

Azure Multi-Factor Authentication

Technical Note

UPDATED: 28 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 Configure NPS Settings to Accept Requests from the LoadMaster **5**

3 Configure the LoadMaster **6**

3.1 Increase the L7 Authentication Timeout 6

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**

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

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.

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

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.

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

3 Configure the LoadMaster

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

3.1 Increase the L7 Authentication Timeout

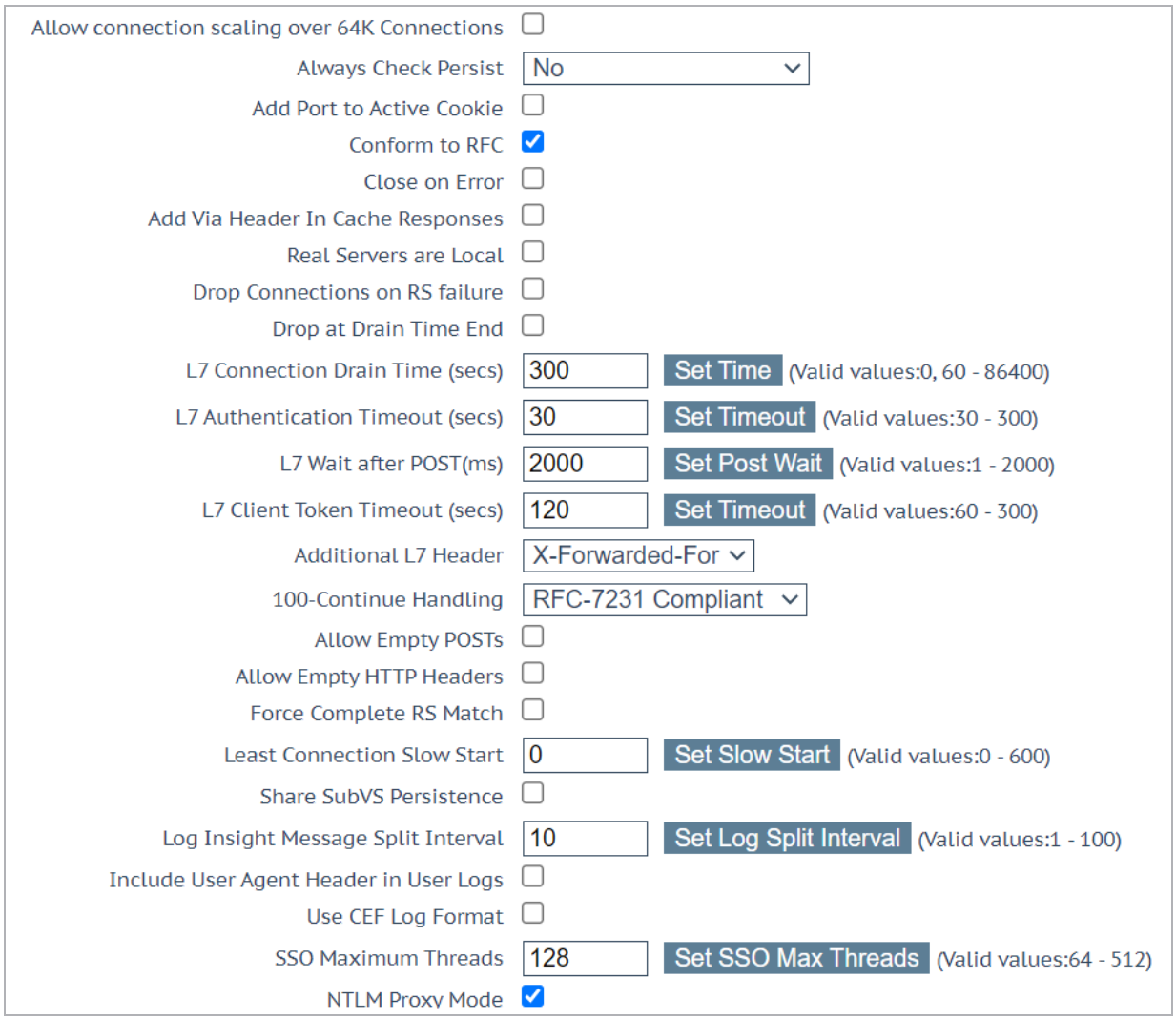
The L7 Authentication Timeout should be increased in order to provide enough time for the following actions to occur:

- 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**.

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



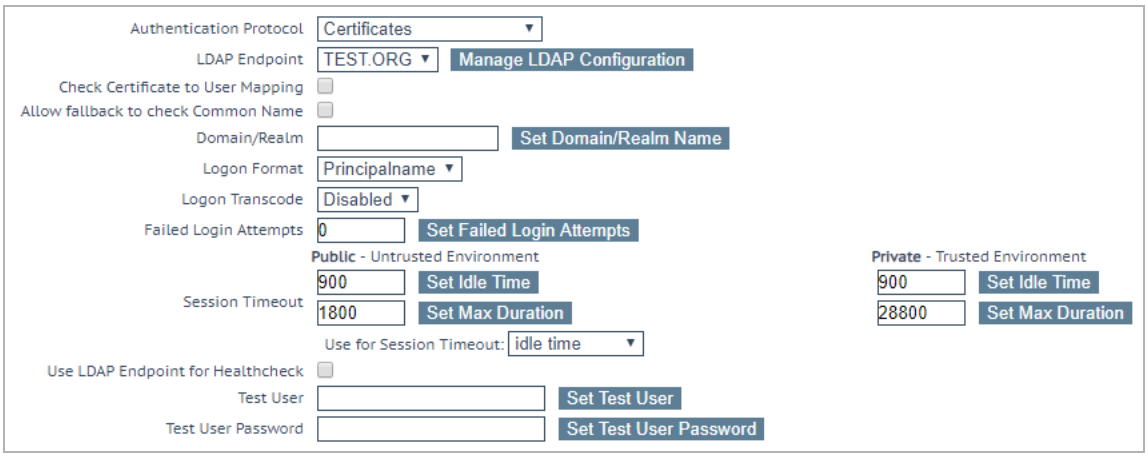
2. Enter the **L7 Authentication Timeout** and click **Set Timeout**.

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**.

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



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

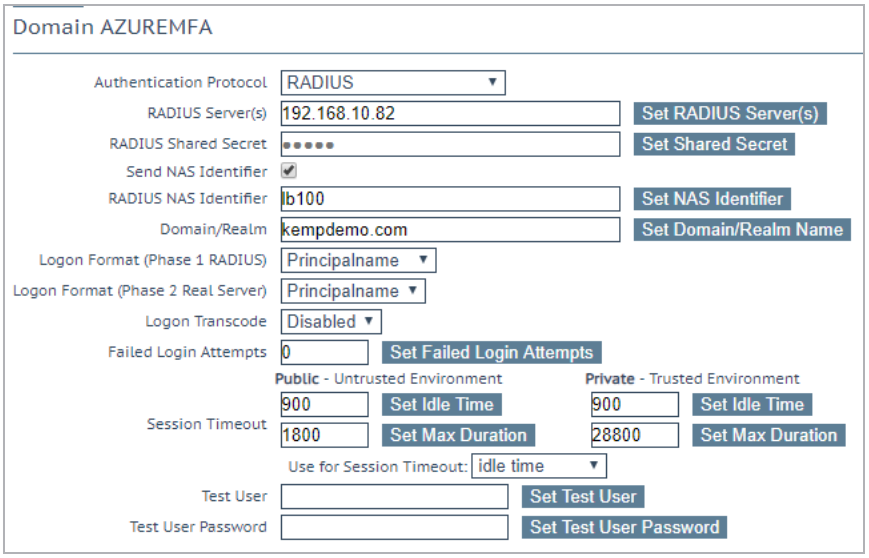
3.2 Create a New SSO Domain

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**.



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



3. Select **RADIUS** as the **Authentication Protocol**.

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

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**.

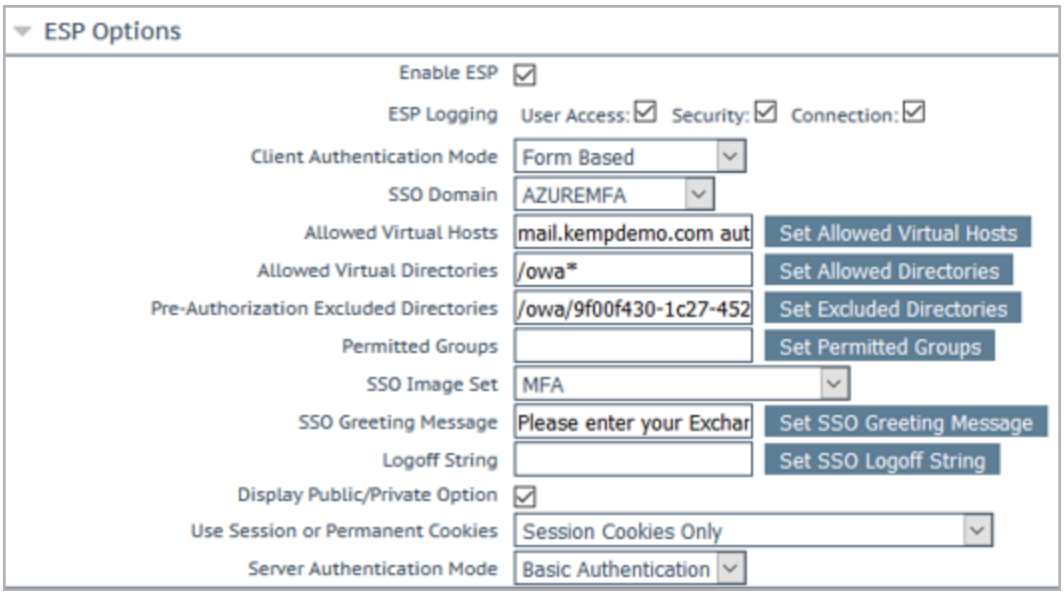
3.3 Configure the ESP Options in the SubVSs

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.



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

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

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.

© 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

Custom Authentication Form, Technical Note

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

Last Updated Date

This document was last updated on 28 July 2023.

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