



Technical Note Azure Multi Factor Authentication

8 January 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: [Product Documentation Copyright Notice & Trademarks | Progress](#)

Table of Contents

Chapter 1: Introduction. 4

 Document Purpose. 5

 Intended Audience. 5

Chapter 2: Configure NPS Settings to Accept Requests from the LoadMaster. 6

Chapter 3: Configure the LoadMaster. 7

 Increase the L7 Authentication Timeout. 7

 Create a New SSO Domain. 9

 Configure the ESP Options in the SubVSs. 10

Chapter 4: References. 12

Introduction

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.

Related Links

- [Document Purpose](#)

- [Intended Audience](#)

Document Purpose

Document Purpose

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

This document uses an Exchange environment as an example scenario.

Intended Audience

Intended Audience

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

Configure NPS Settings to Accept Requests from the LoadMaster

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](#).

Configure the LoadMaster

Configure the LoadMaster

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

Related Links

- [Increase the L7 Authentication Timeout](#)
- [Create a New SSO Domain](#)
- [Configure the ESP Options in the SubVSs](#)

Increase the L7 Authentication Timeout

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	<input type="checkbox"/>	
Always Check Persist	<input type="text" value="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 type="checkbox"/>	
Drop at Drain Time End	<input type="checkbox"/>	
L7 Connection Drain Time (secs)	<input type="text" value="300"/>	Set Time (Valid values:0 - 86400)
L7 Authentication Timeout (secs)	<input type="text" value="30"/>	Set Timeout (Valid values:30 - 300)
L7 Wait after POST(ms)	<input type="text" value="2000"/>	Set Post Wait (Valid values:1 - 2000)
L7 Client Token Timeout (secs)	<input type="text" value="120"/>	Set Timeout (Valid values:60 - 300)
Additional L7 Header	<input type="text" value="X-Forwarded-For"/>	▼
100-Continue Handling	<input type="text" value="RFC-7231 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	<input type="text" value="0"/>	Set Slow Start (Valid values:0 - 600)
Share SubVS Persistence	<input type="checkbox"/>	
Log Insight Message Split Interval	<input type="text" value="10"/>	Set Log Split Interval (Valid values:1 - 100)
Include User Agent Header in User Logs	<input type="checkbox"/>	
Use CEF Log Format	<input type="checkbox"/>	
SSO Maximum Threads	<input type="text" value="128"/>	Set SSO Max Threads (Valid values:64 - 512)
NTLM Proxy Mode	<input checked="" type="checkbox"/>	

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

We recommend 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	<input type="text" value="Certificates"/>	
LDAP Endpoint	<input type="text" value="TEST.ORG"/>	Manage LDAP Configuration
Check Certificate to User Mapping	<input type="checkbox"/>	
Allow fallback to check Common Name	<input type="checkbox"/>	
Domain/Realm	<input type="text"/>	Set Domain/Realm Name
Logon Format	<input type="text" value="Principalname"/>	
Logon Transcode	<input type="text" value="Disabled"/>	
Failed Login Attempts	<input type="text" value="0"/>	Set Failed Login Attempts
Public - Untrusted Environment		
Session Timeout	<input type="text" value="900"/>	Set Idle Time
	<input type="text" value="1800"/>	Set Max Duration
	Use for Session Timeout:	<input type="text" value="idle time"/>
Use LDAP Endpoint for Healthcheck	<input type="checkbox"/>	
Test User	<input type="text"/>	Set Test User
Test User Password	<input type="text"/>	Set Test User Password

Private - Trusted Environment		
	<input type="text" value="900"/>	Set Idle Time
	<input type="text" value="28800"/>	Set Max Duration

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

Create a New SSO Domain

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

[Add](#)

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

Domain AZUREMFA

Authentication Protocol	<input type="text" value="RADIUS"/>	
RADIUS Server(s)	<input type="text" value="192.168.10.82"/>	<input type="button" value="Set RADIUS Server(s)"/>
RADIUS Shared Secret	<input type="text" value="....."/>	<input type="button" value="Set Shared Secret"/>
Send NAS Identifier	<input checked="" type="checkbox"/>	
RADIUS NAS Identifier	<input type="text" value="lb100"/>	<input type="button" value="Set NAS Identifier"/>
Domain/Realm	<input type="text" value="kempdemo.com"/>	<input type="button" value="Set Domain/Realm Name"/>
Logon Format (Phase 1 RADIUS)	<input type="text" value="Principalname"/>	
Logon Format (Phase 2 Real Server)	<input type="text" value="Principalname"/>	
Logon Transcode	<input type="text" value="Disabled"/>	
Failed Login Attempts	<input type="text" value="0"/>	<input type="button" value="Set Failed Login Attempts"/>
	Public - Untrusted Environment	Private - Trusted Environment
	<input type="text" value="900"/>	<input type="text" value="900"/>
	<input type="button" value="Set Idle Time"/>	<input type="button" value="Set Idle Time"/>
Session Timeout	<input type="text" value="1800"/>	<input type="text" value="28800"/>
	<input type="button" value="Set Max Duration"/>	<input type="button" value="Set Max Duration"/>
	Use for Session Timeout:	<input type="text" value="idle time"/>
Test User	<input type="text"/>	<input type="button" value="Set Test User"/>
Test User Password	<input type="text"/>	<input type="button" value="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**.

Configure the ESP Options in the SubVSs

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	<input checked="" type="checkbox"/>	
ESP Logging	User Access: <input checked="" type="checkbox"/> Security: <input checked="" type="checkbox"/> Connection: <input checked="" type="checkbox"/>	
Client Authentication Mode	Form Based	<input type="button" value="Set Allowed Virtual Hosts"/>
SSO Domain	AZUREMFA	<input type="button" value="Set Allowed Directories"/>
Allowed Virtual Hosts	mail.kempdemo.com aut	<input type="button" value="Set Excluded Directories"/>
Allowed Virtual Directories	/owa*	<input type="button" value="Set Permitted Groups"/>
Pre-Authorization Excluded Directories	/owa/9f00f430-1c27-452	
Permitted Groups		
SSO Image Set	MFA	<input type="button" value="Set SSO Greeting Message"/>
SSO Greeting Message	Please enter your Exchar	<input type="button" value="Set SSO Logoff String"/>
Logoff String		
Display Public/Private Option	<input checked="" type="checkbox"/>	
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

References

Unless otherwise specified, the following documents can be found at <https://docs.progress.com/>.

ESP, Feature Description

Custom Authentication Form, Technical Note