# Azure Multi-Factor Authentication

## Technical Note

UPDATED: 19 March 2021

## Copyright Notices

# Table of Contents

**1 Introduction** 4

1.1 Document Purpose 4

1.2 Intended Audience 4

1.3 Related Firmware Version 5

**2 Configure NPS Settings to Accept Requests from the LoadMaster** 6

**3 Configure the LoadMaster** 7

3.1 Increase the L7 Authentication Timeout 7

3.2 Create a New SSO Domain 8

3.3 Configure the ESP Options in the SubVSs 9

**References** 11

ESP, Feature Description 11

Custom Authentication Form, Technical Note 11

**Last Updated Date** 12

# 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.

## 1.3 Related Firmware Version

Published with LMOS version 7.2.48.4 LTS. This document has not required substantial changes since 7.2.48.4 LTS. However, the content is in sync with the latest LoadMaster LTS firmware.

# 2 Configure NPS Settings to Accept Requests from the LoadMaster

The Network Policy Server (NPS) extension for Azure Multi-Factor Authentication (MFA) adds cloud-based MFA capabilities to your authentication infrastructure using your existing servers. For more information, refer to the Integrate your existing NPS infrastructure with Azure Multi-Factor Authentication page.

You must create a RADIUS client so that the LoadMaster can authenticate. For more information, refer to the RADIUS Authentication and Authorization Technical Note.

# 3 Configure the LoadMaster

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

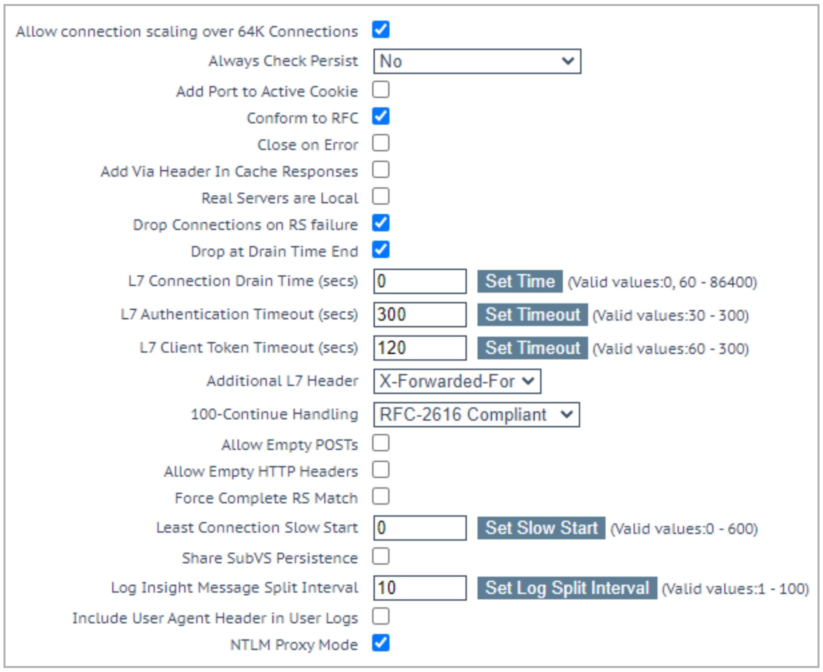
## 3.1 Increase the L7 Authentication Timeout

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**.



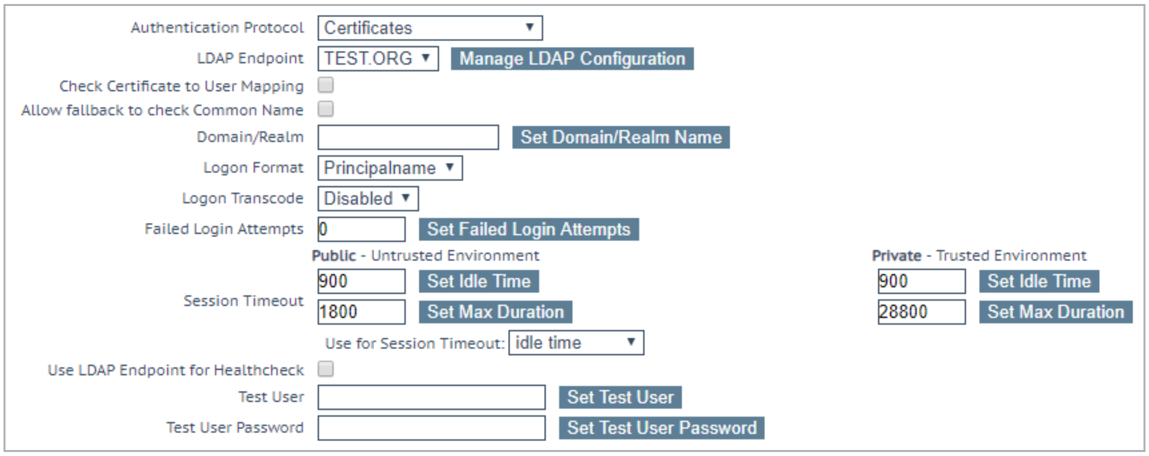
| | | | |
|---|---|---|---|
| Allow connection scaling over 64K Connections | ☑ | | |
| Always Check Persist | No | | |
| Add Port to Active Cookie | □ | | |
| Conform to RFC | ☑ | | |
| Close on Error | □ | | |
| Add Via Header In Cache Responses | □ | | |
| Real Servers are Local | □ | | |
| Drop Connections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

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

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**.



Authentication Protocol: Certificates

LDAP Endpoint: TEST.ORG

Check Certificate to User Mapping: □

Allow fallback to check Common Name: □

Domain/Realm:

Logon Format: Principalname

Logon Transcode: Disabled

Failed Login Attempts: 0

Session Timeout:

| | Public - Untrusted Environment | Private - Trusted Environment |
|---|---|---|
| Idle Time | 900 | 900 |
| Max Duration | 1800 | 28800 |

Use for Session Timeout: idle time

Use LDAP Endpoint for Healthcheck: □

Test User:

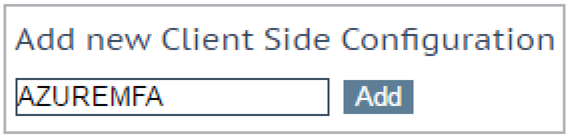
Test User Password:

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

## 3.2 Create a New SSO Domain

Follow the steps below to create a new SSO domain:

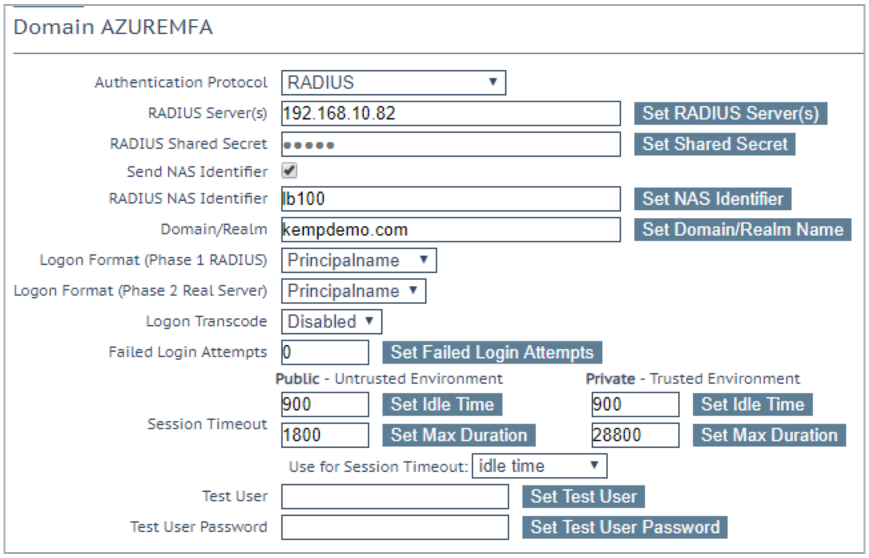
1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Manage SSO**.



Add new Client Side Configuration

AZUREMFA

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



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 | lb100 | 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 |

Session Timeout

| | Public - Untrusted Environment | | Private - Trusted Environment | |
|---|---|---|---|---|
| | 900 | Set Idle Time | 900 | Set Idle Time |
| | 1800 | Set Max Duration | 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**.

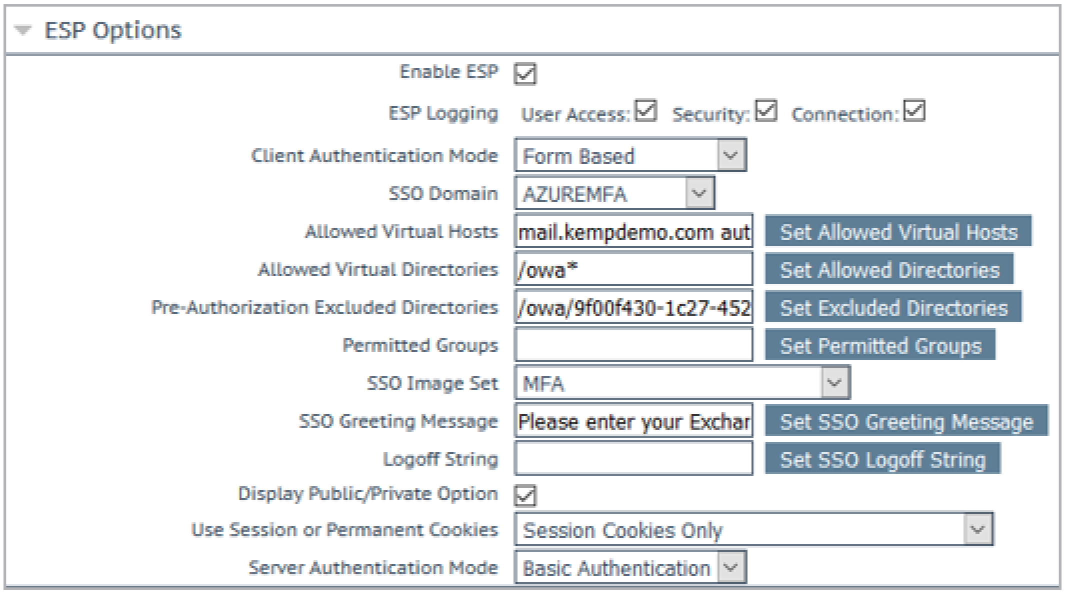
## 3.3 Configure the ESP Options in the SubVSs

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.



ESP Options

| | |
|---|---|
| Enable ESP | ☑ |
| ESP Logging | User Access: ☑ Security: ☑ Connection: ☑ |
| Client Authentication Mode | Form Based |
| SSO Domain | AZUREMFA |
| Allowed Virtual Hosts | mail.kempdemo.com aut |
| Allowed Virtual Directories | /owa* |
| Pre-Authorization Excluded Directories | /owa/9f00f430-1c27-452 |
| Permitted Groups | |
| SSO Image Set | MFA |
| SSO Greeting Message | Please enter your Exchar |
| Logoff String | |
| Display Public/Private Option | ☑ |
| Use Session or Permanent Cookies | Session Cookies Only |
| Server Authentication Mode | Basic Authentication |

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 19 March 2021.