### intercede

## Authlogics

# ADFS Agent Integration Guide

### MFA for Single Sign-On and Federation

Product Version: 4.2.1031.0

Publication date: February 2023

Call us on: +44 1344 568 900 (UK/EMEA) +1 408 706 2866 (US)

Email us: sales@authlogics.com



Authlogics, 329, Doncastle Road, Bracknell, Berkshire, RG12 8PE, UK www.authlogics.com | sales@authlogics.com | +44 1344 568 900 | +1 408 706 2866

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.

Authlogics 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 Authlogics, 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 Authlogics on the issues discussed as of the date of publication. Because Authlogics must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Authlogics, and Authlogics cannot guarantee the accuracy of any information presented after the date of publication.

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

Copyright © 2023 Authlogics. All rights reserved.

### **Table of Contents**

Introduction	3
Licensing	4
Design and Deployment Scenarios	4
Minimum Requirements	4
Deployment	5
Overview	5
Installing the Authlogics ADFS Agent	5
Uninstalling the Authlogics ADFS Agent	7
Active Directory metadata	7
Configuring the Authlogics ADFS Agent	8
General Settings	8
Configuring MFA for ADFS 3.0 on Windows Server 2012 R2	
Enabling the Authlogics ADFS Agent	
Testing the ADFS 3.0 logon process	13
Configuring MFA for ADFS 4.0 on Windows Server 2016	15
Enabling the Authlogics ADFS Agent	15
Configuring the ADFS 4.0 Policy	16
Testing the ADFS 4.0 logon process	
Configuring MFA for ADFS 5.0/6.0 on Windows Server 2019/2022	20
Enabling the Authlogics ADFS Agent as primary authentication	20
Enabling the Authlogics ADFS Agent as additional authentication	22
Configuring the ADFS 5.0/6.0 Policy	23
Testing the ADFS 5.0/6.0 logon process as a primary method	24
Testing the ADFS 5.0 logon process as an additional method	
Configuration Testing	
Enabling the Idp-Initiated sign on page for ADFS 4.0, 5.0 $\&$ 6.0	
Creating a test Relying Party Trust	
Advanced Configuration	
Specifying Active Directory Domain Controllers	
Active Directory Timing	
Diagnostics Logging	
Further ADFS customisation	





#### Introduction

This guide includes details for integrating Authlogics Multi-Factor Authentication with Active Directory Federation Services (ADFS). Integrating Authlogics 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 Authlogics ADFS Agent does not require its own licence however may only be used with a valid Authlogics 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 Authlogics 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 Authlogics 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 password-less logons.



#### Deployment

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

#### **Overview**

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

#### **Installing the Authlogics ADFS Agent**

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

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

Authlogics ADFS Agen	t - InstallAware Wizard	-		×
S	Welcome to the Installation Authlogics ADFS Agent	n Wizard	for	
igel	The Installation Wizard will install Au your computer.	thlogics ADF	S Agent	on
Auth	WARNING: This program is protected international treaties.	d by copyrig	ht law an	d
	To continue, dick Next.			
	< <u>B</u> ack	lext >	Car	ncel

(3) Review the Authlogics 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.

O Authlogics ADFS Agent - InstallAware Wizard		-		×
<u>S</u>	Completing the Installatio Authlogics ADFS Agent	n Wizard f	for	
<u>j</u>	The Installation Wizard is now read ADFS Agent on this computer.	ly to configure	e Authlogi	cs
	- Click Next to begin config	uration		
	- Click Back to change sett	ings		
	- Click Cancel to exit			
Auth				
	< <u>B</u> ack	<u>N</u> ext >	Can	cel

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

🧿 Authlogics	ADFS Agent - InstallAware Wizar	rd	-		×
	Authlogics ADFS Agent am features you selected are being	configured.	Aut	hlog	ics
Q	Please wait while the Installation This may take several minutes.	Wizard installs A	uthlogics ADFS /	Agent.	
	Status: Configuring the Authlogics ADFS	Agent			
Authlogics ——		< <u>B</u> ack	<u>N</u> ext >	Canc	el

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



#### **Uninstalling the Authlogics ADFS Agent**

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

Programs and Features							×
← → × ↑ 🖬 > Control F	Panel > Programs > Programs and Features				<ul> <li>Search Program</li> </ul>	ms 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							
	Organize Uninstall Change					800 ▼	•
Install a program from the network	Name	Publisher	Installed On	Size	Version		
	Authlogics ADFS Agent	Authlogics	2/9/2023		4.2.1018.0		
	Authlogics Authentication Server	Authlogics	2/9/2023		4.2.1030.0		
	🧿 Authlogics Domain Controller Agent	Authlogics	2/21/2023		4.2.1030.0		
	🧿 Authlogics Windows Desktop Agent	Authlogics	2/21/2023		4.2.1030.0		
	📀 Google Chrome	Google LLC	2/6/2023		109.0.5414.120		
	Microsoft Visual C++ 2010 x64 Redistributable - 10.0	Microsoft Corporation	2/1/2023	13.8 MB	10.0.40219		
	Microsoft Visual C++ 2015-2022 Redistributable (x64)		2/20/2023	20.2 MB	14.32.31326.0		
	Microsoft Visual C++ 2015-2022 Redistributable (x86)		2/20/2023	17.6 MB	14.32.31326.0		
	VM Ware Tools	VMware, Inc.	2/20/2023	96.7 MB	12.1.5.20735119		
	Authlogics Product version: 4.2.1018.0	Update information: http	s://authlogics.				
	Help link: https://suppor	rt.authlo Comments: Co	vright © 2007-	2023 Authlogics	s. All rights reserved.		

#### **Active Directory metadata**

Uninstalling Authlogics does NOT remove the metadata from user accounts in the Active Directory. If you are planning to completely remove Authlogics 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 Authlogics information from it.

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



#### **Configuring the Authlogics 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 Authlogics Local policy settings use the Authlogics Local Policy Editor shortcut on the desktop or start menu.



#### **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			

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 Authlogics 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 Authlogics 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 Authlogics Authentication Servers.



Setting	Authlogics Authentication Server Port (HTTPS/SSL)	
Values	(1024 - 65535)	
Default	14443	
Description		

This policy setting configures the Authlogics Authentication Server port number which agents will use to connect to the Authlogics 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 Authlogics Authentication Server.			
If you enable this policy you must specify the interval value in minutes to wait before refreshing which Authlogics Authentication Server to use.			

If you disable or do not configure this policy the agent will wait for 60 minutes before refreshing which Authlogics 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 Authlogics 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 Authlogics Authentication Server			

This policy setting sets the maximum amount of time to wait while locating an Authlogics 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 Authlogics 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 Authlogics Authentication Server.



Setting Enable Debug Logging			
Values	Enabled / Disabled		
Default Disabled			
Description			
This policy setting applies dobug logging on all convers supping the agent. This should only be enabled if			

This policy setting enables debug logging on all servers running the agent. This should only be enabled if requested by an Authlogics 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		_ <b>_</b> ×
翰 <u>F</u> ile <u>A</u> ction <u>V</u> iew <u>W</u> indow <u>H</u> elp			_ <i>8</i> ×
🗢 🔿 📶 🚺 🖬			
🛗 AD FS	Authentication Policies		Actions
⊿ Service Endpoints	Authentication Policies Overview	^	Authentication Policies
Certificates			Edit Global Primary Authentication
Claim Descriptions	You can configure primary authentication and multifactor authentication settings globally or per relying particular	rty trust.	Edit Global Multi-factor Authentica
⊿ In Trust Relationships ☐ Claims Provider Trusts	Learn More		View 🕨
Relying Party Trusts	Configuring Authentication Policies		New Window from Here
Attribute Stores	AD FS Help		Refresh
⊿ Authentication Policies Per Relying Party Trust	Primary Authentication		🛿 Help
	Primary authentication is required for all users trying to access applications that use AD FS for authenticati You can use options below to configure global and custom primary authentication settings.	ion.	
	Global Settings		
	Authentication Methods Extranet Forms Authentication Ed	dit _	
	Intranet Forms Authentication Device Authentication Not enabled	-	
	Custom Settings Per Relying Party Ma	anage	
		anage	
	Multi-factor Authentication		
	You can use options below to configure multi-factor authentication settings based on users/groups, devic location data. Multi-factor authentication is required if there is a match for any of the specified requirement		
	Global Settings		
	Requirements Users/Groups Not configured Ed	dit	
	Device Not configured Location Not configured		
	Authentication Methods Not configured		
	Custom Settings		
	-	anage	
	r or noging r orty		

#### **Enabling the Authlogics 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 Authent	ication Polic	y	×
Primary	Multi-factor				
Configu	ire multi-factor	authentication (MFA) settings.			
Users	/Groups				
MFAi	s required for t	he following users and groups:			
				Ad	ld
				Ren	nove
Devic	es				
MFAi	s required for t	he following devices:			
	nregistered de	vices			
- F	egistered devi	ces			
Locat	ons				
		n accessing applications from t	he following loca	tions:	
	xtranet				
	tranet				
<u>S</u> elect to enab	additional auth Ie MFA:	entication methods. You must s	elect at least on	e of the following i	nethods
	tificate Auther				
Aut	hlogics ADFS	Agent			
What is	multi-factor a	uthentication?			
			OK	Cancel	Apply
			UN	Calice	періу



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

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

(5) Click OK when done.

Edit Global Authentication Policy	x
Primary Multifactor	
Configure multi-factor authentication (MFA) settings.	
Users/Groups	
MFA is required for the following users and groups:	
<u>A</u> dd	
Remove	٦
	_
Devices MFA is required for the following devices:	
Registered devices	
MFA is required when accessing applications from the following locations:	
✓ Intranet	
Select additional authentication methods. You must select at least one of the following method	ls
to enable MFA:	
Certificate Authentication	
Authlogics ADFS Agent	
What is multi-factor authentication?	-
OK Cancel Anniv	
OK Cancel Apply	

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

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

🗲 💮 🧭 https://fs.authlogics.com/adfs/ls/idpinitiatedsignon 🛛 🖓 🕶 🖴 C 🖉 Sign In	× □ ×
	Authlogics Single Sign On
	Sign in with your organizational account
	demouser@authlogics.com
	Sign in



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

C () C Authlogics.com/adfs/ls/idpinitiatedsignon P = 🕯 C C Authlogics ADFS Agent Sig ×	
	Authlogics Single Sign On
	Welcome AUTHLOGICS\steve
	For security reasons, we require additional information to verify your account
	Please enter your PINgrid security information.
	1 1 4 5 1 4
	0 2 2 2 4 3
	1 2 2 5 3 3 4 4 5 1 2 3
	0 4 0 5 3 5
	1 5 0 3 0 0
	······ •
	Sign in Ret
	Please contact your helpdesk for assistance.
	© 2013 Microsoft

(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 Authlogics 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.

	Multi-factor				
rimary					
to enab	le MFA:		You must select at I	east one of the foll	owing methods
	tificate Authentica	tion			
	ire MFA				
Aut	hlogics ADFS Age	ent			
What is	multi-factor authe	entication?			
			ок	Cancel	

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

rimary	Multifactor					
Select		entication meth	ods. You mus	t select at lea	ast one of the foll	owing methods
Az	rtificate Authen ure MFA					
V Au	thlogics ADFS	Agent				
What i	s multi-factor a	uthentication?				

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

The Authlogics 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.





- (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.

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
Permit users	
Permit users and require multi-factor 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.

O Authlogics AD FS Agent Sign In x +					
← → C 🔺 Not secure   localhost/adfs/ls/idpinitiatedsignon?client-request-id=a8edb4b0-ea8f-4a27-0501-0080030000f9	☆	θ	:		
Authlogics ADFS 4.0			*		
For security reasons, we require additional information to verify your account (testuser@mycompany.com) Please enter your PINgrid security information.	ı				
2       0       4       3       1       4         2       2       3       1       5       3         5       5       3       1       0       3					
1 0 4 5 5 3					
1 5 0 2 2 0					
Passcode Sign in					
Please contact your helpdesk for assistance.					





(9) You are successfully signed in to ADFS.



### 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 Authlogics 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.

rimary	Additional	
	authentication methods. By selecting more than one authentication method, you enable b have a choice of what method to authenticate with at sign in.	e
	rated Windows authentication method is specified, it appears as the default tication method on browsers that support Integrated Windows authentication.	
Learn r	nore about Azure MFA (Multi-Factor Authentication).	
Extrar	iet	
	oms Authentication	1
	Certificate Authentication	
	Device Authentication	
	licrosoft Passport Authentication	
Intran	et	
F	oms Authentication	1
	Vindows Authentication	
	Certificate Authentication	
	Device Authentication	
	licrosoft Passport Authentication	
Allo	w additional authentication providers as primary	
• <sup>4</sup>	zure MFA authentication methods will not be available until an Azure Active birectory tenant is configured. <u>Learn More</u>	
	o use device authentication as a primary authentication method, you need to configure levice registration.	e



(3) Check Allow additional authentication providers as primary.

AD FS Management X	
Allowing additional authentication methods as primary anables 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/fwilnk/?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.

dit Aut	hentication Methods	
rimary	Additional	
users to If Integr authent	authentication methods. By selecting more than one authentication method, you enable have a choice of what method to authenticate with at sign n. ated Windows authentication method is specified, it appears as the default ication method on browsers that support Integrated Windows authentication. nore about Azure MFA (Multi-Factor Authentication).	e
Extran	et	
	oms Authentication	1
	Certificate Authentication	
П	Device Authentication	
	ficrosoft Passport Authentication	
A 🗌	uthlogics ADFS Agent	
	Vindows Authentication   etificate Authentication  ficrosoft Passport Authentication  uthlogics ADFS Agent  v	
	w additional authentication providers as primary	
	zure MFA authentication methods will not be available until an Azure Active irrectory tenant is configured. <u>Learn More</u>	
	o use device authentication as a primary authentication method, you need to configure evice registration.	e
	OK Cancel Apply	

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



(8) Click OK to close the tab.

#### **Enabling the Authlogics 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.



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



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

The Authlogics 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 Authlogics 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.

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.

Image: Second secon						× F >
AD FS	Relying Party Trusts				Actions	
✓ Service Attribute Stores	Display Name	Enabled	Туре	Identifier	Relying Party Trusts	-
Authorization Methods	Microsoft Office 365 Identity Platform	Yes	Non	https://logir	Add Relying Party Trust	_
Certificates					View	•
Claim Descriptions					New Window from Here	
Device Registration Endpoints					Q Refresh	
Scope Descriptions					P Help	
📔 Web Application Proxy					-	
Access Control Policies					Microsoft Office 365 Identity Platform	-
Relying Party Trusts Claims Provider Trusts					Update from Federation Metadata	
Application Groups					Edit Access Control Policy	
					Disable	
					Properties	
					🗙 Delete	
					👔 Help	
	<			>		



- (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.

Edi	t Access Control Policy for Microsoft Office 3	55 Identity Platform	Х
Ac	cess control policy		
Edit Access Control Policy for Microsoft Office 365 Identity Platform         Access control policy         Choose an access control policy:         Name       Description         Permit everyone and require MFA       Grant access to everyone and require.         Permit everyone and require MFA from sectara.       Grant access to everyone and require.         Permit everyone and require MFA from sectara.       Grant access to everyone and require.         Permit everyone and require MFA from unast.       Grant access to everyone and require.         Permit everyone and require MFA from sectara secses to everyone and require.       Permit access to everyone and require.         Permit everyone and require MFA from unast.       Grant access to everyone and require.         Permit everyone for intranet access       Grant access to everyone and require.         Permit everyone for intranet access       Grant access to users of one or more         Permit specific group       Grant access to users of one or more         Policy       Permit users         Permit users       and require multifactor authentication			
	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 specific group	Grant access to users of one or more	
	Permit users		
		OK Cancel Apply	

#### 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	× +	- 🗆 ×
← → C ▲ Not se	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





- (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 × +		- 🗆 ×
← → C ▲ Not secure   localhost/adfs/ls/idpinitiat	edsignon?client-request-id=f1a05dc2-c430-46fa-560a-0080010000eb	☆ 😬 :
← → C ▲ Not secure   localhost/adfs/fs/idpinitiat	edsignon?client-request-id=f1a05dc2-c430-46fa-560a-0080010000eb Authlogics ADFS 5.0 Sign in someone@example.com	<b>☆ (9) :</b>
		€ 2018 Microsoft

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

3 Authlogics AD FS Agent Sign In × +	- 🗆 ×
← → 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         4       3       5       4       4       5	
Passcode Sign in	
Please contact your helpdesk for assistance.	



Sign In	× +	- [		×
$\leftrightarrow$ $\rightarrow$ C	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/i/dpinitiatedsignon?client-request-id=f1a05dc2-c430-46fa-560a-0080010000eb Authlogics ADFS 5.0 Nou 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 from this site. Sign Out	*	Θ	
		© 20'	18 Micro	osoft

#### (9) You are successfully signed in to ADFS.

#### 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 Idp-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. https://fs.authlogics.com/adfs/ls/idpinitiatedsignon)





(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.

🕙 Sign In	× +	
e → c	A Not secure   exchange2019.authlogicsdev.com/adfs/ls/idpinitiatedsign	on?client-request-id=4def59ef-1776-47fb-bb02-0080030000f2 🖈 😫
		Authlogics ADFS 5.0
		Sign in
		someone@example.com
		Password
		Sign in
		© 2018 Microsoft

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

1	0		an in
	ð	) Click Sig	gn m.

Authlogics AD FS Agent Sign In X +	- 0	×
← → C A Not secure   exchange2019.authlogicsdev.com/adfs/ls/idpinitiatedsignon?client-request-	id=4def59ef-1776-47fb-bb02-0080030000f2	<b>e</b> :
	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	
	4     2     5     3     1     4       1     0     3     5     2     0	
	3 2 5 2 2 0	
	2 0 4 0 3 0	
	Passcode	
	Sign in	
	Please contact your helpdesk for assistance.	

(9) You are successfully signed in to ADFS.

Sign In X + - C X				
C 🔺 Not secure   exchange2019.authlogicsdev.com/adfs/ls/idpinitiatedsignon?client-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			
	Sign out from all the sites that you have accessed.			
	Sign out from this site.			
	Sign Out			
	© 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: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/troubleshooting/ad-fs-tshoot-initiatedsignon

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



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

Set-AdfsProperties -EnableIdpInitiatedSignonPage \$true







When enabled, the Idp-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.

Note	Э
------	---

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.

🇌 AD FS					_	$\Box$ $\times$
I Eile Action View Window Help						_ 8 ×
🗢 🔿 🔁 📰 🔽 🖬						
AD FS	Relying Party Trusts				Actions	
Service     Attribute Stores	Display Name	Enabled	Туре	Identifier	Relying Party Trusts	•
Authentication Methods				1	Add Relying Party Trust	
Certificates					View	•
Claim Descriptions					New Window from Here	
Device Registration Endpoints					Q Refresh	
Endpoints Scope Descriptions						
Web Application Proxy					👔 Help	
Access Control Policies						
Relying Party Trusts						
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	Webcome to the Add Relying Party Trust Wizard         Claims-aware applications consume claims in security tokens to make authentication and authorizant decisions. Non-claims-aware applications are web-based and use Windows proxy for extranet access. Learn more <ul> <li>Qlaims aware</li> <li>Qlaims aware</li> <li>Mon claims aware</li> </ul>	
	< <u>Previous</u> <u>Start</u> Cance	1

(4) Enter a URL to the local ADFS server as follows: https://<ADFSServer>/federationmetadata/2007-06/federationmetadata.xml



(5)	Click Next.

훾 Add Relying Party Trust	Wizard X
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:  Import data about the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata address (nost name or URL): Intro://cADFSServers/Aderationmetadata/2007/06/Federationmetadata.xml Example: fa cortoso com rhttps://www.cortoso.com/app Import data about the relying party rown a file Use this option to import the necessary data and certificates from a relying party organization that has exported the source of the file. Federation metadata of 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: Federation metadata file location: Federation to manually input the necessary data about this relying party organization.
	< <u>P</u> revious <u>N</u> ext > Cancel

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

翰 Add Relying Party Trust Wizard		
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	N <u>o</u> tes:	
<ul> <li>Choose Access Control Policy</li> </ul>	^	]
<ul> <li>Ready to Add Trust</li> </ul>		
Finish		
	· · · · · · · · · · · · · · · · · · ·	
	< <u>P</u> revious <u>N</u> ext > Cancel	

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

Steps	Choose 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 from unauthenticated devices Permit everyone and require MFA from unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Permit everyone for intranet access Parmit execution or unauthenticated devices Parmit execution or	Description Grant access to everyone. Grant access to everyone and requir Grant access to everyone and requir Grant access to the intranet users an Grant access to everyone and requir Grant access to everyone and requir Grant access to the intranet users. Grant access to the intranet users.
	Permit users and require multifactor authentication	

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

#### (10)Click Next.

🏟 Add Relying Party Trust W	fizard X
Ready to Add Trust	
Steps	The relying 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 Note
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	
Fnish	<ul> <li>Monitor relying party</li> <li>Automatically update relying party</li> <li>This relying party's federation metadata data was last checked on:</li> <li>&lt; never &gt;</li> <li>This relying party was last updated from federation metadata on:</li> <li>&lt; never &gt;</li> </ul>
	< Previous Next > Cancel



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

#### (12)Click Close.

🍿 Add Relying Party Trust \	Vizard	×
Finish		
Steps         Welcome         Select Data Source         Specify Display Name         Choose Access Control Policy         Placy         Ready to Add Trust	The relying party trust was successfully added.	
	Qose	1

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 Authlogics 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 Authlogics support engineer.

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

The Authlogics 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\Authlogics\Authlogics Authentication Server\DomainGCs

Default Value: {blank}

The Authlogics 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 Authlogics 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 Authlogics 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: Authlogics 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 Authlogics support engineer.

HKLM\SOFTWARE\Authlogics\Authentication Server\LoggingFolder

Default Value: C:\Program Files\Authlogics Authentication Server\Log Used by components: Authlogics 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-multi-factor-authentication-in-adfs-part-1-policy

