Password Security Management

MyID PSM Quick Start Guide

Product Version: 5.0.6942.0

Publication date: March 2024

Call us on:	+44 (0)1455 558 111 (UK & EMEA) +1 408 706 2866 (US)
Email us:	info@intercede.com

Intercede Ltd, Lutterworth Hall, St. Mary's Road, Lutterworth, Leicestershire, LE17 4PS, United Kingdom
UK Tel: +44 (0)1455 558 111   US Tel: +1 888 646 6943   email: info@intercede.com   web: www.intercede.com

Introduction

> **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.

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

Considerations

(1) MyID 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) Add AD accounts of MyID administrators to the Authlogics Administrators AD security group.
(4) After the installation, the server will require a reboot.
(5) 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.

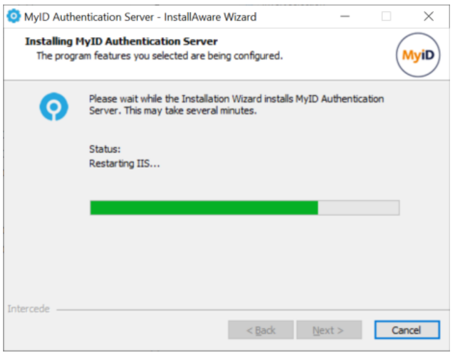
intercede

Installing the Authentication Server

(1) Download the Authentication Server installer from https://www.intercede.com/support/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.



MyID Authentication Server - InstallAware Wizard

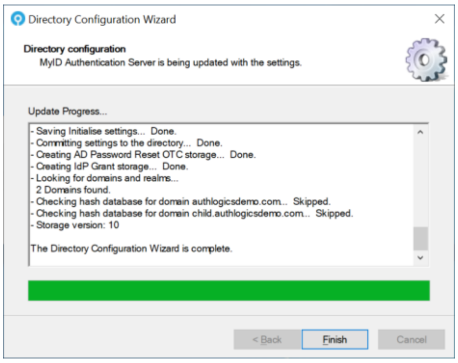
Installing MyID Authentication Server

The program features you selected are being configured.

Please wait while the Installation Wizard installs MyID Authentication Server. This may take several minutes.

Status:
Restarting IIS...

(4) Follow the Directory Configuration Wizard to setup the AD for use with MyID.



Directory Configuration Wizard

Directory configuration

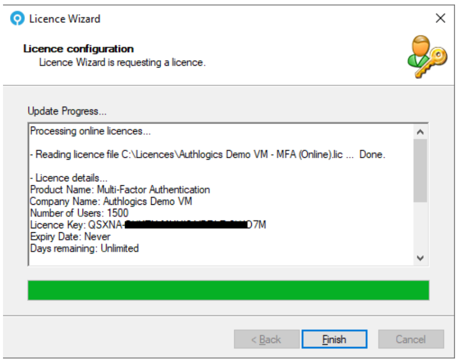
MyID Authentication Server is being updated with the settings.

Update Progress...

```
- Saving Initialise settings...  Done.
- Committing settings to the directory...  Done.
- Creating AD Password Reset OTC storage...  Done.
- Creating IdP Grant storage...  Done.
- Looking for domains and realms...
  2 Domains found.
- Checking hash database for domain authlogicsdemo.com...  Skipped.
- Checking hash database for domain child.authlogicsdemo.com...  Skipped.
- Storage version: 10

The Directory Configuration Wizard is complete.
```

(5) Follow the Licence Wizard to configure a licence for MyID PSM. If you do not have a licence key the wizard can request a 30 day evaluation licence for you.



Licence Wizard

Licence configuration

Licence Wizard is requesting a licence.

Update Progress...

```
Processing online licences...

- Reading licence file C:\Licences\Authlogics Demo VM - MFA (Online).lic ...  Done.

- Licence details...
Product Name: Multi-Factor Authentication
Company Name: Authlogics Demo VM
Number of Users: 1500
Licence Key: QSXNA-[redacted]D7M
Expiry Date: Never
Days remaining: Unlimited
```

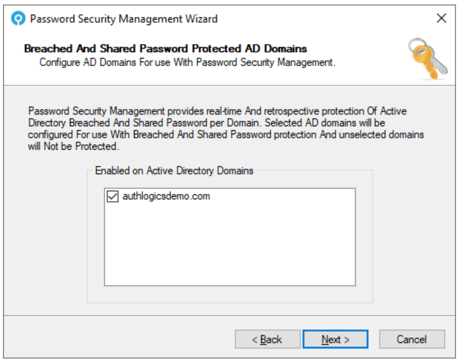
(6) **Reboot the Server** after the MyID Management Console loads to complete the initial setup.

Configuring the Authentication Server

(1) Launch the MyID Management Console, right click “MyID 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 “MyID PSM” and select “Password Security Management Wizard”.
(2) Tick the domains in the forest to protect with PSM.



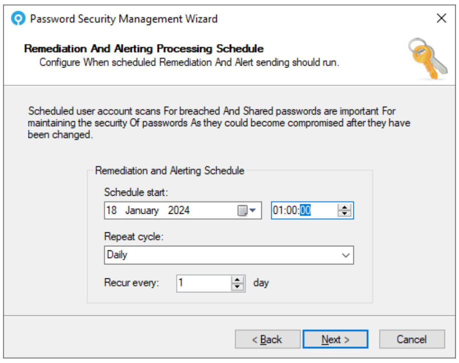
Password Security Management Wizard

Breached And Shared Password Protected AD Domains
Configure AD Domains For use With Password Security Management.

Password Security Management provides real-time And retrospective protection Of Active Directory Breached And Shared Password per Domain. Selected AD domains will be configured For use With Breached And Shared Password protection And unselected domains will Not be Protected.

Enabled on Active Directory Domains
☑ authlogicsdemo.com

(3) Choose a schedule when PSM should look for new breached and shared passwords, as well as send alerts.



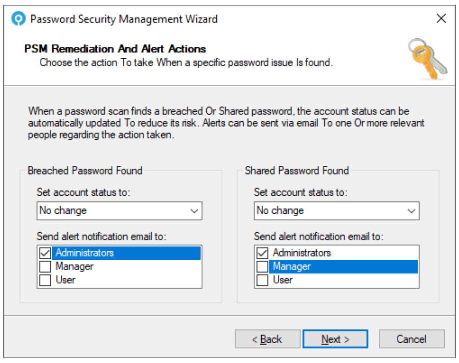
Password Security Management Wizard

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 01:00:00
Repeat cycle: Daily
Recur every: 1 day

(4) Choose the action to take when breached and shared passwords are found.



Password Security Management Wizard

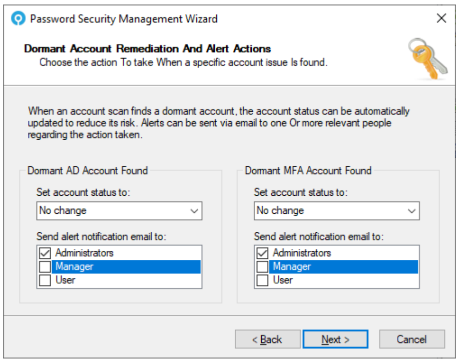
PSM Remediation And Alert Actions
Choose the action To take When a specific password issue Is found.

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

(5) Choose the 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

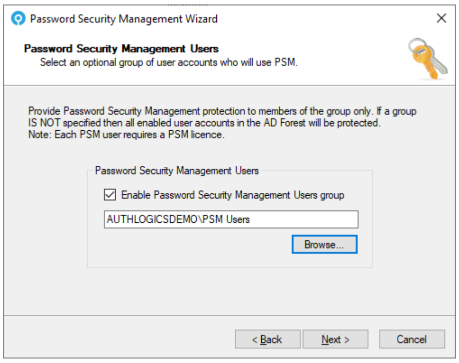
Send alert notification email to:
☑ Administrators
☐ Manager
☐ User

Dormant MFA Account Found

Set account status to: No change

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

(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.



Password Security Management Wizard

Password Security Management Users
Select an optional group of user accounts who will use PSM.

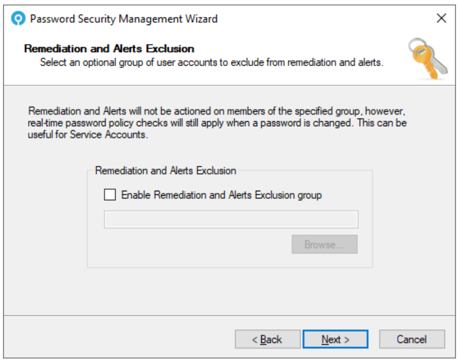
Provide Password Security Management protection to members of the group only. If a group IS NOT specified then all enabled user accounts in the AD Forest will be protected.
Note: Each PSM user requires a PSM licence.

Password Security Management Users

☑ Enable Password Security Management Users group

AUTHLOGICSDEMO\PSM Users

(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.



Password Security Management Wizard

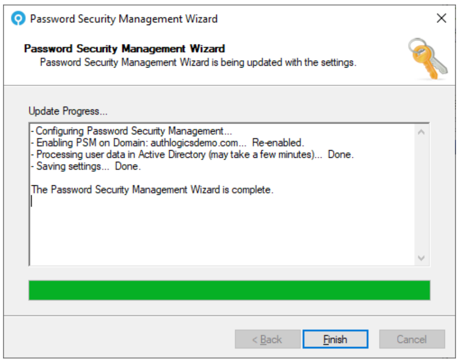
Remediation and Alerts Exclusion
Select an optional group of user accounts to exclude from remediation and alerts.

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.

Remediation and Alerts Exclusion

☐ Enable Remediation and Alerts Exclusion group

(8) Applying settings.



Password Security Management Wizard

Password Security Management Wizard
Password Security Management Wizard is being updated with the settings.

Update Progress...

```
- Configuring Password Security Management...
- Enabling PSM on Domain: authlogicsdemo.com...  Re-enabled.
- Processing user data in Active Directory (may take a few minutes)...  Done.
- Saving settings...  Done.

The Password Security Management Wizard is complete.
```

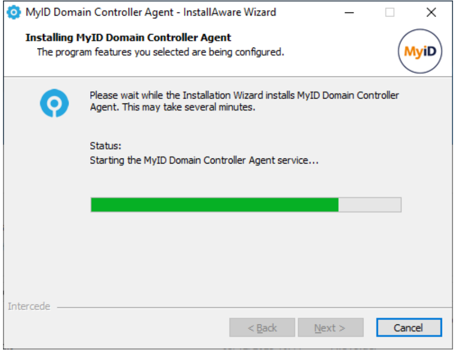
Applying the settings may take some time depending on how many users exist in the AD.

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://www.intercede.com/support/downloads and extract the ZIP.

(1) Start the installation by running the "MyID Domain Controller Agent 5.0.xxxx.x.msi" file.



MyID Domain Controller Agent - InstallAware Wizard

Installing MyID Domain Controller Agent

The program features you selected are being configured.

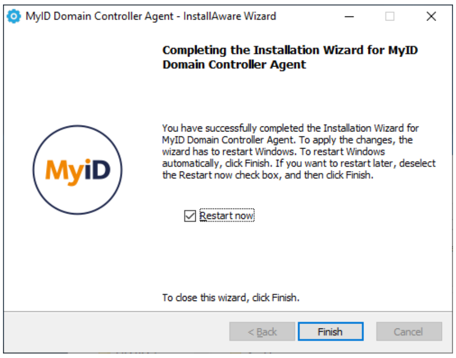
Please wait while the Installation Wizard installs MyID Domain Controller Agent. This may take several minutes.

Status:
Starting the MyID Domain Controller Agent service...

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.

(2) Restart the Domain Controller when complete.



MyID Domain Controller Agent - InstallAware Wizard

Completing the Installation Wizard for MyID Domain Controller Agent

You have successfully completed the Installation Wizard for MyID Domain Controller Agent. To apply the changes, the wizard has to restart Windows. To restart Windows automatically, click Finish. If you want to restart later, deselect the Restart now check box, and then click Finish.

☑ Restart now

To close this wizard, click Finish.

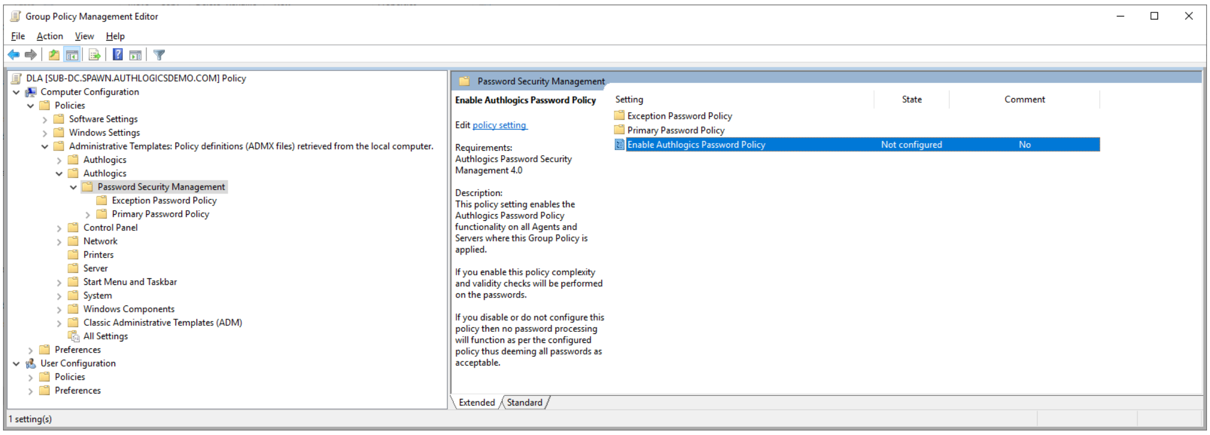
Configuring the MyID Password Policy

The MyID Password Policy is configured using Active Directory group policy. The policy must be applied to the Domain Controllers as well as the MyID 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 “Authlogics.admx”, “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 MyID 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, the “.ADMx” files and “en-US” folders can be copied to the C:\Windows\PolicyDefinitions folder.

(4) Expand the Authlogics Password Security Management policy tree and set “Enable Authlogics Password Policy” to Enabled.



Enable Authlogics Password Policy

Edit policy setting

Requirements:
Authlogics Password Security Management 4.0

Description:
This policy setting enables the Authlogics Password Policy functionality on all Agents and Servers where this Group Policy is applied.

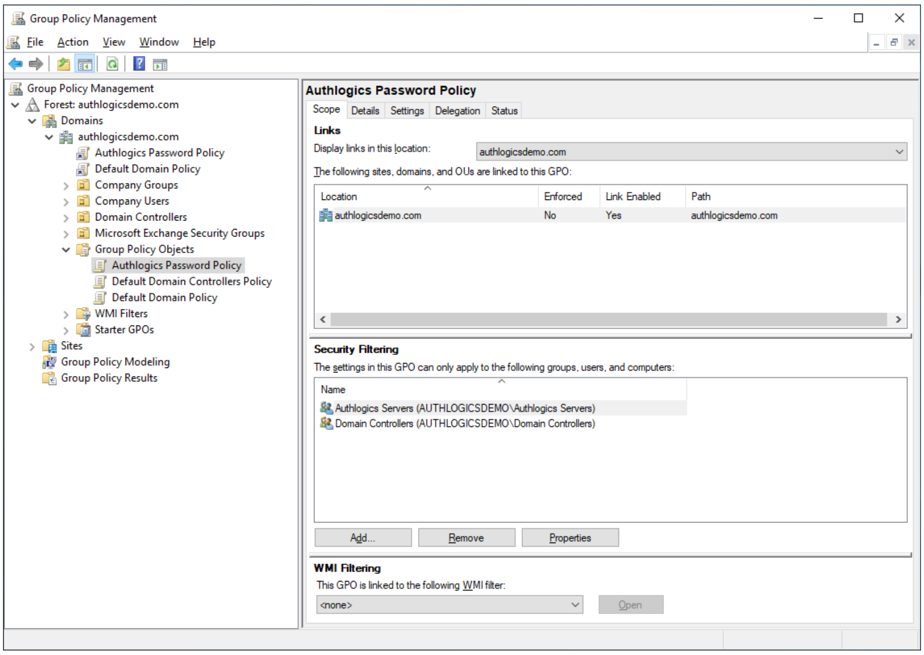
If you enable this policy complexity and validity checks will be performed on the passwords.

If you disable or do not configure this policy then no password processing will function as per the configured policy thus deeming all passwords as acceptable.

Setting	State	Comment
Exception Password Policy		
Primary Password Policy		
Enable Authlogics Password Policy	Not configured	No

(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.



Authlogics Password Policy

Links

Display links in this location: authlogicsdemo.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
authlogicsdemo.com	No	Yes	authlogicsdemo.com

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authlogics Servers (AUTHLOGICSDEMO\Authlogics Servers)
Domain Controllers (AUTHLOGICSDEMO\Domain Controllers)

WMI Filtering

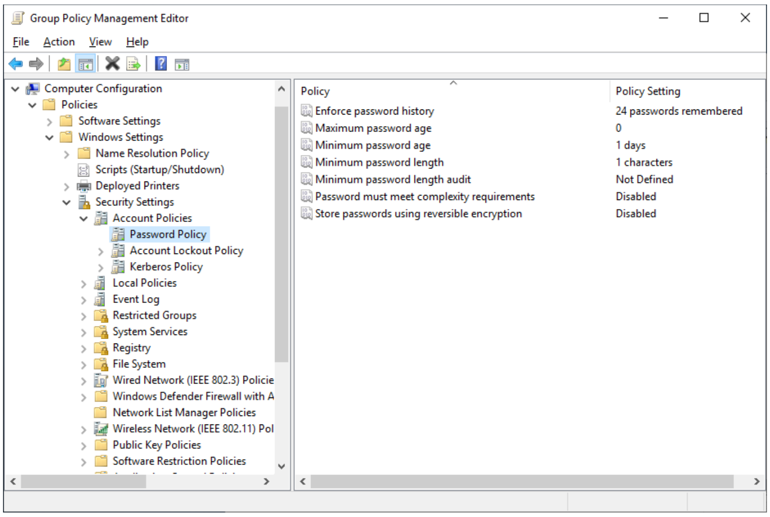
This GPO is linked to the following WMI filter:

<none>

Disabling the Windows Password Policy

The Windows password policy must be disabled 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. 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



- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout Policy
          - Kerberos Policy
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Policie
        - Windows Defender Firewall with A
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11) Pol
        - Public Key Policies
        - Software Restriction Policies

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	0
Minimum password age	1 days
Minimum password length	1 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

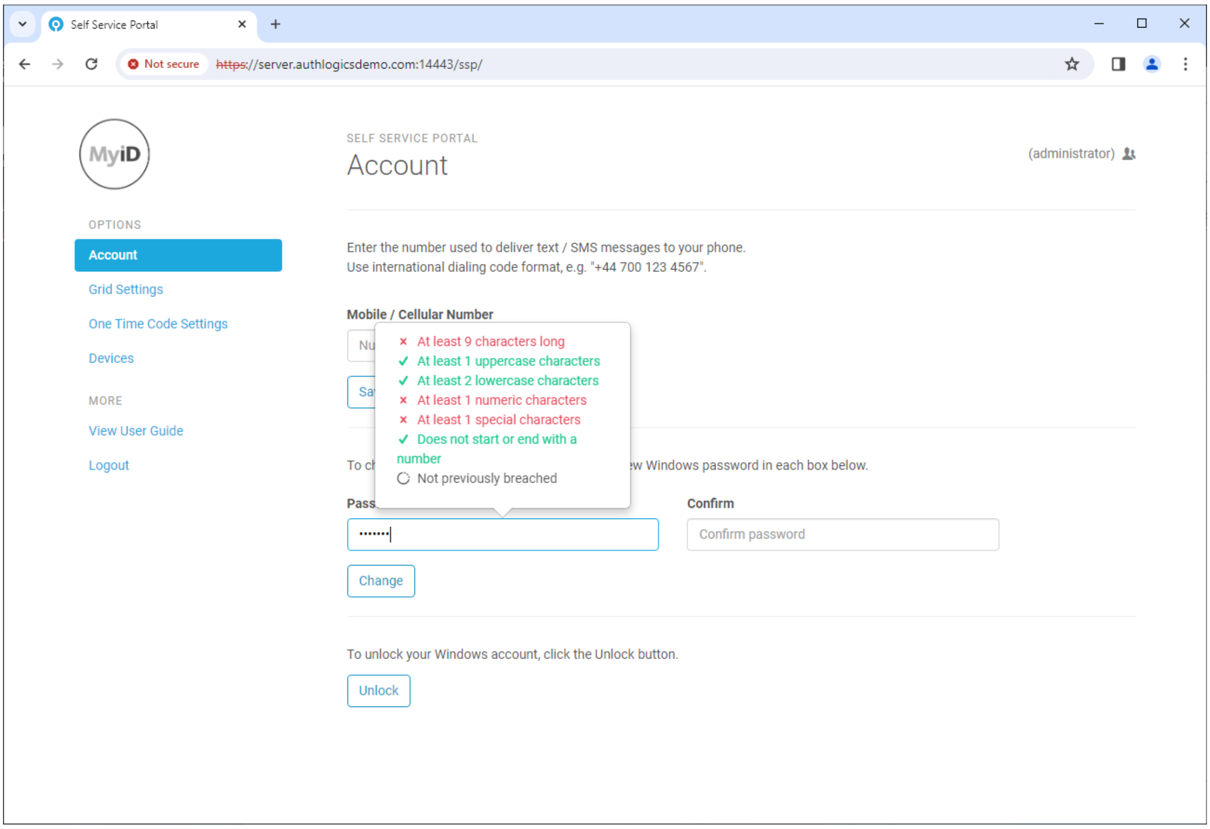
Testing password changes and schedules

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 MyID Authentication Server log in to the Self Service Portal.

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



Enter the number used to deliver text / SMS messages to your phone.
Use international dialing code format, e.g. "+44 700 123 4567".

To ch... ...w Windows password in each box below.

- ✗ At least 9 characters long
- ✓ At least 1 uppercase characters
- ✓ At least 2 lowercase characters
- ✗ At least 1 numeric characters
- ✗ At least 1 special characters
- ✓ Does not start or end with a number
- ○ Not previously breached

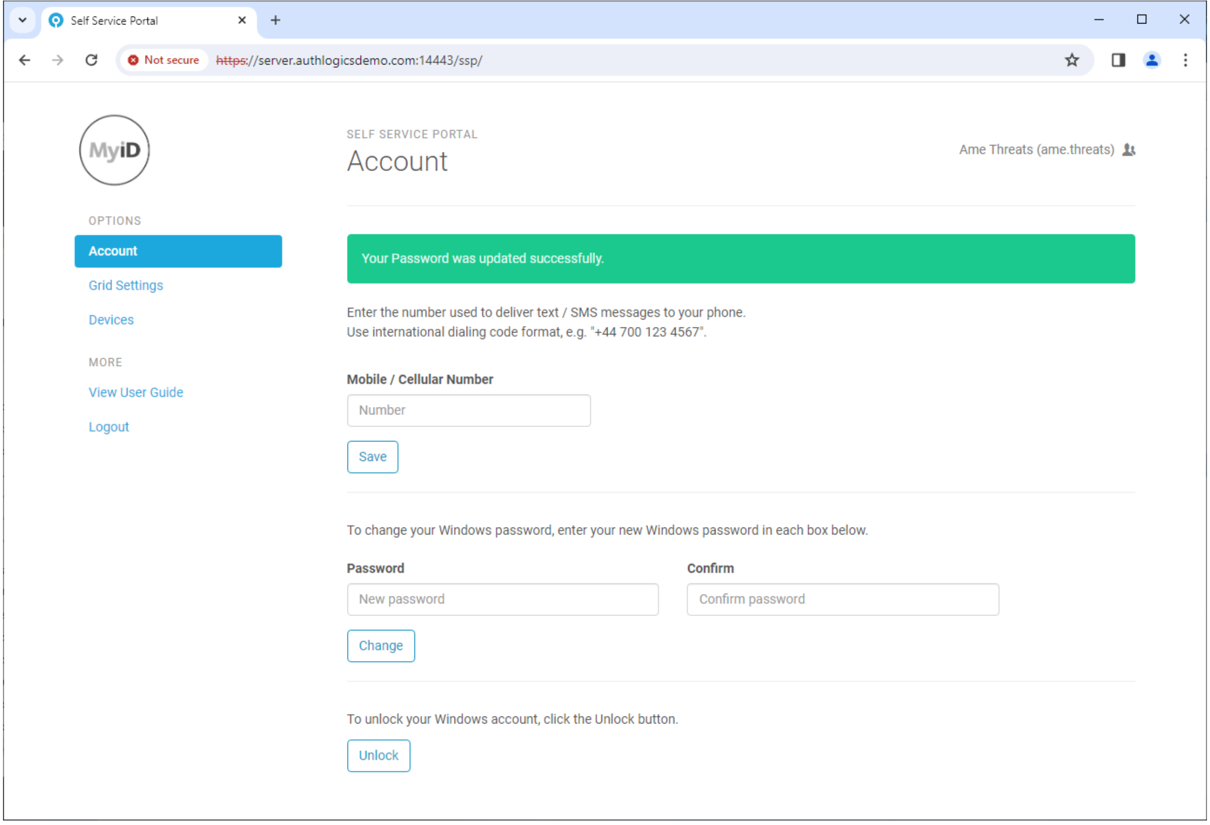
Password: •••••••

To unlock your Windows account, click the Unlock button.

(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!`

(3) When a valid password is entered, click “Change” to save it.



SELF SERVICE PORTAL

Account

Ame Threats (ame.threats)

Your Password was updated successfully.

Enter the number used to deliver text / SMS messages to your phone.
Use international dialing code format, e.g. "+44 700 123 4567".

Mobile / Cellular Number: Number

To change your Windows password, enter your new Windows password in each box below.

Password: New password

Confirm: Confirm password

To unlock your Windows account, click the Unlock button.

(4) Look for Event ID 1425 on the domain controller Application Event Log showing the successful change.

(5) Look for Event ID 1400 on the MyID Authentication Server Application Event Log showing the successful change.

Testing password changes via Active Directory

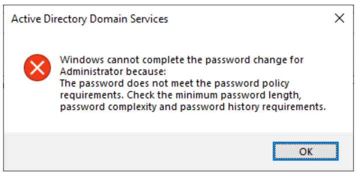
(1) On the Domain Controller open Active Directory Users and Computers.

(2) Locate a test user account, right click and select “Reset Password…”

(3) Enter a known non-complaint password, e.g:

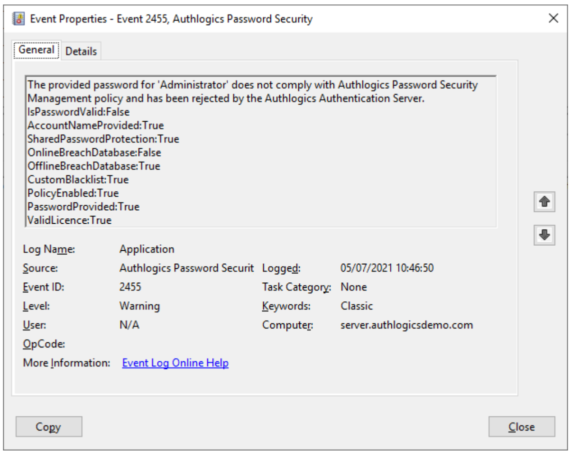
- `Authl0g1c$Test!`
- `IL0v3Coff33!`
- `H@ppyD@y5`
- `Sh@nk5t3r5!`

(4) Ensure the password is not accepted.



Windows cannot complete the password change for Administrator because:
The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.

(2) 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.



```
The provided password for 'Administrator' does not comply with Authlogics Password Security
Management policy and has been rejected by the Authlogics Authentication Server.
IsPasswordValid:False
AccountNameProvided:True
SharedPasswordProtection:True
OnlineBreachDatabase:False
OfflineBreachDatabase:True
CustomBlacklist:True
PolicyEnabled:True
PasswordProvided:True
ValidLicence:True
```

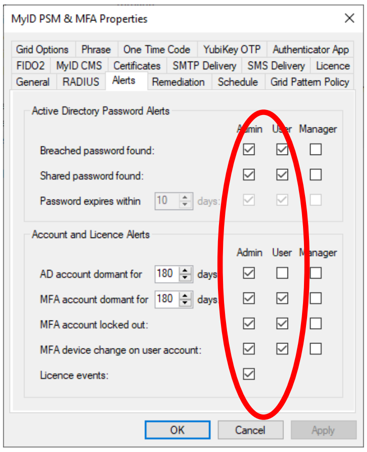
Log Name:	Application		
Source:	Authlogics Password Securit	Logged:	05/07/2021 10:46:50
Event ID:	2455	Task Category:	None
Level:	Warning	Keywords:	Classic
User:	N/A	Computer:	server.authlogicsdemo.com
OpCode:			
More Information:	Event Log Online Help		

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.



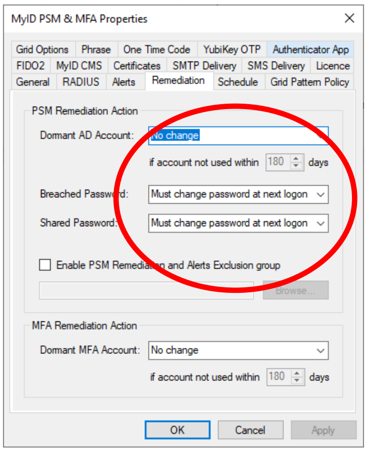
Active Directory Password Alerts

	Admin	User	Manager
Breached password found:	☑	☑	☐
Shared password found:	☑	☑	☐
Password expires within 10 days:	☑	☑	☐

Account and Licence Alerts

	Admin	User	Manager
AD account dormant for 180 days:	☑	☐	☐
MFA account dormant for 180 days:	☑	☑	☐
MFA account locked out:	☑	☑	☐
MFA device change on user account:	☑	☑	☐
Licence events:	☑		

(2) Ensure remediation is configured.



PSM Remediation Action

Dormant AD Account: No change

if account not used within 180 days

Breached Password: Must change password at next logon

Shared Password: Must change password at next logon

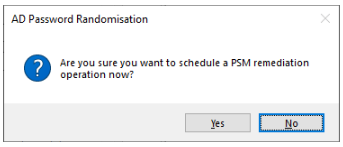
☐ Enable PSM Remediation and Alerts Exclusion group

MFA Remediation Action

Dormant MFA Account: No change

if account not used within 180 days

(3) On the schedule tab, click “Run Now” and click “Yes”.

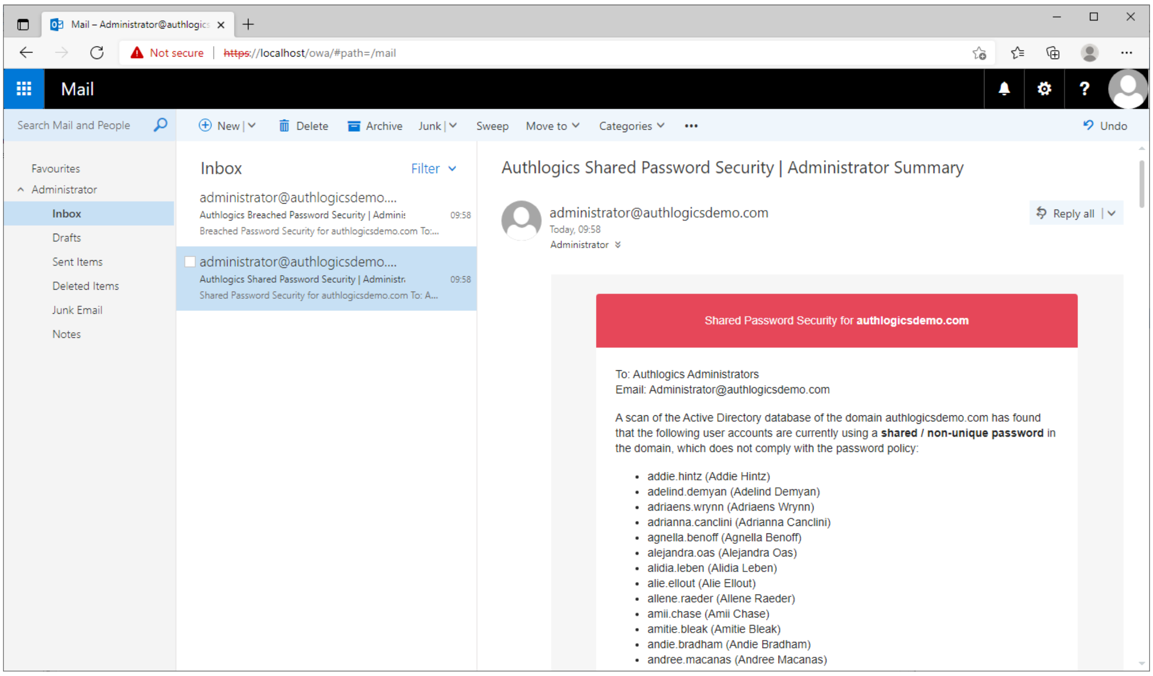


Are you sure you want to schedule a PSM remediation operation now?

(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 MyID 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:



Inbox

administrator@authlogicsdemo....
Authlogics Breached Password Security | Adminis 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 Shared Password Security | Administrator Summary

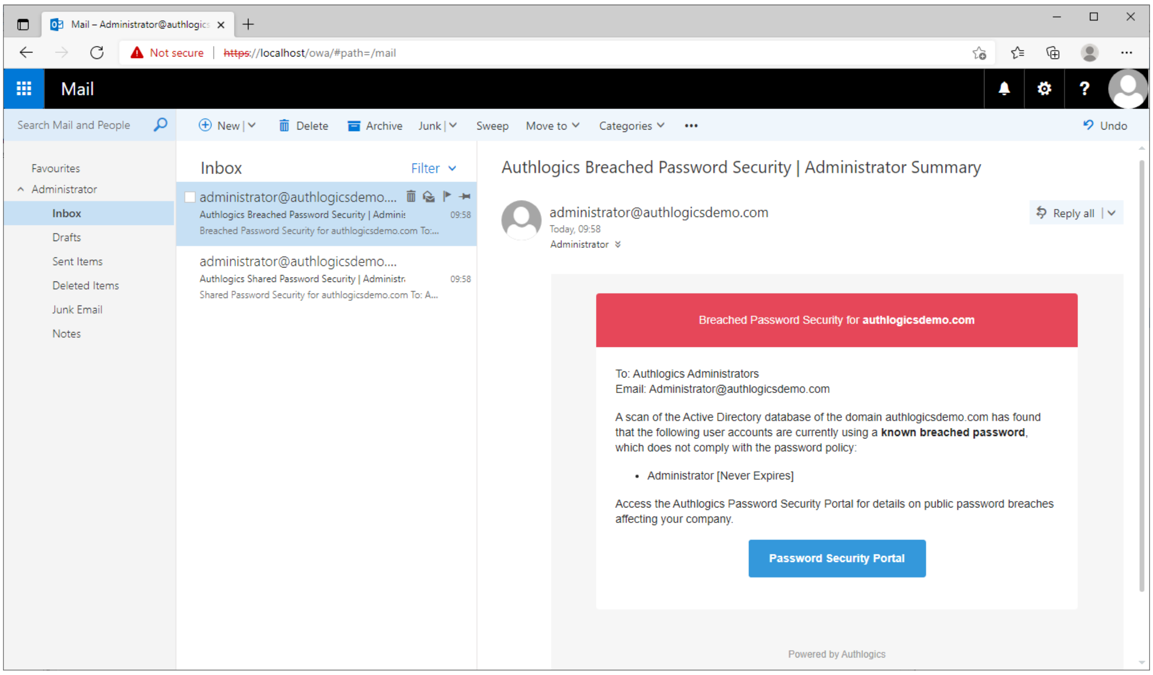
administrator@authlogicsdemo.com
Today, 09:58
Administrator

Shared 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 **shared / non-unique password** in the domain, which does not comply with the password policy:

- addie.hintz (Addie Hintz)
- adelind.demyan (Adelind Demyan)
- adriaens.wrynn (Adriaens Wrynn)
- adrianna.canclini (Adrianna Canclini)
- agnella.benoff (Agnella Benoff)
- alejandra.oas (Alejandra Oas)
- alidia.leben (Alidia Leben)
- alie.ellout (Alie Ellout)
- allene.raeder (Allene Raeder)
- amii.chase (Amii Chase)
- amitie.bleak (Amitie Bleak)
- andie.bradham (Andie Bradham)
- andree.macanas (Andree Macanas)


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
Reply all

administrator@authlogicsdemo.... Authlogics Breached Password Security | Admini: 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

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:

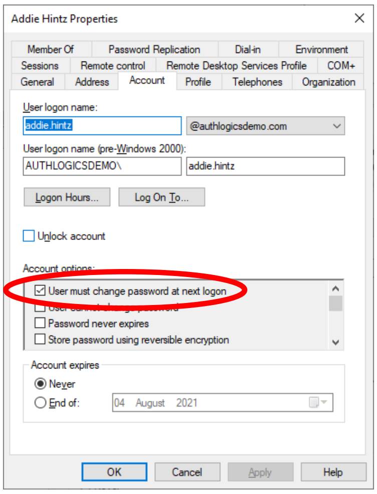
- Administrator [Never Expires]

Access the Authlogics Password Security Portal for details on public password breaches affecting your company.

Password Security Portal

Powered by Authlogics

(7) Verify 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
Logon Hours... | Log On To...
OK | Cancel | Apply | Help

User logon name: addie.hintz @authlogicsdemo.com

User logon name (pre-Windows 2000): AUTHLOGICSDEMO\ addie.hintz

□ 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: 04 August 2021

Monitoring PSM Usage

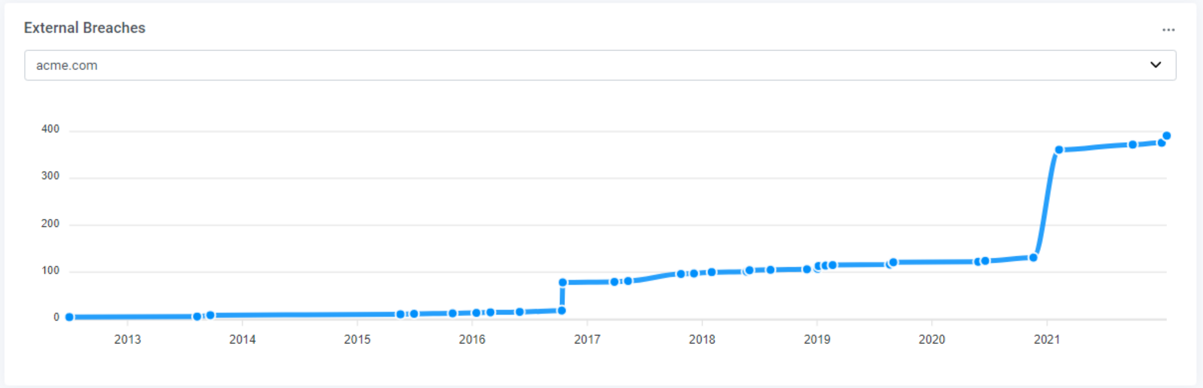
MyID Server includes a Dashboard to graphically display the state of your PSM deployment.

Launch the MyID Admin portal via https://{servername}:14443/admin.

Select System – Dashboards – Password Security.

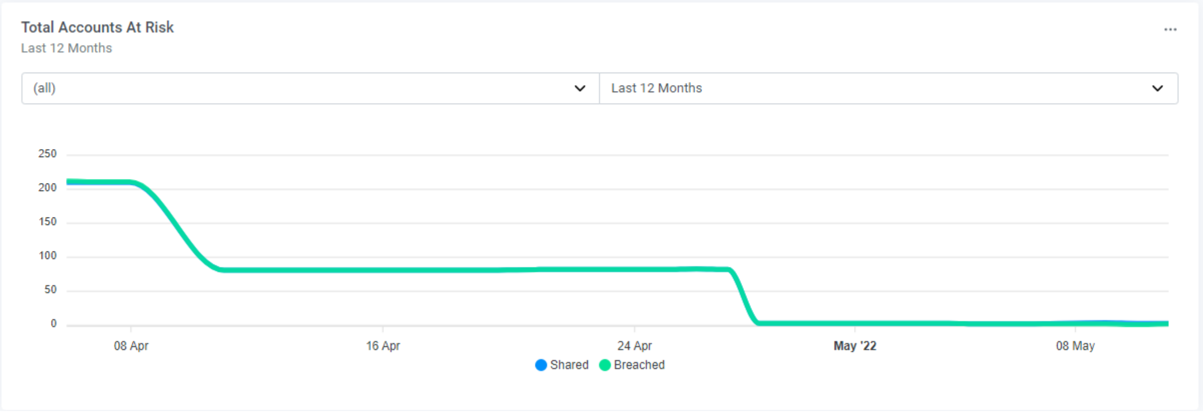
The dashboard reflects MFA actions for:

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



External Breaches

acme.com

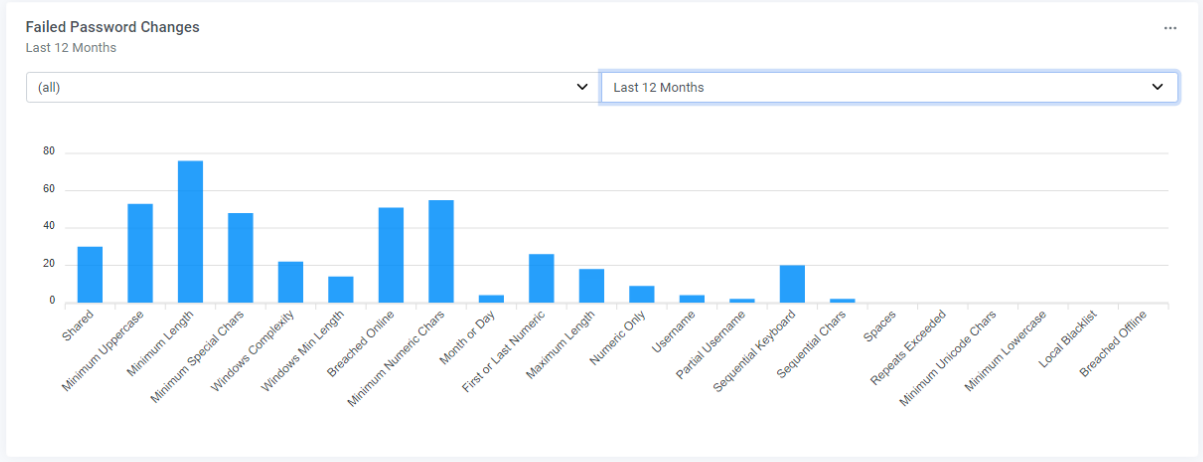


Total Accounts At Risk

Last 12 Months

(all)

Last 12 Months

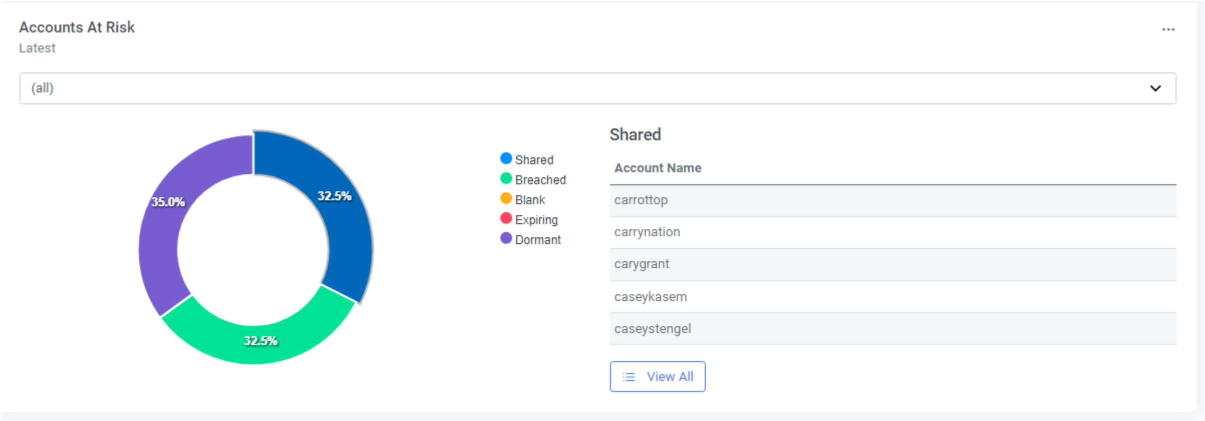


Failed Password Changes

Last 12 Months

(all)

Last 12 Months



Accounts At Risk

Latest

(all)

Shared

Account Name
carrottop
carrynation
carygrant
caseykasem
caseystengel