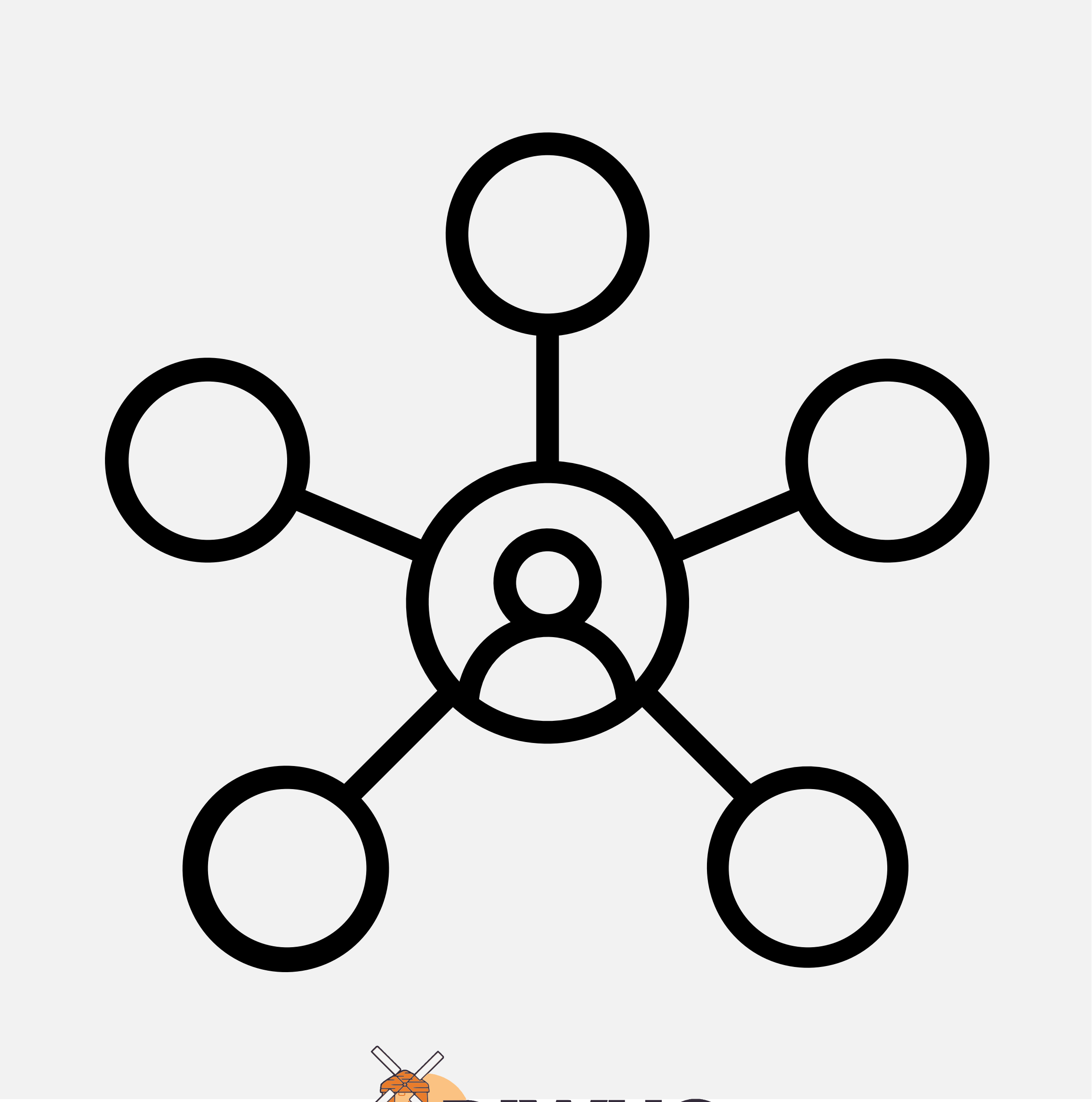
Automated self-service user management

Stefan Strube

Solution architect



Strukton

DIWUG

Stefan Strube

MVP Microsoft® Most Valuable Professional

- Solution architect @ Strukton (NL)
- Microsoft Business Applications MVP
- Co-founder PowerAddictsNL user group

POWERADDICTSNL • POWERADDICTSNL •

2die4it.com

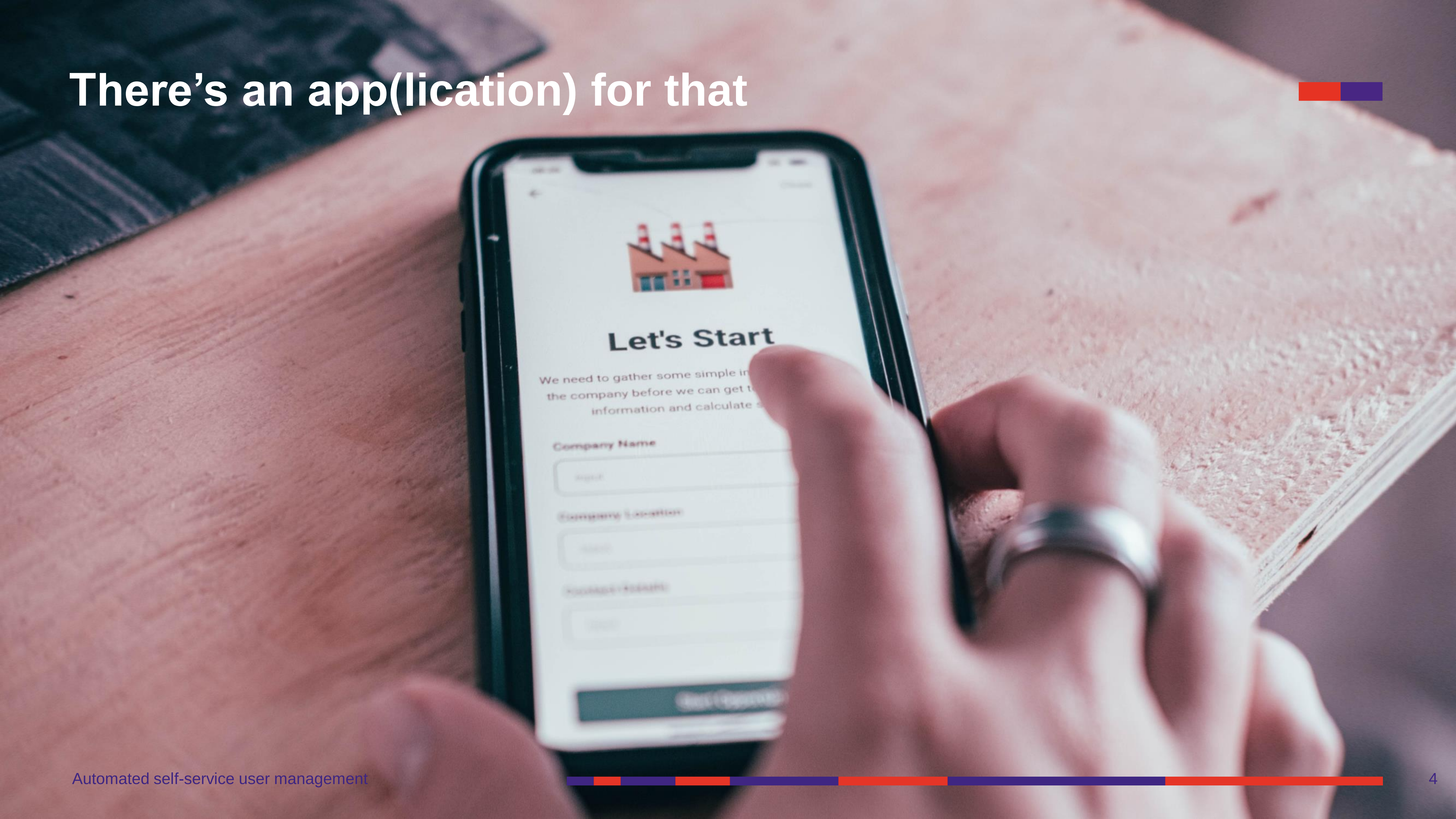
@StefanS365

stefanstrube365

Power Platform experience? ✋

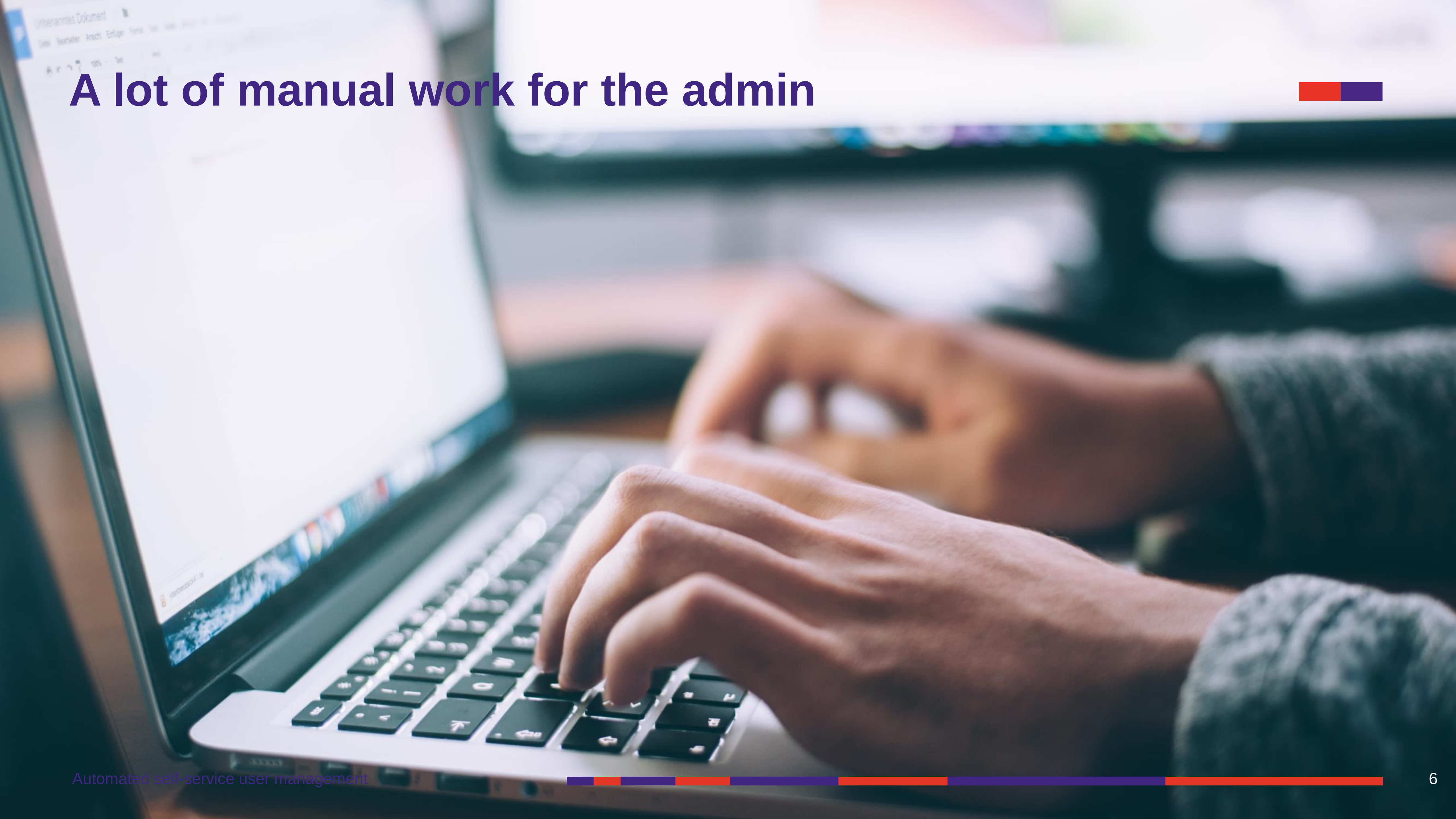
- Canvas apps
- Dataverse as data source
- Model-driven apps
- User management in Dataverse

There’s an app(lication) for that

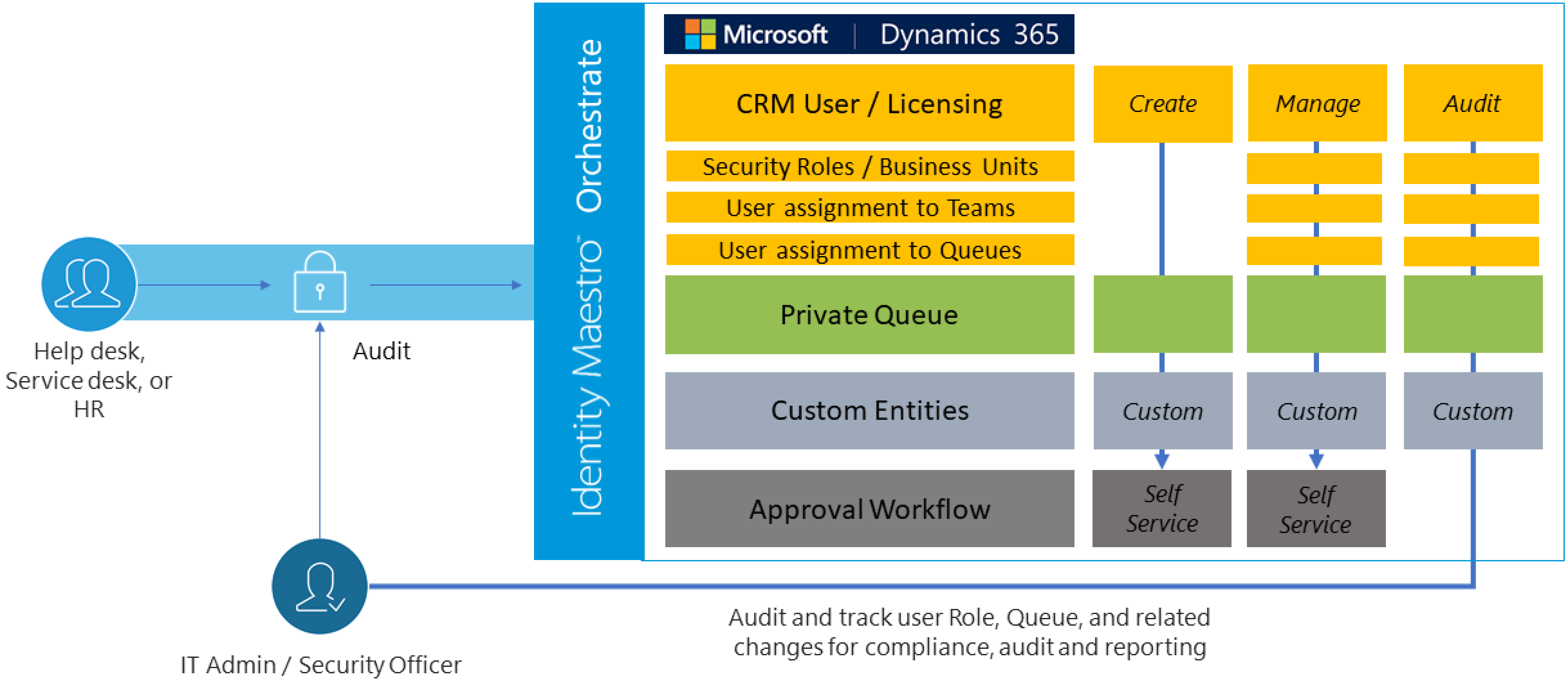

Let's Start
We need to gather some simple in
the company before we can get t
information and calculate s
Company Name
Company Location
Contact Details

User management

A lot of manual work for the admin



Third party tools



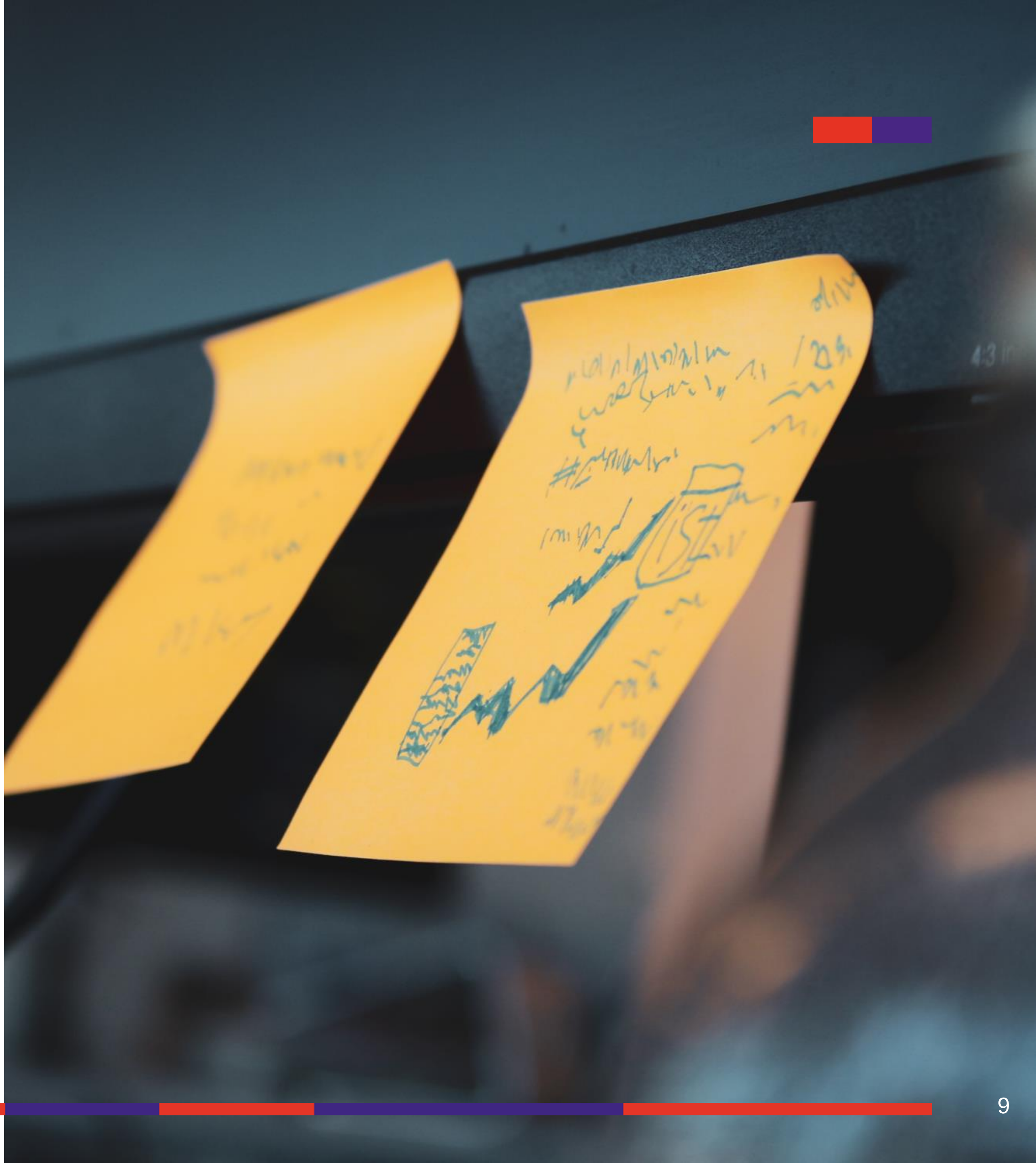
Audit and track user Role, Queue, and related changes for compliance, audit and reporting

Agenda

- User management
- Best practice
- JIT access
- User profile
- Automation
- Wrap up

Input for user management

- Joiners-Movers-Leavers (JML) process, tool
- Business processes
- Self-service



User management

- (Guest) User account in Azure AD
- License(s)
- Access to Dataverse environment(s)
- Access to app(s)
- Access to data source(s)
- Organization-based, role-based functionality

  → Business process flows, forms, views
- Personalized UX (personal user settings)
- Mailbox: approve, test & enable

Best practice: Group-based “everything”

- Group-based licensing
- Group-based access to
  - → Environment(s)
  - → App(s)
  - → Data source(s)
- Group-based security role(s)
  - → Organization-based, role-based functionality

Dataverse: SharePoint integration

- No sync of permissions
- Group-based access to

  → Data source: Dataverse

  → Data source: SharePoint

Dynamics 365: Teams integration

- No sync of permissions
- Group-based access to

  → Data source: Dynamics 365 (Dataverse)

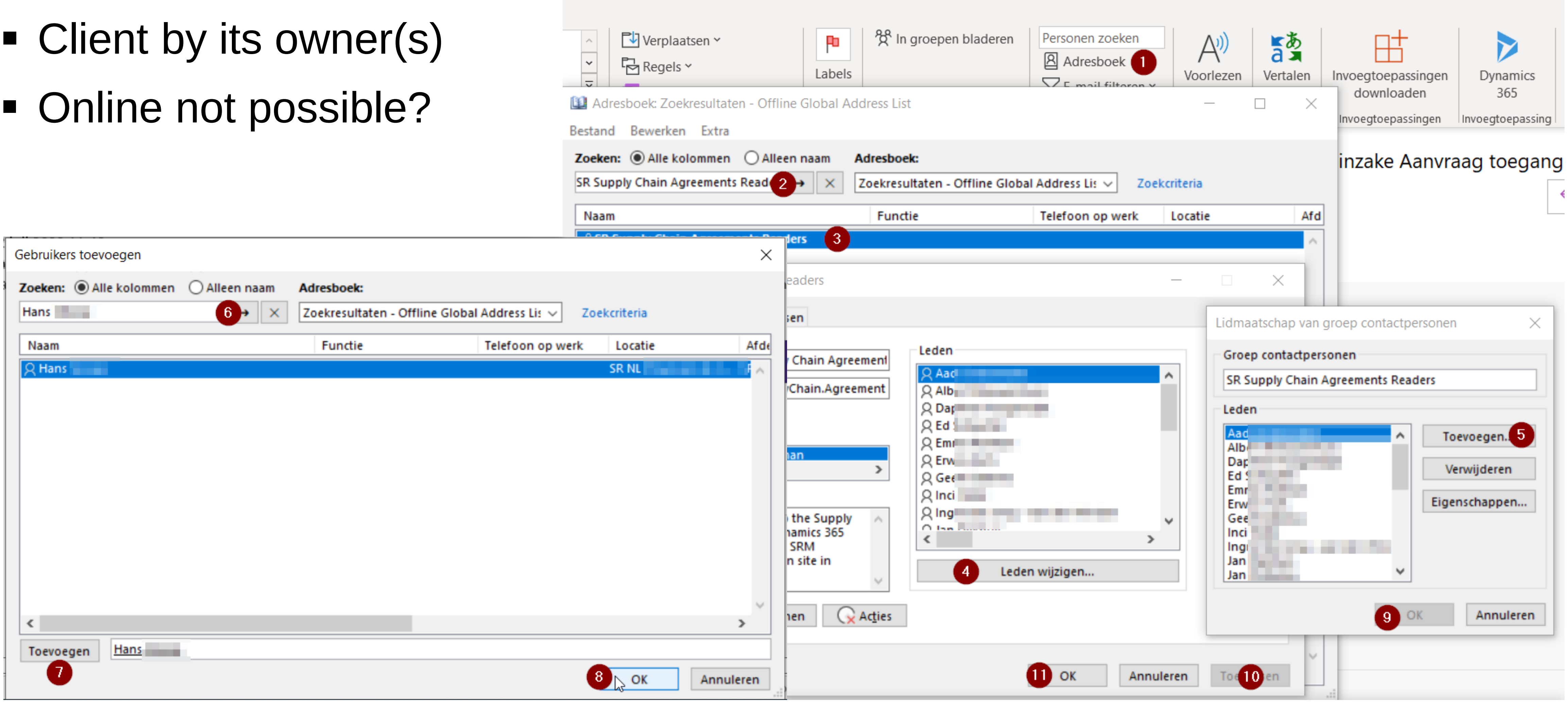
  → Data source: Teams (SharePoint)

Azure AD & Microsoft 365 group types

Support for	Security group		Mail-enabled security group	Microsoft 365 group	
Membership	Assigned	Dynamic[1]	Assigned	Assigned	Dynamic[1]
Group-based licensing[1]	🟩	🟩	🟩	🟩 securityEnabled=TRUE	
Group membership	🟩	🟩	🟩	🟥	🟥
Self-service	🟩 [1]	N/A	🟩	🟩	N/A
Dataverse group team	🟩	🟩	🟩	🟩	🟩
Email address	🟥	🟥	🟩	🟩	🟩
Event triggers	Webhook		Webhook	Connector	
[1]Azure AD Premium P1	🟩 🟥	🟩	🟩 🟥	🟩 🟥	🟩

Mail-enabled security group self-service via Outlook

- Client by its owner(s)
- Online not possible?

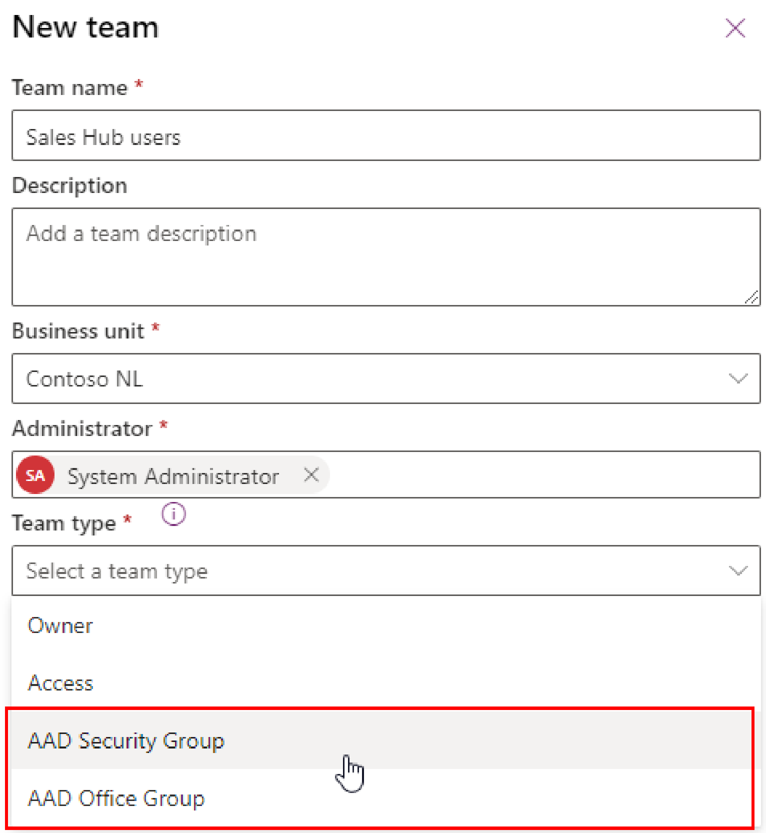


Dataverse group teams

- AAD Security Group
- AAD Office Group

- Differentiate:
  → Owner
  → Member
  → Guest

- Modernized Business Units (GA)



New team

Team name *
Sales Hub users

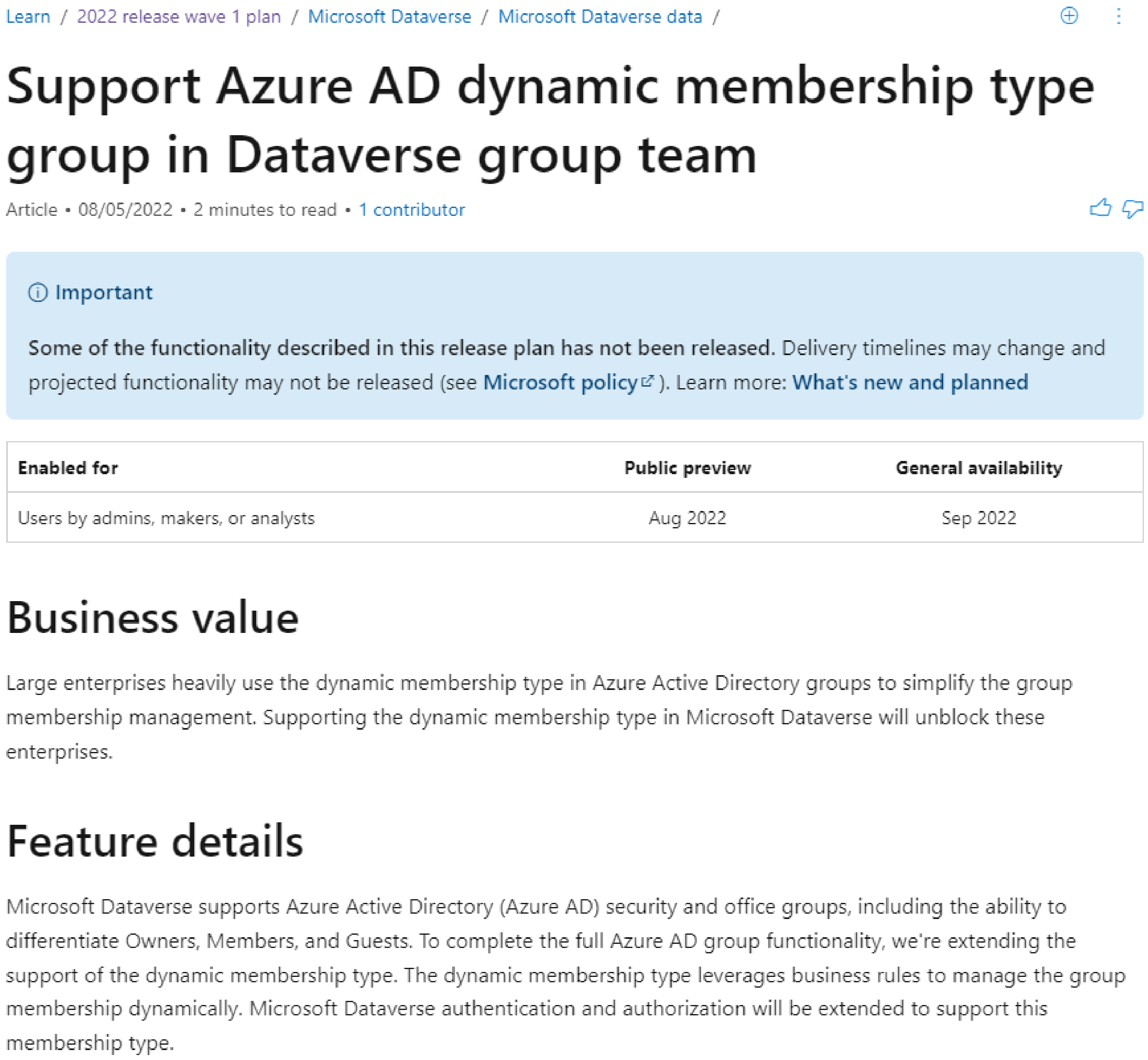
Description
Add a team description

Business unit *
Contoso NL

Administrator *
SA System Administrator

Team type *
Select a team type

Owner
Access
AAD Security Group
AAD Office Group



Learn / 2022 release wave 1 plan / Microsoft Dataverse / Microsoft Dataverse data /

Support Azure AD dynamic membership type group in Dataverse group team

Article • 08/05/2022 • 2 minutes to read • 1 contributor

ⓘ Important

Some of the functionality described in this release plan has not been released. Delivery timelines may change and projected functionality may not be released (see Microsoft policy). Learn more: What's new and planned

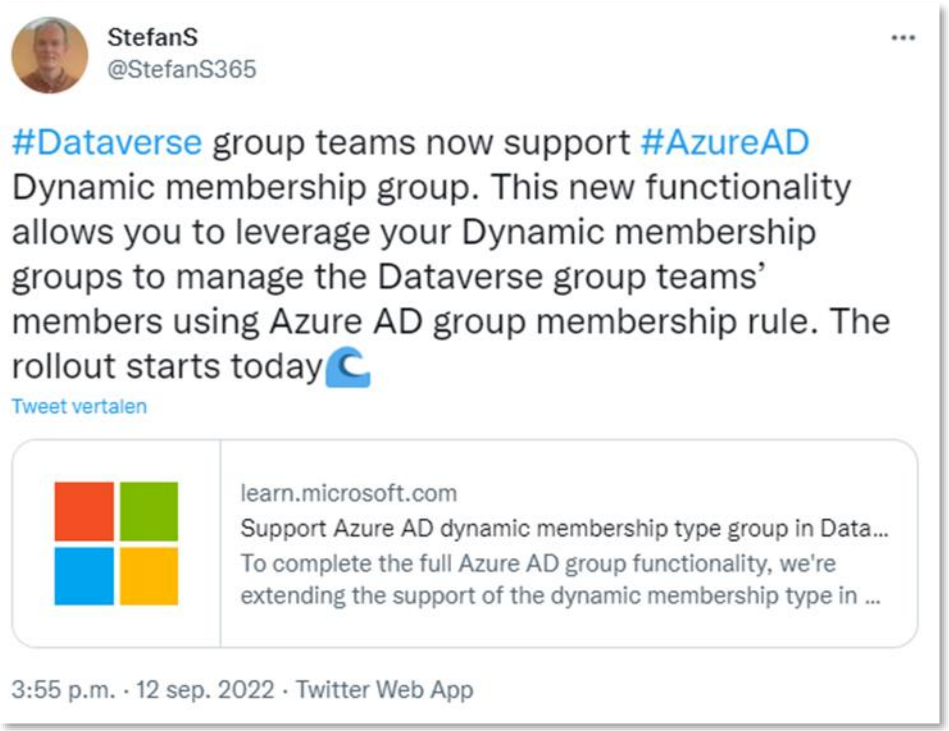
Enabled for	Public preview	General availability
Users by admins, makers, or analysts	Aug 2022	Sep 2022

Business value

Large enterprises heavily use the dynamic membership type in Azure Active Directory groups to simplify the group membership management. Supporting the dynamic membership type in Microsoft Dataverse will unblock these enterprises.

Feature details

Microsoft Dataverse supports Azure Active Directory (Azure AD) security and office groups, including the ability to differentiate Owners, Members, and Guests. To complete the full Azure AD group functionality, we're extending the support of the dynamic membership type. The dynamic membership type leverages business rules to manage the group membership dynamically. Microsoft Dataverse authentication and authorization will be extended to support this membership type.



StefanS
@StefanS365

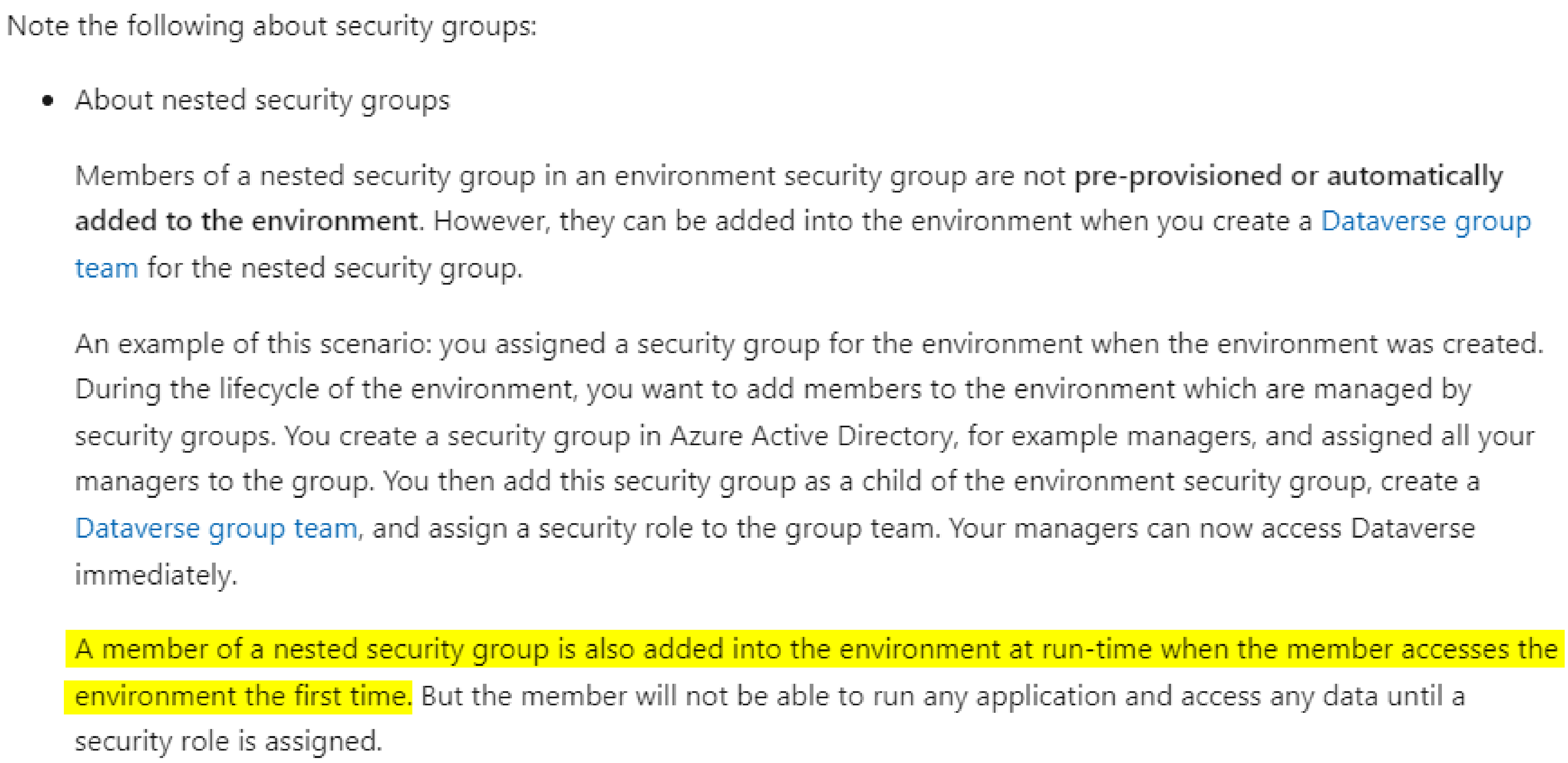
#Dataverse group teams now support #AzureAD Dynamic membership group. This new functionality allows you to leverage your Dynamic membership groups to manage the Dataverse group teams' members using Azure AD group membership rule. The rollout starts today🌊

Tweet vertalen

learn.microsoft.com
Support Azure AD dynamic membership type group in Data...
To complete the full Azure AD group functionality, we're extending the support of the dynamic membership type in ...

3:55 p.m. · 12 sep. 2022 · Twitter Web App

Just-in-time access



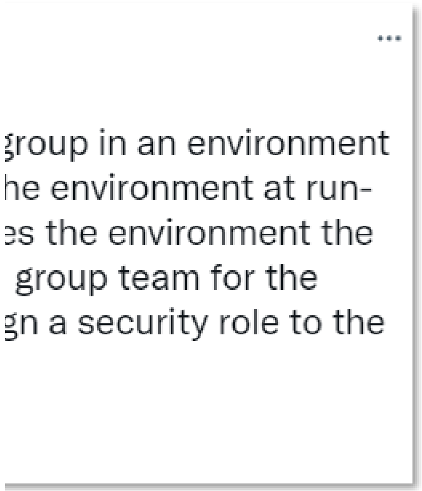
Note the following about security groups:

- About nested security groups

  Members of a nested security group in an environment security group are not **pre-provisioned or automatically added to the environment**. However, they can be added into the environment when you create a Dataverse group team for the nested security group.

  An example of this scenario: you assigned a security group for the environment when the environment was created. During the lifecycle of the environment, you want to add members to the environment which are managed by security groups. You create a security group in Azure Active Directory, for example managers, and assigned all your managers to the group. You then add this security group as a child of the environment security group, create a Dataverse group team, and assign a security role to the group team. Your managers can now access Dataverse immediately.

  A member of a nested security group is also added into the environment at run-time when the member accesses the environment the first time. But the member will not be able to run any application and access any data until a security role is assigned.



group in an environment
he environment at run-
es the environment the
group team for the
gn a security role to the

Force Sync user

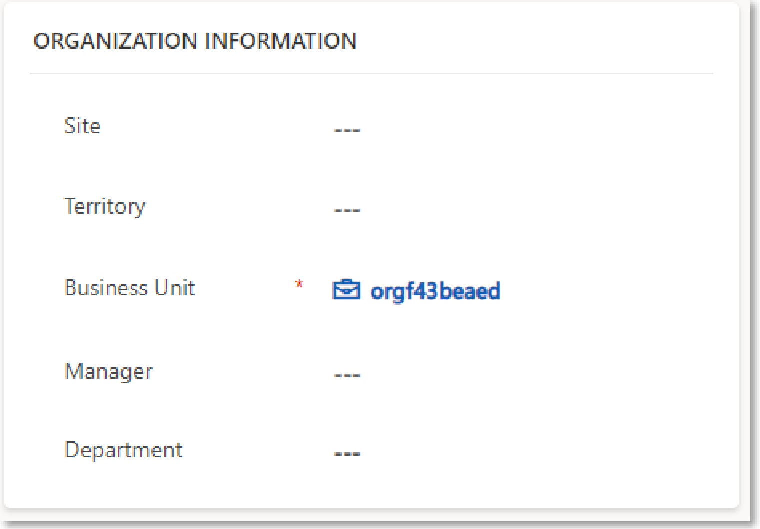
- User interface:
  Power Platform admin center > Environment > Users: + Add user
- Power Automate flow action (Power Platform for Admins connector)
- PowerShell cmdlet Add-AdminPowerAppsSyncUser
- Web API request with impersonation

User profile fields are synchronized to Dataverse

Customer engagement apps user form	Microsoft 365/Azure AD user
User Name	Username
Full Name	First name + Last name
Title	Job title
Primary Email*	Email
Main Phone	Office phone
Mobile Phone	Mobile phone
Fax	Fax number
Address	Street address
Address	City
Address	State or province
Address	Country or region
AzureActiveDirectoryObjectId**	ObjectId

Need for extended user profile

- Full name = First name + Middle name + Last name
- Manager-based logic, security (approvals, hierarchy security)
- Assign to Business Unit
- Assign to Territory
- Assign to Site
- Use Employee ID as key

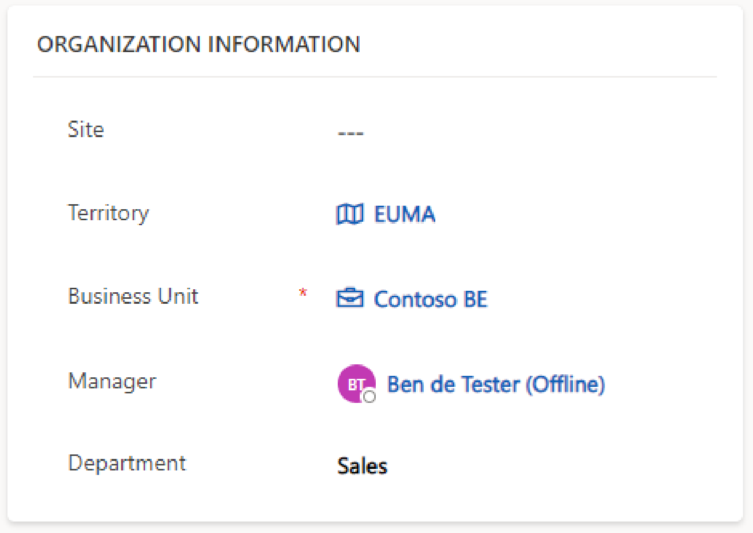


ORGANIZATION INFORMATION

Site		---
Territory		---
Business Unit	*	orgf43beaed
Manager		---
Department		---

Extended sync of user profile fields

Dataverse user form	Microsoft 365/Azure AD user
Middle Name	Display name | Custom
Employee Id	Employee ID
Department*	Department
Manager	Manager
Business Unit	Company name | Logic
Territory	Office location | Logic
Site**	City | Logic



ORGANIZATION INFORMATION

Site	---
Territory	EUMA
Business Unit *	Contoso BE
Manager	BT Ben de Tester (Offline)
Department	Sales

Automation

- Get user profile from Microsoft 365/Azure AD

  → AAD User table in Dataverse

  → Office 365 User connector

  → Azure AD connector

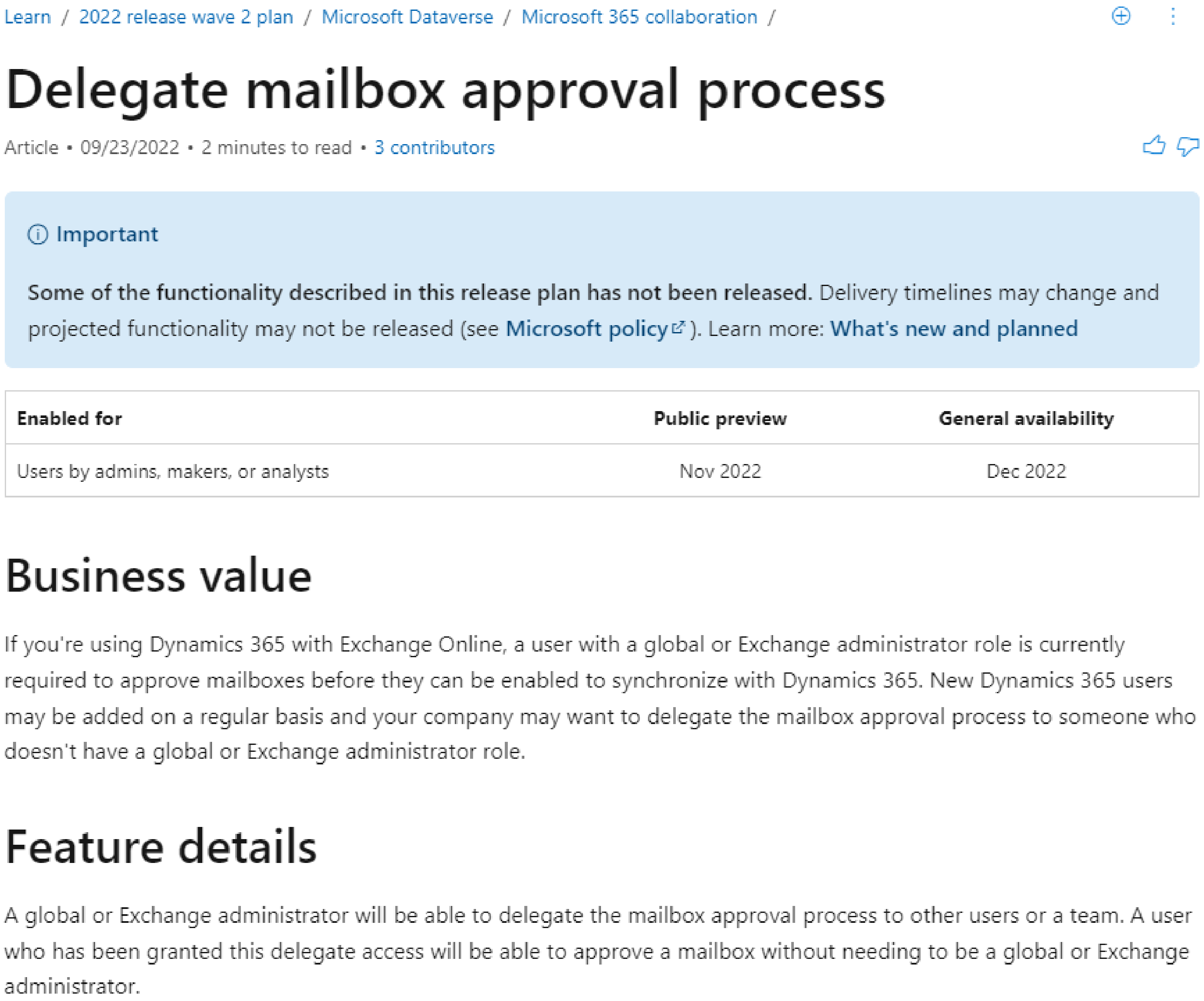
  → Graph API

- Setting

  → User profile in Dataverse

  → Personal User Settings

- Approve, test & enable user’s Mailbox



Learn / 2022 release wave 2 plan / Microsoft Dataverse / Microsoft 365 collaboration /

Delegate mailbox approval process

Article • 09/23/2022 • 2 minutes to read • 3 contributors

ⓘ Important

Some of the functionality described in this release plan has not been released. Delivery timelines may change and projected functionality may not be released (see Microsoft policy). Learn more: What's new and planned

Enabled for	Public preview	General availability
Users by admins, makers, or analysts	Nov 2022	Dec 2022

Business value

If you're using Dynamics 365 with Exchange Online, a user with a global or Exchange administrator role is currently required to approve mailboxes before they can be enabled to synchronize with Dynamics 365. New Dynamics 365 users may be added on a regular basis and your company may want to delegate the mailbox approval process to someone who doesn't have a global or Exchange administrator role.

Feature details

A global or Exchange administrator will be able to delegate the mailbox approval process to other users or a team. A user who has been granted this delegate access will be able to approve a mailbox without needing to be a global or Exchange administrator.

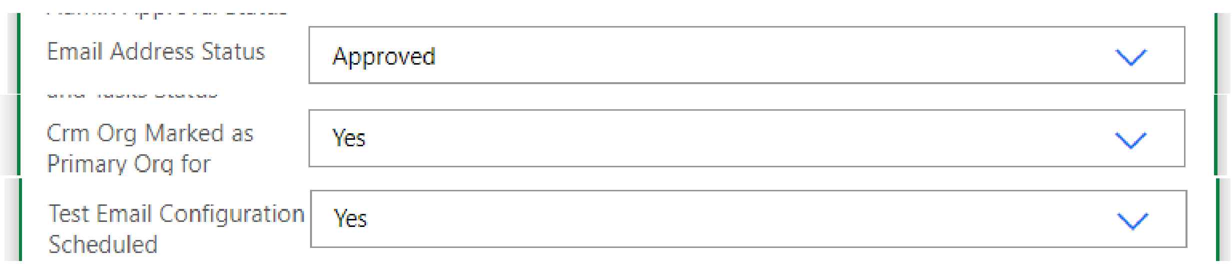
Approve mailbox

- User can approve its own mailbox
- Dataverse ‘When a User row is added’ trigger: Run as Row owner
- Update Mailbox row: Use invoker’s connection

  → Email Address Status = Approved

  → Crm Org Marked as Primary Org for Exchange Mailbox = Yes

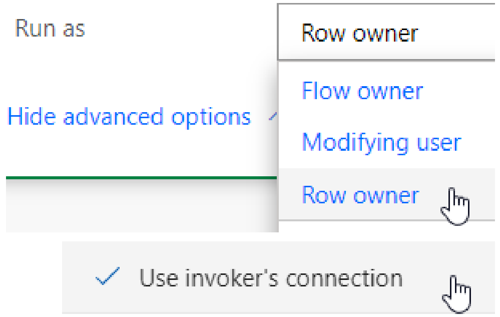
  → Test Email Configuration Scheduled = Yes
- Web API impersonation



Email Address Status: Approved

Crm Org Marked as Primary Org for: Yes

Test Email Configuration Scheduled: Yes



Run as: Row owner

✓ Use invoker's connection

Wrap up

There’s an app for that

- Microsoft 365 Self Service Portal with Power Apps
- Building a JIT app for elevated permissions on Microsoft Power Platform
- User on boarding Walkthrough: Power Apps Portal way
- Dataverse admin app
- Any suggestions?

Questions?