your current configuration will be overwritten.

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

```
ContentServerCustomTimer=20000
```

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

```
jnCookieHeader="MS-WSMAN"
```

This example 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 typically 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"
```

```
Uri="HTTP://demo.jetneus.com/healthcheck/healthcheck.html"
```

### Section 3:

```
[jetnexusdaemon-LocalInterface]
```

This section contains all the details in the IP Services section. Each interface is numbered and includes sub-interfaces for each channel. If your channel has a flightPATH rule applied, then it will also contain a Path section.

*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 the flightPATH rules. The numbers must match what has been applied to the interface. In the example above, we see that flightPATH rule “6” has been applied to the channel, including 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=
```

# flightPATH



## Introduction to flightPATH

### What is flightPATH?

flightPATH is an intelligent rules engine developed by Edgenexus to 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 Layer 7 Service Type equal to HTTP(s). If you choose any other service type, then the flightPATH tab in IP Services will be blank.

### 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” and “Ends With” for example, complete control using powerful Perl-compatible Regular Expressions (RegEx) can be implemented.

For more on RegEx, please see this helpful site <https://www.regexbuddy.com/regex.html>

In addition, custom variables can be created in the Evaluation section, and used in the Action area enabling many different possibilities.

A flightPATH rule has three components:

Option	Description
Details	Used for adding or removing a flightPATH and listing available ones
Condition	Set multiple criteria to trigger the flightPATH rule.
Evaluation	Allows the use of variables that can be used in the Action area.
Action	The behavior once the rule has triggered.

### Condition

Within this section you can specify five individual parameters that apply to a Condition. These are outlined below with a description of each option and an example.

Condition	Description	Example
<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=edgeNEXUS” 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

## Match

The Match parameter is context sensitive depending on the value of the Condition parameter.

Match	Description	Example
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 QWxhZGRpbjpvGVuIHNlc2FtZQ==
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 the 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	The Implementation-specific headers 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

## Check

Check	Description	Example
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.edgenexus.io
Have Length	The string does have length of the value	Host > Does > Have Length > 16 www.edgenexus.io = TRUE www.edgenexus.com = FALSE
Exceed Length	Check that the value does/doesn't exceed specified length.	Path > Does > Exceed Length - 10
Match RegEx	This enables you to enter a full Perl compatible regular expression	Origin IP > Does > Match Regex > 10\.*   11\.*

Match List	Allows the provision of a PIPE (   ) delimited list of values you can check against.	Source IP > Does > Match List > 10.0.0.1   10.0.0.100   192.178.28.32
------------	--	---

## Example

Condition				
Condition	Match	Sense	Check	Value
Request Header		Does	Contain	image
Host		Does	Equal	www.imagepool.com

- The example 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

Evaluation			
Variable	Source	Detail	Value
\$variable1\$	Select a New Source	Select or Type a New Detail	Type a New Value

Adding a Variable is a compelling feature that will allow you to extract data from the request and utilize it 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. For example \$variable1\$
- 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
  - Method = \$method\$
  - Path = \$path\$
  - Querystring = \$querystring\$
  - Sourceip = \$sourceip\$
  - Response code (text also included “200 OK”) = \$resp\$
  - Host = \$host\$
  - Version = \$version\$
  - Clientport = \$clientport\$
  - Clientip = \$clientip\$
  - Geolocation = \$geolocation\$”

### Example Action:

- Action = Redirect 302
  - Target = HTTPs://\$host\$/404.html
- Action = Log
  - 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 browser's 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"

Source	Description	Example
Cookie	This is the name and value of the cookie header	MS-WSMAN=afYfn1CDqgCDqUD::Where the name is MS-WSMAN and the value is afYfn1CDqgCDqUD::
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

Detail	Description	Example
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 QWxhZGRpbjpvGVuIHNIc2FtZQ==
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		
Action	Target	Data
Authentication	Form login	

### 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

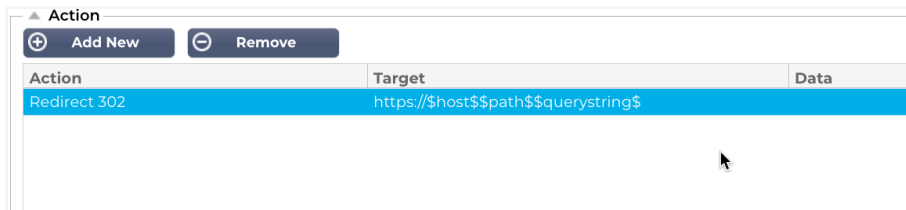
Double click on the Data column to manually add your data that you wish to add or replace.

The list of all the actions are detailed below:

Action	Description	Example
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

---

### 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\$

### 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\$

### 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 =

### 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\$

### 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\$

### 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\$

### 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\$

### 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://

### 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

### 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

### 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

### 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\$/

### 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\$

### 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>

### 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

# SAML and Entra ID

# Setting up the Entra ID Authentication Application in Microsoft Entra

In order for SAML authentication to operate successfully, you will need to set up an Enterprise Application within your Microsoft Entra Admin portal. This is a simple task and allows for the provisioning of the signing certificate needed for SAML authentication requests and tokens, as well as the configuration XML data.

To do this, you should first log into your Microsoft Entra Portal (<https://portal.azure.com>) and make sure you are on the Azure Services page where you will find a list of icons at the top of the page (see below).

## Azure services



- Click on Enterprise Applications. If you cannot see Enterprise Applications in the icon list, you can enter the name in the Search bar at the top. You will see a page as shown below.

[Home](#) > [Enterprise applications](#)

**Enterprise applications** | All applications ...

edgeNEXUS Limited

+ New application Refresh Download (Export) Preview info Columns Preview features Got feedback?

Overview

Manage

All applications

Private Network connectors

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in [application registrations](#).

Search by application name or object ID

Application type == Enterprise Applications X Application ID starts with X Add filters

Click on [New Application](#)

In the next page, click on [Create your own application](#).

[Home](#) > [Enterprise applications](#) | [All applications](#) >

## Browse Microsoft Entra Gallery

+ Create your own application | Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. Users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra described in [this article](#).

- A section will open up on the right side of the page titled, [Create your own application](#).

## Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Microsoft Entra ID (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)



- Provide a name for your application, say, "My Entra ID Auth App". You can choose whatever name you wish.
- Click on the *Integrate any other application you don't find in the gallery (Non-gallery)* radio button option.
- Click the *Create* button.

You will now be presented with a page that looks like the one below.

- Click on the Single Sign-on option located in the left navigation bar.
- Select the SAML box

Select a single sign-on method [Help me decide](#)

- You will now see a page containing the section for Basic SAML Configuration.

Field	Requirement
Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

- In the Basic SAML Configuration area fill out:
  - Identifier (Entity ID)
  - Reply URL (Assertion Consumer Service URL)
  - Sign-on URL
  - Logout URL (optional)

- Save your configuration and test the App.

For more detailed guidance, you can refer to the [Enable single sign-on for an enterprise application](#) documentation on the Microsoft site.

## Technical Support

---

We provide technical support for all our users per the company's standard terms of service.

We will provide technical support if you have an active Support and Maintenance contract for the EdgeADC, EdgeWAF, or EdgeGSLB.

To raise a support ticket, please visit:

<https://www.edgenexus.io/support/>