



Azure Multi-Factor Authentication

Technical Note

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
2 Configure Azure Multi-Factor Authentication	5
2.1 Create a Multi-Factor Authentication Provider in Azure	5
2.2 Install the Multi-Factor Authentication Server on Premises	9
2.3 Add the LoadMaster as a RADIUS Client	11
2.4 Configure the LoadMaster	13
2.4.1 Increase the L7 Authentication Timeout	13
2.4.2 Create a New SSO Domain	14
2.4.3 Configure the ESP Options in the SubVSs	15
References	17
ESP, Feature Description	17
Custom Authentication Form, Technical Note	17
Last Updated Date	18

1 Introduction

Multi-Factor Authentication (MFA) is a method of authentication that requires the use of more than one verification method and adds a critical second layer of security to user sign-ins and transactions. It works by requiring any two or more of the following verification methods:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)
- Something you are (biometrics)

Azure MFA is a method of verifying who you are that requires the use of more than just a username and password. It provides a second layer of security to user sign-ins and transactions.

Azure MFA helps safeguard access to data and applications while meeting user demand for a simple sign-in process. It delivers strong authentication with a range of easy verification options – phone call, text message or mobile app notification – allowing users to choose the method they prefer.

Azure MFA is an easy to use, scalable and reliable solution that provides a second method of authentication so your users are always protected.

The security of multi-factor authentication lies in its layered approach. Comprising multiple authentication factors presents a significant challenge for attackers. Even if an attacker manages to learn the user's password, it is useless without also having possession of the trusted device. Should the user lose the device, the person who finds it will not be able to use it unless they also know the user's password.

1.1 Document Purpose

This document provides step-by-step instructions on how to configure Azure, the MFA server and the Kemp LoadMaster in order to provide multi-factor authentication.

This document uses an Exchange environment as an example scenario.

1.2 Intended Audience

This document is intended to be used by anyone interested in finding out more about using Azure MFA with the Kemp LoadMaster.

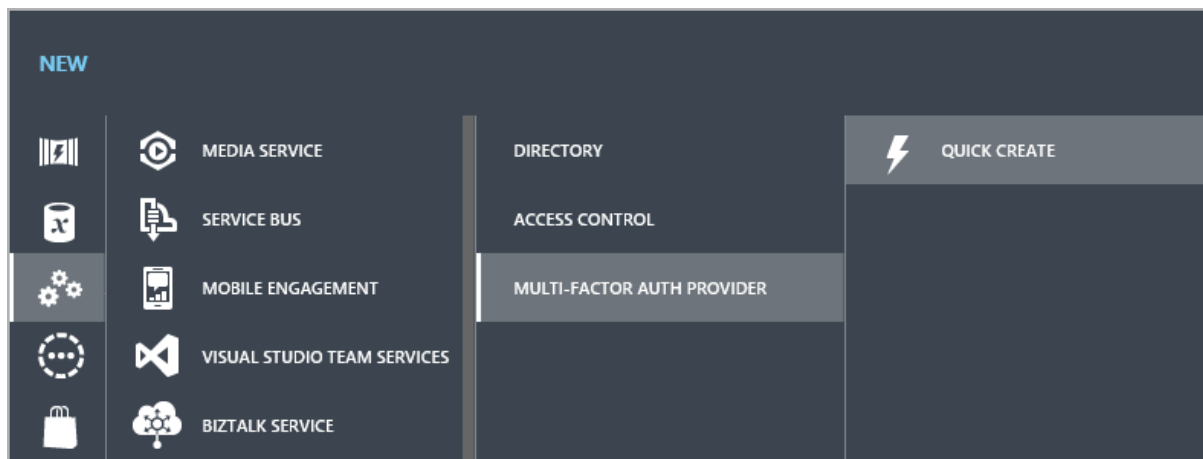
2 Configure Azure Multi-Factor Authentication

Follow the steps in the sections below to configure Azure multi-factor authentication and the Kemp LoadMaster.

2.1 Create a Multi-Factor Authentication Provider in Azure

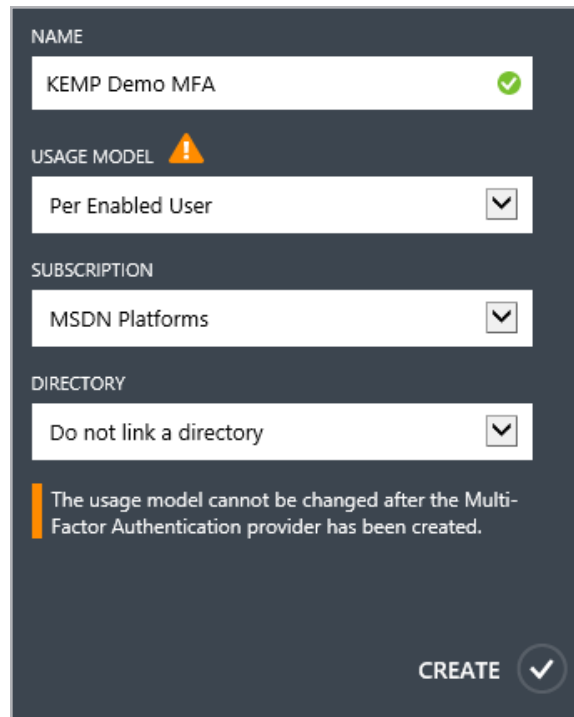
Follow the steps below to create a new multi-factor authentication provider in Azure:

1. Log in to the Azure portal (classic).
2. Go to **ACTIVE DIRECTORY**.



3. Select **NEW**.
4. Select **MULTI-FACTOR AUTH PROVIDER**.
5. Select **QUICK CREATE**.

2 Configure Azure Multi-Factor Authentication



The screenshot shows a configuration form for Azure Multi-Factor Authentication. It has a dark blue background with white text and input fields. The form is divided into sections: NAME, USAGE MODEL, SUBSCRIPTION, and DIRECTORY. The NAME field contains 'KEMP Demo MFA' with a green checkmark. The USAGE MODEL field has a warning icon and contains 'Per Enabled User'. The SUBSCRIPTION field contains 'MSDN Platforms'. The DIRECTORY field contains 'Do not link a directory'. At the bottom, there is a 'CREATE' button with a green checkmark. A warning message is displayed below the DIRECTORY field: 'The usage model cannot be changed after the Multi-Factor Authentication provider has been created.'

NAME

KEMP Demo MFA ✓

USAGE MODEL ⚠

Per Enabled User ▼

SUBSCRIPTION

MSDN Platforms ▼

DIRECTORY

Do not link a directory ▼

The usage model cannot be changed after the Multi-Factor Authentication provider has been created.

CREATE ✓

6. Enter a **NAME** for the authentication provider.
7. Select the **USAGE MODEL**.
8. Select **SUBSCRIPTION**.
9. Leave **DIRECTORY** as the default value.
10. Click **CREATE**.

2 Configure Azure Multi-Factor Authentication

active directory

DIRECTORY

ACCESS CONTROL NAMESPACES

MULTI-FACTOR AUTH PROVIDERS

RIGHTS MANAGEMENT

NAME		STATUS	USAGE MODEL	SUBSCRIPTION
KEMP Demo MFA	→	✓ Active	Per Enabled User	Visual Studio Premium with MSDN

MANAGE

DELETE

11. Once created, select your multi-factor authentication provider and click **MANAGE**.

12. Select **CONFIGURE** on the left.

Configure Settings

Configure your Multi-Factor Authentication settings below.

General Settings

☒ Allow attempts during Multi-Factor Authentication call

☐ Say extension digits when prompting for extension (Server/SDK only)

Caller ID Phone Number

(US phone numbers only)

Two-Way Text Message Timeout Seconds (Server/SDK Only)

One-Time Bypass

Default One-Time Bypass Seconds

Send one-time bypass used notifications to these email addresses

Fraud Alert

☒ Allow users to submit Fraud Alerts

☐ Block user when fraud is reported

Code To Report Fraud During Initial Greeting

Send fraud alert notifications to these email addresses

13. Various options can be configured on this screen, such as:

- The phone number you would like to display when the “phone call” is used as the second factor
- Timeout settings
- Enable/disable features

Downloads Server

Download a copy of the Multi-Factor Authentication Server. Be sure to install directly on the server to be protected.

MULTI-FACTOR AUTHENTICATION SERVER (version 7.0.0) [Release notes](#)

The Multi-Factor Authentication Server supports the following platforms:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008, SP1, SP2
- Windows Server 2003 R2
- Windows Server 2003, SP1, SP2
- Windows 8.1, all editions
- Windows 8, all editions
- Windows 7, all editions
- Windows Vista, all editions, SP1, SP2

[Download](#)

Generate Activation Credentials

[Back](#)

14. Click **Server** underneath the **DOWNLOADS** section on the left.

15. Download the Multi-Factor Authentication Server which will be run in your on-premises data center.

Do not click **Generate Activation Credentials** until you have installed the server on premises and are ready to activate the install. The Activation Credentials are only valid for 10 minutes, at which time you would be required to obtain new credentials.

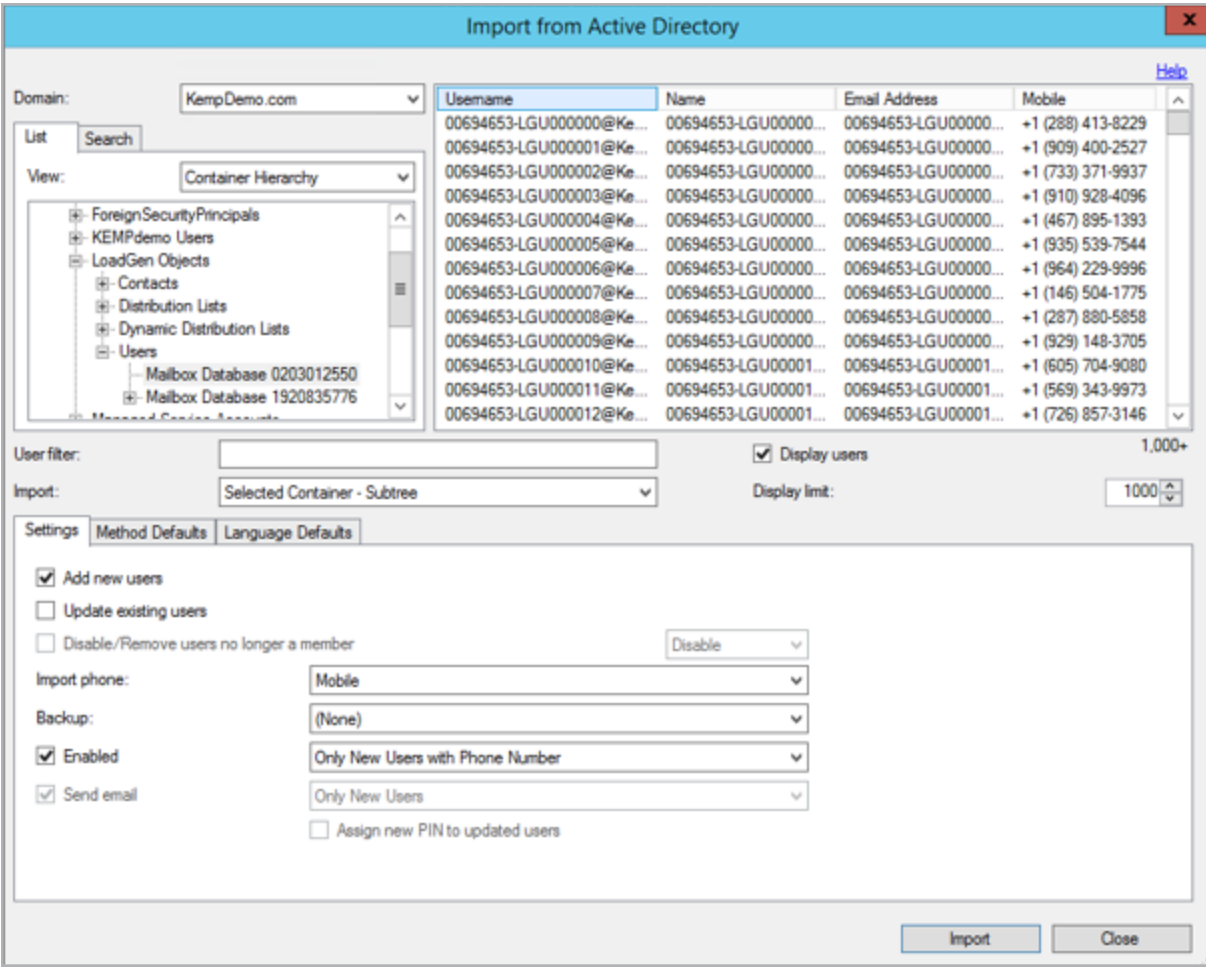
2.2 Install the Multi-Factor Authentication Server on Premises

The MFA server must be a member of the on-premises Active Directory domain. After downloading the MFA server, install it on premises. When prompted, generate the Activation Credentials and enter them in the provided field.

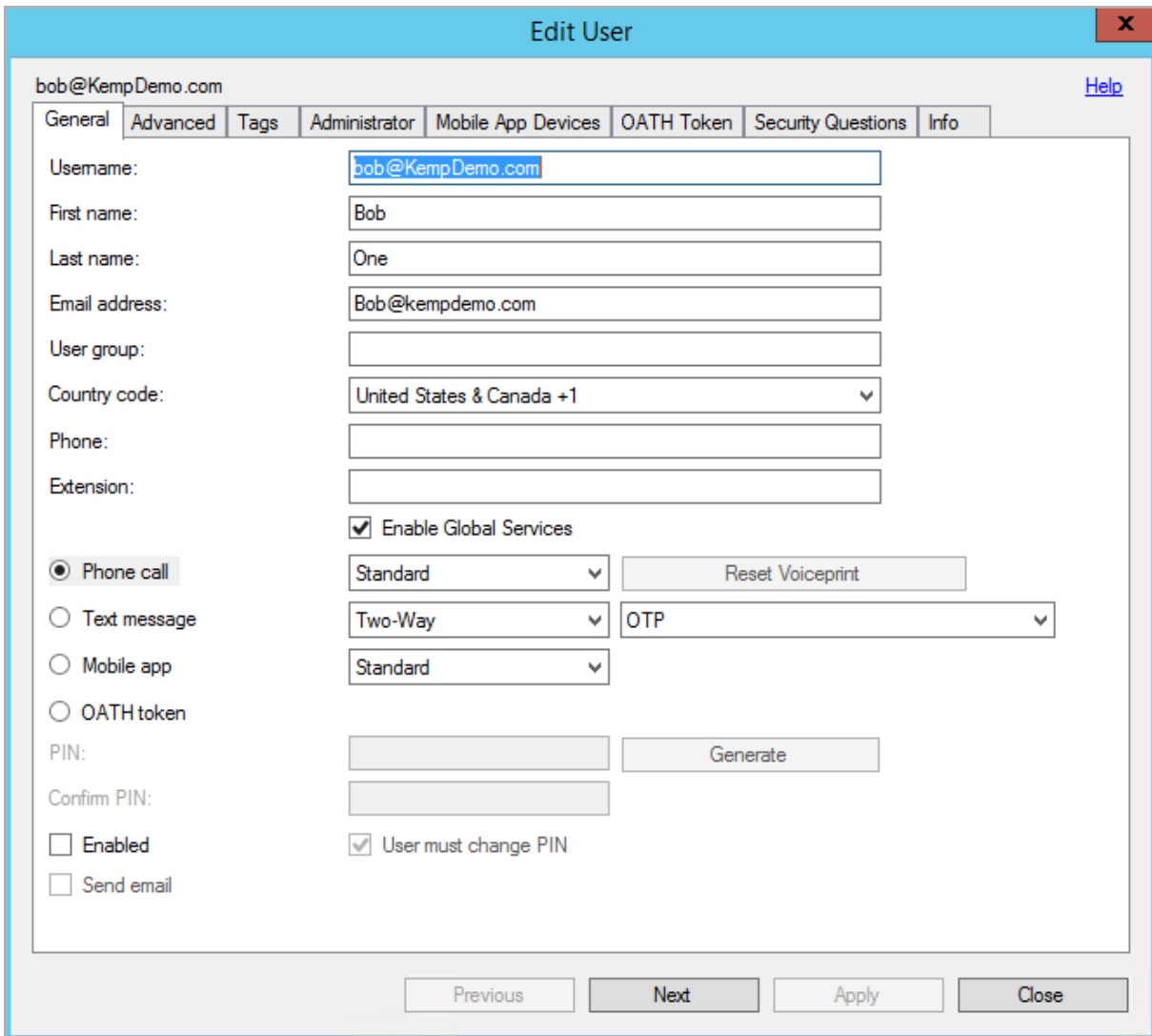
2 Configure Azure Multi-Factor Authentication

Follow the steps below:

- 1. Launch the Multi-Factor Authentication Server console.
- 2. Select **Users**.
- 3. Click **Import from Active Directory**.



- 4. Navigate to the Active Directory Organization Unit you want to import and click **Import**.



bob@KempDemo.com

General Advanced Tags Administrator Mobile App Devices OATH Token Security Questions Info

Username: bob@KempDemo.com

First name: Bob

Last name: One

Email address: Bob@kempdemo.com

User group:

Country code: United States & Canada +1

Phone:

Extension:

☒ Enable Global Services

☒ Phone call Standard Reset Voiceprint

☐ Text message Two-Way OTP

☐ Mobile app Standard

☐ OATH token

PIN: Generate

Confirm PIN:

☐ Enabled ☒ User must change PIN

☐ Send email

Previous Next Apply Close

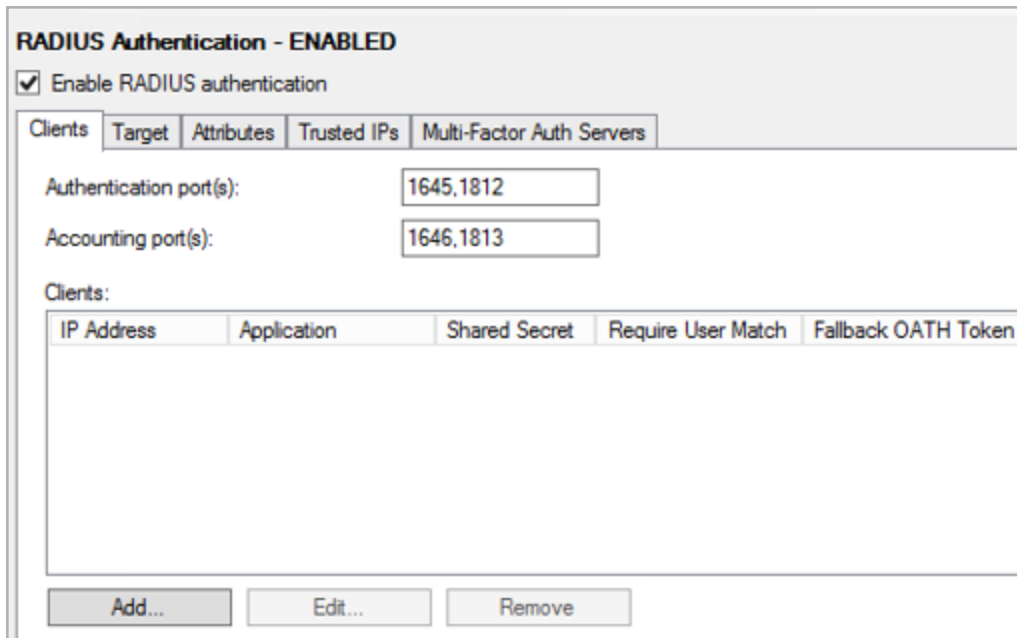
5. Once imported, you can select a user to set authentication methods, etc.

2.3 Add the LoadMaster as a RADIUS Client

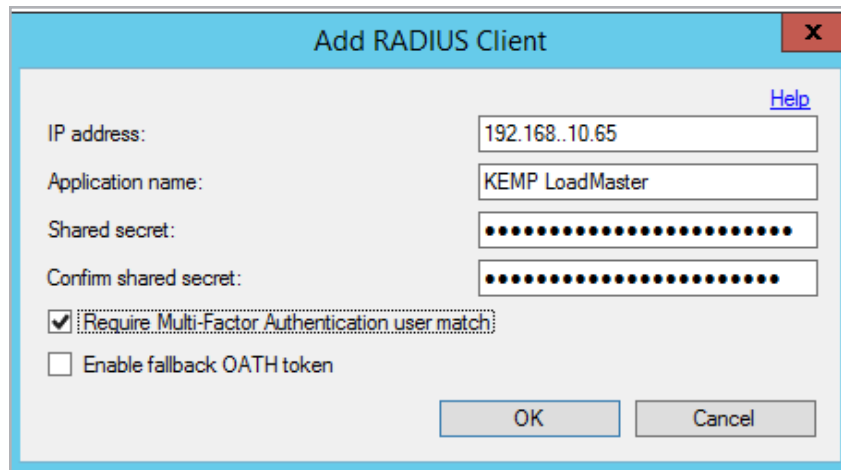
Follow the steps below to add the LoadMaster as a RADIUS client:

1. Select **RADIUS Authentication** within the Azure Multi-Factor Server.

2 Configure Azure Multi-Factor Authentication



2. Select the **Enable RADIUS authentication** check box.
3. Click **Add**.



4. Enter the IP address of the LoadMaster in the **IP address** text box.
5. Enter an **Application name**.
6. Enter a new **Shared secret** password and confirm it in the text boxes provided.
7. Select the **Require Multi-Factor Authentication user match** check box.

2.4 Configure the LoadMaster

Follow the steps in the sub-sections below to configure the LoadMaster.

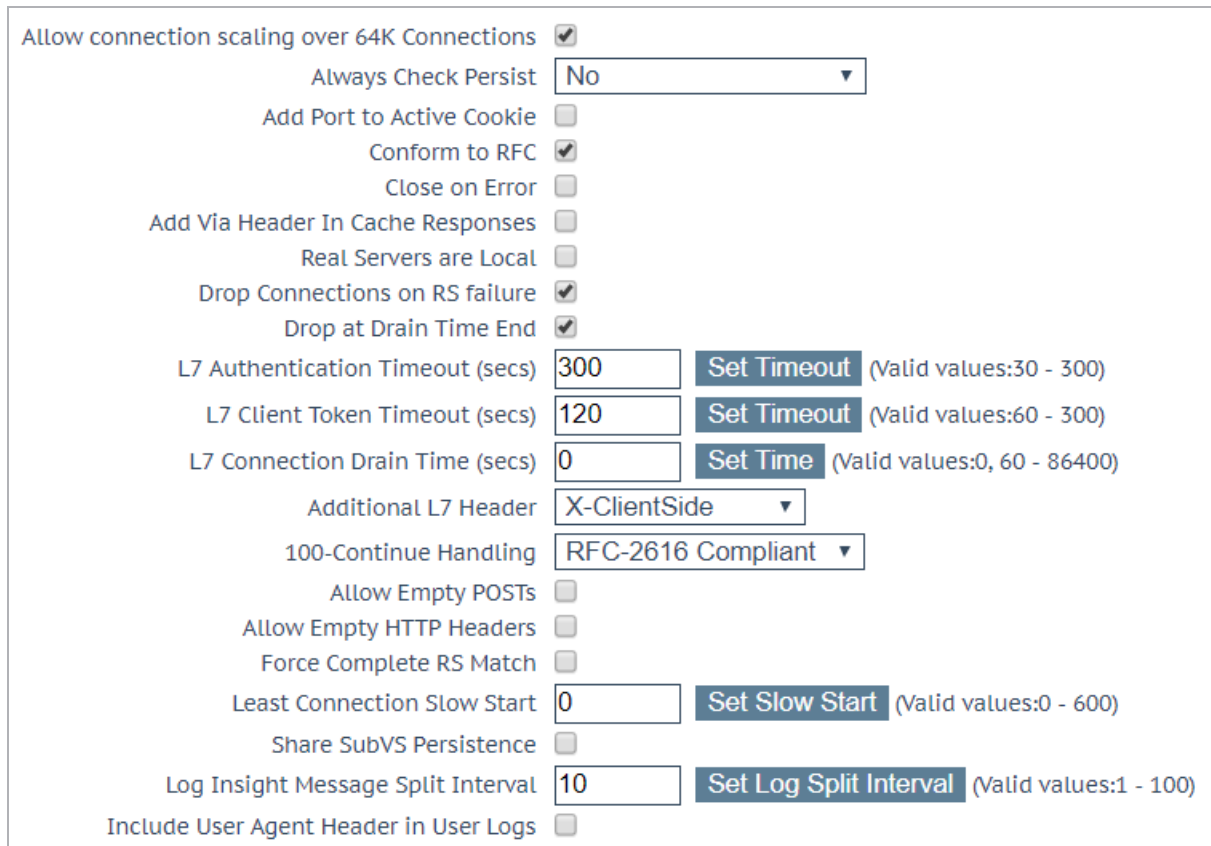
2.4.1 Increase the L7 Authentication Timeout

The L7 Authentication Timeout should be increased in order to provide enough time for the following actions to occur:

- The user enters their credentials
- Azure MFA communicates with the service in the cloud
- The service in the cloud sends the authentication to the user's phone (by app or phone call)

To increase the L7 Authentication Timeout, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **System Configuration > Miscellaneous Options > L7 Configuration**.



The screenshot shows the 'L7 Configuration' page in the LoadMaster WUI. It contains various settings for L7 connections, including checkboxes for connection scaling, persistency, and RFC compliance, as well as input fields for timeouts and drain times. The 'L7 Authentication Timeout (secs)' is currently set to 300, and the 'L7 Client Token Timeout (secs)' is set to 120. The 'L7 Connection Drain Time (secs)' is set to 0. There are also buttons for 'Set Timeout', 'Set Time', and 'Set Slow Start'.

Allow connection scaling over 64K Connections	<input checked="" type="checkbox"/>
Always Check Persist	No
Add Port to Active Cookie	<input type="checkbox"/>
Conform to RFC	<input checked="" type="checkbox"/>
Close on Error	<input type="checkbox"/>
Add Via Header In Cache Responses	<input type="checkbox"/>
Real Servers are Local	<input type="checkbox"/>
Drop Connections on RS failure	<input checked="" type="checkbox"/>
Drop at Drain Time End	<input checked="" type="checkbox"/>
L7 Authentication Timeout (secs)	300 Set Timeout (Valid values:30 - 300)
L7 Client Token Timeout (secs)	120 Set Timeout (Valid values:60 - 300)
L7 Connection Drain Time (secs)	0 Set Time (Valid values:0, 60 - 86400)
Additional L7 Header	X-ClientSide
100-Continue Handling	RFC-2616 Compliant
Allow Empty POSTs	<input type="checkbox"/>
Allow Empty HTTP Headers	<input type="checkbox"/>
Force Complete RS Match	<input type="checkbox"/>
Least Connection Slow Start	0 Set Slow Start (Valid values:0 - 600)
Share SubVS Persistence	<input type="checkbox"/>
Log Insight Message Split Interval	10 Set Log Split Interval (Valid values:1 - 100)
Include User Agent Header in User Logs	<input type="checkbox"/>

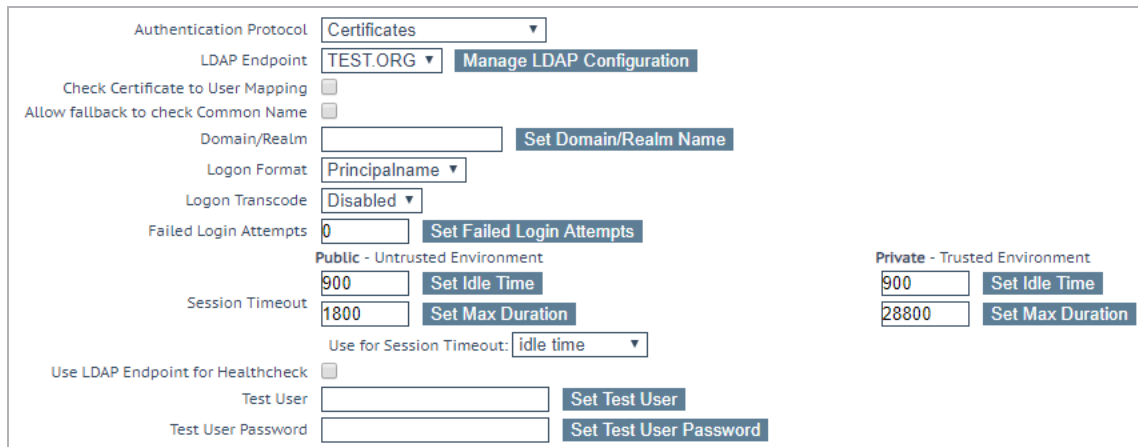
2. Enter the **L7 Authentication Timeout** and click **Set Timeout**.

2 Configure Azure Multi-Factor Authentication

Kemp recommends 300 seconds but this can be adjusted as needed to meet requirements.

You can also adjust the SSO LDAP server timeout by following the steps below:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Manage SSO > Modify**.



2. Configure the **Public Session Timeout** and click **Set Idle Time**.

2.4.2 Create a New SSO Domain

Follow the steps below to create a new SSO domain:

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



2. Enter a name in the **Add new Client Side Configuration** text box and click **Add**.

2 Configure Azure Multi-Factor Authentication

Domain AZUREMFA

Authentication Protocol
RADIUS

RADIUS Server(s)
192.168.10.82
Set RADIUS Server(s)

RADIUS Shared Secret

Set Shared Secret

Send NAS Identifier
☒

RADIUS NAS Identifier
b100
Set NAS Identifier

Domain/Realm
kempdemo.com
Set Domain/Realm Name

Logon Format (Phase 1 RADIUS)
Principalname

Logon Format (Phase 2 Real Server)
Principalname

Logon Transcode
Disabled

Failed Login Attempts
0
Set Failed Login Attempts

Public - Untrusted Environment
900
Set Idle Time
1800
Set Max Duration

Private - Trusted Environment
900
Set Idle Time
28800
Set Max Duration

Use for Session Timeout:
idle time

Test User
Set Test User

Test User Password
Set Test User Password

3. Select **RADIUS** as the **Authentication Protocol**.
4. Enter the IP address of the MFA Server in the **RADIUS server(s)** text box and click **Set RADIUS Server(s)**. Multiple addresses can be entered in this text box, if required.
5. Enter the **RADIUS Shared Secret**, which was created in the MFA configuration earlier, and click **Set Shared Secret**.
6. Enter the **Domain/Realm** and click **Set Domain/Realm Name**.

2.4.3 Configure the ESP Options in the SubVSs

Our example is based on using an Exchange environment. For this example scenario, the Edge Security Pack (ESP) Options for the OWA and Authentication Proxy SubVSs need to be configured. To do this, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > View/Modify Services**.
2. Click **Modify** on the relevant Virtual Service.
3. Expand the **ESP Options** section.

2 Configure Azure Multi-Factor Authentication

▼ ESP Options

Enable ESP ☒

ESP Logging User Access: ☒ Security: ☒ Connection: ☒

Client Authentication Mode

SSO Domain

Allowed Virtual Hosts [Set Allowed Virtual Hosts](#)

Allowed Virtual Directories [Set Allowed Directories](#)

Pre-Authorization Excluded Directories [Set Excluded Directories](#)

Permitted Groups [Set Permitted Groups](#)

SSO Image Set

SSO Greeting Message [Set SSO Greeting Message](#)

Logoff String [Set SSO Logoff String](#)

Display Public/Private Option ☒

Use Session or Permanent Cookies

Server Authentication Mode

4. Select **Form Based** as the **Client Authentication Mode**.
5. Select the **SSO Domain** that was created in the previous section.

6. Configure any of the other settings as needed.

You may want to configure a custom **SSO Image Set** to inform users that MFA will be required. For further information on doing this, please refer to the [Custom Authentication Form, Technical Note](#).

7. Repeat the steps above to configure the other SubVS.

For further information on configuring the LoadMaster to work with Exchange, refer to the relevant Exchange Deployment Guide. For further information on ESP, refer to the [ESP, Feature Description](#).

References

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

ESP, Feature Description

Custom Authentication Form, Technical Note

Last Updated Date

This document was last updated on 27 July 2023.