Microsoft 365 tenant setup & configuration

Been there, done that?

@thomasvochten

About me

Thomas Vochten ☕💻🏃

Technology evangelist Microsoft 365 & Security

@thomasvochten

https://thomasvochten.com

mail@thomasvochten.com

MVP Microsoft® Most Valuable Professional

BIWUG

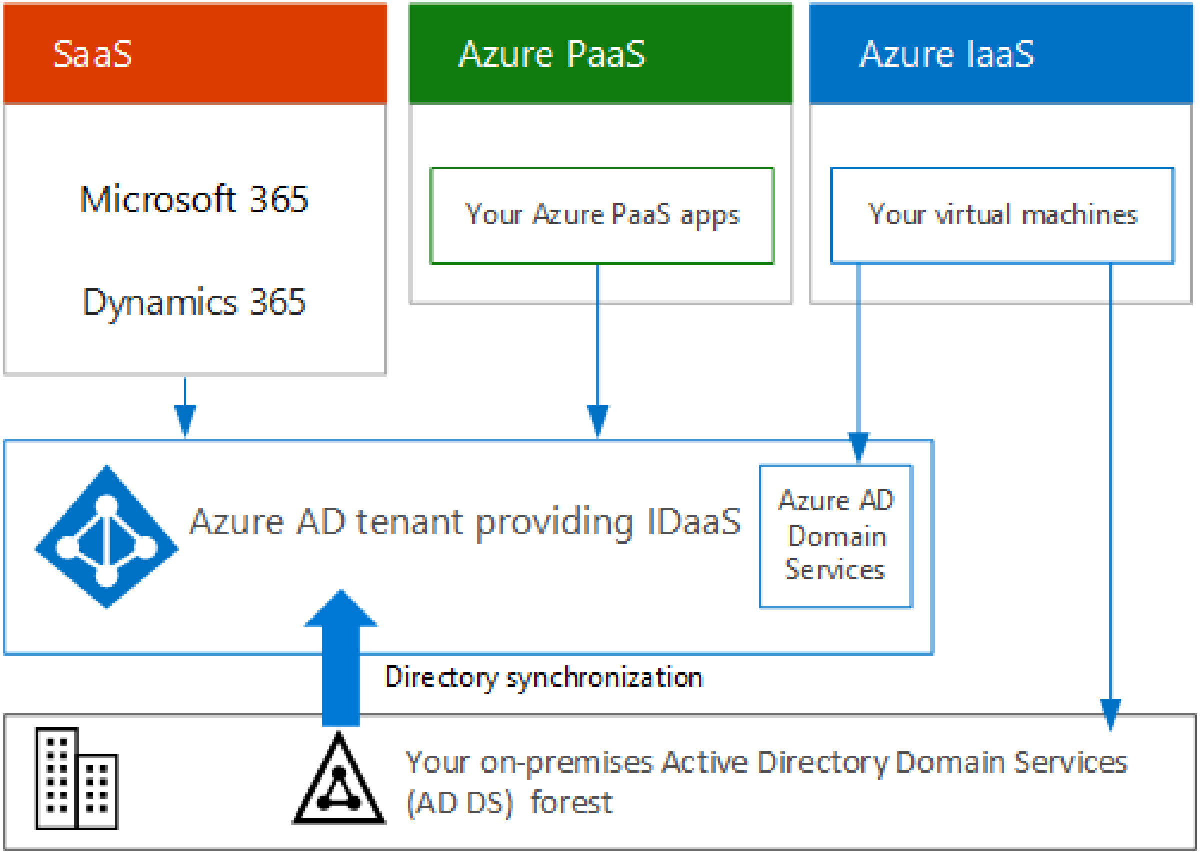
CRONOS GROEP

Agenda

1. General tenant considerations
2. Multi-Geo & Multi-Tenant
3. Domains, DNS & networking
4. Organizational settings
5. Security, security, security!

General tenant considerations

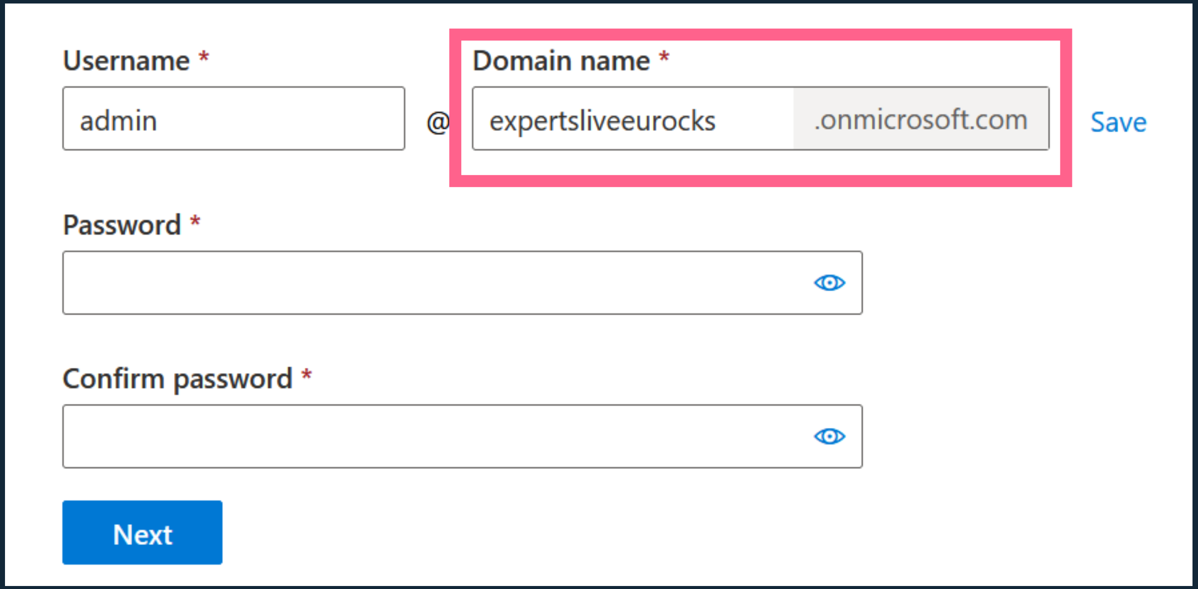
Understanding the Microsoft 365 hierarchy


SaaS
Microsoft 365
Dynamics 365
Azure PaaS
Your Azure PaaS apps
Azure IaaS
Your virtual machines
Azure AD tenant providing IDaaS
Azure AD Domain Services
Directory synchronization
Your on-premises Active Directory Domain Services (AD DS) forest

@thomasvochten

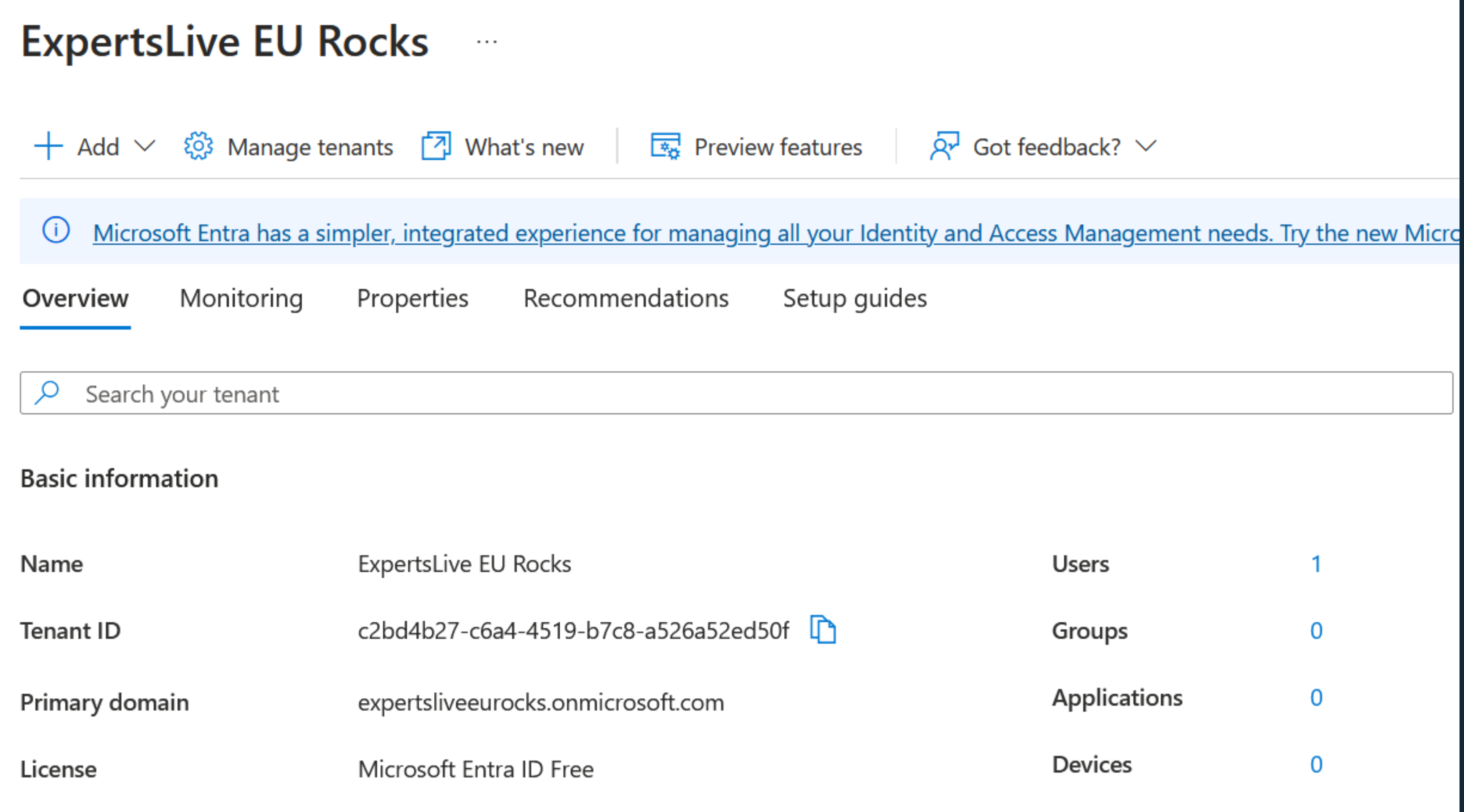
Creating a new tenant

https://signup.microsoft.com



Username * admin @ Domain name * expertsliveeurocks .onmicrosoft.com

Tenant properties in Entra ID



ExpertsLive EU Rocks

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Micro

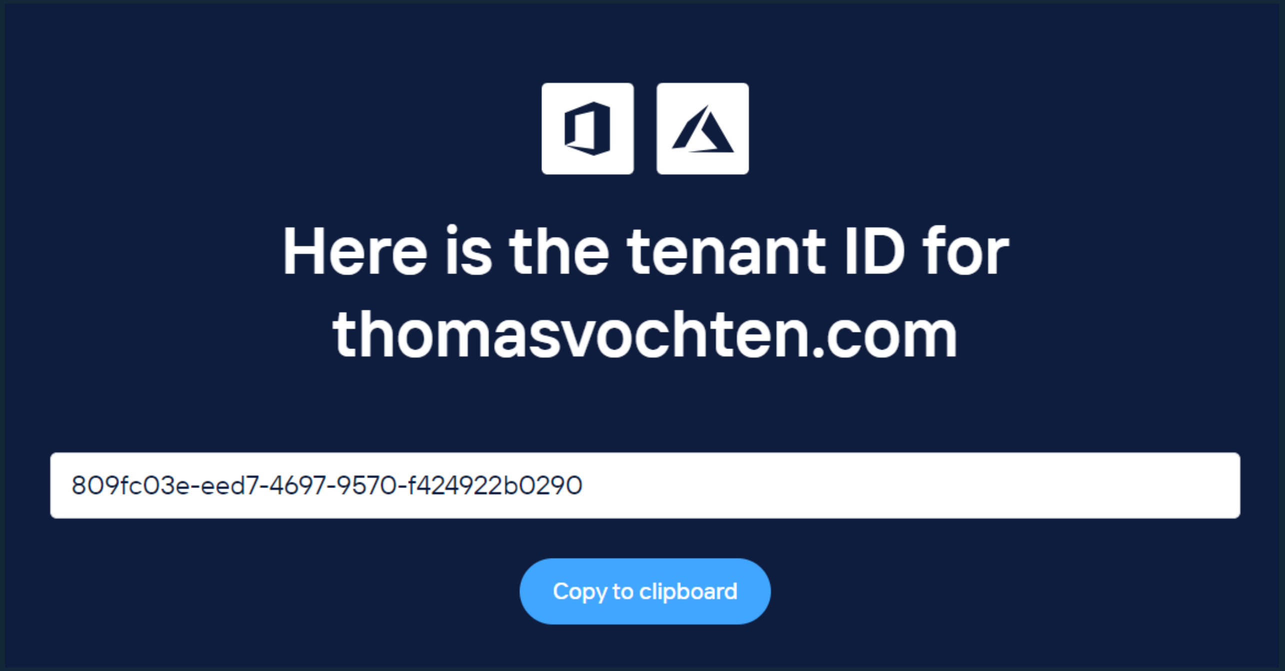
Basic information

Name	ExpertsLive EU Rocks	Users	1
Tenant ID	c2bd4b27-c6a4-4519-b7c8-a526a52ed50f	Groups	0
Primary domain	expertsliveeurocks.onmicrosoft.com	Applications	0
License	Microsoft Entra ID Free	Devices	0

About that Tenant ID 💎

It’s public information!

➡️ https://www.whatismytenantid.com

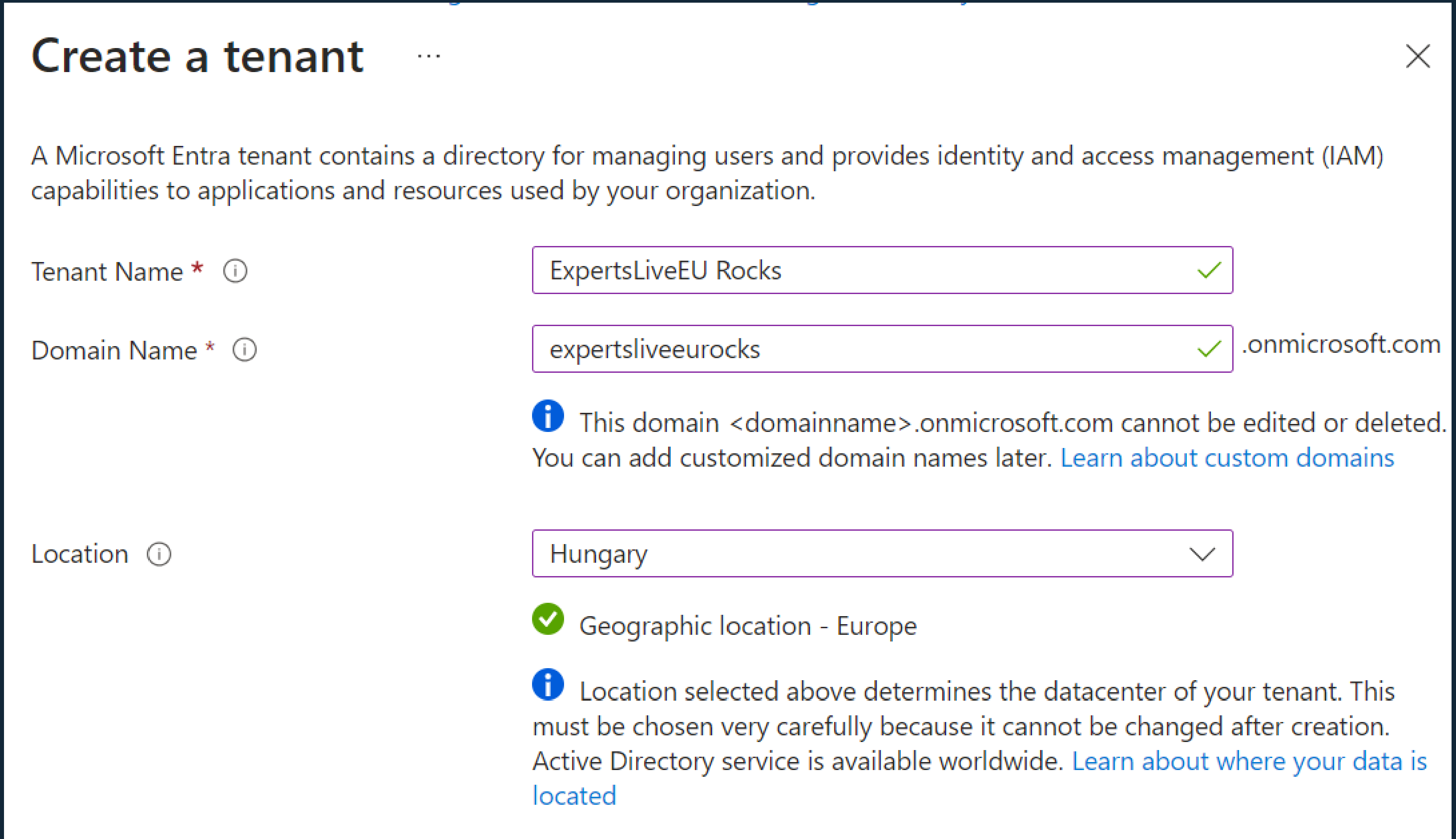


Here is the tenant ID for thomasvochten.com

809fc03e-eed7-4697-9570-f424922b0290

@thomasvochten

Creating a new tenant in Entra ID



Create a tenant

A Microsoft Entra tenant contains a directory for managing users and provides identity and access management (IAM) capabilities to applications and resources used by your organization.

Tenant Name * ⓘ	ExpertsLiveEU Rocks ✓
Domain Name * ⓘ	expertsliveeurocks ✓ .onmicrosoft.com
Location ⓘ	Hungary

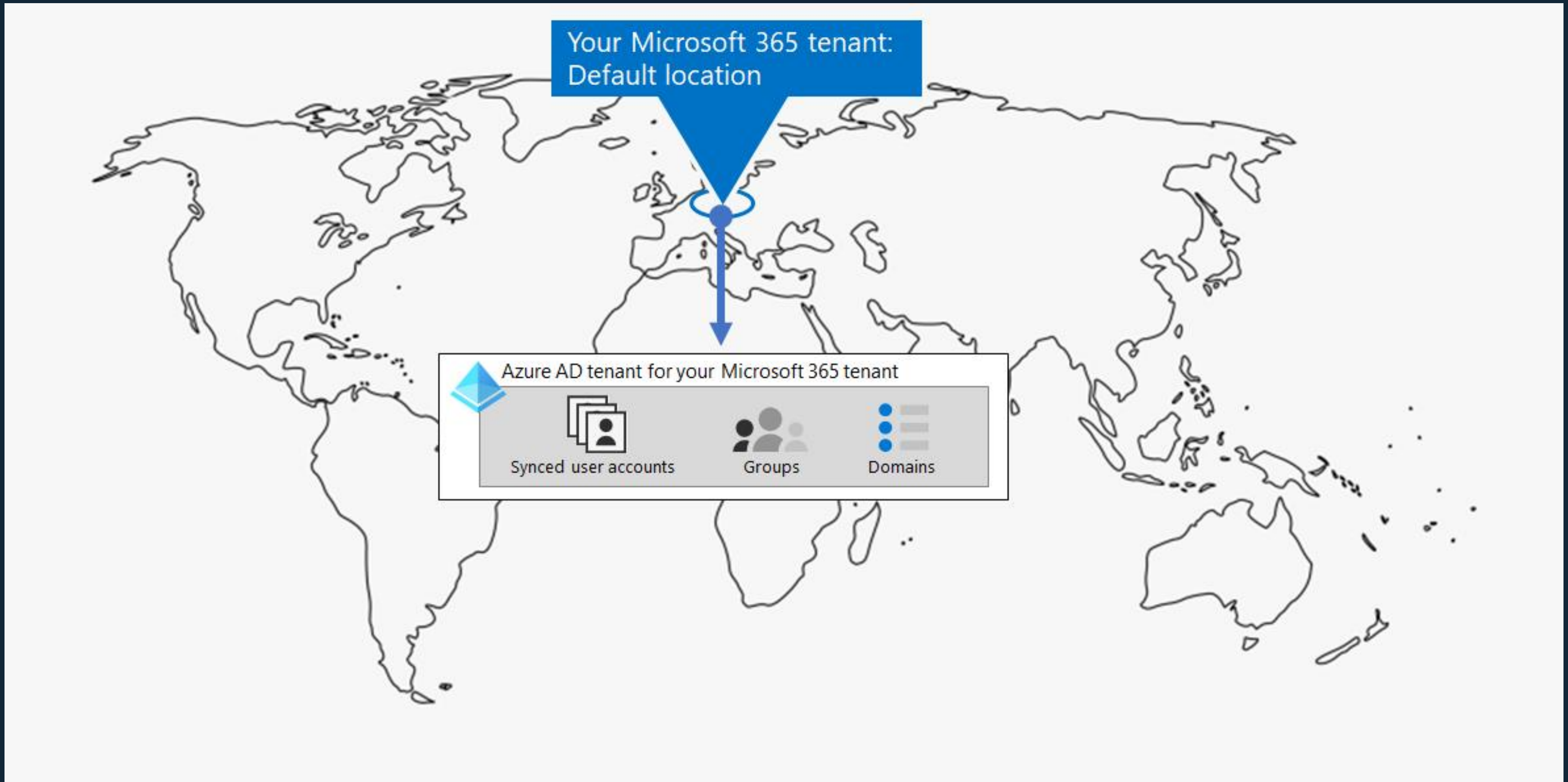
ⓘ This domain <domainname>.onmicrosoft.com cannot be edited or deleted. You can add customized domain names later. Learn about custom domains

✓ Geographic location - Europe

ⓘ Location selected above determines the datacenter of your tenant. This must be chosen very carefully because it cannot be changed after creation. Active Directory service is available worldwide. Learn about where your data is located

@thomasvochten

First things first. Where's my data?


Your Microsoft 365 tenant:
Default location
Azure AD tenant for your Microsoft 365 tenant
Synced user accounts
Groups
Domains

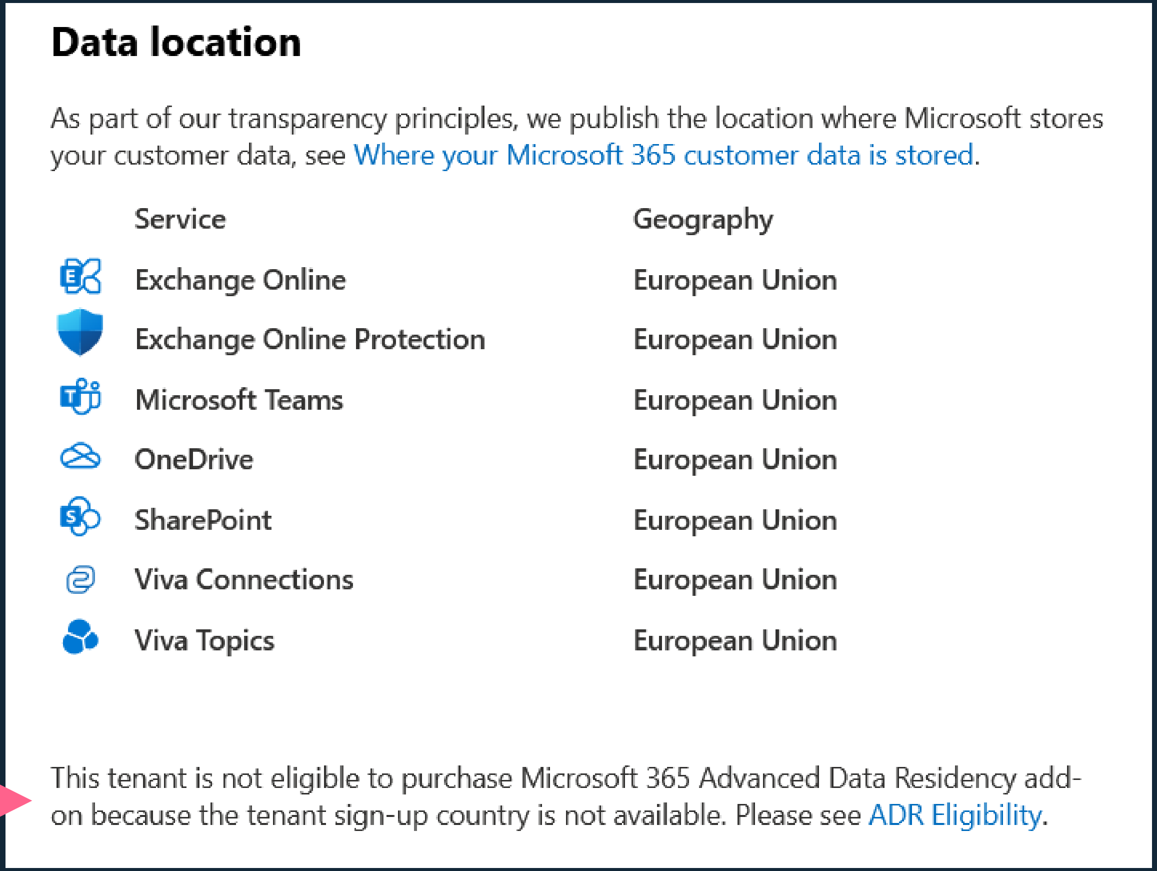
Data Residency primer

- Default Geography of the Microsoft Entra ID Tenant
- Available Geographies for a given service

@thomasvochten

First things first. Where's my data?

Settings > Org Settings > Organization profile > Data location



Data location

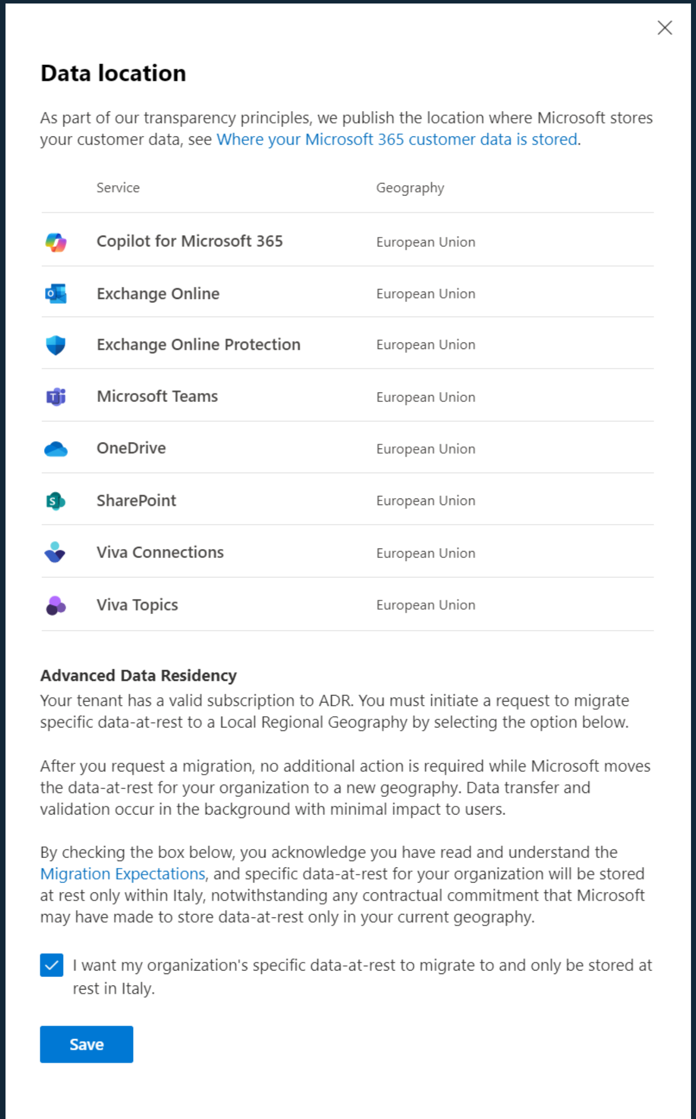
As part of our transparency principles, we publish the location where Microsoft stores your customer data, see Where your Microsoft 365 customer data is stored.

Service	Geography
Exchange Online	European Union
Exchange Online Protection	European Union
Microsoft Teams	European Union
OneDrive	European Union
SharePoint	European Union
Viva Connections	European Union
Viva Topics	European Union

This tenant is not eligible to purchase Microsoft 365 Advanced Data Residency add-on because the tenant sign-up country is not available. Please see ADR Eligibility.

Workloads supported by the ADR add-on

- Exchange Online
- SharePoint and OneDrive
- Microsoft Teams
- Microsoft 365 Copilot
- Microsoft Defender for Office P1 and Exchange Online Protection
- Office for the Web
- Viva Connections
- Viva Topics
- Microsoft Purview



Data location

As part of our transparency principles, we publish the location where Microsoft stores your customer data, see Where your Microsoft 365 customer data is stored.

Service	Geography
Copilot for Microsoft 365	European Union
Exchange Online	European Union
Exchange Online Protection	European Union
Microsoft Teams	European Union
OneDrive	European Union
SharePoint	European Union
Viva Connections	European Union
Viva Topics	European Union

Advanced Data Residency

Your tenant has a valid subscription to ADR. You must initiate a request to migrate specific data-at-rest to a Local Regional Geography by selecting the option below.

After you request a migration, no additional action is required while Microsoft moves the data-at-rest for your organization to a new geography. Data transfer and validation occur in the background with minimal impact to users.

By checking the box below, you acknowledge you have read and understand the Migration Expectations, and specific data-at-rest for your organization will be stored at rest only within Italy, notwithstanding any contractual commitment that Microsoft may have made to store data-at-rest only in your current geography.

☑ I want my organization's specific data-at-rest to migrate to and only be stored at rest in Italy.

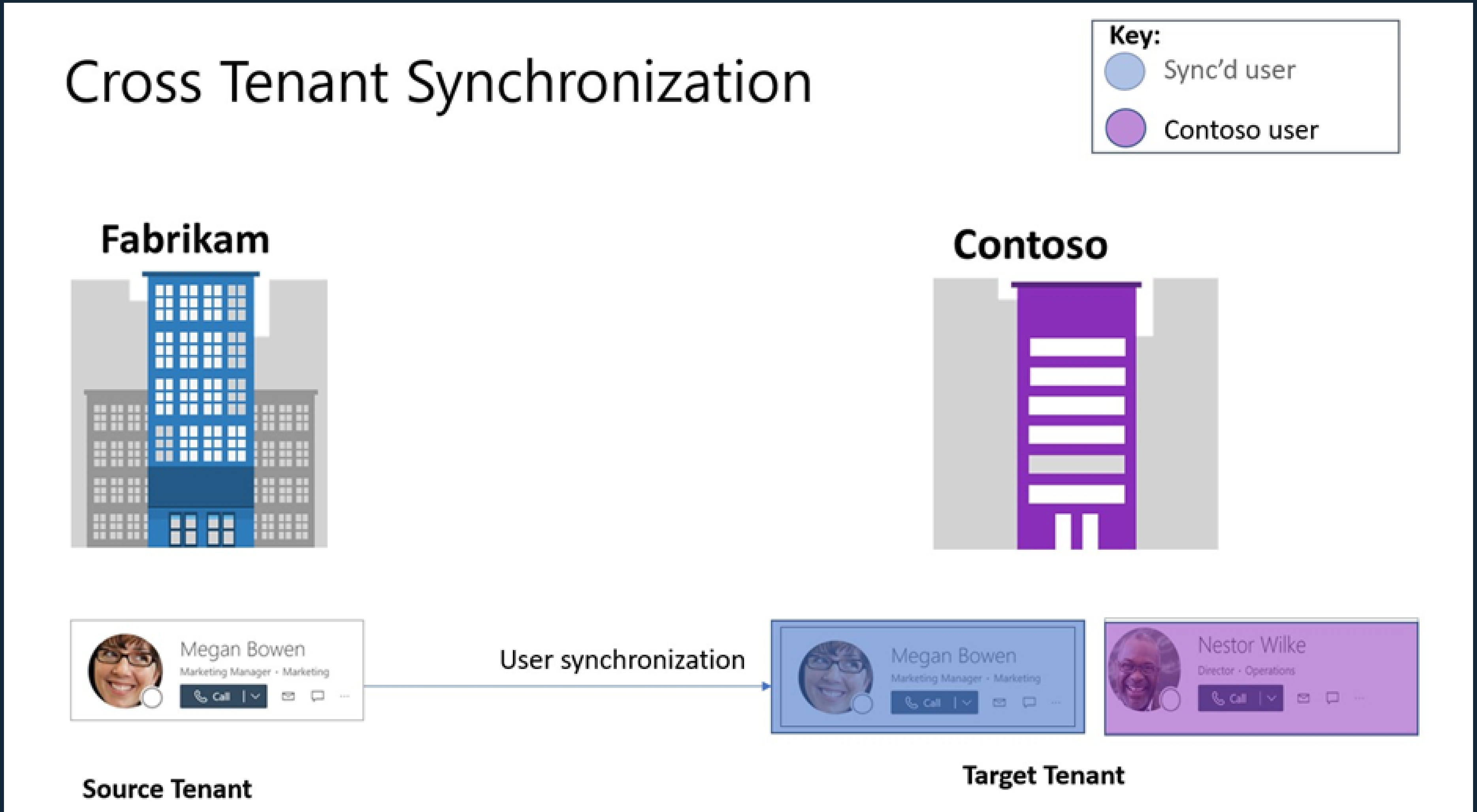
@thomasvochten

Multi-Geo & Multi-Tenant

Multi-geo

- Exchange, SharePoint, OneDrive, Teams
- Home region / Central geo vs Satellite geo
- Preferred data location (account attribute, eg “EUR”)
- Data sovereignty (not performance)
- Move the data to a satellite geo
  (expect OneDrive: Start-SPOUserAndContentMove)
- Cross-region sync for a transparent experience
- EA & multi-geo licenses for at least 5% of accounts

Multi-tenant



Cross Tenant Synchronization

Key:
● Sync'd user
● Contoso user

Fabrikam

Contoso

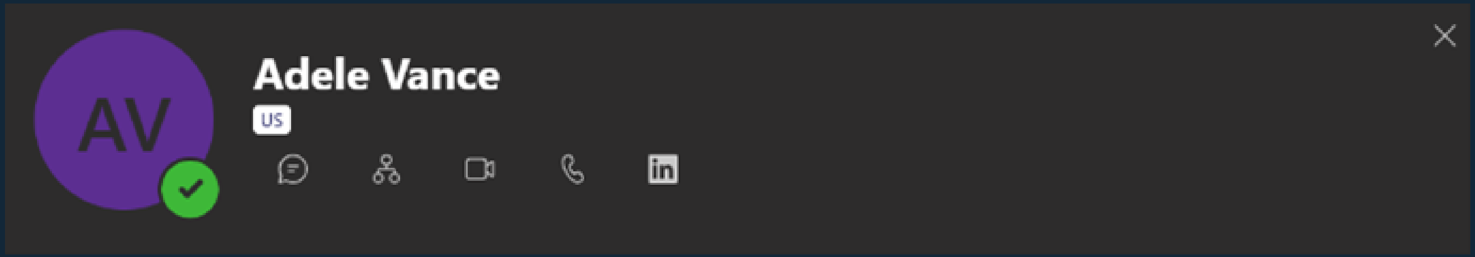
User synchronization

Source Tenant

Target Tenant

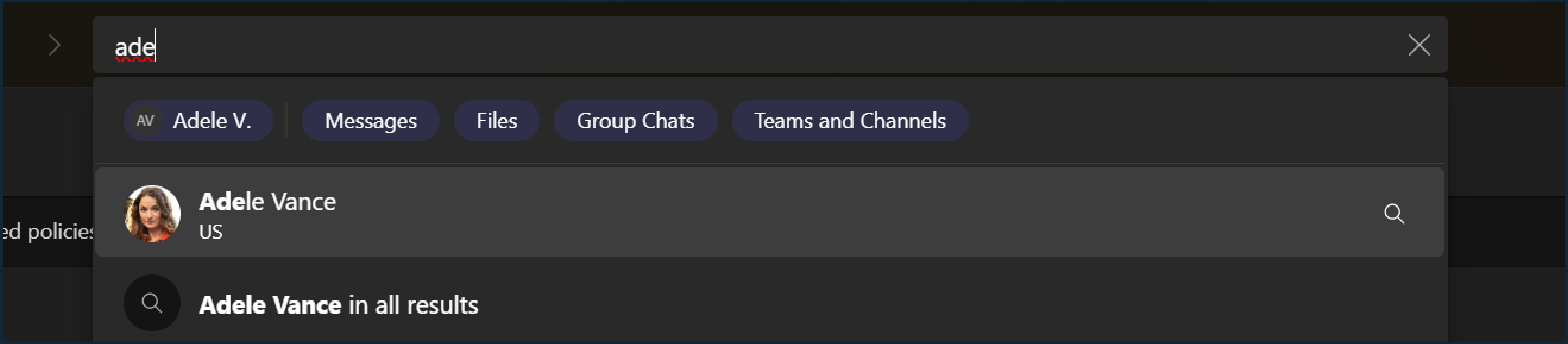
@thomasvochten

Include an optional label



Adele Vance

US



ade

Adele Vance

US

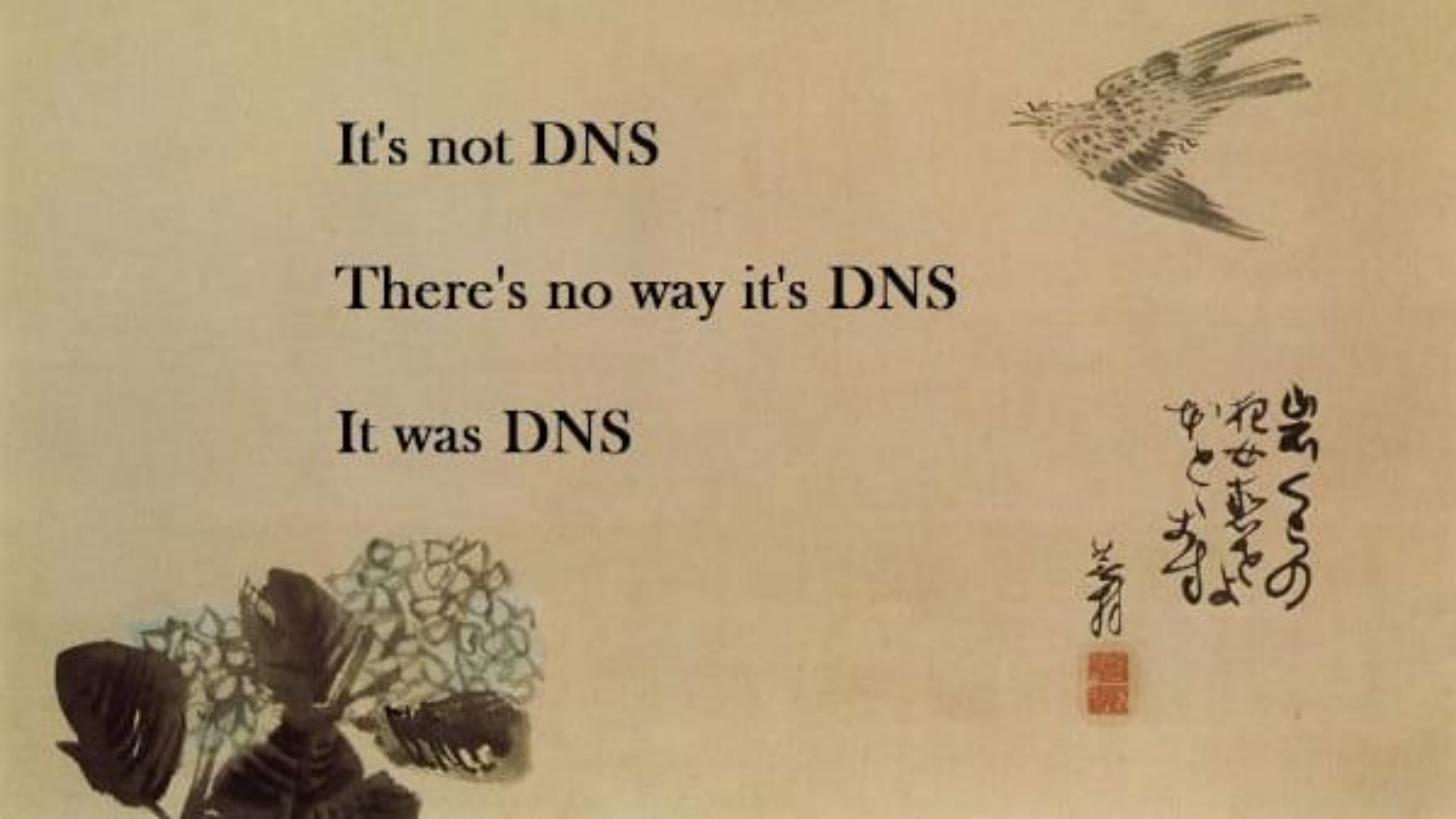
Adele Vance in all results

Multi-tenant

- Cross-tenant synchronization configuration is added with the name MTO_Sync_<TenantID>, but no sync jobs are created yet.
- Organization relationship is added to the cross-tenant access settings based on the multitenant organization templates for cross-tenant access and identity synchronization.
- The multitenant org template for cross-tenant access will be set to automatically redeem user invitations, inbound as well as outbound.
- Maximum of five tenants in the multitenant organization is supported.
- Maximum of 100,000 users per tenant is supported.
- Teams on the web, macOS, Microsoft Teams Rooms (MTR), and VDI/AVD aren't supported.

Domains, DNS & networking

@thomasvochten

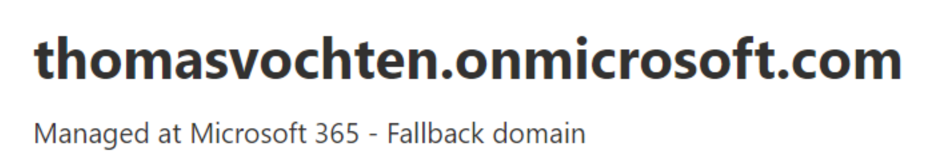


It's not DNS

There's no way it's DNS

It was DNS

Meet your “fallback domain”



thomasvochten.onmicrosoft.com

Managed at Microsoft 365 - Fallback domain

- used for default usernames, email routing,…
- used for your SharePoint Online & OneDrive URL’s

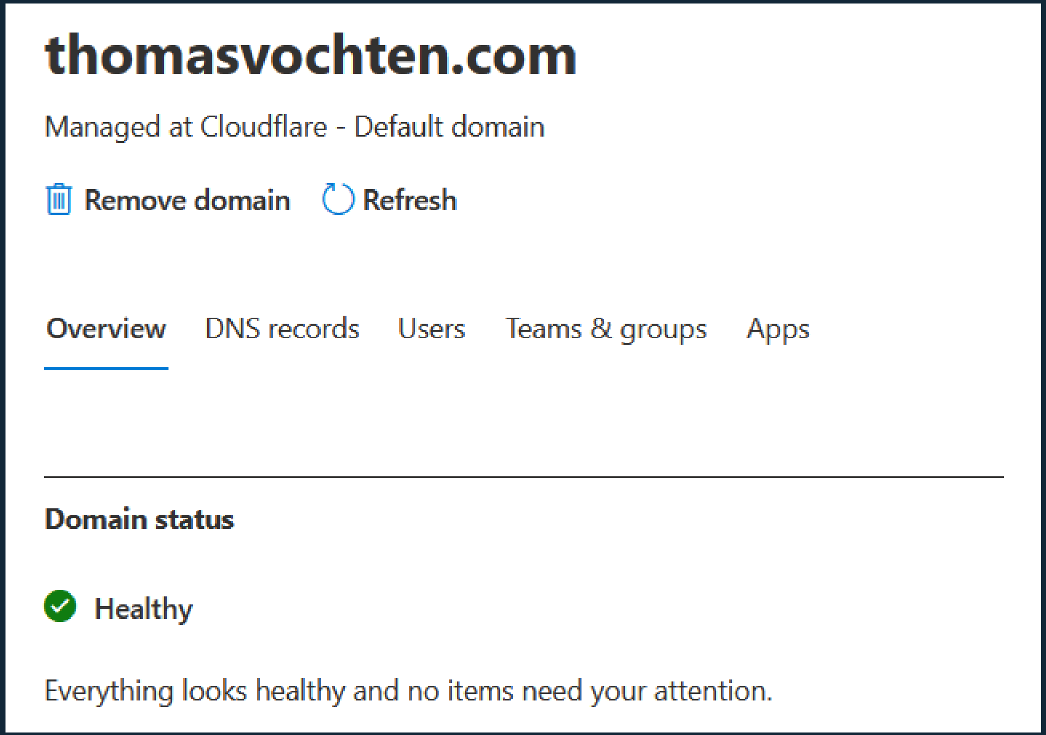
Changing yourdomain.sharepoint.com

- When would you want this?
- Less than 10K sites? Standard Tenant Rename
- Less than 100K sites? Advanced Tenant Rename
- Does not impact email addresses
- Not available for “special” clouds or in a multi-geo situation
- Temporary redirect for one year included

```
Start-SPOTenantRename -DomainName <DomainName> -ScheduledDateTime
<YYYY-MM-DDTHH:MM:SS>
```

Custom domains

- Checking health regularly
- What if you have an external DNS provider?
- Subdomains only through a separate DNS hoster



thomasvochten.com

Managed at Cloudflare - Default domain

Domain status

✓ Healthy

Everything looks healthy and no items need your attention.

Essential DNS records and why you need them

- TXT or MX record for verification of ownership (MS=ms XXXXXXXX)
- MX record for email delivery
- CNAME & SRV records for other services such as Teams
- SPF TXT record to help prevent spam

Proper email authentication is key

Sender Policy Framework

SPF verifies the domain from which emails are sent

SPF protects companies from phishers who spoofed the **5321.MailFrom** address

Domain Keys Identified Mail

DKIM helps prevent attackers from sending messages that look like they came from your domain

DKIM adds a digital signature to email message headers

Domain-based Message and Reporting Compliance

DMARC protects companies from phishers who spoofed the **5322.From** email address

SPF only checks for spoofed **5321.MailFrom** addresses

SPF + DMARC provides complete address verification

Network optimization

- Local DNS & internet egress for M365 endpoints
- Bypass proxies and inspection devices
- Enable direct connection for VPN users

Minimizing latency by reducing round-trip times

Endpoints (URLs & IP ranges)

https://aka.ms/m365ip

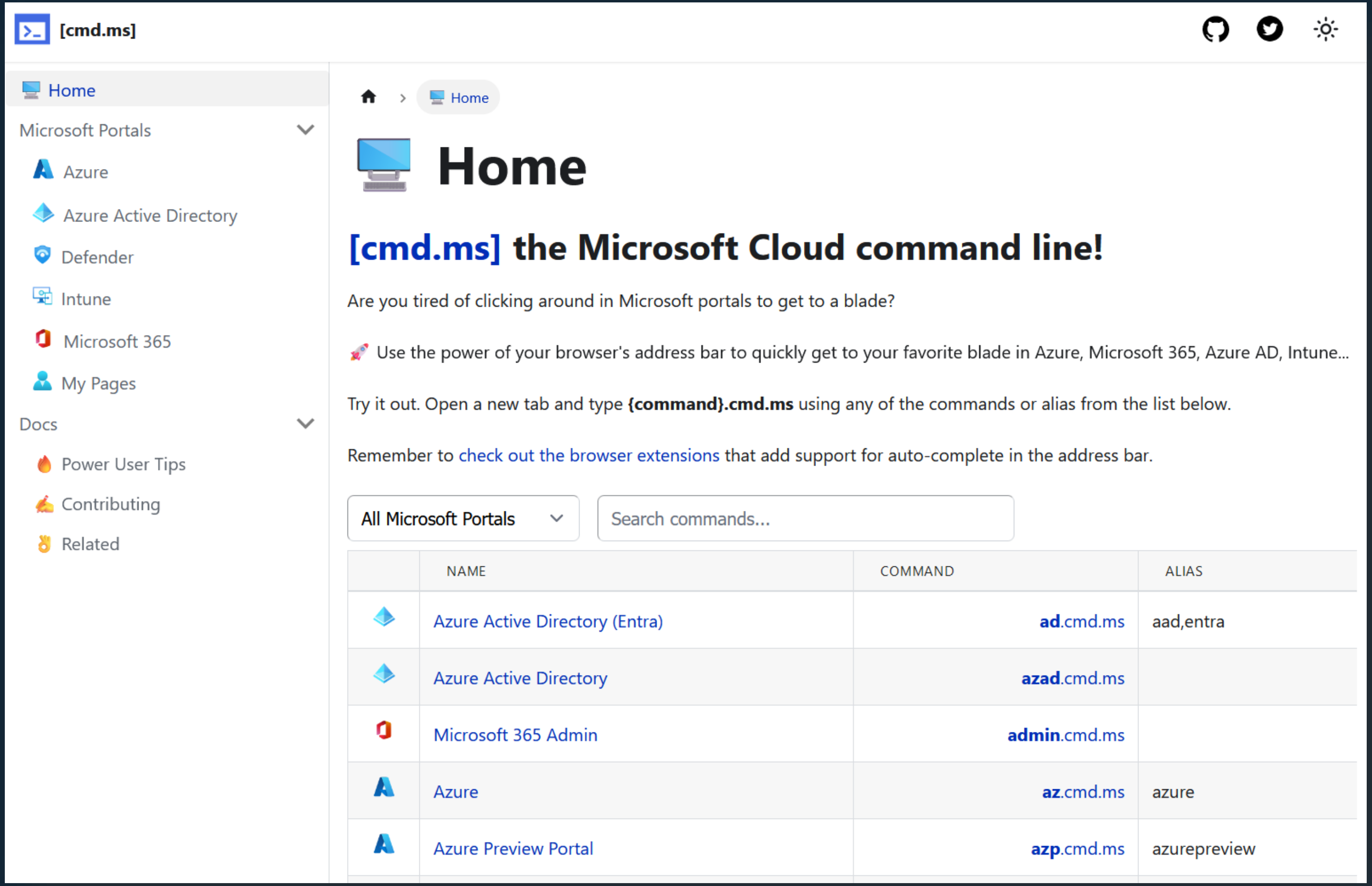
- Web service is available (json)
- Subscribe to the change feed

The new kid on the block

*.cloud.microsoft

Affects:
- Portals (https://admin.cloud.microsoft)
- Endpoints & web services (TBD)

cmd.ms to the rescue! 💎



Home

[cmd.ms] the Microsoft Cloud command line!

Are you tired of clicking around in Microsoft portals to get to a blade?

🚀 Use the power of your browser's address bar to quickly get to your favorite blade in Azure, Microsoft 365, Azure AD, Intune...

Try it out. Open a new tab and type **{command}.cmd.ms** using any of the commands or alias from the list below.

Remember to check out the browser extensions that add support for auto-complete in the address bar.

All Microsoft Portals | Search commands...

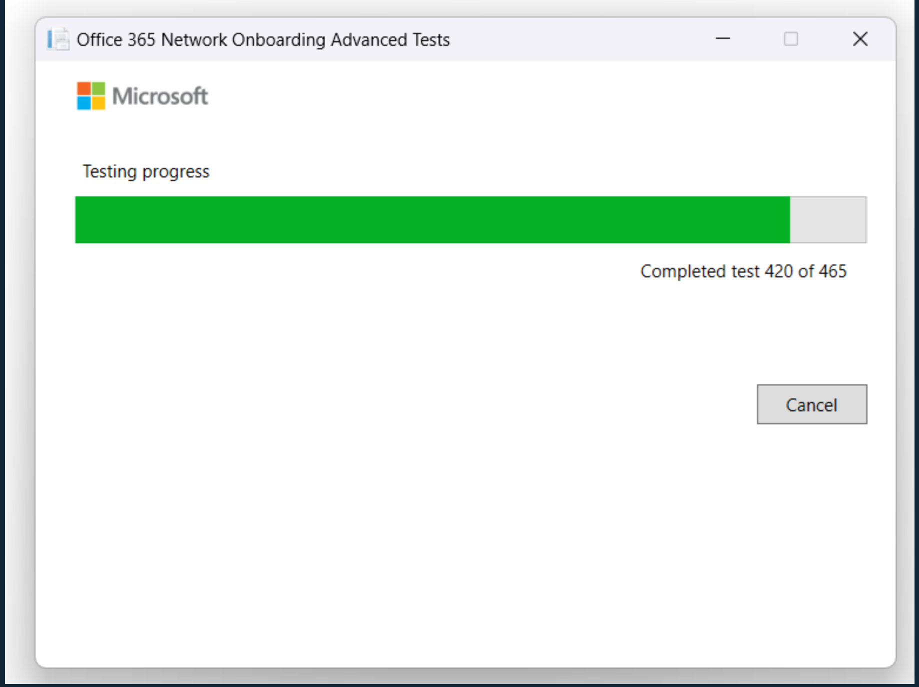
	NAME	COMMAND	ALIAS
	Azure Active Directory (Entra)	**ad**.cmd.ms	aad,entra
	Azure Active Directory	**azad**.cmd.ms	
	Microsoft 365 Admin	**admin**.cmd.ms	
	Azure	**az**.cmd.ms	azure
	Azure Preview Portal	**azp**.cmd.ms	azurepreview

@thomasvochten

Testing connectivity

Don’t assume everything will just work

https://connectivity.office.com

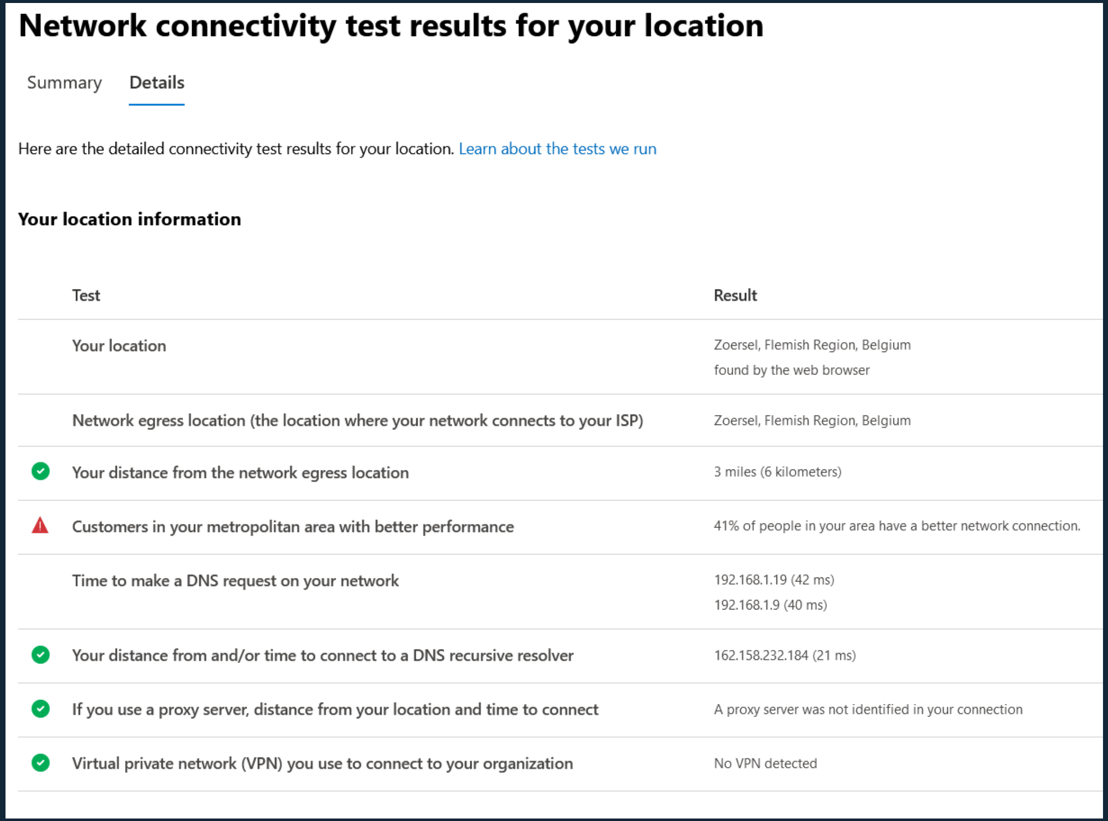


Office 365 Network Onboarding Advanced Tests

Testing progress

Completed test 420 of 465

Testing connectivity



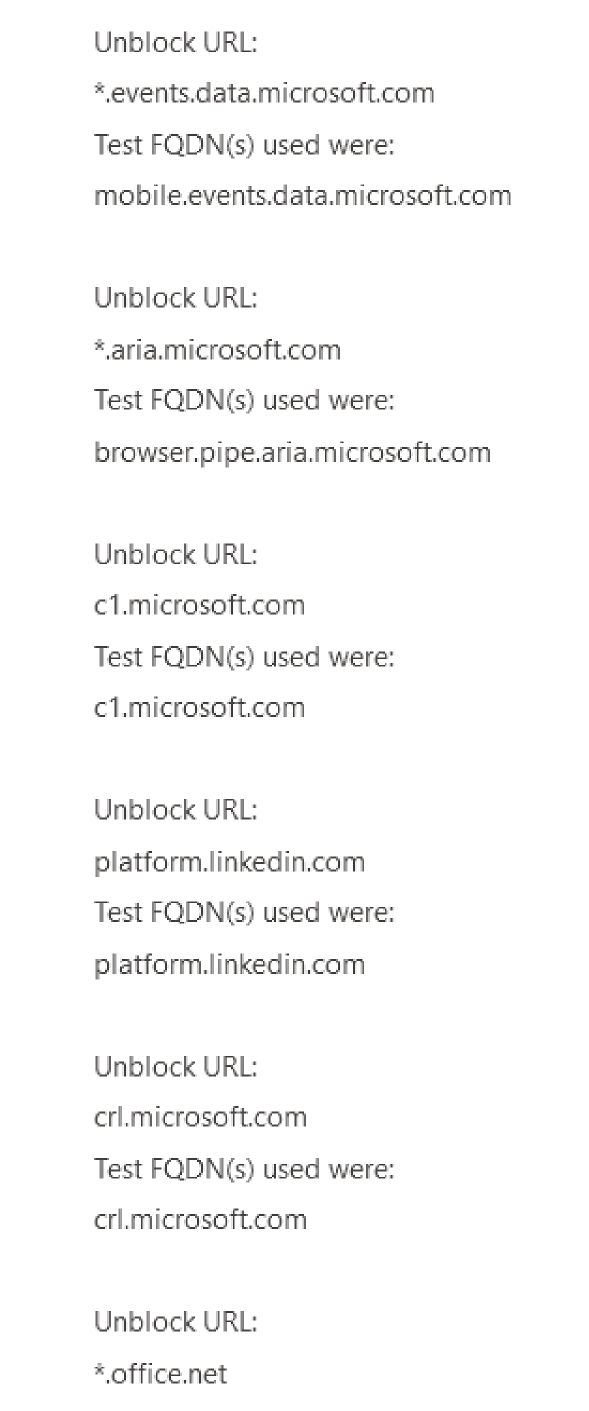
Network connectivity test results for your location

Summary Details

Here are the detailed connectivity test results for your location. Learn about the tests we run

Your location information

	Test	Result
	Your location	Zoersel, Flemish Region, Belgium found by the web browser
	Network egress location (the location where your network connects to your ISP)	Zoersel, Flemish Region, Belgium
✓	Your distance from the network egress location	3 miles (6 kilometers)
▲	Customers in your metropolitan area with better performance	41% of people in your area have a better network connection.
	Time to make a DNS request on your network	192.168.1.19 (42 ms) 192.168.1.9 (40 ms)
✓	Your distance from and/or time to connect to a DNS recursive resolver	162.158.232.184 (21 ms)
✓	If you use a proxy server, distance from your location and time to connect	A proxy server was not identified in your connection
✓	Virtual private network (VPN) you use to connect to your organization	No VPN detected



Unblock URL:

*.events.data.microsoft.com

Test FQDN(s) used were:

mobile.events.data.microsoft.com

Unblock URL:

*.aria.microsoft.com

Test FQDN(s) used were:

browser.pipe.aria.microsoft.com

Unblock URL:

c1.microsoft.com

Test FQDN(s) used were:

c1.microsoft.com

Unblock URL:

platform.linkedin.com

Test FQDN(s) used were:

platform.linkedin.com

Unblock URL:

crl.microsoft.com

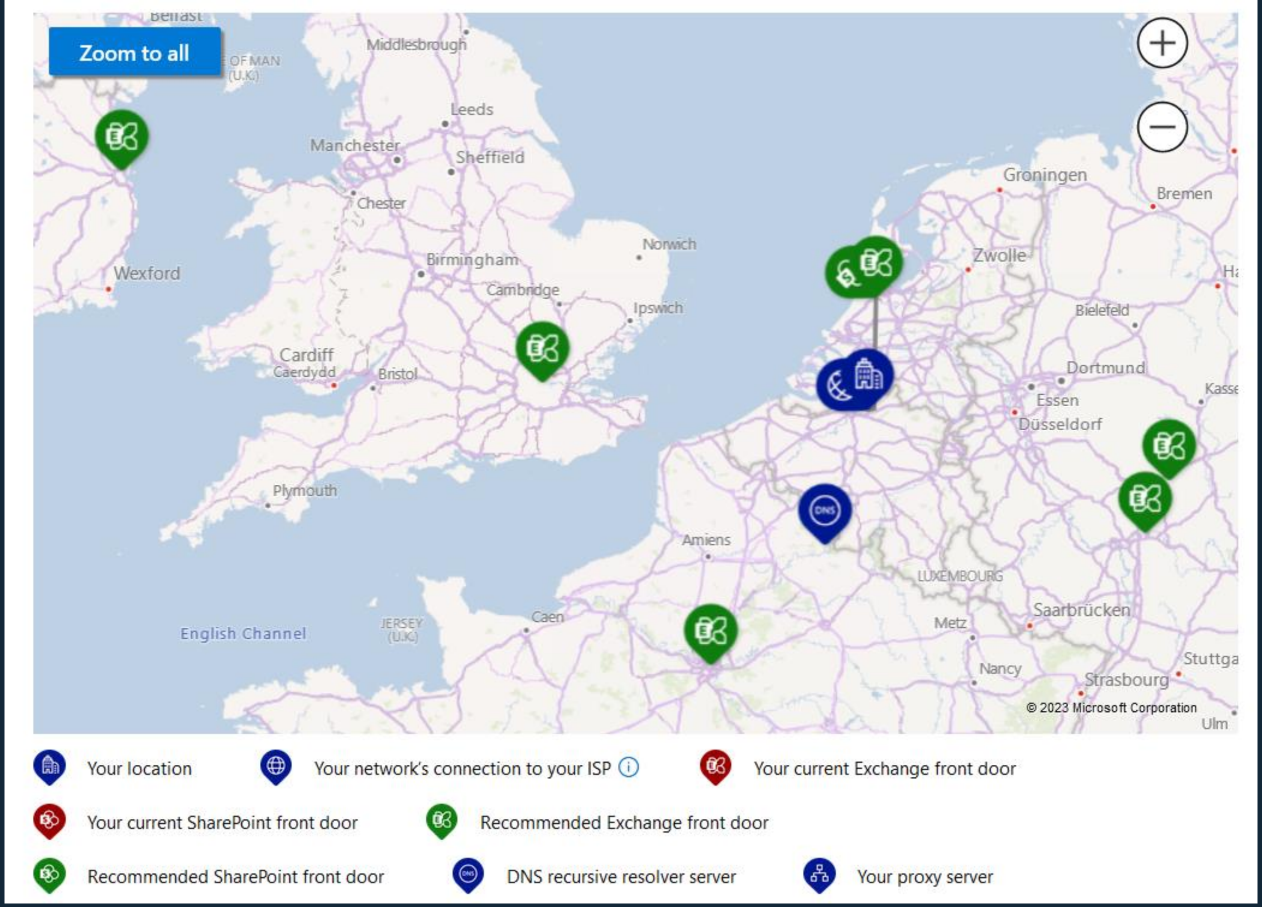
Test FQDN(s) used were:

crl.microsoft.com

Unblock URL:

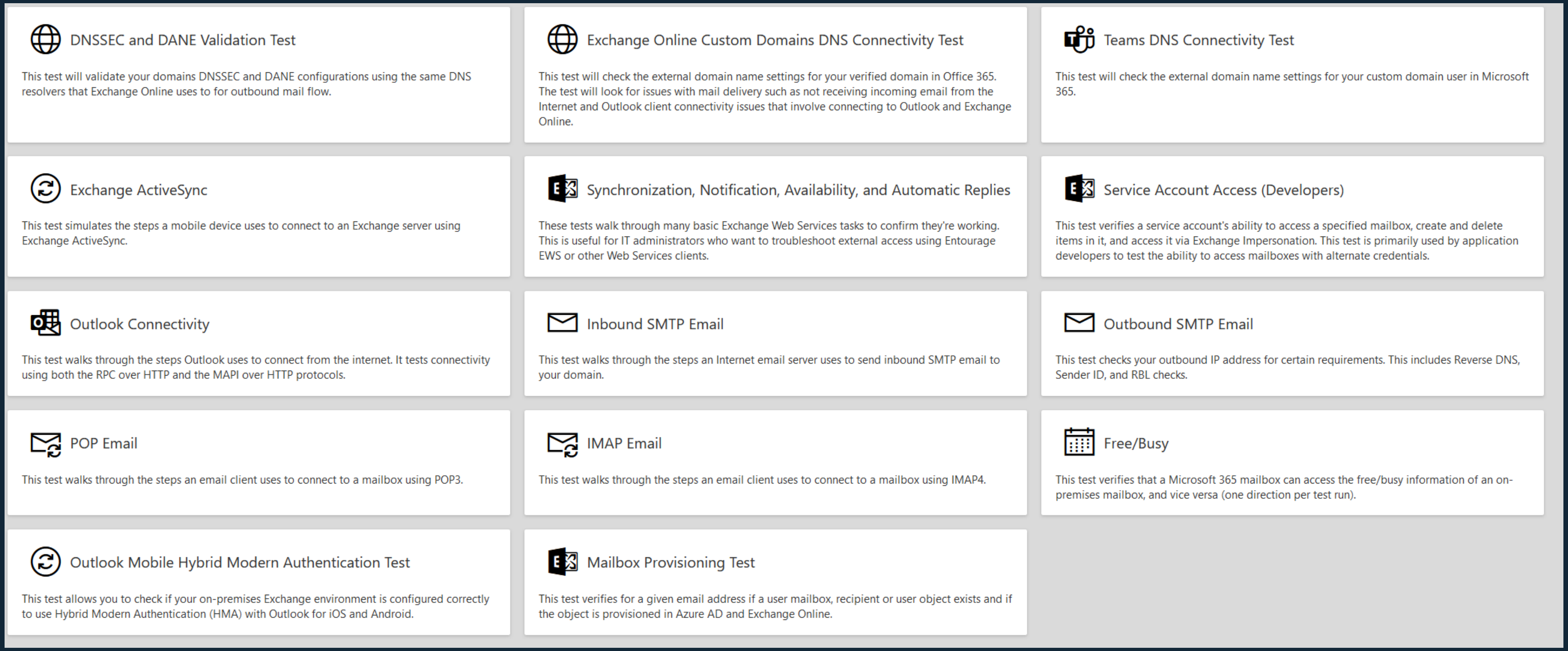
*.office.net

Testing connectivity



Remote Connectivity Analyzer

https://testconnectivity.microsoft.com



DNSSEC and DANE Validation Test

This test will validate your domains DNSSEC and DANE configurations using the same DNS resolvers that Exchange Online uses to for outbound mail flow.

Exchange Online Custom Domains DNS Connectivity Test

This test will check the external domain name settings for your verified domain in Office 365. The test will look for issues with mail delivery such as not receiving incoming email from the Internet and Outlook client connectivity issues that involve connecting to Outlook and Exchange Online.

Teams DNS Connectivity Test

This test will check the external domain name settings for your custom domain user in Microsoft 365.

Exchange ActiveSync

This test simulates the steps a mobile device uses to connect to an Exchange server using Exchange ActiveSync.

Synchronization, Notification, Availability, and Automatic Replies

These tests walk through many basic Exchange Web Services tasks to confirm they're working. This is useful for IT administrators who want to troubleshoot external access using Entourage EWS or other Web Services clients.

Service Account Access (Developers)

This test verifies a service account's ability to access a specified mailbox, create and delete items in it, and access it via Exchange Impersonation. This test is primarily used by application developers to test the ability to access mailboxes with alternate credentials.

Outlook Connectivity

This test walks through the steps Outlook uses to connect from the internet. It tests connectivity using both the RPC over HTTP and the MAPI over HTTP protocols.

Inbound SMTP Email

This test walks through the steps an Internet email server uses to send inbound SMTP email to your domain.

Outbound SMTP Email

This test checks your outbound IP address for certain requirements. This includes Reverse DNS, Sender ID, and RBL checks.

POP Email

This test walks through the steps an email client uses to connect to a mailbox using POP3.

IMAP Email

This test walks through the steps an email client uses to connect to a mailbox using IMAP4.

Free/Busy

This test verifies that a Microsoft 365 mailbox can access the free/busy information of an on-premises mailbox, and vice versa (one direction per test run).

Outlook Mobile Hybrid Modern Authentication Test

This test allows you to check if your on-premises Exchange environment is configured correctly to use Hybrid Modern Authentication (HMA) with Outlook for iOS and Android.

Mailbox Provisioning Test

This test verifies for a given email address if a user mailbox, recipient or user object exists and if the object is provisioned in Azure AD and Exchange Online.

@thomasvochten

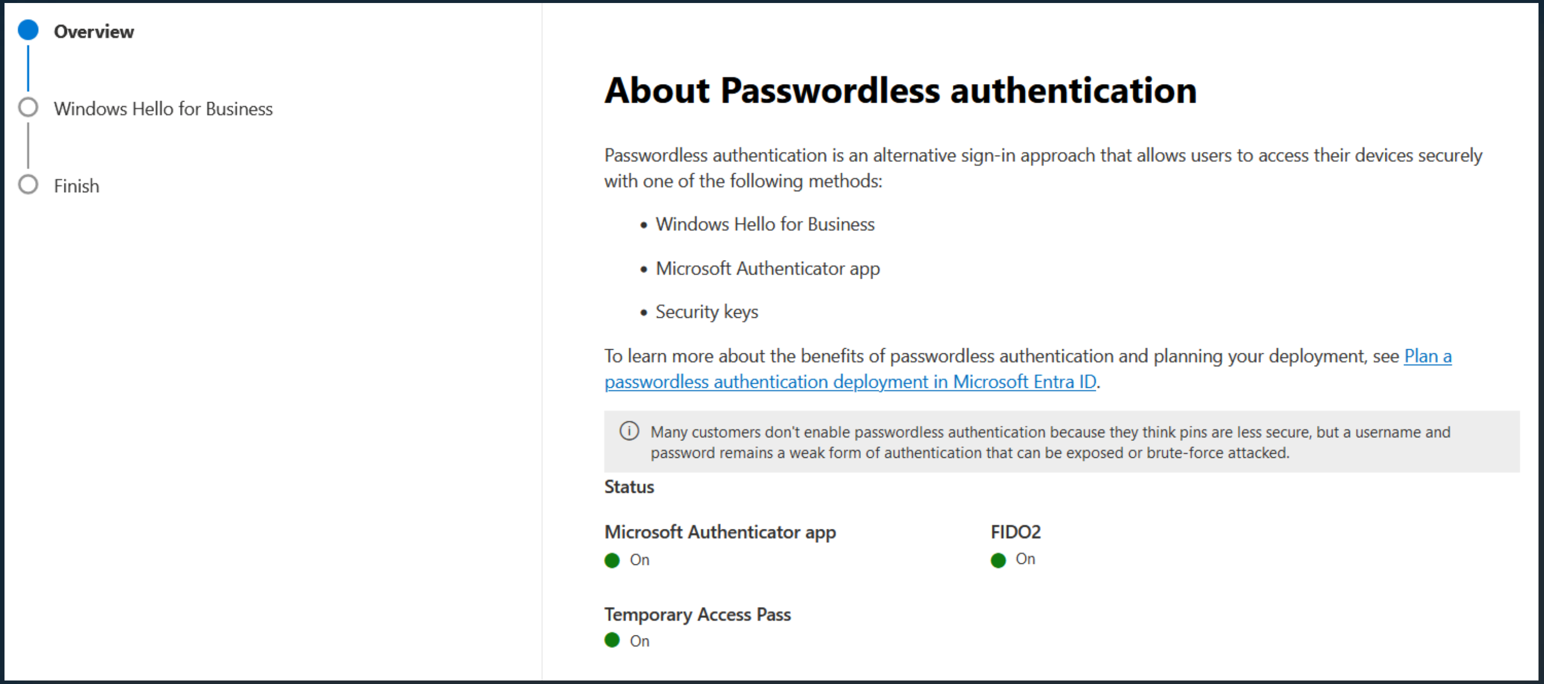
Organizational settings & advanced deployment guides

Organizational settings

- Central tenant and services settings
  - User consent to apps (set up an admin consent workflow)
  - Let users start trials on behalf of your organization
  - Let users auto-claim licenses
- Security & privacy settings
  - Control customer lockbox
  - Disable password expiration
  - Enable privileged access
  - Let users add guests to the organization
- Organization profile
  - Custom themes, tiles, helpdesk information, email notifications
  - Multitenant collaboration (preview)

Advanced deployment guides 💎

https://setup.microsoft.com



About Passwordless authentication

Passwordless authentication is an alternative sign-in approach that allows users to access their devices securely with one of the following methods:

- Windows Hello for Business
- Microsoft Authenticator app
- Security keys

To learn more about the benefits of passwordless authentication and planning your deployment, see Plan a passwordless authentication deployment in Microsoft Entra ID.

ⓘ Many customers don't enable passwordless authentication because they think pins are less secure, but a username and password remains a weak form of authentication that can be exposed or brute-force attacked.

Status

Microsoft Authenticator app
● On

FIDO2
● On

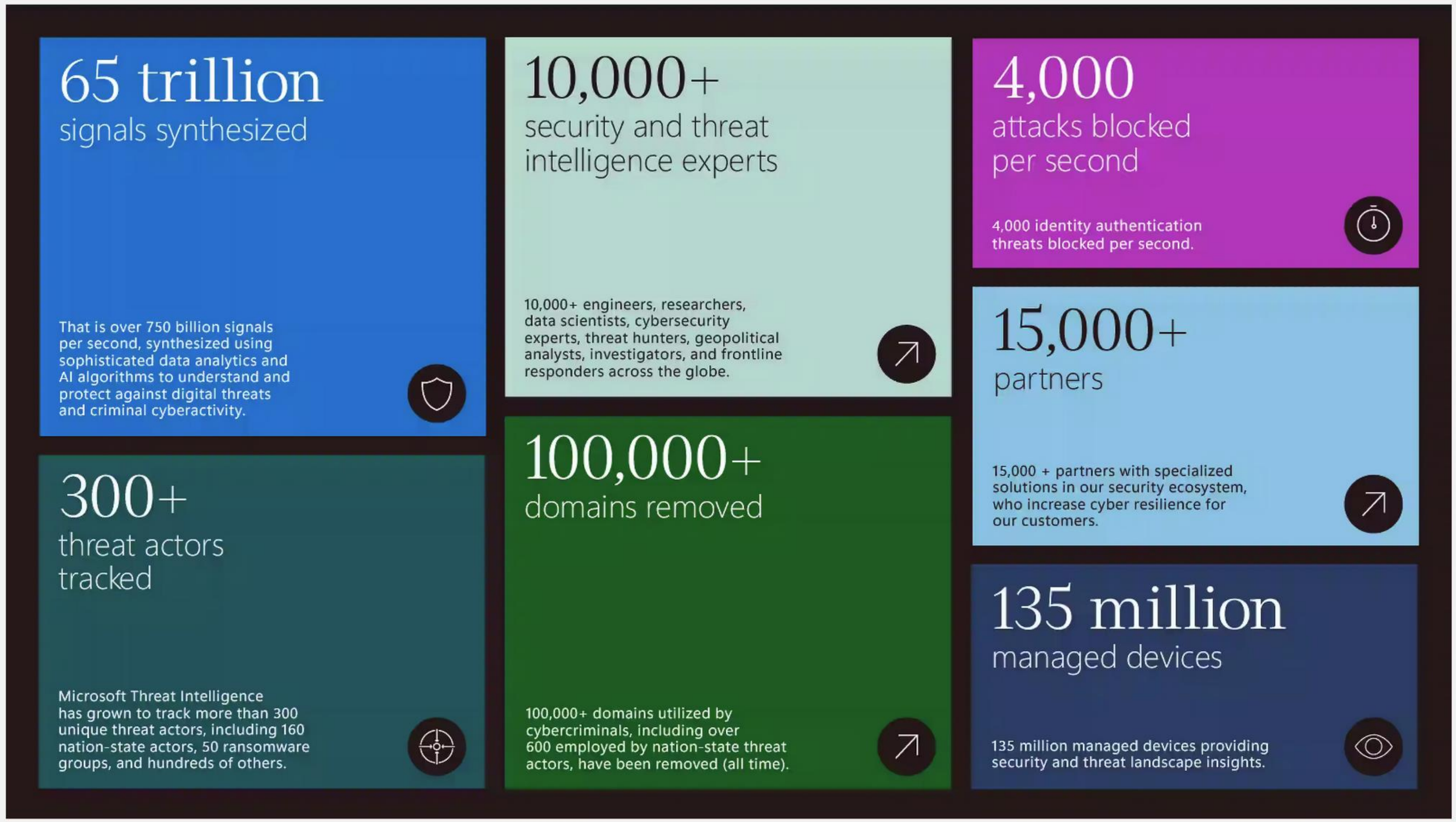
Temporary Access Pass
● On

@thomasvochten

Security security security!

Microsoft Digital Defense Report 2023

Required reading



65 trillion
signals synthesized

That is over 750 billion signals per second, synthesized using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.

10,000+
security and threat intelligence experts

10,000+ engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across the globe.

4,000
attacks blocked per second

4,000 identity authentication threats blocked per second.

15,000+
partners

15,000 + partners with specialized solutions in our security ecosystem, who increase cyber resilience for our customers.

300+
threat actors tracked

Microsoft Threat Intelligence has grown to track more than 300 unique threat actors, including 160 nation-state actors, 50 ransomware groups, and hundreds of others.

100,000+
domains removed

100,000+ domains utilized by cybercriminals, including over 600 employed by nation-state threat actors, have been removed (all time).

135 million
managed devices

135 million managed devices providing security and threat landscape insights.

@thomasvochten

How can we protect against 99% of attacks?

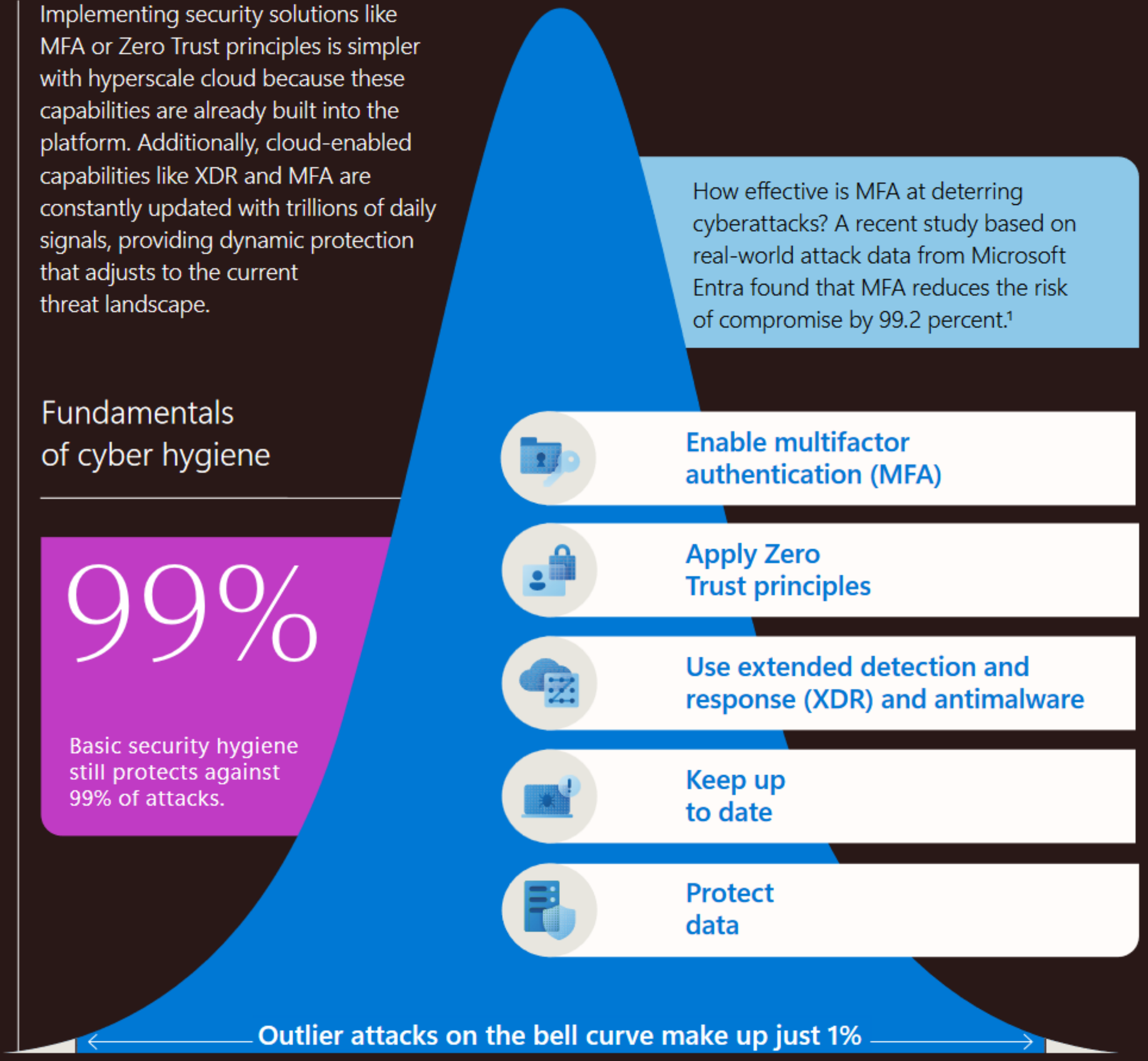
While we explore the many dimensions of the cyber threat landscape, there is one crucial point we must emphasize across them all: the vast majority of successful cyberattacks could be thwarted by implementing a few fundamental security hygiene practices.

By adhering to these minimum-security standards, it is possible to protect against over 99 percent of attacks:

1. **Enable multifactor authentication (MFA):** This protects against compromised user passwords and helps to provide extra resilience for identities.
2. **Apply Zero Trust principles:** The cornerstone of any resilience plan is to limit the impact of an attack on an organization. These principles are:
   - Explicitly verify. Ensure users and devices are in a good state before allowing access to resources.
   - Use least privilege access. Allow only the privilege that is needed for access to a resource and no more.
   - Assume breach. Assume system defenses have been breached and systems may be compromised. This means constantly monitoring the environment for possible attack.
3. **Use extended detection and response (XDR) and antimalware:** Implement software to detect and automatically block attacks and provide insights to the security operations software. Monitoring insights from threat detection systems is essential to being able to respond to threats in a timely fashion.
4. **Keep up to date:** Unpatched and out-of-date systems are a key reason many organizations fall victim to an attack. Ensure all systems are kept up to date including firmware, the operating system, and applications.
5. **Protect data:** Knowing your important data, where it is located, and whether the right defenses are implemented is crucial to implementing the appropriate protection.

Hyperscale cloud makes it easier to implement fundamental security practices by either enabling them by default or abstracting the need for customers to implement them. With software-as-a-service (SaaS) and platform-as-a-service (PaaS) solutions, the cloud provider takes responsibility for keeping up with patch management.

Implementing security solutions like MFA or Zero Trust principles is simpler with hyperscale cloud because these capabilities are already built into the platform. Additionally, cloud-enabled capabilities like XDR and MFA are constantly updated with trillions of daily signals, providing dynamic protection that adjusts to the current threat landscape.



Fundamentals of cyber hygiene

99%

Basic security hygiene still protects against 99% of attacks.

How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.[1]

- Enable multifactor authentication (MFA)
- Apply Zero Trust principles
- Use extended detection and response (XDR) and antimalware
- Keep up to date
- Protect data

Outlier attacks on the bell curve make up just 1%

The State of Cybercrime

Key developments

Cybercriminals are leveraging the cybercrime-as-a-service ecosystem to launch phishing, identity, and distributed denial of service (DDoS) attacks at scale. Simultaneously, they are increasingly bypassing multifactor authentication and other security measures to conduct targeted attacks.

Ransomware operators are shifting heavily toward hands on keyboard attacks, using living-off-the-land techniques and remote encryption to conceal their tracks, and exfiltrating data to add pressure to their ransom demands. And cybercriminals are improving their ability to impersonate or compromise legitimate third parties, making it even harder for users to identify fraud until it's too late.

80-90%

of all successful ransomware compromises originate through unmanaged devices.

Find out more on page 18

A return on mitigation (ROM) framework is helpful for prioritization and may highlight actions requiring low effort or resources but that have a high impact.

Find out more on page 41

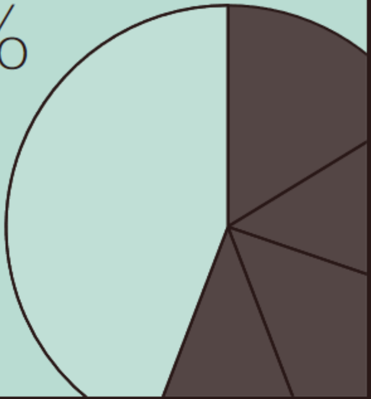
70%

of organizations encountering human-operated ransomware had fewer than 500 employees.

Find out more on page 18

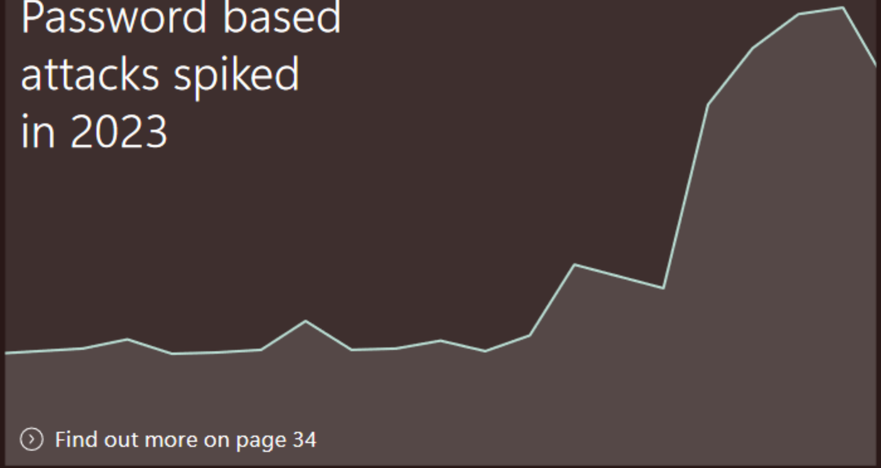
Human-operated ransomware attacks are up more than

200%



Find out more on page 17

Password based attacks spiked in 2023



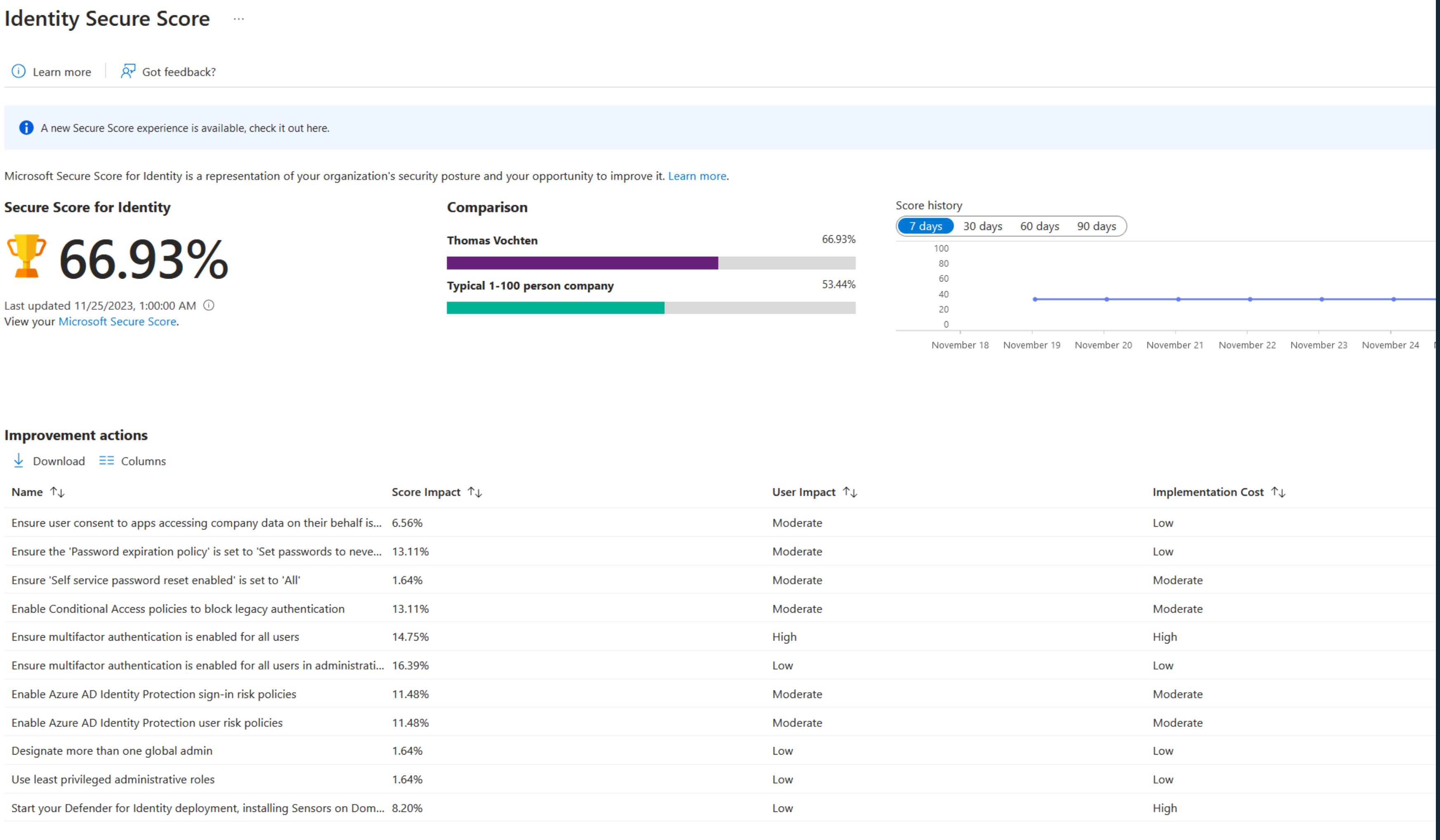
Find out more on page 34

Last year marked a significant shift in cybercriminal tactics

with threat actors exploiting cloud computing resources such as virtual machines to launch DDoS attacks. When hundreds of millions of requests per second originating from tens of thousands of devices constitute an attack, the cloud is our best defense, due to the scale needed to mitigate the largest attacks.

Find out more on page 39

Where do I start?



Identity Secure Score ···

A new Secure Score experience is available, check it out here.

Microsoft Secure Score for Identity is a representation of your organization's security posture and your opportunity to improve it. Learn more.

Secure Score for Identity

66.93%

Last updated 11/25/2023, 1:00:00 AM

View your Microsoft Secure Score.

Comparison

Thomas Vochten	66.93%
Typical 1-100 person company	53.44%

Score history

Improvement actions

Name ↑↓	Score Impact ↑↓	User Impact ↑↓	Implementation Cost ↑↓
Ensure user consent to apps accessing company data on their behalf is...	6.56%	Moderate	Low
Ensure the 'Password expiration policy' is set to 'Set passwords to neve...	13.11%	Moderate	Low
Ensure 'Self service password reset enabled' is set to 'All'	1.64%	Moderate	Moderate
Enable Conditional Access policies to block legacy authentication	13.11%	Moderate	Moderate
Ensure multifactor authentication is enabled for all users	14.75%	High	High
Ensure multifactor authentication is enabled for all users in administrati...	16.39%	Low	Low
Enable Azure AD Identity Protection sign-in risk policies	11.48%	Moderate	Moderate
Enable Azure AD Identity Protection user risk policies	11.48%	Moderate	Moderate
Designate more than one global admin	1.64%	Low	Low
Use least privileged administrative roles	1.64%	Low	Low
Start your Defender for Identity deployment, installing Sensors on Dom...	8.20%	Low	High

@thomasvochten

~~Five~~ Six steps to securing your identities

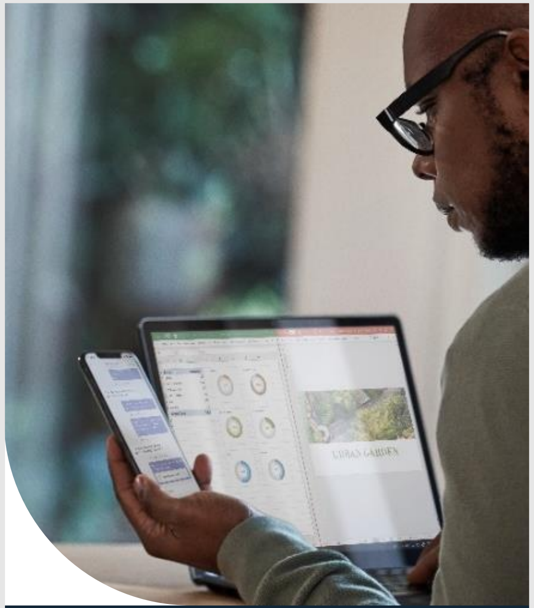
0) Protect ~~privileged~~ accounts with MFA
1) Strengthen your credentials
2) Reduce your attack surface area
3) Automate threat response
4) Utilize cloud intelligence
5) Enable end-user self-service

Step 0 - Protect accounts with MFA

- Whatever you do, do this first
- MFA will be mandatory soon
- Use conditional access policies or
- Security Defaults

Five steps to securing your identities

Authentication methods



We support a **broad range of multifactor authentication options**

Passwordless, phishing-resistant technology

Microsoft Authenticator*

Windows Hello (supports passkey)

FIDO2 Security key

Biometrics

Certificate based Auth

Push Notification

Soft Tokens OTP

Hard Tokens OTP

SMS, Voice

Multifactor authentication prevents 99.9% of identity-based attacks

*Must use with Conditional Access policy requiring managed devices to get protection from external phishing threats.

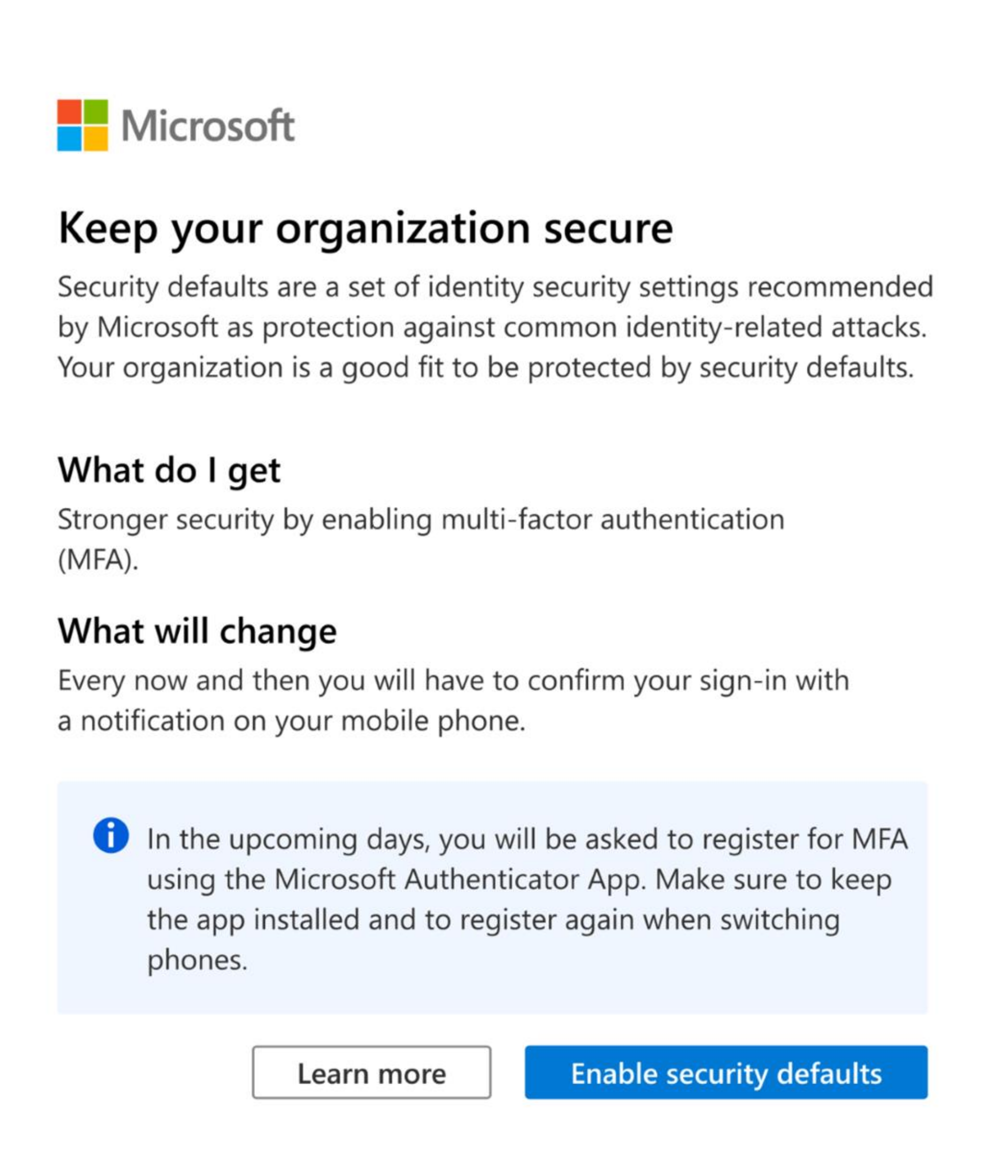
@thomasvochten

Five steps to securing your identities

Security Defaults?

Preconfigured security settings

- MFA *registration* for all users
- MFA enforced for admin users
- Protect privileged activities
- Blocks legacy AuthN



Microsoft

Keep your organization secure

Security defaults are a set of identity security settings recommended by Microsoft as protection against common identity-related attacks. Your organization is a good fit to be protected by security defaults.

What do I get

Stronger security by enabling multi-factor authentication (MFA).

What will change

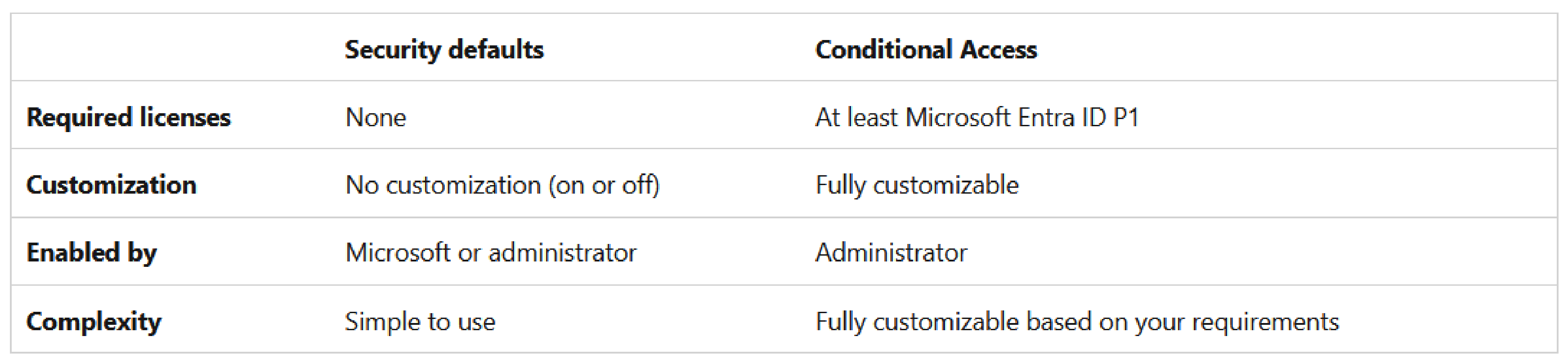
Every now and then you will have to confirm your sign-in with a notification on your mobile phone.

In the upcoming days, you will be asked to register for MFA using the Microsoft Authenticator App. Make sure to keep the app installed and to register again when switching phones.

@thomasvochten

From Security Defaults to Conditional Access

Security Defaults are just the bare minimum

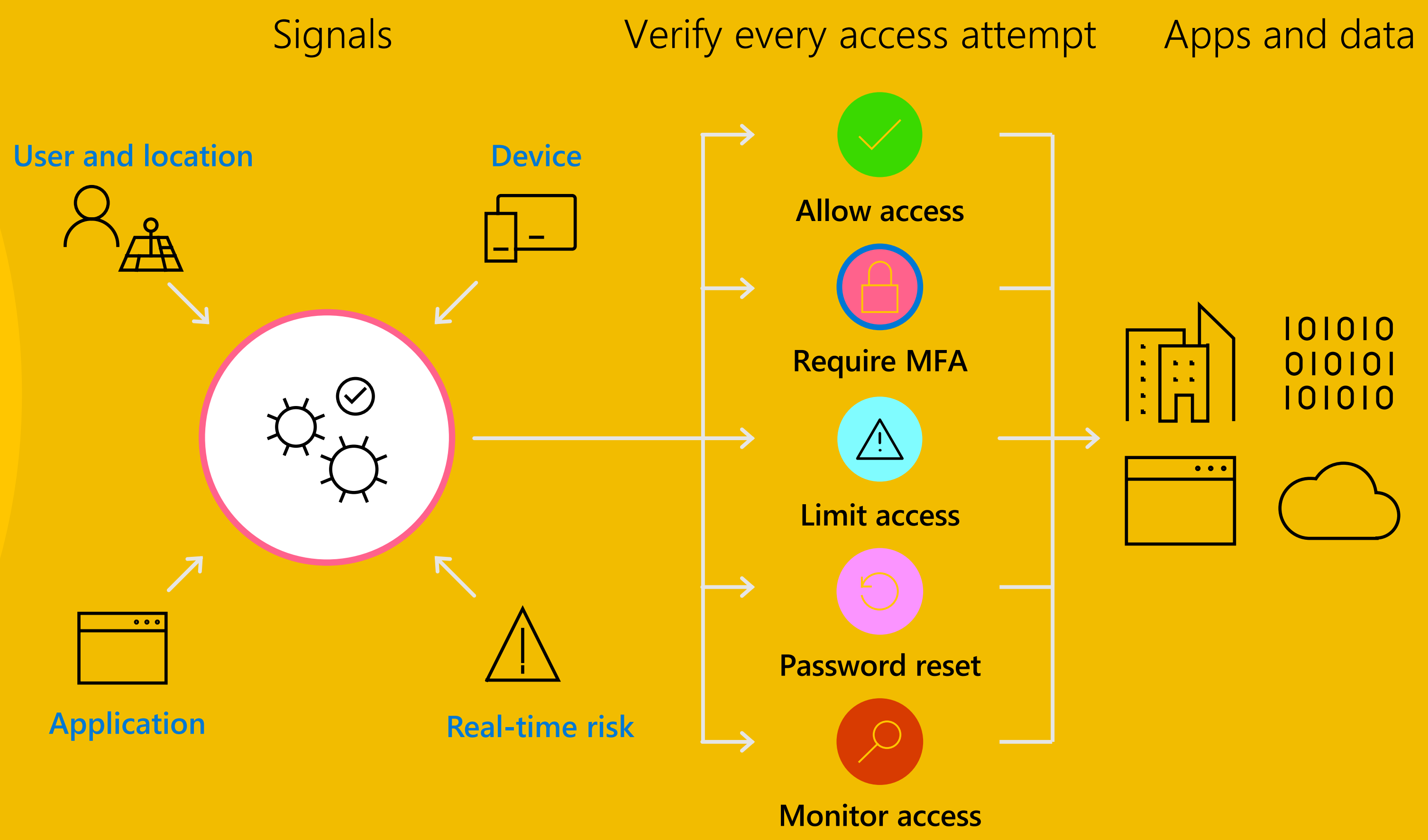


	Security defaults	Conditional Access
Required licenses	None	At least Microsoft Entra ID P1
Customization	No customization (on or off)	Fully customizable
Enabled by	Microsoft or administrator	Administrator
Complexity	Simple to use	Fully customizable based on your requirements

Five steps to securing your identities

Conditional Access

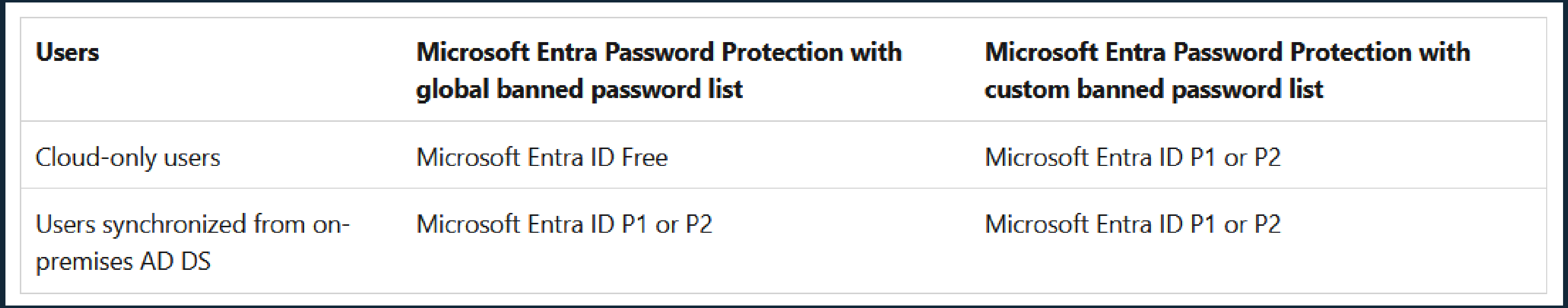
- Enforce access controls with adaptive policies
- Protect data inside applications
- Restrict access for vulnerable and compromised devices



Five steps to securing your identities

Step 1 - Strengthen your credentials

- Enforce MFA for *all* users
- Rethink password complexity rules
  Microsoft Entra Password Protection provides (custom) banned password list



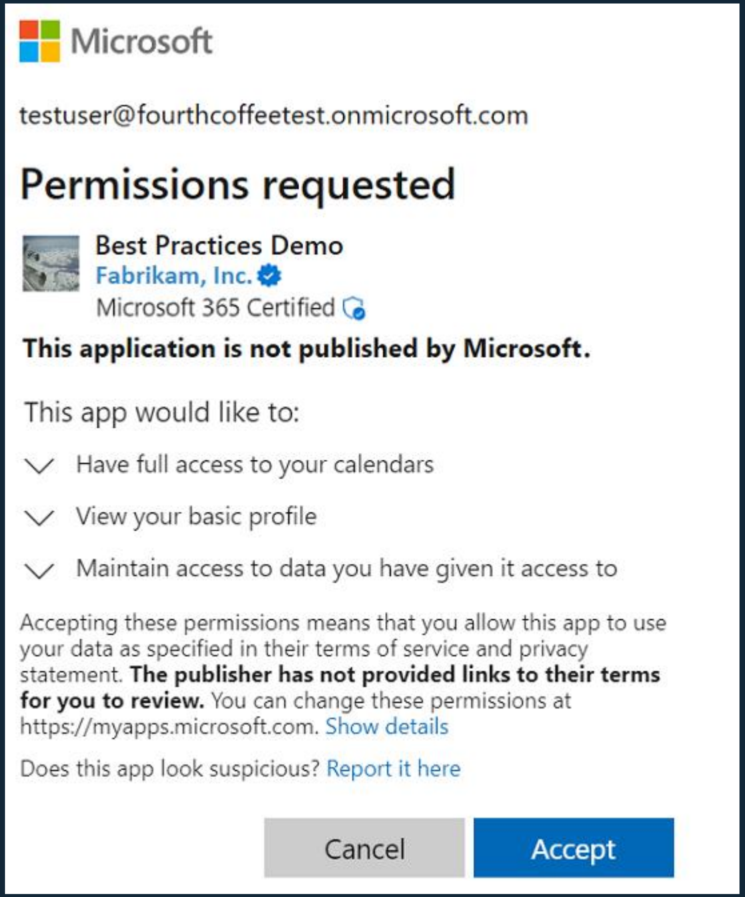
Users	Microsoft Entra Password Protection with global banned password list	Microsoft Entra Password Protection with custom banned password list
Cloud-only users	Microsoft Entra ID Free	Microsoft Entra ID P1 or P2
Users synchronized from on-premises AD DS	Microsoft Entra ID P1 or P2	Microsoft Entra ID P1 or P2

- Rethink password expiration rules

Step 2 - Reduce your attack surface area

- Only allow strong cloud authentication
- Block legacy authentication (look at your sign-in logs)
- Block invalid authentication entry points (disable inactive accounts)
- Evaluate your admin roles, make sure they are cloud-only
- Implement Privilege Identity Management
- Restrict user consent operations

Restricting user consent operations



Microsoft

testuser@fourthcoffeetest.onmicrosoft.com

Permissions requested

Best Practices Demo
Fabrikam, Inc.
Microsoft 365 Certified

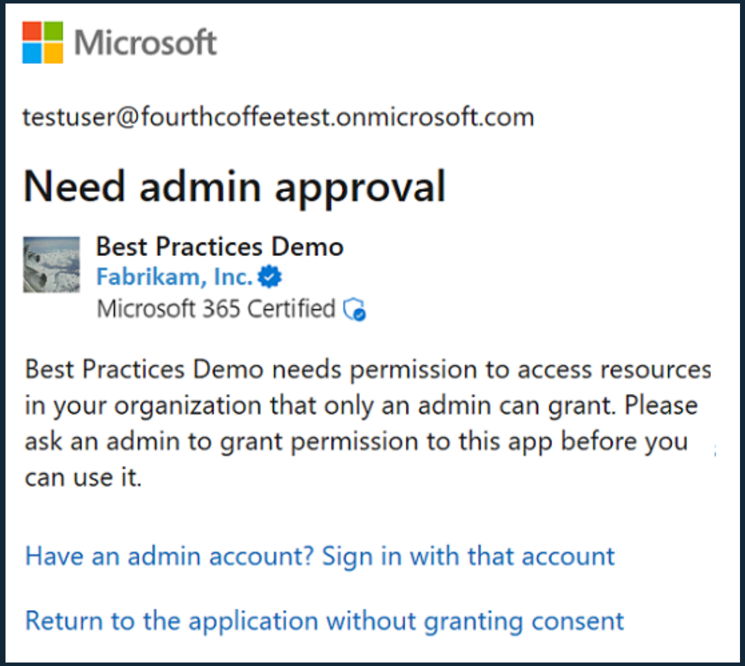
This application is not published by Microsoft.

This app would like to:

- Have full access to your calendars
- View your basic profile
- Maintain access to data you have given it access to

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here



Microsoft

testuser@fourthcoffeetest.onmicrosoft.com

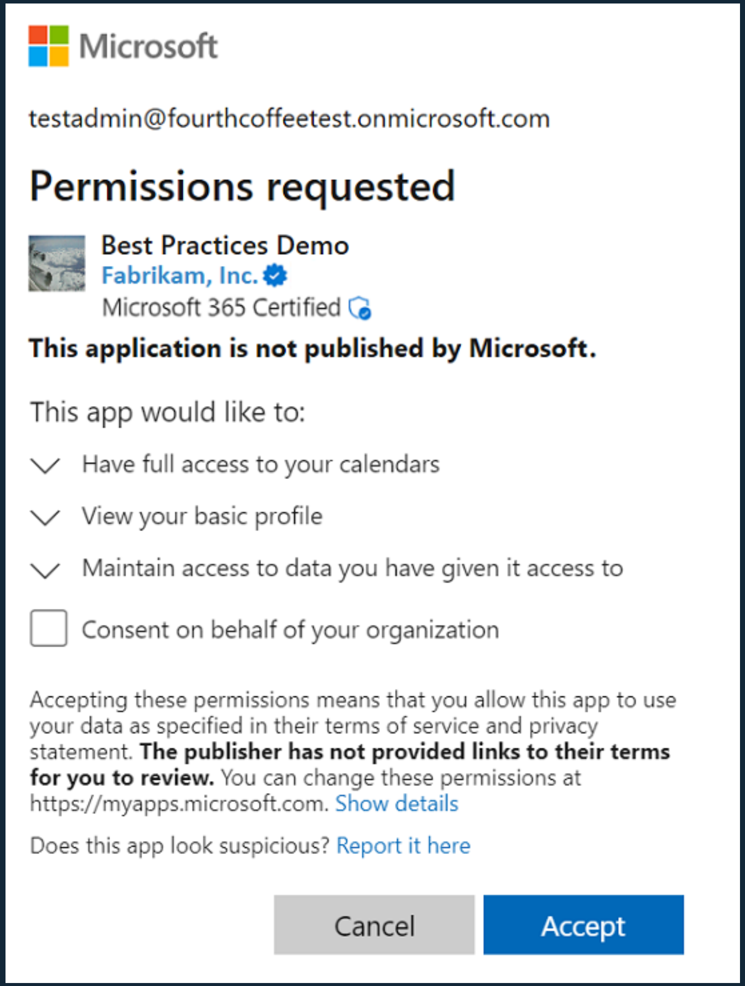
Need admin approval

Best Practices Demo
Fabrikam, Inc.
Microsoft 365 Certified

Best Practices Demo needs permission to access resources in your organization that only an admin can grant. Please ask an admin to grant permission to this app before you can use it.

Have an admin account? Sign in with that account

Return to the application without granting consent



Microsoft

testadmin@fourthcoffeetest.onmicrosoft.com

Permissions requested

Best Practices Demo
Fabrikam, Inc.
Microsoft 365 Certified

This application is not published by Microsoft.

This app would like to:

- Have full access to your calendars
- View your basic profile
- Maintain access to data you have given it access to

□ Consent on behalf of your organization

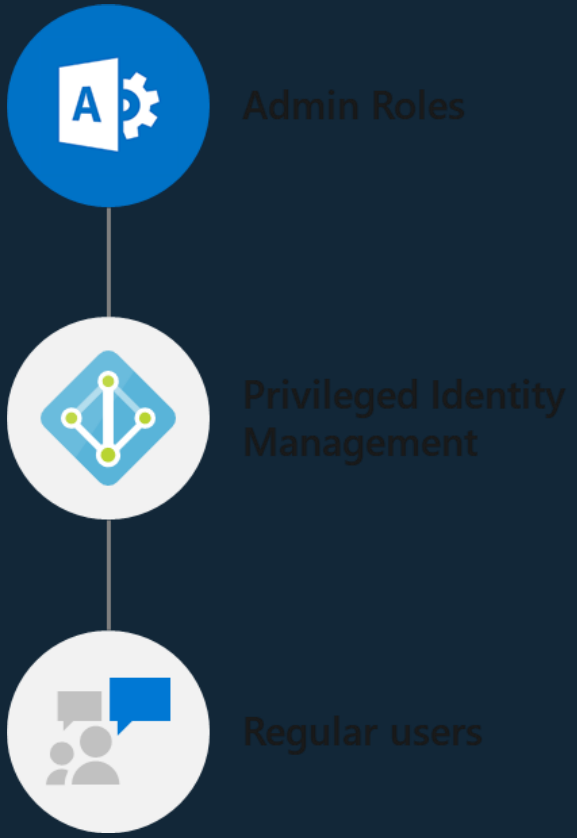
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Five steps to securing your identities

Privileged Identity Management

- Just-in-time administrative access
- History of administrator role activation and changes made
- Get alerts when something changes
- Approvals & justification
- Time-bound access
- Review membership



Admin Roles

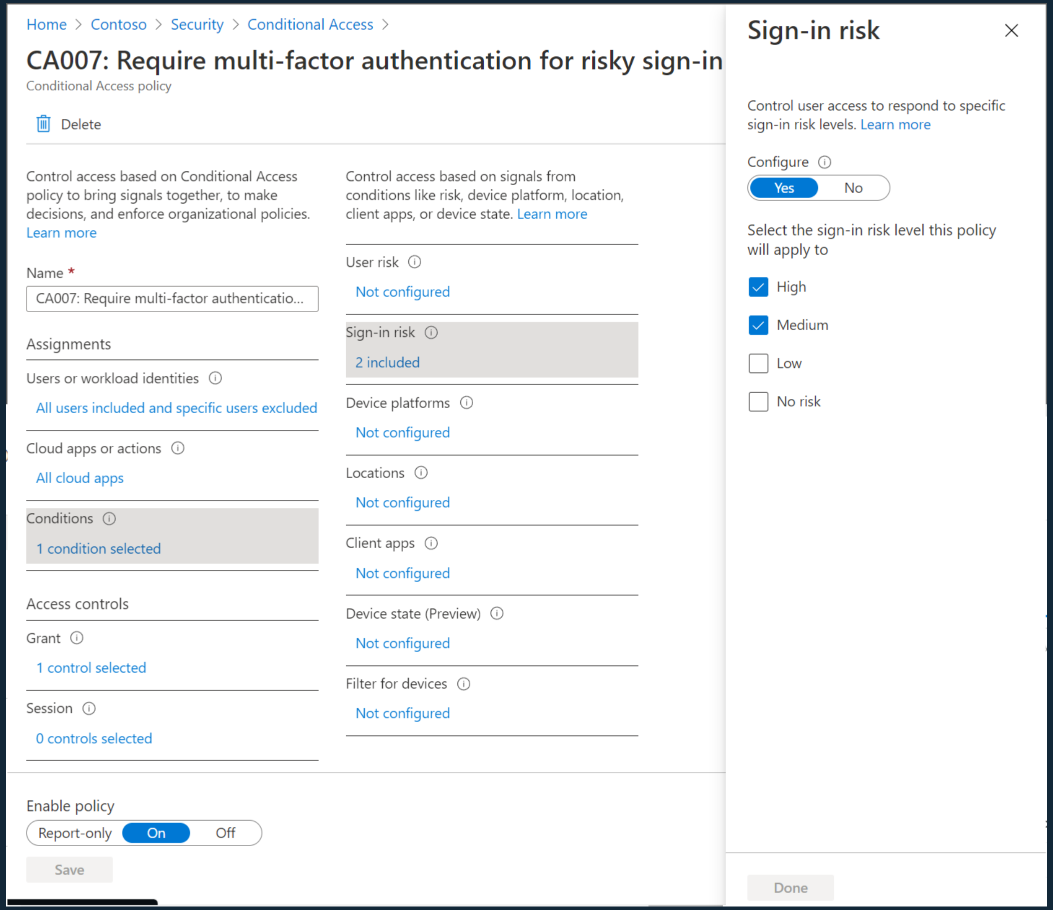
Privileged Identity Management

Regular users

Five steps to securing your identities

Step 3 - Automate threat response

- Implement **sign-in risk** policies (high/medium/low risk) with conditional access
- Implement **user risk** security policy
- Integrate Microsoft 365 Defender with Microsoft Entra ID Protection



Home > Contoso > Security > Conditional Access >

CA007: Require multi-factor authentication for risky sign-in

Conditional Access policy

Delete

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

CA007: Require multi-factor authenticatio...

Assignments

Users or workload identities: All users included and specific users excluded

Cloud apps or actions: All cloud apps

Conditions: 1 condition selected

Access controls

Grant: 1 control selected

Session: 0 controls selected

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk: Not configured

Sign-in risk: 2 included

Device platforms: Not configured

Locations: Not configured

Client apps: Not configured

Device state (Preview): Not configured

Filter for devices: Not configured

Enable policy: Report-only [✓ On] Off

Save

Sign-in risk

Control user access to respond to specific sign-in risk levels. Learn more

Configure: [✓ Yes] No

Select the sign-in risk level this policy will apply to

☑ High

☑ Medium

☐ Low

☐ No risk

Done

@thomasvochten

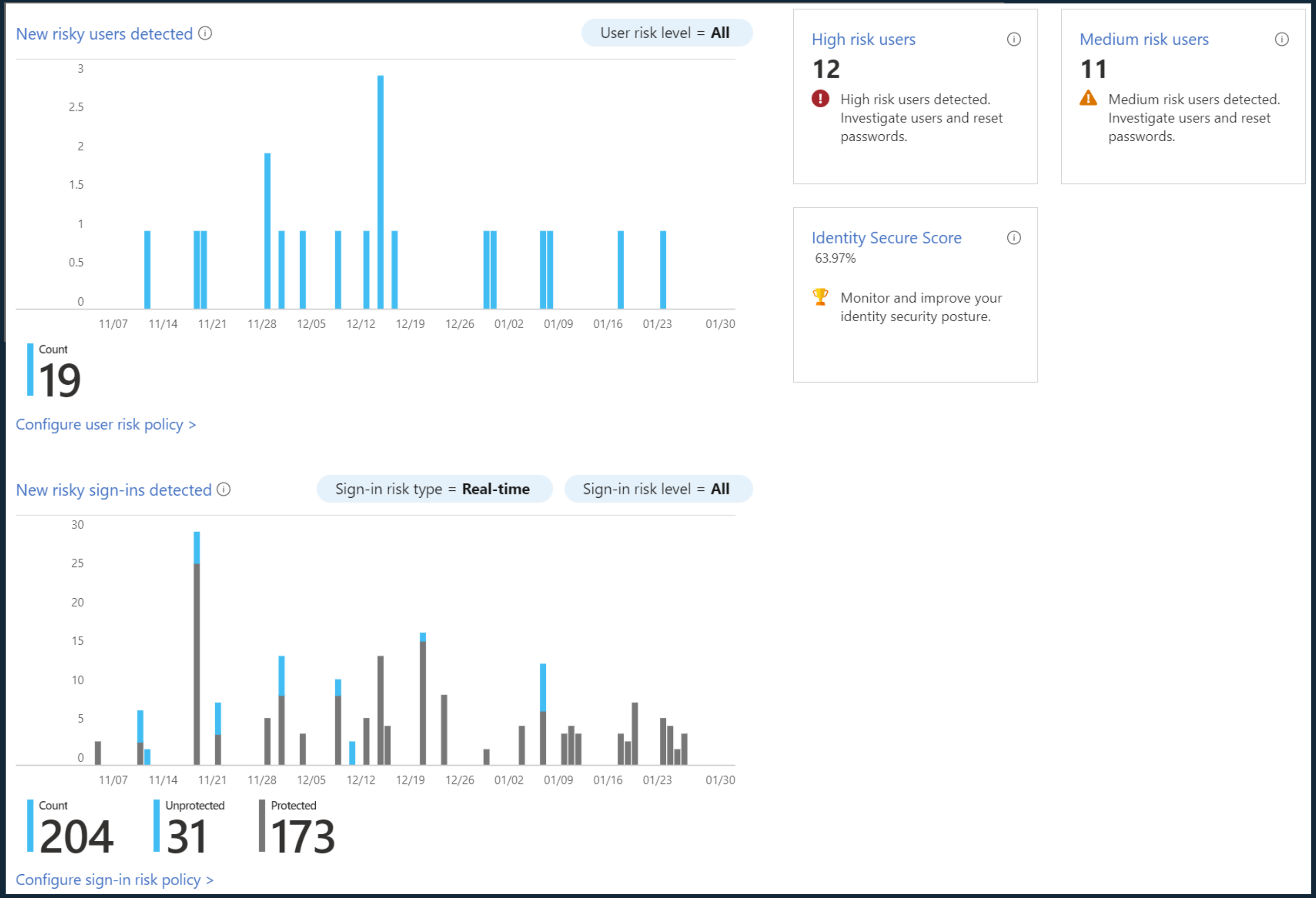
Five steps to securing your identities

Step 4 - Utilize cloud intelligence

Setup monitoring and alerting for:

- Risky sign-ins
- Risky users

Audit apps and consented permissions



New risky users detected ⓘ

User risk level = **All**

Count
19

Configure user risk policy >

New risky sign-ins detected ⓘ

Sign-in risk type = **Real-time**

Sign-in risk level = **All**

Count
204

Unprotected
31

Protected
173

Configure sign-in risk policy >

High risk users ⓘ

12

High risk users detected. Investigate users and reset passwords.

Medium risk users ⓘ

11

Medium risk users detected. Investigate users and reset passwords.

Identity Secure Score ⓘ

63.97%

Monitor and improve your identity security posture.

@thomasvochten

Step 5 - Enable end-user self-service

- Implement self-service password reset (SSPR)
- Implement self-service group and application access (look at entitlement management)
- Implement access reviews
- Implement automatic user provisioning

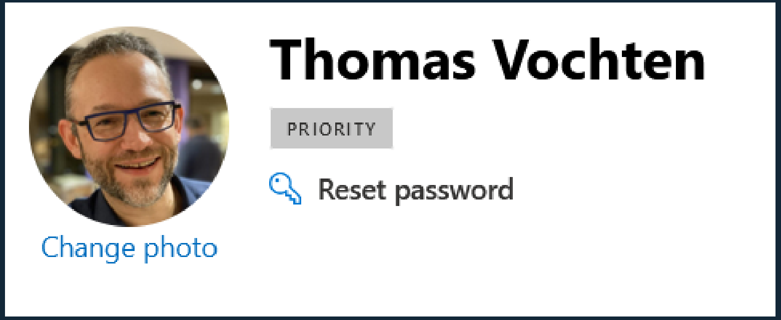
Break-glass accounts 💎

- Highly privileged (global administrator)
- Cloud-only account
- Not assigned to specific people (or devices, or phones)
- Should be locked away physically
- Monitor and audit its use
- Validate and test regularly

🦺 EXCLUDE FROM CONDITIONAL ACCESS POLICIES

Priority accounts protection 💎

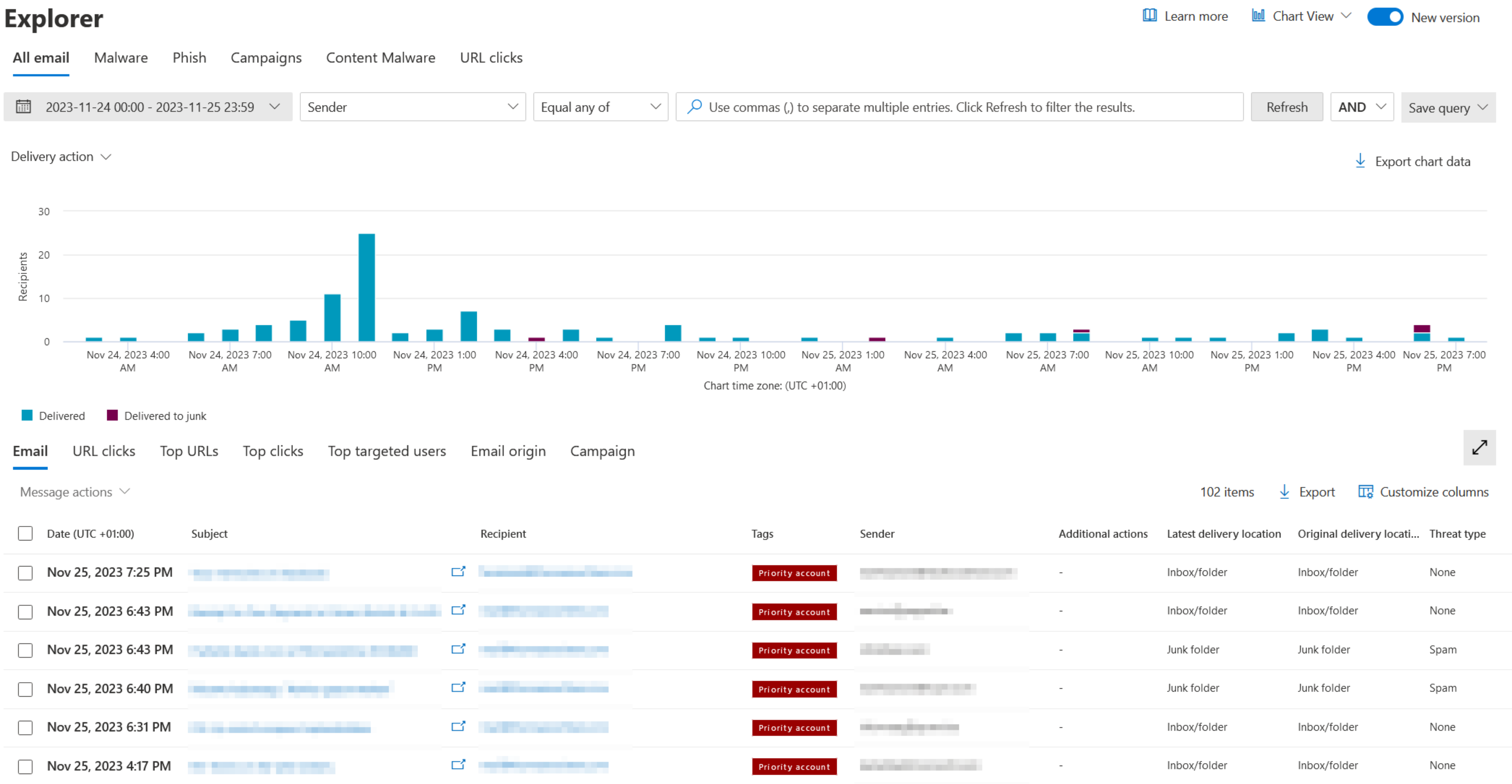
- Reduce impact of VIP accounts being breached
- Additional detection heuristics and visibility in reporting



Thomas Vochten

PRIORITY

@thomasvochten



Explorer

Learn more | Chart View | New version

All email | Malware | Phish | Campaigns | Content Malware | URL clicks

2023-11-24 00:00 - 2023-11-25 23:59 | Sender | Equal any of | Use commas (,) to separate multiple entries. Click Refresh to filter the results. | Refresh | AND | Save query

Delivery action

Export chart data

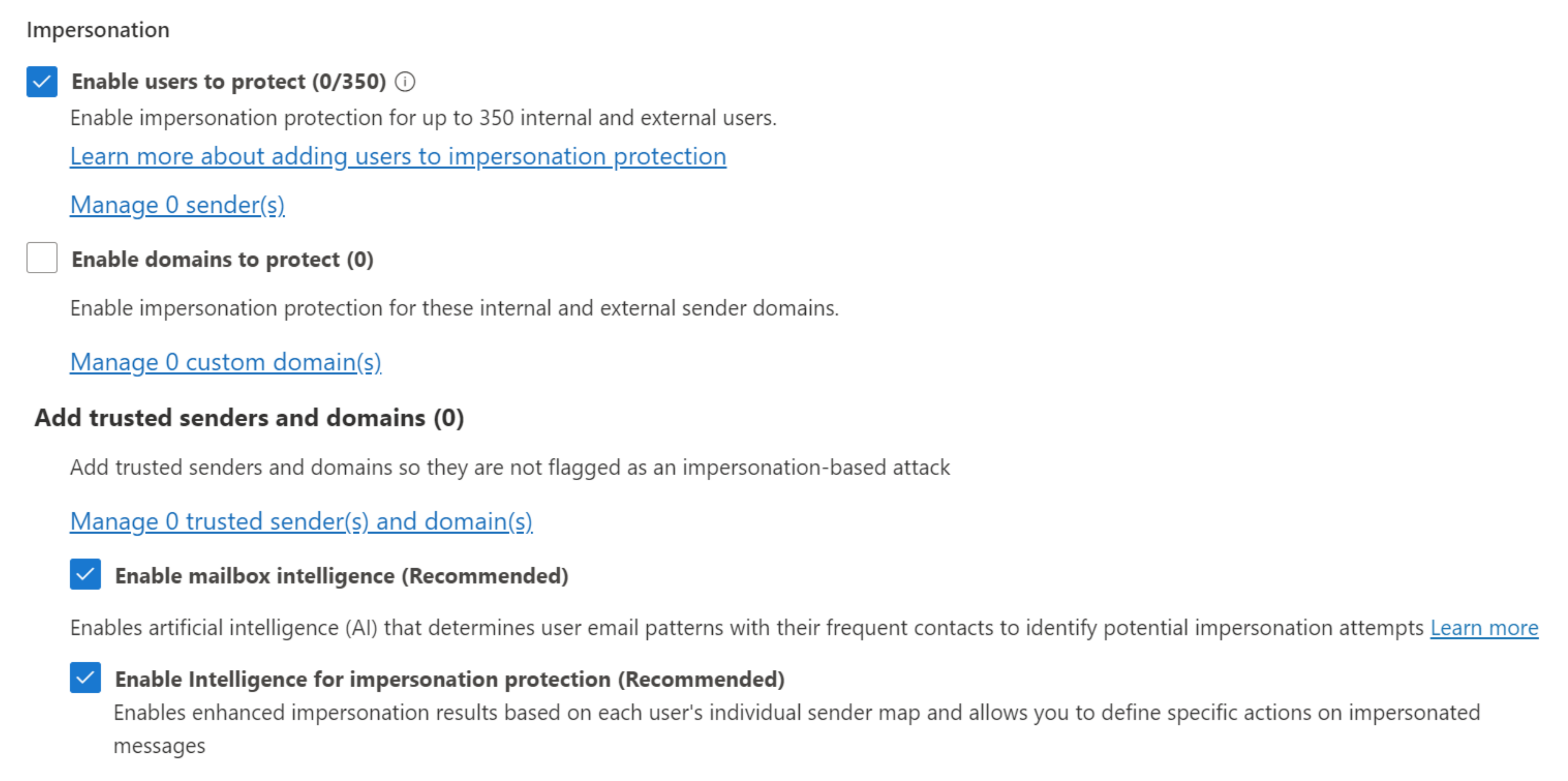
Email | URL clicks | Top URLs | Top clicks | Top targeted users | Email origin | Campaign

Message actions

102 items | Export | Customize columns

☐	Date (UTC +01:00)	Subject	Recipient	Tags	Sender	Additional actions	Latest delivery location	Original delivery locati...	Threat type
☐	Nov 25, 2023 7:25 PM	[redacted]	[redacted]	Priority account	[redacted]	-	Inbox/folder	Inbox/folder	None
☐	Nov 25, 2023 6:43 PM	[redacted]	[redacted]	Priority account	[redacted]	-	Inbox/folder	Inbox/folder	None
☐	Nov 25, 2023 6:43 PM	[redacted]	[redacted]	Priority account	[redacted]	-	Junk folder	Junk folder	Spam
☐	Nov 25, 2023 6:40 PM	[redacted]	[redacted]	Priority account	[redacted]	-	Junk folder	Junk folder	Spam
☐	Nov 25, 2023 6:31 PM	[redacted]	[redacted]	Priority account	[redacted]	-	Inbox/folder	Inbox/folder	None
☐	Nov 25, 2023 4:17 PM	[redacted]	[redacted]	Priority account	[redacted]	-	Inbox/folder	Inbox/folder	None

Impersonation Protection



Impersonation

☑ **Enable users to protect (0/350)** ⓘ

Enable impersonation protection for up to 350 internal and external users.

Learn more about adding users to impersonation protection

Manage 0 sender(s)

□ **Enable domains to protect (0)**

Enable impersonation protection for these internal and external sender domains.

Manage 0 custom domain(s)

Add trusted senders and domains (0)

Add trusted senders and domains so they are not flagged as an impersonation-based attack

Manage 0 trusted sender(s) and domain(s)

☑ **Enable mailbox intelligence (Recommended)**

Enables artificial intelligence (AI) that determines user email patterns with their frequent contacts to identify potential impersonation attempts Learn more

☑ **Enable Intelligence for impersonation protection (Recommended)**

Enables enhanced impersonation results based on each user's individual sender map and allows you to define specific actions on impersonated messages

Takeaways

- Revisit the basics, such as data location
- Don’t dismiss foundational technologies like DNS & networking
- Have a look at your organization settings regularly
- Multi-Geo & Multi-Tenant, but just because you can, doesn’t mean you should
- MFA is a must, but it’s just the start for security

Thank you

@thomasvochten

https://thomasvochten.com

mail@thomasvochten.com

Get the slides