LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing Microsoft AD FS

Version 1.6.0

Table of Contents

1. About this Guide . . . 4
2. Loadbalancer.org Appliances Supported . . . 4
3. Software Versions Supported . . . 4
   3.1. Loadbalancer.org Appliance . . . 4
   3.2. Microsoft Windows . . . 4
4. Active Directory Federation Services (AD FS) . . . 4
   4.1. Introduction . . . 4
   4.2. AD FS SSO Scenarios . . . 4
      Web SSO . . . 4
      Federated Web SSO . . . 5
   4.3. AD FS Versions . . . 5
   4.4. Role Services . . . 5
   4.5. How AD FS Works . . . 6
      Internal Clients . . . 6
      External Clients . . . 7
      Other Useful References . . . 8
5. Load Balancing AD FS . . . 8
   5.1. Basic Concepts . . . 8
   5.2. Load Balanced Ports & Services . . . 8
   5.3. Persistence (Server Affinity) Requirements & Options . . . 8
   5.4. Server Health checking . . . 9
   5.5. SSL Termination . . . 9
   5.6. Load Balancer Deployment . . . 9
   5.7. Load Balancer Deployment Mode . . . 10
6. Loadbalancer.org Appliance – the Basics . . . 10
   6.1. Virtual Appliance . . . 10
   6.2. Initial Network Configuration . . . 10
   6.3. Accessing the Appliance WebUI . . . 10
      Main Menu Options . . . 12
   6.4. Appliance Software Update . . . 13
      Determining the Current Software Version . . . 13
      Checking for Updates using Online Update . . . 13
      Using Offline Update . . . 13
   6.5. Ports Used by the Appliance . . . 14
   6.6. HA Clustered Pair Configuration . . . 15
7. Server & Appliance Configuration - AD FS 2.0 . . . 15
   7.1. Federation Servers . . . 15
      Federation Server Installation & Configuration . . . 15
      Load Balancer Configuration . . . 15
      DNS Configuration . . . 17
      Testing & Verification . . . 17
   7.2. Federation Proxy Servers . . . 17
      Proxy Server Installation & Configuration . . . 17
      Load Balancer Configuration . . . 17
      DNS Configuration . . . 19
      Testing & Verification . . . 19
8. Server & Appliance Configuration - AD FS 3.0 / 4.0 / 5.0 . . . 19
   8.1. Federation Servers . . . 19

Federation Server Installation & Configuration . . . 19
Load Balancer Configuration . . . 22
DNS Configuration . . . 24
Testing & Verification . . . 24
8.2. Web Application Proxy (WAP) Servers . . . 25
WAP Server Installation & Configuration . . . 25
Load Balancer Configuration . . . 26
DNS Configuration . . . 28
Testing & Verification . . . 29
9. Technical Support . . . 29
10. Further Documentation . . . 29
11. Appendix . . . 30
11.1. Configuring HA - Adding a Secondary Appliance . . . 30
Non-Replicated Settings . . . 30
Configuring the HA Clustered Pair . . . 31
12. Document Revision History . . . 33

1. About this Guide

This guide details the steps required to configure a load balanced Microsoft AD FS environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Microsoft AD FS configuration changes that are required to enable load balancing.

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the Administration Manual.

2. Loadbalancer.org Appliances Supported

All our products can be used with AD FS. For full specifications of available models please refer to https://www.loadbalancer.org/products.

Some features may not be available or fully supported in all cloud platforms due to platform specific limitations. For more details, please refer to the "Main Differences to our Standard (Non-Cloud) Product" section in the appropriate cloud platform Quick Start Guide or check with Loadbalancer.org support.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.9.1 and later

> **Note** The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If you're using an older version, or the very latest, the screenshots presented here may not match your WebUI exactly.

3.2. Microsoft Windows

- Windows 2008 R2 and later (AD FS v2.0+)

4. Active Directory Federation Services (AD FS)

4.1. Introduction

AD FS provides simplified, secured identity federation and Web single sign-on (SSO) capabilities for end users who need access to applications within an AD FS secured enterprise, in federation partner organizations, or in the cloud.

AD FS is a Web Service that authenticates users against Active Directory and provides them access to claims-aware applications. These applications are typically used through the client's web browser. The applications can be on-premises, off-premises, or even hosted by other companies.

4.2. AD FS SSO Scenarios

Web SSO

This is the most common scenario. Here users login to web applications, either off-premises or on-premises, from their browsers using their Active Directory credentials. Examples of such applications include:

- salesforce.com
- servicenow.com
- SharePoint Online (SPO)
- Office 365
- etc.

Federated Web SSO

The following scenarios are examples of Federated SSO. These scenarios aren't as common but they illustrate how AD FS can be used to collaborate with a partner, another company, or another AD forest:

1. You want users from another organization to login to your web applications using their own identity credentials.
2. You want to login to another organization's web applications using your own Active Directory credentials.
3. You want users from another internal Active Directory forest to login to your web applications in your Active Directory using their own AD credentials without a domain and/or forest trust.
4. You want to use your production Active Directory credentials to login to test web applications located in your test Active Directory environment without a domain and/or forest trust.
5. You want users to be able to login to your web applications using their Google, Facebook, Live ID, Yahoo, etc. credentials.

4.3. AD FS Versions

The following table lists the various versions of AD FS and in which Windows version they were initially released:

AD FS Version	Released in Windows Version
v1.0	2003 R2
v1.1	2008
v2.0	2008 R2
v2.1	2012
v3.0	2012 R2
v4.0	2016
V5.0	2019

4.4. Role Services

The following role services can be deployed as part of the AD FS role:

Role Service	Purpose
Federation Server	Acts as an identity provider - *Authenticates users to provide security tokens to applications that trust AD FS* or Acts as a federation provider - *Consumes tokens from other identity providers and then provides security tokens to applications that trust AD FS*
Federation Server Proxy / Web Application Proxy	The Federation Service Proxy functions as an intermediary proxy service between an Internet client and a Federation Server that is located behind a firewall on a corporate network. **Note:** In Windows 2012 R2 and later, the dedicated Proxy role service has been removed. Instead, the proxy is based on WAP (Web Application Proxy).

4.5. How AD FS Works

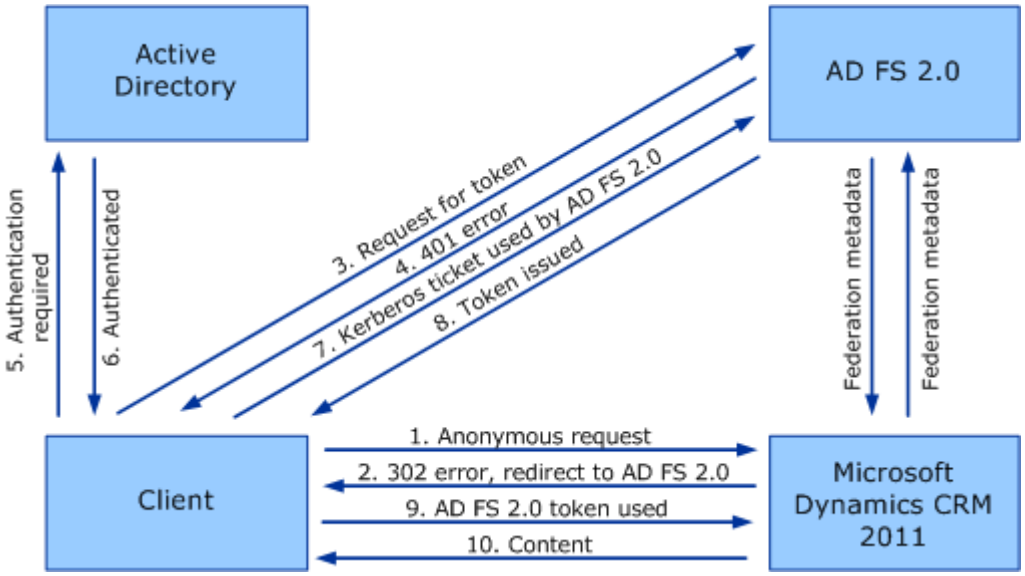
The following sections explain how AD FS authenticates internal LAN based users and external Internet based users.

A Microsoft Dynamics CRM example is used with AD FS v2.0, although the general flow is the same for other applications and different AD FS versions.

> **Note** For a reference of key AD FS concepts, please refer to this URL.

Internal Clients

The authentication process for internal clients is shown below:



1. The client sends a request to access the Microsoft Dynamics CRM website.
2. IIS refuses the connection with an HTTP 302 error message and redirects the user to the trusted claims provider (also known as the STS) for Microsoft Dynamics CRM (AD FS v2.0).
3. The client sends a request for a security token to AD FS v2.0.
4. AD FS 2.0 returns an HTTP 401.1 error, indicating that the client must supply a Kerberos ticket.
5. The client sends a Kerberos authentication request to Active Directory.
6. Active Directory validates the client and sends a Kerberos ticket.
7. The client sends a request for a security token to AD FS v2.0 and includes the Kerberos ticket.

> **Note** If the client already has a valid Kerberos ticket on the network, this ticket is sent to AD FS v2.0 in step 3 and steps 4 through 7 are skipped.

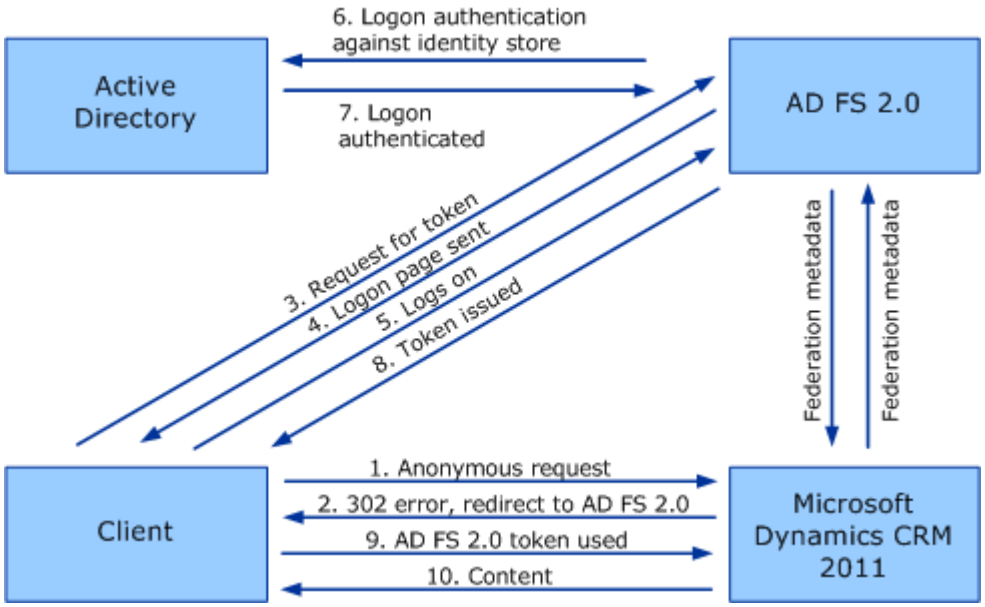
8. AD FS v2.0 provides a security token containing claims for access to Microsoft Dynamics CRM data.
9. The client sends the security token containing claims obtained from AD FS v2.0 to the Microsoft Dynamics CRM server.
10. The Microsoft Dynamics CRM server decrypts and validates the security token and presents the user with the requested information.

> **Note** For more information, please refer to this URL.

External Clients

The flow for external access is largely unchanged from the flow described above for internal access. The major difference is that user authentication does not include a Kerberos ticket.

The authentication process for external clients is shown below:



> **Note** For more information, please refer to this URL.

When an AD FS proxy is used, the client is redirected to the proxy which then connects to the internal AD FS server where authentication occurs. For more details of AD FS proxy, please refer to this URL.

Other Useful References

How To Install AD FS 2016 For Office 365:

https://blogs.technet.microsoft.com/rmilne/2017/04/28/how-to-install-ad-fs-2016-for-office-365/

Setting up AD FS and Enabling Single Sign-On to Office 365:

https://blogs.technet.microsoft.com/canitpro/2015/09/11/step-by-step-setting-up-ad-fs-and-enabling-single-sign-on-to-office-365/

5. Load Balancing AD FS

> **Note** It's highly recommended that you have a working AD FS environment first before implementing the load balancer. The initial environment would normally include a single Federation Server and a single Proxy Server. If the Federation Service Name was set to **adfs.lbtestdom.com** at initial deployment, additional Federation Servers can be added to the same farm, then DNS entries must be changed so that **adfs.lbtestdom.com** points to the VIP on the load balancer rather than the primary Federation Server.

5.1. Basic Concepts

To provide resilience and high availability for your AD FS infrastructure, multiple Federation Servers and multiple Federation Proxy Servers (WAPs in Windows 2012 & later) must be deployed with a load balancer. This helps ensure that users can be authenticated and obtain access to the required systems and applications by constantly checking the health of the AD FS servers and only forwarding client authentication requests to those that are functional.

5.2. Load Balanced Ports & Services

The following table shows the ports that are load balanced:

Port	Protocols	Use
443	TCP/HTTPS	AD FS communications
49443	TCP	Used for certificate authentication in AD FS v3.0 and later

5.3. Persistence (Server Affinity) Requirements & Options

As mentioned here, Microsoft do not recommend using source IP persistence (affinity) For AD FS. However, under certain complex scenarios persistence may be required for the Federation Server VIP.

> **Note** Source IP persistence can easily be enabled by modifying the VIP, setting ***Persistence Mode*** to

Source IP, clicking **Update** and reloading/restarting HAProxy.

5.4. Server Health checking

By default the load balancer uses a TCP port connect to verify the health of back-end servers. For AD FS we recommend that more comprehensive checks are used.

For AD FS v2.0, the load balancer is configured to look for specific content on the AD FS login page: **https://<server IP address>/adfs/ls/idpinitiatedsignon.aspx**

For AD FS v3.0 prior to update rollup KB2975719, the load balancer is configured to use a script to carry out an SNI based health check that looks for specific content on the AD FS login page: **https://<server IP address>/adfs/ls/idpinitiatedsignon.htm**

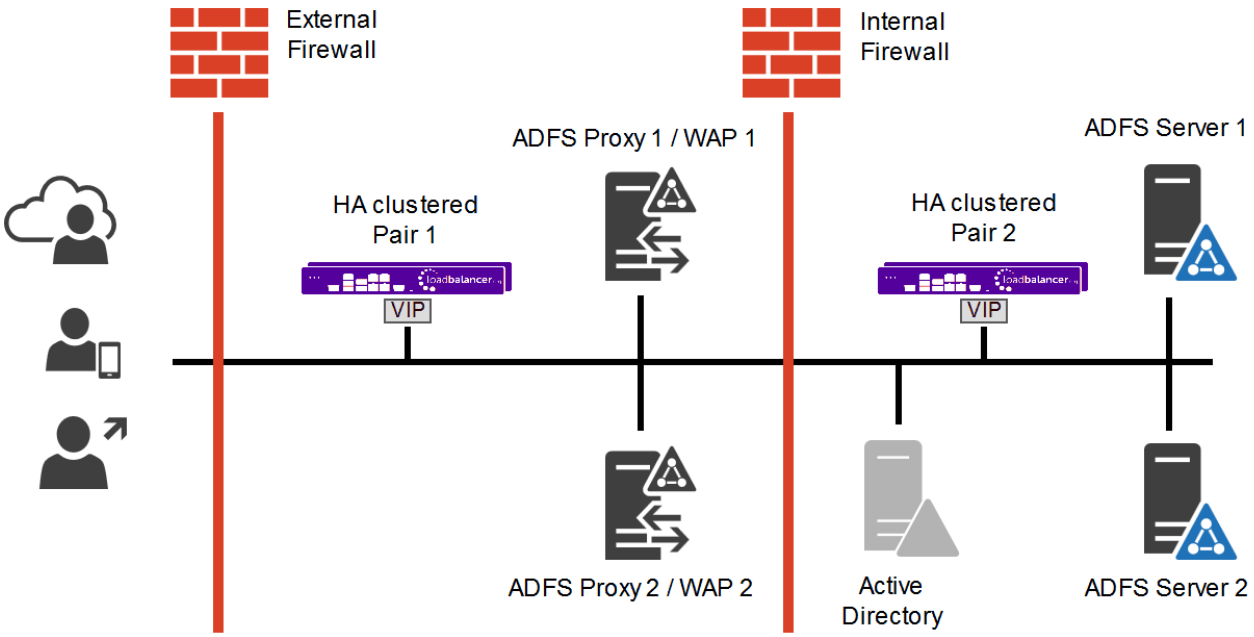
For AD FS v3.0 with update rollup KB2975719 and later, the load balancer is configured to look for a HTTP 200 OK response when the built-in probe URL is read: **http://<server IP address>/adfs/probe**

5.5. SSL Termination

Microsoft state that SSL termination between the Proxy Servers and the Federation Servers is not supported and that SSL Termination between Client and Proxy is only supported under certain situations. For the configurations presented in this guide, SSL is terminated on the Federation & WAP servers and not the load balancer.

5.6. Load Balancer Deployment

The following diagram shows a typical load balanced AD FS deployment.



Note

Load balancers can be deployed as single units or as a clustered pair. Loadbalancer.org always recommend deploying clustered pairs for HA and resilience.

The Federation Proxy servers / WAP servers must be able to access the internal AD FS VIP on port 443 via the "Federation Service Name" specified during installation / configuration. Make

sure that firewalls, routing and DNS are configured to allow this. In this guide, the Federation Service Name used is **adfs.lbtestdom.com**, so an entry for this is added to the local hosts file on each Federation Proxy Server / WAP server which resolves to the AD FS VIP on the internal LAN.

5.7. Load Balancer Deployment Mode

Layer 7 SNAT mode (HAProxy) is recommended for AD FS and is used for the configurations presented in this guide. This mode offers high performance and is simple to configure since it requires no mode-specific configuration changes to the load balanced AD FS Servers.

Layer 4 DR mode, NAT mode and SNAT mode can also be used if preferred. For DR mode you'll need to solve the ARP problem on each AD FS server - for more information please refer to DR Mode Considerations. For NAT mode the default gateway of the AD FS servers must be the load balancer.

6. Loadbalancer.org Appliance – the Basics

6.1. Virtual Appliance

A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM, XEN and Nutanix AHV and has been optimized for each Hypervisor. By default, the VA is allocated 2 vCPUs, 4GB of RAM and has a 20GB virtual disk. The Virtual Appliance can be downloaded here.

Note The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance's WebUI.

Note Please refer to Virtual Appliance Installation and the ReadMe.txt text file included in the VA download for additional information on deploying the VA using the various Hypervisors.

Note The VA has 4 network adapters. For VMware only the first adapter (**eth0**) is connected by default. For HyperV, KVM, XEN and Nutanix AHV all adapters are disconnected by default. Use the network configuration screen within the Hypervisor to connect the required adapters.

6.2. Initial Network Configuration

After boot up, follow the instructions on the appliance console to configure the management IP address, subnet mask, default gateway, DNS servers and other network and administrative settings.

Important Be sure to set a secure password for the load balancer, when prompted during the setup routine.

6.3. Accessing the Appliance WebUI

The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to External Authentication.

> **Note** There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant Quick Start / Configuration Guide.

1. Using a browser, navigate to the following URL:

   https://<IP-address-configured-during-the-network-setup-wizard>:9443/lbadmin/

   > **Note** You'll receive a warning about the WebUI's SSL certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more information, please refer to Appliance Security Features.

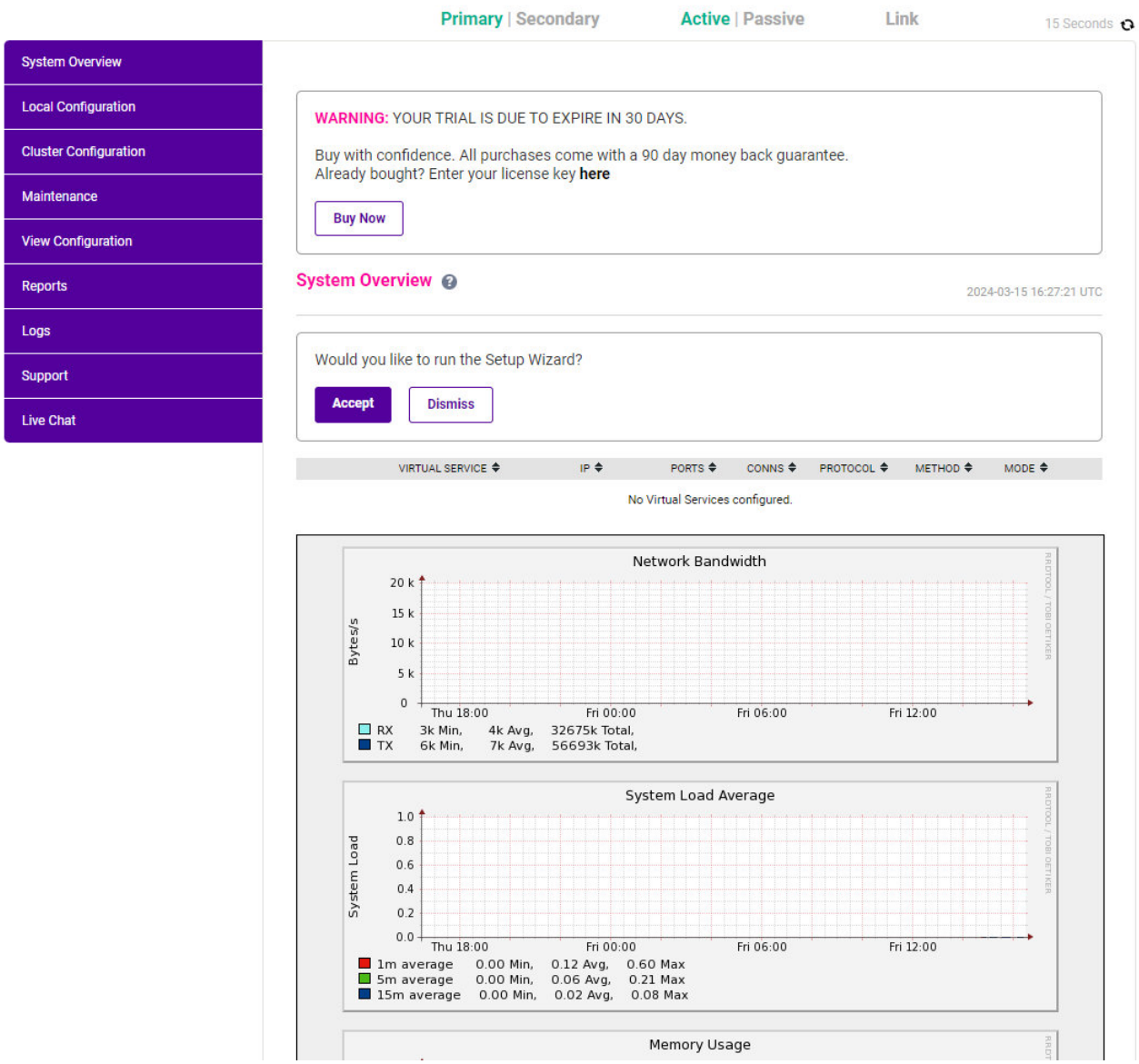
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

2. Log in to the WebUI using the following credentials:

   Username: loadbalancer
   Password: <configured-during-network-setup-wizard>

   > **Note** To change the password, use the WebUI menu option: ***Maintenance > Passwords.***

   Once logged in, the WebUI will be displayed as shown below:



3. You'll be asked if you want to run the Setup Wizard which can be used to configure layer 7 services. Click **Dismiss** if you're following a guide or want to configure the appliance manually or click **Accept** to start the wizard.

Main Menu Options

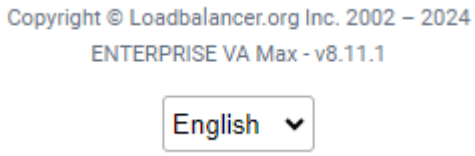
System Overview - Displays a graphical summary of all VIPs, RIPs and key appliance statistics
Local Configuration - Configure local host settings such as IP address, DNS, system time etc.
Cluster Configuration - Configure load balanced services such as VIPs & RIPs
Maintenance - Perform maintenance tasks such as service restarts and taking backups
View Configuration - Display the saved appliance configuration settings
Reports - View various appliance reports & graphs
Logs - View various appliance logs
Support - Create a support download, contact the support team & access useful links
Live Chat - Start a live chat session with one of our Support Engineers

6.4. Appliance Software Update

To ensure that the appliance(s) are running the latest software version, we recommend a software update check is performed.

Determining the Current Software Version

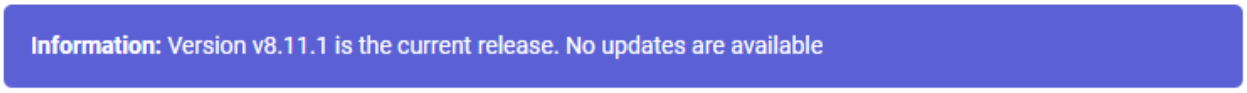
The software version is displayed at the bottom of the WebUI as shown in the example below:



Checking for Updates using Online Update

> **Note** By default, the appliance periodically contacts the Loadbalancer.org update server and checks for updates. An update check can also be manually triggered as detailed below.

1. Using the WebUI, navigate to: ***Maintenance > Software Update***.
2. Select **Online Update**.
3. If the latest version is already installed, a message similar to the following will be displayed:



4. If an update is available, you'll be presented with a list of new features, improvements, bug fixes and security related updates.
5. Click **Online Update** to start the update process.

> **Note** Do not navigate away whilst the update is ongoing, this may cause the update to fail.

6. Once complete (the update can take several minutes depending on download speed and upgrade version) the following message will be displayed:

7. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

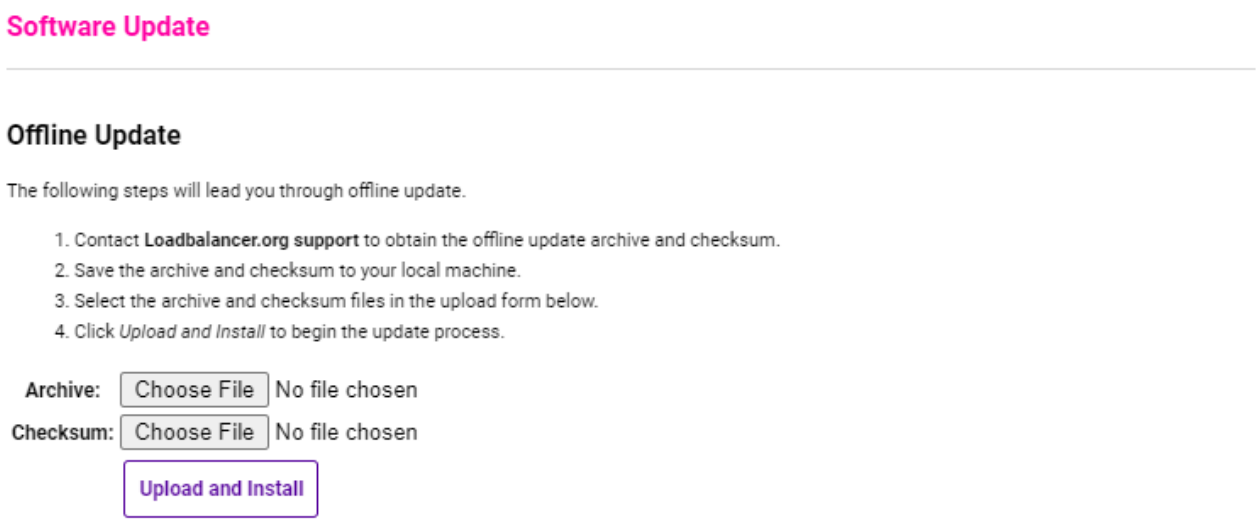
Using Offline Update

If the load balancer does not have access to the Internet, offline update can be used.

> **Note** Please contact support@loadbalancer.org to check if an update is available and obtain the latest offline update files.

To perform an offline update:

1. Using the WebUI, navigate to: *Maintenance > Software Update*.
2. Select **Offline Update**.
3. The following screen will be displayed:



4. Select the *Archive* and *Checksum* files.
5. Click **Upload and Install**.
6. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

6.5. Ports Used by the Appliance

By default, the appliance uses the following TCP & UDP ports:

Protocol	Port	Purpose
TCP	22 *	SSH
TCP & UDP	53 *	DNS / GSLB
TCP & UDP	123	NTP
TCP & UDP	161 *	SNMP
UDP	6694	Heartbeat between Primary & Secondary appliances in HA mode
TCP	7778	HAProxy persistence table replication
TCP	9000 *	Gateway service (Centralized/Portal Management)
TCP	9080 *	WebUI - HTTP (disabled by default)
TCP	9081 *	Nginx fallback page

Protocol	Port	Purpose
TCP	9443 *	WebUI - HTTPS
TCP	25565 *	Shuttle service (Centralized/Portal Management)

> **Note** The ports used for SSH, GSLB, SNMP, the WebUI, the fallback page, the gateway service and the shuttle service can be changed if required. For more information, please refer to Service Socket Addresses.

6.6. HA Clustered Pair Configuration

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary unit is covered in Configuring HA - Adding a Secondary Appliance.

7. Server & Appliance Configuration - AD FS 2.0

7.1. Federation Servers

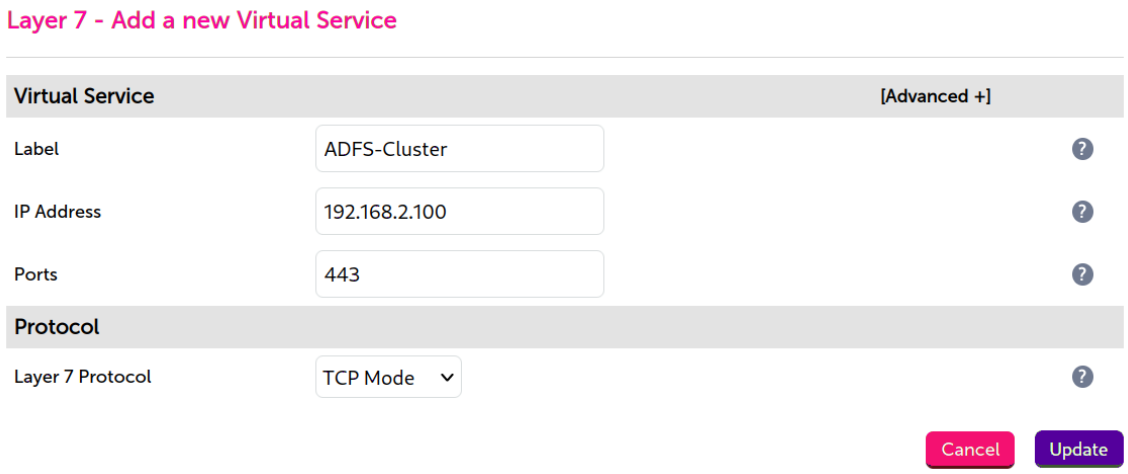
Federation Server Installation & Configuration

- AD FS v2.0 for Windows 2008 R2 must be downloaded and installed manually on each AD FS server. If installed using Server Manager/Add Roles, v1.0 will be installed, ***NOT*** v2.0.
- AD FS update rollup 3 is available here
- For information on configuring the Federation Servers please refer to this URL

Load Balancer Configuration

Setting up the Virtual Service (VIP)

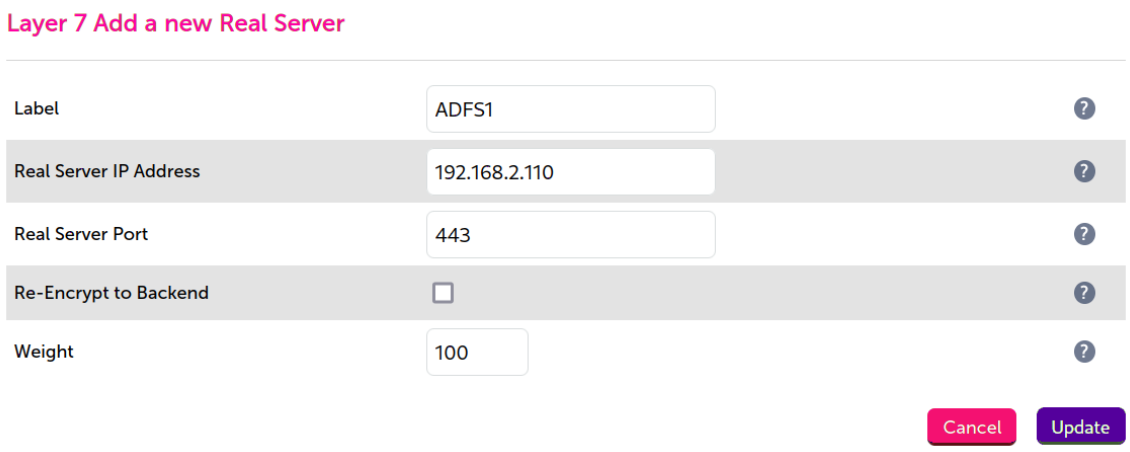
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**.
2. Enter the following details:



3. Enter an appropriate name (Label) for the Virtual Service, e.g. **ADFS-Cluster**.
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.100**.
5. Set the *Virtual Service Ports* field to **443**.
6. Set *Layer 7 Protocol* to **TCP Mode**.
7. Click **Update**.
8. Now click **Modify** next to the newly created Virtual Service.
9. Change *Persistence Mode* to **None**.
10. In the *Health Checks* section, click **Advanced** to show more options.
11. Change *Health Checks* to **Negotiate HTTPS (GET)**.
12. Set *Check Port* to **443**.
13. Set *Request to Send* to **adfs/ls/idpinitiatedsignon.aspx**.
14. Set *Response Expected* to **Sign-In**.
15. In the *Other* section, click **Advanced** to show more options.
16. Enable (check) the *Timeout* checkbox, set both *Client Timeout* and *Real Server Timeout* to **5m**.
17. Click **Update**.

Setting up the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service.
2. Enter the following details:



3. Enter an appropriate name (Label) for the first AD FS server, e.g. **ADFS1**.
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.110**.
5. Set the *Real Server Port* field to **443**.
6. Click **Update**.
7. Now repeat for your remaining Federation server(s).

Applying the new Layer 7 Settings

1. Once the configuration is complete, use the **Restart/Reload HAProxy** button at the top of the screen to commit the changes, or use the WebUI option: *Maintenance > Restart Services*.

DNS Configuration

Create a suitable DNS entry for the load balanced Federation Servers, i.e. for the VIP on the load balancer.

e.g. **adfs.lbtestdom.com**

Testing & Verification

> **Note** For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.

The load balanced AD FS servers should now be accessible using the DNS entry for the VIP. Connect to the login page from a browser.

e.g. **https://adfs.lbtestdom.com/adfs/ls/idpinitiatedsignon.aspx**

7.2. Federation Proxy Servers

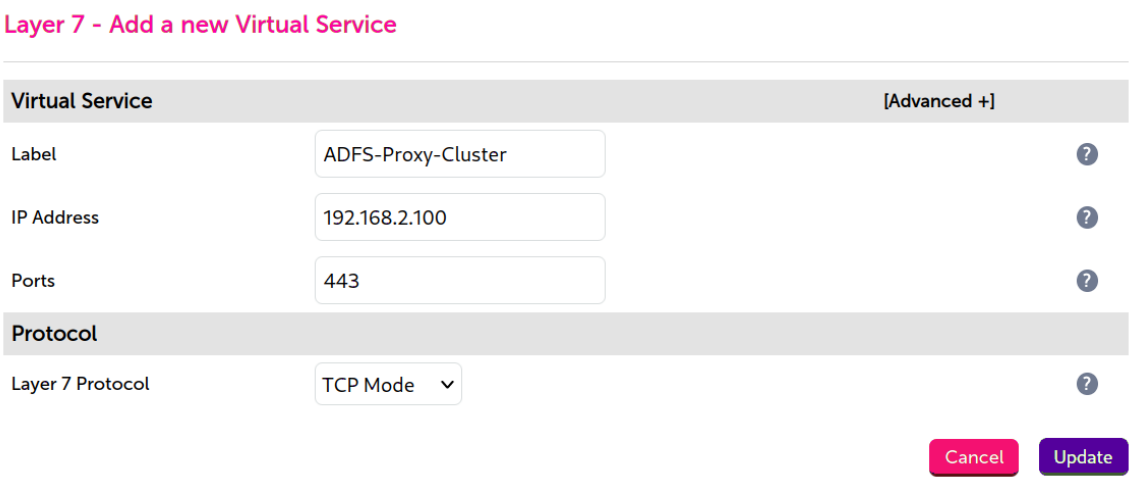
Proxy Server Installation & Configuration

- AD FS v2.0 for Windows 2008 R2 must be downloaded and installed manually on each AD FS Proxy Server. If installed using Server Manager/Add Roles, v1.0 will be installed, ***NOT*** v2.0.
- AD FS update rollup 3 is available here.
- When running the wizard, the Federation Service Name should be the load balanced VIP of the Federation Servers.
- For information on configuring the Proxy Servers please refer to this URL.
- The Federation Proxy servers must be able to access the internal AD FS VIP on port 443 via the "Federation Service Name" specified during installation / configuration. Make sure that firewalls, routing and DNS are configured to allow this. In this guide, the Federation Service Name used is **adfs.lbtestdom.com**, so an entry for this is added to the local hosts file on each Federation Proxy Server which resolves to the AD FS VIP on the internal LAN.

Load Balancer Configuration

Setting up the Virtual Service (VIP)

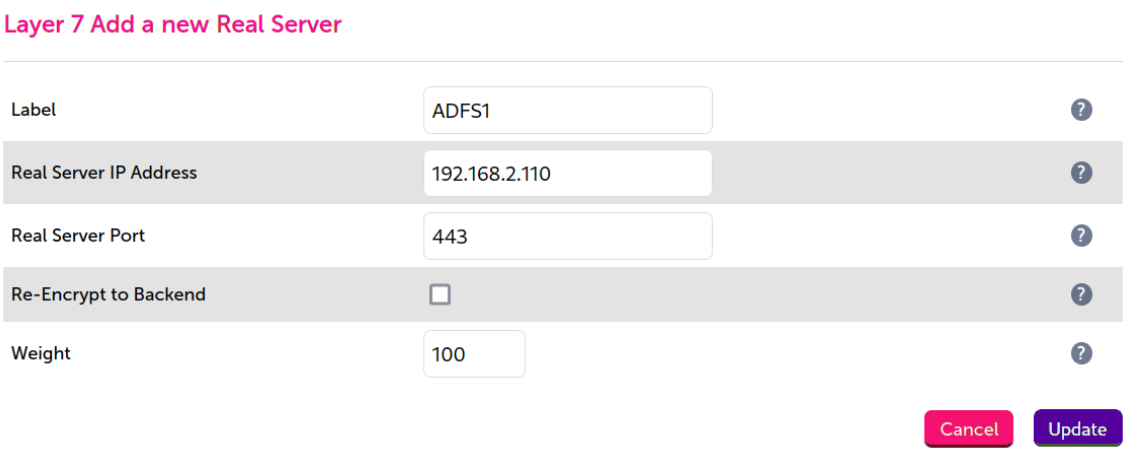
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**.
2. Enter the following details:



3. Enter an appropriate name (Label) for the Virtual Service, e.g. **ADFS-Proxy-Cluster**.
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.100**.
5. Set the *Virtual Service Ports* field to **443**.
6. Set the *Layer 7 Protocol* to **TCP Mode**.
7. Click **Update**.
8. Now click **Modify** next to the newly created Virtual Service.
9. Change *Persistence Mode* to **None**.
10. In the *Health Checks* section, click **Advanced** to show more options.
11. Change *Health Checks* to **Negotiate HTTPS (GET)**.
12. Set *Check Port* to **443**.
13. Set *Request to Send* to **adfs/ls/idpinitiatedsignon.aspx**.
14. Set *Response Expected* to **Sign-In**.
15. In the *Other* section, click **Advanced** to show more options.
16. Enable (check) the *Timeout* checkbox, set both *Client Timeout* and *Real Server Timeout* to **5m**.
17. Click **Update**.

Setting up the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service.
2. Enter the following details:



3. Enter an appropriate name (Label) for the first AD FS server, e.g. **ADFS1**.
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.110**.
5. Set the *Real Server Port* field to **443**.
6. Click **Update**.
7. Now repeat for your remaining Federation Proxy server(s).

Applying the new Layer 7 Settings

1. Once the configuration is complete, use the **Restart/Reload HAProxy** button at the top of the screen to commit the changes, or use the WebUI option: *Maintenance > Restart Services*.

DNS Configuration

Create a suitable DNS entry for the load balanced Proxy Servers, i.e. for the VIP on the load balancer.

e.g. **adfs.robstest.com**

Testing & Verification

> **Note** For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.

The load balanced AD FS servers should now be accessible using the DNS entry for the VIP. Connect to the login page from a browser.

e.g. **https://adfs.robstest.com/adfs/ls/idpinitiatedsignon.aspx**

8. Server & Appliance Configuration - AD FS 3.0 / 4.0 / 5.0

8.1. Federation Servers

Federation Server Installation & Configuration

The key points of the installation process are covered below. For more details, please also refer to the following Microsoft URL:

- How To Install AD FS 2016 For Office 365

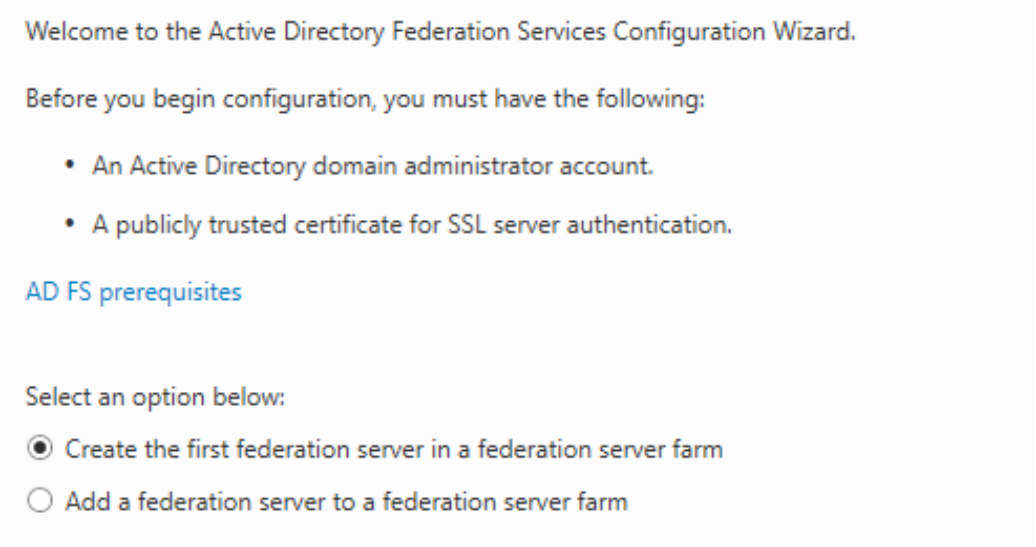
STEP 1 – Prepare AD FS Certificates

In this guide an Internal CA was used to issue the certificate. As mentioned here the Private Key must be exportable so that the certificate and private key can be exported from the first Federation Server, and used on other Federation Servers and on the WAPs.

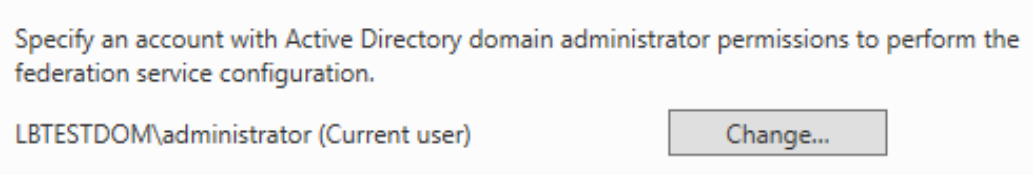
> **Note**
>
> In this guide, the Common Name is set to **adfs.lbtestdom.com**. As mentioned on page 9, for AD FS v4.0 and later, an additional SAN can be added (**certuth.adfs.lbtestdom.com**) to allow certificate authentication over port 443. If this is not done, certificate authentication occurs over TCP 49443. In this scenario, port 49443 must be included in the VIP.
>
> The following warning is displayed for AD FS v4.0+ if the additional SAN is not included:
>
> ⚠ The SSL certificate subject alternative names do not support host name 'certauth.adfs.lbtestdom.com'. Configuring certificate authentication binding on port '49443' and hostname 'adfs.lbtestdom.com'.

STEP 2 – Install AD FS on the first (Primary) Federation Server

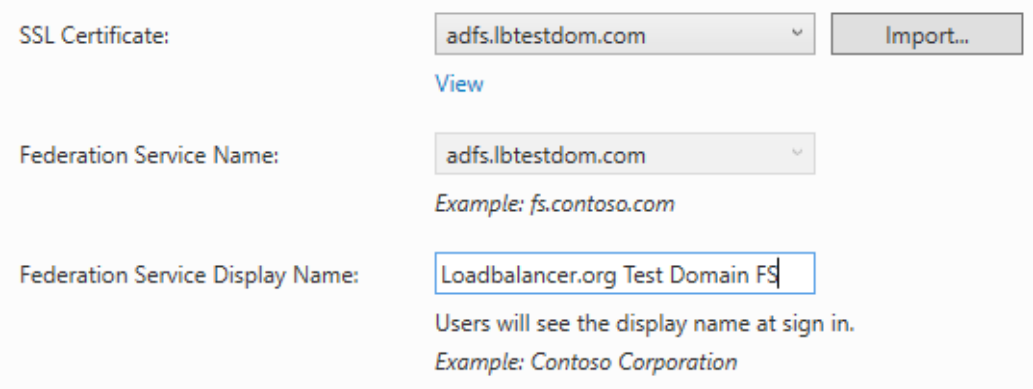
Use *Server Manager > Add Roles and Features* to install AD FS, then run the Configuration Wizard:.



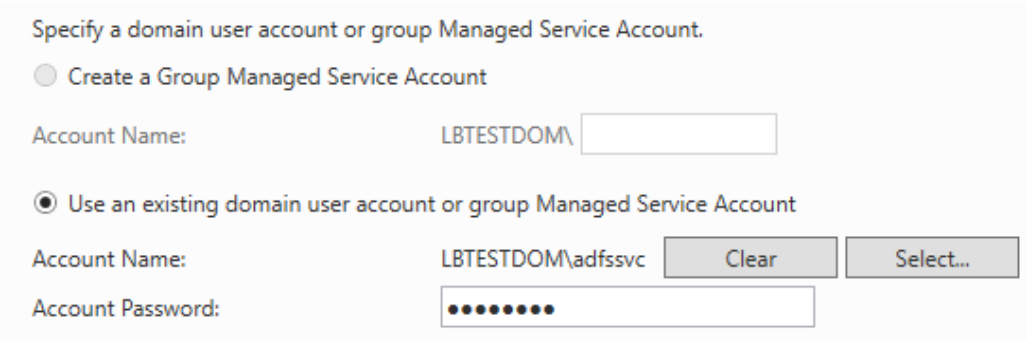
Select *Create the first federation server in federation server farm* and click **Next**.



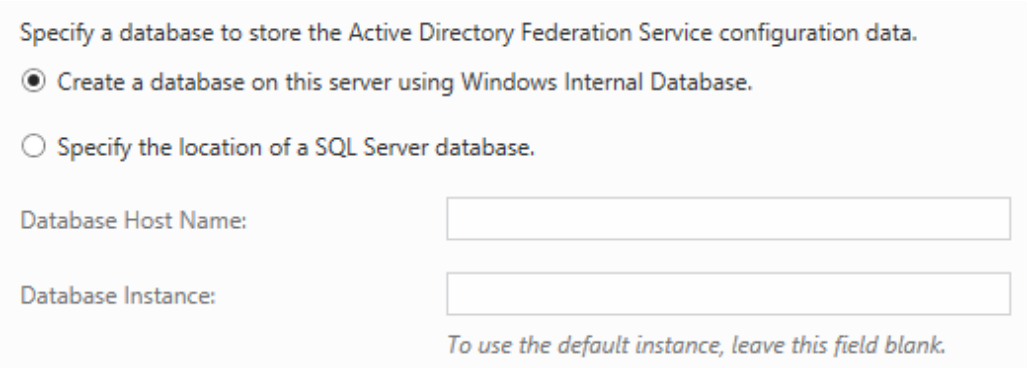
Specify a suitable account and click **Next**.



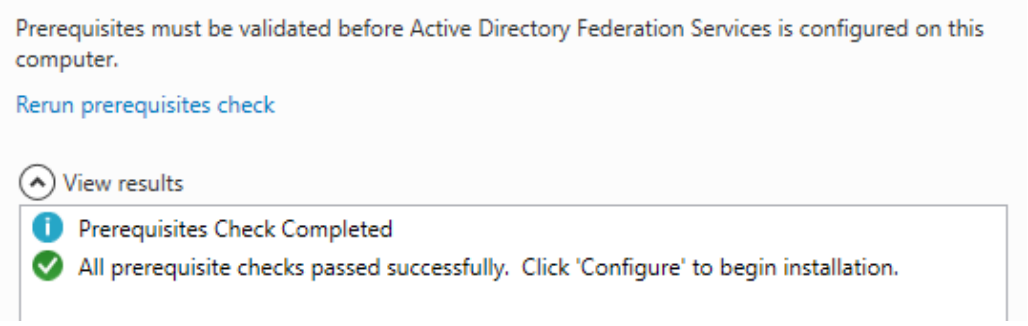
Choose the certificate created in Step 1, enter a display name and click Next.



Choose a suitable service account and click **Next**.



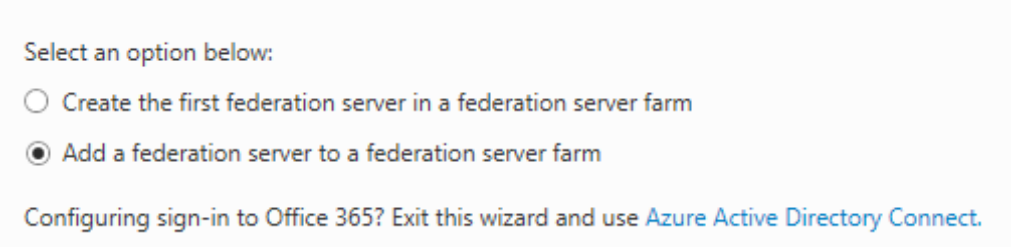
Choose where configuration data will be stored and click **Next**.



As mentioned, click **Configure** to begin the installation.

STEP 3 – Install AD FS on the remaining Federation Server(s)

Use *Server Manager > Add Roles and Features* to install AD FS, then run the Configuration Wizard:

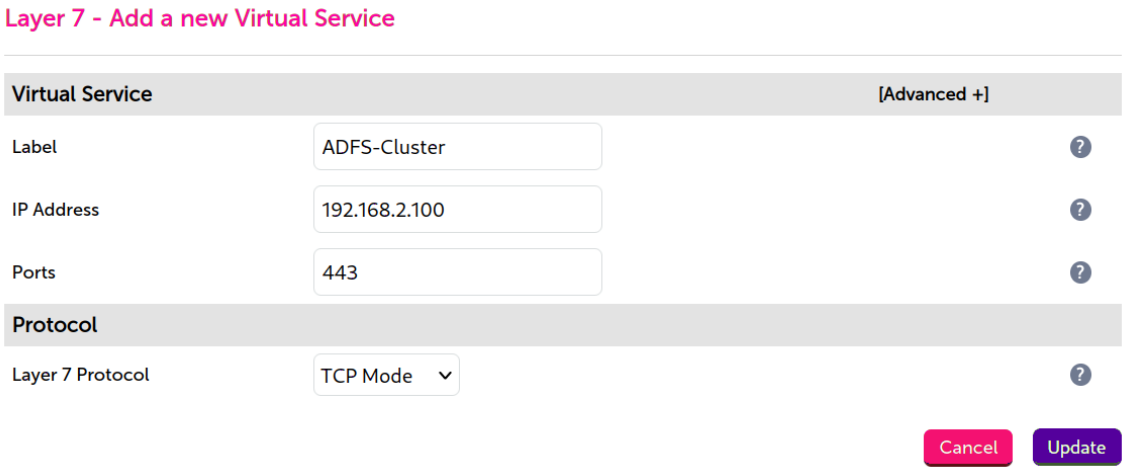


In this case, select *Add a federation server to the federation server farm* and click **Next** , then continue through the remaining screens until the installation & configuration is complete.

Load Balancer Configuration

Setting up the Virtual Service (VIP)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**.
2. Enter the following details:

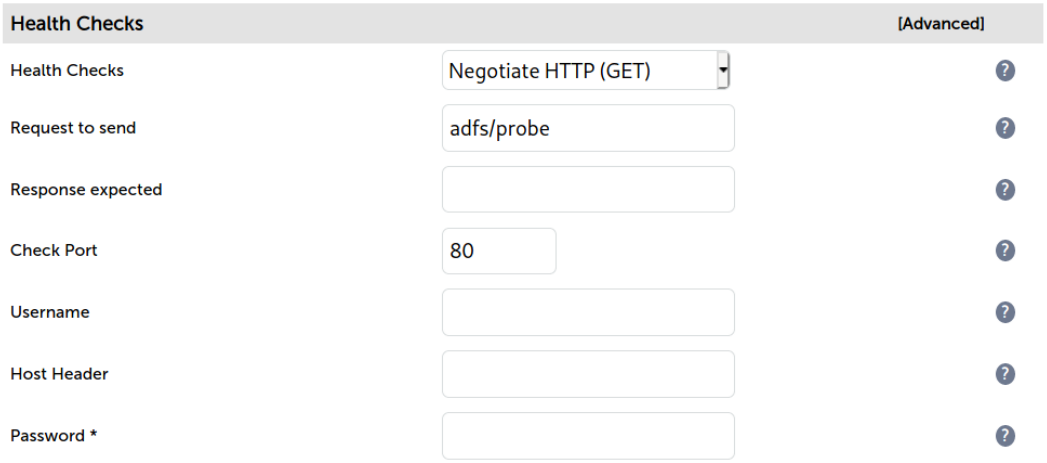


3. Enter an appropriate name (Label) for the Virtual Service, e.g. **ADFS-Cluster**.
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.100**.
5. Set the *Virtual Service Ports* field to **443**.

> **Note** If you don't have the SAN **certauth.your_adfs_service_name** added to your SSL certificate, make sure port 49443 is also included in the VIP, i.e. set the *Virtual Service Ports* field to: **443,49443** rather than: **443**.

6. Set the *Layer 7 Protocol* to **TCP Mode**.
7. Click **Update**.
8. Now click **Modify** next to the newly created Virtual Service.

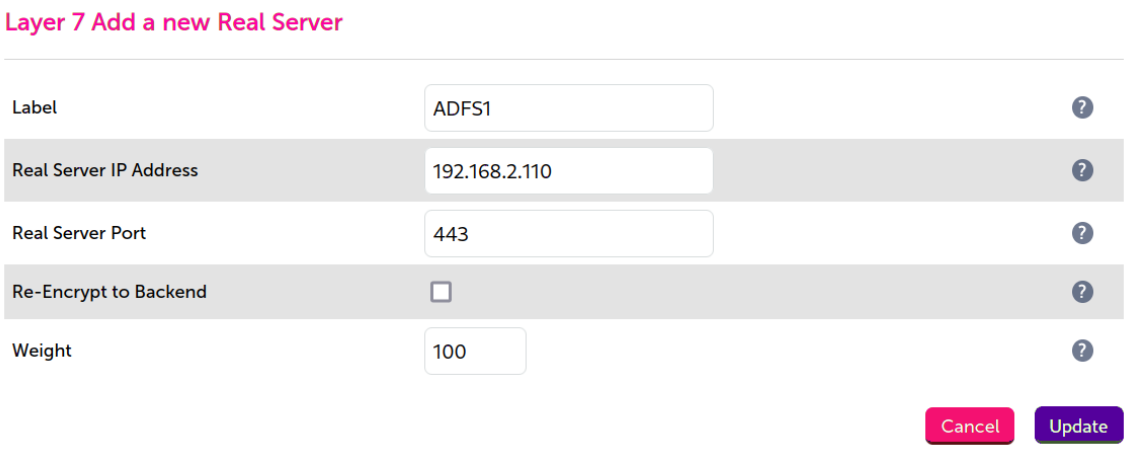
9. In the *Other* section, click **Advanced** to show more options.
10. Enable (check) the *Timeout* checkbox, set both *Client Timeout* and *Real Server Timeout* to **5m**.
11. In the *Health Checks* section, click **Advanced** to show more options.
12. Configure the health check settings as shown below, this will configure the load balancer to look for an **HTTP 200 OK** response from each server:



    a. Change *Health Checks* to **Negotiate HTTP (GET)**.
    b. Set *Request to send* to **adfs/probe**.
    c. Leave *Response Expected* blank.
    d. Set *Check Port* to **80**.
13. Click **Update**.

Setting up the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service.
2. Enter the following details:



3. Enter an appropriate name (Label) for the first AD FS server, e.g. **ADFS1**.

4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.110**.
5. Set the *Real Server Port* field to **443**.

> **Note** If you included port 49443 in the VIP, leave the *Real Server Port* field blank.

6. Click **Update**.
7. Now repeat for your remaining Federation server(s).

Applying the new Layer 7 Settings

1. Once the configuration is complete, use the **Restart/Reload HAProxy** button at the top of the screen to commit the changes, or use the WebUI option: *Maintenance > Restart Services*.

DNS Configuration

Create a suitable DNS entry for the load balanced AD FS servers, i.e. for the VIP on the load balancer.

e.g. **adfs.lbtestdom.com**

If your SSL certificate includes the additional SAN for certificate authentication, you'll also need a suitable DNS entry for this.

e.g. **certauth.adfs.lbtestdom.com**

Testing & Verification

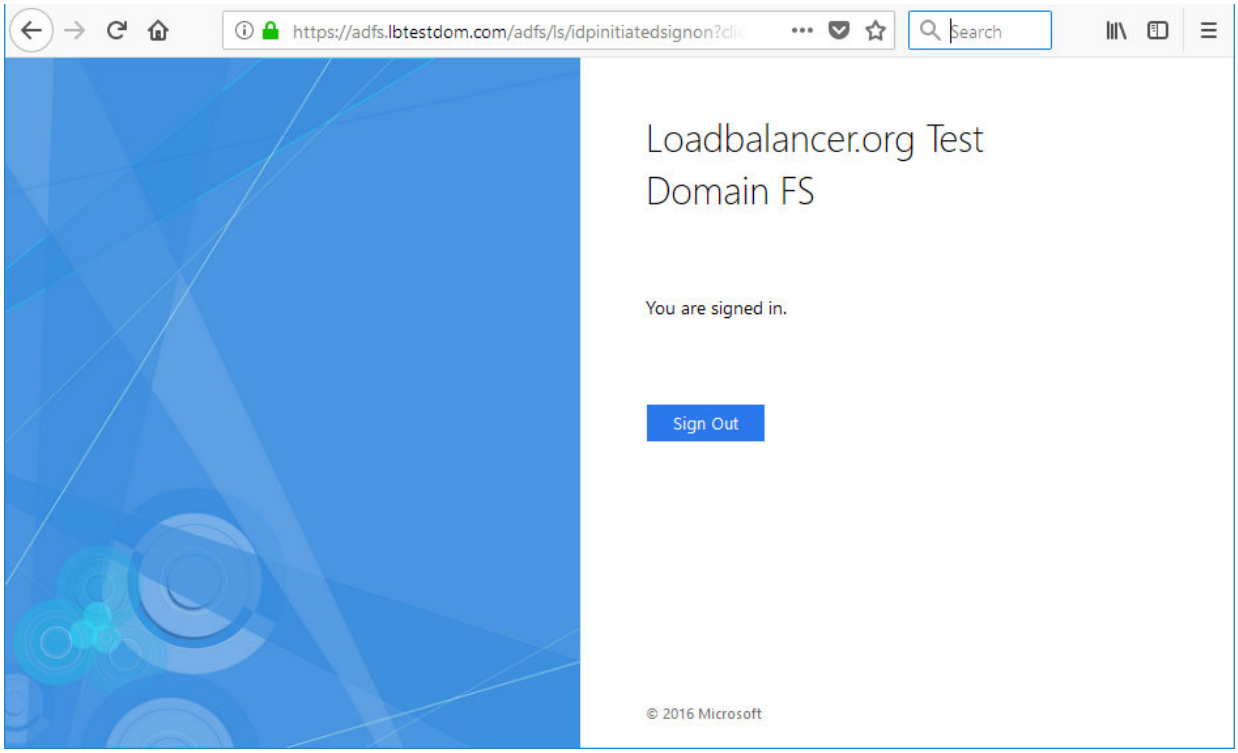
> **Note** For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.

The load balanced AD FS servers should now be accessible using the DNS entry for the VIP. Connect to the login page from a browser.

e.g. **https://adfs.robstest.com/adfs/ls/idpinitiatedsignon.htm**

> **Note** As mentioned here, the Sign In page is disabled by default in AD FS 2016 (AD FS v4.0) and later. To manually enable it, use the following PowerShell command on the Primary Federation Server:
>
> ```
> Set-AdfsProperties -EnableIdPInitiatedSignonPage $true
> ```

Log in when prompted. Once logged in, your browser should display something similar to the following:



8.2. Web Application Proxy (WAP) Servers

WAP Server Installation & Configuration

The key points of the installation process are covered below. For more details, please also refer to the following Microsoft URLs:

- How To Install AD FS 2016 For Office 365

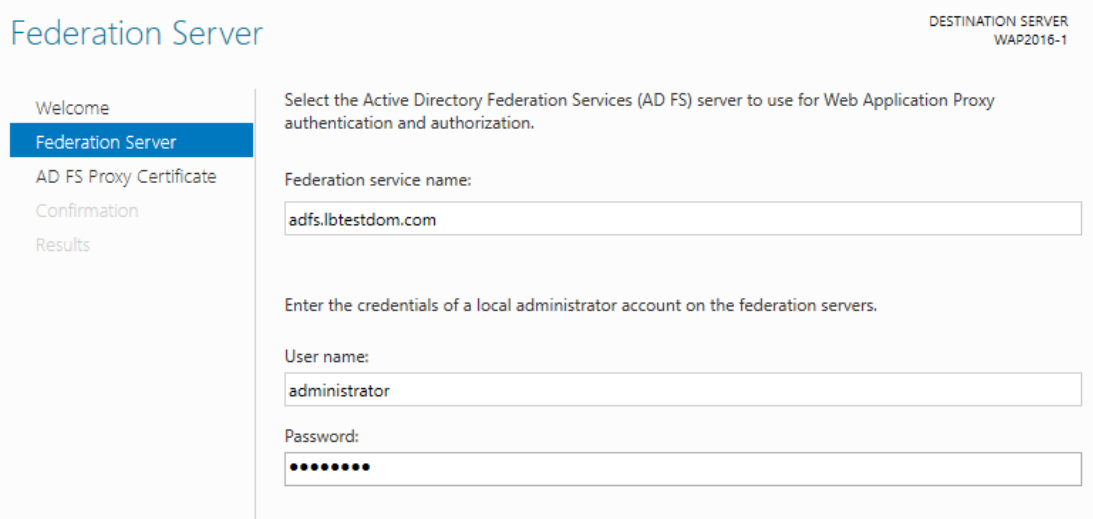
> **Note** The WAP servers must be able to access the internal AD FS VIP on port 443 via the "Federation Service Name" specified during installation / configuration. Make sure that firewalls, routing and DNS are configured to allow this. In this guide, the Federation Service Name used is **adfs.lbtestdom.com**, so an entry for this is added to the local hosts file on each WAP server which resolves to the AD FS VIP on the internal LAN.

STEP 1 – Prepare the SSL Certificate

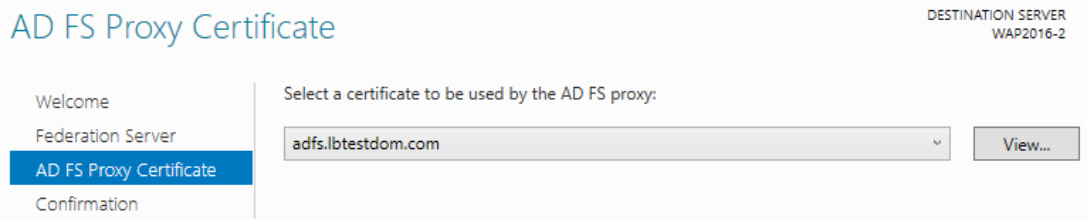
Export the certificate & private key from one of the Federation Servers, then import the certificate into the local computer account certificate store on each WAP server. This will ensure the certificate is ready to use when the configuration wizard is run.

STEP 2 – Install & Configure Web Application Proxy (WAP) on the each WAP Server

1. Use *Server Manager > Add Roles and Features* to install Web Application Proxy, then run the Configuration Wizard:



2. Enter the *Federation service name* and the user credentials and click **Next**.

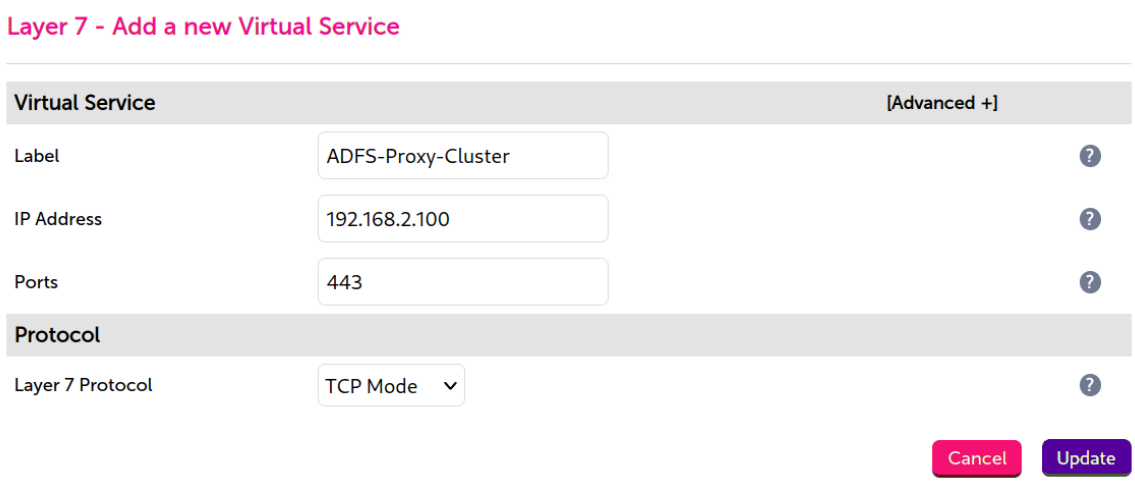


3. Select the certificate to be used by the Proxy and click **Next**, then click **Configure** to start the configuration.

Load Balancer Configuration

Setting up the Virtual Service (VIP)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**.
2. Enter the following details:

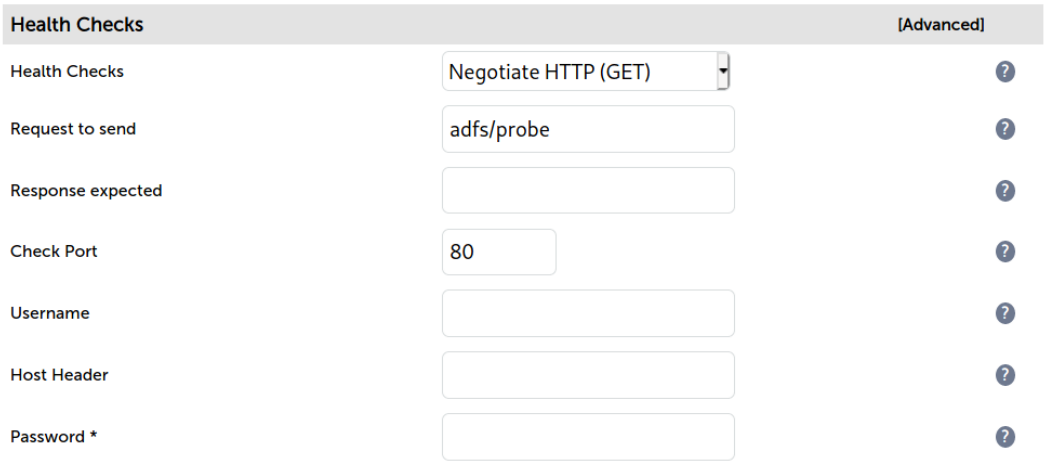


3. Enter an appropriate name (Label) for the Virtual Service, e.g. **ADFS-Proxy-Cluster**.
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.100**.

5. Set the *Virtual Service Ports* field to **443**.

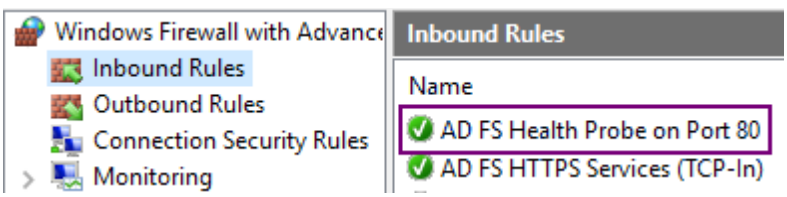
> **Note** If you don't have the SAN **certauth.your_adfs_service_name** added to your SSL certificate, make sure port 49443 is also included in the VIP, i.e. set the *Virtual Service Ports* field to: **443,49443** rather than: **443**.

6. Set the *Layer 7 Protocol* to **TCP Mode**.
7. Click **Update**.
8. Now click **Modify** next to the newly created Virtual Service.
9. In the *Other* section, click **Advanced** to show more options.
10. Enable (check) the *Timeout* checkbox, set both *Client Timeout* and *Real Server Timeout* to **5m**.
11. In the *Health Checks* section, click **Advanced** to show more options.
12. Configure the health check settings as shown below, this will configure the load balancer to look for an **HTTP 200 OK** response from each server:.



a. Change *Health Checks* to **Negotiate HTTP (GET)**.
b. Set *Request to send* to **adfs/probe**.
c. Leave *Response Expected* blank.
d. Set *Check Port* to **80**.

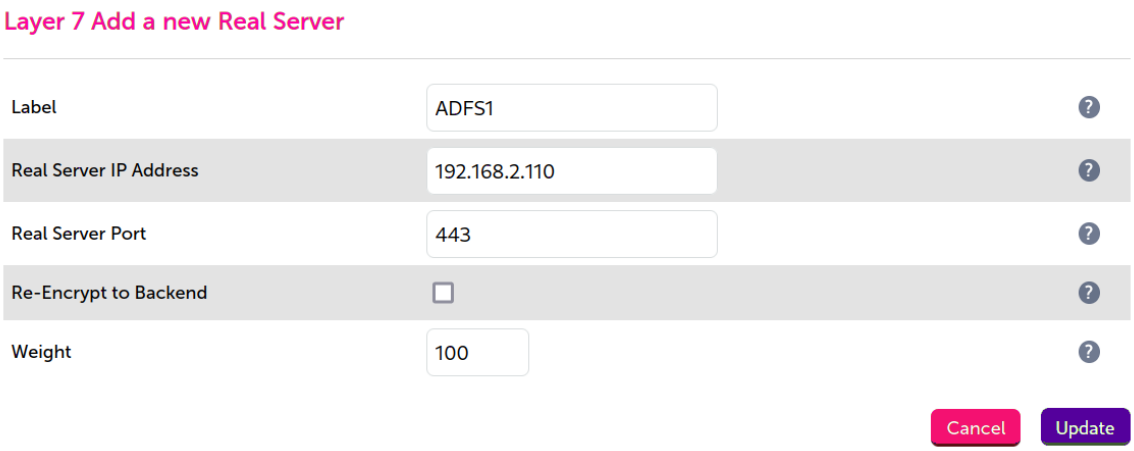
> **Note** As mentioned here, you'll need to create an inbound rule to open port 80 on the firewall of each WAP server for this health-check to work. For the Federation servers this is configured automatically, but not for the WAPs.



13. Click **Update**.

Setting up the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service.
2. Enter the following details:



3. Enter an appropriate name (Label) for the first AD FS server, e.g. **ADFS1**.
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.110**.
5. Set the *Real Server Port* field to **443**.

> **Note** If you included port 49443 in the VIP, leave the *Real Server Port* field blank.

6. Click **Update**.
7. Now repeat for your remaining WAP server(s).

Applying the new Layer 7 Settings

1. Once the configuration is complete, use the **Restart/Reload HAProxy** button at the top of the screen to commit the changes, or use the WebUI option: *Maintenance > Restart Services*.

DNS Configuration

Create a suitable DNS entry for the load balanced AD FS servers, i.e. for the VIP on the load balancer.

e.g. **adfs.lbtestdom.com**

If your SSL certificate includes the additional SAN for certificate authentication, you'll also need a suitable DNS entry for this.

e.g. **certauth.adfs.lbtestdom.com**

> **Note** The WAP servers must be able to access the internal AD FS VIP on port 443 via the "Federation Service Name" specified during installation / configuration. Make sure that firewalls, routing and

DNS are configured to allow this. In this guide, the Federation Service Name used is **adfs.lbtestdom.com**, so an entry for this is added to the local hosts file on each WAP server which resolves to the AD FS VIP on the internal LAN.

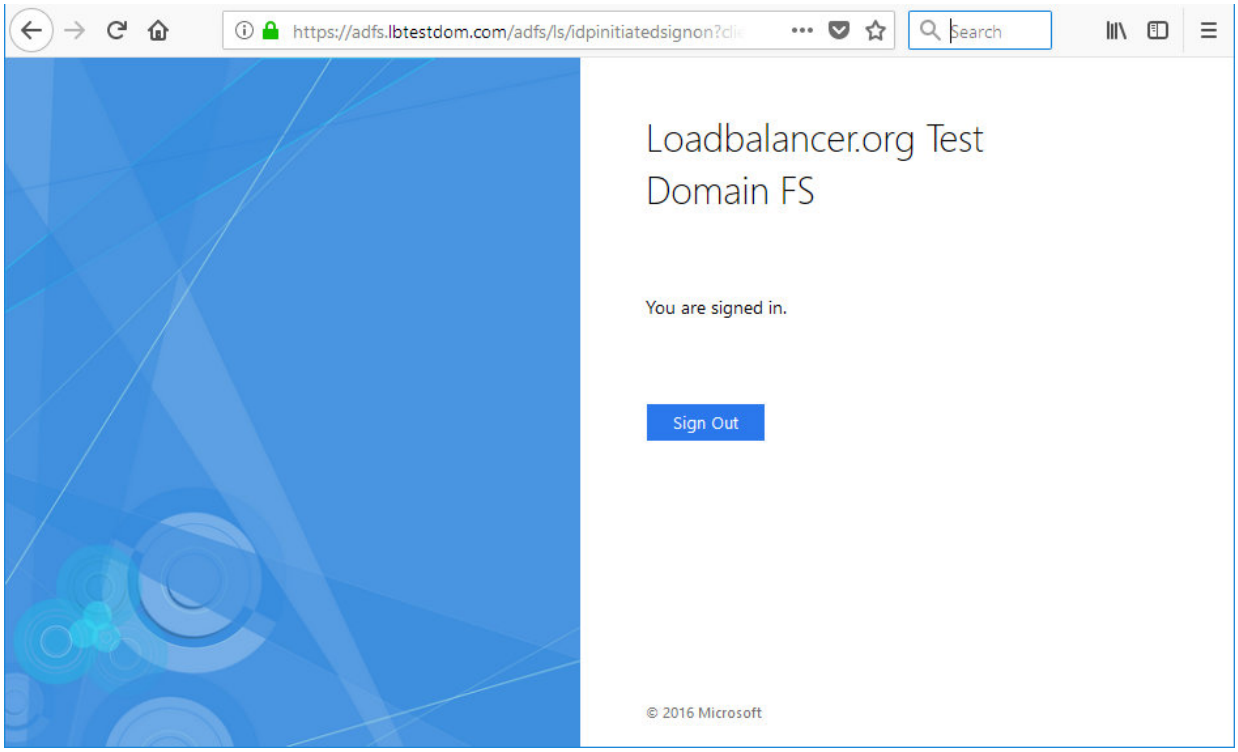
Testing & Verification

> **Note** For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.

The load balanced AD FS servers should now be accessible using the DNS entry for the VIP. Connect to the login page from a browser.

e.g. **https://adfs.robstest.com/adfs/ls/idpinitiatedsignon.htm**

Login as prompted. Once logged in, your browser should display something similar to the following:



9. Technical Support

If you have any questions regarding the appliance or would like assistance designing your deployment, please don't hesitate to contact our support team: support@loadbalancer.org.

10. Further Documentation

For additional information, please refer to the Administration Manual.

11. Appendix

11.1. Configuring HA - Adding a Secondary Appliance

Our recommended configuration is to use a clustered HA pair of load balancers to provide a highly available and resilient load balancing solution. We recommend that the Primary appliance is fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services must be configured and modified on the Primary appliance. The Secondary appliance will be automatically kept in sync.

> **Note** For Enterprise Azure, the HA pair should be configured first. For more information, please refer to the Azure Quick Start/Configuration Guide available in the documentation library

The clustered HA pair uses Heartbeat to determine the state of the other appliance. Should the active device (normally the Primary) suffer a failure, the passive device (normally the Secondary) will take over.

Non-Replicated Settings

A number of settings are not replicated as part of the Primary/Secondary pairing process and therefore must be manually configured on the Secondary appliance. These are listed by WebUI menu option in the table below:

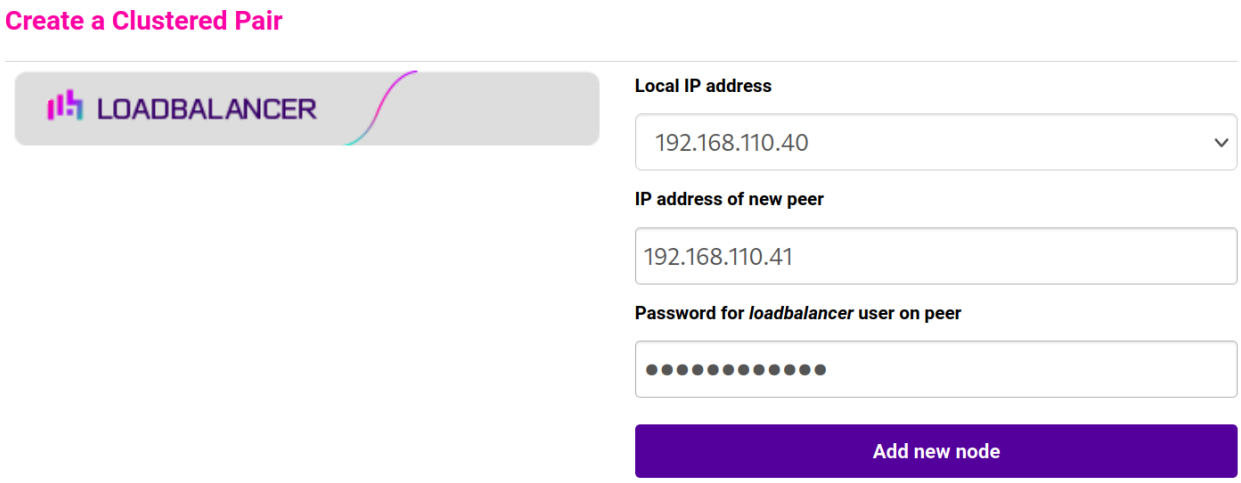
WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration	System Date & time	Time and date related settings
Local Configuration	Physical – Advanced Configuration	Various appliance settings
Local Configuration	Portal Management	Portal management settings
Local Configuration	Security	Security settings
Local Configuration	SNMP Configuration	SNMP settings
Local Configuration	Graphing	Graphing settings
Local Configuration	License Key	Appliance licensing
Maintenance	Backup & Restore	Local XML backups
Maintenance	Software Updates	Appliance software updates
Maintenance	Fallback Page	Fallback page configuration
Maintenance	Firewall Script	Firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

> **Important** Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

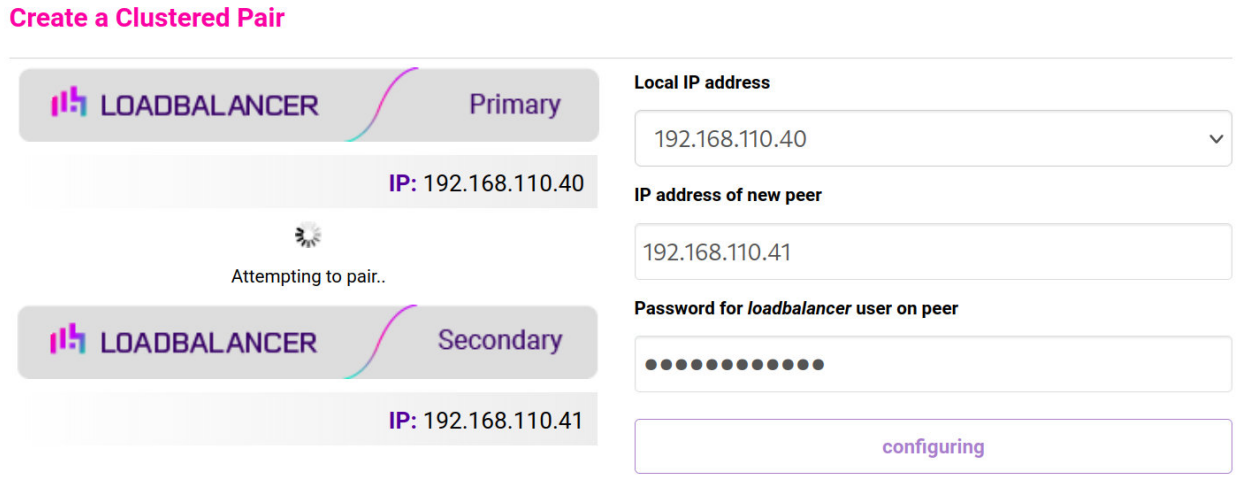
Configuring the HA Clustered Pair

> **Note** If you have already run the firewall lockdown wizard on either appliance, you'll need to ensure that it is temporarily disabled on both appliances whilst performing the pairing process.

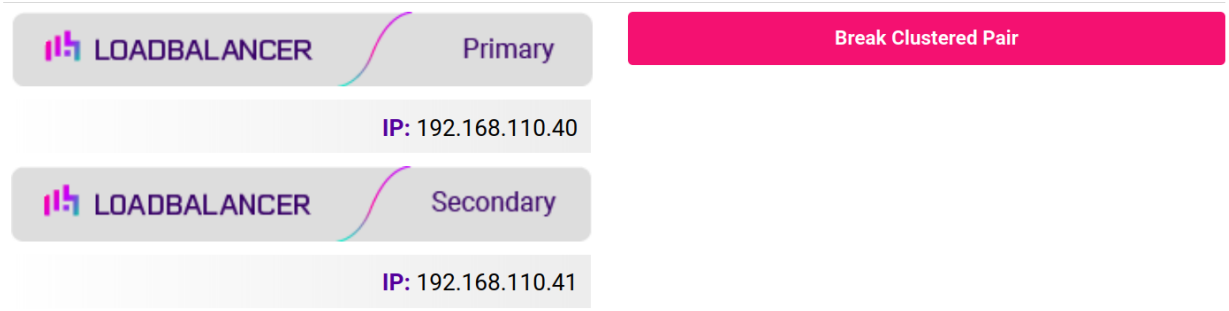
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.



3. Specify the IP address and the *loadbalancer* user's password for the Secondary (peer) appliance as shown in the example above.
4. Click **Add new node**.
5. The pairing process now commences as shown below:



6. Once complete, the following will be displayed on the Primary appliance:



7. To finalize the configuration, restart heartbeat and any other services as prompted in the "Commit changes" message box at the top of the screen.

> **Note** Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

> **Note** For more details on configuring HA with 2 appliances, please refer to Appliance Clustering for HA.

> **Note** For details on testing and verifying HA, please refer to Clustered Pair Diagnostics.

12. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.4.0	7 August 2019	Styling and layout Added AD FS v5.0 (Win2019)	General styling updates Support for latest version	RJC
1.4.1	7 January 2020	Removed links to certain Microsoft reference material	The related links are no longer available at microsoft.com	RJC
1.4.2	16 July 2020	New title page Updated Canadian contact details Revised instructions and screenshots for configuring health checks and VIP timeouts	Branding update Change to Canadian contact details Changes to the appliance WebUI	AH
1.5.0	1 January 2022	Converted the document to AsciiDoc	Move to new documentation system	AH, RJC, ZAC
1.5.1	12 May 2022	Removed outdated health check configuration sections	Now obsolete	RJC
1.5.2	28 September 2022	Updated layer 7 VIP and RIP creation screenshots	Reflect changes in the web user interface	AH
1.5.3	5 January 2023	Combined software version information into one section Added one level of section numbering Added software update instructions Added table of ports used by the appliance Reworded 'Further Documentation' section	Housekeeping across all documentation	AH
1.5.4	2 February 2023	Updated screenshots	Branding update	AH
1.5.5	7 March 2023	Removed conclusion section	Updates across all documentation	AH

Version	Date	Change	Reason for Change	Changed By
1.6.0	24 March 2023	New document theme Modified diagram colours	Branding update	AH

LOADBALANCER

Visit us: www.loadbalancer.org

Phone us: +44 (0)330 380 1064

Phone us: +1 833 274 2566

Email us: info@loadbalancer.org

Follow us: @loadbalancer.org

About Loadbalancer.org

Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.