MANUAL

UniLock integration med Microsoft Entra

Projekt: PCS125-20
Rev.: 2026-11-02

Med denne integration kan Microsoft Entra anvendes til at udføre administration af personer/operatører og deres rettigheder i UniLock.

Personer/operatører og deres attributter hentes i Microsoft Entra af UniLock, hvor personerne automatisk kan blive medlem af persongrupper i UniLock og derved få persongruppernes adgangsrettigheder, mens operatører kan få en operatørgruppes operatørrettigheder.

Når personer eller deres rettigheder fjernes i Entra, så fjernes personerne eller deres rettigheder også automatisk i UniLock.

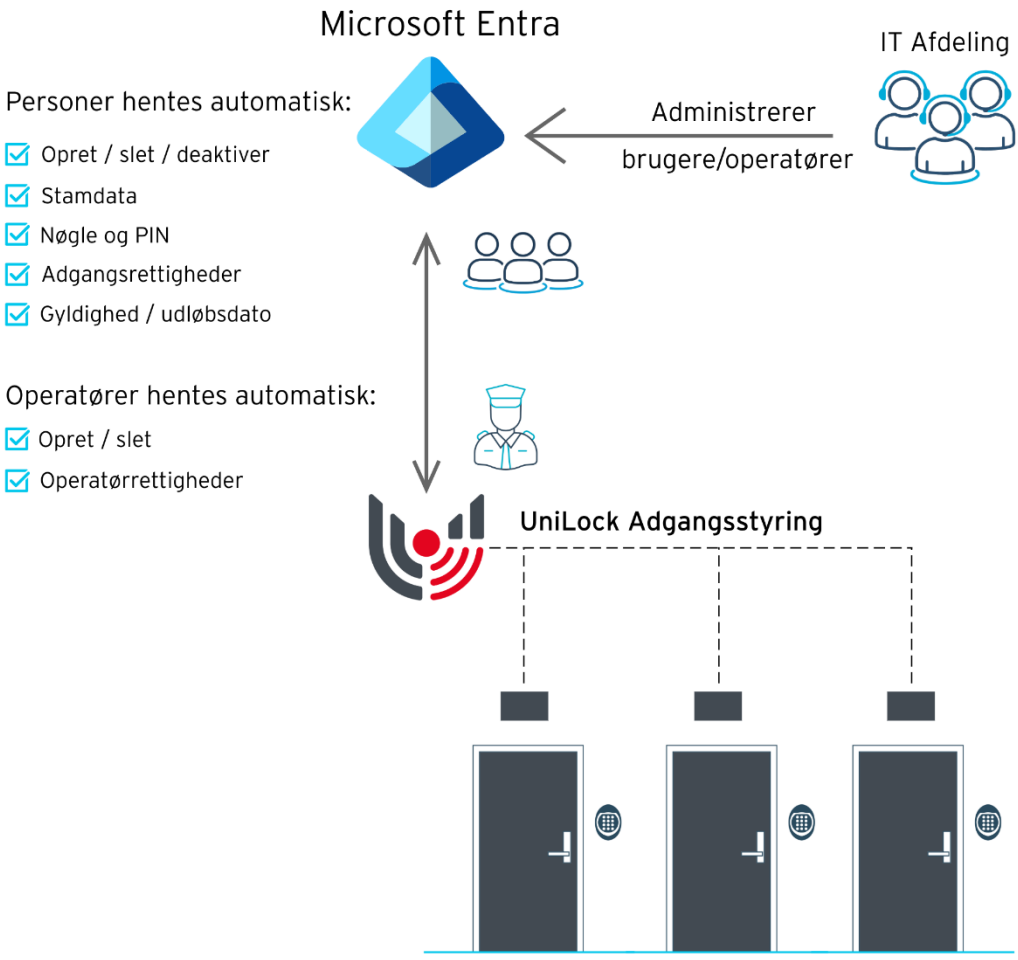
Unitek A/S
Vævervej 5, 8800 Viborg
Tlf. +45 86 61 44 22
unitek.dk

Indhold

1. Beskrivelse 2
1.1 Generel beskrivelse 2
1.2 Kanaler 3
1.3 Program-moduler 3
2. Operatør-vejledning 4
2.1 Stamdata 4
2.2 Personers adgangsrettigheder 4
2.3 Operatørers adgangsrettigheder 4
2.4 UniLock Afdelinger 4
2.5 Microsoft Entra 4
2.5.1 Personer i Entra 4
2.5.2 Grupper 6
3. Installations-vejledning 6
3.1 Microsoft Entra 6
3.1.1 Tilladelse via App registrering 6
3.1.2 Grupper 9
3.2 UniLock 9
3.2.1 Forbindelse 9
3.2.2 Personer 10
3.2.3 Stamdata 14
3.2.4 Adgangsrettigheder 15
3.2.5 Operatører 16
3.2.6 Synkronisering 16
3.2.7 Logfiler 17
4. Personattributter i Microsoft Entra 17

1. Beskrivelse

1.1 Generel beskrivelse



Anvendelse

Kunder med UniLock adgangskontrol og Microsoft Entra kan nu effektivisere arbejdsgange, da systemerne automatisk udveksler data.

Når ansatte mv. og deres rettigheder administreres i Microsoft Entra - så administreres disse også automatisk i UniLock.

Entra anvendes bl.a. til at styre personers adgang til virksomhedens IT-systemer, hvor det nu også kan kombineres med styring af personers adgang i UniLock pc-program samt personers fysiske adgangsrettigheder til virksomhedens døre i lokationer, bygninger, kontorer, lokaler mv.

Når personer oprettes i et Windows miljø sker dette typisk i Entra, hvorfra andre systemer automatisk kan hente personers stamdata, login, mailadresse, grupperettigheder mv. Personers placering og grupperettigheder i Entra kan fx fortælle noget om, hvilken afdeling personerne hører til, og hvilke systemer personerne må anvende.

Med denne integration kan personers stamdata og rettigheder automatisk hentes af UniLock adgangskontrol. Oprettes Julia fx i Entra med medlemskab af gruppen for receptionister, så kan Julia automatisk oplåse døre og frakoble tyverialarmer i kontorområdet styret af UniLock og anvende UniLock pc-programmet med begrænsede operatørrettigheder.

Opret, rediger eller slet blot personer og deres rettigheder i Entra og UniLock sørger automatisk for at personernes adgang i døre og pc-program tilrettes.

Beskrivelse

Med denne import mulighed kan Microsoft Entra anvendes til at styre personer/operatører og deres rettigheder i UniLock.

UniLock henter altid seneste status for personer og grupper, således at editeringer og sletninger i Entra også automatisk udføres i UniLock. Herved sikres automatisk fx at tidligere medarbejdere ikke har adgang i døre.

Sideløbende med den automatiske vedligeholdelse af personer fra Entra, så har UniLock operatører også mulighed for manuelt at oprette/ændre personer i UniLock. Som noget specielt er det muligt at give UniLock operatøren mulighed for at overstyre de adgangsrettigheder i UniLock, som personer automatisk tildeles fra Entra.

1.2 Kanaler

Man kan importere ved hjælp af en eller flere kanaler. Man kan fx have en kanal, som synkroniserer personer og deres rettigheder med Microsoft Entra, og en kanal som henter lokalebookinger fra Outlook (Exchange Server).

1.3 Program-moduler

Import er mulig, når der er tegnet licens til en integrationskanal. Alt opsætning kan foretages mens programmet er i demo-mode.

2. Operatør-vejledning

2.1 Stamdata

De stamdatafelter (inklusiv nøgler og PIN) Microsoft Entra integrationen er konfigureret til at administrere, vil ikke være redigerbare for UniLock operatører og blive vist som sådan.

2.2 Personers adgangsrettigheder

Aktiveres synkronisering af personers adgangsrettigheder fra Microsoft Entra, vil personers medlemskab af grupper i UniLock blive styret fra Entra på lige fod med styring fra UniLock operatører. Medlemskaber styret af Entra vil ikke være redigerbare for UniLock operatører og blive vist som sådan.

Entra ændrer ikke på personers direkte adgangsrettigheder til k-punkter.

2.3 Operatørers adgangsrettigheder

Aktiveres synkronisering af operatører fra Microsoft Entra, vil de importerede operatørers medlemskab af operatørgruppe i UniLock blive styret fra Entra på lige fod med styring fra UniLock operatører. Medlemskaber styret af Entra vil ikke være redigerbare for UniLock operatører og blive vist som sådan.

Operatører oprettet af Entra kan logge ind i UniLock ud fra reglerne (geo-fencing mv.) i Entra, da UniLock videresender login-anmodninger til Entra.

2.4 UniLock Afdelinger

Når integrationen er oprettet i en normal afdeling, kan den administrere personer/operatører oprettet i afdelingen. Personer kan tildeles medlemskab af de persongrupper, som er oprettet i afdelingen eller delt til afdelingen med rettighed til at tildele personers medlemskab.

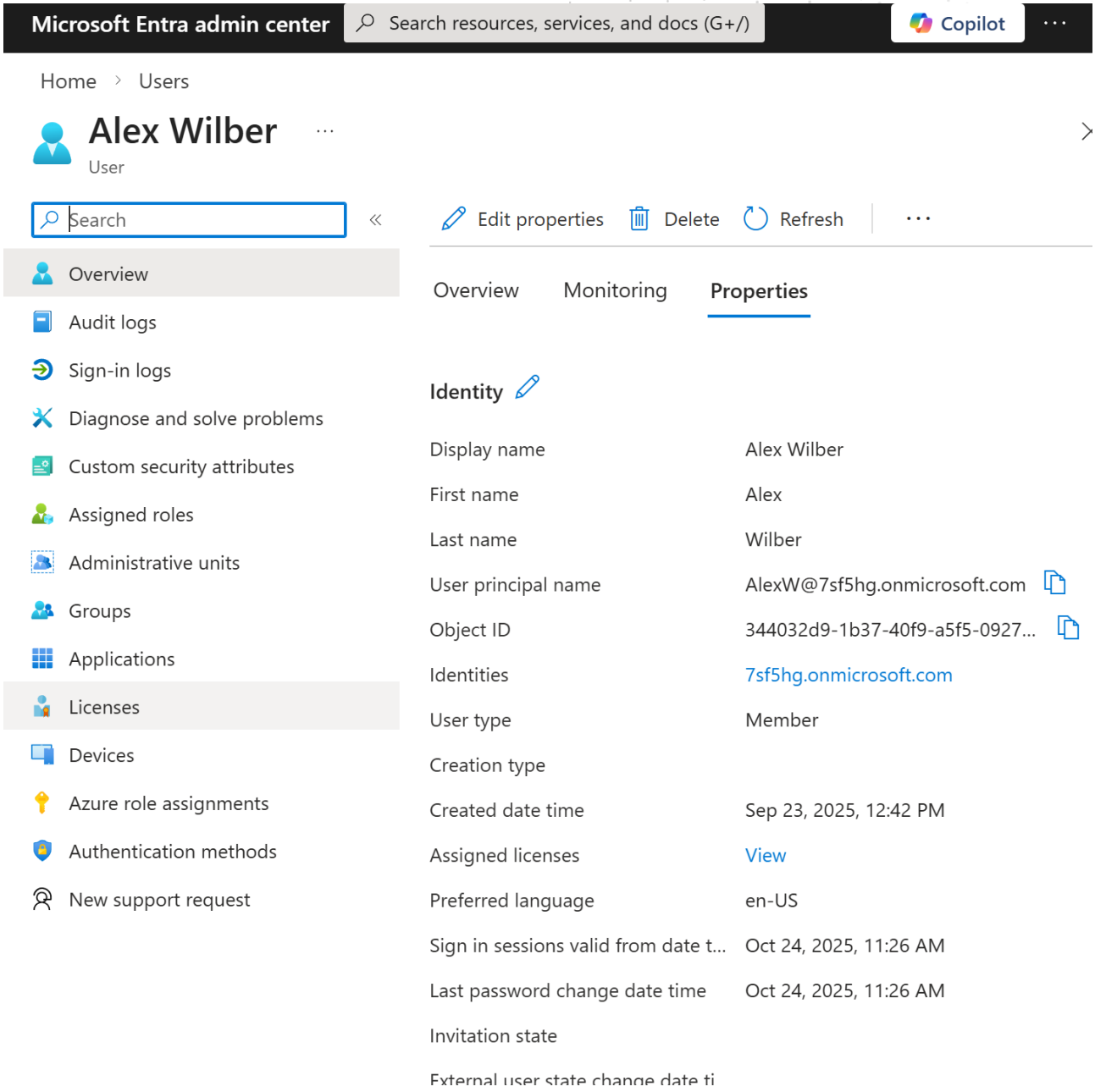
2.5 Microsoft Entra

2.5.1 Personer i Entra

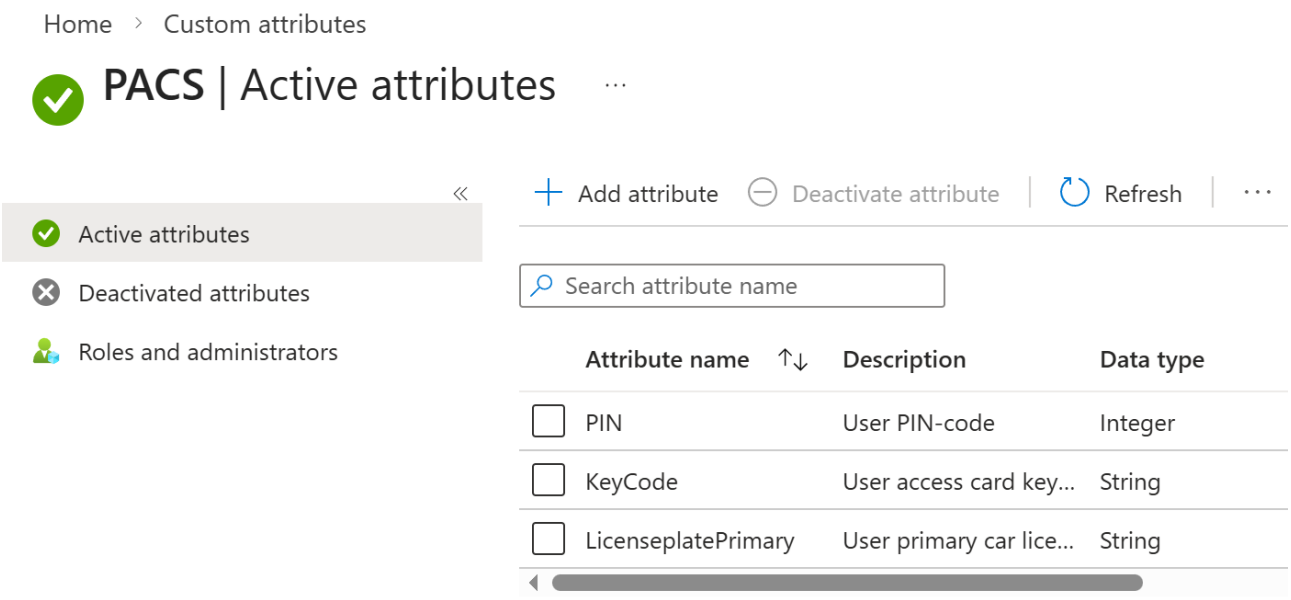
Entra personer kan have tilknyttet en række attributter, hvor en oversigt over de mest almindelige kan findes i afsnit 4.

Herudover kan der oprettes specielle attributter (Custom attributes), som fx kunne anvendes til PIN og nøgle i adgangskontrol og PIN i tyverialarm.

Nedenstående er et eksempel på hvordan en person kan ses/editeres i Entra:



Nedenstående er et eksempel på redigering af Custom attributes:



2.5.2 Grupper

I Entra kan grupper oprettes for at lette den daglige drift af rettigheder mv. Disse grupper kan anvendes til automatisk at tildele rettigheder i andre systemer som fx UniLock adgangskontrol.

I Entra kan personer have medlemskab af flere grupper.

3. Installations-vejledning

3.1 Microsoft Entra

Microsoft Entra er et meget udbredt online IT-værktøj til at styre rettigheder mv. i Windows og lignende IT-miljøer.

3.1.1 Tilladelse via App registrering

Entra administratoren kan administrere hvilke rettigheder UniLock skal have i Entra ved at oprette en Applikation Registrering med de fornødne rettigheder. Registreringen oprettes i Entra menuen [App registrations].

3.1.1.1 Minimums rettigheder

Applikationen skal gives følgende minimum rettigheder, for at kunne fungere:

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	Granted for MSFT
User.Read	Delegated	Sign in and read user profile	No	Granted for MSFT
User.Read.All	Application	Read all users' full profiles	Yes	Granted for MSFT

3.1.1.2 Rettigheder til Custom Security Attributes

Anvendes Entra Custom Security Attributes, skal disse tilføjes i registreringen:

CustomSecAttributeAssignm	Application	Read custom security attribute assignments	Yes	Granted for MSFT
CustomSecAttributeDefinitio	Application	Read custom security attribute definitions	Yes	Granted for MSFT

3.1.1.3 Rettigheder til Custom Directory Extension Attributes

Anvendes Custom Directory Extensions, skal rettigheden til “Application.Read.All” tilføjes:

Application.Read.All	Application	Read all applications	Yes	Granted for MSFT

UniLock medtager kun extensions, der følger nomenklaturen ”extension_UnitekAppClientID_xxx”.

3.1.1.4 Rettigheder til alle UniLock muligheder

Anvendes alle muligheder i UniLock, så skal følgende App rettigheder anvendes:

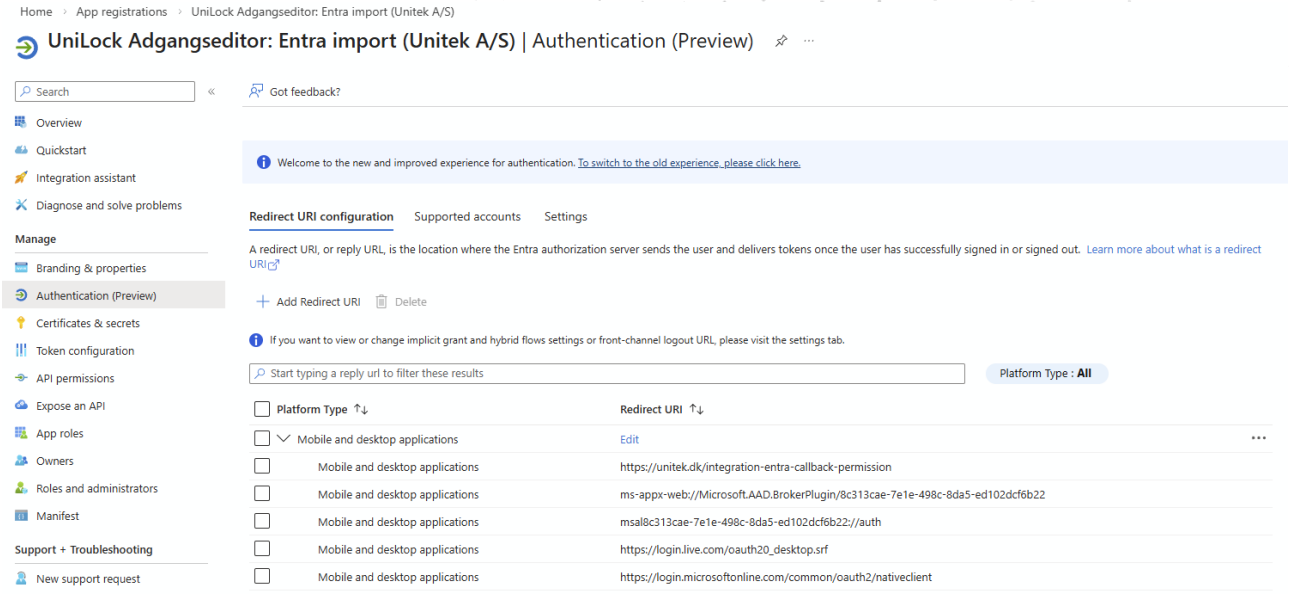
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (6)				
Application.Read.All	Application	Read all applications	Yes	Granted for MSFT
CustomSecAttributeAssignm	Application	Read custom security attribute assignments	Yes	Granted for MSFT
CustomSecAttributeDefinitio	Application	Read custom security attribute definitions	Yes	Granted for MSFT
Group.Read.All	Application	Read all groups	Yes	Granted for MSFT
User.Read	Delegated	Sign in and read user profile	No	Granted for MSFT
User.Read.All	Application	Read all users' full profiles	Yes	Granted for MSFT

3.1.1.5 Redirect URL

Redirect URL anvendes når operatører skal logge ind i UniLock WebAdgangseditor og overholde Entra loginregler (MFA, Geofencing mv.).

I App registreringen indtastes den redirect URL, som UniLock forbinder til Microsoft Entra fra (WAN sidens domænenavn for WebAdgangseditor), hvilket alternativt også kan indtastes i [Authentication]. Vær opmærksom på at URL er case-sensitiv (brug korrekte store og små bogstaver) og skal være helt magen til URL (domænenavn) angivet i konfiguration af UniLock [Indstillinger], [PollerService], [Webserver], [WebAdgang] (husk også eventuel ”https://” og ”www”).

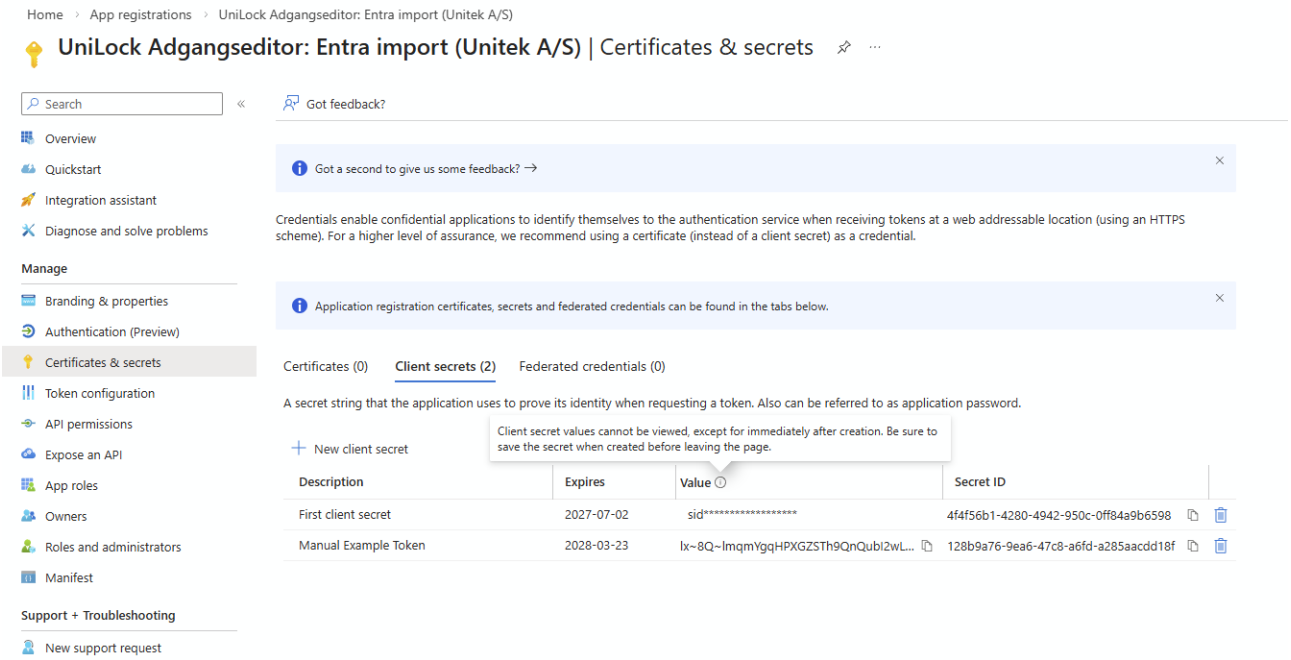
Redirect URL indsættes også i UniLock integrationen.



3.1.1.6 Client secret

Client secret er det UniLock skal bruge for at logge ind.”Client Secret” genereres ved at navigere til Certificates & Secrets. Oprette en ny ”Client Secret”. Det er vigtigt at bemærke her, at man skal kopiere value-feltet inden man forlader denne side, da dette er det eneste tidspunkt, man kan se værdien af ”Client Secret”. Værdien indsættes i UniLock integrationen.

Client Secret skal ikke deles med andre og holdes hemmelig.



3.1.2 Grupper

I Entra kan grupper oprettes for at lette den daglige drift af rettigheder mv. Disse grupper kan anvendes til automatisk at tildele rettigheder i andre systemer som fx UniLock adgangskontrol.

3.2 UniLock

Opsætning foretages under [Integrationer]. Her oprettes et nyt objekt af typen [Microsoft Entra].

3.2.1 Forbindelse

Det er muligt at vælge to forskellige forbindelsesmetoder til Entra.

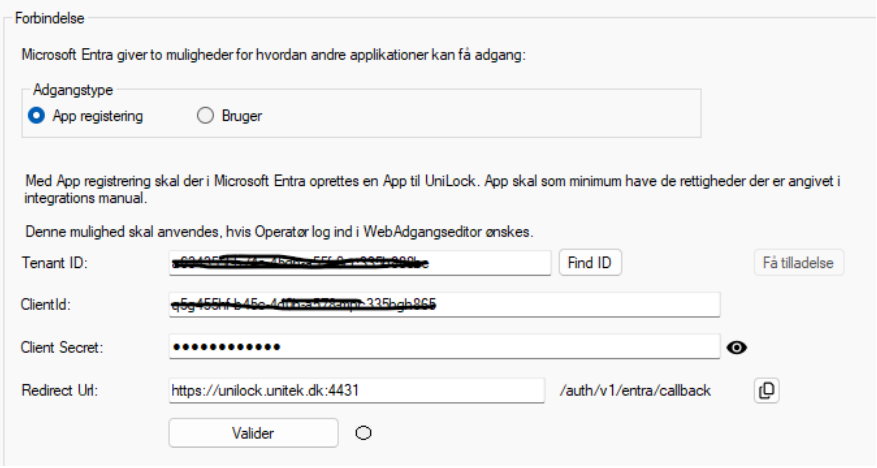
UniLock skal bruge Microsoft [Tenant ID] fra Entra for at forbinde til kundens Entra. Som en hjælp vil et tryk på [Find ID] åbne en webbrowser, hvor kundens Microsoft Entra IT-administrator kan logge ind og finde sin organisations ID (Tenant ID).

Metode 1: App registrering

Her logger UniLock ind med de på forhånd oprettede Entra App Registration.

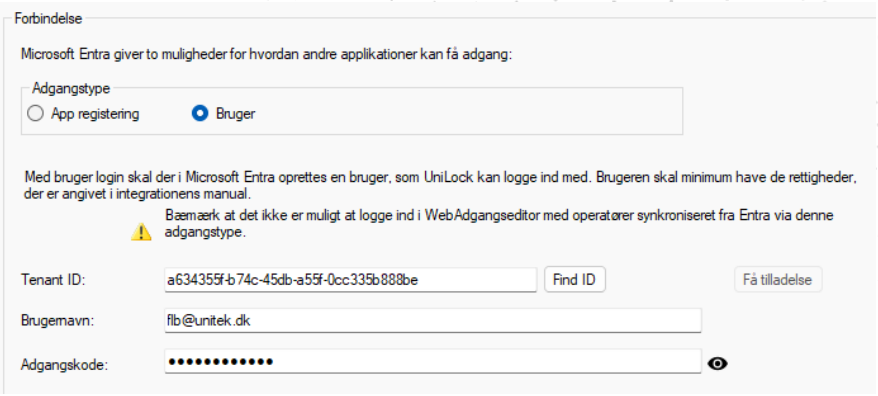
Indhold til felterne [ClientID] og [Client Secret] udleveres af kundens IT-afdeling, som har oprettet disse i forbindelse med "App registrering" til UniLock jf. afsnit 3.1.1 Tilladelse via App registrering.

Indhold i feltet [Redirect Url] bruges når operatører skal logge ind i UniLock WebAdgangseditor via operatør/login godkendelse i Entra. Url er således den web-adresse Entra skal sende operatøren til efter login, som typisk er den WebAdgangseditor tilgås på fra Internettet (fx unilock.firmawebside.dk. Url er også angivet i opsætning af UniLock WebAdgangseditor, [Indstillinger], [PollerService], [Webserver], [Webadgang].



Metode 2: Brugernavn / adgangskode

Her logger UniLock ind i Microsoft Entra med det angivne login.



Her bruges UniLock Enterprise App til at logge ind med og skal således have tilladelse til at læse fra kundens Microsoft Entra Organisation. Tryk på [Få tilladelse] som åbner en webbrowser hvor IT-administratoren kan logge ind og godkende UniLock Enterprise App.

[Valider] knappen validerer om det er muligt at hente listen af grupper i Entra.

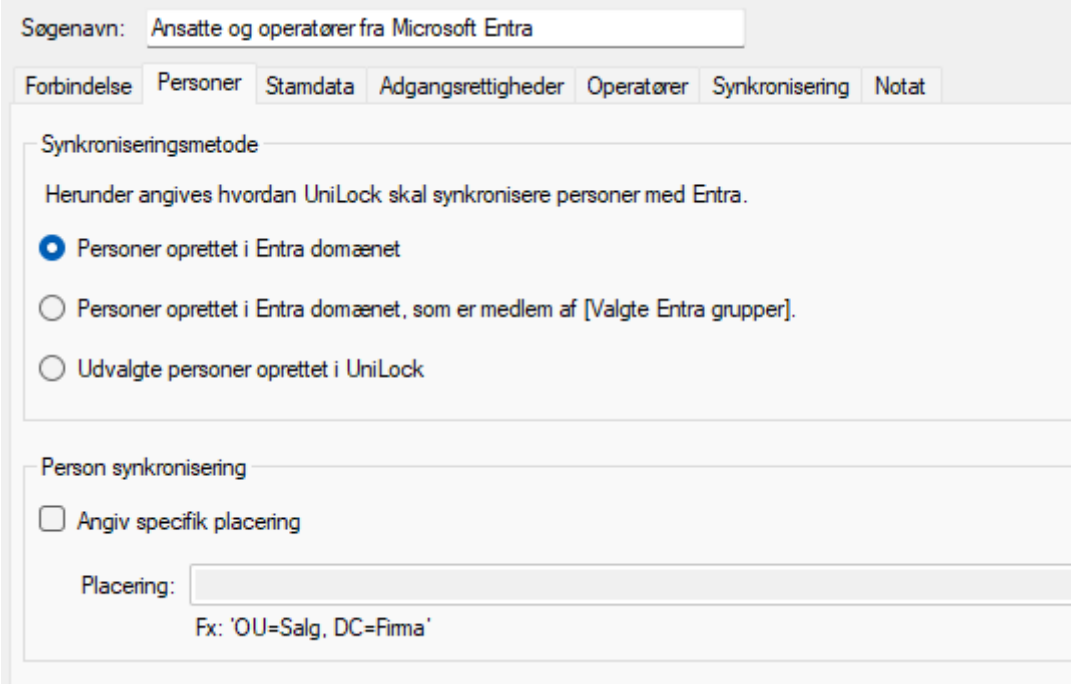
3.2.2 Personer

I dette faneblad angives hvordan UniLock skal finde personer i Entra, som skal synkroniseres til UniLock og hvordan UniLock skal håndtere personer, som er fjernet eller har fået fjernet deres rettigheder i Entra.

Personer som oprettes på anden måde i UniLock og ikke synkroniseres med Entra, vil ikke blive berørt af synkroniseringen.

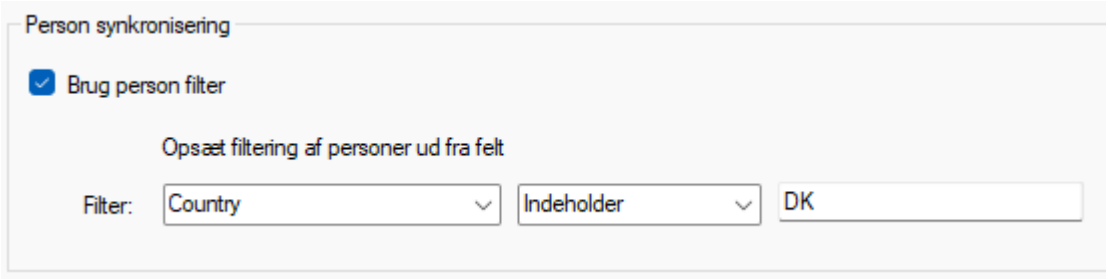
Når en person er synkroniseret med Entra, så anvendes personens bagvedliggende Entra guid (Global Unique Identifier) fremadrettet, således at de synkroniserede data for personen altid genetableres ved næste synkronisering.

Personer oprettet i organisationen

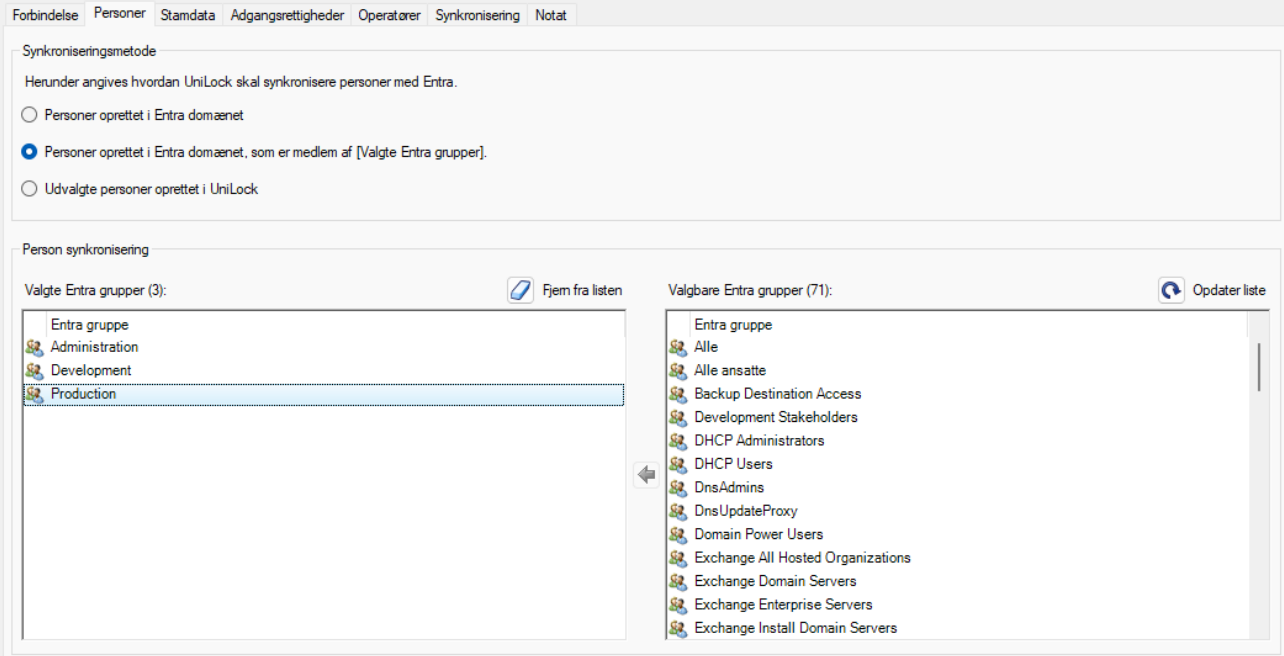


Her hentes alle personer oprettet i Entra organisationen.

Dette kan dog begrænses ved at tilføje valgbar filtrering af personer:



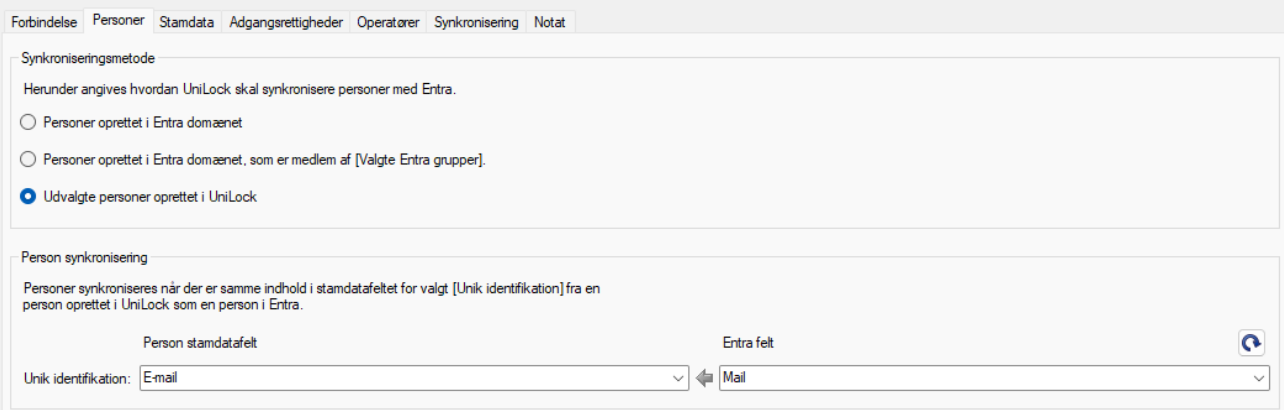
Personer oprette i organisationen fra udvalgte grupper



Her hentes alle personer oprettet i Entra domænet, som er medlem af valgte Entra grupper.

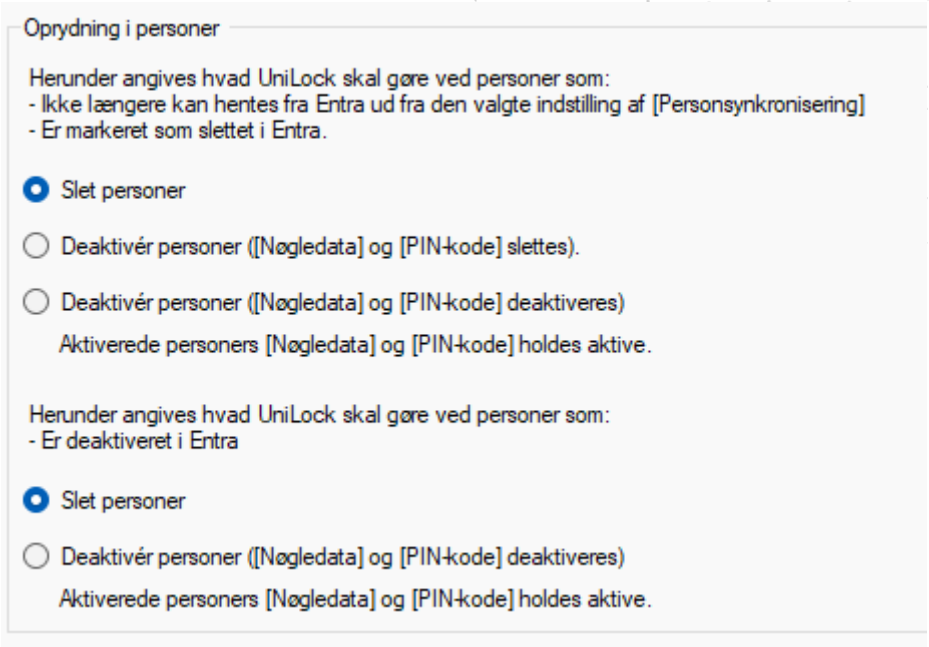
[Opdater liste] knappen indlæser tilgængelige Entra-grupper, som herefter kan vælges for synkronisering. Bemærk at Microsoft angiver at der kan være en forsinkelse på timer, fra en gruppe oprettes til den er tilgængelige for eksterne system, som fx UniLock.

Udvalgte personer oprettet i UniLock



Her oprettes personer manuelt i UniLock med unikt [Søgenavn] og unikke data i personers stamdatafeltet valgt for [Unik identifikation]. Findes personen ved næste synkronisering i Entra ud fra [Unik identifikation], indlæses personens øvrige data fra Entra til UniLock. Nu er UniLock personen bundet til personen i Entra og den valgte metode til [Oprydning i personer] vil blive anvendt.

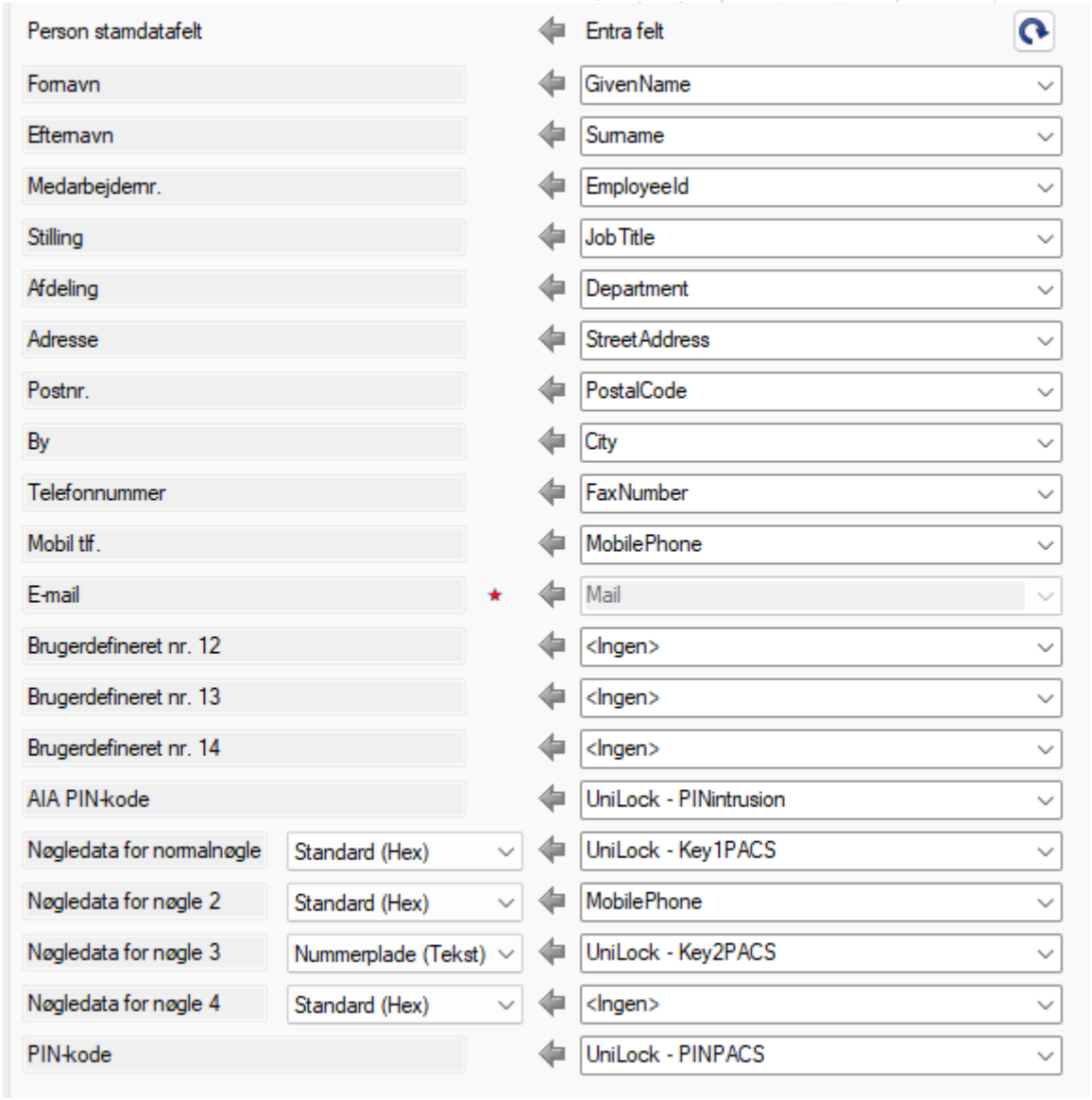
Oprydning i personer



Når personer deaktiveres/fjernes eller personers rettigheder fjernes i Entra, vil deres adgang i k-punkter blive fjernet med det samme da nøglen og PIN-koden slettes/deaktiveres i UniLock.

Bevares personer i UniLock databasen, skal operatøren udføre oprydning på et senere tidspunkt, men det vil samtidig blive nemmere at efterforske, hvor personerne har fået adgang i bygningerne, inden personerne ikke længere kunne hentes fra Entra. Hvis operatører tilføjer personers nøgle i UniLock, vil denne indstilling også sikre at personers nøgler ikke slettes, hvis personer fejlagtigt flyttes/slettes i Entra.

3.2.3 Stamdata



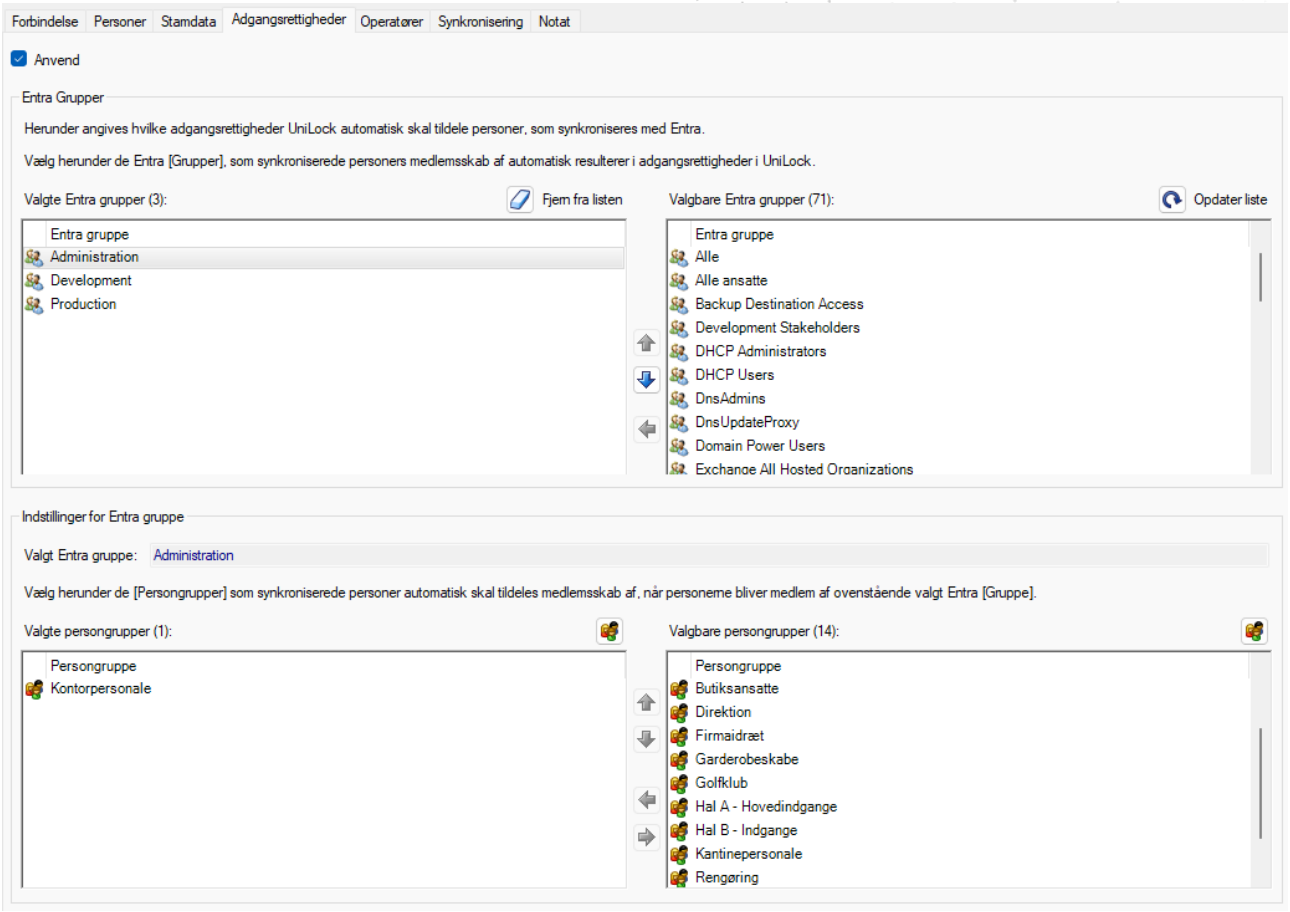
Her indstilles hvordan personers data skal overføres fra Entra til UniLock.

knappen indlæser valgmuligheder for [Entra felt], som en hjælp til at finde de respektive felter. Herefter kan man indtaste noget af feltets navn i feltet, som så vil vise søgeresultatet ud fra indtastningen.

I det viste eksempel hentes fx personers Nøgledata fra Entra Custom Security Attributes [Key1PACS] og PIN-kode fra Entra Custom Security Attribute [PINPACS] som begge er oprettet til adgangskontrol formål (Navngivet PACS: Physical Access Control System). Nøgledata og PIN-kode kan udfyldes i UniLock af operatøren, hvis UniLock ikke er indstillet til at synkronisere felterne.

PS: UniLock understøtter både Custom Security Attributes og Custom Directory Extensions Attributes, hvor sidstnævnte skal følge nomenklaturen: ”extension_UnitekAppClientID_xxx”.

3.2.4 Adgangsrettigheder

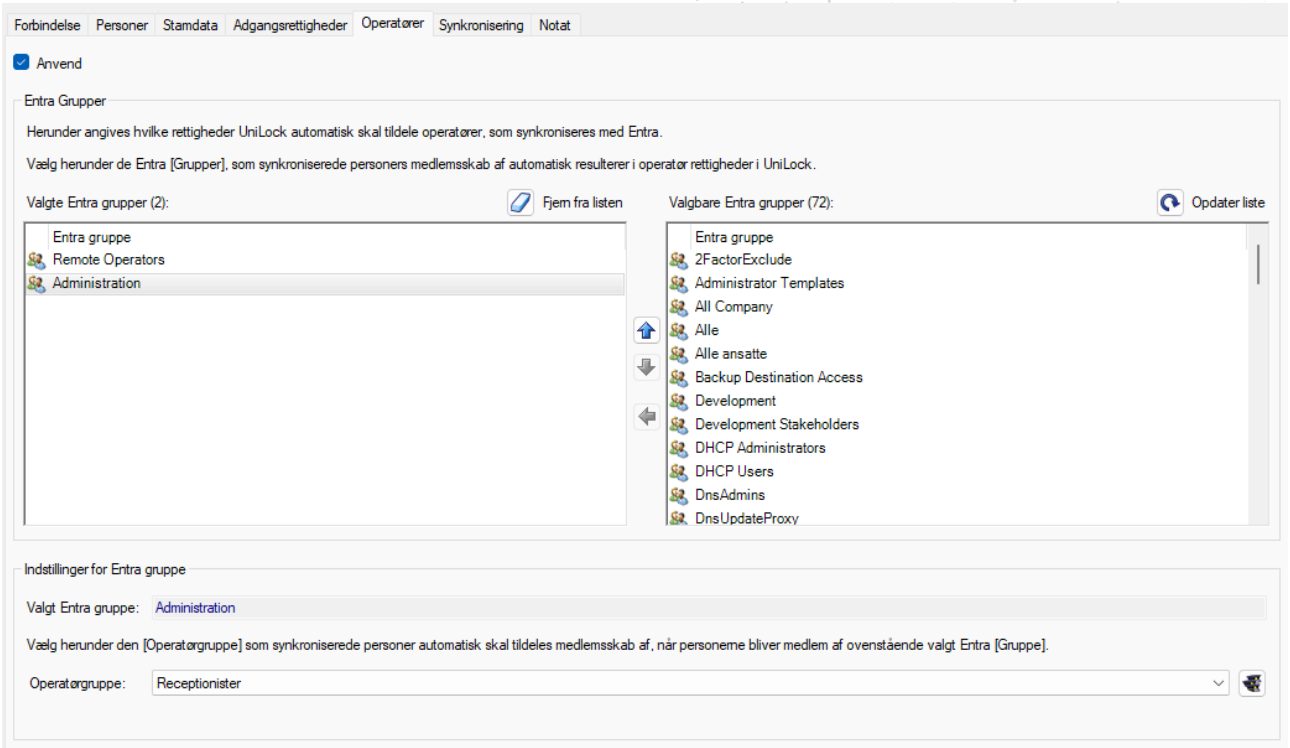


Her indstilles eventuelt hvordan personer automatisk tildeles adgangsrettigheder i UniLock ud fra hvilke Entra-grupper og deres undergrupper (nested groups) personer er medlem af.

Aktiveres synkronisering af adgangsrettigheder, vil personers medlemskab af de valgte synkroniseringsgrupper i UniLock blive styret udelukkende fra Entra, hvor eventuelle operatørændringer af disse grupper automatisk overskrives ved næste Entra-synkronisering. Operatører vil altid have mulighed for at ændre personers øvrige adgangsrettigheder (medlemskab af persongrupper og direkte adgangsrettigheder til k-punkter).

Både [Valgte Entra grupper] og [Valgte persongrupper] er prioriteret således, at den nederste valgte gruppe har højeste prioritet. For yderligere information henvises til manual for pc-programmet.

3.2.5 Operatører



Her kan indstilles hvordan personer i Entra automatisk oprettes som UniLock operatører og tildeles adgangsrettigheder i UniLock ud fra hvilke Entra-grupper og deres undergrupper (nested groups) personer er medlem af.

Aktiveres synkronisering af operatører, vil importerede operatørers medlemskab af operatørgrupper i UniLock blive styret udelukkende fra Entra.

Operatørers søgenavn er Entra attributten ”displayname” som fx ”Hans Peder Jensen. Loginnavnet er Entra attributten “Email”, som er samme login som når personen skal logge ind i Windows.

En Entra importeret operatør slettes fra UniLock, når personen slettes fra Entra eller ikke længere har medlemskab af de valgte Entra-grupper.

Logge ind

En Entra importeret operatør kan logge ind i UniLock så længe vedkommende er aktiv i Entra (og ikke ’expired’ eller ’disabled’ i Entra) og overholder de sikkerhedspolitikker der er konfigureret i Entra.

3.2.6 Synkronisering

UniLock henter automatisk de nyeste informationer fra Entra én gang i timen og en fuld synkronisering hver nat ca. kl. 3.

[Synkroniser] knappen udfører en fuld synkronisering fra Entra til UniLock.

3.2.7 Logfiler

Logfiler for de seneste importresultater gemmes, og kan vises som en hjælp i forbindelse med test og fejlfinding. Logfiler genereres kun, når der er nye informationer at hente i Entra.

4. Personattributter i Microsoft Entra

Som en hjælp til opsætning af automatisk udfyldning af personers stamdatafelter i UniLock med data fra personattributter fra Microsoft Entra, viser denne tabel en oversigt over relevante personattributter i Microsoft Entra og deres beskrivelse.

Den fuldstændige liste over personattributter i Microsoft Entra kan pt. findes hos Microsoft via dette link: https://learn.microsoft.com/en-us/entra/external-id/customers/concept-user-attributes

Attribut	Beskrivelse
givenName	First name
surname	Surname (family- or last name)
displayName	Name displayed in address book (usual first, inital, last names)
email	SMTP address
postalCode	Postal code or ZIP code
streetAddress	Street address of place of businness
jobtitle	Job title
city	City
country	Country/Region
state	State/Province