MyID MFA and PSM

Version 5.3.2

Windows Desktop 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: IMP2063-5.3.2

November 2025

Copyright

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

Integrating MyID Password Security Management (PSM) and Multi Factor Authentication (MFA) with Windows is an ideal way to deploy a modern password policy and add strong authentication to Windows desktops.

The Windows Desktop Agent supports online and offline logon functionality for Windows 10 and 11, and Windows Server 2016, 2019, 2022, and 2025 – you can use it virtually anywhere.

The Windows Desktop Agent supports Azure Entra joined user accounts, so you can use multi-factor authentication for user accounts that are authenticated and managed by Microsoft Entra ID.

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 Password Security Management

The Windows Desktop agent provides the following password security management features:

- Password Change: The Windows Desktop Agent provides intuitive user feedback when users change their passwords to help the users create a password that complies with the current password policy.
- Self Service Reset: On the login screen, users can click **Forgot Password**. This sends them a One Time Code by email or SMS to allow them to reset their password.

1.2 Multi Factor Authentication

The Windows Desktop Agent provides Multi Factor Authentication (MFA) and deviceless OTP logon capabilities to Windows as well as Self Service device management. This allows users to add and remove MFA devices.

The authentication technologies available for signing in depend on the **Authentication Provider UI** and **Allow Any Authentication Type** GPO settings.

The **Authentication Provider UI** setting decides which authentication technology types may be used; the UI selected maps to technologies as follows:

- **Grid** – Grid Patterns
- **Mobile Push** – Push
- **Off** – OTC or YubiKey OTP

  OTC and YubiKey OTP use the same generic OTC field.
- **Phrase** – Phrase
- **Web Sign-in** – the authentication technologies decided by the **Windows Desktop Web Sign-in** application in the MMC.

  See the *Windows Desktop Agent Properties* section of the ***MyID Authentication Server Installation and Configuration Guide***.

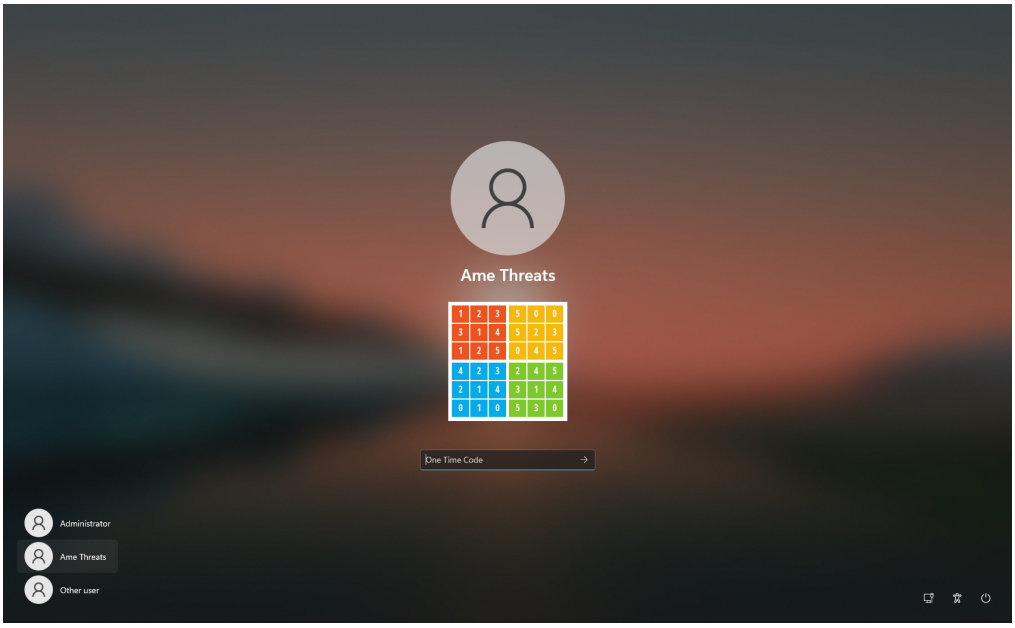
To allow users instead to use *any* authentication technology for which they are configured, you must enable the **Allow Any Authentication Type** setting. If you do not configure this setting, it is treated as disabled; this setting is not configured by default, as authentication technology restriction is more secure.

Note: The **Authentication Provider UI** and **Allow Any Authentication Type** GPO settings do not affect a user's ability to manage their own MFA technologies.

For more information on the settings, see section *3.9.1*, *General settings*.

1.2.1 Deviceless and Passwordless login screen example

This example shows the MyID Windows Desktop Agent installed on a Windows 11 PC. Deviceless OTP and Passwordless logins have been configured.



1.3 Passwordless MFA for Active Directory

1.3.1 Overview

The MyID Windows Desktop Agent allows users to log on to Windows with MFA without having to enter their Windows password.

This form of passwordless logon is achieved by storing the user's Active Directory passwords in a secure password vault. The password is retrieved and delivered to the Windows desktop on the user's behalf when logging on. Logging on to 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, set the **Enable Passwordless logons** group policy option on the Windows Desktop Agent.

1.3.2 The offline password vault

You can carry out an offline login to each PC with the MyID Windows Desktop Agent installed (if allowed through group policy). To cater for offline logons, a subset of the Active Directory user account information is stored in an encrypted cache on the PC; this includes Active Directory passwords to cater for offline passwordless logons.

The Offline Cache and the MyID Authentication Server Password Vault use RSA 2048-bit asymmetric keys in a certificate to protect the data.

Each Offline Cache uses a unique certificate installed in the Windows Certificate Store that is created during the agent installation; this ensures that no two Offline Cache databases use the same encryption keys.

The MyID Authentication Server Password Vault is disabled by default, and you must enable it before use. When disabled, the Offline Cache does not store Active Directory passwords; however the remaining metadata is still protected in the same way.

1.3.3 The Offline Cache update process

For a Windows Desktop to receive a password for storage in the Offline Cache:

- The Windows machine must have a local certificate installed.

  This can be restricted to a specified trusted root.
- The user must successfully authenticate to the server with MFA.

When a user is authenticated with the Authentication Server for passwordless logon, the public key in the certificate installed on the Windows Desktop is also sent to the Authentication Server.

If the authentication request is successful, the Authentication Server retrieves the password from the MyID Password Vault and decrypts it using its private key, then immediately re-encrypts the password using the supplied public key and returns it to the Windows Desktop Agent. The Windows Desktop Agent then verifies that it can decrypt the returned password using its private key and stores the password in its Offline Password Vault for later offline passwordless logon use.

This process ensures that:

- The password is never transmitted in cleartext.

  Even when SSL is not used, the password is still protected.
- The password is always stored in the Vault using the correct key pairs.
- The password can only be decrypted on the machine that the user used to authenticate from.

Note: The offline cache periodically updates all user accounts stored in it, except for Active Directory passwords. Active Directory passwords are updated only after a successful user online logon. This is similar to how Windows caches Active Directory passwords for offline logon purposes.

1.3.4 The Domain Controller Agent

The Domain Controller Agent is a lightweight service that ensures that compliant passwords are set in Active Directory. It also captures password changes made on the Windows Domain and stores them securely in the MyID Authentication Server Password Vault. This keeps the Active Directory password database and the MyID Authentication Server Password Vault synchronized at all times, regardless of what mechanism is used to change or reset an Active Directory password.

Note: You *must* install the Domain Controller Agent on all domain controllers in the Active Directory domain when using passwordless logon.

1.4 Considerations

1.4.1 Requirements

A MyID Authentication Server 5.x or higher must be deployed and functional for all Windows Desktop Agent functionality to be available.

The V5.x agent is backwards compatible with a MyID Authentication Server version 4.2.1052.0 or above (formerly known as Authlogics Authentication Server) but can deliver the functionality applicable only to the deployed server version. In addition, you should carefully examine the various Active Directory Group Policy options to assist in planning for the deployment of the Windows Desktop Agent for both MFA and PSM.

Desktop Agents are generally designed to be backwards compatible with previous Authentication Server versions but may work with more recent servers.

1.4.2 Deviceless logon limitations with Grid on Server 2016

Deviceless logon with Grid is supported on Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, and Windows Server 2025, but not Windows Server 2016. This is because of Microsoft limitations in the Windows Credential provider v2 that limit the ability to display the required grid graphic. This limitation does not apply to Phrase deviceless logons. All other product features are supported on Server 2016.

1.4.3 Upgrades

You can upgrade from an earlier version to version 4.2 and existing cache data is migrated. Upgrades to the current version are supported only from Authentication Server version 4.2 servers.

When you upgrade from Authentication Server version 4.2 and Windows Desktop Agent versions 4.1 and below, you must upgrade the Windows Desktop Agent to version 4.2 *first* and then upgrade the Authlogics Authentication Server to version 4.2.1052.0 or higher. The Authlogics Windows Desktop Agent version 5.0 is backwards compatible with version 4.2 Authentication Servers.

For example, if you start from Authentication Server 4.2 and Windows Desktop Agent 4.2, to upgrade to the latest version you must:

1. Deploy a new Group Policy template for version 5.0.
2. Upgrade all Windows machines to Windows Desktop Agent 5.0.

   For more information, see section *3.3*, *Updating the MyID Windows Desktop Agent*.
3. Upgrade all Authentication Servers to version 4.2.1052.0 or higher (for details, see the*Updates and upgrades* section of the ***MyID Authentication Server Installation and Configuration Guide***).

MyID Windows Desktop Agents are backwards compatible with older Authentication Server versions, not the other way around. Because of this, you must upgrade the Windows Desktop Agent *before* the Authentication Server.

1.5 Language requirements

The MyID Windows Desktop Agent is available in the following languages:

- English
- German

Additional languages may be provided in the future.

Product support and documentation are available only in English.

1.6 Processor requirements

The MyID Windows Desktop Agent supports the following processors:

- Intel
- ARM

  Specifically, Windows for ARM64.

1.7 FIDO considerations

Currently, the MyID Windows Desktop Agent supports the following FIDO token providers:

- YubiKey
- Swissbit – Swissbit iShield Key 2 Pro Mifare USB-C only.
- OneSpan – Onespan Digipass FX7 only.

The MyID Windows Desktop Agent allows you to register YubiKey BIO series keys.

Note: FIDO BIO keys registered through the FIDO specific Security Key Credential Provider do not register a user's biometric values. To register a FIDO BIO key with biometrics, add the security key using the MFA Credential Provider.

Synced passkeys through the Web sign-in option are supported only on Windows 10 workstations. Synced passkeys are not supported on Windows 11 workstations.

2 Design and deployment scenarios

The MyID Windows Desktop Agent is designed to work seamlessly in a Windows Workgroup and Active Directory environment.

The MyID Windows Desktop Agent is contained in an MSI installation package that you can automate and deploy using Active Directory Group Policy or an alternative software deployment tool. The agent's settings are controlled through Active Directory Group Policy for flexible, centralized management.

To deploy the Desktop Agent, configure a GPO to target a machine and install the agent software. The agent automatically and dynamically locates MyID Authentication Servers in the Active Directory forest to process logons.

When installed on a workgroup-based machine, you must configure the agent using the local machine policy.

2.1 Offline logons

The MyID Windows Desktop Agent supports offline logons and Passwordless logons. These work similarly to the password-based Windows offline logon functionality; when a user logs onto a PC, the user details are cached on the PC for future logons in cases where the authentication server is not available. The agent can perform an MFA logon using a soft token even while offline.

Offline logon functionality is enabled by default, and you can control or disable it through AD Group Policy. The offline cache is also used to accelerate the generation of Deviceless OTP challenges.

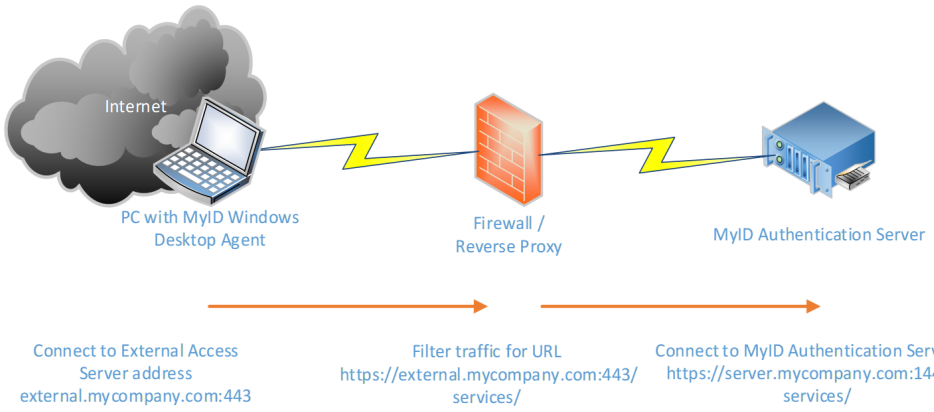
The MyID Windows Desktop Agent can use an **External Access Server** configuration when it needs to communicate with the MyID Authentication Server but is not on the internal network. This allows mobile PCs that are connected to the Internet but are not on the LAN to authenticate without working offline. This allows the server to trigger the sending of Mobile Push and SMS/text messages, and allows you to use central auditing and logging.

2.1.1 External Access Server configuration

This is used in the event that the agent must use an HTTPS connection to an External Access Server address. This facilitates central logging and provides the ability to send SMS/text message tokens to users while their PC is on the move.

You configure the address of the External Access Server on the PC through Active Directory Group Policy. You are recommended to use a reverse proxy server or SSL capable firewall to allow external access to the External Access URL of the MyID Authentication Server.

You can configure the External Access Server to use a different SSL certificate to the Self-Service Portal if required.



Note: MyID Authentication servers from 4.1.3200.0 to 4.2 used a dedicated External Access Server role on port 14444. From version 5.0 this is no longer necessary or supported. By default, port 14443 is used instead. You can specify the **External Access Server Address**, including port, using the GPO of that name. For more information, see section *3.9.4*, *Server configuration settings*.

2.1.2 Only require OTP when working remotely

You can configure the MyID Windows Desktop Agent to disable itself automatically when the PC is on the LAN; the user would only be required to enter an OTP when logging on remotely. This caters for remote access policies that require 2FA for remote connections, but not for local connections.

To enable this functionality, configure the **Disable Windows Desktop Agent when on the LAN** group policy setting.

2.1.3 Known issues and limitations

- **IKB-440 - Offline logon caches only the last successful FIDO authentication method**

  When the **Manage the Windows password** option is enabled on the **FIDO2** tab of the global settings, you can use only the last successful FIDO authentication method. If a user logs in with biometric FIDO before going offline, only biometric works offline, and similarly for non-biometric logon. Even if the user has previously logged in with both devices, only the most recent one is cached when working offline. This affects physical FIDO authentication devices only.

- **IKB-441 – Unable to carry out an offline logon after using a temporary access code**

  When the **Manage the Windows password** option is enabled on the **FIDO2** tab of the global settings, if you use a temporary access code before going offline, all cached credentials are cleared, preventing you from carrying out an offline logon with either biometric or non-biometric FIDO devices, even if you have successfully logged in with FIDO devices before.

2.2 Workgroup based installations

The MyID Windows Desktop Agent supports installations on Workgroup (non-domain joined) systems. When the MyID Windows Desktop Agent is installed on Workgroup systems, Active Directory is not available for deploying the policy to the machine or for detecting the MyID Authentication Server.

When installed on a Workgroup system, a local MyID Policy Editor is installed. This allows for the configuration of the policy where at least the name of the MyID Authentication Server *must* be specified.

To enable MFA for a local SAM based user account:

1. Create a Realm on the MyID Authentication Server that matches the local computer name.
2. Within the Realm, create a user account that matches the name of the SAM-based user.

   For example, to secure a local user account `bobm` hosted on a workstation called `Window11Desktop`, create a realm `Windows11Desktop` and an MFA user `bobm`. The user then logs in with the account `Windows11Desktop\bobm` or `bobm@Windows11Desktop`.

2.3 Remote Desktop / Terminal services

You can also secure terminal servers using the MyID Windows Desktop Agent. This allows for strong authentication to be enforced on RDP connections independent of any remote access or gateway security.

Note: The Windows Desktop Agent is not required to be installed on the RDP client, only on the RDP server.

3 Deployment

The following deployment overview walks through the installation process for deploying the MyID Windows Desktop Agent.

To follow this deployment section, you must have at least one MyID Authentication Server installed and functional. For further information on the installation and configuration of the MyID Authentication Server, see the ***MyID Authentication Server Installation and Configuration Guide***.

In addition, your MyID user accounts should already be configured for users.

1. Configure a Group Policy object to target the systems you are installing the MyID Windows Desktop Agent onto with the required agent settings.
2. Install the MyID Windows Desktop Agent on a Windows system.
3. Test user logins.

The agent installation can be performed manually, through an automated script or through Group Policy Software Distribution; however this is beyond the scope of this document.

This chapter covers the following deployment related subjects:

- The prerequisites to installation.

  See section *3.1*, *Prerequisites*.
- Installing the MyID Windows Desktop Agent.

  See section *3.2*, *Installing the MyID Windows Desktop Agent*.
- Updating the MyID Windows Desktop Agent.

  See section *3.3*, *Updating the MyID Windows Desktop Agent*.
- Uninstalling the MyID Windows Desktop Agent.

  See section *3.4*, *Uninstalling the MyID Windows Desktop Agent*.
- Using the MyID Desktop Health Service.

  See section *3.5*, *The MyID Desktop Health Service*.
- Working with and locating the Group Policy Templates.

  See section *3.6*, *Working with and locating Group Policy Templates*.
- Adding Group Policy ADMX Templates to the local computer.

  See section *3.7*, *Adding Group Policy ADMX Templates to the local computer*.
- Using a Group Policy "Central Store".

  See section *3.8*, *Using a Group Policy "Central Store"*.
- Configuring the MyID Windows Desktop Agent.

  See section *3.9*, *Configuring the MyID Windows Desktop Agent*.

  Note: For advanced configuration, see section *8*, *Advanced configuration*.
- Using Automated / command line setups.

  See section *3.10*, *Automated / command line setups*.

3.1 Prerequisites

The installer checks for prerequisites and installs them automatically where possible. The required prerequisites are:

- .NET 8

If the installation of a prerequisite fails, the installation also fails.

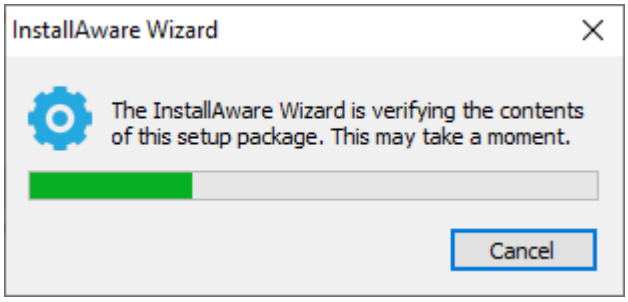
3.2 Installing the MyID Windows Desktop Agent

The MyID Windows Desktop Agent enables a Windows PC or server to use MyID MFA and PSM services.

You can install the MyID Windows Desktop Agent using the installation wizard, or by running a PowerShell headless installation script.

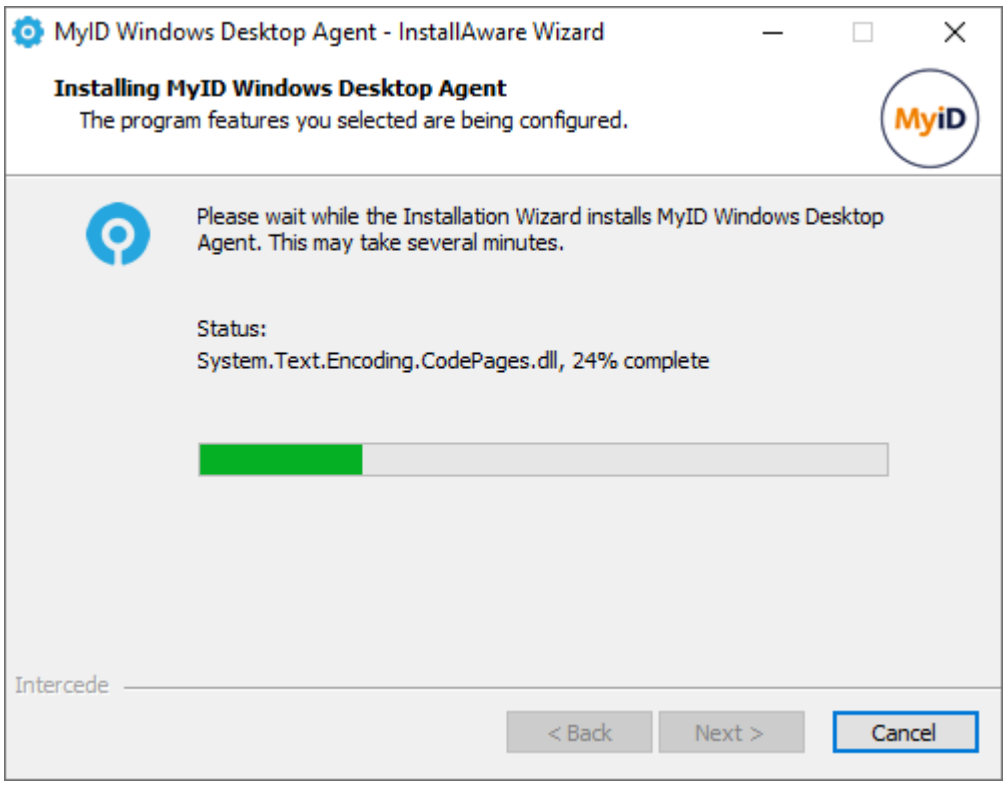
3.2.1 Installing the MyID Windows Desktop Agent using the installation wizard

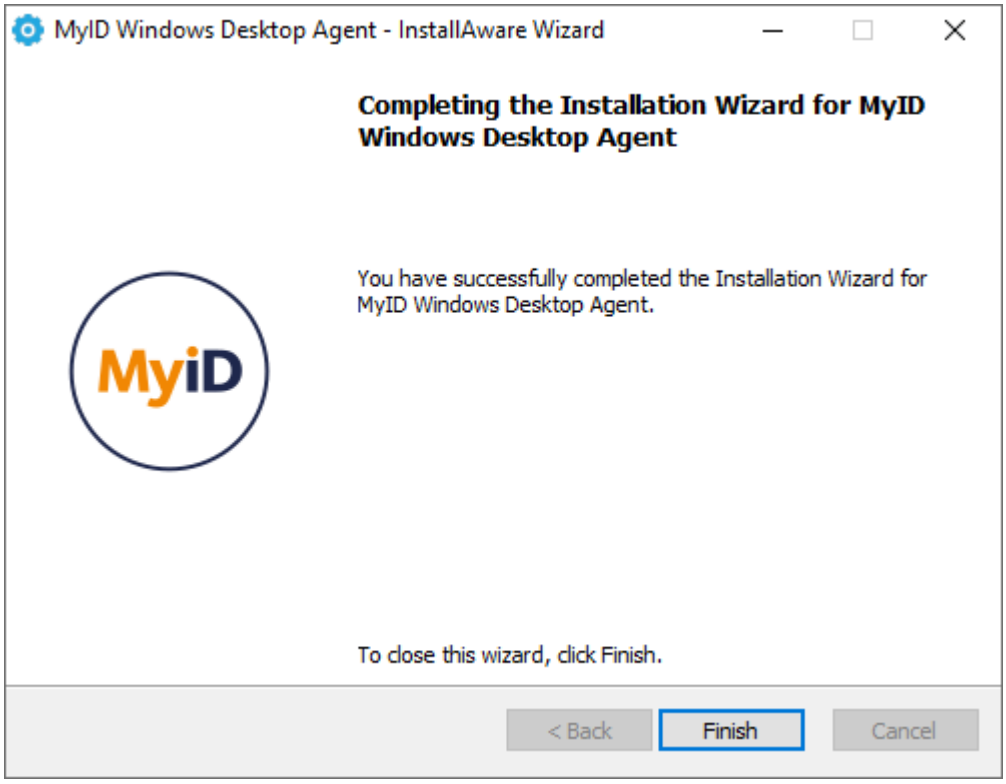
1. To start the MyID Windows Desktop Agent installation, run the `MyID Windows Desktop Agent xxxx.msi` installer with elevated privileges.



2. Click **Next**.

   The installation is being performed.





3. Click **Finish**.

   All necessary MyID Windows Desktop Agent files have been installed.

3.2.2 Installing the MyID Windows Desktop Agent using the PowerShell script

A PowerShell script is provided to allow you to carry out a headless installation of the MyID Windows Desktop Agent. This script downloads a specific version of the installer and then runs the installation without user interaction.

Note: By default, the MyID Windows Desktop Agent PowerShell script also installs the Health Service; see section *3.5*, *The MyID Desktop Health Service*. If you do not want to install the Health Service, you must edit the PowerShell script before you run it; see section *3.2.3*, *Installing the MyID Windows Desktop Agent without the Health Service using the PowerShell script*.

To install the MyID Windows Desktop Agent with the Health Service using the PowerShell headless installation script:

1. Navigate to the `Reskit` folder of your MyID Windows Desktop Agent download.
2. Open the `Install-WindowsDesktopAgent.ps1` script with a text editor.
3. Set the `$exeUrl` variable to the URL that contains the version of the MyID Windows Desktop Agent that you want to install.

   To set up the URL for the latest version of the MyID Windows Desktop Agent:

   a. Download the zip of the latest version of the MyID Windows Desktop Agent from the intercede website.

   b. Extract the download.

   c. Copy the installer `.exe` file to a web server that is available from the PC on which you want to run the script.

      The installer `.exe` file is in the following location in the download zip file:

      `\Install\MyID Windows Desktop Agent xxxx.exe`

   d. Set the `$exeUrl` in the script to the location of your hosted installer.

      For example:

      `https://myserver.example.com/Intercede/MyID%20Windows%20Desktop%20Agent%20xxxx.exe`

4. Save the script.
5. Open a Windows PowerShell command prompt as an administrator, and run the script:

   `.\Install-WindowsDesktopAgent.ps1`

3.2.3 Installing the MyID Windows Desktop Agent without the Health Service using the PowerShell script

To install the MyID Windows Desktop Agent without the Health Service using the PowerShell headless installation script, before you run the PowerShell script, edit the script to comment out the silent install including the Windows Desktop Health Service, and uncomment the standard silent install as follows:

```
# Standard silent install
Start-Process -FilePath $exePath -ArgumentList "/s" -Wait -NoNewWindow -PassThru

# Silent install including Windows Desktop Health Service
# Start-Process -FilePath $exePath -ArgumentList "HEALTHSERVICE /s" -Wait -NoNewWindow -
PassThru
```

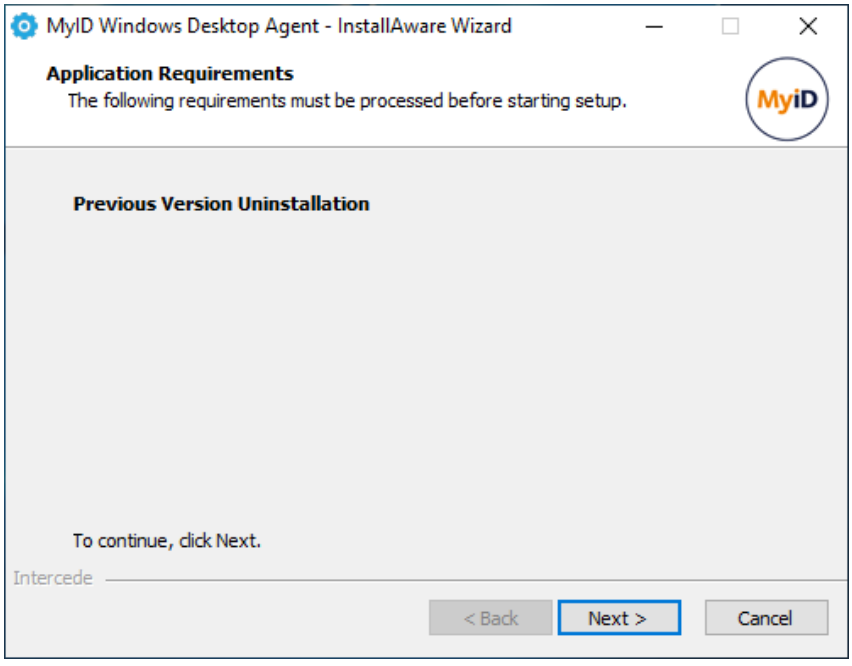
Once you have saved the file with these changes, you can install the MyID Windows Desktop Agent without the Health Service following the instructions in section *3.2.2*, *Installing the MyID Windows Desktop Agent using the PowerShell script*.

3.3 Updating the MyID Windows Desktop Agent

To update the MyID Windows Desktop Agent, download the installer for the latest version of the agent from the Intercede website.

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.

1. Run the `MyID Windows Desktop Agent xxxxx.msi` installer with elevated privileges.



2. Click **Next** to uninstall the previous version.

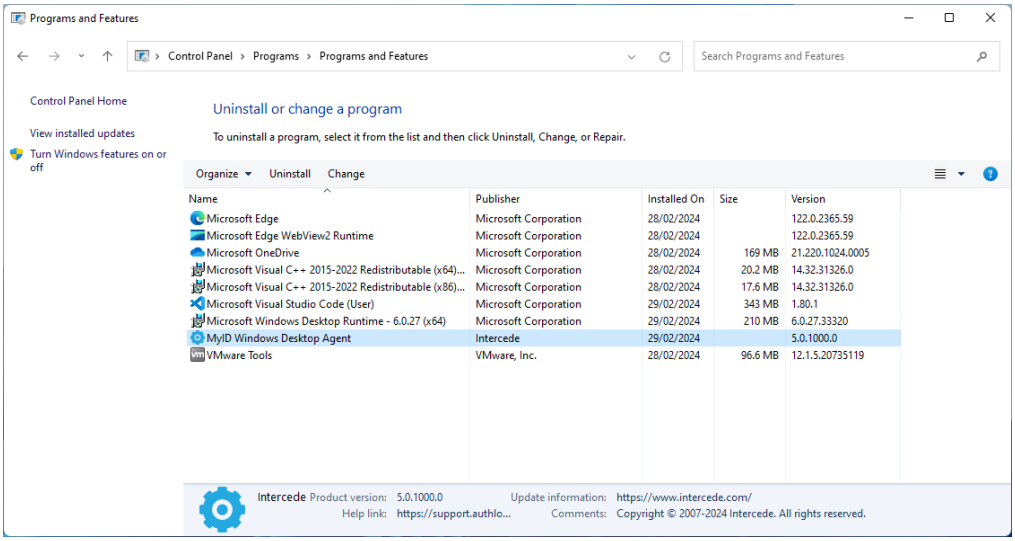
You can now click **Next** and follow the MyID Windows Desktop Agent installation instructions. For more information, see section *3.2*, *Installing the MyID Windows Desktop Agent*.

If you are using the browser reporting extension, see section *5.3*, *Updating the browser reporting extension* for information on updating the extension.

Note: In MyID Windows Desktop Agent version 5.0.8.0, the MyID Windows Desktop Agent installer created a desktop shortcut that you could use to update the software. This shortcut is no longer available, as of MyID Windows Desktop Agent version 5.0.8.1 and MyID Windows Desktop Agent version 5.1.0.

3.4 Uninstalling the MyID Windows Desktop Agent

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



Note: The offline cache database files and the certificates generated during the installation are not removed after performing an uninstall.

3.5 The MyID Desktop Health Service

The MyID Desktop Health Service is a Windows service that provides monitoring for credential providers and the MyID Windows Desktop Agent.

The MyID Desktop Health Service ensures that when a user attempts to log on, the credential providers hosted within `LogonUI.exe` and the MyID Windows Desktop Agent are running using the latest versions of the components installed.

The health service monitors the following folder:

```
C:\Program Files\dotnet\shared\Microsoft.WindowsDesktop.App
```

When the health service detects a change, it starts a two minute timer. If any subsequent changes are detected, the timer resets to two minutes. Once the timer has completed its two minute countdown without additional changes being detected, it triggers the `LogonUI.exe` process to be killed if it is running – this is where the credential providers are hosted. The service also restarts the MyID Windows Desktop Agent.

3.5.1 Installing the MyID Desktop Health Service with the MyID Windows Desktop Agent

You can install the MyID Desktop Health Service with the MyID Windows Desktop Agent using the headless PowerShell script. For more information, see section *3.2.2*, *Installing the MyID Windows Desktop Agent using the PowerShell script*.

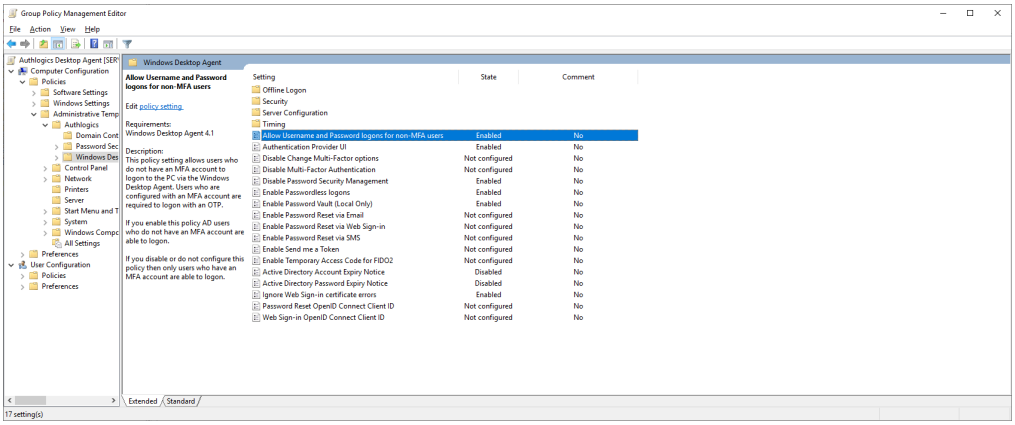
3.5.2 Logging

The service writes the following messages to the event log:

EventID	Type	Text
5100	Information	Change to DotNet folder detected.
5101	Information	Restarting Desktop Agent.
7200	Error	Unable to create Service: {Error Message}

3.6 Working with and locating Group Policy Templates

You can configure application-specific policy settings using the Group Policy Management Editor:

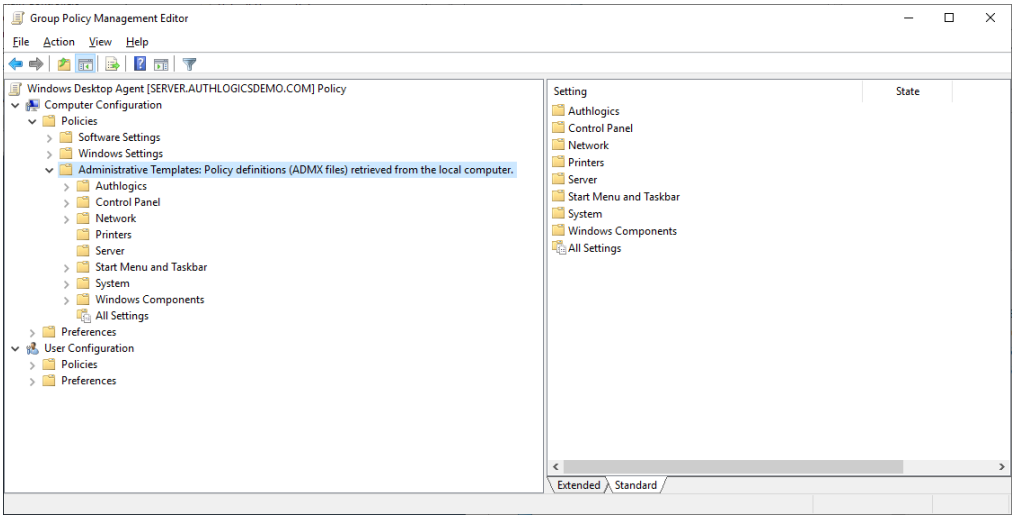


The Group Policy Management Editor loads application specific settings from template files. The template files can either be loaded from the local computer through the `C:\Windows\PolicyDefinitions` folder (added by the Agent installer) or the Active Directory central store.

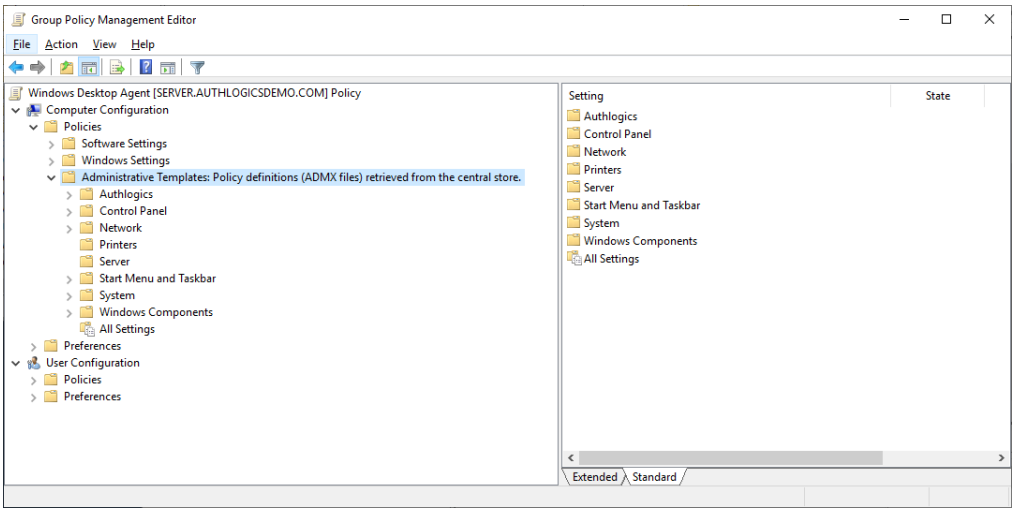
Note: The template files are required by the Group Policy Management Editor only during the editing of Group Policy objects. They are *not* required on PCs where the policy is being applied.

The Group Policy Management Editor states whether templates (ADMX files) are being loaded from the Local Computer or the Central Store. This varies depending on your Active Directory environment setup.

If the ADMX is located on local computer:



If the ADMX is located in central store:



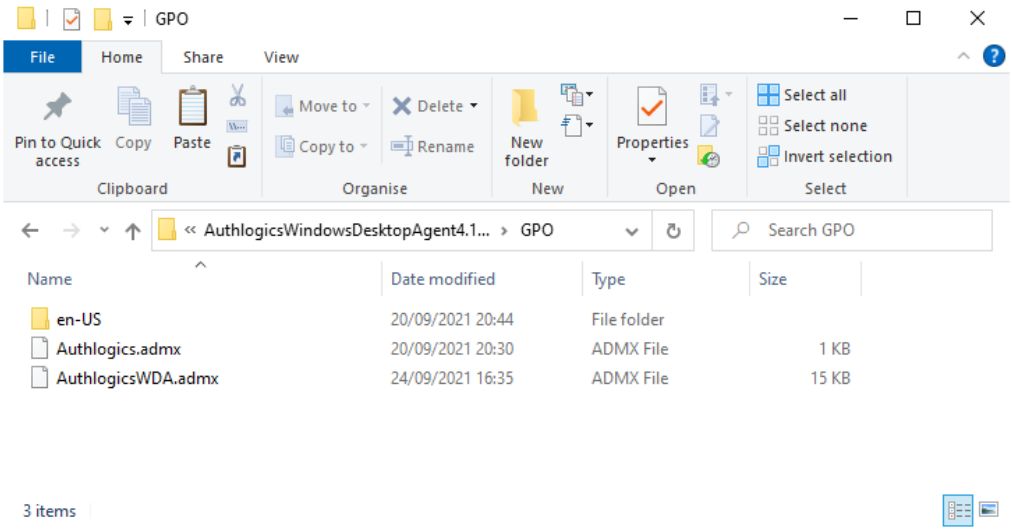
3.7 Adding Group Policy ADMX Templates to the local computer

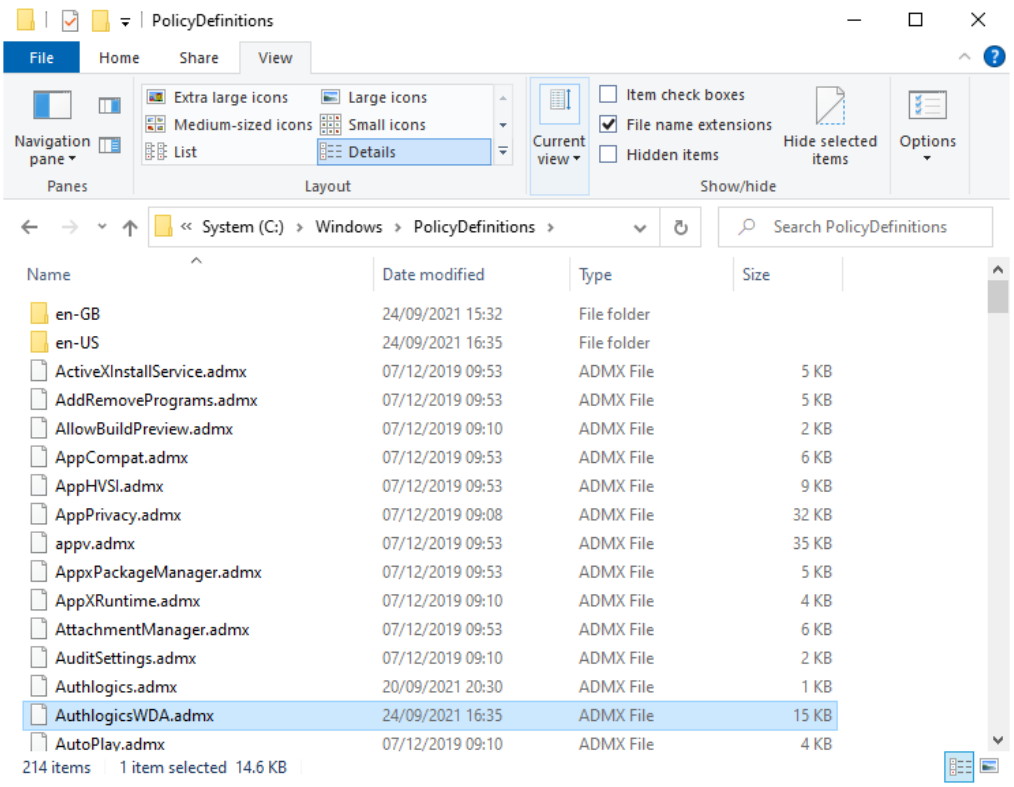
If you are creating or editing the Group Policy on a PC that does *not* have the MyID Windows Desktop Agent installed and there is no Central Store configured in Active Directory, you must copy all the template files, including the `en-US` language folder, from the `\GPO` folder of the installation media to the folder where the Group Policy Management Editor is being run. This is located:

```
C:\Windows\PolicyDefinitions\
```

Source	Destination
`\GPO\*.*`	`C:\Windows\PolicyDefinitions\`

Note: The templates folder includes an `en-US` language folder that must be copied. If the destination computer does not have an `en-US` language folder, you must create it. Do not copy the language files from the `en-US` folder to a different language folder on the destination computer.





3.8 Using a Group Policy "Central Store"

You can centralize the storage of the Group Policy Administrative Template to a **Central Store** in Active Directory. If a **Central Store** is already being used, copy the files from the installation media `\GPO` folder to the following folder on the domain controller:

`\\<dnsdomain>\SYSVOL\<dnsdomain>\policies\PolicyDefinitions`

Where `<dnsdomain>` is the domain of the DNS.

If the `PolicyDefinitions` folder does not exist, you have not configured a Central Store. For further information on creating and managing a Group Policy Central Store, see the following Microsoft documentation:

docs.microsoft.com/en-us/troubleshoot/windows-client/group-policy/create-and-manage-central-store

3.9 Configuring the MyID Windows Desktop Agent

When the Group Policy Templates are correctly installed, the settings are visible in the Group Policy Management Editor. You can disable the User Configuration section of the GPO as the settings only apply to the Computer Configuration.

By default, installing the MyID Windows Desktop Agent does *not* disable the existing Windows Credential Providers and only adds an additional Credential Provider for MyID MFA. You must use Group Policy to disable other providers that you do not require.

The following Active Directory Group Policy settings are available for configuring the agent:

3.9.1 General settings

Setting	Active Directory Account Expiry Notice
Values	(0-365)
Default	10 (Days)
Description	This policy setting sets the number of days before an Active Directory account will expire for a notice is displayed to the user. Setting this value too high can cause excessive prompts, whereas setting this value too low may not give the user enough notice. If you enable this policy you must specify the number of days before an Active Directory account expires for a notice is displayed to the user. Setting this value to 0 will disable the notice. If you disable or do not configure this policy the Windows Desktop Agent will not display a notice to the user.
License	MFA or PSM

Setting	Active Directory Password Expiry Notice
Values	(0-365)
Default	10 (Days)
Description	This policy setting sets the number of days before an Active Directory password will expire for a notice is displayed to the user. Setting this value too high can cause excessive prompts, whereas setting this value too low may not give the user enough notice. If you enable this policy you must specify the number of days before an Active Directory password expires for a notice is displayed to the user. Setting this value to 0 will disable the notice. If you disable or do not configure this policy the Windows Desktop Agent will not display a notice to the user.
License	MFA or PSM

Setting	Allow Any Authentication Type
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting allows the logon agent to use any technology to authenticate a logon. If you enable this policy then all technologies will be checked for a valid otc. If you disable or do not configure this policy then only the technology determined by the Authentication Provider UI policy will be used to validate the otc.
License	MFA

Setting	Allow Username and Password logons for non-MFA users
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting allows users who do not have an MFA account to logon to the PC via the MFA Windows Desktop Agent. Users who are configured with an MFA account are required to logon with an OTP. If you enable this policy AD users who do not have an MFA account are able to logon. If you disable or do not configure this policy then only users who have an MFA account are able to logon.
License	MFA

Setting	Authentication Provider UI
Values	Off / Grid / Phrase / Mobile Push / Web Sign-in
Default	Disabled
Description	This policy setting specifies the authentication UI to be used on the PC, if any. If you enable this policy you must specify the required authentication UI. If you disable or do not configure this policy then no specific authentication UI will be disabled on the PC.
License	MFA

Note: Synced passkey authentication through the Web Sign-in UI is currently not supported on Windows 11 systems.

Setting	Disable Multi-Factor Authentication
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables Multi-Factor Authentication on the PC. If you enable this policy, users will not be prompted to enter Multi-Factor Authentication credentials at logon. If you disable or do not configure this policy then Multi-Factor Authentication will be enabled on the PC.
License	MFA

Setting	Disable Password Security Management
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables Password Security Management on the PC. If you enable this policy, password policy checks will not be performed. If you disable or do not configure this policy then password policy checks will be performed when a user changes their password.
License	PSM

Setting	Disable Change Multi-Factor options
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the 'Change Multi-Factor options' link from being displayed on the Windows password change screen which when clicked allows users to manage their MFA devices and information. If you enable this policy a 'Change Multi-Factor options' link will not appear on the Windows password change screen. If you disable or do not configure this policy then a 'Change Multi-Factor options' link will be displayed on the Windows password change screen.
License	MFA

Setting	Enable Password Reset via Email
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting enables a 'Forgot Password' link to be displayed on the logon screen which when clicked sends a One Time Code to the user via email. If you enable this policy a 'Forgot Password' link will appear on the Windows logon screen if the user has a configured email address. If you disable or do not configure this policy then a 'Forgot Password' link will not be displayed on the Windows logon screen.
License	MFA or PSM

Setting	Enable Password Reset via SMS
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting enables a 'Forgot Password' link to be displayed on the logon screen which when clicked sends a One Time Code to the user via SMS. If you enable this policy a 'Forgot Password' link will appear on the Windows logon screen if the user has a configured phone number. If you disable or do not configure this policy then a 'Forgot Password' link will not be displayed on the Windows logon screen.
License	MFA or PSM

Setting	Enable Passwordless logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting removes the Active Directory password from the Windows logon screen allowing users to logon with only a Username and One Time Passcode. If you enable this policy the Windows Desktop Agent will not ask for an AD password when a user logs on; unless there is no password available in the Password Vault. If you disable or do not configure this policy then users will be required to enter their AD password together with a One Time Passcode at each logon.
License	MFA

Setting	Enable Password Vault (Local Only)
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting enables the local Password Vault independently from the Authentication Server Password Vault. If you enable this policy then the local Password Vault will be used to allow passwordless logons, if enabled, regardless of the status of the Authentication Server Password Vault. The password will not be stored on the Authentication Server unless the Authentication Server Password Vault is enabled, in which case, this setting does not need to be enabled. If you disable or do not configure this policy then local Password Vault will mirror the status of the Authentication Server Password Vault.
License	MFA

Setting	Enable the 'Send me a Token' link
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting enables a 'Send me a Token' link to be displayed on the logon screen which when clicked sends a Real-Time token to the user. If the user is not configured for MFA or is set to use a soft token only then no token will be sent. If you enable this policy a 'Send me a Token' link will appear on the Windows logon screen. If you disable or do not configure this policy then a 'Send me a Token' link will not be displayed on the Windows logon screen.
License	MFA

- **IKB-425 – Grid and OTC notifications different behavior.**

  When the Windows Desktop Agent is in deviceless (Grid) mode, the system automatically sends email/SMS notifications when the user attempts to log on. In non-deviceless (OTC) mode, the user must click the **Send me a Token** link.

Setting	Enable Temporary Access Code for FIDO2
Values	Enabled / Disabled
Default	Disabled
Description	This setting allows the user to use the Temporary Access Code to login when they do not have access to their FIDO2 passkey. If you enable this policy, a Temporary Access Code can be used instead of the FIDO2 passkey. If you disable or do not configure this policy then a Temporary Access Code will not be accepted.
License	MFA

Setting	Enable Password Reset via Web Sign-in
Values	Enabled / Disabled
Default	Disabled
Description	This allows users to use the Web Sign-in feature for password resets via the forgot password link on the desktop logon screen. If you enable this policy, Web Sign-in can be used for Password Resets. If you disable or do not configure this policy then Web Sign-in cannot be used for Password Resets.
License	MFA or PSM

Setting	Ignore Web Sign-in certificate errors
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting ignores SSL certificate errors and allows Web Sign-in to function. This should be enabled if you are using a self-signed SSL certificate on the MFA server. If you enable this policy Web Sign-in SSL certificate checks will be ignored. If you disable or do not configure this policy then Web Sign-in SSL certificate validity checks will be performed.
License	MFA or PSM

Setting	Password Reset OpenID Connect Client ID
Values	Client ID
Default	
Description	This policy setting configures the OpenID Connect Client ID used for AD password resets. If you enable this policy, you must specify the OpenID Connect Client ID of the custom Application to be used for password resets. If you disable or do not configure this policy, the built in Web Sign-in Application will be used.
License	MFA or PSM

Setting	Web Sign-in OpenID Connect Client ID
Values	Client ID
Default	
Description	This policy setting configures the OpenID Connect Client ID used for Web Sign-in. If you enable this policy, you must specify the OpenID Connect Client ID of the custom Application to be use for Web Sign-in. If you disable or do not configure this policy the built in Web Sign-in Application will be used.
License	MFA

3.9.2 Security Settings

Setting	Allow logon with local SAM accounts
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting allows the use of local SAM username and password for logon to the PC. If you enable this policy local SAM accounts can be used for logon without an OTP. If you disable or do not configure this policy local SAM accounts cannot be used for logon.
License	MFA

Setting	Disable MyID MFA for Windows Credential Prompting
Values	All / Admin / User / Other
Default	
Description	This policy setting disables MFA for Windows Credential Prompting. If you enable this policy MFA will not be not be available for use when Windows prompts users for credentials of the types specified or combinations of these types: • All – This applies to all credentials and is the equivalent of enabling all of the options below. • Admin – The user is required to enter Administrator credentials. • User – The user is required to re-enter their own credentials. • Other – The user is required to enter credentials for a non-specific user. If you disable or do not configure this policy the Windows Desktop Agent will use MFA when Windows prompts users for credentials.
License	MFA

Note: In previous versions of MyID MFA, you could configure this setting as **Enabled** or **Disabled**, but could not select the specific credential types. If you previously set **Disable MyID MFA for Windows Credential Prompting** to **Enabled** in a version of MyID MFA that did not allow you to select specific credential types, when you upgrade, this setting is set to **All**.

Setting	Disable Windows Cloud Experience logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the built in Windows Cloud Experience logon functionality. This should be enabled if MyID is the only authentication type which is required. If you enable this policy the built in Windows Cloud Experience logon functionality will not be available for use. If you disable or do not configure this policy the Windows Cloud Experience logon functionality will be available for use.
License	MFA or PSM

Setting	Disable Windows Desktop Agent when on the LAN
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the Windows Desktop Agent functionality when the PC is connected to the local area network. If you enable this policy the Windows Desktop Agent functionality will not be available for use when the PC is on the LAN and will only function when the PC is working remotely. If you disable or do not configure this policy the Windows Desktop Agent functionality will be available at all locations.
License	MFA

Setting	Disable Windows FIDO2 logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the built in Windows FIDO2 logon functionality. This should be enabled if MyID is the only authentication type which is required. If you enable this policy the built in Windows FIDO2 logon functionality will not be available for use. If you disable or do not configure this policy the Windows FIDO2 logon functionality will be available for use.
License	MFA or PSM

Setting	Disable Custom 3rd party credential providers
Values	Disabled / GUID CSV
Default	Disabled
Description	This policy setting disables 3rd party credential provider functionality so that their functionality is not available for use. If you enable this policy the GUID(s) of any 3rd party credential provider to be disabled must be specified. Multiple GUID entries must be separated by a comma. If you disable or do not configure this policy, then 3rd party credential providers will not be disabled and will be available for use.
License	MFA or PSM

Setting	Disable Windows Hello for Business Face Recognition logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the built in Windows Hello for Business Face Recognition logon functionality. This should be enabled if MyID is the only authentication type which is required. If you enable this policy the built in Windows Hello for Business Face Recognition logon functionality will not be available for use. If you disable or do not configure this policy the Windows Hello for Business Face Recognition logon functionality will be available for use.
License	MFA or PSM

Setting	Disable Windows Hello for Business Fingerprint logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the built in Windows Hello for Business Fingerprint logon functionality. This should be enabled if MyID is the only authentication type which is required. If you enable this policy the built in Windows Hello for Business Fingerprint logon functionality will not be available for use. If you disable or do not configure this policy the Windows Hello for Business Fingerprint logon functionality will be available for use.
License	MFA or PSM

Setting	Disable Windows Hello for Business PIN logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the built in Windows Hello for Business PIN logon functionality. This should be enabled if MyID is the only authentication type which is required. If you enable this policy the built in Windows Hello for Business PIN logon functionality will not be available for use. If you disable or do not configure this policy the Windows Hello for Business PIN logon functionality will be available for use.
License	MFA or PSM

Setting	Disable Windows Hello for Business Trusted Signal logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the built in Windows Hello for Business Trusted Signal (Phone proximity, Network location etc) logon functionality. This should be enabled if MyID is the only authentication type which is required. If you enable this policy the built in Windows Hello for Business Trusted Signal logon functionality will not be available for use. If you disable or do not configure this policy the Windows Hello for Business Trusted Signal logon functionality will be available for use.
License	MFA or PSM

Setting	Disable Windows Iris logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the built in Windows Iris logon functionality. This should be enabled if MyID is the only authentication type which is required. If you enable this policy the built in Windows Iris logon functionality will not be available for use. If you disable or do not configure this policy the Windows Iris logon functionality will be available for use.
License	MFA or PSM

Setting	Disable Windows Picture Password logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the built in Windows Picture Password logon functionality. This should be enabled if MyID is the only authentication type which is required. If you enable this policy the built in Windows Picture Password logon functionality will not be available for use. If you disable or do not configure this policy the Windows Picture Password logon functionality will be available for use.
License	MFA or PSM

Setting	Disable Windows Smart Card logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the built in Windows Smart Card logon functionality. This should be enabled if MyID is the only authentication type which is required. If you enable this policy the built in Windows Smart Card logon functionality will not be available for use. If you disable or do not configure this policy the Windows Smart Card logon functionality will be available for use.
License	MFA or PSM

Setting	Disable Windows Smart Card Password Changes
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the built in Windows Smart Card logon functionality for Password Changes. This should be enabled if MyID is the only authentication type which is required. If you enable this policy the built in Windows Smart Card logon functionality will not be available for use during a password change. If you disable or do not configure this policy the Windows Smart Card logon functionality will be available for use during a password change.
License	MFA or PSM

Setting	Disable Windows Username and Password logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the built in Windows username and password logon functionality. This should be enabled if MyID is the only authentication type which is required. If you enable this policy the built in Windows username and password logon functionality will not be available for use. If you disable or do not configure this policy the Windows username and password logon functionality will be available for use.
License	MFA or PSM

Setting	Enable Windows Desktop Agent in Windows Safe Mode
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting enables the use of Windows Desktop Agent while Windows is running in Safe Mode. By default, Windows disables 3rd party authentication providers, such as Windows Desktop Agent, and non-critical services while in Safe mode. If you enable this policy the MyID Windows Desktop Agent will be active and the Windows Desktop Agent service will be allowed to run while in Safe Mode. If you disable or do not configure this policy the MyID Windows Desktop Agent will not be available when in Safe Mode and the built in Windows Username and Password logon option will be available.
License	MFA or PSM

Setting	Disable MyID MFA logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the MyID MFA logon functionality, excluding FIDO2 passkeys. If you enable this policy the MyID MFA logon functionality, excluding FIDO2 passkeys, will not be available for use. If you disable or do not configure this policy the MyID MFA logon functionality will be available for use.
License	MFA

Setting	Disable MyID FIDO2 passkey logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting disables the MyID FIDO2 passkey logon functionality. This should be enabled if MyID FIDO2 passkey logons are required. If you enable this policy the MyID FIDO2 passkey logon functionality will not be available for use. If you disable or do not configure this policy the MyID FIDO2 passkey logon functionality will be available for use.
License	MFA

3.9.3 Offline login settings

Setting	Disable Offline Deviceless OTP Authentication
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting configures the Deviceless OTP authentication offline functionality of the Windows Desktop Agent. Note: If the "Disable Offline logons" policy is enabled then this policy will not take effect. If you enable this policy the Windows Desktop Agent will not provide any Deviceless OTP authentication offline functionality, including External Server Access. Only 2FA offline logons will be allowed. If you disable or do not configure this policy the Windows Desktop Agent will cache required user and settings information from the Active Directory to allow for Deviceless OTP offline logons.
License	MFA

Setting	Disable Offline logons
Values	Enabled / Disabled
Default	Disabled
Description	This policy setting configures the offline functionality of the Windows Desktop Agent. If you enable this policy the Windows Desktop Agent will not provide any offline functionality, including External Server Access. If you disable or do not configure this policy the Windows Desktop Agent will cache required user and settings information from the Active Directory to allow for offline logons.
License	MFA

Setting	Offline AD sync schedule
Values	(1-9999)
Default	24 (Hours)
Description	This policy setting specifies the interval between scheduled synchronisations between the Windows Desktop Agent and the Active Directory to refresh locally cached data for offline logons. Note: If the "Disable Offline logons" policy is enabled then this policy will not take effect. If you enable this policy you must specify the interval value in hours between synchronisations between the Windows Desktop Agent and the Active Directory. If you disable or do not configure this policy the Windows Desktop Agent will synchronise with the Active Directory every 24 hours.
License	MFA or PSM

3.9.4 Server configuration settings

Setting	Authlogics Authentication Server Names
Values	Any DNS based server address (CSV)
Default	
Description	This policy setting configures the server name(s) which PCs 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.
License	MFA or PSM

Setting	Authlogics Authentication Server Standard Port (HTTPS/SSL)
Values	(1024 – 65535)
Default	14443
Description	This policy setting configures the MyID Authentication Server port number which PCs will use to connect to the MyID Authentication Server when they are on the LAN. 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.
License	MFA or PSM

Setting	Domain Controller Server Names
Values	Any DNS based server address (CSV)
Default	
Description	This policy setting configures the server name(s) which PCs 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.
License	MFA or PSM

Setting	External Access Server Address
Values	Any DNS based server address and TCP port
Default	
Description	This policy setting configures the server name and port number which PCs will use to connect to the MyID Authentication Server when they are outside of the LAN. External Access allows an MyID Authentication Server to authenticate a user if even if the PC is not on the LAN. External Access always uses SSL encryption (HTTPS) and should be published via a reverse proxy server for extra security. If you enable this policy you must specify a DNS server address and port number, e.g. eas.mycompany.com:14443 If you disable or do not configure this policy the External Address functionality will be disabled.
License	MFA or PSM

Setting	Global Catalog Server Names
Values	Any DNS based server address (CSV)
Default	
Description	This policy setting configures the server name(s) which PCs will use to connect to Global Catalogs 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.
License	MFA or PSM

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 Authlogics Cloud Password Breach Database on the URL https://passwordsecurityapi.authlogics.com/api/*. 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 and Proxy Server Use System Proxy is not configured then proxy server will not be used and a routable Internet connection will be required.
License	MFA or PSM

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.
License	MFA or PSM

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

Setting	Proxy Server Use System Proxy
Values	Enabled / Disabled
Default	Enabled
Description	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. If you disable this policy then the system proxy will not be used. Note: If Proxy Server Host is configured then it will be used in precedence to the system configuration if this policy is enabled.
License	MFA or PSM

3.9.5 Timing Settings

Setting	Active Directory access timeout
Values	(0 – 120)
Default	15 (seconds)
Description	This policy setting sets the maximum amount of time to wait while connecting to an Active Directory Domain Controller before going offline. 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 the Windows Desktop Agent running in offline mode 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 before reverting to offline mode. Setting this value to 0 will disable the timeout and connections will wait indefinitely. If you disable or do not configure this policy the Windows Desktop Agent will wait for 15 seconds while locating an Active Directory Domain before reverting to offline mode.
License	MFA or PSM

Setting	Active Directory Domain Controller refresh time
Values	(1 – 1440)
Default	60 (minutes)
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 Windows Desktop Agent will retest the Domain Controller connectivity every 60 minutes.
License	MFA or PSM

Setting	Authenticator App device pairing timeout
Values	(30 – 300)
Default	120 (seconds)
Description	This policy setting sets the maximum amount of time to wait while the MyID Windows Desktop Agent Service pairs a new profile with the Authlogics Authenticator App and waits for a response. If you disable or do not configure this policy the Windows Desktop Agent will wait for 120 seconds for a response from the app.
License	MFA

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

Setting	Authlogics Authentication Server access timeout
Values	(0 – 120)
Default	15 (seconds)
Description	This policy setting sets the maximum amount of time to wait while connecting to an MyID Authentication Server before trying an alternative server if available or going offline. If you enable this policy you must specify the interval value in seconds to wait while connecting to 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 Windows Desktop Agent will wait for 15 seconds for a response from an MyID Authentication Server.
License	MFA or PSM

Setting	Authlogics Authentication Server refresh time
Values	(1 – 1440)
Default	60 (minutes)
Description	This policy setting sets the maximum amount of time to use the current MyID Authentication Server before refreshing the most suitable 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 Windows Desktop Agent will wait for 60 minutes before refreshing which MyID Authentication Server to use.
License	MFA or PSM

Setting	Authlogics External Access Server timeout
Values	(0 – 120)
Default	8 (seconds)
Description	This policy setting sets the maximum amount of time to wait while connecting to an MyID External Access Server before going offline. If you enable this policy you must specify the interval value in seconds to wait while connecting to an MyID External Access 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 Windows Desktop Agent will wait for 8 seconds for a response from an MyID External Access Server.
License	MFA or PSM

Setting	Authlogics Windows Desktop Agent Service access timeout
Values	(0 – 120)
Default	15 (seconds)
Description	This policy setting sets the maximum amount of time to wait while the MyID Windows Desktop Agent Service attempts to start before timing out and reverting to a standard Windows logon. If you enable this policy you must specify the interval value in seconds to wait for the service to start. Setting this value to 0 will disable the timeout and connections will wait indefinitely preventing a fallback to standard Windows logon. If you disable or do not configure this policy the Windows Desktop Agent will wait for 45 seconds for the MyID Windows Desktop Agent service to start.
License	MFA or PSM

Setting	Offline access timeout
Values	(1 – 30)
Default	4 (seconds)
Description	This policy setting sets the maximum amount of time to wait while locating an available MyID Authentication Server or Active Directory Domain Controller going offline. Setting this value too high can make offline status detection take longer while an available MyID Authentication Server or Active Directory Domain Controller is being located, whereas setting this value too low could result in the Windows Desktop Agent running in offline mode even when a server is available. If you enable this policy you must specify the interval value in seconds to wait while locating an available MyID Authentication Server or Active Directory Domain Controller before reverting to offline mode. If you disable or do not configure this policy the Windows Desktop Agent will wait for 4 seconds while locating an available MyID Authentication Server or Active Directory Domain Controller before reverting to offline mode.
License	MFA or PSM

3.10 Automated / command line setups

3.10.1 Running an installation with verbose logging

In scenarios where the installation may not succeed on a system, it may be necessary to run setup with logging enabled to help identify the problem. The following command runs setup and create a `setup.log` file containing information about the install:

```
msiexec /i "MyID Windows Desktop Agent xxxxx.msi" /lv setup.log
```

3.10.2 Fully automated silent installation

You can run the setup silently as follows:

```
msiexec /i "MyID Windows Desktop Agent xxxxx.msi" CMDLINE="ALLUSERS=TRUE"
/quiet
```

3.10.3 Fully automated silent removal

You can remove the agent silently as follows:

```
msiexec /x "MyID Windows Desktop Agent xxxxx.msi" CMDLINE="ALLUSERS=TRUE"
/quiet
```

4 Using the Windows Desktop Agent

You can use the Windows Desktop Agent for more than just authentication to Windows (see section *1.2*, *Multi Factor Authentication*); you can also:

- Get feedback on attempted password changes.

  See section *4.1*, *Changing an Active Directory password*.
- Manage your Multi-Factor options.

  See section *4.2*, *Managing Multi-Factor options*.

  Specifically, you can:
  - Change a Grid Pattern.

    See section *4.2.1*, *Changing a Grid Pattern*.
  - Add a new MFA device.

    See section *4.2.2*, *Adding a new MFA device*.
  - Re-sync a device.

    See section *4.2.3*, *Resyncing a device*.
  - Register a passkey through the Security Key Credential Provider.

    See section *4.2.4*, *Passkey registration through the Security Key Credential Provider*.
  - Register a passkey using the MFA Credential Provider.

    See section *4.2.5*, *Passkey registration using the MFA Credential Provider*.
- Use MFA for Windows credential prompting.

  See section *4.3*, *Using MFA for Windows credential prompting*.

For information on using the browser reporting extension, see section *5.4*, *Using browser reporting*.

4.1 Changing an Active Directory password

The method you use to change your password depends on if you are already authenticated, whether you are using security phrases or basic passwords, and whether you are using MyID MFA to authenticate.

Authenticated	Security phrases	MFA	Method
✓		n/a	See section *4.1.1*, *Changing a basic password*.
✓	✓	n/a	See section *4.1.2*, *Changing a security phrase*.
			See section *4.1.3*, *Resetting a forgotten basic password with SMS or email*.
	✓		See section *4.1.4*, *Resetting a forgotten security phrase with SMS or email*.
		✓	See section *4.1.5*, *Resetting a forgotten basic password with MyID MFA*.
	✓	✓	See section *4.1.6*, *Resetting a forgotten security phrase with MFA*.

If your administrators have enabled security phrases, you do not type a new password; instead, you choose a randomly generated phrase. This phrase is used as your Windows password.

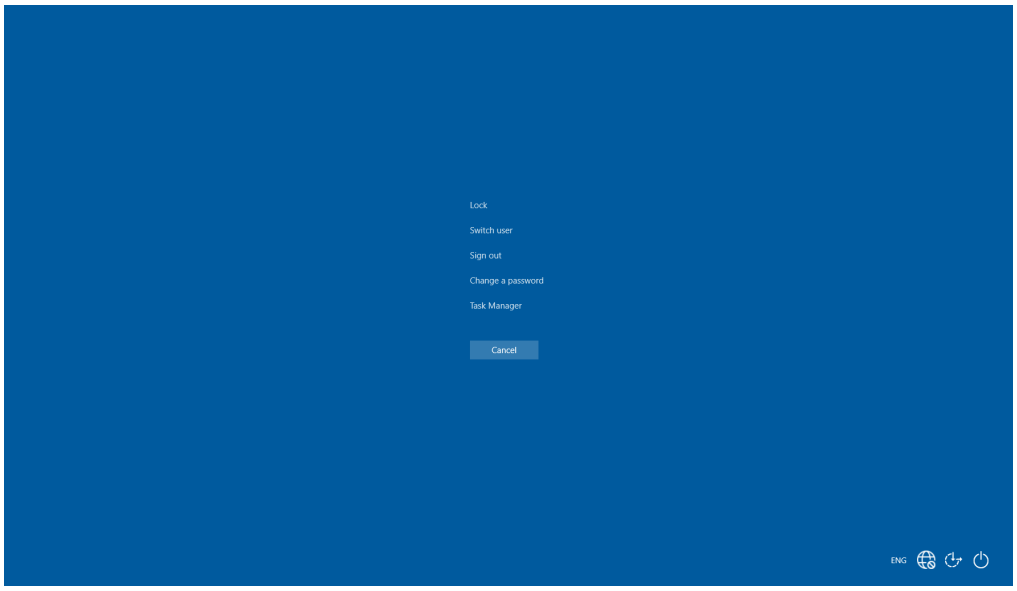
When you change your basic password, Windows Desktop Agent enforces PSM password policies on the new password. It also provides feedback on failed password changes.

4.1.1 Changing a basic password

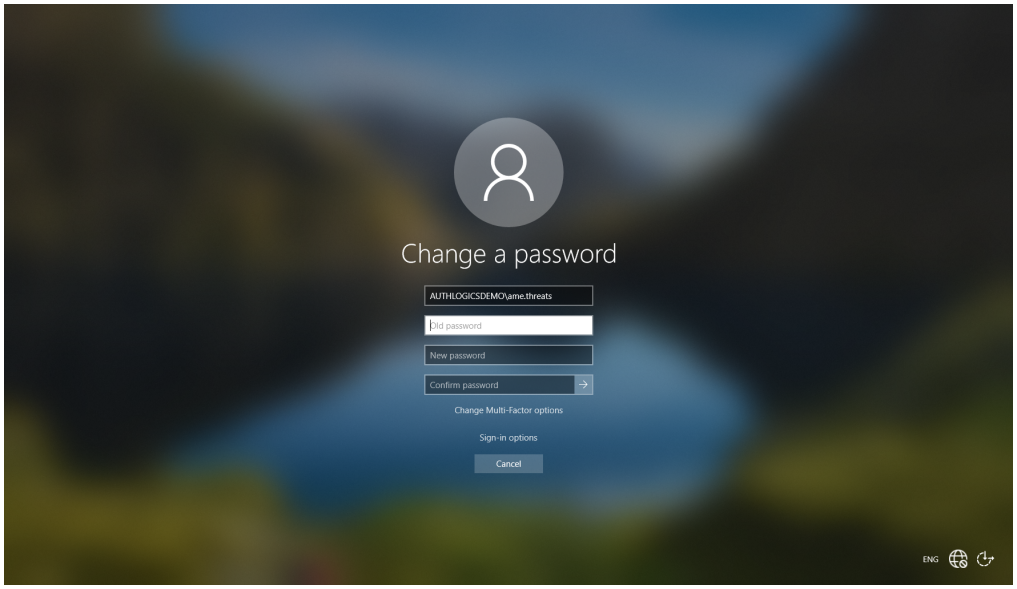
To change your basic password when you are already authenticated:

1. Press CTRL + ALT + DEL.

   This shows the Windows security screen.



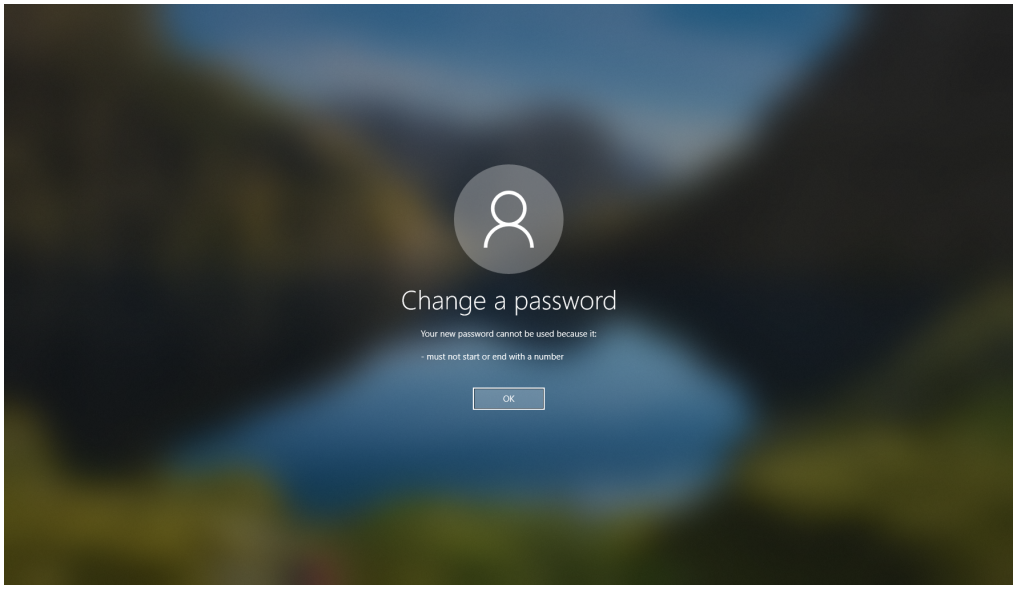
2. Click **Change a password**.



3. Enter your old password.
4. Enter your new password twice.

5. Click the **Submit** arrow.

   If the new password does not comply with the policies, the exact reason it failed is displayed.



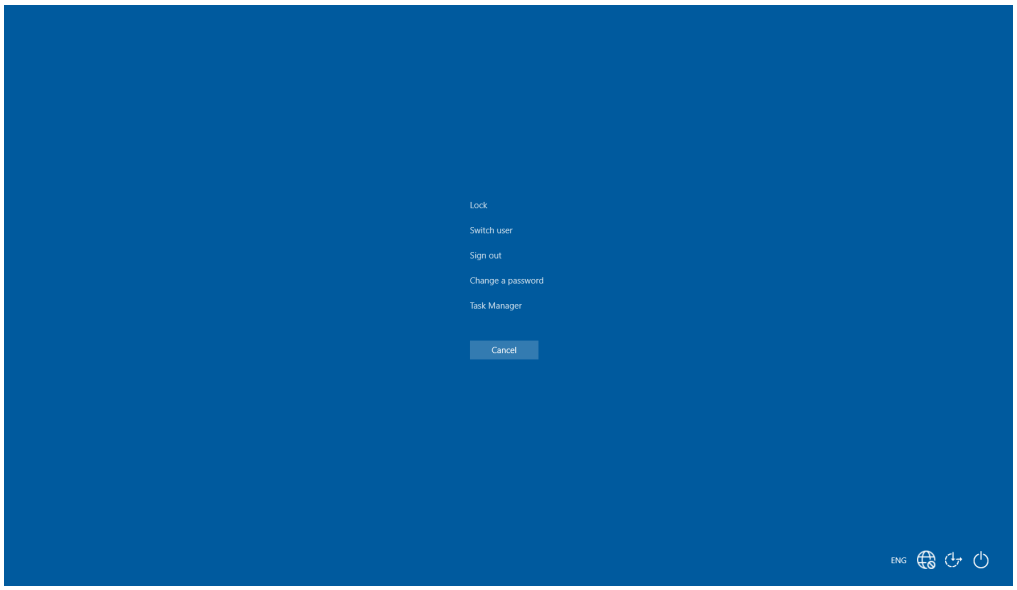
   This helps the user choose a new valid password without having to call the helpdesk.

4.1.2 Changing a security phrase

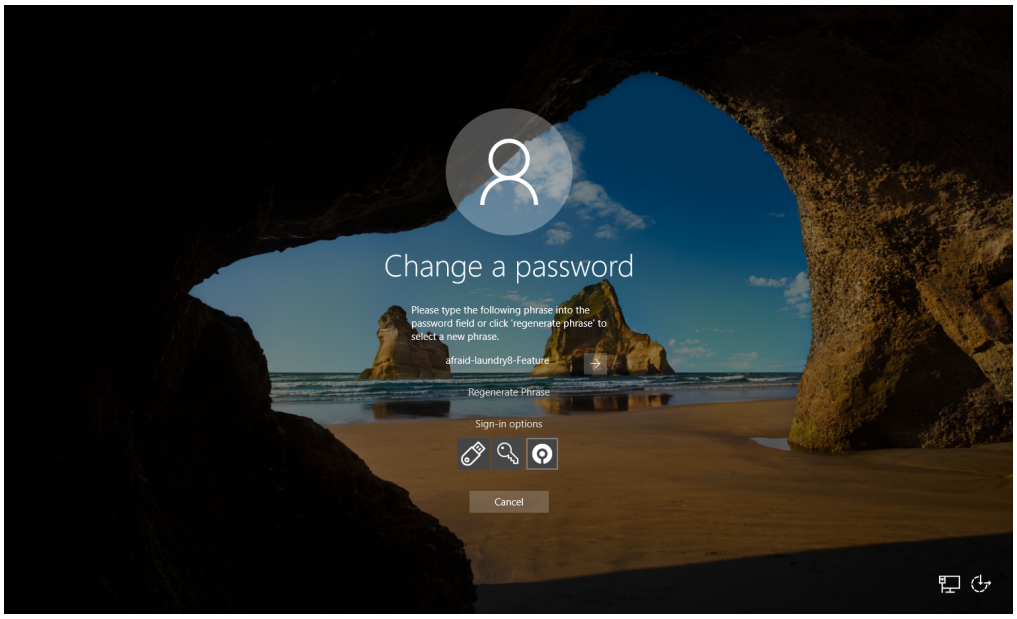
To change your security phrase when you are already authenticated:

1. Press CTRL + ALT + DEL.

   This shows the Windows security screen.



2. Click **Change a password**.

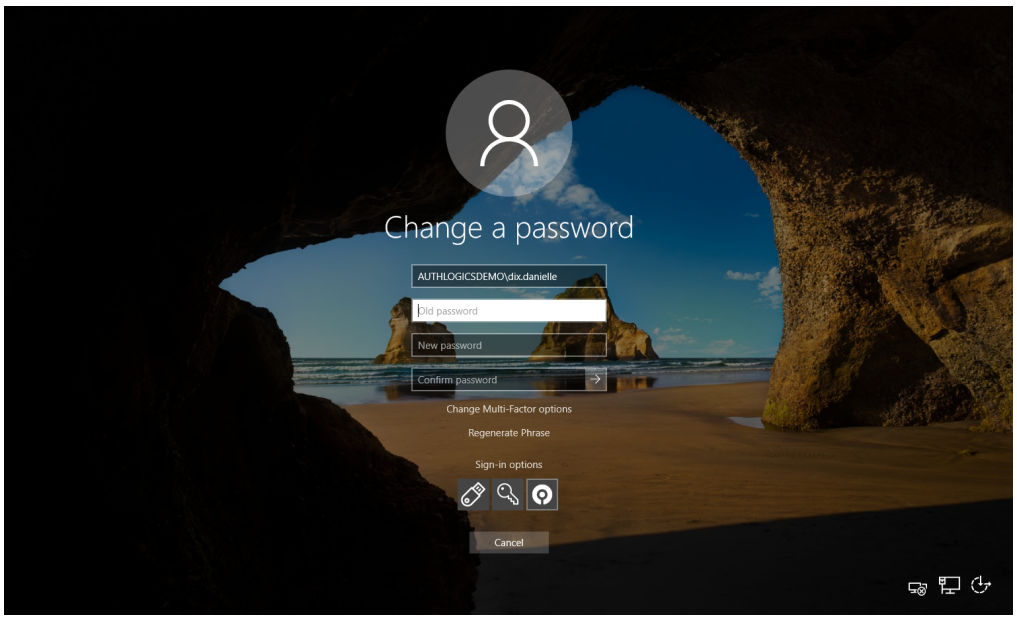


An automatically generated security phrase is displayed.

3. If you dislike the generated phrase, click **Regenerate Phrase**.

   You can regenerate your security phrase as many times as you want. Choose a phrase that you are confident you can recall.

4. Once you have a generated phrase that you like, ensure that you have memorized the security phrase, including capitalization and numbers, and click the **Submit** arrow.

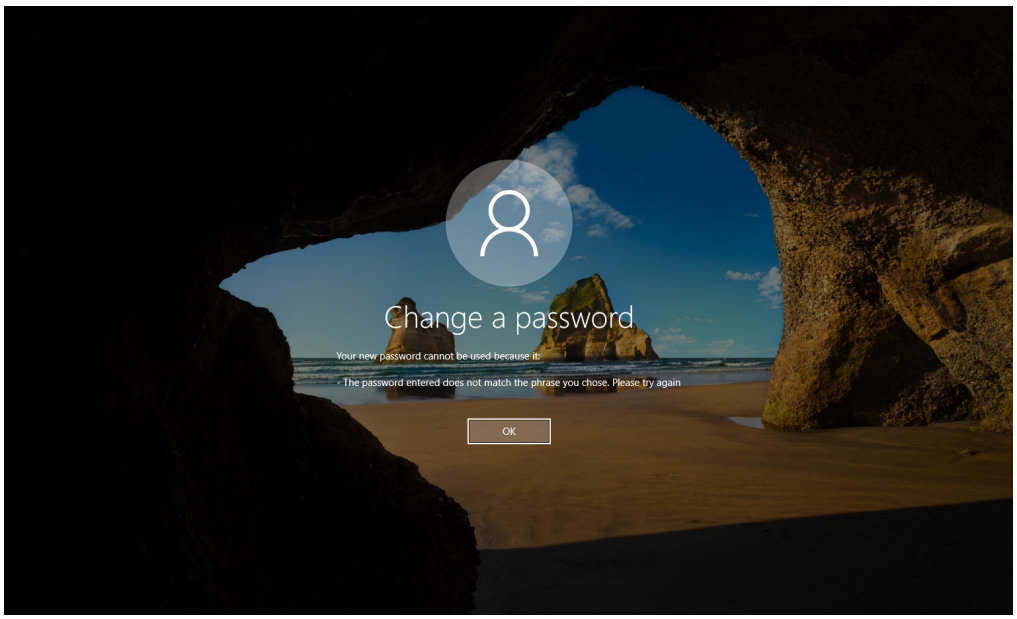


5. Enter your old password.
6. Enter your generated security phrase twice.

   If you forget your generated phrase, you can click **Regenerate Phrase** to view your generated phrase again.

7. Click the **Submit** arrow.

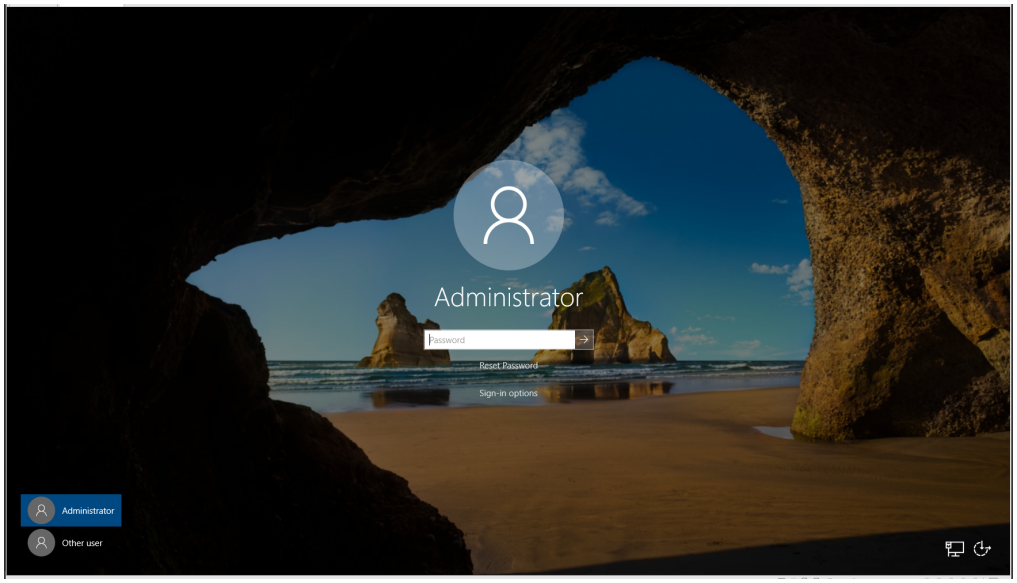
   If you mistype your new security phrase, you cannot proceed. Click **OK** to try again.



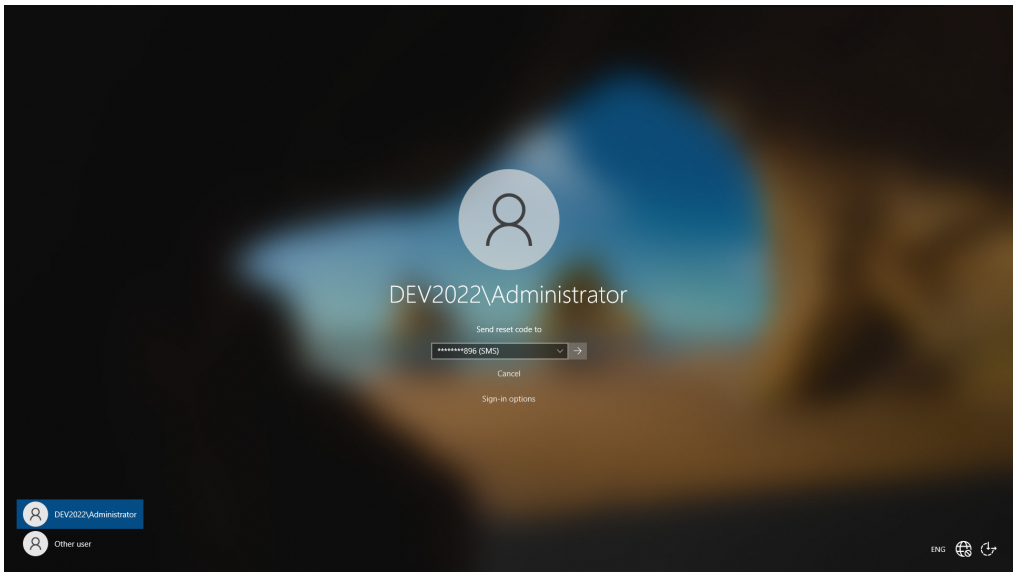
4.1.3 Resetting a forgotten basic password with SMS or email

If you have forgotten your password, you may be able to reset your password from the Windows logon screen using your access to your configured SMS or email to authenticate:

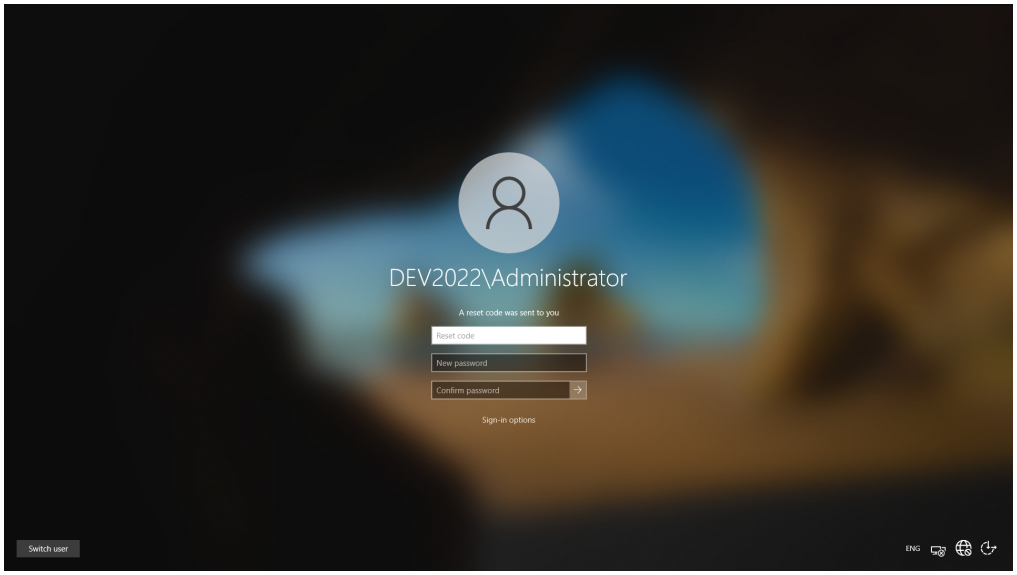
1. Navigate to your Windows logon screen.



2. Click **Reset Password**.



3. Depending on the technologies set by your administrators, you may be able to get a one-time code through SMS or email. From the drop down list, select where you want your reset code to be sent. If you have more than one SMS or email set, you can choose which one.
4. Click the **Submit** arrow.

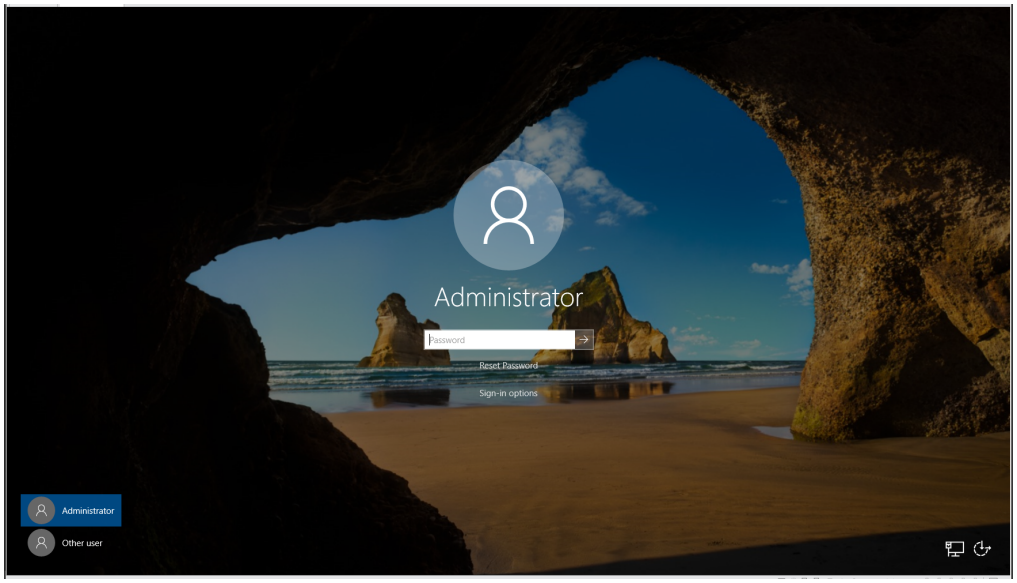


5. Check your SMS or email for the reset code.
6. Enter your reset code in the **Reset Code** field.
7. Enter your new password twice.
8. Click the **Submit** arrow.

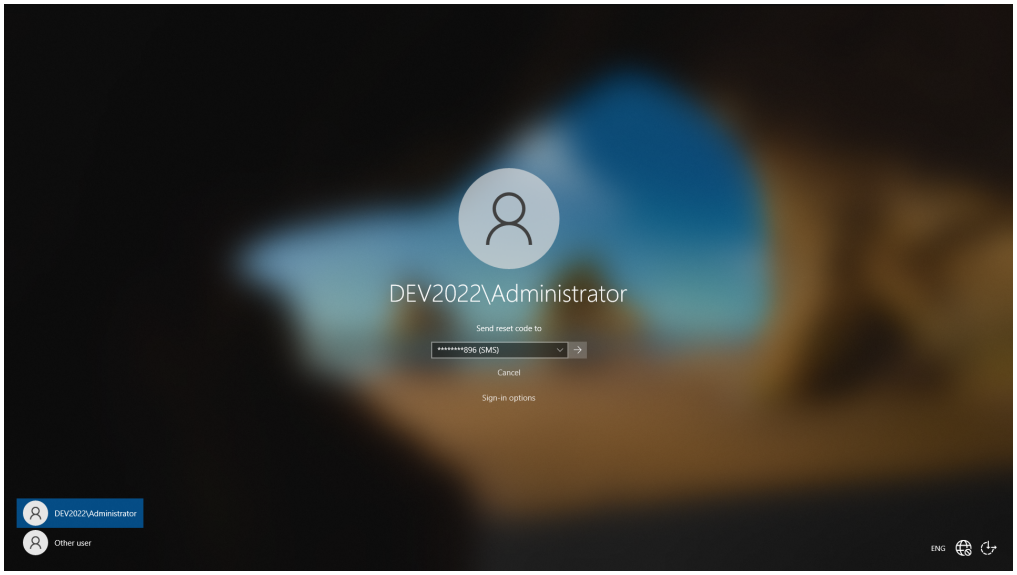
4.1.4 Resetting a forgotten security phrase with SMS or email

If you have forgotten your security phrase, you may be able to reset your security phrase from the Windows logon screen using your access to your configured SMS or email to authenticate:

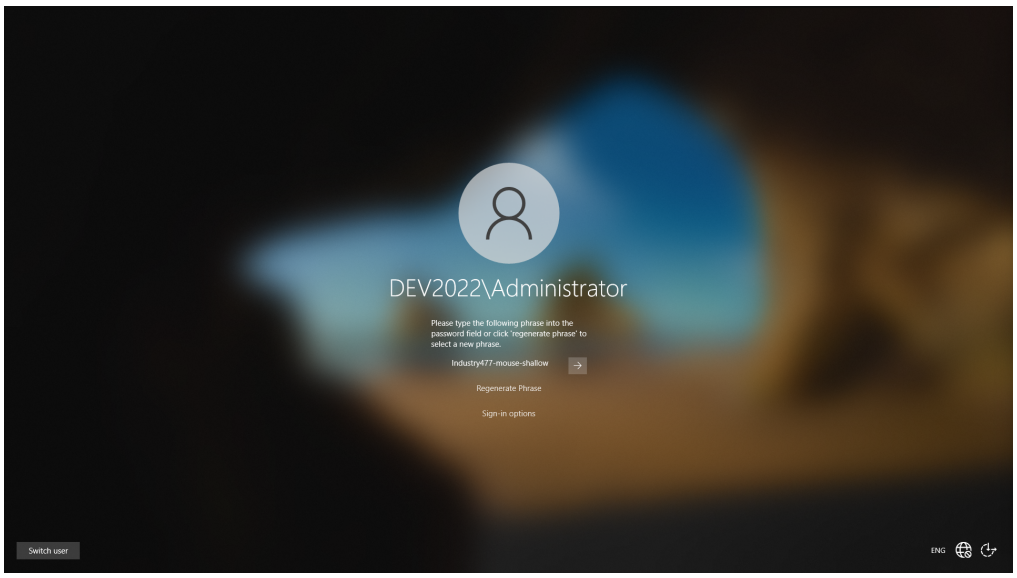
1. Navigate to your Windows logon screen.



2. Click **Reset Password**.



3. Depending on the technologies set by your administrators, you may be able to get a one-time code through SMS or email. From the drop down list, select where you want your reset code to be sent. If you have more than one SMS or email set, you can choose which one.
4. Check your SMS or email for the reset code.
5. Click the **Submit** arrow.

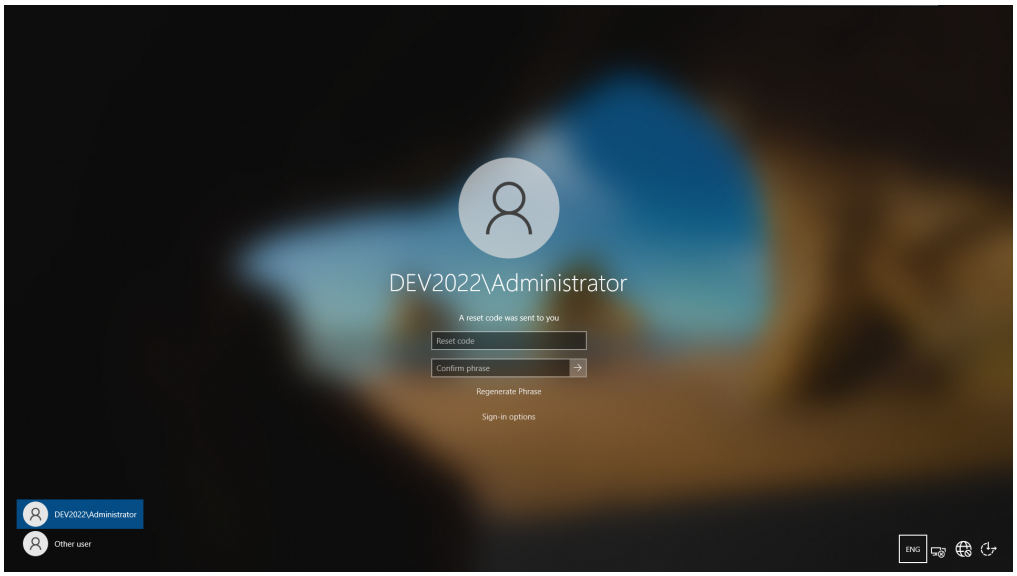


You are shown the password regeneration screen.

6. If you dislike the generated phrase, click **Regenerate Phrase**.

   You can regenerate your security phrase as many times as you want. Choose a phrase that you are confident you can recall.

7. Once you have a generated phrase that you like, ensure that you have memorized the security phrase, including capitalization and numbers, and click the **Submit** arrow.



8. Enter your reset code in the **Reset Code** field.
9. Enter your generated security phrase.

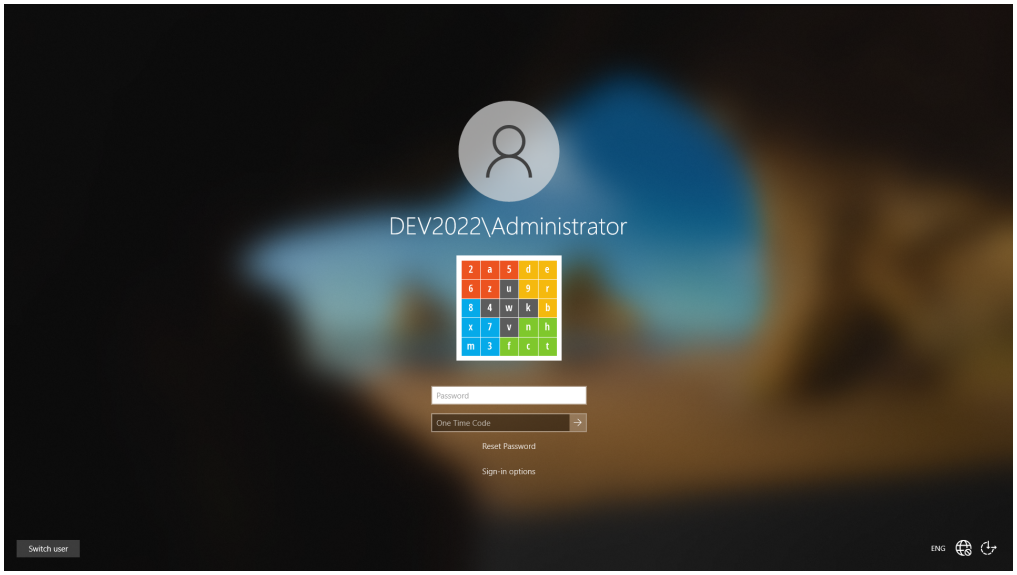
   If you forget your generated phrase, you can click **Regenerate Phrase** to view your generated phrase again.

10. Click the **Submit** arrow.

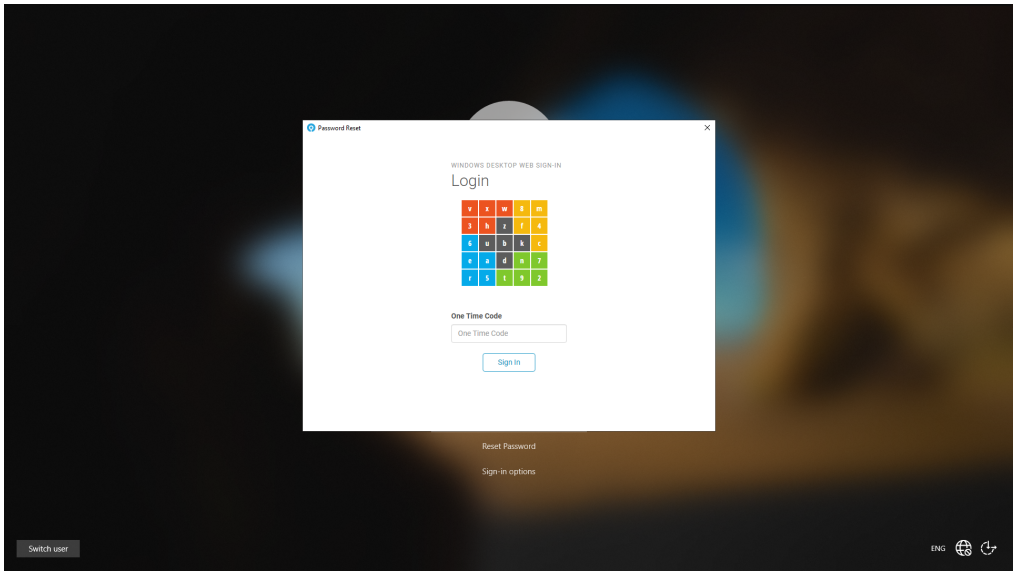
4.1.5 Resetting a forgotten basic password with MyID MFA

If you use MyID MFA to authenticate to Windows and you have forgotten your basic password, you may be able to reset your password using your MyID MFA technology to authenticate:

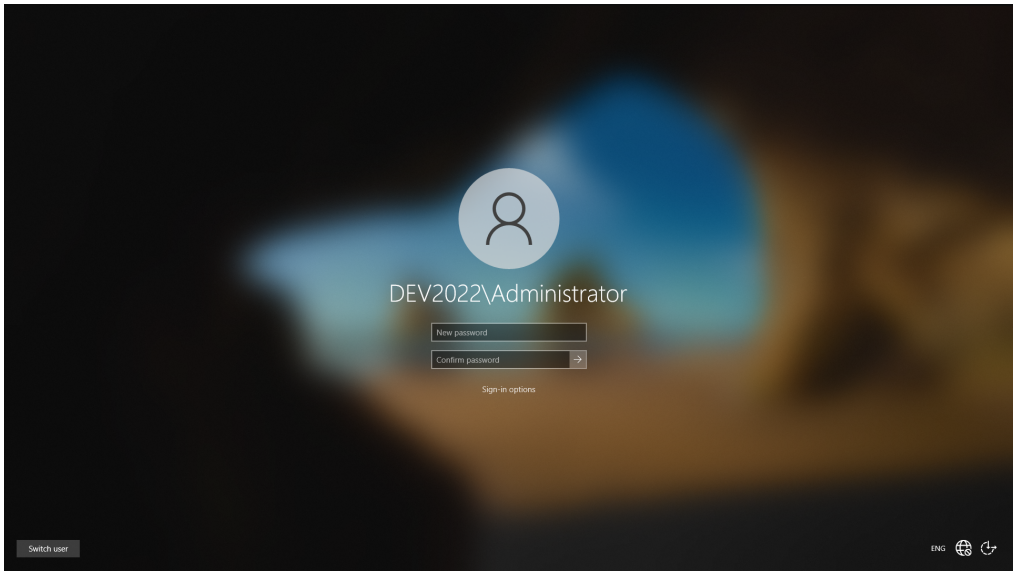
1. Navigate to your Windows logon screen.



2. Click **Reset Password**.



3. Authenticate with your MFA technology.
4. Click **Sign in**.

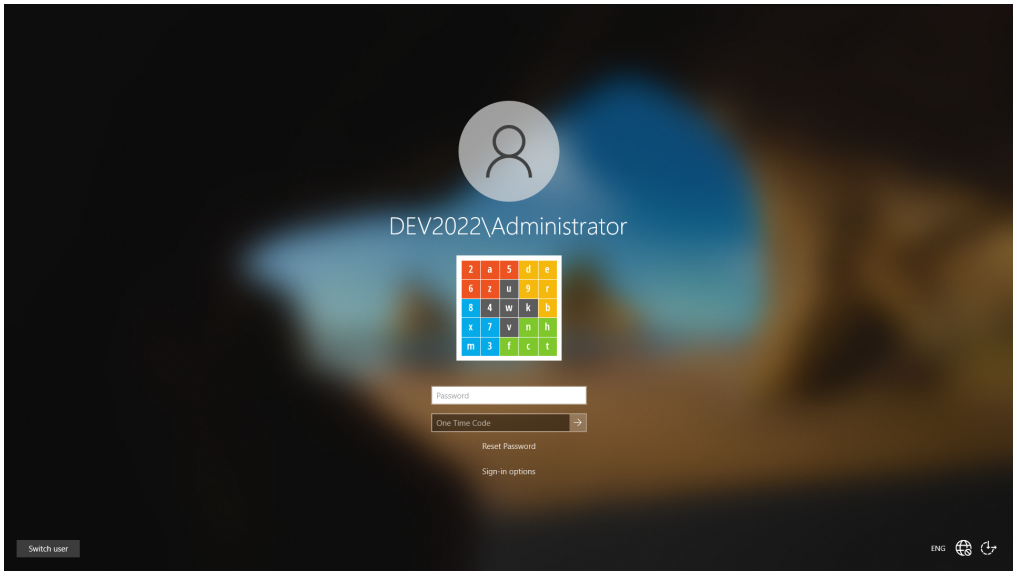


5. Enter your new password.
6. Confirm your new password.
7. Click the **Submit** arrow.

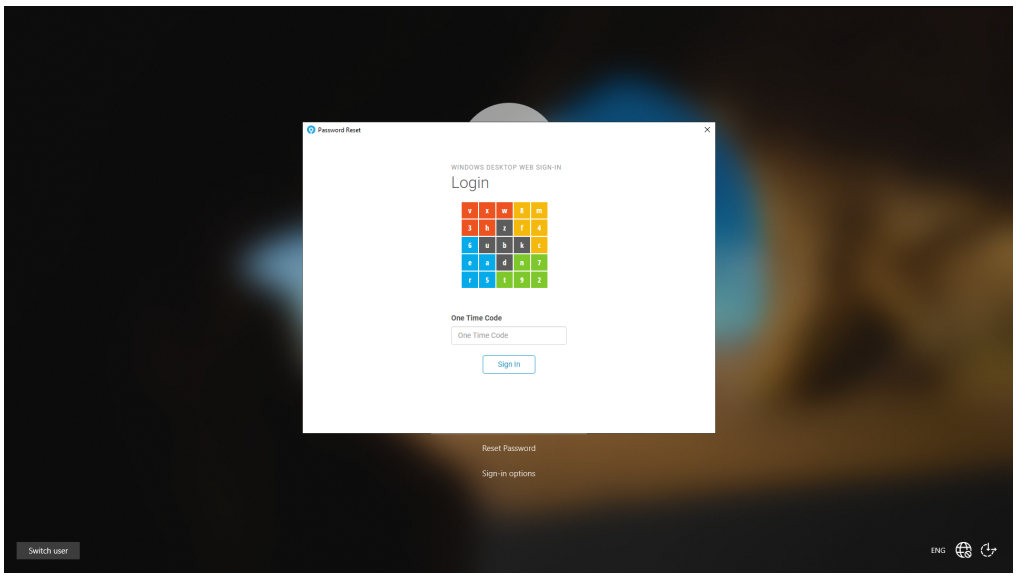
4.1.6 Resetting a forgotten security phrase with MFA

If you use MyID MFA to authenticate to Windows and you have forgotten your security phrase, you may be able to reset your password using your MyID MFA technology to authenticate:

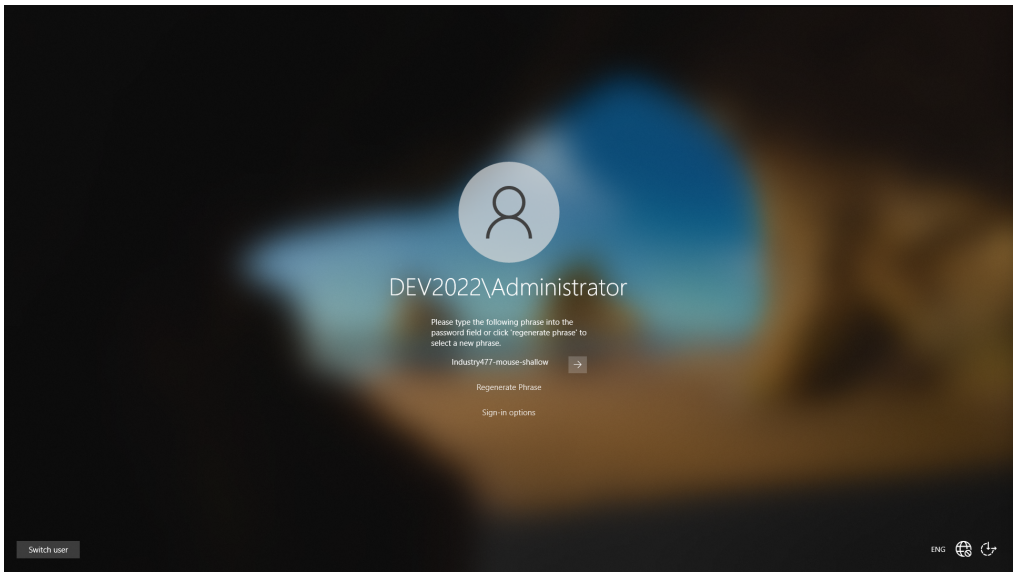
1. Navigate to your Windows logon screen.



2. Click **Reset Password**.



3. Authenticate with your MFA technology.
4. Click **Sign in**.

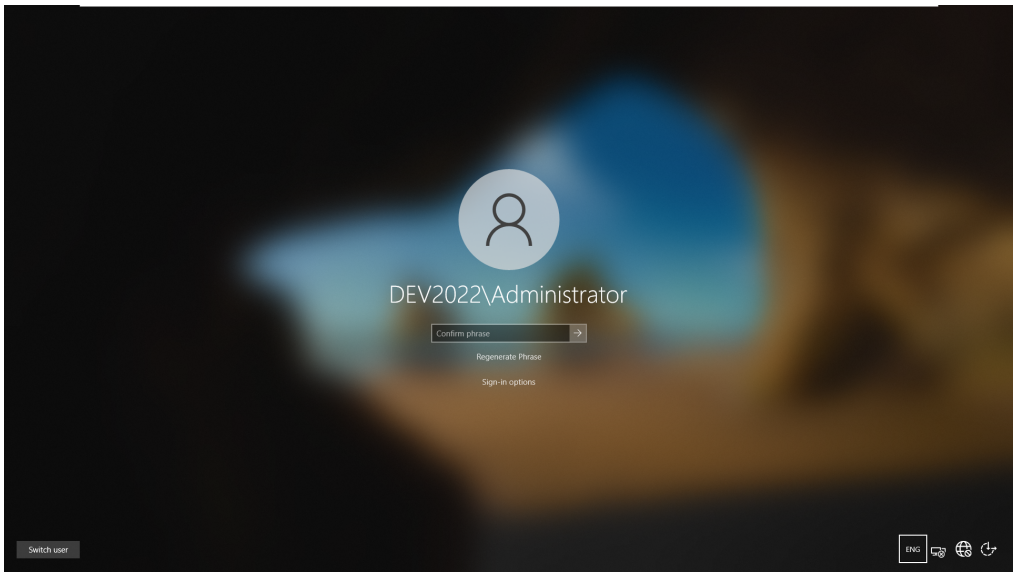


You are shown the password regeneration screen.

5. If you dislike the generated phrase, click **Regenerate Phrase**.

   You can regenerate your security phrase as many times as you want. Choose a phrase that you are confident you can recall.

6. Once you have a generated phrase that you like, ensure that you have memorized the security phrase, including capitalization and numbers, and click the **Submit** arrow.



7. Enter your generated security phrase.

   If you forget your generated phrase, you can click **Regenerate Phrase** to view your generated phrase again.

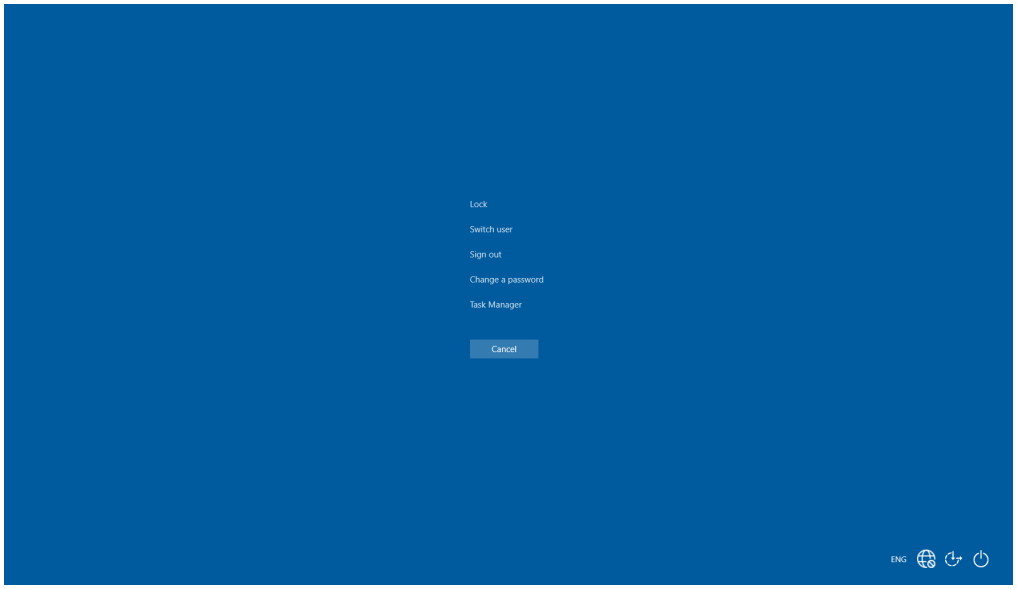
8. Click the **Submit** arrow.

4.2 Managing Multi-Factor options

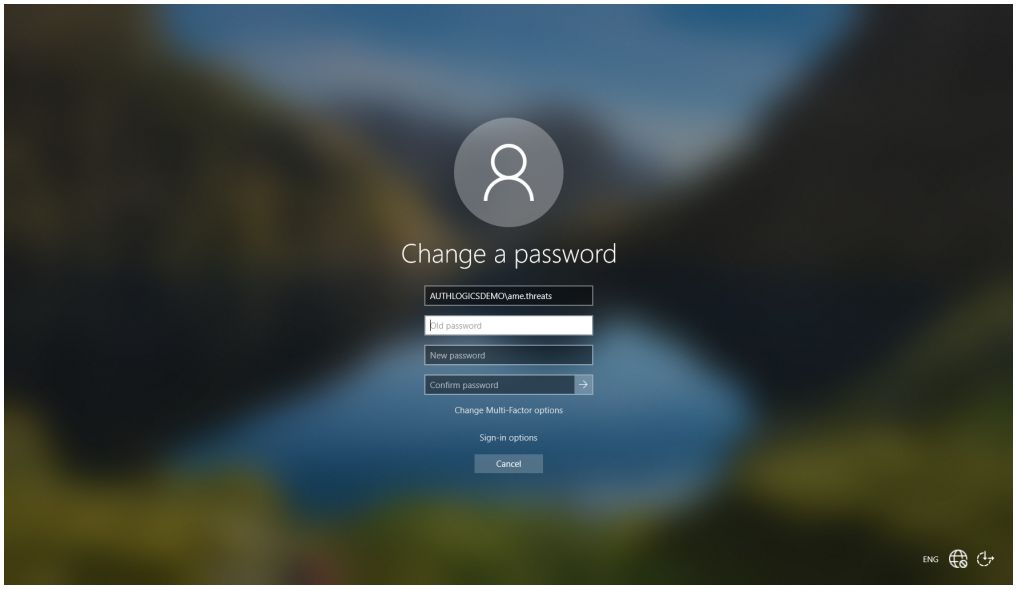
The Windows Desktop Agent allows users to manage MFA knowledge factors. This is similar to what they can do through the MyID Self Service Portal.

1. Press CTRL + ALT + DEL.

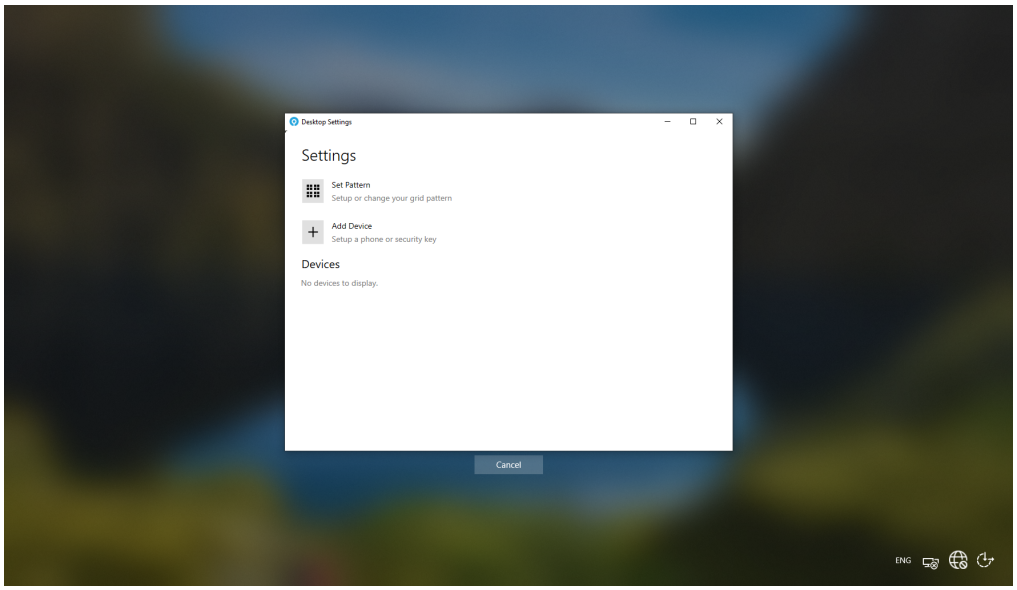
   This shows the Windows security screen.



2. Click **Change a password**.



3. Click **Change Multi-Factor options**.



You can:

- Change a Grid Pattern.

  See section *4.2.1*, *Changing a Grid Pattern*.
- Add a new MFA device.

  See section *4.2.2*, *Adding a new MFA device*.
- Resynchronize a device.

  See section *4.2.3*, *Resyncing a device*.
- Set up passkey registration using the Security Key Credential Provider.

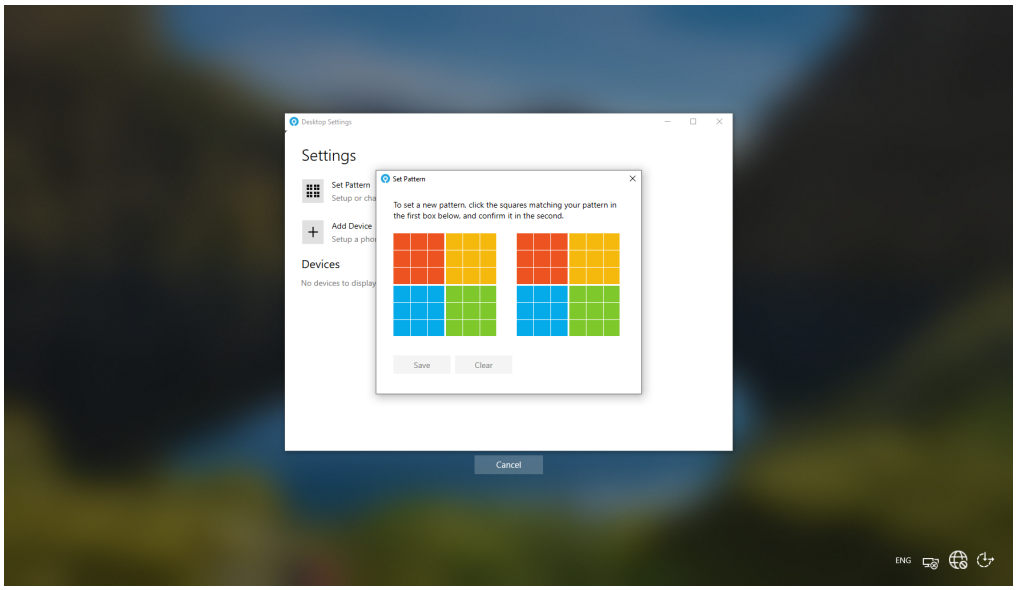
  See section *4.2.4*, *Passkey registration through the Security Key Credential Provider*.
- Set up passkey registration using the MFA Credential Provider.

  See section *4.2.5*, *Passkey registration using the MFA Credential Provider*.

Note: Your ability to manage your multi-factor technologies may be affected by the **Disable Change Multi-Factor options** GPO setting. For more information, see section *3.9.1*, *General settings*.

4.2.1 Changing a Grid Pattern

1. Click **Set Pattern**.



2. Enter a new pattern.

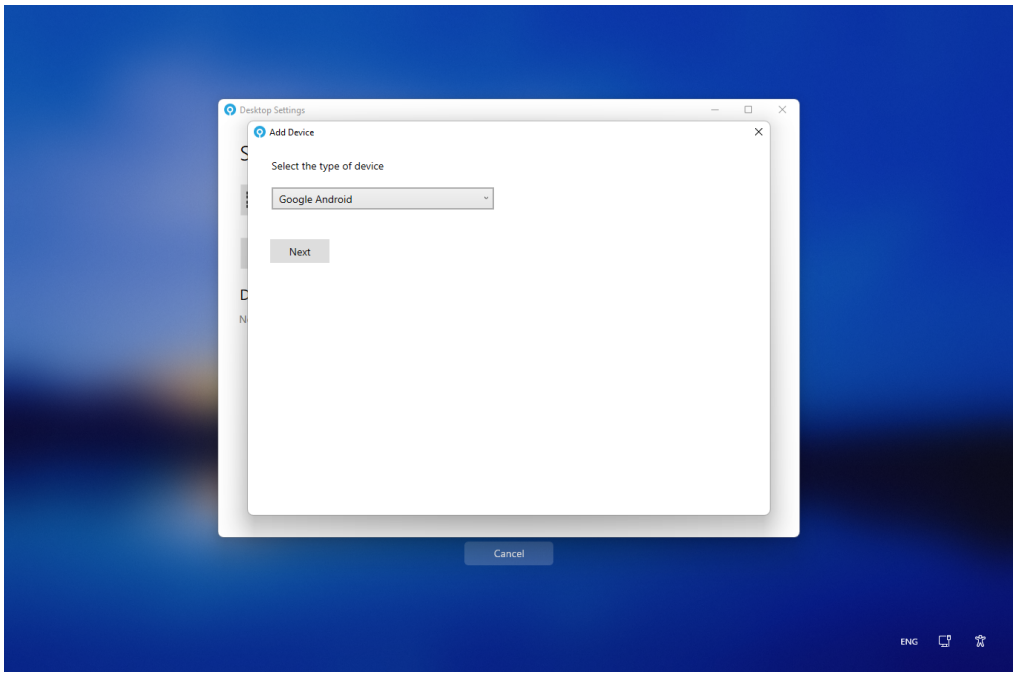
   To do this, click on the squares that you want, in sequence.

   You must click on the same sequence of squares on both grids.

3. Click **Save**.

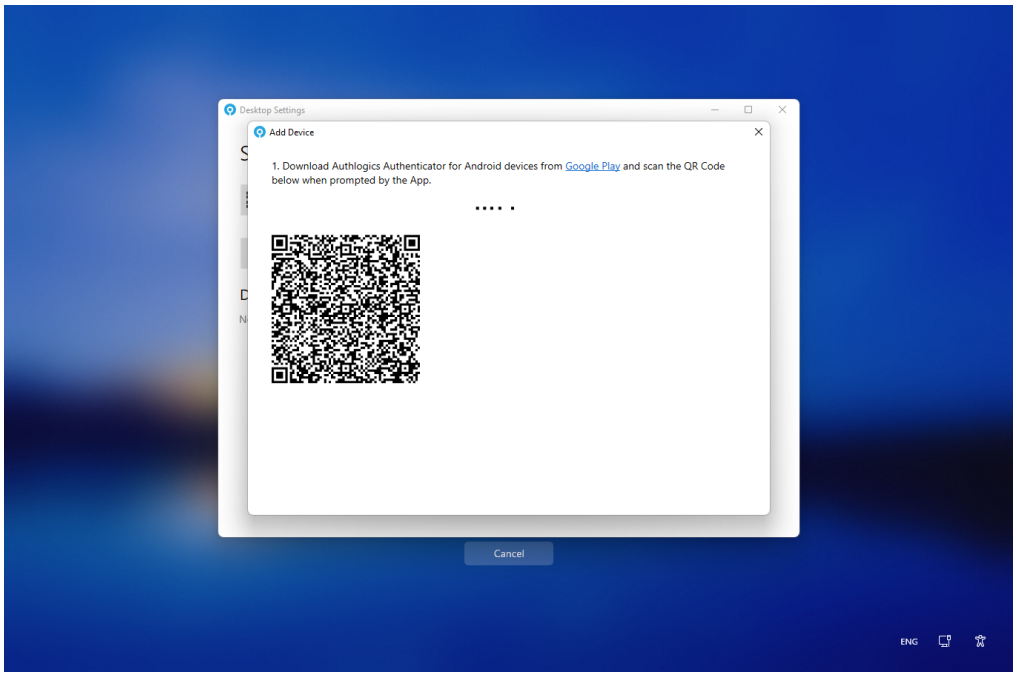
4.2.2 Adding a new MFA device

1. Click **Add Device**.

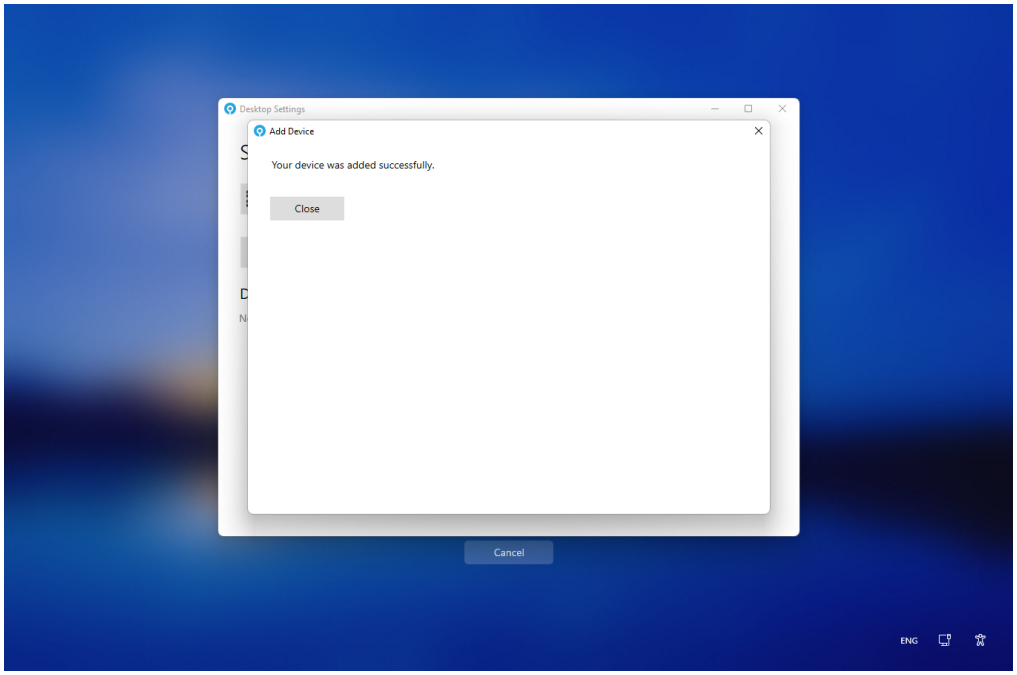


2. Select the device type of your device.

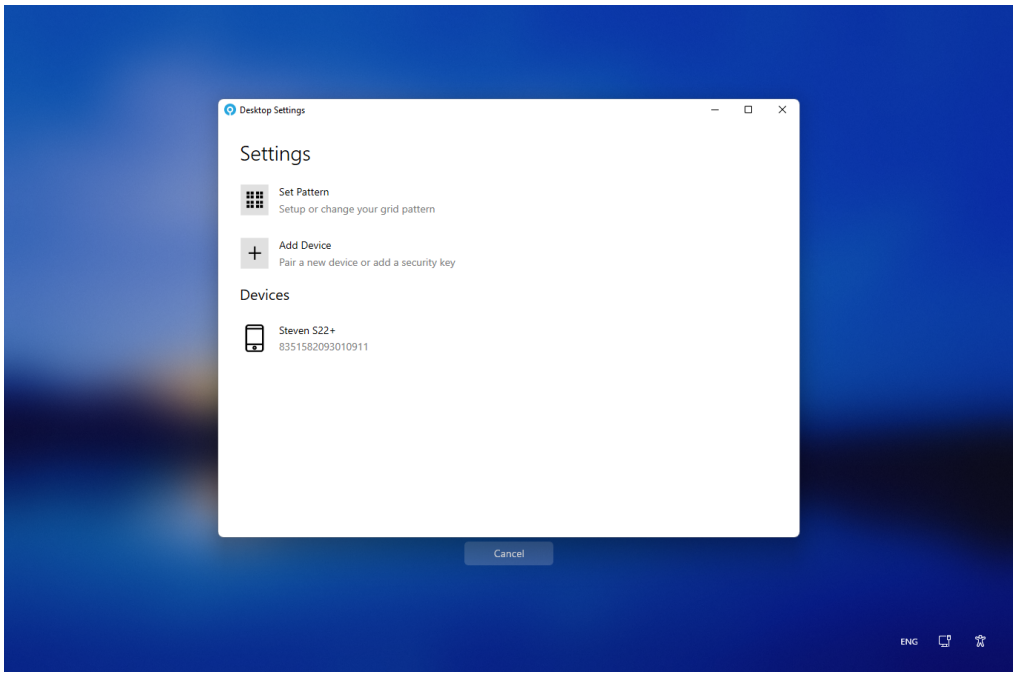
3. Click **Next**.



4. Scan the QR code with the MyID Authenticator App.



5. Click **Close**.



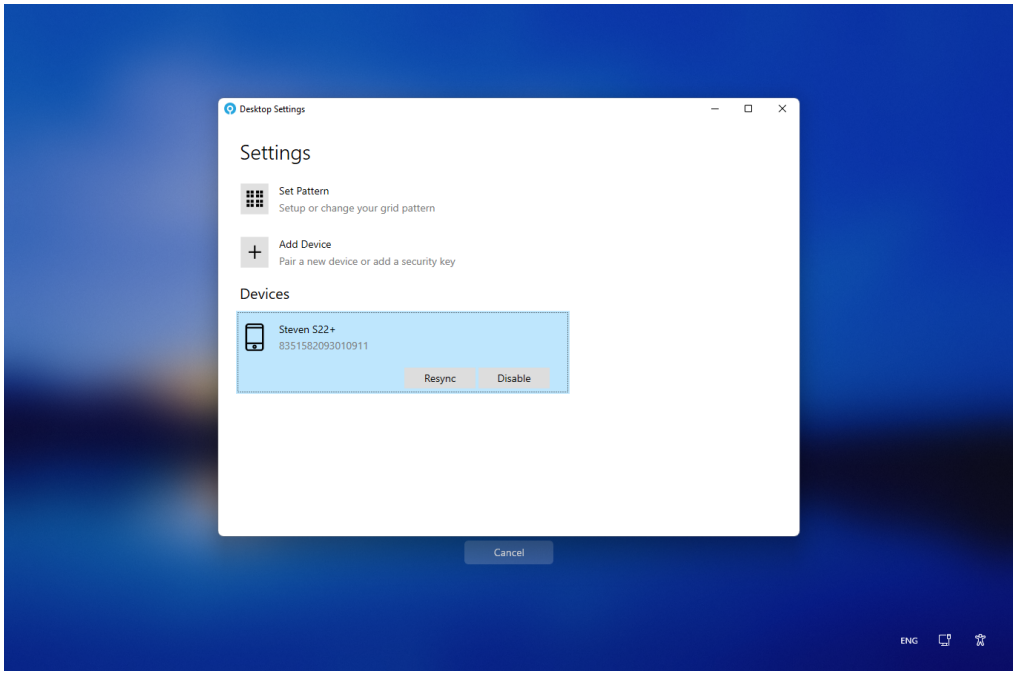
The new device is shown in the **Devices** list.

4.2.3 Resyncing a device

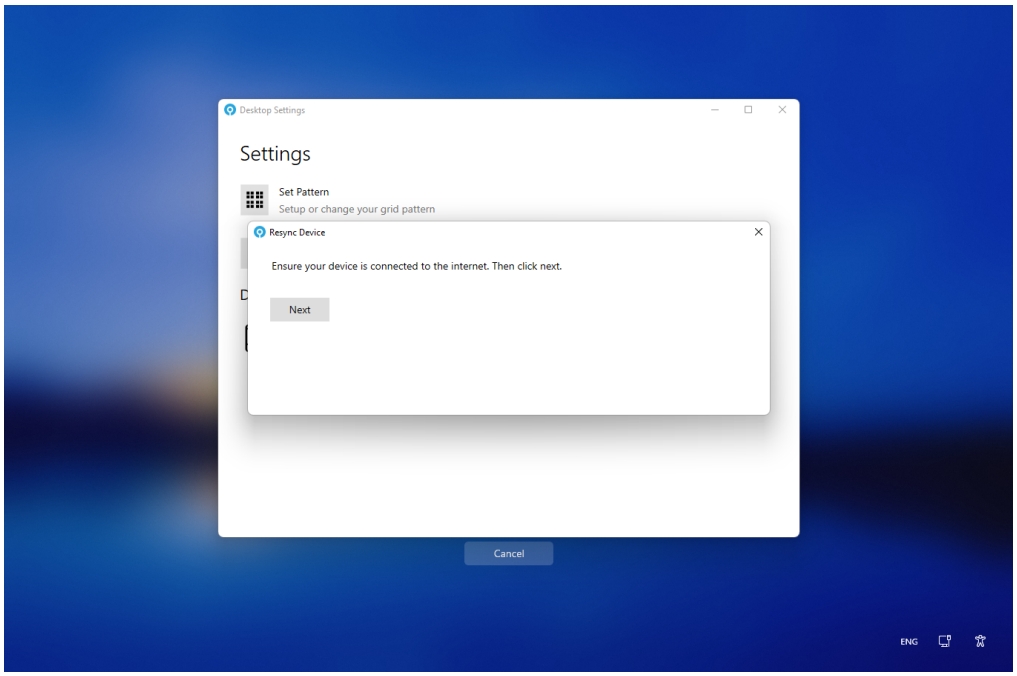
You can use the MyID Desktop Agent to resync an already paired device.

This can be useful if the user account settings have changes in a way that affects the MyID Authenticator App. For example, if the user is provisioned for a new authentication factor.

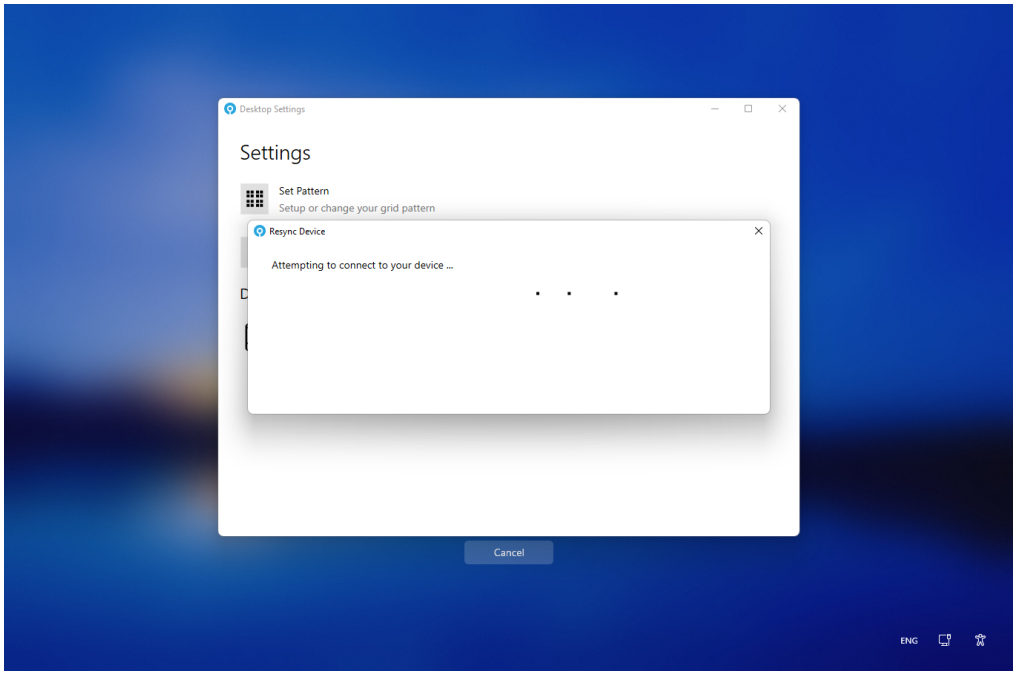
1. From the list of **Devices**, select the device to resync.



2. Click **Resync**.

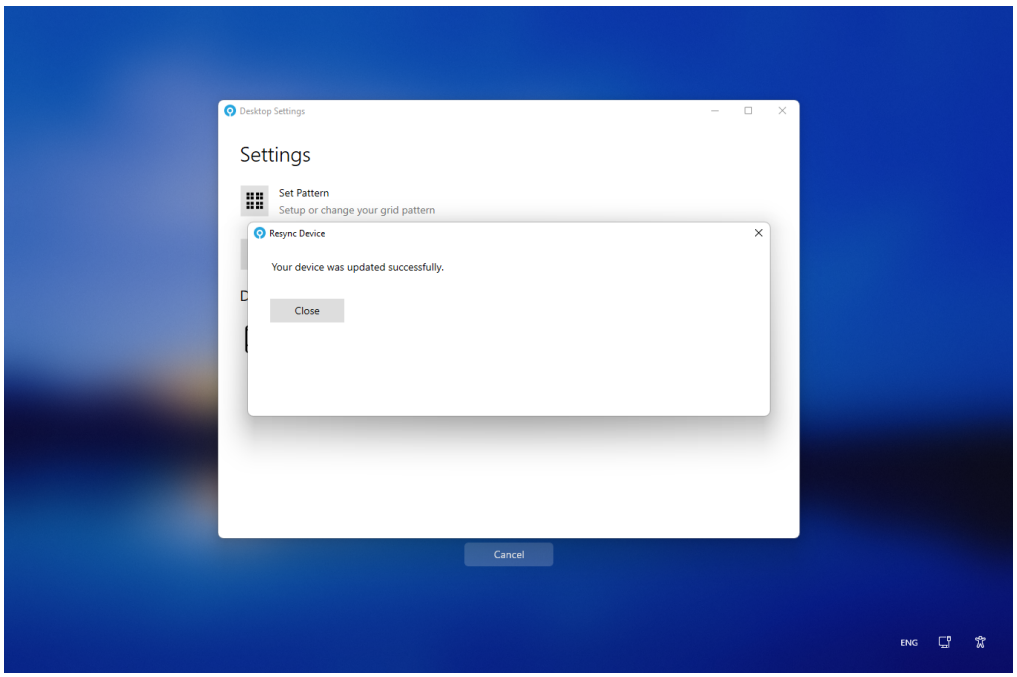


3. Click **Next**.



4. Check the MyID Authenticator App for any steps required.

   For example, you may be required to carry out biometric verification.



5. Click **Close**.

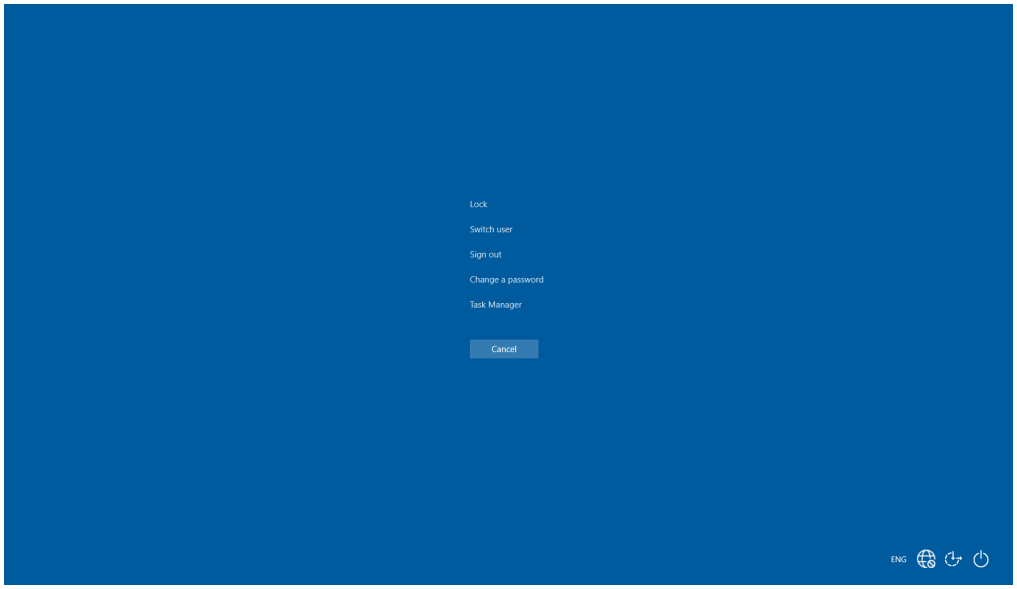
4.2.4 Passkey registration through the Security Key Credential Provider

You can provision Passkey Security devices through the MyID Desktop Agent Security Key credential provider.

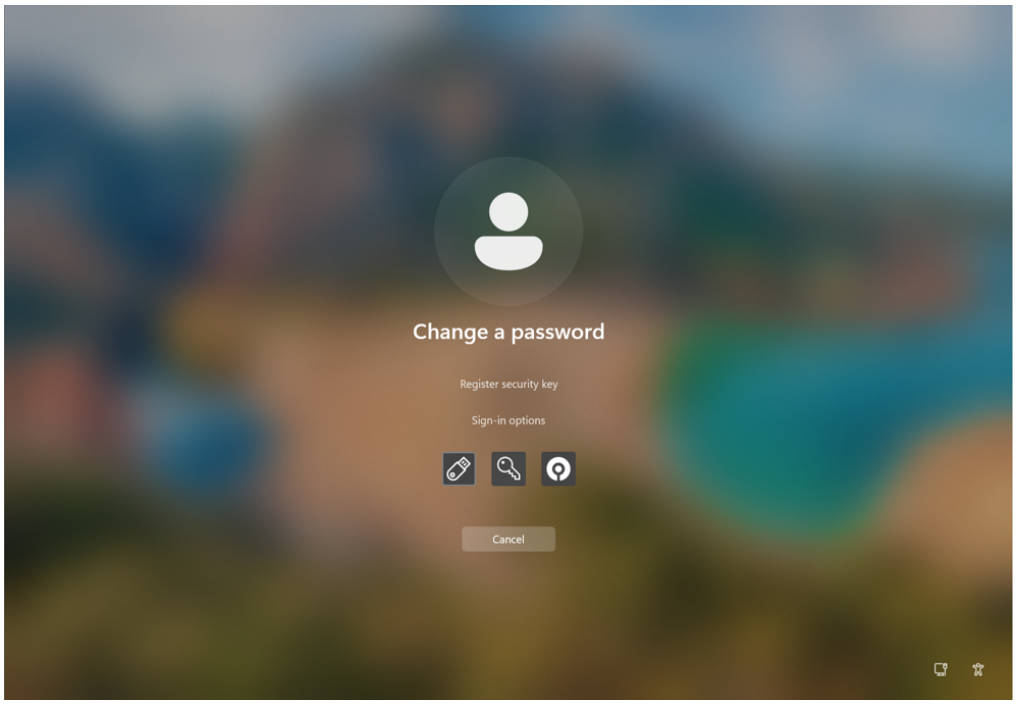
To enroll a Biometric Security Key and fingerprint.

1. Press CTRL + ALT + DEL.

   This shows the Windows security screen.

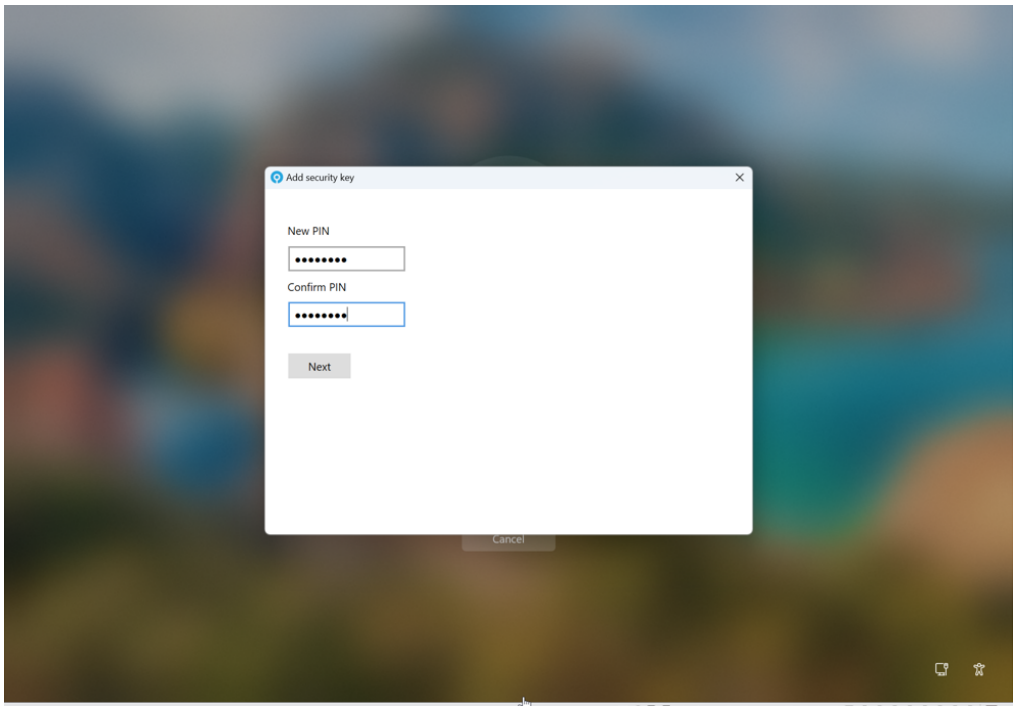


2. Click **Change a password**.



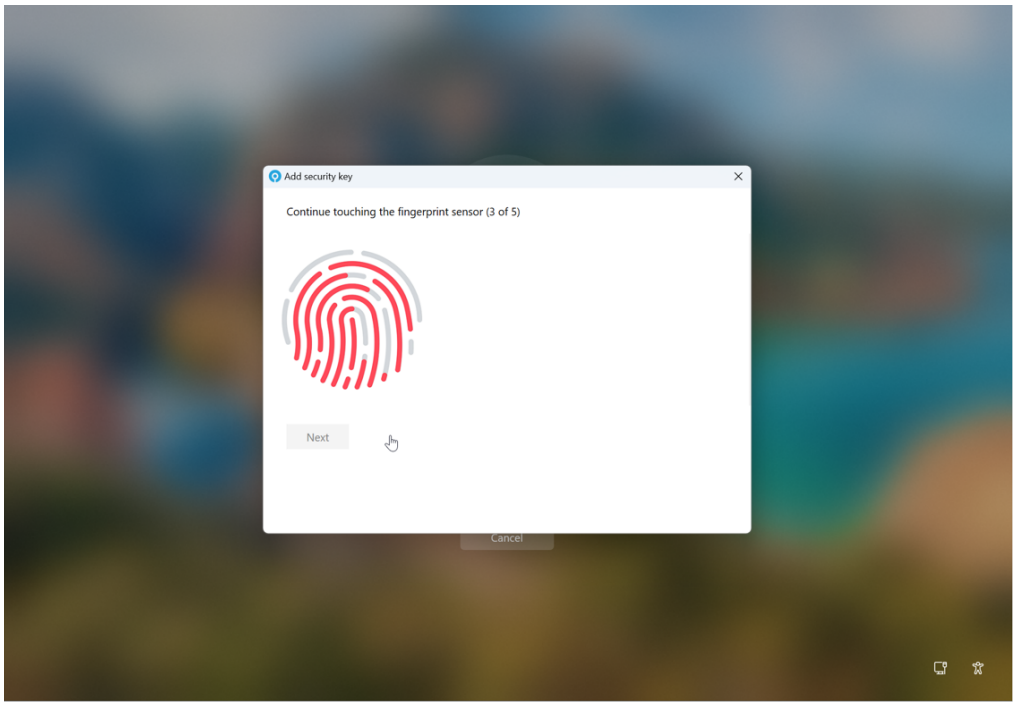
3. Click **Register security key**.
4. Enter a new PIN for the security key.

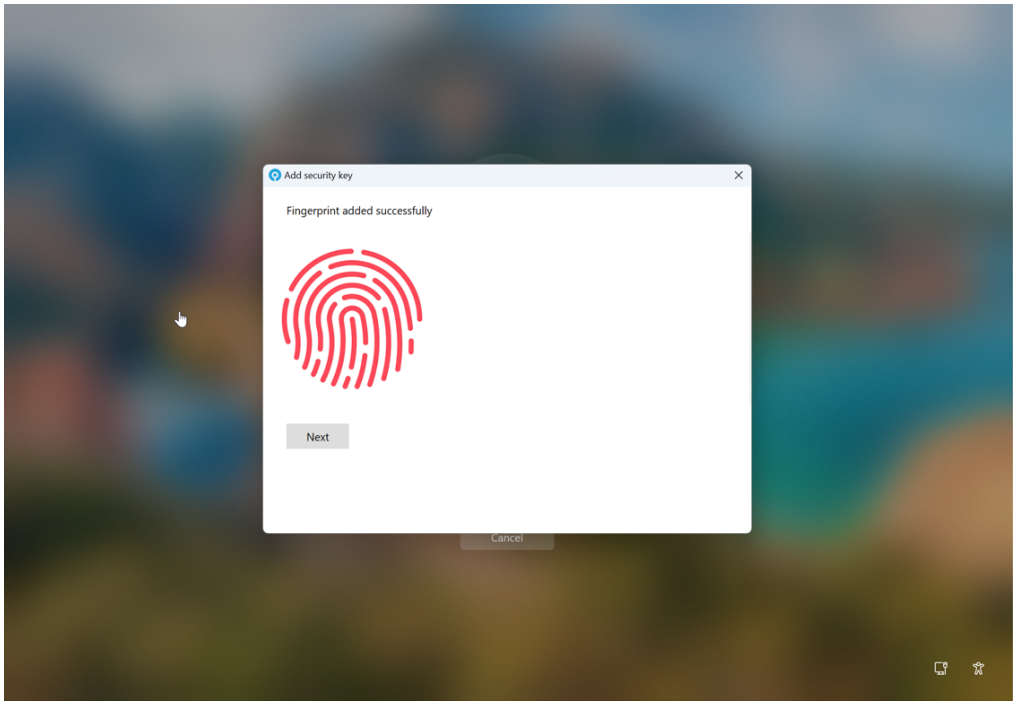
   You must repeat the same key to confirm it.



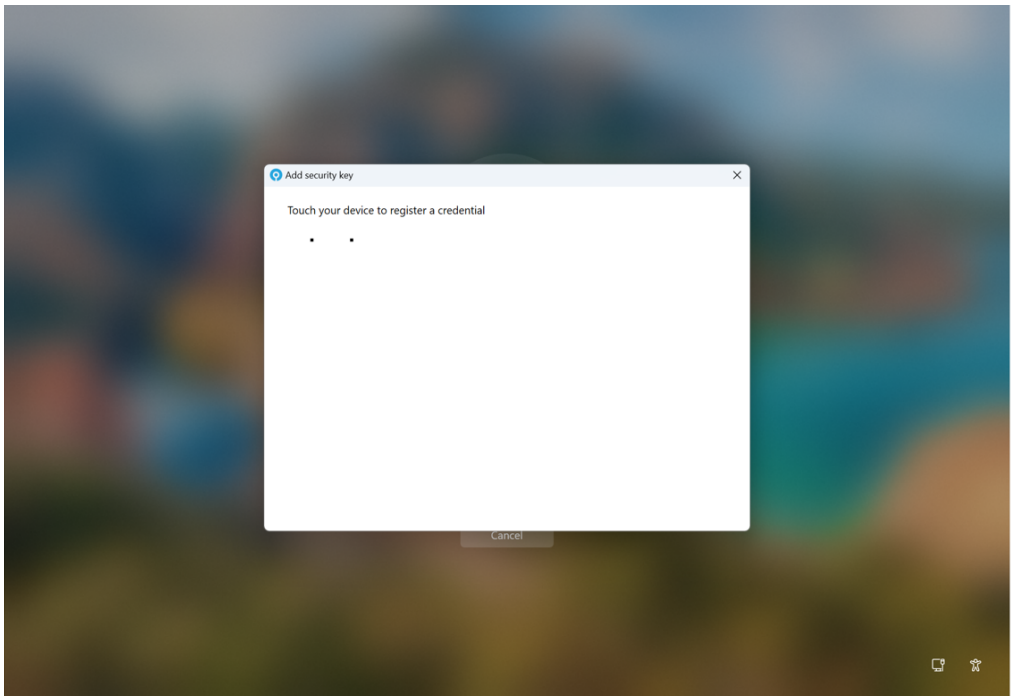
5. Click **Next**.

6. Touch the BIO key multiple times to register your fingerprint to the security key.



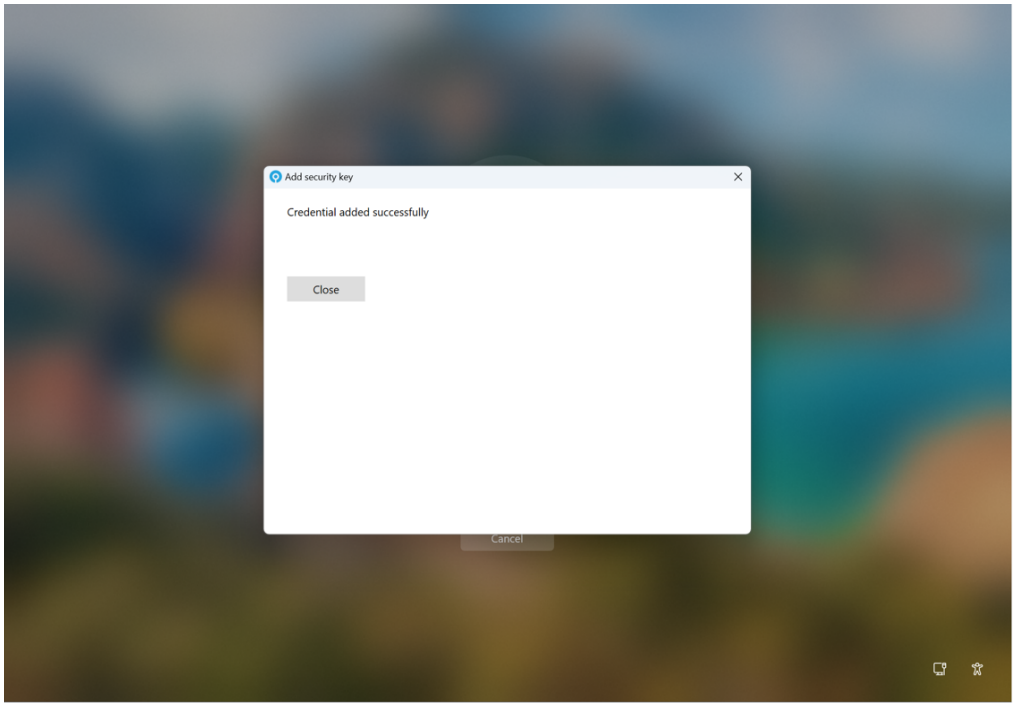


7. Click **Next**.



8. Touch the BIO Security key with your registered fingerprint.

   Your device is now fully registered.



9. Click **Close**.

4.2.5 Passkey registration using the MFA Credential Provider

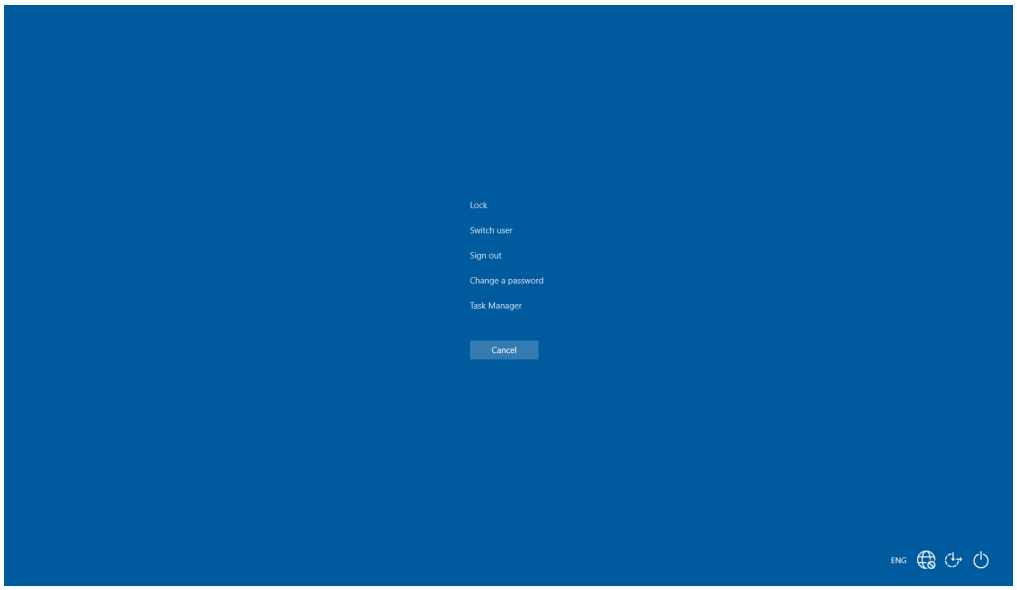
You can provision Passkey Security devices through the MyID Desktop Agent Security Key credential provider.

Note: The security key must be installed before you can enroll it.

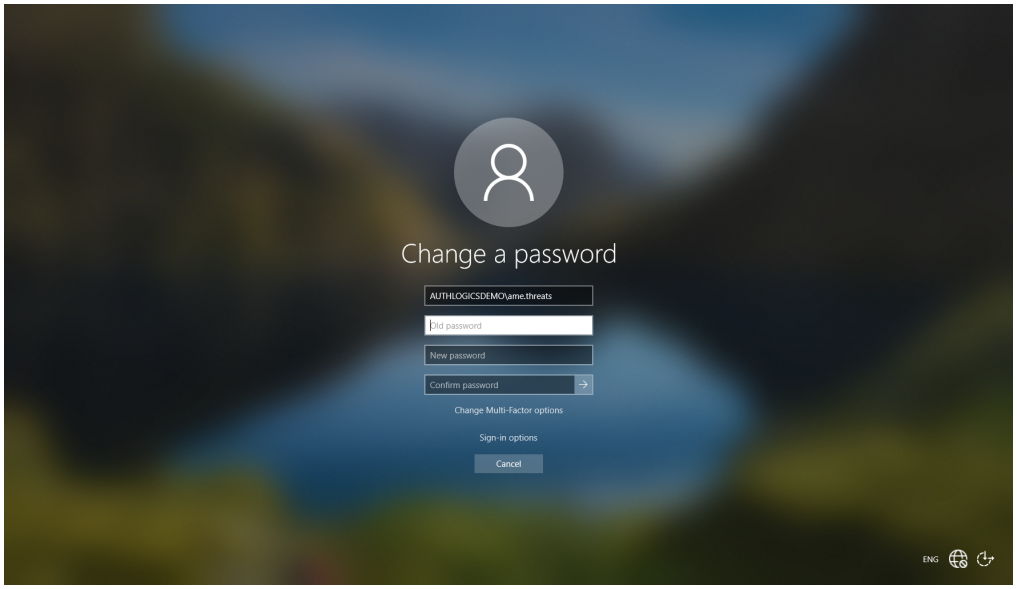
To enroll a Biometric Security Key and fingerprint:

1. Press CTRL + ALT + DEL.

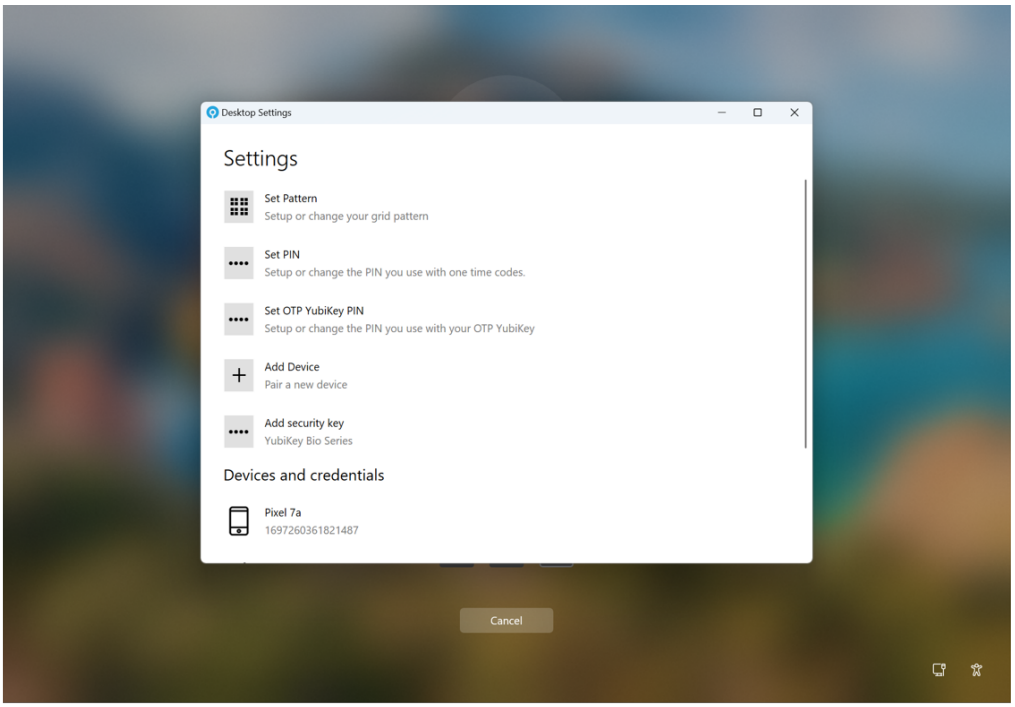
   This shows the Windows security screen.



2. Click **Change a password**.

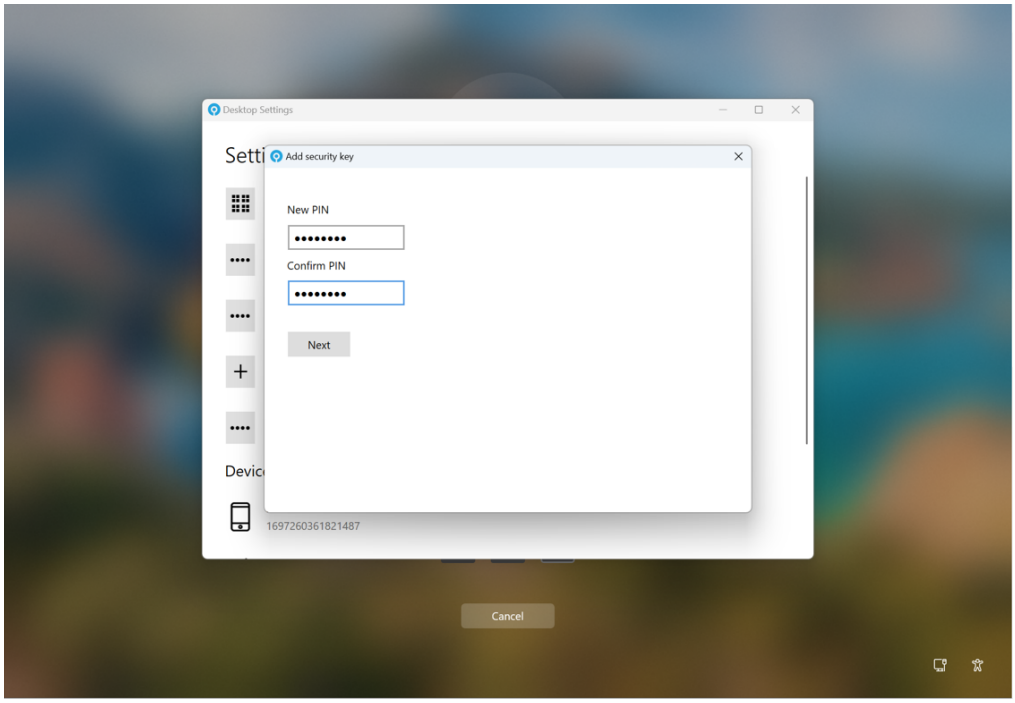


3. Click **Change Multi-Factor options**.



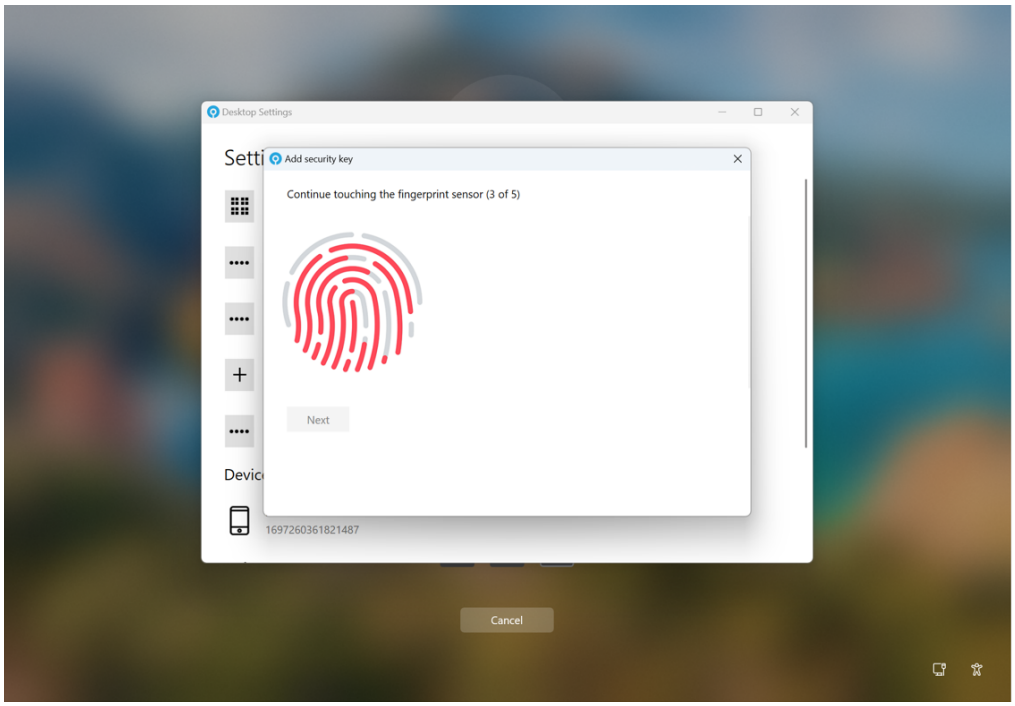
4. Click **Add security key**.
5. Enter a new PIN for the security key.

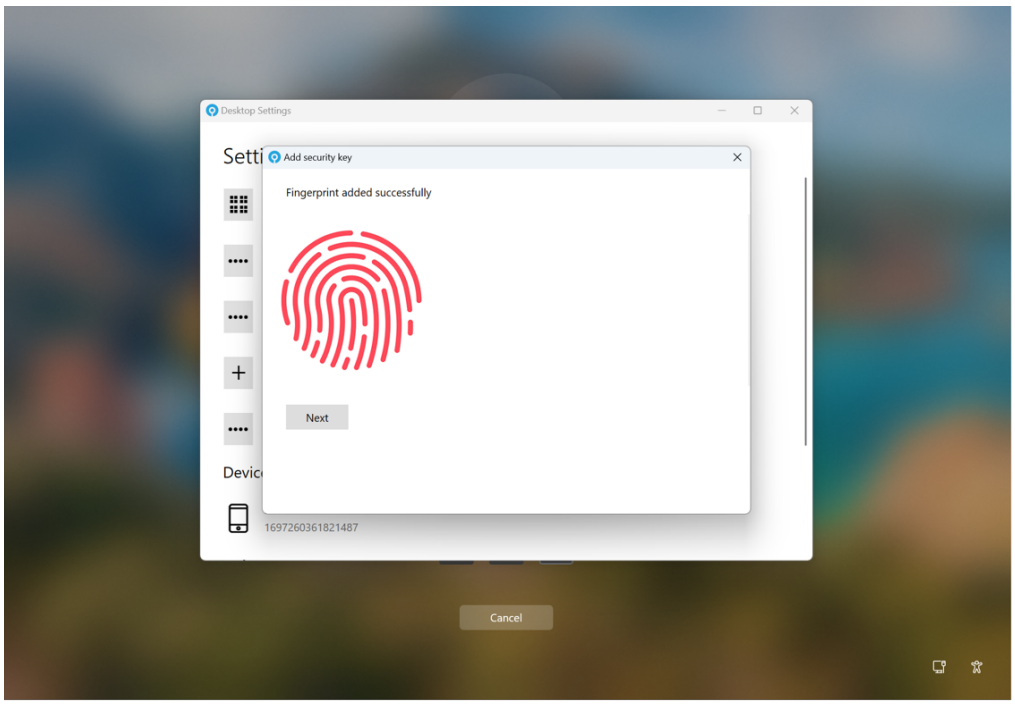
   You must repeat the same key to confirm it.



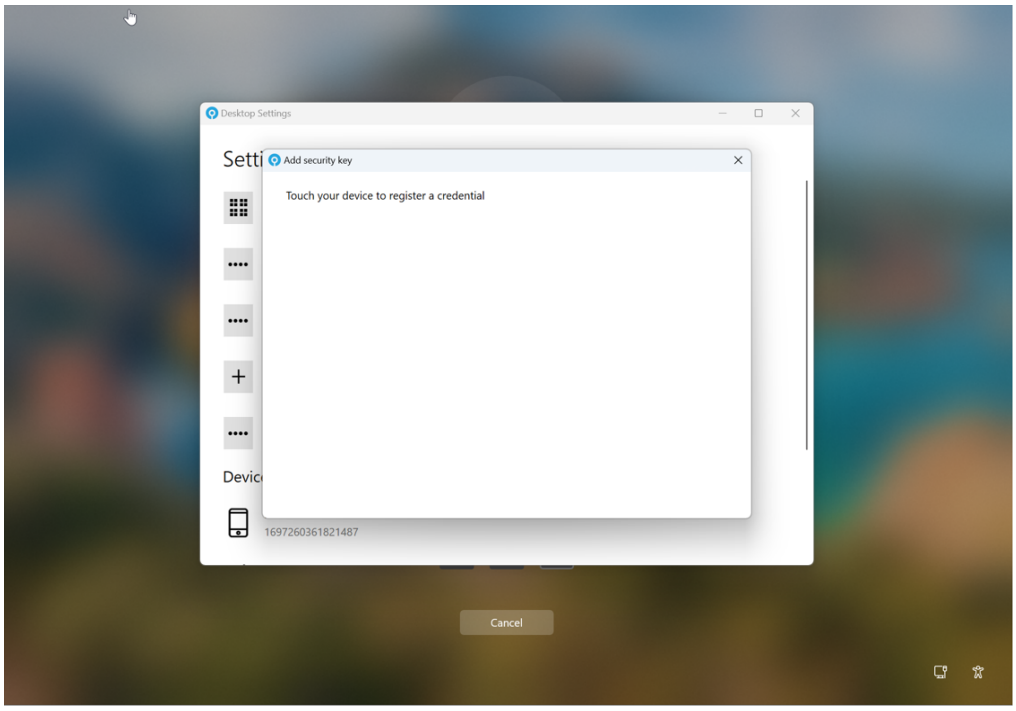
6. Click **Next**.

7. Touch the BIO key multiple times to register your fingerprint to the security key.



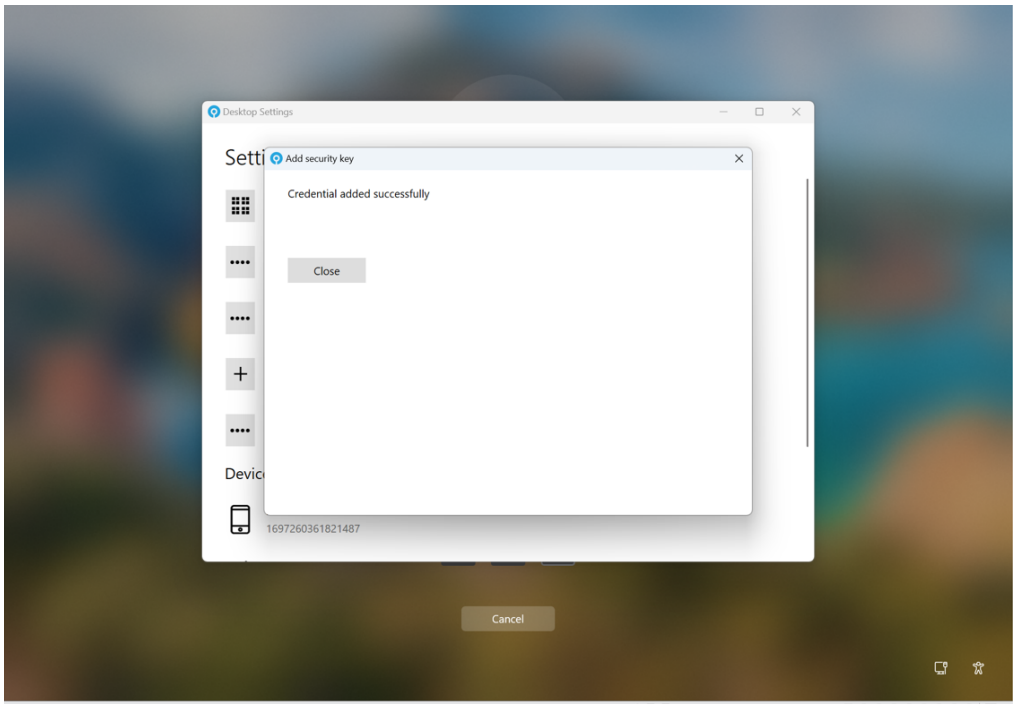


8. Click **Next**.



9. Touch the BIO Security key with your registered fingerprint.

   Your device is now fully registered.



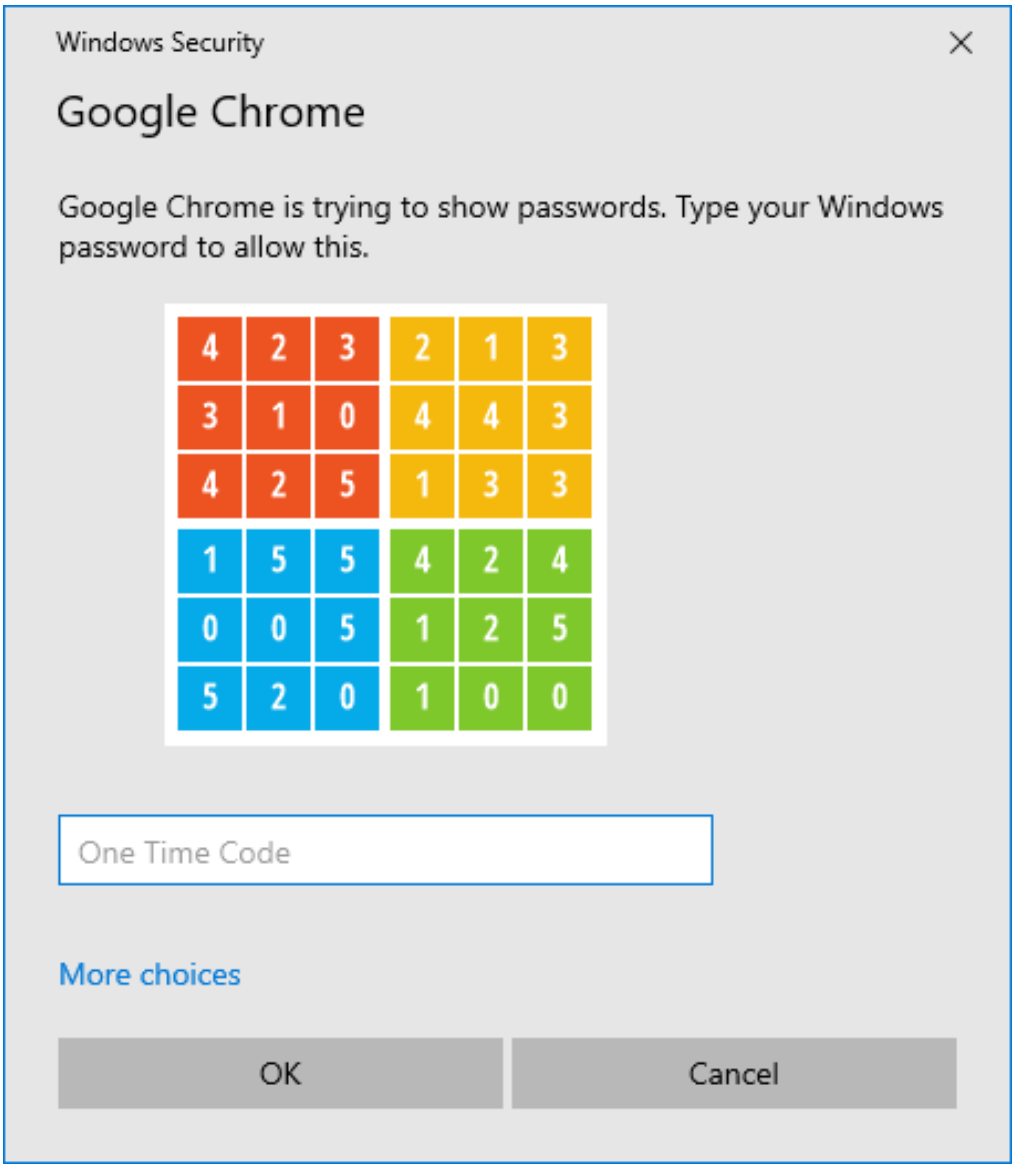
10. Click **Close**.

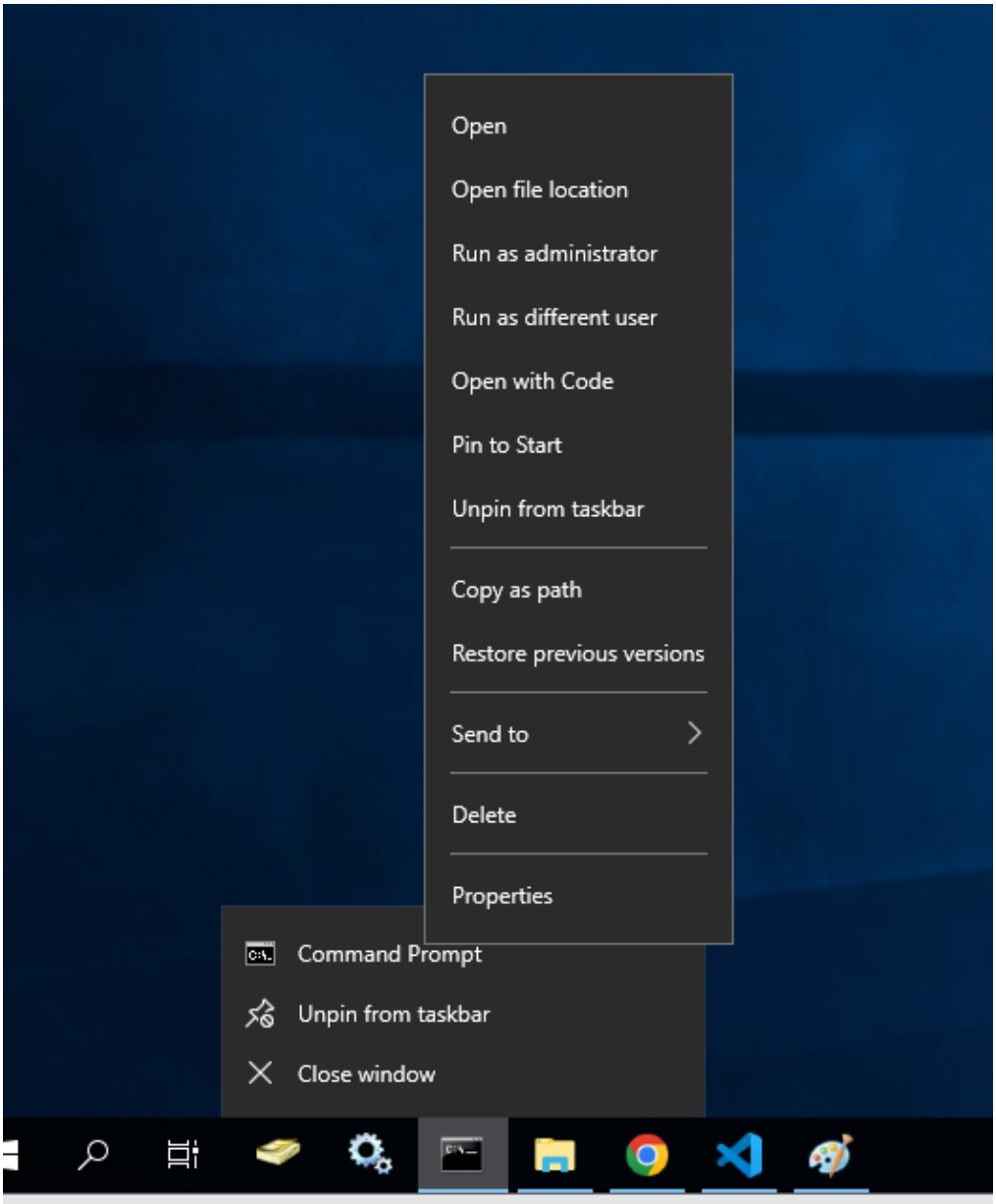
4.3 Using MFA for Windows credential prompting

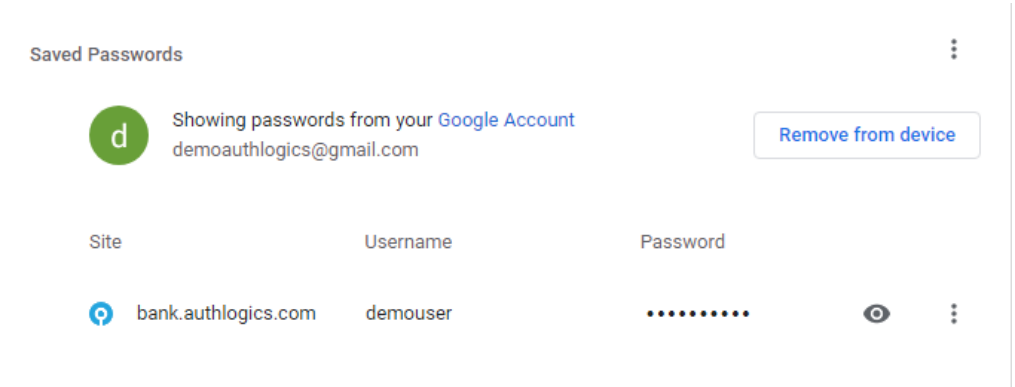
The MyID Desktop Agent can enforce MFA onto Windows credential prompting when operations you carry out tasks such as **Run as different user** and **Show password within Saved Passwords in a browser**.

MyID MFA options for the Credential Prompting operations (Deviceless and Passwordless) are configurable though Group Policy; you can disable this by enabling the **Disable MyID MFA for Windows Credential Prompting** GPO. For more information, see section *3.9.2*, *Security Settings*.

Some examples of this are:




Open
Open file location
Run as administrator
Run as different user
Open with Code
Pin to Start
Unpin from taskbar
Copy as path
Restore previous versions
Send to
Delete
Properties
Command Prompt
Unpin from taskbar
Close window


Saved Passwords
Showing passwords from your Google Account
demoauthlogics@gmail.com
Remove from device
Site
Username
Password
bank.authlogics.com
demouser

5 Browser reporting

The MyID Windows Desktop Agent has an optional browser extension that allows you to check the security of external passwords. It detects when you use a password in your browser and performs a known breached password check against the password.

If you use a known breached password in your browser, the extension triggers a Windows notification on your client PC, and an event log on the authentication server.

You can use the Browser Reports Monthly and External Vulnerable Password Reports charts on the Password Security dashboard in the Web Management Portal to visualize where your users are attempting to use breached passwords over time, and which users are repeatedly attempting to use breached passwords on which websites. For more information, see the *Password Security* section of the ***Web Management Portal User Guide***.

You can also use Browser Password Reports. This shows how many times each user has attempted to log in using a breached password. For more information, see the *Browser Password Reports* section of the ***Web Management Portal User Guide***.

The browser extension is compatible with Edge and Chrome.

Note: Browser reporting does hash checking on the client machine, which is supported only on Windows 10 clients and above.

This section contains information on the following:

- Setting up browser reporting for Edge.

  See section *5.1*, *Deploying browser reporting for Edge*.
- Setting up browser reporting for Chrome.

  See section *5.2*, *Deploying browser reporting for Chrome*.
- Updating the browser reporting extension.

  See section *5.3*, *Updating the browser reporting extension*.
- How to use the browser reporting extension.

  See section *5.4*, *Using browser reporting*.
- The security of the browser reporting extension.

  See section *5.5*, *Browser reporting security*.

5.1 Deploying browser reporting for Edge

Before deploying browser reporting on client machines, you must acquire the ID of the browser reporting extension from the MyID Application Server:

1. Open the browser reporting `update.xml` file.

   By default, this is in the following location:

   ```
   C:/Program Files/Authlogics Windows Desktop
   Agent/Extensions/BrowserReporting
   ```

2. Note the `appid`.

   This is the ID of the browser reporting extension.

3. Download the Edge ADMX files.

   These are available from the following location:

   www.microsoft.com/en-gb/edge/business/download?cs=357927189&form=MA13FJ

4. Unzip the Edge ADMX files.

5. Within the unzipped folder, navigate to the `MicrosoftEdgePolicyTemplates\windows\admx` folder.

6. Copy the `msedge.admx`, `msedgeupdate.admx`, and `msedgewebreview.admx` files to the following location:

   ```
   C:\Windows\PolicyDefinitions\
   ```

7. Navigate to the folder that contains your language from the `MicrosoftEdgePolicyTemplates\windows\admx` folder.

   For example, the `en-US` folder.

8. Copy the `msedge.adml`, `msedgeupdate.adml` and `msedgewebreview.adml`files to the equivalent folder within `C:\Windows\PolicyDefinitions\`

   For example:

   ```
   C:\Windows\PolicyDefinitions\en-US
   ```

9. Open the Group Policy Editor.

10. Navigate to **Computer Configuration** > **Policies** > **Administrative Templates** > **Microsoft Edge** > **Extensions**.

11. Enable the **Control which extensions are installed silently** setting.

12. Click **Show**.

13. Add a new **Value** with the following format:

    ```
    <extension ID>;<update URL>
    ```

    Where:

    - `<extension ID>` is the Extension ID that you acquired from your MyID Application Server.
    - `<update URL>` is the location of the browser reporting `update.xml` file.

    For example:

    ```
    oehmegijabaecfgdepjmkelbpmogdggg;file://C:/Program Files/Authlogics Windows Desktop Agent/Extensions/BrowserReporting/update.xml
    ```

    Note: The client computer must be able to access the update URL.

14. Click **OK**.

15. Ensure that each machine refreshes its Group Policy Objects.

    To do this, open a command prompt and run the following on each machine:

    ```
    gpupdate /force
    ```

16. Restart any currently running browser sessions.

17. You can check that the policy is correctly set by opening Edge and going to the following page:

    ```
    edge://policy
    ```

    You should see your policy settings under **Microsoft Edge Policies**.

18. You can check the extension is installed by opening Edge and going to the following page:

    ```
    edge://extensions
    ```

    You should see MyID Browser Reporting under **Installed extensions**.

5.2 Deploying browser reporting for Chrome

You can deploy the browser reporting extension for your users through group policy.

On the MyID Application Server:

1. Open the browser reporting `update.xml` file.

   By default, this is in the following location:

   ```
   C:/Program Files/Authlogics Windows Desktop Agent/Extensions/BrowserReporting
   ```

2. Note the `appid`.

   This is the ID of the browser reporting extension.

3. Download the Chrome ADMX files.

   These are available from the following location:

   chromeenterprise.google/download/?modal-id=download-chrome#management-download

4. Unzip the Chrome ADMX files.

5. Within the unzipped folder, navigate to the `policy_templates\windows\admx\` folder.

6. Copy the `chrome.admx` and `google.admx` files to the following location:

   `C:\Windows\PolicyDefinitions\`

7. Navigate to the folder that contains your language from the `policy_templates\windows\admx\` folder.

   For example, the `en-US` folder.

8. Copy the `chrome.adml` and `google.adml` files to the equivalent folder within `C:\Windows\PolicyDefinitions\`

   For example:

   `C:\Windows\PolicyDefinitions\en-US`

9. Open the Group Policy Editor.

10. Navigate to **Computer Configuration** > **Policies** > **Administrative Templates** > **Google** > **Google Chrome** > **Extensions**.

11. Enable the **Configure the list of force-installed apps and extensions** setting.

12. Click **Show**.

13. Add a new **Value** with the following format:

    `<extension ID>;<update URL>`

    Where:

    - `<extension ID>` is the extension ID that you acquired from your MyID Application Server.
    - `<update URL>` is the location of the browser reporting `update.xml` file.

    For example:

    ```
    oehmegijabaecfgdepjmkelbpmogdggg;file://C:/Program Files/Authlogics
    Windows Desktop Agent/Extensions/BrowserReporting/update.xml
    ```

    Note: The client computer must be able to access the update URL.

14. Click **OK**.
15. Ensure that each machine refreshes its Group Policy Objects.

    To do this, open a command prompt and run the following on each machine:

    ```
    gpupdate /force
    ```

16. Restart any currently running browser sessions.
17. You can check that the policy is correctly set by opening Chrome and going to the following page:

    ```
    chrome://policy
    ```

    Your policy settings should be visible under **Chrome Policies**.

18. You can check the extension is installed by opening Chrome and going to the following page:

    ```
    chrome://extensions
    ```

    You should see MyID Browser Reporting.

5.3 Updating the browser reporting extension

If changes have been made to the browser reporting extension since the previous release of MyID MFA and PSM, updating the Windows Desktop Agent may automatically update the browser reporting extension.

However, if updating the Windows Desktop Agent has not updated the browser reporting extension on your browser, you can force the update:

- To update the browser reporting extension for Edge, see section *5.3.1*, *Updating browser reporting in Edge*.
- To update the browser reporting extension for Chrome, see section *5.3.2*, *Updating browser reporting in Chrome*.

5.3.1 Updating browser reporting in Edge

If the browser reporting extension does not automatically update for Edge:

1. If you previously enabled the **Configure extension management settings** group policy for Edge:
   - If the policy has values relating to other extensions, remove the value relating to browser reporting and click **OK**.
   - If the policy does not have values relating to other extensions, disable the policy and click **OK**.
2. Copy the **Control which extensions are installed silently** value and save it.
3. Disable the **Control which extensions are installed silently** policy.
4. Ensure that each machine refreshes its Group Policy Objects.

   To do this, open a command prompt and run the following on each machine:

   ```
   gpupdate /force
   ```
5. Enable the **Control which extensions are installed silently** policy, and set the value to the value that you copied earlier.
6. Ensure that each machine refreshes its Group Policy Objects.

   To do this, open a command prompt and run the following on each machine:

   ```
   gpupdate /force
   ```
7. Restart any currently running browser sessions.

5.3.2 Updating browser reporting in Chrome

If the browser reporting extension does not automatically update for Chrome:

1. If you previously enabled the **Configure extension, app, and user script install source** group policy for Chrome:
   - If the policy has values relating to other extensions, remove the value relating to browser reporting and click **OK**.
   - If the policy does not have values relating to other extensions, disable the policy and click **OK**.
2. Copy the **Configure the list of force-installed apps and extensions** value and save it.
3. Disable the **Configure the list of force-installed apps and extensions** policy.
4. Ensure that each machine refreshes its Group Policy Objects.

   To do this, open a command prompt and run the following on each machine:

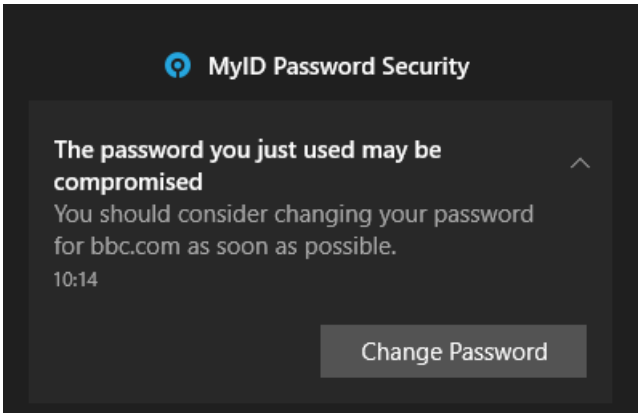
   ```
   gpupdate /force
   ```
5. Enable the **Configure the list of force-installed apps and extensions** policy, and set the value to the value that you copied earlier.
6. Ensure that each machine refreshes its Group Policy Objects.

   To do this, open a command prompt and run the following on each machine:

   ```
   gpupdate /force
   ```
7. Restart any currently running browser sessions.

5.4 Using browser reporting

Once browser reporting is deployed on your system, you can use your computer as normal. When you use a compromised password in a browser that is set up for browser reporting, you get a Windows notification with the following format:



When you get this notification, click the **Change Password** button and reset the compromised password. If the web page that allows you to change the password for that website is known, the button links to that page directly; otherwise, the button links to the homepage of the website on which you used the compromised password.

Administrators can see that you have used a breached password, and the website on which you have used a breached password, but they cannot see the password itself.

5.5 Browser reporting security

The browser reporting extension hashes the password and then sends the first portion of the hashed password to the MyID Authentication Server, where it is compared against the first portions of the hashed passwords in the most expansive, accessible configured Password Breach Database.

When there are matches, a large portion of the hashes of the matches are sent back to the user's client, where they are locally compared to a larger portion of hash of the user's password. If there is a match, your MyID Authentication Server is informed that the user is attempting to use a breached password, and the website on which the user is using a breached password.

Note: Hash checking is supported only on Windows 10 clients and above.

No passwords are sent unsecured.

The user's full password is never sent to the MyID Authentication Server – no more than six characters of the hash of the user's password are sent to the MyID Authentication Server.

The user's password is handled in a way that preserves k-anonymity.

6 Network Level Authentication (NLA) and Remote Desktop

MyID Windows Desktop Agent is designed to work with Windows Terminal Services and Remote Desktop connections. The login process looks and works the same as when logging onto a physical PC directly, except using the Remote Desktop client.

Network Level Authentication is an authentication method that you can use to enhance RD Session Host server security by requiring that the user be authenticated to the RD Session Host server before a session is created.

Network Level Authentication completes user authentication before you establish a remote desktop connection and the logon screen appears. This is a more secure authentication method that can help protect the remote computer from malicious users and malicious software. The advantages of Network Level Authentication are:

- It requires fewer remote computer resources initially.

  The remote computer uses a limited number of resources before authenticating the user, rather than starting a full remote desktop connection as in previous versions.
- It can help provide better security by reducing the risk of denial-of-service attacks.

Source: ***technet.microsoft.com/en-gb/library/cc732713.aspx***

6.1 Issues with NLA and Multi-Factor Authentication

Microsoft does not provide any third-party support in Windows for custom Security Support Providers (SSP) that can be used with NLA. Therefore, NLA is compatible only through built-in Windows authentication routines (for example passwords and smart cards) not with Multi-Factor Authentication.

You can use the MyID Windows Desktop Agent with NLA enabled; however, the user may experience a *double logon* scenario:

1. The user is challenged for username and password through the RDP client (used for NLA).
2. The user is challenged for username, optional password, and OTP through MyID Windows Desktop Agent within the RDP screen.

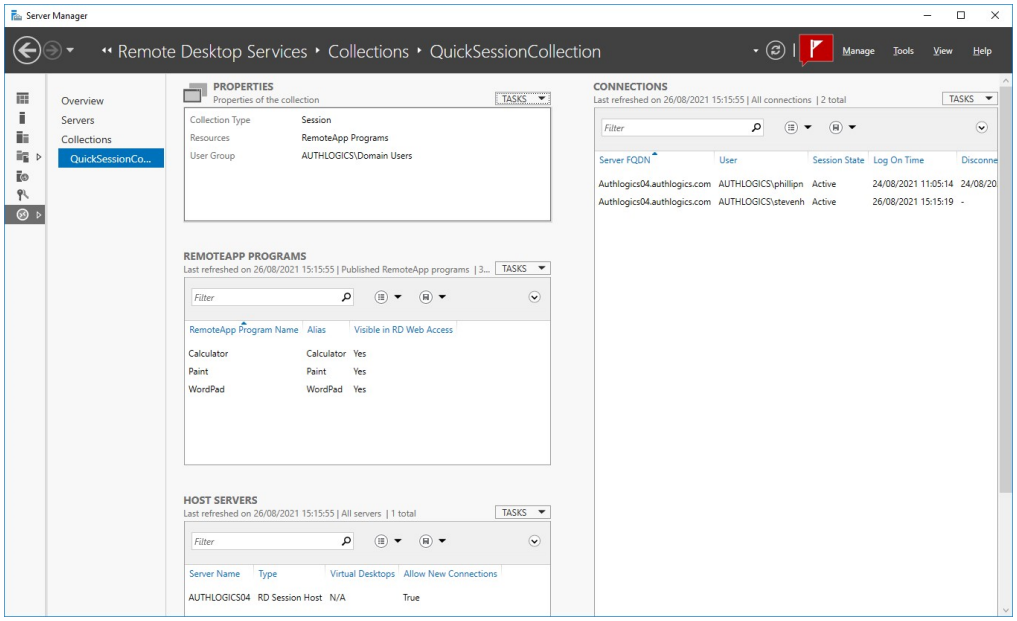
You can mitigate the double logon by either:

- If NLA is Enabled: Caching the user password within the remote desktop client.
- If NLA is Disabled: Removing the logon prompt from the RDP client through a custom .RDP file or a third-party RDP client that does not use NLA.

6.2 Disabling NLA on Windows Server 2016

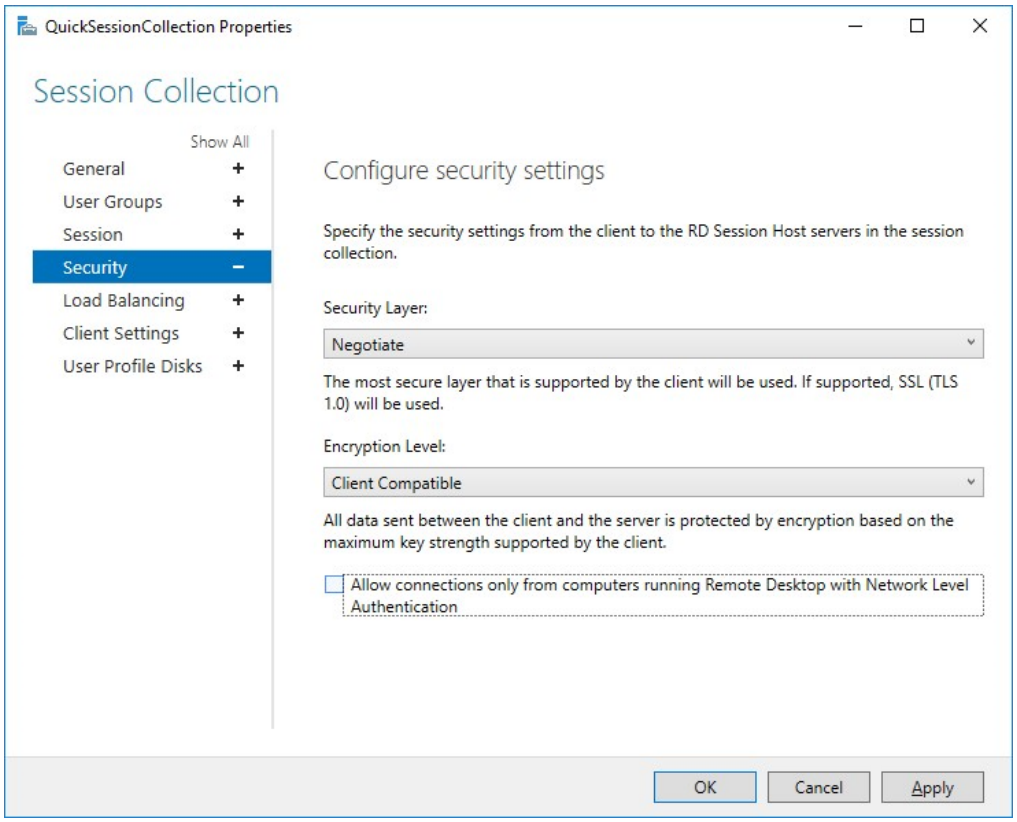
The steps required to disable NLA on Windows server vary depending on the OS version. On Windows Server 2016, you can:

1. Open Server Manager.
2. Select **Remote Desktop Services**.
3. Select the active **Session Collection**.



4. Click **Tasks**, and select **Edit Properties**.

5. Select **Security** from the list.



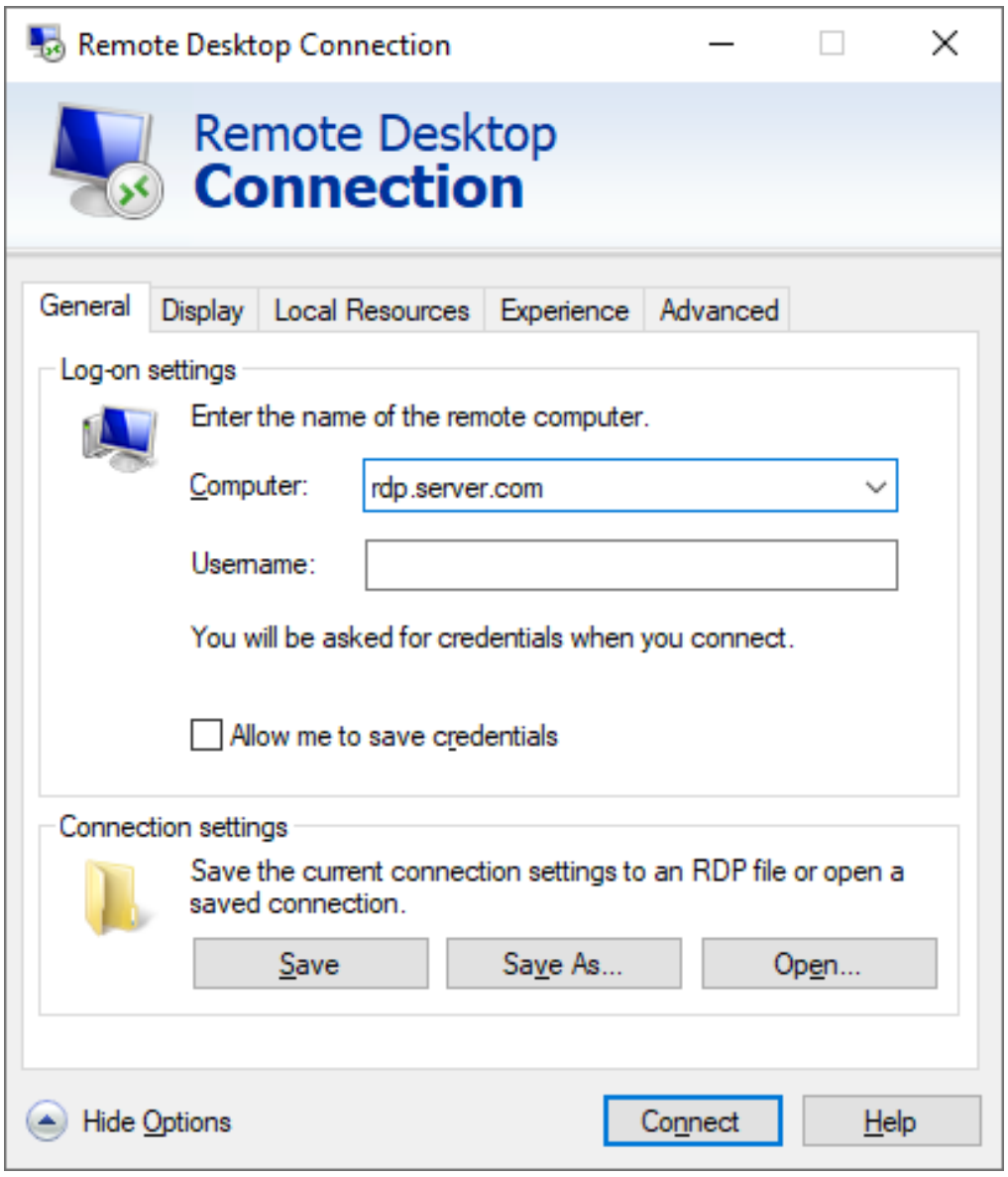
6. Untick **Allow connections only from computers running Remote Desktop with Network Level Authentication**.
7. Click **Ok**.

   Server Manager closes.

6.3 Disabling NLA on the RDP Client

Note: NLA must be disabled, or at least not required, on the server before you disable NLA on the client otherwise connections are rejected.

1. Create an RDP connection on a client with the required connection information.



2. Click **Save As**.

   This saves the RDP configuration to a file.

3. Edit the RDP file in Notepad and add the following line to the file:

   ```
   enablecredsspsupport:i:0
   ```

4. Save and close the RDP file in Notepad.

   You can now use the new RDP configuration file to connect to the server without NLA.

6.4 Disabling NLA on the macOS client

Note: NLA must be disabled, or at least not required, on the server before you disable NLA on the client otherwise connections are rejected.

macOS Remote Desktop clients prior to version 10.2.2 do not support NLA; NLA is off by default.

7 Agent Architecture

The architecture of the MyID Windows Desktop Agent is made up of the following key components:

- A MyID Windows Desktop Agent Windows Service which caters for:
- Password policy processing.
- Offline logons.
- Caching and synchronizing with AD when online.
- Deviceless OTP challenge generation.
- Processing AD Group Policy settings.
- A Windows Credential Provider which plugs into the Windows logon screen and communicates with the MyID Windows Desktop Agent Service.
- An AES256 bit encrypted cache database.

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 Windows Desktop Agent. You should, typically, change them only if instructed by Intercede support.

You can carry out the following:

- Allow duplicate computer or Active Directory domain names.

  See section *8.1*, *Allowing duplicate names*.

- Log diagnostic messages.

  See section *8.2*, *Diagnostics logging*.

8.1 Allowing duplicate names

If you are a Managed Service Provider with a centrally hosted MyID MFA and PSM server, you may need to cater for duplicate names:

- You may need to support duplicate Active Directory domain names if two organizations use the same domain name.
- You may need to support multiple workgroup based computers with the same computer name.

The Windows Desktop agent supports multiple domain and computer names by allowing you to substitute the names with a GUID, an ID that is guaranteed to be unique.

8.1.1 Allowing duplicate Active Directory domain names

To allow duplicate Active Directory domain names, create the following registry value on the client PC:

```
HKLM\SOFTWARE\Policies\Authlogics\Windows Desktop Agent\MspEnableUniqueDomainId
```

Accepted values:

- `0` – disabled.
- `1` – enabled.

When you enable this value, the Windows Desktop Agent associates each Active Directory domain name with a unique GUID, and replaces the Active Directory domain name with the relevant GUID when sending logon requests to the server. The Windows Desktop Agent obtains the GUID from the Active Directory configuration automatically.

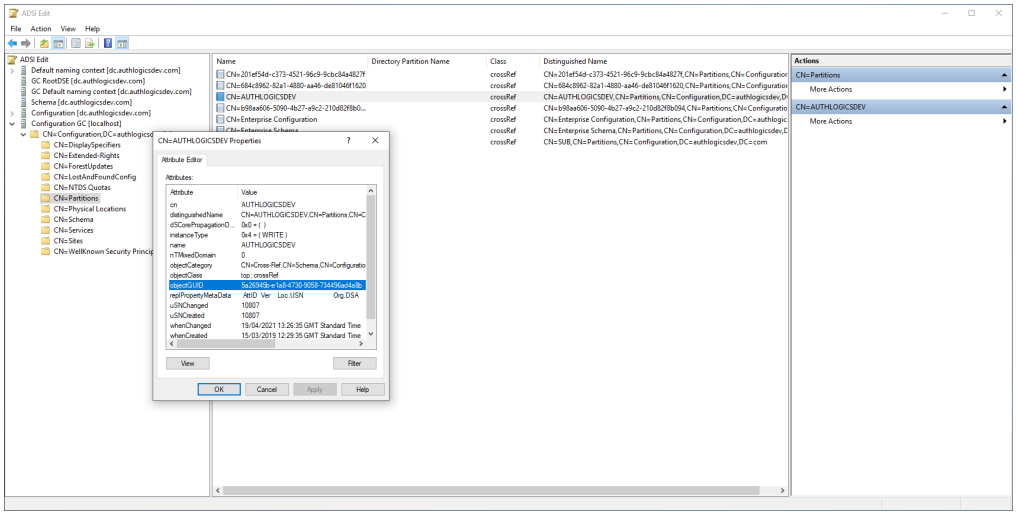
Note: This setting is in the `Policies` section of the registry, but is not visible in the Group Policy Template.

To complete the setup of allowing duplicate Active Directory domain names, you must also:

1. Get the GUID from the Active Directory Configuration Partition.

   This is available in all Global Catalog servers and is named:

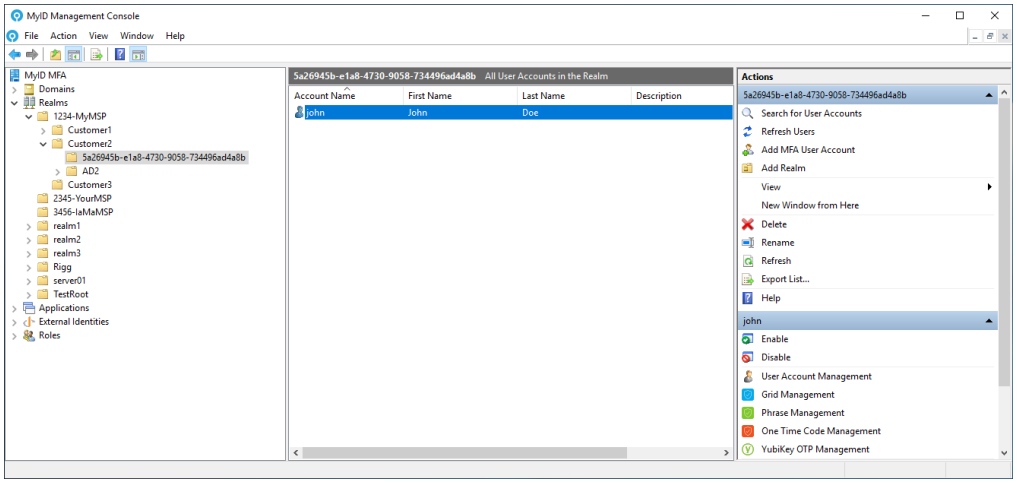
   `objectGUID`



2. On the authentication server, in the MyID Management console:

   a. Create a realm with the name of the Active Directory domain name GUID.

   b. Within the new realm, create the external users associated with the computer associated with that Active Directory domain name GUID.



8.1.2 Allowing duplicate computer names

To allow duplicate computer names, create the following registry keys on the client PC:

- `HKLM\SOFTWARE\Policies\Authlogics\Windows Desktop Agent\MspUniqueIdKeyName`

  Accepted value:

  - A path to the registry key where you have stored a unique GUID.

- `HKLM\SOFTWARE\Policies\Authlogics\Windows Desktop Agent\MspUniqueIdKeyValue`

  Accepted value:

  - The name of the registry value within the above key where you have stored a unique GUID.

Note: These settings are in the `Policies` section of the registry, but are not visible in the Group Policy Template.

For example, if you have stored a GUID in the following registry value:

`HKEY_LOCAL_MACHINE\SOFTWARE\SoftwareName\Subfolder\DeviceGuid`

Set the following key values:

- `MspUniqueIdKeyName` = `"HKEY_LOCAL_MACHINE\SOFTWARE\SoftwareName\Subfolder"`
- `MspUniqueIdKeyValue` = `"DeviceGuid"`

When enabled, the Windows Desktop Agent associates the name of each computer with the unique GUID provided by the `MspUniqueIdKeyName` and `MspUniqueIdKeyValue` registry settings, and replaces the computer's name with this GUID when sending logon requests to the server.

For example, if you have a PC with the name `mypc`, with users `jane` and `susan`, if you set the following in the PC registry:

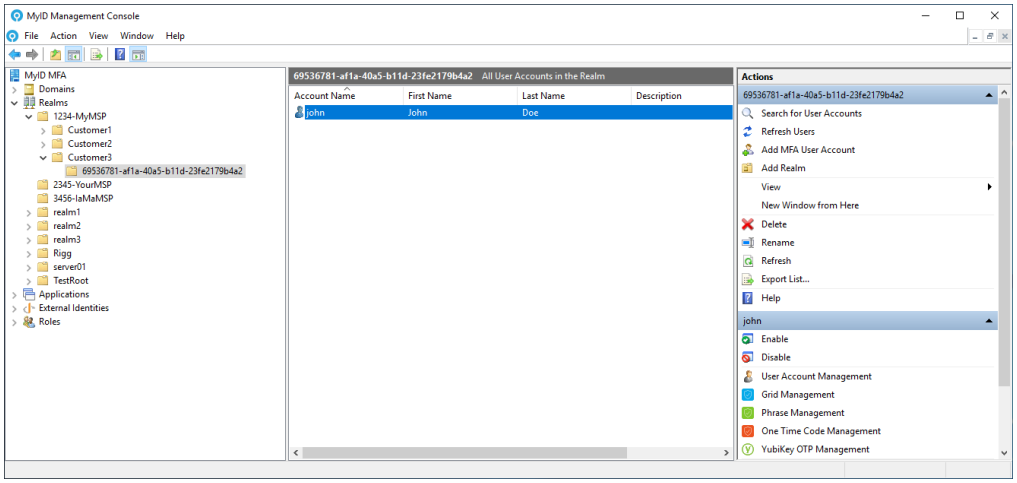
```
[HKEY_LOCAL_MACHINE\SOFTWARE\SoftwareName\Subfolder]
"DeviceGuid "="723ea5f0-e796-4507-9234-ac35d9bc37e0"
```

when the Windows Desktop Agent sends logon requests to the server, it makes the following substitutions:

- `mypc\jane` becomes `723ea5f0-e796-4507-9234-ac35d9bc37e0\jane`
- `mypc\susan` becomes `723ea5f0-e796-4507-9234-ac35d9bc37e0\susan`

To complete the setup of allowing duplicate computer names, in the MyID Management console on the authentication server, you must also:

1. Create a realm with the name of the computer name GUID.
2. Within the new realm, create the external users associated with the computer associated with that computer name GUID.



8.2 Diagnostics logging

You can control the diagnostics logging using the Windows registry.

8.2.1 Enabling logging

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

`HKLM\SOFTWARE\Authlogics\Windows Desktop Agent\LoggingEnabled`

The default value is `1`.

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.

8.2.2 Setting the logging location

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

`HKLM\SOFTWARE\Authlogics\Windows Desktop Agent\LoggingFolder`

The default value is:

`C:\Program Files\Authlogics Windows Desktop Agent\Log\`

Accepted values:

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

8.2.3 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\Windows Desktop 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 *8.2.4*, *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\Windows Desktop Agent\LoggingFileCountLimit`

The default value is `5` – after five intervals, the logs from the first interval are deleted.

Accepted values:

- A number of intervals.

8.2.4 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:

```
AuthlogicsAuthenticationServerManager-20250325-0001.log
```

```
AuthlogicsAuthenticationServerManager-20250325-0002.log
```

or for year interval logs:

```
AuthlogicsAuthenticationServerManager-2025-0001.log
```

```
AuthlogicsAuthenticationServerManager-2025-0002.log
```

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

```
HKLM\SOFTWARE\Authlogics\Windows Desktop 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.

8.2.5 Example of rolling logs

With the default values of:

- `LoggingRollingIntervalType` – 3 (Day intervals)
- `LoggingFileCountLimit` – 5 (five days)
- `LoggingRollingSizeLimit` – 20 (MB)

Old log files are deleted after five days.

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

```
AuthlogicsAuthenticationServerManager-20250325-0001.log
AuthlogicsAuthenticationServerManager-20250325-0002.log
AuthlogicsAuthenticationServerManager-20250326-0001.log
AuthlogicsAuthenticationServerManager-20250326-0002.log
AuthlogicsAuthenticationServerManager-20250326-0003.log
AuthlogicsAuthenticationServerManager-20250327-0001.log
AuthlogicsAuthenticationServerManager-20250327-0002.log
AuthlogicsAuthenticationServerManager-20250328-0001.log
AuthlogicsAuthenticationServerManager-20250328-0002.log
AuthlogicsAuthenticationServerManager-20250328-0003.log
AuthlogicsAuthenticationServerManager-20250329-0001.log
AuthlogicsAuthenticationServerManager-20250329-0002.log
AuthlogicsDomainControllerManager-20250325-0001.log
AuthlogicsDomainControllerManager-20250327-0001.log
CredentialProvider-20250325-0001.log
CredentialProvider-20250327-0001.log
CredentialProvider-20250329-0001.log
FidoCredentialProvider-20250326-0001.log
FidoCredentialProvider-20250327-0001.log
FidoCredentialProvider-20250329-0001.log
WDA-20250325-0001.log
WDA-20250328-0001.log
WDADirectory-20250325-0001.log
WDADirectory-20250326-0001.log
WDADirectory-20250327-0001.log
WDADirectory-20250328-0001.log
WDADirectory-20250329-0001.log
WDAService-20250325-0001.log
WDAService-20250326-0001.log
WDAService-20250327-0001.log
```

```
WDAService-20250328-0001.log
WDAService-20250329-0001.log
WDAYubiKey-20250325-0001.log
WDAYubiKey-20250326-0001.log
WDAYubiKey-20250328-0001.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 30th, the cleanup process is triggered, deleting the files from March 25th, as those are then more than five days old.