

## MyID MFA and PSM Version 5.1

# **ADFS 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<sup>®</sup> and MyID<sup>®</sup> word marks and the MyID<sup>®</sup> 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

ADFS Agent Integration Guide	1
Copyright	2
Conventions used in this document	3
Contents	4
1 Introduction	5
1.1 Licensing	5
2 Design and deployment scenarios	6
2.1 Minimum requirements	6
3 Deployment	7
3.1 Installing the MyID ADFS Agent	7
3.2 Updating the MyID ADFS Agent	10
3.3 Uninstalling the MyID ADFS Agent	11
3.3.1 Active Directory metadata	11
3.4 Configuring the MyID ADFS Agent	12
3.4.1 General settings	12
4 Configuring MFA for ADFS 3.0 on Windows Server 2012 R2	
4.1 Enabling the MyID ADFS Agent	17
4.2 Testing the ADFS 3.0 logon process	18
5 Configuring MFA for ADFS 4.0 on Windows Server 2016	
5.1 Enabling the MyID ADFS Agent	21
5.2 Configuring the ADFS 4.0 policy	23
5.3 Testing the ADFS 4.0 logon process	25
6 Configuring MFA for ADFS 5.0 / 6.0 on Windows Server 2019 / 2022	
6.1 Enabling the MyID ADFS Agent as primary authentication	
6.2 Enabling the MyID ADFS Agent as additional authentication	31
6.3 Configure the ADFS 5.0 / 6.0 policy	
6.4 Testing the ADFS 5.0 / 6.0 logon process as a primary method	
6.5 Testing the ADFS 5.0 / 6.0 logon process as an additional method	37
7 Configuration testing	
7.1 Enabling the IdP-Initiated sign-on page for ADFS 4.0, 5.0, & 6.0	
7.2 Creating a test Relying Party Trust	41
8 Advanced configuration	
8.1 Specifying Active Directory Domain Controllers	
8.1.1 Specifying Global Catalog Servers	49
8.1.2 Specifying Domain Controllers	49
8.2 Active Directory timing	
8.2.1 Domain access timeout	49
8.2.2 Domain controller refresh	50
8.3 Diagnostics logging	50
8.3.1 Enabling logging	
8.3.2 Setting the logging location	
8.4 Further ADFS configuration	



## 1 Introduction

This guide describes how to integrate MyID Multi-Factor Authentication (MFA) with Active Directory Federation Services (ADFS).

Integrating MyID MFA with ADFS is an ideal way to add strong authentication to Single Signon and Federation for cloud-based and on-premises applications.

**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 ADFS Agent does not require its own license; however you can use it 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 Design and deployment scenarios

You can install the MyID ADFS Agent directly onto a Windows Server if you are running the ADFS role.

The installation integrates the agent directly into the Microsoft ADFS Manage Console UI.

### 2.1 Minimum requirements

The MyID ADFS Agent has been designed to work with:

- ADFS 3.0 on Windows Server 2012 R2
- ADFS 4.0 on Windows Server 2016
- ADFS 5.0 on Windows Server 2019
- ADFS 6.0 on Windows Server 2022

**Note:** A minimum of ADFS 5.0 on Windows Server 2019 is required to support passwordless logons.



## 3 Deployment

The following deployment overview walks through the installation process for deploying the MyID ADFS Agent. The installation process is the same for all versions of ADFS.

This deployment section assumes that you have already installed and configured at least one MyID Authentication Server. See the *MyID Authentication Server Installation and Configuration Guide* for further information on setting up the MyID Authentication Server. In addition, you must already have configured MyID MFA user accounts for your users.

This chapter covers the following deployment related subjects:

- Installing the MyID ADFS Agent.
   See section 3.1, Installing the MyID ADFS Agent.
- Uninstalling the MyID ADFS Agent.
   See section 3.3, Uninstalling the MyID ADFS Agent.
- Updating the MyID ADFS Agent. See section 3.2, Updating the MyID ADFS Agent.
- Configuring the MyID ADFS Agent.
   See section 3.4, Configuring the MyID ADFS Agent.
   Note: For advanced configuration, see section 8, Advanced configuration.

## 3.1 Installing the MyID ADFS Agent

Perform the installation on the server while running the ADFS role.

1. Run the MyID ADFS Agent xxxxx.exe installer with elevated privileges.



2. Click Next.



3. Read the license agreement and click I accept the terms in the terms in the license agreement.

🧿 MyID ADFS Agent - InstallAware Wizard	_		Х
Licence Agreement Please carefully read the following licence agreement.		M	/iD
			^
Important			
END USER LICENCE AGREEMENT			
THE USE OF ALL INTERCEDE SOFTWARE PROVIDED VIA AUTHLO TO THIS END USER LICENCE AGREEMENT (THE AGREEMENT).	GICS	IS SUBJEC	т
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE INSTALLIN DOWNLOADING, COPYING OR OTHERWISE USING THE SOFTWAR	NG, Re.		
If you are viewing this agreement in connection with a download	d onlin		~
$\checkmark$ I accept the terms of the licence agreement			
Intercede			
< <u>B</u> ack <u>N</u> ext	>	Cance	el

### 4. Click Next.





### 5. Click Next.

The installation is being performed. The ADFS services restart.

🧿 MyID ADFS A	Agent - Install	Aware Wizard		_	×
Installing M The progra	<b>yID ADF5 Ag</b> m features you	ent I selected are bein	ig configured.		MyiD
Q	Please wait w may take seve	hile the Installatio eral minutes.	n Wizard installs f	MyID ADFS Ager	nt. This
	Status: Configuring th	ne MyID ADFS Age	ent		
Intercede ———			< <u>B</u> ack	<u>N</u> ext >	Cancel
O MyID ADFS	Agent - Install	Aware Wizard		_	
		Completing ADFS Agen	the Installat t	tion Wizard f	for MyID
My	iD	You have succ MyID ADFS Ag	essfully completer ent.	d the Installation	n Wizard for
		To close this w	izard, dick Finish.		
			< <u>B</u> ack	Finish	Cancel

### 6. Click Finish.

All necessary MyID ADFS Agent files are installed.



## 3.2 Updating the MyID ADFS 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.

Perform the update on the server while running the ADFS role.

1. Run the MyID ADFS Agent xxxx.exe installer with elevated privileges. See section 3.1, Installing the MyID ADFS Agent for details.

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

Overwrite	a	×
?	C:\Program Files\Authlogics ADFS Agent\AuthlogicsAdfsReg.ps1 Old file version: <no information="" version=""> Old file date: 19/07/2024 08:22:42 New file version: <no information="" version=""> New file date: 24/01/2025 12:01:30</no></no>	
<u>Y</u> e	Would you like to overwrite this file?       s     No     Cancel     No to All     Yes to All	

2. Click Yes.



3. Click Finish.

All necessary MyID ADFS Agent files have been updated.



## 3.3 Uninstalling the MyID ADFS Agent

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

0	Programs and Features						- 🗆	×
~	> -> 🕆 🗖 > Control P	anel > Programs > Programs and Features				<ul> <li>・ ひ</li> <li>Search Program</li> </ul>	ns and Features	P
	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	1.5.1						
	off	Organize 🔻 Uninstall Change					833 👻	?
	Install a program from the network	Name	Publisher	Installed On	Size	Version		^
		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		
		E 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		
		I Microsoft Visual C++ 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		
		B Microsoft Visual C++ 2015-2022 Redistributable (x64)	Microsoft Corporation	06/03/2024	20.6 MB	14.36.32532.0		
		B Microsoft Visual C++ 2015-2022 Redistributable (x86)	Microsoft Corporation	24/11/2023	17.6 MB	14.32.31326.0		
		👹 Microsoft Windows Desktop Runtime - 6.0.25 (x64)	Microsoft Corporation	06/03/2024	210 MB	6.0.25.33020		
		📇 MyDefrag v4.3.1	J.C. Kessels	02/01/2020	4.77 MB	4.0.0.0		
		O MyID ADFS Agent	Intercede	12/03/2024		5.0.6942.0		
		MyID Authentication Server	Intercede	06/03/2024		5.0.1000.0		
		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: http: .authlo Comments: Cop	s://www.interce yright © 2007-2	de.com/ 024 Intercede. A	All rights reserved.		

### 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 MFA information from them.

For detailed information about MyID Active Directory metadata see Authlogics KB 207256965:

support.authlogics.com/hc/en-us/articles/207256965



## 3.4 Configuring the MyID ADFS Agent

Once you have installed the MyID ADFS 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.

Group Policy Management Editor				-		×
Eile Action View Help						
🗢 🔿 🔁 📷 🔒 🛛 🖬 🛛 🍸						
Besktop Agent [CHILDSRV.CHILD.AUTHLOGICSDEMO.COM] Policy	📋 ADFS Agent	-				
Generation     Policies	Select an item to view its description.	Setting	State		Comme	ent
> 🔛 Software Settings		E Authentication Technology	Enabled		No	
> 🧾 Windows Settings		Authlogics Authentication Server access timeout	Not configured		No	
<ul> <li>Administrative Templates: Policy definitions (ADMX files) retr</li> </ul>		Authlogics Authentication Server Names	Not configured		No	
ADFS Agent		Authorities Authentication Server refresh time	Not configured		No	
Domain Controller Agent		E Disable Deviceless OTP logons	Not configured		No	
> Password Security Management		🔚 Enable Debug Logging	Not configured		No	
Windows Desktop Agent     Gontrol Panel		Authenticator App Push Authentication timeout	Not configured		No	
> iii Network		E All users must use Multi-Factor Authentication	Not configured		INO	
Printers						
Server						
> System						
> Windows Components						
C All Settings						
Preferences     Mer Configuration						
> Policies						
> iii Preferences						
		٢				>
	Extended Standard					

### 3.4.1 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	Auto / 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.
	Auto: If Auto-detect is configured and a user is enabled for multiple technologies then the chosen technology is in the following preference order: PINgrid, PINphrase, PINpass.
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 OTP logons" policy setting.

Setting	Disable Deviceless OTP logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables Deviceless OTP logons and a separate MFA device will be required to login.
	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 login with or without a separate MFA device, depending on any user specific settings.



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 <b>"Authlogics Authentication Server Names"</b> 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 ADFS 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 ADFS 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	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

## Configuring MFA for ADFS 3.0 on Windows Server 2012 R2

Microsoft ADFS has native support for Multi-Factor Authentication through the UI.

<b>\$</b>	AD FS	_ <b>_</b> ×
翰 <u>F</u> ile <u>A</u> ction <u>V</u> iew <u>W</u> indow <u>H</u> elp		_ 5 ×
🗢 🔿 🙍 🖬 📓 🖬		
AD FS	Authentication Policies	Actions
<ul> <li></li></ul>	Authentication Policies         Authentication Policies Overview         You can configure primary authentication and multifactor authentication settings globally or per relying party trust.         Learn More         Cardigating Authentication Policies         AD FS Help         Primary Authentication         Robal Settings         Authentication Methods         Externet         Forms Authentication         Ext         Device Authentication         Not enabled         Custom Settings         Per Relying Party         Multi-factor Authentication is required if there is a match for any of the specified requirements.         Global Settings         Requirements       Users/Groups         Not configured       Ext         Device       Not configured         Location       Not configured         Location       Not configured         Location       Not configured         Location       Not configured <t< td=""><td>Actions Authentication Policies Edit Global Primary Authentication Edit Global Multi-factor Authentica View New Window from Here Refresh Help</td></t<>	Actions Authentication Policies Edit Global Primary Authentication Edit Global Multi-factor Authentica View New Window from Here Refresh Help
	Per Relying Party Manage	

To configure MyID MFA for ADFS 3.0 on Windows Server 2012 R2:

- Enable the MyID ADFS Agent. See section 4.1, Enabling the MyID ADFS Agent.
- Test the logon process. See section 4.2, Testing the ADFS 3.0 logon process.



## 4.1 Enabling the MyID ADFS Agent

- 1. In the ADFS management console, open the Authentication Policies section.
- 2. Click the Edit Global Multi-factor Authentication action.



- 3. Enable the Authlogics ADFS Agent option.
- 4. Use the **User/Groups**, **Devices** and **Locations** options to configure how and when you would like to use MyID MFA authentication.

You can also enable MyID Authentication for each application through the **Per Relying Party Trust** section.

5. Click OK.



## 4.2 Testing the ADFS 3.0 logon process

 Open the Identity Provider (IdP)-Initiated sign on page. For example:

https://fs.authlogics.com/adfs/ls/idpinitiatedsignon

2. Enter your username and password.

		- • ×
G 🗇 🖉 https://fs.authlogics.com/adfs/ls/idpinitiatedsignon 🖉 🗕 C 🦉 Sign In	×	fi ★ 9
	Authlogics Single Sign On	
	Sign in with your organizational account	
	demouser@authlogics.com	
	······	1
	Sign in	
	olgi m	
	© 2013 Microsoft	

3. Click Sign in.





4. If you are using PINgrid, enter your PINgrid One Time Code.



5. Click Sign in.

You are successfully logged in to ADFS.

		_ <b>D</b> X
(⇐) (② https://fs.authlogics.com/adfs/ls/idpinitiatedsignon (₽ マ ▲ ♥) (② Sign In	×	
	Authlogics Single Sign On	
	You are signed in.	
	Sign Out	
	© 2013 Microsoft	



## 5

## Configuring MFA for ADFS 4.0 on Windows Server 2016

Microsoft ADFS has native support for Multi-Factor Authentication through the UI.



To configure MyID MFA for ADFS 4.0 on Windows Server 2016:

- Enable the MyID ADFS Agent. See section 5.1, Enabling the MyID ADFS Agent.
- Configure the ADFS policy. See section 5.2, Configuring the ADFS 4.0 policy.
- Test the logon process.

See section 5.3, Testing the ADFS 4.0 logon process.



## 5.1 Enabling the MyID ADFS Agent

- 1. In the ADFS management console, open the **Services >Authentication Methods** section.
- 2. Click the Edit Global Multi-factor Authentication action.

rimany	Multi-factor							
Coloct -	additional auti	hantication me	thada Va	umust select a	t least on	e of the foll	owing method	le.
to enab	le MFA:	nontroduori int			it iceat on	e or the roll	owing method	10
Cer	tificate Auther	ntication						
Azu	ire MFA							
Aut	hlogics ADFS	Agent						
What is	multi-factor a	uthentication	?					





3. Enable the Authlogics ADFS Agent option.

dit Authentication Methods
Primary Multifactor
$\underline{\underline{S}}\text{elect}$ additional authentication methods. You must select at least one of the following methods to enable MFA:
Cettificate Authentication
What is multifactor authentication?
OK Cancel Apply

4. Click OK.



## 5.2 Configuring the ADFS 4.0 policy

The MyID ADFS Agent works with the built-in Access Control Policies. These include policies that require MFA. Alternatively, you can create a custom policy; however, this is outside the scope of this document.

To change an existing Relying Party Trust to use an Access Control Policy that includes MFA:

- 1. In the ADFS management console, open the **Relying Party Trusts** section.
- 2. Select the relying party trust entry you want to modify.
- 3. Click Edit Access Control Policy.







4. Choose the Access Control Policy you want the Relying Party Trust to use.

This is typically Permit everyone and require MFA.

Edit Access Control Policy for Microsoft Office 3	65 Identity Platform	×
Access control policy		
Choose an access control policy:		_
Name	Description	
Permit everyone	Grant access to everyone.	
Permit everyone and require MFA	Grant access to everyone and requir	
Permit everyone and require MFA for specific g	Grant access to everyone and requir	
Permit everyone and require MFA from extranet	Grant access to the intranet users an	
Permit everyone and require MFA from unauth	Grant access to everyone and requir	
Permit everyone and require MFA, allow autom	Grant access to everyone and requir	
Permit everyone for intranet access	Grant access to the intranet users.	
Permit specific group	Grant access to users of one or more	
Policy		-
Permit users and require multifactor authentication		
		_
	OK Cancel Apply	

5. Click OK.



## 5.3 Testing the ADFS 4.0 logon process

1. Ensure the IdP-Initiated sign on page is enabled.

For more information on enabling this functionality, see section 7.1, *Enabling the IdP-Initiated sign-on page for ADFS 4.0, 5.0, & 6.0.* 

2. Ensure at least one Relying Party Trust is configured to use an Access Control Policy that requires MFA.

If you do not do this, the MFA prompt does not appear in the IdP-Initiated sign on page. To add a test Relying Party Trust, see section 7.2, *Creating a test Relying Party Trust*.

3. Open the IdP-Initiated sign on page.

For example:

https://fs.authlogics.com/adfs/ls/idpinitiatedsignon

4. Ensure that Sign in to this site is selected.



- 5. Click Sign in.
- 6. Enter your username and password.
- 7. Click Sign in.





8. If you are using PINgrid, enter your PINgrid One Time Code.



### 9. Click Sign in.

You are successfully logged in to ADFS.



6



# Configuring MFA for ADFS 5.0 / 6.0 on Windows Server 2019 / 2022

Microsoft ADFS has native support for Multi-Factor Authentication through the UI.

A feature introduced in ADFS 5.0 allows 3rd party authentication methods to be used as *primary* authentication. This allows for new logon scenarios, including passwordless logons.



To configure MyID MFA for ADFS 5.0 / 6.0 on Windows Server 2019 / 2022:

- Enable the MyID ADFS Agent. You can either:
  - Enable the MyID ADFS Agent as primary authentication. See section 6.1, Enabling the MyID ADFS Agent as primary authentication.
  - Enable the MyID ADFS Agent as additional authentication.

See section 6.2, Enabling the MyID ADFS Agent as additional authentication.

Configure the ADFS policy.

See section 6.3, Configure the ADFS 5.0 / 6.0 policy.

- Test the logon process. You can either:
  - Test the logon process with ADFS as primary authentication.
     See section 6.4, Testing the ADFS 5.0 / 6.0 logon process as a primary method.
  - Test the logon process with ADFS as additional authentication. See section 6.5, Testing the ADFS 5.0 / 6.0 logon process as an additional method.



## 6.1 Enabling the MyID ADFS Agent as primary authentication

- 1. In the ADFS management console, open the **Services >Authentication Methods** section.
- 2. Click the Edit Primary Authentication Methods action.

Edit Authentication Methods	Х
Primary Additional	
Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in. If Integrated Windows authentication method is specified, it appears as the default authentication method on browsers that support Integrated Windows authentication.	
Learn more about Azure MFA (Multi-Factor Authentication).	
Extranet	
Certificate Authentication Device Authentication Microsoft Passport Authentication	
Intranet	
Forms Authentication     Windows Authentication     Certificate Authentication     Device Authentication     Microsoft Passport Authentication	
Allow additional authentication providers as primary	
Azure MFA authentication methods will not be available until an Azure Active Directory tenant is configured. Learn More	
To use device authentication as a primary authentication method, you need to configure device registration.	
OK Cancel Apply	

3. Enable the Allow additional authentication providers as primary option.



- 4. Click OK.
- 5. Click OK again, closing the Edit Primary Authentication Methods tab.



6. Click the Edit Primary Authentication Methods action.

### The Authlogics ADFS Agent now appears as a Primary method.

Edit Authentication Methods	×
Primary Additional	
Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in. If Integrated Windows authentication method is specified, it appears as the default authentication method on browsers that support Integrated Windows authentication. Learn more about Azure MFA (Multi-Factor Authentication).	3
Extranet	
Forms Authentication Cettificate Authentication Device Authentication Microsoft Passport Authentication Authologics ADFS Agent	
Intranet	
<ul> <li>Windows Authentication</li> <li>Certificate Authentication</li> <li>Device Authentication</li> <li>Microsoft Passport Authentication</li> <li>Authlogics ADFS Agent</li> </ul>	
Allow additional authentication providers as primary	
Azure MFA authentication methods will not be available until an Azure Active     Directory tenant is configured. Learn More	
To use device authentication as a primary authentication method, you need to configure device registration.	,
OK Cancel Apply	



7. Select the MyID ADFS Agent for Extranet and Intranet, and deselect other methods as required:

Edit Authentication Methods	$\times$
Primary Additional	
Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in. If Integrated Windows authentication method is specified, it appears as the default authentication method on browsers that support Integrated Windows authentication.	•
Extranet	
Forms Authentication     Certificate Authentication     Device Authentication     Microsoft Passport Authentication     Authlogics ADFS Agent	
Intranet	
Windows Authentication Cettificate Authentication Device Authentication Microsoft Passport Authentication Authologics ADFS Agent V	
Allow additional authentication providers as primary	
Azure MFA authentication methods will not be available until an Azure Active Directory tenant is configured. Learn More	
To use device authentication as a primary authentication method, you need to configure device registration.	•
OK Cancel Apply	

8. Click OK again, closing the Edit Primary Authentication Methods tab.



## 6.2 Enabling the MyID ADFS Agent as additional authentication

- 1. In the ADFS management console, open the **Services >Authentication Methods** section.
- 2. Click the Edit Global Multi-factor Authentication action.

rimary	Multi-factor				
Select additional authentication methods. You must select at least one of the following methods to enable MFA:					
Cer Azu Aut	tificate Auther ire MFA hlogics ADFS	Agent		 	 
What is	s multi-factor a	uthentication	?		





3. Enable the Authlogics ADFS Agent option.

Edit Authentication Methods	<
Primary Multifactor	
$\underline{S}\text{elect}$ additional authentication methods. You must select at least one of the following methods to enable MFA:	
Certificate Authentication	
What is multi factor subpositionian?	
What is moundation during mucation ?	
OK Cancel Apply	

4. Click OK.



## 6.3 Configure the ADFS 5.0 / 6.0 policy

The MyID ADFS Agent works with the built in Access Control Policies. This includes policies that require MFA. Alternatively, you can create a custom policy; however, this is outside the scope of this document.

Typically, you configure an Access Control Policy to use a policy that requires MFA; however, within ADFS this means that there must be at least one primary and one additional method configured to meet the built-in MFA requirement. If a third party authentication method, such as the MyID ADFS Agent, delivers full multi-factor by itself, or a secondary authentication method is not required, you cannot use a built-in Access Control Policy that requires MFA. This is because ADFS assumes that only a single factor is being used.

**Note:** If configured as Primary authentication, you must enable **All users must use Multi-Factor Authentication**. Otherwise, a non-MFA user could bypass authentication altogether.

To change an existing Relying Party Trust to use an Access Control Policy that includes MFA:

- 1. In the ADFS management console, open the Relying Party Trusts section.
- 2. Select the relying party trust entry you want to modify.
- 3. Click Edit Access Control Policy.







4. Choose the Access Control Policy you want the Relying Party Trust to use.

This is typically Permit everyone and require MFA.

Access control policy		
Choose an access control policy:		
Name	Description	
Permit everyone	Grant access to everyone.	
Permit everyone and require MFA	Grant access to everyone and requir	
Permit everyone and require MFA for specific g	Grant access to everyone and requir	
Permit everyone and require MFA from extranet	Grant access to the intranet users an	
Permit everyone and require MFA from unauth	Grant access to everyone and requir	
Permit everyone and require MFA, allow autom	Grant access to everyone and requir	
Permit specific aroun	Grant access to users of one or more	
Policy		
Permit users and require multi-factor authentication		
	OK Cancel Apply	

5. Click OK.



## 6.4 Testing the ADFS 5.0 / 6.0 logon process as a primary method

1. Ensure the IdP-Initiated sign on page is enabled.

For more information on enabling this functionality, see section 7.1, *Enabling the IdP-Initiated sign-on page for ADFS 4.0, 5.0, & 6.0.* 

2. Ensure at least one Relying Party Trust is configured to use an Access Control Policy that requires MFA.

If you do not do this, the MFA prompt does not appear in the IdP-Initiated sign on page. To add a test Relying Party Trust, see section 7.2, *Creating a test Relying Party Trust*.

3. Open the IdP-Initiated sign on page.

For example:

https://fs.authlogics.com/adfs/ls/idpinitiatedsignon

4. Ensure that Sign in to this site is selected.



5. Click Sign in.





6. Enter your username.



7. Click Next.

S Authlogics AD FS Agent Sign In 🗴 🕂	- 🗆 X
← → C ▲ Not secure   localhost/adfs/ls/idpinitiatedsignon?client-request-id=f1a05dc2-c430-46fa-560a-0080010000eb	☆ \varTheta :
★ → C ▲ Not secure   localhost/adfs/ls/idpinitiatedsignon?client-request-id=f1a05dc2-c430-46fa-560a-0080010000eb Authlogics ADFS 5.0 Please enter your PINgrid security information.          1       2       3       1       2       3         4       1       4       1       2       3         1       5       0       2       0       0         1       3       5       2       3       0         0       4       5       2       5       0         1       3       5       4       4       5         1       3       5       4       4       5         2       3       0       0       4       5       2         1       3       5       4       4       5         1       3       5       4       4       5         2       5       0       4       5       5       0         4       3       5       4       4       5       5       0         4       3       5       4       4       5       5       0         4       3       5       4       4       5       5       5	★ ● :
	© 2018 Microsoft

8. If you are using PINgrid, enter your PINgrid One Time Code.





### 9. Click Sign in.

You are successfully logged in to ADFS.

Sign In	× +	- 0	I	×
$\leftrightarrow \   \Rightarrow \   G$	A Not secure   exchange2019.authlogicsdev.com/adfs/ls/idpinitiatedsignon?client-request-id=f1a05dc2-c430-46fa-560a-0080010000eb	\$	θ	:
← → C	▲ Not secure       exchange2019.authlogicsdev.com/adfs/ls//dpinitiatedsignon?client-request-id=f1a05dc2-c430-46fa-560a-0080010000eb         Authlogics ADFS 5.0       Nu are signed in.         • Sign in to one of the following sites:       •         Test Relying Party Trust       •         • Sign out from all the sites that you have accessed.       •         • Sign out from this site.       •         Sign Out       •	*	<b>e</b>	
				+
		© 2018	3 Micro	soft

6.5 Testing the ADFS 5.0 / 6.0 logon process as an additional method

1. Ensure the IdP-Initiated sign on page is enabled.

For more information on enabling this functionality, see section 7.1, *Enabling the IdP-Initiated sign-on page for ADFS 4.0, 5.0, & 6.0.* 

2. Ensure at least one Relying Party Trust is configured to use an Access Control Policy that requires MFA.

If you do not do this, the MFA prompt does not appear in the IdP-Initiated sign on page. To add a test Relying Party Trust, see section 7.2, *Creating a test Relying Party Trust*.

3. Open the IdP-Initiated sign on page.

For example:

```
https://fs.authlogics.com/adfs/ls/idpinitiatedsignon
```





4. Ensure that Sign in to this site is selected.



5. Click Sign in.

Sign In x +	-		×
← → C 🔺 Not secure   exchange2019.authlogicsdev.com/adfs/ls/idpinitiatedsignon?client-request-	id=4def59ef-1776-47fb-bb02-0080030000f2	Θ	:
	Authlogics ADFS 5.0		
	Sign in		
	someone@example.com		
	Password		
	Sign in		
	© 2018 Microsoft		

- 6. Enter your username and password.
- 7. Click Sign in.





8. If you are using PINgrid, enter your PINgrid One Time Code.



### 9. Click Sign in.

You are successfully logged in to ADFS.

Sign In × +	– 🗆 ×
← → C 🔺 Not secure   exchange2019.authlogicsdev.com/adfs/ls/idpinitiatedsignon?client	t-request-id=4def59ef-1776-47fb-bb02-0080030000f2 🖈 😝 :
	Authlogics ADFS 5.0
	You are signed in.
	Sign in to one of the following sites:     Test Relying Party Trust
	Sign in
	<ul> <li>Sign out from all the sites that you have accessed.</li> <li>Sign out from this site.</li> </ul>
	Sign Out
	© 2018 Microsoft



## 7 Configuration testing

To help you do configuration testing, you may want to:

- Enable the IdP-Initiated sign-on page. See section 7.1, Enabling the IdP-Initiated sign-on page for ADFS 4.0, 5.0, & 6.0.
- Create a test Relying Party Trust. See section 7.2, *Creating a test Relying Party Trust.*

## 7.1 Enabling the IdP-Initiated sign-on page for ADFS 4.0, 5.0, & 6.0

You can test the ADFS logon process by using the IdP-Initiated sign on page; however, from ADFS 4.0 on Windows Server 2016 it is disabled by default and you must enable it using PowerShell.

For more information, see:

### docs.microsoft.com/en-us/windows-server/identity/ad-fs/troubleshooting/ad-fstshoot-initiatedsignon

If you attempt to access the IdP-Initiated sign on page before enabling it, you get the following error page:



To enable the IdP-Initiated sign on page, open a PowerShell Admin command prompt and run the following command:

Set-AdfsProperties -EnableIdpInitiatedSignonPage \$true





When the IdP-Initiated sign on page is enabled, it asks you to sign in.



## 7.2 Creating a test Relying Party Trust

This test entry ensures that at least one Relying Party Trust entry exists on the ADFS server. You require a Relying Party Trust to assign an Access Control Policy to it so that the MFA login option appears in the IdP-Initiated sign on page.

**Note:** Most production systems do not require you to follow the instructions in this section; this relying party trust does not function as an actual trusted party, but allows you to test your system.

1. In the ADFS management console, open the Relying Party Trusts section.





2. Click the Add Relying Party Trust action.



3. Click Start.



4. Enter a URL to the local ADFS server.

### It should have the form:

https://<ADFSServer>/federationmetadata/2007-06/federationmetadata.xml

### Where <ADFSServer> is the URL to your ADFS server.

### For example:

https://fs.authlogicsdemo.com/federationmetadata/2007-06/federationmetadata.xml

Madd Relying Party Trust	Wizard ×	
Steps Welcome	Select an option that this wizard will use to obtain data about this relying party:	
<ul> <li>Select Data Source</li> <li>Choose Access Control Policy</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	<ul> <li>Import data about the regimp party published online or on a local network.</li> <li>Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata address (host name or URL):</li> <li>https://<adfsserver>/federationmetadata/2007-06/federationmetadata.xml</adfsserver></li> <li>Example: fs.contoso.com or https://www.contoso.com/app</li> <li>Import data about the relying party from a file</li> <li>Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file.</li> <li>Federation metadata file location:</li> </ul>	
	<ul> <li>Enter data about the relying party manually</li> <li>Use this option to manually input the necessary data about this relying party organization.</li> </ul>	
	< <u>P</u> revious <u>N</u> ext > Cancel	

5. Click Next.



6. Enter a name for the entry.

For example, Test Relying Party Trust.

🇌 Add Relying Party Trust W	fizard	×
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	Test Relying Party Trust	
Specify Display Name	Notes:	
<ul> <li>Choose Access Control Policy</li> </ul>		^
Ready to Add Trust		
Finish		
		$\sim$
	< Previous Next > Cancel	

7. Click Next.



8. Select the Permit everyone and require MFA access control policy.

-		
🖬 Add Relying Party Trust Wi:	zard	×
Choose Access Control	Policy	
Steps	Choose an access control policy:	
<ul> <li>Welcome</li> <li>Select Data Source</li> <li>Specify Display Name</li> <li>Choose Access Control Policy</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	Name       Permit everyone       Permit everyone and require MFA       Permit everyone and require MFA for specific group       Permit everyone and require MFA from extranet access       Permit everyone and require MFA from unauthenticated devices       Permit everyone and require MFA, allow automatic device registr       Permit everyone for intranet access       Permit everyone for intranet access	Description Grant access to everyone. Grant access to everyone and requir Grant access to everyone and requir Grant access to the intranet users and Grant access to everyone and requir Grant access to everyone and requir Grant access to the intranet users. Grant access to users of one or more Stant access to users of one or Stant access to users of one or more S
	I do not want to configure access control policies at this time. No application.	user will be permitted access for this rious <u>N</u> ext > Cancel



#### 9. Click Next.



10. Click Next.





11. Unselect **Configure claims issuance policy for this application**.

输 Add Relying Party Trust W	izard ×
Finish	
Steps • Welcome • Select Data Source • Specify Display Name • Choose Access Control Policy • Ready to Add Trust • Finish	The relying party trust was successfully added.
	Qose

12. Click Close.

You have now created a test relying party trust entry that uses an access control policy with MFA.

**Note:** The Test Relying Party entry does not function as an actual trusted party as it points to itself; however, its existence does make the ADFS IdP-Initiated sign on page display the MFA login screen.



## 8 Advanced configuration

You can control the advanced configuration options for MyID MFA through the Windows registry.

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

You can carry out the following:

- Specify Active Directory domain controllers.
   See section 8.1, Specifying Active Directory Domain Controllers.
- Set the timing for Active Directory. See section 8.2, Active Directory timing.
- Log diagnostic messages.
   See section 8.3, *Diagnostics logging*.
- Further ADFS customization. See section 8.4, Further ADFS configuration.



## 8.1 Specifying Active Directory Domain Controllers

The MyID ADFS 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. You can use the following registry keys; each can contain one or more server names (FQDN recommended), separated by commas.

### 8.1.1 Specifying Global Catalog Servers

HKLM\SOFTWARE\Authlogics\ADFS Agent\DomainGCs

By default, this is blank.

Accepted values:

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

The MyID ADFS 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 ADFS Agent.

### 8.1.2 Specifying Domain Controllers

HKLM\SOFTWARE\Authlogics\ADFS Agent\DomainDCs

By default, this is blank.

Accepted values:

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

The MyID ADFS 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 ADFS 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 ADFS Agent.

## 8.2 Active Directory timing

You can set the following values in the registry:

- Domain access timeout.
- Domain controller refresh.

### 8.2.1 Domain access timeout

HKLM\SOFTWARE\Authlogics\ADFS 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.

### 8.2.2 Domain controller refresh

HKLM\SOFTWARE\Authlogics\ADFS 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 Global Catalog Server and Domain Controller.

## 8.3 Diagnostics logging

You can control the diagnostics logging using the Windows registry.

### 8.3.1 Enabling logging

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

HKLM\SOFTWARE\Authlogics\ADFS 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.

### 8.3.2 Setting the logging location

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

HKLM\SOFTWARE\Authlogics\ADFS Agent\LoggingFolder

The default value is:

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

Accepted values:

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

## 8.4 Further ADFS configuration

Further information can be found online from Microsoft about customizing ADFS:

docs.microsoft.com/en-gb/archive/blogs/ramical/under-the-hood-tour-on-multifactor-authentication-in-adfs-part-1-policy