DUTCH MICROSOFT ENTRA COMMUNITY

Entra ID: Just apply the basics, already!

Sander Berkouwer
Entraordinary Architect, DirTeam
dirteam.com

Microsoft Most Valuable Professional | VEEAM VANGUARD | vmware vEXPERT

Agenda

Basics for user accounts

- Default user settings may not apply to your organization
- Require multi-factor authentication
- Guests are also members of All Users

Basics for privileged accounts

- Multi-factor authentication everywhere, all the time
- Segregation of Duties (SoD) applies to the cloud, too
- Emergency access admins to the rescue!

DUTCH MICROSOFT ENTRA COMMUNITY

A little background…

Azure AD is now Entra ID

- Good idea? Yes, I think so.
- It never was Active Directory…
- Entra as a product family positions identity as an overall solution instead of a part of Azure
  - Azure
  - Microsoft 365
  - Dynamics 365
- Entra vs Entra ID: future positioning of features
  https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/new-name#azure-ad-renaming-exceptions-and-clarifications

DUTCH MICROSOFT ENTRA COMMUNITY


DUDE
SWEET
imgflip.com

About Entra ID

Active Directory (AD DS)

- Typically, on-premises
- Run by domain controllers
- Windows devices can be domain joined
- Devices can be managed with Group Policy when connected to the network or VPN
- Kerberos, LDAP(S), NTLM, LM

Entra ID

- Microsoft Cloud service
- Automatically scales (currently +300K CPUs)
- Windows 10+ devices can be Entra joined, other devices can be registered
- Devices can be managed with Microsoft Intune* regardless of the location of the device
- Modern authentication protocols (WS-FED, SAML, OAuth, OpenID Connect, SCIM

DUTCH MICROSOFT ENTRA COMMUNITY

Basics for User Accounts

Licenses for Entra ID and Microsoft 365

Entra ID Premium P2

Part of Microsoft 365 E5, A5

Includes Entra ID Premium P1

- Risk-based Conditional Access
- Identity Protection
- Entitlement Management
  - Access Packages
  - Access Reviews
- Privileged Identity Management (PIM)

Entra ID Premium P1

Part of Microsoft 365 E3, A3, and Business Premium

Includes all of Entra ID Free

- Conditional Access
  - Multi-factor Authentication for cloud and on-premises

Entra ID Free

Free 😆

- Security Defaults
  - Multi-factor Authentication for cloud
  - No exceptions
- Single Sign-on access to cloud apps

DUTCH MICROSOFT ENTRA COMMUNITY


CONDITIONAL ACCESS
SECURITY DEFAULTS

Security Defaults Free

Requires all users to register for Entra ID Multi-Factor Authentication

Requires administrators to register and perform multi-factor authentication

Global administrator
Application administrator
Authentication administrator
Billing administrator
Cloud application administrator
Conditional Access administrator
Exchange administrator
Helpdesk administrator
Password administrator
Privileged authentication administrator
Security administrator
SharePoint administrator
User administrator

Requires users to register and perform multifactor authentication when necessary

Blocks legacy authentication

Protects privileged activities like access to the Azure portal

Enabled, by default, on all new Entra ID tenants since February 2020

Enabled, by default, on all tenants without Conditional Access policies since July 2022

DUTCH MICROSOFT ENTRA COMMUNITY

TO DO: Require Multi-factor Authentication

Entra MFA

- Entra ID Security Defaults Free
- Entra ID Conditional Access P1/P2
- NPS Extension for Azure MFA (RADIUS) P1/P2
- Azure MFA Adapter for Active Directory Federation Services (AD FS) P1/P2

Azure MFA Server Stops working September 30th, 2024

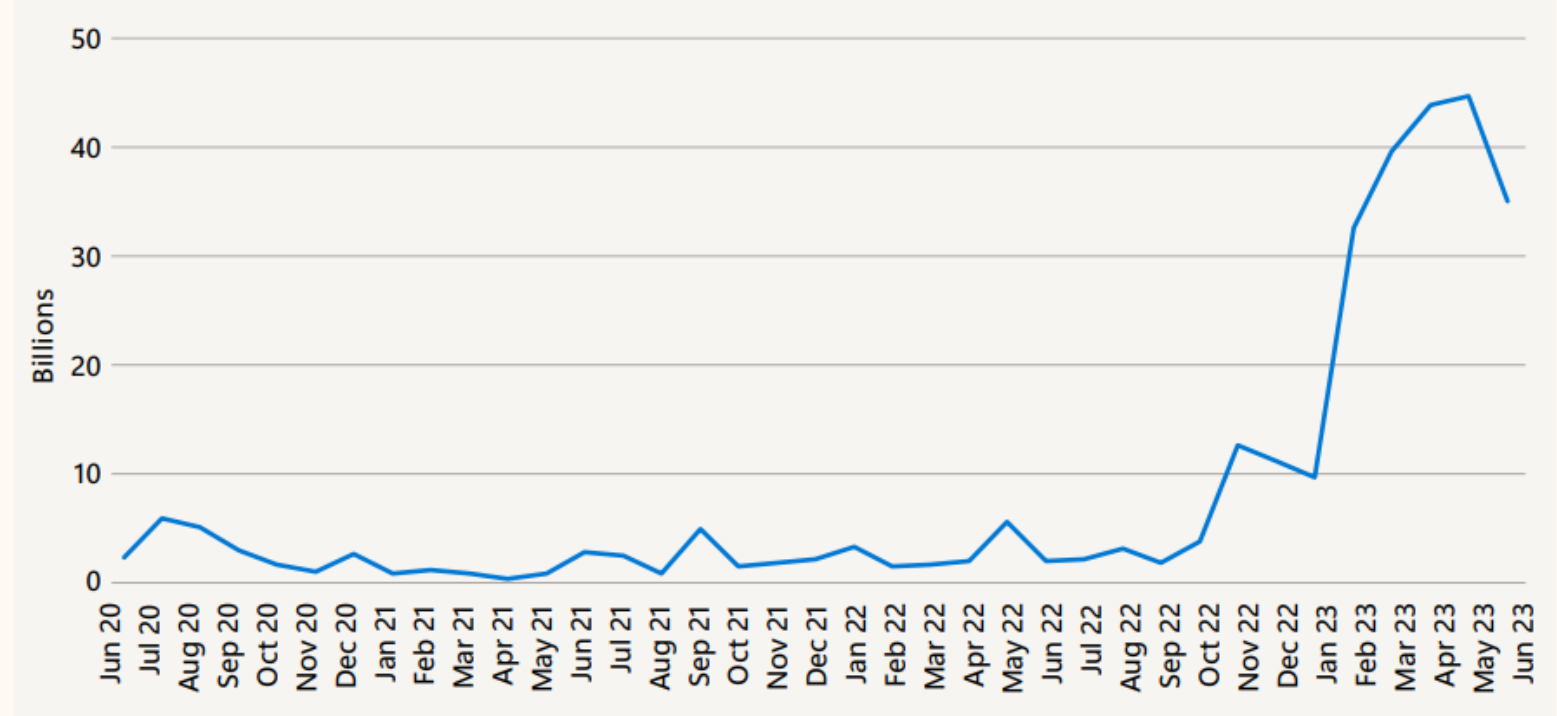
- RADIUS
- Internet Information Services (IIS)
- Azure MFA Server Adapter for Active Directory Federation Services (AD FS)

DUTCH MICROSOFT ENTRA COMMUNITY

Password-based attacks spiked in 2023

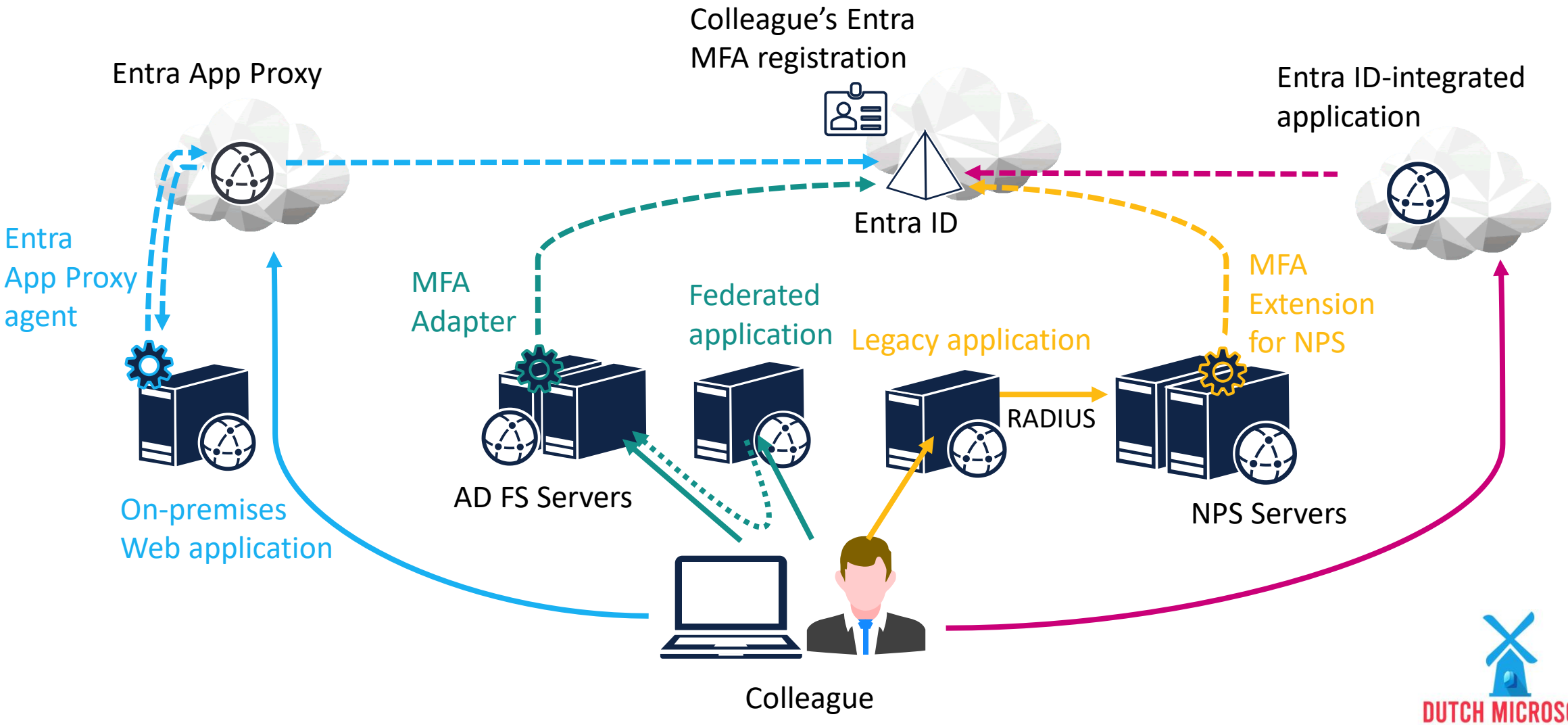
After a notable increase in the number of password-based attacks per month in October 2022, the number skyrocketed in 2023. In April, there were 11,000 attacks per second, a tenfold increase from the same time last year.

Source: Microsoft Digital Defense Report, October 2023



DUTCH MICROSOFT ENTRA COMMUNITY

The four faces of Entra MFA



DUTCH MICROSOFT ENTRA COMMUNITY

Tips and Tricks

There is a difference between registering and practicing MFA

- People need to register MFA before they can use it

Choose how to have people register for MFA

- People brought in scope for SSPR need to register their security information at next sign-in
- People brought in scope of MFA through Conditional Access or Security Defaults need to register within a 14-day grace period

Choose how people perform MFA

- Through Conditional Access, they are prompted when and how often you want them to be
- Through Identity Protection and Security Defaults they are prompted only for risky sign-ins

Don’t use the legacy PhoneFactor portal to require or configure MFA

Migrate to the Authentications Methods blade before 30 September 2025

DUTCH MICROSOFT ENTRA COMMUNITY

One more thing about MFA everywhere…

TO DO: Limit the ability to invite guests

By default, Guest collaboration is enabled in Entra ID

- Any account, even guests can invite guests to collaborate with in SharePoint Online and O4B
- Invitation can be sent to any domain and sharing is enabled to any domain, by default
  - Allow and Deny lists are available, both for inviting and sharing

- Invitations and access do not expire, by default
- Access is granted to anyone with the link, by default
- Edit access is granted, by default. (not View)

Configure the right invitation settings in the Entra ID Portal Free

Configure the right sharing settings in the Entra ID Portal M365

DUTCH MICROSOFT ENTRA COMMUNITY

TO DO: Limit the ability to add apps Free

By default, App integration is enabled in Entra ID

- Any account, even guests, can delegate access to any app to their data
- Group owners can delegate access to the groups data

Incorrectly configured and overpermissioned apps may syphon data in a supplier attack scenario

Configure the user consent settings in the Entra ID Portal

Enable the Admin consent workflow in the Entra ID Portal

When an admin provides admin consent, the app can be used by All Users, by default. This includes guests.

DUTCH MICROSOFT ENTRA COMMUNITY

TO DO: Disable full access to SharePoint from unmanaged devices P1/P2

Unmanaged devices are

- Not domain-joined or Hybrid Entra ID-joined
- Not Entra ID-joined
- Not Intune-managed (or managed through another Entra ID-integrated MDM solution)

Basically, you can’t guarantee anything on these devices…

Do they run BitLocker? Do they have running and up to date anti-malware?

Attackers may gain access to access tokens and impersonate the user

Limit access in Conditional Access to Exchange Online, SharePoint Online and OneDrive for Business to web-only access, with no possibilities to download files

DUTCH MICROSOFT ENTRA COMMUNITY

Basics for Privileged Accounts

Global admin rights are not human rights.

Thanks for the inspiration, Sami ;-)

TO DO: Sync mere mortals, but not privileged accounts Free

When Active Directory is compromised, you don’t want Entra ID to be compromised, too.

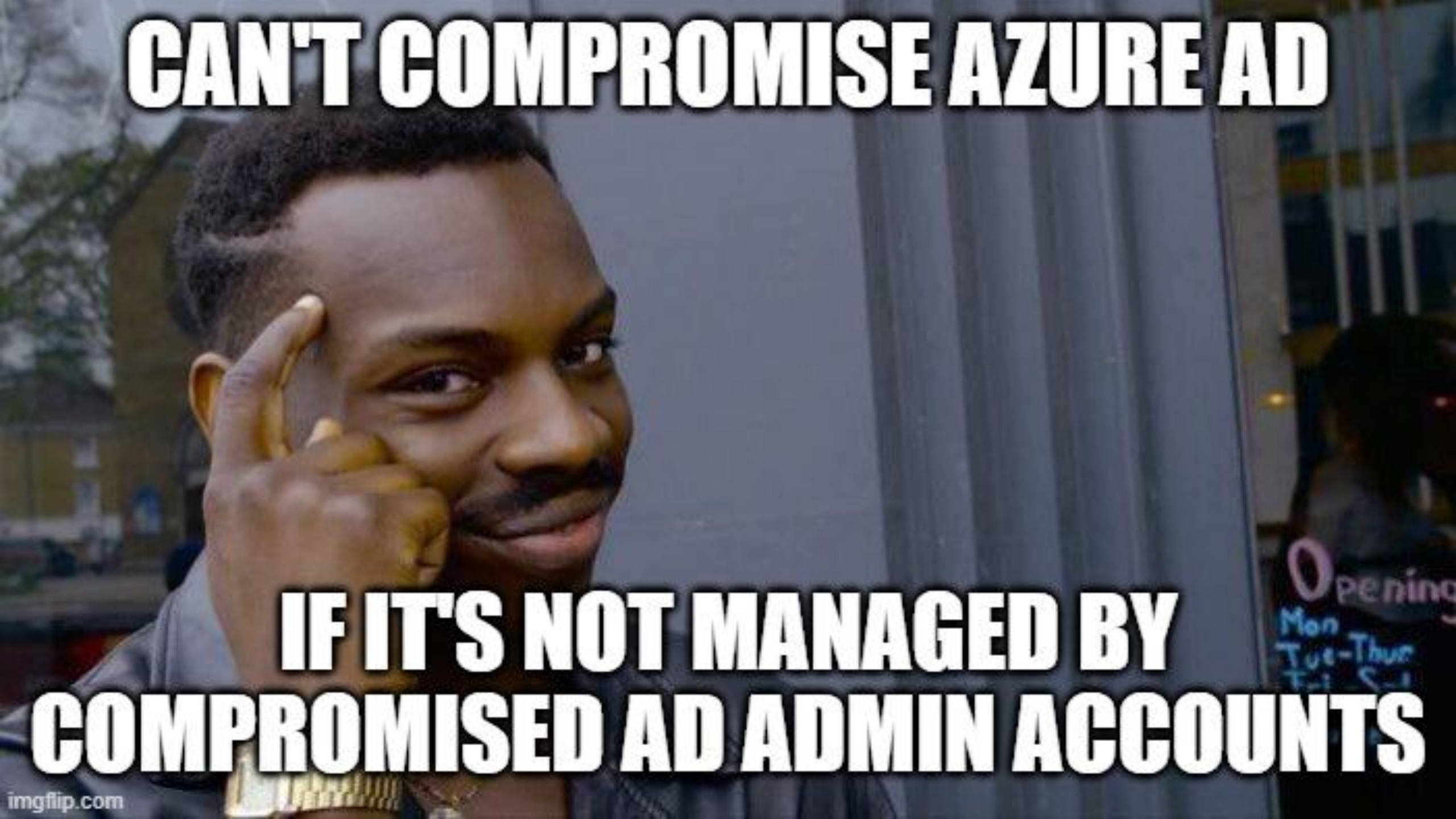
- Do not synchronize accounts in privileged Entra ID roles
- Instead, create named cloud-only admin accounts
- Change tenant-side Entra Connect sync settings to disable soft matching

Delegate least privileges to admin accounts

- Limit the number of Global Administrators to three persons
- Delegate the User administrator role, Hybrid Identity administrator role, etc.

Apply Segregation of Duties (SoD)

DUTCH MICROSOFT ENTRA COMMUNITY


CAN'T COMPROMISE AZURE AD
IF IT'S NOT MANAGED BY COMPROMISED AD ADMIN ACCOUNTS
imgflip.com

TO DO: Configure emergency access accounts Free

Configure two emergency access accounts, that:

- Are non-personal accounts
- Are not synchronized from an on-premises directory
- Are not federated towards an on-premises deployment
- Are provided with non-expiring strong credentials
- Are permanently endowed with the Global administrator role

At least one of these two accounts should not be provided with an obligation to perform multi-factor authentication upon signing in, or the emergency access account is configured with a Security Key.

The other account must be exempt from any Conditional Access policy

Sign-ins should result in an alert both by e-mail and text message

DUTCH MICROSOFT ENTRA COMMUNITY

Concluding

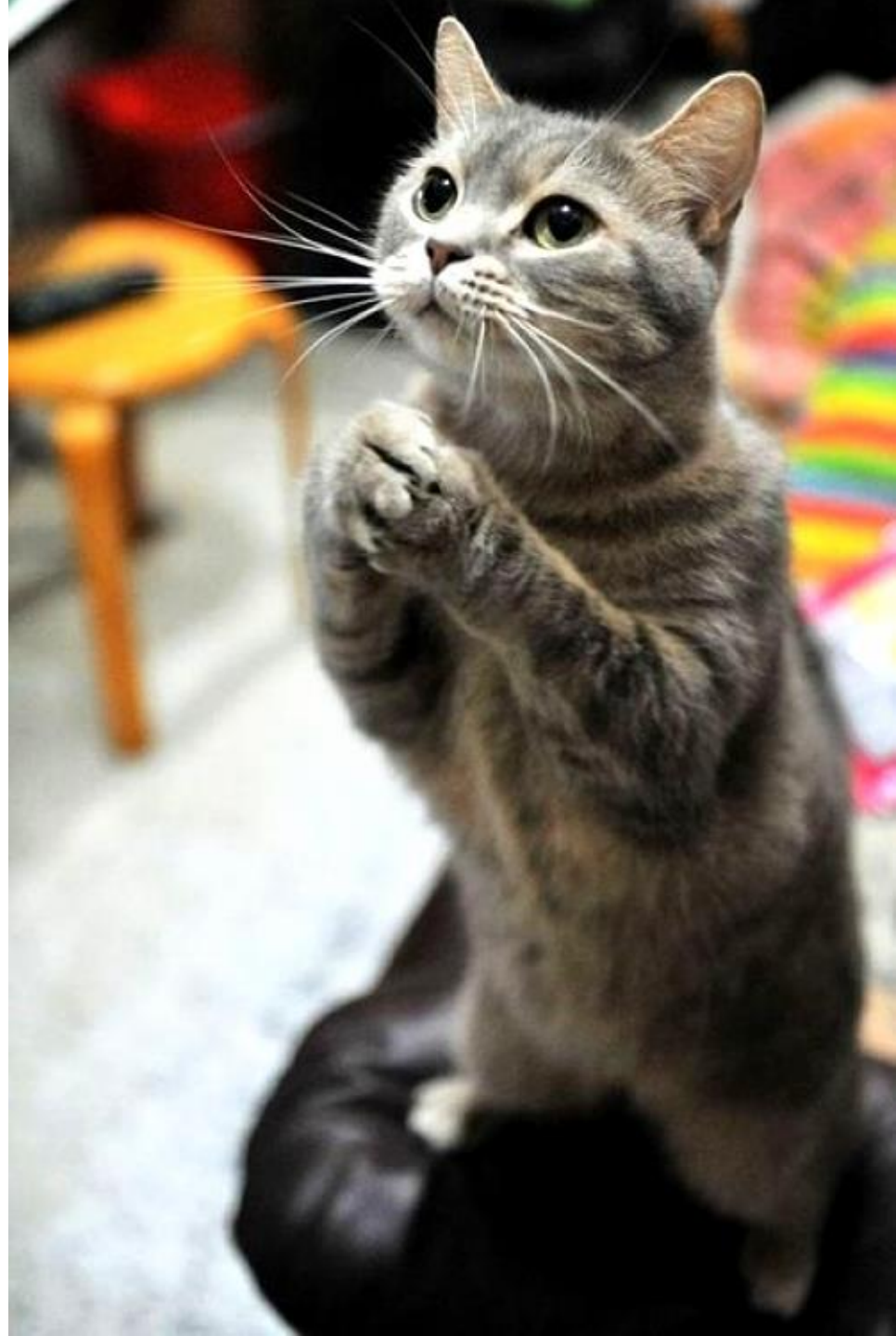
Just apply the basics in your Entra ID tenant!

Basics for user accounts

- Require multi-factor authentication
- Limit the ability to invite guests
- Limit the ability to add apps
- Limit access to data from unmanaged devices

Basics for privileged accounts

- Sync mere mortals, but not privileged accounts
- Apply Segregation of Duties (SoD)
- Apply the principle of least privileges
- Configure emergency access accounts



Questions?

Thank you

DirTeam.com

@SanderBerkouwer

www.linkedin.com/in/SanderBerkouwer

www.youtube.com/c/SanderBerkouwer