MyID MFA and PSM

Version 5.0.7

Exchange Agent Integration Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111

Copyright

Conventions

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important.
  - Bulleted lists are used when the order is unimportant or to show alternatives.

- **Bold** is used for menu items and for labels.

  For example:
  - “Record a valid email address in **'From' email address**"
  - Select **Save** from the **File** menu.

- *Italic* is used for emphasis and to indicate references to other sections within the current document:

  For example:
  - "Copy the file *before* starting the installation"
  - "See *Issuing a Card* for further information"

- ***Bold and Italic*** are used to identify the titles of other documents.

  For example: “See the ***Release Notes*** for further information.”

  Unless otherwise explicitly stated, all referenced documentation is available on the product media.

- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.

- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.

- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

Warning:	You must take a backup of your database before making any changes to it.

Contents

1 Introduction

This guide describes the process of integrating MyID Multi-Factor Authentication (MFA) with Microsoft Exchange Server using the web interface.

Integrating MyID with Microsoft Exchange is an ideal way to add strong authentication to Outlook Web App and Exchange Admin Centre.

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.

1.1 Licensing

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

Note: For detailed information on the license types, refer to the license agreement document embedded within the installation package.

1.2 Change log

Version	Description
INT2057-01	Reformatted and released with MyID MFA and PSM version 5.0.7.

2 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 integrates the agent directly into the IIS on the Exchange Server, and does not require any web page customization.

By default, the Exchange Agent allows users who are *not* configured for MFA to log in with their Active Directory username and password. This allows for a gradual implementation of MFA user accounts; you do not need to set up all your users for MFA at the same time. You can disable this functionality at any time by enabling the **All users must use Multi-Factor Authentication** policy setting.

2.1 Minimum requirements

The MyID Exchange Agent is designed to work with Microsoft Exchange Server 2013, 2016, and 2019 Mailbox and CAS servers.

The minimum supported .NET Framework version is 4.8; therefore, 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

3 Deployment

This is the installation process for deploying the MyID Exchange Agent.

3.1 Pre-requisites

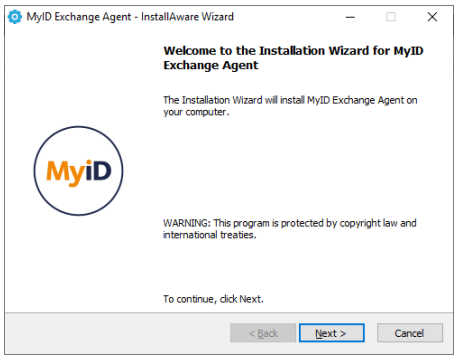
You must have at least one MyID Authentication Server installed and functional. For more information on setting up the MyID Authentication Server, see the ***MyID Authentication Server Installation and Configuration*** guide.

You must already have MyID MFA user accounts configured for users.

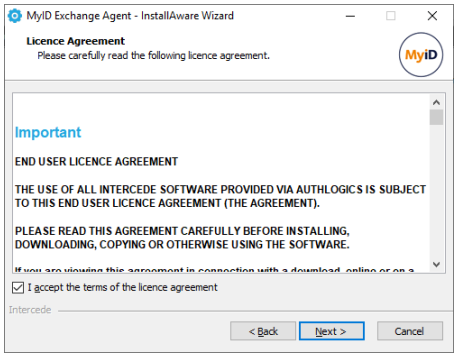
3.2 Installing the MyID Exchange Agent

Carry out the installation on the server running the Microsoft Exchange Server.

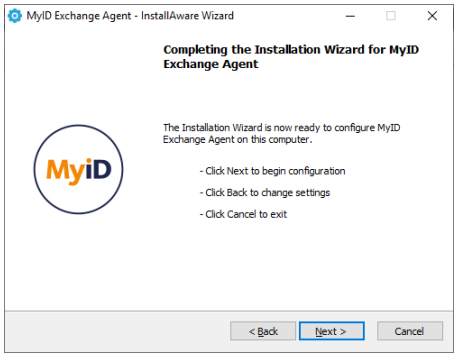
1. With elevated privileges, run the `Authlogics Exchange Agent xxxxx.exe` installer.



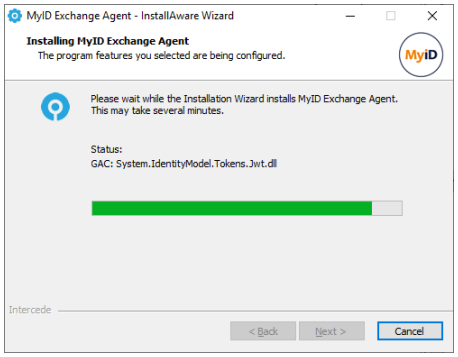
2. Click **Next**.
3. Review the license agreement and check the **I accept the terms of the licence agreement** box.

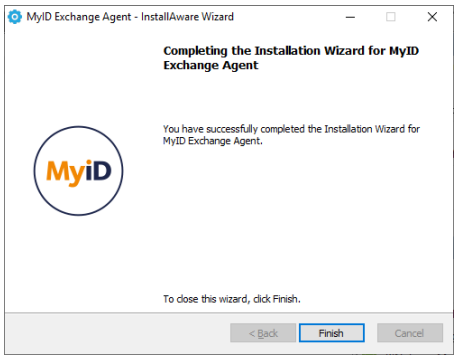


4. Click **Next**.



5. Click **Next**.



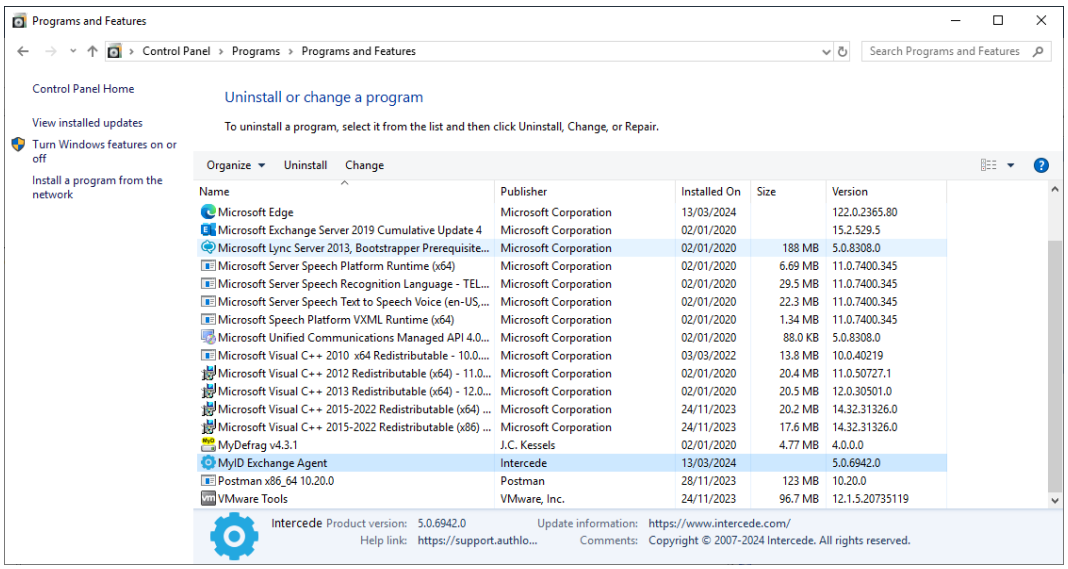


6. Click Finish.

   All necessary MyID Exchange Agent files have been installed.

3.3 Uninstalling the MyID Exchange Agent

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



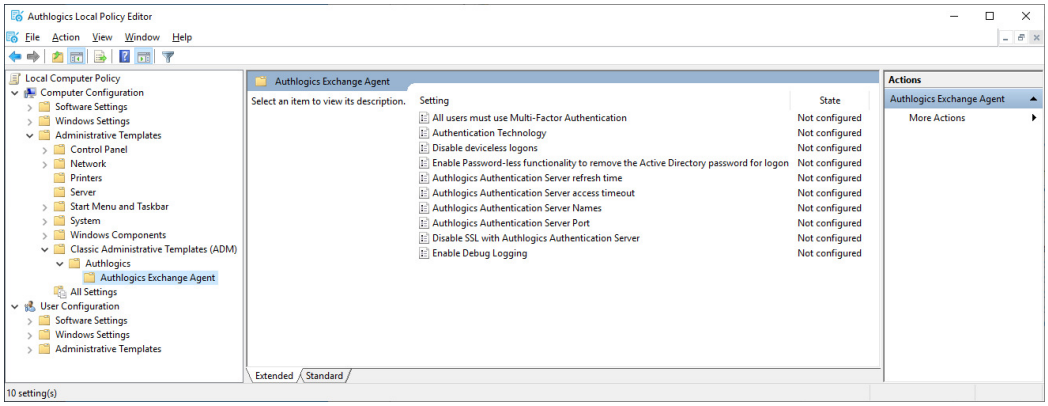
3.3.1 Active Directory metadata

Uninstalling the MyID Exchange Agent does *not* remove the metadata from user accounts in the Active Directory. If you want to remove MyID MFA from your environment completely, delete all user accounts using the MMC before uninstalling. This does *not* delete the user accounts in the Active Directory; it just removes all MyID information from them.

4 Configuring Exchange for Multi-Factor Authentication

Once you have installed the MyID Exchange Agent, you can configure it. You can manage the configuration settings using either Local Directory Group Policy or Active Directory Group Policy.

To access the MyID Local policy settings, use the MyID Local Policy Editor shortcut on the desktop or start menu.



4.1 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 / Disabled
Default	Disabled
Description	This policy setting configures the authentication technology which the agent will use. If you enable this policy you must specify which authentication technology to use. If you disable or do not configure this policy the agent will automatically detect the technology the user is configured to use. PINgrid: If Deviceless OTP is allowed and the user does not require MFA then a PINgrid challenge grid will be displayed, otherwise, a PINgrid logo will be displayed. PINphrase: If Deviceless OTP is allowed and the user does not require MFA then a PINphrase challenge phrase will be displayed, otherwise, a PINphrase logo will be displayed. PINpass: A PINpass logo will be displayed. Push: Deliver a Push notification to the user's mobile device. Disabled: A generic icon will be displayed only and Deviceless OTP is also disabled regardless of the "Disable Deviceless logons" policy setting.

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	
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.

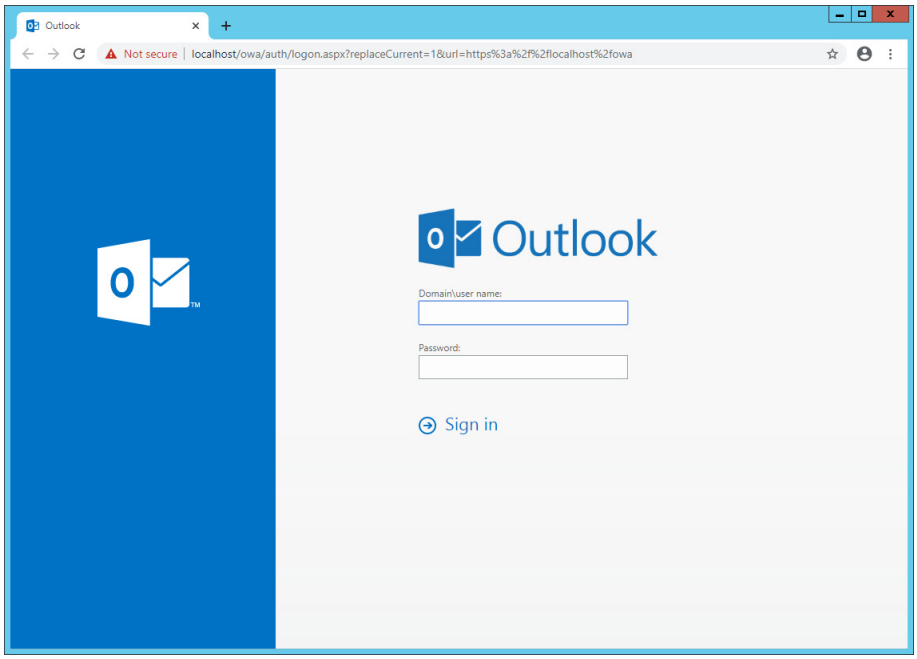
5 The OWA logon process overview

1. Open the Exchange Outlook Web App logon page.

   For example:

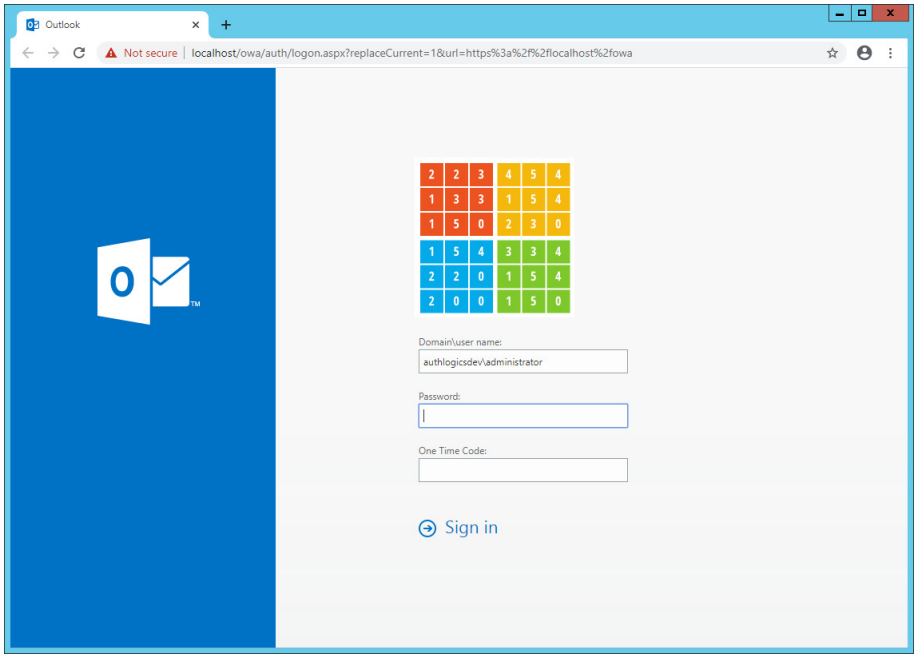
   `https://owa.<mycompany>.com/owa`

   Where `<mycompany>` is your company's Outlook Web App name.



2. Enter your username.

   If your user account is provisioned for MyID MFA, the One Time Code box appears along with an MFA challenge.



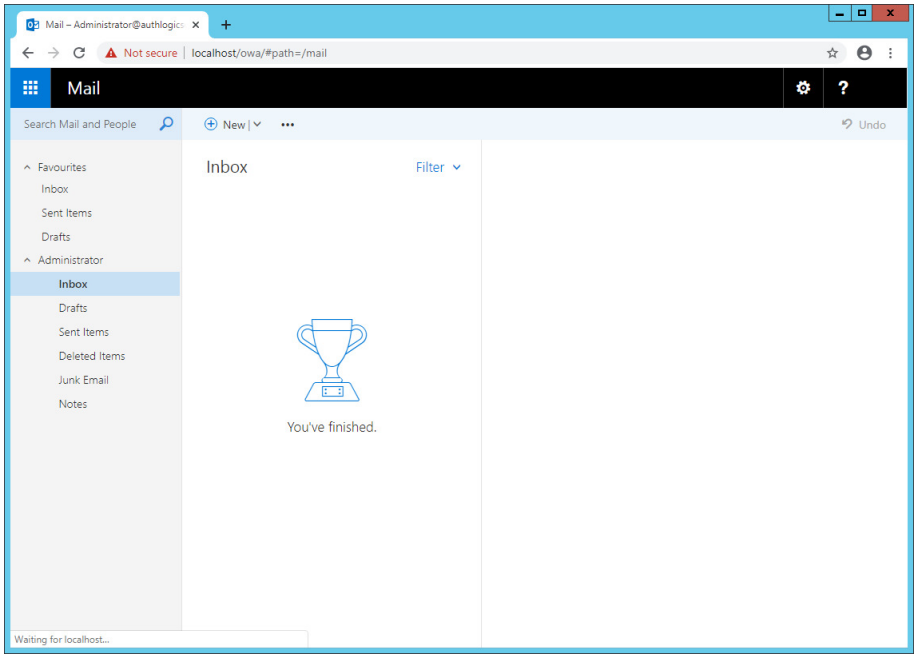
   If the **Disable deviceless logons** policy is enabled, an MFA challenge does not appear; instead, the MFA technology logo that you must use is displayed.

3. Enter your Active Directory password and One Time Code.

   Note: If the password-less policy is enabled, you do not need to enter your Active Directory Password.

4. Click **Sign in**.

   You are successfully logged in to the Exchange Outlook Web App.



6 Installing an Exchange Cumulative Update

Microsoft release updates, hotfixes, and cumulative updates on a relatively regular basis.

When installing Exchange Cumulative Updates, carry out the following steps to ensure that the update process completes successfully.

1. Uninstall the MyID Exchange Agent.
2. Test Outlook Web Access on your Exchange server.

   Ensure that you can successfully authenticate using a valid standard Active Directory username and password.
3. Install the Exchange Cumulative Update.
4. When the cumulative update is complete, retest Outlook Web Access on your Exchange server.
5. Reinstall the MyID Exchange Agent.
6. Test Outlook Web Access on your exchange server again.

   If the user account has been provisioned for MyID MFA, you should require another factor of authentication. See section *5*, *The OWA logon process overview* for details.

Note: This update process does not impact the MyID Exchange Agent's local policies and only affects the OAW and EAC login pages.

6.1 Incorrect procedure

If, when you install an Exchange Cumulative Update, MyID Exchange Agent is not working as expected, perform the following operations to rectify that:

1. Back up the configuration file.

   The configuration file is named:

   ```
   Web.Config
   ```

   And can be found in the following folder:

   ```
   C:\Program Files\Microsoft\Exchange
   Server\V15\FrontEnd\HttpProxy\owa
   ```

   Put a copy of the file in a temporary folder elsewhere.
2. Uninstall the MyID Exchange Agent.
3. Return your configuration file.

   Copy your backup of the configuration and return it to:

   ```
   C:\Program Files\Microsoft\Exchange
   Server\V15\FrontEnd\HttpProxy\owa
   ```
4. Test Outlook Web Access on your Exchange server.

   Ensure that you can successfully authenticate using a valid standard Active Directory username and password.
5. Reinstall the MyID Exchange Agent.
6. Test Outlook Web Access on your exchange server again.

   If the user account has been provisioned for MyID MFA, you should require another factor of authentication. See section *5*, *The OWA logon process overview* for details.

7 Advanced configuration

Advanced configuration options for MyID are controlled through the Windows registry.

These entries are created during the installation of the MyID Exchange Agent. You should, typically, only change them if instructed by Intercede support.

7.1 Specifying Active Directory Domain Controllers

The MyID Exchange Agent automatically locates Domain Controllers as needed. In environments where network segmentation exists, you may not be able to contact all Domain Controllers. This can cause connectivity problems and logon delays.

In those environments, you can specify which Domain Controllers and Global Catalog Servers should be used by configuring registry keys. There are two registry keys that you can configure, and each can contain one or more server names (FQDN recommended), separated by commas.

The following registry key is used to specify Global Catalog Servers:

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

By default, this is blank.

The MyID Exchange Agent attempts to connect to each specified Global Catalog Server and then remains connected to the server that responds to the LDAP queries the quickest.

The following registry key is used to specify Domain Controllers:

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

By default, this is blank.

The MyID Exchange Agent attempts to connect to each specified Domain Controller and then remains connected to the controller that responds to the LDAP queries the quickest.

The MyID Exchange Agent initially finds the names of each Domain in the Forest, and each Domain Controller in each Domain by querying the Global Catalog. It then maps the results against the Domain Controller list in the registry to calculate which server to use for each Domain. If a Domain does not have a Domain Controller specified, then one is selected automatically.

7.2 Active Directory Timing

The following registry key is used to define the Domain Controller time out.

`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.

The following registry key is used to define the Domain Controller refresh time.

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

Default Value: `15`

Accepted Values:

- `1` to `9999` – timeout in minutes

The time taken in minutes before the MyID Exchange Agent does another search to locate the quickest Global Catalog Server and Domain Controller.

7.3 Disabling SSL connections

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

Note: When SSL is disabled, most traffic between the MyID Exchange Server and the MyID Authentication Server is not encrypted, but data being retrieved from the password vault is always encrypted even without SSL.

To configure the MyID Authentication Server, you must add an IIS binding that uses HTTP and a port; Intercede recommends port 14443 for HTTP connections. The existing HTTPS binding should *not* be removed.

The MyID WebAPI denies any non-SSL connection by default for security. To allow the MyID Exchange Agent to communicate over HTTP, you must add the IP address of the Exchange server to the `AllowedHttpIpAddresses` registry key on the MyID Authentication Server. The `AllowedHttpIpAddresses` registry key is a CSV value that allows for multiple IP address entries.

Configure the Exchange Agent by enabling the **Disable SSL with Authlogics Authentication Server** policy setting. In addition, you must set the **Authlogics Authentication Server Port** policy setting to match the HTTP (non-SSL) port in IIS on the MyID Authentication Server.

7.4 Diagnostics logging

The following registry key is used to define if logging is enabled or not.

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

Default Value: `0`

Accepted Values:

- `0` – disabled
- `1` – enabled

When this value is enabled, various log files are created in the logging folder. These logs may be requested by Intercede support.

The following registry key is used to define the folder where the logs go.

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

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

You can change this to an alternative valid local folder with the same NTFS permissions as the default folder.