intercede

Authlogics

Password Security Management

Quick Start Guide

Product Version: 4.2.1030.0

Call us on: +44 1344 568 900 (UK/EMEA)
                +1 408 706 2866 (US)

Email us: sales@authlogics.com

Introduction

This guide provides an overview of the steps required to setup Authlogics Password Security Management in a new environment. For detailed information about a specific feature or deployment scenario please see the *Authlogics Authentication Server Installation and Configuration Guide.*

Considerations

(1) Authlogics Password Security Management requires a Windows Server and an Active Directory domain to be available before installation.
(2) A Domain Administrator / Enterprise Administrator account is required to perform the installation.
(3) After the installation, the server will require a reboot.
(4) Internet access to https://*.authlogics.com is required.

Required information

(1) AD administrator credentials.
(2) SMTP Server details: name, port, authentication requirements.
(3) The DNS name for the server.
(4) Understanding of which password policy settings to use.

# Installing the Authentication Server

(1) Download the Authentication Server installer from https://authlogics.com/downloads/ and extract the ZIP.

(2) Run the setup file in the *Install* folder.

(3) Follow the Installation Wizard instructions to install the product binaries.
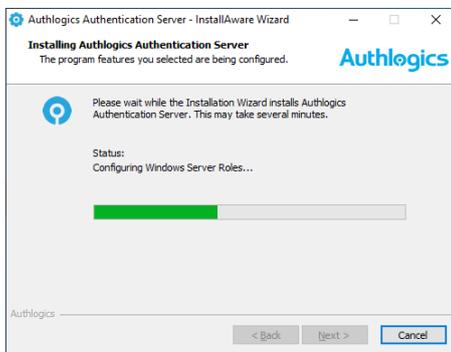
(4) Follow the Directory Configuration Wizard to setup the AD for use with Authlogics.
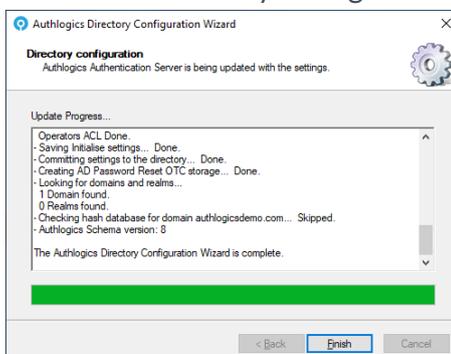
(5) Follow the Licence Wizard to configure a licence for Authlogics PSM. If you do not have a licence key the wizard can request a 30 day evaluation licence for you.
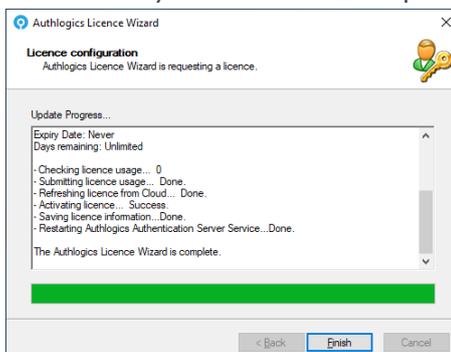
(6) **Reboot the Server** after the Authlogics Management Console loads to complete the initial setup.

Configuring the Authentication Server

(1) Launch the Authlogics Management Console, right click "Authlogics PSM" and select properties.
(2) Configure the SMTP Server settings to be able to deliver alerts and new user emails.

Running the PSM Wizard

(1) Right click "Authlogics PSM" and select "Password Security Management Wizard".
(2) Tick the domains in the forest to protect with PSM.
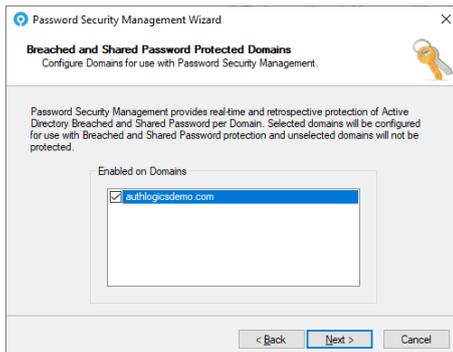
(3) Choose a schedule when PSM should look for new breached and shared passwords, as well as send alerts.
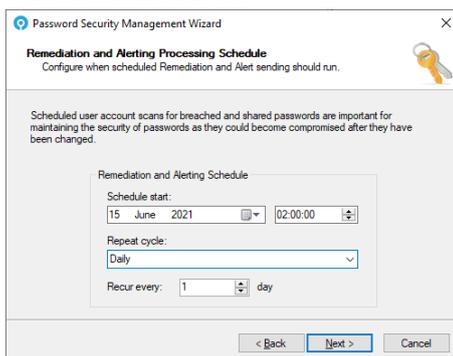
(4) Choose the action to take when breached and shared passwords are found.
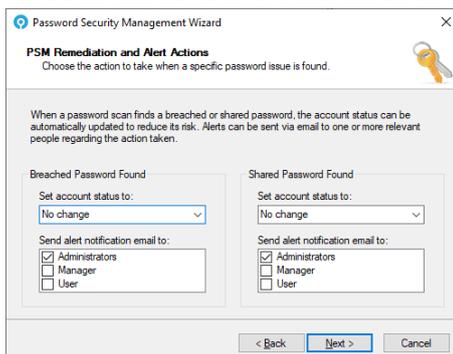
(5) Choose the action to take when dormant accounts are found
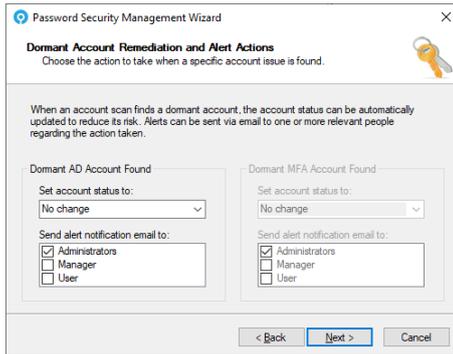
(6) PSM will protect all ENABLED user accounts in the domain. This can be limited to members of an AD group if required. This can be useful for gradual deployments of new policy settings to users, or if sufficient licences are not currently available.

(7) PSM will perform alerting and remediation on all PSM enabled user accounts. Accounts can be excluded from remediation and alerting by adding them to an AD group. This may be useful for service accounts.
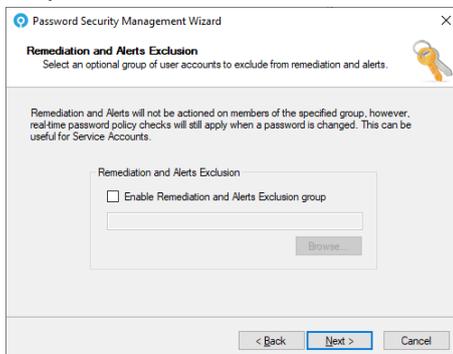

(8) Applying settings.
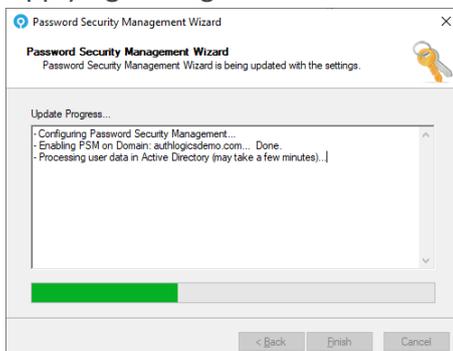
Applying the settings may take some time depending on how many users exist in the AD.

Install the Domain Controller Agent

The Domain Controller agent must be installed on ALL domain controllers in the domain to protect all password changes are protected. The domain controllers MUST be rebooted after the agent is installed. Installing the agent will have no effect on password changes until the policy is configured later on.

(1) Download the Domain Controller Agent installer from https://authlogics.com/downloads/ and extract the ZIP.

(2) Start the installation by running the "Authlogics Domain Controller Agent 4.0.xxxx.x.msi" file.
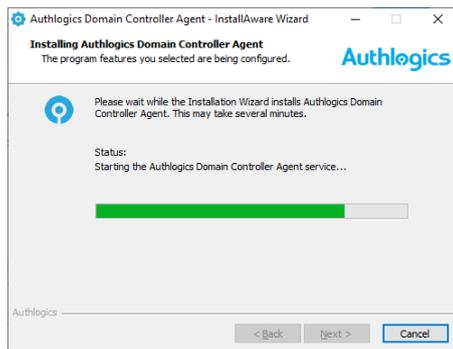
> 📝 **Note**
>
> If Windows does not allow the installer to be run due to a policy, simply start an Admin Command prompt and run the MSI from the command prompt to ensure it is launched with admin rights.

(3) Restart the Domain Controller when complete.
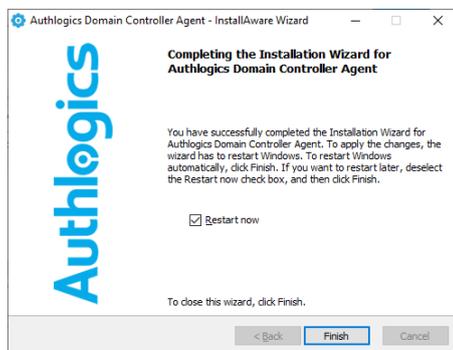
Configuring the Authlogics Password Policy

The Authlogics Password Policy is configured using Active Directory group policy. The policy must be applied to the Domain Controllers as well as the Authlogics Authentication Servers.

These steps are typically done on a Domain Controller however can be done from anywhere that has the AD management tools installed.

(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 "AuthlogicsDCAgent.admx" and "AuthlogicsPasswordPolicy.admx" template files. The templates can be found inside the downloaded ZIP files GPO folder, or the "C:\Program Files\Authlogics Authentication Server\" on the Authlogics Authentication Server.

(4) Expand the Authlogics Password Security Management policy tree and set "Enable Authlogics Password Policy" to Enabled.
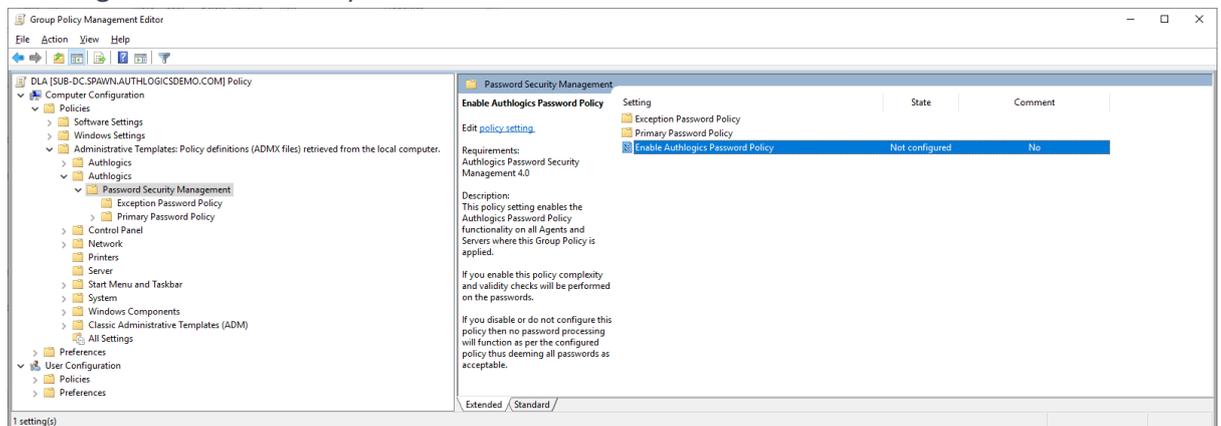
(5) Review the rest of the password policy options and set them accordingly. In most cases, the default complexity rules should suffice.
(6) We recommend enabling the following features:
    a. Enable Passphrases = Enabled
    b. Password Expiry Default Zone
    c. Password Never Expires Zone

(7) Link the new "Authlogics Password Policy" to the Domain. Configure the security filtering to "Domain Controllers" and "Authlogics Servers" groups only.
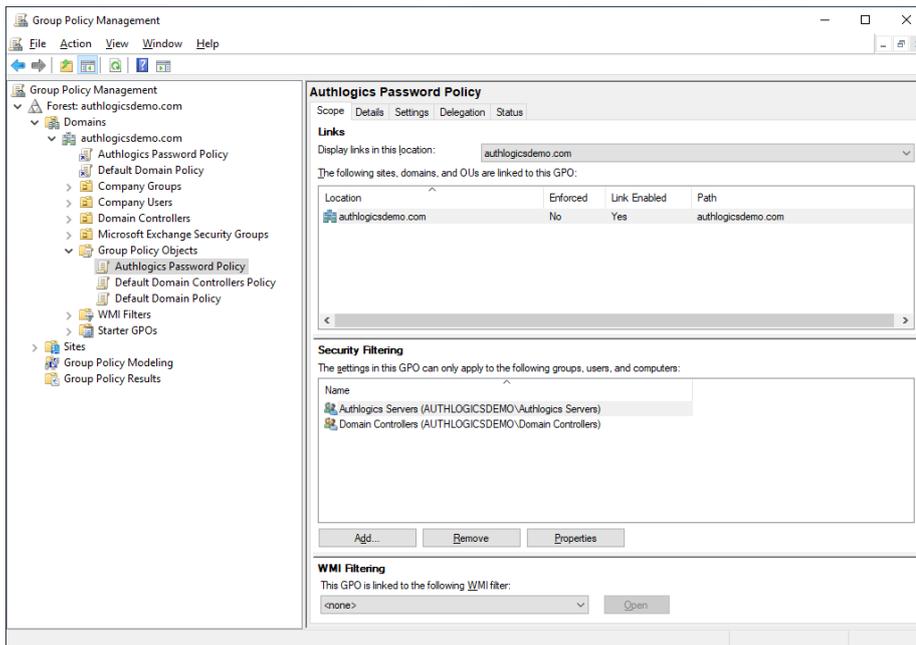
Disabling the Windows Password Policy

The Windows password policy must be disabled so that it does not conflict with the Authlogics password policy.

(1) Open the Group Policy Management Console.
(2) Edit the "Default Domain Policy".
(3) Change the following settings. The settings must be set to the specified values, DO NOT set them to "Not Defined":

    a. Maximum password age: 0

    b. Minimum password length: 1

    c. Passwords must meet complexity requirements: Disabled
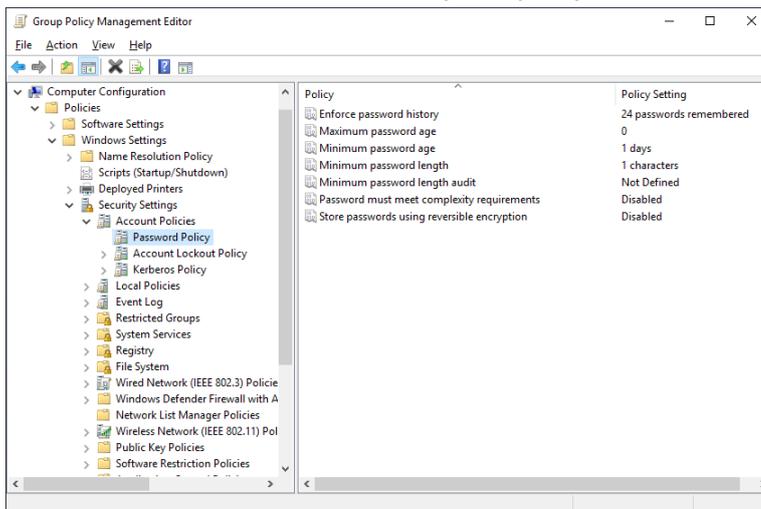
Testing password changes and schedules

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 avoid waiting this can be sped up by running "GPUPDATE /FORCE" from an admin command prompt and rebooting the server.

Testing password changes via the Self Service Portal

(1) On the Authlogics Authentication Server log in to the Self Service Portal.

(2) Enter some test passwords to see which pass/fail the current policy.

(3) The following "test" passwords are designed to pass most password complexity checked but are contained within our ONLINE breach database and thus should fail.

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

(4) When a valid password is entered, click "Change" to save it.
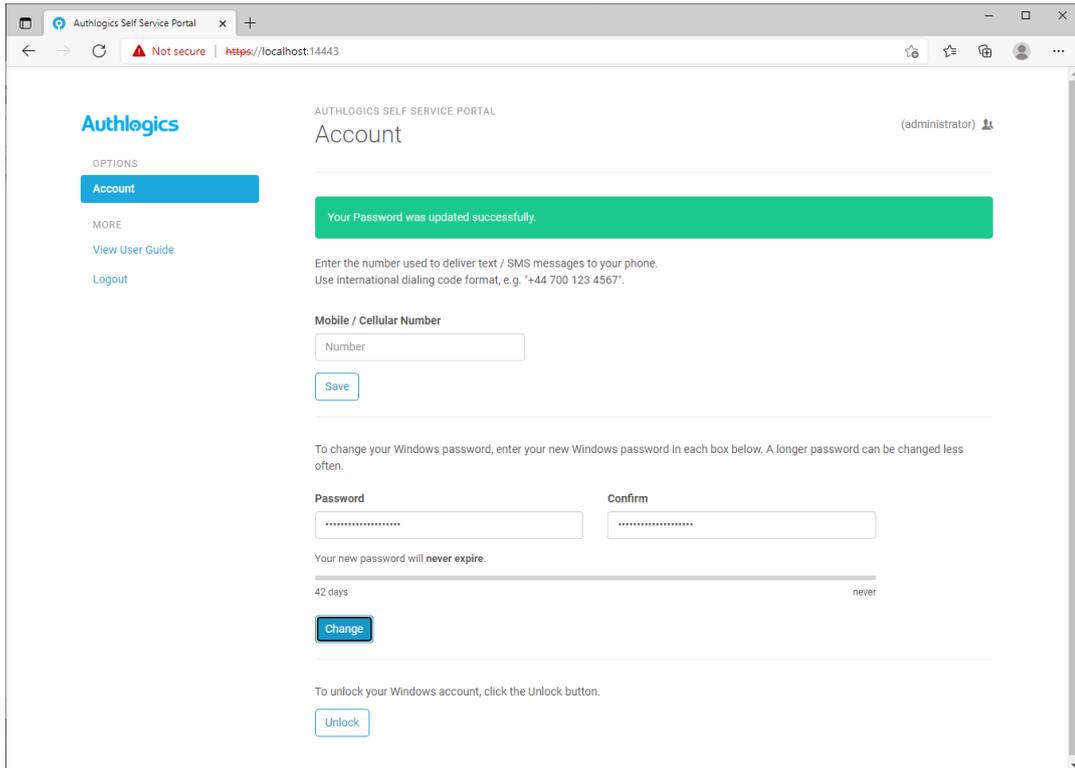
(5) Look for Event ID 1425 on the domain controller Application Event Log showing the successful change.
(6) Look for Event ID 1400 on the Authlogics Authentication Server Application Event Log showing the successful change.

Testing password changes via 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, e.g:

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

(4) Ensure the password is not accepted.
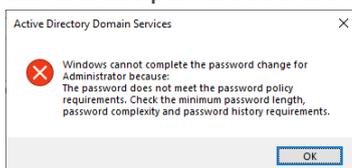
(4) Look for Event ID 2455 on the domain controller Application Event Log showing the unsuccessful change, including the results of the checks that were performed.
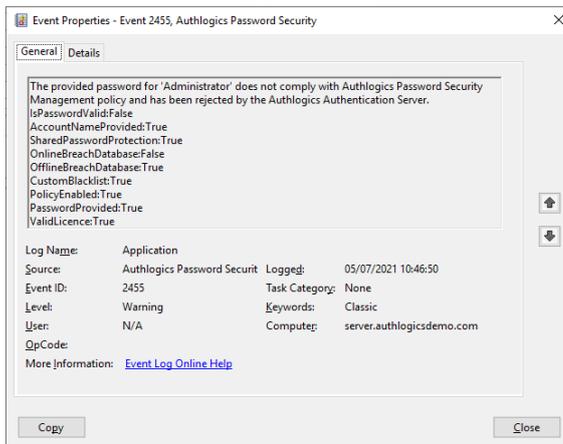

> 📝 **Note**
>
> Event ID 2455 will appear twice when resets are performed via Active Directory Users and Computers due to a known issue with the Active Directory Users and Computers tool. This does not happen during normal user password changes.

Testing Alerting and Remediation

(1) Ensure alerts are enabled for the administrators and users.
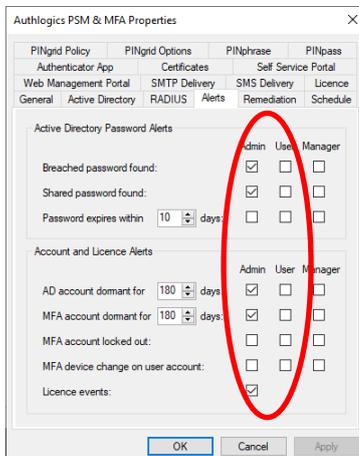
(2) Ensure remediation is configured.
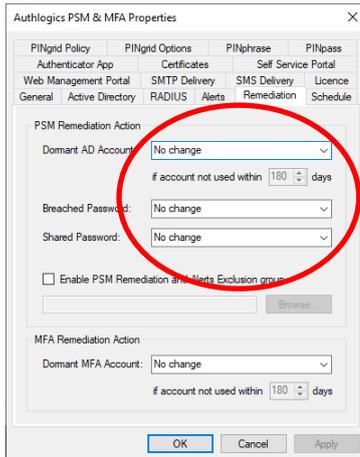
(3) On the schedule tab, click "Run Now" and click "Yes".
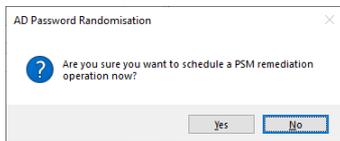
(4) To avoid waiting up to 15 mins for the schedule to run simply restart the "Authlogics Authentication Server" Windows service.

(5) Look for Event IDs 1966 and 1962 on the Authlogics Authentication Server Application Event Log to show when the tasks have completed. Also look for Event ID 1953 to see when the schedule will next run.

(6) Check the user and administrator mailbox for alters:
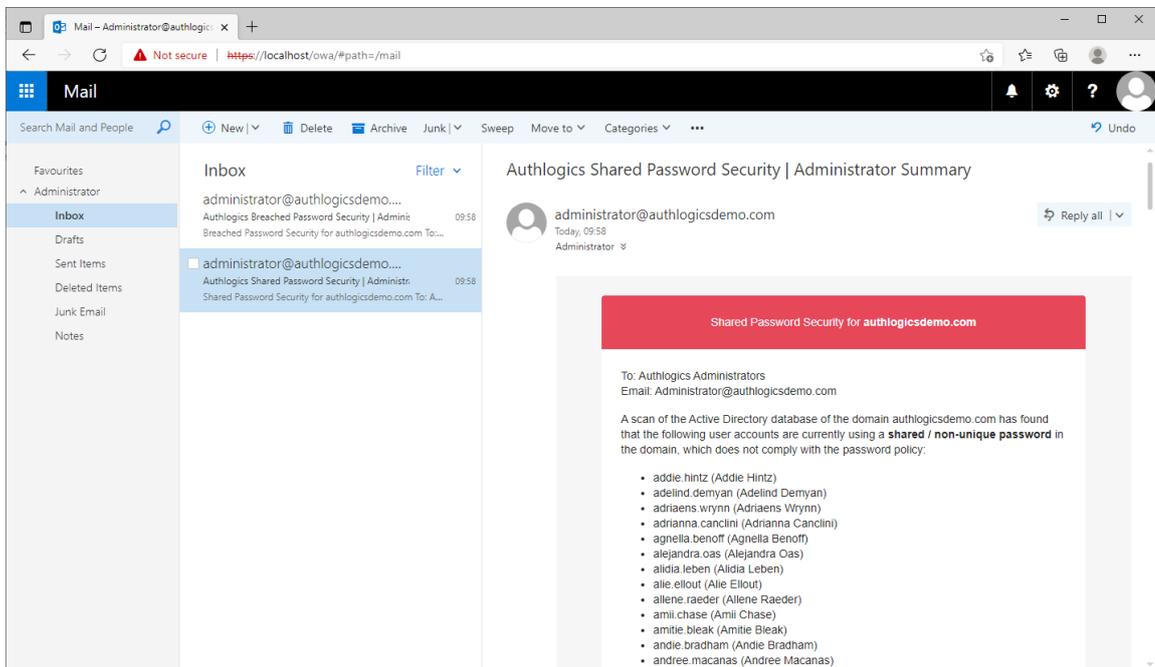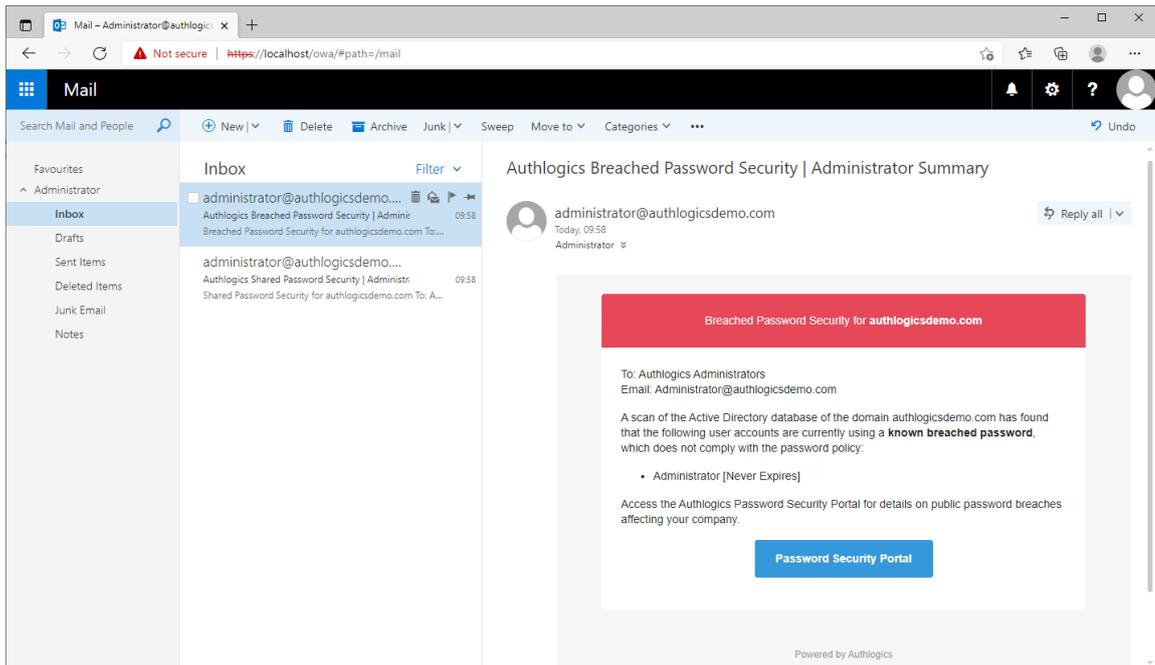
(7) Verify the remediation action was performed on the reported accounts:
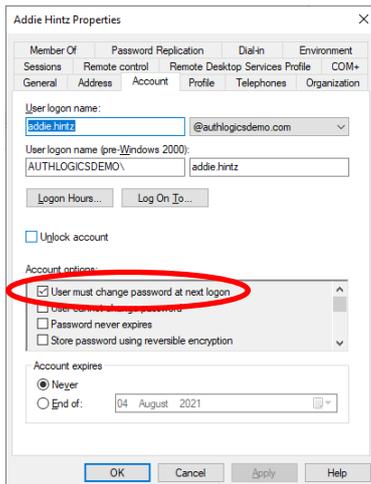
Monitoring PSM Usage

Authlogics Server includes a Dashboard to graphically display the state of your PSM deployment.

Launch the Authlogics Admin portal via https://localhost:14443/admin.

Select System – Dashboards – Password Security.

The dashboard reflects MFA actions for:

- External Breaches
- Total Accounts at Risk
- Failed Password Changes
- Accounts at Risk

Failed Password Changes
Last 12 Months

(all) ▾   Last 12 Months ▾

Chart categories (x-axis): Shared, Windows Complexity, Windows Min Length, Breached Online, Minimum Length, Minimum Uppercase, Minimum Numeric Chars, Month or Day, First or Last Numeric, Maximum Length, Minimum Special Chars, Local Blacklist, Numeric Only, Username, Partial Username, Sequential Keyboard, Sequential Chars, Minimum Lowercase, Spaces, Repeats Exceeded, Minimum Unicode Chars, Breached Offline

Accounts At Risk
Latest

(all) ▾

- ● Shared
- ● Breached
- ● Blank
- ● Expiring
- ● Dormant

30.0%
20.0%
50.0%

Shared

Account Name
jordans
dj
ghiggo

☰ View All