



Azure AD Security Recommendations and the Customer Stories That Prove It

Mark Morowczynski
Principal Program Manager- Identity Division
[@markmorow](#)

Who am I?

Identity Product Group,

Customer Experience (CXP) Team

Premier Field Engineer

SANS STI Student

How Many People have Azure
Active Directory?

Agenda

Protect Privileged Accounts

Enable Password Hash Sync (PHS)

Update Your Password Policy

Block Legacy Authentication

Enroll End Users for MFA

Recommendation 1

MFA your Privileged Accounts!

I shouldn't have to say this!!

Admin Accounts MFA Sept 2017- 0.7%

Admin Accounts MFA Sept 2018- 1.7%

Customer Story 1

Tech Company

Global footprint

100k+ users

Global admin phished

No MFA

Changes made to O365 mailboxes for key executives

Was discovered when a user reported “weirdness”

MFA Privileged Accounts Deployment Tips

Good: Turn MFA on!

Better: Baseline Policy for Admins

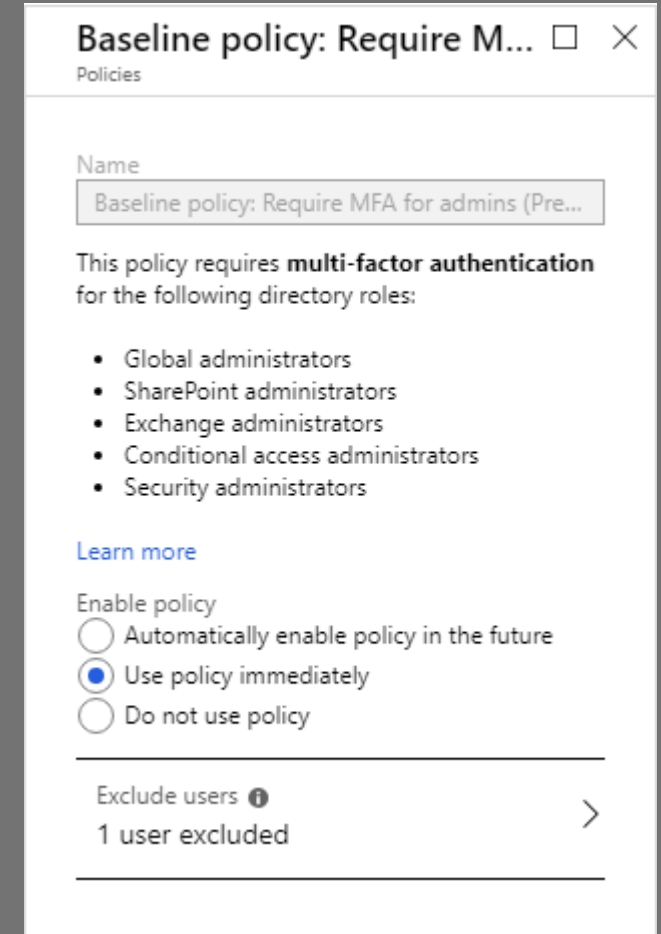
Learn more at: <https://aka.ms/aadbaseline>

Best: Azure AD PIM

Admin access requires elevation + MFA

Can buy P2 license for just your admins

<https://aka.ms/deploymentplans>



The screenshot shows the configuration page for a baseline policy in Microsoft Entra ID. The title is "Baseline policy: Require MFA for admins" with a close button. Below the title, the name of the policy is displayed in a text box: "Baseline policy: Require MFA for admins (Pre...". The main content area states: "This policy requires **multi-factor authentication** for the following directory roles:" followed by a bulleted list of roles: Global administrators, SharePoint administrators, Exchange administrators, Conditional access administrators, and Security administrators. There is a "Learn more" link. Under the "Enable policy" section, three radio buttons are present: "Automatically enable policy in the future", "Use policy immediately" (which is selected), and "Do not use policy". At the bottom, there is an "Exclude users" section with an information icon and a right-pointing arrow, showing "1 user excluded".

Agenda

Protect Privileged Accounts

Enable Password Hash Sync (PHS)

Update Your Password Policy

Block Legacy Authentication

Enroll End Users for MFA

Recommendation 2

Turn on Azure AD Password Hash Sync

<http://aka.ms/auth-options>

Leaked Credentials

Dark Web, Law Enforcement, Security Researchers

When something catastrophic happens

WannaCry, NotPetya

Customer Story 2

The Untold Story Of Notpeya, The Most Devastating Cyberattack In History

<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>



Ned Pyle ✓
@NerdPyle

Follow



Always lovely to see a vendor product that not only requires SMB1 but also *prohibits* use of NTLMv2 and allows LM...

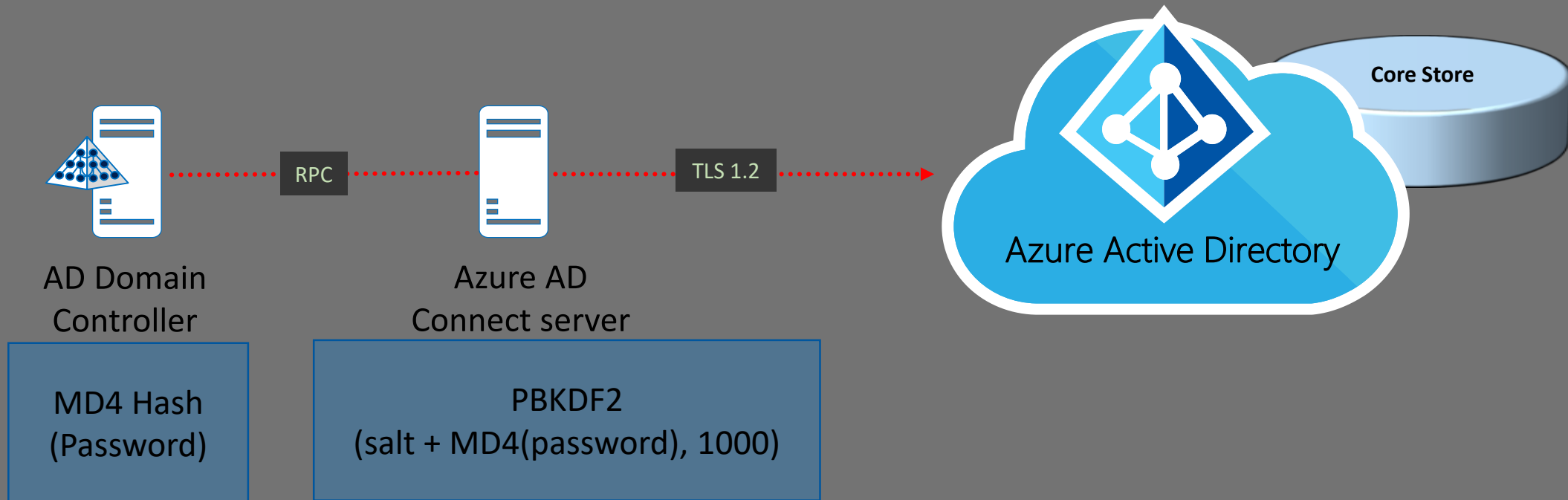
aka.ms/stillneedssmb1



Password Hash Sync Deployment Tips

Understand how PHS works

<http://aka.ms/aadpsh>



Treat Azure AD Connect like a Domain Controller!

Agenda

Protect Privileged Accounts

Enable Password Hash Sync (PHS)

Update Your Password Policy

Block Legacy Authentication

Enroll End Users for MFA

Recommendation 3

Modernize your password policy

People choose “strong” but easily guessable passwords.

April 2019! Or Summer 2019!

<https://aka.ms/passwordguidance>

[NIST 800-63B](https://nist.gov/800-63B)

Implement Azure AD Banned Password Policy

Applies to on-prem AD as well!

<https://aka.ms/deploypasswordprotection>

The screenshot shows the configuration for password protection in Windows Server Active Directory. It includes sections for 'Custom smart lockout', 'Custom banned passwords', and 'Password protection for Windows Server Active Directory'. The 'Custom smart lockout' section has 'Lockout threshold' set to 10 and 'Lockout duration in seconds' set to 70. The 'Custom banned passwords' section has 'Enforce custom list' set to 'Yes' and a list of banned passwords: seahawks, mariners, sounders, redmond, and washington. The 'Password protection for Windows Server Active Directory' section has 'Enable password protection on Windows Server Active Directory' set to 'Yes' and 'Mode' set to 'Enforced'.

Section	Property	Value
Custom smart lockout	Lockout threshold	10
	Lockout duration in seconds	70
Custom banned passwords	Enforce custom list	Yes
	Custom banned password list	seahawks, mariners, sounders, redmond, washington
Password protection for Windows Server Active Directory	Enable password protection on Windows Server Active Directory	Yes
	Mode	Enforced

Azure AD Banned Password

Requirements

Azure AD P1 License

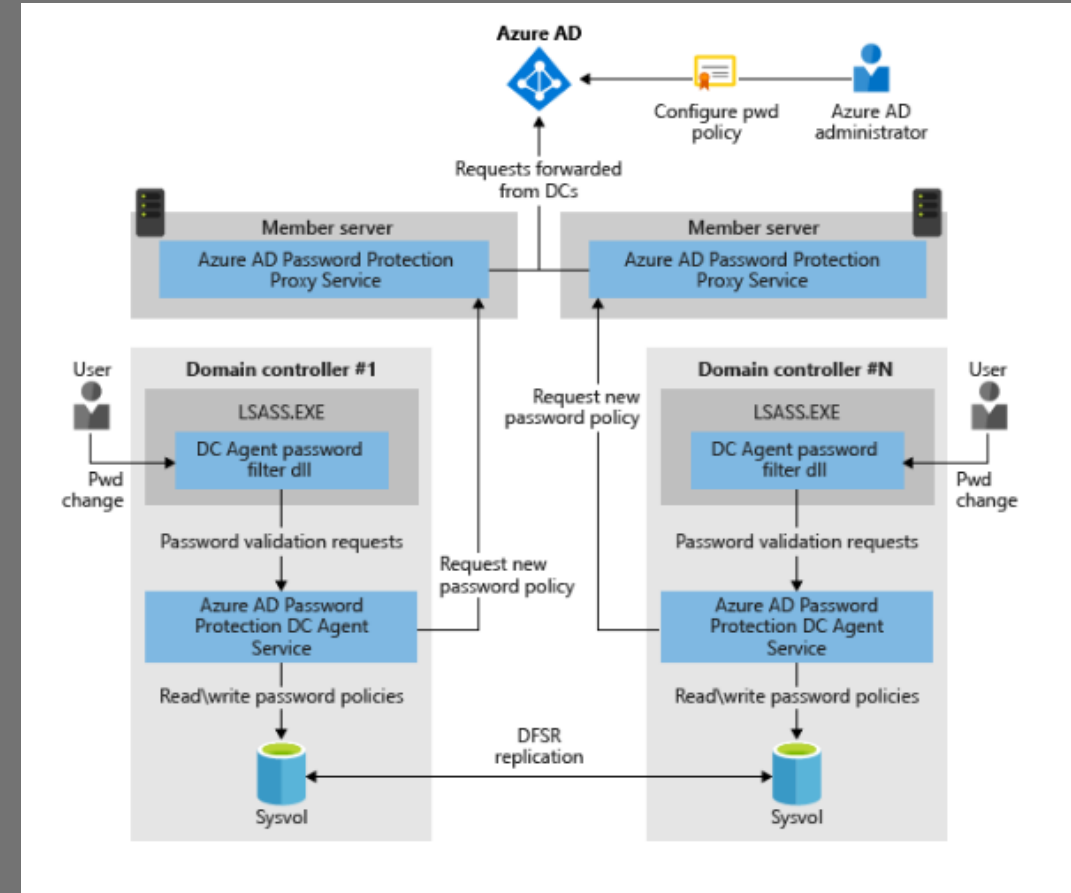
DCs need to be 2012 or later

No Domain or Forest functional level

Sysvol should be at DFSR (aka.ms/dfsrmig)

How passwords are scored

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>



Customer Story 3 Part 1

Media Company

Global footprint

50k+ users

Deployed Azure AD Banned Password

Was blocking about 20% of passwords

Help desk calls "Why can't I set my password"

Management instructed turn off blocking banned passwords...

Recommendation 4

Turn off Legacy Authentication

200k accounts compromised in Aug 2018 due to password spray

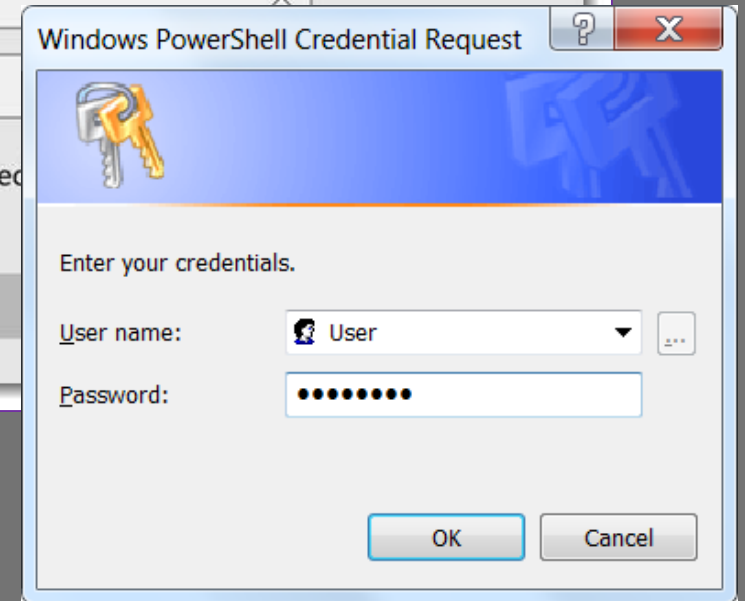
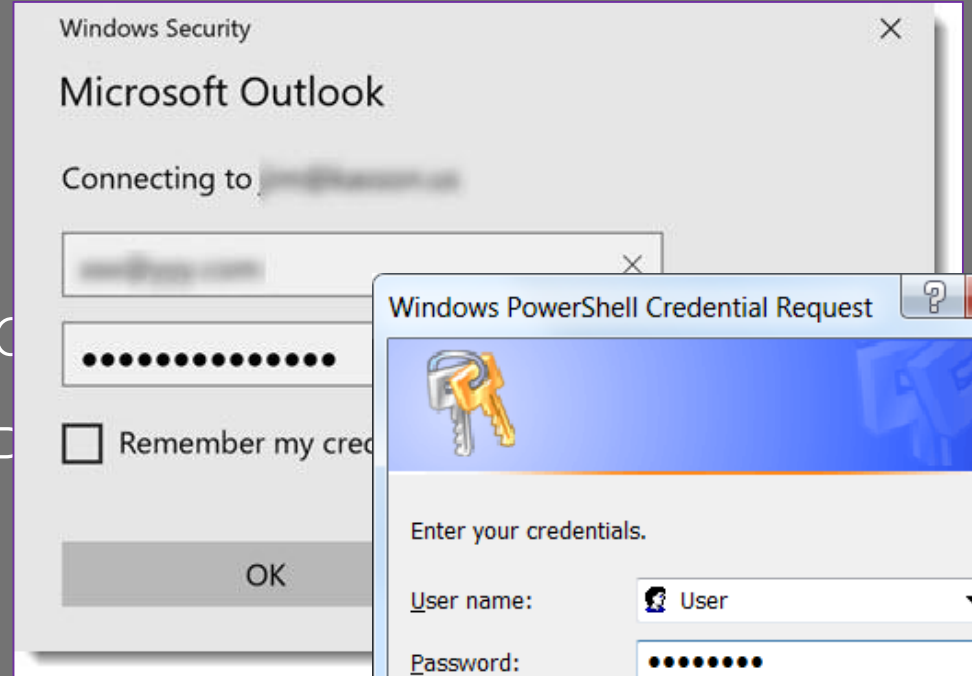
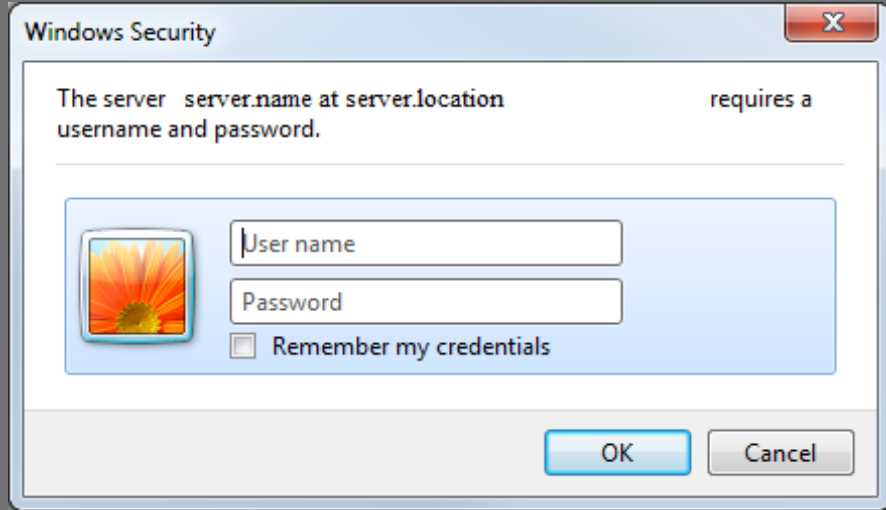
Nearly 100% of password spray attacks we see are from legacy authentication

Blocking legacy auth reduces compromise rate by 66%

<https://aka.ms>PasswordSprayBestPractices>

Legacy Authentication, Examples

Clients that use legacy authentication



Updated Azure AD modules at <https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell>

Updated O365 modules at <https://docs.microsoft.com/en-us/office365/enterprise/powershell/manage-office-365-with-office-365-powershell>

Customer Story 3 Part 2

Media Company

Global footprint

50k+ users

Turned off POP3

Didn't turn off IMAP4, or other legacy protocols...

Required client app updates and policy of supported clients

Customer Story 3 Part 3

Media Company

Global footprint

50k+ users

Started MFA enrollment, slowly

Resistance from end users

Lack of policy stopped enrollment...

Customer Story 3 Part 4

150+ users successfully password spray

Weak passwords were used

Legacy protocols IMAP4 and SMTP initial foothold

Other apps then accessed with no MFA required

Modernizing Your Password Policy Deployment Tips

Have conversation with policy makers

Help them understand the **NEW** recommendations

<https://aka.ms/passwordguidance>

[NIST 800-63B](#)

Customize Banned Password List

Deploy in Audit mode first

Use this data to go back to policy makers

Blocking Legacy Auth Deployment Tips

Determine Legacy Auth Usage

<https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Mailbag-Discovering-and-blocking-legacy-authentication/ba-p/369725>

Block those that are NOT using FIRST

Block Today with Conditional Access

Requires Azure AD P1

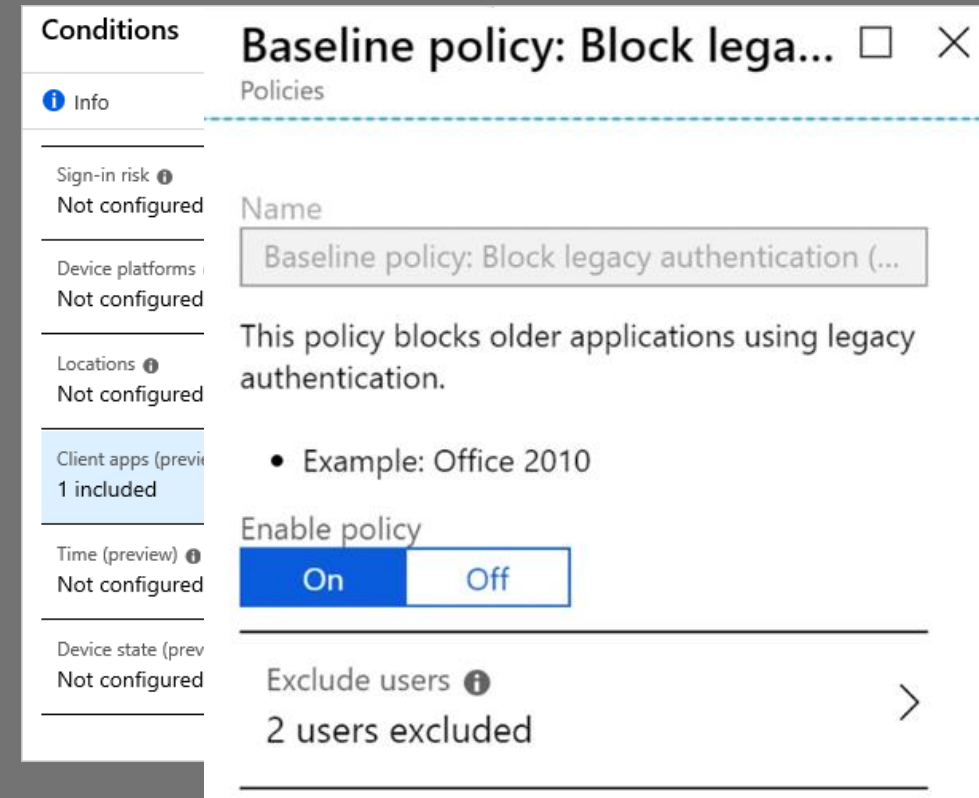
Update Clients

Coming Soon! Baseline: Block Legacy Auth

Available to all tenants

Exclude specific users or service accounts

Does not block Exchange ActiveSync



Enable MFA for End Users Deployment Tips

Leverage the Azure AD deployment plans

<https://aka.ms/deploymentplans>

Don't block deployment on the last 5%

Pair with Self Service Password Reset registration

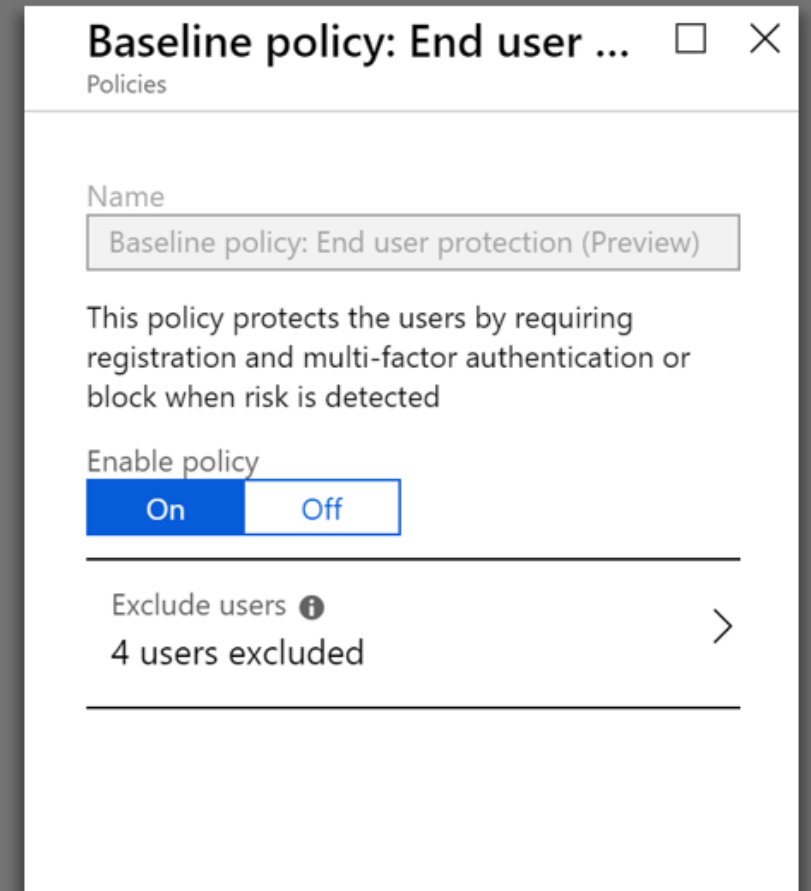
Coming Soon! Baseline Policy End User Protection

Available to all tenants

Prompt for MFA only during risky sign-ins

Requires users to register for MFA within 14 days

Deploy the Azure MFA Authenticator App



Recommendation Recap

Protect your admins!

Turn on Password Hash Sync

Update Your Password Policy & use Azure AD Banned Passwords

Block Legacy Authentication

Enable MFA for End Users

<https://aka.ms/securitysteps>

Questions

@markmorow
Markmoro@Microsoft.com

Mark Morowczynski
Principal Program Manager