

Paul Borisov

HR Onboarding and Offboarding web app for Entra ID and Hybrid Local AD with flexible Organizational Charts

Next.js, Auth.js, Entra ID, Hybrid Local AD, Azure Automaton with Hybrid Worker, Prisma with Azure SQL / PostgreSQL / Sqlite providers, React Hook Forms, Redux Toolkit, hosted on Azure App service

9-15-2024

Table of Contents

Introduction.....2

User interface2

 Default view, Employee hierarchy3

 Organizational structure3

 Demo mode3

Security roles.....5

 Regular employees5

 HR Managers.....5

 User Administrators5

Onboarding of new employees5

 HR Managers.....5

 User Administrators8

Offboarding of existing employees.....11

 HR Managers.....11

 User Administrators12

Introduction

This is known that onboarding of a new employee to the company's working staff and offboarding of leaving members are continuous processes. However, significant parts of these routines can be automated. For instance, the new employee typically joins a specific manager's team. This implies we can copy repeating parts of employee's attributes such as unit, department, country, subsidiary address and so on from the manager. Also, there are standard routines such as generating new sign-in credentials, joining required security groups, sending a summary report to the manager.

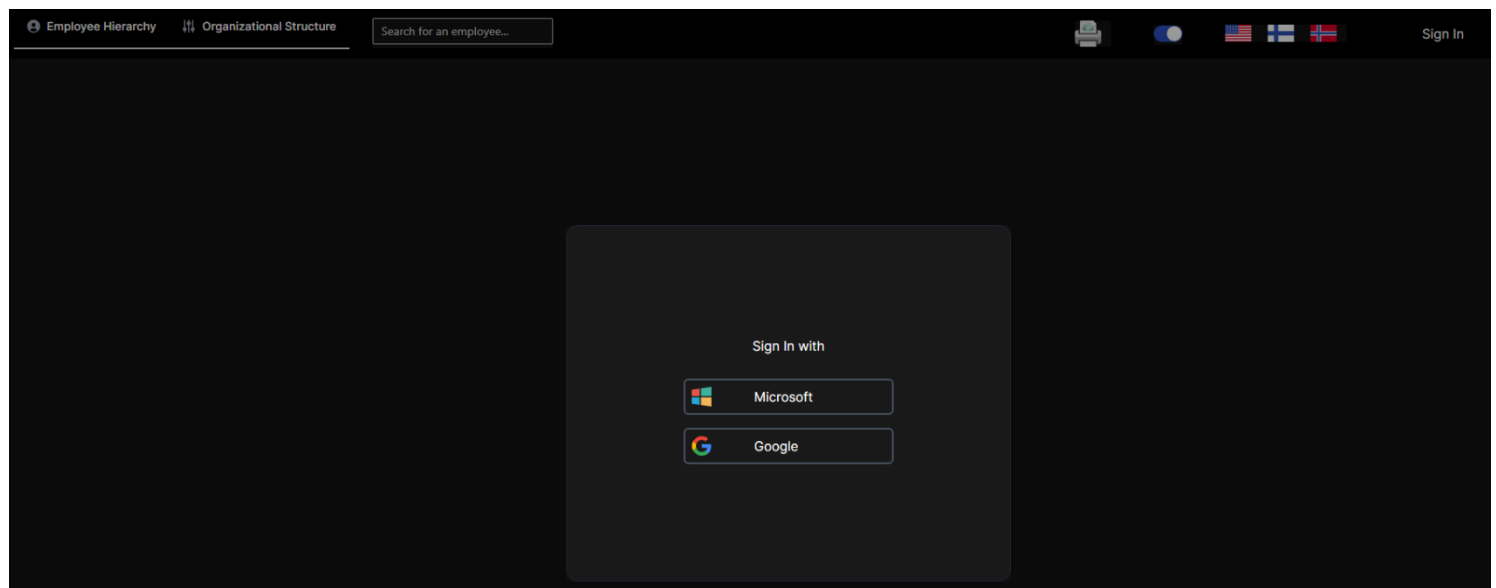
This HR onboarding and offboarding web application solves most frequent problems related to managing employee accounts in Entra ID and Hybrid Local AD.

- It provides secure convenient options to quickly create, update, and delete Entra ID and Hybrid Local AD accounts without a need of opening a VPN connection.
- The app offers configurable Organizational Charts that provide displaying company hierarchies based on users' attributes stored in Azure AD.
- Organizational Charts support flexible grouping by multiple user attributes up to 5 levels deep and up to 5 columns long.
- Optional operations on local AD are done using proxy-capabilities of Azure Automation Hybrid Worker connected to a VM with access to local AD.

User interface

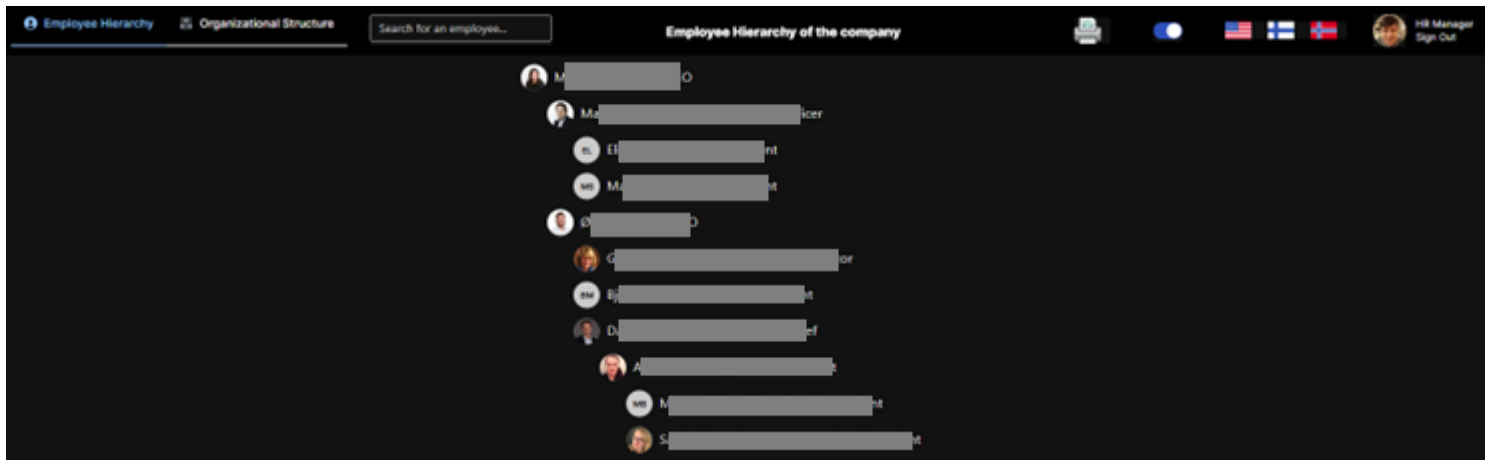
When the user comes to the site for the first time, the site shows only minimal UI with navigation and link to sign in.

- To see organizational hierarchies of the company, the user should login with regular M365 credentials.

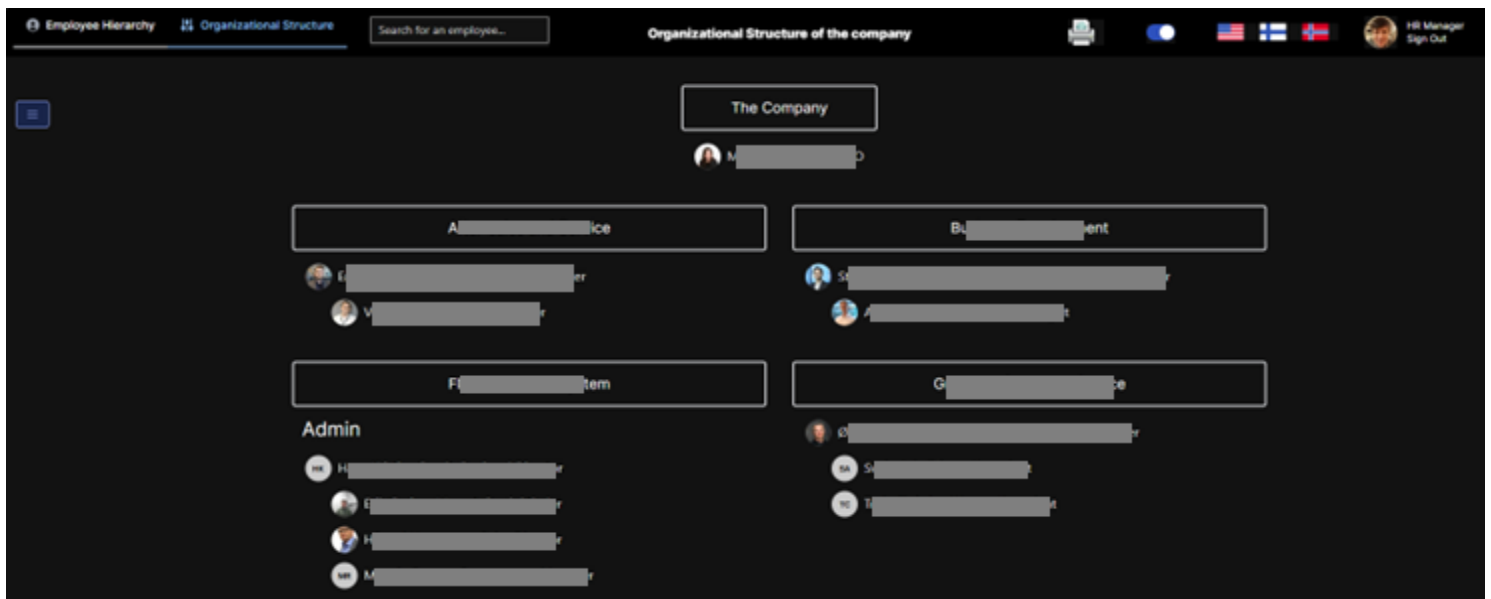


- It takes a few seconds after the login to extract users' data from Entra ID and shape hierarchical views.
- Data is cached to a database and automatically refreshed in the background every hour if the user is still active.

Default view, Employee hierarchy



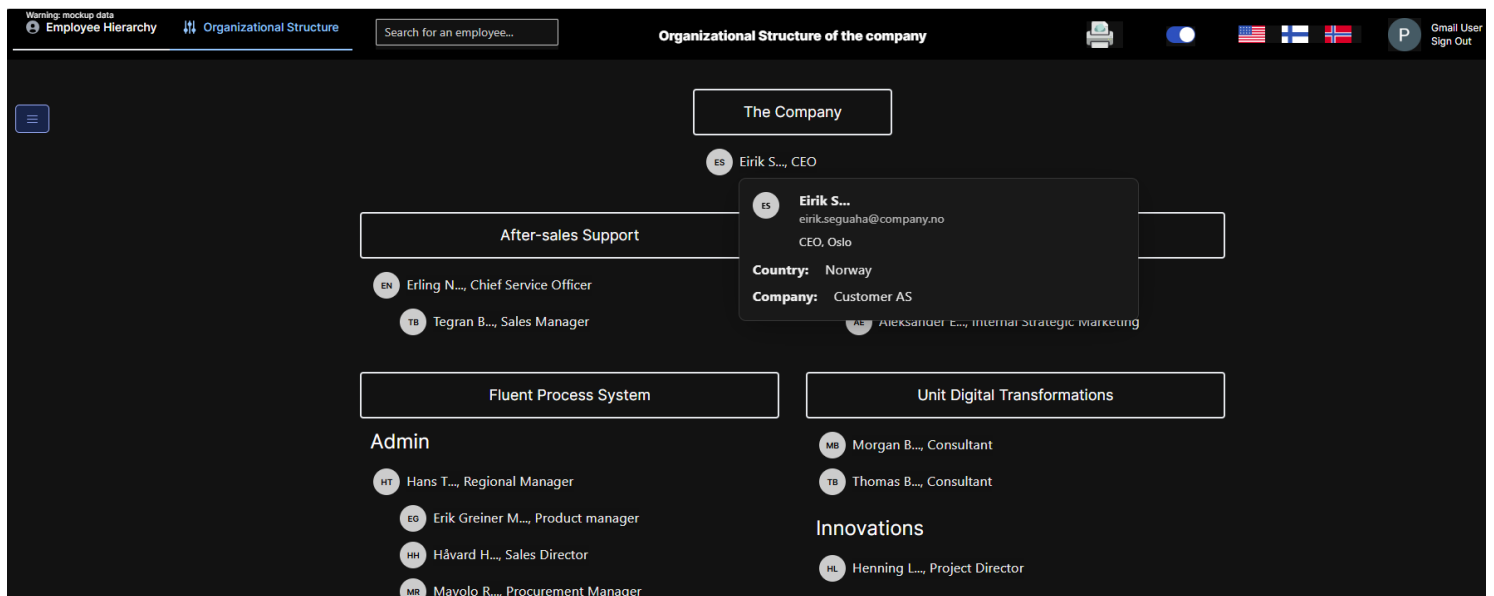
Organizational structure



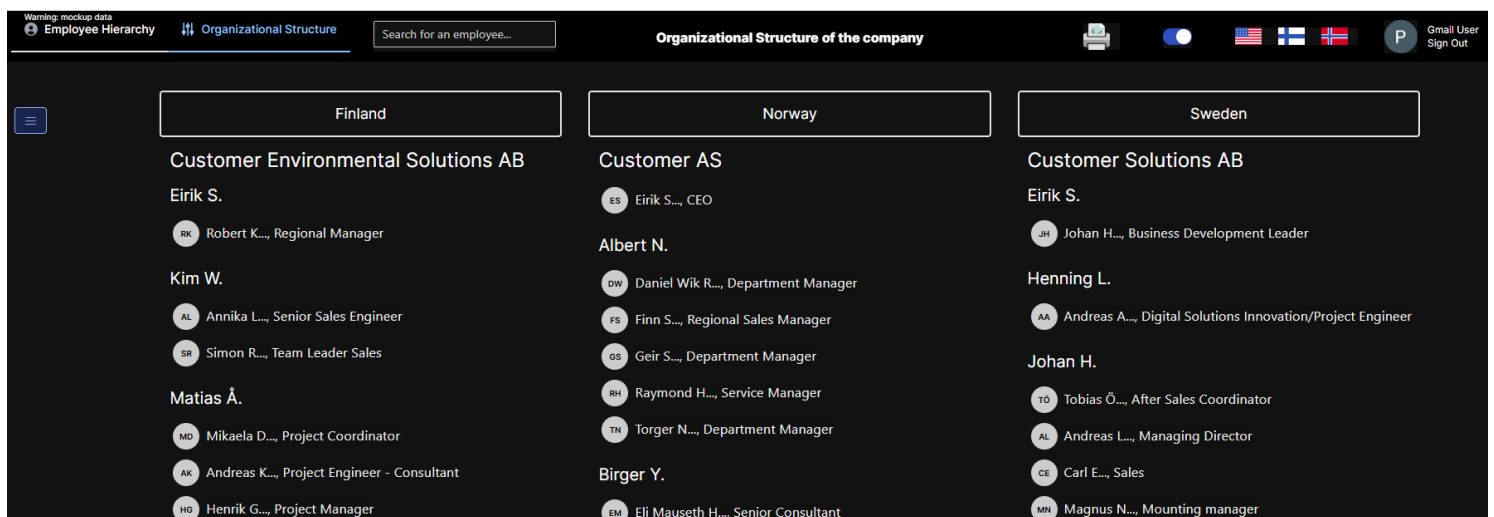
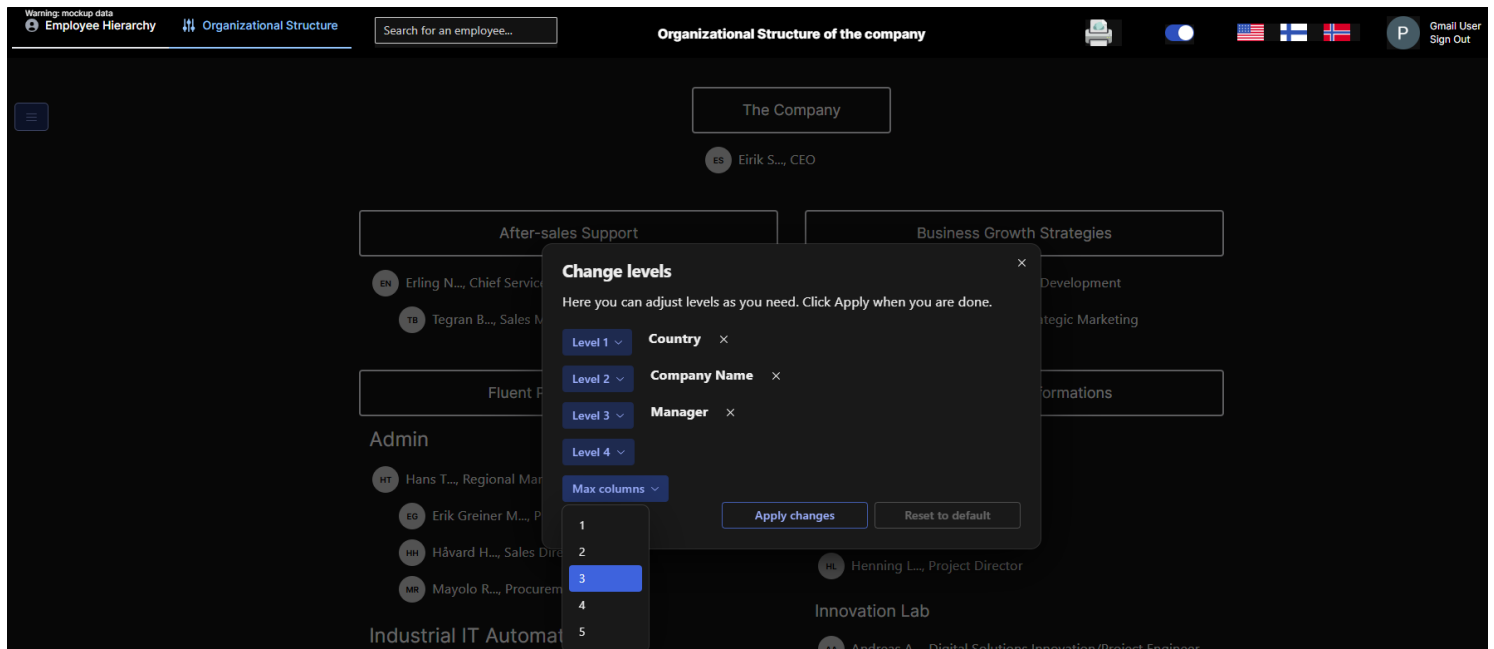
Demo mode

Alternatively, the user can login with any Gmail account. In this case the site will be switched to demo mode with predefined static content displayed.

- In demo mode, all data including user and department names, job titles, locations etc. is not real.



- However, all filters and configurable data structures will work in the same way as with regular company data



Security roles

There are three types of security roles for authenticated in the application. The system automatically detects the role of a signed in user based on his access rights.

Regular employees

This is the basic limited role. These users can browse organizational hierarchies, search for people, configure and save views for personal use and print them.

HR Managers

The role of HR Managers extends the capabilities of regular employees. Typically, HR Managers start the onboarding process for a new employee and register initial records to create the new account.

- They register and manage only records in HR systems.
- They have no rights to manage Entra ID and Local AD accounts.

User Administrators

The role of User Administrators is the most powerful. It extends the capabilities of HR Managers.

- Members of this role finalize the onboarding process initiated by HR Managers.
- They can create, update, and delete user accounts in Entra ID and in hybrid Local AD.

Onboarding of new employees

HR Managers

Typically, HR Managers

- Start the onboarding process for a new employee and register initial records to create the new account.
- Choose a presumed manager for the new employee, fill out the basic form, upload supplemental documents such as CV, working contract, photo, etc.
- Send the summary email on the completed actions to the manager and/or to the User Administrator.

Admin

HK

Han: [redacted] t, Regional Director



Han [redacted] t

h [redacted]

Regional Director, Oslo

Create new employee

Offboard employee

Country: Norway

Company: [redacted] AS

Manager: M [redacted] e

Organizational Unit: Fl [redacted] n

Department: Admin

LTLi



New employee



Manager

H [redacted] t

Employee ID *



74000

Proposed

First name *

Magnus

Required

Last name *

Hanson

Required

Name

Magnus Hanson

Job title

Mobile phone

01215451

Work phone

Organizational Unit

[redacted]

☒ Add to SharePoint list

Upload documents

Magnus-Hanson-confidential.docx



Magnus-Hanson-NDA.pdf



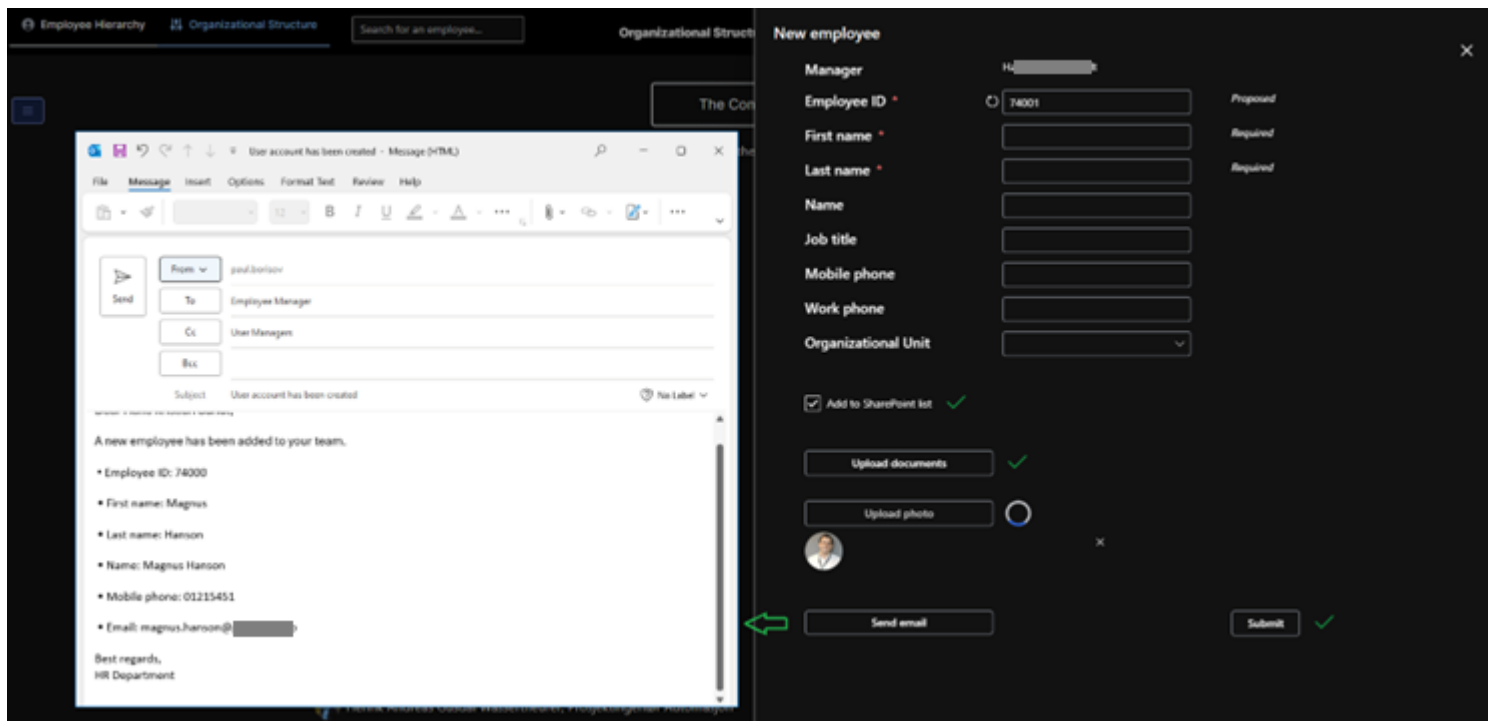
Magnus-Hanson-work-contract.docx



Upload photo




Submit



- The informational form filled out by an HR Manager is short and always fits into one screen.
- Any relevant additional attributes - for instance, unit, department, team, street address, etc. - are automatically copied from the record of the chosen employee manager.

New records registered in internal subsystems of Employee Registry and Employee Documents.

General	Personal Contact Info	Detailed Info	Emergency Contact	Policy
Employee ID	74000			
Last Name	Hanson			
First Name	Magnus			
Display Name	Magnus Hanson			
IT-user?	<input checked="" type="checkbox"/>			
	 Magnus Hanson			
Employee Main Status	Active			
Employee Status	Active			
Employee Category	Employee			
Employee Type	Permanent			
Date of Hire				
Date of Exit				
Date of Birth				
Drivers License				
Company	AS			
Location	Oslo			
Location Street Address	Inn 15			
Location Post Office	Oslo			
Location Postal Code	NO-0607			
Location Country	Norway			
Location P.O. Box	6578 Etterstad			
Organizational Unit	Flytystem			
Department	Admin			
Team				
Manager	<input type="checkbox"/> Halvordt			

Employee Documents

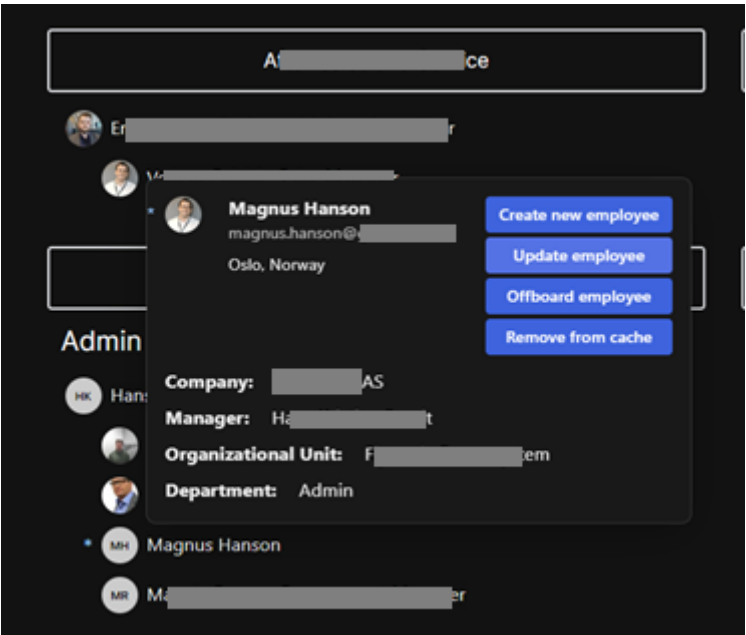
Active Employees

✓	📄	Name	Employee	Employee:Location Post Office	Employee:Employee ID	Employee:Employee Main Status
	📄	CV				
✓	📄	Magnus-Hanson-work-contract ✳️	Magnus Hanson	Oslo	74000	Active
✓	📄	Magnus-Hanson-confidential ✳️	Magnus Hanson	Oslo	74000	Active
✓	📄	userphoto-magnus.hanson@goodtech.no ✳️	Magnus Hanson	Oslo	74000	Active
✓	📄	Magnus-Hanson-NDA ✳️	Magnus Hanson	Oslo	74000	Active

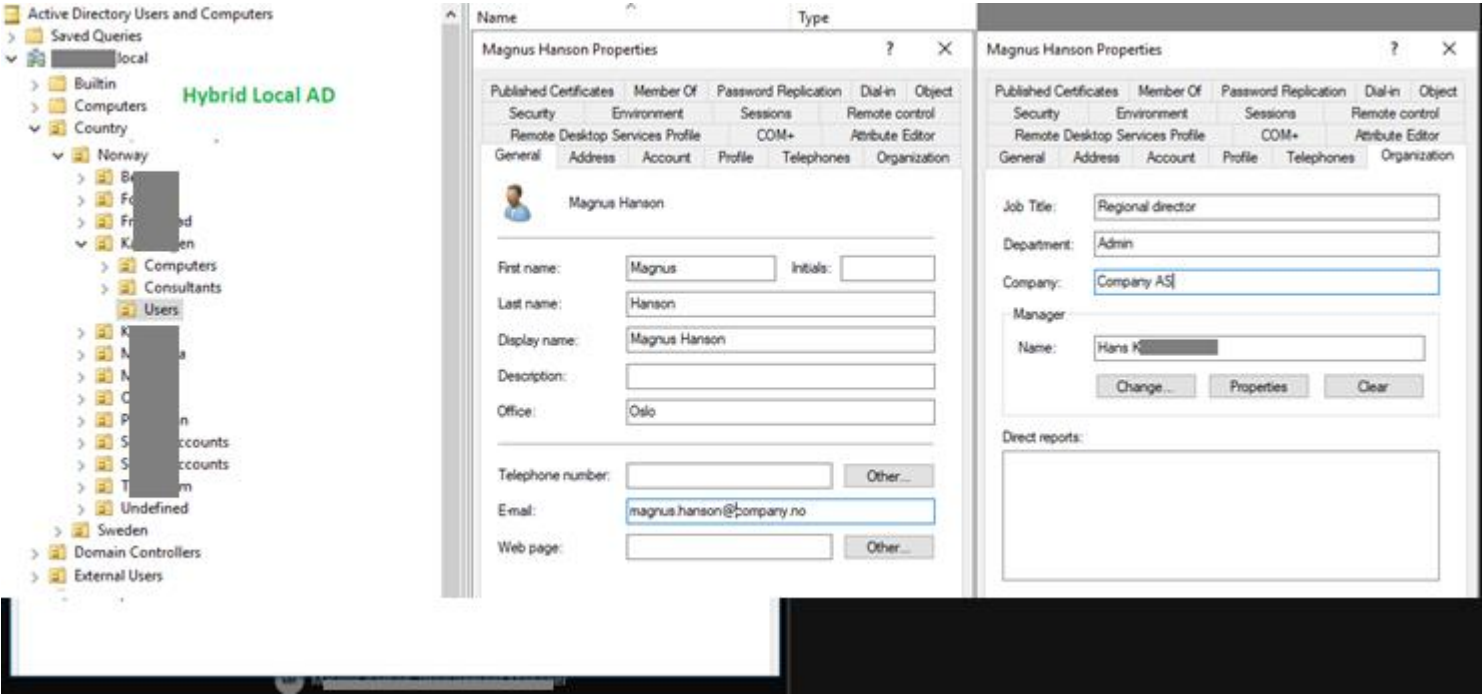
User Administrators

Typically, members of this role finalize the onboarding process initiated by HR Managers.

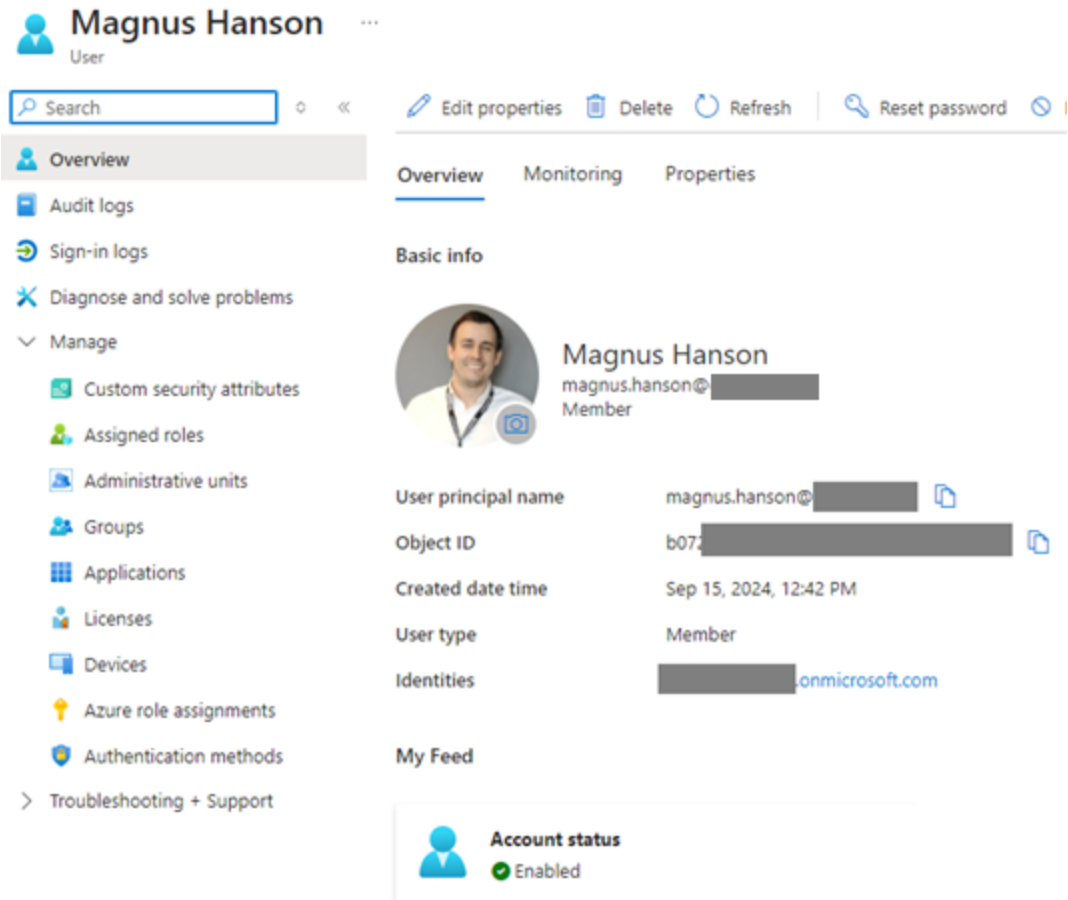
- HR Managers inform User Administrators by email generated in the basic form.
- User Administrators then create, update, and delete user accounts in Entra ID and in hybrid Local AD using the forms provided for them in application UI.



New user account created in Hybrid Local AD.



The new Entra ID account automatically synchronized by AD Connect from Hybrid Local AD in 15-30 minutes.



Magnus Hanson | Groups

User

Search

»

«

+ Add memberships

✕ Remove memberships

↻ Refresh

☰ Columns

🗨 Got feedback?

Overview

Audit logs

Sign-in logs

Diagnose and solve problems

Manage

Custom security attributes

Assigned roles

Administrative units

Groups

Search groups

Add filters

	Name	↑↓	Object Id	Group Type	Source
<input type="checkbox"/>	<div>D</div> D365_Test_Sales		27dc6b9b-...p5e3a5f...	Security	Windows Server AD
<input type="checkbox"/>	<div>T</div> Test1		bc4aec96-...acedec...	Security	Windows Server AD
<input type="checkbox"/>	<div>T</div> Test2		ec522159-...bd3b8...	Security	Windows Server AD

Offboarding of existing employees

HR Managers

HR Managers start the offboarding process and mark employee records in internal HR systems as disabled.

- There is the only option available for them.

Offboard employee


Employee

Magnus Hanson

☒ Disable account

Submit

- After they click on the button, the employee record is marked as Inactive and User Administrators get informed automatically.
- Entra ID and Hybrid Local AD accounts are not yet affected.

General	Personal Contact Info	Detailed Info	Emergency Contact
Employee ID	74000		
Last Name	Hanson		
First Name	Magnus		
Display Name	Magnus Hanson		
IT-user?	<input checked="" type="checkbox"/>		
	 Magnus Hanson		
Job Title			
Job Title (local)			
Employee Main Status	Inactive		
Employee Status	Retention		
Employee Category	Employee		
Employee Type	Permanent		

User Administrators

User Administrators finalize the offboarding process initiated by HR Managers. Typically, they split the offboarding process into two stages.

- At Stage 1, they disable Entra ID and/or Hybrid Local AD accounts. Clicking on the Submit button removes the employee from all groups, resets password and marks the AD accounts as disabled.

Offboard employee


Employee

Magnus Hanson

☒ Disable account☐ Delete account


Submit

✓

Name	Type	Description
 Magnus Hanson	User	Ended on 15.09.2024

Magnus Hanson Properties
?
X

Security	Environment	Sessions	Remote control
Remote Desktop Services Profile		COM+	Attribute Editor
Published Certificates	Member Of	Password Replication	Dial-in
Object			
General	Address	Account	Profile
	Telephones	Organization	


Magnus Hanson

First name:
Initials:

Last name:

Display name:

Description:

Office:



Magnus Hanson

User

Search



Edit properties



Delete



Refresh



Reset password



Overview



Audit logs



Sign-in logs



Diagnose and solve problems



Manage



Custom security attributes



Assigned roles



Administrative units



Groups



Applications



Licenses



Devices



Azure role assignments



Authentication methods



Troubleshooting + Support

Overview

Monitoring

Properties

Basic info



Magnus Hanson

magnus.hanson@

Member

User principal name

magnus.hanson@



Object ID

b0725



Created date time

Sep 15, 2024, 12:42 PM

User type

Member

Identities

.onmicrosoft.com

My Feed



Account status



Disabled

- At Stage 2, the account is deleted from Entra ID and/or Hybrid Local. Clicking on the Submit button removes it.

Offboard employee

Employee

Magnus Hanson



Disable account



Delete account

Submit



Delete AD account?



Users | Deleted users ...

Goodtech



Bulk restore



Delete permanently



Restore users



All users



Audit logs



Sign-in logs



Diagnose and solve problems



Manage



Deleted users



[Azure Active Directory is now Microsoft Entra ID.](#)



Users are permanently deleted automatically 30 days after they are deleted.



Add filter

13 users found



Display name ↑↓

User principal name



Magnus Hanson

b0725c91b0aa4d5c87c