Azure AD
Identity protection

Work Together

SharePoint and office 365 Architect

Arjan Cornelisssen
SharePoint & Office 365 Architect
WorkTogether.tech
@arjancornelis

Microsoft CERTIFIED Solutions Associate Office 365

Microsoft CERTIFIED Solutions Expert SharePoint

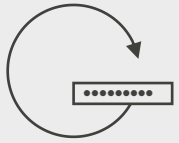
WORK TOGETHER

Azure AD Plans

	Free	O365 Apps	P1	P2
Identity and access management	500.000 objecten	Unlimited	Unlimited	Unlimited
SSO	10 apps	10 apps	Unlimited	Unlimited
Guest Users	X	X	X	X
Company branding		X	X	X
MFA		X	X	X
Self service password reset		X	X	X
Password Protection			X	X
Microsoft Cloud App Discovery			X	X
Azure AD Join			X	X
Dynamic groups			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X

WORK TOGETHER

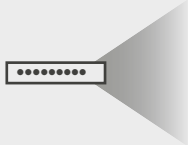
Top attacks against Azure AD



Breach Replay

4.6B

attacker-driven sign-ins detected in **May 2018**



Password Spray

200K

password spray attacks blocked in **August 2018**

Phishing

5B

high risk enterprise sign-in attempts detected in **2018**

Passwords are the problem

WORK TOGETHER

Sobering statistics

140+

median # days attackers reside **within** a victim's network before detection

75%+

network intrusions due to compromised user credentials

$6T

annual cost of cybercrime to the global economy

$4M

average cost of a data breach to a company

The frequency and sophistication of cybersecurity attacks are escalating

WORK TOGETHER

Updated NIST Guidelines

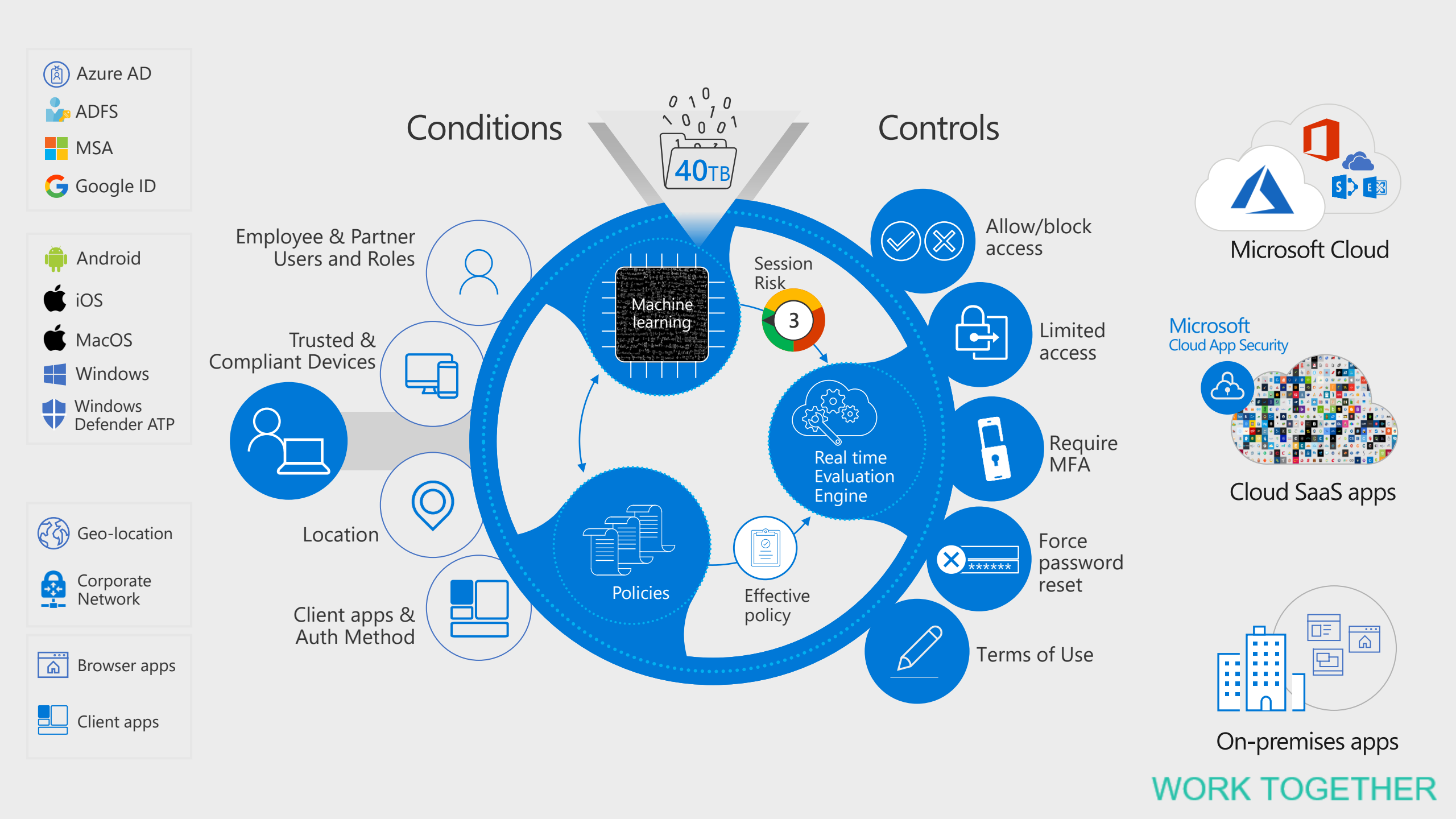
National Institute of Standards and Technology
U.S. Department of Commerce

Three main changes:

1. No more periodic password changes
2. No more imposed password complexity
3. Validate new passwords against commonly used passwords

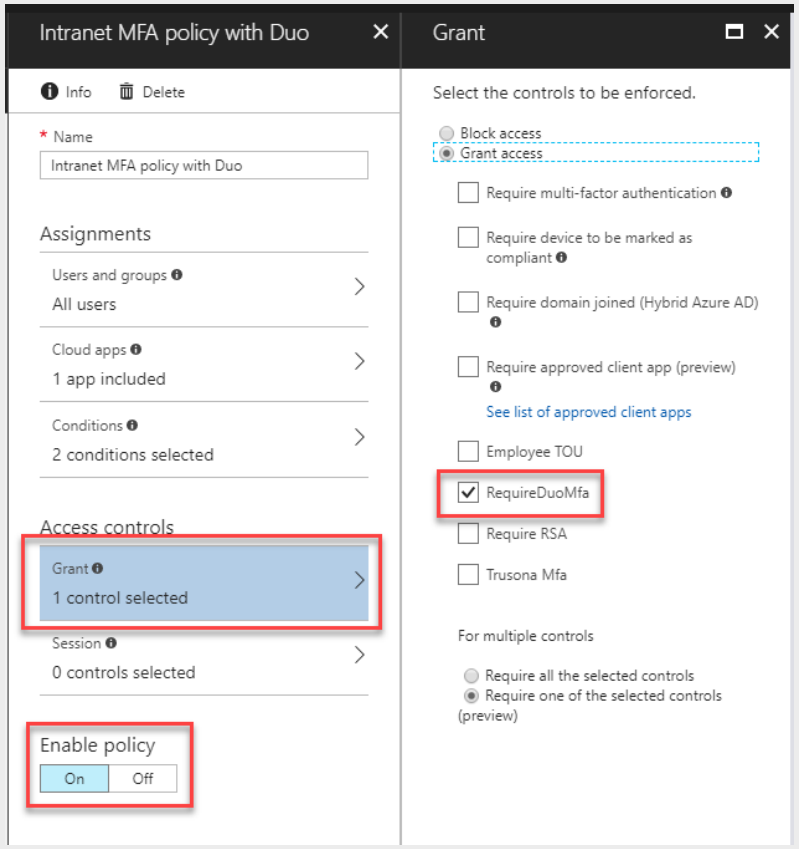
http://aka.ms/passwordguidance

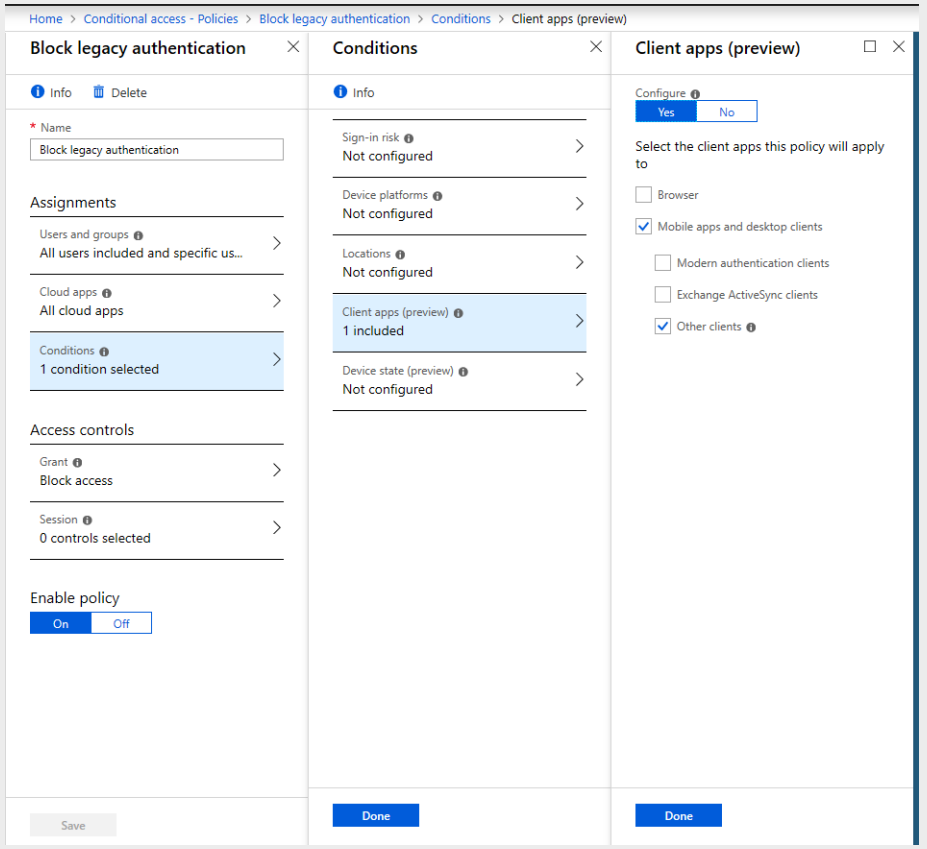
Minimum Length Requirements (to defeat brute force hash attacks)
Don’t use commonly attacked passwords
Use unique passwords


Azure AD
ADFS
MSA
Google ID
Android
iOS
MacOS
Windows
Windows Defender ATP
Geo-location
Corporate Network
Browser apps
Client apps
Conditions
40TB
Employee & Partner Users and Roles
Trusted & Compliant Devices
Location
Client apps & Auth Method
Machine learning
Session Risk
3
Real time Evaluation Engine
Policies
Effective policy
Controls
Allow/block access
Limited access
Require MFA
Force password reset
******
Terms of Use
Microsoft Cloud
Microsoft
Cloud App Security
Cloud SaaS apps
On-premises apps
WORK TOGETHER

Demo Conditional Acces

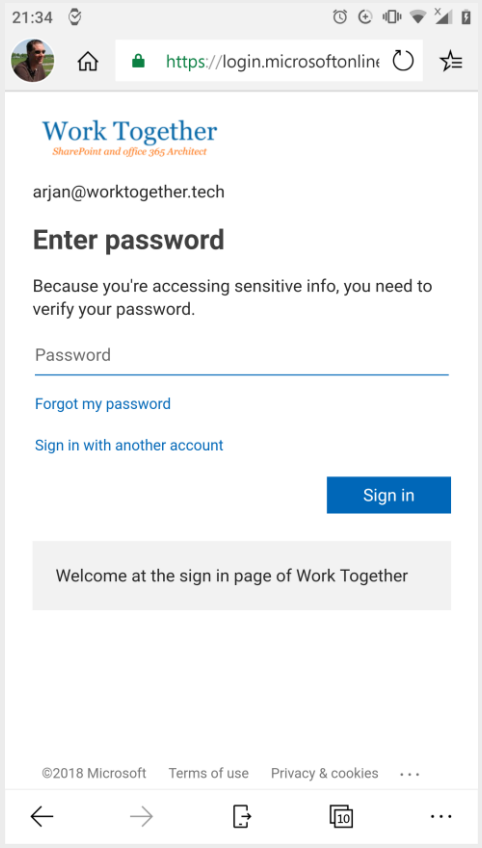
Conditional Access

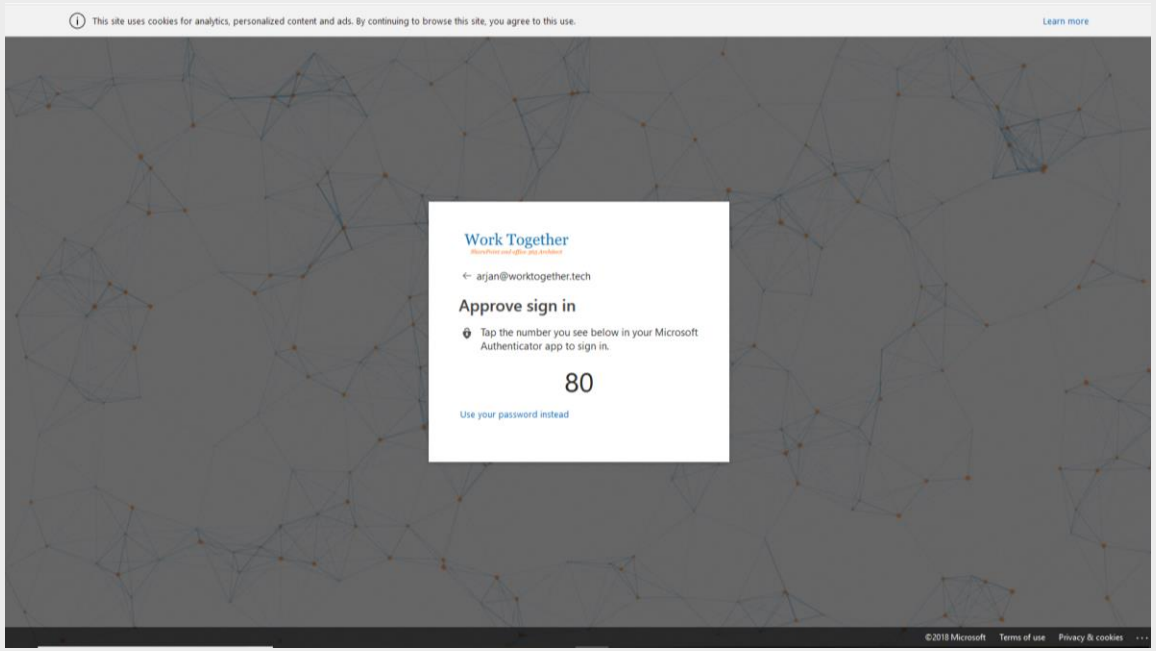




WORK TOGETHER

Company Branding

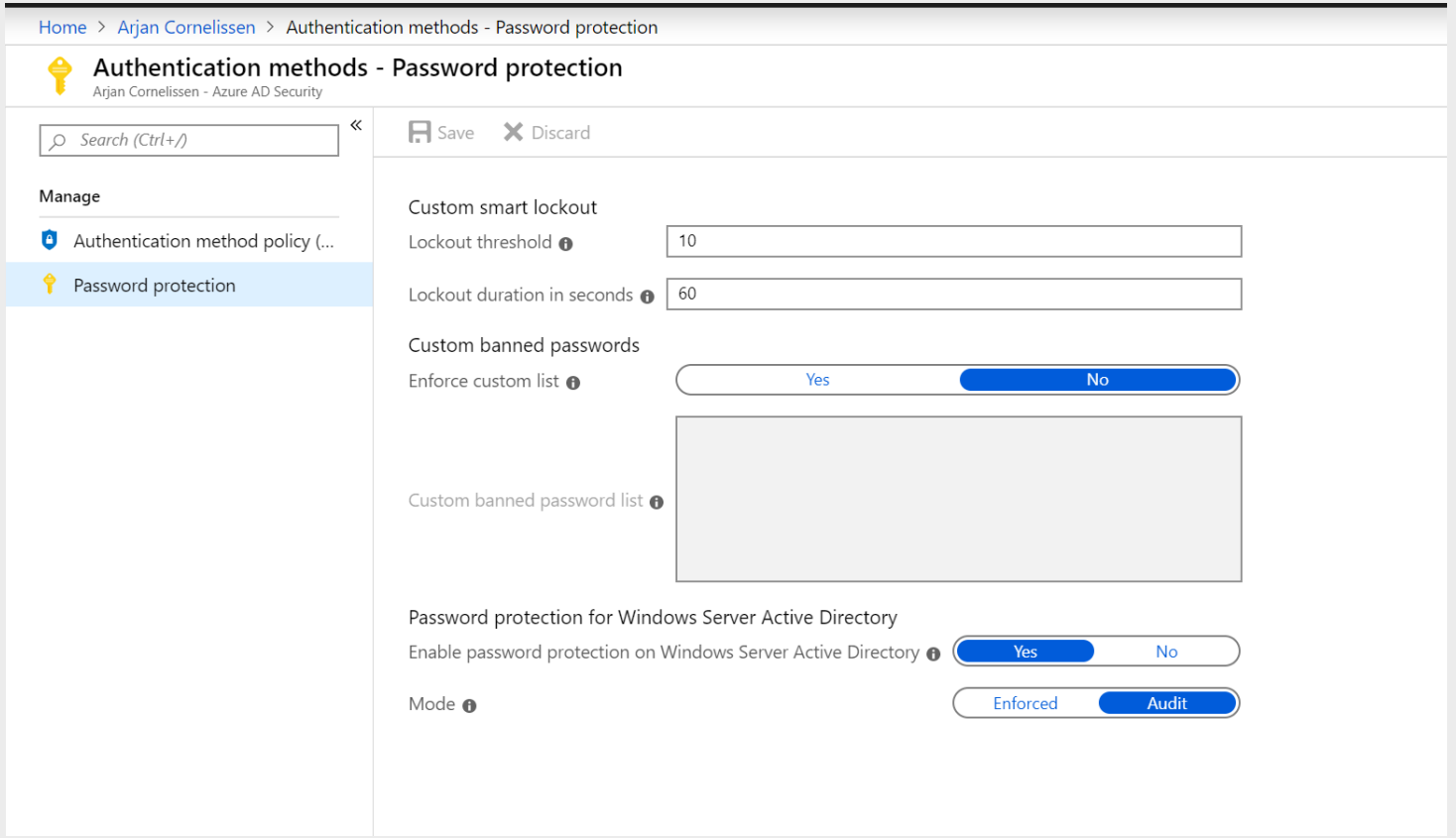




WORK TOGETHER

Demo Company Branding

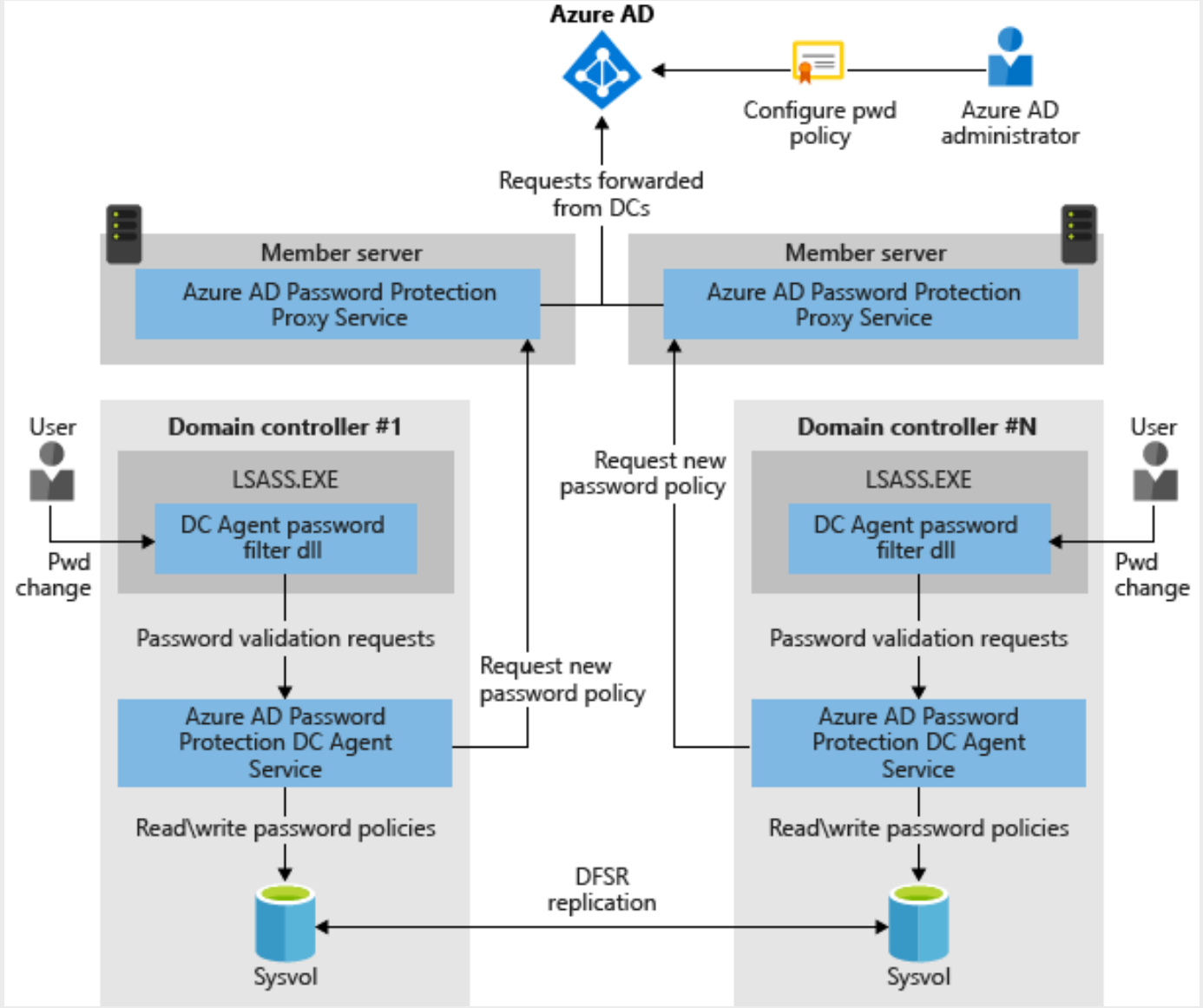
Password protection



WORK TOGETHER

Demo Password Protection

Hybrid Password Protection

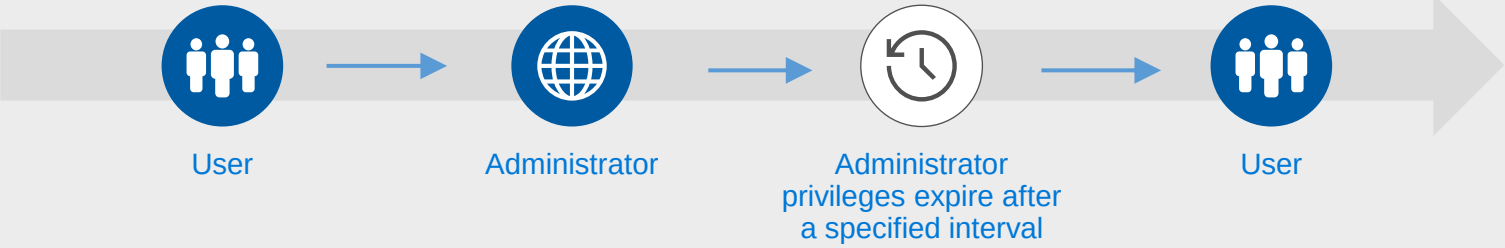


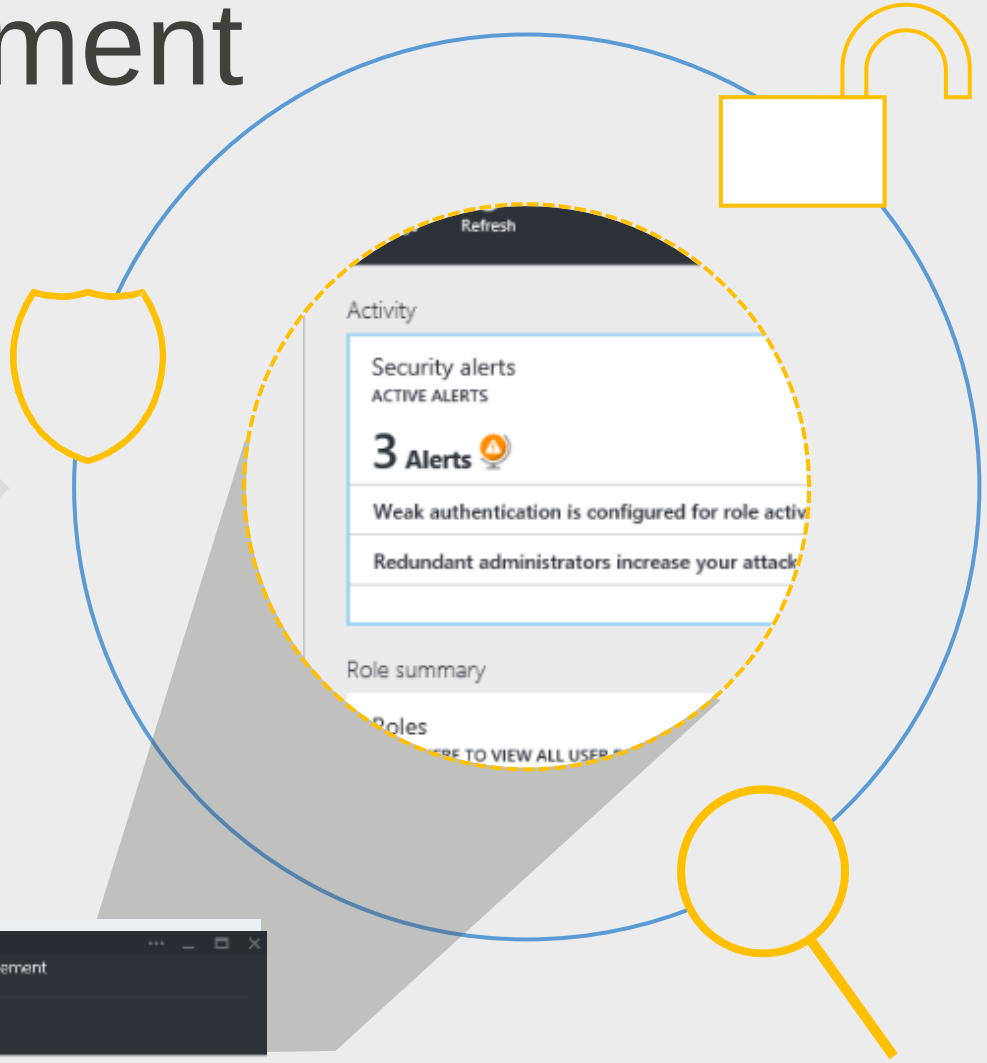
WORK TOGETHER

Admin side

Privileged Identity Management

Discover, restrict, and monitor privileged identities

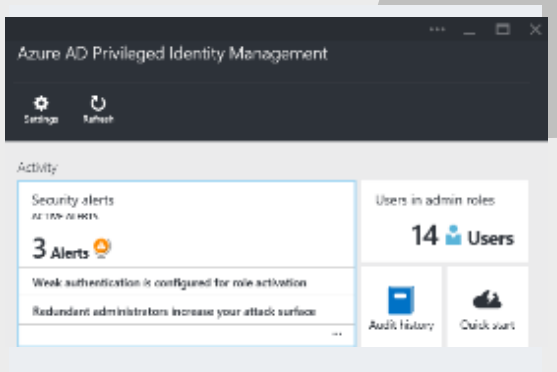




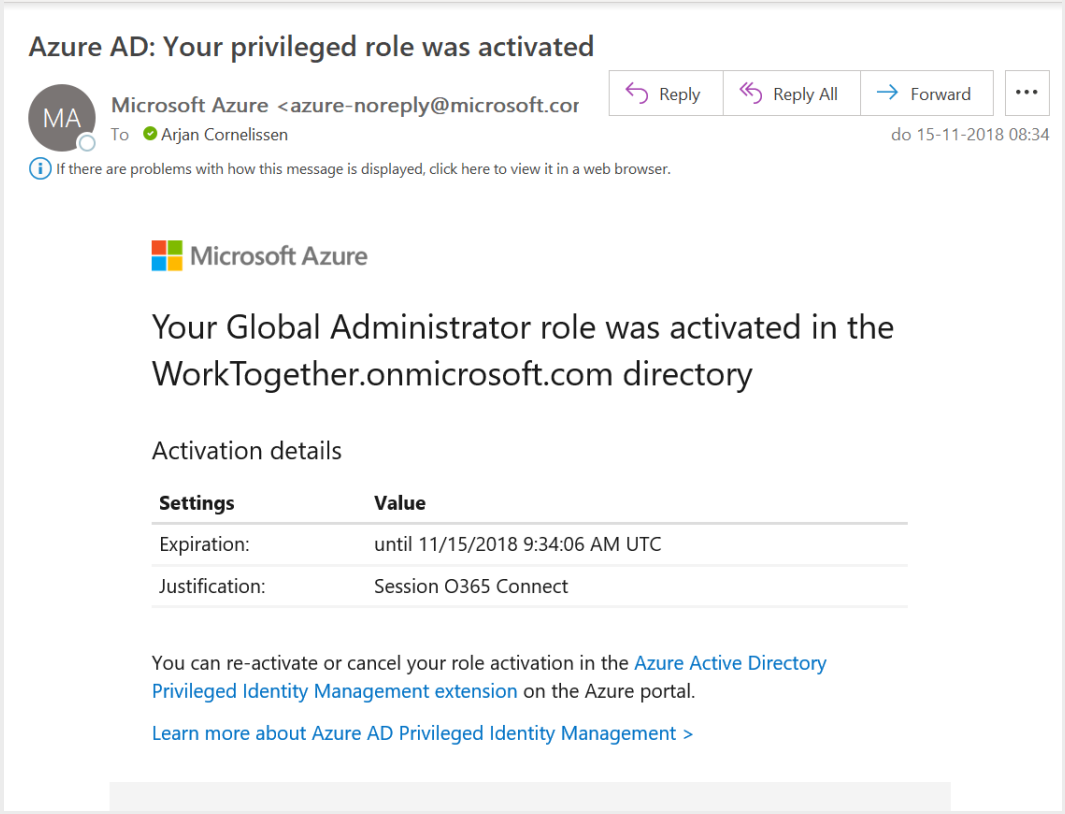
Enforce on-demand, just-in-time administrative access when needed

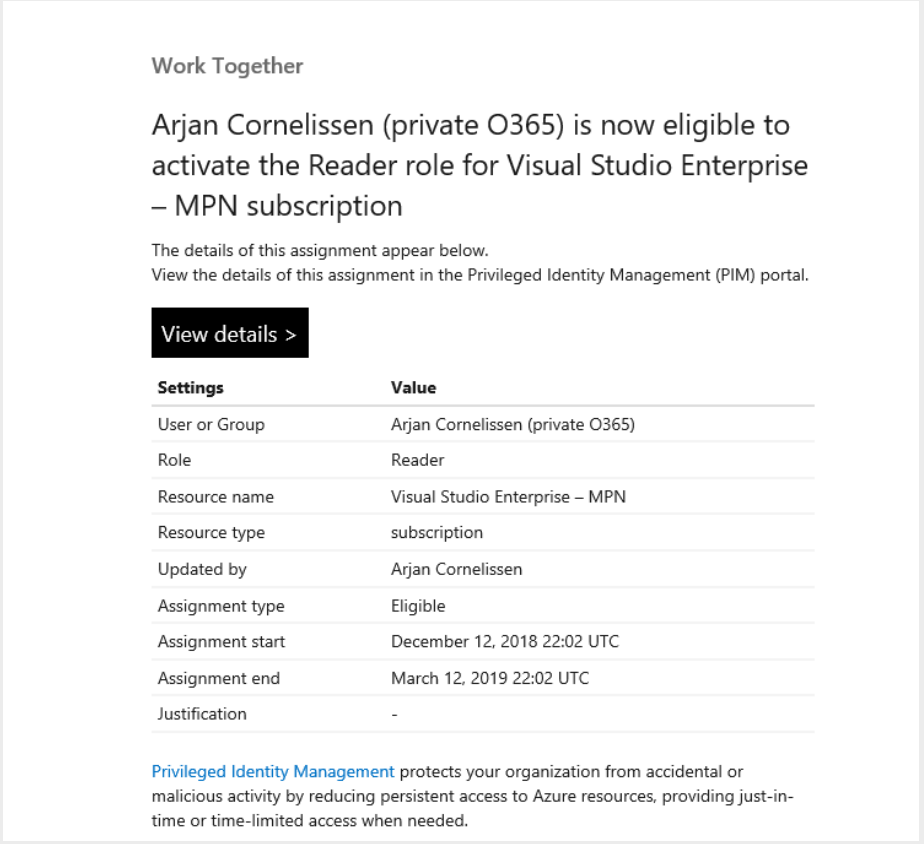
Ensure policies are met with alerts, audit reports and access reviews

Manage admins access in Azure AD and in Azure RBAC

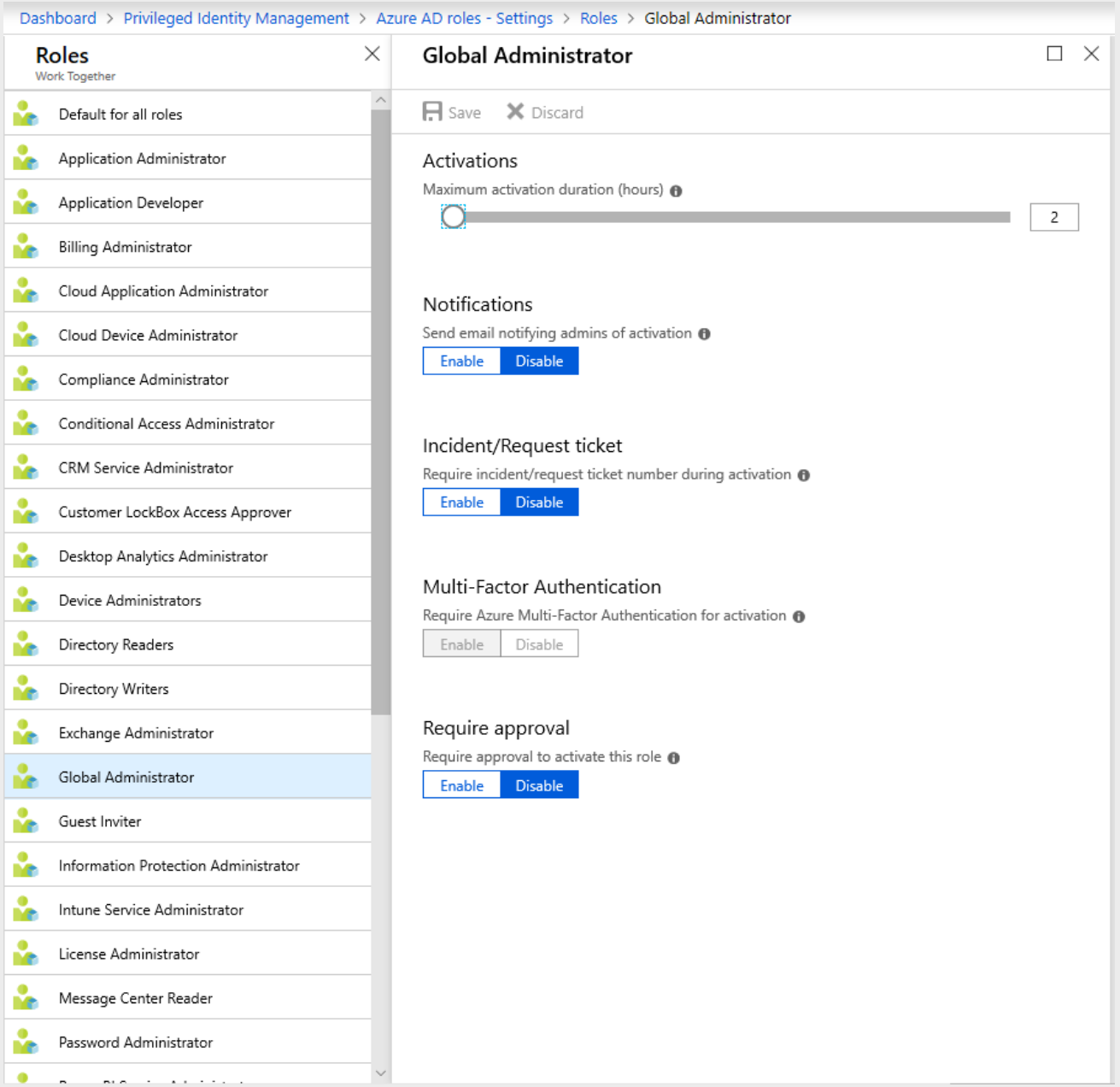


WORK TOGETHER





Privileged Identity



Identity Secure Score

Visibility into your Identity security position and how to improve it

Insights into your Identity security position

- Easily compare score against other organizations
- View trends

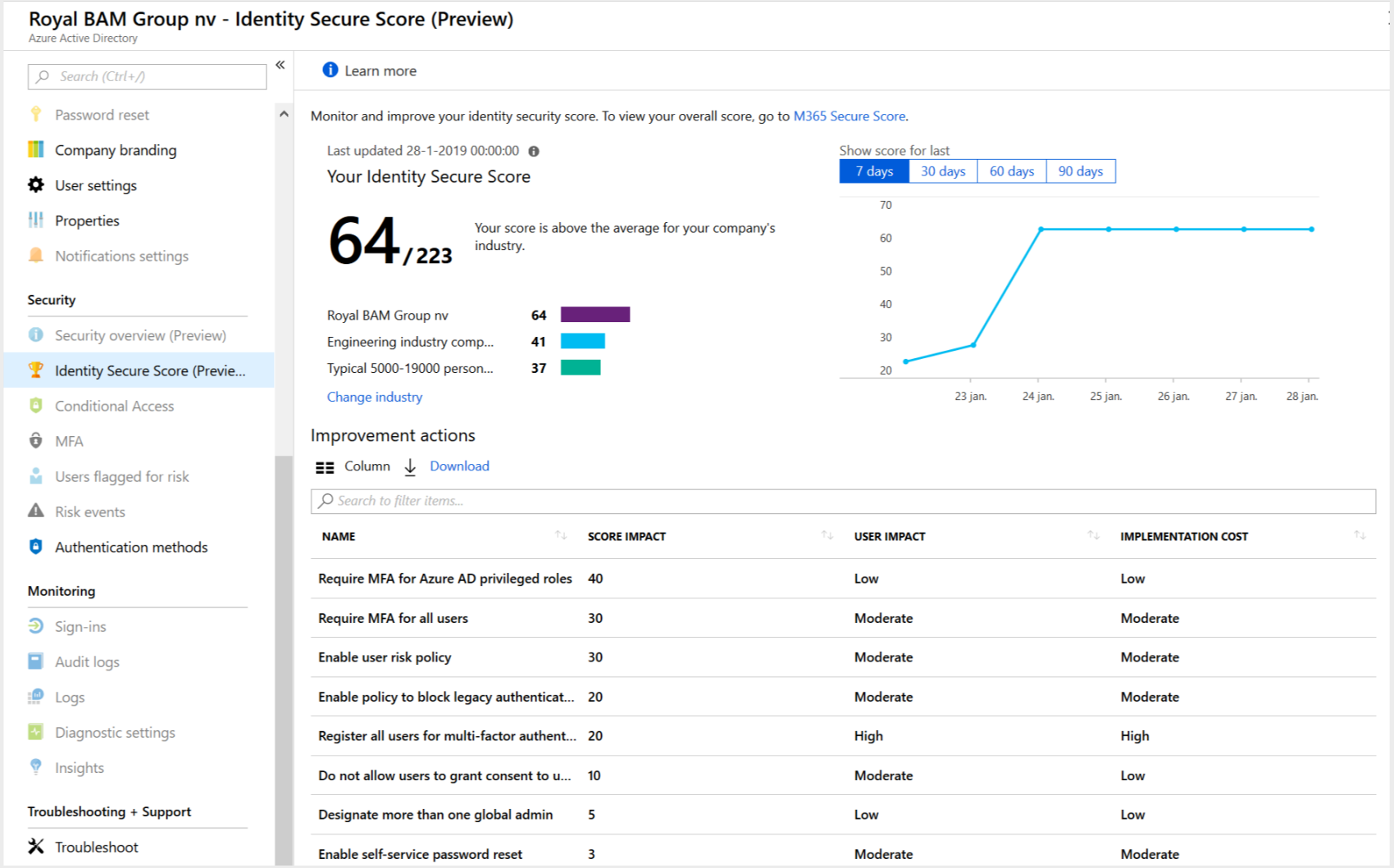
Guidance to increase your security level

- Set an ideal score.
- Choose controls to achieve ideal score based on impact.
- Ignore controls that are not valid for you.
- 3rd party product support.

Checkout your Identity secure score now @ http://aka.ms/MyIdentitySecureScore

WORK TOGETHER

Secure Score



Checkout your Identity secure score now @ http://aka.ms/MyIdentitySecureScore

WORK TOGETHER

Preview features

Password-less with Microsoft Authenticator app

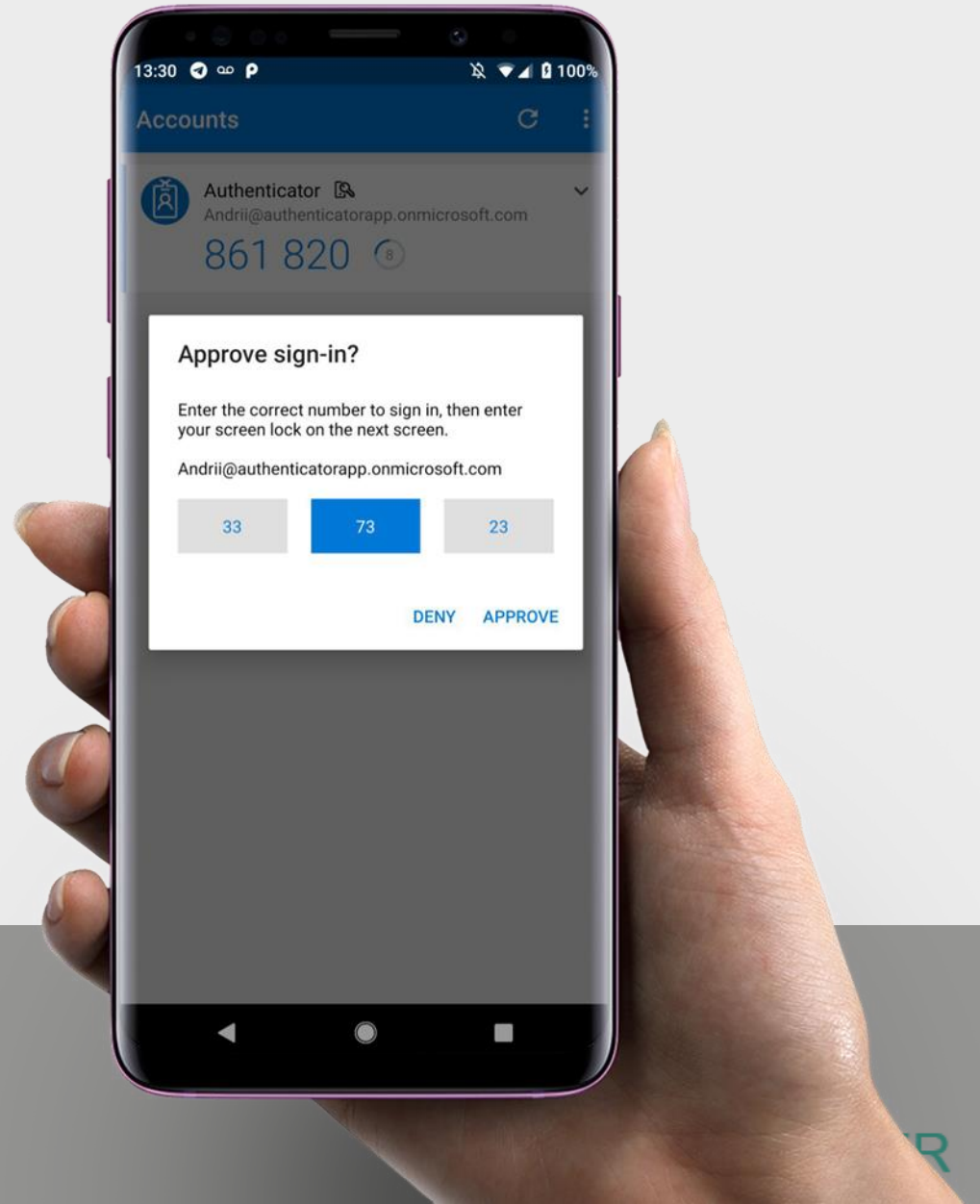
Password-less for MSA accounts

Available today

Password-less for Azure AD accounts

In Public preview today

aka.ms/gopasswordless



Demo Password less authentication

Getting the basics right

Strengthen your credentials

MFA reduces compromise by 99.99%

Reduce your attack surface

Blocking legacy authentication reduces compromise by 66%.

Automate threat response

Implementing risk policies reduces compromise by 96%

Increase your awareness with auditing and monitor security alerts

Attackers escape detection inside a victim's network for a median of 101 days. *(Source: FireEye)*

Enable self-help for more predictable and complete end user security

60% of enterprises experienced social engineering attacks in 2016. *(Source: Agari)*

WORK TOGETHER

Our Security mindset needs to be updated

WORK TOGETHER