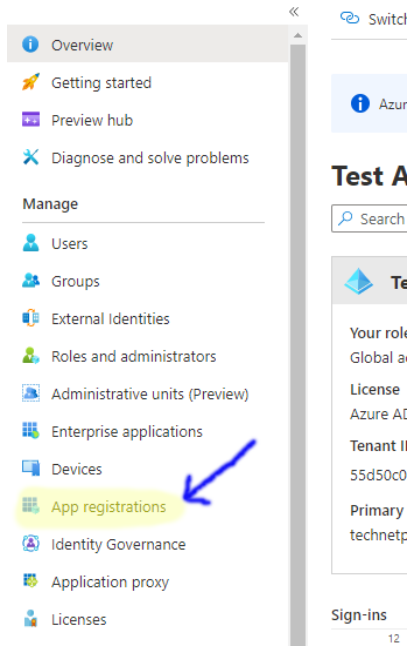


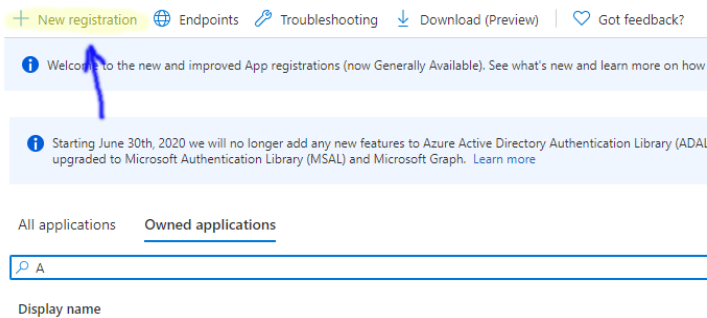
Koble More Service Discovery til Azure AD

Oppsett i Azure AD

For at More Service Discovery skal kunne få tilgang til brukere i Azure AD så må det registreres en ny «App» i Azure AD. Dette gjøres i Azure AD ved å velge «App registration»



Under velger man igjen «New Registration»:



Du må da gi applikasjonen ett navn og den skal kun ha tilgang gjeldene Tenant:
Register an application

* Name
The user-facing display name for this application (this can be changed later).

Discovery

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Test AD only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Applikasjonen er nå registrert og vil få en egen «Client ID» som vist under:

 Delete  Endpoints

^ Essentials

Display name : Discovery

Application (client) ID : [REDACTED]

Directory (tenant) ID : [REDACTED]

Object ID : [REDACTED]

Her skal vi bruke «Tenant ID» og «Client ID» inne i More Service Discovery for å koble mot Azure AD. Vi må videre sette riktig tilgang, og lage en «Client Secret».

Tilgang Azure AD Applikasjon

More Service Discovery trenger kun lese tilgang til brukere i Azure AD. For en ny applikasjon så gis den automatisk tilgang til å lese brukere, men dette er en «Delegated» tilgang.

For at Discovery skal kunne lese så må det gis en «Application» tilgang for å lese brukere for denne.

Overview

Quickstart

Integration assistant (preview)

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

Owners

Roles and administrators (Preview)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admin all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

✓ Grant admin consent for Test AD

API / Permissions name	Type	Description
▼ Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

Man velger «Add a permission» og deretter velger man «Microsoft Graph»:

Request API permissions


Select an API

Microsoft APIs


APIs my organization uses

My APIs


Commonly used Microsoft APIs



Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Service Management
Programmatic access to much of the functionality available through the Azure portal



Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

Deretter velger man «Application permission» Request API permissions

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Man velger deretter «User.Read.All» og trykker «Add permissions»:

✓ User (1)

<input type="checkbox"/>	User.Export.All Export user's data	Yes
<input type="checkbox"/>	User.Invite.All Invite guest users to the organization	Yes
<input type="checkbox"/>	User.ManageIdentities.All Manage all users' identities	Yes
<input checked="" type="checkbox"/>	User.Read.All Read all users' full profiles	Yes
<input type="checkbox"/>	User.ReadWrite.All Read and write all users' full profiles	Yes

Add permissions Discard

Denne rettigheten vil da bli lagt til for Discovery, men den er ikke aktiv før denne er godkjent av en administrator:

+ Add a permission ✓ Grant admin consent for Test AD

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				...
User.Read	Delegated	Sign in and read user profile	-	...
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for Test AD ...

Dersom man har administrator rettigheter så kan dette gjøres ved å klikke på «Grant admin consent» som vist over. Discovery skal da ha fått rettigheten for å lese brukere.

Client Secret

For at Discovery skal kunne koble seg til Azure AD og lese brukere trenger den ett passord/Client secret. Dette tildeles via «Certificates & secrets»:

Quickstart

Integration assistant (preview)

Manage

- Branding
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- Owners
- Roles and administrators (Preview)
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Certificates

Certificates can be used as secrets to prove the application's identity.

Upload certificate

Thumbprint

No certificates have been added for this application.

Client secrets

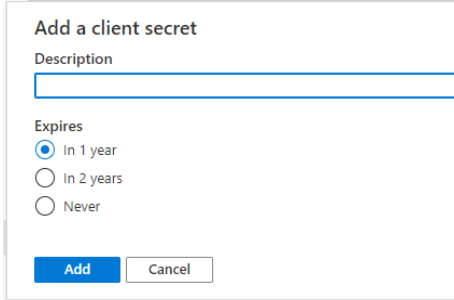
A secret string that the application uses to prove its identity with.

+ New client secret

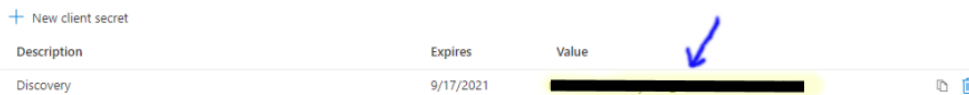
Description

No client secrets have been created for this application.

Under «Certificates & secrets» så velger man «New client secret». Man vil da få legge inn ett navn på denne og hvor denne skal gjelde:



Legg inn ett navn og velg hvor lenge denne skal gjelde og trykk «Add»



Description	Expires	Value
Discovery	9/17/2021	[Redacted]

En ny «Client secret» legges da til og vises på skjermen som vist over. Denne må kopieres ut og brukes i Discovery når man legger til koblingen mot Azure AD.

1120pxViktig

Kopier ut «Client secret» strengen med en gang. Dersom man forlater siden så kommer ikke denne opp igjen, og man må lage en ny.

Note

Det er 2 typer tilganger:

- Delegated: Tilganger som gis til brukere som logger seg på.
- Application: Tilganger som gis til applikasjoner som logger seg på.

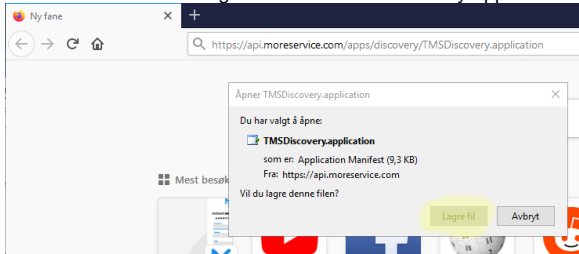
Oppsett Discovery

Installasjon More Service Discovery

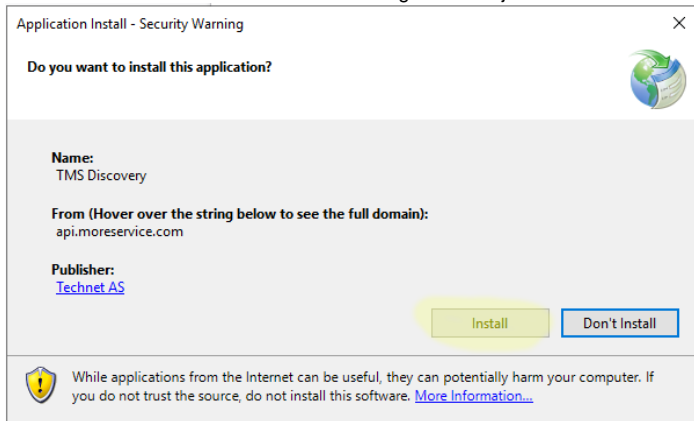
Bruk følgende URL for å installere More Service Discovery

[https://api.moreservice.com/apps/discovery/More ServiceDiscovery.application](https://api.moreservice.com/apps/discovery/More%20ServiceDiscovery.application)

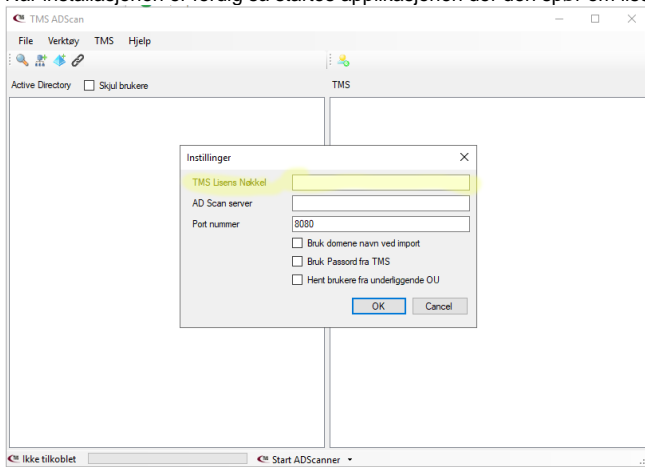
Dette vil starte nedlasting av More ServiceDiscovery.application som brukes for å starte More Service Discovery installasjonen:



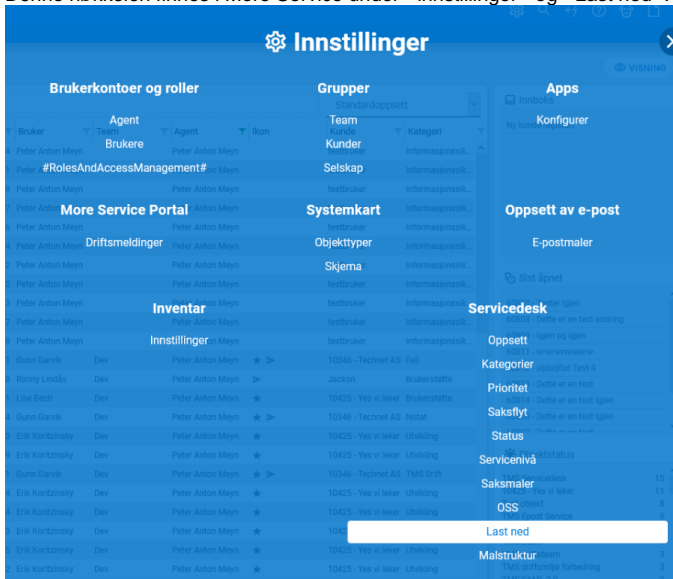
Velg lagre for å lagre denne filen.
Deretter startes denne filen. Man vil da få følgende beskjed:



Her velges «Install» for å installere applikasjonen. Denne installeres da i profilen til den påloggede brukeren, og den legges til i start menyen. Hver gang applikasjonen startes så sjekker den for oppdateringer. Dersom en oppdatering finnes så spør den om denne skal lastes ned og installeres. Når installasjonen er ferdig så startes applikasjonen der den spør om lisens nøkkel:



Denne nøkkelen finnes i More Service under «innstillinger» og «Last ned»:



Her er det «din lisensnøkkel» som skal brukes som vist under:

TMS Discovery 1.5

Din lisensnøkkel: [REDACTED]

Programvare for å importere brukere, servere og PCer fra nettverket ditt til TMS.

[Klikk her for å se video om bruk av TMS Discovery](#)

ADScan Service Setup 1.5 (.msi)

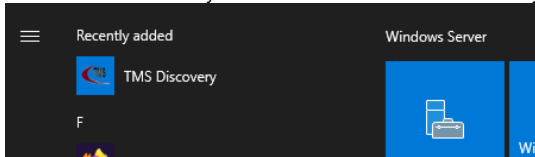
Automatisk import av nye brukere, servere og PCer til More Service.

Når denne legges inn så kobler More Service Discovery seg mot More Service.

VIKTIG

Det er viktig å ta en restart av More Service Discovery for å få opp data fra databases i More Service Discovery. Så etter at lisens nøkkelen er lagt inn og godtatt så lukk More Service Discovery. Deretter start More Service Discovery fra start menyen.

More Service Discovery skal nå kunne startes fra Start Menyen:

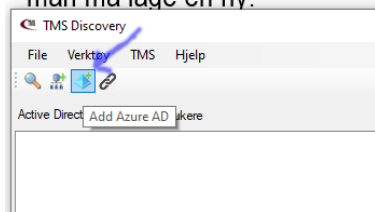


Det er viktig å restarte More Service Discovery etter at lisens nøkkelen er lagt inn. Når den er startet på nytt så kan man gå videre med å koble den mot Azure AD.

Koble mot Azure AD

Når tilgangen er gitt i Azure AD så kan man sette opp koblingen i Discovery mot Azure AD.

Dette gjøres på følgende måte inne i Discovery:

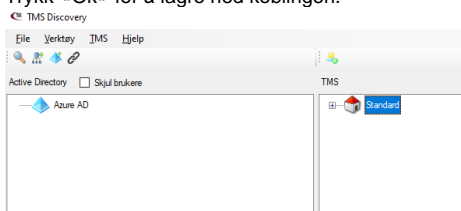


Velg «Add Azure AD» og legg inn informasjon for å koble til Azure:

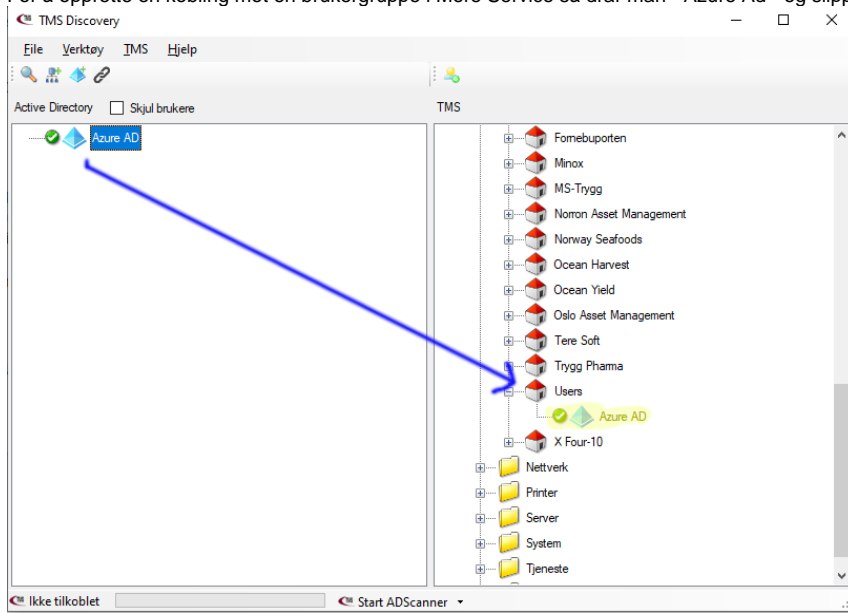
A screenshot of the 'Add Azure AD' dialog box. It has a close button (X) in the top right corner. The fields are: 'Name' (containing 'Azure AD'), 'Tenant ID' (containing a redacted value), 'Client ID' (containing a redacted value), and 'Client Secret' (containing a redacted value). At the bottom are 'Ok' and 'Cancel' buttons.

«Name» er kun en label som brukes i Discovery for visning av denne koblingen, og brukes ikke under selve autentiseringen.

Trykk «Ok» for å lagre ned koblingen.



For å opprette en kobling mot en brukergruppe i More Service så drar man «Azure Ad» og slipper den på den bruker gruppen som skal motta brukere:



Brukere kan da importeres på normal måte via «More Service | Oppdater Brukere»