

MyID MFA and PSM Version 5.2

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

© 2001-2025 Intercede Limited. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished exclusively under a restricted license or non-disclosure agreement. Copies of software supplied by Intercede Limited may not be used resold or disclosed to third parties or used for any commercial purpose without written authorization from Intercede Limited and will perpetually remain the property of Intercede Limited. They may not be transferred to any computer without both a service contract for the use of the software on that computer being in existence and written authorization from Intercede Limited.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Intercede Limited.

Whilst Intercede Limited has made every effort in the preparation of this manual to ensure the accuracy of the information, the information contained in this manual is delivered without warranty, either express or implied. Intercede Limited will not be held liable for any damages caused, or alleged to be caused, either directly or indirectly by this manual.

Licenses and Trademarks

The Intercede[®] and MyID[®] word marks and the MyID[®] logo are registered trademarks of Intercede in the UK, US and other countries.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such. All other trademarks acknowledged.



Conventions used in this document

- · 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:

For example:

- Copy the file *before* starting the installation.
- Do not remove the files before you have backed them up.
- Bold and italic hyperlinks 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 installation 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

Exchange Agent Integration Guide	1
Copyright	2
Conventions used in this document	3
Contents	4
1 Introduction	5
1.1 Licensing	5
2 Deployment considerations	6
2.1 Minimum requirements	6
3 Deployment	7
3.1 Prerequisites	7
3.2 Installing the MyID Exchange Agent	8
3.3 Updating the MyID Exchange Agent	11
3.4 Uninstalling the MyID Exchange Agent	12
3.4.1 Active Directory metadata	12
3.5 Configuring the MyID Exchange Agent	12
3.5.1 General settings	13
4 The OWA logon process overview	17
5 Installing an Exchange cumulative update	20
5.1 Incorrect procedure	21
6 Advanced configuration	22
6.1 Specifying Active Directory Domain Controllers	22
6.1.1 Specifying Global Catalog Servers	22
6.1.2 Specifying Domain Controllers	22
6.2 Active Directory timing	23
6.2.1 Domain access timeout	23
6.2.2 Domain controller refresh	23
6.3 Disabling SSL connections	24
6.4 Diagnostics logging	24
6.4.1 LoggingEnabled	24
6.4.2 LoggingFolder	24



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

The 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.



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:

docs.microsoft.com/en-us/exchange/plan-and-deploy/supportabilitymatrix?view=exchserver-2019#microsoft-net-framework



3 Deployment

This chapter covers the following deployment related subjects:

- The prerequisites to installation. See section *3.1*, *Prerequisites*.
- Installing the MyID Exchange Agent. See section section *3.2, Installing the MyID Exchange Agent.*
- Updating the MyID Exchange Agent. See section 3.3, Updating the MyID Exchange Agent.
- Uninstalling the MyID Exchange Agent.
 See section 3.4, Uninstalling the MyID Exchange Agent.
- Configuring of the MyID Exchange Agent.
 See section 3.5, Configuring the MyID Exchange Agent.
 Note: For advanced configuration, see section 6, Advanced configuration.

3.1 Prerequisites

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.

🧿 MylD Excha	ange Agent - InstallAware Wizard —		×
Installing I The progr	MyID Exchange Agent am features you selected are being configured.	M	yiD
Q	Please wait while the Installation Wizard installs MyID Exchange Age This may take several minutes.	ent.	
	Status: GAC: System.IdentityModel.Tokens.Jwt.dll		
Intercede			
andereeue	< <u>B</u> ack <u>N</u> ext >	Cano	el







6. Click Finish.

All necessary MyID Exchange Agent files have been installed.



3.3 Updating the MyID Exchange Agent

You can use the installation program of an update for a full clean install, or to perform an inplace update of an existing installation.

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

1. With elevated privileges, run the Authlogics Exchange Agent xxxxx.exe installer. See section 3.2, *Installing the MyID Exchange Agent* for details.

At the end of the installation, the following pop-up appears:

2	\times
C:\Windows\PolicyDefinitions\en-us\Authlogics.adml Old file version: <no information="" version=""> Old file date: 21/11/2024 08:32:29 New file version: <no information="" version=""> New file date: 28/01/2025 12:27:30</no></no>	
s No Cancel No to All Yes to All	
	C:\Windows\PolicyDefinitions\en-us\Authlogics.adml Old file version: <no information="" version=""> Old file date: 21/11/2024 08:32:29 New file version: <no information="" version=""> New file date: 28/01/2025 12:27:30 Would you like to overwrite this file?</no></no>

2. Click Yes to All.

🧿 MyID Exchange Agent - In	stallAware Wizard	_		\times
	Completing the Installation Exchange Agent	Wizard 1	or MyI	D
MyiD	You have successfully completed the MyID Exchange Agent.	Installation	Wizard fi	or
	To close this wizard, click Finish.			
	< <u>B</u> ack	Finish	Can	cel

3. Click Finish.

All necessary MyID Exchange Agent files have been updated.



3.4 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**:

Ē	Programs and Features						- 🗆	×
	← → ~ ↑ 🖬 > Control P	anel > Programs > Programs and Features				 ・ ご Search Program 	ns and Features	Q
	Control Panel Home	Uninstall or change a program						
	View installed updates	To uninstall a program, select it from the list and then	click Uninstall, Change, or Repair.					
	Turn Windows features on or							
	off	Organize 🕶 Uninstall Change					833 👻	?
	Install a program from the	Name	Publisher	Installed On	Size	Version		^
	neuron	C 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		- 10
		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		
		5 Microsoft Unified Communications Managed API 4.0	Microsoft Corporation	02/01/2020	88.0 KB	5.0.8308.0		
		Figure 2010 x64 Redistributable - 10.0	Microsoft Corporation	03/03/2022	13.8 MB	10.0.40219		
		B Microsoft Visual C++ 2012 Redistributable (x64) - 11.0	Microsoft Corporation	02/01/2020	20.4 MB	11.0.50727.1		
		B Microsoft Visual C++ 2013 Redistributable (x64) - 12.0	Microsoft Corporation	02/01/2020	20.5 MB	12.0.30501.0		
		Hicrosoft Visual C++ 2015-2022 Redistributable (x64)	Microsoft Corporation	24/11/2023	20.2 MB	14.32.31326.0		
		Hicrosoft 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		
		O 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 Help link: https://support	Update information: https: authlo Comments: Copy	://www.interce rright © 2007-2	de.com/ 024 Intercede. A	All rights reserved.		

3.4.1 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.

3.5 Configuring the MyID Exchange Agent

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.

K Authlogics Local Policy Editor				- 0	×
IN File Action View Window Help					_ 8 ×
🗢 🔶 🙍 🖬 🗟 🖬 🍸					
Local Computer Policy	Authlogics Exchange Agent			Actions	
v 👰 Computer Configuration		6 m	C	Authlanias Euchanna Ana	
> Software Settings	select an item to view its description.	setung	State	Authorities exchange Ager	
> Interpretation Settings		All users must use Multi-Factor Authentication	Not configured	More Actions	•
Administrative Templates		Authentication Technology	Not configured		
> 🧮 Control Panel		IE Disable deviceless logons	Not configured		
> 🧮 Network		Enable Password-less functionality to remove the Active Directory password for logon	Not configured		
Printers		E Authlogics Authentication Server refresh time	Not configured		
Server		E Authlogics Authentication Server access timeout	Not configured		
> iii Start Menu and Taskbar		Authlogics Authentication Server Names	Not configured		
> 📫 System		E Authlogics Authentication Server Port	Not configured		
> iii Windows Components		Disable SSL with Authlogics Authentication Server	Not configured		
Classic Administrative Templates (ADM)		E Enable Debug Logging	Not configured		
Authlogics					
Authlogics Exchange Agent					
🐴 All Settings					
🗸 🏂 User Configuration					
> Software Settings					
> iii Windows Settings					
> Administrative Templates					
	Extended Standard				
10 setting(s)					



3.5.1 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
	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
	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.
Description	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
	This policy setting disables the ability to login without a separate MFA device.
Description	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
	This policy setting removes the Active Directory password from the logon page allowing users to logon with only a Username and One Time Passcode.
Description	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	
	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.
Description	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		
	This policy setting sets the maximum amount of time before refreshing the most suitable MyID Authentication Server.		
Description	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		
	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.		
Description	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.		



4 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.

0 Outlook	× +		_ _ X
$\leftrightarrow \rightarrow G$	A 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 0 2 3 0 1 5 4 3 3 4 2 0 0 1 5 0 Domain/user name:	

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.





5 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 *4*, *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.



5.1 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 *4*, *The OWA logon process overview* for details.



6 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.

With advanced configuration you can:

- Specify which Active Directory Domain Controllers are used. See section 6.1, Specifying Active Directory Domain Controllers.
- Change the Active Directory timing.

See section 6.2, Active Directory timing.

- Disable SSL connections.
 See section 6.3, Disabling SSL connections.
- Make changes to the location or enabled status of the diagnostics logging. See section 6.4, *Diagnostics logging*.

6.1 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.

6.1.1 Specifying Global Catalog Servers

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.

Note: This setting disables the auto-detect global catalog servers functionality within the MyID Exchange Agent.

6.1.2 Specifying Domain Controllers

HKLM\SOFTWARE\Authlogics\Exchange Agent\DomainDCs

The following registry key is used to specify Domain Controllers:

By default, this is blank.

Accepted values:

• One or more Domain Controller names (FQDN recommended), separated by commas.

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.

Note: This setting disables the auto-detect Domain Controller functionality within the MyID Exchange Agent.

6.2 Active Directory timing

You can set the following values in the registry:

- Domain access timeout.
- Domain controller refresh.

6.2.1 Domain access timeout

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.

6.2.2 Domain controller refresh

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 carries out another search to locate the quickest Global Catalog Server and Domain Controller.



6.3 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.

6.4 Diagnostics logging

6.4.1 LoggingEnabled

To enable or disable diagnostics logging, set the following registry value:

HKLM\SOFTWARE\Authlogics\Exchange Agent\LoggingEnabled

The default value is 0.

- Accepted values:
 - 0-disabled.
 - 1 enabled.

When you enable this value, various log files are created in the logging folder. Intercede support may request these logs from you.

6.4.2 LoggingFolder

To control the location of the log file, set the following registry value:

HKLM\SOFTWARE\Authlogics\Exchange Agent\LoggingFolder

The default value is:

C:\Program Files\Authlogics Exchange Agent\Log\

Accepted values:

• Any valid local folder with the same NTFS permissions as the default folder.