MyID Domain Controller Agent Integration Guide

With MyID PSM and MFA functionality

Product Version: 5.0.6942.0

Call us on:	+44 (0)1455 558 111 (UK & EMEA) +1 408 706 2866 (US)
Email us:	info@intercede.com

Intercede Ltd, Lutterworth Hall, St. Mary's Road, Lutterworth, Leicestershire, LE17 4PS, United Kingdom
UK Tel: +44 (0)1455 558 111   US Tel: +1 888 646 6943   email: info@intercede.com   web: www.intercede.com

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

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

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

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

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

Table of Contents

Introduction

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.

The MyID Domain Controller Agent is a lightweight service component of both MyID Password Security Management (PSM) and Multi-Factor Authentication (MFA) solutions which provides the following features:

Password Security Management:

- 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 has:
  - been breached online
  - already been used in the AD
- Randomise passwords of user accounts that no longer require a password.

Multi-Factor Authentication:

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

In summary, the Domain Controller Agent ensures that all new passwords comply with the latest NIST SP 800-63B guidance and it keeps the Microsoft password database and the MyID Password Vault in sync at all times regardless of which mechanism is used to change/reset an AD password.

Note

The Domain Controller Agent MUST be installed on all writable Domain Controllers in the Active Directory domain.

Passwordless logon for Active Directory

The MyID Authentication Server includes a highly secure Password Vault which stores a copy of users Active Directory passwords which are later used to automatically log the user in to various applications which require Windows authentication if they have used an alternative logon method.

The Password Vault is disabled by default and must be explicitly enabled. When active it 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.

The MyID Windows Desktop Agent

The MyID Windows Desktop Agent allows users to logon to Windows desktops and servers without having to enter their Windows password. This form of passwordless logon is achieved by using the password stored in the Password Vault which is retrieved and delivered to the Windows desktop on the user's behalf when logging on. Logging onto Windows in this way ensures compatibility with existing Windows applications that rely on Active Directory credentials.

Like the Password Vault, Passwordless logon is disabled by default and can be enabled on the Windows systems by setting the "Enable Passwordless functionality to remove the Active Directory password for logon" group policy option on the Windows Desktop Agent.

Other Agents

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

The MyID ADFS Agent, when installed on Windows Server 2019 or higher, provides passwordless access to federated applications however it does not require the Password Vault to provide this functionality.

Considerations

Password Policies

The MyID PSM Password Policy complies with NIST SP 800-63B guidance, whereas the Windows Default Domain Policy does not have this ability. The Windows password policy must be modified 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.

System Requirements

The MyID Domain Controller Agent is designed to work with an MyID Authentication Server which must be deployed before installing the agent.

The installer will check for pre-requisites and install them automatically where possible. The required pre-requisites are:

- Microsoft Visual C++ 2010 SP1 Runtime Libraries
- Microsoft .NET Framework 6

Note

The Visual C++ 2010 Runtime and .NET Framework 6 Libraries for 64bit systems are included in the agent installer. If the installation of a pre-requisite fails, then the agent installation will also fail.

Direct Internet Failover

The 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, the Domain Controller Agent can be configured to connect to the cloud in a failover scenario if the MyID Authentication Server is unavailable. This option is disabled by default.

In order for the Domain Controller Agent to communicate with the MyID Cloud Password Breach Database if the MyID Authentication Server is unavailable **(failover scenario only)**, all Domain Controllers will require Internet access to the following destination (depending on the capabilities of the network firewall):

- Destination URL: `https://passwordsecurityapi.authlogics.com/api/*`
- Host: `passwordsecurityapi.authlogics.com` on port `443`

A web proxy server can be configured using Group Policy to allow indirect Internet access instead of a routed connection. Proxy authentication will automatically be performed using the Windows Machine account credentials. If the proxy does not support Windows Authentication then anonymous access must be granted to the Domain Controllers. Static proxy server credentials are not supported.

Language Requirements

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

Design and Deployment Scenarios

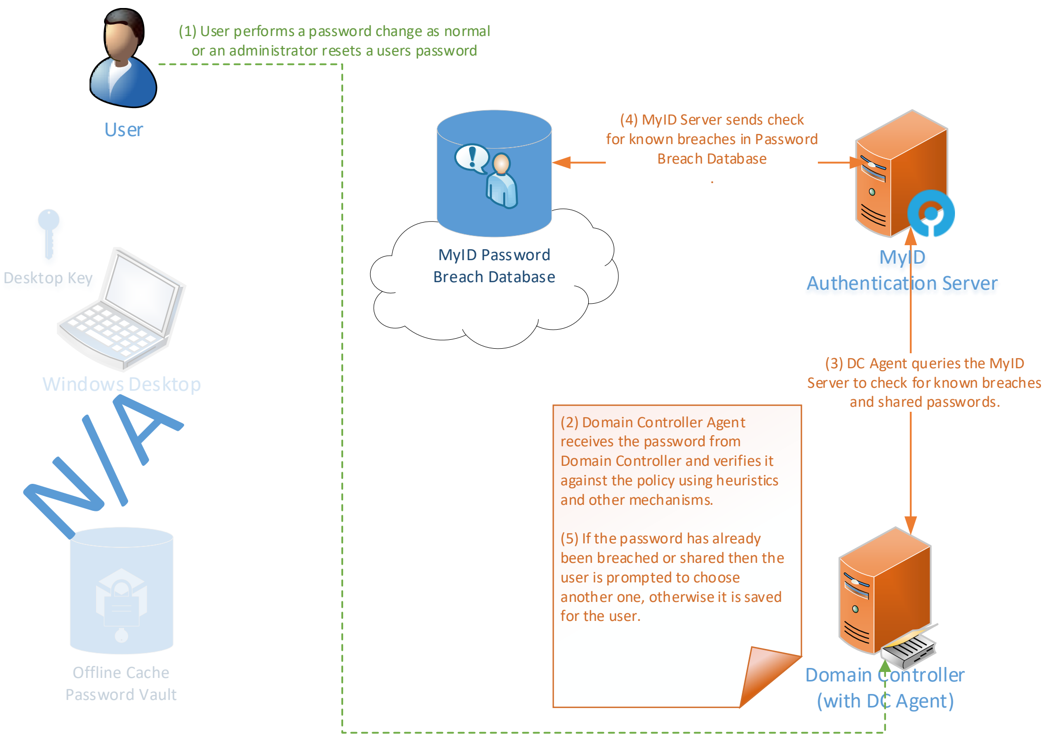
The MyID Domain Controller Agent has been designed to work seamlessly in a Windows and Active Directory environment.

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

Active Directory password change workflow – Policy Check

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

MyID PSM Active Directory AD password change policy check



(1) User performs a password change as normal or an administrator resets a users password

(4) MyID Server sends check for known breaches in Password Breach Database

(3) DC Agent queries the MyID Server to check for known breaches and shared passwords.

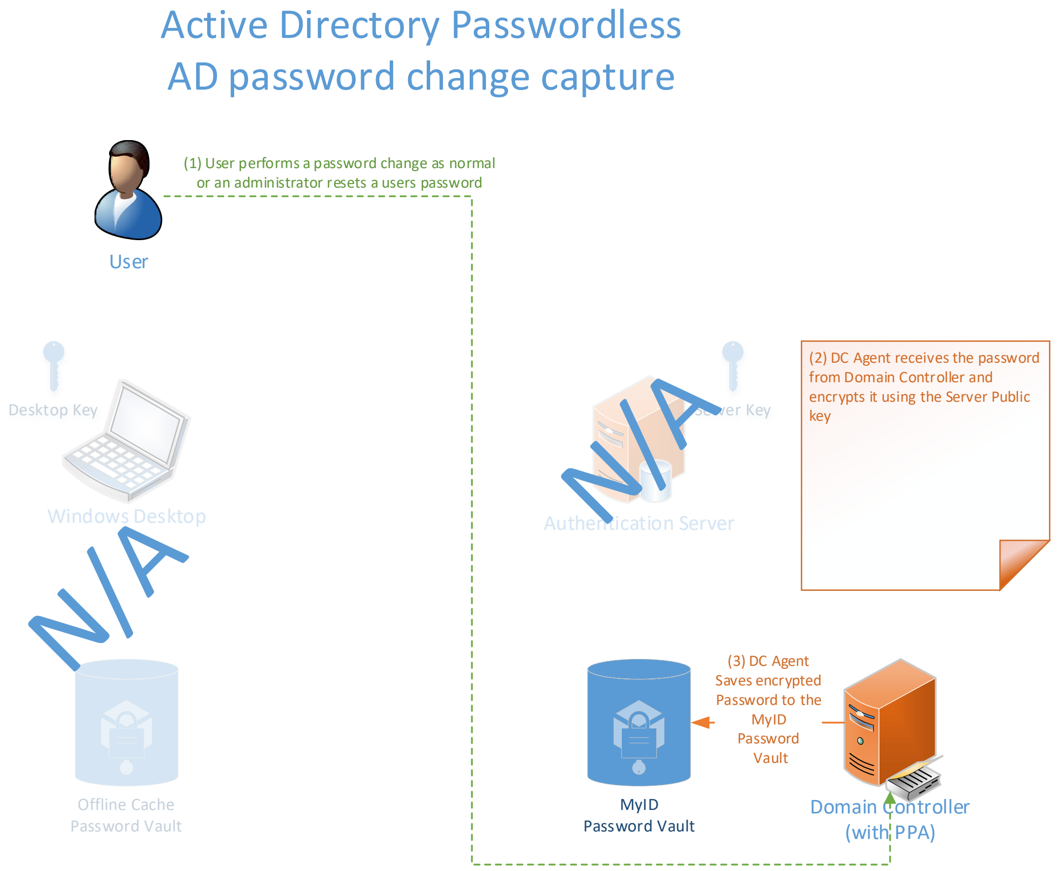
(2) Domain Controller Agent receives the password from Domain Controller and verifies it against the policy using heuristics and other mechanisms.

(5) If the password has already been breached or shared then the user is prompted to choose another one, otherwise it is saved for the user.

User
MyID Password Breach Database
MyID Authentication Server
Desktop Key
Windows Desktop
N/A
Offline Cache Password Vault
Domain Controller (with DC Agent)

Active Directory password change workflow – Password Vault Update

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



(1) User performs a password change as normal or an administrator resets a users password

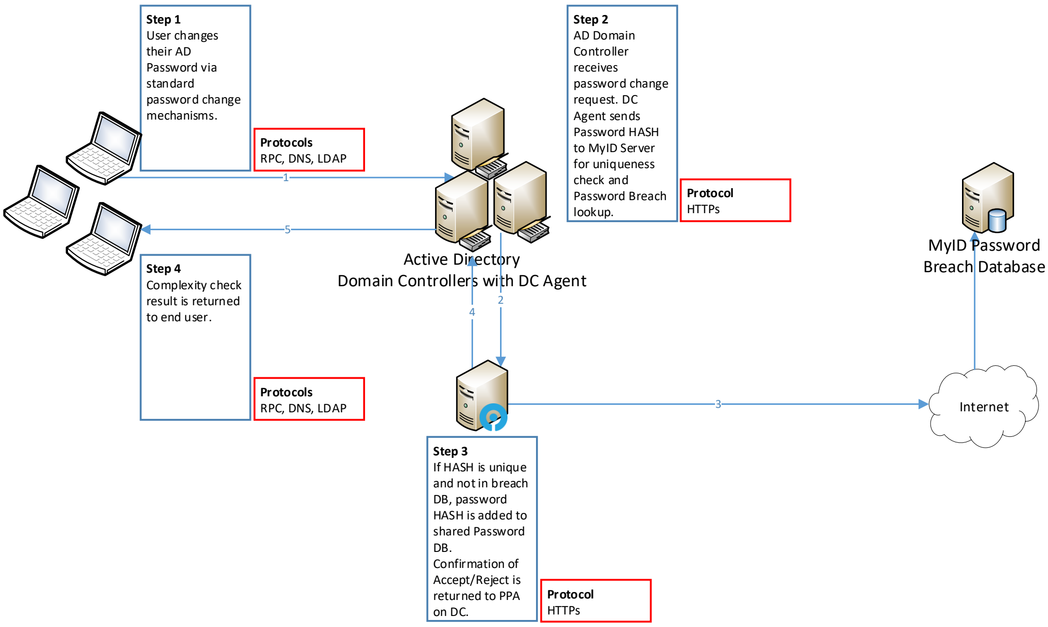
(2) DC Agent receives the password from Domain Controller and encrypts it using the Server Public key

(3) DC Agent Saves encrypted Password to the MyID Password Vault

Active Directory Shared password protection workflow

The following workflows depict the steps performed by the Domain Controller Agent during an AD 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



Step 1
User changes their AD Password via standard password change mechanisms.

Protocols
RPC, DNS, LDAP

Step 2
AD Domain Controller receives password change request. DC Agent sends Password HASH to MyID Server for uniqueness check and Password Breach lookup.

Protocol
HTTPs

Step 3
If HASH is unique and not in breach DB, password HASH is added to shared Password DB.
Confirmation of Accept/Reject is returned to PPA on DC.

Protocol
HTTPs

Step 4
Complexity check result is returned to end user.

Protocols
RPC, DNS, LDAP

Note

To prevent shared passwords from being selected, the Password Security Management Wizard needs to be run on the MyID Authentication Server with the current domain being enabled for PSM. Please refer to the MyID Authentication Server documentation for further information.

Deployment

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

Overview

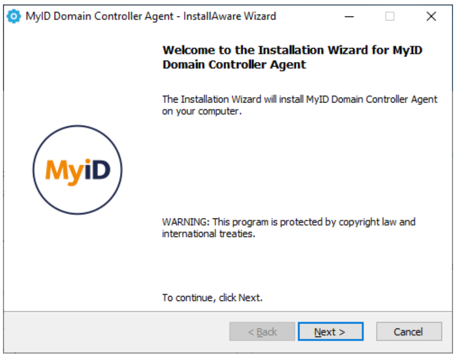
This deployment section assumes that at least one MyID Authentication Server has already been installed and is functional. See the MyID Authentication Server Installation and Configuration Guide for further information on setting up the MyID Authentication Server.

Installing the MyID Domain Controller Agent

> **Note**
>
> This section of the installation process requires Administrator rights on the Domain Controller.

(1) To start the MyID Domain Controller Agent installation, 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* to continue.



MyID Domain Controller Agent - InstallAware Wizard

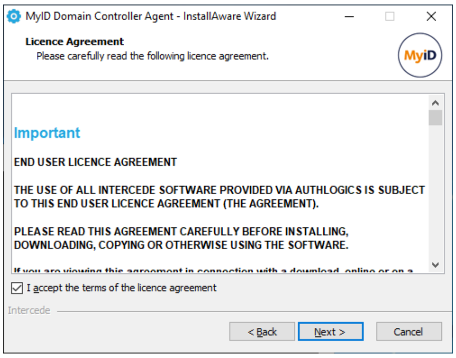
Welcome to the Installation Wizard for MyID Domain Controller Agent

The Installation Wizard will install MyID Domain Controller Agent on your computer.

WARNING: This program is protected by copyright law and international treaties.

To continue, click Next.

(3) After **reading** the licence agreement click *I accept the terms in the terms in the Licence Agreement* if you agree to the terms, then click *Next* to continue.



MyID Domain Controller Agent - InstallAware Wizard

Licence Agreement

Please carefully read the following licence agreement.

Important

END USER LICENCE AGREEMENT

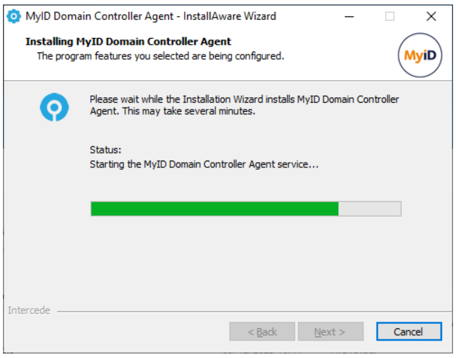
THE USE OF ALL INTERCEDE SOFTWARE PROVIDED VIA AUTHLOGICS IS SUBJECT TO THIS END USER LICENCE AGREEMENT (THE AGREEMENT).

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE INSTALLING, DOWNLOADING, COPYING OR OTHERWISE USING THE SOFTWARE.

If you are viewing this agreement in connection with a download, online or on a

☑ I accept the terms of the licence agreement

The installation is being performed.



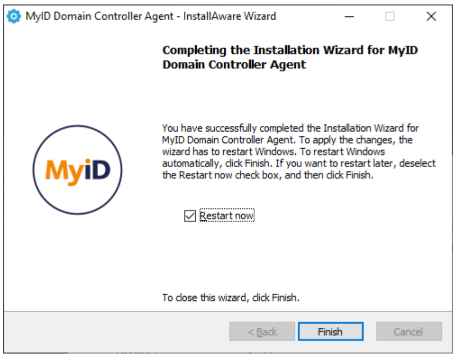
Installing MyID Domain Controller Agent

The program features you selected are being configured.

Please wait while the Installation Wizard installs MyID Domain Controller Agent. This may take several minutes.

Status:
Starting the MyID Domain Controller Agent service...

(4) If you plan to reboot later untick the *Restart now* box.
Click *Finish* to complete the installation process.



Completing the Installation Wizard for MyID Domain Controller Agent

You have successfully completed the Installation Wizard for MyID Domain Controller Agent. To apply the changes, the wizard has to restart Windows. To restart Windows automatically, click Finish. If you want to restart later, deselect the Restart now check box, and then click Finish.

☑ Restart now

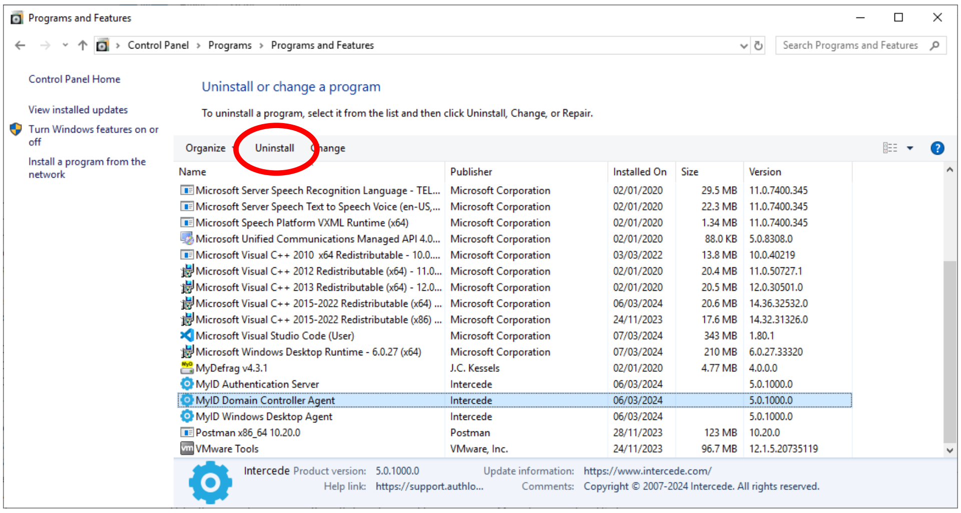
To close this wizard, click Finish.

Note

The Domain Controller MUST be restarted for changes to take effect.

Uninstalling MyID Domain Controller Agent

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


Programs and Features
Control Panel > Programs > Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize
Uninstall
Change

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
Microsoft Server Speech Recognition Language - TEL...	Microsoft Corporation	02/01/2020	29.5 MB	11.0.7400.345
Microsoft Server Speech Text to Speech Voice (en-US,...	Microsoft Corporation	02/01/2020	22.3 MB	11.0.7400.345
Microsoft Speech Platform VXML Runtime (x64)	Microsoft Corporation	02/01/2020	1.34 MB	11.0.7400.345
Microsoft Unified Communications Managed API 4.0...	Microsoft Corporation	02/01/2020	88.0 KB	5.0.8308.0
Microsoft Visual C++ 2010 x64 Redistributable - 10.0....	Microsoft Corporation	03/03/2022	13.8 MB	10.0.40219
Microsoft Visual C++ 2012 Redistributable (x64) - 11.0...	Microsoft Corporation	02/01/2020	20.4 MB	11.0.50727.1
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0...	Microsoft Corporation	02/01/2020	20.5 MB	12.0.30501.0
Microsoft Visual C++ 2015-2022 Redistributable (x64) ...	Microsoft Corporation	06/03/2024	20.6 MB	14.36.32532.0
Microsoft Visual C++ 2015-2022 Redistributable (x86) ...	Microsoft Corporation	24/11/2023	17.6 MB	14.32.31326.0
Microsoft Visual Studio Code (User)	Microsoft Corporation	07/03/2024	343 MB	1.80.1
Microsoft Windows Desktop Runtime - 6.0.27 (x64)	Microsoft Corporation	07/03/2024	210 MB	6.0.27.33320
MyDefrag v4.3.1	J.C. Kessels	02/01/2020	4.77 MB	4.0.0.0
MyID Authentication Server	Intercede	06/03/2024		5.0.1000.0
MyID Domain Controller Agent	Intercede	06/03/2024		5.0.1000.0
MyID Windows Desktop Agent	Intercede	06/03/2024		5.0.1000.0
Postman x86_64 10.20.0	Postman	28/11/2023	123 MB	10.20.0
VMware Tools	VMware, Inc.	24/11/2023	96.7 MB	12.1.5.20735119

Intercede Product version: 5.0.1000.0 Update information: https://www.intercede.com/
Help link: https://support.authlo... Comments: Copyright © 2007-2024 Intercede. All rights reserved.

Automated / command line Setups

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 will run setup and create a setup.log file containing information about the install:

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

Fully automated silent installation

Setup can be run silently directly by simply running the MSI file with a /q switch, or via the MSI Executive interface as follows:

```
"MyID Domain Controller Agent xxxxx.msi" /q
```

or

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

Fully automated silent removal

The agent can be removed silently using the /x switch as follows:

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

Deploying Certificates

The Domain Controller Agent does not explicitly require any certificates to be installed on Domain Controllers to function. However, if the MyID Authentication Server Certificate (with private key) is installed on the Domain Controllers then the DC agent will be able to access MyID encrypted data stored on the DC directly. This will improve performance as less connections are required from the DC Agent to the MyID Authentication Server.

Configuring the Domain Controller Agent Policy Settings

The Domain Controller Agent Policy is designed to configure infrastructure components of the agent. This policy is configured separately to the actual password policy which is detailed in the Installation and Configuration Guide.

Deploying the MyID Domain Controller Agent Policy involves the following step:

(1) Create an MyID Domain Controller Agent Policy in Group Policy
(2) Deploy the Domain Controller Agent
(3) Group Policy changes:
    a. Assign the MyID Domain Controller Agent Policy to the Domain Controllers OU

The MyID Domain Controller agent includes an AD Group Policy Template files `AuthlogicsDCAgent.admx` and `AuthlogicsDCAgent.adml` which are used to create policies. The *User Configuration* section of the GPO can be disabled as the settings only apply to the *Computer Configuration*.

General Settings

Setting	Disable Domain Controller Agent
Values	Enabled / Disabled
Default	Disabled
Description	
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. If you enable this policy no Domain Controller Agent tasks will be performed. If you disable or do not configure this policy then the agent will function as normal.	

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

Setting	Authlogics Authentication Server Port (HTTPS/SSL)
Values	(1024 – 65535)
Default	14443
Description	
This policy setting configures the MyID Authentication Server port number which agents will use to connect to the MyID Authentication Server. The server name will be located automatically via an Active Directory search unless specified in the "Authlogics Authentication Server Names" policy. If you enable this policy you must specify a TCP port number, e.g.14443 If you disable or do not configure this policy the default port 14443 will be used.	

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

Setting	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	Domain Controller Server Names
Values	Any DNS based server address (CSV)
Default	{blank}
Description	
This policy setting configures the server name(s) which Domain Controller Agents will use to connect to Domain Controllers instead of auto detecting them. 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 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.	

Setting	Global Catalog Server Names
Values	Any DNS based server address (CSV)
Default	{blank}
Description	
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. 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 If you disable or do not configure this policy the PC will auto detect which Global Catalog to use.	

Setting	Active Directory Domain Controller refresh time
Values	(1 – 1440)
Default	60
Description	
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. If you enable this policy you must specify the interval value in minutes to wait before retesting the Domain Controller connectivity. If you disable or do not configure this policy the Domain Controller Agent will retest the Domain Controller connectivity every 60 minutes.	

Setting	Active Directory access timeout
Values	(0 – 120)
Default	15
Description	
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. 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. If you disable or do not configure this policy the Domain Controller Agent will wait for 15 seconds while locating an Active Directory Domain.	

Setting	Disable Fail-Safe
Values	Enabled / Disabled
Default	Disabled
Description	
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. If you enable this policy then any agent failure will result in password changes being ALLOWED. If you disable or do not configure this policy then any agent failure will result in password changes being DENIED.	

Setting	Direct Internet Failover
Values	Enabled / Disabled
Default	Disabled
Description	

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.

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.

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.

Setting	Proxy Server Host
Values	A DNS based server address
Default	{blank}
Description	

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 https://passwordsecurityapi.authlogics.com/api/* if Direct Internet Failover is enabled.

If you enable this policy you must specify a FQDN or IP Address, e.g. proxy.mycompany.com

If you disable or do not configure this policy a proxy server will not be used and a routable Internet connection will be required.

Setting	Proxy Server Port
Values	Any TCP port value
Default	8080
Description	

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.

If you enable this policy you must specify a TCP port number, e.g.8080

If you disable or do not configure this policy the default port 8080 will be used.

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.