MyID MFA and PSM

Version 5.0.7

Domain Controller 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

Copyright

Conventions

- 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 and to indicate references to other sections within the current document:

  For example:
  - "Copy the file *before* starting the installation"
  - "See *Issuing a Card* for further information"

- ***Bold and Italic*** 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 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

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 functionality to remove the Active Directory password for logon** 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.
- 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, 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 be 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 is available only in English.

1.5 Change history

Version	Description
IMP2054-01	Reformatted and released with MyID MFA and PSM version 5.0.7.

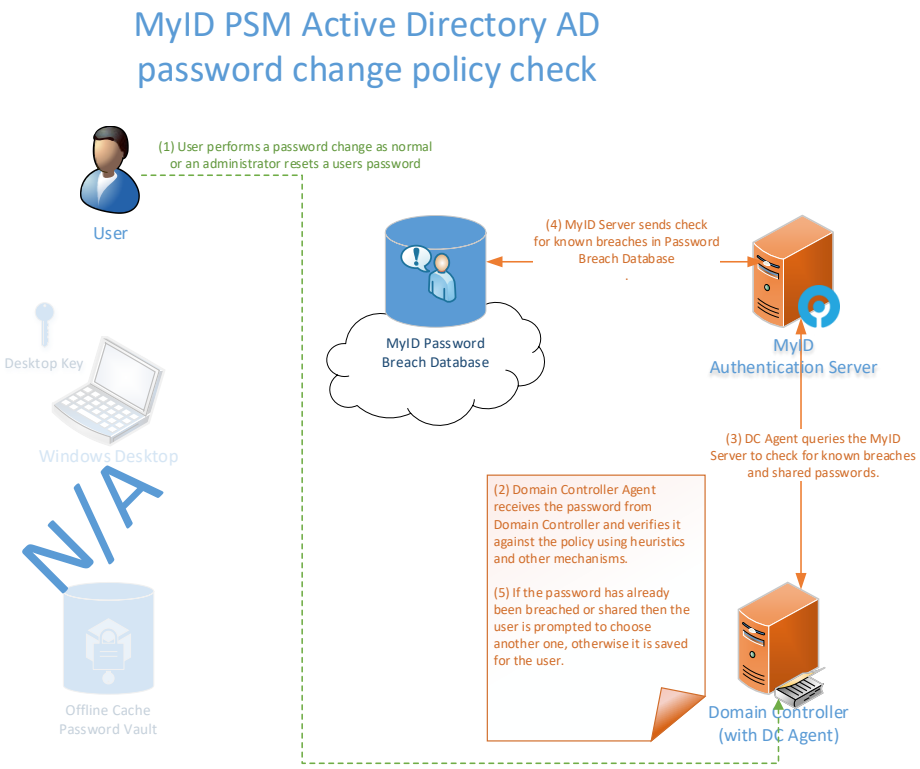
2 Design and deployment scenarios

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.

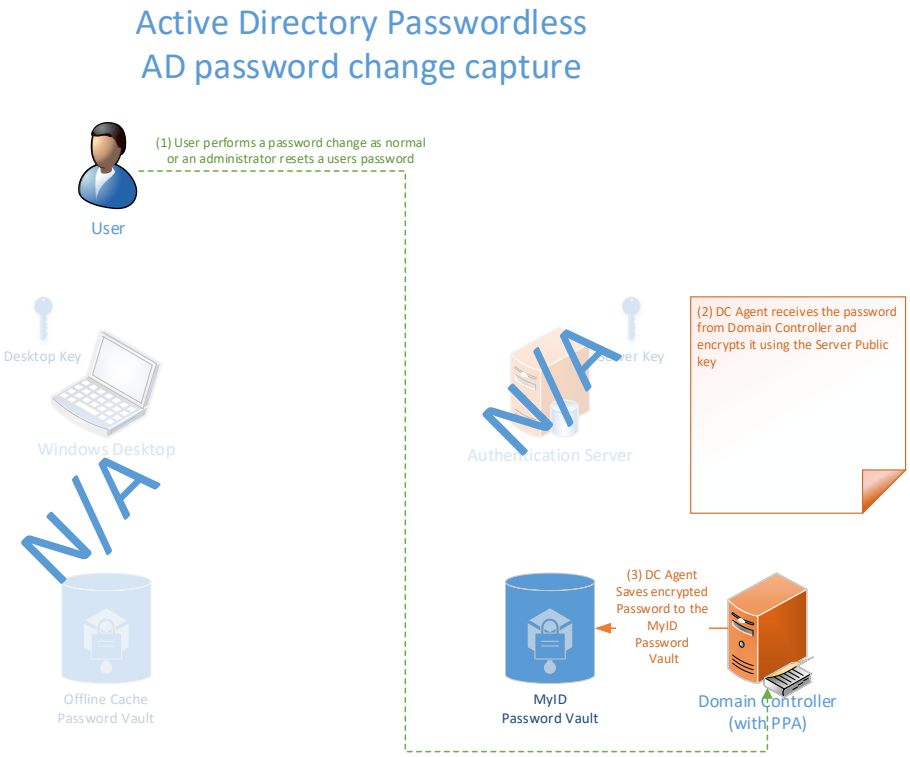
2.1 Active Directory password change workflow – Policy Check

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



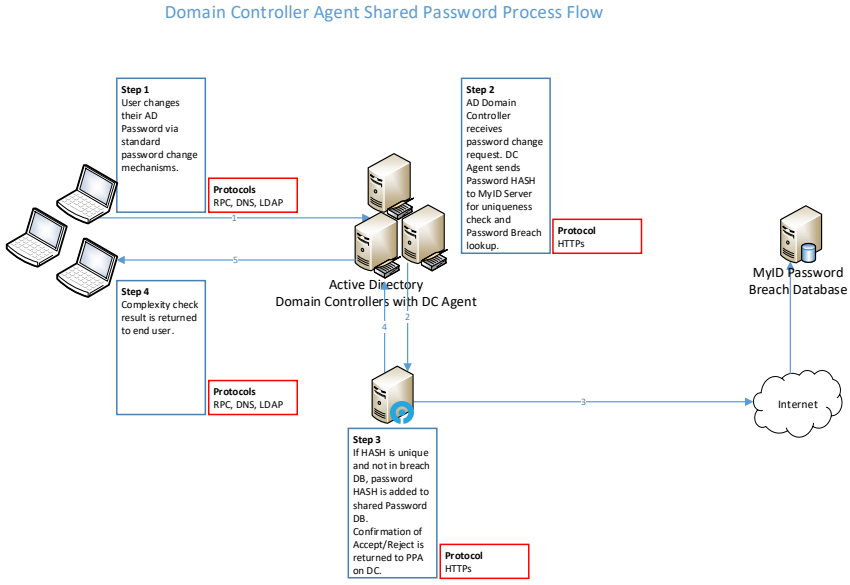
2.2 Active Directory password change workflow – Password Vault Update

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



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:



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*** guide for further information.

3 Deployment

This is the installation process for deploying the MyID Domain Controller Agent.

3.1 Pre-requisites

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***.

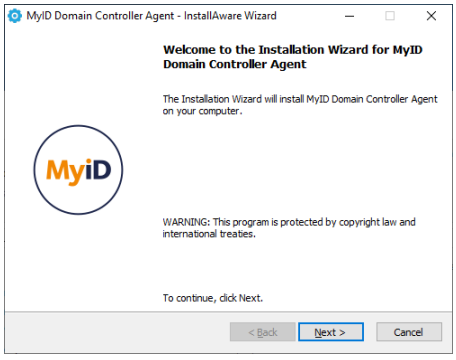
3.2 Installing the MyID Domain Controller Agent

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

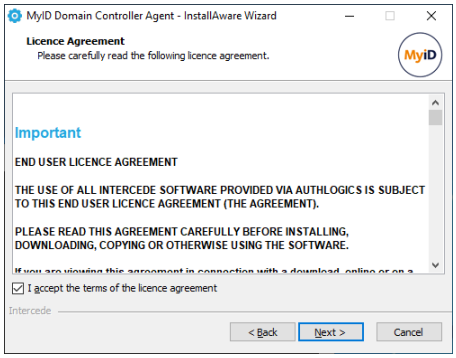
1. Run the `MyID Domain Controller Agent xxxxx.msi` installer with elevated privileges.

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

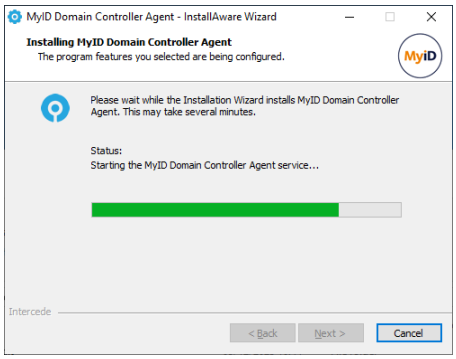
2. Click **Next**.



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

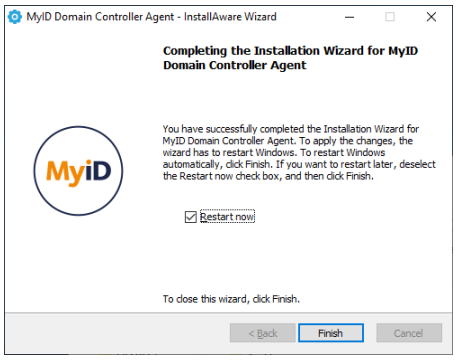


4. Click **Next**.



The installation is being performed.

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

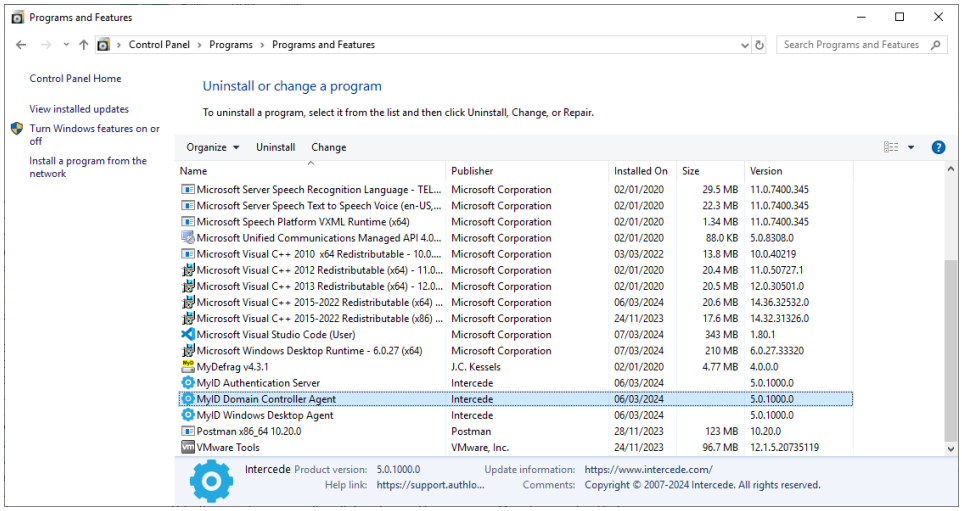


Note: The Domain Controller *must* be restarted for changes to take effect.

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

3.3 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**.



4 Automated / command line setups

4.1 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
```

4.2 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 through the MSI Executive interface:

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

4.3 Fully automated silent removal

You can remove the MyID Domain Controller Agent silently by using the MSI Executive interface with the following switches: `/x` and `/q`.

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

4.4 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.

4.5 Configuring the 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**.

4.5.1 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	
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	
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	
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

Setting	Direct Internet Failover
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	
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.