No

# ADFS Agent Integration Guide

### MyID MFA for Single Sign-On and Federation

Product Version: 5.0.6947.0

Publication date: July 2024



Call us on: +44 (0)1455 558 111 (UK & EMEA) +1 408 706 2866 (US)

Email us: info@intercede.com

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organisations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organisation, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

Intercede may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written licence agreement from Intercede, the furnishing of this document does not give you any licence to these patents, trademarks, copyrights, or other intellectual property.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

The information contained in this document represents the current view of Intercede on the issues discussed as of the date of publication. Because Intercede must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Intercede, and Intercede cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. INTERCEDE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS Document.

Copyright © 2024 Intercede. All rights reserved.

### **Table of Contents**

Introduction	3
Licensing	4
Design and Deployment Scenarios	4
Minimum Requirements	4
Deployment	5
Overview	5
Installing the MyID ADFS Agent	5
Uninstalling the MyID ADFS Agent	7
Active Directory metadata	7
Configuring the MyID ADFS Agent	8
General Settings	8
Configuring MFA for ADFS 3.0 on Windows Server 2012 R2	12
Enabling the MyID ADFS Agent	12
Testing the ADFS 3.0 logon process	13
Configuring MFA for ADFS 4.0 on Windows Server 2016	15
Enabling the MyID ADFS Agent	15
Configuring the ADFS 4.0 Policy	16
Testing the ADFS 4.0 logon process	17
Configuring MFA for ADFS 5.0/6.0 on Windows Server 2019/2022	19
Enabling the MyID ADFS Agent as primary authentication	19
Enabling the MyID ADFS Agent as additional authentication	21
Configuring the ADFS 5.0/6.0 Policy	22
Testing the ADFS 5.0/6.0 logon process as a primary method	23
Testing the ADFS 5.0 logon process as an additional method	25
Configuration Testing	28
Enabling the Idp-Initiated sign on page for ADFS 4.0, 5.0 $\&$ 6.0	28
Creating a test Relying Party Trust	30
Advanced Configuration	34
Specifying Active Directory Domain Controllers	34
Active Directory Timing	35
Diagnostics Logging	36
Further ADFS customisation	

### Introduction

#### Note Note

MyID MFA and MyID PSM were previously known as Authlogics products. Authlogics is now an Intercede Group company and the products have been rebranded accordingly. The term 'Authlogics' may still appear in certain areas of the product.

This guide includes details for integrating MyID Multi-Factor Authentication with Active Directory Federation Services (ADFS). Integrating MyID with ADFS is an ideal way to add strong authentication to Single Sign-on and Federation for cloud-based and on-prem applications.

#### Licensing

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

Note

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

### **Design and Deployment Scenarios**

The MyID ADFS Agent has been designed to be installed directly onto a Windows Server running the ADFS role.

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

#### **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

1

#### Note

A minimum of ADFS 5.0 on Windows Server 2019 is required to support password-less logons.

### 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.

#### **Overview**

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

#### Installing the MyID ADFS Agent

The installation should be performed on the server running the ADFS role.

- (1) To start the MyID ADFS Agent installation, run the MyID ADFS Agent xxxxx.exe installer with elevated privileges.
- (2) Click Next to begin the install or Cancel to quit.

🧿 MyID ADFS Agent - In:	tallAware Wizard —	• ×
	Welcome to the Installation Wizard for ADFS Agent	or MyID
	The Installation Wizard will install MyID ADFS Ager computer.	t on your
MyiD		
$\bigcirc$	WARNING: This program is protected by copyright international treaties.	law and
	To continue, click Next.	
	< <u>B</u> ack <u>N</u> ext >	Cancel

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



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

🧿 MyID ADFS Agent - Install	Aware Wizard	-		×
	Completing the Installation ADFS Agent	Wizard	for MyI	D
MyiD	The Installation Wizard is now ready t Agent on this computer. - Click Next to begin configur - Click Back to change setting - Click Cancel to exit	o configur ation s	e MyID A	DFS
	< <u>B</u> ack Ne	ext >	Car	icel

(5) The installation is being performed and the ADFS services will be restarted.



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



#### **Uninstalling the MyID ADFS Agent**

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

o	Programs and Features						- 🗆	$\times$
<	> · 🛧 🚺 > Control Pa	anel > Programs > Programs and Features				🗸 🖸 Search Program	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							
	off	Organize 👻 Uninstall Chinge					888 👻	?
	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		
		Microsoft Unified Communications Managed API 4.0	Microsoft Corporation	02/01/2020	88.0 KB	5.0.8308.0		
		Microsoft Visual C++ 2010 x64 Redistributable - 10.0	Microsoft Corporation	03/03/2022	13.8 MB	10.0.40219		
		Hicrosoft Visual C++ 2012 Redistributable (x64) - 11.0	Microsoft Corporation	02/01/2020	20.4 MB	11.0.50727.1		
		Microsoft Visual C++ 2013 Redistributable (x64) - 12.0	Microsoft Corporation	02/01/2020	20.5 MB	12.0.30501.0		
		Microsoft Visual C++ 2015-2022 Redistributable (x64)	Microsoft Corporation	06/03/2024	20.6 MB	14.36.32532.0		
		Microsoft Visual C++ 2015-2022 Redistributable (x86)	Microsoft Corporation	24/11/2023	17.6 MB	14.32.31326.0		
		Wicrosoft 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		
		O 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	ps://www.interce pyright © 2007-2	ede.com/ 024 Intercede. A	Il rights reserved.		

#### **Active Directory metadata**

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

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

#### **Configuring the MyID ADFS Agent**

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

Group Policy Management Editor				– 🗆 X
<u>File Action View H</u> elp				
◆ ⇒   2 📷   🗟 📷   🍸				
Desktop Agent [CHILDSRV.CHILD.AUTHLOGICSDEMO.COM] Policy     Computer Configuration     Dicics     Software Settings	ADFS Agent Select an item to view its description.	Setting E: Authentication Technology	State Enabled	Comment No
<ul> <li>Software Settings</li> <li>Mindows Settings</li> <li>Administrative Templates: Policy definitions (ADMX files) retr</li> <li>Administrative Templates: Policy definitions (ADMX files) retr</li> <li>Domain Controller Agent</li> <li>Domain Controller Agent</li> <li>Polyasword Security Management</li> <li>Control Panel</li> <li>Network</li> <li>Printers</li> <li>Server</li> <li>System</li> <li>System</li> <li>Windows Components</li> </ul>		Authlogics Authentication Server Access timeout     Authlogics Authentication Server Names     Authlogics Authentication Server Names     Authlogics Authentication Server Port (HTTPS/SSL)     Authlogics Authentication Server refresh time     Disable Deviceless OTP logons     Enable Debug Logging     Authenticator App Push Authentication timeout     All users must use Multi-Factor Authentication	Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured	No No No No No No
<pre>     All Settings     Preferences     Oniguration     Discies     Preferences     Perferences      Setting(s) </pre>	Extended / Standard /	<		>

#### **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 / PINphrase / Mobile 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.		
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.		

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.

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

Setting	Authlogics Authentication Server Port (HTTPS/SSL)	
Values	(1024 – 65535)	
Default	14443	
Description		
This policy setting configures the MyID Authentication Server port number which agents will use to connect to the MyID Authentication Server. The server name will be located automatically via an Active Directory search unless		

specified in the "Authlogics Authentication Server Names" policy.

If you enable this policy you must specify a TCP port number, e.g. 14443

If you disable or do not configure this policy the default port  $14443\ will be used.$ 

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

Setting	Authenticator App Push Authentication timeout	
Values	(30 – 300)	
Default	120	
Description		
This policy setting sets the maximum amount of time to wait while the MyID 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.

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

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

<b>\$</b>	AD FS
File Action View Window Help	- 8
🗢 🔿 🙍 🖬	
AD FS	Authentication Policies Actions
⊿ Service Endpoints	Authentication Policies Overview
Certificates	You can configure primary authentication and multifactor authentication settings globally or per relying party trust
☐ Claim Descriptions ⊿ <sup>™</sup> Trust Relationships	Edit Global Multi-factor Authentica
Claims Provider Trusts	Configuring Authentication Policies
Relying Party Trusts Attribute Stores	AD FS Help
A Authentication Policies	
Per Relying Party Trust	Primary Authentication
	Primary authentication is required for all users trying to access applications that use AD FS for authentication. You can use options below to configure global and custom primary authentication settings.
	Global Settings
	Authentication Methods Extranet Forms Authentication Edit
	Device Authentication Not enabled
	Custom Settings
	Per Relying Party Manage
	Multi-factor Authentication You can use options below to configure multi-factor authentication settings based on users/groups, device, and
	location data. Multi-factor authentication is required if there is a match for any of the specified requirements.
	Global Settings
	Device Not configured
6	Location Not configured
	Authentication Methods Not configured
	Custom Settings
	Per Relying Party Manage

#### **Enabling the MyID ADFS Agent**

- (1) Open the "Authentication Policies" section of the ADFS management console.
- (2) Click the Edit Global Multi-factor Authentication action in the top right corner.

Edit Global Authentication Policy
Primary Multifactor
Configure multi-factor authentication (MFA) settings.
Users/Groups
MFA is required for the following users and groups:
<u>A</u> dd
Remove
Devices MEA is required for the following devices:
Unregistered devices
Registered devices
Locations
MFA is required when accessing applications from the following locations:
Extranet
Intranet
Select additional authentication methods. You must select at least one of the following methods
to enable MFA:
Certificate Authentication Authloaics ADFS Agent
What is multi-factor authentication?
OK Cancel Apply

www.intercede.com | info@intercede.com | +44(0)1455 558 111| +1 888 646 6943

- (3) Check the "Authlogics ADFS Agent" box to enable it.
- (4) Choose how/when you would like to use MyID Authentication, e.g. by User/Group, Device or Location.

You can also enable MyID Authentication per application via the "Per Relying Party Trust" section.

(5) Click *OK* when done.

Edit Global Authentication Policy
Primary Multifactor
Configure multi-factor authentication (MFA) settings.
Users/Groups
MFA is required for the following users and groups:
<u>A</u> dd
Remove
Durizza
MFA is required for the following devices:
Unregistered devices
Registered devices
Locations
MFA is required when accessing applications from the following locations:
✓ Extranet
✓ Intranet
Select additional authentication methods. You must select at least one of the following methods
to enable MFA:
Certificate Authentication
What is multifactor authentication?
OK Cancel Apply

#### **Testing the ADFS 3.0 logon process**

(1) Open the ldp-Initiated sign on page and enter your username and password (e.g. https://fs.authlogics.com/adfs/ls/idpinitiatedsignon). Click Sign in.

Sign in Comparison and the second an	Authlogics Single Sign On
	Sign in with your organizational account
	demouser@authlogics.com
	······•
	Sign in
	© 2013 Microsoft

www.intercede.com | info@intercede.com | +44(0)1455 558 111| +1 888 646 6943

- (2) Enter the PINgrid One Time Code (if using PINgrid).
- (3) Click Sign in.



(4) You are successfully signed in to ADFS.

×	n ★ 🛱
Authlogics Single Sign On	
You are signed in.	
Sign Out	
© 2013 Microsoft	

### **Configuring MFA for ADFS 4.0 on Windows Server** 2016

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



#### **Enabling the MyID ADFS Agent**

- (1) Open the "Services / Authentication Methods" section of the ADFS management console.
- (2) Click the Edit Multi-factor Authentication Methods... action in the top right corner.

rimary	Multi-factor						
<u>S</u> elect at	additional authe le MFA:	entication meth	iods. You m	ust select at	least one of t	the following	g methods
Cer	tificate Authent	tication					
Azu	Ine MFA	Agent					
	niogica Abi 37	ngent					
What is	multi-factor au	thentication?					
				01/	<b>C</b>		01

- (3) Check the "Authlogics ADFS Agent" box to enable it.
- (4) Click *OK* when done.

		í
rimary Multi-factor		
Select additional authentication methods. You must select at leas to enable MFA:	t one of the following methods	
Certificate Authentication		
Authlogics ADF5 Agent		
What is multifactor authentication?		
OK	Cancel Apply	

#### **Configuring the ADFS 4.0 Policy**

The MyID ADFS Agent will work with the built in Access Control Policies which include "require MFA". Alternatively a custom policy can be created, however this is outside the scope of this document.

To change an existing Relying Party Trust to use an Access Control Policies which includes MFA:

- (1) Open the "Relying Party Trusts" section of the ADFS management console.
- (2) Select the relying party trust entry you want to modify.
- (3) Click Edit Access Control Policy... on the right.

翰 AD FS					- 🗆 X	
I Eile Action View Window Help					- 5	×
🔶 🤿 🗾 📰 🔢 🖬						
📔 AD FS	Relying Party Trusts				Actions	-
V Service	Display Name	Enabled	Туре	Identifier	Relying Party Trusts	•
Authentication Methods	Microsoft Office 365 Identity Platform	Yes	Non	https://lo	Add Relying Party Trust	
Certificates					View	▶
Claim Descriptions					New Window from Here	
Device Registration					Q Refresh	
Scope Descriptions					2 Help	
Web Application Proxy						
Access Control Policies					Microsoft Office 365 Identity Platform	•
Claims Provider Trusts					Update from Federation Metadata	
Application Groups					Edit Access Control Policy	
					Disable	
					Properties	
					🗙 Delete	
					👔 Help	
	<			>		
Edit the access control policy for the selected rel	ying party trust					

- (4) Choose the Access Control Policy you would like to use for the Relying Party Trust. Typically this would be "Permit everyone and require MFA".
- (5) Click OK when done.

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
and require multifactor authentication	

#### **Testing the ADFS 4.0 logon process**

- (1) Ensure the Idp-Initiated sign on page is enabled. To enable this functionality see the *"Enabling the Idp-Initiated sign on page"* section at the end of this document.
- (2) Ensure at least one Relying Party Trust has been configure to use an Access Control Policy that requires MFA, otherwise the MFA prompt will not appear in the Idp-Initiated sign on page. To add a test Relying Party Trust see the "Creating a test Relying Party Trust to ADFS 4.0 & 5.0" section at the end of this document.
- (3) Open the Idp-Initiated sign on page (e.g. <u>https://fs.authlogics.com/adfs/ls/idpinitiatedsignon</u>)
- (4) Ensure *Sign in to this site* is selected (not a Test Relying Party entry) and click *Sign in*.



- (5) Enter the username and password.
- (6) Click Sign in.

- (7) Enter the PINgrid One Time Code (if using PINgrid).
- (8) Click Sign in.



(9) You are successfully signed in to ADFS.

		🗅 Sign In 🛛 🗙 🕂	- 0	×
$\leftarrow$	С	8 Not secure https://server.authlogicsdemo.com/adfs/ls/idpinitiatedsignon?client-request-id=24b4a19f-7931-42d2-5d0a-008	30020000de A 🏠 🛈 🕼 🎕 🖤	- 📀
				Q
			SERVER.authlogicsdemo.com	0
				•
			You are signed in.	+
			Sign in to one of the following sites:	
			ADFSServer 👻	
			Sign in	
			Sign out from all the sites that you have accessed.	
			○ Sign out from this site.	
			Sign Out	
			© 2018 Microsoft	ŝ

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

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

A new feature since ADFS 5.0 allows 3<sup>rd</sup> party authentication methods to be used as primary authentication. Previous versions of ADFS would only allow 3<sup>rd</sup> party authentication methods to be used as additional methods. This allows for new logon scenarios including passwordless logons.



#### **Enabling the MyID ADFS Agent as primary authentication**

- (1) Open the "Services / Authentication Methods" section of the ADFS management console.
- (2) Click the Edit Primary Authentication Methods... action in the top right corner.

Edit Authentication Methods	×
Primary Additional	
Select authentication methods. By selecting more than one authentication method, you en users to have a choice of what method to authenticate with at sign in.	able
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	
Forms Authentication     Centricate Authentication     Device Authentication     Microsoft Passport Authentication	
Intranet	
Forms 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 config device registration.	gure
UK Cancel Ap	ріу

(3) Check Allow additional authentication providers as primary.

AD FS N	lanagement X
4	Allowing additional authentication methods as primary enables new AD FS sign on page behavior. If you have customized your AD FS web pages, first test this feature in a lab to ensure your customizations work with the new behavior. You can find further guidance here https://go.microsoft.com/fwlink/?linkid=871096.
	ОК

- (4) Click OK.
- (5) Click OK again to close the tab.
- (6) Click the *Edit Primary Authentication Methods...* action in the top right corner again. The "Authlogics ADFS Agent" now appears as a Primary method.

1 C C C C C C C C C C C C C C C C C C C			
nmary	Additional		
Select users to	authentication methods. By selecting have a choice of what method to a	a more than one authentication method, yo authenticate with at sign in.	ou enable
lf Integ authen	rated Windows authentication metho tication method on browsers that sup	od is specified, it appears as the default oport Integrated Windows authentication.	
Learn r	nore about Azure MFA (Multi-Facto	or Authentication).	
Extrar	net		
	oms Authentication		
	Certificate Authentication		
	Device Authentication		
	Acrosoft Passport Authentication		
- F	uthlogics ADFS Agent		
Interne	at		
Intran	et		
<u>ا</u> ک	Vindows Authentication		^
	ertificate Authentication		
	Jevice Authentication		
	Acrosoft Passport Authentication		
L /	uthlogics ADFS Agent		~
	w additional authentication providers	a se primany	
		, do printery	
0 f	zure MFA authentication methods Jirectory tenant is configured. Lear	will not be available until an Azure Activ <u>n More</u>	/e
0 ]	o use device authentication as a pri levice registration.	mary authentication method, you need to	configure

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



(8) Click OK to close the tab.

#### Enabling the MyID ADFS Agent as additional authentication

- (1) Open the "Services / Authentication Methods" section of the ADFS management console.
- (2) Click the Edit Multi-factor Authentication Methods... action in the top right corner.

dit Aut	henticatior	Methods						×
Primary	Additional							
<u>S</u> elect to enab	additional au ole MFA:	thentication m	ethods. You	must select	t at least (	one of the f	ollowing n	nethods
Cer	tificate Auth	entication						
	ire MFA blogics ADF	S Agent						
L								
Leam r	nore about a	dditional authe	ntication pro	viders				
				04		Connel		A
				OK		Cancel		мерту

- (3) Check the "Authlogics ADFS Agent" box to enable it.
- (4) Click OK when done.



#### **Configuring the ADFS 5.0/6.0 Policy**

The MyID ADFS Agent will work with the built-in Access Control Policies which include "require MFA". Alternatively, a custom policy can be created, however, this is outside the scope of this document.

Typically, an Access Control Policy would be configured to use a policy which requires MFA, however, within ADFS this simply means that there must be at least one primary and one additional method configured to meet the built-in "MFA" requirement. If a 3<sup>rd</sup> party authentication method, such as the MyID ADFS Agent, can deliver full multi-factor by itself, or a secondary authentication method is not required, then you cannot use a built-in Access Control Policy which requires MFA as ADFS will assume only a single factor is being used.

#### Note

If configured as Primary authentication, then "All users must use Multi-Factor Authentication" should be enabled. Otherwise, a non-MFA user could bypass authentication altogether.

To change an existing Relying Party Trust to use an Access Control Policies which includes MFA:

- (1) Open the "Relying Party Trusts" section of the ADFS management console.
- (2) Select the relying party trust entry you want to modify.
- (3) Click Edit Access Control Policy... on the right.



- (4) Choose the Access Control Policy you would like to use for the Relying Party Trust. Typically this would be "Permit everyone and require MFA".
- (5) Click OK when done.

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	Granic access to users of one of more.
Pemit users and require multi-factor authentication	

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

- (1) Ensure the Idp-Initiated sign on page is enabled. To enable this functionality see the *"Enabling the Idp-Initiated sign on page"* section at the end of this document.
- (2) Ensure at least one Relying Party Trust has been configured to use an Access Control Policy that requires MFA, **otherwise the MFA prompt will not appear** in the Idp-Initiated sign on page. To add a test Relying Party Trust see the *"Creating a test Relying Party Trust to ADFS 4.0 & 5.0"* section at the end of this document.
- (3) Open the Idp-Initiated sign on page (e.g. https://fs.authlogics.com/adfs/ls/idpinitiatedsignon):

	Sign In	× +	-		×
Authlogics ADFS 5.0         Vou are not signed in.         ® Sign in to this site.         © Sign in to one of the following sites:         Test Relying Party Trust         Sign in	$\leftrightarrow$ $\rightarrow$ G	A Not secure   localhost/adfs/ls/idpinitiatedsignon	\$	Θ	:
		Authlogics ADFS 5.0 Vou are not signed in. © Sign in to this site. © Sign in to one of the following sites: Test Relying Party Trust Sign in			

www.intercede.com | info@intercede.com | +44(0)1455 558 111| +1 888 646 6943

- (4) Ensure Sign in to this site is selected (not a Test Relying Party entry) and click Sign in.
- (5) Enter the username.
- (6) Click Next.

Sign In × +		- 🗆 X
← → C ▲ Not secure   localhost/adfs/ls/idpinitiated	signon?client-request-id=f1a05dc2-c430-46fa-560a-0080010000eb	☆ 😝 :
← → C ▲ Not secure   localhost/adfs/ls/idpinitiated	aignon?client-request-id=f1a05dc2-c430-46fa-560a-0080010000eb Authlogics ADFS 5.0 Sign in someone@example.com	<b>☆ ⊖</b> :
		© 2018 Mirmood

- (7) Enter the PINgrid One Time Code (if using PINgrid).
- (8) Click Sign in.

Authlogics AD FS Agent Sign In × +	- 0	×
← → C 🚺 Not secure   localhost/adfs/ls/idpinitiatedsignon?client-request-id=f1a05dc2-c430-46fa-560a-0080010000eb	\$	9 :
Authlogics ADFS 5.0 Please enter your PINgrid security information.		
1 3 5 2 3 0		
0     4     5     2     5     0       4     3     5     4     4     5		
Passcode Sign in		
Please contact your helpdesk for assistance.		

TOU are successionly signed in to ADFS.			
Sign In x +	-		×
← → C 🔺 Not secure   exchange2019.authlogicsdev.com/adfs/ls/idpinitiatedsignon?client-request-id=f1a05dc2-c430-46fa-560a-0080010000eb	4	9	) :
Authlogics ADFS 5.0         Vou are signed in.         Sign in to end.         Sign in to end.         Sign out from all the sites that you have accessed.         Sign out from this site.         Sign Out		6	
		2018 M	lieroroft

#### c ... . . . . . . . (9)

#### Testing the ADFS 5.0 logon process as an additional method

- (1) Ensure the Idp-Initiated sign on page is enabled. To enable this functionality see the "Enabling the *Idp-Initiated sign on page*" section at the end of this document.
- (2) Ensure at least one Relying Party Trust has been configured to use an Access Control Policy that requires MFA, otherwise the MFA prompt will not appear in the ldp-Initiated sign on page. To add a test Relying Party Trust see the "Creating a test Relying Party Trust" section at the end of this document.
- (3) Open the Idp-Initiated sign on page (e.g. <u>https://fs.authlogics.com/adfs/ls/idpinitiatedsignon</u>)

(4) Ensure Sign in to this site is selected (not a Test Relying Party entry) and click Sign in.

Sign In × +	- 🗆 X
← → C ▲ Not secure   localhost/adfs/ls/idpinitiatedsignon	☆ 😝 :
	Authlogics ADFS 5.0
	You are not signed in.
	Sign in to this site.     Sign in to one of the following sites:     Test Relying Party Trust
	Sign in
	© 2018 Microsoft

- (5) Enter the username and password.
- (6) Click Sign in.

Sign In × +	- 🗆 ×
← → C ▲ Not secure   exchange2019.authlogicsdev.com/adfs/ls/idpinitiatedsignon?client-request-	id=4def59ef-1776-47fb-bb02-0080030000f2 ☆ 🛛 🛠 😫 :
	Authlogics ADFS 5.0
	Sign in
	someone@example.com
	Password
	Sign in

(7) Enter the PINgrid One Time Code (if using PINgrid).

(8)	Click	Sign	in.

Authlogics AD FS Agent Sign In x +	- 0	×
← → C ▲ Not secure   exchange2019.authlogicsdev.com/adfs/ls/idpinitiatedsignon?client-request	-id=4def59ef-1776-47fb-bb02-0080030000f2 🏠 😫	:
	Authlogics ADFS 5.0	*
	For security reasons, we require additional information to verify your account Please enter your PINgrid security information.	
	1     5     3     5     1     4       4     1     4     1     3     5	
	Passcode Sign in	
	Please contact your helpdesk for assistance.	•

(9) You are successfully signed in to ADFS.

Sign In	× +	- 🗆 X
$\ \ \leftarrow \ \ \rightarrow \ \ G$	A Not secure   exchange2019.authlogicsdev.com/adfs/ls/idpinitiat	edsignon?client-request-id=4def59ef-1776-47fb-bb02-0080030000f2 📩 🔶 😫 :
		Authlogics ADFS 5.0
		You are signed in.
		<ul> <li>⊛ Sign in to one of the following sites:</li> <li>Test Relying Party Trust</li> </ul>
		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
O		
		© 2018 Microsoft

### **Configuration Testing**

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

An ideal way to test the ADFS logon process is to use the Idp-Initiated sign on page, however, since ADFS 4.0 on Windows Server 2016 it is disabled by default and must be enabled via PowerShell. For further information see the following Microsoft document: <u>https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/troubleshooting/ad-fs-tshoot-initiatedsignon</u>

The following error page will be shown if you access the ldp-Initiated sign on page prior to it being enabled.



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

Set-AdfsProperties -EnableIdpInitiatedSignonPage \$true

When enabled, the ldp-Initiated sign on page should ask you to sign in as follows:



#### **Creating a test Relying Party Trust**

The purpose of this section is to ensure at least one Relying Party Trust entry exists on the ADFS server so that you can assign an Access Control Policy to it in order for the MFA login option to appear in the Idp-Initiated sign on page.

ľ	Note		

This section is not required for usual production purposes.

- (1) Open the "Relying Party Trusts" section of the ADFS management console.
- (2) Click the Add Relying Party Trust... action in the top right corner.

翰 AD FS				_	D X
<u> ¶ <u> </u> <u> </u></u>					_ 8 ×
🗢 🔿 🔁 📰 🛛 🖬					
AD FS	Relying Party Trusts			Actions	
V Service	Display Name	Enabled Type	e Identifier	Relying Party Trusts	
Authentication Methods				Add Relying Party Trust	
Certificates				View	•
Claim Descriptions				New Window from Here	
Endpoints				Q Refresh	
Scope Descriptions				I Help	
Web Application Proxy					
Access Control Policies					
Claims Provider Trusts					
Application Groups					
	<		>		
				1	

#### (3) Click Start.

翰 Add Relying Party Trust Wi	izard	×
Welcome		
Steps • Welcome • Select Data Source • Choose Access Control Policy • Ready to Add Trust • Finish	Wecknee to the Add Relying Party Trust Wizard         Claims-aware applications conclaims-aware applications are web-based and use Windows and can be published through Web Application Prox for extranet access. Learn more <ul> <li></li></ul>	
	< Previous Start Cance	:

 (4) Enter a URL to the local ADFS server as follows: "
 https://fs.authlogicsdemo.com/federationmetadata/2007-06/federationmetadata.xml".

www.intercede.com | info@intercede.com | +44(0)1455 558 111| +1 888 646 6943

#### (5) Click Next.

Select Data Source	
Steps • Welcome • Select Data Source • Choose Access Control Policy • Ready to Add Trust • Finish	Select an option that this wizard will use to obtain data about this relying party:  (e) Import data about the relying party published online or on a local network. Use this control in import the necessary data and certificates from a relying party organization that publishes its federation metadata address (host name or URL): Integr//CADFSSever-/federationmetadata/2007/96/federationmetadata.xml Example: fs contoso com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Federation metadata file location: Derowse.

(6) Enter a name for the entry, e.g. "Test Relying Party Trust"

훾 Add Relying Party Trust	t Wizard
Specify Display Nam	le
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	
<ul> <li>Finish</li> </ul>	
	· · · · · · · · · · · · · · · · · · ·
	< Previous Next > Cancel

- (7) Select the Permit everyone and require MFA access control policy.
- (8) Click Next.

Steps	Change an access control policy:	
Welcome     Select Data Source     Specify Display Name     Choose Access Control     Policy     Ready to Add Trust     Finish	Name Permit everyone Permit everyone and require MFA Permit everyone and require MFA fors specific group Permit everyone and require MFA from unauthenticated devices Permit everyone for intranet access Permit e	Description Grant access to everyone. Grant access to everyone and requir Grant access to the intranet users. Crant access to the intranet users.
	Permit users and require multifactor authentication	user will be permitted access for this

(9) Nothing needs to be configured on this screen.

#### (10)Click Next.

翰 Add Relying Party Trust V	Vizard X
Ready to Add Trust	
Steps	The relving party trust has been configured. Review the following settings, and then click Next to add the
Welcome	relying party trust to the AD FS configuration database.
Select Data Source	Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Not
Specify Display Name	Specify the monitoring settings for this relying party trust.
<ul> <li>Choose Access Control Policy</li> </ul>	Relying party's federation metadata URL:
Ready to Add Trust	
Finish	Monitor relying party
	Automatically update relying party
	This solving parts is finderation materialized data was but sheaded and
	c never >
	This relation native use last undated from federation metadata on
	<pre><never></never></pre>
	< Previous Next > Cancel

(11)Uncheck Configure claims issuance policy for this application.

#### (12)Click Close.

Finish		
Steps	The relying party trust was successfully added.	
Welcome	Configure eleien income e elevitentia enetration	
Select Data Source	Conligure gains issuance policy for this application	
Specify Display Name		
Choose Access Control Policy		
Ready to Add Trust		
Finish		

A test relying party trust entry has now been created which 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.

### **Advanced Configuration**

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

#### **Specifying Active Directory Domain Controllers**

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

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

HKLM\SOFTWARE\ MyID \Authlogics Authentication Server\DomainGCs

**Default Value:** {blank}

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

HKLM\SOFTWARE\Authlogics\Authlogics Authentication Server\DomainDCs

Default Value: {blank}

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

#### **Active Directory Timing**

HKLM\SOFTWARE\Authlogics\Authentication Server\DomainAccessTimeout

Default Value: 60
Accepted Values:
0 = Disabled, indefinite timeout
1 to 120 = Timeout in seconds

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

HKLM\SOFTWARE\Authlogics\Authentication Server\DomainControllerRefeshTime

Default Value: 15 Accepted Values: 1 to 9999 = Timeout in minutes

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

#### **Diagnostics Logging**

HKLM\SOFTWARE\Authlogics\Authentication Server\LoggingEnabled

Default Value: 0
Accepted Values:
0 = Disabled
1 = Enabled

Used by components: MyID Authentication Server

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

HKLM\SOFTWARE\Authlogics\Authentication Server\LoggingFolder

Default Value: C:\Program Files\Authlogics Authentication Server\Log Used by components: MyID Authentication Server

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

#### **Further ADFS customisation**

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

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