

MyID MFA and PSM

Version 5.3.2

Password Security Management Quick Start Guide

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

Copyright

© 2001-2025 Intercede Limited. All rights reserved.

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

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

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

Licenses and Trademarks

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

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

Conventions used in this document

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

For example:

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

For example:

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

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

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

For example:

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

For example:

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

Contents

Password Security Management Quick Start Guide	1
Copyright	2
Conventions used in this document	3
Contents	4
1 Introduction	5
1.1 Considerations	5
1.2 Required information	5
2 Installing the Authentication Server	6
3 Configuring the Authentication Server	9
3.1 Running the PSM Wizard	9
4 Installing the MyID Domain Controller Agent	15
5 Configuring the MyID Password Policy	16
6 Disabling the Windows Password Policy	18
7 Testing password changes and schedules	19
7.1 Testing password changes through the Self Service Portal	19
7.2 Testing password changes through Active Directory	20
7.3 Testing alerting and remediation	22
7.4 Monitoring PSM Usage	27

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`

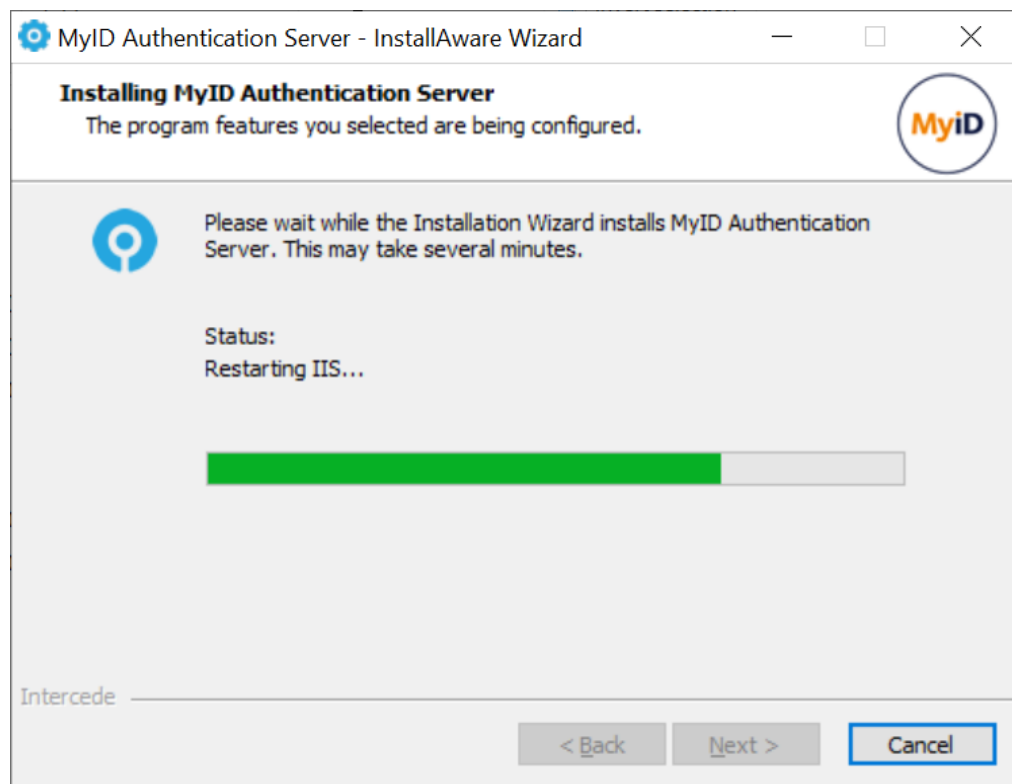
1.2 Required information

- 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.

2 Installing the Authentication Server

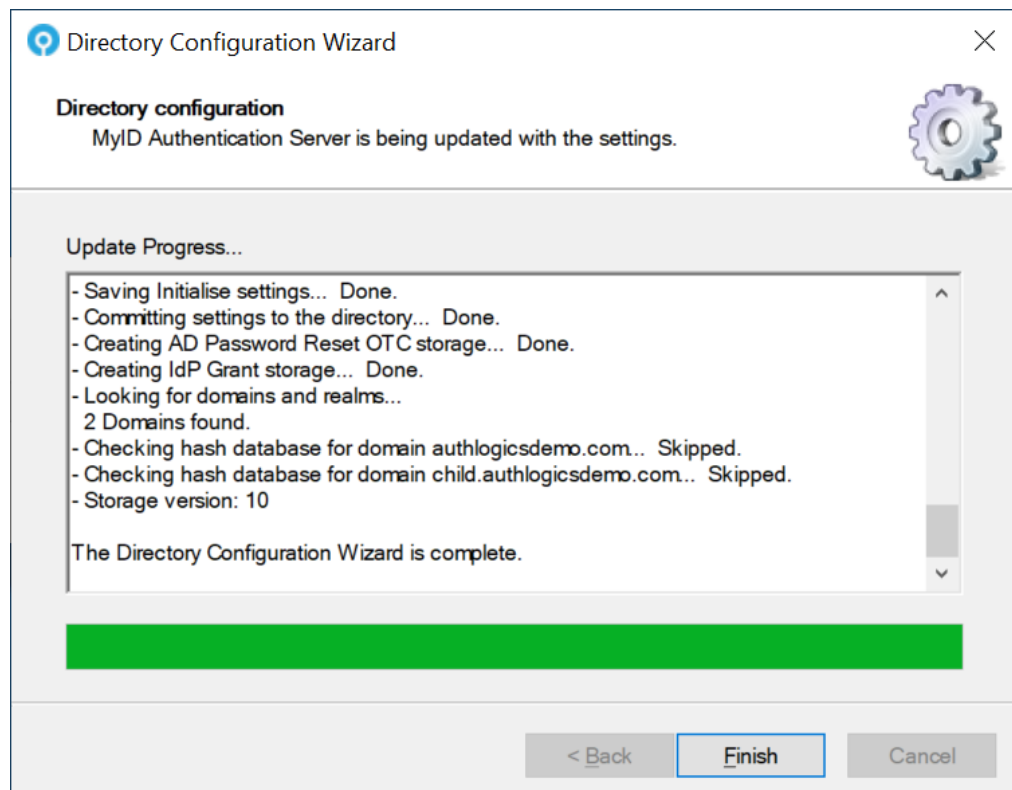
1. Download the Authentication Server installer from:
www.intercede.com/support/downloads
2. Extract the files from the zip archive.
3. Run the setup file in the `Install` folder.
4. Follow the instructions in the Installation wizard.

This installs the product binaries.



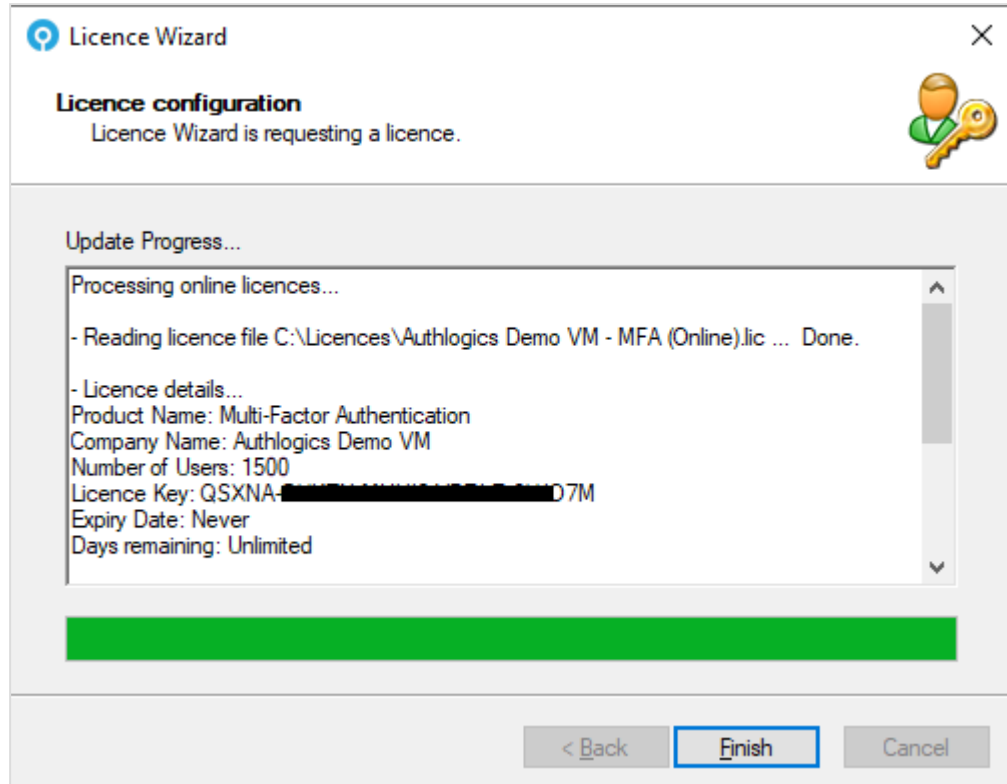
5. Follow the instructions in the Directory Configuration Wizard

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.

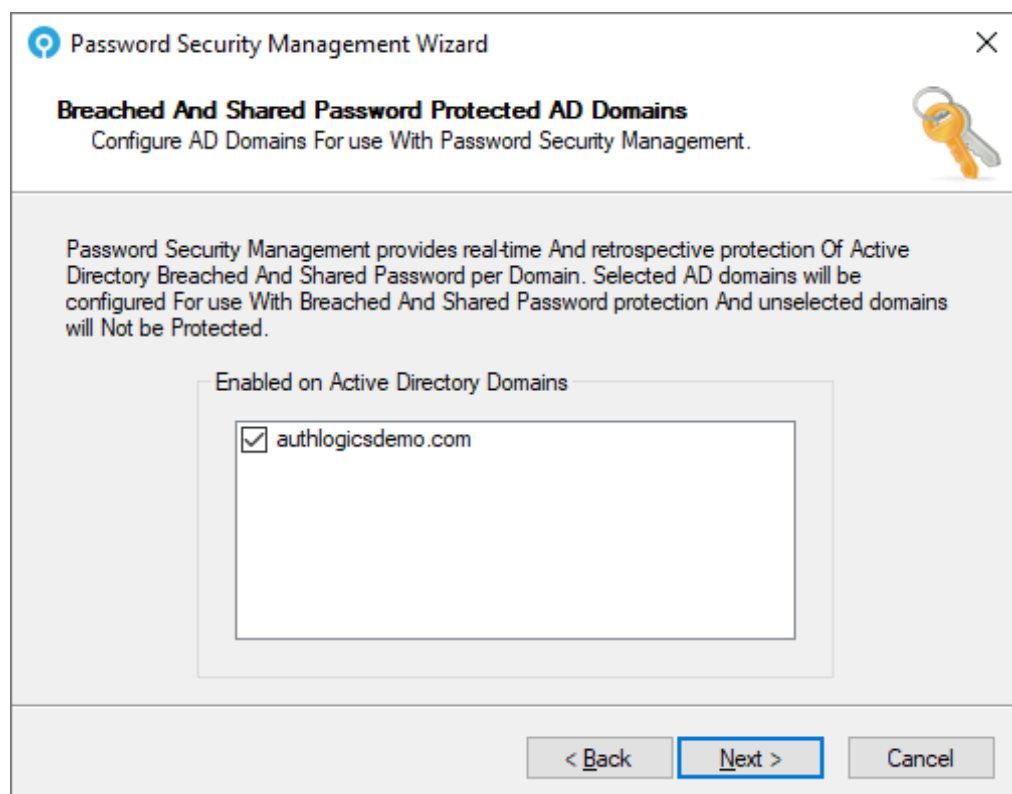
3 Configuring the Authentication Server

To configure the Authentication Server:

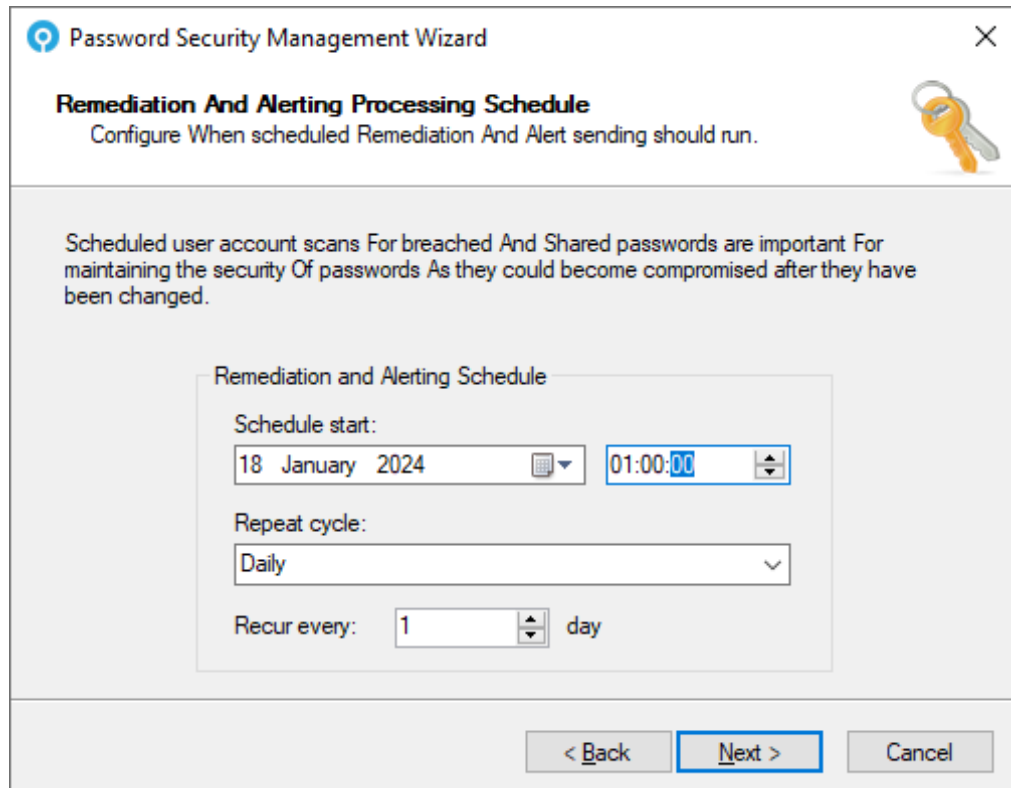
1. Launch the MyID Management Console.
2. Right click **MyID PSM** and select **Properties**.
3. Configure the SMTP Server settings to be able to deliver alerts and new user emails.

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.



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



Password Security Management Wizard [Close]

Remediation And Alerting Processing Schedule
Configure When scheduled Remediation And Alert sending should run.

Scheduled user account scans For breached And Shared passwords are important For maintaining the security Of passwords As they could become compromised after they have been changed.

Remediation and Alerting Schedule

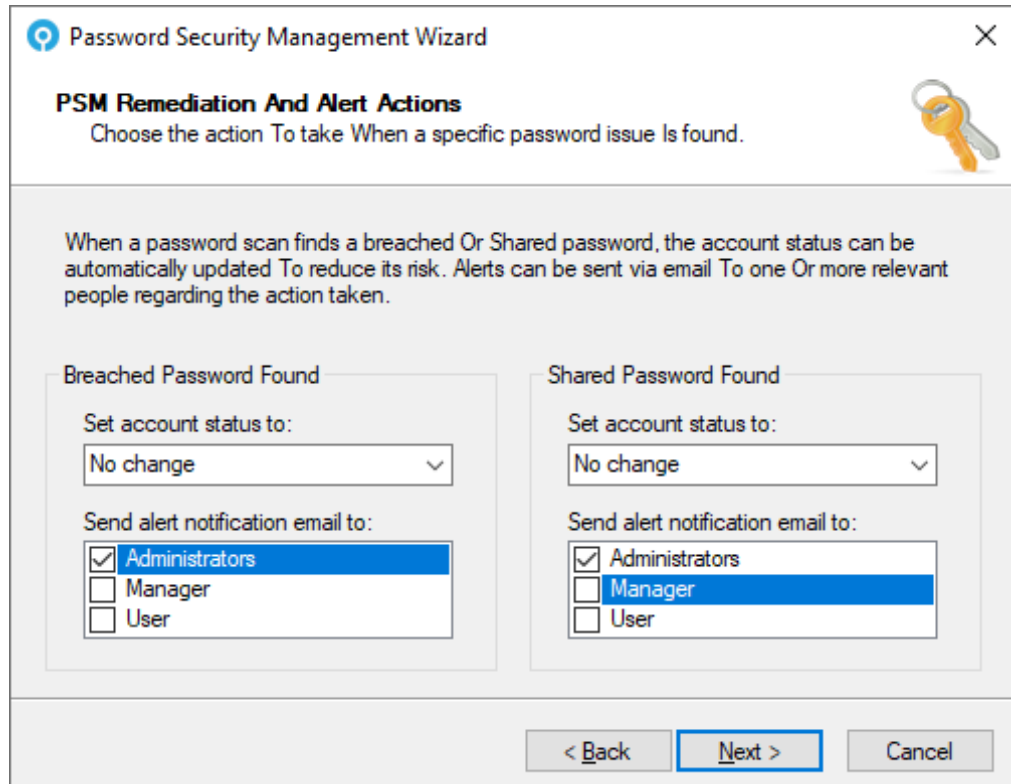
Schedule start:
18 January 2024 [Calendar icon] 01:00:00 [Time picker]

Repeat cycle:
Daily [Dropdown arrow]

Recur every: 1 [Spinner] day

< Back Next > Cancel

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



Password Security Management Wizard

PSM Remediation And Alert Actions
Choose the action To take When a specific password issue Is found.

When a password scan finds a breached Or Shared password, the account status can be automatically updated To reduce its risk. Alerts can be sent via email To one Or more relevant people regarding the action taken.

Breached Password Found

Set account status to:
No change

Send alert notification email to:
☒ Administrators
☐ Manager
☐ User

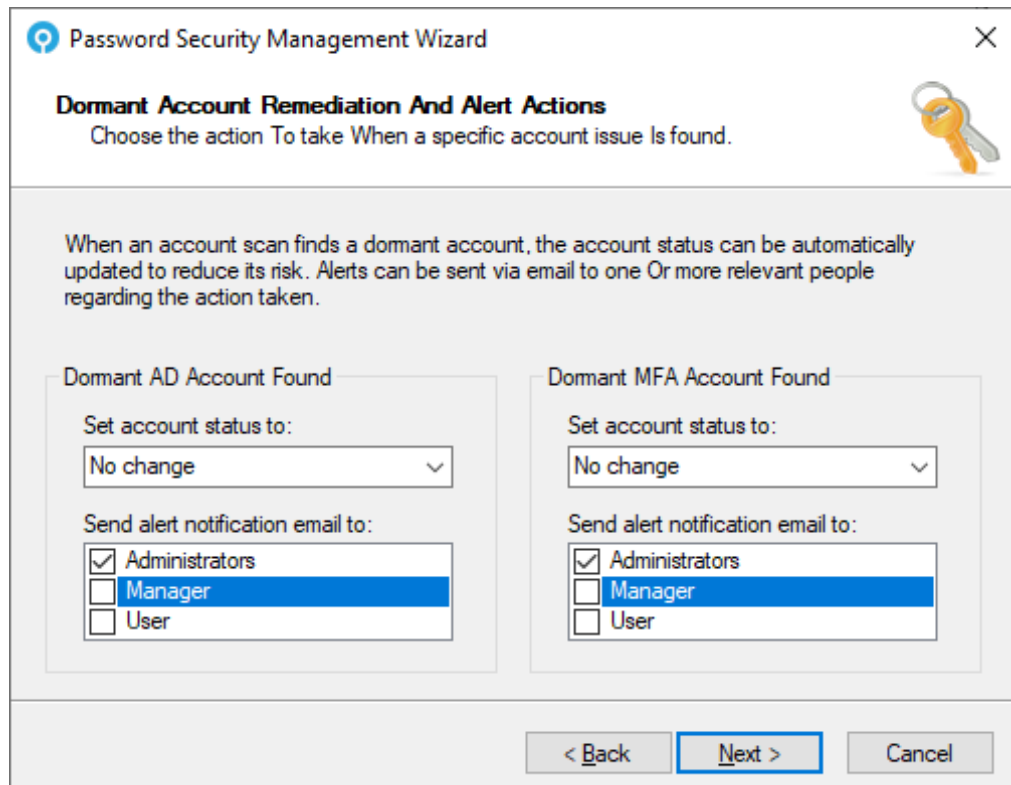
Shared Password Found

Set account status to:
No change

Send alert notification email to:
☒ Administrators
☐ Manager
☐ User

< Back Next > Cancel

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



Password Security Management Wizard

Dormant Account Remediation And Alert Actions
Choose the action To take When a specific account issue Is found.

When an account scan finds a dormant account, the account status can be automatically updated to reduce its risk. Alerts can be sent via email to one Or more relevant people regarding the action taken.

Dormant AD Account Found

Set account status to:
No change

Send alert notification email to:
☒ Administrators
☐ Manager
☐ User

Dormant MFA Account Found

Set account status to:
No change

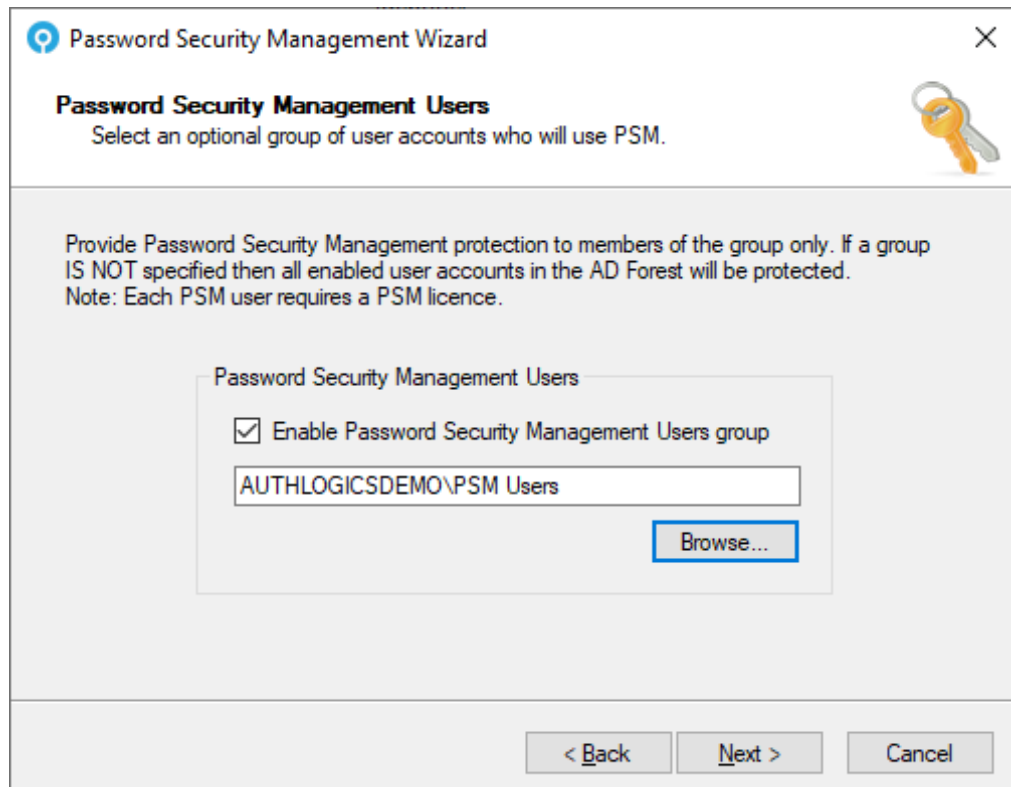
Send alert notification email to:
☒ Administrators
☐ Manager
☐ User

< Back Next > Cancel

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.

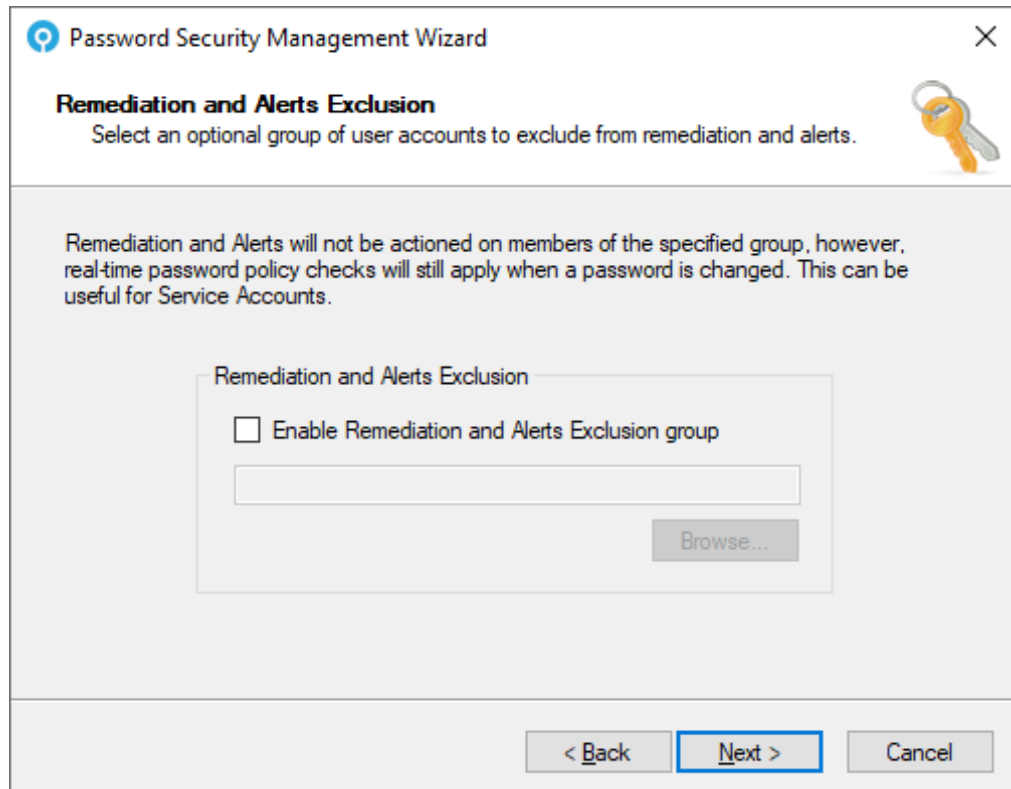
This can be useful for gradual deployments of new policy settings to users, or if sufficient licenses are not currently available.



The screenshot shows the 'Password Security Management Wizard' window. The title bar reads 'Password Security Management Wizard'. The main heading is 'Password Security Management Users' with a sub-instruction: 'Select an optional group of user accounts who will use PSM.' There is a key icon in the top right corner. Below this, a text block states: 'Provide Password Security Management protection to members of the group only. If a group IS NOT specified then all enabled user accounts in the AD Forest will be protected. Note: Each PSM user requires a PSM licence.' A section titled 'Password Security Management Users' contains a checked checkbox 'Enable Password Security Management Users group' and a text box containing 'AUTHLOGICSDemo\PSM Users'. A 'Browse...' button is next to the text box. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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

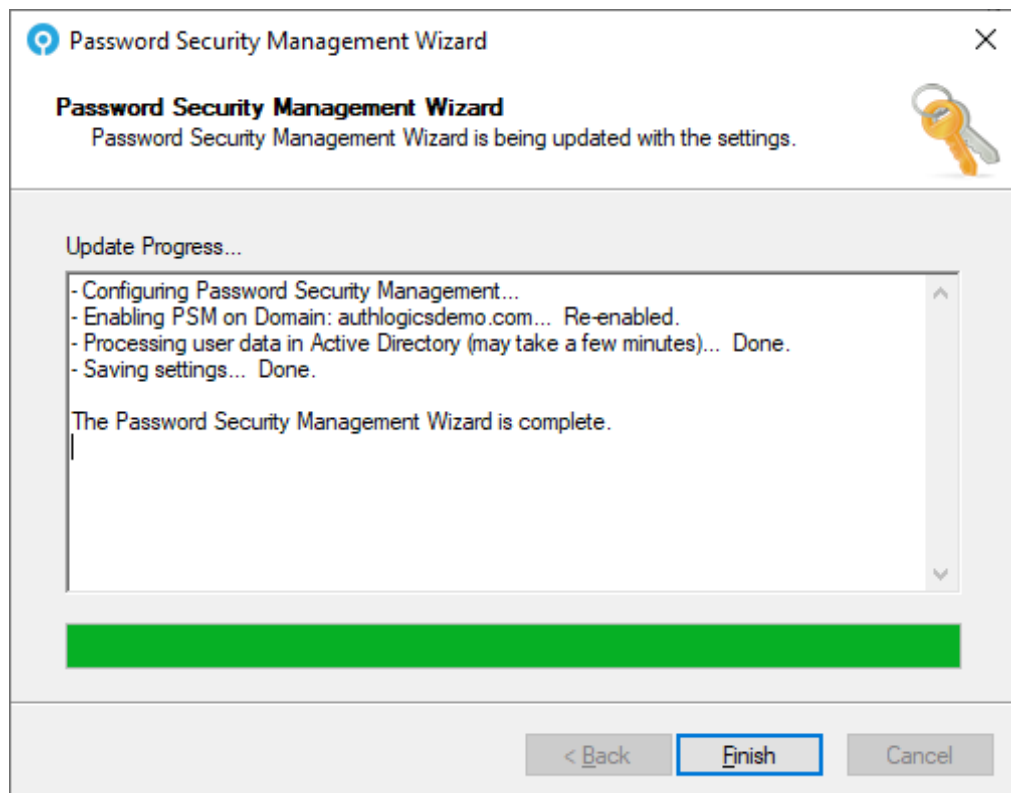
PSM performs alerting and remediation on all PSM enabled user accounts. You can exclude accounts from remediation and alerting by adding them to an Active Directory group and excluding that group. This may be useful for service accounts.



The screenshot shows a window titled "Password Security Management Wizard" with a close button (X) in the top right corner. The main heading is "Remediation and Alerts Exclusion" with a subtext: "Select an optional group of user accounts to exclude from remediation and alerts." There is a key icon in the top right. Below this, a text block states: "Remediation and Alerts will not be actioned on members of the specified group, however, real-time password policy checks will still apply when a password is changed. This can be useful for Service Accounts." In the center, there is a section titled "Remediation and Alerts Exclusion" containing a checkbox labeled "Enable Remediation and Alerts Exclusion group". Below the checkbox is a text input field and a "Browse..." button. At the bottom of the window are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

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

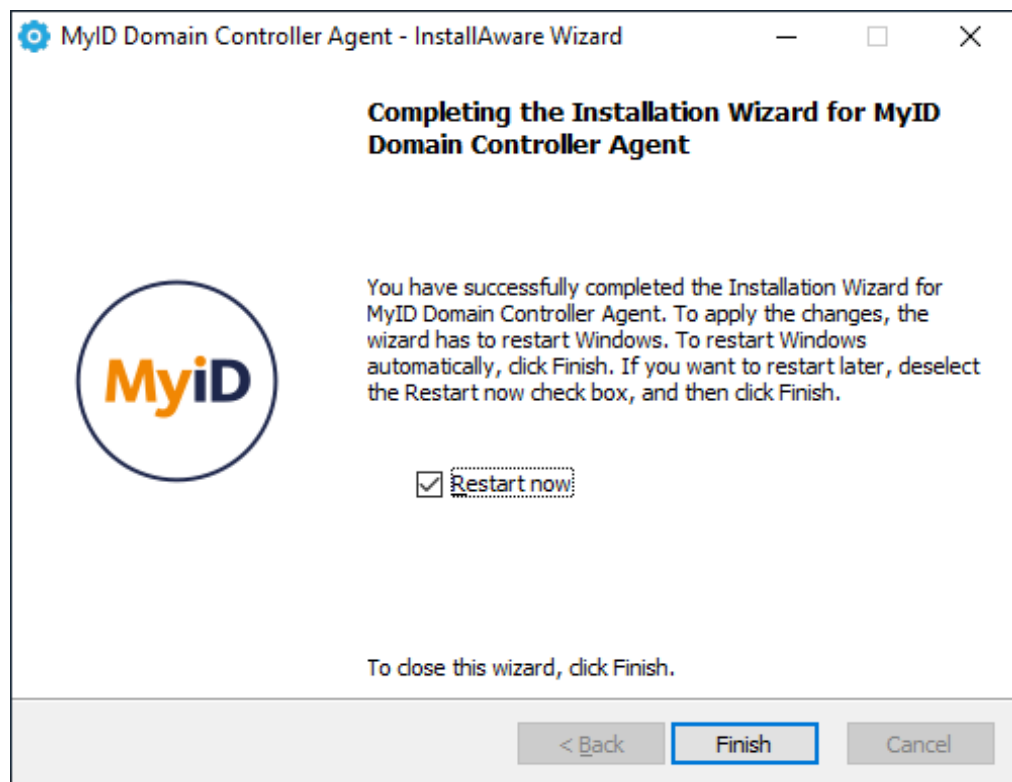
2. Extract the files from the zip archive.

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:

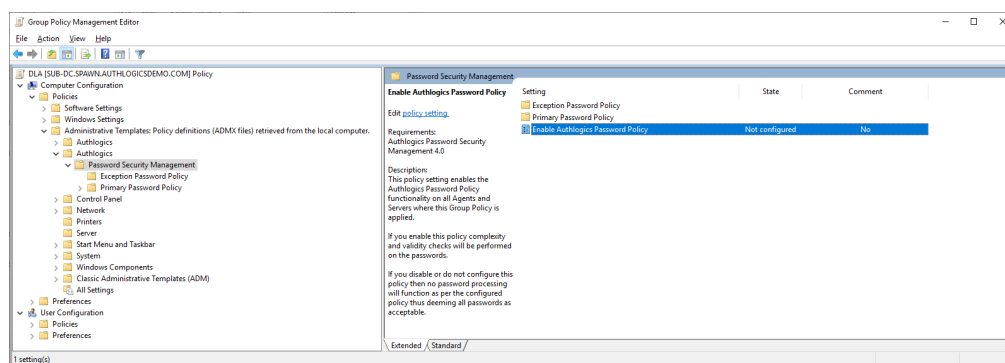
`C:\Program Files\Authlogics Authentication Server\`

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

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

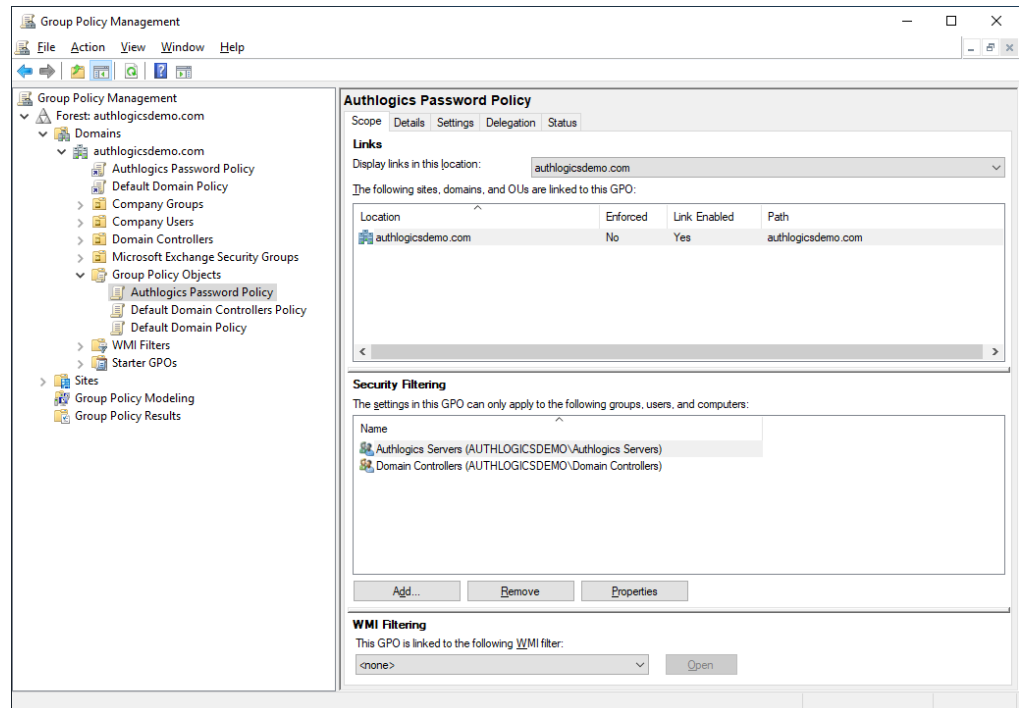
Note: For standalone deployments, you can copy the `.ADMx` files and `en-US` folders to the `C:\Windows\PolicyDefinitions` folder.

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**

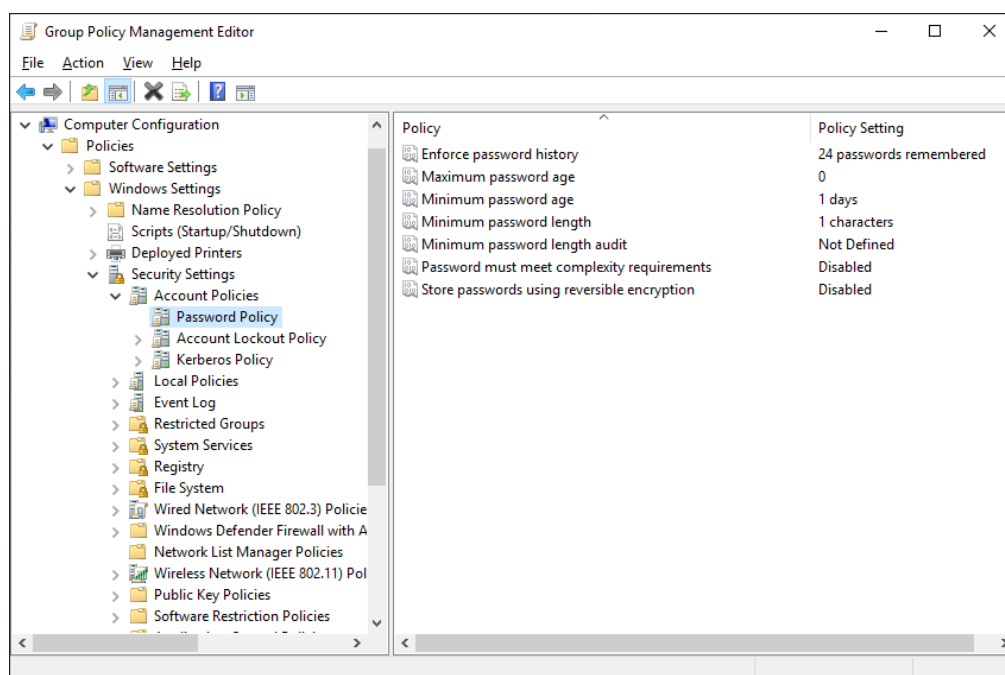
7. In the new the **Authlogics Password Policy** object:
 - a. Add a link to the Domain.
 - b. Configure the security filtering to **Authlogics Servers** and **Domain Controllers** groups only.



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:

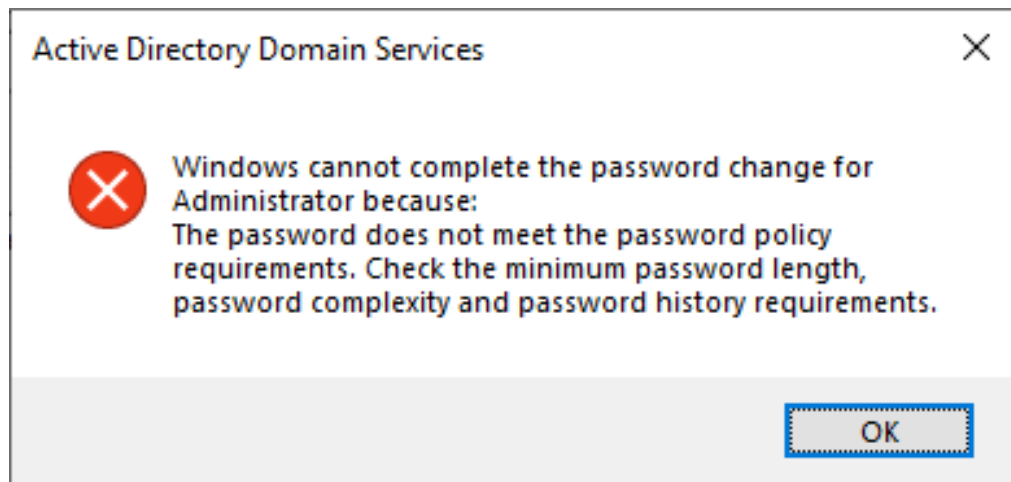
- Auth10g1c\$Test!
- IL0v3Coff33!
- H@ppyD@y5
- Sh@nk5t3r5!

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.

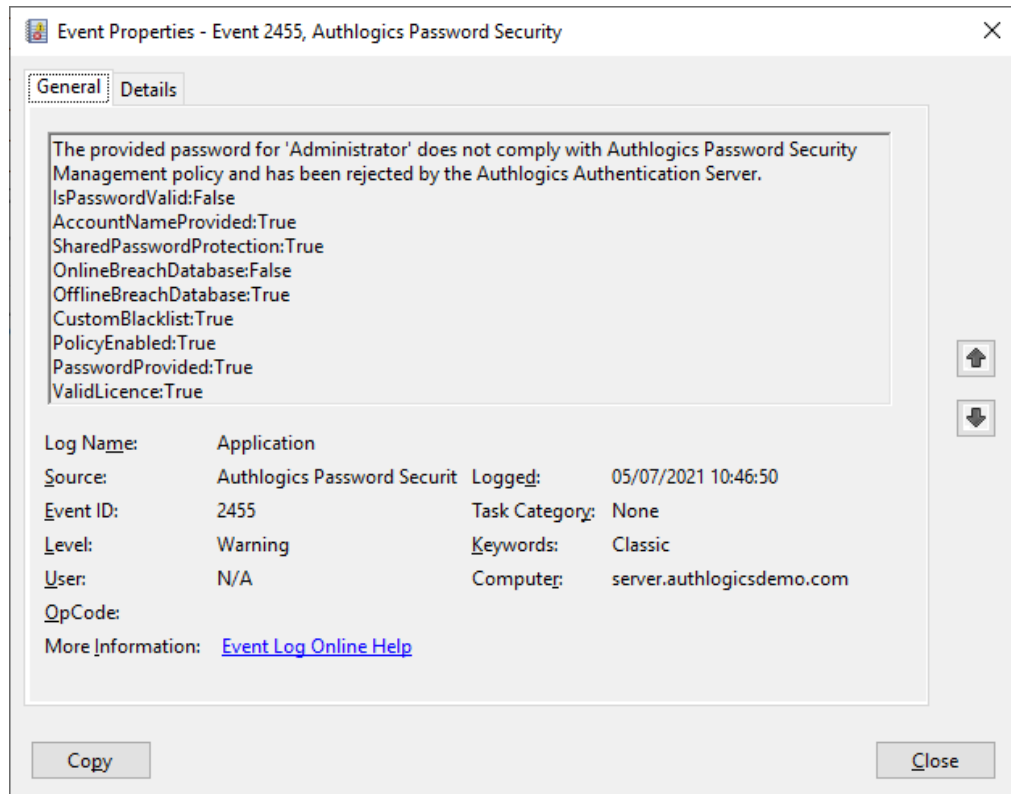
7.2 Testing password changes through Active Directory

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:
 - Auth10g1c\$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.

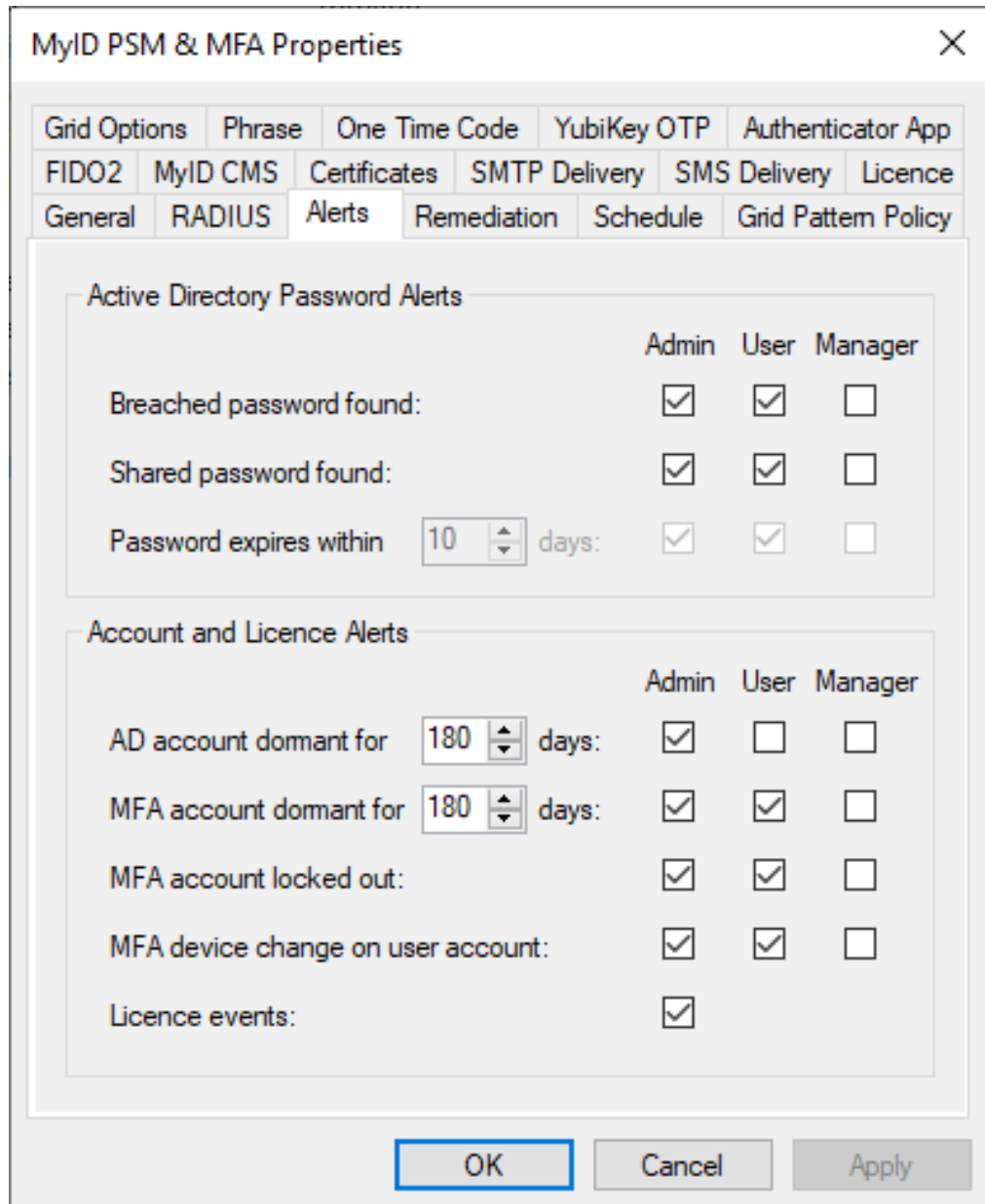
This shows an unsuccessful change, and includes the results of the checks that were performed.



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.



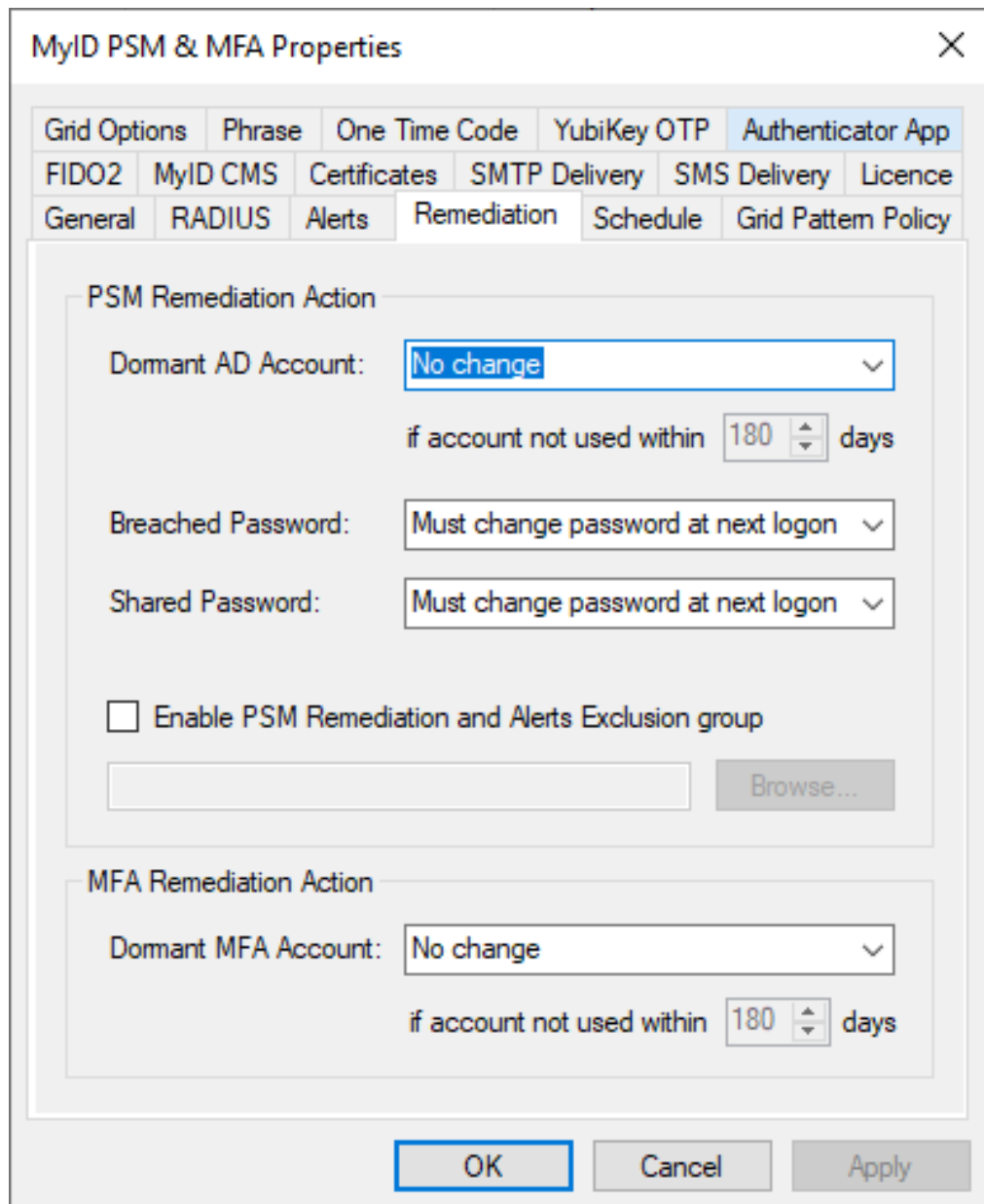
The image shows the 'MyID PSM & MFA Properties' dialog box with the 'Alerts' tab selected. The dialog has a title bar with a close button. Below the title bar is a tabbed interface with the following tabs: Grid Options, Phrase, One Time Code, YubiKey OTP, Authenticator App, FIDO2, MyID CMS, Certificates, SMTP Delivery, SMS Delivery, Licence, General, RADIUS, Alerts (selected), Remediation, Schedule, and Grid Pattern Policy. The 'Alerts' tab is divided into two sections: 'Active Directory Password Alerts' and 'Account and Licence Alerts'. Each section contains a list of alert types with checkboxes for 'Admin', 'User', and 'Manager'.

Active Directory Password Alerts			
	Admin	User	Manager
Breached password found:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shared password found:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Password expires within <input type="text" value="10"/> days:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Account and Licence Alerts			
	Admin	User	Manager
AD account dormant for <input type="text" value="180"/> days:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MFA account dormant for <input type="text" value="180"/> days:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
MFA account locked out:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
MFA device change on user account:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Licence events:	<input checked="" type="checkbox"/>		

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

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



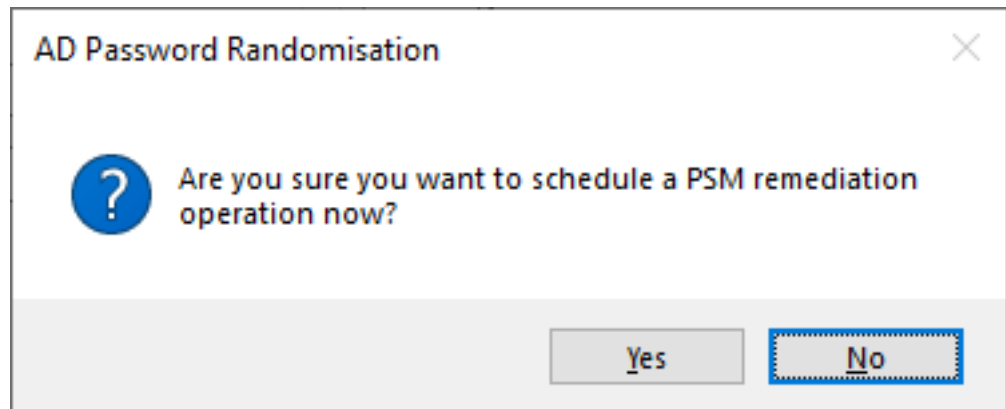
The image shows a screenshot of the 'MyID PSM & MFA Properties' dialog box, specifically the 'Remediation' tab. The dialog has a title bar with a close button (X) and a tabbed interface. The tabs include: Grid Options, Phrase, One Time Code, YubiKey OTP, Authenticator App, FIDO2, MyID CMS, Certificates, SMTP Delivery, SMS Delivery, Licence, General, RADIUS, Alerts, Remediation (selected), Schedule, and Grid Pattern Policy.

Under the 'Remediation' tab, there are two main sections:

- PSM Remediation Action:**
 - Dormant AD Account:** A dropdown menu set to 'No change'. Below it, a text field indicates 'if account not used within 180 days'.
 - Breached Password:** A dropdown menu set to 'Must change password at next logon'.
 - Shared Password:** A dropdown menu set to 'Must change password at next logon'.
 - ☐ **Enable PSM Remediation and Alerts Exclusion group**
 - A text input field with a 'Browse...' button next to it.
- MFA Remediation Action:**
 - Dormant MFA Account:** A dropdown menu set to 'No change'. Below it, a text field indicates 'if account not used within 180 days'.

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

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

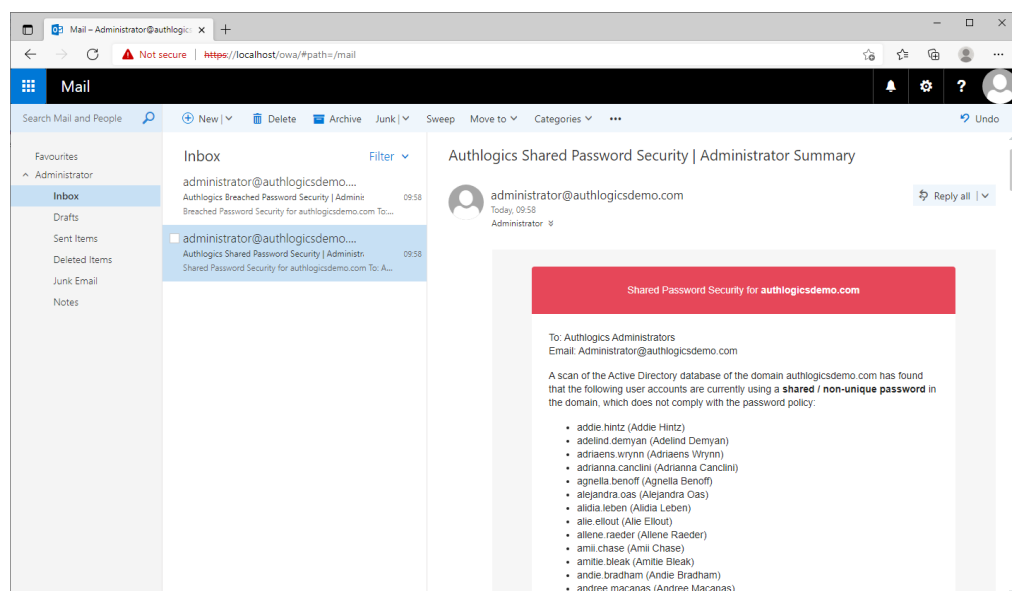


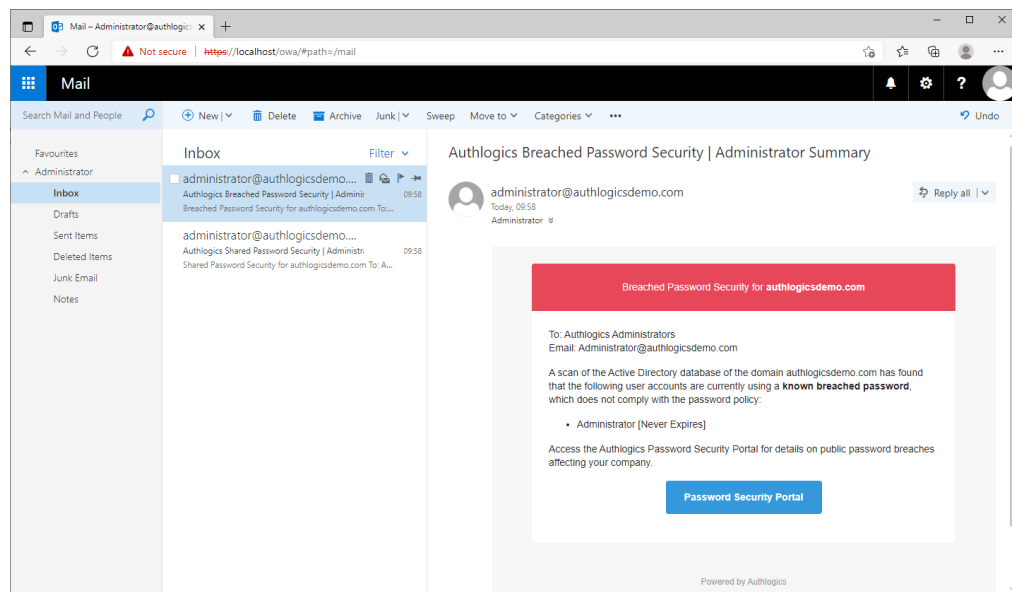
- b. Click **Yes**.
6. To avoid waiting for the schedule to run, open the Windows service control panel and restart the **MyID Authentication Server Service**.

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.





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

Addie Hintz Properties

Member Of Password Replication Dial-in Environment
Sessions Remote control Remote Desktop Services Profile COM+
General Address Account Profile Telephones Organization

User logon name:
 @authlogicsdemo.com

User logon name (pre-Windows 2000):

☐ Unlock account

Account options:

- ☒ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Store password using reversible encryption

Account expires

☒ Never

☐ End of:

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:

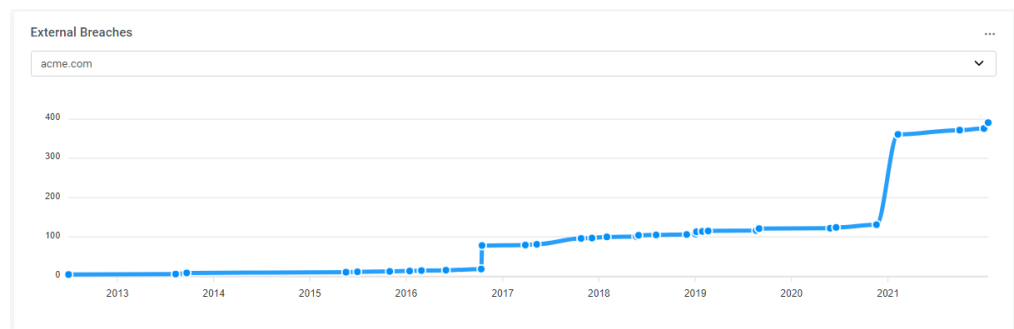
`https://<servername>:14443/admin`

Where <servername> is the name of your server.

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

This dashboard reflects contains information on:

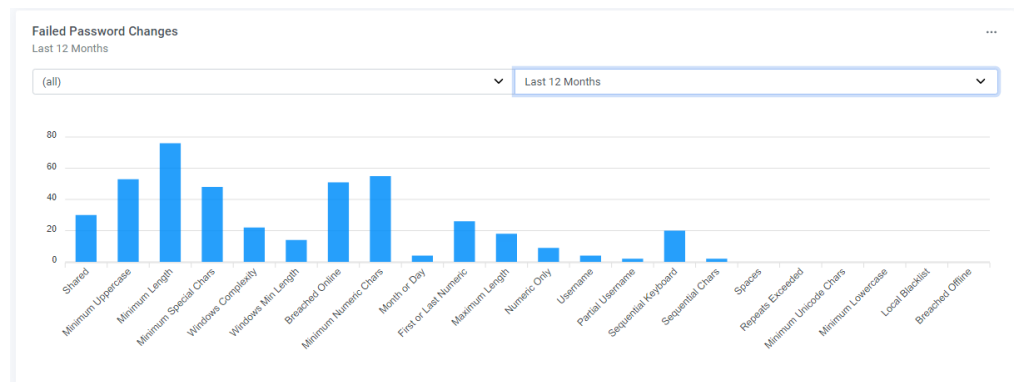
- External Breaches



- Total Accounts at Risk



- Failed Password Changes



• Accounts at Risk

