MyID MFA and PSM

Version 5.0.8

Password Security Management Quick Start 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: IMP2059-5.0.8

January 2025

Copyright

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Copyright [yyyy] [name of copyright owner]

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

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

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

Conventions used in this document

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

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

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

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

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

  For example:

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

  For example:

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

Contents

1 Introduction

This guide provides an overview of the steps required to set up MyID Password Security Management (PSM) in a new environment. For detailed information about a specific feature or deployment scenario, see the ***MyID Authentication Server Installation and Configuration Guide***.

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 Considerations

- MyID Password Security Management requires a Windows Server and an Active Directory domain to be available before installation.
- A Domain Administrator / Enterprise Administrator account is required to perform the installation.
- You must add the Active Directory accounts of MyID administrators to the Authlogics Administrators Active Directory security group.
- After the installation, you are required to reboot the server.
- MyID PSM requires Internet access to:

  `https://*.authlogics.com`

1.2 Required information

- Active Directory administrator credentials.
- The following details about your SMTP Server:
  - Name.
  - Port.
  - Authentication requirements.
- The DNS name for the server.
- Understanding of which password policy settings to use.

1.3 Change history

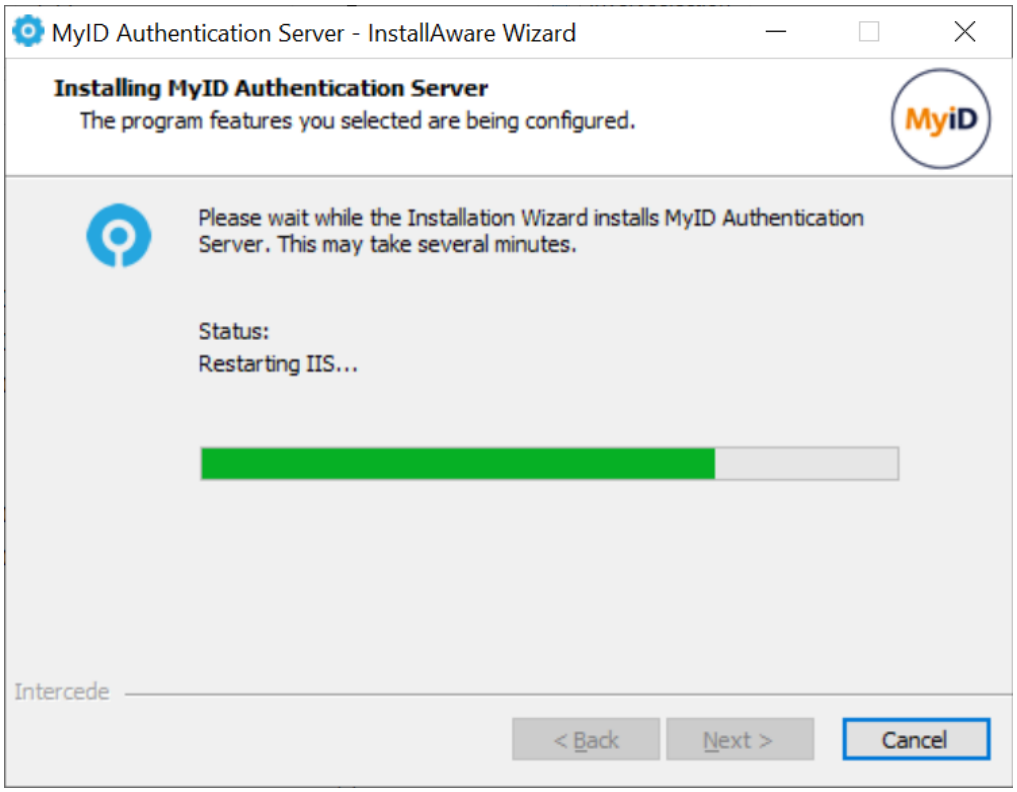
Version	Description
IMP2059-01	Reformatted and released with MyID MFA and PSM version 5.0.7.
IMP2059-5.0.8	Released with MyID MFA and PSM version 5.0.8.

2 Installing the Authentication Server

1. Download the Authentication Server installer from:

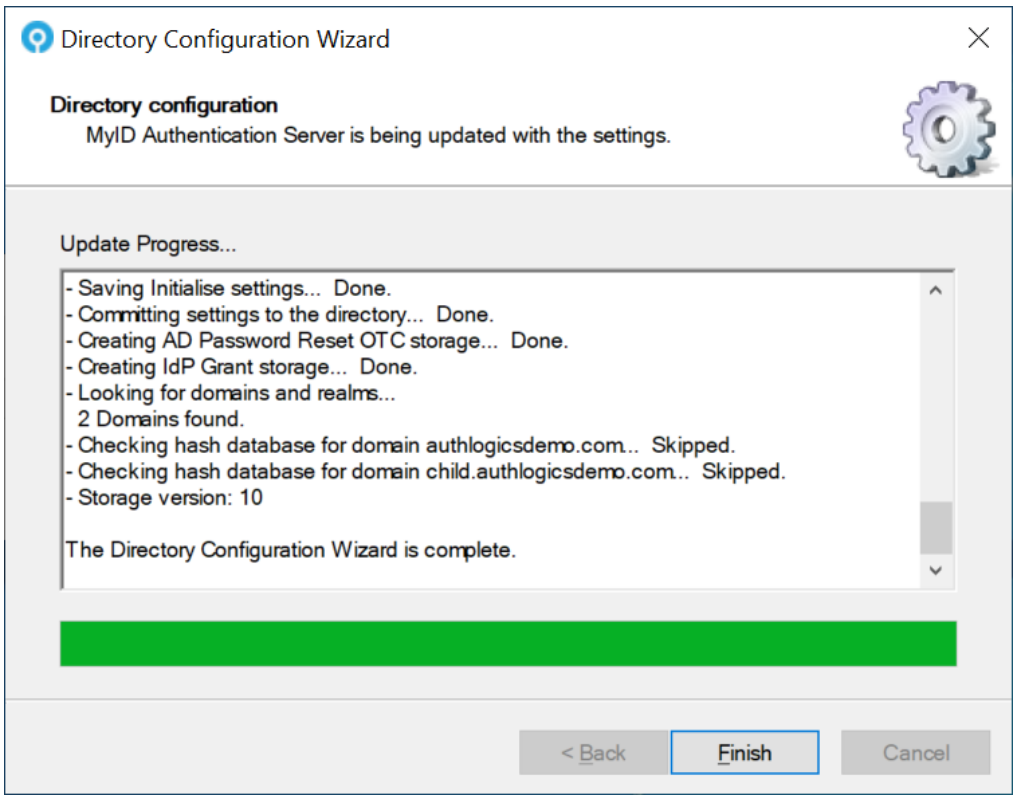
   www.intercede.com/support/downloads
2. Extract the files from the zip archive.
3. Run the setup file in the `Install` folder.
4. Follow the instructions in the Installation wizard.

   This installs the product binaries.



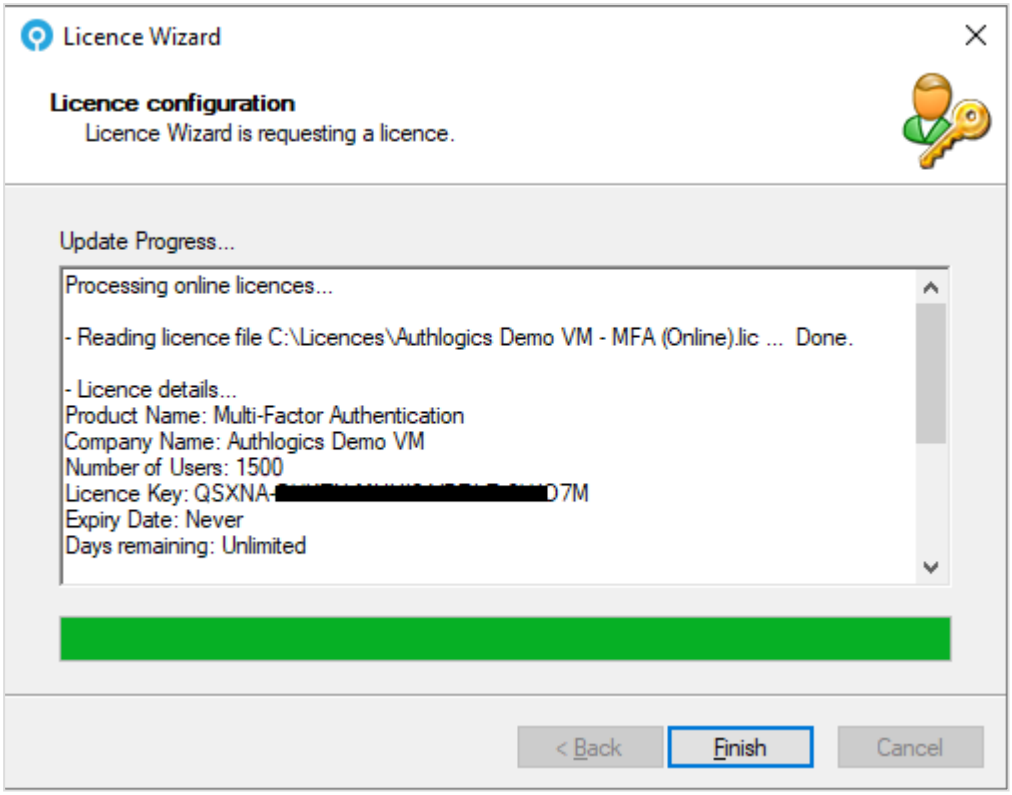
5. Follow the instructions in the Directory Configuration Wizard

   This sets up the Active Directory for use with MyID



6. Use the Licence Wizard to configure your MyID PSM license.

   If you do not have a license key, you can use the Licence Wizard to request a 30 evaluation license.



7. Reboot the server.

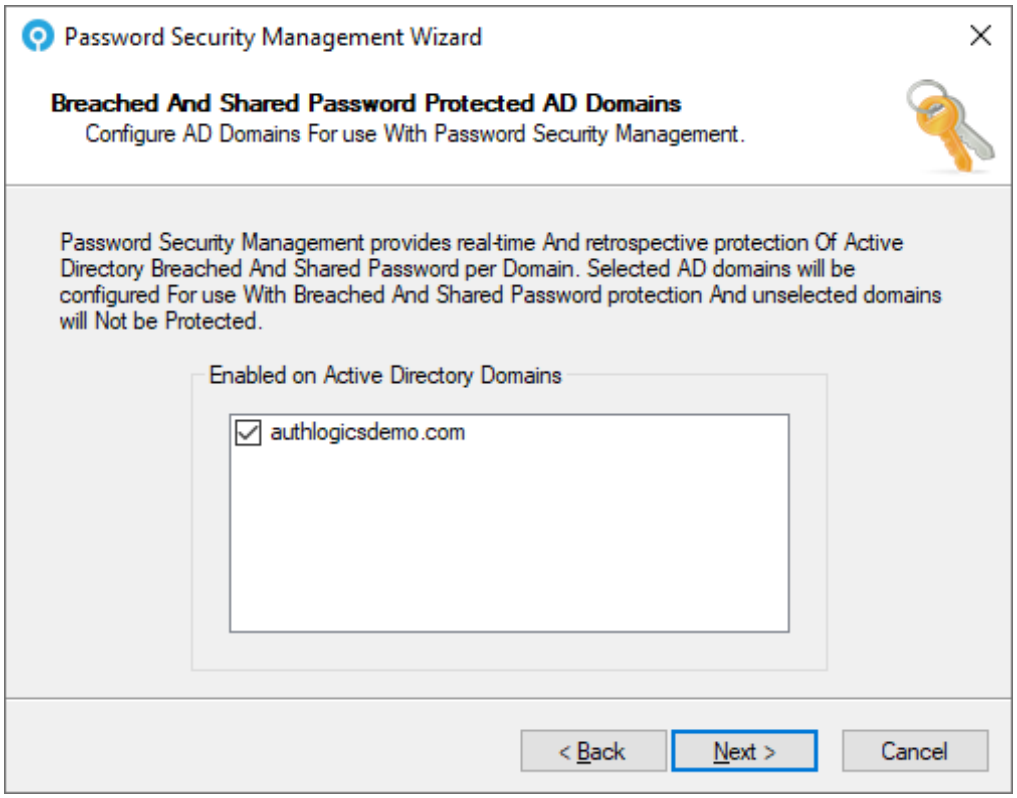
3 Configuring the Authentication Server

To configure the Authentication Server:

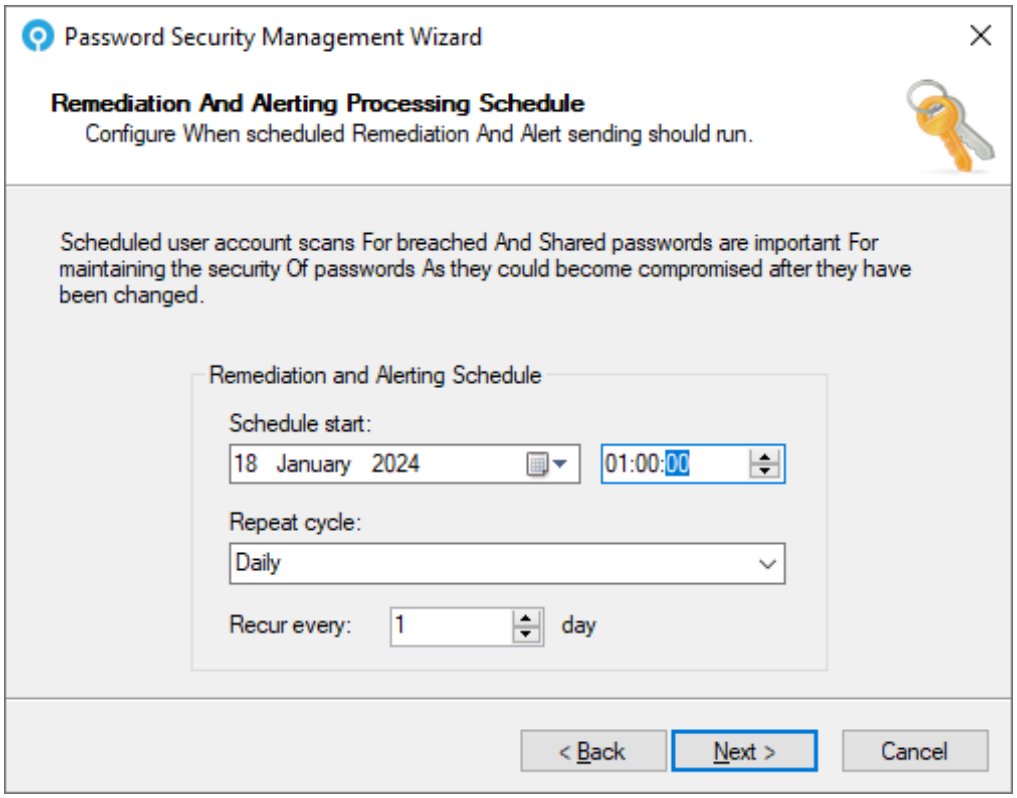
1. Launch the MyID Management Console.
2. Right click **MyID PSM** and select **Properties**.
3. Configure the SMTP Server settings to be able to deliver alerts and new user emails.

3.1 Running the PSM Wizard

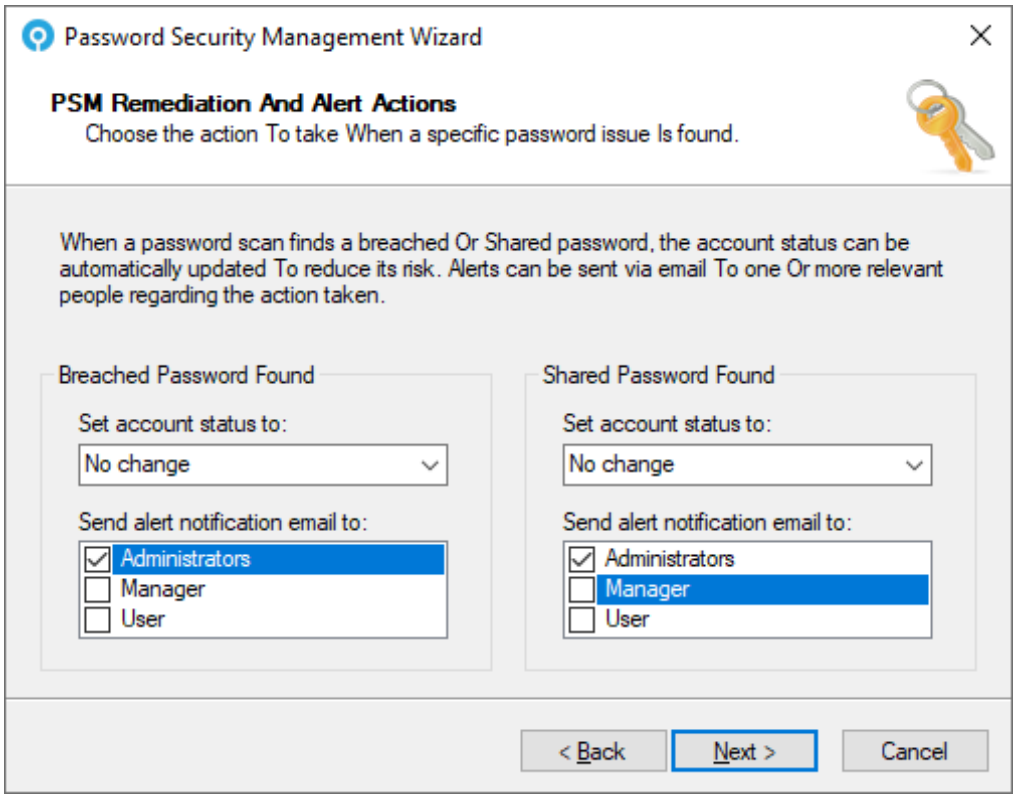
1. Right click **MyID PSM** and select **Password Security Management Wizard**.
2. Select the domains in the forest to protect with PSM.



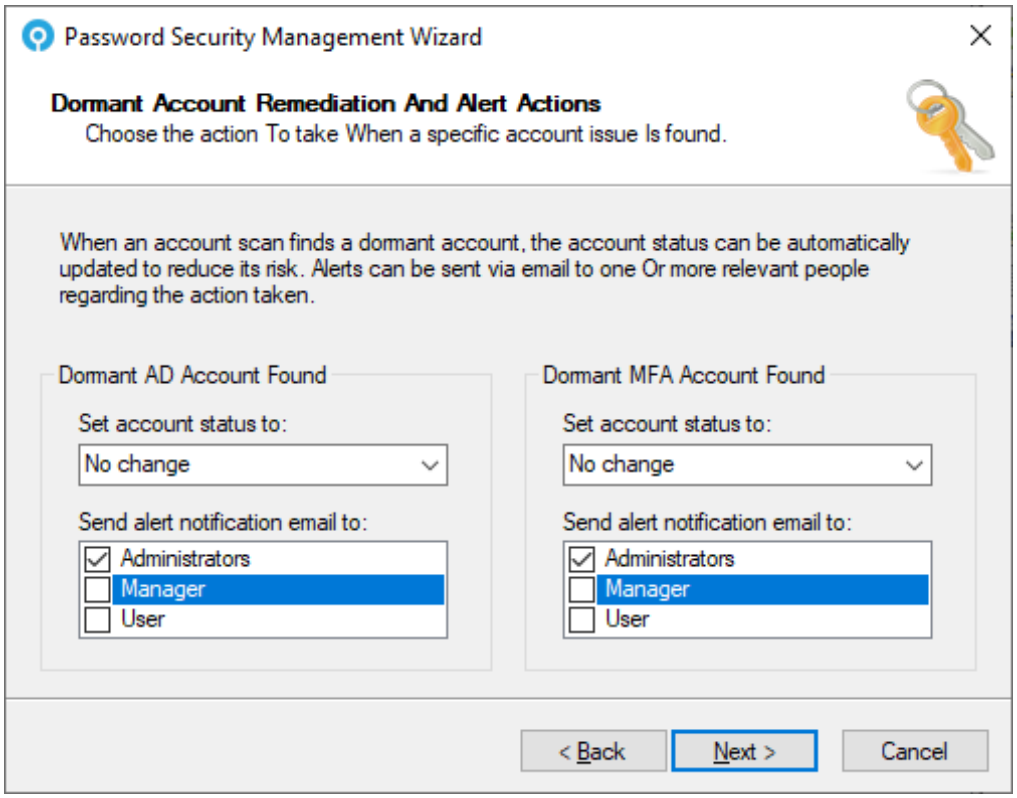
3. Schedule when PSM should check for new breached and shared passwords and send alerts.



4. Select what action to take when breached and shared passwords are found.



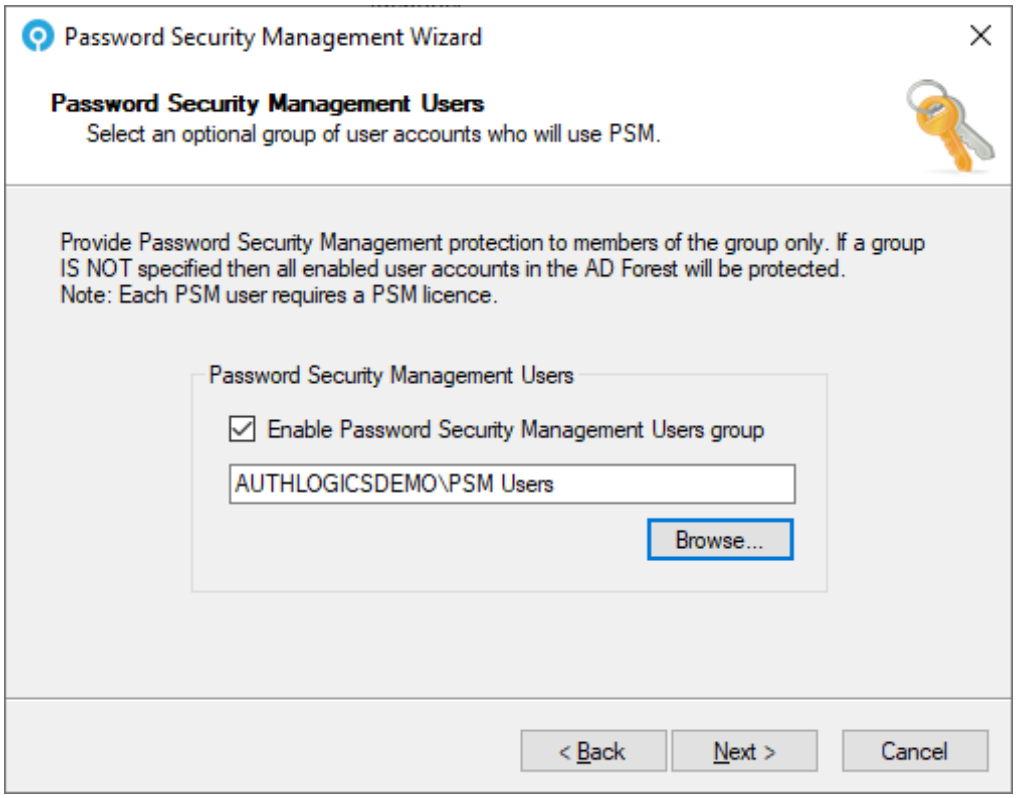
5. Select what action to take when dormant accounts are found.



6. Choose the user accounts for which you want to enable protection.

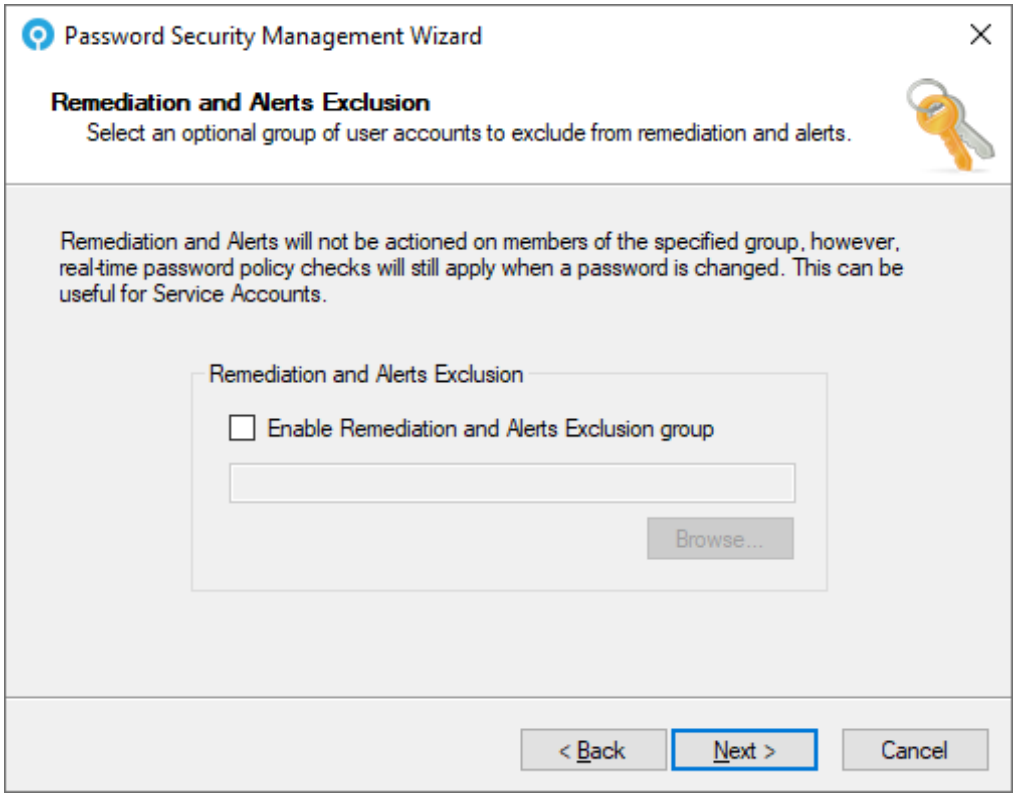
   MyID PSM protects all enabled user accounts in the domain. You can limit this to members of an Active Directory group.

   This can be useful for gradual deployments of new policy settings to users, or if sufficient licenses are not currently available.



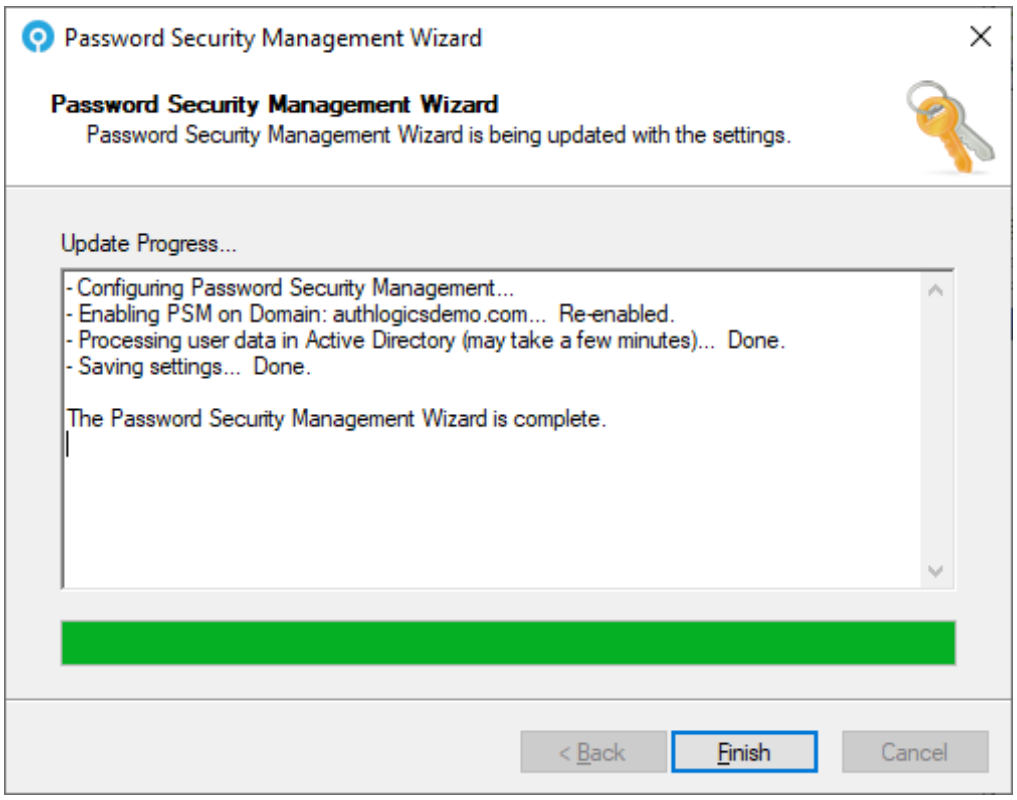
7. Choose the user accounts for which you want to enable alerts.

   PSM performs alerting and remediation on all PSM enabled user accounts. You can exclude accounts from remediation and alerting by adding them to an Active Directory group and excluding that group. This may be useful for service accounts.



8. Click **Next**.

   Your settings are applied. This may longer if many users exist in your Active Directory.



4 Installing the MyID Domain Controller Agent

You must install the Domain Controller Agent on *all* domain controllers in the domain to protect all password changes. You must reboot the domain controllers after the agent is installed. Installing the agent has no effect on password changes until the policy is configured later on.

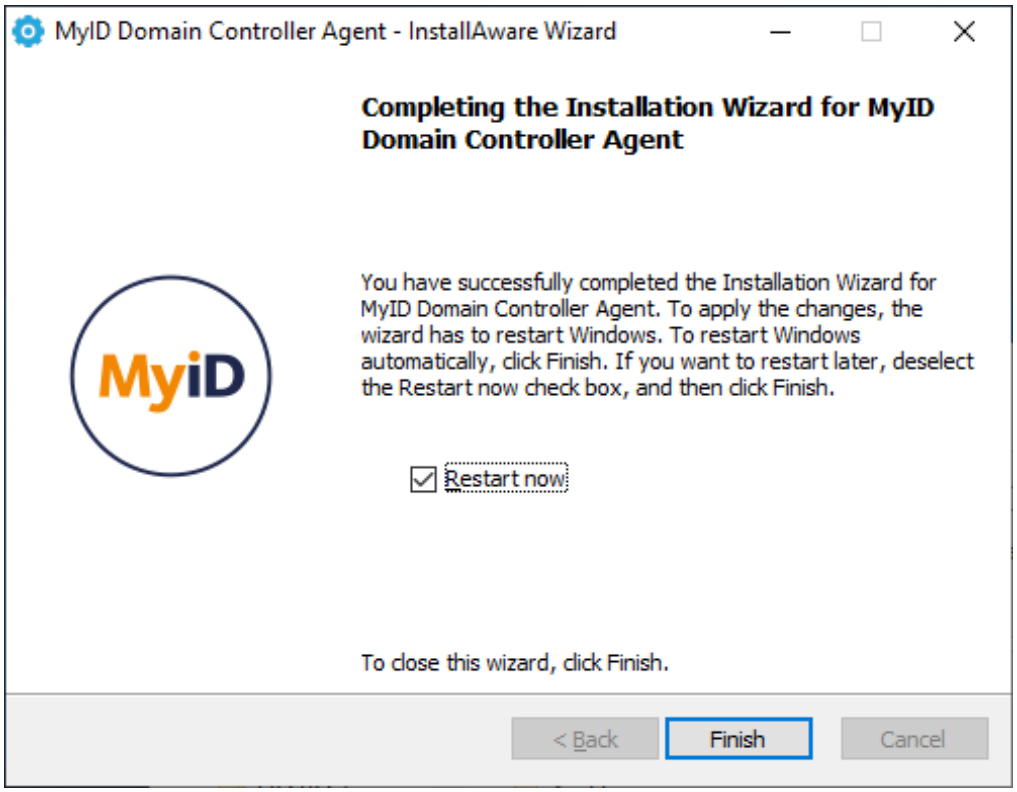
1. Download the MyID Domain Controller Agent installer from:

   www.intercede.com/support/downloads

2. Extract the files from the zip archive.
3. Run the `MyID Domain Controller Agent 5.0.xxxx.x.msi` file.

   Note: If Windows does not allow the installer to be run due to a policy, run the MSI file from an Admin command prompt.

4. Follow the installation wizard.
5. Restart the Domain Controller.



6. Click **Finish**.

5 Configuring the MyID Password Policy

You can configure the MyID Password Policy using an Active Directory group policy.

You must apply the policy to the Domain Controllers as well as the MyID Authentication Servers.

These steps are typically done on a Domain Controller; however, you can carry out the steps from anywhere that you have installed the Active Directory management tools.

1. Open the Group Policy Management Console.
2. Create a new Group Policy Object called `Authlogics Password Policy`.
3. Edit the new policy and import the following template files:
   - `Authlogics.admx`
   - `AuthlogicsDCAgent.admx`
   - `AuthlogicsPasswordPolicy.admx`

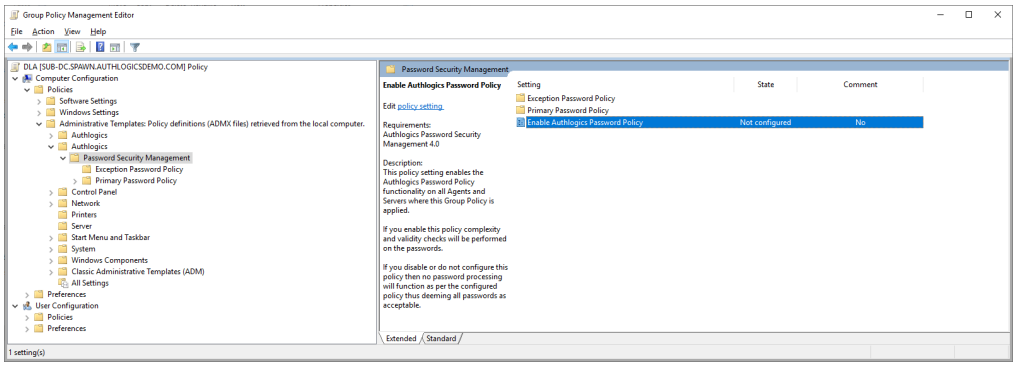
   You can find these templates the downloaded ZIP files Group Policy Object folder, or on the MyID Authentication Server in the following location:

   `C:\Program Files\Authlogics Authentication Server\`

   To import the policy files, copy the contents of the GPO folder to the domain's `PolicyDefinitions` folder:

   `\\%userdomain%\sysvol\%userdnsdomain%\policies\policydefinitions`

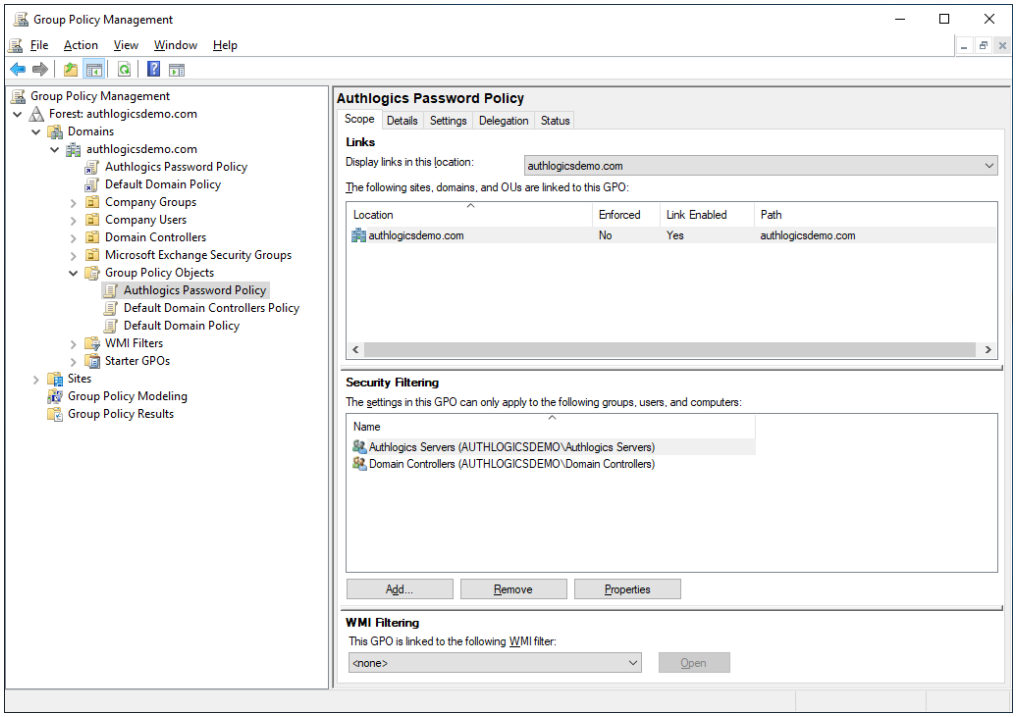
   Note: For standalone deployments, you can copy the `.ADMx` files and `en-US` folders to the `C:\Windows\PolicyDefinitions` folder.
4. Expand the **Authlogics Password Security Management** policy tree and set **Enable Authlogics Password Policy** to **Enabled**.



5. Review the rest of the password policy options and set them accordingly.

   The default complexity rules are normally sufficient.
6. You are recommended to enable the following features:
   - **Enable Passphrases – Enabled**
   - **Password Expiry Default Zone**
   - **Password Never Expires Zone**

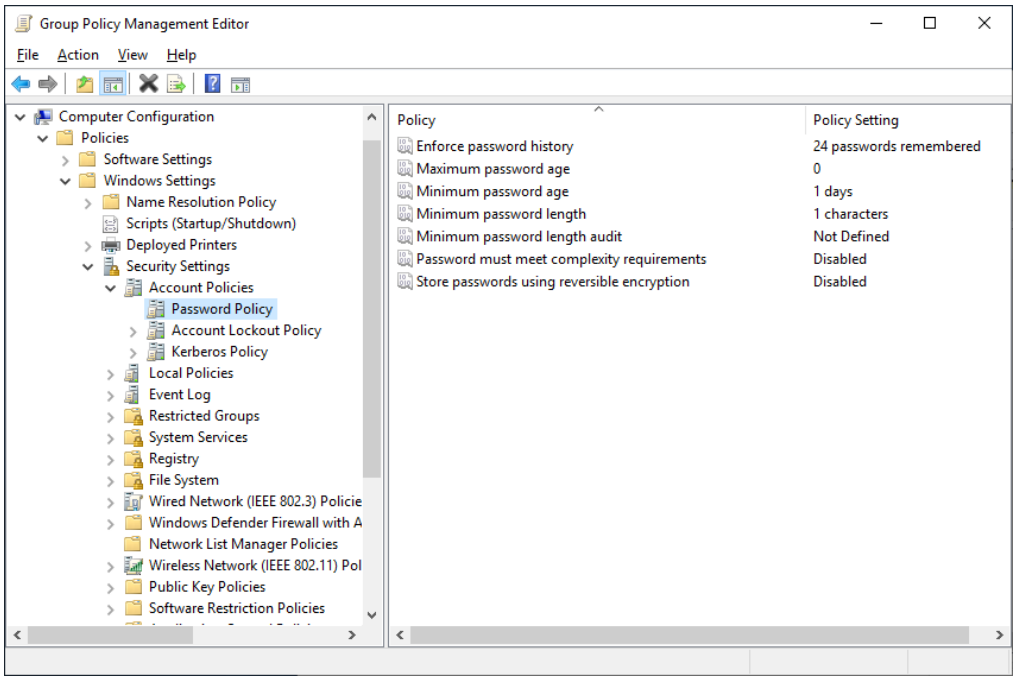
7. In the new the **Authlogics Password Policy** object:
   a. Add a link to the Domain.
   b. Configure the security filtering to **Authlogics Servers** and **Domain Controllers** groups only.



6 Disabling the Windows Password Policy

You must disable the Windows password policy so that it does not conflict with the MyID password policy.

1. Open the Group Policy Management Console.
2. Edit the **Default Domain Policy**.
3. Change the following settings. You *must* set the settings to the specified values:
   - **Maximum password age**: `0`
   - **Minimum password length**: `1`
   - **Passwords must meet complexity requirements**: `Disabled`



7 Testing password changes and schedules

Group Policy changes can take up to 15 minutes to apply to a server and up to a further 15 mins to take effect within Windows. To speed this up:

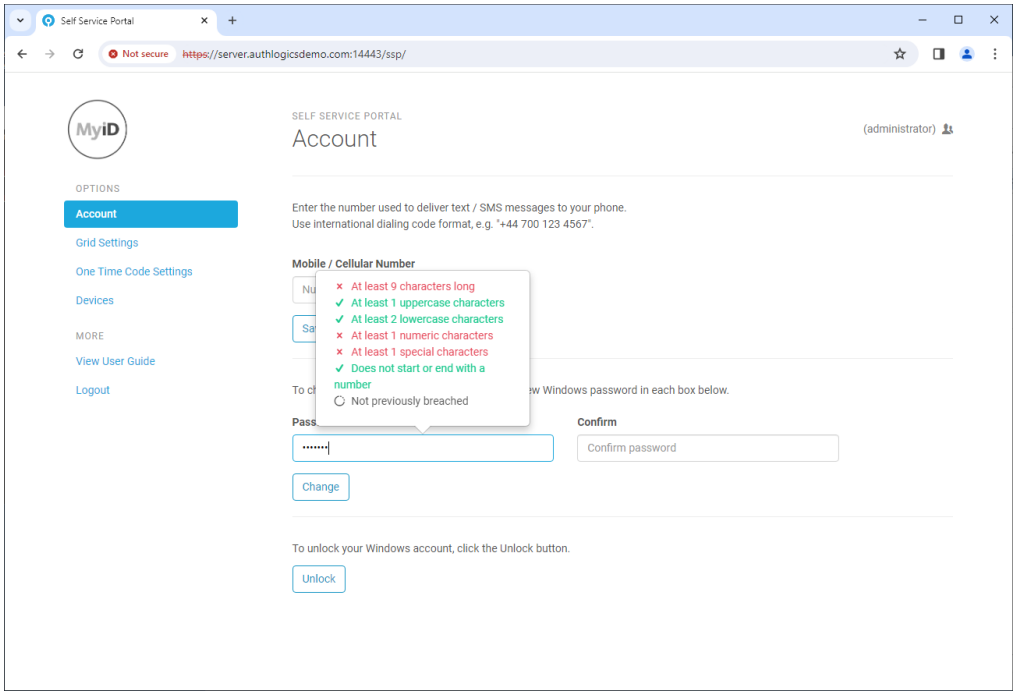
1. Open an admin command prompt.
2. Run the following command:

   ```
   GPUPDATE /FORCE
   ```

3. Reboot the server.

7.1 Testing password changes through the Self Service Portal

1. On the MyID Authentication Server, log in to the Self Service Portal.
2. Enter a variety of test passwords that should pass or fail the current policy.



The following test passwords are designed to pass most password complexity checks, but are contained within the online breach database and should therefore fail:

- `Authl0g1c$Test!`
- `IL0v3Coff33!`
- `H@ppyD@y5`
- `Sh@nk5t3r5!`

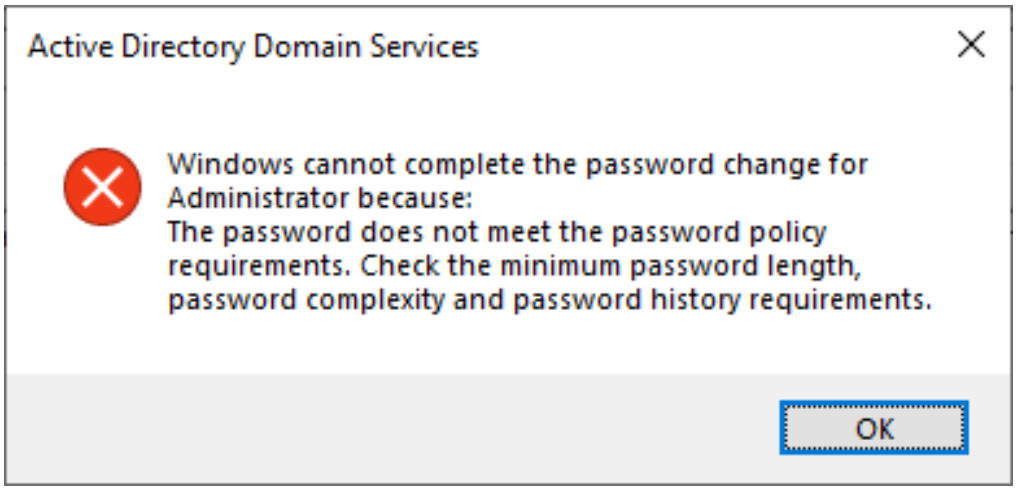
3. When a valid password is entered and confirmed, click **Change** to save it.
4. On the Domain Controller, in the Application Event Log, look for Event ID 1425.

   This shows a successful change.

5. On the MyID Authentication Server, in the Application Event Log, look for Event ID 1400. This shows a successful change.

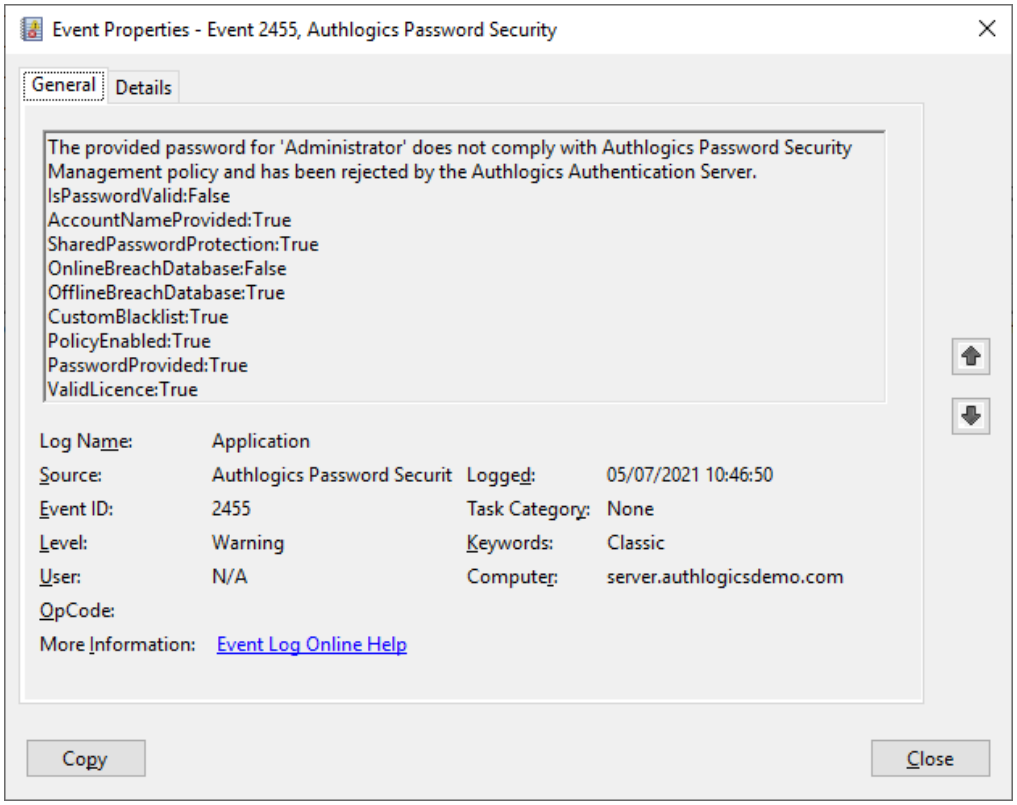
7.2 Testing password changes through Active Directory

1. On the Domain Controller, open Active Directory Users and Computers.
2. Locate a test user account, right click, and select **Reset Password**.
3. Enter a known non-complaint password; for example:
   - `Authl0g1c$Test!`
   - `IL0v3Coff33!`
   - `H@ppyD@y5`
   - `Sh@nk5t3r5!`
4. Receive an error confirming that the password is not accepted.



5. On the Domain Controller, in the Application Event Log, look for Event ID 2455.

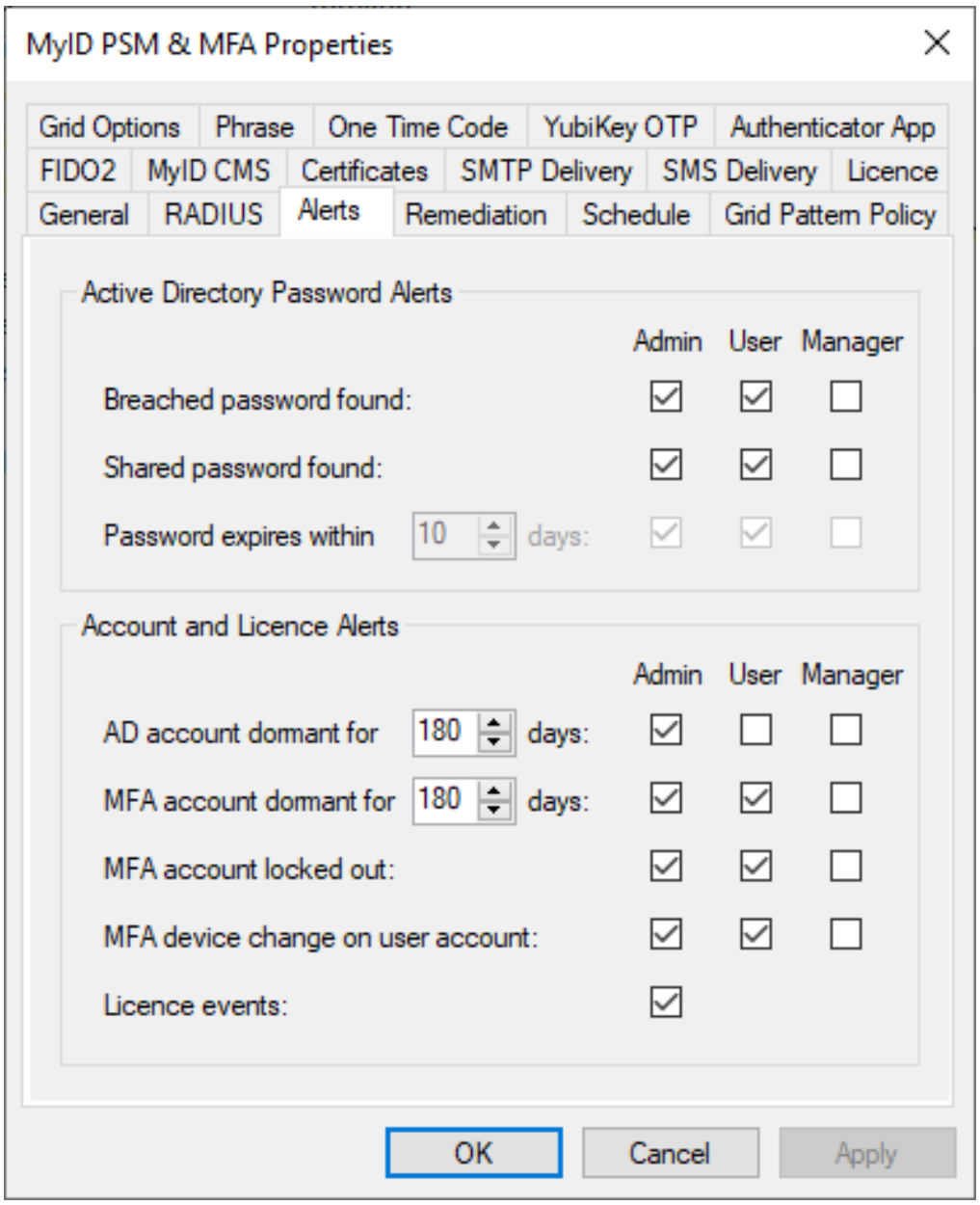
   This shows an unsuccessful change, and includes the results of the checks that were performed.



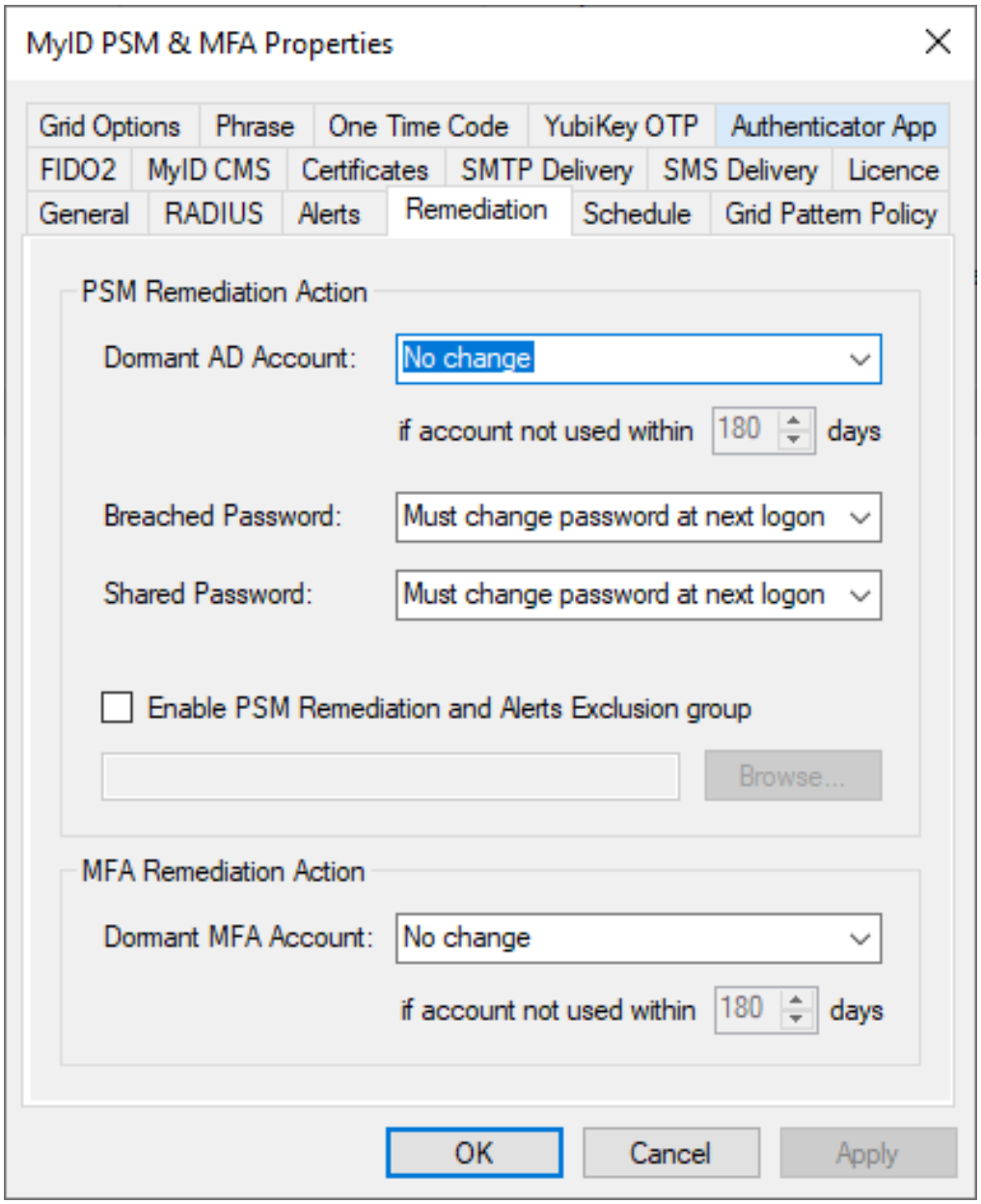
Note: Event ID 2455 appears twice when resets are performed through Active Directory Users and Computers; this is due to a known issue with the Active Directory Users and Computers tool. This does not happen during normal user password changes.

7.3 Testing alerting and remediation

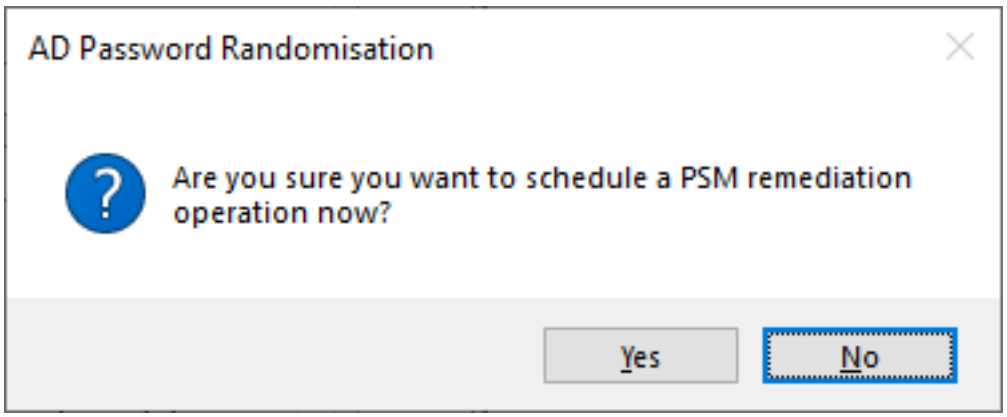
1. Launch the MyID Management Console.
2. Right click **MyID PSM** and select **Properties**.
3. On the **Alerts** tab, ensure that alerts are enabled for the administrators and users.



4. On the **Remediation** tab, ensure that remediation is configured.



5. On the **Schedule** tab:
   a. Click **Run Now**.

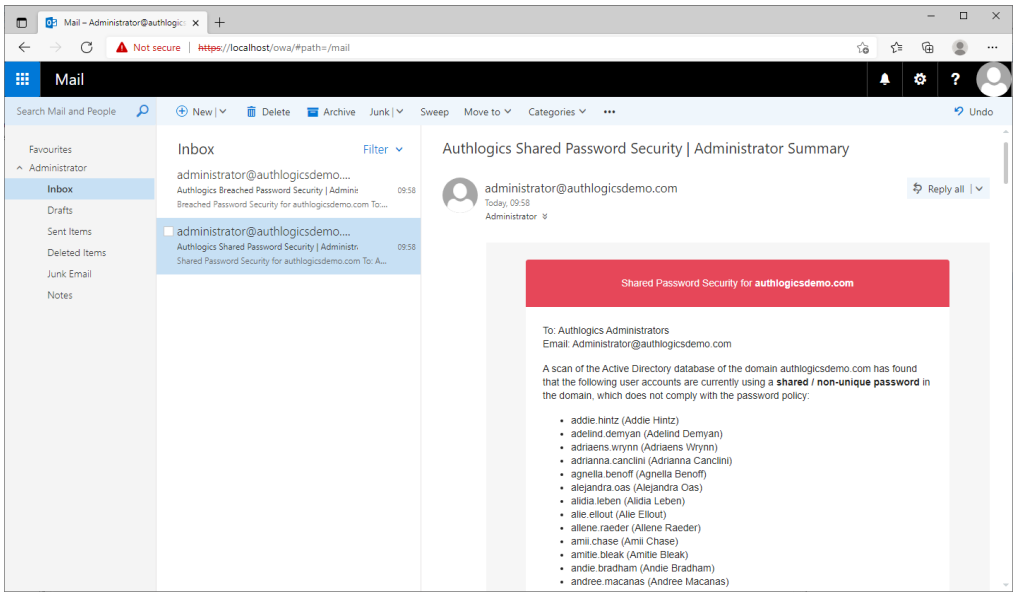


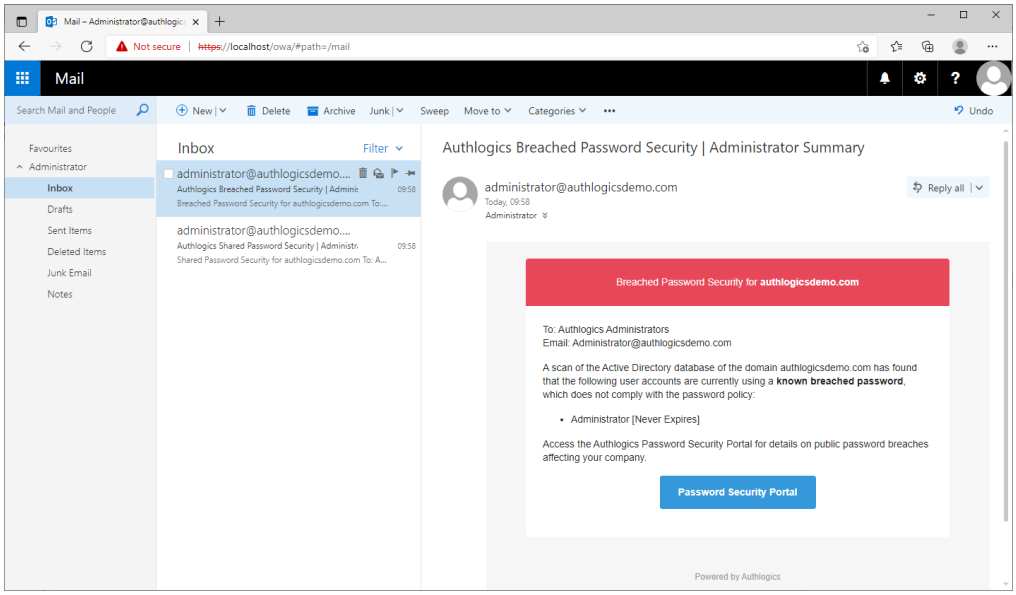
   b. Click **Yes**.
6. To avoid waiting for the schedule to run, open the Windows service control panel and restart the **MyID Authentication Server Service**.

   If you do not manually restart the service, the schedule takes up to 15 minutes to run.
7. On the MyID Authentication Server, in the Application Event Log, look for Event IDs 1966 and 1962.

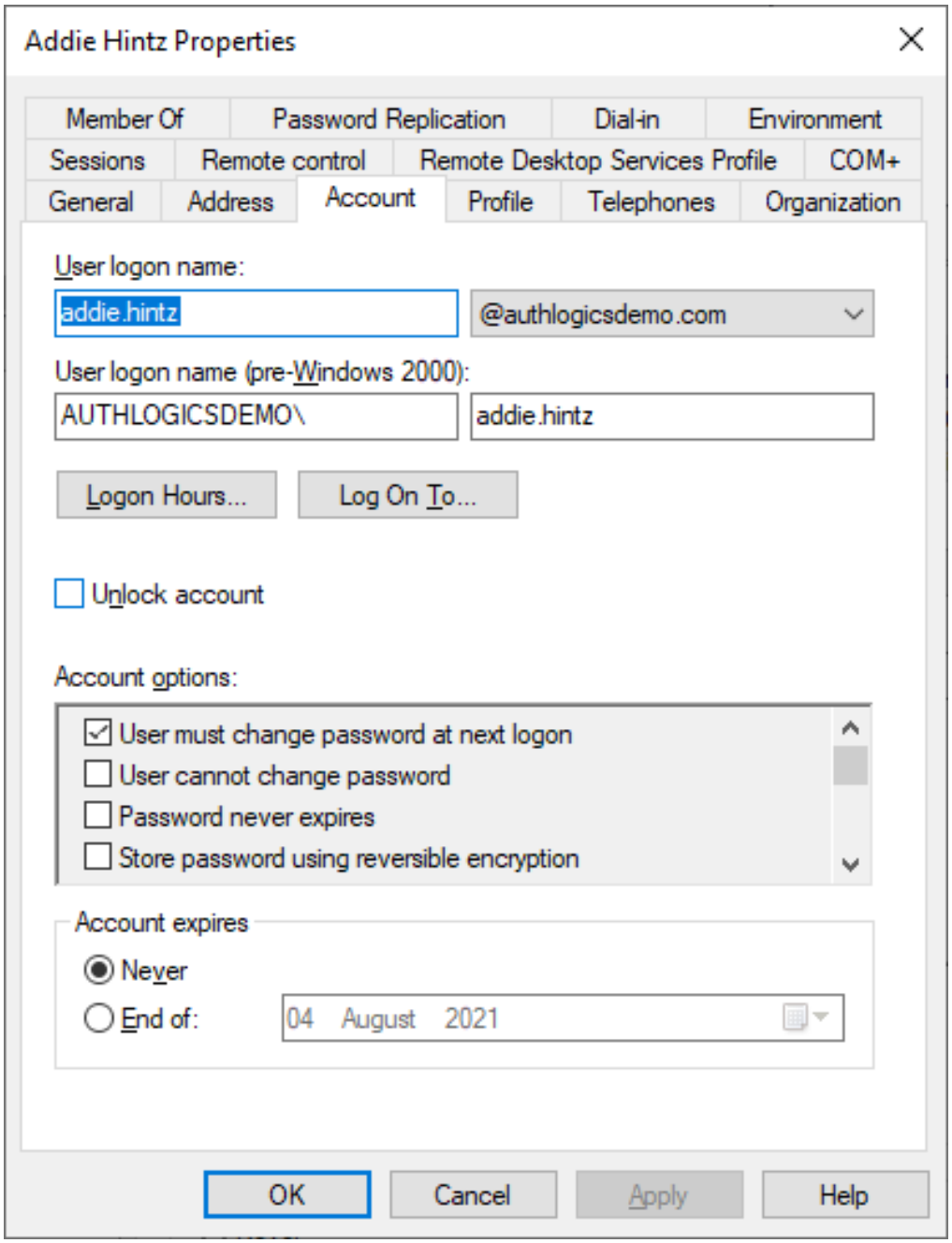
   This shows when the tasks have been completed.

   To see when the schedule will next be run, you can also look for Event ID 1953.
8. Check the mailboxes of both a user and an administrator.




Mail – Administrator@authlogic
Not secure
https://localhost/owa/#path=/mail
Mail
Search Mail and People
New
Delete
Archive
Junk
Sweep
Move to
Categories
Undo
Favourites
Administrator
Inbox
Drafts
Sent Items
Deleted Items
Junk Email
Notes
Inbox
Filter
administrator@authlogicsdemo....
Authlogics Breached Password Security | Administ
09:58
Breached Password Security for authlogicsdemo.com To:...
administrator@authlogicsdemo....
Authlogics Shared Password Security | Administr
09:58
Shared Password Security for authlogicsdemo.com To: A...
Authlogics Breached Password Security | Administrator Summary
administrator@authlogicsdemo.com
Today, 09:58
Administrator
Reply all
Breached Password Security for authlogicsdemo.com
To: Authlogics Administrators
Email: Administrator@authlogicsdemo.com
A scan of the Active Directory database of the domain authlogicsdemo.com has found that the following user accounts are currently using a known breached password, which does not comply with the password policy:
Administrator [Never Expires]
Access the Authlogics Password Security Portal for details on public password breaches affecting your company.
Password Security Portal
Powered by Authlogics

9. Check that the remediation action was performed on the reported accounts.



The **User must change password at next login** option should be checked.

7.4 Monitoring PSM Usage

MyID Server includes a dashboard to graphically display the state of your PSM deployment.

To open the password security dashboard:

1. Launch the MyID Web Management Portal.

   This is available at:

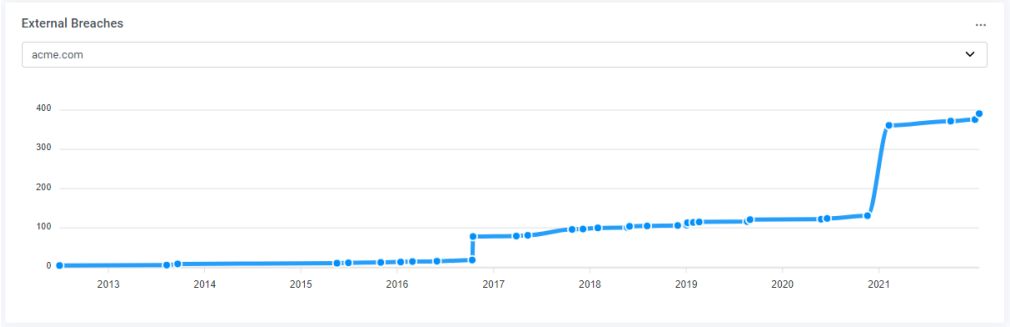
   `https://<servername>:14443/admin`

   Where `<servername>` is the name of your server.

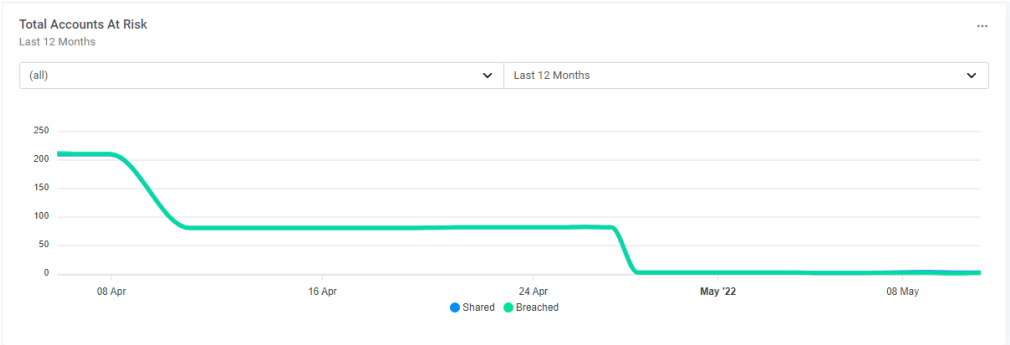
2. Under **Dashboards**, select **Password Security**.

   This dashboard reflects contains information on:

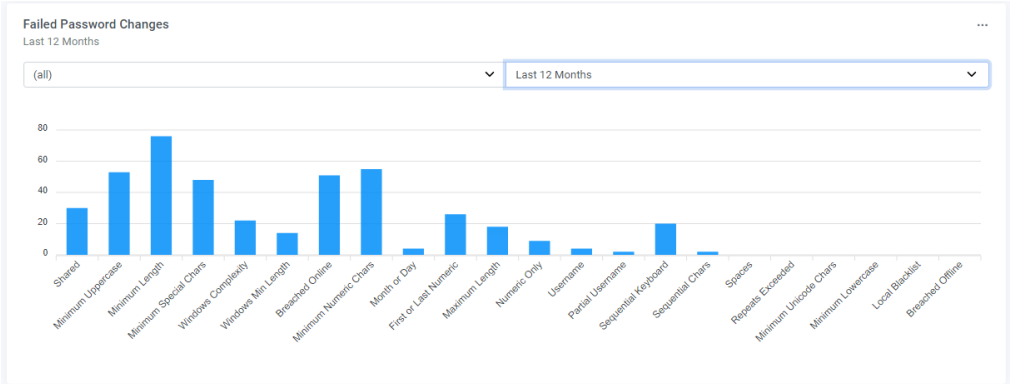
   - External Breaches



   - Total Accounts at Risk



   - Failed Password Changes



- Accounts at Risk