

# 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





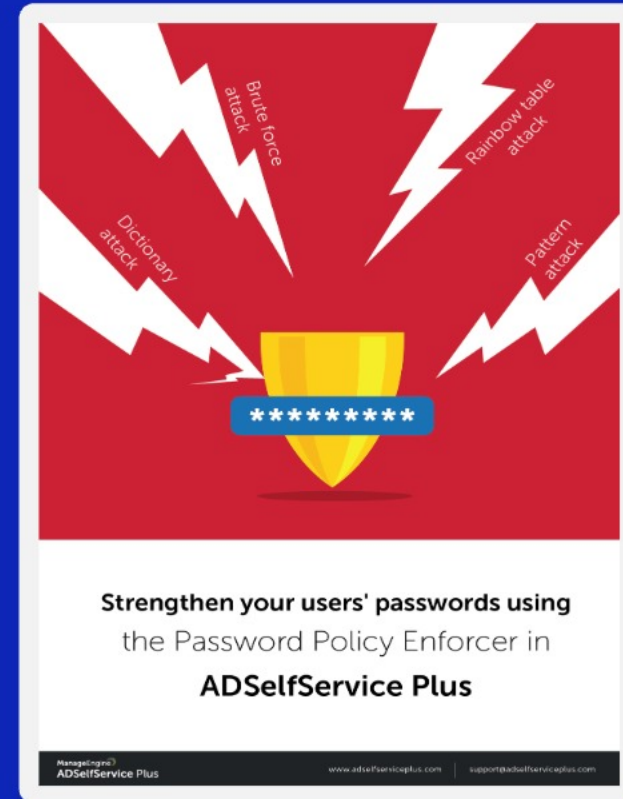
# ADSelfService Plus is the answer!

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
- 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

The screenshot shows the ADSelfService Plus interface for configuring the Password Policy Enforcer. The left sidebar lists navigation options: 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, and Security Center. The main content area is titled 'Password Policy Enforcer' and includes a dropdown for 'Select the Policy' set to 'adselfservice.com'. A checkbox 'Enforce Custom Password Policy' is checked. A progress indicator shows 'Restrict Characters' as 6/7. The 'Restrict Characters' section contains several settings: 'Number of special characters to include' (2), 'Number of numeric characters to include' (1), 'Number of unicode characters' (1), 'Must contain at least 1 upper case character', 'Must contain at least 1 lower case character', 'Password must begin with' (an uppercase alphabet, a low), and 'Disallow numeric last character' (unchecked). Below this, there are three more checkboxes: 'Override all complexity rules if password length is at least 20', 'Password must satisfy at least [ ] of the above complexity requirements', and 'Show this policy requirement in Reset and Change Password pages' (checked). The final checkbox is 'Enforce this policy in GINA/CP (Ctrl+Alt+Del) screen and ADUC Password resets through Password Sync Agent' (unchecked). 'Save' and 'Cancel' buttons are at the bottom right.

# Restrict repetition

The screenshot shows the ADSelfService Plus interface for configuring the Password Policy Enforcer. The left sidebar lists various self-service options, with 'Password Policy Enforcer' selected. The main content area is titled 'Password Policy Enforcer' and includes a dropdown for 'Select the Policy' set to 'adselfservice.com'. A checkbox for 'Enforce Custom Password Policy' is checked. Below this, a table shows progress for various 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 active, with options to '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 are also checkboxes for overriding complexity rules, requiring a minimum number of requirements, showing requirements in password reset pages, and enforcing the policy in GINA/CP screens. '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
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

The screenshot shows the ADSelfService Plus interface. The top navigation bar includes 'Dashboard', 'Reports', 'Configuration', 'Admin', and 'Support'. The left sidebar lists various self-service options, with 'Password Policy Enforcer' selected. The main content area is titled 'Password Policy Enforcer' and shows a dropdown menu for 'Select the Policy' set to 'adselfservice.com'. A checkbox for 'Enforce Custom Password Policy' is checked. Below this, a table lists policy requirements: 'Restrict Characters' (6/7), 'Restrict Repetition' (3/4), 'Restrict Pattern' (3/3), and 'Restrict Length' (2/2). To the right of the table, three checkboxes are checked: 'Disallow palindrome passwords', 'Disallow the use of dictionary words' (with a 'Choose Dictionary' link), and 'Disallow the use of these patterns' (with a 'Modify Patterns' link). At the bottom, there are four unchecked 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' (with a 'Customize View' link), 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	<input checked="" type="checkbox"/> Disallow palindrome passwords
Restrict Repetition	3/4	<input checked="" type="checkbox"/> Disallow the use of dictionary words <a href="#">Choose Dictionary</a>
Restrict Pattern	3/3	<input checked="" type="checkbox"/> Disallow the use of these patterns. <a href="#">Modify Patterns</a>
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 length

The screenshot shows the ADSelfService Plus interface for configuring the Password Policy Enforcer. The left sidebar lists various self-service options, with 'Password Policy Enforcer' selected. The main content area is titled 'Password Policy Enforcer' and includes a dropdown for 'Select the Policy' set to 'adselfservice.com'. A checkbox for 'Enforce Custom Password Policy' is checked. Below this, a table shows the status of various complexity rules:

Rule	Status	Configuration
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	

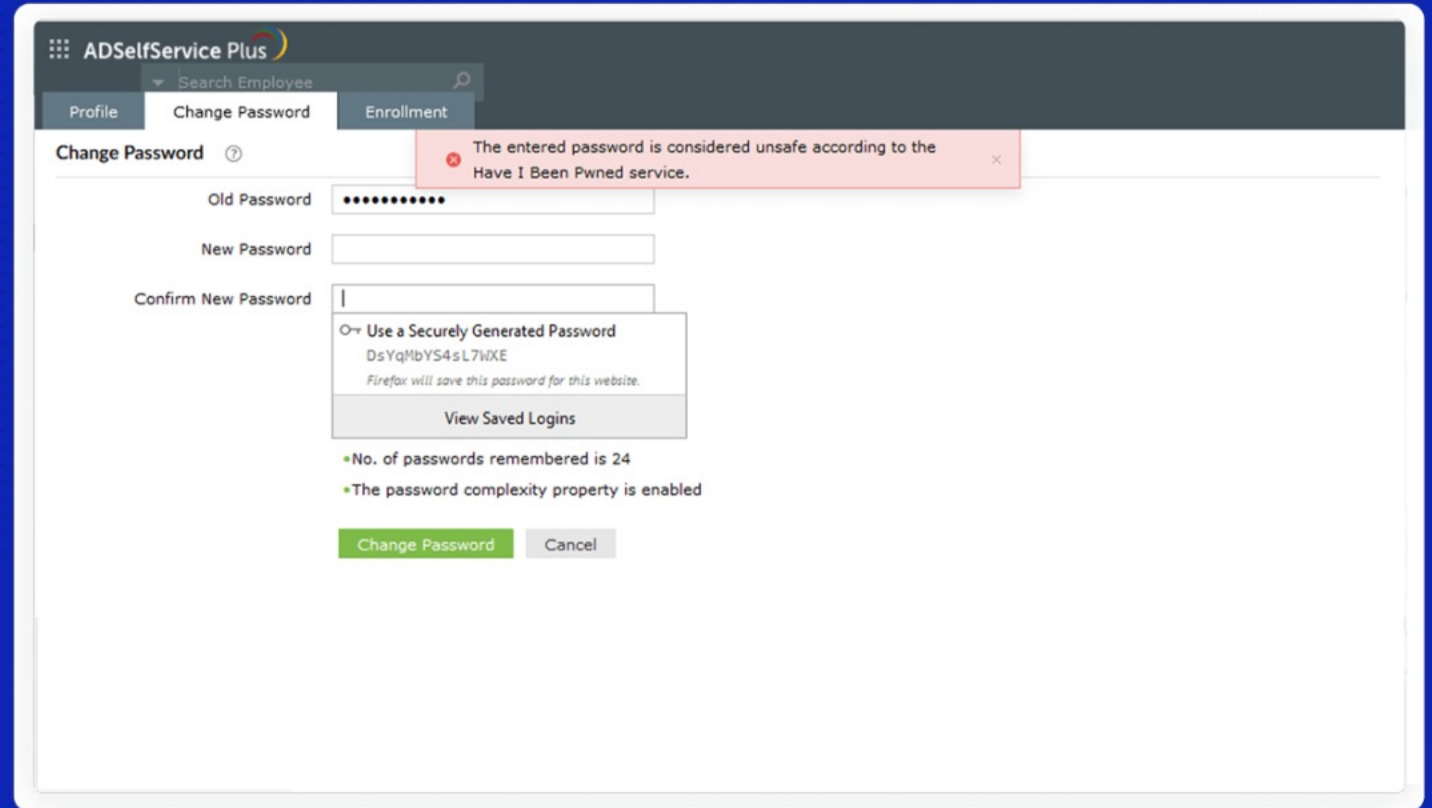
At the bottom, there are several checkboxes for advanced settings:

- 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' and 'Cancel' buttons are located at the bottom right.



# Restrict compromised passwords





# 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**

 **www.adselfserviceplus.com**

 **Chat live with our support team**

[Personalized web demo](#)

[Download ADSelfService Plus now](#)