



AD FS v3

Deployment Guide

UPDATED: 27 July 2023

Copyright Notices

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

Table of Contents

1 Introduction	4
1.1 Document Purpose	4
1.2 Intended Audience	4
1.3 Intended use of Kemp LoadMaster products with AD FS and AD FS proxy (WAP) farms	5
2 Load Balancing AD FS	6
3 Example Environment Setup	9
4 Prerequisites	12
4.1 DNS	12
4.2 AD FS SSL Certificate Import on LoadMaster	12
5 Enable Subnet Originating Requests Globally	14
6 Virtual Service (VS) Configuration	16
6.1 Configure an AD FS Internal Farm Virtual Service	16
6.2 Configure an AD FS Proxy Farm (WAP) Virtual Service	18
References	20
Last Updated Date	21

1 Introduction

Active Directory Federation Services (AD FS) is a Microsoft identity access solution. It was an optional component of Microsoft Windows Server® 2003 R2. It is now built into Windows Server® 2008, Windows Server® 2012, Windows Server 2012 R2, and Windows Server 2016. AD FS helps to establish trust relationships and reduces the need for provisioning and managing user accounts. Its implementation provides clients (internal or external to the trusted internal LAN) with simplified access to systems and applications relying on claims-based authorization. AD FS also supports web Single-Sign-On (SSO) technologies to improve User Experience across multiple protected applications.

Trust relationships are used to project a user's digital identity and access rights to trusted partners and can be deployed in multiple organizations to facilitate business-to-business (B2B) transactions between trusted partner organizations.

1.1 Document Purpose

This documentation is intended to provide guidance on how to configure Kemp LoadMaster products to provide high availability for an AD FS 3.0 or AD FS 4.0 environment, based on Windows Server 2012 R2 or Windows Server 2016. This documentation is created using a representative sample environment described later in the document. As this documentation is not intended to cover every possible deployment scenario, it may not address unique setup or requirements. The Kemp Support Team is always available to provide solutions for scenarios not explicitly defined.

1.2 Intended Audience

It is assumed that the reader is a server/network administrator or a person otherwise familiar with networking and general computer terminology and is familiar with AD FS technology.

If you are using Advanced Claims with the AD FS infrastructure, the LoadMaster cannot be used as an AD FS proxy. However, you can create an SSL-offloaded AD FS farm Virtual Service.

1.3 Intended use of Kemp LoadMaster products with AD FS and AD FS proxy (WAP) farms

Kemp LoadMaster family of products provide high availability to AD FS and AD FS proxy farms (WAP). AD FS proxy servers provide termination of external traffic at the DMZ and provides an additional layer of protection against external threats. AD FS proxy servers also help internal AD FS servers clearly identify which authentication attempts are external. This is achieved by inserting x-ms-proxy claims in AD FS requests.

AD FS administrators can configure advanced claim rules that allow granular control over user authentication restrictions such as requiring users to be a part of a certain group or requiring users to authenticate from certain IP networks. When such claims rules are configured on AD FS servers, it becomes critical to identify if the user is trying to authenticate from an external or internal location.

In deployments where select advanced claim rules such as IP network and trust levels for instance are not in use, Kemp LoadMaster devices can be placed in the DMZ and can proxy authentication requests to internal AD FS servers without requiring additional AD FS proxy (WAP) servers. This can help customers save on hardware, software and management costs associated with maintaining additional AD FS proxy servers. Instructions on how to do this are below:

1. In the LoadMaster Web User Interface (WUI), go to **Virtual Services > Add New**.
2. Enter the settings as required and click **Add this Virtual Service**.
3. Expand the **SSL Properties** section.
4. Select the **Enabled** and **Reencrypt** check boxes. Select the appropriate SSL certificate with full root and chain installed.
5. Click **OK** to the warning.
6. Expand the **Advanced Properties** section.
7. In the **Add Header to Request** boxes, enter **X-MS-Proxy** in the first field and **Kemp** in the second.
8. Click **Set Headers**.
9. Add the Real Servers from the ADFS farm to the service and set the Real Server health checks to HTTPS with a url of “/federationmetadata/2007-06/federationmetadata.xml”.

Alternatively, you could change the name to that of the LoadMaster. The purpose of this is to inform AD FS that clients are external and the form will be provided.

2 Load Balancing AD FS

The core components of AD FS are as follows:

- An AD FS server which is responsible for issuance of claims and user authentication. This server must be able to connect to a Domain Controller. It authenticates users from multiple domains by using Windows Trust. The AD FS server can be set up in a cluster to ensure high availability.
- An AD FS proxy server (Windows Application Proxy (WAP)) which protects the AD FS server from internet-based threats. The WAP server also authenticates users from the internet. The WAP server cannot be set up as a cluster and must be used with a load balancer to provide high availability.

Terminating SSL between the WAP and AD FS server is not supported. Terminating SSL breaks the trust between the WAP and AD FS.

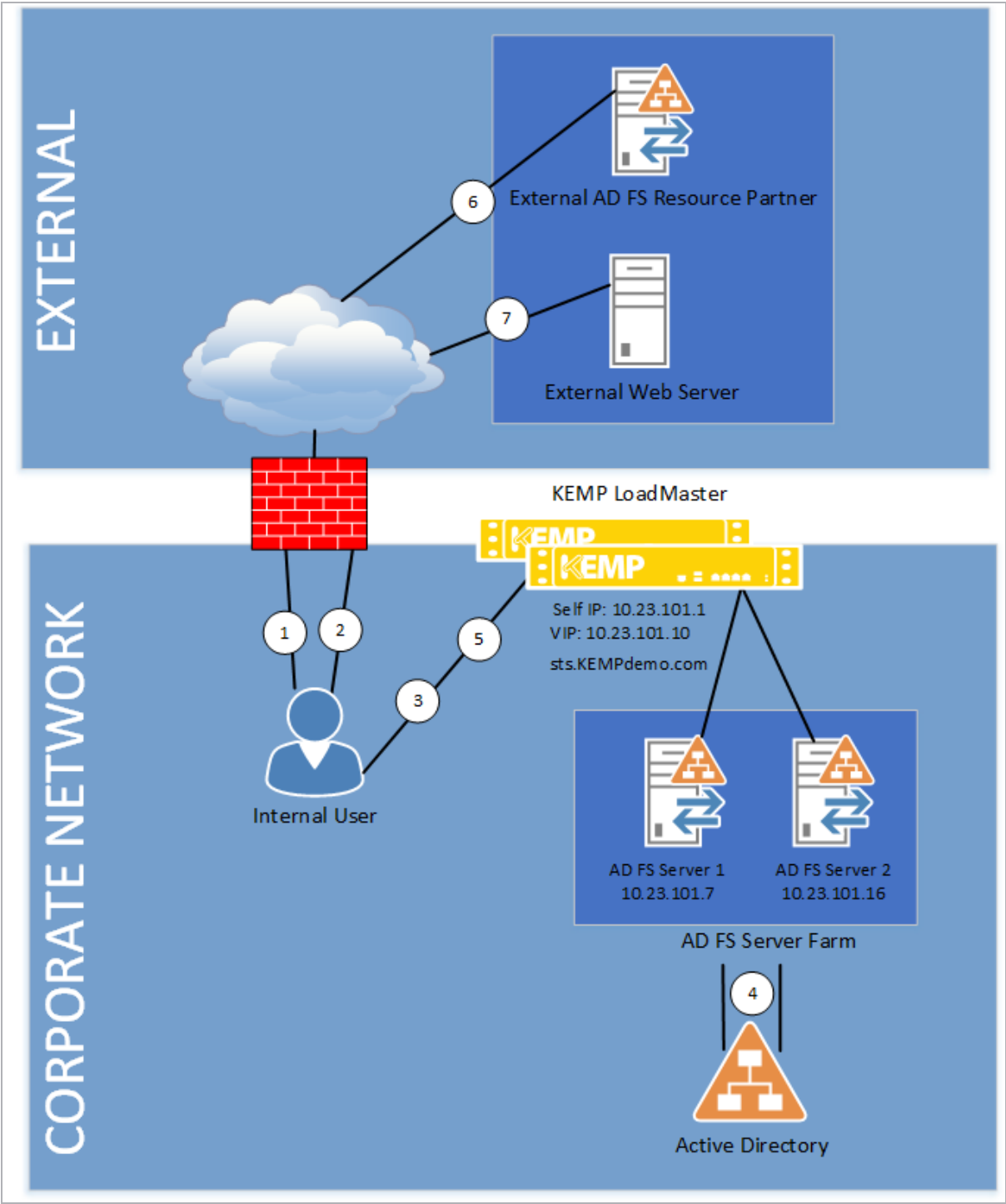
For further information, please refer to the following Microsoft TechNet article:

<https://blogs.technet.microsoft.com/applicationproxyblog/2014/07/04/ssl-termination-with-web-application-proxy-and-ad-fs-2012-r2>

- An AD FS configuration database which can be stored in a SQL database or Windows Internal Database (maximum of 5 servers) but not both at the same time. This database stores the following items:
 - Relying Party Trust
 - Certificates
 - Claim Provider Trust
 - Claims description
 - Service configuration
 - Attributes

2 Load Balancing AD FS

The diagram below shows a common authentication process flow for applications located in a resource organization and secured with AD FS, of which Office 365 is a popular example. The steps, which correspond to the numbers in the diagram, are outlined as follows.



1. The internal user tries to access the AD FS-enabled resource.
2. The client is redirected to the resource's Federation Service.
3. If the resource's federation service is configured as a trusted partner, the client is redirected to the organisation's internal Federation Service.
4. The AD FS server uses the Active Directory to authenticate the user.
5. The AD FS server sends an authorization cookie to the client. This contains the signed security token and a set of claims for the resource partner.
6. The client connects to the resource partner's Federation Service where the token and claims are verified. If appropriate, the resource partner may send a new security token.
7. The client presents the new authorisation cookie with the security token to the resource in order to access it.

3 Example Environment Setup

In our example deployment, “Kemp Demo” has deployed AD FS 3.0 in their environment to facilitate claims-based authentication for their Exchange 2010 infrastructure and allow for SSO capabilities across applications. The deployment contains the following:

- Two AD FS 3.0 Servers
- Two AD FS 3.0 Proxy Servers (Windows Application Proxy)
- Two Exchange 2013 Multi-Role Servers
- A Kemp LoadMaster High Availability (HA) Cluster

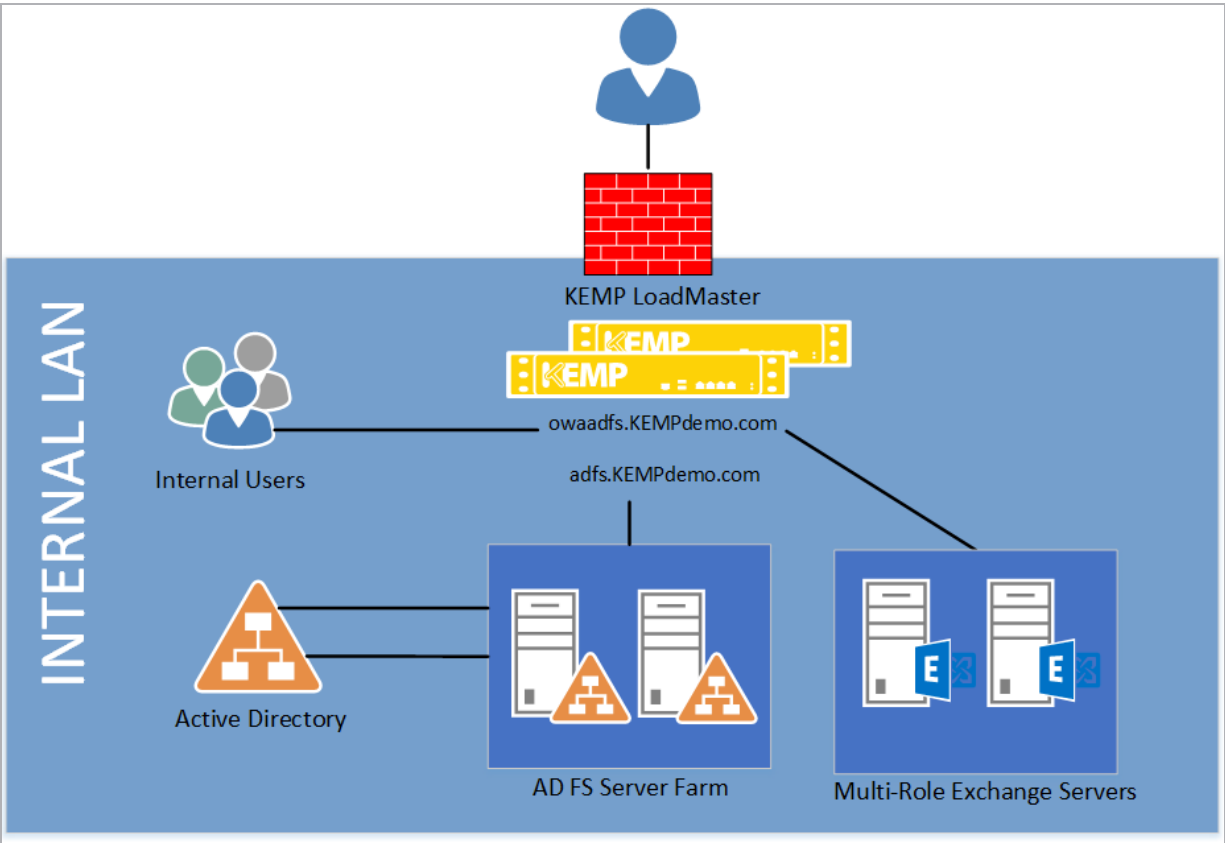
A name space of **owaADFS.Kempdemo.com** is used for access to the Microsoft Exchange environment. A name space of **myADFS.Kempdemo.com** is used for access to the AD FS environment. Split DNS is implemented, which allows these name spaces to be used both internally and externally in the environment.

The following scenarios are defined:

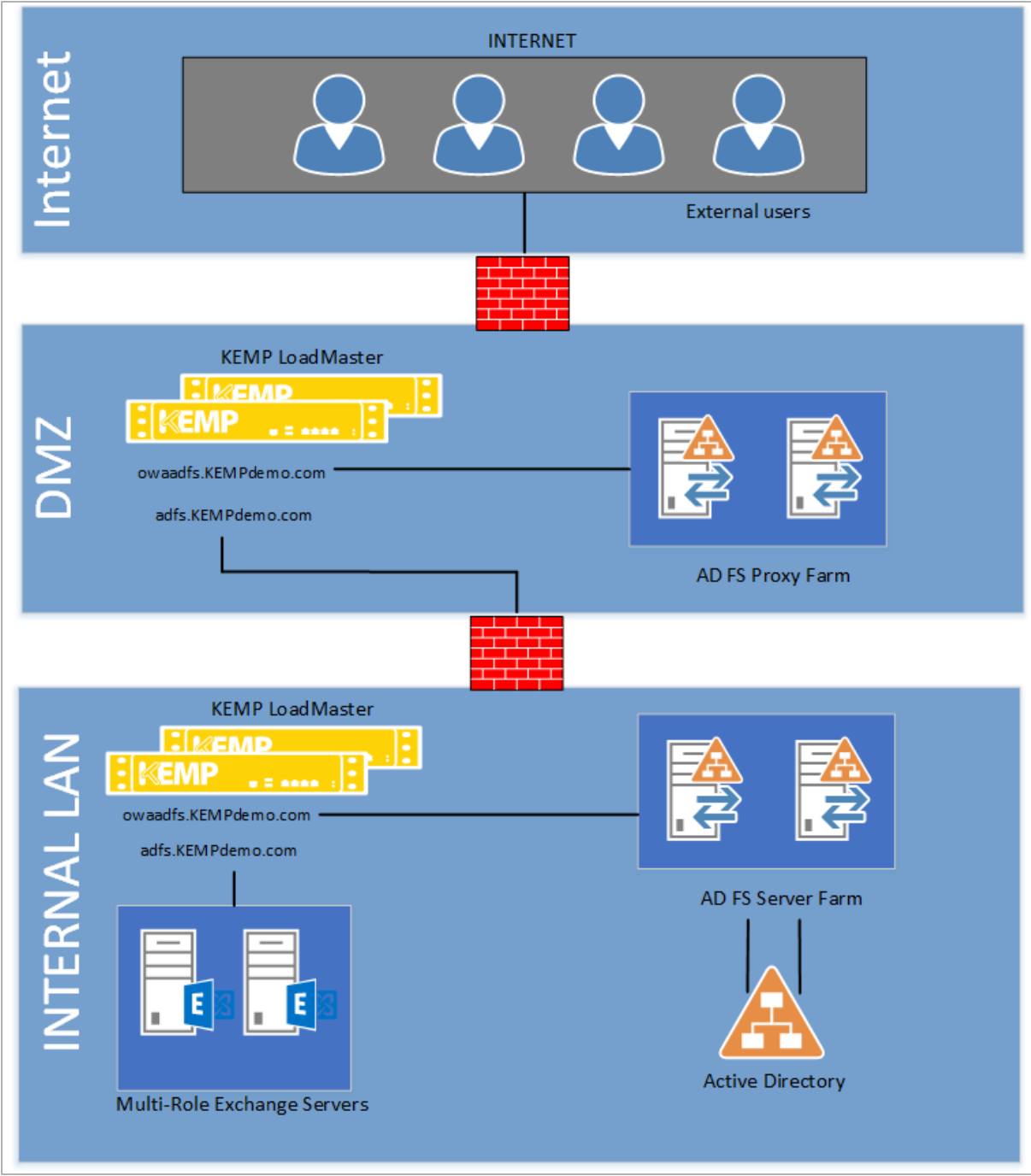
- Internal access to Outlook Web App (OWA) using the internal AD FS farm, both of which are being load-balanced by the Kemp LoadMaster
- External access to OWA using the Proxy Farm and Internal Farm all three of which are being load-balanced by the Kemp LoadMaster

The following diagrams represent the respective environments:

3 Example Environment Setup



3 Example Environment Setup



4 Prerequisites

There are some prerequisites to be aware of before deploying the Kemp LoadMaster with AD FS.

It is assumed that the AD FS 3.0 or AD FS 4.0 environment is already set up and the Kemp LoadMaster has been installed. We recommend reviewing the [LoadMaster Web User Interface \(WUI\), Configuration Guide](#).

At a minimum, the following actions should be completed:

- Implemented Active Directory, AD FS, Domain Name System (DNS), Federation Server Proxy (FSP), and other Microsoft requirements
- Configured the application servers to support claims-based authentication
- Installed the LoadMaster on the same network as the servers
- Established access to the LoadMaster WUI

4.1 DNS

Access to the DNS used in the environment must be available. This is needed to set up name resolution of the AD FS services to the Virtual Service IP addresses that will be configured on the Kemp LoadMaster.

4.2 AD FS SSL Certificate Import on LoadMaster

The AD FS SSL certificate has to be imported into the LoadMaster before deployment. To import the certificate, follow the steps below:

1. Log in to the relevant Virtual Load Master (VLM).
2. In the main menu, click **Certificates & Security** and select **SSL Certificates**.
3. Click the **Import Certificate** button.

4 Prerequisites

Please specify the name of the file that contains the certificate. The file can also hold the private key.
If the file does not contain the private key, then the file containing the private key must also be specified.
The certificate can be in either .PEM or .PFX (IIS) format.

Certificate File	<input type="button" value="Choose File"/>	testcert.crt
Key File (optional)	<input type="button" value="Choose File"/>	No file chosen
Pass Phrase	<input type="password" value="....."/>	
Certificate Identifier	<input type="text" value="ADFScertificate"/>	

4. Click **Choose File** next to the **Certificate File** field.
5. Browse to and select the certificate file.
6. Click **Open**.
7. Browse to and select the **Key File** if needed.
8. Enter the **Pass Phrase** of the certificate.
9. Enter a name for the certificate in the **Certificate Identifier** field.
10. Click **Save**.
11. If it works a success message will be displayed. Click **OK**.

Despite the fact that clients establish a single Transmission Control Protocol (TCP) connection with the AD FS server to request and receive a security token, certain applications can suffer from multiple login redirections if persistence is not enabled on the load balancer. For this reason, a Layer 7 service is used, along with SSL reencryption, to allow for the more intelligent forms of persistence that are not available at Layer 4 or when SSL traffic is not terminated at the LoadMaster.

5 Enable Subnet Originating Requests Globally

It is best practice to enable the **Subnet Originating Requests** option globally.

In a one-armed setup (where the Virtual Service and Real Servers are on the same network/subnet) **Subnet Originating Requests** is usually not needed. However, enabling **Subnet Originating Requests** should not affect the routing in a one-armed setup.

In a two-armed setup where the Virtual Service is on network/subnet A, for example, and the Real Servers are on network B, **Subnet Originating Requests** should be enabled on LoadMasters with firmware version 7.1-16 and above.

When **Subnet Originating Requests** is enabled, the LoadMaster routes traffic so that the Real Server sees traffic arriving from the LoadMaster interface that is in that network/subnet.

When **Subnet Originating Requests** is enabled globally, it is automatically enabled on all Virtual Services. If the **Subnet Originating Requests** option is disabled globally, you can choose whether to enable **Subnet Originating Requests** on a per-Virtual Service basis.

To enable **Subnet Originating Requests** globally, follow the steps below:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **System Configuration > Miscellaneous Options > Network Options**.

5 Enable Subnet Originating Requests Globally

Enable Server NAT	<input checked="" type="checkbox"/>
Connection Timeout (secs)	<input type="text" value="660"/> Set Time (Valid values:0, 60-86400)
Enable Non-Local Real Servers	<input type="checkbox"/>
Enable Alternate GW support	<input type="checkbox"/>
Enable TCP Timestamps	<input type="checkbox"/>
Enable TCP Keepalives	<input checked="" type="checkbox"/>
Enable Reset on Close	<input type="checkbox"/>
Subnet Originating Requests	<input checked="" type="checkbox"/>
Enforce Strict IP Routing	<input type="checkbox"/>
Handle non HTTP Uploads	<input type="checkbox"/>
Enable Connection Timeout Diagnostics	<input type="checkbox"/>
Enable SSL Renegotiation	<input checked="" type="checkbox"/>
Size of SSL Diffie-Hellman Key Exchange	<input type="text" value="2048 Bits"/> ▼
Use Default Route Only	<input type="checkbox"/>
HTTP(S) Proxy	<input type="text"/> Set HTTP(S) Proxy

2. Select the **Subnet Originating Requests** check box.

6 Virtual Service (VS) Configuration

Steps on how to configure the AD FS Virtual Services that can be used are outlined in the sections below.

6.1 Configure an AD FS Internal Farm Virtual Service

Follow the steps below to configure the AD FS internal farm Virtual Service:

Do not enable **SSL Acceleration** on this Virtual Service. When using the Web Application Proxy role, the proxy server needs to present a certificate of trust to the AD FS server.

1. Log in to the relevant VLM.
2. In the main menu, click **Virtual Services** and select **Add New**.

Please Specify the Parameters for the Virtual Service.

Virtual Address	<input type="text" value="10.154.11.41"/>
Port	<input type="text" value="443"/>
Service Name (Optional)	<input type="text" value="AD FS Internal Farm"/>
Use Template	<input type="text" value="Select a Template"/>
Protocol	<input type="text" value="tcp"/>

3. Enter the **Virtual Address**.

This is the Virtual IP address used for the service and must be unique and not in use by any other device on the network.

4. Enter **443** in the **Port** field.
5. Enter a name for the VS in the **Service Name (Optional)** field.
6. Ensure that **tcp** is selected as the **Protocol**.

6 Virtual Service (VS) Configuration

7. Click **Add this Virtual Service**.

8. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
Standard Options	Persistence Mode	Source IP	If the traffic is being Network Address Translated (NATed), set the Service Type to Generic and set the Persistence Mode to SSL Session ID.
	Timeout	1 Hour	
	Scheduling Method	least connection	

9. Expand the **Real Servers** section.

10. In the first Real Server Check Parameters field, select **HTTPS Protocol**.

11. Enter the health check **URL** and click **Set URL**.

The **Health Check URL** can be set to **adfs/services/trust/mex** or **/adfs/ls/idpInitiatedSignon.aspx**.

12. Select the **Use HTTP/1.1** check box.

13. Enter the **HTTP/1.1 Host** name and click **Set Host**.

14. Select **GET** as the **HTTP Method**.

15. Click the **Add New...** button.

16. Enter the IP address of the server to be added to the real server pool. Click **Add This Real Server**. A success message will be displayed after adding. Click **OK**. Repeat this for any other real servers that need to be added.

17. In the main menu, click **Virtual Services** and select **View/Modify Services**.

18. Confirm that the service is listed with a **Status** of **Up** and that all added member servers are listed in non-bold font.

19. Test access to the AD FS Internal Farm by opening a browser and going to **https://<AD FS URL>/ADFS/ls/idpinitiatedsignon.aspx** and following the instructions to log in.

20. Once all other Microsoft-defined AD FS prerequisites and application configurations are complete, test access to the application to ensure authentication success. To do this, open a browser and go to **https://owAD FS/<AD FS URL>/owa**.

A successful login will result in access to the protected application.

Login experience is dependent upon the parameters set in the web.config file located on the AD FS servers.

6.2 Configure an AD FS Proxy Farm (WAP) Virtual Service

The steps to set up an AD FS Proxy Farm Virtual Service, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.

Please Specify the Parameters for the Virtual Service.

Virtual Address	<input type="text" value="10.154.11.72"/>
Port	<input type="text" value="443"/>
Service Name (Optional)	<input type="text" value="AD FS Proxy Farm"/>
Use Template	<input type="text" value="Select a Template"/>
Protocol	<input type="text" value="tcp"/>

2. Enter a valid IP address.
3. Enter **443** as the **Port**.
4. Enter a recognizable **Service Name**, for example **AD FS Proxy Farm**.
5. Click **Add this Virtual Service**.
6. Configure the settings as recommended in the following table:

Section	Option	Value	Comments
SSL Properties	SSL	Enabled	
	Acceleration		
	Reencrypt	Selected	
	Require SNI Hostname		Type your SNI Hostname then click Set SNI Hostname .

6 Virtual Service (VS) Configuration

Section	Option	Value	Comments
Standard Options	Persistence Mode	Super HTTP	
	Timeout	1 Hour	
	Scheduling Method	least connection	
Advanced Properties	Enable Caching	Selected	The maximum cache usage should be configured dependent upon the number of services on the LoadMaster that are leveraging this feature. If there are no other services, the Maximum Cache usage can be set to No Limit . Otherwise, it can be set as needed.
	Enable Compression	Selected	
Real Servers	Real Server Check Parameters	HTTPS Protocol	
	URL	adfs/services/trust/mex or /adfs/ls/idpInitiatedSignon.aspx	Click Set URL .
	Use HTTP/1.1 check box	Selected	
	HTTP/1.1 Host		Type the host name and click Set Host .
	HTTP Method	GET	

7. Continue from the **Click the Add New... button.** step in the **Configure an AD FS Internal Farm Virtual Service** section.

References

Unless otherwise specified, the following documents can be found at <http://kemptechnologies.com/documentation>.

ESP, Feature Description

LoadMaster Web User Interface (WUI), Configuration Guide

Last Updated Date

This document was last updated on 27 July 2023.