

# MyID MFA and PSM

Version 5.3.2

## Domain Controller Agent Integration Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK  
[www.intercede.com](http://www.intercede.com) | [info@intercede.com](mailto:info@intercede.com) | [@intercedemyid](https://twitter.com/intercedemyid) | +44 (0)1455 558111

## Copyright

© 2001-2025 Intercede Limited. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished exclusively under a restricted license or non-disclosure agreement. Copies of software supplied by Intercede Limited may not be used resold or disclosed to third parties or used for any commercial purpose without written authorization from Intercede Limited and will perpetually remain the property of Intercede Limited. They may not be transferred to any computer without both a service contract for the use of the software on that computer being in existence and written authorization from Intercede Limited.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Intercede Limited.

Whilst Intercede Limited has made every effort in the preparation of this manual to ensure the accuracy of the information, the information contained in this manual is delivered without warranty, either express or implied. Intercede Limited will not be held liable for any damages caused, or alleged to be caused, either directly or indirectly by this manual.

### **Licenses and Trademarks**

The Intercede® and MyID® word marks and the MyID® logo are registered trademarks of Intercede in the UK, US and other countries.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such. All other trademarks acknowledged.

## Conventions used in this document

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

For example:

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

For example:

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

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

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

For example:

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

For example:

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

## Contents

<b>Domain Controller Agent Integration Guide</b>	<b>1</b>
<b>Copyright</b>	<b>2</b>
<b>Conventions used in this document</b>	<b>3</b>
<b>Contents</b>	<b>4</b>
<b>1 Introduction</b>	<b>5</b>
1.1 Multi-factor authentication	5
1.2 Password security management	5
1.3 Passwordless logon for Active Directory	5
1.3.1 The MyID Windows Desktop Agent	6
1.3.2 Other agents	6
1.4 Considerations	6
1.4.1 Password policies	6
1.4.2 System requirements	6
1.4.3 Direct Internet Failover	6
1.4.4 Language requirements	7
<b>2 Design and deployment scenarios</b>	<b>8</b>
2.1 Active Directory password change workflow – policy check	8
2.2 Active Directory password change workflow – passwordless vault update	9
2.3 Active Directory shared password protection workflow	10
<b>3 Deployment</b>	<b>11</b>
3.1 Prerequisites	11
3.2 Installing the MyID Domain Controller Agent	12
3.3 Updating the MyID Domain Controller Agent	15
3.4 Uninstalling the MyID Domain Controller Agent	16
3.5 Deploying certificates	16
3.6 Configuring the MyID Domain Controller Agent Policy settings	17
3.6.1 General settings	17
3.7 Automated / command line setups	22
3.7.1 Running an installation with verbose logging	22
3.7.2 Fully automated silent installation	22
3.7.3 Fully automated silent removal	22
<b>4 Advanced configuration</b>	<b>23</b>
4.1 Diagnostics logging	23
4.1.1 Enabling logging	23
4.1.2 Setting the logging location	23
4.1.3 Setting the retention time for rolling logs	24
4.1.4 Size limit of rolling log files	25
4.1.5 Example of rolling logs	25

## 1 Introduction

The MyID Domain Controller Agent is a lightweight service component that ensures that all new passwords comply with the latest NIST SP 800-63B guidance and keeps the Microsoft password database and the MyID Password Vault in sync at all times, regardless of what mechanism is used to change or reset an Active Directory password.

**Note:** The Domain Controller Agent *must* be installed on all writable Domain Controllers in the Active Directory domain.

The MyID Domain Controller Agent is a service component of both MyID Multi-Factor Authentication (MFA) and MyID Password Security Management (PSM) solutions.

**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 Multi-factor authentication

The MyID Domain Controller Agent is used by MyID MFA to do the following:

- Intercept successful password changes and store them in the MyID Password Vault.

### 1.2 Password security management

The MyID Domain Controller Agent is used by MyID PSM to do the following:

- Intercept password change requests made on the Windows Domain in real-time.
- Process password change requests against a modern and secure password policy to see if they comply, including checking if the password is:
  - breached online.
  - already used in the AD.
- Randomize the passwords of user accounts that no longer require a password.

### 1.3 Passwordless logon for Active Directory

The MyID Authentication Server includes a highly secure password vault that stores a copy of users' Active Directory passwords.

If a user logs into an application that requires Windows authentication using an alternative logon method, MyID MFA uses the passwords from the password vault to log the user in.

The password vault is disabled by default and must be explicitly enabled. When active, it is secured with AES256 bit encryption using an asymmetric key pair from a digital certificate. The private key may be stored in a Hardware Security Module (HSM) if required.

### 1.3.1 The MyID Windows Desktop Agent

The MyID Windows Desktop Agent allows users to log on to Windows desktops and servers without needing to enter their Windows password. This form of passwordless logon is achieved by retrieving the user's password stored in the password vault and delivering it to the Windows desktop on the user's behalf when they log on.

Logging onto Windows in this way ensures compatibility with existing Windows applications that rely on Active Directory credentials.

Passwordless logon is disabled by default; to enable it on Windows systems, set the **Enable Passwordless logons** group policy option on the Windows Desktop Agent.

### 1.3.2 Other agents

MyID also has the following agents:

- The MyID Exchange Agent.

The MyID Exchange Agent also uses the Password Vault to provide passwordless access into the Outlook Web App.

- The MyID ADFS Agent.

The MyID ADFS Agent, when installed on Windows Server 2019 or higher, provides passwordless access to federated applications. It does not require the password vault to provide this functionality.

## 1.4 Considerations

### 1.4.1 Password policies

The MyID PSM Password Policy complies with NIST SP 800-63B guidance, but the Windows Default Domain Policy does not have this ability. You must modify the Windows password policy after deploying the MyID PSM Password Policy to avoid conflicts.

The MyID Authentication Server and the MyID Domain Controller Agent work together to provide the overall password security management functionality.

### 1.4.2 System requirements

The MyID Domain Controller Agent is designed to work with a MyID Authentication Server; you must deploy the server before installing the agent.

The installer checks for pre-requisites and installs them automatically where possible. The pre-requisites are:

- Microsoft Visual C++ 2010 SP1 Runtime Libraries.
- .NET 8.

**Note:** The Visual C++ 2010 Runtime and .NET 8 Libraries for 64-bit systems are included in the agent installer. If the installation of a prerequisite fails, the agent installation will also fail.

### 1.4.3 Direct Internet Failover

The MyID Domain Controller Agent does not require direct access to the Internet, as all connectivity to the cloud is performed by the MyID Authentication Server. However, you can configure the MyID Domain Controller Agent to connect to the cloud in a failover scenario if the MyID Authentication Server is unavailable. This option is disabled by default.

To allow this, all Domain Controllers require Internet access to the following URLs:

- The destination URL:  
`https://passwordsecurityapi.authlogics.com/api/*`
- The host:  
`passwordsecurityapi.authlogics.com`  
Specifically, on port 443.

You can configure a web proxy server using Group Policy to allow indirect Internet access instead of a routed connection. Proxy authentication is automatically performed using the Windows Machine account credentials. If the proxy does not support Windows Authentication, you must grant anonymous access to the domain controllers. Static proxy server credentials are not supported.

#### 1.4.4 Language requirements

MyID Domain Controller Agent is available only in English. Product support and documentation are available only in English.

## 2 Design and deployment scenarios

The MyID Domain Controller Agent has been designed to work seamlessly in a Windows and Active Directory environment.

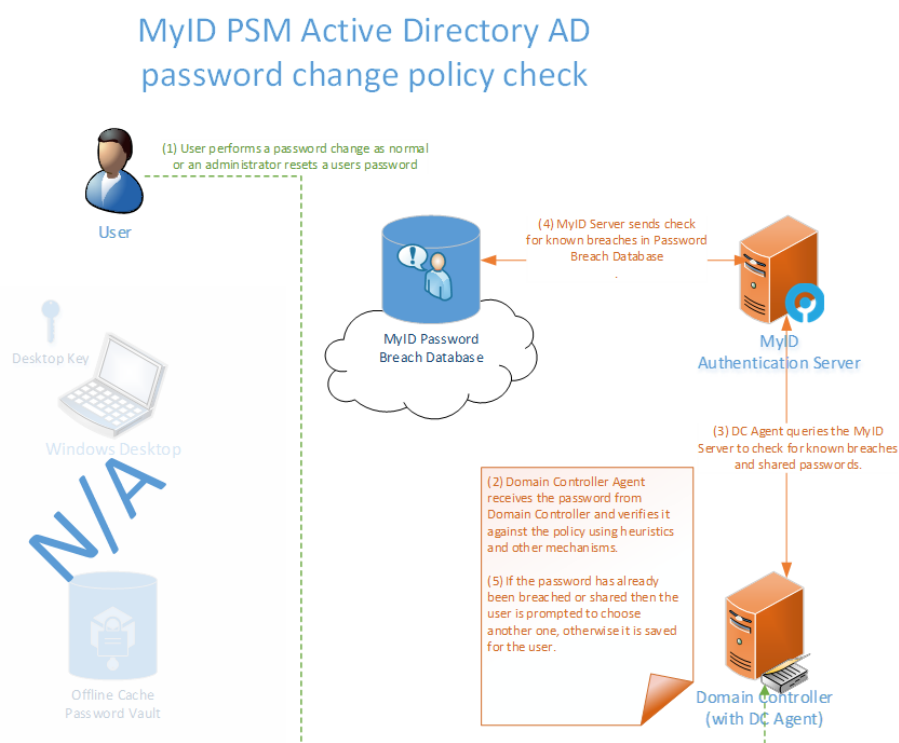
The Password Security Management password policy is controlled through Active Directory Group Policy for flexible, centralized management.

This chapter contains information on the following scenarios:

- An Active Directory password reset/change to check the password against the defined policy.  
See section [2.1, Active Directory password change workflow – policy check](#)
- An Active Directory password reset/change to update the MyID Server Password Vault.  
See section [2.2, Active Directory password change workflow – passwordless vault update](#).
- An Active Directory password reset/change to ensure the uniqueness of a password and prevent the use of shared passwords in the domain.  
See section [2.3, Active Directory shared password protection workflow](#).

### 2.1 Active Directory password change workflow – policy check

The following workflows depict the steps that are performed during an AD password reset/change to check the password against the defined policy:

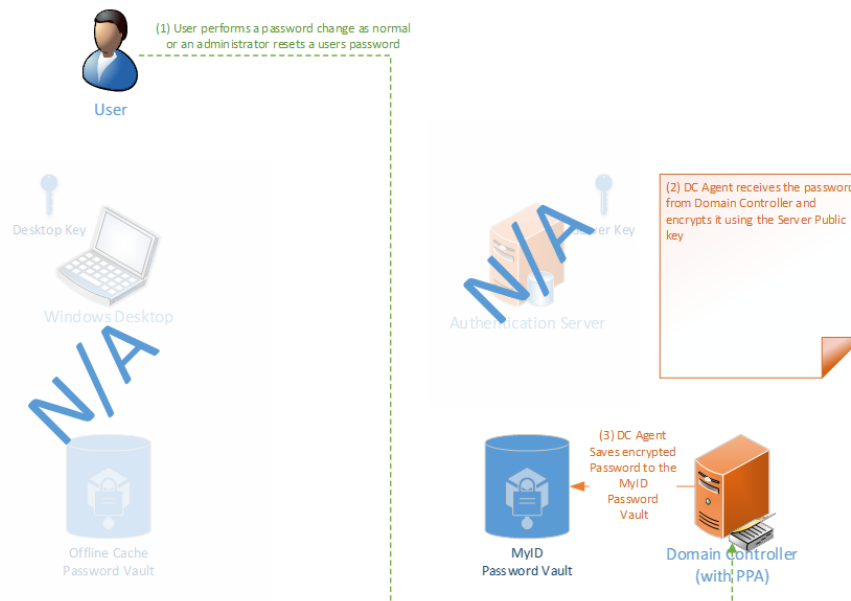




## 2.2 Active Directory password change workflow – passwordless vault update

The following workflows depict the steps that are performed during an AD password reset/change to update the MyID Server Password Vault:

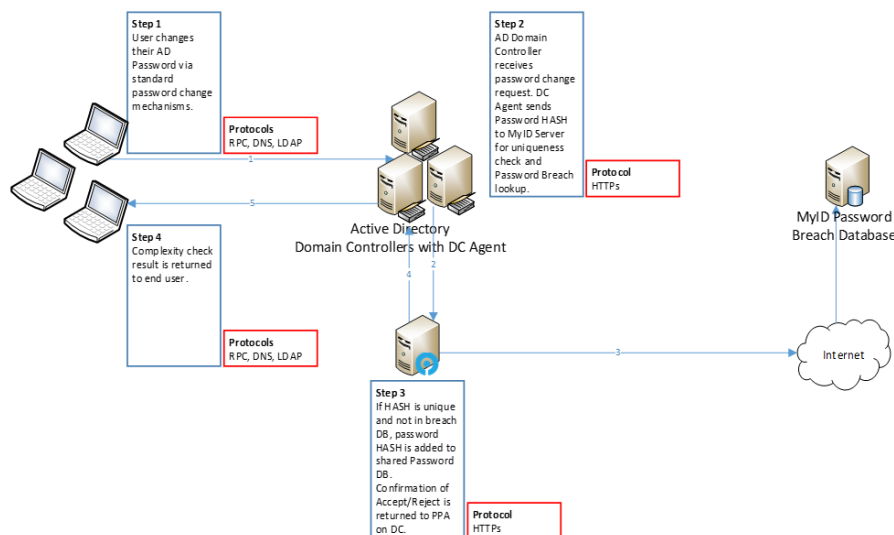
### Active Directory Passwordless AD password change capture



## 2.3 Active Directory shared password protection workflow

The following workflows depict the steps that the MyID Domain Controller Agent performs during an Active Directory password reset/change to ensure the uniqueness of a password and prevent the use of shared passwords in the domain:

Domain Controller Agent Shared Password Process Flow



**Note:** To prevent shared passwords from being selected, you must run the Password Security Management Wizard on the MyID Authentication Server with the current domain being enabled for PSM. See the [MyID Authentication Server Installation and Configuration Guide](#) for further information.

## 3 Deployment

The following deployment overview walks through the installation process for deploying the MyID Domain Controller Agent.

This chapter covers the following deployment related subjects:

- The prerequisites to installation.  
See section [3.1, Prerequisites](#).
- Installing the MyID Domain Controller Agent.  
See section [3.2, Installing the MyID Domain Controller Agent](#).
- Updating the MyID Domain Controller Agent.  
See section [3.3, Updating the MyID Domain Controller Agent](#).
- Uninstalling the MyID Domain Controller Agent.  
See section [3.4, Uninstalling the MyID Domain Controller Agent](#).
- Deploying certificates.  
See section [3.5, Deploying certificates](#).
- Configuring the MyID Domain Controller.  
See section [3.6, Configuring the MyID Domain Controller Agent Policy settings](#).
- Using Automated / command line setups.  
See section [3.7, Automated / command line setups](#).

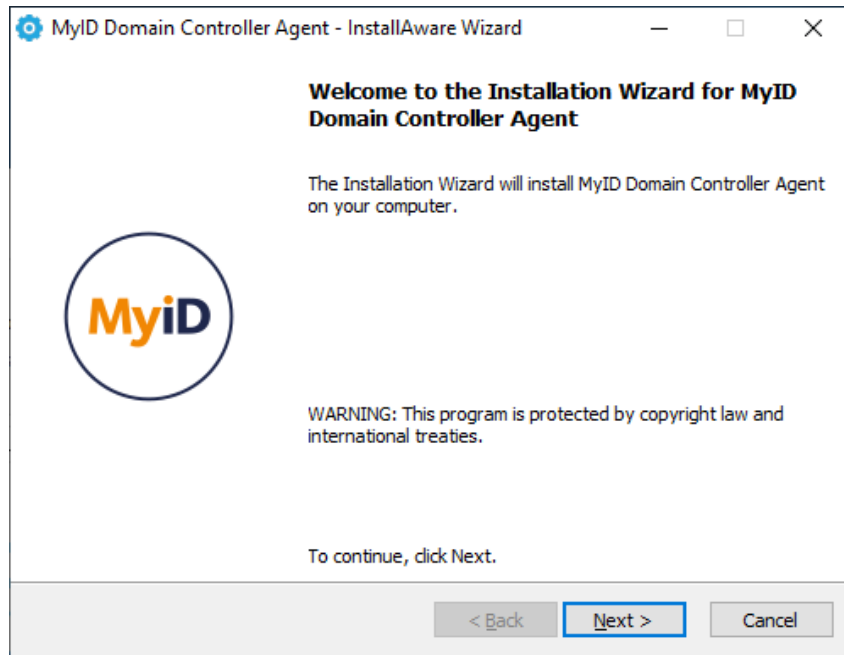
### 3.1 Prerequisites

This deployment section assumes that at least one MyID Authentication Server has already been installed and is functional. For more information on setting up the MyID Authentication Server, see the [MyID Authentication Server Installation and Configuration Guide](#).

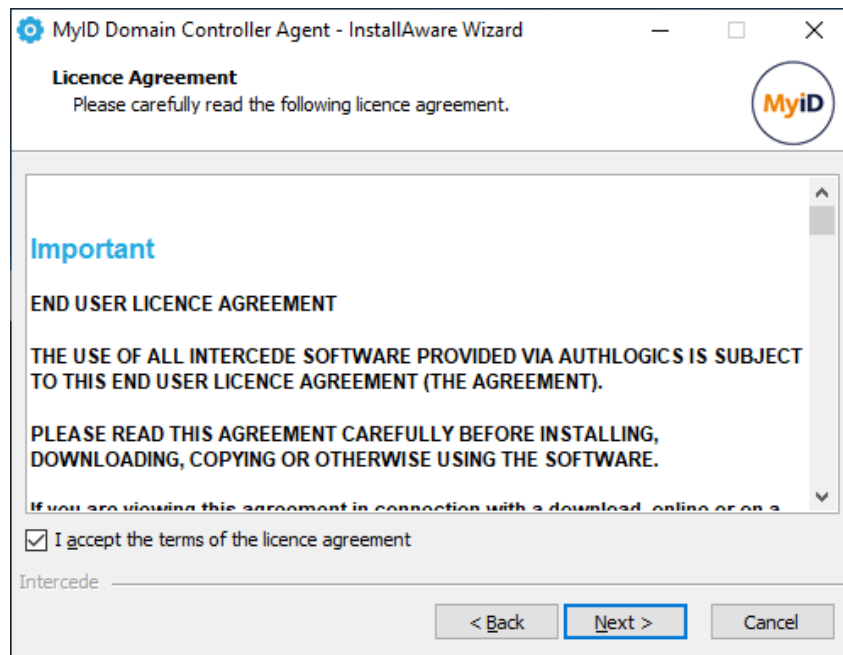
## 3.2 Installing the MyID Domain Controller Agent

**Note:** This section of the installation process requires Administrator rights on the domain controller.

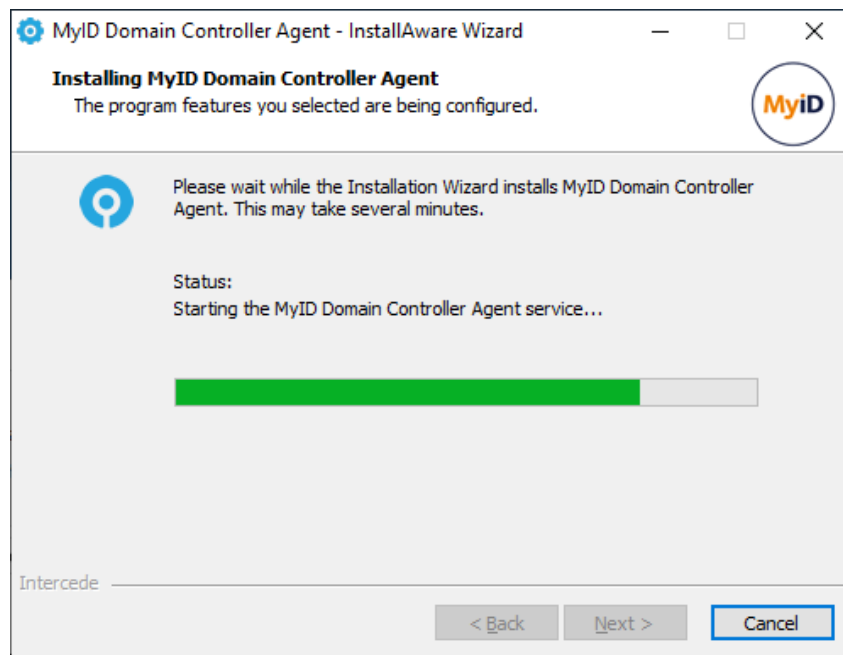
1. Run the MyID Domain Controller Agent `xxxxx.msi` installer with elevated privileges.  
Depending on the Windows security settings you may need to start the setup from an elevated command prompt.
2. Click **Next**.



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

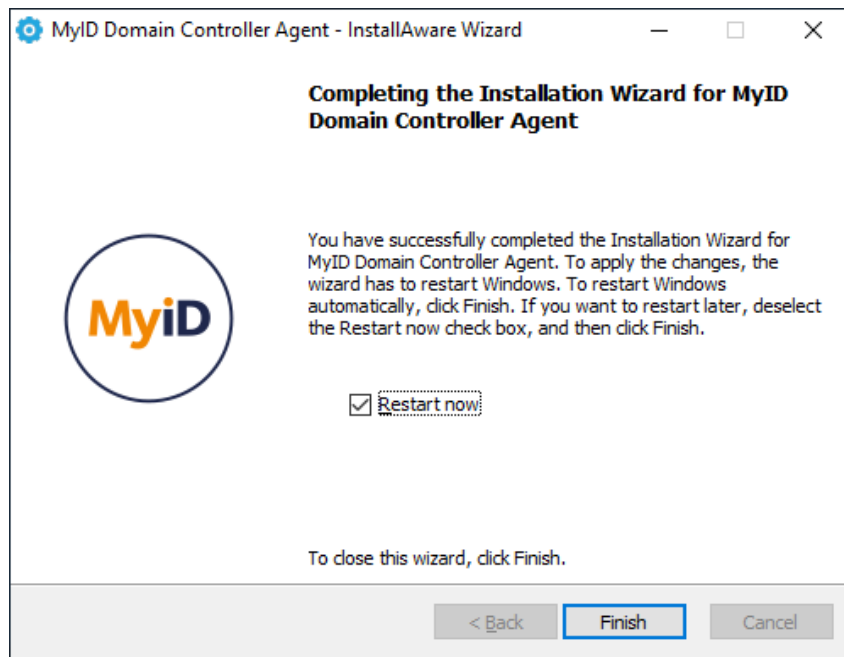


4. Click **Next**.



The installation is being performed.

5. If you plan to reboot later, uncheck the **Restart now** box.



**Note:** The Domain Controller *must* be restarted for changes to take effect.

6. Click **Finish** to complete the installation process.

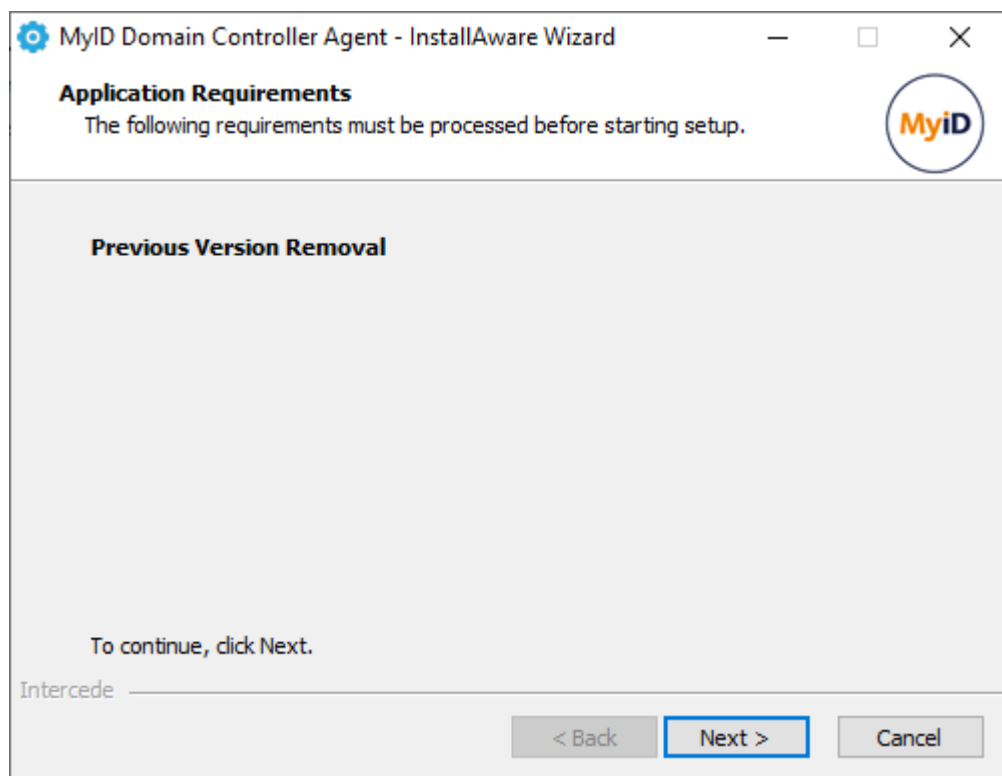
### 3.3 Updating the MyID Domain Controller Agent

You can use the installation program of an update for a full clean install, or to perform an in-place update of an existing installation.

**Note:** This section of the installation process requires Administrator rights on the domain controller.

1. Run the MyID Domain Controller Agent `xxxxx.msi` installer with elevated privileges.

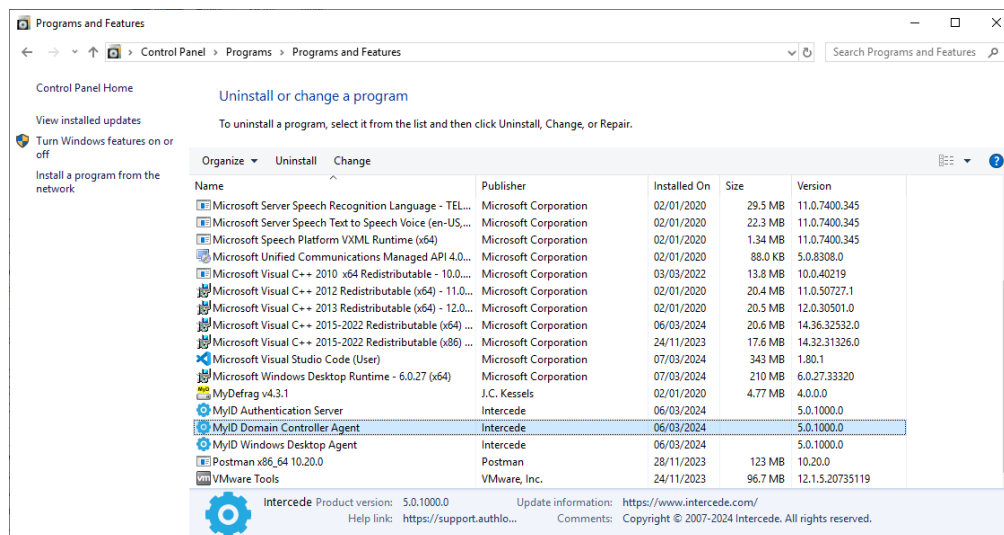
Depending on the Windows security settings you may need to start the setup from an elevated command prompt.



2. Click **Next**.
3. Continue as though you are installing the MyID Domain Controller for the first time. For information on installing the MyID Domain Controller, see section [3.2, Installing the MyID Domain Controller Agent](#).

### 3.4 Uninstalling the MyID Domain Controller Agent

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



### 3.5 Deploying certificates

The MyID Domain Controller Agent does not explicitly require any certificates to be installed on domain controllers to function. If, however, the MyID Authentication Server Certificate (with a private key) is installed on the domain controllers, the MyID Domain Controller Agent can access MyID encrypted data stored on the domain controller directly. This will improve performance as less connections are required from the DC agent to the MyID Authentication Server.



## 3.6 Configuring the MyID Domain Controller Agent Policy settings

You can use the policy settings of the MyID Domain Controller Agent to configure infrastructure components of the agent. The policy is configured separately to the actual password policy which is detailed in the Installation and Configuration Guide.

To deploy the MyID Domain Controller Agent Policy:

1. Create a MyID Domain Controller Agent Policy in Group Policy.
2. Deploy the MyID Domain Controller Agent.
3. Make the following Group Policy change:
  - Assign the MyID Domain Controller Agent Policy to the Domain Controllers OU.

The MyID Domain Controller agent includes the following AD Group Policy Template files:

- AuthlogicsDCAgent.admx
- AuthlogicsDCAgent.adml

These are used to create policies. The **User Configuration** section of the group policy object can be disabled as the settings only apply to the **Computer Configuration**.

### 3.6.1 General settings

Setting	Disable Domain Controller Agent
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting disables the MyID Domain Controller Agent functionality without needing to uninstall the product, which would require a reboot of the Domain Controllers.</p> <p>If you enable this policy no Domain Controller Agent tasks will be performed.</p> <p>If you disable or do not configure this policy then the agent will function as normal.</p>

Setting	Authlogics Authentication Server Names
Values	Any DNS based server address (CSV)
Default	
Description	<p>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.</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 MyID Authentication Servers.</p>

Setting	Authlogics Authentication Server Port (HTTPS/SSL)
Values	(1024 – 65535)
Default	14443
Description	<p>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.</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>

Setting	Authlogics Authentication Server refresh time
Values	(5-1440)
Default	60
Description	<p>This policy setting sets the maximum amount of time before refreshing the most suitable MyID Authentication Server.</p> <p>If you enable this policy you must specify the interval value in minutes to wait before refreshing which MyID 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 MyID Authentication Server to use.</p>

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

Setting	Domain Controller Server Names
Values	Any DNS based server address (CSV)
Default	
Description	<p>This policy setting configures the server name(s) which Domain Controller Agents will use to connect to Domain Controllers instead of auto detecting them.</p> <p>If you enable this policy you must specify at least one Domain Controller DNS name, however, multiple server names can be specified separated by a comma, e.g. dc1.domain.com,dc2.domain.com</p> <p>If you disable or do not configure this policy the PC will auto detect which Domain Controller to use however the local machine will always be used for the local domain.</p>

Setting	Global Catalog Server Names
Values	Any DNS based server address (CSV)
Default	
Description	<p>This policy setting configures the server name(s) which Domain Controller Agents will use to connect to Global Catalog Servers instead of auto detecting them.</p> <p>If you enable this policy you must specify at least one Global Catalog DNS name, however, multiple server names can be specified separated by a comma, e.g. gc1.domain.com,gc2.domain.com</p> <p>If you disable or do not configure this policy the PC will auto detect which Global Catalog to use.</p>

Setting	Active Directory Domain Controller refresh time
Values	(1 – 1440)
Default	60
Description	<p>This policy setting sets the maximum amount of time to wait before retesting the Domain Controller connectivity for the quickest connection. Setting this value too high will make connections stay on a single server for longer, whereas setting this value too low could result in too many checks being performed.</p> <p>If you enable this policy you must specify the interval value in minutes to wait before retesting the Domain Controller connectivity.</p> <p>If you disable or do not configure this policy the Domain Controller Agent will retest the Domain Controller connectivity every 60 minutes..</p>

Setting	Active Directory access timeout
Values	(0 – 120)
Default	15
Description	<p>This policy setting sets the maximum amount of time to wait while connecting to an Active Directory Domain Controller. Setting this value too high can make HA failovers take longer while the AD is being located, whereas setting this value too low could result in connections failing even when the AD is available.</p> <p>If you enable this policy you must specify the interval value in seconds to wait while locating an Active Directory Domain. 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 Domain Controller Agent will wait for 15 seconds while locating an Active Directory Domain.</p>

Setting	Disable Fail-Safe
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting controls the behaviour of the agent in the case of a catastrophic failure. E.g. The agent is unable to connect to the MyID Cloud Password Breach Database, or the licence becomes invalid. Fail-safe relates to the security of the AD passwords, not the ability to change AD passwords, this is to ensure passwords are kept secure.</p> <p>If you enable this policy then any agent failure will result in password changes being ALLOWED.</p> <p>If you disable or do not configure this policy then any agent failure will result in password changes being DENIED.</p>

Setting	Direct Internet Failover
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting allows the MyID Domain Controller Agent to connect directly to the Internet to access the MyID Cloud Password Breach Database if the MyID Authentication Server is unavailable.</p> <p>If you enable this policy the Domain Controller Agent will attempt to connect to the Internet directly if the MyID Authentication Server is unavailable in addition a local blacklist.txt file.</p> <p>If you disable or do not configure this policy then the agent will not attempt to connect directly to the Internet if the MyID Authentication Server is unavailable.</p>

Setting	Proxy Server Host
Values	A DNS based server address
Default	
Description	<p>This policy setting configures the Proxy Server Host name which will be used to connect to the Internet for access to the MyID Cloud Password Breach Database on the URL <a href="https://passwordsecurityapi.authlogics.com/api/*">https://passwordsecurityapi.authlogics.com/api/*</a> if Direct Internet Failover is enabled.</p> <p>If you enable this policy you must specify a FQDN or IP Address, e.g. proxy.mycompany.com</p> <p>If you disable or do not configure this policy a proxy server will not be used and a routable Internet connection will be required.</p>

Setting	Proxy Server Port
Values	Any TCP port value
Default	8080
Description	<p>This policy setting configures the Proxy Server TCP Port number which will be used to connect to the Internet if Direct Internet Failover is enabled. This setting MUST be used in conjunction with the "Proxy Server Host" policy setting.</p> <p>If you enable this policy you must specify a TCP port number, e.g.8080</p> <p>If you disable or do not configure this policy the default port 8080 will be used.</p>

Setting	Proxy Server Use Default Credentials
Values	Enabled / Disabled
Default	Enabled
Description	<p>This policy setting, when enabled, will connect to the proxy server using the Desktop Agent Service credentials.</p> <p>If you enable or do not configure this policy then the Desktop Agent Service credentials are used.</p> <p>If you disable this policy then no credentials are used to connect to the proxy server.</p>

Setting	Proxy Server Use System Proxy
Values	Enabled / Disabled
Default	Enabled
Description	<p>This policy setting will use the system proxy server if one is configured. If you enable or do not configure this policy then the system proxy will be used.</p> <p>If you disable this policy then the system proxy will not be used.</p> <p>Note: If Proxy Server Host is configured then it will be used in precedence to the system configuration if this policy is enabled.</p>

Setting	Enable Debug Logging
Values	Enabled / Disabled
Default	Disabled
Description	<p>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.</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>

## 3.7 Automated / command line setups

### 3.7.1 Running an installation with verbose logging

In scenarios where the installation may not succeed successfully on a system, it may be necessary to run setup with logging enabled to help identify the problem.

The following command runs the setup and creates a `setup.log` file containing information about the install:

```
msiexec /i "MyID Domain Controller Agent xxxxx.msi" /lv setup.log
```

### 3.7.2 Fully automated silent installation

You can run the setup of the MyID Domain Controller Agent silently by running the MSI file with the `/q` switch, or using the `msiexec` command with the `/quiet` option:

- `"MyID Domain Controller Agent xxxxx.msi" /q`
- `msiexec /i "MyID Domain Controller Agent xxxxx.msi" /quiet`

### 3.7.3 Fully automated silent removal

You can remove the MyID Domain Controller Agent silently by using the `msiexec` command with the following switches: `/x` and `/quiet`.

- `msiexec /x "MyID Domain Controller Agent xxxxx.msi" /quiet`

## 4 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 Domain Controller Agent. You should, typically, change them only if instructed by Intercede support.

You can carry out the following:

- Log diagnostic messages.

See section [4.1, \*Diagnostics logging\*](#).

### 4.1 Diagnostics logging

You can control the diagnostics logging using the Windows registry.

#### 4.1.1 Enabling logging

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

`HKLM\SOFTWARE\Authlogics\Domain Controller Agent\LoggingEnabled`

The default value is 0.

Accepted values:

- 0 – disabled.
- 1 – enabled.

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

#### 4.1.2 Setting the logging location

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

`HKLM\SOFTWARE\Authlogics\Domain Controller Agent\LoggingFolder`

The default value is:

`C:\Program Files\Authlogics Domain Controller Agent\Log\`

Accepted values:

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

### 4.1.3 Setting the retention time for rolling logs

Old logs are deleted after a specified interval has passed; for example, after three days (which is the default), or two months. You specify this retention time using the interval type (`LoggingRollingIntervalType`) – for example, days or months, and the number of intervals (`LoggingFileCountLimit`) – for example, three (days) or two (months).

To set the interval type, set the following registry value:

```
HKLM\SOFTWARE\Authlogics\Domain Controller Agent\LoggingRollingIntervalType
```

The default value is 3 (days).

Accepted values:

- 0 – Infinite time between rolling logs – this means that old logs are never deleted.
- 1 – Years.
- 2 – Months.
- 3 – Days.
- 4 – Hours.
- 5 – Minutes.

This setting also determines when new logs are created; for example, new logs are created every day, or every year. Multiple logs may be created within each interval depending on the size limit you have set for the logs; see section [4.1.4, Size limit of rolling log files](#).

To set the number of intervals of logs stored, for example, three (days) or two (months), set the following registry value:

```
HKLM\SOFTWARE\Authlogics\Domain Controller Agent\LoggingFileCountLimit
```

The default value is 3 – after three intervals, the logs from the first interval are deleted.

Accepted values:

- A number of intervals.



#### 4.1.4 Size limit of rolling log files

New log files are created every interval (for example, every day, or every month). To prevent these files from becoming too large, you can set the maximum size of each log file. When this size is reached, a new log file is created within the same interval; for example, if you are using day interval logs:

```
AuthlogicsActiveDirectoryConnection-20250325-0001.log
```

```
AuthlogicsActiveDirectoryConnection-20250325-0002.log
```

or for year interval logs:

```
AuthlogicsActiveDirectoryConnection-2025-0001.log
```

```
AuthlogicsActiveDirectoryConnection-2025-0002.log
```

To set the maximum size of each log file, set the following registry value:

```
HKLM\SOFTWARE\Authlogics\Domain Controller Agent\LoggingRollingSizeLimit
```

The default value is 20 megabytes.

Accepted values:

- A number in megabytes.

**Note:** This setting does not reduce the total size of the logs; by limiting the size of the individual files, it increases the number of files.

#### 4.1.5 Example of rolling logs

With the default values of:

- `LoggingRollingIntervalType` – 3 (Day intervals)
- `LoggingFileCountLimit` – 3 (three days)
- `LoggingRollingSizeLimit` – 20 (MB)

Old log files are deleted after three days.

An example of rolling log files produced starting on March 25th 2025 is:

```
AuthlogicsActiveDirectoryConnection-20250325-0001.log
```

```
AuthlogicsActiveDirectoryConnection-20250325-0002.log
```

```
AuthlogicsActiveDirectoryConnection-20250326-0001.log
```

```
AuthlogicsActiveDirectoryConnection-20250326-0002.log
```

```
AuthlogicsActiveDirectoryConnection-20250326-0003.log
```

```
AuthlogicsActiveDirectoryConnection-20250327-0001.log
```

```
AuthlogicsActiveDirectoryConnection-20250327-0002.log
```

Each day has several files, each with a maximum size of 20 megabytes. When the logger starts writing to the first file of March 28th, the cleanup process is triggered, deleting the files from March 25th, as those are then more than three days old.