

# AD FS v2

## Deployment Guide

UPDATED: 27 July 2023

**© 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.


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

# Table of Contents

**1 Introduction** ..... **4**

1.1 Document Purpose ..... 4

1.2 Intended Audience ..... 4

**2 Load Balancing AD FS** ..... **5**

**3 Example Environment Setup** ..... **8**

**4 Prerequisites** ..... **11**

4.1 DNS ..... 11

4.2 AD FS SSL Certificate Import on LoadMaster ..... 11

**5 Virtual Service (VS) Configuration** ..... **13**

5.1 Template ..... 13

5.2 Configure an AD FS Internal Farm Virtual Service ..... 13

5.3 Configure an AD FS Proxy Farm Virtual Service ..... 15

**References** ..... **18**

**Last Updated Date** ..... **19**


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

# 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 and Windows Server® 2012. 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 UX 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 organisations to facilitate business-to-business (B2B) transactions between trusted partner organisations.

## 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 2.0 environment. 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.


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

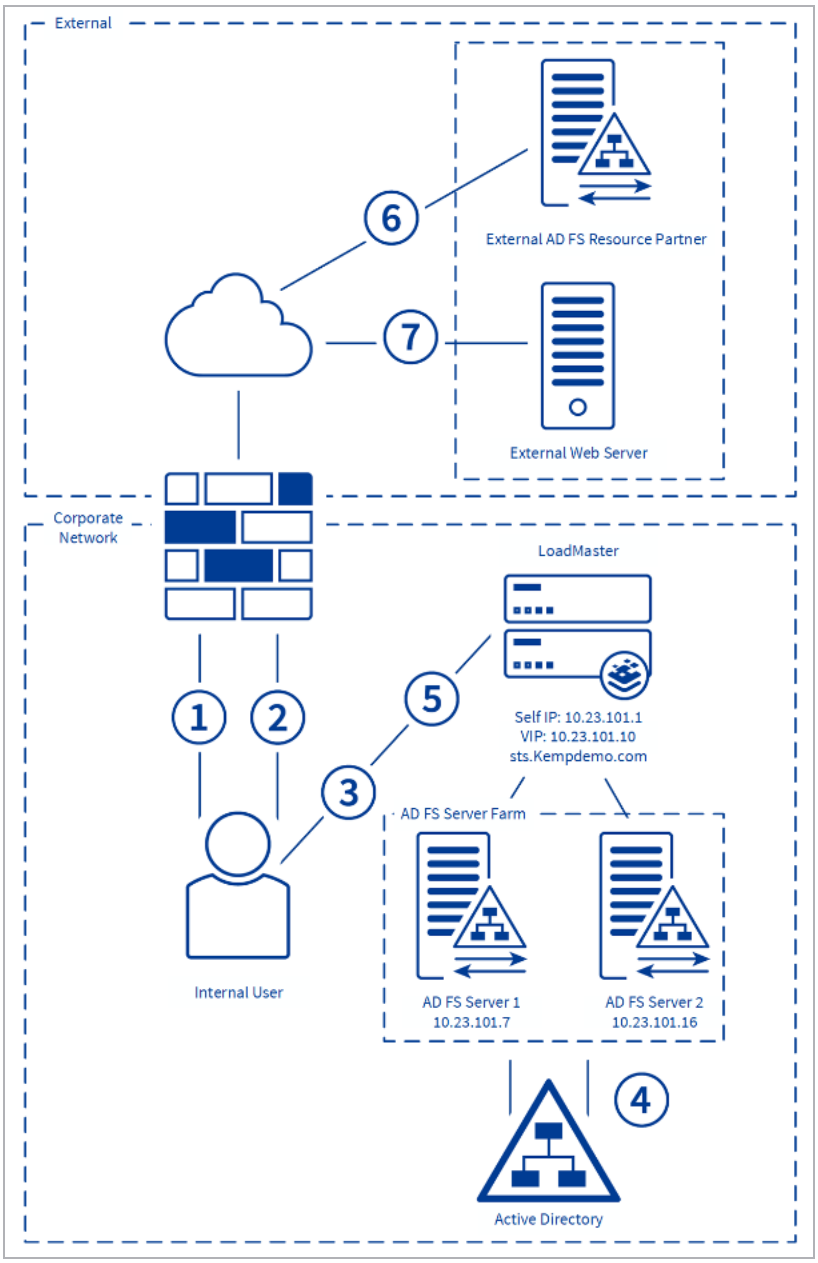
# 2 Load Balancing AD FS

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 which protects the AD FS server from internet-based threats. The AD FS proxy server also authenticates users from the internet. Again, the AD FS proxy server can be set up in a cluster to ensure high availability.
- An AD FS configuration database which can be stored in an 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

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.


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




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.


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

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.


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

# 3 Example Environment Setup

In our example deployment, “Kemp Demo” has deployed AD FS 2.0 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 2.0 Servers
- Two AD FS 2.0 Proxy Servers
- Two Exchange 2010 Multi-Role Servers
- A Kemp LoadMaster High Availability (HA) Cluster

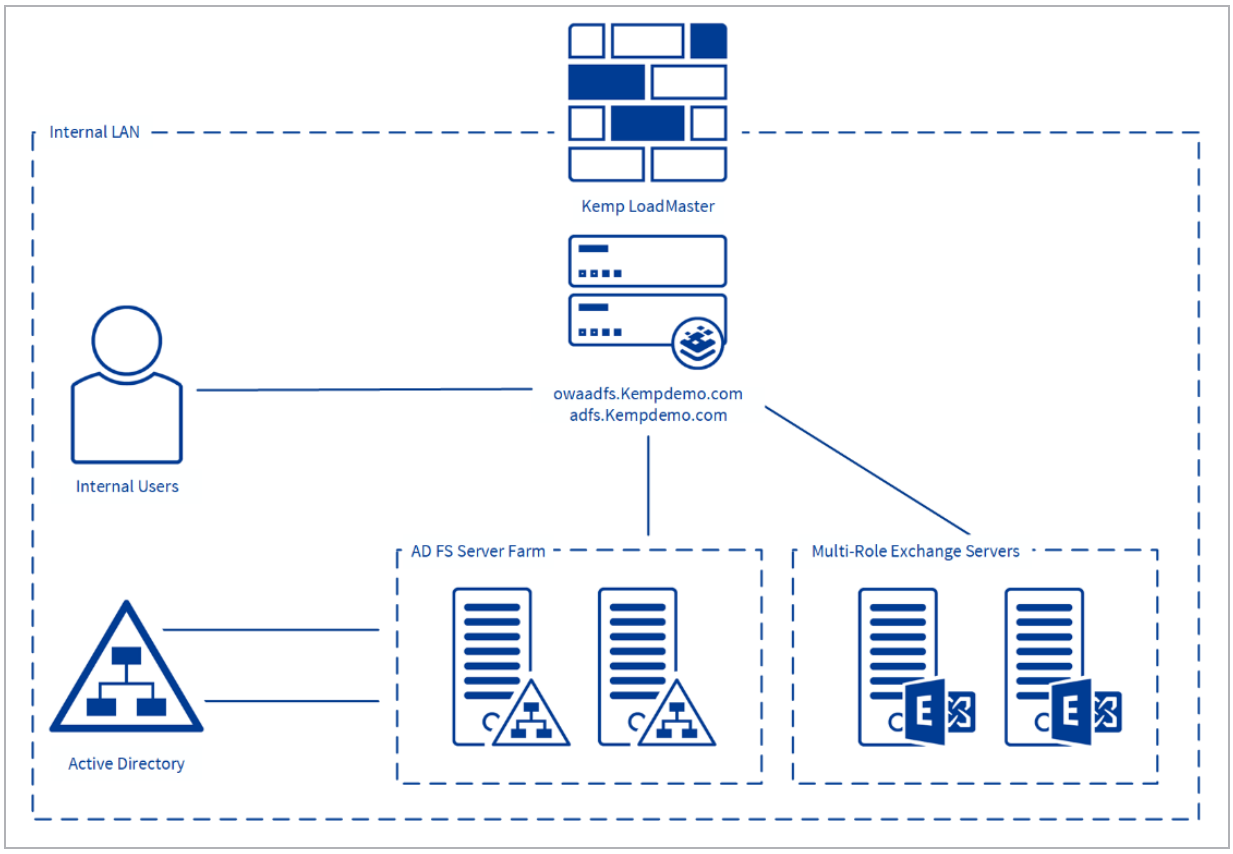
A name space of **owaADFS.Kempdemo.com** is used for access to the Microsoft Exchange environment. A name space of **myADFS.Kempdemo.com** is used for access to the AD FS environment. Split DNS is implemented, which allows these name spaces to be used both internally and externally in the environment.

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

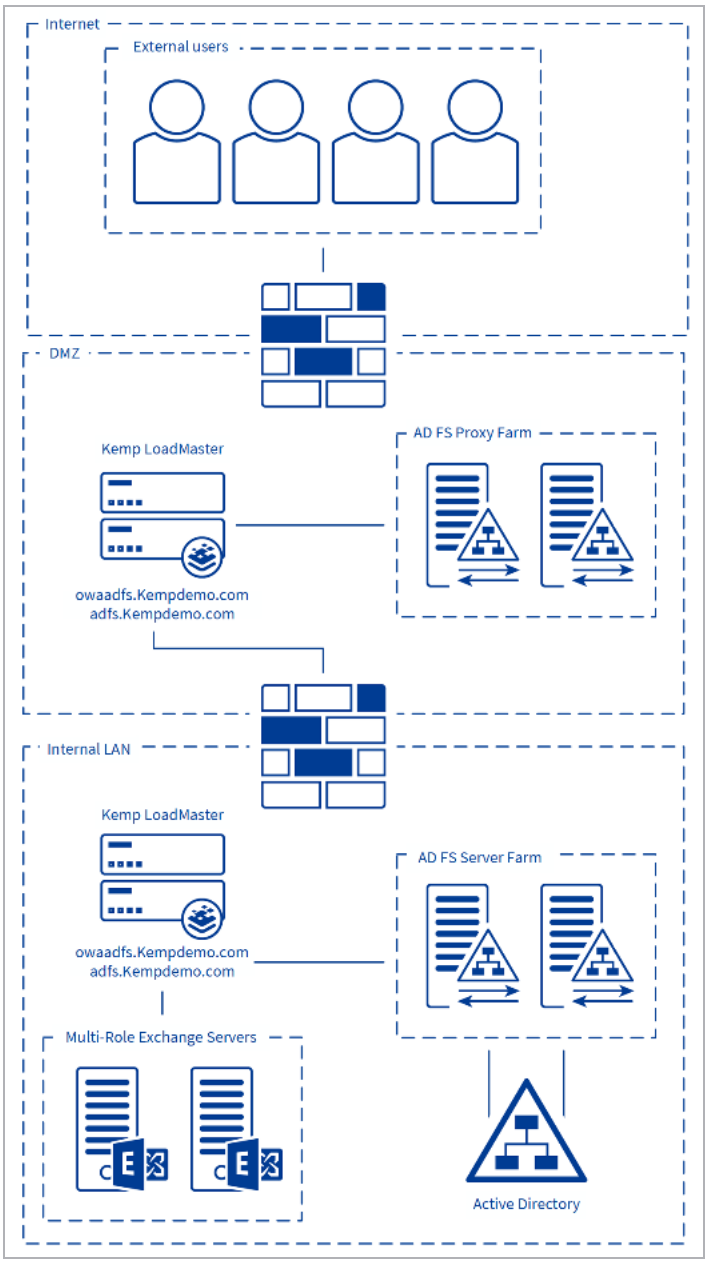
The following diagrams represent the respective environments:


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





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





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

# 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 2.0 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

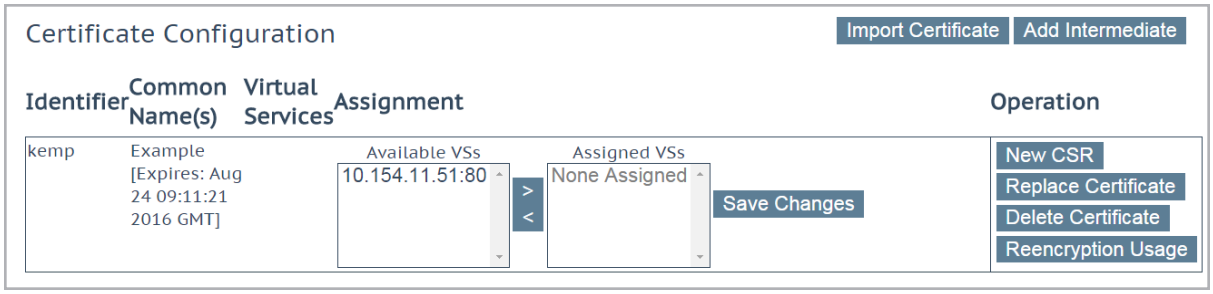
## 4.1 DNS

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

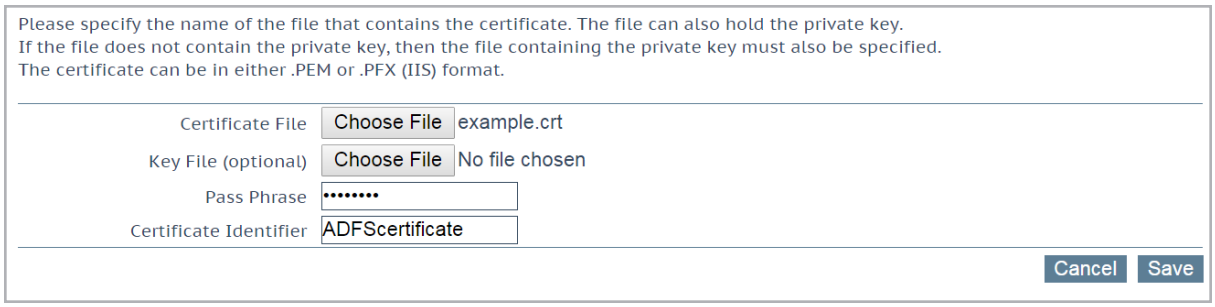
The AD FS SSL certificate has to be imported into the LoadMaster before deployment. To import the certificate, follow the steps below:

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.


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




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 bridging, 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.


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

# 5 Virtual Service (VS) Configuration

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

## 5.1 Template

Kemp has developed a template containing our recommended settings for this workload. You can install this template to help create Virtual Services (VSs) because it automatically populates the settings. You can use the template to easily create the required VSs with the recommended settings. For some workloads, additional manual steps may be required such as assigning a certificate or applying port following. These steps are covered in the document, if needed.

You can remove templates after use and this will not affect deployed services. If needed, you can make changes to any of the VS settings after using the template.

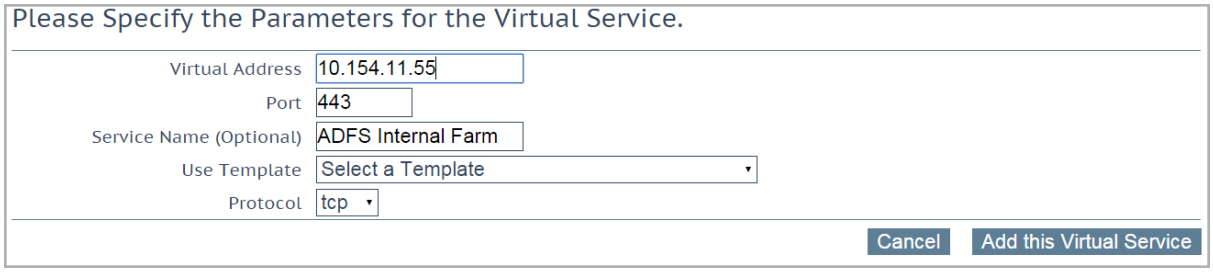
Download released templates from the following page: LoadMaster Templates.

For more information and steps on how to import and use templates, refer to the Virtual Services and Templates, Feature Description on the Kemp Documentation page.

## 5.2 Configure an AD FS Internal Farm Virtual Service

Follow the steps below to configure a VS:

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




3. Enter the **Virtual Address**.


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

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**.
7. Click **Add this Virtual Service**.
8. Configure the settings as recommended in the following table:

| Section | Option | Value | Comment |
|---|---|---|---|
| SSL Properties | SSL Acceleration | Enabled | |
| | Cipher Set | Default | |
| | Reencrypt | Enabled | Set the **Reencryption SNI Hostname** if required. ADFS 3.0 requires the Reencryption SNI Hostname to be set. |
| Standard Options | Persistence Mode | Super HTTP | |
| | Timeout | 1 Hour | |
| | Scheduling Method | least connection | ESP can be enabled if an ESP license is in place. For more information on ESP, refer to the ESP, Feature Description. |

9. Expand the **Real Servers** section.
10. In the first **Real Server Check Parameters** field, select **HTTPS Protocol.**
11. Enter **/federationmetadata/2007-06/federationmetadata.xml** in the URL text box and click the **Set URL** button.
12. Select the **Use HTTP/1.1** check box.
13. Select **GET** as the **HTTP Method**.
14. Click the **Add New...** button.


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

15. 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.

16. In the main menu, click **Certificates & Security** and select **SSL Certificates**.

17. Locate the certificate that was added earlier. In the **Available VSs** field, select the Virtual Service that has just been added and click the right arrow button to assign it.

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

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

20. 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.

21. 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.

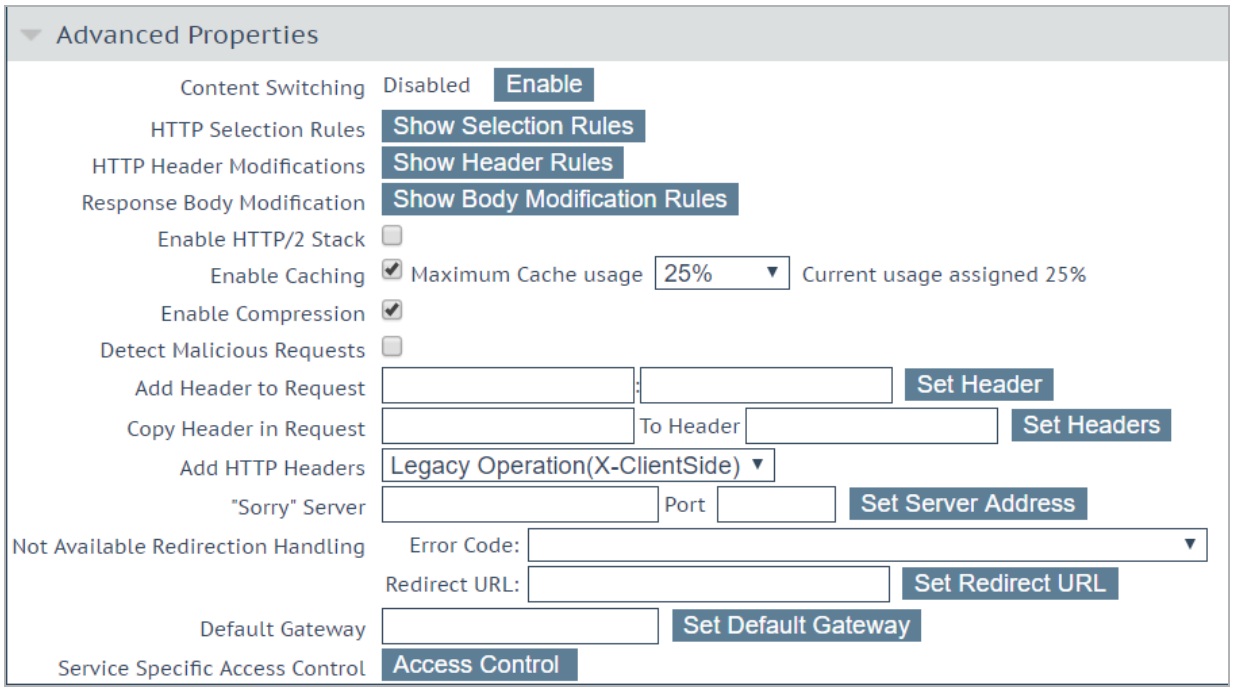
> Login experience is dependent upon the parameters set in the web.config file located on the AD FS servers.

## 5.3 Configure an AD FS Proxy Farm Virtual Service

The steps to set up an AD FS Proxy Farm are almost identical to the ones listed above in the **Configure an AD FS Internal Farm Virtual Service** section. The only difference is, you should give the Virtual Service a different name and follow the steps below:

1. Expand the **Advanced Properties** section.

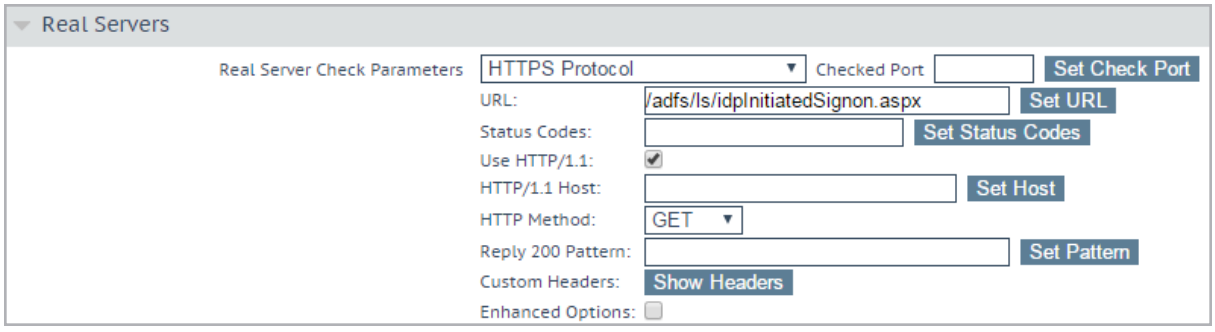

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.




2. Select **Enable Caching**.
3. Select **Enable Compression**.

> The maximum cache usage should be configured dependent upon the number of services on the LoadMaster that are leveraging this feature.

4. Expand the **Real Servers** section.




5. In the first **Real Server Check Parameters** drop-down list, select **HTTPS Protocol**.
6. Enter **/adfs/ls/idpInitiatedSignon.aspx** in the **URL** text box and click **Set URL**.
7. Select **GET** as the **HTTP Method**.


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

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


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

# 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**


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

# Last Updated Date

This document was last updated on 27 July 2023.


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