

# 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](mailto:sales@authlogics.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.

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 .....	12
Enabling the Authlogics ADFS Agent .....	12
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 .....	17
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 .....	26
Configuration Testing.....	29
Enabling the Idp-Initiated sign on page for ADFS 4.0, 5.0 & 6.0 .....	29
Creating a test Relying Party Trust .....	31
Advanced Configuration.....	35
Specifying Active Directory Domain Controllers.....	35
Active Directory Timing .....	36
Diagnostics Logging.....	37
Further ADFS customisation .....	37



## 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.

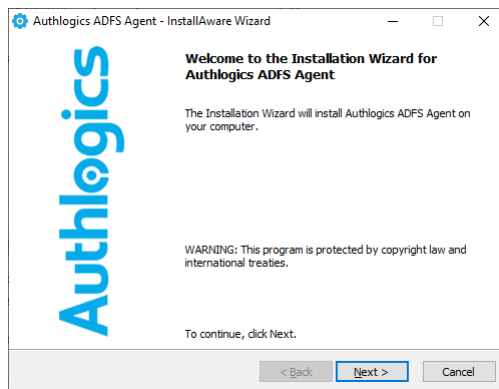
### Overview

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.

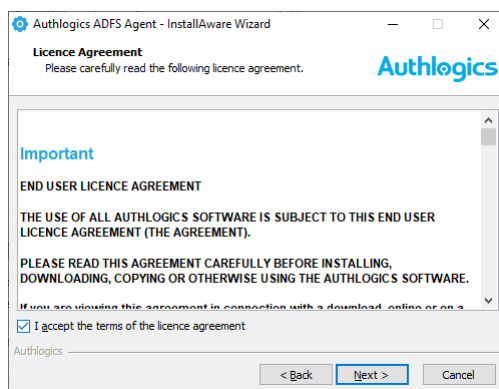
### Installing the Authlogics ADFS Agent

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

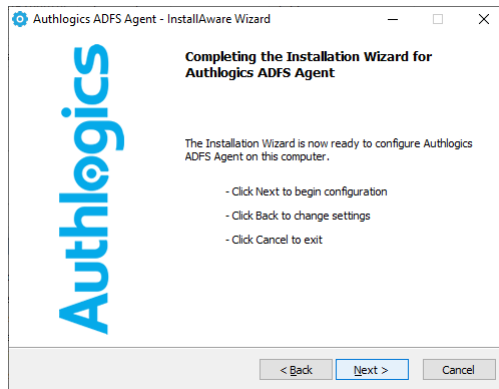
- (1) To start the Authlogics ADFS Agent installation, run the Authlogics ADFS Agent xxxxx.exe installer with elevated privileges.
- (2) Click Next to begin the install or Cancel to quit.



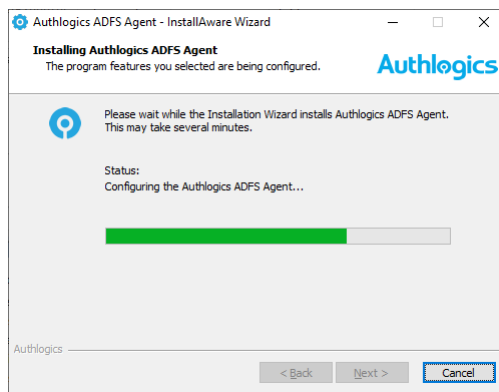
- (3) Review the Authlogics Licence Agreement, check the *I accept the terms of the licence agreement* box and click *Next*.



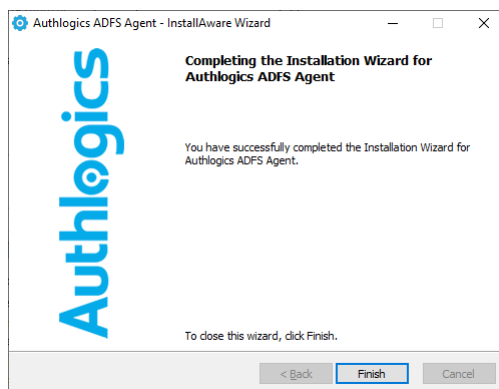
- (4) Click *Next* to begin the install or *Cancel* to quit.



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

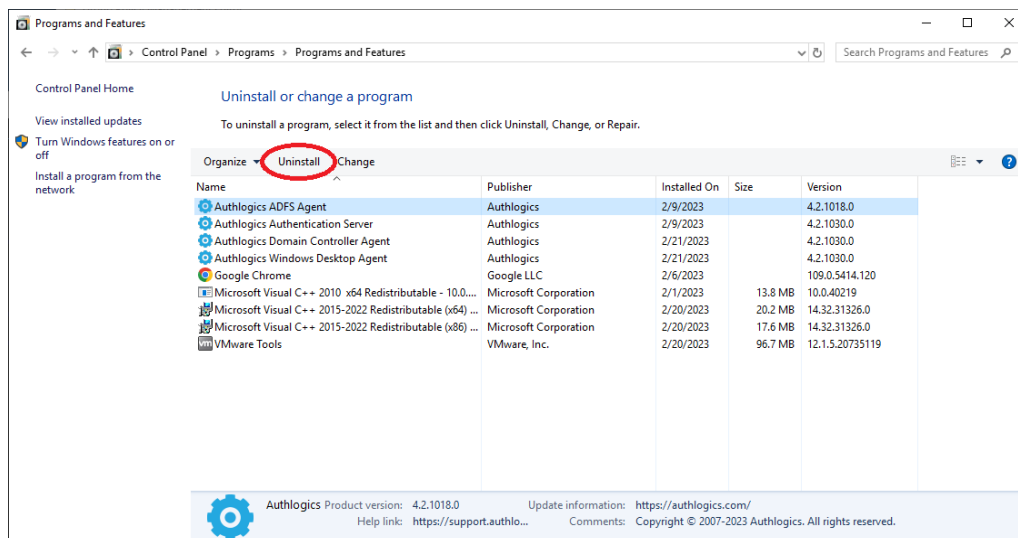


- (6) All necessary Authlogics ADFS Agent files have been installed. Click *Finish* to complete the installation process.



## 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:



## 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.

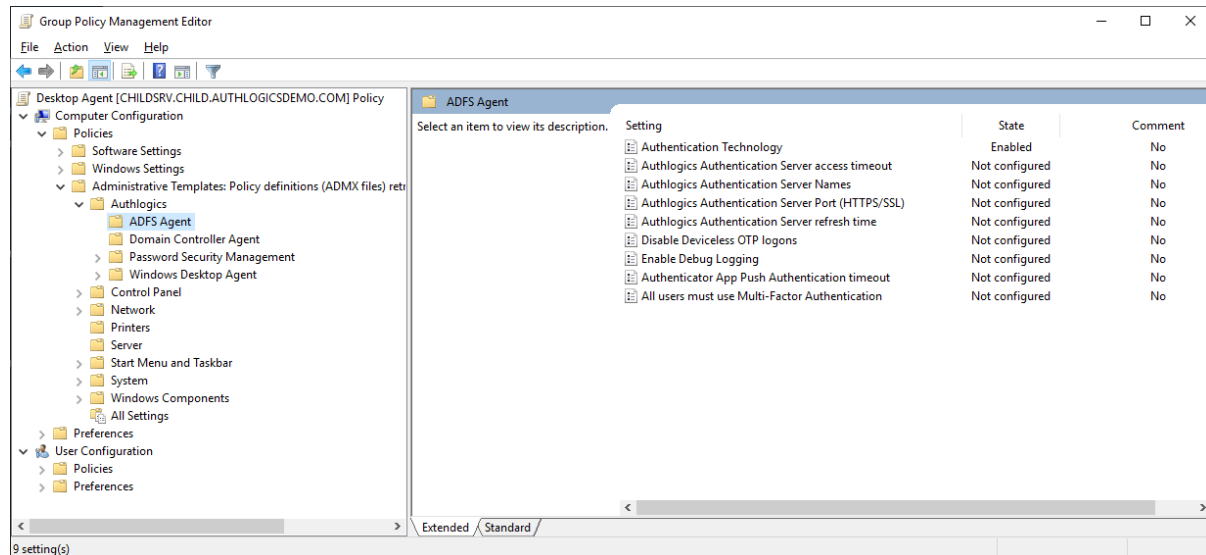
For detailed information about Authlogics AD metadata see Authlogics KB207256965 (<https://support.authlogics.com/hc/en-us/articles/207256965>).





## 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	
<p>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.</p> <p>If you enable this policy then all users must be provisioned for MFA to access the agent.</p> <p>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.</p>	



<b>Setting</b>	Authentication Technology
<b>Values</b>	Auto / PINgrid / PINphrase / PINphrase / Mobile Push/ Disabled
<b>Default</b>	Disabled
<b>Description</b>	
<p>This policy setting configures the authentication technology which the agent will use.</p> <p>If you enable this policy you must specify which authentication technology to use.</p> <p>If you disable or do not configure this policy the agent will automatically detect the technology the user is configured to use.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>PINpass: A PINpass logo will be displayed.</p> <p>Disabled: A generic Authlogics icon will be displayed only and Deviceless OTP is also disabled regardless of the "Disable Deviceless OTP logons" policy setting.</p>	

<b>Setting</b>	Disable Deviceless OTP logons
<b>Values</b>	Enabled / Disabled
<b>Default</b>	Disabled
<b>Description</b>	
<p>This policy setting disables Deviceless OTP logons and a separate MFA device will be required to login.</p> <p>If you enable this policy a user must login to the agent using a separate MFA device.</p> <p>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.</p>	

<b>Setting</b>	Authlogics Authentication Server Names
<b>Values</b>	Any DNS based server address (CSV)
<b>Default</b>	{blank}
<b>Description</b>	
<p>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.</p> <p>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</p> <p>If you disable or do not configure this policy the Active Directory will be searched to locate one or more Authlogics Authentication Servers.</p>	



<b>Setting</b>	Authlogics Authentication Server Port (HTTPS/SSL)
<b>Values</b>	(1024 - 65535)
<b>Default</b>	14443
<b>Description</b>	
<p>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.</p> <p>If you enable this policy you must specify a TCP port number, e.g. 14443</p> <p>If you disable or do not configure this policy the default port 14443 will be used.</p>	

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

<b>Setting</b>	Authenticator App Push Authentication timeout
<b>Values</b>	(30 - 300)
<b>Default</b>	120
<b>Description</b>	
<p>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.</p> <p>If you disable or do not configure this policy the ADFS Agent will wait for 120 seconds for a response.</p>	

<b>Setting</b>	Authlogics Authentication Server access timeout
<b>Values</b>	(0 - 120)
<b>Default</b>	5
<b>Description</b>	
<p>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.</p> <p>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.</p> <p>If you disable or do not configure this policy the agent will wait for 5 seconds while locating an Authlogics Authentication Server.</p>	

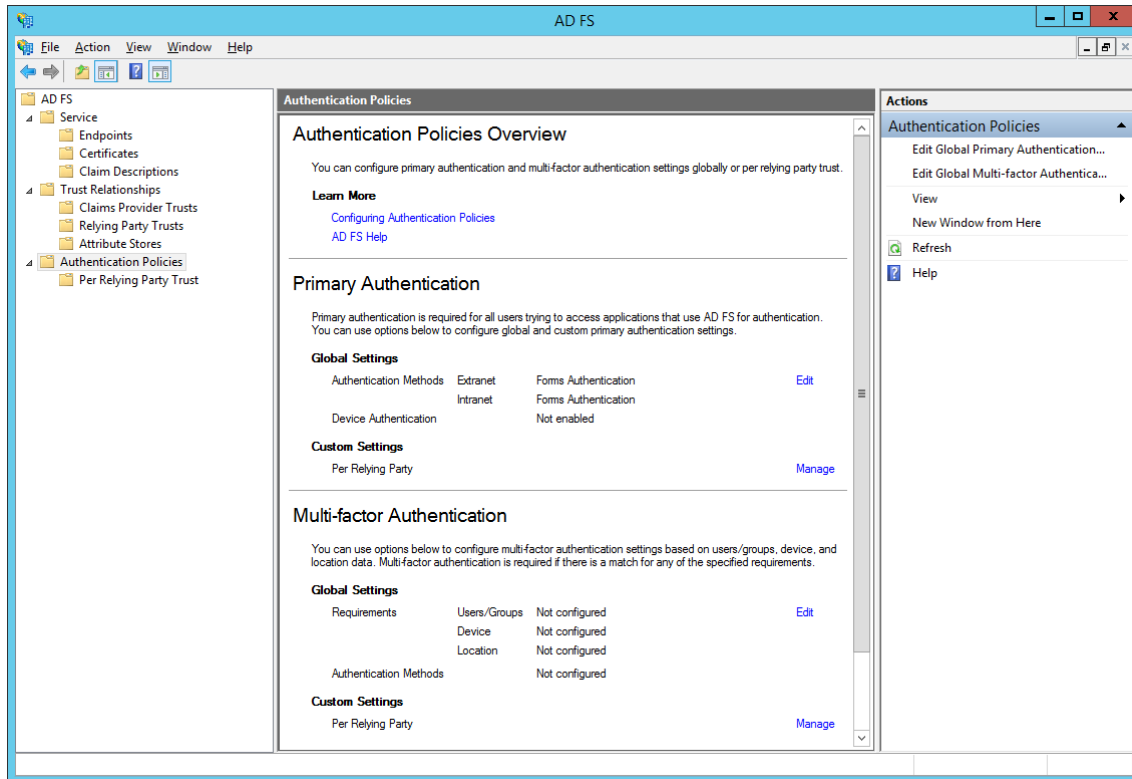


<b>Setting</b>	Enable Debug Logging
<b>Values</b>	Enabled / Disabled
<b>Default</b>	Disabled
<b>Description</b>	
<p>This policy setting enables debug logging on all servers running the agent. This should only be enabled if requested by an Authlogics Support engineer. This setting performs the same function as manually setting the LoggingEnabled registry key to 1.</p> <p>If you enable this policy debug logging will be active.</p> <p>If you disable or do not configure this policy then debug logging will not be active.</p>	



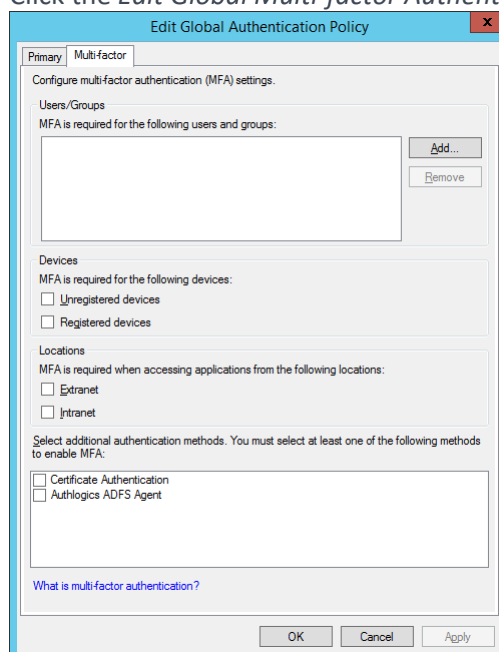
## Configuring MFA for ADFS 3.0 on Windows Server 2012 R2

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

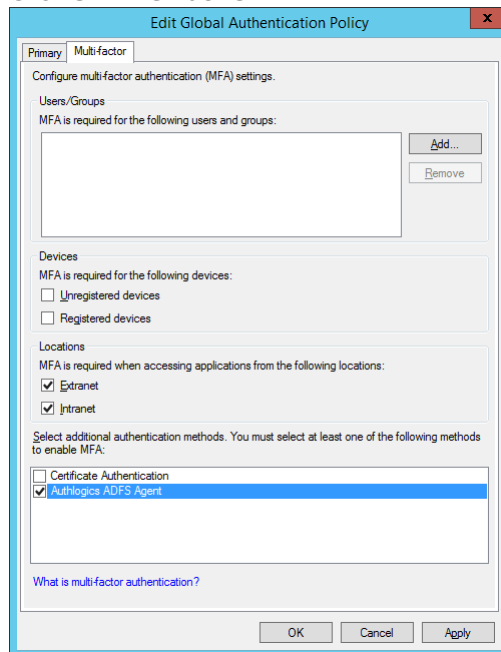


### Enabling the Authlogics ADFS Agent

- (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.

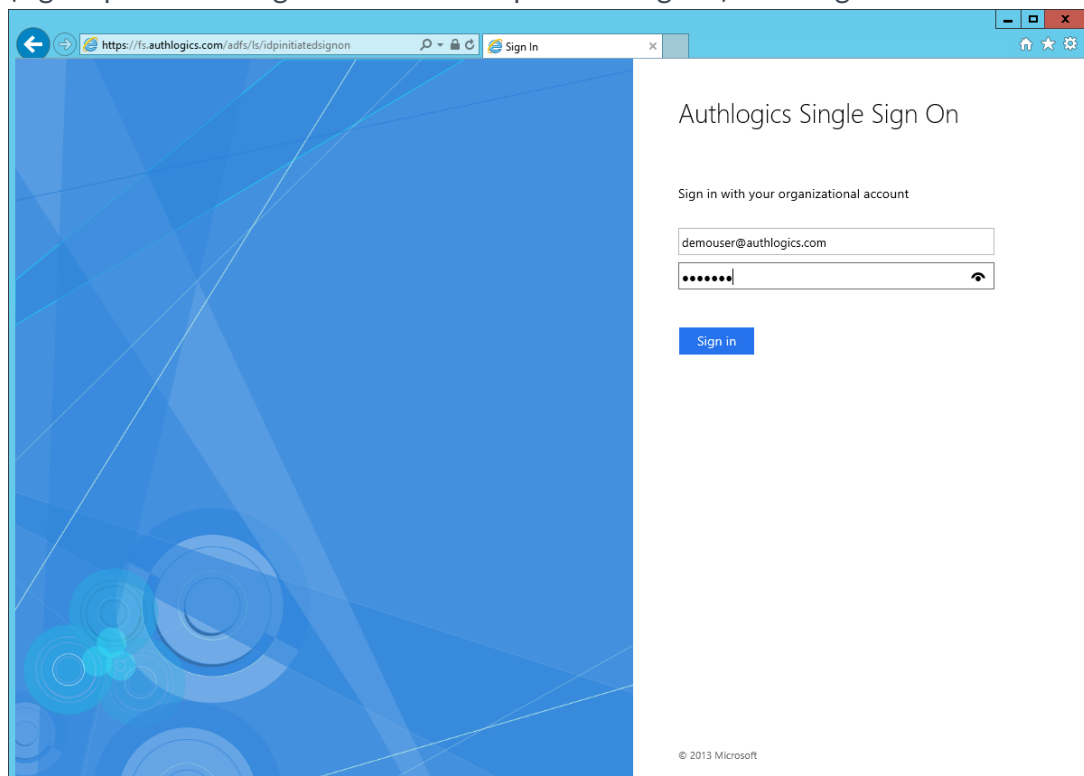


- (3) Check the “Authlogics ADFS Agent” box to enable it.
- (4) Choose how/when you would like to use Authlogics Authentication, e.g. by User/Group, Device or Location.  
You can also enable Authlogics Authentication per application via the “Per Relying Party Trust” section.
- (5) Click *OK* when done.

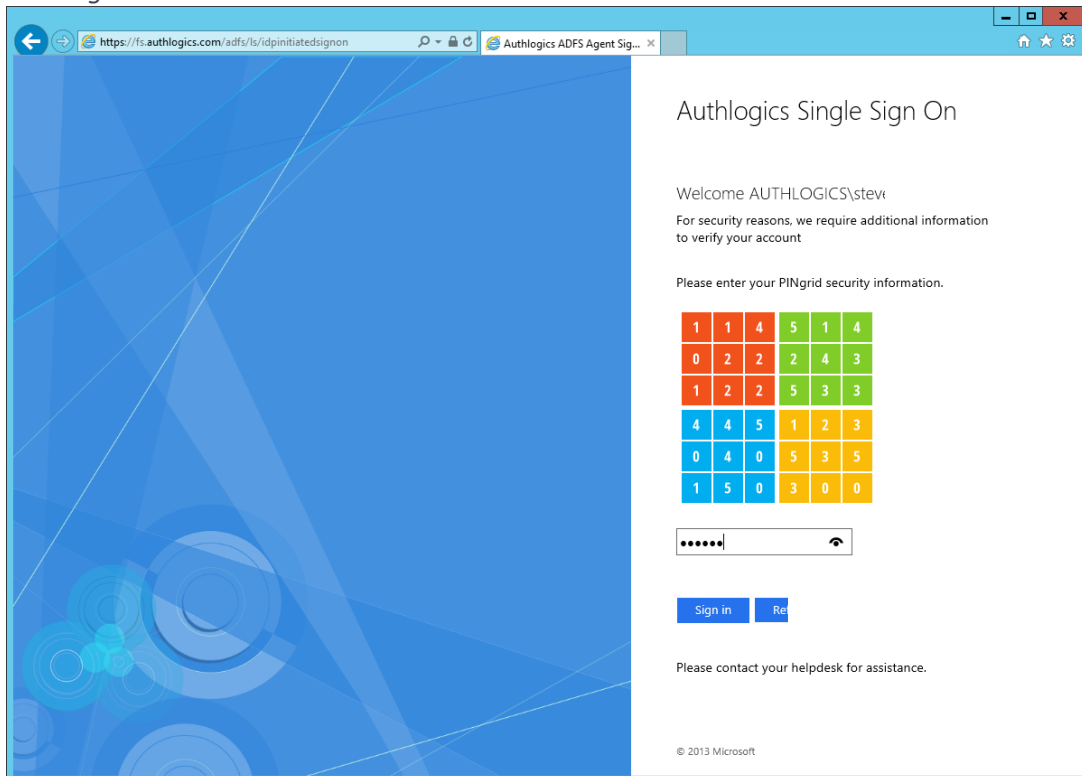


## Testing the ADFS 3.0 logon process

- (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.

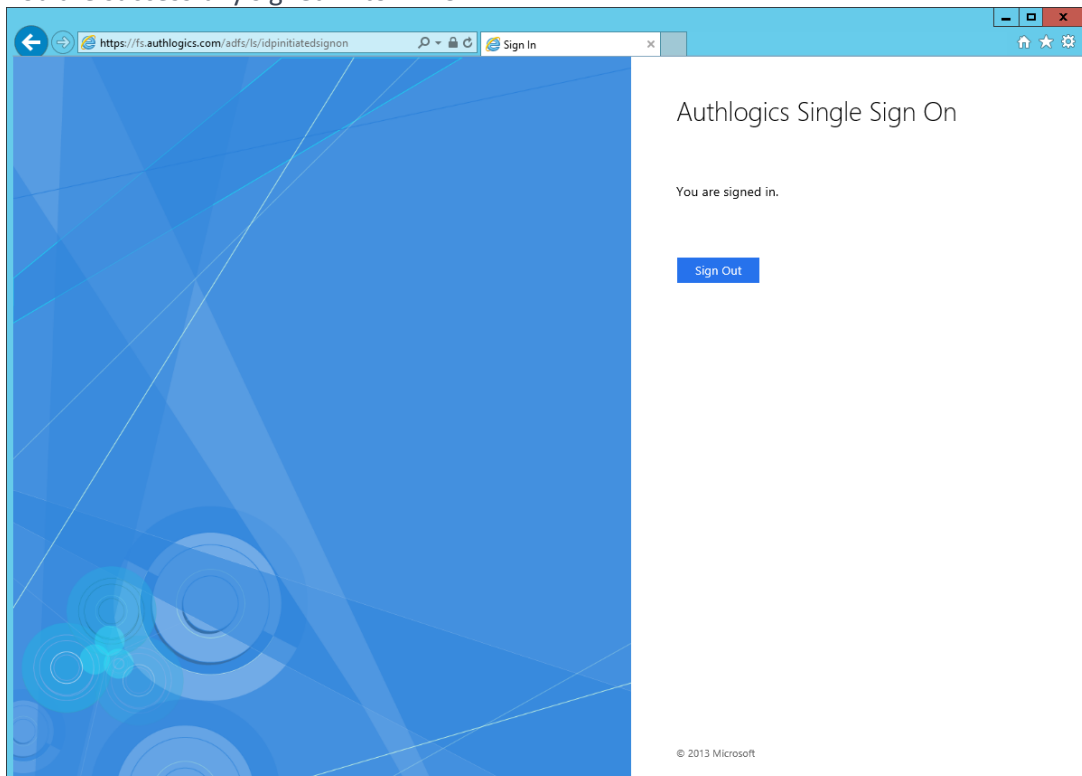


- (2) Enter the PINgrid One Time Code (if using PINgrid).
- (3) Click *Sign in*.



The screenshot shows a web browser window with the URL <https://fs.authlogics.com/adfs/ls/idpinitiatedsignon>. The page title is "Authlogics Single Sign On". The main content area displays a welcome message: "Welcome AUTHLOGICS\stevr". Below this, it states: "For security reasons, we require additional information to verify your account". The instruction "Please enter your PINgrid security information." is followed by a 4x4 grid of colored squares (red, green, blue, yellow) containing numbers. Below the grid is a password input field with a masked password "....." and a "Sign in" button. A "Sign Out" button is also visible. At the bottom, there is a link to "Please contact your helpdesk for assistance." and a copyright notice "© 2013 Microsoft".

- (4) You are successfully signed in to ADFS.

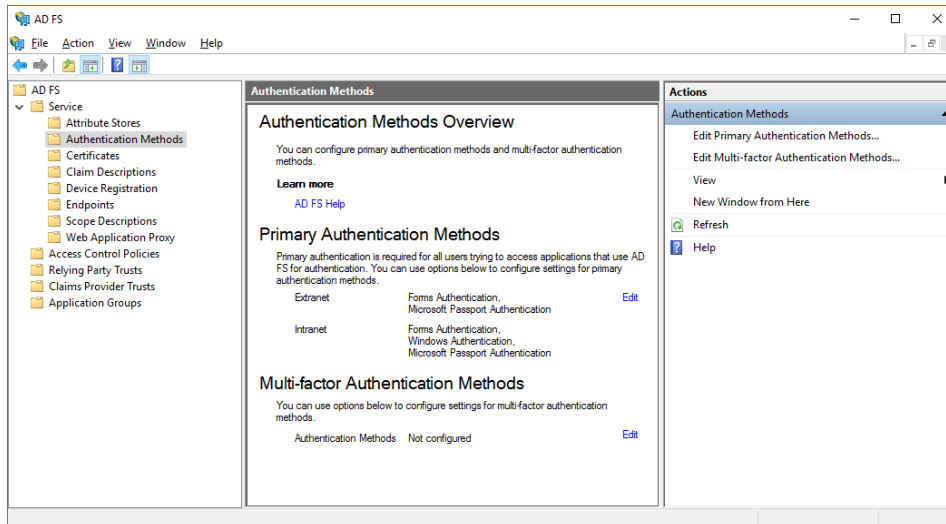


The screenshot shows the same web browser window, but the page content has changed. The main content area now displays "You are signed in." and a "Sign Out" button. The "Sign in" button is no longer visible. The copyright notice "© 2013 Microsoft" remains at the bottom.



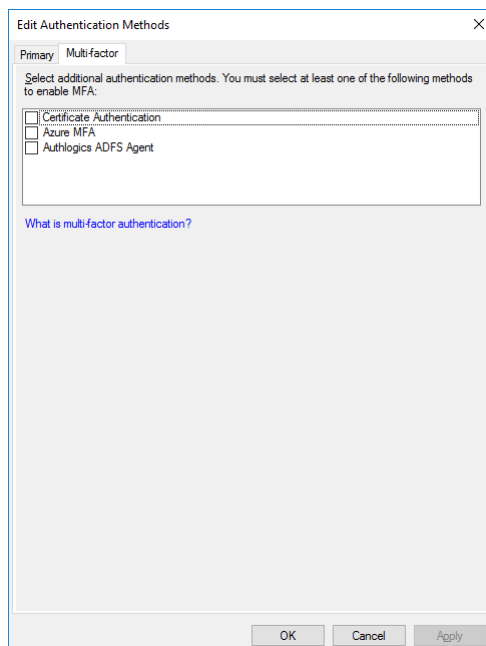
# Configuring MFA for ADFS 4.0 on Windows Server 2016

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



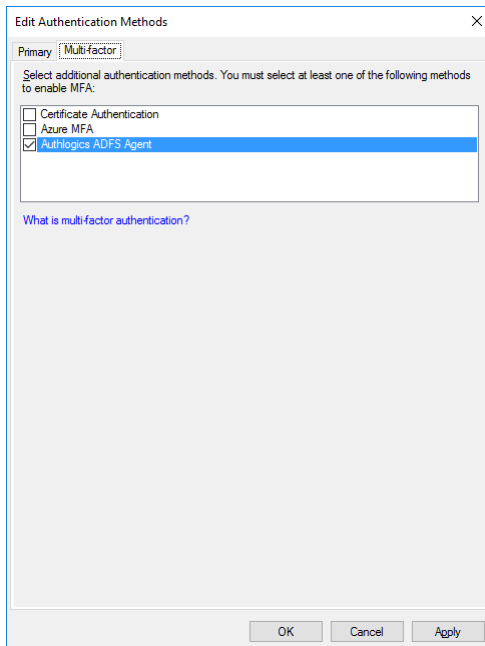
## Enabling the Authlogics ADFS Agent

- (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.





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

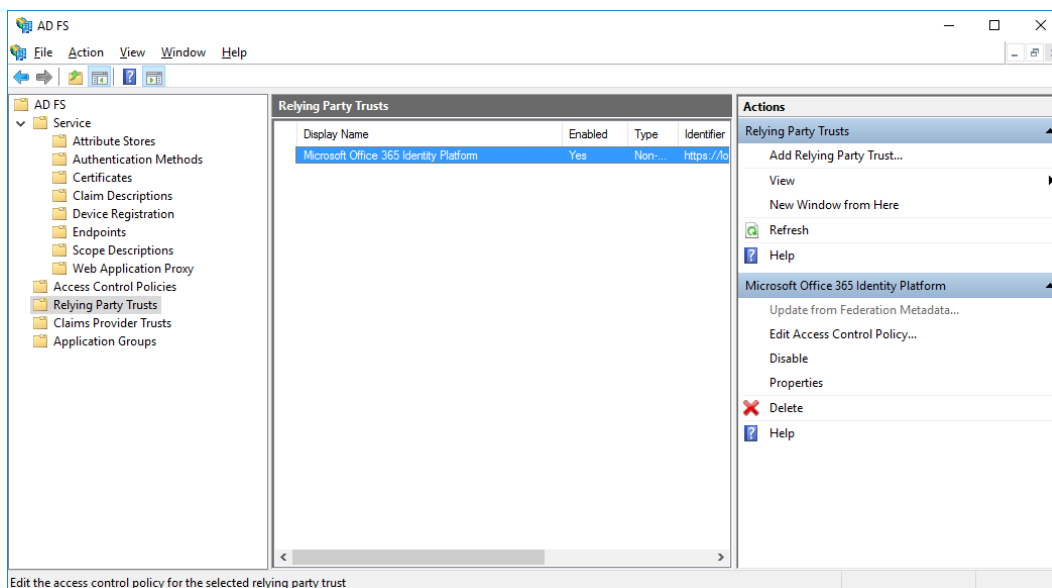


## Configuring the ADFS 4.0 Policy

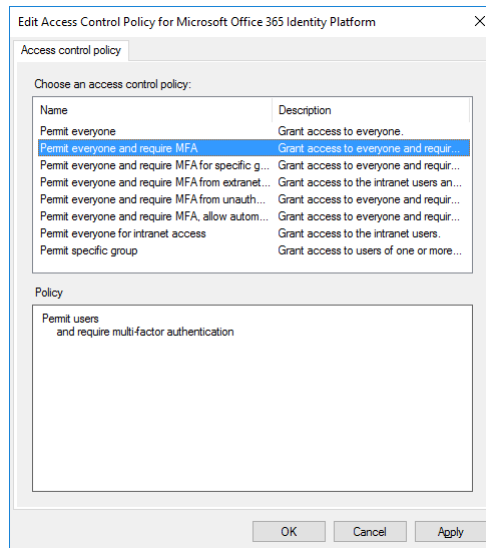
The Authlogics ADFS Agent will work with the built in Access Control Policies which include “require MFA”. Alternatively a custom policy can be created, however this is outside the scope of this document.

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.

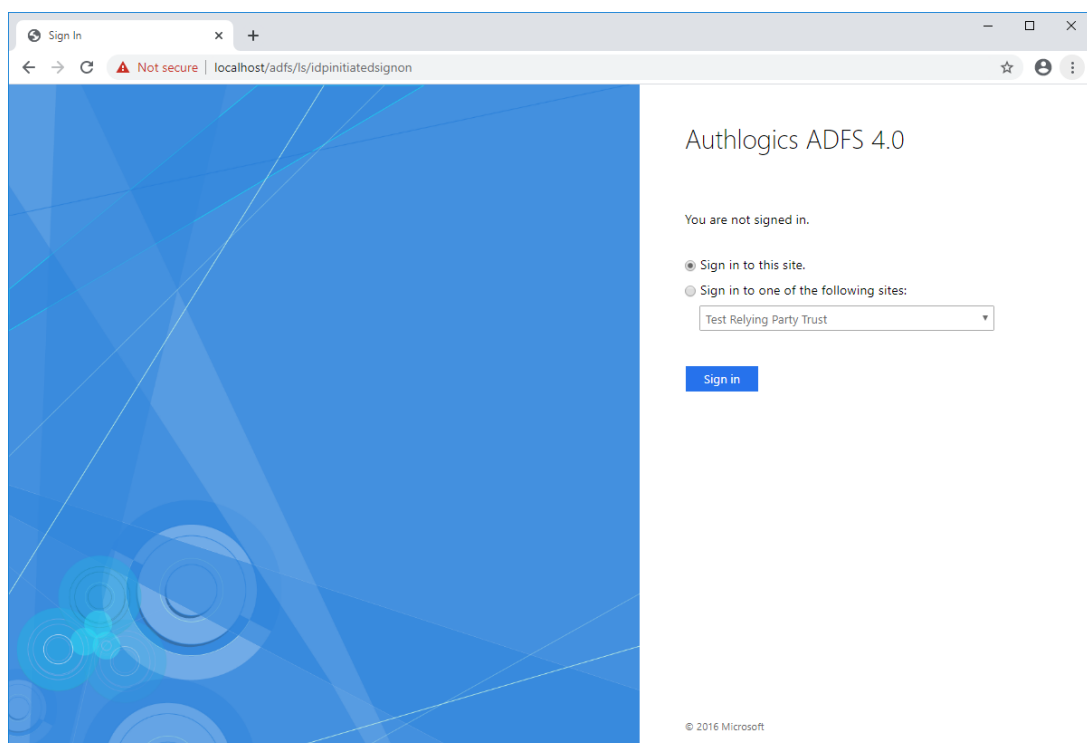


- (4) Choose the Access Control Policy you would like to use for the Relying Party Trust. Typically this would be "Permit everyone and require MFA".
- (5) Click *OK* when done.



## 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. <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*.



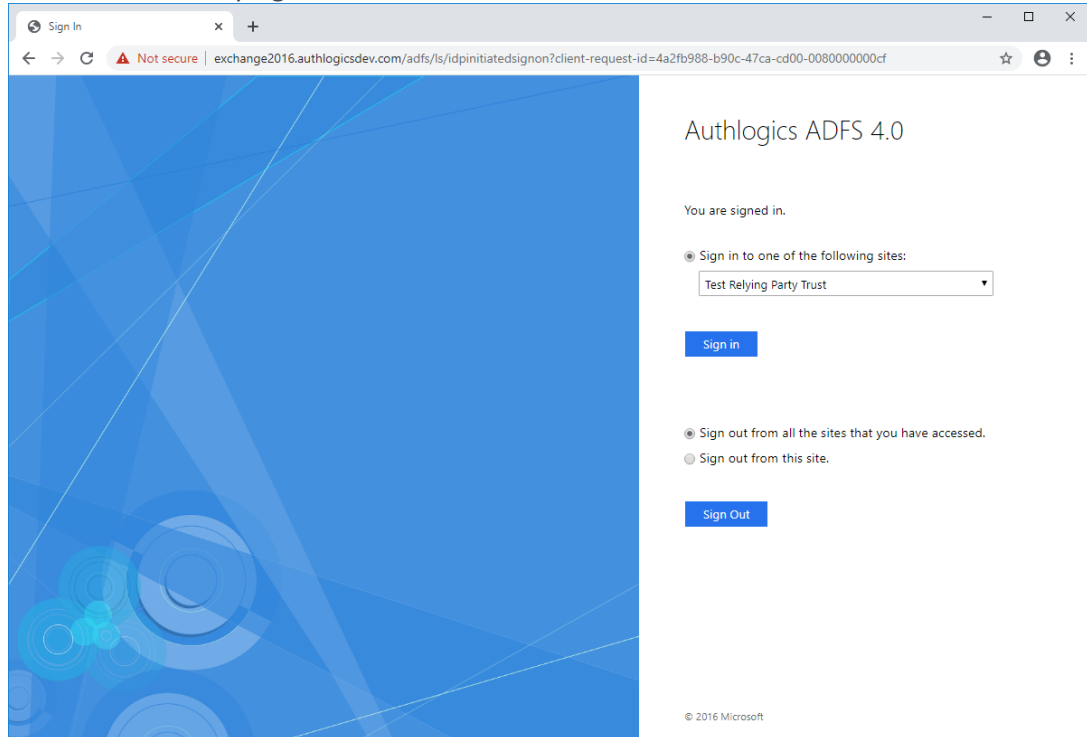
- (5) Enter the username and password.
- (6) Click *Sign in*.

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

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	4	0	4	2	4
1	5	0	2	2	0



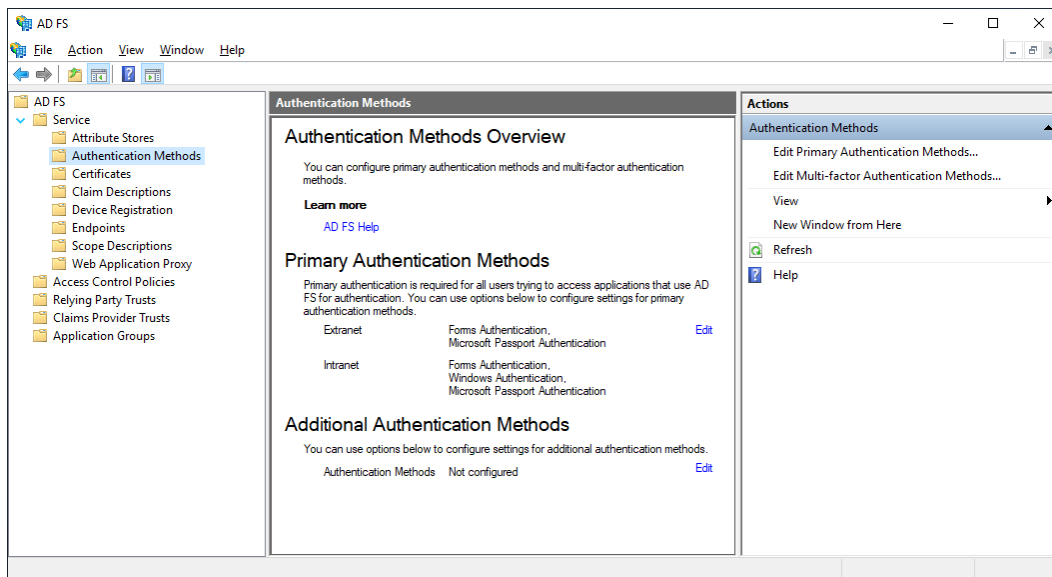
(9) You are successfully signed in to ADFS.



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

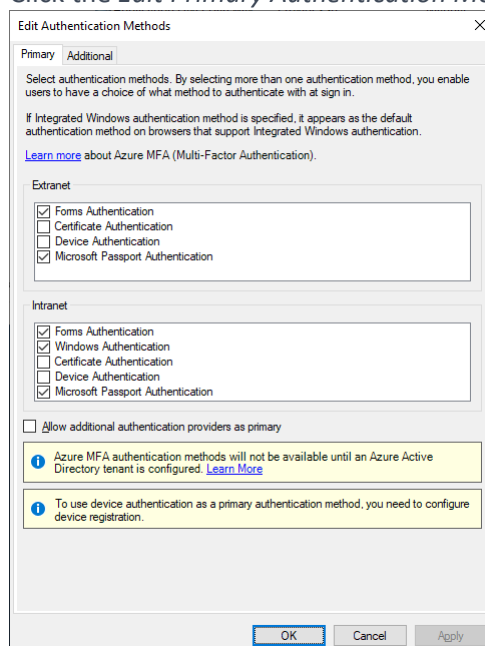
Microsoft ADFS has native support for Multi-Factor Authentication via the UI.

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.

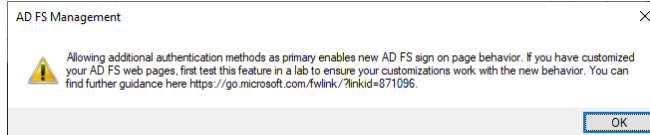


## Enabling the Authlogics ADFS Agent as primary authentication

- (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.



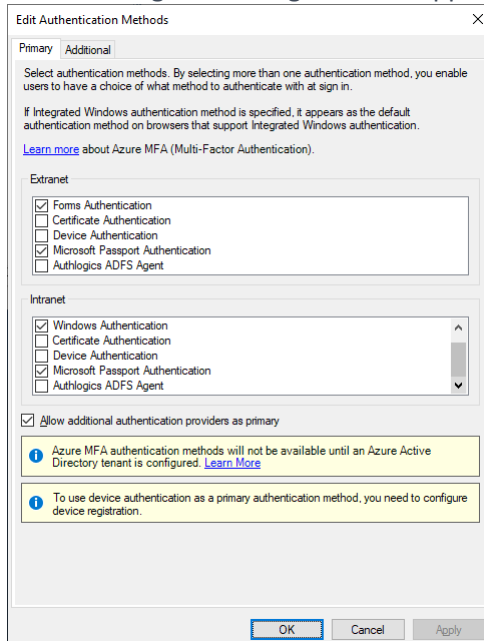
- (3) Check Allow additional authentication providers as primary.



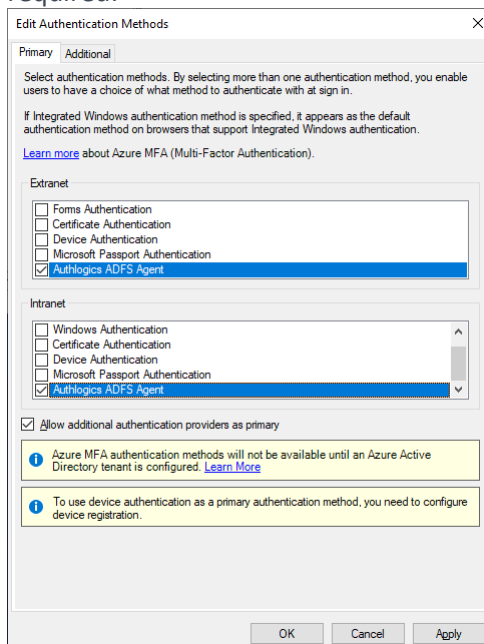
- (4) Click *OK*.

- (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.



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

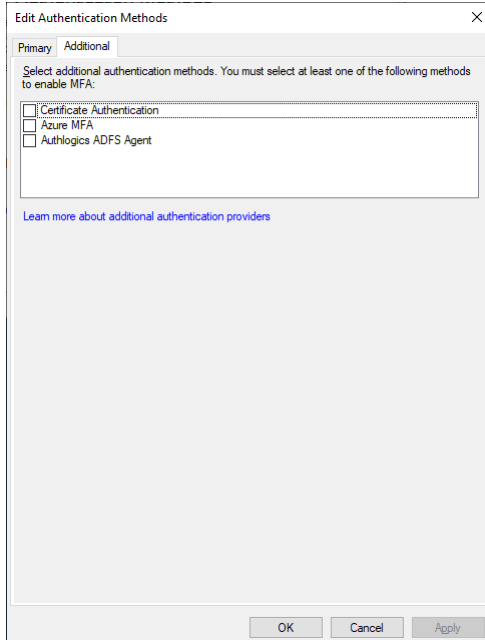


- (8) Click *OK* to close the tab.



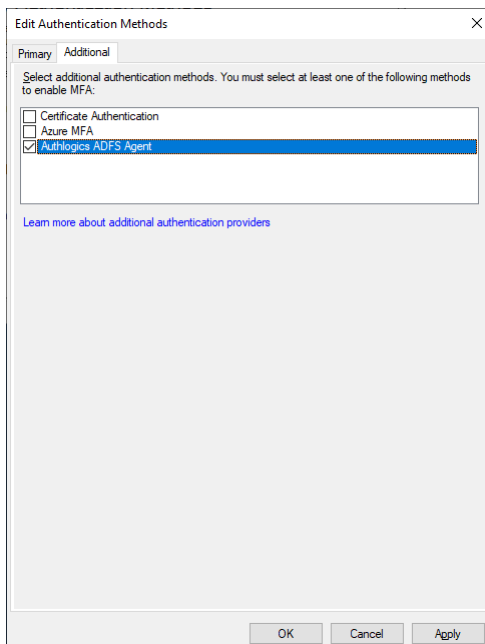
## Enabling the Authlogics ADFS Agent as additional authentication

- (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.



Dialog box titled "Edit Authentication Methods". It has two tabs: "Primary" and "Additional". The "Additional" tab is selected. Below the tabs, it says "Select additional authentication methods. You must select at least one of the following methods to enable MFA:". There is a list box containing three items: "Certificate Authentication", "Azure MFA", and "Authlogics ADFS Agent". Each item has a checkbox to its left. The "Authlogics ADFS Agent" checkbox is currently unchecked. Below the list box, there is a link that says "Learn more about additional authentication providers". At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Apply".

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



Dialog box titled "Edit Authentication Methods". It has two tabs: "Primary" and "Additional". The "Additional" tab is selected. Below the tabs, it says "Select additional authentication methods. You must select at least one of the following methods to enable MFA:". There is a list box containing three items: "Certificate Authentication", "Azure MFA", and "Authlogics ADFS Agent". Each item has a checkbox to its left. The "Authlogics ADFS Agent" checkbox is now checked. Below the list box, there is a link that says "Learn more about additional authentication providers". At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Apply".



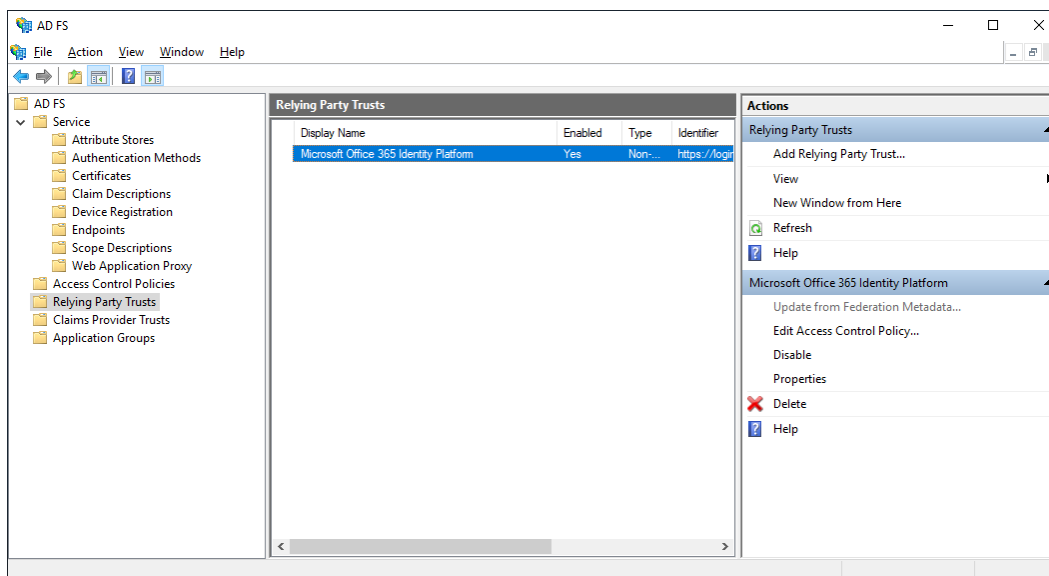
## Configuring the ADFS 5.0/6.0 Policy

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.

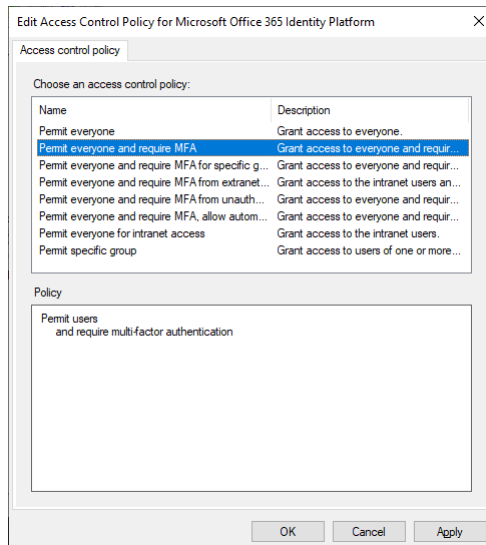
To change an existing Relying Party Trust to use an Access Control Policies which includes MFA:

- (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.



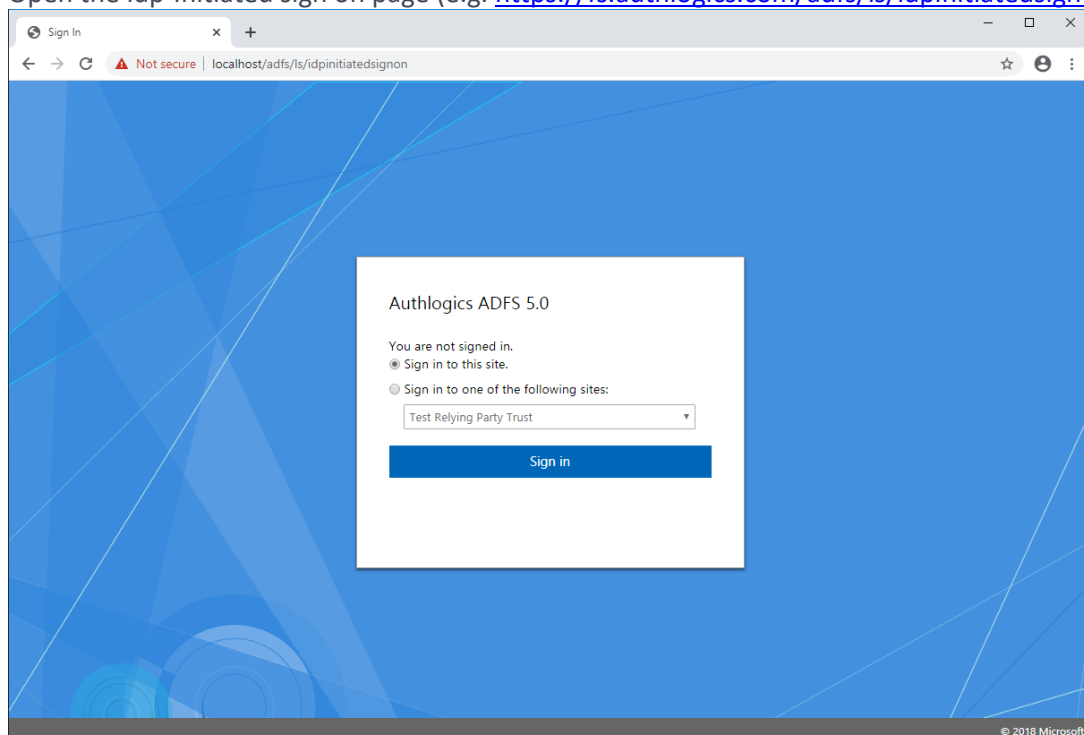


- (4) Choose the Access Control Policy you would like to use for the Relying Party Trust. Typically this would be “Permit everyone and require MFA”.
- (5) Click *OK* when done.

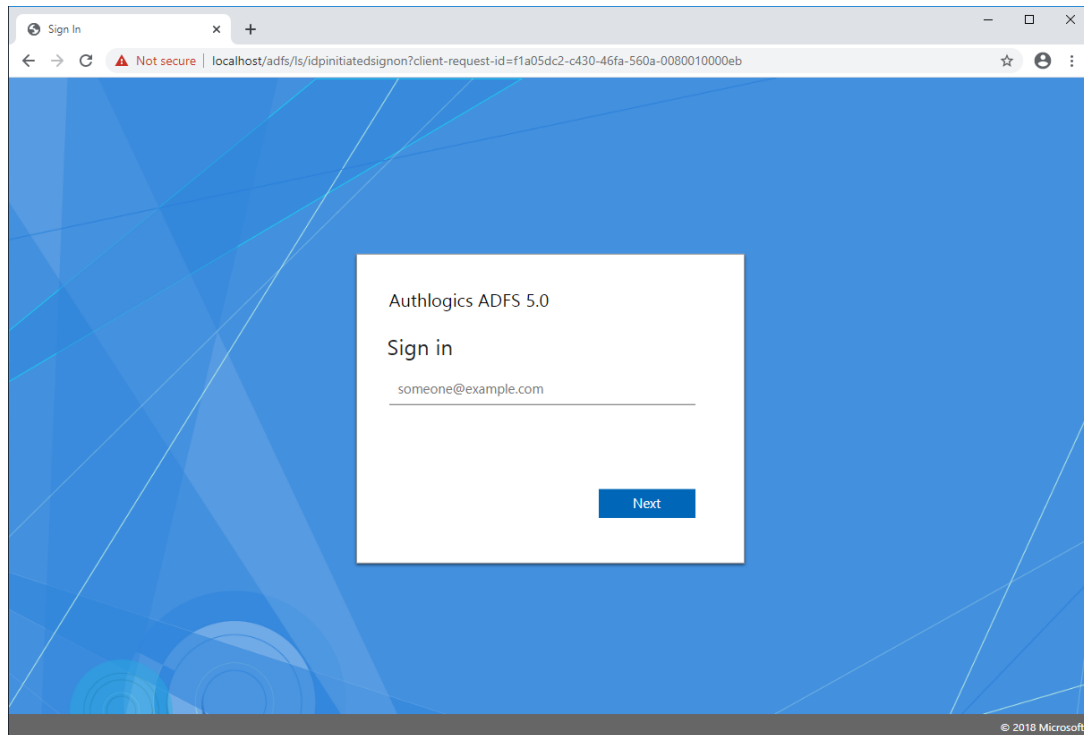


## Testing the ADFS 5.0/6.0 logon process as a primary method

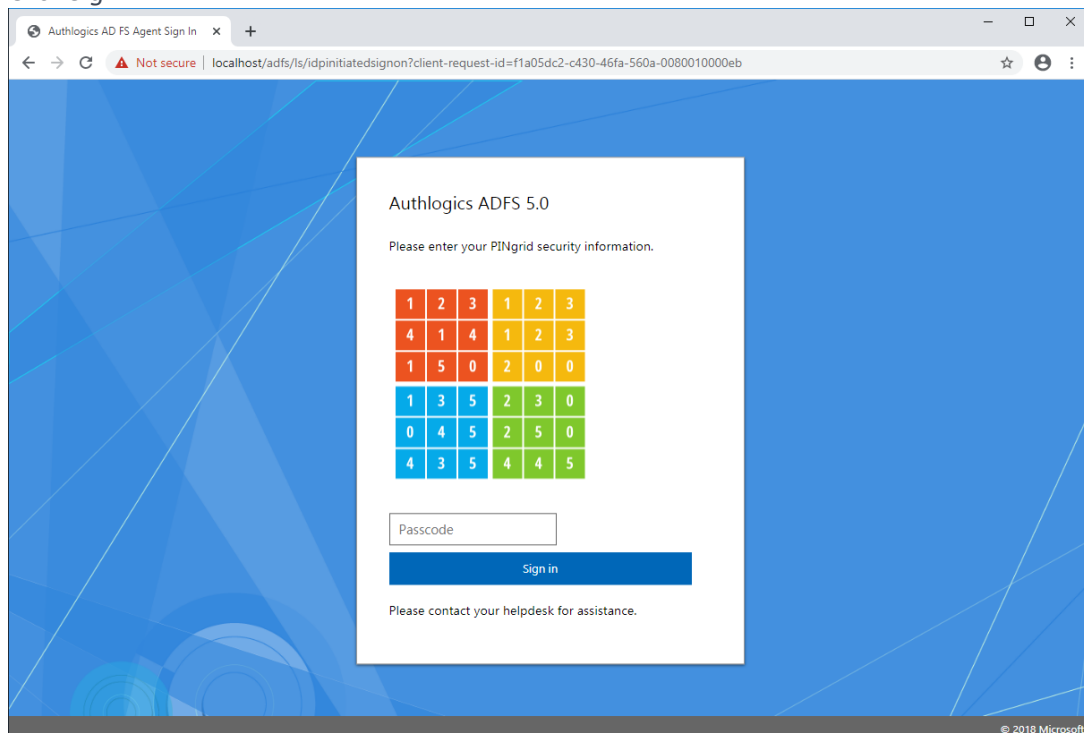
- (1) Ensure the Idp-Initiated sign on page is enabled. To enable this functionality see the “*Enabling the Idp-Initiated sign on page*” section at the end of this document.
- (2) Ensure at least one Relying Party Trust has been configured to use an Access Control Policy that requires MFA, **otherwise 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>):



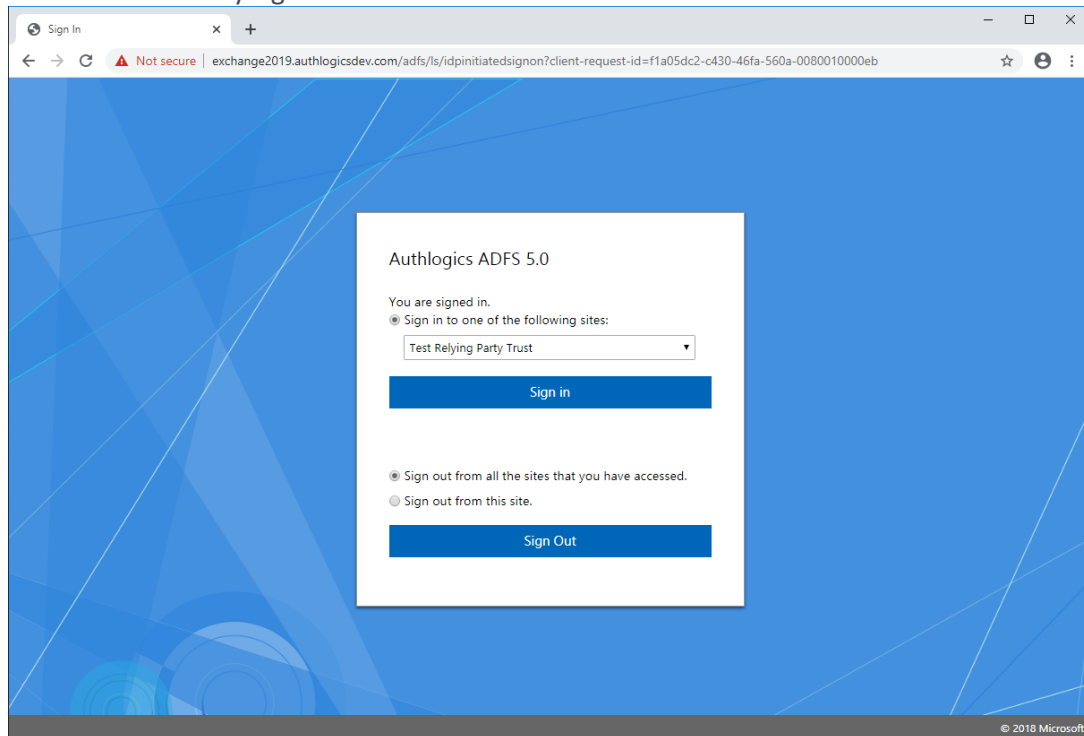
- (4) Ensure *Sign in to this site* is selected (not a Test Relying Party entry) and click *Sign in*.
- (5) Enter the username.
- (6) Click *Next*.



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



(9) You are successfully signed in to ADFS.

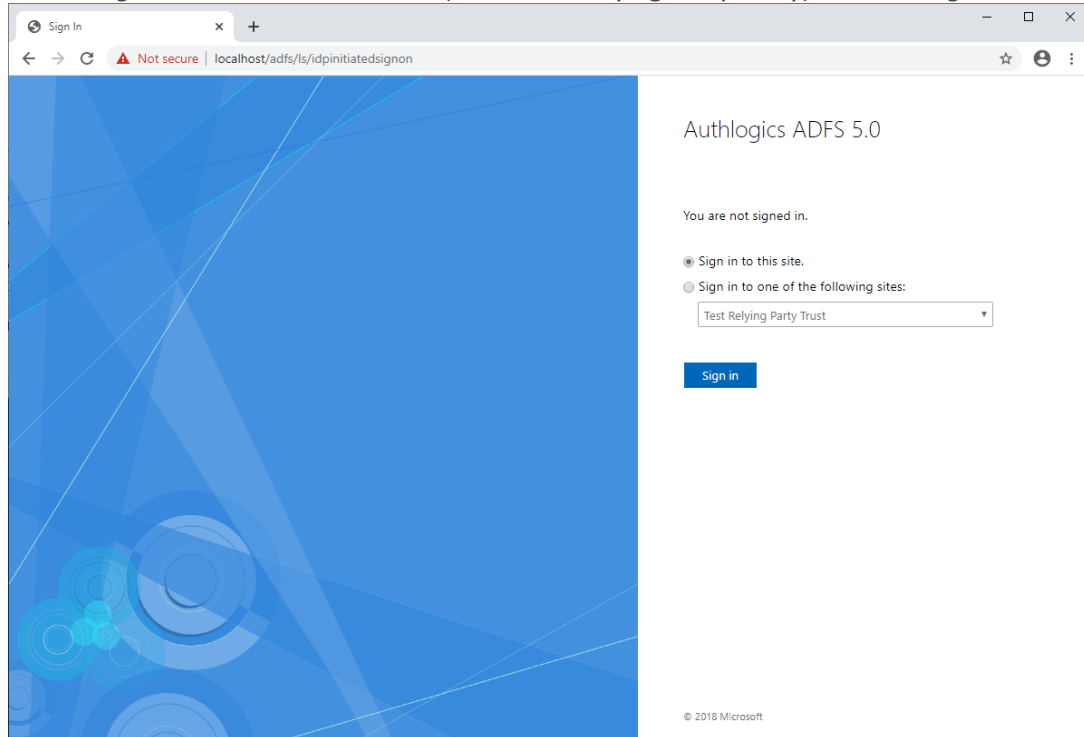


## Testing the ADFS 5.0 logon process as an additional method

- (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>)

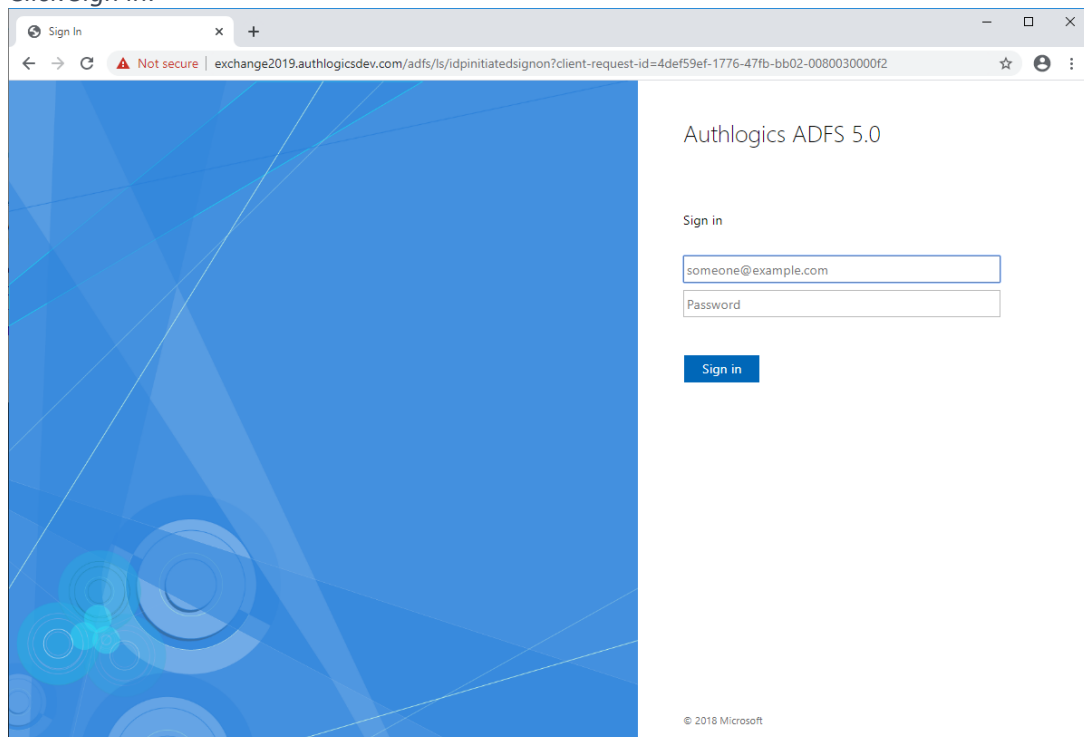


(4) Ensure *Sign in to this site* is selected (not a Test Relying Party entry) and click *Sign in*.

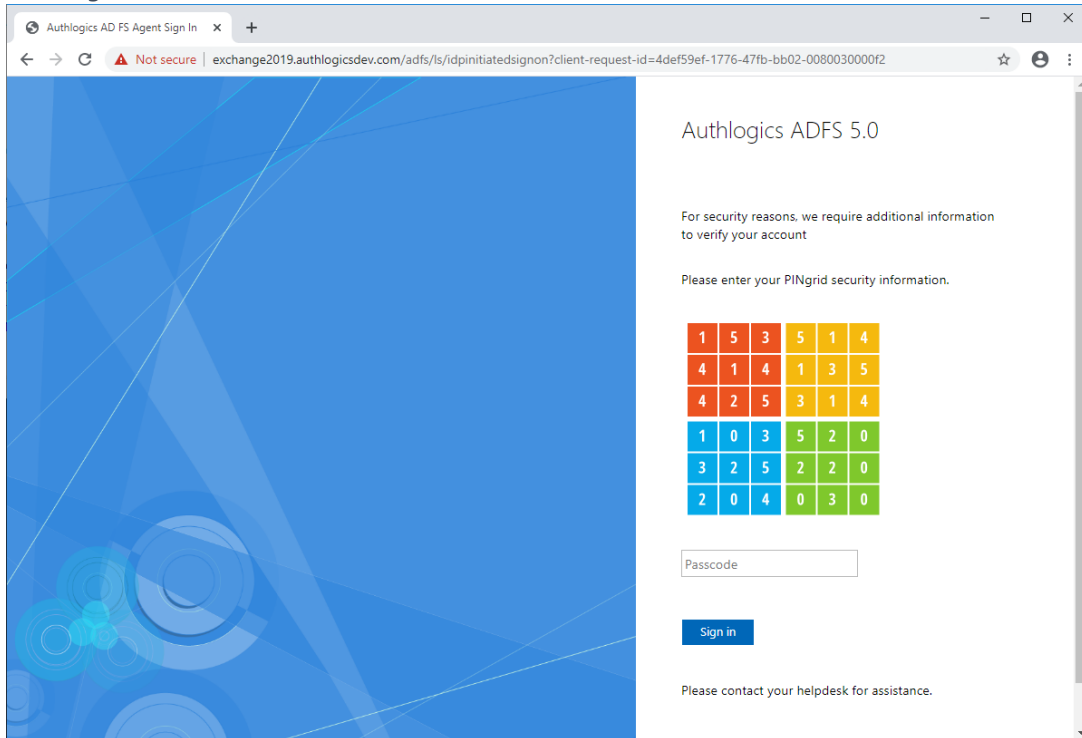


(5) Enter the username and password.

(6) Click *Sign in*.



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



Authlogics AD FS Agent Sign In

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.

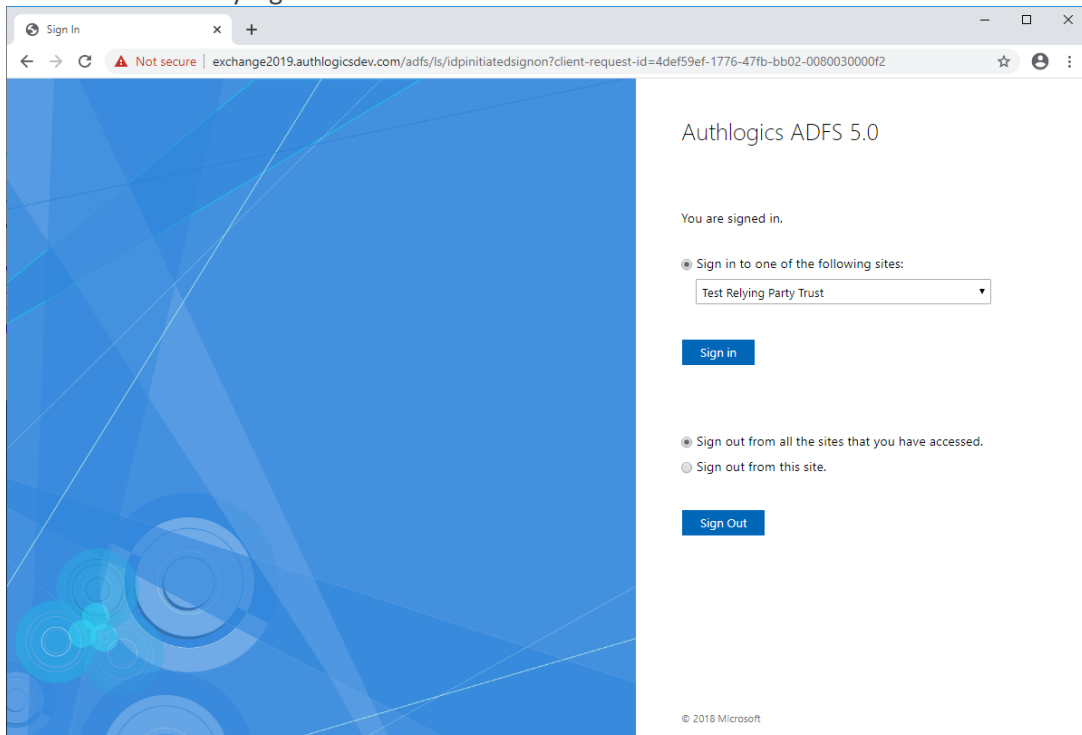
1	5	3	5	1	4
4	1	4	1	3	5
4	2	5	3	1	4
1	0	3	5	2	0
3	2	5	2	2	0
2	0	4	0	3	0

Passcode

Sign in

Please contact your helpdesk for assistance.

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



Sign In

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



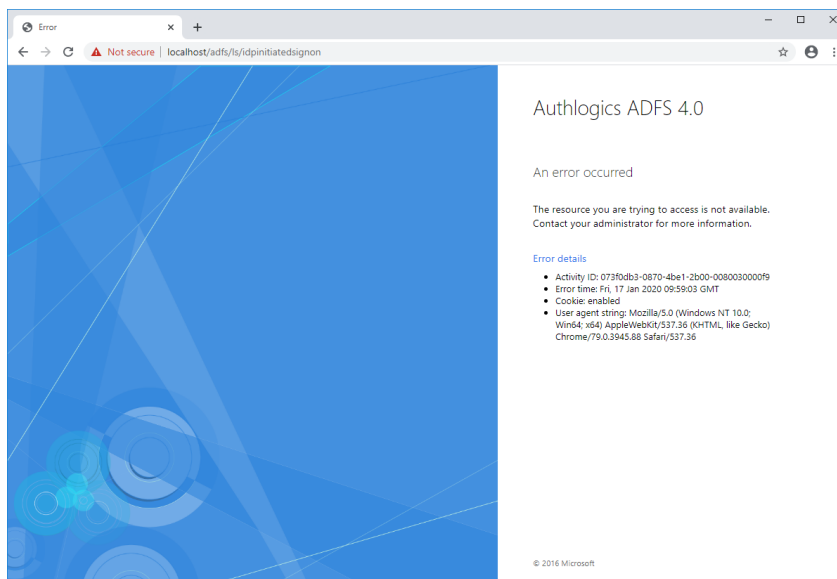
## Configuration Testing

### 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 Idp-Initiated sign on page prior to it being enabled.

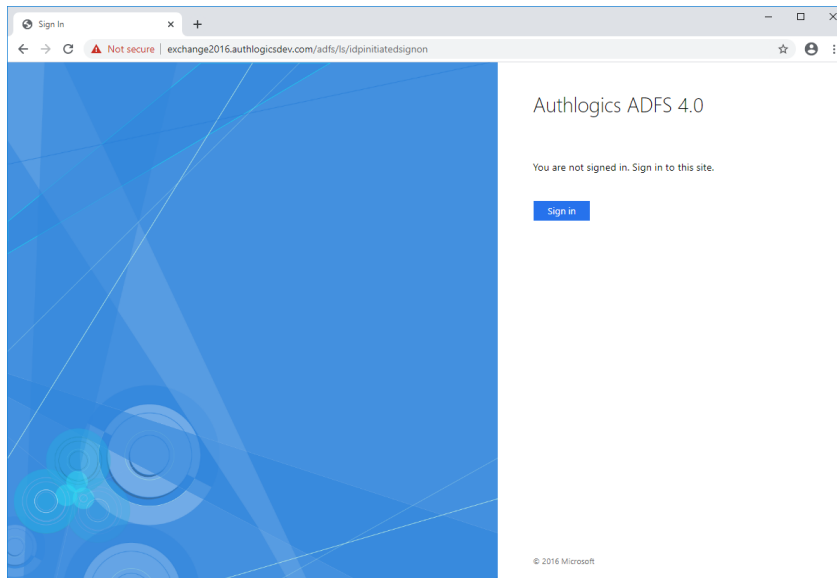


To enable the Idp-Initiated sign on page open a **PowerShell Admin** command prompt and run the following command:

```
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

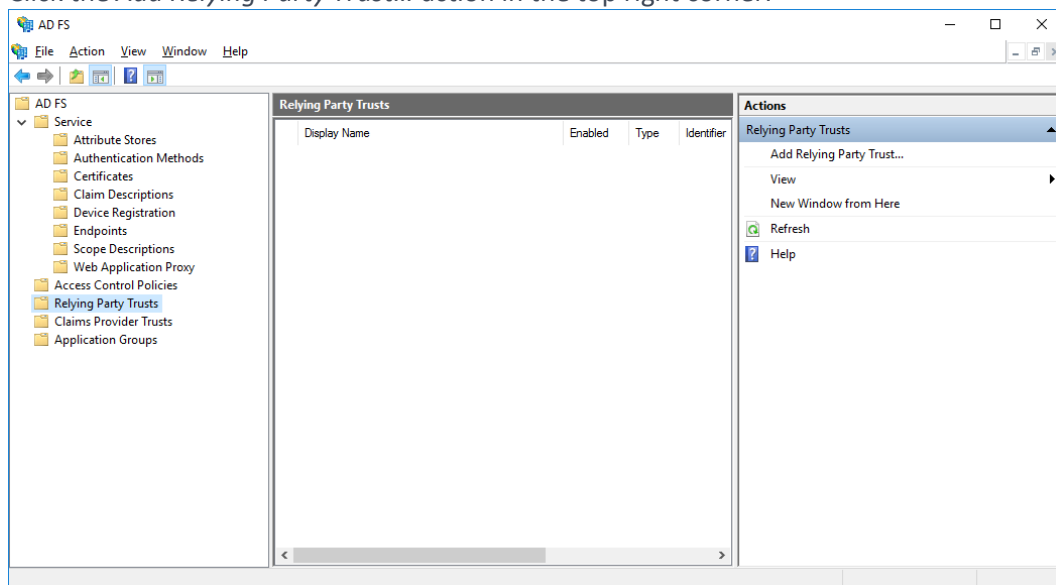
The purpose of this section is to ensure at least one Relying Party Trust entry exists on the ADFS server so that you can assign an Access Control Policy to it in order for the MFA login option to appear in the Idp-Initiated sign on page.



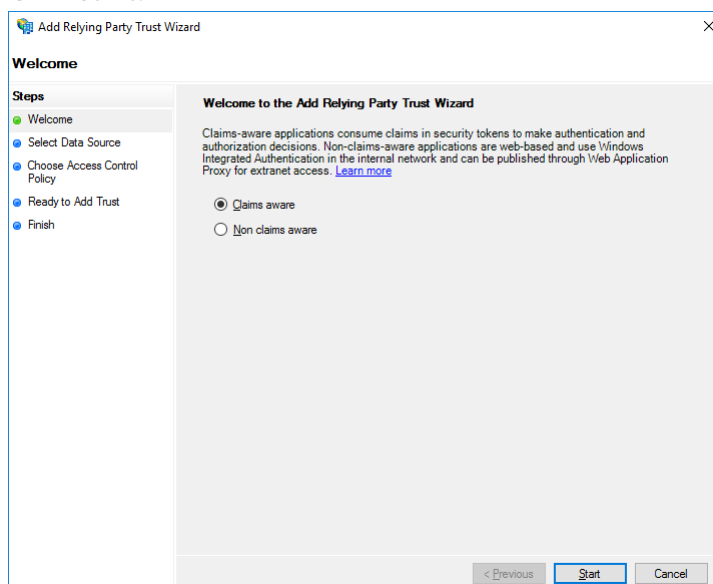
### Note

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.



- (3) Click *Start*.



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





(5) Click Next.

The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Select Data Source' step. The 'Steps' pane on the left shows the progression: Welcome, Select Data Source (current), Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains three radio button options for selecting data source information. The first option, 'Import data about the relying party published online or on a local network', is selected. Below it, a text box contains the URL 'https://<ADFSServer>/federationmetadata/2007-06/federationmetadata.xml'. The second option is 'Import data about the relying party from a file', and the third is 'Enter data about the relying party manually'. At the bottom, there are buttons for '< Previous', 'Next >', and 'Cancel'.

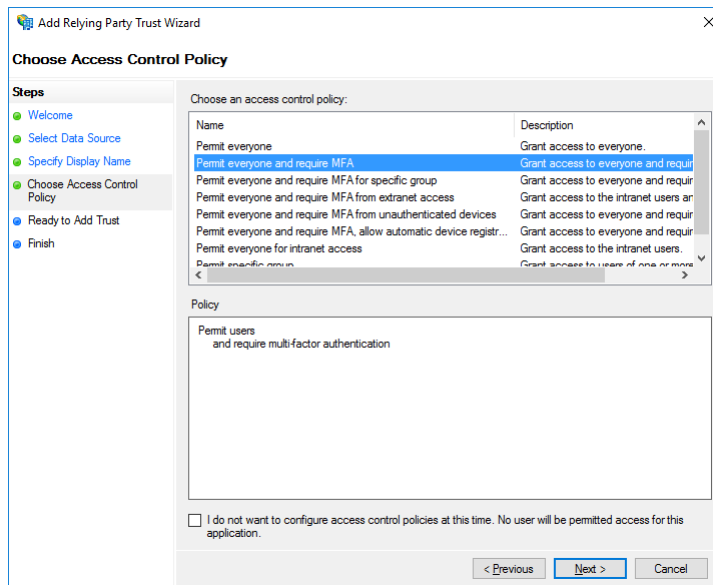
(6) Enter a name for the entry, e.g. "Test Relying Party Trust"

The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Specify Display Name' step. The 'Steps' pane on the left shows the progression: Welcome, Select Data Source, Specify Display Name (current), Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains a text box labeled 'Display name:' with the text 'Test Relying Party Trust' entered. Below it is a large text area labeled 'Notes:'. At the bottom, there are buttons for '< Previous', 'Next >', and 'Cancel'.



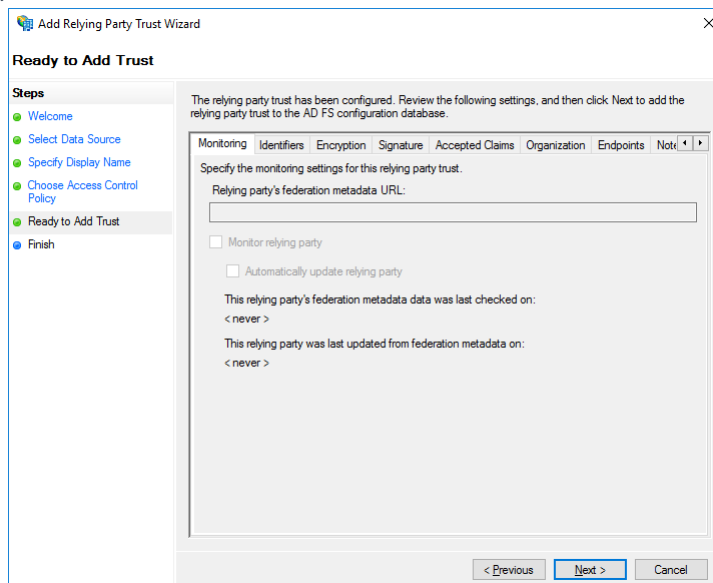
(7) Select the *Permit everyone and require MFA* access control policy.

(8) Click Next.



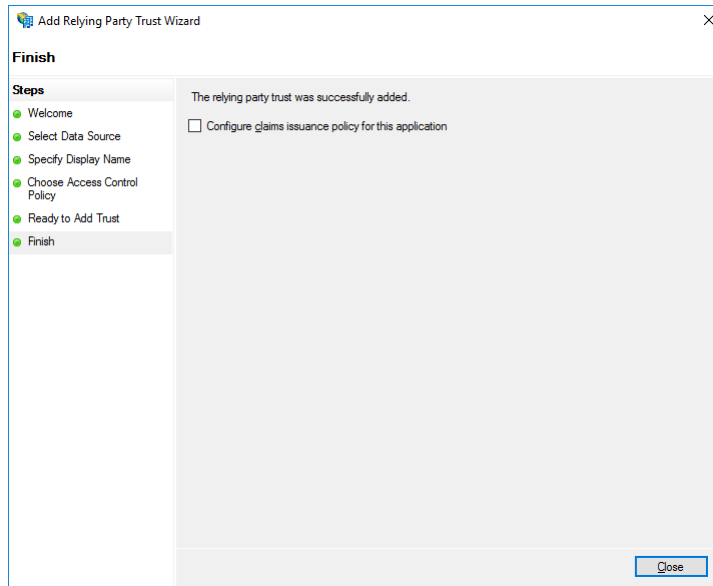
(9) Nothing needs to be configured on this screen.

(10) Click Next.



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

(12) Click *Close*.



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\DomainControllerRefreshTime

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>

