Authlogics and Office 365

ADFS Integration Guide

Product Version: 4.0

Publication date: August 2020

Call us on:	+44 1344 568 900 (UK/EMEA) +1 408 706 2866 (US)
Email us:	sales@authlogics.com

Table of Contents

Introduction

Authlogics MFA integrates seamlessly with Office 365 via the Authlogics ADFS agent. By leveraging ADFS the solution is fully compliant with Microsoft's preferred and supported architecture.

Prerequisites

1. Active Directory (on-prem/private cloud) configured with DirSync to Office 365 with Azure AD Connect.
2. ADFS Server or Farm and federation configured for use with Office 365.
    a. https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/set-up-adfs-for-single-sign-on
    b. Although a minimum of ADFS 2.0 is required for basic Office 365 Federation, a minimum of ADFS 3.0 is required for hybrid modern authentication (step 4) although Authlogics recommends ADFS 5.0 for maximum flexibility.
3. Ensure that Exchange Clients are Modern Authentication capable.
    a. https://docs.microsoft.com/en-us/microsoft-365/enterprise/modern-auth-for-office-2013-and-2016
4. Ensure Exchange Servers are at least Exchange Server 2013 CU19 for hybrid modern authentication deployments.
    a. https://docs.microsoft.com/en-us/microsoft-365/enterprise/hybrid-modern-auth-overview
5. Configure Exchange for Modern Authentication
    a. https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/enable-or-disable-modern-authentication-in-exchange-online

Deployment

Once the prerequisites are in place and the infrastructure is fully working with Modern Authentication using username + password for Office Desktop and Mobile apps then MFA can be deployed.

Firstly, an Authlogics Authentication Server must be deployed in the Active Directory and users must be provisioned for Authlogics MFA. The Authlogics Authentication Server Installation and Configuration Guide should be followed to ensure the correct deployment of the Authentication Server.

Finally, the Authlogics ADFS Agent can be deployed on the ADFS server. Once installed it must be explicitly enabled for used in ADFS and relying parties. The Authlogics ADFS Integration Guide includes detailed instructions for each version of ADFS that may be used.

Application / Relying party Configuration

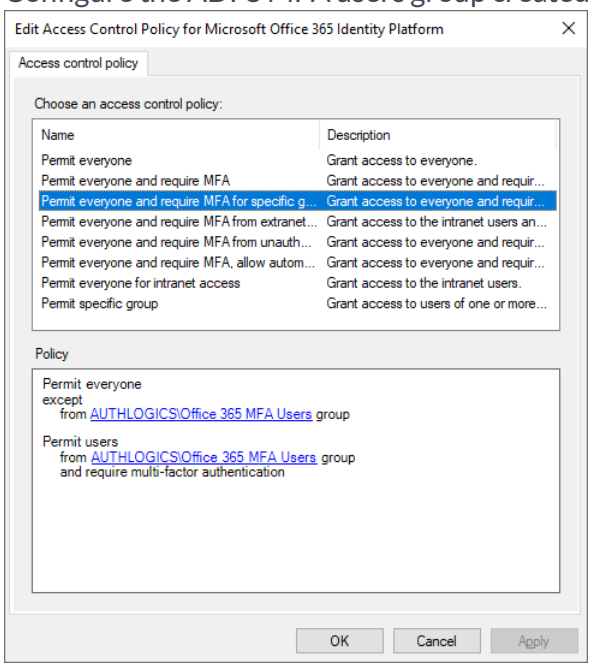
You can configure multiple ways for users to access applications via ADFS, depending on your deployment strategy. Common approaches are as follows:

(1) All users must use MFA for all applications.
(2) All users of specific applications must use MFA.
(3) Only members of a specific AD group can access an application and must use MFA.
(4) Users of specific applications do NOT require MFA, except members of an AD group must use MFA.

Option 1 is an ideal end goal from a security perspective however when planning a gradual deployment of MFA users' option 4 may be more suitable.

Configuring ADFS for gradual user migration

(1) Create an AD group for ADFS MFA users.
(2) Configure **Forms Authentication** as a Primary authentication method.
(3) Configure **Authlogics ADFS Agent** as an Additional authentication method.
    Tip: For ADFS 5.0 select the *Allow additional authentication providers as primary* box to use the updated login page layout.
(4) Edit the Access Control Policy for each application you want to implement a gradual user migration and select the "Permit everyone and require MFA for specific group" access control policy.
(5) Configure the ADFS MFA users group created in step 1.



(6) After a user has been provisioned for MFA simply add them to the ADFS MFA users group. Users who are not in the ADFS MFA users can still logon with their AD username and password.
(7) When all users of the application have been setup for MFA change the Access Control Policy to "Permit everyone and require MFA", or another appropriate access control policy that does not use the exception group.