ManageEngine
ADSolutions

Increasing Password Security and Incorporating MFA

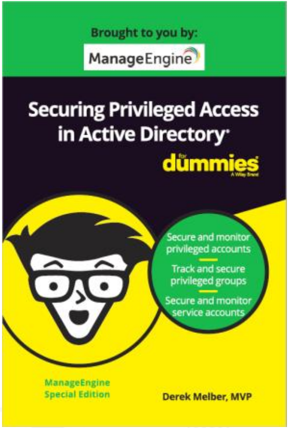
Derek Melber

derek@manageengine.com

About Your Speaker

About Derek Melber

- Derek Melber
  - Chief Technology Evangelist
  - MVP (AD and Group Policy)
  - derek@manageengine.com
- Online Resources
  - ManageEngine Active Directory Blog
  - Security Hardening Site
  - Download free Dummies book
- 2019 World Tour



Brought to you by:

ManageEngine

Securing Privileged Access in Active Directory for dummies

A Wiley Brand

Secure and monitor privileged accounts

Track and secure privileged groups

Secure and monitor service accounts

ManageEngine Special Edition

Derek Melber, MVP

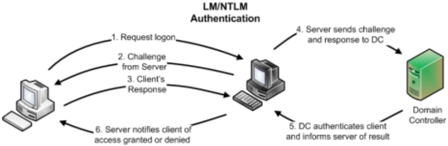
Agenda

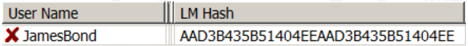
- How insecure are passwords?
- Increasing password security
- Using MFA

HOW SECURE ARE PASSWORDS?

How secure are passwords?

- Foundations are weak
  - Authentication protocols
    - LM/NTLM
    - NTLMv2
    - Kerberos
  - Password hashes
    - Dictionary attacks
    - Brute-force attacks
    - Rainbow table attacks


LM/NTLM Authentication
1. Request logon
2. Challenge from Server
3. Client's Response
4. Server sends challenge and response to DC
5. DC authenticates client and informs server of result
6. Server notifies client of access granted or denied
Domain Controller



User Name	LM Hash
✗ JamesBond	AAD3B435B51404EEAAD3B435B51404EE

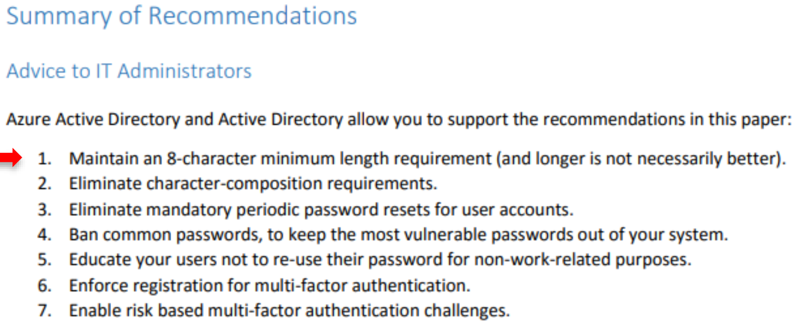
INCREASING PASSWORD SECURITY

Increasing password security

- Negate/Disable weak authentication protocols
- Improve password structure
  - Deny dictionary words
  - Require special characters
  - Deny company/vertical specific words (ME, ManageEngine, Zoho, etc)

Increasing password security

- Azure AD: Improved password structure



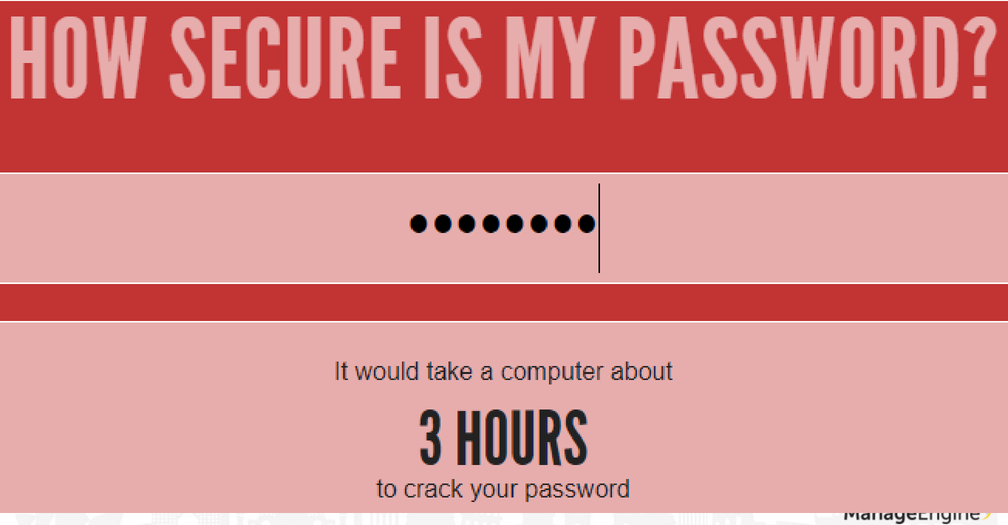
Summary of Recommendations

Advice to IT Administrators

Azure Active Directory and Active Directory allow you to support the recommendations in this paper:

1. Maintain an 8-character minimum length requirement (and longer is not necessarily better).
2. Eliminate character-composition requirements.
3. Eliminate mandatory periodic password resets for user accounts.
4. Ban common passwords, to keep the most vulnerable passwords out of your system.
5. Educate your users not to re-use their password for non-work-related purposes.
6. Enforce registration for multi-factor authentication.
7. Enable risk based multi-factor authentication challenges.

- https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf



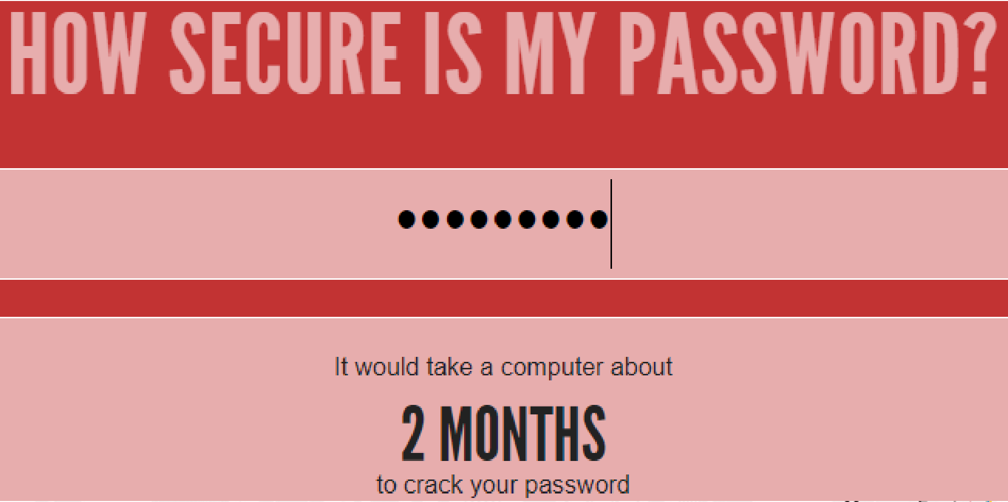
HOW SECURE IS MY PASSWORD?

●●●●●●●●

It would take a computer about

3 HOURS

to crack your password



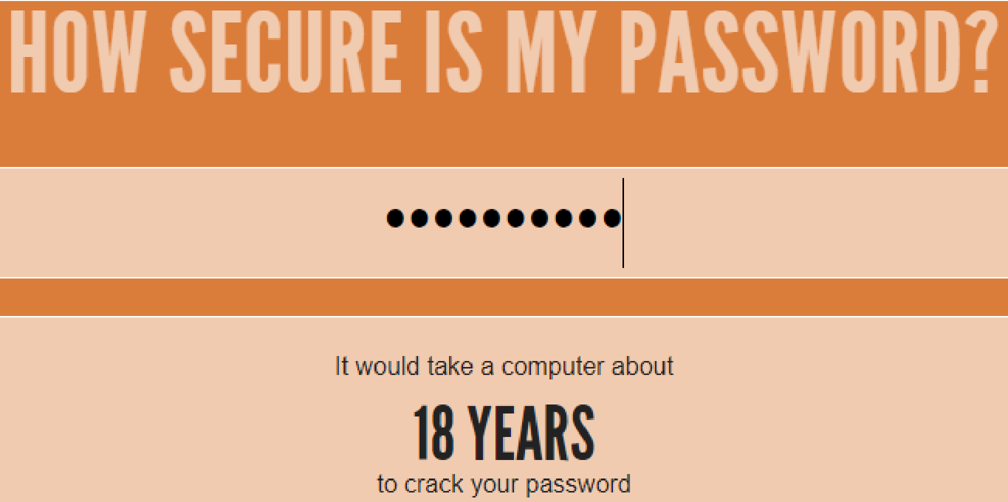
HOW SECURE IS MY PASSWORD?

●●●●●●●●●

It would take a computer about

2 MONTHS

to crack your password



HOW SECURE IS MY PASSWORD?

●●●●●●●●●●

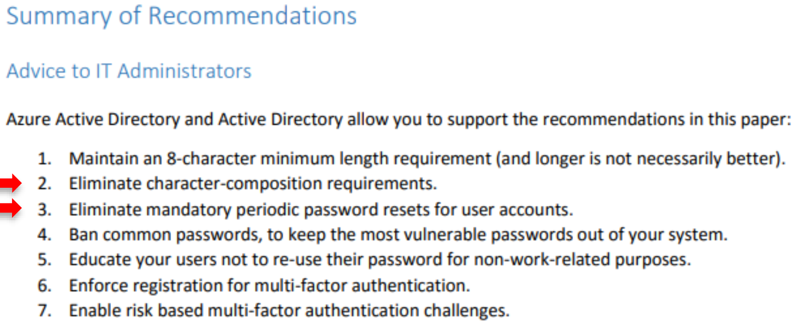
It would take a computer about

18 YEARS

to crack your password

Increasing password security

- Azure AD: Improved password structure



Summary of Recommendations

Advice to IT Administrators

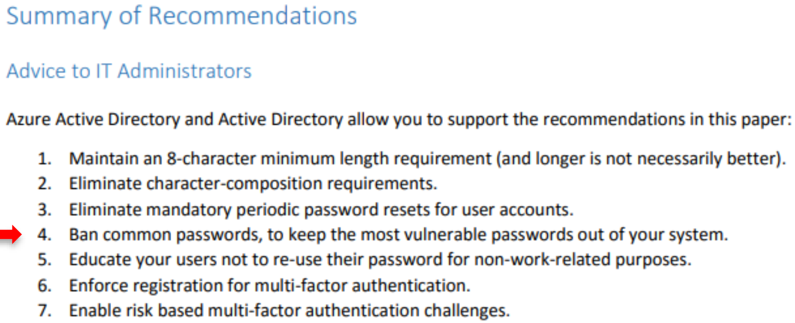
Azure Active Directory and Active Directory allow you to support the recommendations in this paper:

1. Maintain an 8-character minimum length requirement (and longer is not necessarily better).
2. Eliminate character-composition requirements.
3. Eliminate mandatory periodic password resets for user accounts.
4. Ban common passwords, to keep the most vulnerable passwords out of your system.
5. Educate your users not to re-use their password for non-work-related purposes.
6. Enforce registration for multi-factor authentication.
7. Enable risk based multi-factor authentication challenges.

- https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf

Increasing password security

- Azure AD: Improved password structure



Summary of Recommendations

Advice to IT Administrators

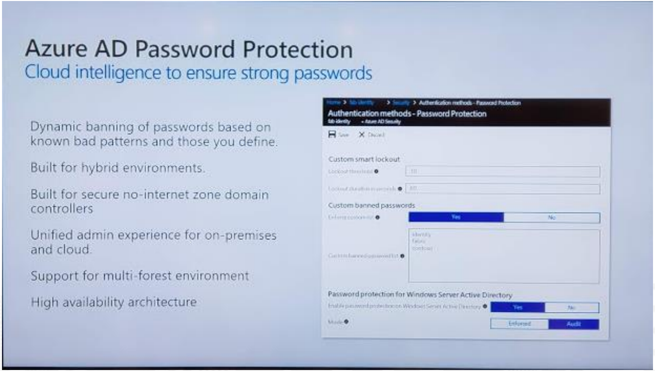
Azure Active Directory and Active Directory allow you to support the recommendations in this paper:

1. Maintain an 8-character minimum length requirement (and longer is not necessarily better).
2. Eliminate character-composition requirements.
3. Eliminate mandatory periodic password resets for user accounts.
4. Ban common passwords, to keep the most vulnerable passwords out of your system.
5. Educate your users not to re-use their password for non-work-related purposes.
6. Enforce registration for multi-factor authentication.
7. Enable risk based multi-factor authentication challenges.

- https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf

Increasing password security

- Azure AD: Improved password structure



Azure AD Password Protection

Cloud intelligence to ensure strong passwords

Dynamic banning of passwords based on known bad patterns and those you define.

Built for hybrid environments.

Built for secure no-internet zone domain controllers

Unified admin experience for on-premises and cloud.

Support for multi-forest environment

High availability architecture

Home > fab identity > Security > Authentication methods - Password Protection
fab identity - Azure AD Security
Save
Discard

Authentication methods - Password Protection

Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: [✓ Yes] No

Custom banned password list:
identity
failure
contoso

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: [✓ Yes] No

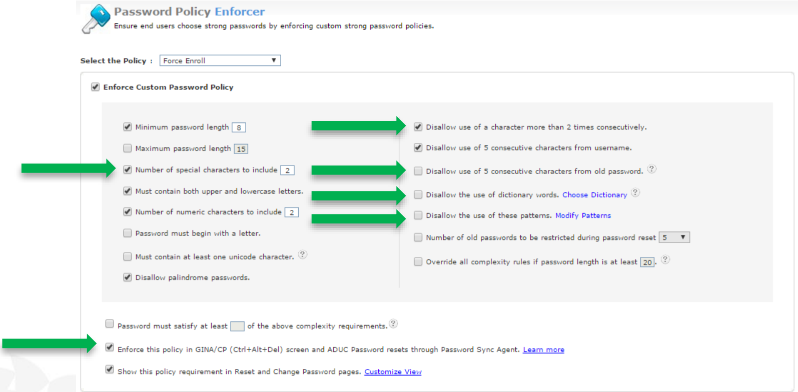
Mode: Enforced [✓ Audit]

Increasing password security

- The details matter!
  - Longer is more secure
  - Character composition is essential (especially special characters)
  - Resetting passwords help protect against attacks
  - Dictionary word negation is important
  - Banning common words is important
  - Negating part of old password is important

Increasing password security

- ADSelfService Plus: Improved password structure



Password Policy Enforcer

Ensure end users choose strong passwords by enforcing custom strong password policies.

Select the Policy : Force Enroll ▼

☑ Enforce Custom Password Policy

☑ Minimum password length 8

□ Maximum password length 15

☑ Number of special characters to include 2

☑ Must contain both upper and lowercase letters.

☑ Number of numeric characters to include 2

□ Password must begin with a letter.

□ Must contain at least one unicode character. ?

☑ Disallow palindrome passwords.

☑ Disallow use of a character more than 2 times consecutively.

☑ Disallow use of 5 consecutive characters from username.

□ Disallow use of 5 consecutive characters from old password. ?

□ Disallow the use of dictionary words. Choose Dictionary ?

□ Disallow the use of these patterns. Modify Patterns

□ 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. ?

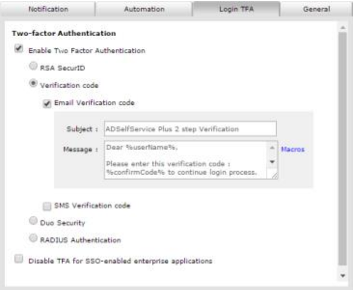
☑ Enforce this policy in GINA/CP (Ctrl+Alt+Del) screen and ADUC Password resets through Password Sync Agent. Learn more

☑ Show this policy requirement in Reset and Change Password pages. Customize View

USING MFA

Using MFA

- Securing access to computer!
  - No longer just require password at Windows logon
  - ADSelfService Plus has 5 options!



Two-factor Authentication

☑ Enable Two Factor Authentication

○ RSA SecurID

● Verification code

☑ Email Verification code

Subject : ADSelfService Plus 2 step Verification

Message : Dear %userName%,

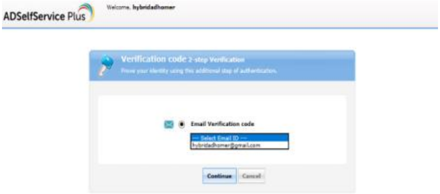
Please enter this verification code : %confirmCode% to continue login process.

□ SMS Verification code

○ Duo Security

○ RADIUS Authentication

□ Disable TFA for SSO-enabled enterprise applications



Welcome, **hybridadhomer**

Verification code 2-step Verification

Prove your identity using this additional step of authentication.

● **Email Verification code**

-- Select Email ID --
hybridadhomer@gmail.com

Summary

- How insecure are passwords?
- Increasing password security
- Using MFA

ManageEngine

Thank you!

Derek Melber

derek@manageengine.com