

How Not to Manage Your Microsoft 365 Tenant

And What To Do Instead

1 April 2026

CUSTOMER SUCCESS

CO-CREATE

AMBITIOUS

EXPERT

INNOVATE

Rubicon

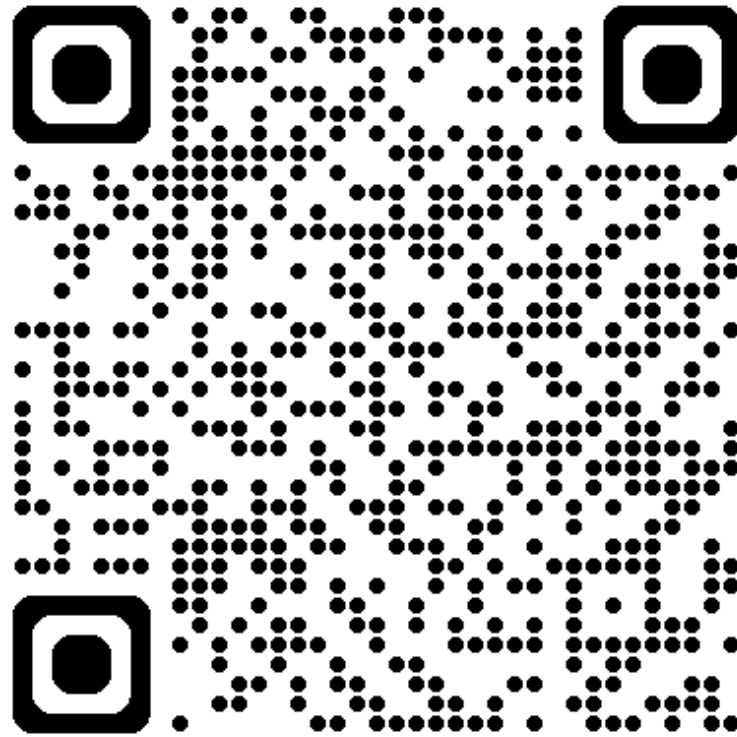
Who am I?

Dave Stork (he/him)
Cloud Architect @ Rubicon

Microsoft MVP M365 App
Microsoft Certified Trainer

d.stork@rubicon.nl
<https://davestork.nl/>
<https://bsky.app/profile/dmstork>
[@dmstork@mastodon.social](https://dmstork@mastodon.social)

Microsoft Partner



Kind request: follow me on LinkedIn!



<https://about.me/dmstork>

Rubicon

Why this session?

Things I've encountered in production environments

- Common mistakes

- Misconceptions

- Bad practices

- Unknown new features & methods

High over point by point

- | Discussing Users & Objects, Administration and Configuration

Feel free to interact and provide feedback!

Sources:

Admin account security in Microsoft 365 for business

Best practices for Microsoft Entra roles

Microsoft Partner

Rubicon

User & Objects

CUSTOMER SUCCESS

CO-CREATE

AMBITIOUS

EXPERT

INNOVATE

Rubicon

How not to manage...

Users & Objects

Incorrect licensing

Why not?

You are not license compliant, which is a legal issue

Some features are tenant wide active, but you still need to have the correct amount of licenses in possession: *if you benefit from a feature, you pay for a feature**

What to do?

Use Group based licensing and use it in user provisioning

Talk to a Microsoft licensing expert and get things in writing

Exclude accounts from tenant wide features explicitly (e.g. Defender for Office 365 P2).

Shared Mailboxes that can authenticate require at least Exchange Online P1

* Office 365 for IT Pros: Microsoft Issues Updated Guidance for Defender for Office 365 Licensing

How not to manage...

Users & Objects

Default domain is not custom

Why not?

MOERA domain has limits

Often not properly authenticated (SPF, DKIM, DMARC)

What to do?

Change default domain

Correct primary SMTP address on existing objects: Shared Booking, Distribution Groups, Mail enabled Public Folders *ducks* etc.

| Limiting Onmicrosoft Domain Usage for Sending Emails

How not to manage...

Users & Objects

Handing over admin created passwords to users

Why not?

Password is now known by at least two people

Require password change, which is sometimes difficult to enforce

What to do?

Use Temporary Access Pass (TAP) with an appropriate expiration time (probably requires multiple use)

Admin hands-over TAP, let user register MFA and then do SSPR (if needed)

Might need to enable Web-signin for Windows

How not to manage...

Users & Objects

No Lifecycle Management & governance

Why not?

Objects and permissions are retained beyond their use

What to do?

Have a policy (personas) and process in place

Use Access Reviews (Entra P2) and/or Entra Life Cycle Management (Entra Suite)

Sync all objects from AD

Why not?

Adds complexity to objects and their management due to dependency on AD

What to do?

Sync only objects that require an instance on-prem and in cloud

If a synced object is no longer required on-prem, change Start-of-Authority

Change Start-of-authority of Exchange attributed for hybrid users

Adminstrators

CUSTOMER SUCCESS

CO-CREATE

AMBITIOUS

EXPERT

INNOVATE

Rubicon

Administrators

Permanent Active Permissions

Why not?

Security risk

What to do?

Use PIM (yes, costs Entra ID P2), best with approval

Least privilege (built-in or with custom)

Admins synced from AD

Why not?

Lateral movement

Dependency on AD

What to do?

Separate AD and Entra accounts

Azure Bastion

Microsoft Partner

Administrators

No break-glass accounts

Why not?

In case of misconfiguration or other issues and normal admin accounts are accidentally prohibited access or elevation.

What to do?

Two inconspicuous cloud accounts

Permanent exclusion of Conditional Access & active Global Admin role

Monitoring and alerting

Process for activation

Do not forget AD!

How not to manage...

Administrators

Admin accounts with focus on passwords

Why not?

Passwords are legacy

What to do?

Passkeys & Authentication Strength

Admins do not know their password

Because you might still need password: Assign explicit SSPR to admin accounts (when using PIM)

Create exception group for Authentication Strength Conditional Access policy via PIM

Rotate passwords every x days (Azure function)

How not to manage...

Administrators

Admins with custom domain

Why not?

What if the domain expires, is compromised or there is a company name change?

Any domain dependency (e.g. VPN MFA authentication)

Tenant 2 tenant migration with domain relocation

What to do?

Use MOERA domain e.g. <tenant>.onmicrosoft.com

You can create up to 4 additional MOERA domains

How not to manage...

Administrators

Admin account with mailbox

Why not?

Phishing risks on accounts with potential high privileges (even with MFA)

What to do?

Use plus forwarding
Create dedicated admin mail addresses

Mail flow settings

Manage your organization's settings for sending and receiving messages.

General

☐ Turn off plus addressing for your organization. [Learn more](#)

Admin Istrator

Properties



Refresh



Got feedback?

Controls

Settings

On-premises

Zip or postal code

Country or region

NL

Business phone

Mobile phone

063

Email

dmstork+admin@stalpaert.nl

Other emails

d.storkl

Microsoft Partner

Rubicon

Configuration

CUSTOMER SUCCESS

CO-CREATE

AMBITIOUS

EXPERT

INNOVATE

Rubicon

How not to manage...

Configuration

Not using your tenant's Message Center

Why not?

Contains tenant specific notifications for new features, deprecations and (breaking) changes

What to do?

Use Message Center, with Custom View and/or Mail Notifications

Optionally use Planner for tasks & assigning them

Alternative: Microsoft 365 Message Center Archive <https://mc.merill.net/>

How not to manage...

Config

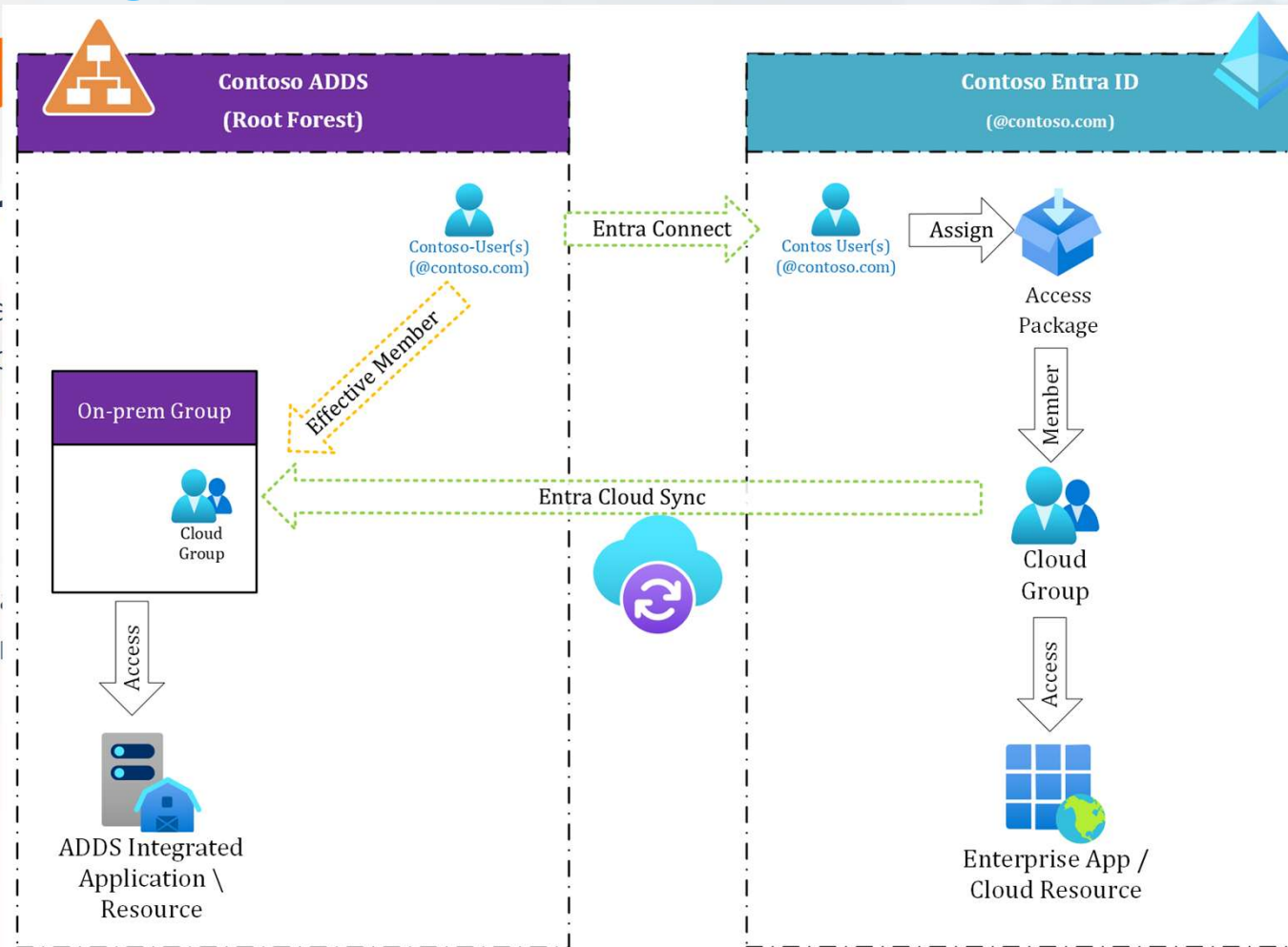
Still using Entra

Why not?

No new investment
Relatively large footprint
No real high availability

What to do?

Use Entra Cloud
Is the future forward
Has supported global



How not to manage...

Configuration

Click-ops vs DevOps (IaC)

Why not Click-ops?

There is no documentation

Hard to perform configuration drift detection

No backup of your configuration

What to do?

Microsoft 365 DSC

Native: Entra Tenant Governance Preview

| Microsoft Entra Tenant Governance: Secure and manage multi-tenant environments at scale

How not to manage...

Configuration

No Need for Backup in the cloud

Why not?

You are still responsible for your own data
Configuration is data

What to do?

See Click-ops vs DevOps (IaC)
Entra ID Backup in preview

| [Microsoft Entra Backup and Recovery overview \(Pr](#)
Microsoft 365 Backup or vendor using Microsoft API capabilities
Do not rely on Exchange Web Services!

	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	Customer	Customer	Customer	Customer
	Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
	Accounts and identities	Customer	Customer	Customer	Customer
Responsibility varies by type	Identity and directory infrastructure	Shared	Shared	Customer	Customer
	Applications	Microsoft	Shared	Customer	Customer
	Network controls	Microsoft	Shared	Customer	Customer
	Operating system	Microsoft	Customer	Customer	Customer
Responsibility transfers to cloud provider	Physical hosts	Microsoft	Microsoft	Customer	Customer
	Physical network	Microsoft	Microsoft	Customer	Customer
	Physical datacenter	Microsoft	Microsoft	Customer	Customer

Microsoft Customer Shared

What did you encounter?

CUSTOMER SUCCESS

CO-CREATE

AMBITIOUS

EXPERT

INNOVATE

Rubicon