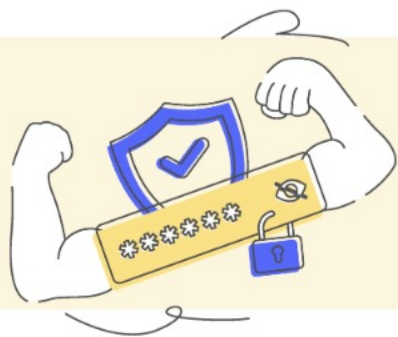


# Password policy enhancement with ADSelfService Plus

Fortify user passwords with strong password policy controls



# Are your users constantly creating weak passwords and putting your company at risk?



**Strong passwords can only be achieved with strong password policies!**

## **Are Active Directory password policies strong enough?**

Active Directory password policies cannot:

- Be tailored for specific OUs
- Restrict character repetition, dictionary words, and patterns
- Defend against today's sophisticated password attacks
- Make passwords comply with regulatory standards





# ADSelfService Plus

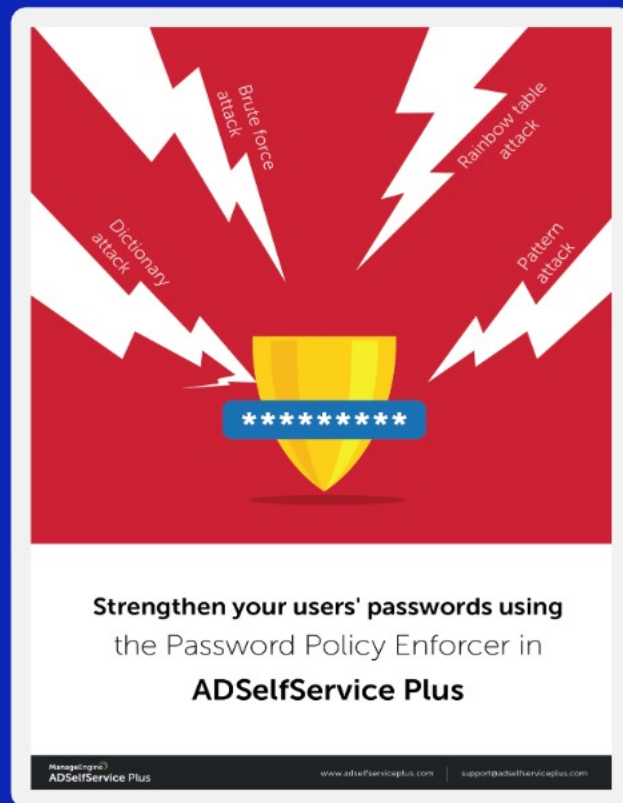
is the answer!

Implement strong and sophisticated password policies  
with ADSelfService Plus' **Password Policy Enhancer**.



# With ADSelfService Plus' Password policy enhancer, you can:

- Enforce custom, fine-grained, and strong password policies
- Specify character types to include
- Restrict consecutive characters from usernames and previous passwords
- Restrict custom dictionary words, patterns, and palindromes
- Enforce passwords to match the regex pattern
- Specify the minimum and maximum length of passwords
- Restrict compromised passwords
- Overcome drawbacks of AD password policies
- Create passwords that comply with regulatory standards





# Restrict characters

ADSelfService Plus

DashboardReportsConfigurationAdminSupport

Self-Service

- Policy Configuration
- Multi-factor Authentication
- Password Expiration Notification
- Password Policy Enforcer**
- Password Sync/Single Sign On
- Conditional Access
- Directory Self Service

Administrative Tools

Security Center

Password Policy Enforcer

Select the PolicySelfservice Users

☒ Enforce Custom Password Policy

Restrict Characters	5/7
Restrict Repetition	2/4
Restrict Pattern	4/4
Restrict Length	2/2

☒ Disallow palindrome passwords

☒ Disallow the use of dictionary words

Choose Dictionary- Browse file -BrowseDictionary in use : defaultDictionary.txt

☒ Disallow the use of these patterns.

qwerty,asdf,1234

Use comma (,) to separate patterns. Words are verified as case insensitive.

☒ Enforce passwords to match the regex pattern.

Please type your regex pattern here. For example, {.\*\s.\*}{3}

Click here to know more about regex definitions.

☐ Override all complexity rules if password length is at least20

☐ Password must satisfy at least of the above complexity requirements.

☒ Show this policy requirement in Reset and Change Password pagesCustomize View

☐ Enforce this policy in GINA/CP (Ctrl+Alt+Del) screen and ADUC Password resets through Password Sync Agent.

SaveCancel

ManageEngine  
ADSelfService Plus

# Restrict repetition

The screenshot shows the 'ADSelfService Plus' interface with the 'Configuration' tab selected. The left sidebar lists various self-service options, with 'Password Policy Enforcer' highlighted. The main content area is titled 'Password Policy Enforcer' and includes a dropdown to 'Select the Policy' (currently set to 'adselfservice.com'). A checkbox 'Enforce Custom Password Policy' is checked. Below this, a table lists four restriction rules: 'Restrict Characters' (6/7), 'Restrict Repetition' (3/4), 'Restrict Pattern' (3/3), and 'Restrict Length' (2/2). The 'Restrict Repetition' rule is currently selected. To the right of the table, three checkboxes are checked: 'Disallow use of a character more than 2 times consecutively', 'Disallow use of 5 consecutive characters from username', and 'Disallow use of 5 consecutive character(s) from old password'. There is also an unchecked checkbox for 'Number of old passwords to be restricted during password reset' with a value of 5. At the bottom, there are four more checkboxes: 'Override all complexity rules if password length is at least 20', 'Password must satisfy at least [ ] of the above complexity requirements', 'Show this policy requirement in Reset and Change Password pages' (checked), and 'Enforce this policy in GINA/CP (Ctrl+Alt+Del) screen and ADUC Password resets through Password Sync Agent'. 'Save' and 'Cancel' buttons are at the bottom right.

ADSelfService Plus

Dashboard Reports Configuration Admin Support

Self-Service

- Policy Configuration
- Multi-factor Authentication
- Password Expiration Notification
- Password Policy Enforcer**
- Password Sync/Single Sign On
- Conditional Access
- Directory Self Service

Administrative Tools

Security Center

Password Policy Enforcer ⓘ

Select the Policy: adselfservice.com

☒ Enforce Custom Password Policy ⓘ

Restrict Characters	6/7
<b>Restrict Repetition</b>	3/4
Restrict Pattern	3/3
Restrict Length	2/2

☒ Disallow use of a character more than 2 times consecutively

☒ Disallow use of 5 consecutive characters from username

☒ Disallow use of 5 consecutive character(s) from old password ⓘ

☐ Number of old passwords to be restricted during password reset: 5

☐ Override all complexity rules if password length is at least 20 ⓘ

☐ Password must satisfy at least [ ] of the above complexity requirements. ⓘ

☒ Show this policy requirement in Reset and Change Password pages [Customize View](#)

☐ Enforce this policy in GINA/CP (Ctrl+Alt+Del) screen and ADUC Password resets through Password Sync Agent. ⓘ

Save Cancel

# Restrict pattern

ADSelfService Plus

DashboardReportsConfigurationAdminSupport

Self-Service

Policy Configuration

Multi-factor Authentication

Password Expiration Notification

Password Policy Enforcer

Password Sync/Single Sign On

Conditional Access

Directory Self Service

Administrative Tools

Security Center

Password Policy Enforcer

Select the PolicySelfservice Users

☒ Enforce Custom Password Policy

Restrict Characters	5/7
Restrict Repetition	2/4
Restrict Pattern	4/4
Restrict Length	2/2

☒ Disallow palindrome passwords

☒ Disallow the use of dictionary words

Choose Dictionary

- Browse file -

Browse

Dictionary in use : defaultDictionary.txt

☒ Disallow the use of these patterns.

qwerty,asdf,1234

Use comma (,) to separate patterns. Words are verified as case insensitive.

☒ Enforce passwords to match the regex pattern.

Please type your regex pattern here. For example, (.\*){3}

Click [here](#) to know more about regex definitions.

☐ Override all complexity rules if password length is at least 

20

☐ Password must satisfy at least  of the above complexity requirements.

☒ Show this policy requirement in Reset and Change Password pages [Customize View](#)

☐ Enforce this policy in GINA/CP (Ctrl+Alt+Del) screen and ADUC Password resets through Password Sync Agent.

Save

Cancel



# Restrict length

The screenshot shows the 'ADSelfService Plus' interface with the 'Configuration' tab selected. The left sidebar lists various self-service options, with 'Password Policy Enforcer' highlighted. The main content area is titled 'Password Policy Enforcer' and includes a dropdown to 'Select the Policy' (currently set to 'adselfservice.com'). Below this, the 'Enforce Custom Password Policy' checkbox is checked. A table lists four policy rules: 'Restrict Characters' (6/7), 'Restrict Repetition' (3/4), 'Restrict Pattern' (3/3), and 'Restrict Length' (2/2). The 'Restrict Length' rule is expanded, showing 'Minimum password length' set to 8 and 'Maximum password length' set to 15, both with checked checkboxes. At the bottom, there are three unchecked checkboxes: 'Override all complexity rules if password length is at least 20', 'Password must satisfy at least [ ] of the above complexity requirements.', and 'Enforce this policy in GINA/CP (Ctrl+Alt+Del) screen and ADUC Password resets through Password Sync Agent.'. A 'Show this policy requirement in Reset and Change Password pages' checkbox is checked, with a 'Customize View' link. 'Save' and 'Cancel' buttons are at the bottom right.

ADSelfService Plus

Dashboard Reports Configuration Admin Support

Self-Service

- Policy Configuration
- Multi-factor Authentication
- Password Expiration Notification
- Password Policy Enforcer**
- Password Sync/Single Sign On
- Conditional Access
- Directory Self Service

Administrative Tools

Security Center

### Password Policy Enforcer

Select the Policy: adselfservice.com

☒ Enforce Custom Password Policy

Restrict Characters	6/7	
Restrict Repetition	3/4	<input checked="" type="checkbox"/> Minimum password length 8
Restrict Pattern	3/3	<input checked="" type="checkbox"/> Maximum password length 15
Restrict Length	2/2	

☐ Override all complexity rules if password length is at least 20

☐ Password must satisfy at least [ ] of the above complexity requirements.

☒ Show this policy requirement in Reset and Change Password pages [Customize View](#)

☐ Enforce this policy in GINA/CP (Ctrl+Alt+Del) screen and ADUC Password resets through Password Sync Agent.

Save Cancel



# Restrict compromised passwords

The screenshot displays the 'ADSelfService Plus' web interface. At the top, there is a navigation bar with 'Profile', 'Change Password', and 'Enrollment' tabs. The 'Change Password' tab is active. Below the tabs, there is a search bar labeled 'Search Employee'. The main form area contains three input fields: 'Old Password' (filled with dots), 'New Password', and 'Confirm New Password'. A red warning box at the top right of the form states: 'The entered password is considered unsafe according to the Have I Been Pwned service.' Below the 'Confirm New Password' field, a dropdown menu is open, showing a suggestion: 'Use a Securely Generated Password' with the example 'DsYqMbYS4sL7vXE'. Below the suggestion, it says 'Firefox will save this password for this website.' and there is a 'View Saved Logins' button. At the bottom of the form, there are two status messages: '•No. of passwords remembered is 24' and '•The password complexity property is enabled'. At the very bottom, there are two buttons: 'Change Password' (green) and 'Cancel' (grey).



# Switch to **ADSelfService Plus today**

and **enjoy enhanced identity security for your organization!**



## **Guaranteed ROI**

ADSelfService Plus gives you an immediate ROI by nearly eliminating password-related tickets.

[\*\*Calculate ROI\*\*](#)



ManageEngine  
ADSelfService Plus

# Contact us



For technical support:

📞 **+1-408-916-9890**

✉ **[support@adselfserviceplus.com](mailto:support@adselfserviceplus.com)**

🌐 **[www.adselfserviceplus.com](http://www.adselfserviceplus.com)**

💬 **[Chat live with our support team](#)**

**[Personalized web demo](#)**

**[Download ADSelfService Plus now](#)**