intercede

MyID Exchange Agent Integration Guide

MyID MFA for Exchange and Outlook Web App

Product Version: 5.0.6942.0

Publication date: March 2024

MyID MFA PSM

Call us on:	+44 (0)1455 558 111 (UK & EMEA) +1 408 706 2866 (US)
Email us:	info@intercede.com

Intercede Ltd, Lutterworth Hall, St. Mary's Road, Lutterworth, Leicestershire, LE17 4PS, United Kingdom
UK Tel: +44 (0)1455 558 111   US Tel: +1 888 646 6943   email: info@intercede.com   web: www.intercede.com

Table of Contents

Introduction.. 3
Licensing 4
Deployment Considerations 4
Minimum Requirements 4
Deployment.. 5
Overview 5
Installing the MyID Exchange Agent.. 5
Uninstalling the MyID Exchange Agent 7
Active Directory metadata.. 7
Configuring Exchange for Multi-Factor Authentication 8
General Settings... 8
The OWA logon process overview 12
Installing an Exchange Cumulative Update 14
Incorrect procedure.. 14
Advanced Configuration.. 15
Specifying Active Directory Domain Controllers 15
Active Directory Timing.. 16
Disabling SSL connections 16
Diagnostics Logging 17

Introduction

Note

MyID MFA and MyID PSM were previously known as Authlogics products. Authlogics is now an Intercede Group company and the products have been rebranded accordingly.

The term ‘Authlogics’ may still appear in certain areas of the product.

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

Licensing

MyID Exchange Agent does not require its own licence however may only be used with a valid MyID MFA licence.

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

Deployment Considerations

The MyID 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 and does not require any web page customisation.

By default, the Exchange Agent will allow users who have NOT been configured for MFA to login with their AD username and password. This allows for a gradual implementation of MFA user accounts instead of all users having to be setup for MFA at the same time. This functionality can be disabled at any time by enabling the "All users must use Multi-Factor Authentication" policy setting.

Minimum Requirements

The MyID 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 4.8, thus the agent requires the minimum of the following Exchange Cumulative Updates:

- Exchange 2013 – Cumulative Update 23
- Exchange 2016 – Cumulative Update 13
- Exchange 2019 – Cumulative Update 2

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 MyID Exchange Agent.

Overview

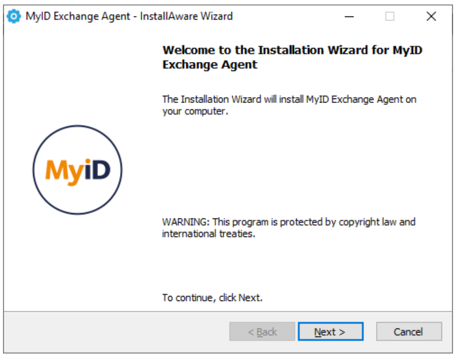
This deployment section assumes that at least one MyID Authentication Server has already been installed and is functional. See the MyID Authentication Server Installation and Configuration guide for further information on setting up the MyID Authentication Server. In addition, MyID user accounts should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

Installing the MyID Exchange Agent

The installation should be performed on the server running Microsoft Exchange Server.

(1) To start the MyID Exchange Agent installation, run the Authlogics Exchange Agent xxxxx.exe installer with elevated privileges

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



MyID Exchange Agent - InstallAware Wizard

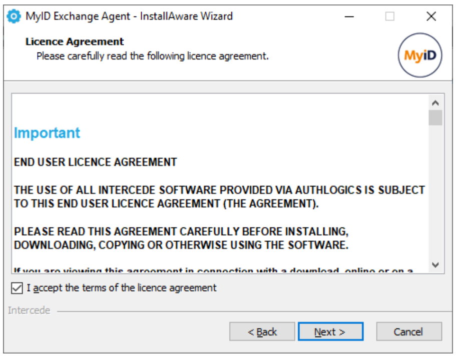
Welcome to the Installation Wizard for MyID Exchange Agent

The Installation Wizard will install MyID Exchange Agent on your computer.

WARNING: This program is protected by copyright law and international treaties.

To continue, click Next.

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



MyID Exchange Agent - InstallAware Wizard

Licence Agreement

Please carefully read the following licence agreement.

Important

END USER LICENCE AGREEMENT

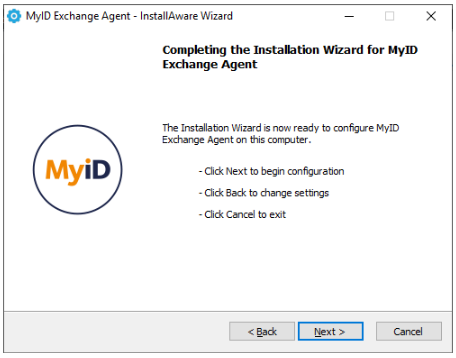
THE USE OF ALL INTERCEDE SOFTWARE PROVIDED VIA AUTHLOGICS IS SUBJECT TO THIS END USER LICENCE AGREEMENT (THE AGREEMENT).

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE INSTALLING, DOWNLOADING, COPYING OR OTHERWISE USING THE SOFTWARE.

If you are viewing this agreement in connection with a download, online or on a

☑ I accept the terms of the licence agreement

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

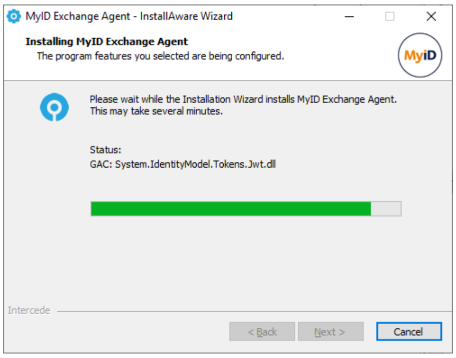


Completing the Installation Wizard for MyID Exchange Agent

The Installation Wizard is now ready to configure MyID Exchange Agent on this computer.

- Click Next to begin configuration
- Click Back to change settings
- Click Cancel to exit

(5) The installation is being performed.



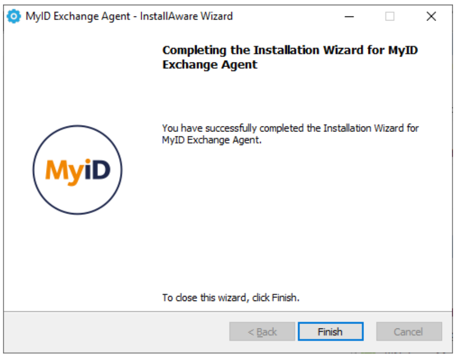
Installing MyID Exchange Agent

The program features you selected are being configured.

Please wait while the Installation Wizard installs MyID Exchange Agent. This may take several minutes.

Status:
GAC: System.IdentityModel.Tokens.Jwt.dll

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



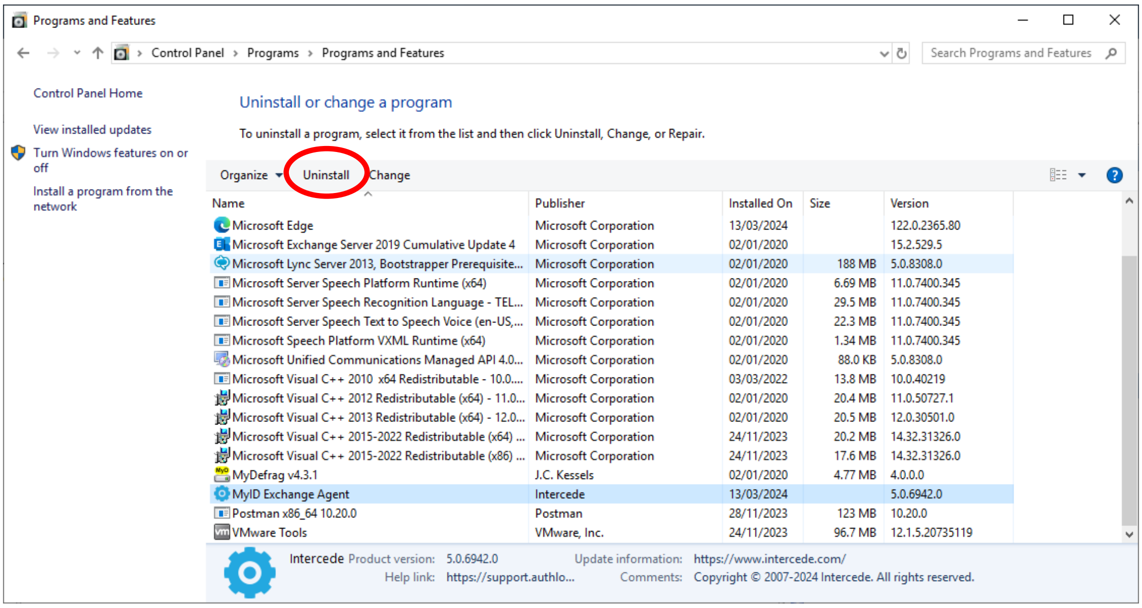
Completing the Installation Wizard for MyID Exchange Agent

You have successfully completed the Installation Wizard for MyID Exchange Agent.

To close this wizard, click Finish.

Uninstalling the MyID Exchange Agent

If you no longer require MyID Exchange Agent on a server, you can remove it by performing an uninstall from Control Panel > Programs > Programs and Features:



Programs and Features
Control Panel > Programs > Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize
Uninstall
Change

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
Microsoft Edge	Microsoft Corporation	13/03/2024		122.0.2365.80
Microsoft Exchange Server 2019 Cumulative Update 4	Microsoft Corporation	02/01/2020		15.2.529.5
Microsoft Lync Server 2013, Bootstrapper Prerequisite...	Microsoft Corporation	02/01/2020	188 MB	5.0.8308.0
Microsoft Server Speech Platform Runtime (x64)	Microsoft Corporation	02/01/2020	6.69 MB	11.0.7400.345
Microsoft Server Speech Recognition Language - TEL...	Microsoft Corporation	02/01/2020	29.5 MB	11.0.7400.345
Microsoft Server Speech Text to Speech Voice (en-US,...	Microsoft Corporation	02/01/2020	22.3 MB	11.0.7400.345
Microsoft Speech Platform VXML Runtime (x64)	Microsoft Corporation	02/01/2020	1.34 MB	11.0.7400.345
Microsoft Unified Communications Managed API 4.0...	Microsoft Corporation	02/01/2020	88.0 KB	5.0.8308.0
Microsoft Visual C++ 2010 x64 Redistributable - 10.0....	Microsoft Corporation	03/03/2022	13.8 MB	10.0.40219
Microsoft Visual C++ 2012 Redistributable (x64) - 11.0...	Microsoft Corporation	02/01/2020	20.4 MB	11.0.50727.1
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0...	Microsoft Corporation	02/01/2020	20.5 MB	12.0.30501.0
Microsoft Visual C++ 2015-2022 Redistributable (x64) ...	Microsoft Corporation	24/11/2023	20.2 MB	14.32.31326.0
Microsoft Visual C++ 2015-2022 Redistributable (x86) ...	Microsoft Corporation	24/11/2023	17.6 MB	14.32.31326.0
MyDefrag v4.3.1	J.C. Kessels	02/01/2020	4.77 MB	4.0.0.0
MyID Exchange Agent	Intercede	13/03/2024		5.0.6942.0
Postman x86_64 10.20.0	Postman	28/11/2023	123 MB	10.20.0
VMware Tools	VMware, Inc.	24/11/2023	96.7 MB	12.1.5.20735119

Intercede Product version: 5.0.6942.0 Update information: https://www.intercede.com/
Help link: https://support.authlo... Comments: Copyright © 2007-2024 Intercede. All rights reserved.

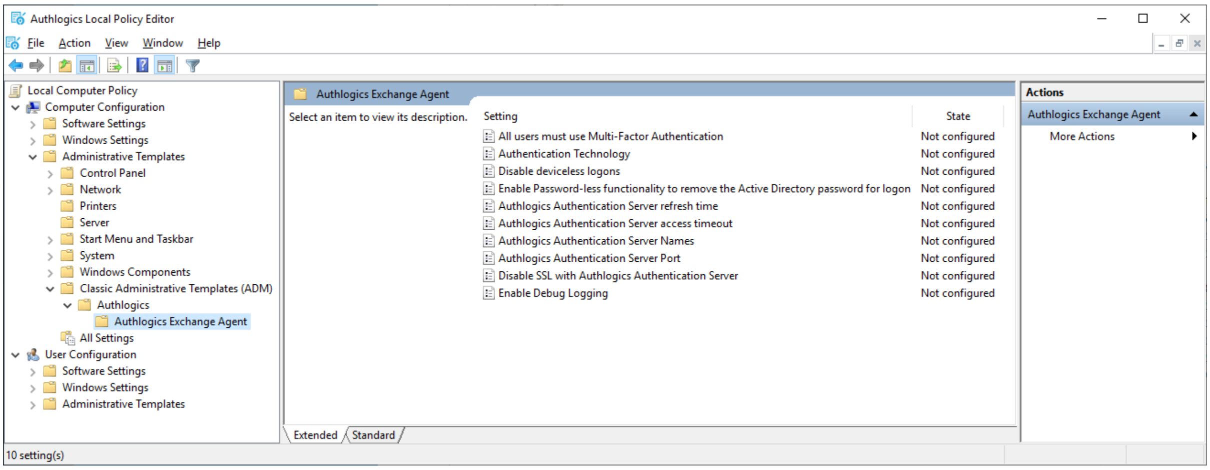
Active Directory metadata

Uninstalling MyID does NOT remove the metadata from user accounts in the Active Directory. If you are planning to completely remove MyID from your environment you should delete all user accounts via the MMC prior to uninstalling – this does NOT delete the actual AD user account, it simply removes all MyID information from it.

For detailed information about MyID AD metadata see Authlogics KB207256965 (https://support.authlogics.com/hc/en-us/articles/207256965).

Configuring Exchange for Multi-Factor Authentication

Once the agent has been installed, there are a few settings that can be modified to change the configuration of the agent. These settings are managed via either Local or Active Directory Group Policy. To easily access the MyID Local policy settings use the MyID Local Policy Editor shortcut on the desktop or start menu.



Authlogics Exchange Agent

Select an item to view its description.

Setting	State
All users must use Multi-Factor Authentication	Not configured
Authentication Technology	Not configured
Disable deviceless logons	Not configured
Enable Password-less functionality to remove the Active Directory password for logon	Not configured
Authlogics Authentication Server refresh time	Not configured
Authlogics Authentication Server access timeout	Not configured
Authlogics Authentication Server Names	Not configured
Authlogics Authentication Server Port	Not configured
Disable SSL with Authlogics Authentication Server	Not configured
Enable Debug Logging	Not configured

General Settings

Setting	All users must use Multi-Factor Authentication
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting configures if the agent should only allow MFA provisioned user to login, or if the agent should also allow users who have not been provisioned for MFA to login with their Active Directory password. If you enable this policy then all users must be provisioned for MFA to access the agent. If you disable or do not configure this policy then MFA provisioned users must use MFA, however non-MFA provisioned users may still use their Active Directory username + password to login.	

Setting	Authentication Technology
Values	PINgrid / PINphrase / PINpass / Push
Default	Disabled
Description	
his policy setting disables the ability to login without a separate MFA device. If you enable this policy a user must login to the agent using a separate MFA device. If you disable or do not configure this policy a user may logon with or without a separate MFA device, depending on any user specific restrictions.	

Setting	Disable deviceless logons
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables the ability to login without a separate MFA device. If you enable this policy a user must login to the agent using a separate MFA device. If you disable or do not configure this policy a user may logon with or without a separate MFA device, depending on any user specific restrictions.	

Setting	Enable Password-less functionality to remove the Active Directory password for logon
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting removes the Active Directory password from the logon page allowing users to logon with only a Username and One Time Passcode. If you enable this policy the Exchange Agent will not ask for an AD password when a user logs on; unless there is no password available in the Password Vault. If you disable or do not configure this policy then users will be required to enter their AD password together with a One Time Passcode at each logon.	

Setting	Authlogics Authentication Server Names
Values	Any DNS based server address (CSV)
Default	{blank}
Description	
This policy setting configures the server name(s) which agents will use to connect to the MyID Authentication Server instead of searching the Active Directory for server names. If you enable this policy you must specify at least one server DNS name, however multiple server names can be specified separated by a comma, e.g. server1.domain.com,server2.domain.com If you disable or do not configure this policy the Active Directory will be searched to locate one or more MyID Authentication Servers.	

Setting	Authlogics Authentication Server Port (HTTPS/SSL)
Values	(1024 – 65535)
Default	14443
Description	
This policy setting configures the MyID Authentication Server port number which agents will use to connect to the MyID Authentication Server. The server name will be located automatically via an Active Directory search unless specified in the "Authlogics Authentication Server Names" policy. If you enable this policy you must specify a TCP port number, e.g.14443 If you disable or do not configure this policy the default port 14443 will be used.	

Setting	Authlogics Authentication Server refresh time
Values	(5 – 1440)
Default	60
Description	
This policy setting sets the maximum amount of time before refreshing the most suitable MyID Authentication Server. If you enable this policy you must specify the interval value in minutes to wait before refreshing which MyID Authentication Server to use. If you disable or do not configure this policy the agent will wait for 60 minutes before refreshing which MyID Authentication Server to use.	

Setting	Authenticator App Push Authentication timeout
Values	(30 – 300)
Default	120
Description	
This policy setting sets the maximum amount of time to wait while the MyID Exchange Agent sends a push notification to the Authlogics Authenticator App and waits for a response. If you disable or do not configure this policy the Windows Desktop Agent will wait for 120 seconds for a response.	

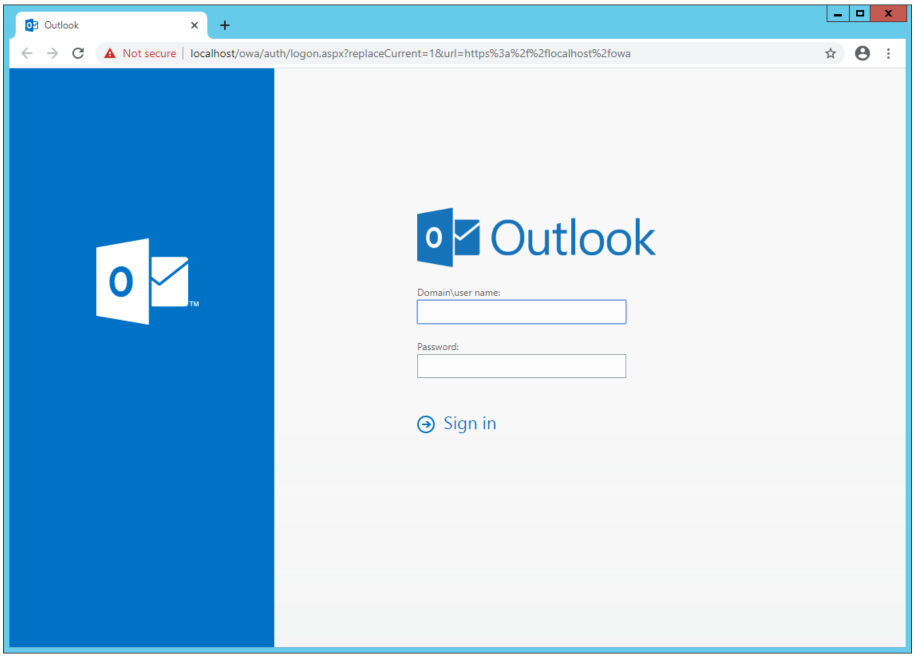
Setting	Authlogics Authentication Server access timeout
Values	(0 – 120)
Default	5
Description	
This policy setting sets the maximum amount of time to wait while locating an MyID Authentication Server before attempting an alternative server or the request failing. If you enable this policy you must specify the interval value in seconds to wait while locating an MyID Authentication Server. Setting this value to 0 will disable the timeout and connections will wait indefinitely. If you disable or do not configure this policy the agent will wait for 5 seconds while locating an MyID Authentication Server.	

Setting	Disable SSL with Authlogics Authentication Server
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting configures if SSL will be used when connecting to an MyID Authentication Server. If you enable this policy HTTP (No SSL) will be used when connecting to an MyID Authentication Server. If you disable or do not configure this policy HTTPS (SSL) will be used when connecting to an MyID Authentication Server.	

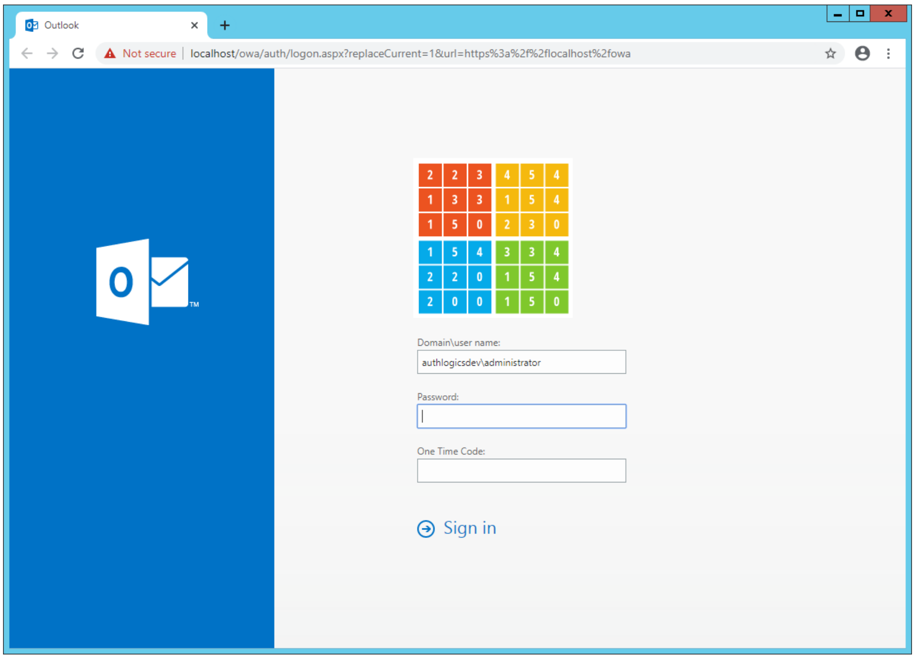
Setting	Enable Debug Logging
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting enables debug logging on all servers running the agent. This should only be enabled if requested by an Intercede Support engineer. This setting performs the same function as manually setting the LoggingEnabled registry key to 1. If you enable this policy debug logging will be active. If you disable or do not configure this policy then debug logging will not be active.	

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.


Outlook
Not secure
localhost/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2flocalhost%2fowa
Outlook
Domain\user name:
Password:
Sign in

2. If your user account has been provisioned for MyID MFA the One Time Code box will appear along with an MFA challenge. If the “Disable deviceless logons” policy 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 (unless the Password-less policy has been enabled) and One Time Code
   Click *Sign in*.


Outlook
Not secure
localhost/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2flocalhost%2fowa

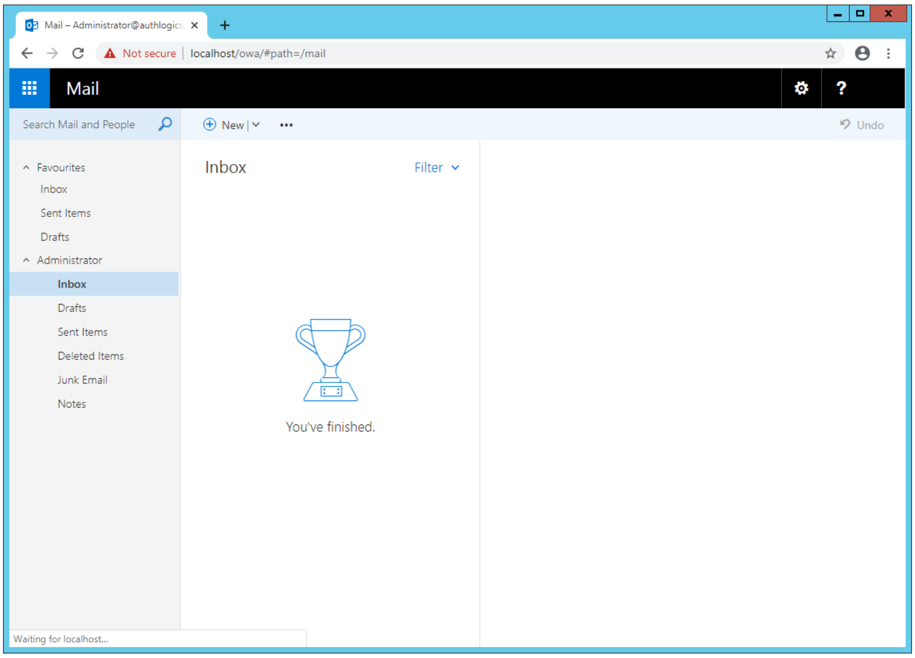
2	2	3	4	5	4
1	3	3	1	5	4
1	5	0	2	3	0
1	5	4	3	3	4
2	2	0	1	5	4
2	0	0	1	5	0

Domain\user name: authlogicsdev\administrator

Password:

One Time Code:

4. You are successfully logon onto Exchange



Installing an Exchange Cumulative Update

Microsoft release updates, hotfixes and cumulative updates on a relatively regular basis. When installing an Exchange Cumulative Updates (CU), the following steps should be followed to ensure that the update process completes successfully.

1. Uninstall MyID Exchange Agent
2. Test Outlook Web Access on that server ensuring that you can authenticate using a standard AD username and password credentials
3. Install the Exchange Cumulative Update
4. Upon completion of the Cumulative Update, retest the OWA authentication using a valid AD username and password
5. Re-install MyID Exchange Agent
6. Retest OWA authentication

> **Note**
> The upgrade process detailed above will not impact the MyID Exchange Agent local policies and only affect the OWA and EAC login pages.

Incorrect procedure

If you have not followed the steps detailed above and have already installed the latest Microsoft Cumulative Update, MyID Exchange Agent may not be working as expected. To rectify this, please perform the following operations:

1. Take a backup of the **Web.Config** file located in **C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa** and place this file into a temporary folder.
2. Uninstall the MyID Exchange Agent
3. Copy the **Web.Config** backup file from Step 1 back over the file located in the **C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa** folder.
4. Test Outlook Web Access on that server ensuring that you can authenticate using a standard AD username and password credentials
5. Re-install MyID Exchange Agent
6. Retest OWA authentication

Advanced Configuration

Advanced configuration options for MyID are controlled via the Windows registry. The following entries are created during the installation of the agent and typically most of them should only be changed if instructed by an Intercede support engineer.

Specifying Active Directory Domain Controllers

The MyID agent will automatically locate domain controllers as needed. In environments where network segmentation exists not all DC’s may be contactable. This can cause connectivity problems and logon delays.

In these environments, you can specify which Domain Controllers (DCs) and Global Catalog Servers (GCs) should be used via registry keys. There are two keys which can be configured and each can contain one or many server names (FQDN recommended) separated by commas.

```
HKLM\SOFTWARE\Authlogics\Exchange Agent\DomainGCs
```

Default Value: `{blank}`

The MyID agent will use attempt to connect to each specified GC and then remain connected to the server that responds to LDAP queries the quickest.

```
HKLM\SOFTWARE\Authlogics\Exchange Agent\DomainDCs
```

Default Value: `{blank}`

The MyID agent will use attempt to connect to each specified DC and then remain connected to the server that responds to LDAP queries the quickest. The MyID agent will initially find the names of all the Domains in the Forest, and the DC’s in each Domain by querying the Global Catalog. It will then map the results against the DC list in the registry to calculate which server to use for each Domain. If a Domain does not have a DC specified then one will be selected automatically.

Active Directory Timing

```
HKLM\SOFTWARE\Authlogics\Exchange Agent\DomainAccessTimeout
```

Default Value: `60`

Accepted Values:

`0 = Disabled, indefinite timeout`

`1 to 120 = Timeout in seconds`

The time taken in seconds before a connection to a Domain Controller times out.

```
HKLM\SOFTWARE\Authlogics\ Exchange Agent\DomainControllerRefeshTime
```

Default Value: `15`

Accepted Values:

`1 to 9999 = Timeout in minutes`

The time taken in minutes before a new search is done to locate the quickest GC and DC.

Disabling SSL connections

The MyID Exchange Agent will use HTTPS (SSL) when connecting to an MyID Authentication Server by default. In scenarios where SSL is not required it can be disabled, however this requires configuration on the Exchange Agent as well as on the MyID Authentication Server.

> **Note**
> When SSL is disabled most traffic between the Exchange Server and the MyID Authentication Server will not be encrypted. An exception exists for data being retrieved from the Password Vault which is always encrypted even without SSL.

To configure the MyID Authentication Server an IIS binding must be added which uses HTTP and a port; Intercede recommends port 14443 for HTTP connections. The existing HTTPS binding should NOT be removed.

The MyID WebAPI will deny any non SSL connection by default for security. To allow the Exchange Agent to communicate over HTTP the IP address of the Exchange Server must be added to the “AllowedHttpIpAddresses” registry key on the MyID Authentication Server. The “AllowedHttpIpAddresses” registry key is a CSV value which allows for multiple IP address entries.

The Exchange Agent is configured by enabling the “Disable SSL with Authlogics Authentication Server” policy setting. In addition, the “Authlogics Authentication Server Port” policy setting should be set to match the HTTP (Non SSL) port in IIS on the MyID Authentication Server.

Diagnostics Logging

```
HKLM\SOFTWARE\Authlogics\Exchange Agent\LoggingEnabled
```

Default Value: `0`

Accepted Values:

```
0 = Disabled
1 = Enabled
```

Notes: When this value is enabled various log files will be created in the logging folder. These logs may be requested by an Intercede support engineer.

```
HKLM\SOFTWARE\Authlogics\Exchange Agent\LoggingFolder
```

Default Value: `C:\Program Files\Authlogics Exchange Agent\Log`

Notes: This Value may be changed to an alternative valid local folder with the same NTFS permissions as the default folder.