Microsoft 365 Tenant setup & configuration

Been there, done that?

About me

Thomas Vochten ☕ 👨‍💻 🏃

Talk to me about Microsoft 365 & Security

thomasvochten.com

mail@thomasvochten.com

MVP Microsoft® Most Valuable Professional

collabdays.org

CRONOS

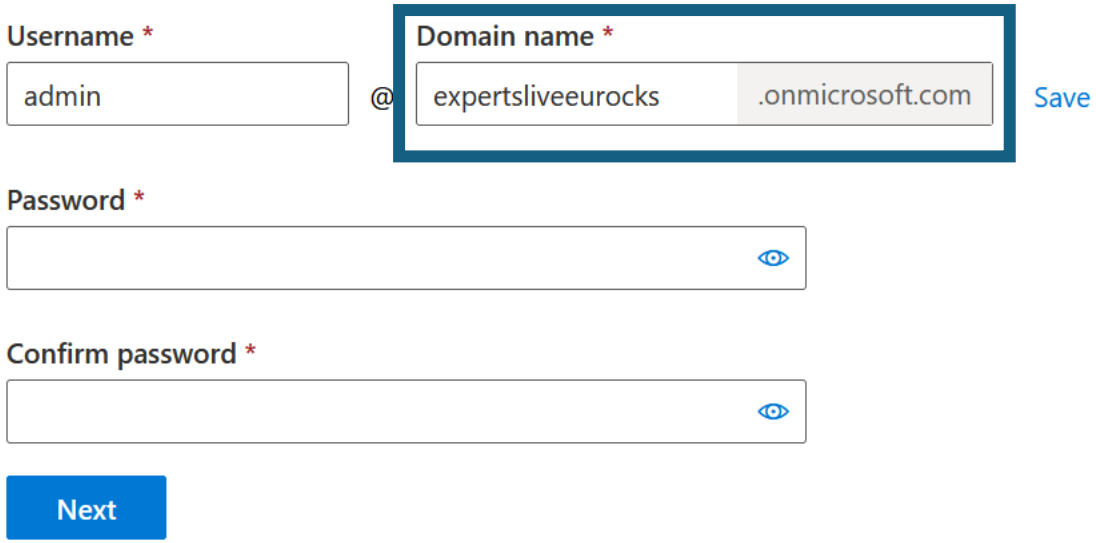
Agenda

1. Tenant creation & data residency
2. Domains, DNS & networking
3. Organizational settings & some useful tools

Tenant creation & data residency

Creating a new tenant

https://signup.microsoft.com

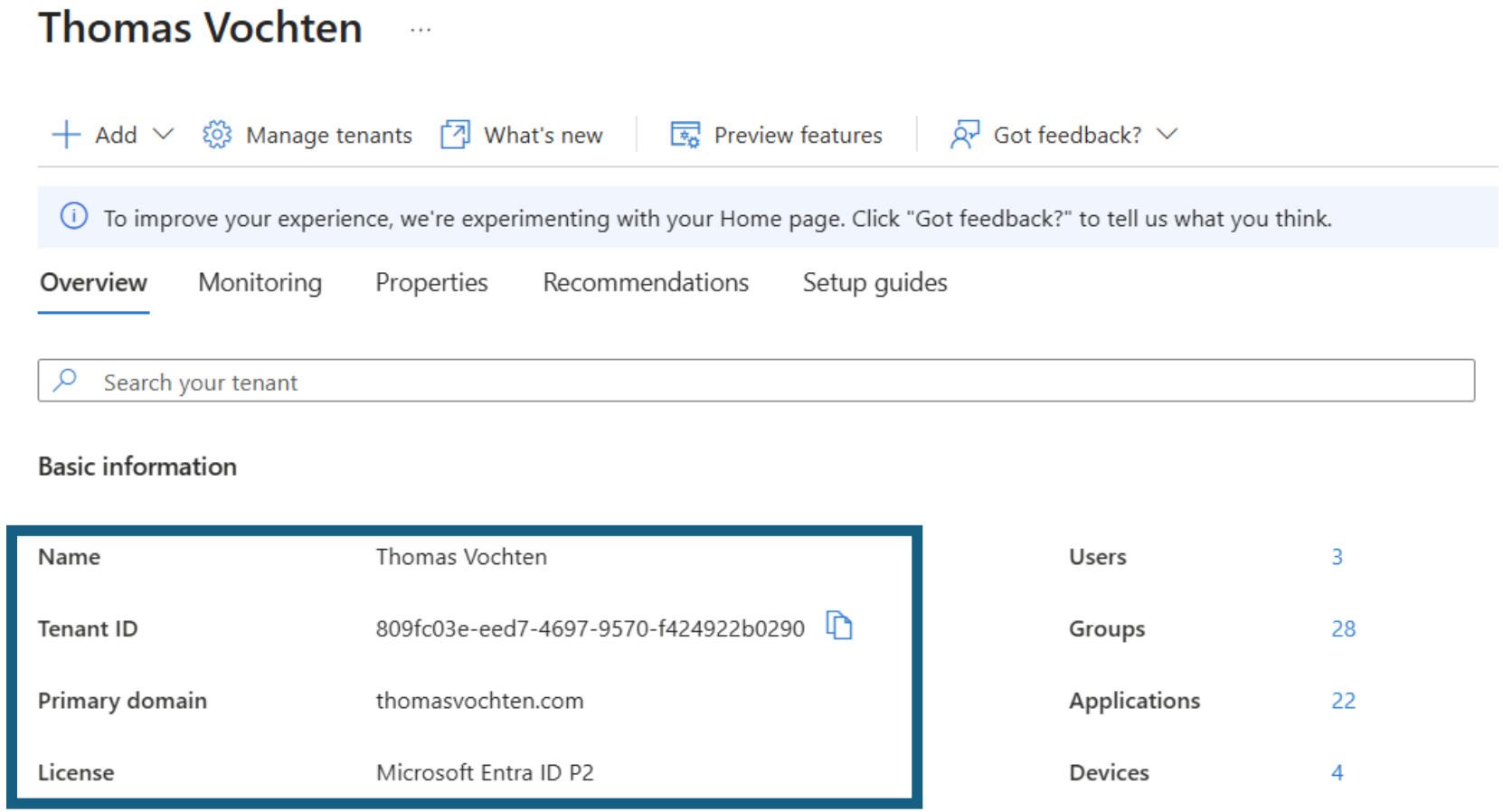


Creating a new tenant

We're checking to make sure we can offer you Microsoft products and services.

This review won't affect your current services. Buying new products and services and some subscription actions will be restricted until the review is complete. The review process usually takes up to 2 days, but can last longer.

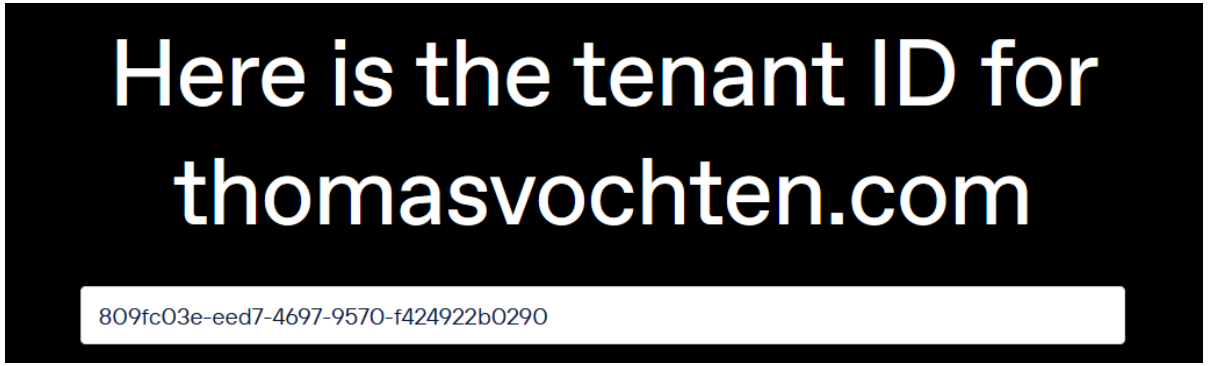
Tenant properties in Entra ID



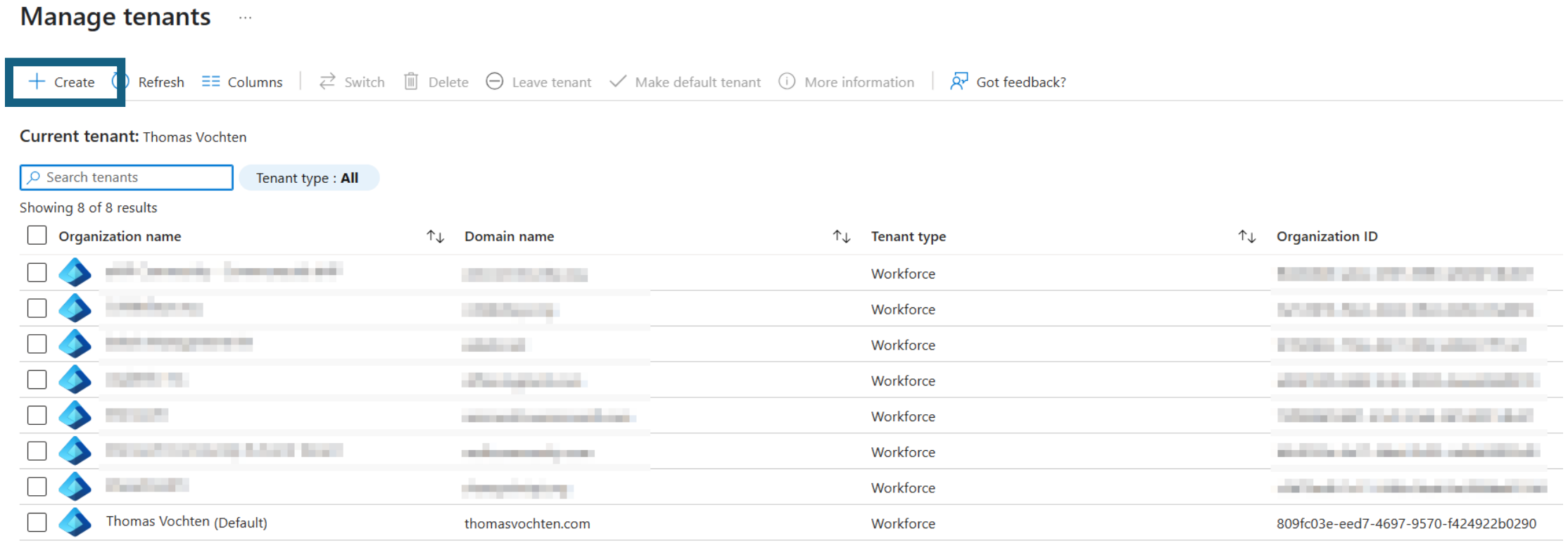
About that Tenant ID

It’s public information!

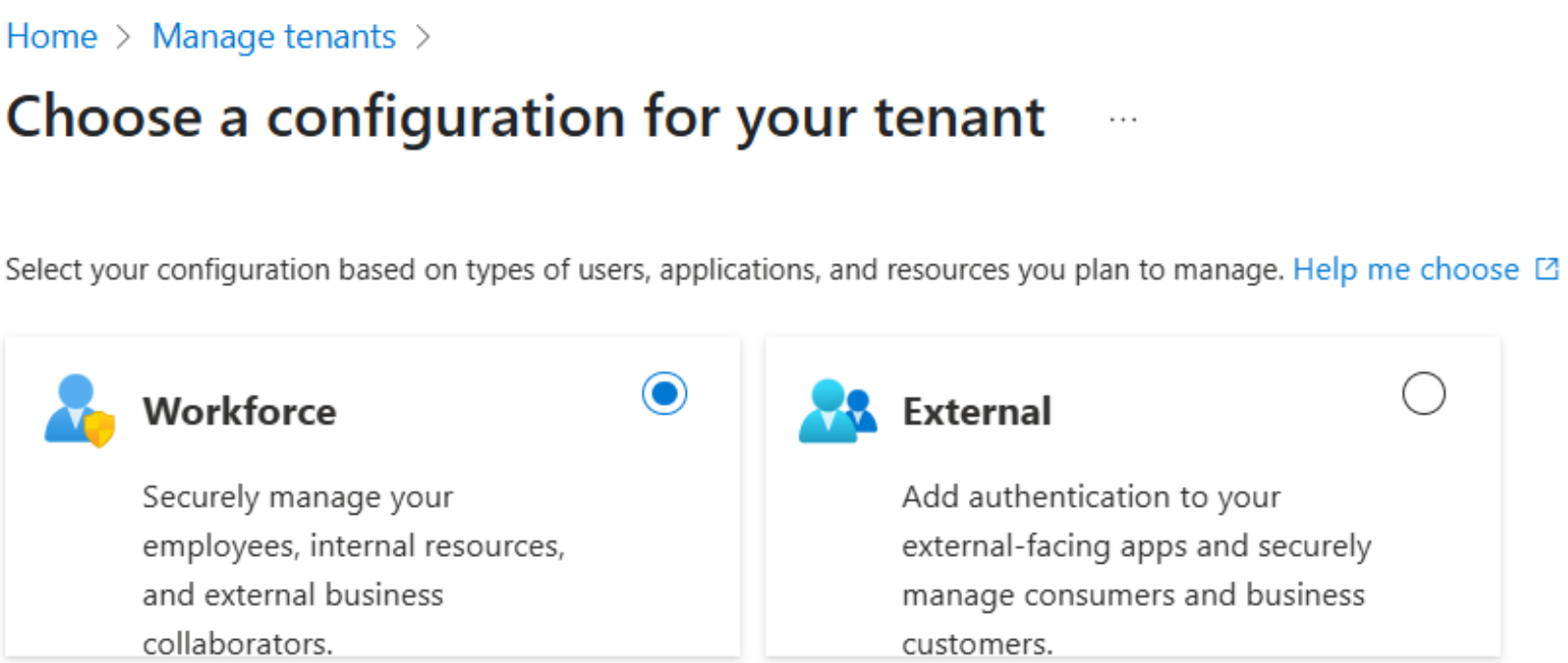
➡️ https://www.whatismytenantid.com



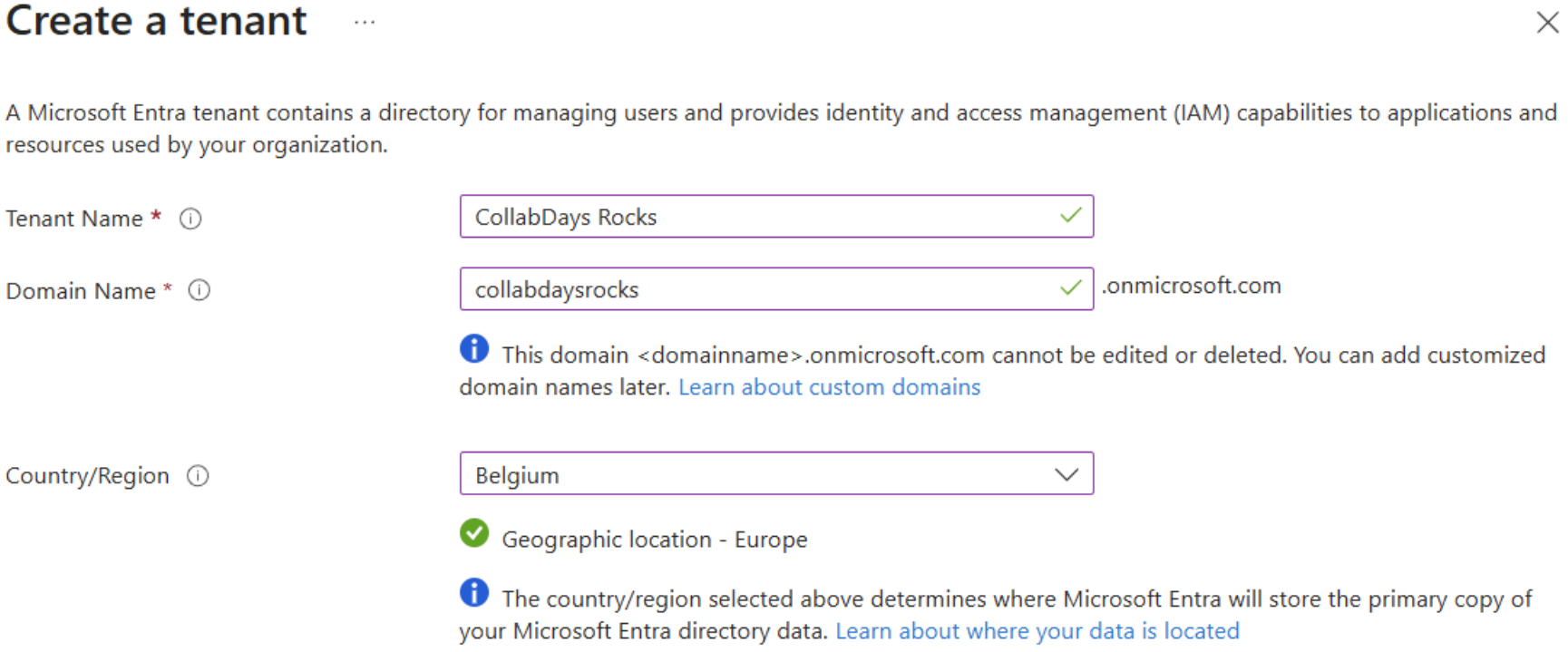
Creating a new tenant in Entra ID



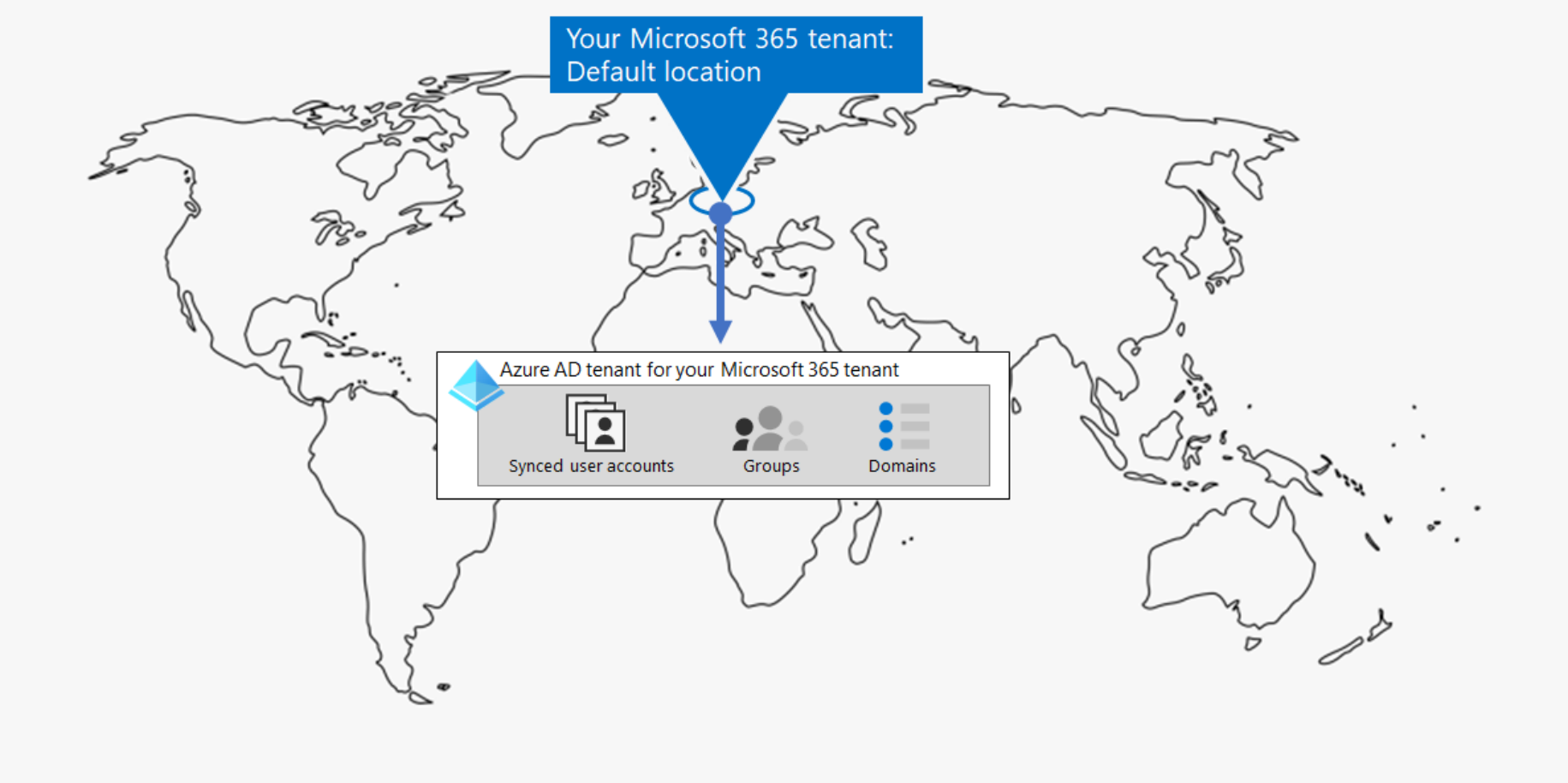
Creating a new tenant in Entra ID



Creating a new tenant in Entra ID



First things first. Where’s my data?



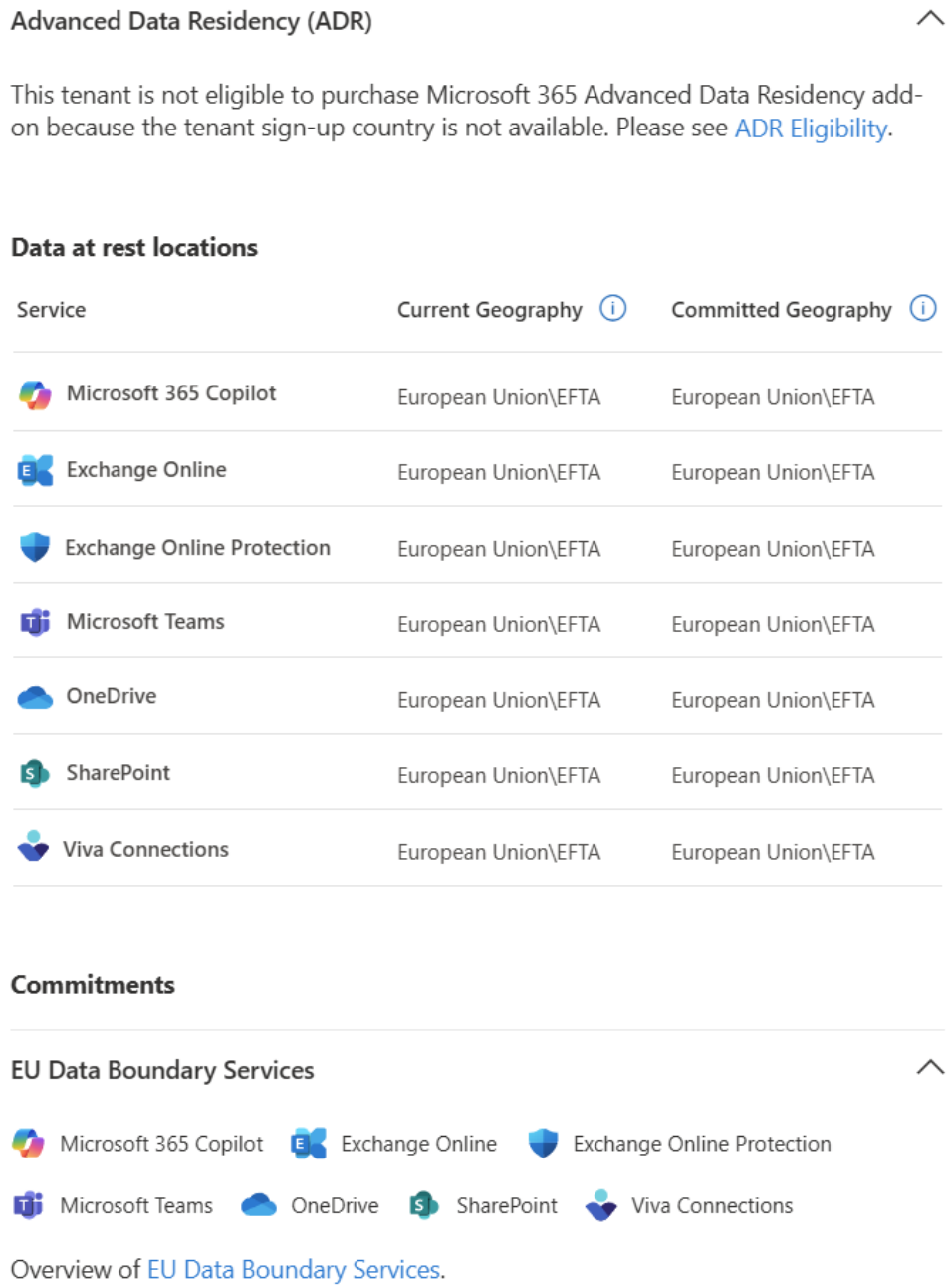
Data Residency primer

Default Geography of the Microsoft Entra ID Tenant

Available Geographies for a given service

Where’s my data?

Settings > Org Settings > Organization profile > Data location



Advanced Data Residency (ADR)

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.

Data at rest locations

Service	Current Geography	Committed Geography
Microsoft 365 Copilot	European Union\EFTA	European Union\EFTA
Exchange Online	European Union\EFTA	European Union\EFTA
Exchange Online Protection	European Union\EFTA	European Union\EFTA
Microsoft Teams	European Union\EFTA	European Union\EFTA
OneDrive	European Union\EFTA	European Union\EFTA
SharePoint	European Union\EFTA	European Union\EFTA
Viva Connections	European Union\EFTA	European Union\EFTA

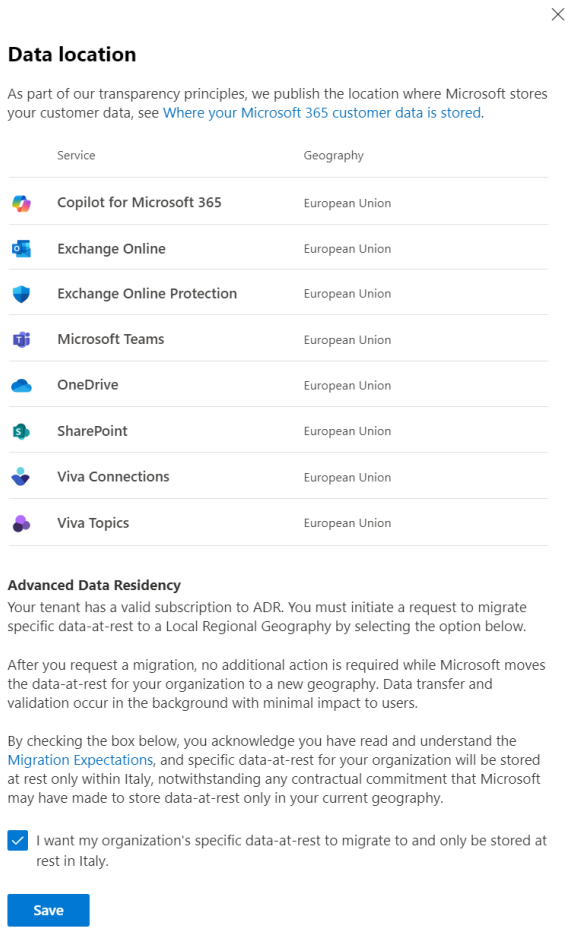
Commitments

EU Data Boundary Services

Microsoft 365 Copilot, Exchange Online, Exchange Online Protection, Microsoft Teams, OneDrive, SharePoint, Viva Connections

Overview of EU Data Boundary Services.

Workloads supported by the ADR add-on



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.

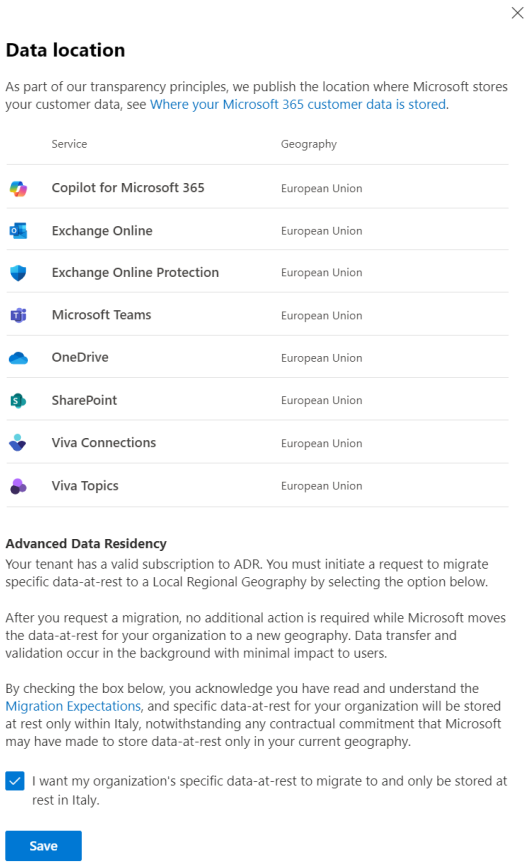
By checking the box below, you acknowledge you have read and understand the Migration Expectations, and specific data-at-rest for your organization will be stored at rest only within Italy, notwithstanding any contractual commitment that Microsoft may have made to store data-at-rest only in your current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

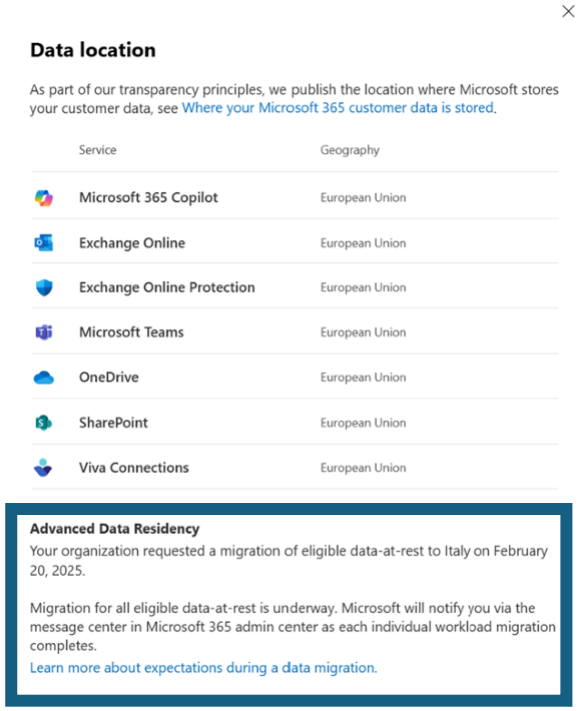
I want my organization's specific data-at-rest to migrate to and only be stored at rest in Italy.

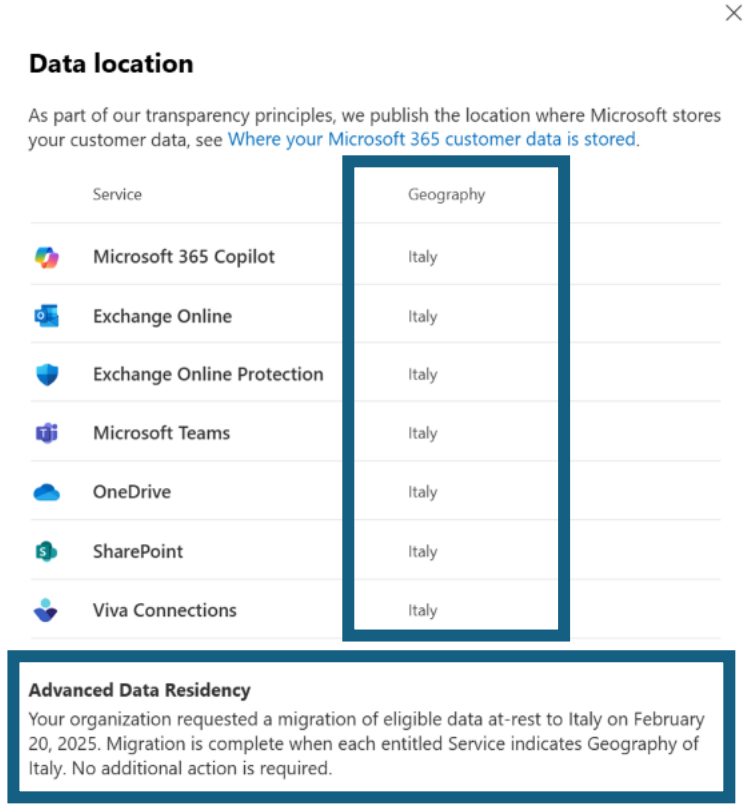
Save

- 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

Before, during and after data migration





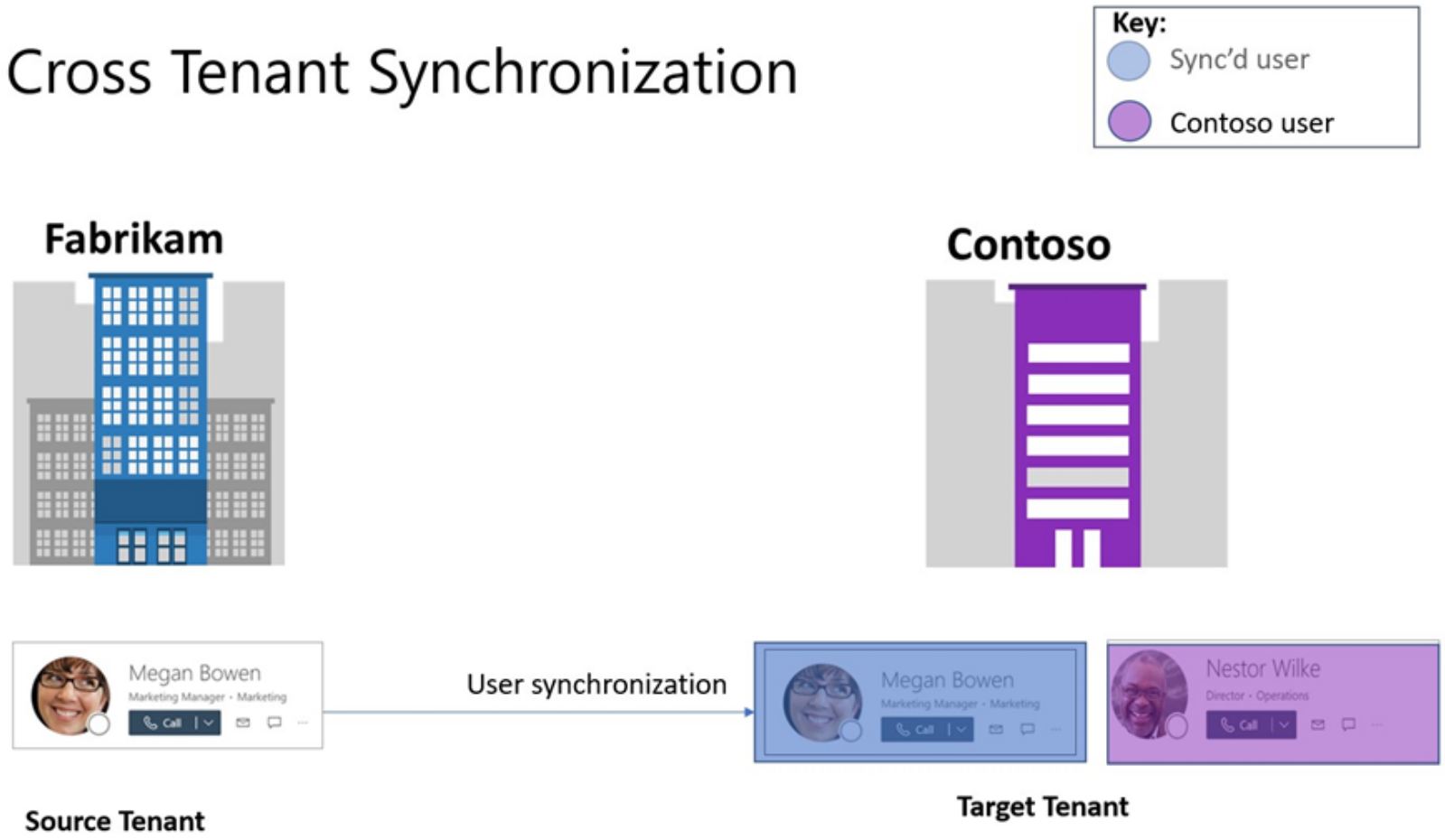


Multi-Geo & Multi-Tenant

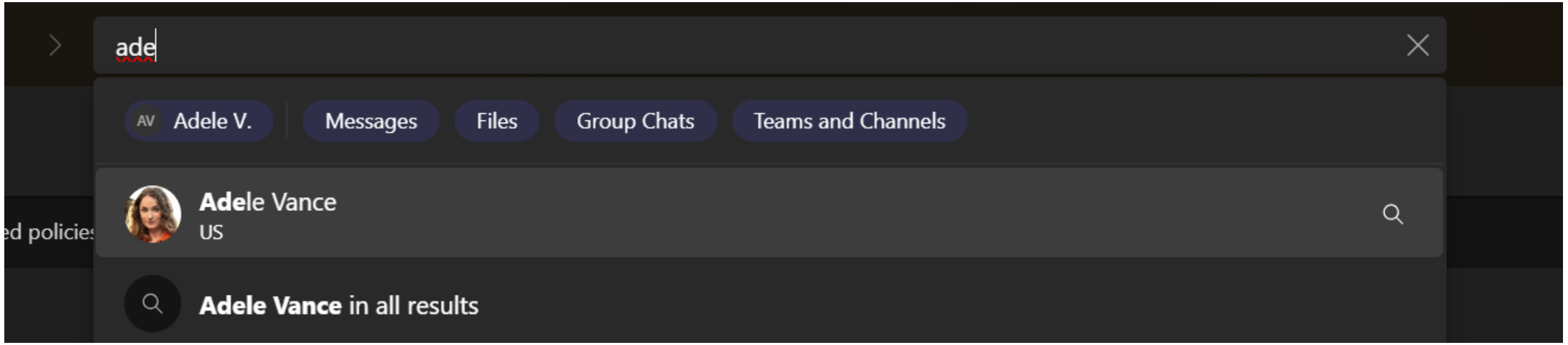
Multi-geo

- 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



Include an optional label



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

It's not DNS

There's no way it's DNS

It was DNS

thomasvochten.onmicrosoft.com

Managed at Microsoft 365 - Fallback domain

Meet your “fallback domain”

used for default usernames, email routing,…

used for your SharePoint Online & OneDrive URL’s

MOERA! … MOERA? 🤔

- Microsoft Online Email Routing Address
- Useful for testing mail flow, do not use it for regular messaging
- Due to a lot of abuse, additional restrictions will be put in place!

  100 external recipients per organization per 24 hour

- Inbound messages won’t be affected

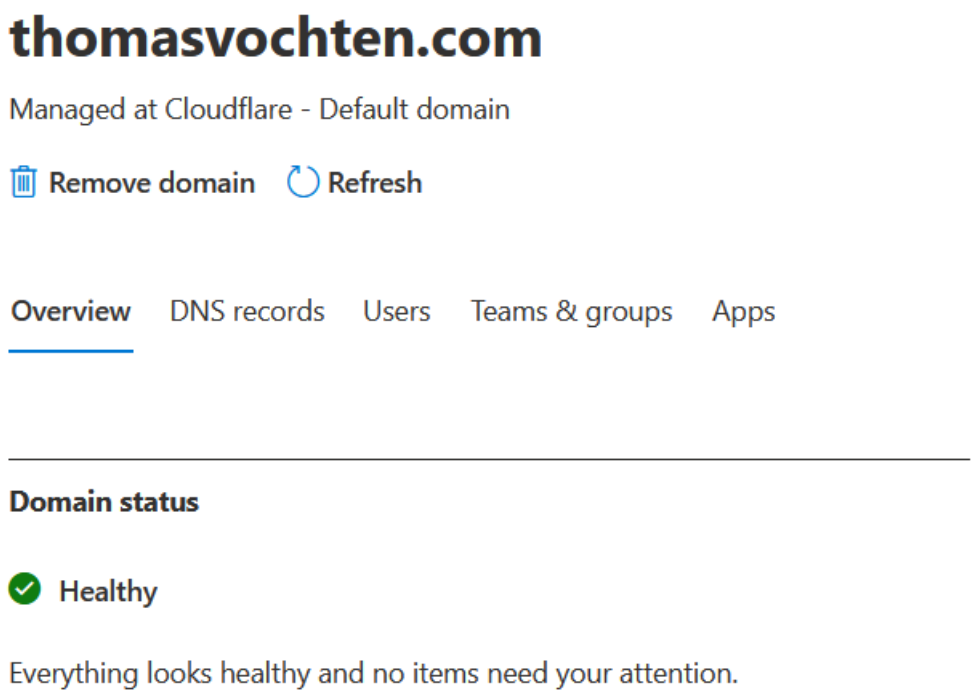
More info @

Changing yourdomain.sharepoint.com

- When would you want this?
- Less than 10K sites? Standard Tenant Rename (free)
- Less than 100K sites? Advanced Tenant Rename (add-on)
- 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

Custom domains

thomasvochten.com

Managed at Cloudflare - Default domain

Remove domain Refresh

Overview | DNS records | Users | Teams & groups | Apps

To manage DNS records for thomasvochten.com, go to your DNS hosting provider: Cloudflare.

Connect your services to your domain by adding these DNS records at your domain registrar or DNS hosting provider. Select a record to see all of its details and 'copy and paste' the expected values to your registrar. Learn more about DNS and record types.

Check health Manage DNS Download CSV file Download zone file Print Search records

Microsoft Exchange

Type	Status	Name	Value	TTL
MX	OK	@	0 thomasvochten-com.mail.protection.outlook.com	1 Hour
TXT	OK	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour
CNAME	OK	autodiscover	autodiscover.outlook.com	1 Hour

Skype for Business

Type	Status	Name	Value	TTL
CNAME	OK	sip	sipdir.online.lync.com	1 Hour
CNAME	OK	lyncdiscover	webdir.online.lync.com	1 Hour
SRV	OK	_sip._tls	100 1 443 sipdir.online.lync.com	1 Hour
SRV	OK	_sipfederationtls._tcp	100 1 5061 sipfed.online.lync.com	1 Hour

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 device registration or exchange autodiscover
- 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

“v=spf1 include:spf.protection.outlook.com –all”

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

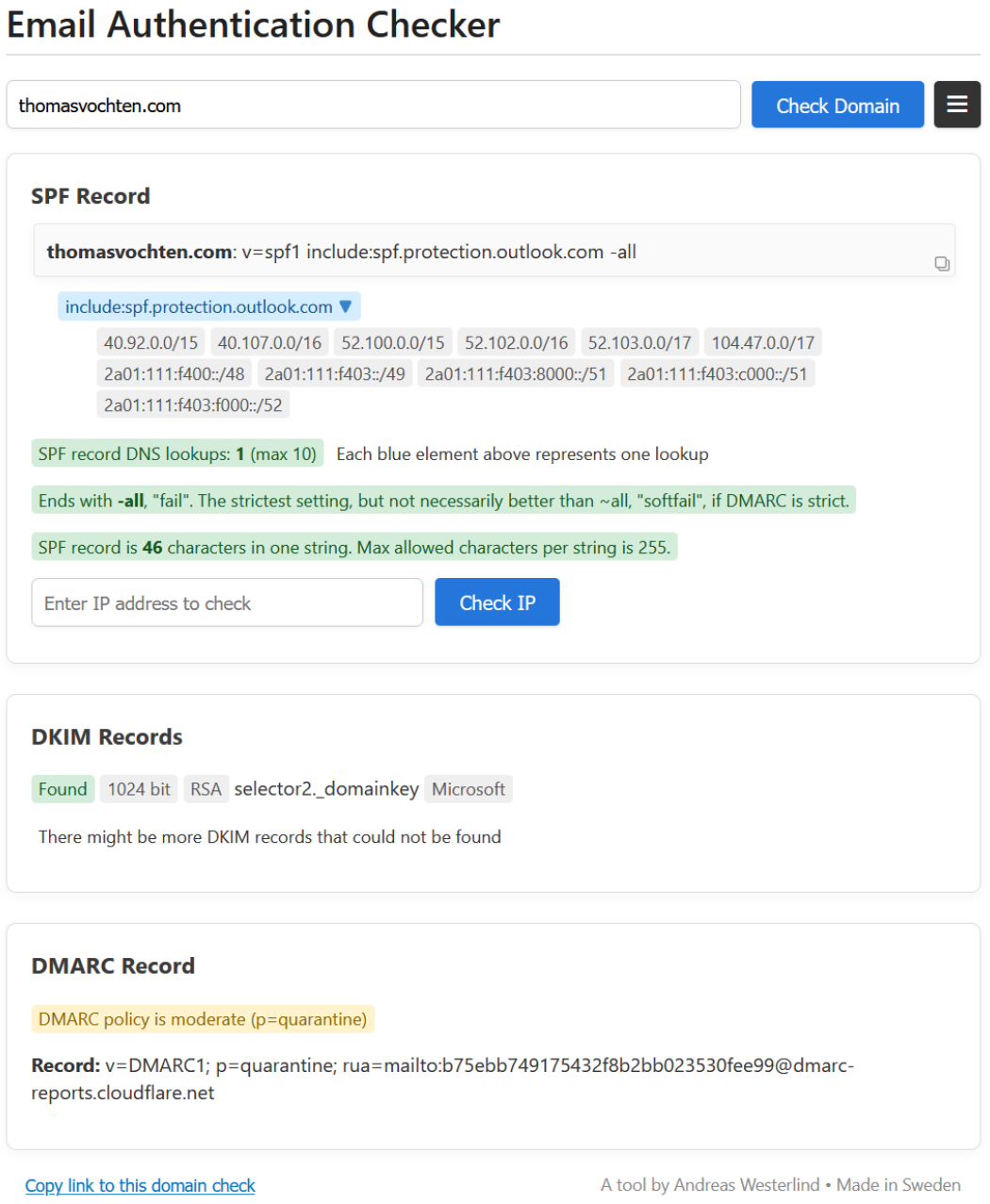
SPF only checks for spoofed **5321.MailFrom** addresses

SPF + DMARC provides complete address verification

"v=DMARC1; p=quarantine; rua=mailto:b75ebb749175432f8b2bb023530fee99@dmarc-reports.cloudflare.net"

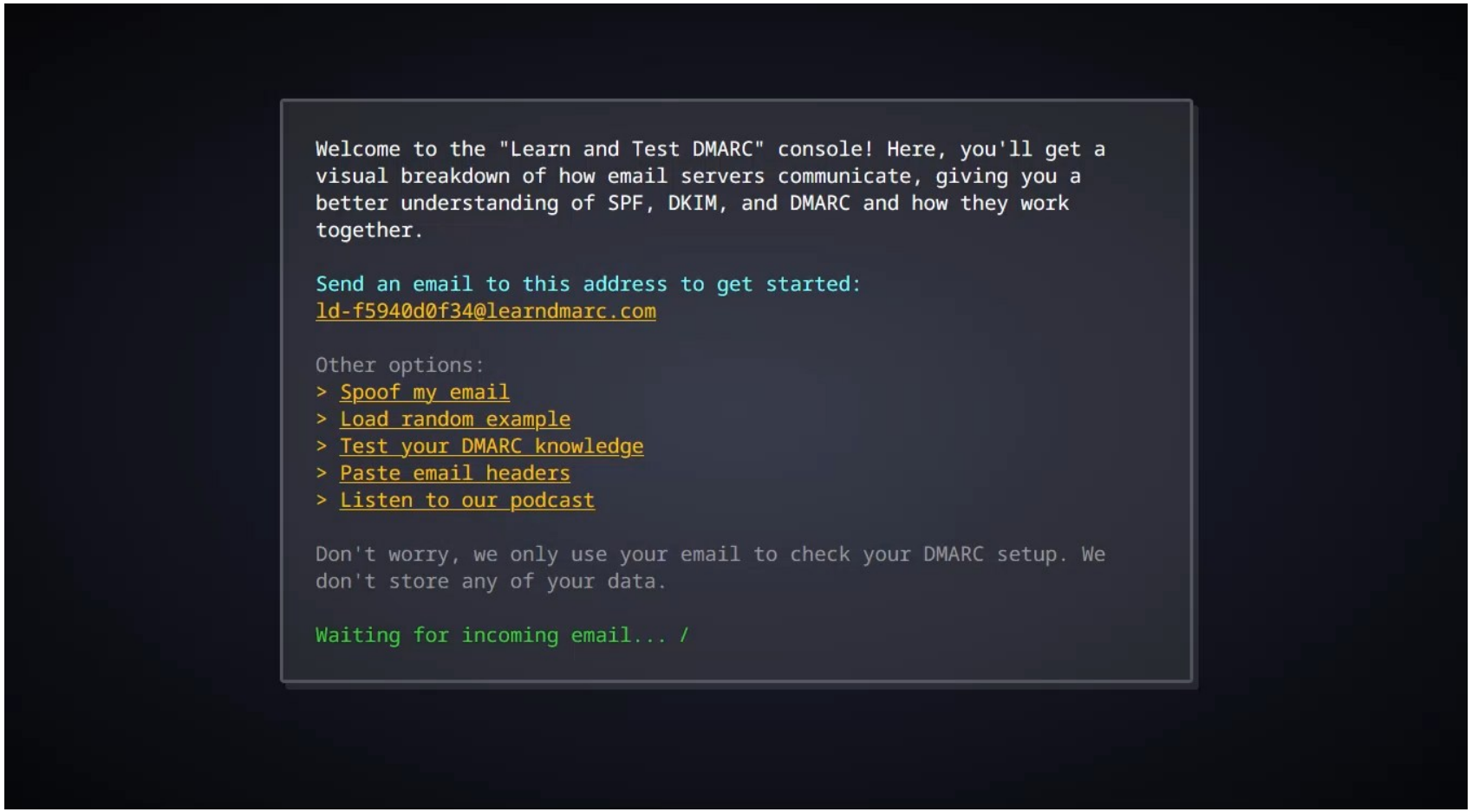
Check email authentication

https://spf.access.nu/



Check email authentication (for geeks with time 🤓)

https://www.learndmarc.com/

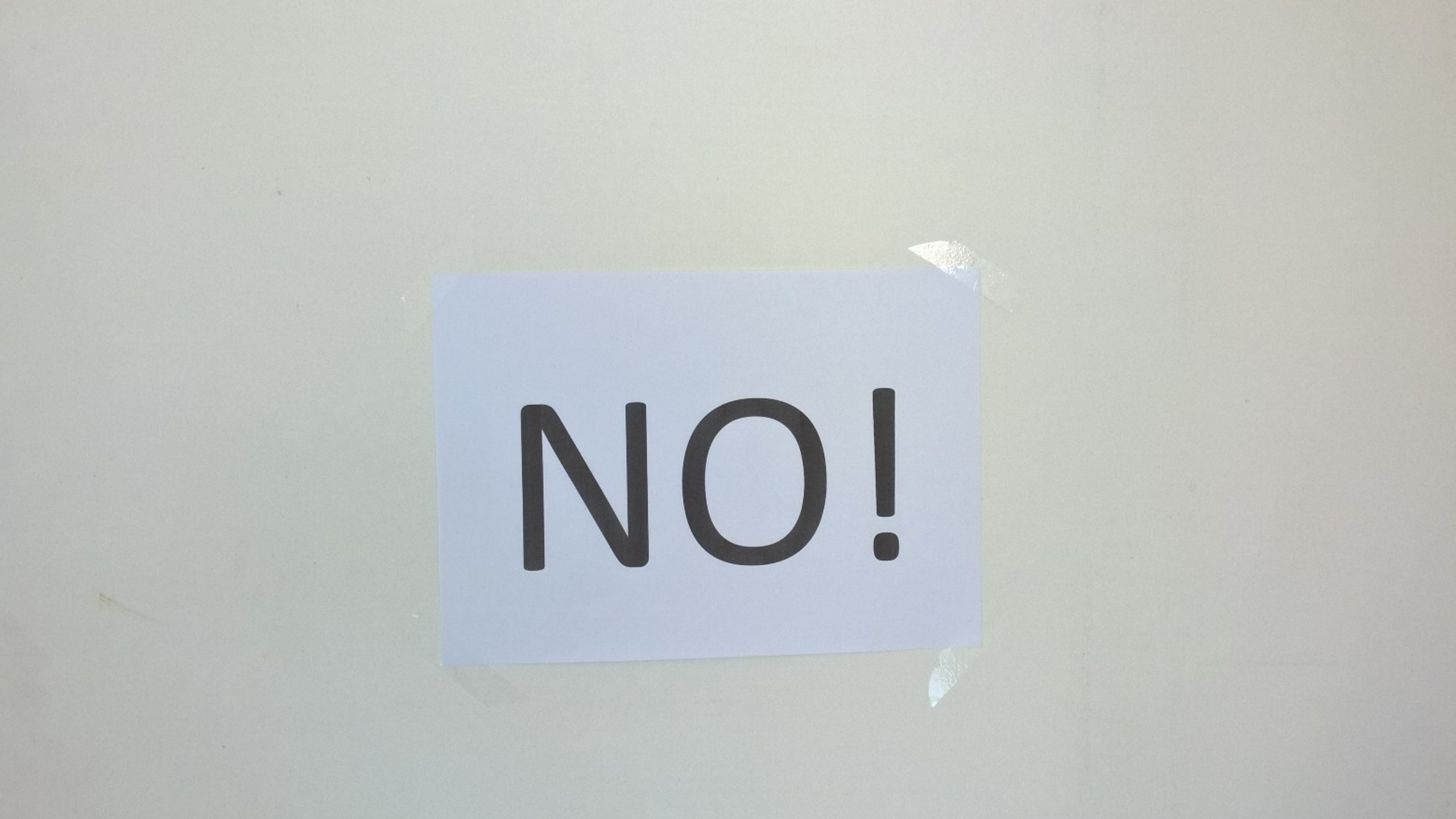


Network optimization

- 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

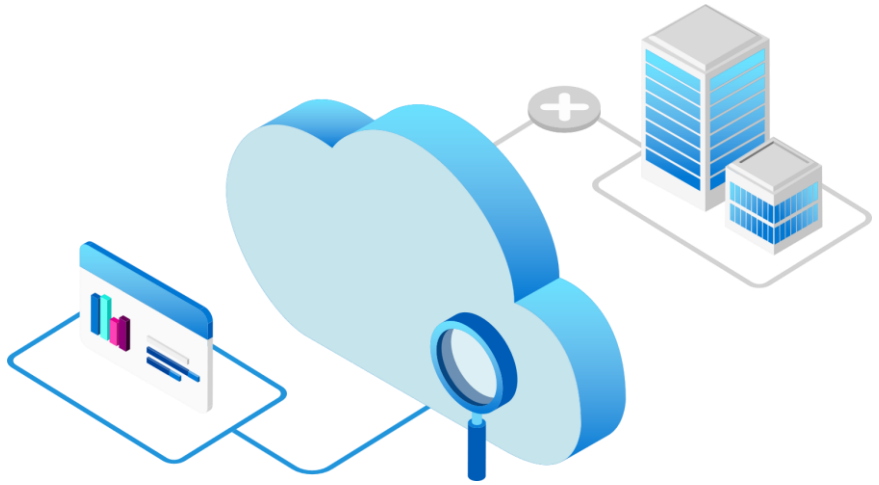
Wait a minute... 😨 😓


NO!

Endpoints (URLs & IP ranges)

https://aka.ms/m365ip

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



The new kids on the block

*.cloud.microsoft
*.static.microsoft
*.usercontent.microsoft

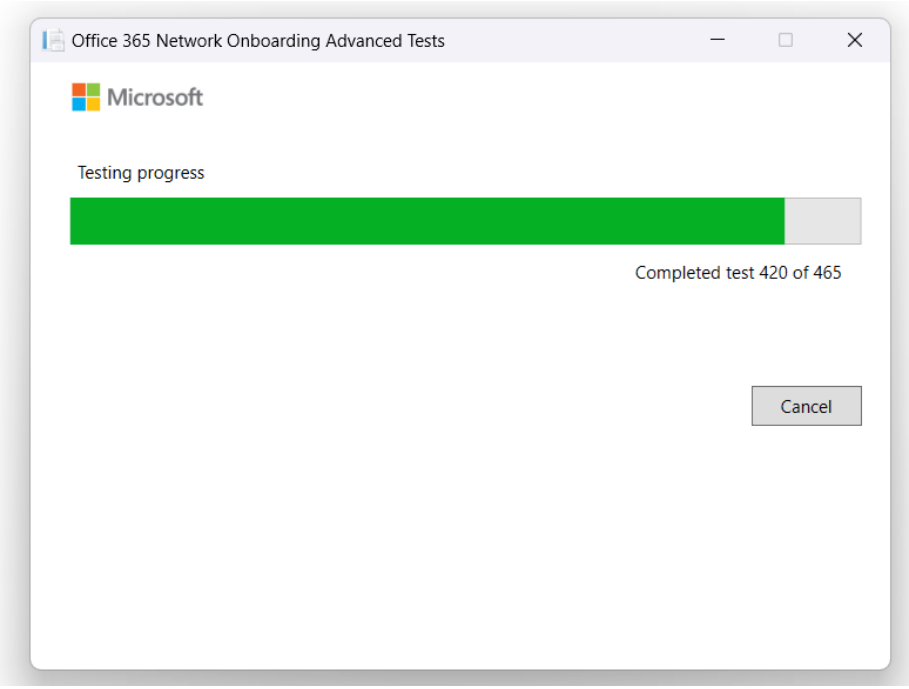
Affects:

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

Testing connectivity

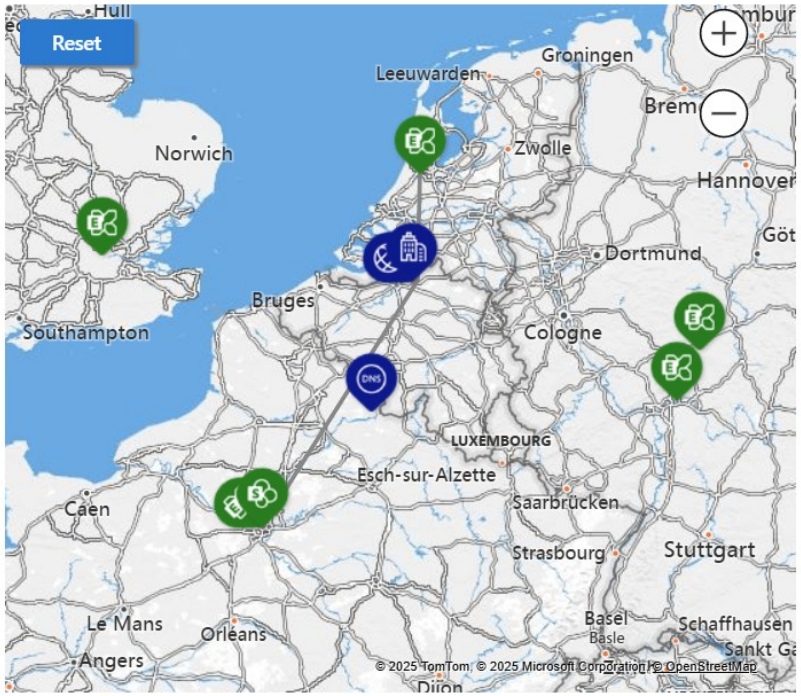
Don’t assume everything will just work

https://connectivity.office.com



Testing connectivity

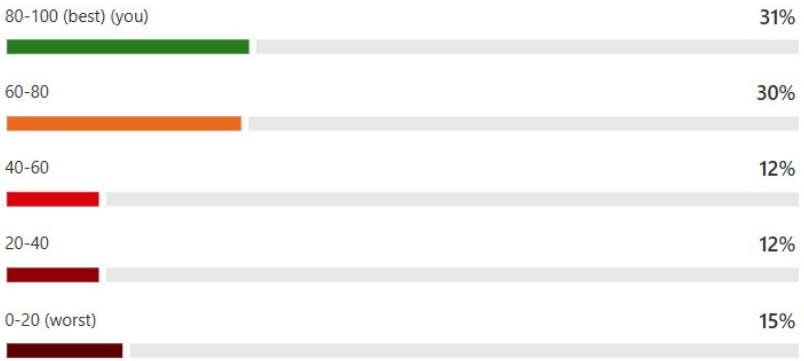
Map of your network connections



Your location
Your network's connection to your ISP
Your current Exchange front door
Your current SharePoint front door
Recommended Exchange front door
Recommended SharePoint front door
DNS recursive resolver server
Your proxy server

No one in nearby locations have better network connectivity to Microsoft 365 than your location.

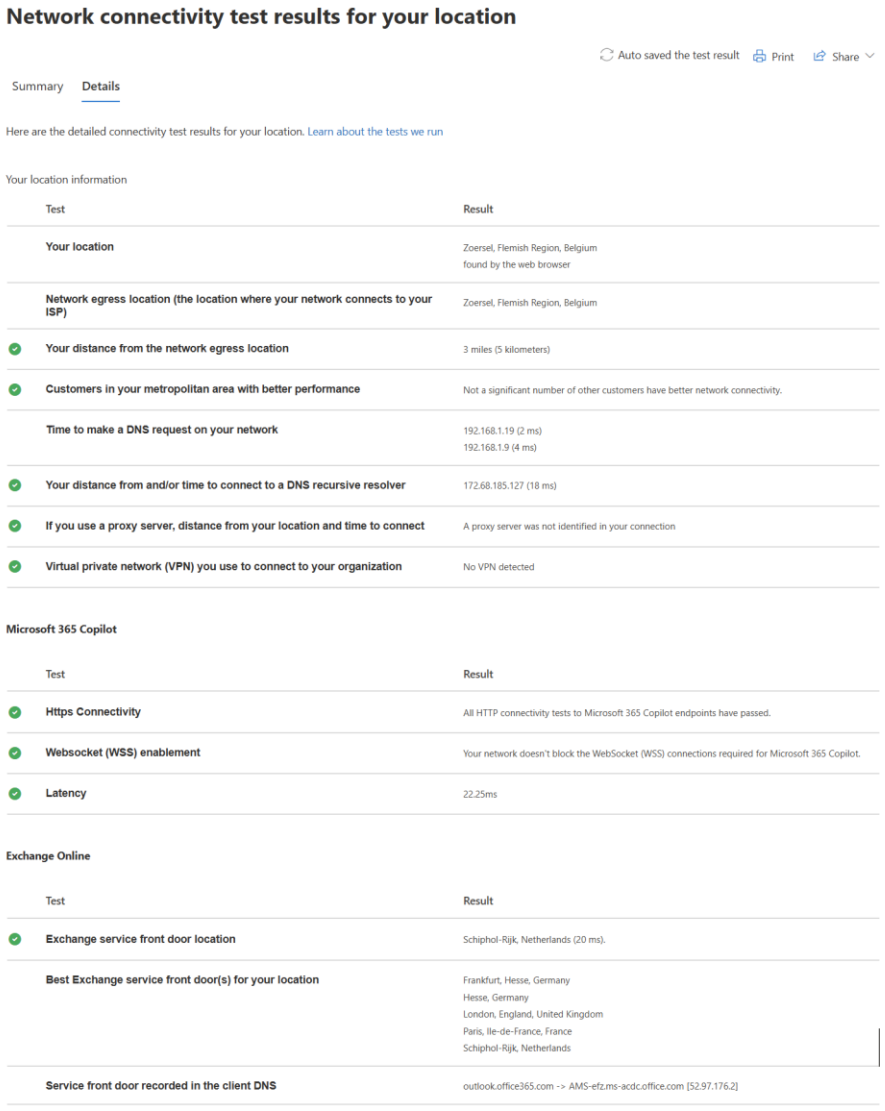
This chart shows the network connection quality for Microsoft 365 customers in your area.



Your network location was classified as a Unknown

Thanks for answering

Testing connectivity



Network connectivity test results for your location

Auto saved the test result | Print | Share

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 (5 kilometers)
Customers in your metropolitan area with better performance	Not a significant number of other customers have better network connectivity.
Time to make a DNS request on your network	192.168.1.19 (2 ms) 192.168.1.9 (4 ms)
Your distance from and/or time to connect to a DNS recursive resolver	172.68.185.127 (18 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

Microsoft 365 Copilot

Test	Result
Https Connectivity	All HTTP connectivity tests to Microsoft 365 Copilot endpoints have passed.
Websocket (WSS) enablement	Your network doesn't block the WebSocket (WSS) connections required for Microsoft 365 Copilot.
Latency	22.25ms

Exchange Online

Test	Result
Exchange service front door location	Schiphol-Rijk, Netherlands (20 ms).
Best Exchange service front door(s) for your location	Frankfurt, Hesse, Germany Hesse, Germany London, England, United Kingdom Paris, Ile-de-France, France Schiphol-Rijk, Netherlands
Service front door recorded in the client DNS	outlook.office365.com -> AMS-efz.ms-acdc.office.com [52.97.176.2]

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

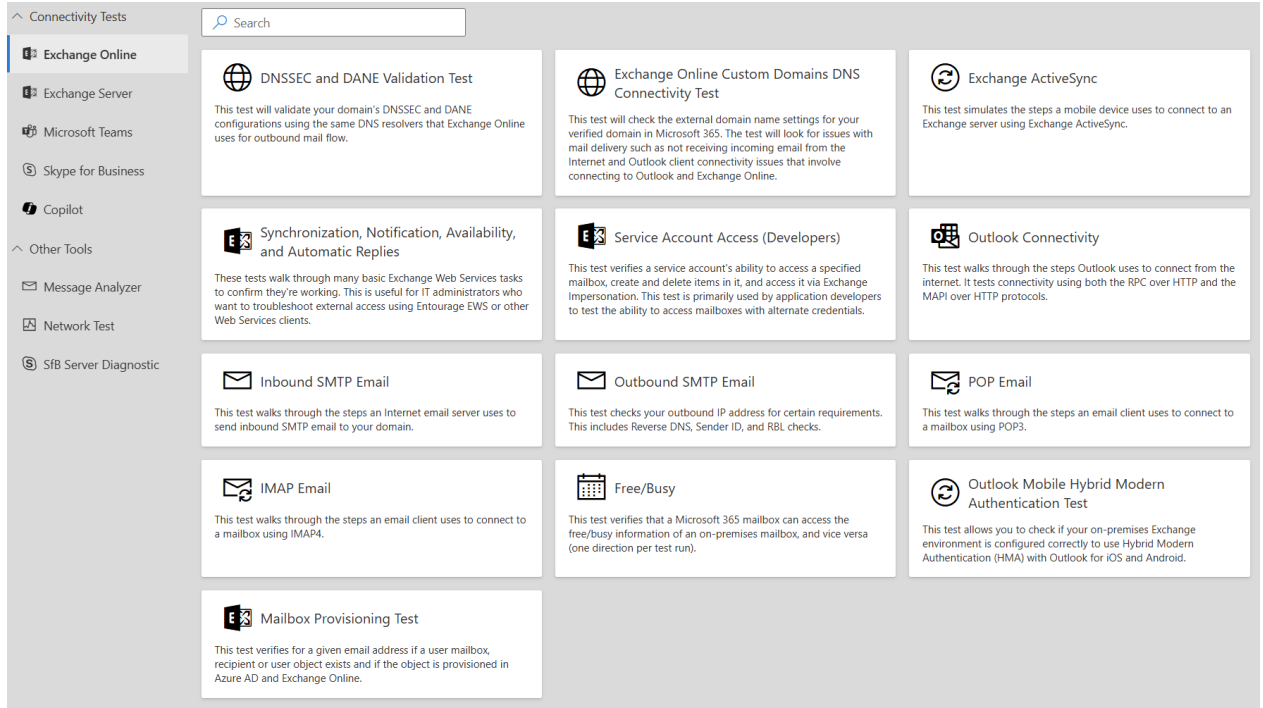
Unblock URL:
platform.linkedin.com
Test FQDN(s) used were:
platform.linkedin.com

Unblock URL:
crl.microsoft.com
Test FQDN(s) used were:
crl.microsoft.com

Unblock URL:
*.office.net

Remote Connectivity Analyzer

https://testconnectivity.microsoft.com



Connectivity Test Successful

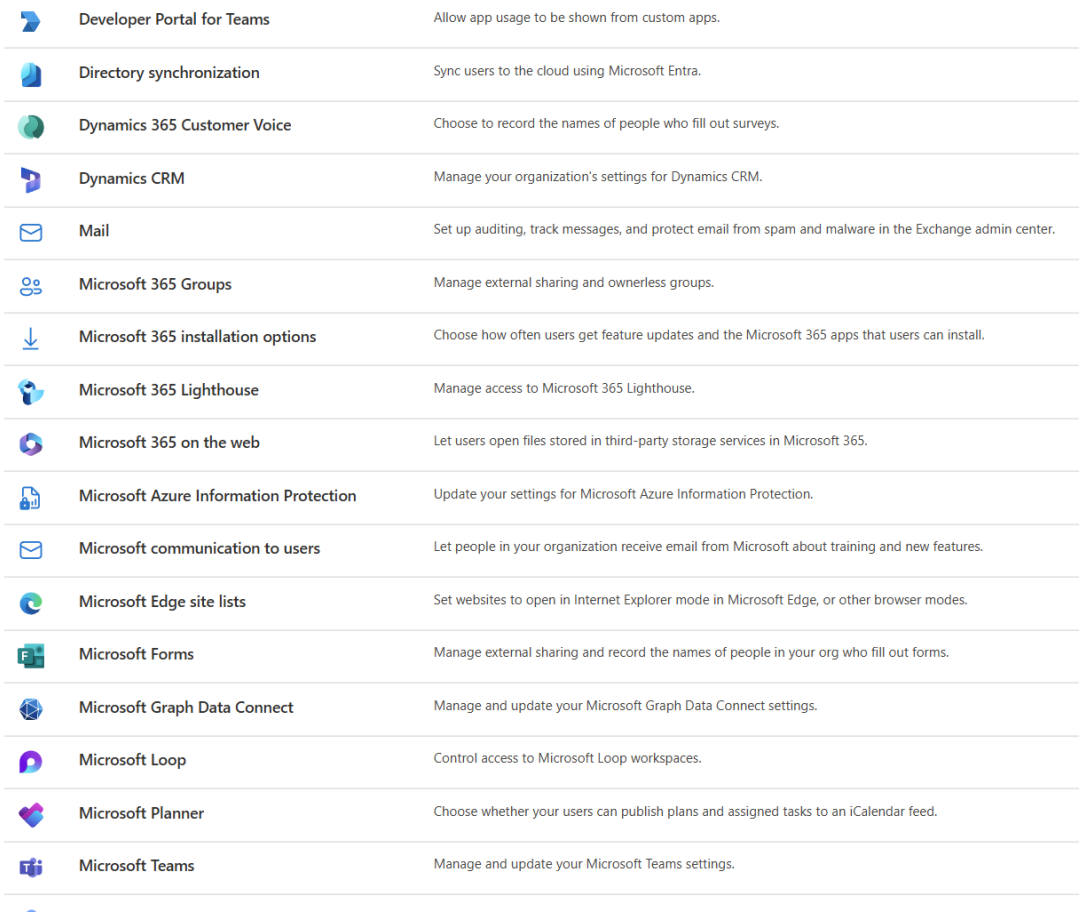
Test Details

- Checking if user mail@thomasvochten.com is assigned a Copilot license.
  - The user has a valid Copilot license.
  - Test Steps
    - Sending a request for the user's license and service details to the Microsoft Graph service.
      - The Microsoft Graph service returned a valid response.
      - Test Steps
        - Attempting to send a GET request to https://graph.microsoft.com/v1.0/users/mail@thomasvochten.com/licenseDetails
          - The request received a successful response.
          - Additional Details
        - Attempting to parse the response content.
          - Successfully parsed the response content.
          - Additional Details
    - Sending a request to Microsoft Graph to retrieve the AAD attributes for internal Teams user 'mail@thomasvochten.com'.
      - Successfully retrieved the attributes from Microsoft Graph.
      - Test Steps
        - Sending a request for user information to the Microsoft Graph service.
          - The Microsoft Graph service returned a valid response.
          - Test Steps
    - Verifying user attributes for user 'mail@thomasvochten.com'.
      - Successfully retrieved the attributes from Microsoft Graph.
      - Additional Details
        - The user account is enabled for sign in.
    - Checking if user mail@thomasvochten.com is assigned a Copilot license.
      - The user has a valid Copilot license.
    - Checking Copilot feature details for user mail@thomasvochten.com.
      - Copilot features are enabled for the user.
      - Test Steps
        - Checking Copilot Studio in Copilot for M365 feature details for user mail@thomasvochten.com.
          - Copilot Studio in Copilot for M365 feature is enabled for the user.
        - Checking Microsoft 365 Copilot for SharePoint feature details for user mail@thomasvochten.com.
          - Microsoft 365 Copilot for SharePoint feature is enabled for the user.
        - Checking Graph Connectors in Microsoft 365 Copilot feature details for user mail@thomasvochten.com.
          - Graph Connectors in Microsoft 365 Copilot feature is enabled for the user.
        - Checking Power Platform Connectors in Microsoft 365 Copilot feature details for user mail@thomasvochten.com.
          - Power Platform Connectors in Microsoft 365 Copilot feature is enabled for the user.
        - Checking Microsoft 365 Copilot in Productivity Apps feature details for user mail@thomasvochten.com.
          - Microsoft 365 Copilot in Productivity Apps feature is enabled for the user.
        - Checking Microsoft 365 Copilot in Microsoft Teams feature details for user mail@thomasvochten.com.
          - Microsoft 365 Copilot in Microsoft Teams feature is enabled for the user.
        - Checking Microsoft Copilot with Graph-grounded chat feature details for user mail@thomasvochten.com.
          - Microsoft Copilot with Graph-grounded chat feature is enabled for the user.
        - Checking Intelligent Search feature details for user mail@thomasvochten.com.
          - Intelligent Search feature is enabled for the user.

Organizational settings & some useful tools

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
  - Pay-as-you-go services NEW
- Security & privacy settings
  - Control customer lockbox
  - Name pronunciation NEW
  - Disable password expiration
  - Enable privileged access
  - Let users add guests to the organization
- Organization profile
  - Custom themes, tiles, helpdesk information, custom email notifications
  - Multitenant collaboration



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

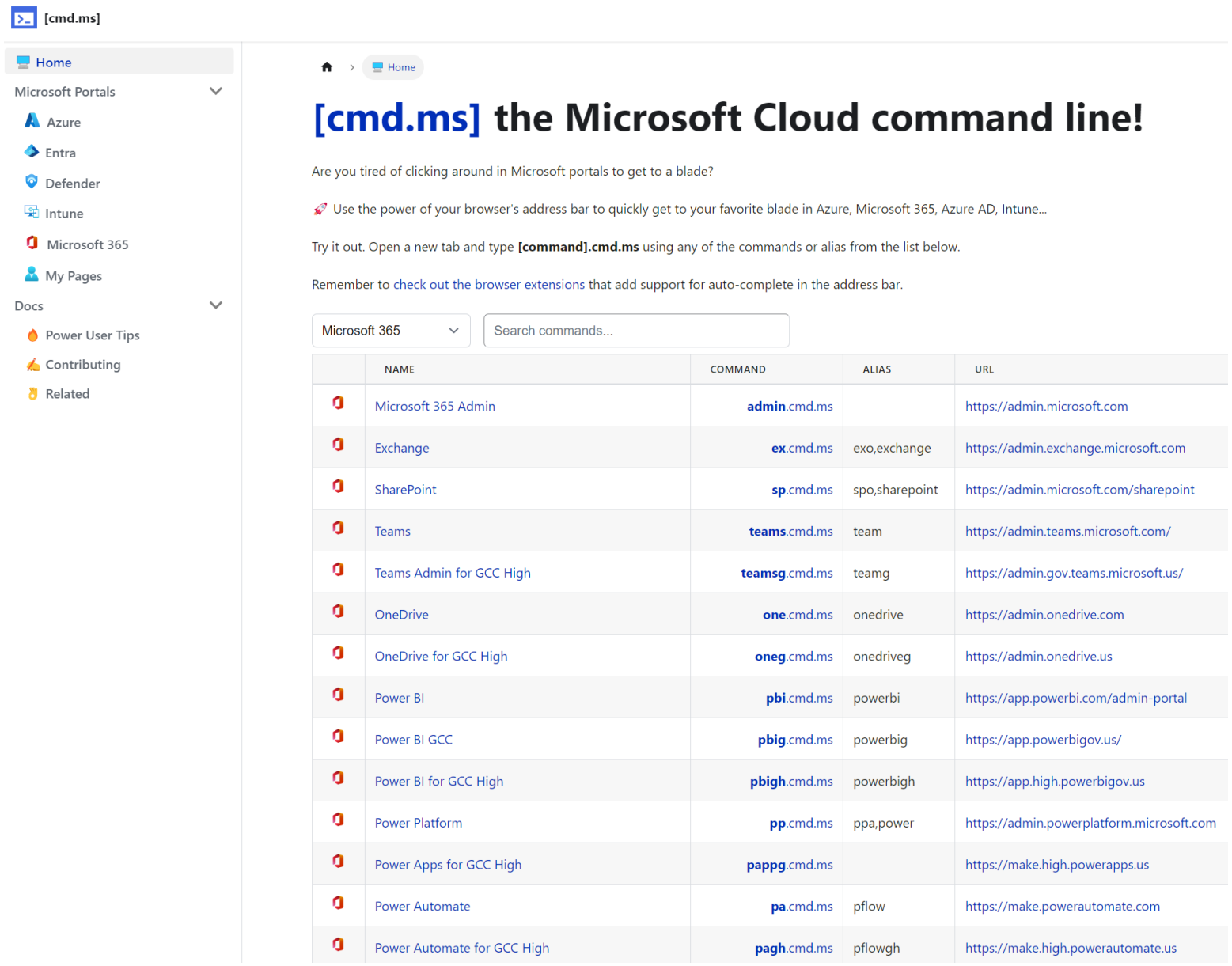
- Overview
- Deployment options
- **Predeployment**
- Identity
- Networking
- Licensing
- **Management**
- Security
- Applications
- User experience
- Business continuity and disaster recovery
- Review
- Finish

Management

Consider these items before your deployment.

Item	Priority
Has Intune been configured to use the default mobile device management (MDM) URLs?	High
Is there an Intune enrollment restriction policy to block Windows devices from Intune enrollment?	High
Has co-management been set up in Configuration Manager and any workloads moved to Intune?	Optional
Do you plan to deploy Windows Update to Cloud PCs?	Low
Do you plan to use Windows Autopatch to manage updates on Cloud PCs?	Optional
Are there any packages (like apps or configurations) deployed to all devices or users that can impact Cloud PCs?	Low
Has the device configuration policy for Endpoint analytics enrollment been configured to include Cloud PCs?	Low
Has a dynamic group that includes all Cloud PCs been created?	Optional

cmd.ms


[cmd.ms]
Home
Microsoft Portals
Azure
Entra
Defender
Intune
Microsoft 365
My Pages
Docs
Power User Tips
Contributing
Related
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.
Microsoft 365
Search commands...
NAME COMMAND ALIAS URL
Microsoft 365 Admin admin.cmd.ms https://admin.microsoft.com
Exchange ex.cmd.ms exo,exchange https://admin.exchange.microsoft.com
SharePoint sp.cmd.ms spo,sharepoint https://admin.microsoft.com/sharepoint
Teams teams.cmd.ms team https://admin.teams.microsoft.com/
Teams Admin for GCC High teamsg.cmd.ms teamg https://admin.gov.teams.microsoft.us/
OneDrive one.cmd.ms onedrive https://admin.onedrive.com
OneDrive for GCC High oneg.cmd.ms onedriveg https://admin.onedrive.us
Power BI pbi.cmd.ms powerbi https://app.powerbi.com/admin-portal
Power BI GCC pbig.cmd.ms powerbig https://app.powerbigov.us/
Power BI for GCC High pbigh.cmd.ms powerbigh https://app.high.powerbigov.us
Power Platform pp.cmd.ms ppa,power https://admin.powerplatform.microsoft.com
Power Apps for GCC High pappg.cmd.ms https://make.high.powerapps.us
Power Automate pa.cmd.ms pflow https://make.powerautomate.com
Power Automate for GCC High pagh.cmd.ms pflowgh https://make.high.powerautomate.us

Takeaways

- Revisit the basics
- Don’t dismiss foundational technologies like DNS
- Don’t take your network topology for granted
- Keep tabs on your organizational settings
- “Just because you can, doesn’t mean you should” (especially when it comes to multi-tenant or multi-geo)

Name one of the other two unified domains besides

`cloud.microsoft`

`static.microsoft`
`usercontent.microsoft`

We would love to hear your feedback!

Session feedback available in home feed of the app after the session

Thank You!