Authlogics Exchange Agent Integration Guide

With PINgrid, PINphrase & PINpass Technology

Product Version: 3.3.5820.0

Publication date: March 2020

Authlogics, 12th Floor, Ocean House, The Ring, Bracknell, Berkshire, RG12 1AX, United Kingdom
UK Tel: +44 1344 568 900 US Tel: +1 857 214 2174 email: info@authlogics.com web: http://authlogics.com/

Table of Contents

Introduction

Authlogics Authentication Server is a multi-factor authentication system which provides:

- Token and token-less multi-factor authentication.
- Award winning transaction signing / verification technology.
- Self-service password reset and unlocking.
- Web Service API and RADIUS interfaces for connectivity.
- Authentication technologies:
    - PINgrid Pattern Based Authentication.
    - PINphrase Random Character Authentication
    - PINpass OATH (TOTP) Compliant Authentication

This guide includes details for integrating Authlogics with Microsoft Exchange Server via the web interface. Integrating Authlogics with Microsoft Exchange is an ideal way to add strong authentication to Outlook Web App and Exchange Admin Centre.

Licensing

Authlogics Exchange Agent is free of charge however may only be used with a correctly licenced Authlogics Authentication Server.

> **Note**
> For detailed information on the licence types please refer to the licence agreement document embedded within the installation package.

Design and Deployment Scenarios

The Authlogics Exchange Agent has been designed to be installed directly onto the Exchange server hosting the web based logon page.

The installation will integrate the agent directly into IIS on the Exchange Server.

Minimum Requirements

The Authlogics Exchange Agent has been designed to work with Microsoft Exchange Server 2013, 2016 and 2019 Mailbox and CAS servers.

The minimum supported .NET Framework version is 4.6.1, thus the agent requires the minimum of the following Exchange updates:

- Exchange 2013 – Cumulative Update 13
- Exchange 2016 – Cumulative Update 3
- Exchange 2019 – N/A

For further details about .NET and Exchange version compatibility see the following Microsoft article: https://docs.microsoft.com/en-us/exchange/plan-and-deploy/supportability-matrix?view=exchserver-2019#microsoft-net-framework

Deployment

The following deployment overview walks through the installation process for deploying the Authlogics Exchange Agent.

Overview

This deployment section assumes that at least one Authlogics Authentication Server has already been installed and is functional. See the Authlogics Authentication Server Installation and Configuration guide for further information on setting up the Authlogics Authentication Server. In addition, Authlogics user accounts should already be configured for users.

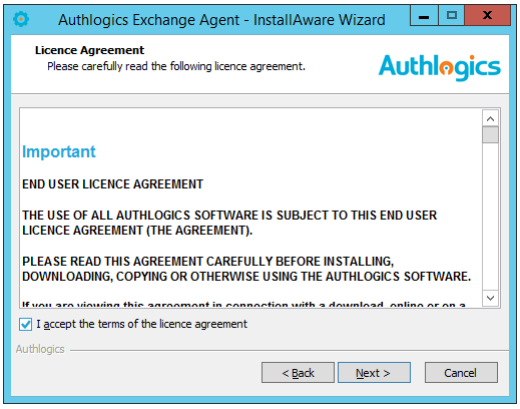
Installing/Removing the Authlogics Exchange Agent

The installation should be performed on the server running the Remote Desktop Web Access role.

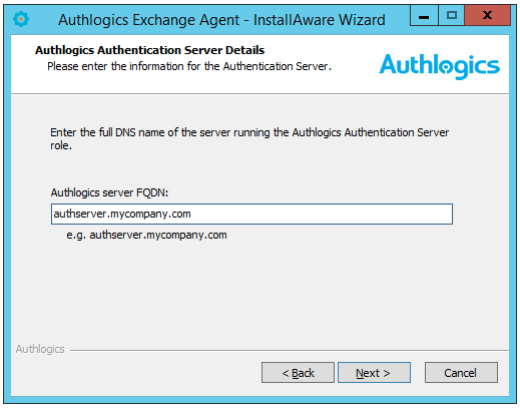
Running an installation

(1) To start the Authlogics Windows Desktop Logon Agent installation, run the *Authlogics Exchange Agent xxxxx.exe* installer with **elevated privileges**.

(2) Click *Next* to begin the install or *Cancel* to quit.



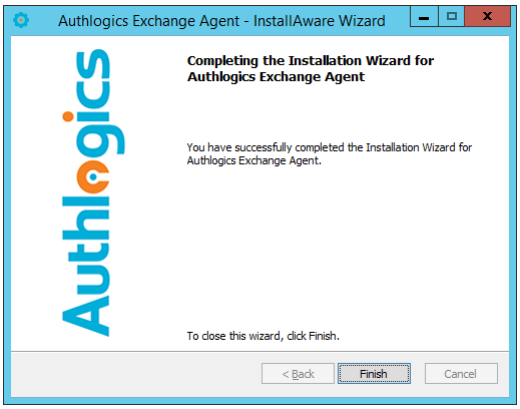
(3) Review the Authlogics Licence Agreement, check the *I accept the terms of the licence agreement* box and click *Next*.



(4) Enter the FQDN of the Authlogics Authentication Server, click *Next*.

(5) Click *Next* to begin the install or *Cancel* to quit.

The installation is being performed.



(6) All necessary Authlogics Exchange Agent files have been installed. Click *Finish* to complete the installation process.

Running a removal

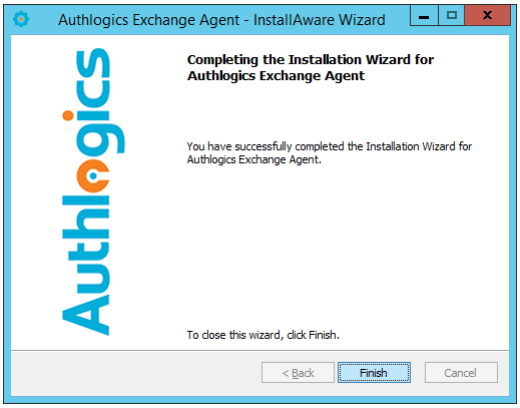
Uninstalling the Authlogics Exchange Agent does NOT remove the metadata from user accounts in the Active Directory.

If you no longer require Authlogics Exchange Agent on a server, you can remove it by performing an uninstall as follows:

(1) To start the Authlogics Exchange Agent un-installation, execute the *Authlogics Exchange Agent xxxxx.exe* installer or use the *Uninstall or change a program* option in Control Panel and click *Remove*.

(2) Select *Uninstall.* Click *Next* to continue.

(3) Click *Next* to continue.

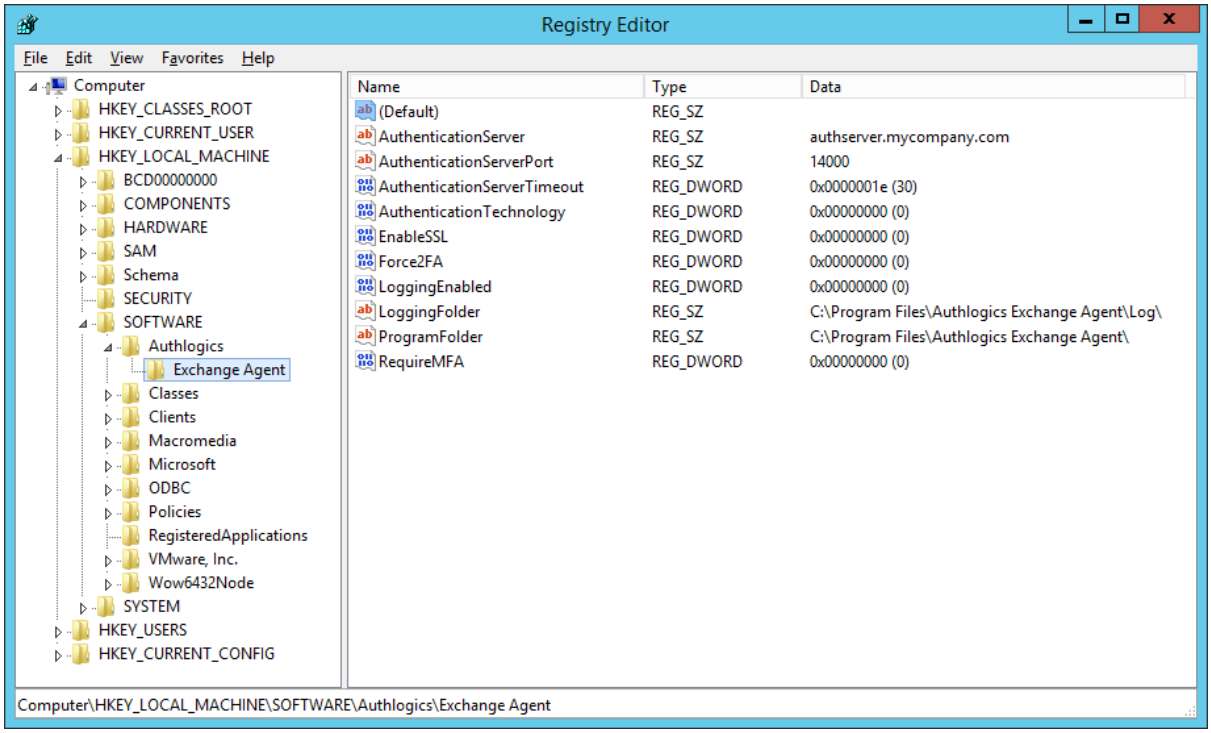


(4) Click *Finish* to complete the uninstall process.

Configuring Exchange for Multi-Factor Authentication

Once the agent has been installed, there are a few settings that can be modified to change the behaviour of the agent. These reside in the registry in the following location.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Authlogics\Exchange Agent\
```



MFA vs none MFA users

The Exchange Agent is dynamic and will automatically prompt a user for Multi-Factor Authentication (MFA) if they have been provisioned for MFA on the Authlogics Server. Any users that have not been provisioned for MFA may continue to login using the standard AD username and password method by default.

Once all users have been provisioned for MFA it is recommended to configure the Exchange Agent to require MFA for all users. This can be done by setting the ***RequireMFA*** registry key to 1.

Setting the authentication technology

The Exchange Agent works with PINgrid, PINphrase and PINpass technologies. The agent will use PINgrid by default, however this can be altered by changing the ***AuthenticationTechnology*** registry key as follows:

- PINgrid = 0
- PINphrase = 1
- PINpass = 2

Deviceless MFA options

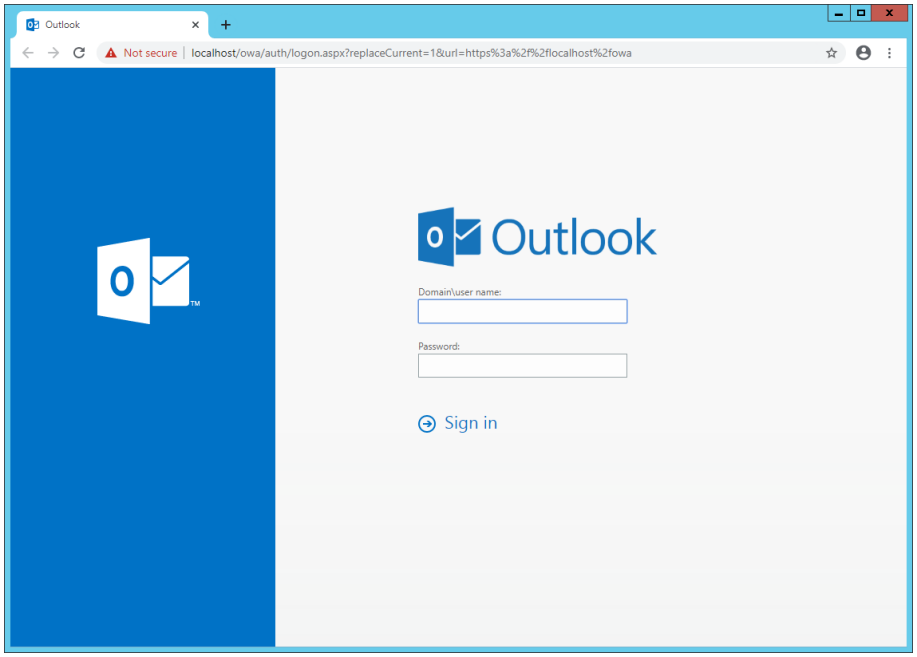
The Exchange Agent supports deviceless MFA allowing users to login without requiring a physical device. This is very convenient for users and is much more secure than a simple password. Individual user accounts can be configured to require 2 factor authentication (disable deviceless) on the Authlogics Authentication, in addition the Exchange Agent can also be configured to force 2 factor authentication by setting the ***Force2FA*** registry key to 1.

Note

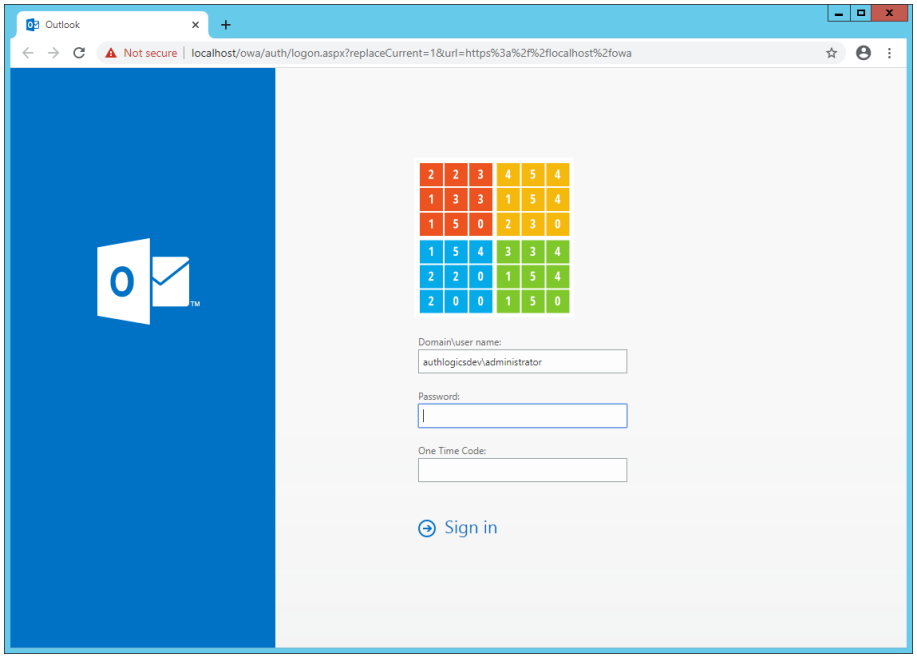
It is recommended to run **IISRESET** from an admin command prompt for registry key changes to take effect immediately.

The OWA logon process overview

1. Open the Exchange Outlook Web App logon page URL (e.g. https://owa.mycompany.com/owa) and enter your username usual.



2. If your user account has been provisioned for Authlogics MFA the One Time Code box will appear along with an MFA challenge. If Force2FA has been enabled then a MFA challenge will not appear, instead the MFA technology logo the user must use will be displayed.
3. Enter your AD password and One Time Code
   Click *Sign in*.



4. You are successfully logon onto Exchange