TEMENOS TRANSACT (T24)

AN EDGENEXUS ADC DEPLOYMENT GUIDE

EDGENEXUS

Contents

Document Properties

Document Number: 2.0.12.17.21.14.12

Document Creation Date: December 16, 2021

Document Last Edited: December 17, 2021

Document Author: Jay Savoor

Document Last Edited by:

Document Referral: EdgeADC - Version All

Document Disclaimer

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

Copyrights

Trademarks

Edgenexus Support

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

Introduction

This EdgeADC (ADC) application deployment guide is intended for persons administering the Temenos Transact (T24) Core Banking application and its load balancing. This document contains general suggestions and guidance, which may or may not be relevant for use within your organization.

What is Temenos Transact (aka T24)?

Previously known as Temenos T24, the newly rebranded Temenos Transact is probably the most successful and widely used digital core-banking solution worldwide. Used by over 1000 banks in almost all countries globally, Temenos Transact delivers a wide range of banking functionality aimed at market segments including, but not limited to retail, corporate, payments, and more.

Recommendations for load balancing Temenos Transact

We recommend the following:

The ADC is deployed as a pair of appliances in either a virtualization technology, installing it as a virtualized appliance or as a hardware appliance in approved server hardware.

When external users access the network via the Internet, we recommend that the ADC pair is deployed in the DMZ and the traffic rerouted through the firewall to the LAN zone.

The ADC's operate in a high-availability (HA) mode when placed in pairs and provide you the level of redundancy and resilience required for mission-critical systems.

The ADC is fully capable of load-balancing your Temenos Transact (T24) system, and this guide explains how to set this up.

Prerequisites for supporting Temenos Transact (T24)

As usual, it is assumed that the person installing and configuring the ADC is familiar with the terminology used within this document and networking in general. We strongly suggest that both the network technician and Temenos Transact (T24) administrator work in tandem when setting up the load balancing and that this is first done for a sandbox environment before replicating to the production environment.

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

- The latest ADC firmware should be used
- The Temenos Transact (T24) system should be installed and operational.
- The initial ADC configuration should be done against the Temenos Transact (T24) sandbox deployment.
- DNS entries for both internal and external access should be configured and working.
- The ADC should be reachable using a web browser and the management IP.

Acronyms used

VIP – Virtual IP	VS – Virtual Service
RS – Real Server	RSIP – Real Server IP

ADC – Edgenexus EdgeADC

VIPs, Ports, and Other Bits

When load balancing Temenos Transact (T24), the following VIPs will be needed for operations.

Port	Protocol	Service Type	Explanation
443	TCP	L4-TCP or L7 HTTPS	This port is used to handle all HTTPS requests from client applications. You can use Layer 4 TCP with SSL Passthrough or Layer 7 with SSL Offload or SSL Bridging.

Sizing the EdgeADC

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

In virtualized environments, we recommend that you set the ADC to 8 vCPU with 16GB RAM, to begin with, and scale up when you need to.

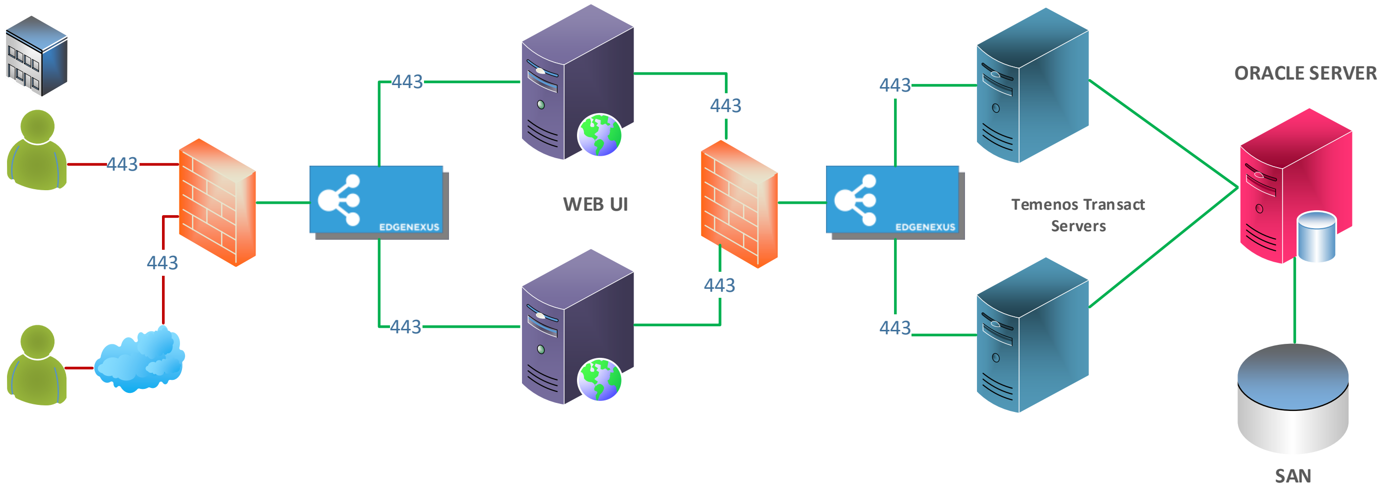
We recommend that you utilize the hardware platforms from our partners in physical environments, with the base system being a quad-core Intel Xeon with 8GB RAM.

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

Deployment Scenarios

Connections to the Temenos Transact (T24) system occur by clients connecting to the VIP or Virtual IP service created on the ADC. The ADC then load-balances the connections to the nodes configured within the ADC and linked to the VIP. An example diagram is shown below.

In the diagram, we show two EdgeADC devices. The dual ADCs are only for representational purposes to indicate traffic flow.



Virtual Service Methods

There are several ways to configure the ADC for use with Temenos Transact (T24), but we recommend using SSL Bridging for security reasons.

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

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

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

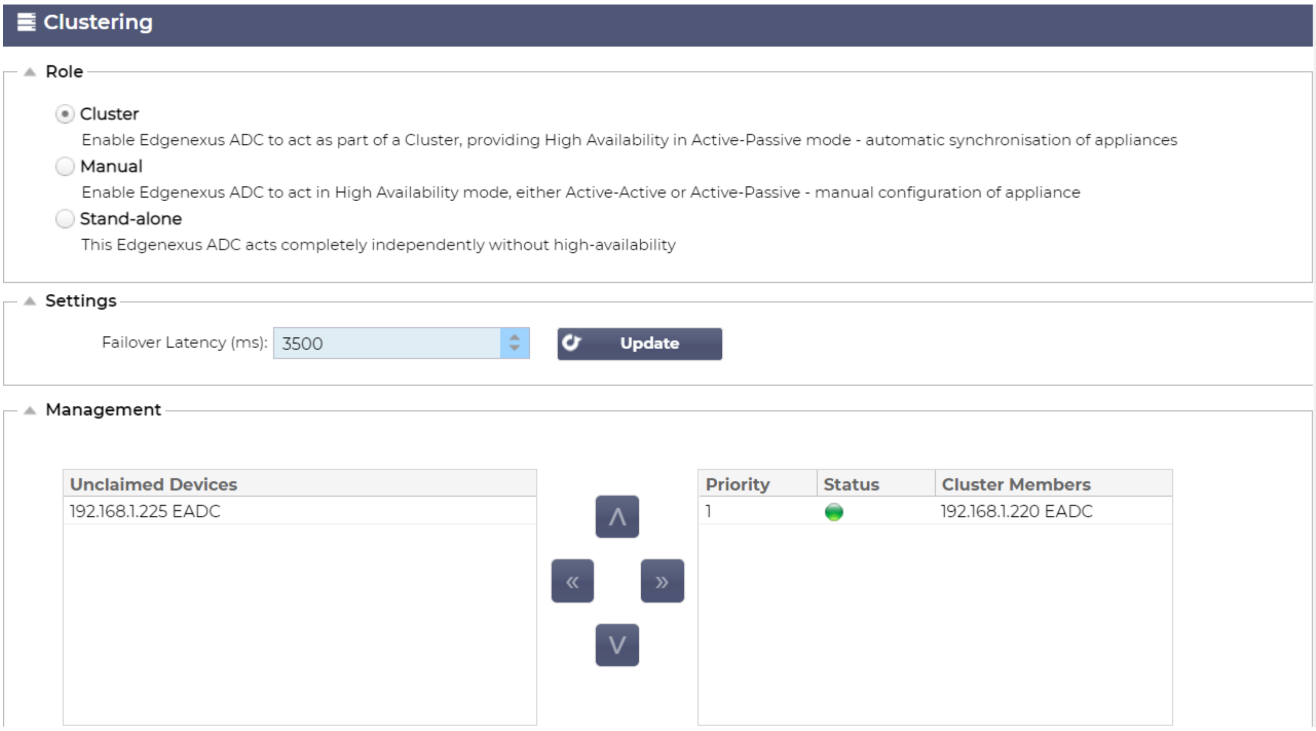
The recommended method(s) are shown highlighted in Green.

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

Clustering the EdgeADC

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

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



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

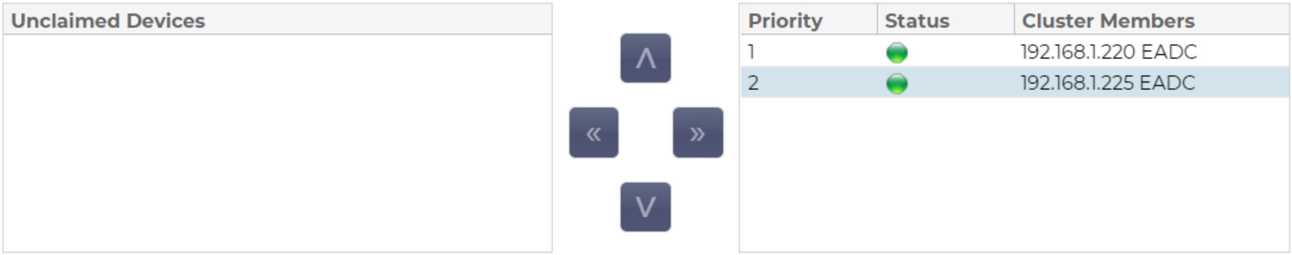
Failover Latency (ms): 3500

Management

Unclaimed Devices
192.168.1.225 EADC

Priority	Status	Cluster Members
1	●	192.168.1.220 EADC

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

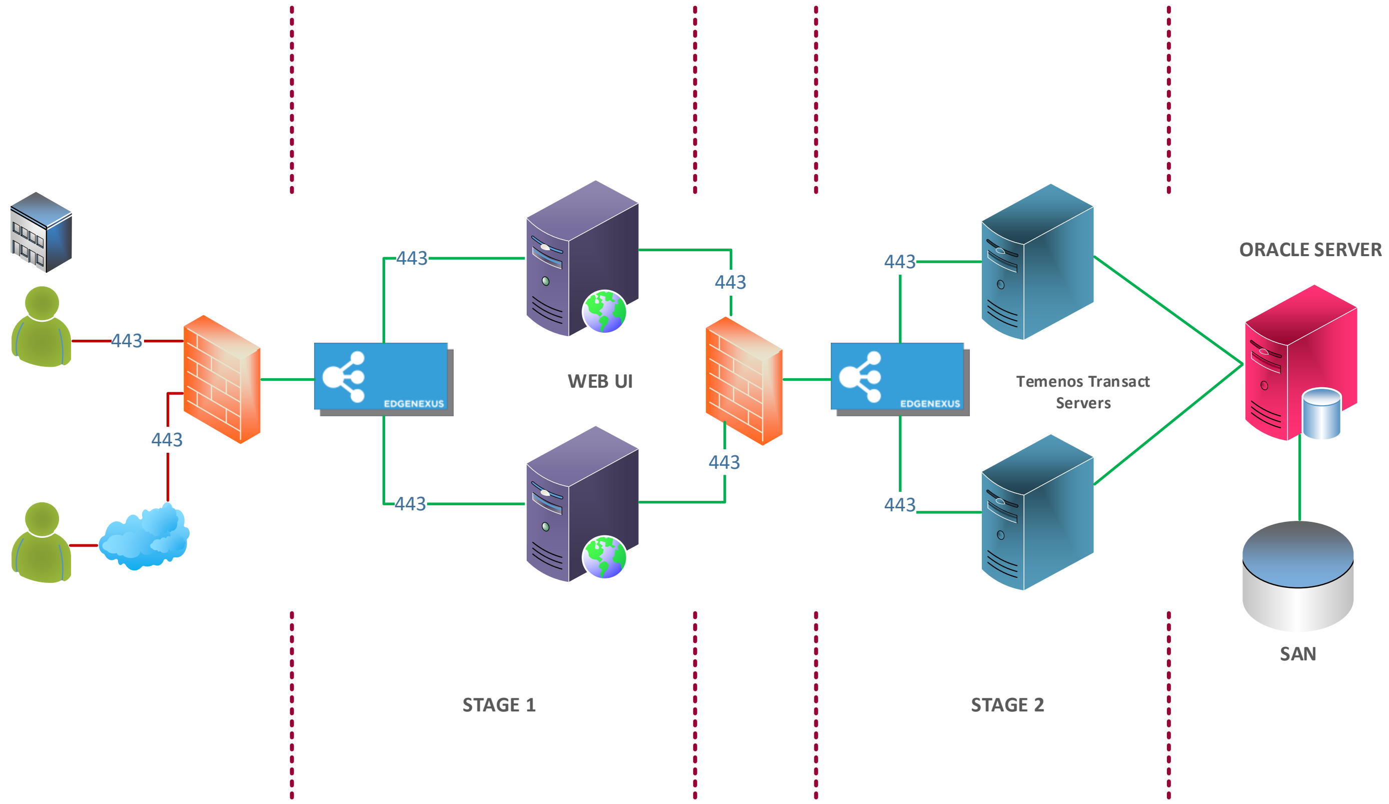


Unclaimed Devices

Priority	Status	Cluster Members
1	●	192.168.1.220 EADC
2	●	192.168.1.225 EADC

Planning the deployment

The load balancing deployment comprises two stages, as shown in the diagram below.



Stage 1 comprises the VIP and Virtual Services for load balancing the WebUI servers. These could be IIS, or as more sometimes used, Apache on Jboss.

Stage 2 of the deployment comprises the load balancing of the Temenos Transact servers. The web servers that would normally be pointed to the Transact servers will now be pointed to the Ingress VIP that handles the Virtual Services serving the Transact servers.

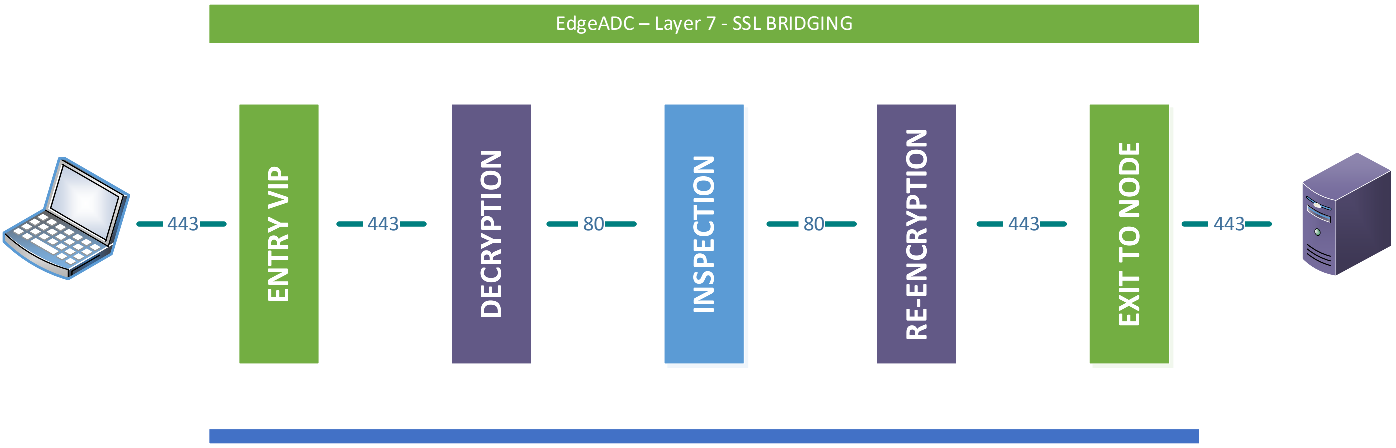
For this exercise, we will be using SSL Re_Encryption as the load balancing method as this gives us a high level of control over the data using flightPATH.

Note: Your Temenos Transact system may differ from the one we have shown, and consequently, you may need to tailor the system accordingly.

Using
SSL Re-Encryption

Stage 1 – WebUI Virtual Services

As mentioned earlier, we will be using SSL Re-Encryption, also known as SSL Bridging. An SSL certificate is required to be present on the ADC. In this method, the SSL traffic enters the ADC, is terminated internally, any inspection required is carried out, and the traffic is then re-encrypted and sent to the nodes.



- The first step is to create the VIP and initial VS
- Log into the ADC and go to IP Services. This location should be the default entry point.
- Click Add Service
- You will see an empty row to add values similar to the one below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.10.222	255.255.255.0	443	Ingress WebUI	HTTP

- Click Update

Now we will define the Real Servers (RS) section.

- The cursor will automatically be taken to a ready-created blank entry to aid you in adding the RS entries.
- Please enter the details relevant to your infrastructure following the examples provided below. In our case, we have three array nodes, but you may have more.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.201	443	100	100	WebUI-1	

- Click Update to save.
- Click the Copy Server button and make changes for the second array node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.202	443	100	100	WebUI-1	

- Click Update to save.

You can add a name for the server group if you wish.

We have now defined our first VIP and two connected WebUI Server nodes. We have some more work yet to do.

Basic Tab

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Persistent Cookie
Server Monitoring	TCP Connect, 200OK (*or your custom monitor)*
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	Any

- Click Update when done.

Note: To add your SSL certificate, please consult the EdgeADC Administration Guide

Advanced Tab

There are no configurations to be done within the Advanced tab.

- Click the Advanced tab within the Real Servers section.
- Make changes as follows:

Field	Value
Connectivity	Reverse Proxy
Cipher Options	Defaults
Client SSL Renegotiation	Checked
Client SSL Resumption	Checked
SNI Default Certificate	None
Security Log	On
Connection Timeout (sec)	600
Monitoring Interval (sec)	10
Monitoring Timeout (sec)	10
Monitoring In Count	2
Monitoring Out Count	3
Switch to Offline on Failure	Unchecked
Max Connections (per RS)	

Creating the HTTP Redirector

If your corporate IT rules dictate that all connections must be secure, you must create a redirector rule. To do this, follow the procedure below:

- Click on the 443 VIP you want redirection to from Port 80
- Now go to the flightPATH tab in the Real Servers section.
- Select Force HTTPS and click the Right-Arrow button in the central cluster.
- The flightPATH rule is now activated, and all traffic entering the VIP on port 80 will be switched to use port 443.

Stage 2 – Transact Server Virtual Services

As before, we will be using SSL Re-Encryption. Again, an SSL certificate is required to be present on the ADC.

- The first step is to create the VIP and initial VS for the Transact servers.
- Log into the ADC and go to IP Services. This location should be the default entry point.
- Click Add Service
- You will see an empty row to add values similar to the one below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.12.222	255.255.255.0	443	Ingress to Transact	HTTP

- Click Update

Now we will define the Real Servers (RS) section.

- The cursor will automatically be taken to a ready-created blank entry to aid you in adding the RS entries.
- Please enter the details relevant to your infrastructure following the examples provided below. In our case, we have three array nodes, but you may have more.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.13.201	443	100	100	Transact-01	

- Click Update to save.
- Click the Copy Server button and make changes for the second array node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.13.202	443	100	100	Transact-02	

- Click Update to save.

You can add a name for the server group if you wish.

We have now defined our first VIP and two connected WebUI Server nodes. We have some more work yet to do.

Basic Tab

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Persistent Cookie
Server Monitoring	TCP Connect, 200OK (*or your custom monitor)*
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	Any

- Click Update when done.

Note: To add your SSL certificate, please consult the EdgeADC Administration Guide

Advanced Tab

There are no configurations to be done within the Advanced tab.

- Click the Advanced tab within the Real Servers section.
- Make changes as follows:

Field	Value
Connectivity	Reverse Proxy
Cipher Options	Defaults
Client SSL Renegotiation	Checked
Client SSL Resumption	Checked
SNI Default Certificate	None
Security Log	On
Connection Timeout (sec)	600
Monitoring Interval (sec)	10
Monitoring Timeout (sec)	10
Monitoring In Count	2
Monitoring Out Count	3
Switch to Offline on Failure	Unchecked
Max Connections (per RS)	

Creating the HTTP Redirector

If your corporate IT rules dictate that all connections must be secure, you must create a redirector rule. To do this, follow the procedure below:

- Click on the 443 VIP you want redirection to from Port 80
- Now go to the flightPATH tab in the Real Servers section.
- Select Force HTTPS and click the Right-Arrow button in the central cluster.
- The flightPATH rule is now activated, and all traffic entering the VIP on port 80 will be switched to use port 443.

Using SSL Passthrough

Stage 1 – WebUI Virtual Services

In this example, we will be using Layer 4 SSL Passthrough, allowing data to pass through the EdgeADC without intervention and therefore does not require the presence of any SSL certificates in the EdgeADC.

- The first step is to create the VIP and initial VS
- Log into the ADC and go to IP Services. This location should be the default entry point.
- Click Add Service
- You will see an empty row to add values similar to the one below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.10.222	255.255.255.0	443	Ingress WebUI	Layer 4 TCP

- Click Update

Now we will define the Real Servers (RS) section.

- The cursor will automatically be taken to a ready-created blank entry to aid you in adding the RS entries.
- Please enter the details relevant to your infrastructure following the examples provided below. In our case, we have three array nodes, but you may have more.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.201	443	100	100	WebUI-1	

- Click Update to save.
- Click the Copy Server button and make changes for the second array node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.202	443	100	100	WebUI-1	

- Click Update to save.

You can add a name for the server group if you wish.

We have now defined our first VIP and two connected WebUI Server nodes. We have some more work yet to do.

Basic Tab

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Persistent Cookie
Server Monitoring	TCP Connect, 200OK (*or your custom monitor)*
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	None
Real Server SSL Cert	None

- Click Update when done.

Note: To add your SSL certificate, please consult the EdgeADC Administration Guide

Advanced Tab

There are no configurations to be done within the Advanced tab.

- Click the Advanced tab within the Real Servers section.
- Make changes as follows:

Field	Value
Connectivity	Reverse Proxy
Cipher Options	Defaults
Client SSL Renegotiation	Checked
Client SSL Resumption	Checked
SNI Default Certificate	None
Security Log	On
Connection Timeout (sec)	600
Monitoring Interval (sec)	10
Monitoring Timeout (sec)	10
Monitoring In Count	2
Monitoring Out Count	3
Switch to Offline on Failure	Unchecked
Max Connections (per RS)	

Creating the HTTP Redirector

If your corporate IT rules dictate that all connections must be secure, you must create a redirector VIP and attach the corresponding flightPATH rule. To do this, follow the procedure below:

- Click on the 443 VIP you want redirection to from Port 80
- Click Copy Service
- Change the Port to **80** and the Service Type from Layer 4 TCP to **HTTP**
- Now go to the flightPATH tab in the Real Servers section.

- Select Force HTTPS and click the Right-Arrow button in the central cluster.
- The flightPATH rule is now activated, and all traffic entering the VIP on port 80 will be switched to use port 443.

Stage 2 – Transact Server Virtual Services

As before, we will be using SSL Re-Encryption. Again, an SSL certificate is required to be present on the ADC.

- The first step is to create the VIP and initial VS for the Transact servers.
- Log into the ADC and go to IP Services. This location should be the default entry point.
- Click Add Service
- You will see an empty row to add values similar to the one below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.12.222	255.255.255.0	443	Ingress to Transact	Layer 4 TCP

- Click Update

Now we will define the Real Servers (RS) section.

- The cursor will automatically be taken to a ready-created blank entry to aid you in adding the RS entries.
- Please enter the details relevant to your infrastructure following the examples provided below. In our case, we have three array nodes, but you may have more.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.13.201	443	100	100	Transact-01	

- Click Update to save.
- Click the Copy Server button and make changes for the second array node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.13.202	443	100	100	Transact-02	

- Click Update to save.

You can add a name for the server group if you wish.

We have now defined our first VIP and two connected WebUI Server nodes. We have some more work yet to do.

Basic Tab

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Persistent Cookie
Server Monitoring	TCP Connect, 200OK *(or your custom monitor)*
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	None
Real Server SSL Cert	None

- Click Update when done.

Note: To add your SSL certificate, please consult the EdgeADC Administration Guide

Advanced Tab

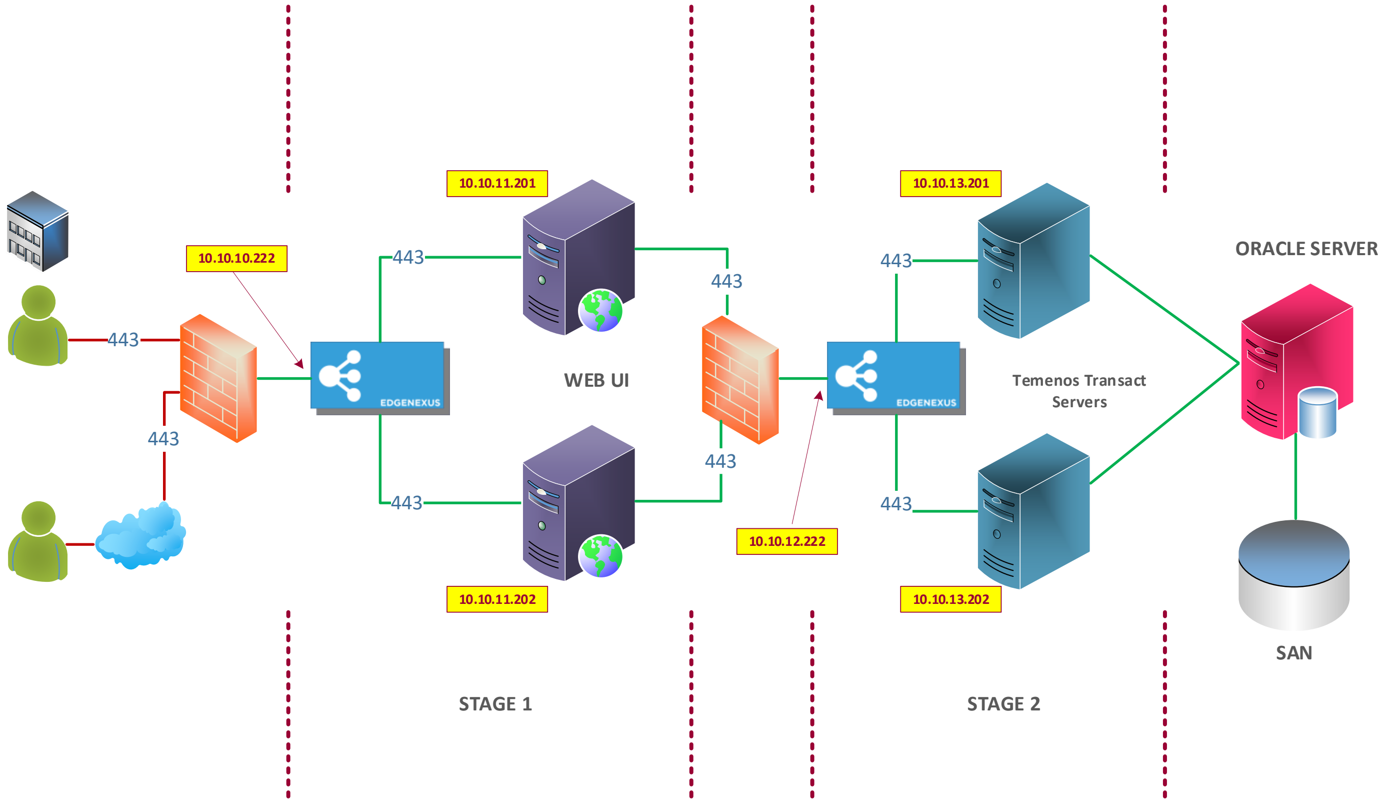
There are no configurations to be done within the Advanced tab.

- Click the Advanced tab within the Real Servers section.
- Make changes as follows:

Field	Value
Connectivity	Reverse Proxy
Cipher Options	Defaults
Client SSL Renegotiation	Checked
Client SSL Resumption	Checked
SNI Default Certificate	None
Security Log	On
Connection Timeout (sec)	600
Monitoring Interval (sec)	10
Monitoring Timeout (sec)	10
Monitoring In Count	2
Monitoring Out Count	3
Switch to Offline on Failure	Unchecked
Max Connections (per RS)	

The Final Configuration

In the diagram below, you can see the final configuration in the network diagram.



An important point to note is that this is only an example. The topology of the servers and port usage may vary due to the highly flexible nature of Temenos Transact.