thomasvochten.com

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 GROEP

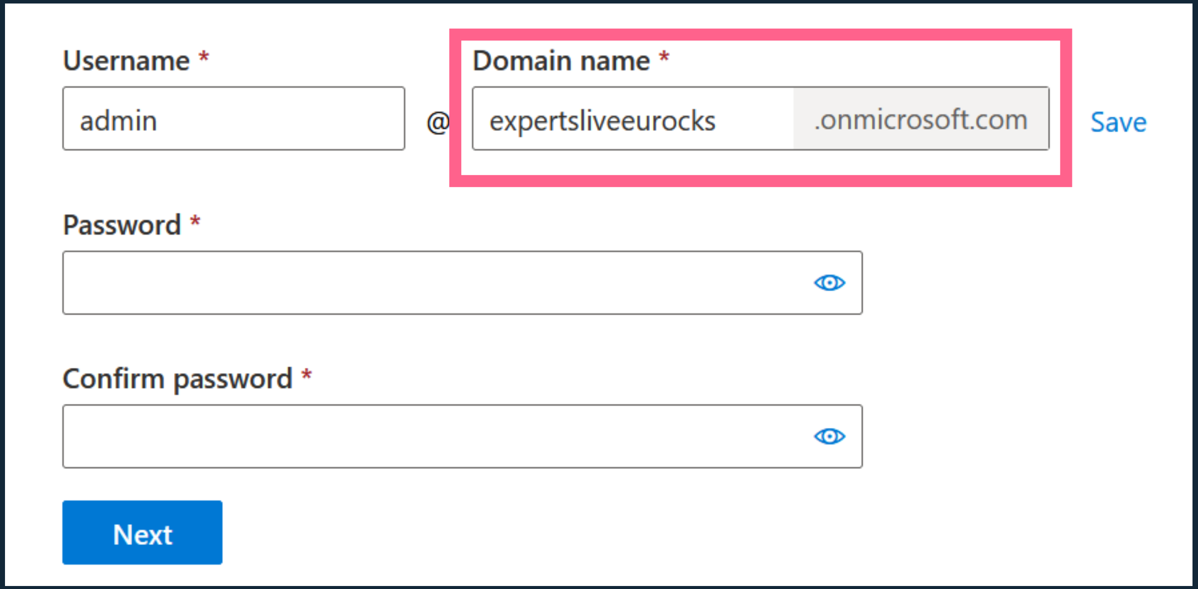
Agenda

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

General tenant considerations

Creating a new tenant

https://signup.microsoft.com



Username *

admin

@

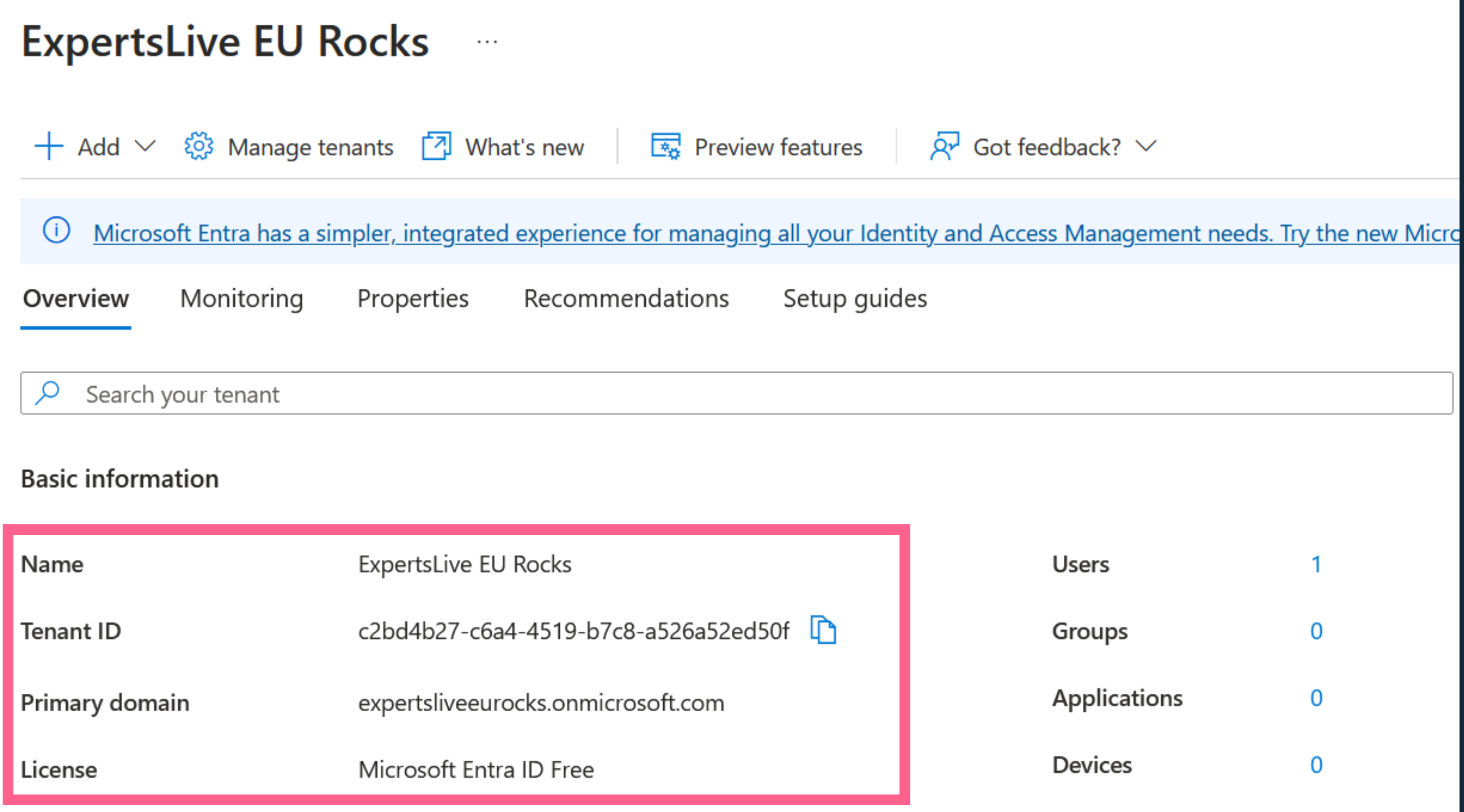
Domain name *

expertsliveeurocks .onmicrosoft.com

Password *

Confirm password *

Tenant properties in Entra ID



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

Basic information

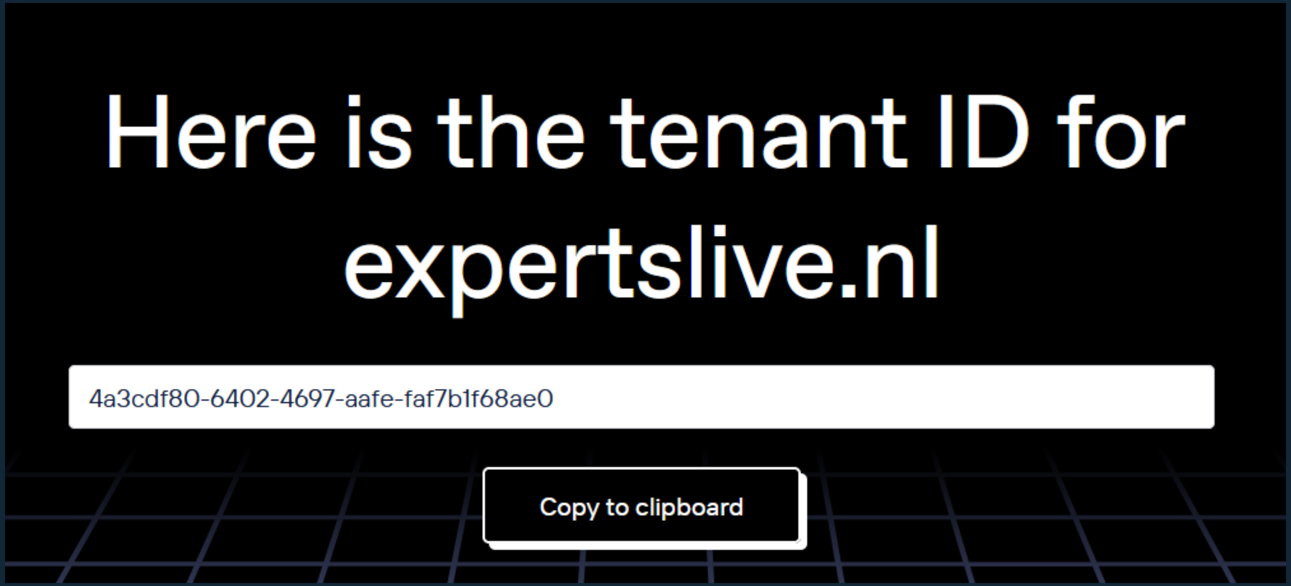
Name	ExpertsLive EU Rocks
Tenant ID	c2bd4b27-c6a4-4519-b7c8-a526a52ed50f
Primary domain	expertsliveeurocks.onmicrosoft.com
License	Microsoft Entra ID Free

Users	1
Groups	0
Applications	0
Devices	0

About that Tenant ID 💎

It’s public information!

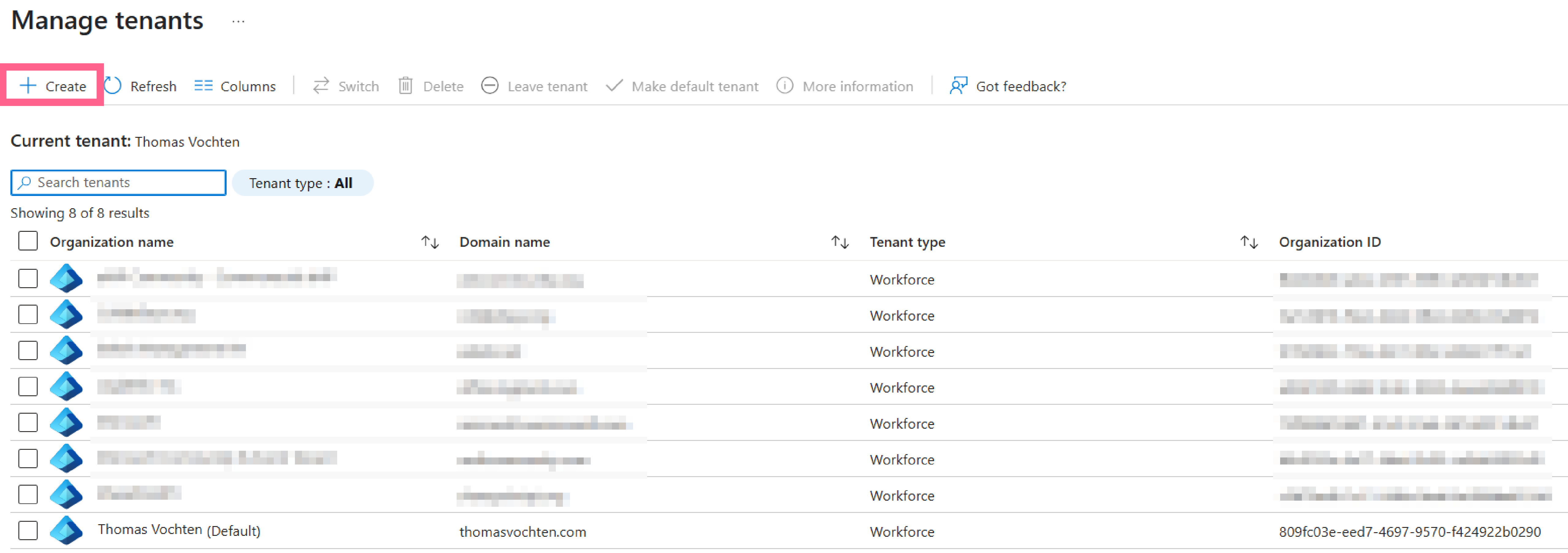
➡️ https://www.whatismytenantid.com



Here is the tenant ID for expertslive.nl

4a3cdf80-6402-4697-aafe-faf7b1f68ae0

Creating a new tenant in Entra ID



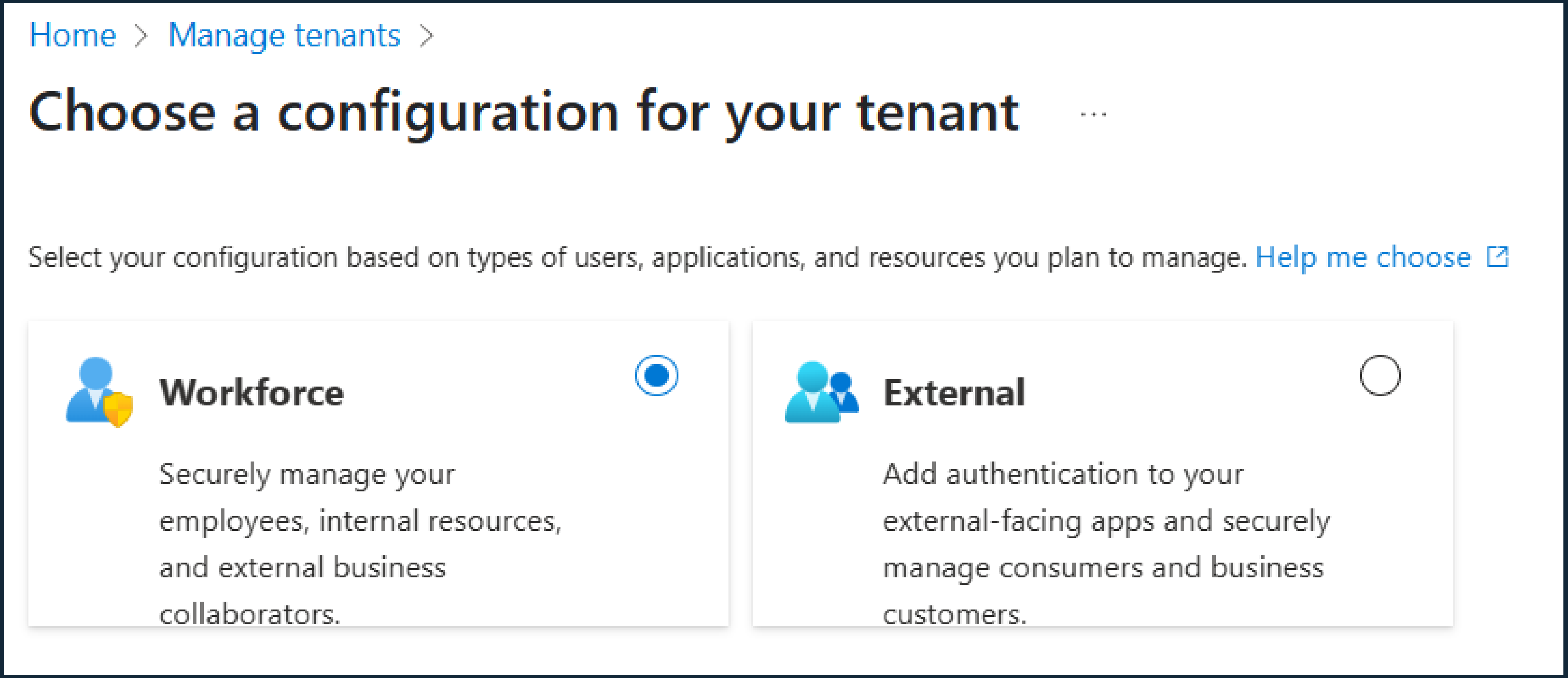
Manage tenants

Current tenant: Thomas Vochten

Showing 8 of 8 results

Organization name	Domain name	Tenant type	Organization ID
[redacted]	[redacted]	Workforce	[redacted]
[redacted]	[redacted]	Workforce	[redacted]
[redacted]	[redacted]	Workforce	[redacted]
[redacted]	[redacted]	Workforce	[redacted]
[redacted]	[redacted]	Workforce	[redacted]
[redacted]	[redacted]	Workforce	[redacted]
[redacted]	[redacted]	Workforce	[redacted]
Thomas Vochten (Default)	thomasvochten.com	Workforce	809fc03e-eed7-4697-9570-f424922b0290

Creating a new tenant in Entra ID



Home > Manage tenants >

Choose a configuration for your tenant ...

Select your configuration based on types of users, applications, and resources you plan to manage. Help me choose

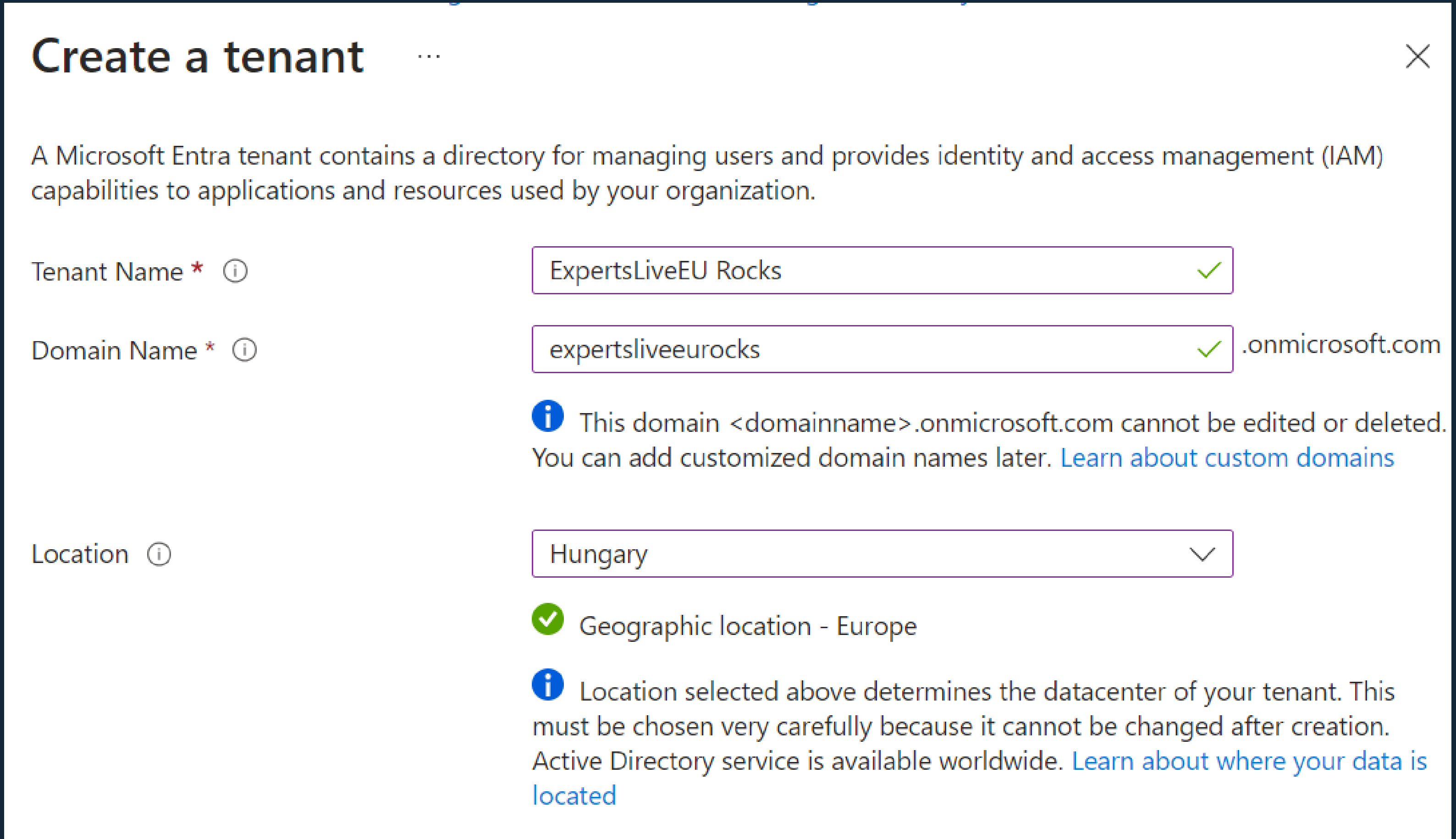
Workforce ●

Securely manage your employees, internal resources, and external business collaborators.

External ○

Add authentication to your external-facing apps and securely manage consumers and business customers.

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.

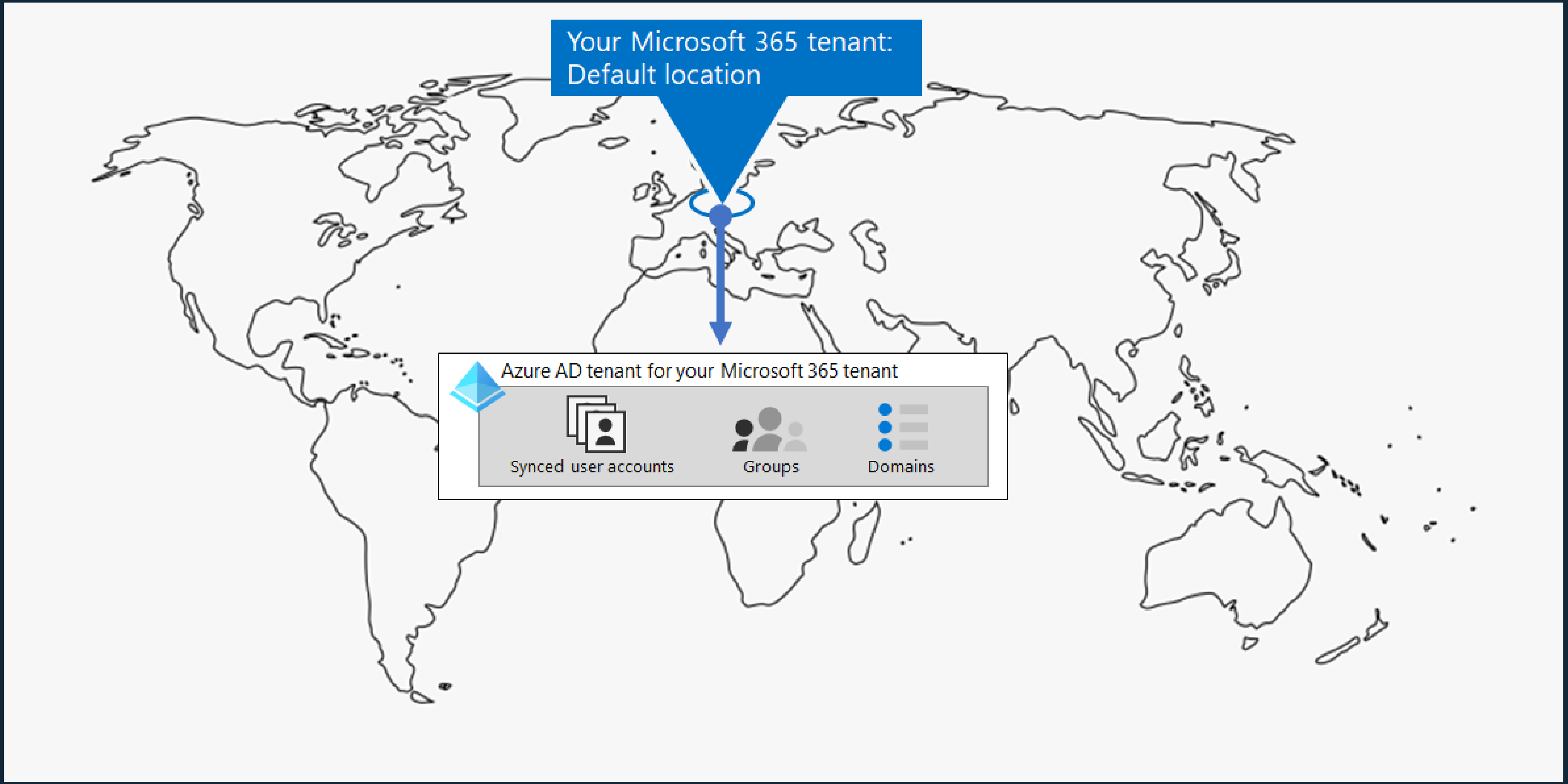
Tenant Name *	ExpertsLiveEU Rocks ✓
Domain Name *	expertsliveeurocks ✓ .onmicrosoft.com
Location	Hungary

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

First things first. Where’s my data?



Your Microsoft 365 tenant: Default location

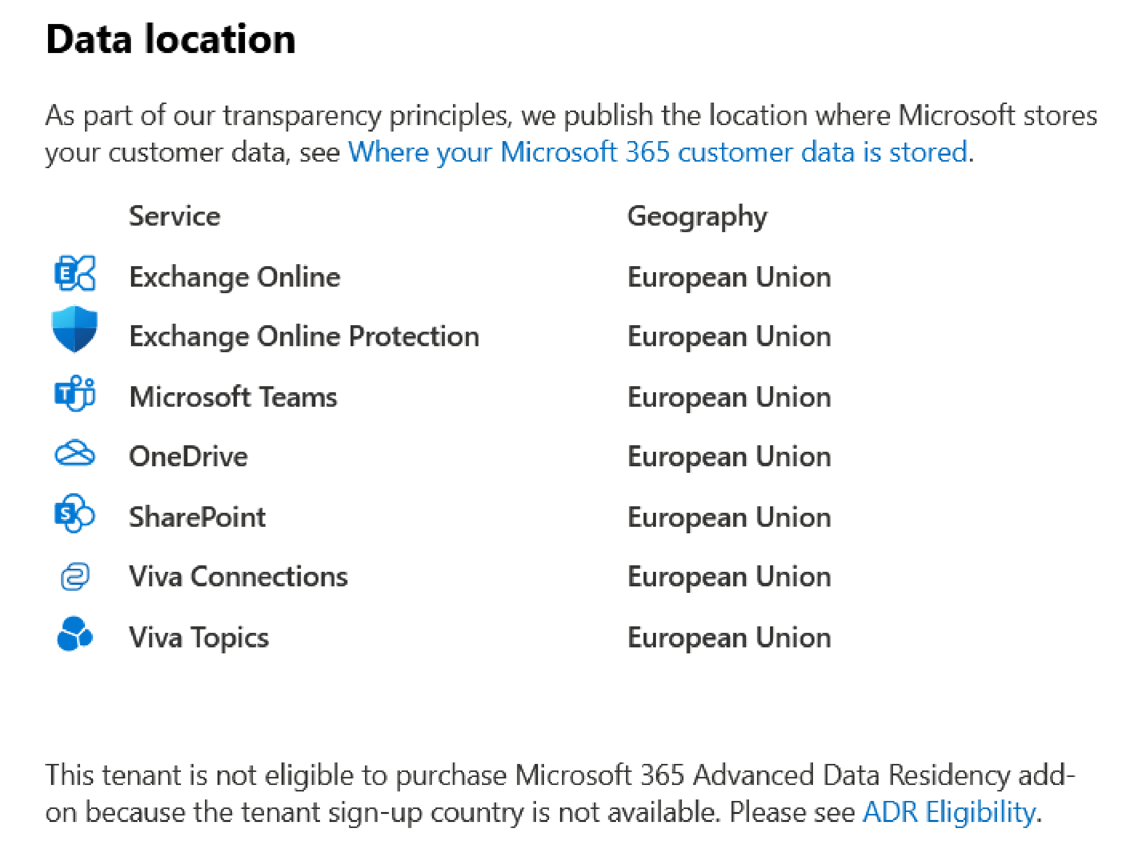
Azure AD tenant for your Microsoft 365 tenant

Data Residency primer

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

First things first. Where’s my data?

Settings > Org Settings > Organization profile > Data location



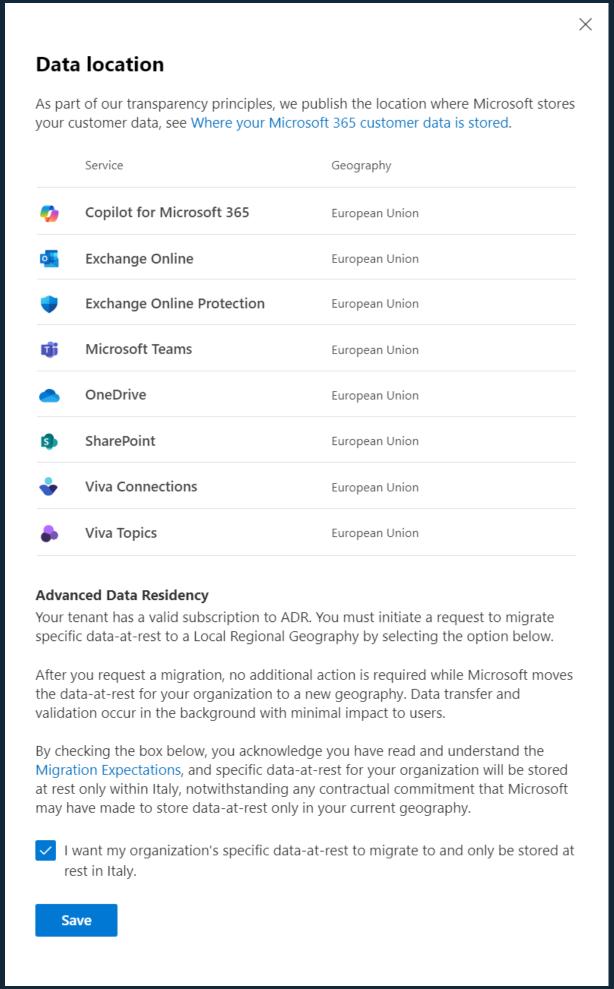
Data location

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



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.

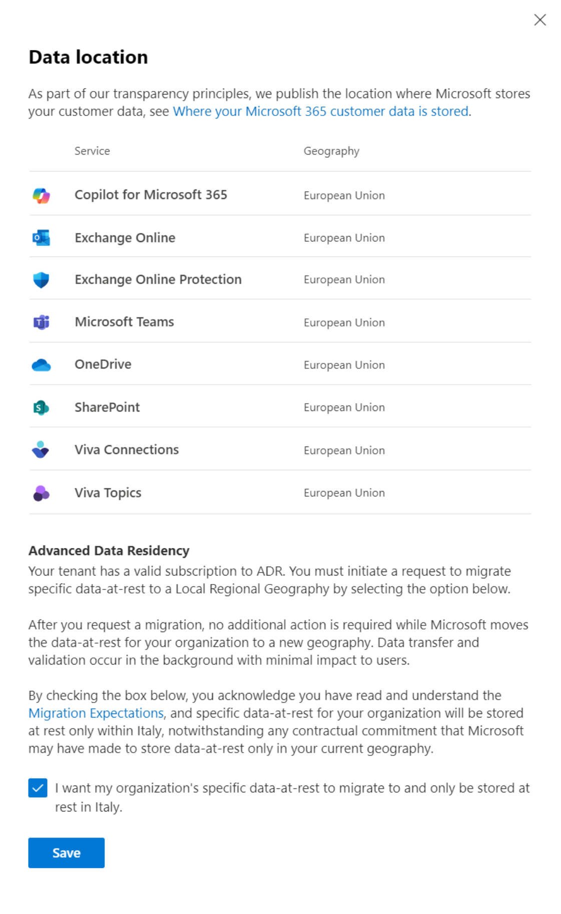
After you request a migration, no additional action is required while Microsoft moves the data-at-rest for your organization to a new geography. Data transfer and validation occur in the background with minimal impact to users.

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.

- 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



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

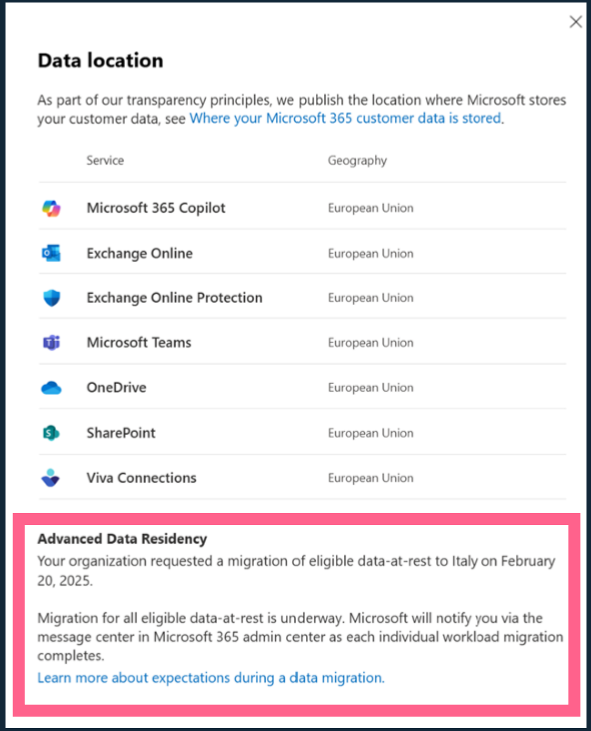
Advanced Data Residency

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.



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.

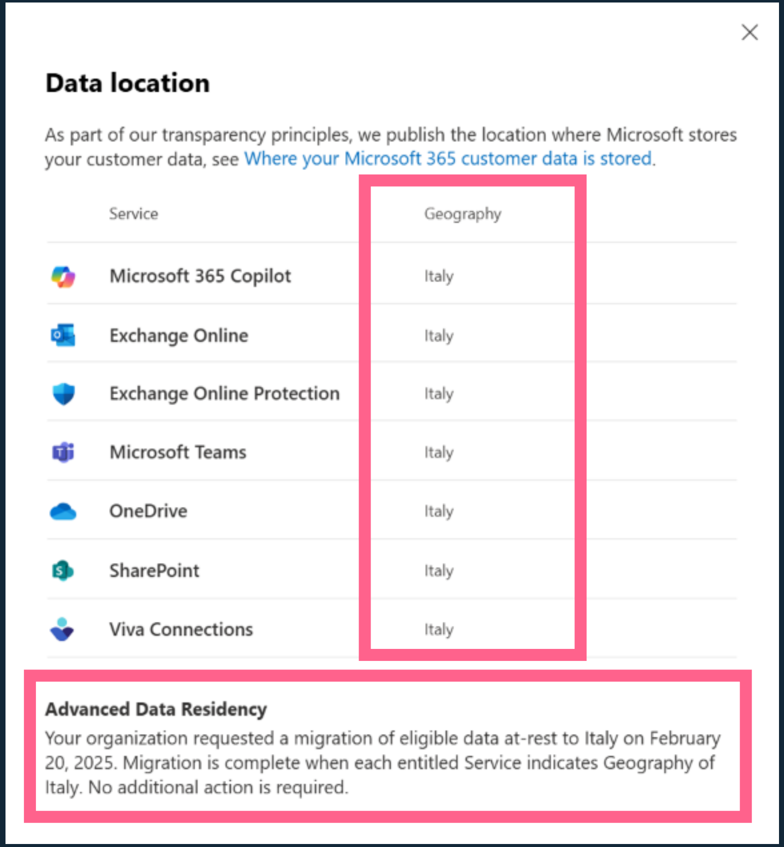
Service	Geography
Microsoft 365 Copilot	European Union
Exchange Online	European Union
Exchange Online Protection	European Union
Microsoft Teams	European Union
OneDrive	European Union
SharePoint	European Union
Viva Connections	European Union

Advanced Data Residency

Your organization requested a migration of eligible data-at-rest to Italy on February 20, 2025.

Migration for all eligible data-at-rest is underway. Microsoft will notify you via the message center in Microsoft 365 admin center as each individual workload migration completes.

Learn more about expectations during a data migration.



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

Advanced Data Residency

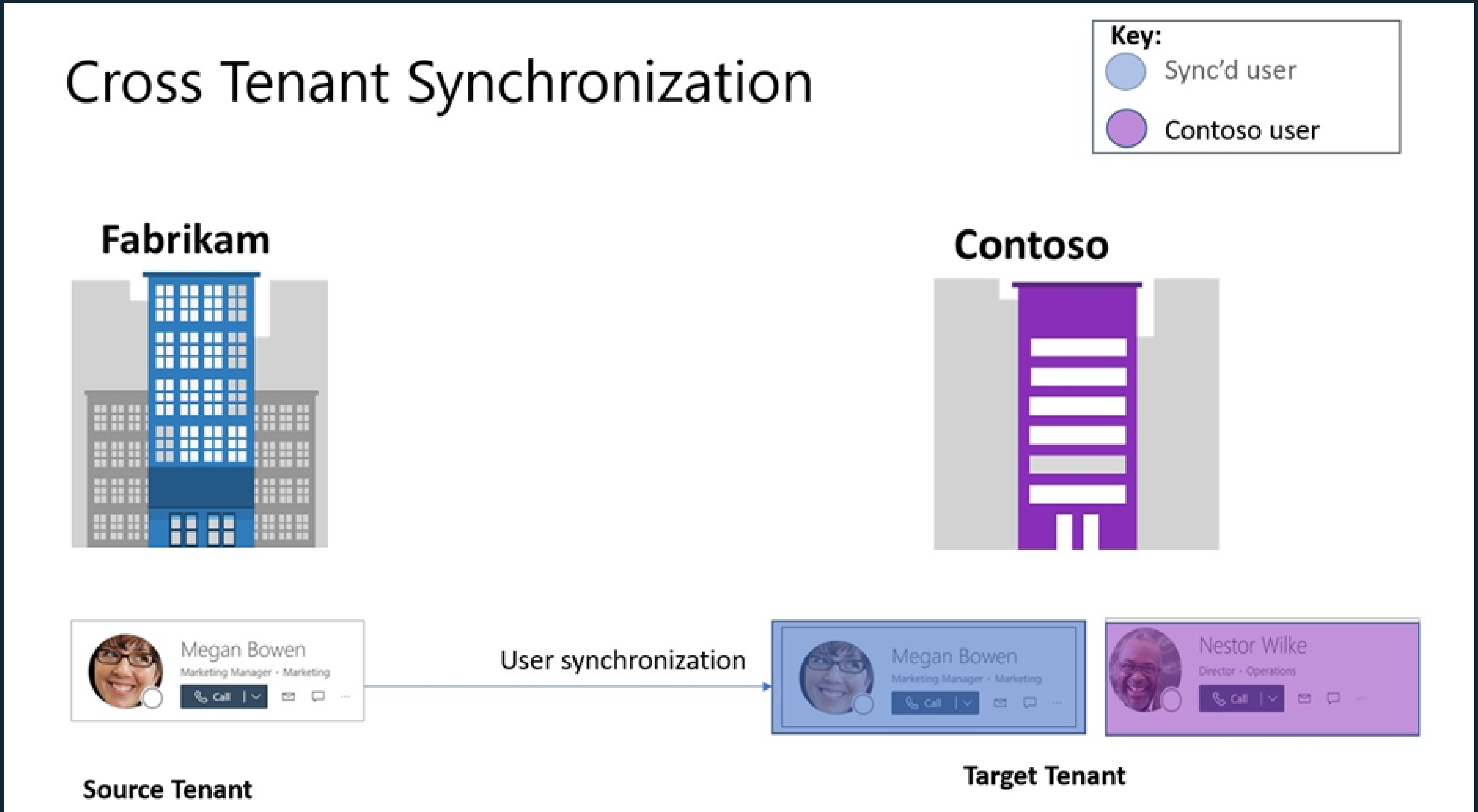
Your organization requested a migration of eligible data at-rest to Italy on February 20, 2025. Migration is complete when each entitled Service indicates Geography of Italy. No additional action is required.

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

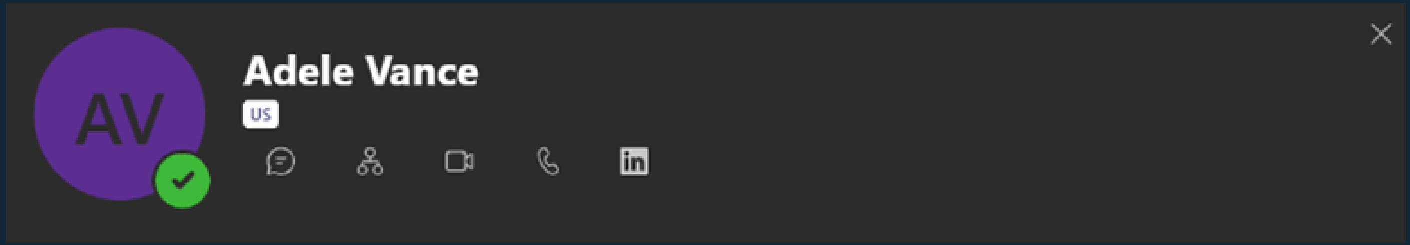
Multi-tenant

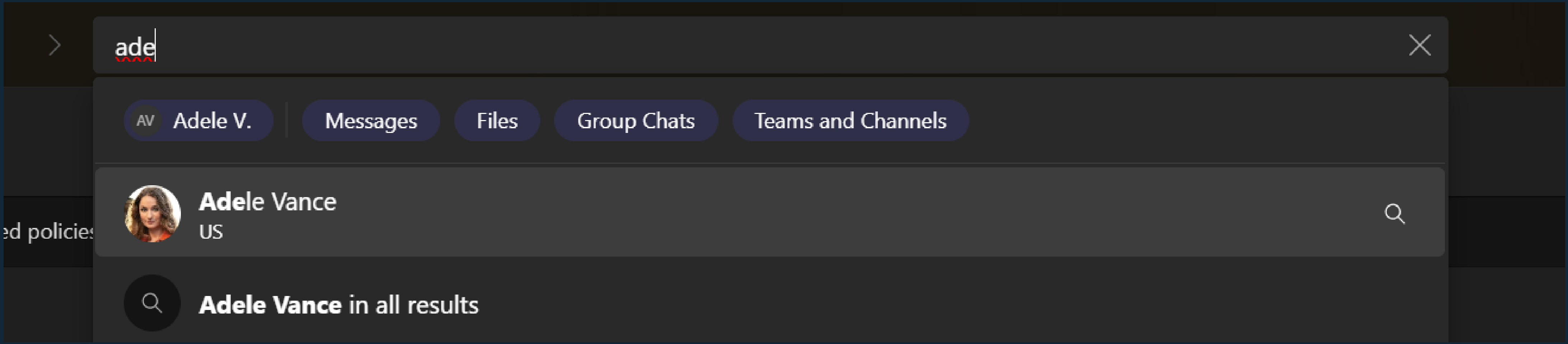


Cross Tenant Synchronization

Key:
● Sync'd user
● Contoso user

Include an optional label





ade

Multi-tenant

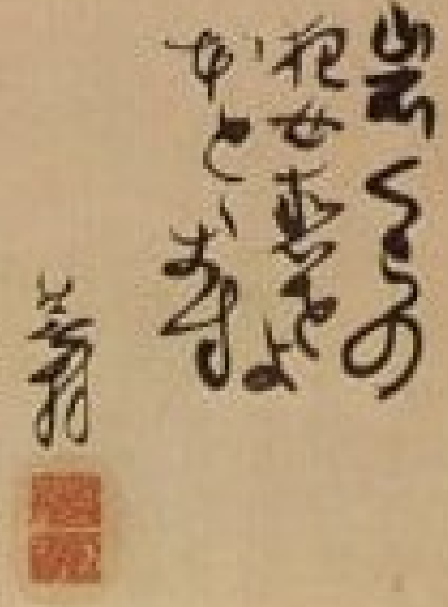
- Cross-tenant synchronization configuration is added with the name MTO_Sync_<TenantID>, but no sync jobs are created yet.
- Organization relationship is added to the cross-tenant access settings based on the multitenant organization templates for cross-tenant access and identity synchronization.
- The 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.

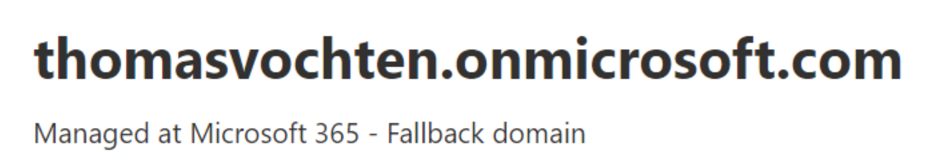
Domains, DNS & networking

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,…

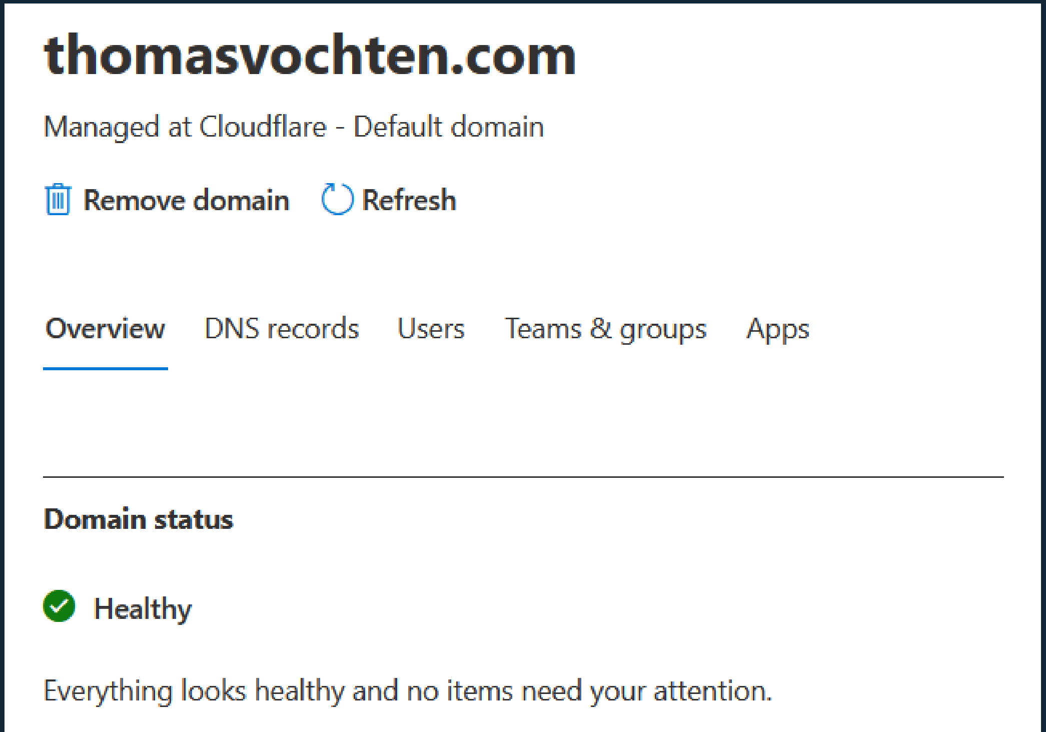
used for your SharePoint Online & OneDrive URL’s

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



thomasvochten.com

Managed at Cloudflare - Default domain

Domain status

✓ Healthy

Everything looks healthy and no items need your attention.

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

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

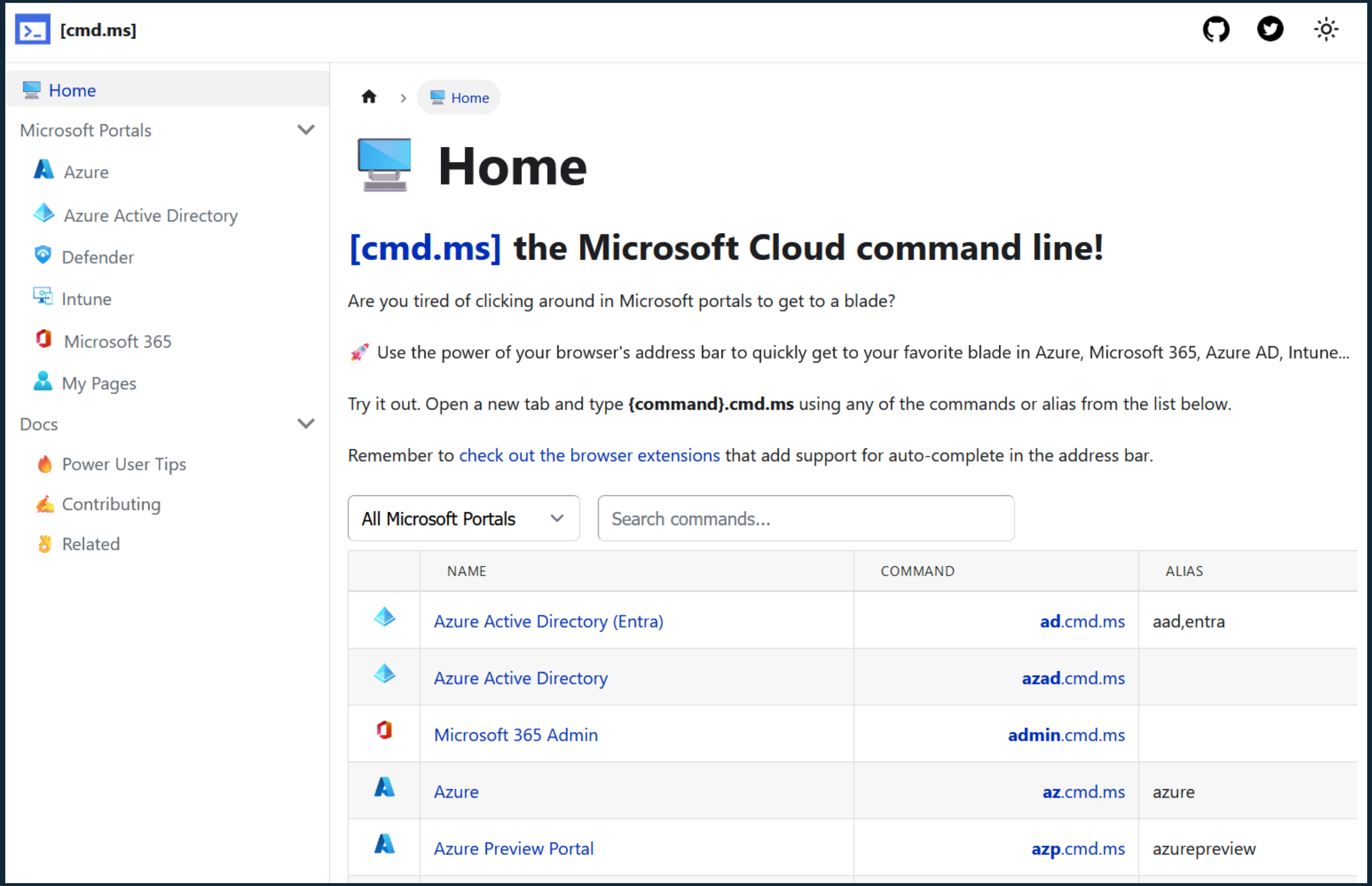
The new kid on the block

*.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.

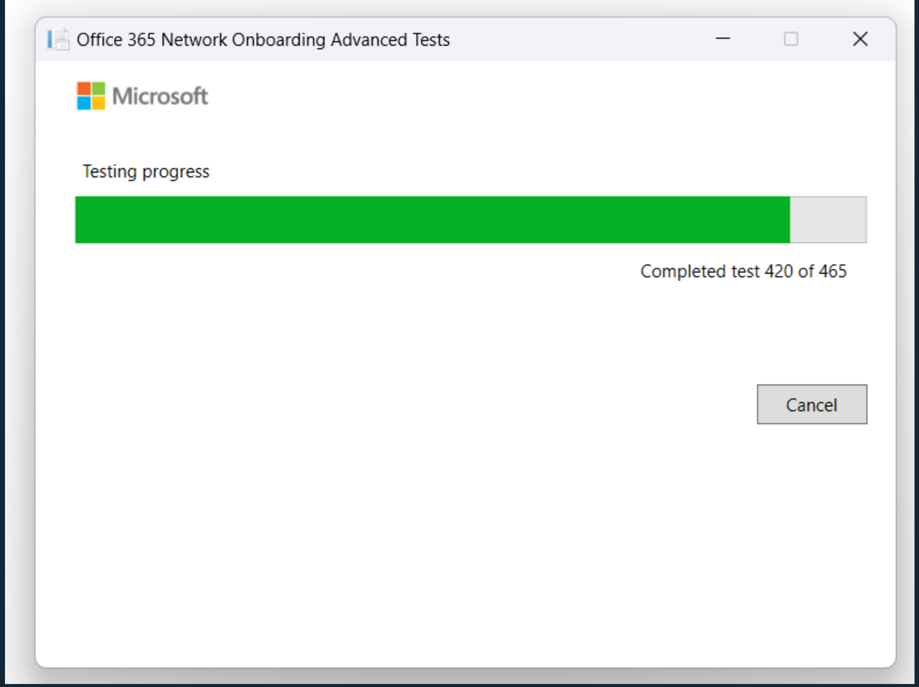
Remember to check out the browser extensions that add support for auto-complete in the address bar.

	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

Testing connectivity

Don’t assume everything will just work

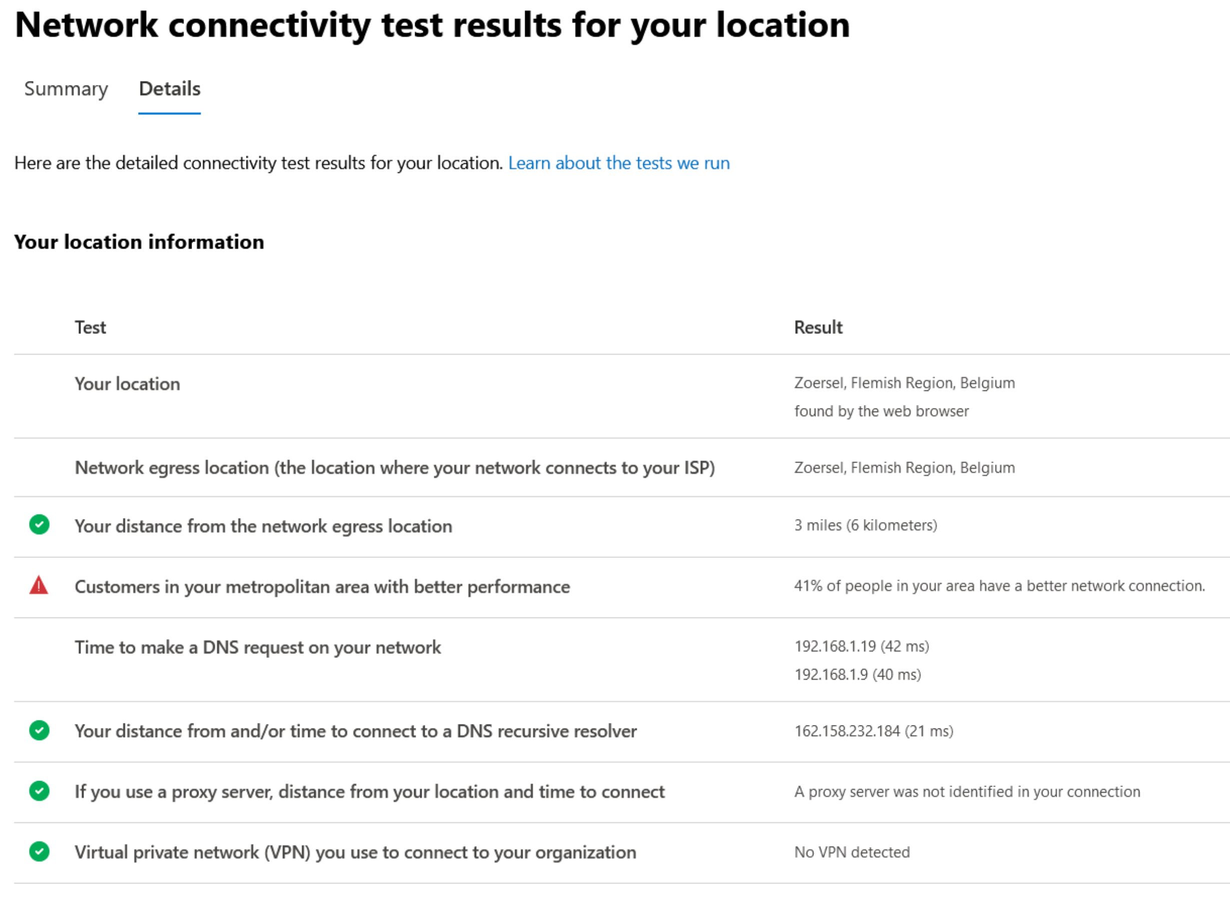
https://connectivity.office.com



Testing progress

Completed test 420 of 465

Testing connectivity



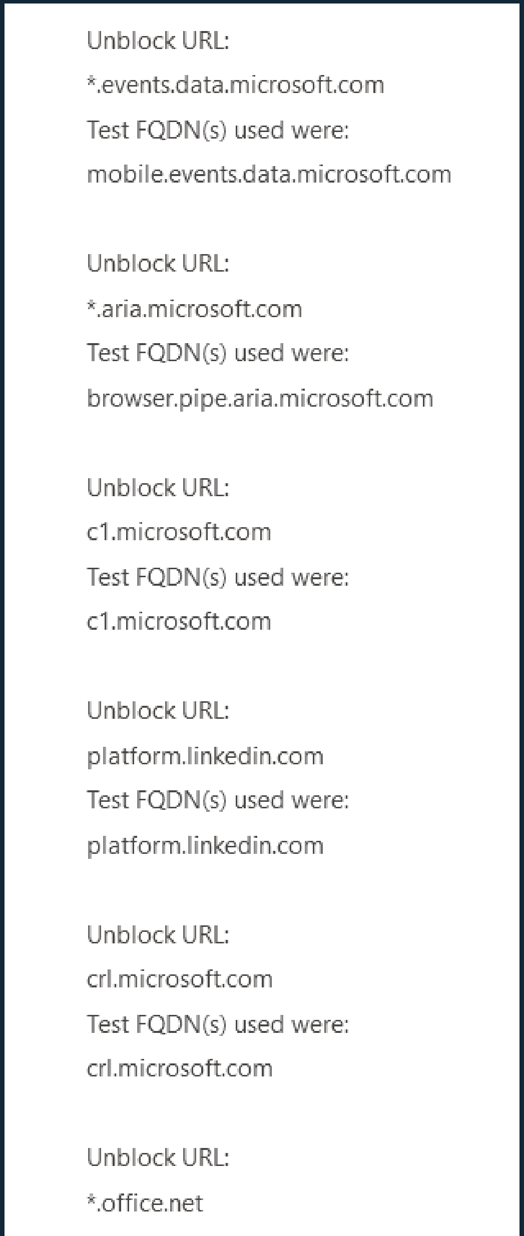
Network connectivity test results for your location

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

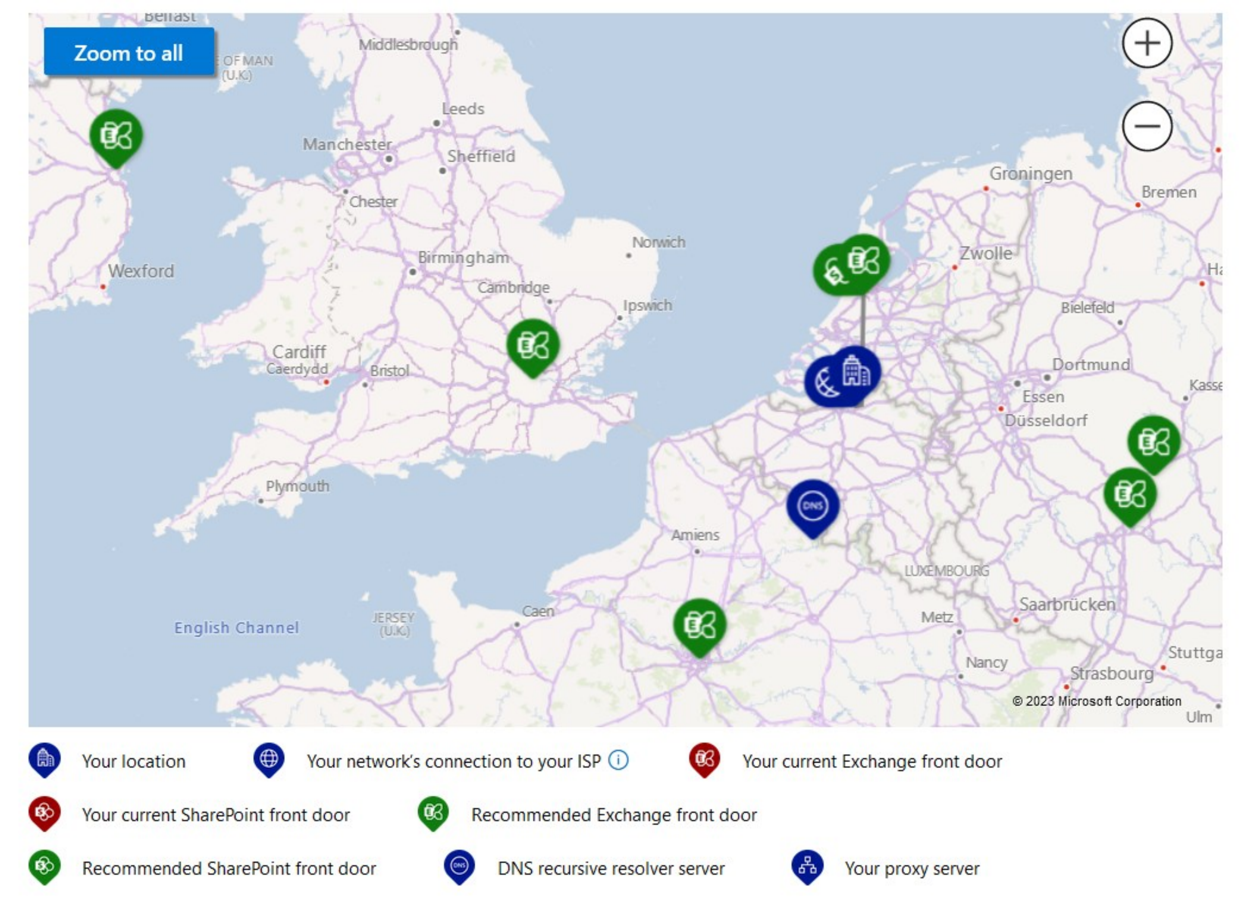
Unblock URL:
c1.microsoft.com
Test FQDN(s) used were:
c1.microsoft.com

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

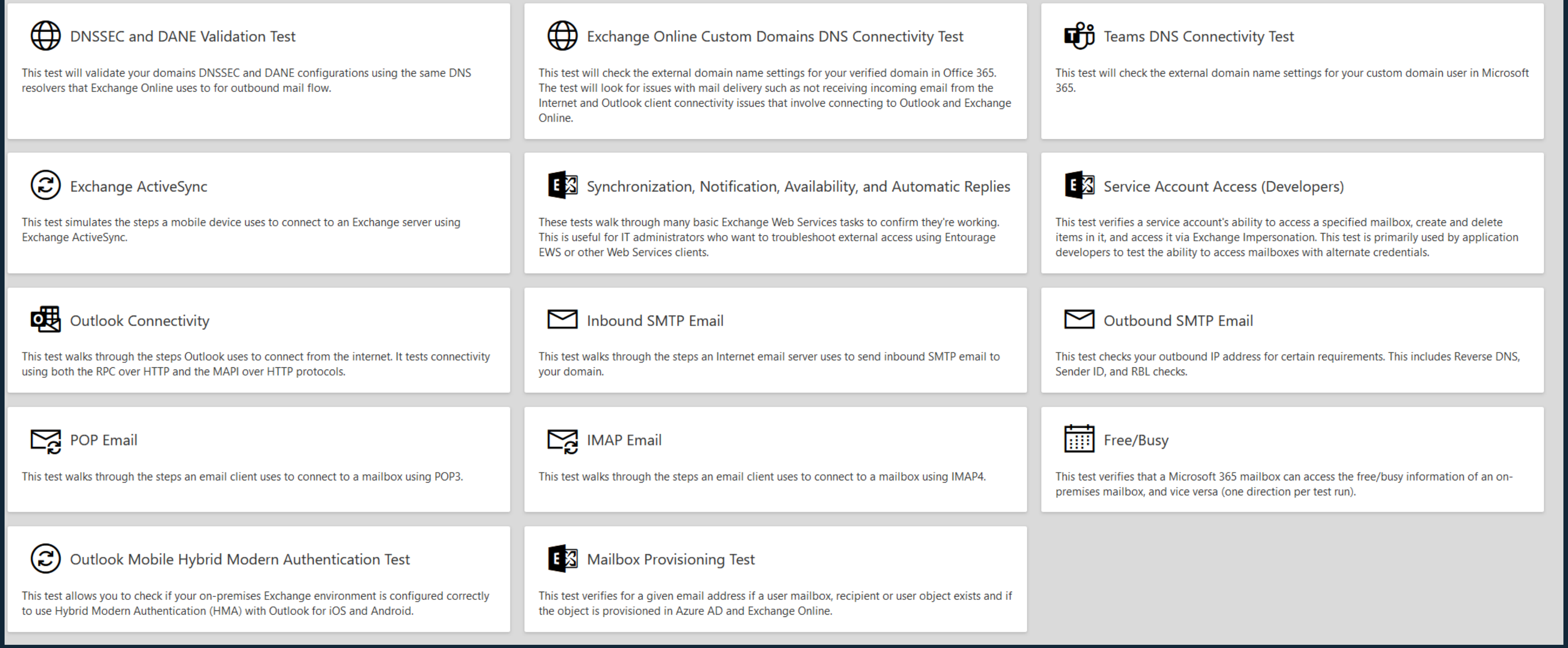
Unblock URL:
*.office.net

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.

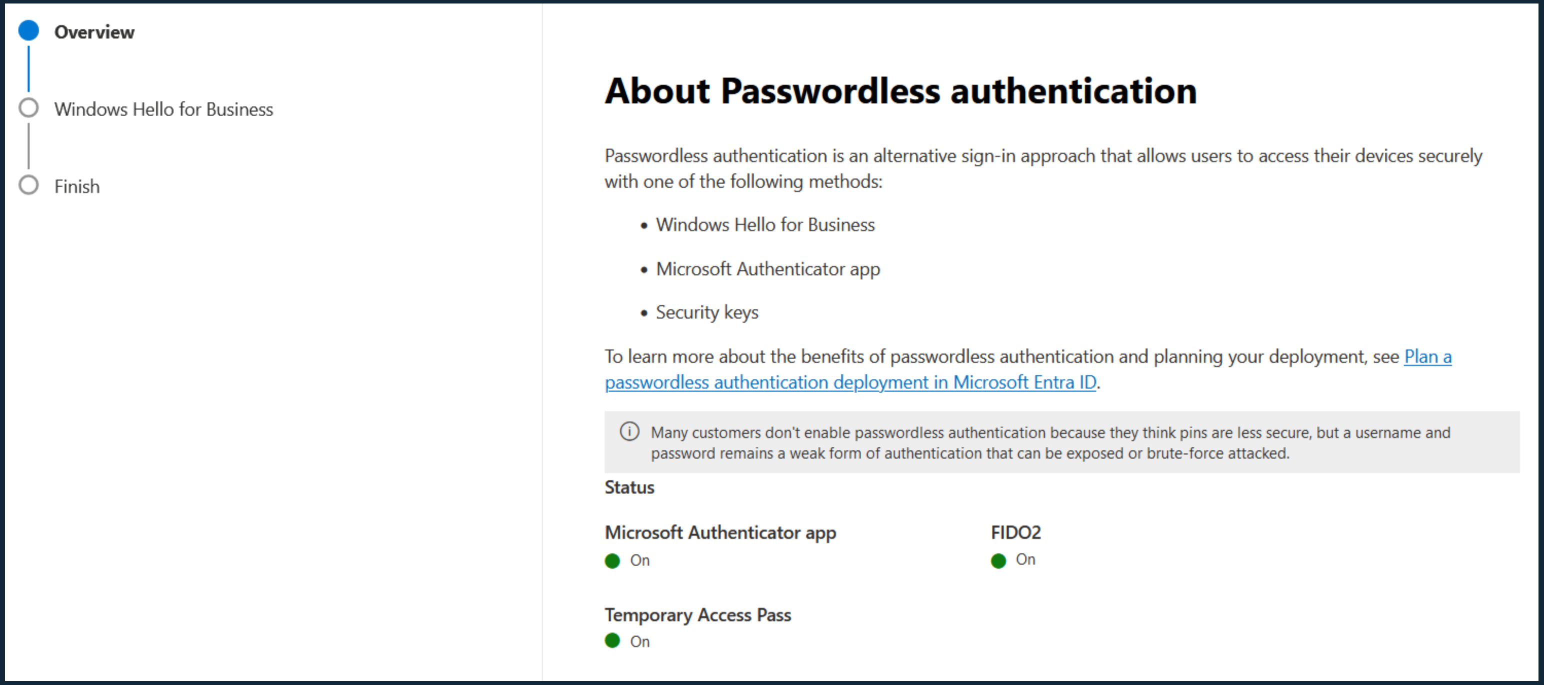
Organizational settings & advanced deployment guides

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

Takeaways

- Revisit the basics, such as data location
- Don’t dismiss foundational technologies like DNS & networking
- Multi-Geo & Multi-Tenant:
  just because you can, doesn’t mean you should
- Have a look at your organization settings regularly

Thank you

🦋 thomasvochten.com

✉ mail@thomasvochten.com