MyID MFA and PSM

Version 5.0.8

ADFS Agent Integration Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111

Document reference: IMP2061-5.0.8

January 2025

Copyright

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

© You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. ---

Conventions used in this document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important.
  - Bulleted lists are used when the order is unimportant or to show alternatives.
- **Bold** is used for menu items and for labels.

  For example:
  - Record a valid email address in **'From' email address**.
  - Select **Save** from the **File** menu.
- *Italic* is used for emphasis:

  For example:
  - Copy the file *before* starting the installation.
  - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks are used to identify the titles of other documents.

  For example: "See the ***Release Notes*** for further information."

  Unless otherwise explicitly stated, all referenced documentation is available on the product installation media.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.
- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

  Warning: You must take a backup of your database before making any changes to it.

Contents

1 Introduction

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

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

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

1.1 Licensing

The MyID ADFS Agent does not require its own license; however you can use it only with a valid MyID MFA license.

Note: For detailed information on the license types, refer to the license agreement document embedded within the installation package.

1.2 Change history

Version	Description
IMP2061-01	Reformatted and released with MyID MFA and PSM version 5.0.7.
IMP2061-5.0.8	Released with MyID MFA and PSM version 5.0.8..

2 Design and deployment scenarios

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

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

2.1 Minimum requirements

The MyID ADFS Agent has been designed to work with:

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

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

3 Deployment

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

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

You can do the following:

- Install the MyID ADFS Agent.

  See section *3.1*, *Installing the MyID ADFS Agent*.
- Uninstall the MyID ADFS Agent.

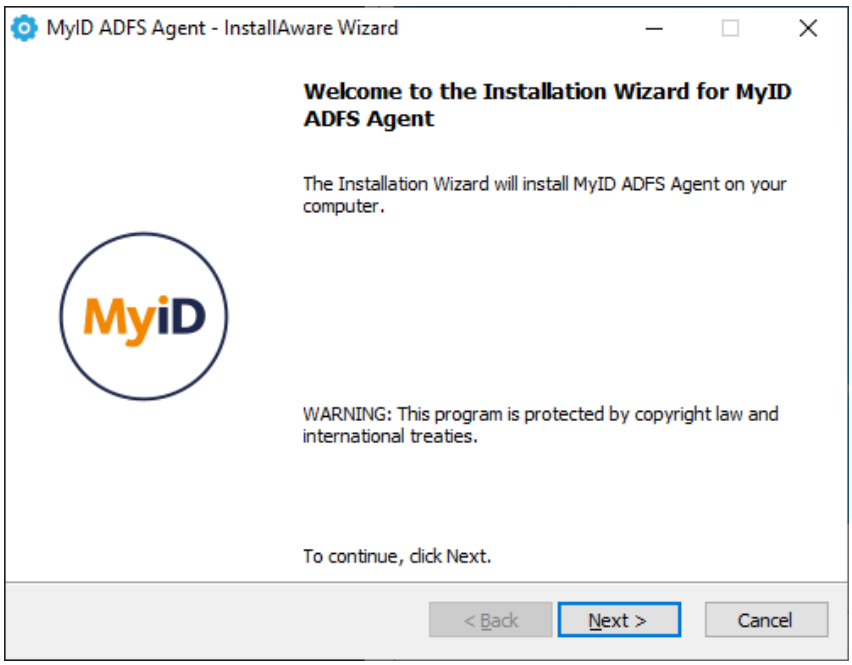
  See section *3.2*, *Uninstalling the MyID ADFS Agent*.
- Configure the MyID ADFS Agent.

  See section *3.3*, *Configuring the MyID ADFS Agent*.

3.1 Installing the MyID ADFS Agent

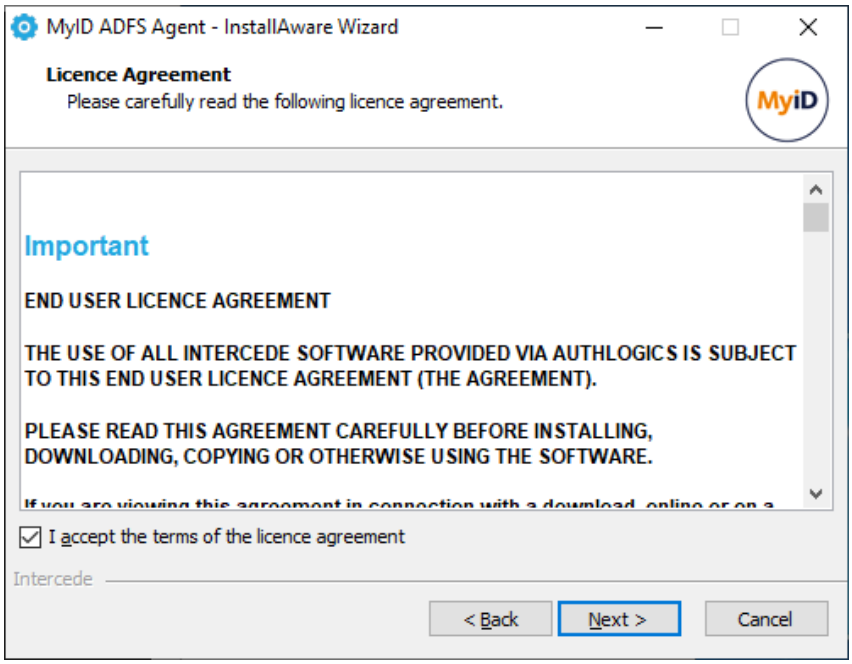
Perform the installation on the server while running the ADFS role.

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

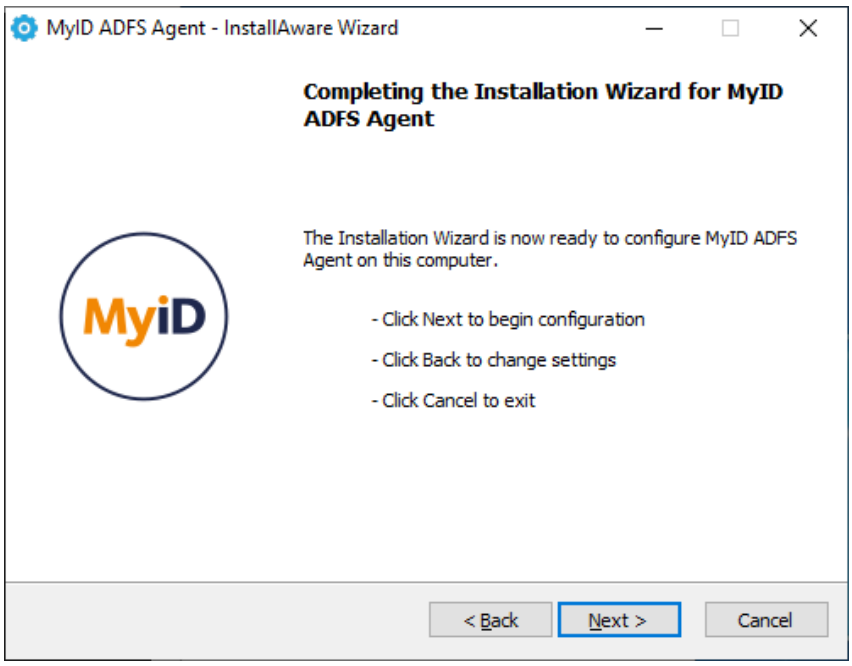


2. Click **Next**.

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

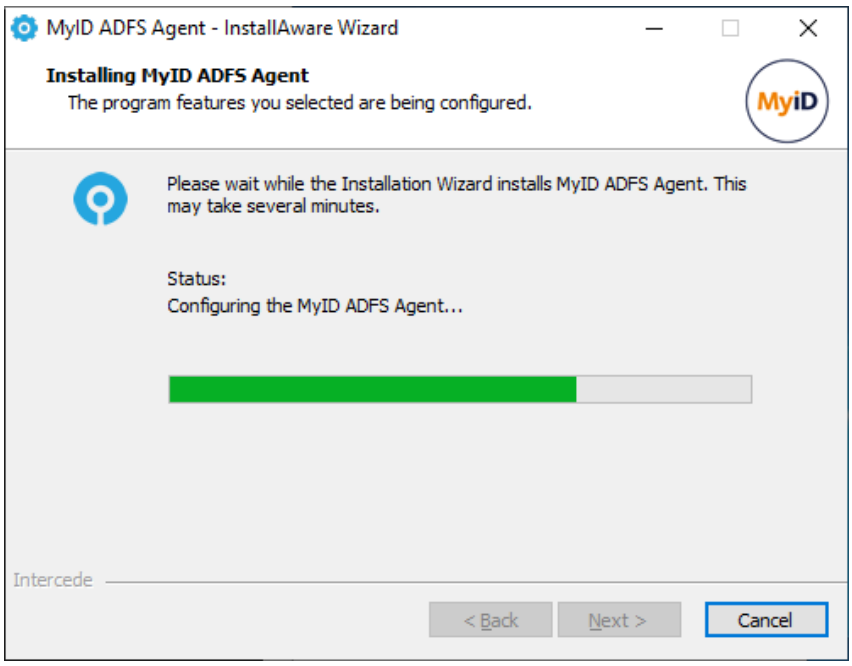


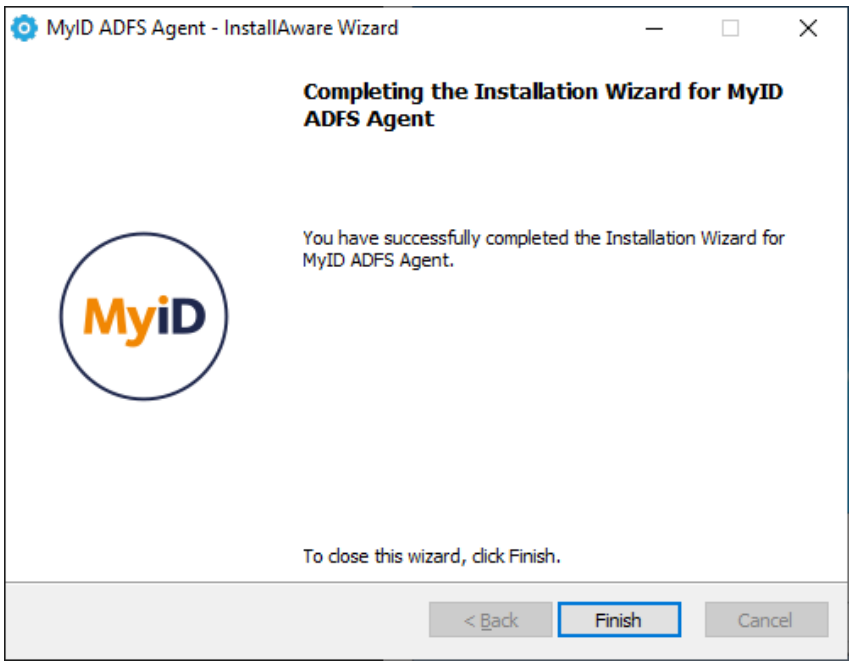
4. Click **Next**.



5. Click **Next**.

   The installation is being performed. The ADFS services restart.



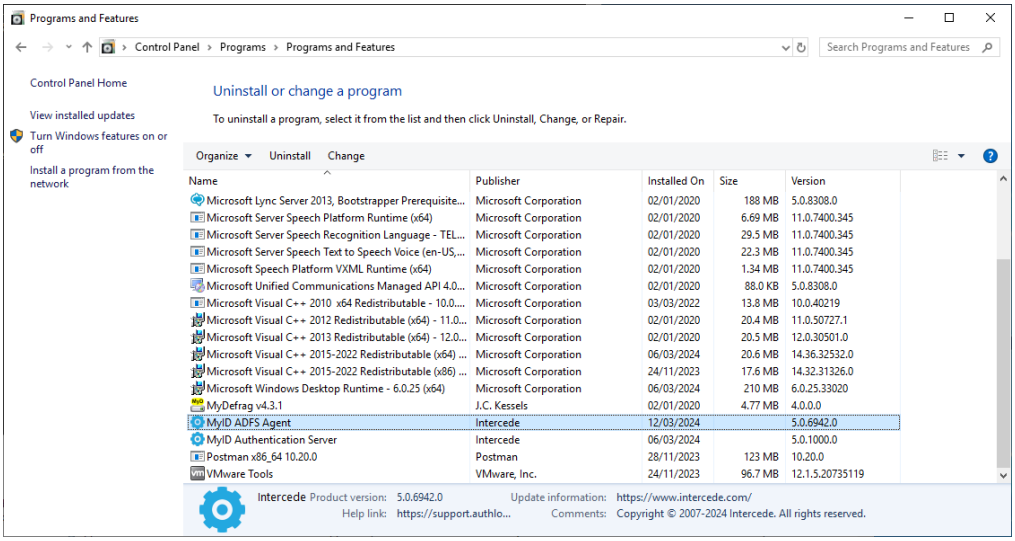


6. Click **Finish**.

   All necessary MyID ADFS Agent files are installed.

3.2 Uninstalling the MyID ADFS Agent

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



3.2.1 Active Directory metadata

Uninstalling the MyID Exchange Agent does *not* remove the metadata from user accounts in the Active Directory. If you want to remove MyID MFA from your environment completely, delete all user accounts using the MMC before uninstalling. This does *not* delete the user accounts in the Active Directory; it just removes all MyID MFA information from them.

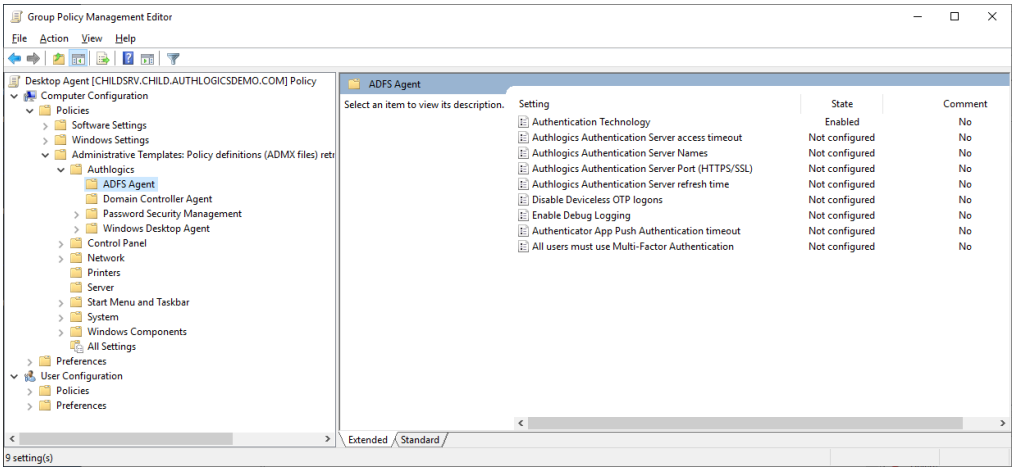
For detailed information about MyID Active Directory metadata see Authlogics KB 207256965:

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

3.3 Configuring the MyID ADFS Agent

Once you have installed the MyID ADFS Agent, you can configure it. You can manage the configuration settings using either Local Directory Group Policy or Active Directory Group Policy.

To access the MyID Local policy settings, use the MyID Local Policy Editor shortcut on the desktop or start menu.



3.3.1 General settings

Setting	All users must use Multi-Factor Authentication
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting configures if the agent should only allow MFA provisioned user to login, or if the agent should also allow users who have not been provisioned for MFA to login with their Active Directory password. If you enable this policy then all users must be provisioned for MFA to access the agent. If you disable or do not configure this policy then MFA provisioned users must use MFA, however non-MFA provisioned users may still use their Active Directory username + password to login.

Setting	Authentication Technology
Values	Auto / PINgrid / PINphrase / PINpass / Push / Disabled
Default	Disabled
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. Push: Deliver a Push notification to the user's mobile device. Disabled: A generic icon will be displayed only and Deviceless OTP is also disabled regardless of the "Disable Deviceless OTP logons" policy setting.

Setting	Disable Deviceless OTP logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables Deviceless OTP logons and a separate MFA device will be required to login. If you enable this policy a user must login to the agent using a separate MFA device. If you disable or do not configure this policy a user may login with or without a separate MFA device, depending on any user specific settings.

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

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

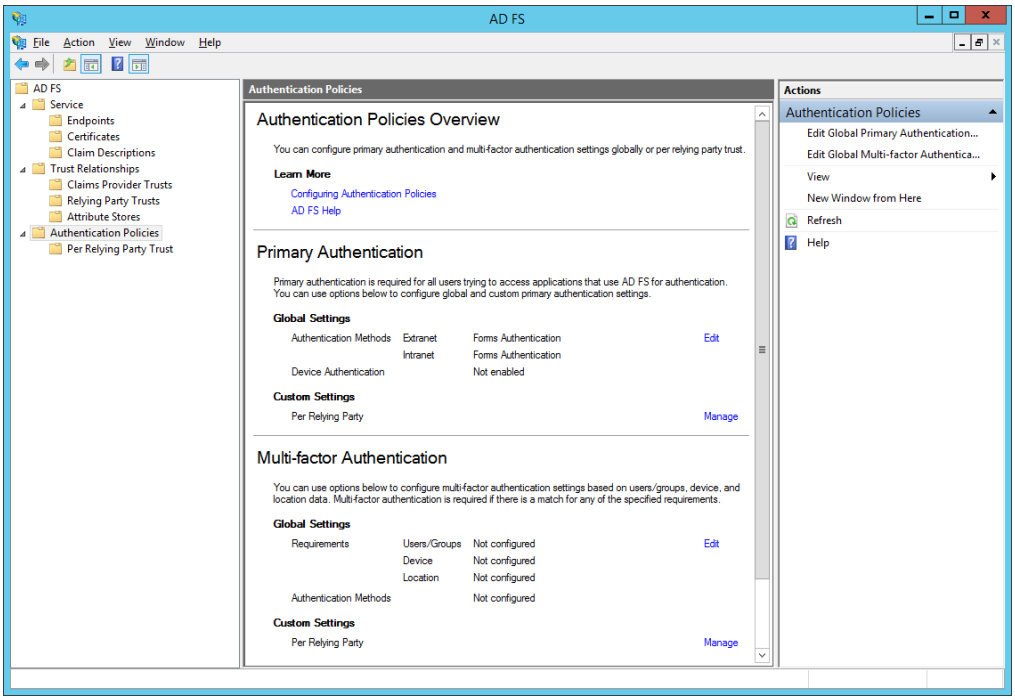
Setting	Authenticator App Push Authentication timeout
Values	(30 – 300)
Default	120
Description	This policy setting sets the maximum amount of time to wait while the MyID ADFS Agent sends a push notification to the Authlogics Authenticator App and waits for a response. If you disable or do not configure 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.

4 Configuring MFA for ADFS 3.0 on Windows Server 2012 R2

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



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

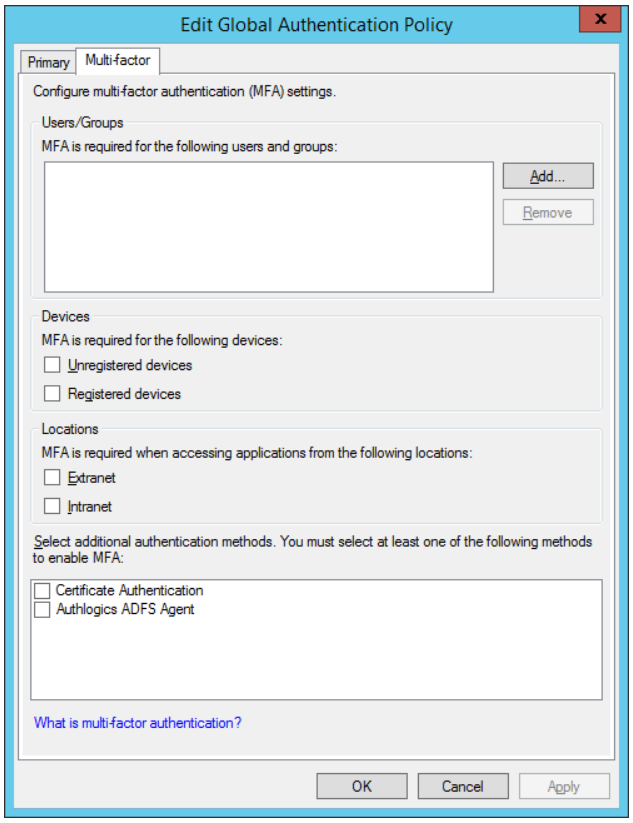
- Enable the MyID ADFS Agent.

  See section *4.1*, *Enabling the MyID ADFS Agent*.
- Test the logon process.

  See section *4.2*, *Testing the ADFS 3.0 logon process*.

4.1 Enabling the MyID ADFS Agent

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



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

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

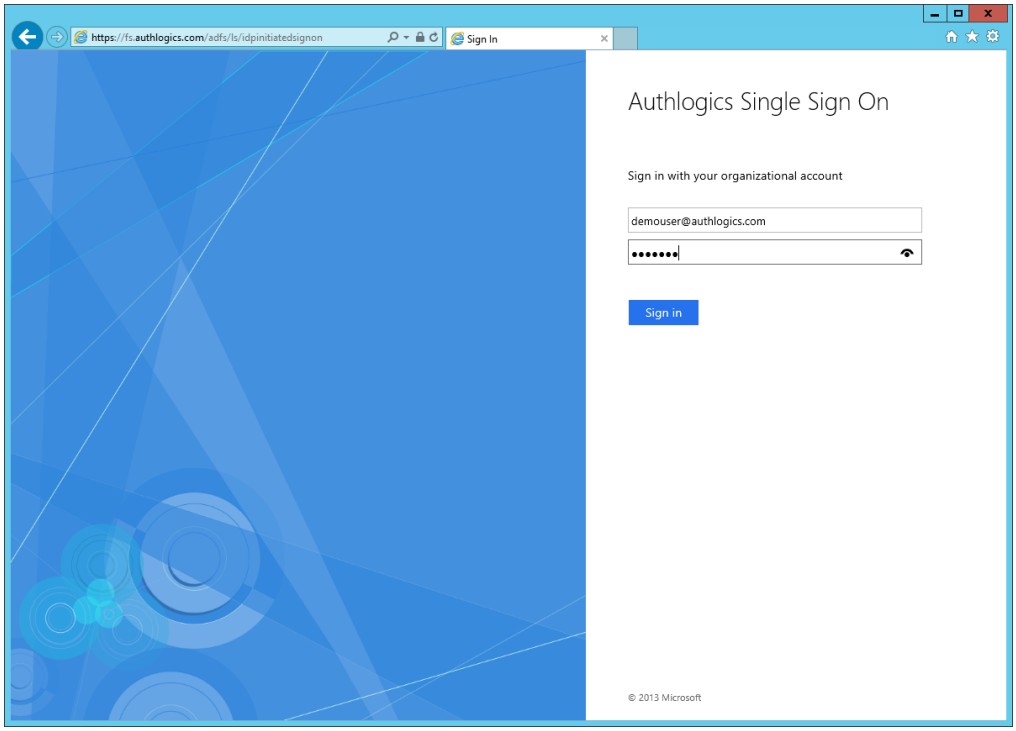
4.2 Testing the ADFS 3.0 logon process

1. Open the Identity Provider (IdP)-Initiated sign on page.

   For example:

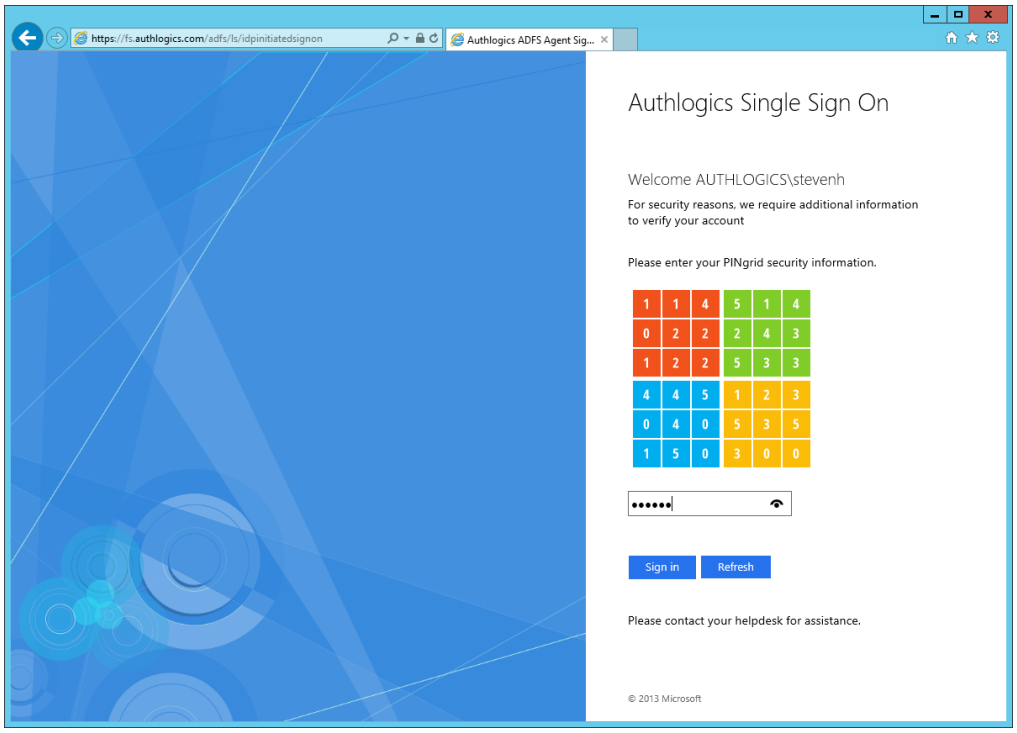
   `https://fs.authlogics.com/adfs/ls/idpinitiatedsignon`

2. Enter your username and password.



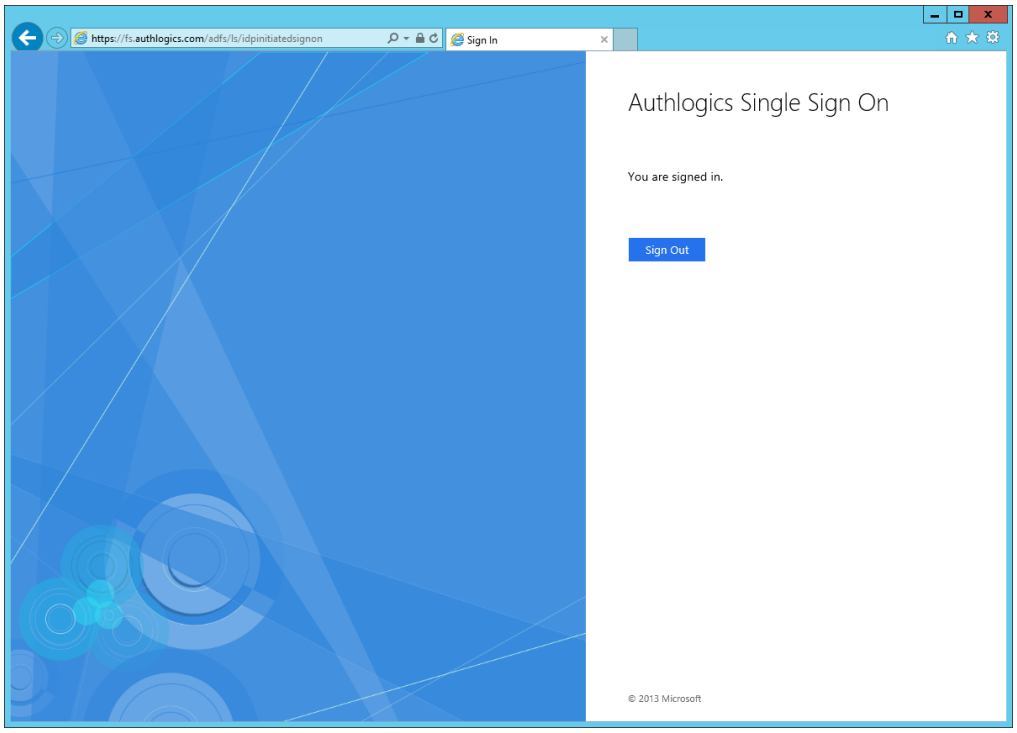
3. Click **Sign in**.

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



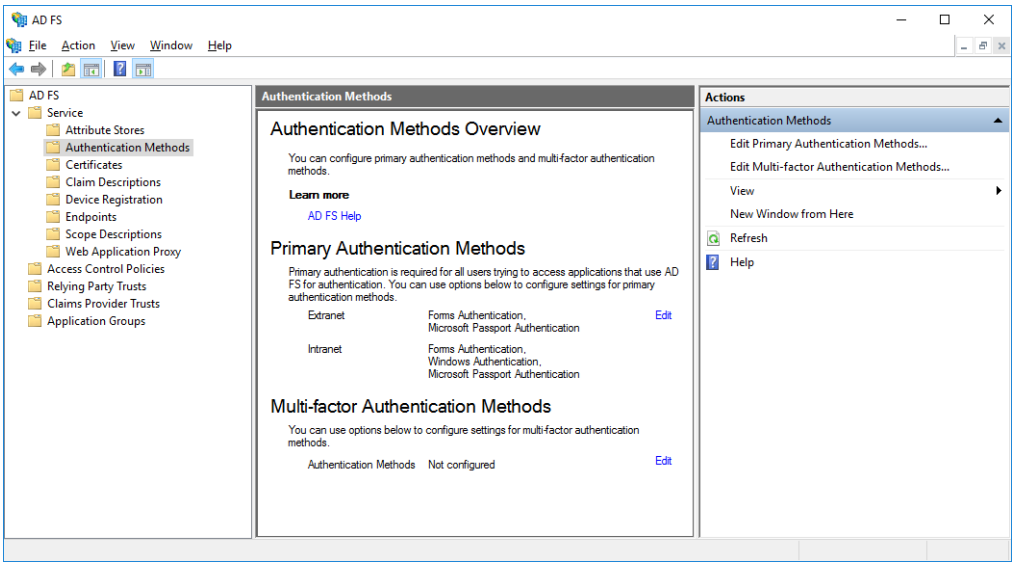
5. Click **Sign in**.

   You are successfully logged in to ADFS.



5 Configuring MFA for ADFS 4.0 on Windows Server 2016

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



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

- Enable the MyID ADFS Agent.

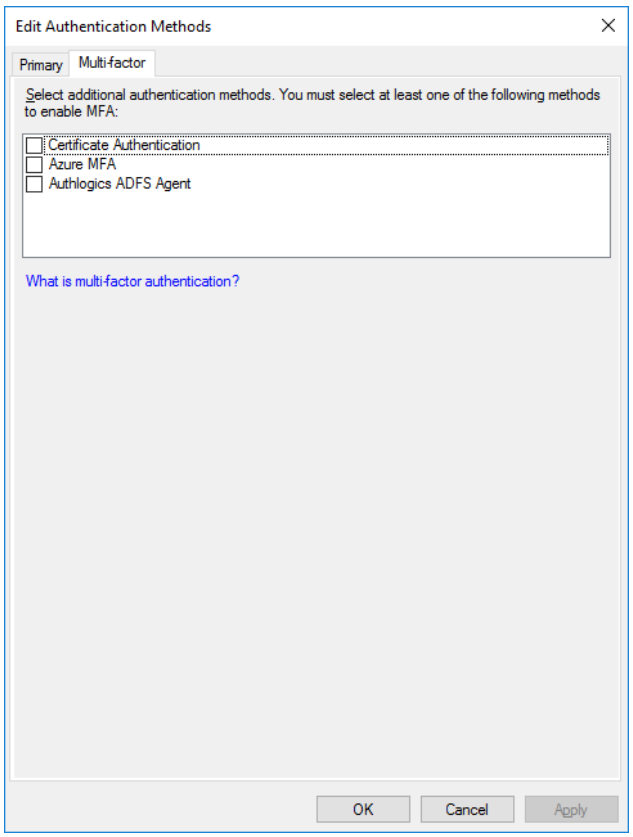
  See section *5.1*, *Enabling the MyID ADFS Agent*.
- Configure the ADFS policy.

  See section *5.2*, *Configuring the ADFS 4.0 policy*.
- Test the logon process.

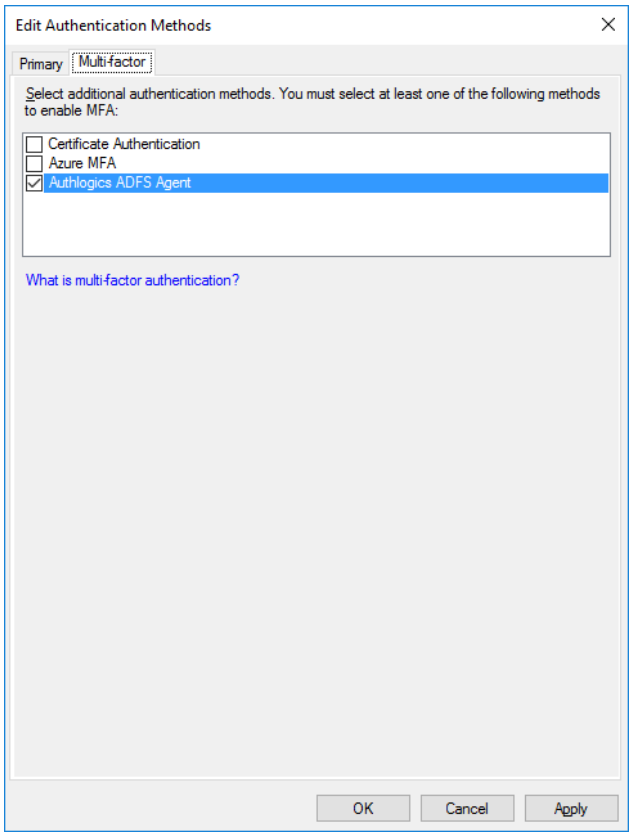
  See section *5.3*, *Testing the ADFS 4.0 logon process*.

5.1 Enabling the MyID ADFS Agent

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



3. Enable the **Authlogics ADFS Agent** option.



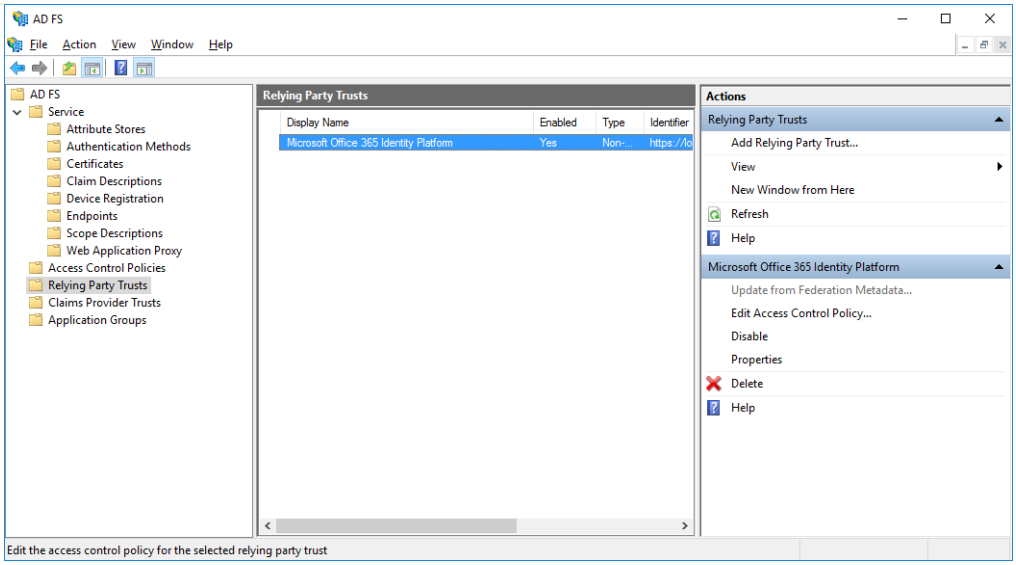
4. Click **OK**.

5.2 Configuring the ADFS 4.0 policy

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

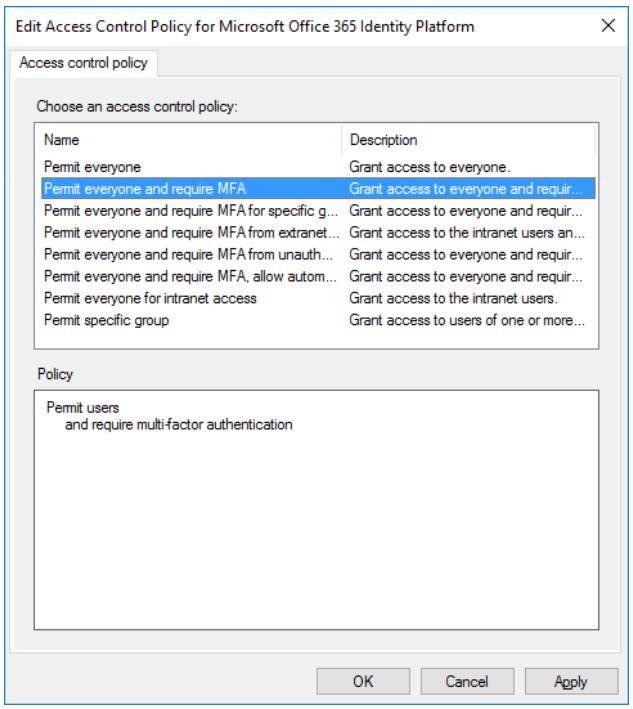
To change an existing Relying Party Trust to use an Access Control Policy that includes MFA:

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



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

   This is typically **Permit everyone and require MFA**.



5. Click **OK**.

5.3 Testing the ADFS 4.0 logon process

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

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

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

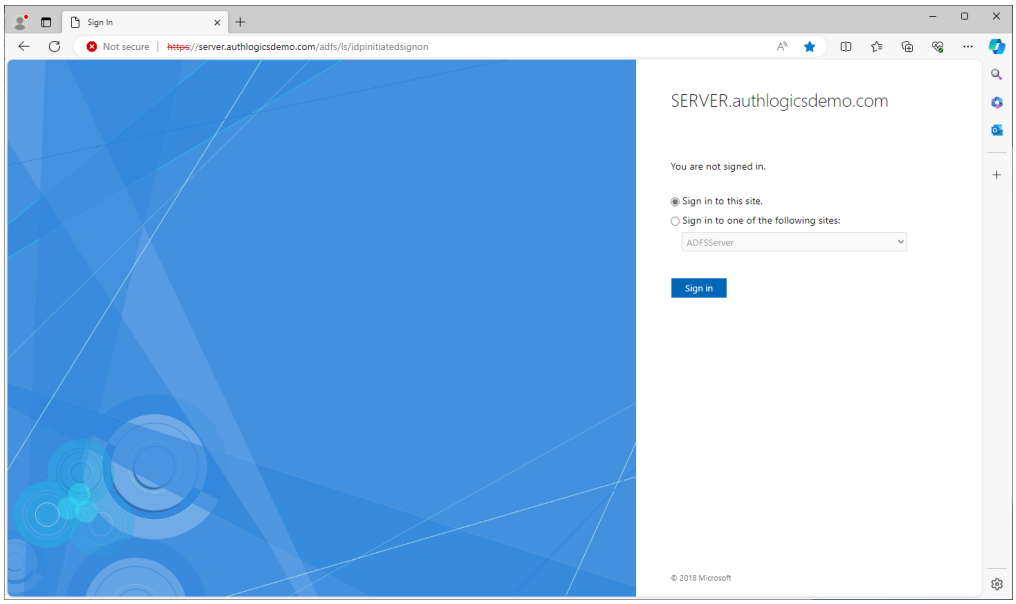
   If you do not do this, the MFA prompt does not appear in the IdP-Initiated sign on page. To add a test Relying Party Trust, see section *7.2*, *Creating a test Relying Party Trust*.

3. Open the IdP-Initiated sign on page.

   For example:

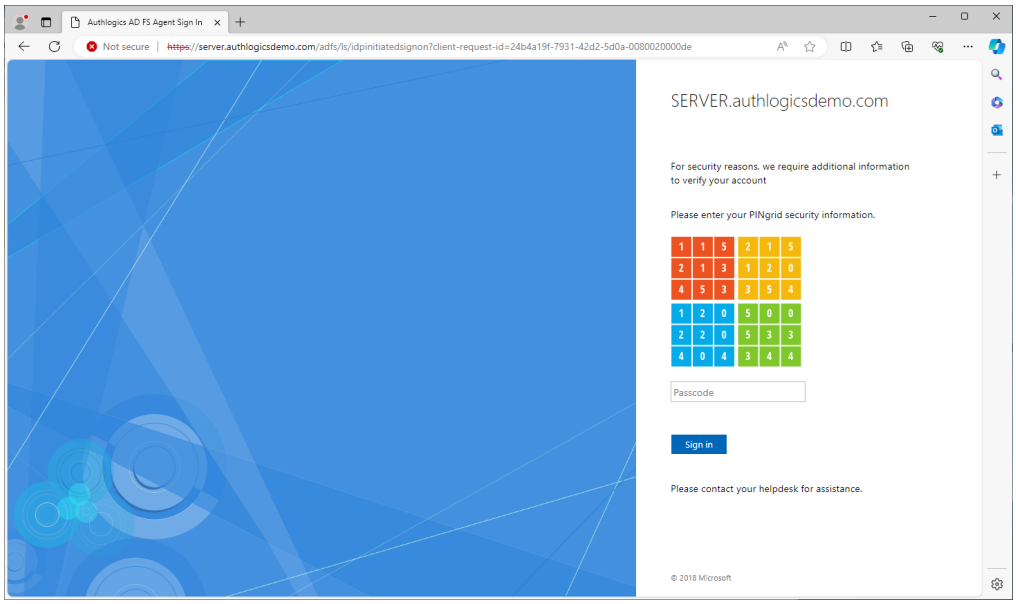
   `https://fs.authlogics.com/adfs/ls/idpinitiatedsignon`

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



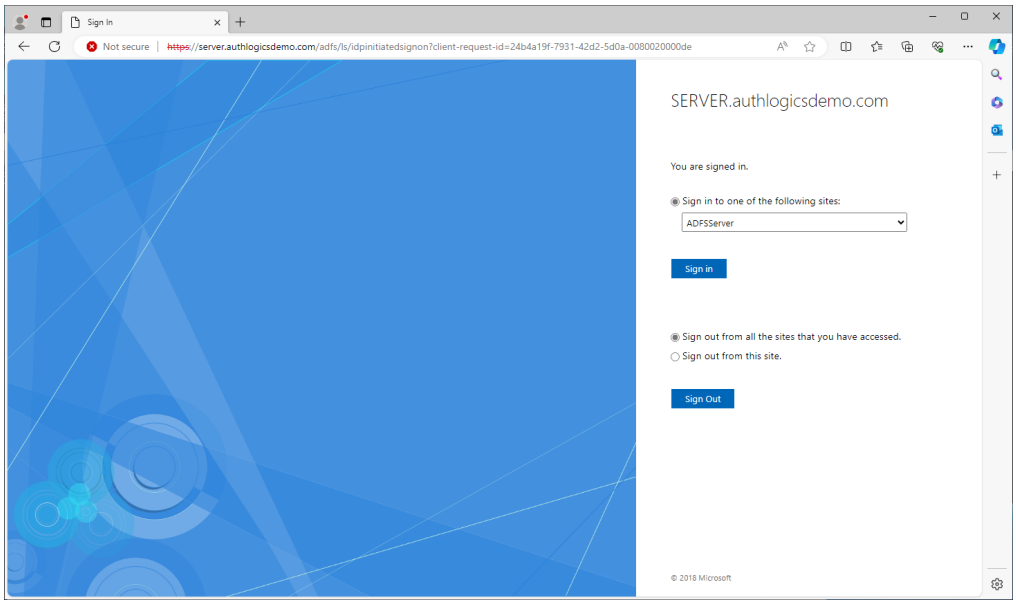
5. Click **Sign in**.
6. Enter your username and password.
7. Click **Sign in**.

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



9. Click **Sign in**.

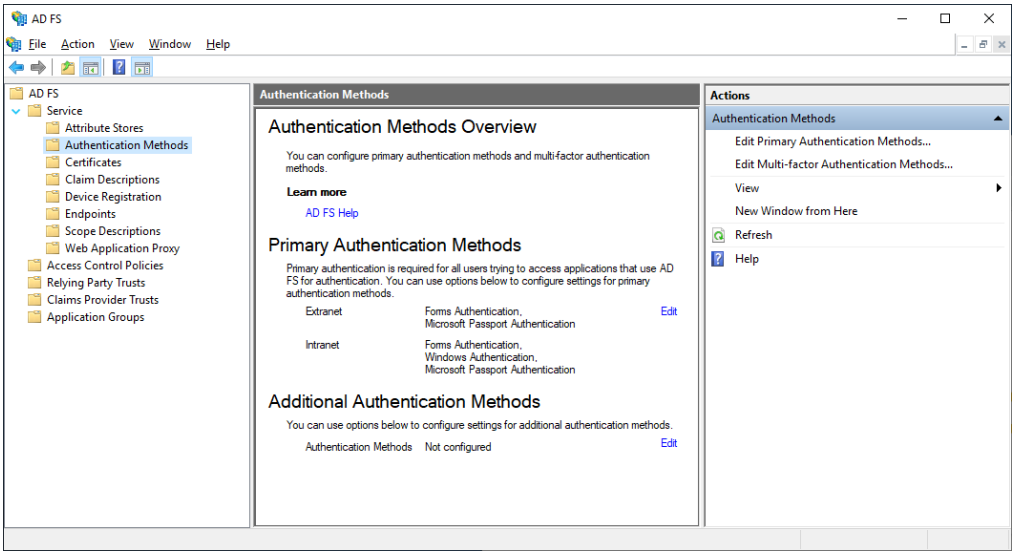
   You are successfully logged in to ADFS.



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

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

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



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

- Enable the MyID ADFS Agent. You can either:
  - Enable the MyID ADFS Agent as primary authentication.

    See section *6.1*, *Enabling the MyID ADFS Agent as primary authentication*.
  - Enable the MyID ADFS Agent as additional authentication.

    See section *6.2*, *Enabling the MyID ADFS Agent as additional authentication*.
- Configure the ADFS policy.

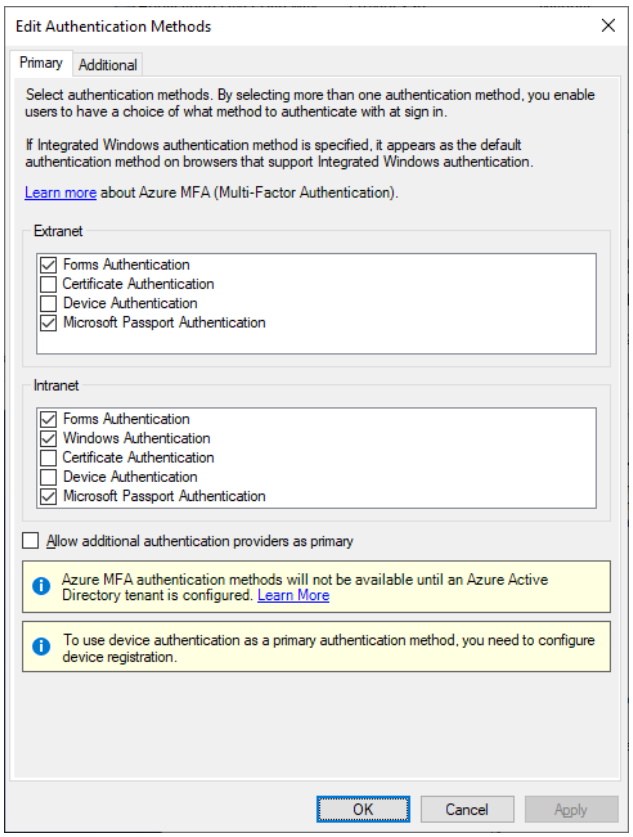
  See section *6.3*, *Configure the ADFS 5.0 / 6.0 policy*.
- Test the logon process. You can either:
  - Test the logon process with ADFS as primary authentication.

    See section *6.4*, *Testing the ADFS 5.0 / 6.0 logon process as a primary method*.
  - Test the logon process with ADFS as additional authentication.

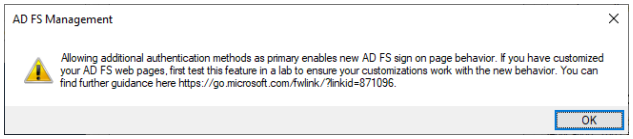
    See section *6.5*, *Testing the ADFS 5.0 / 6.0 logon process as an additional method*.

6.1 Enabling the MyID ADFS Agent as primary authentication

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



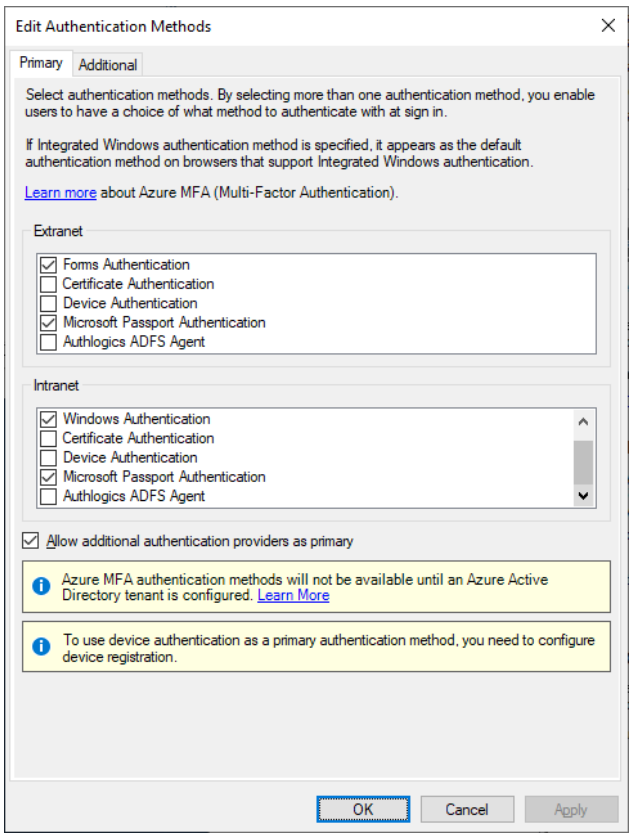
3. Enable the **Allow additional authentication providers as primary** option.



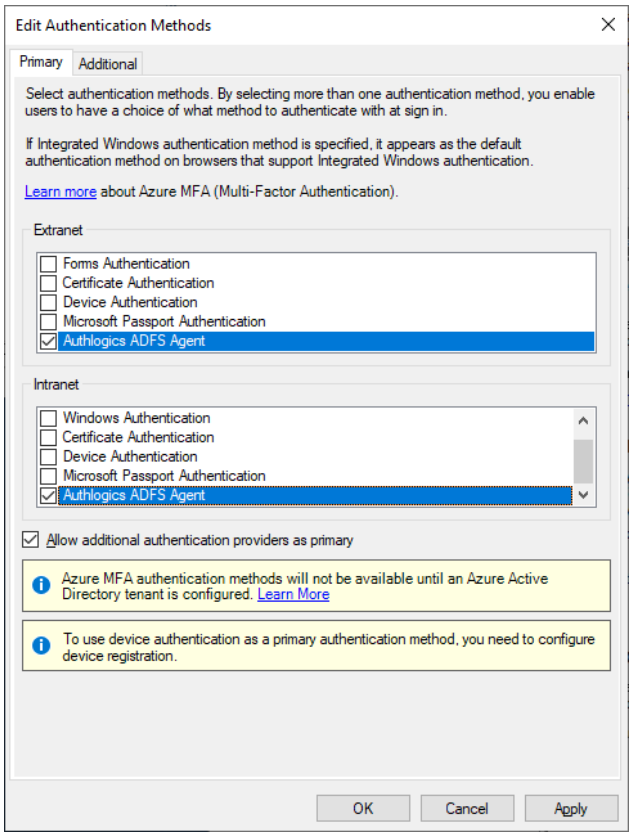
4. Click **OK**.
5. Click **OK** again, closing the **Edit Primary Authentication Methods** tab.

6. Click the Edit Primary Authentication Methods action.

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



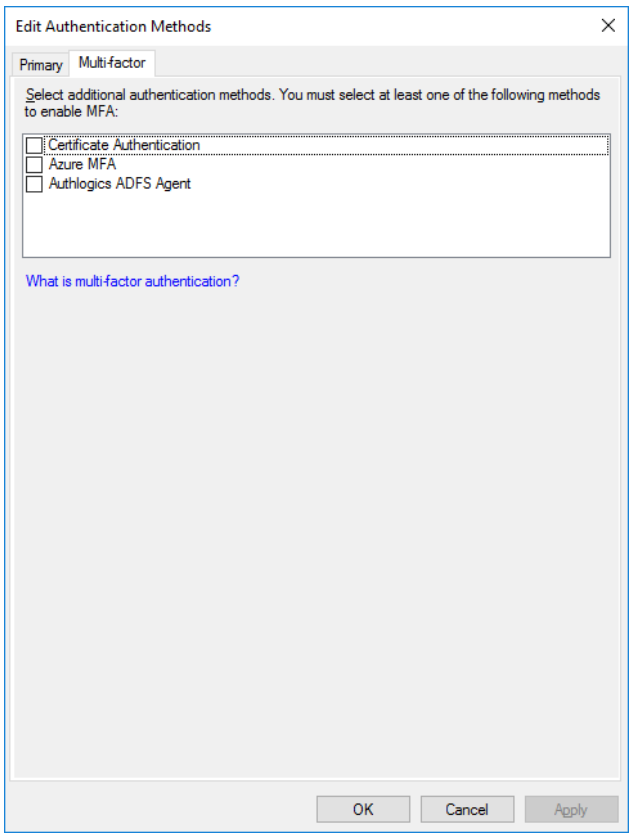
7. Select the MyID ADFS Agent for Extranet and Intranet, and deselect other methods as required:



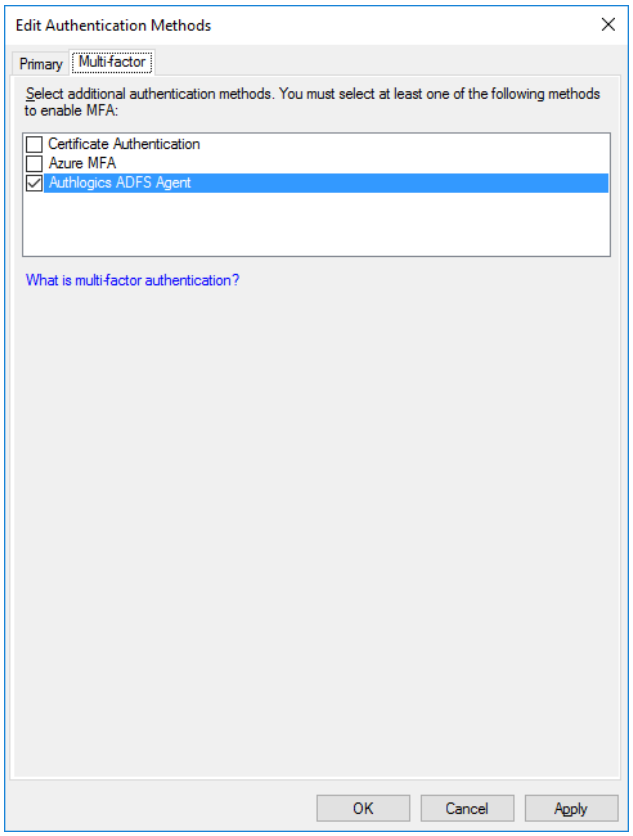
8. Click **OK** again, closing the **Edit Primary Authentication Methods** tab.

6.2 Enabling the MyID ADFS Agent as additional authentication

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



3. Enable the **Authlogics ADFS Agent** option.



4. Click **OK**.

6.3 Configure the ADFS 5.0 / 6.0 policy

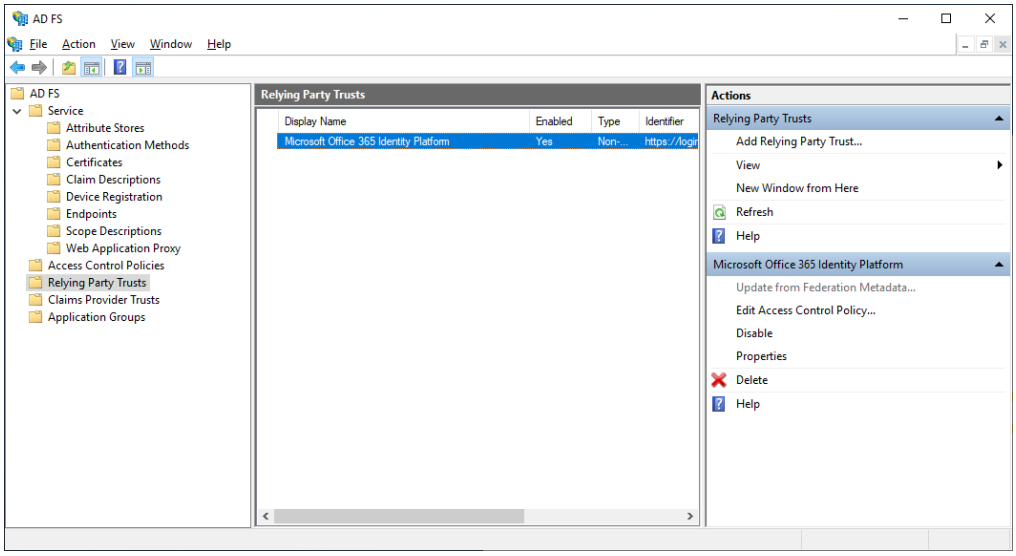
The MyID ADFS Agent works with the built in Access Control Policies. This includes policies that require MFA. Alternatively, you can create a custom policy; however, this is outside the scope of this document.

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

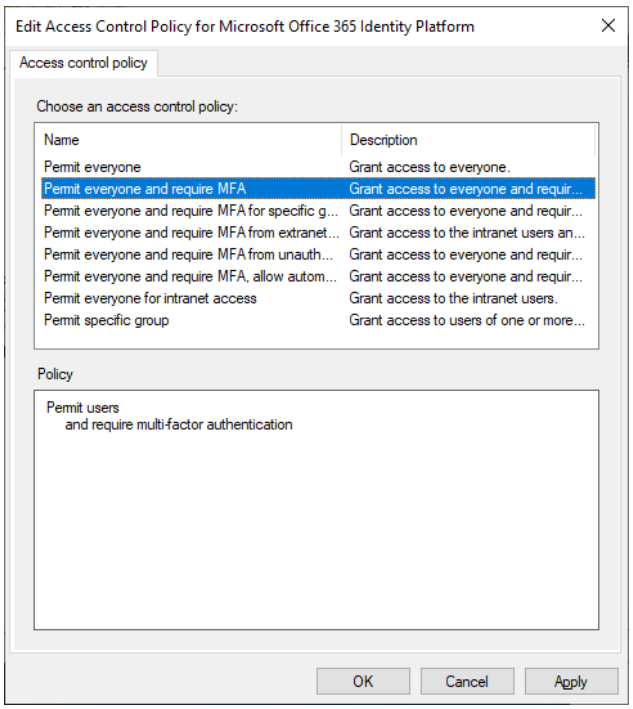
Note: If configured as Primary authentication, you must enable **All users must use Multi-Factor Authentication**. Otherwise, a non-MFA user could bypass authentication altogether.

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

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



4. Choose the Access Control Policy you want the Relying Party Trust to use. This is typically **Permit everyone and require MFA**.



5. Click **OK**.

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

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

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

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

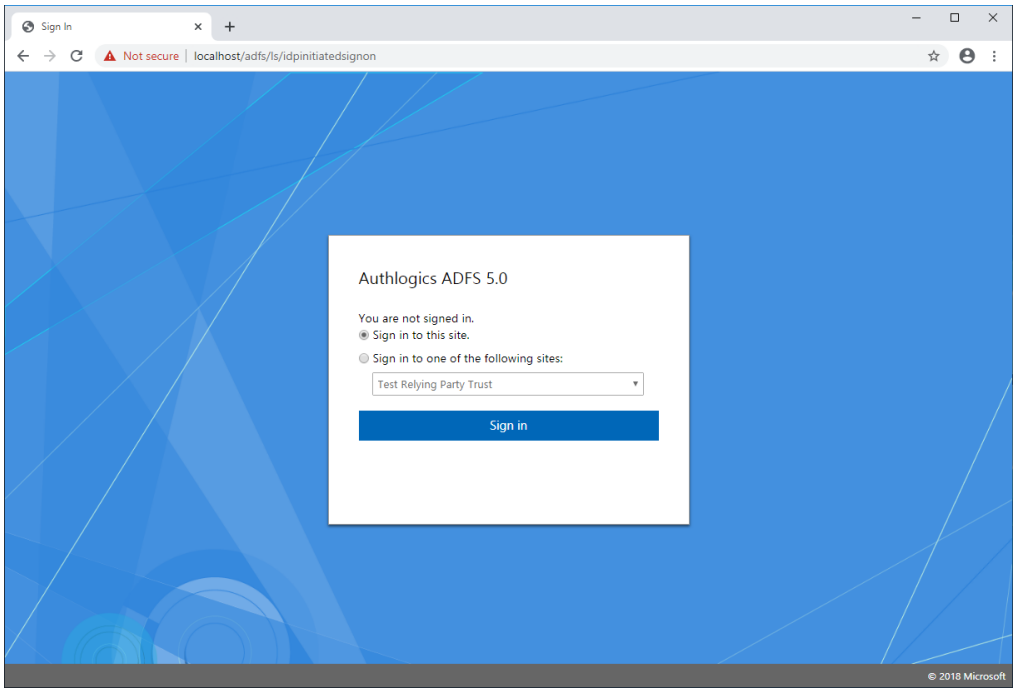
   If you do not do this, the MFA prompt does not appear in the IdP-Initiated sign on page. To add a test Relying Party Trust, see section *7.2*, *Creating a test Relying Party Trust*.

3. Open the IdP-Initiated sign on page.

   For example:

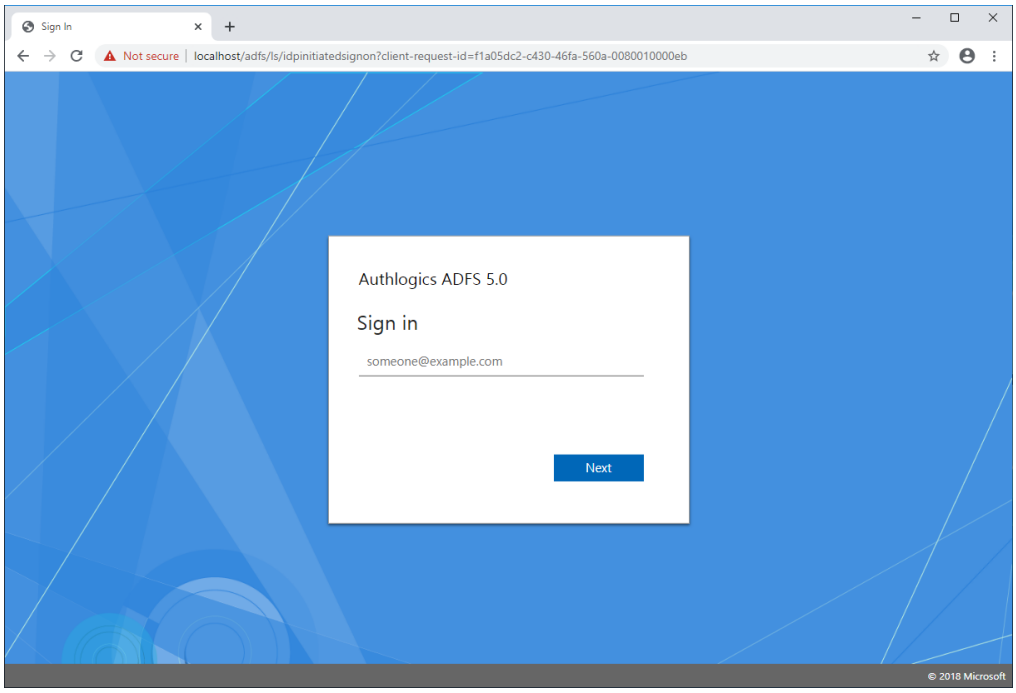
   `https://fs.authlogics.com/adfs/ls/idpinitiatedsignon`

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

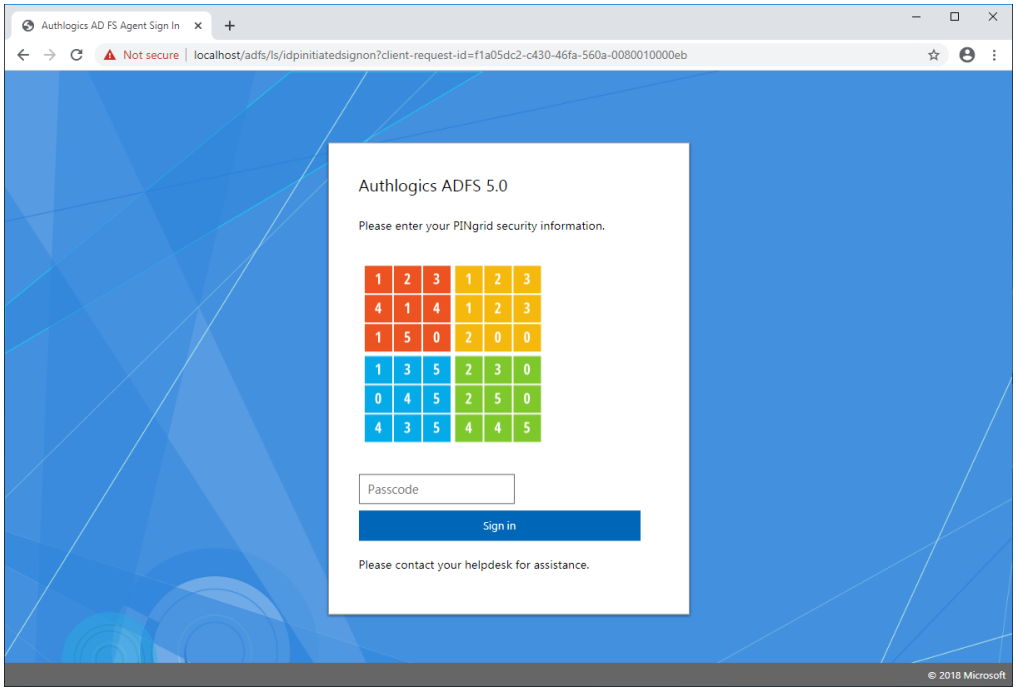


5. Click **Sign in**.

6. Enter your username.



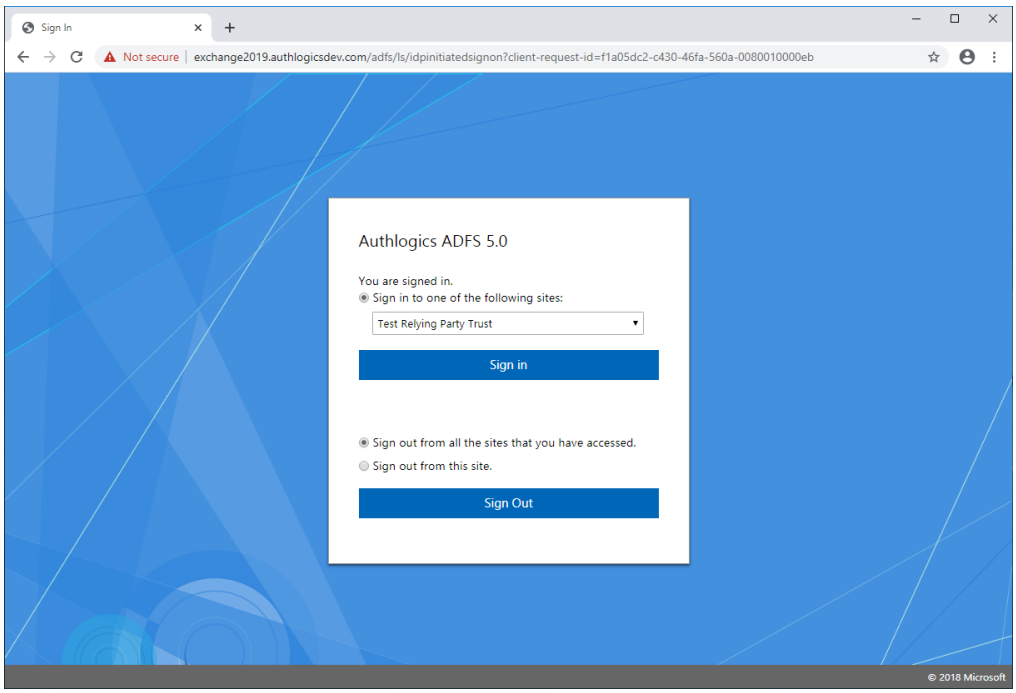
7. Click **Next**.



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

9. Click **Sign in**.

   You are successfully logged in to ADFS.



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

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

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

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

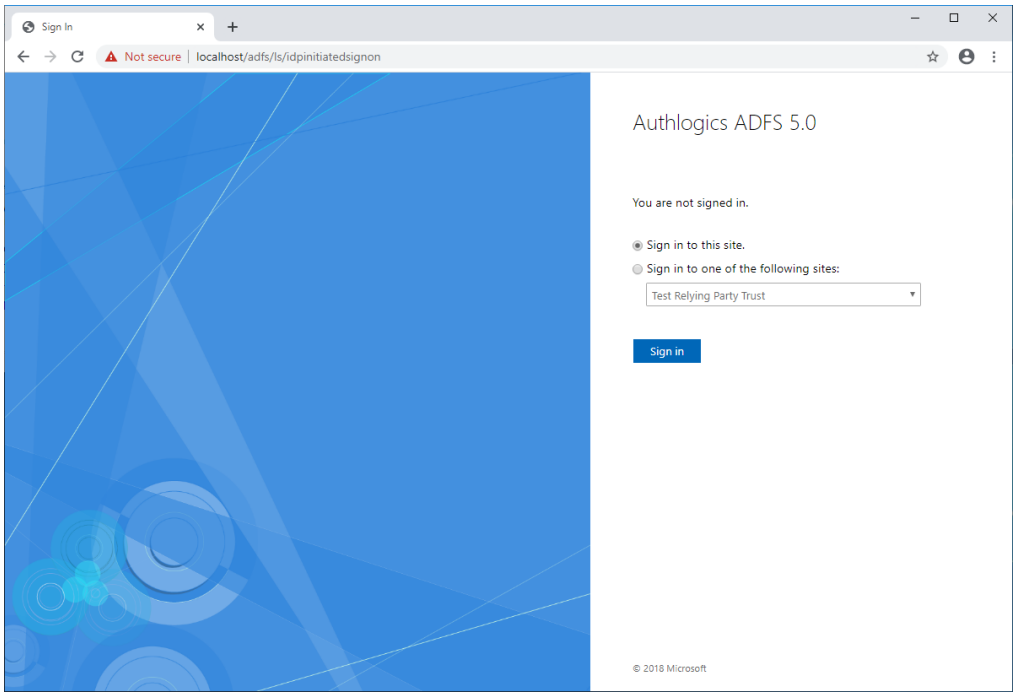
   If you do not do this, the MFA prompt does not appear in the IdP-Initiated sign on page. To add a test Relying Party Trust, see section *7.2*, *Creating a test Relying Party Trust*.

3. Open the IdP-Initiated sign on page.

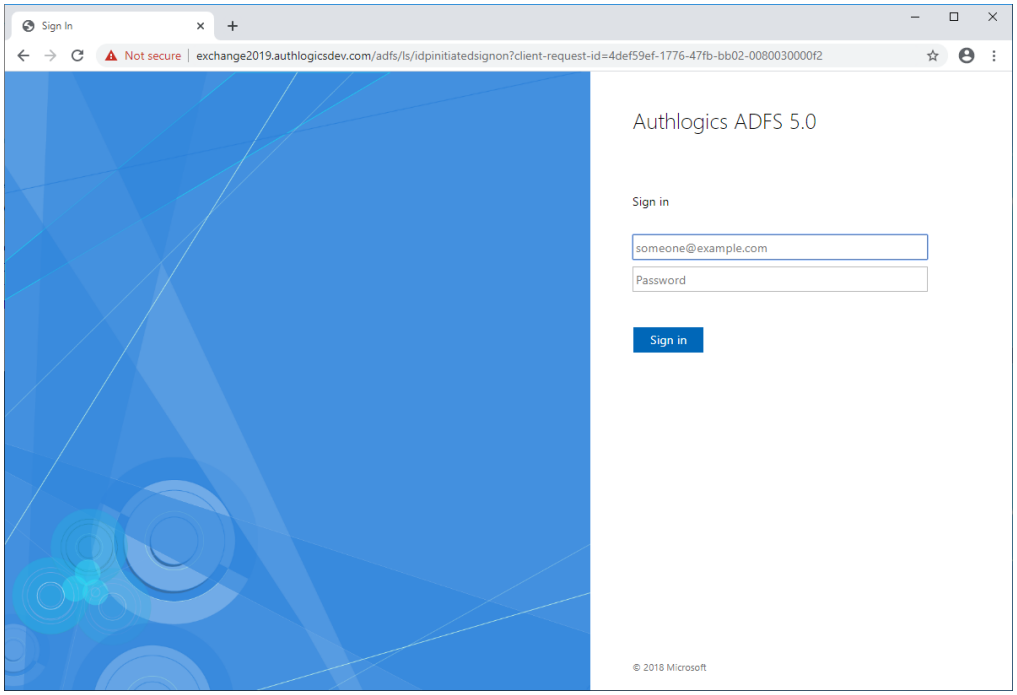
   For example:

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

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

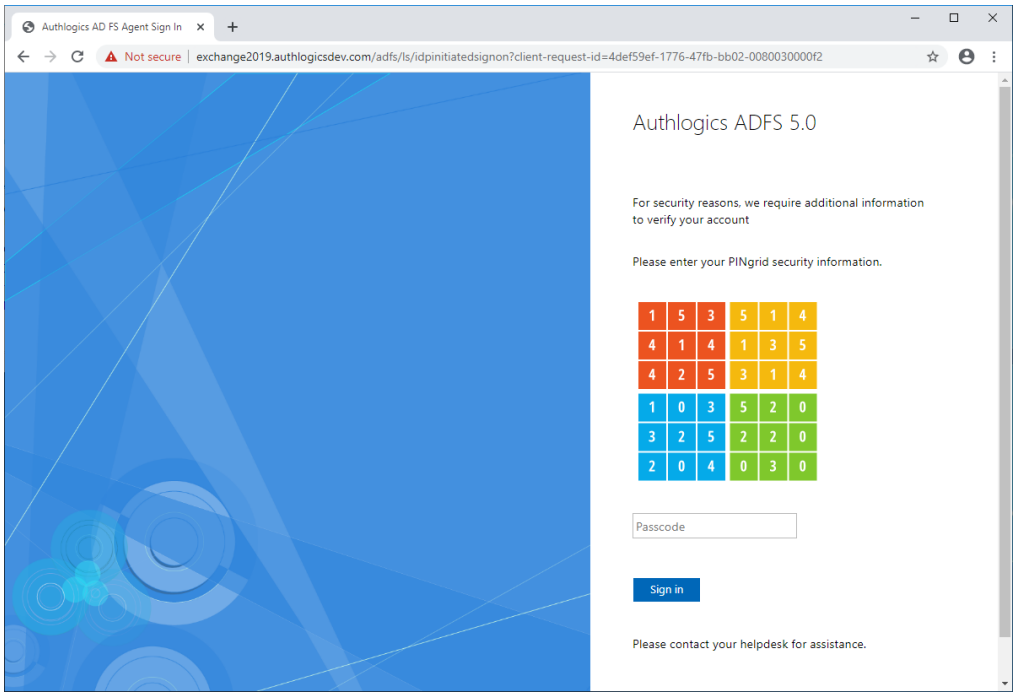


5. Click **Sign in**.



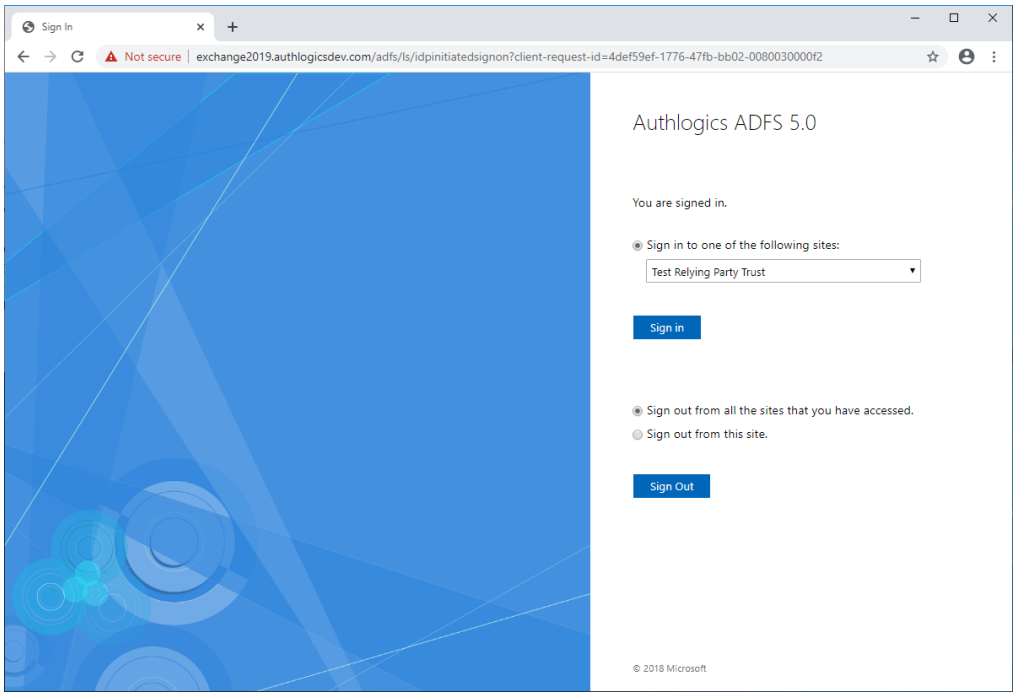
6. Enter your username and password.
7. Click **Sign in**.

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



9. Click **Sign in**.

   You are successfully logged in to ADFS.



7 Configuration testing

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

- Enable the IdP-Initiated sign-on page.

  See section *7.1*, *Enabling the IdP-Initiated sign-on page for ADFS 4.0, 5.0, & 6.0*.

- Create a test Relying Party Trust.

  See section *7.2*, *Creating a test Relying Party Trust*.

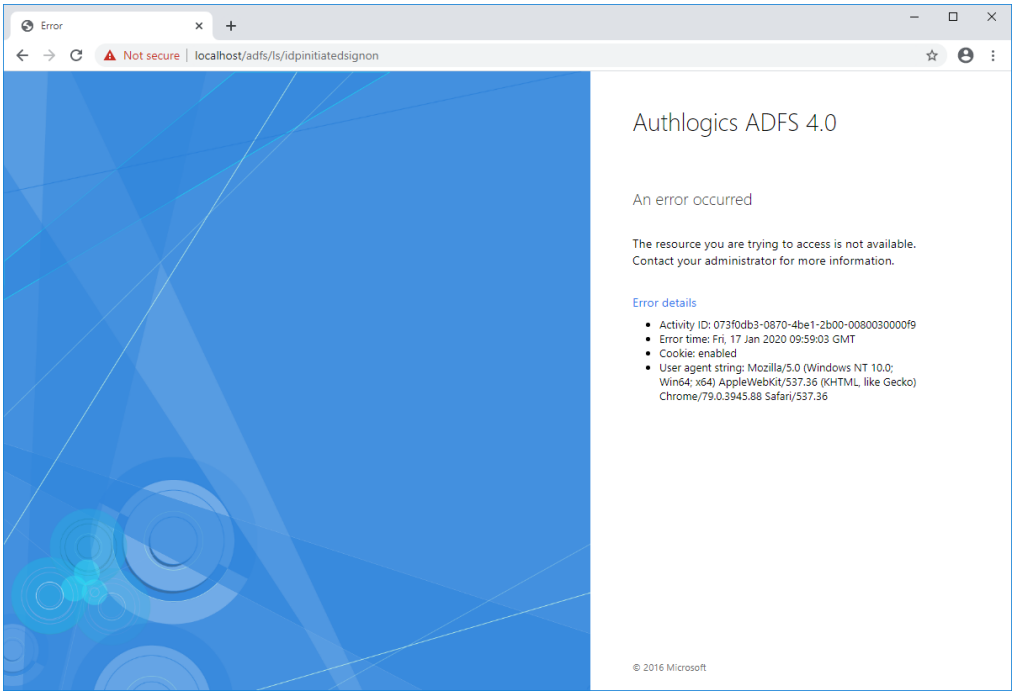
7.1 Enabling the IdP-Initiated sign-on page for ADFS 4.0, 5.0, & 6.0

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

For more information, see:

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

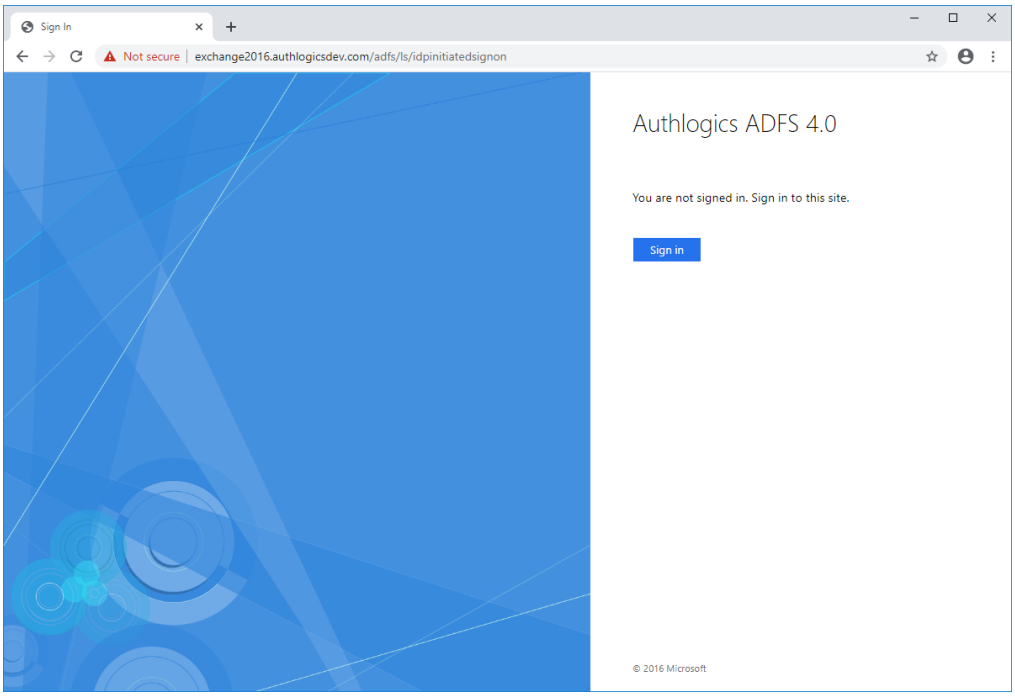
If you attempt to access the IdP-Initiated sign on page before enabling it, you get the following error page:



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

```
Set-AdfsProperties -EnableIdpInitiatedSignonPage $true
```

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

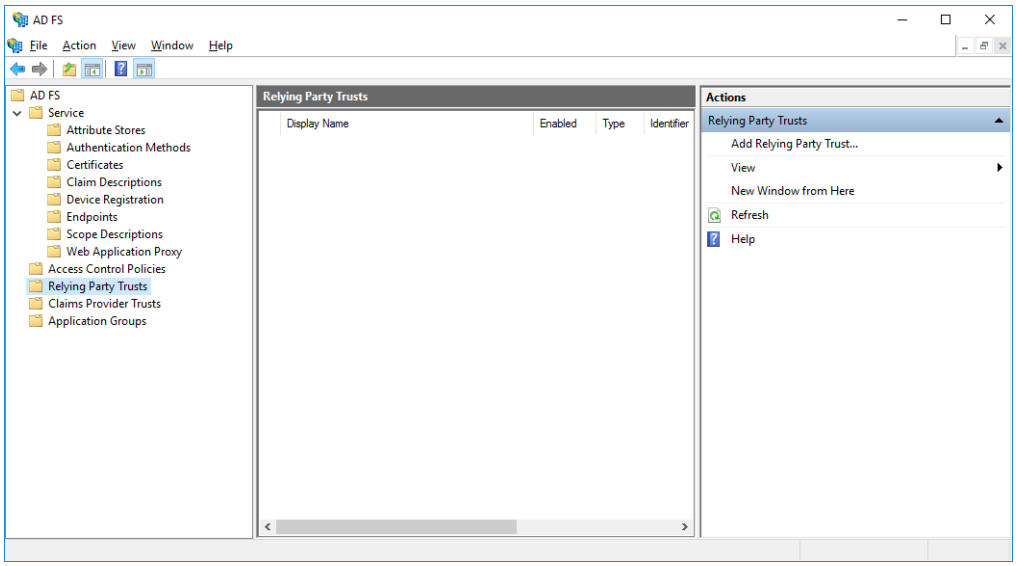


7.2 Creating a test Relying Party Trust

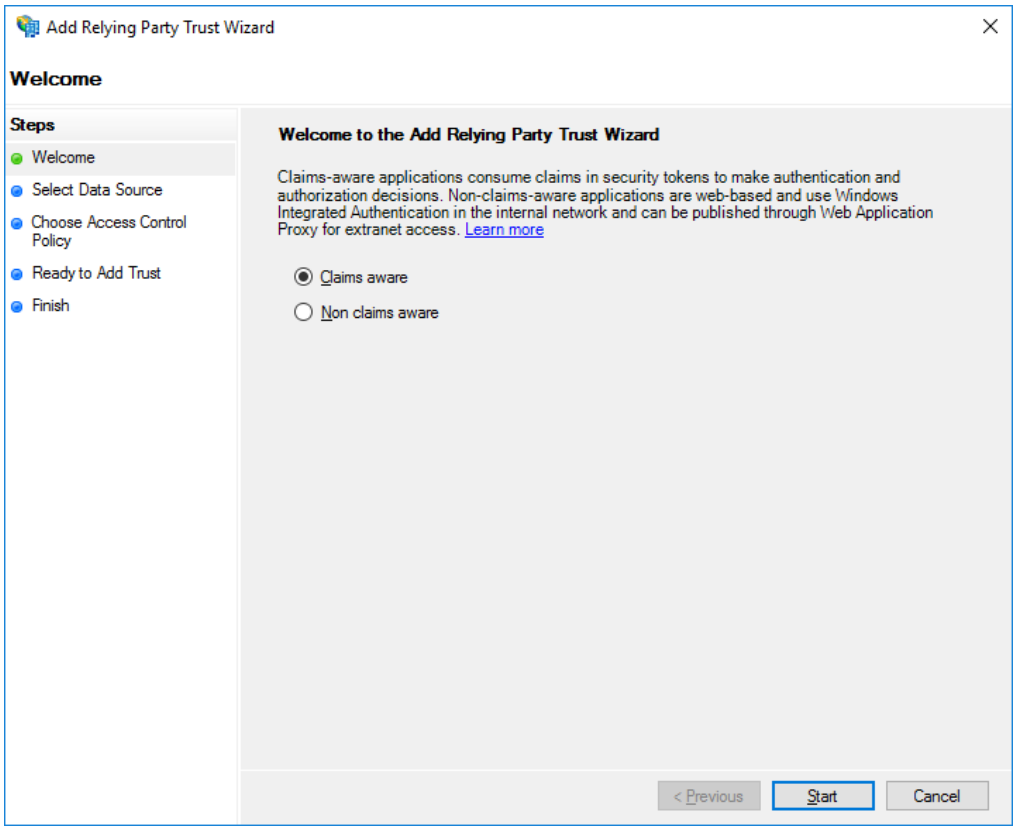
This test entry ensures that at least one Relying Party Trust entry exists on the ADFS server. You require a Relying Party Trust to assign an Access Control Policy to it so that the MFA login option appears in the IdP-Initiated sign on page.

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

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



2. Click the **Add Relying Party Trust** action.



3. Click **Start**.

4. Enter a URL to the local ADFS server.

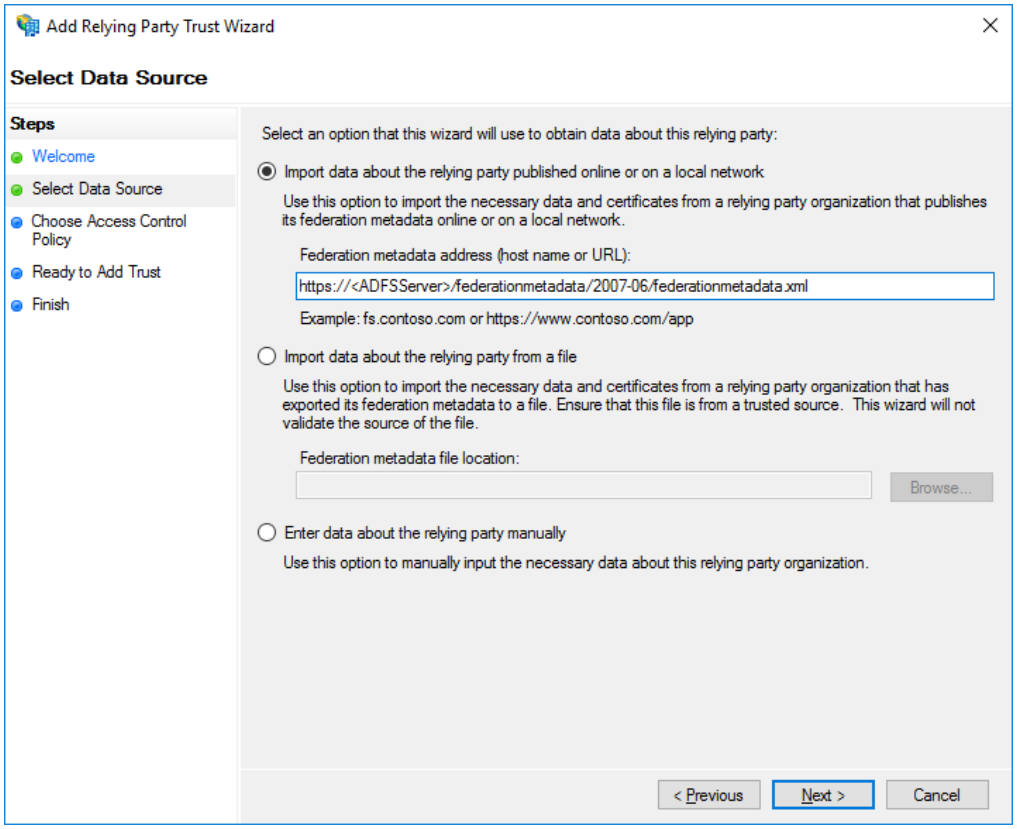
   It should have the form:

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

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

   For example:

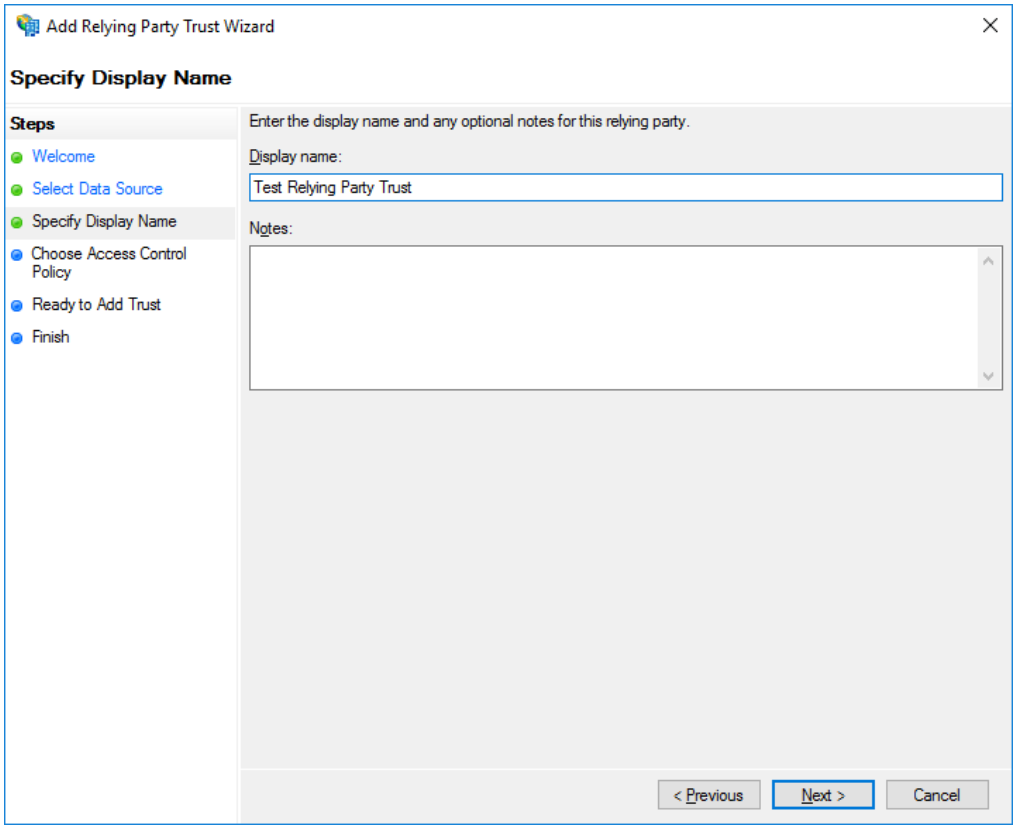
   `https://fs.authlogicsdemo.com/federationmetadata/2007-06/federationmetadata.xml`



5. Click **Next**.

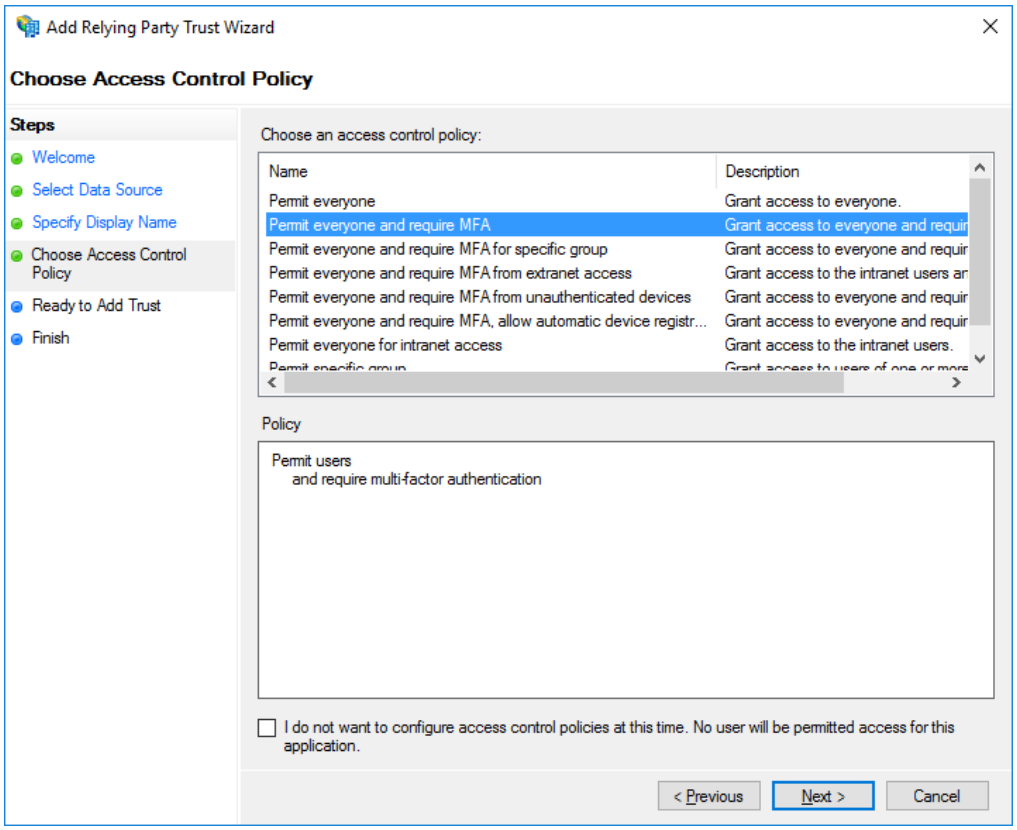
6. Enter a name for the entry.

   For example, `Test Relying Party Trust`.

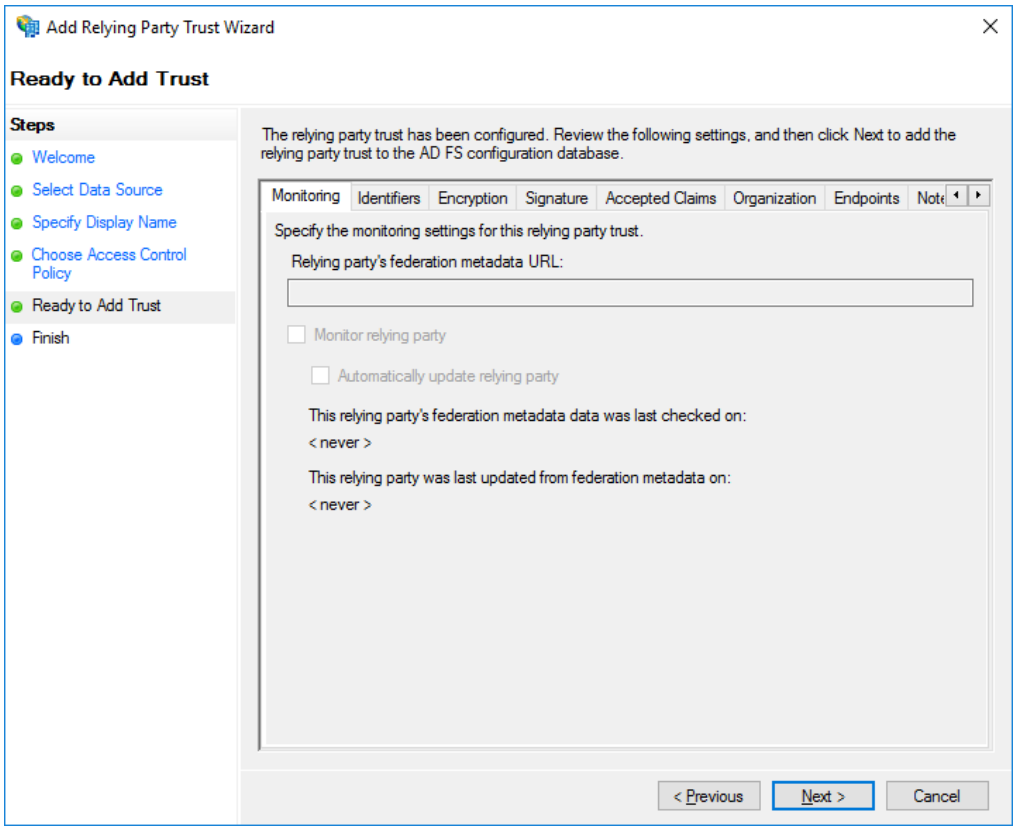


7. Click **Next**.

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

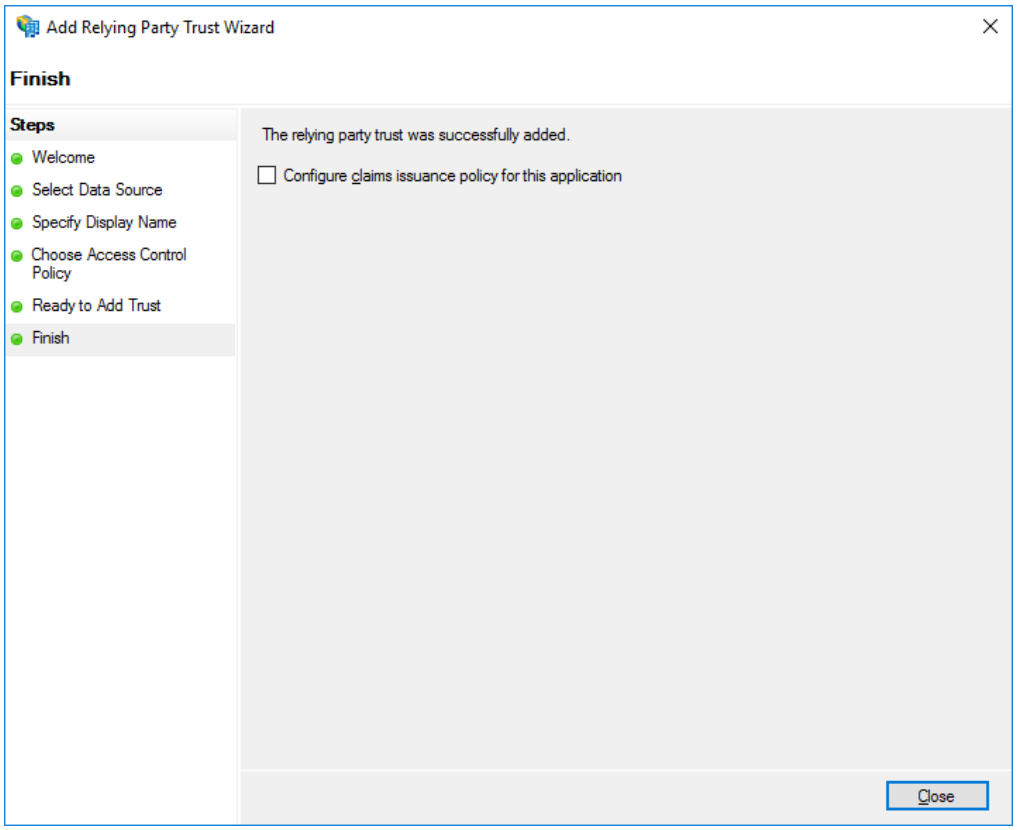


9. Click **Next**.



10. Click **Next**.

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



12. Click **Close**.

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

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

8 Advanced configuration

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

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

You can carry out the following:

- Specify Active Directory domain controllers.

  See section *8.1*, *Specifying Active Directory Domain Controllers*.
- Set the timing for Active Directory.

  See section *8.2*, *Active Directory timing*.
- Log diagnostic messages.

  See section *8.3*, *Diagnostics logging*.
- Further ADFS customization.

  See section *8.4*, *Further ADFS configuration*.

8.1 Specifying Active Directory Domain Controllers

The MyID ADFS Agent automatically locates Domain Controllers as needed. In environments where network segmentation exists, you may not be able to contact all Domain Controllers. This can cause connectivity problems and logon delays.

In those environments, you can specify which Domain Controllers and Global Catalog Servers should be used by configuring registry keys. You can use the following registry keys; each can contain one or more server names (FQDN recommended), separated by commas.

8.1.1 Specifying Global Catalog Servers

`HKLM\SOFTWARE\Authlogics\ADFS Agent\DomainGCs`

By default, this is blank.

Accepted values:

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

The MyID ADFS Agent attempts to connect to each specified Global Catalog Server and then remains connected to the server that responds to the LDAP queries the quickest.

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

8.1.2 Specifying Domain Controllers

`HKLM\SOFTWARE\Authlogics\ADFS Agent\DomainDCs`

By default, this is blank.

Accepted values:

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

The MyID ADFS Agent attempts to connect to each specified Domain Controller and then remains connected to the controller that responds to the LDAP queries the quickest.

The MyID ADFS Agent initially finds the names of each Domain in the Forest, and each Domain Controller in each Domain by querying the Global Catalog. It then maps the results against the Domain Controller list in the registry to calculate which server to use for each Domain. If a Domain does not have a Domain Controller specified, then one is selected automatically.

Note: This setting disables the auto-detect domain controller functionality within the MyID ADFS Agent.

8.2 Active Directory timing

You can set the following values in the registry:

- Domain access timeout.
- Domain controller refresh.

8.2.1 Domain access timeout

`HKLM\SOFTWARE\Authlogics\ADFS Agent\DomainAccessTimeout`

Default value: `60`

Accepted values:

- `0` – disabled, indefinite timeout.
- `1` to `120` – timeout in seconds.

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

8.2.2 Domain controller refresh

`HKLM\SOFTWARE\Authlogics\ADFS Agent\DomainControllerRefeshTime`

Default Value: `15`

Accepted Values:

- `1` to `9999` – timeout in minutes.

The time taken in minutes before a new search is done to locate the quickest Global Catalog Server and Domain Controller.

8.3 Diagnostics logging

You can control the diagnostics logging using the Windows registry.

8.3.1 Enabling logging

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

```
HKLM\SOFTWARE\Authlogics\ADFS Agent\LoggingEnabled
```

The default value is `0`.

Accepted values:

- `0` – disabled.
- `1` – enabled.

The MyID Server uses this setting.

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

8.3.2 Setting the logging location

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

```
HKLM\SOFTWARE\Authlogics\ADFS Agent\LoggingFolder
```

The default value is:

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

The MyID Server uses this setting.

Accepted values:

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

8.4 Further ADFS configuration

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

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