UniLock
System 10

Manual
Integration med Active Directory

Projekt	PCS125
Version	2.0
Revision	2024-08-29

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

Personer/operatører og deres attributter hentes i Active Directory 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 AD, så fjernes personerne eller deres rettigheder også automatisk i UniLock.

Indholdsfortegnelse

1. Beskrivelse 3

1.1 Generel beskrivelse 3
1.2 Kanaler 4
1.3 Program-moduler 4

2. Operatør-vejledning 5

2.1 Personers adgangsrettigheder 5
2.2 Operatørers adgangsrettigheder 5
2.3 Active Directory 5
2.3.1 Personer i Active Directory 5
2.3.2 Grupper 6

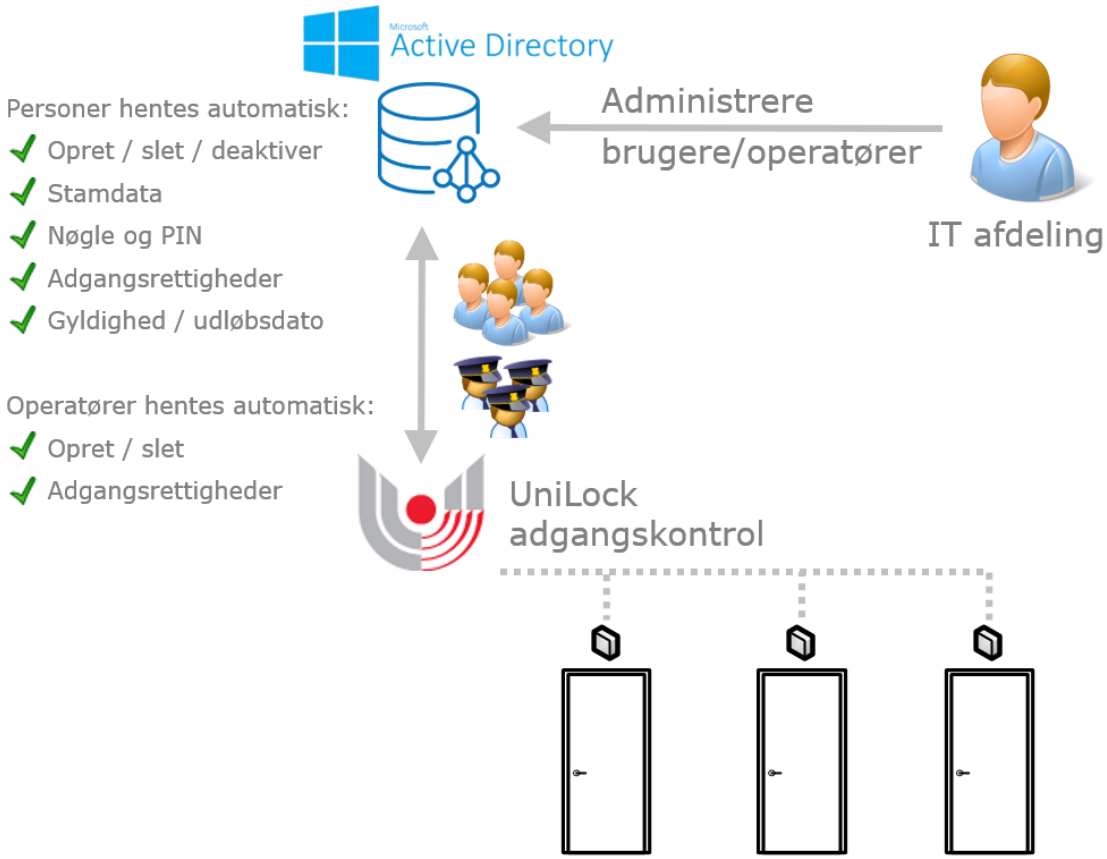
3. Installations-vejledning 7

3.1 Active Directory (AD) 7
3.1.1 Formål med AD og LDAP 7
3.1.2 Login og adgang 7
3.1.3 Grupper 7
3.2 UniLock 8
3.2.1 Forbindelse 8
3.2.2 Personer 8
3.2.3 Stamdata 12
3.2.4 Adgangsrettigheder 13
3.2.5 Operatører 14
3.2.6 Synkronisering 14
3.2.7 Logfiler 15

4. Personattributter i Active Directory 16

1. Beskrivelse

1.1 Generel beskrivelse



Anvendelse

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

Når ansatte mv. og deres rettigheder administreres i Active Directory - så administreres disse også automatisk i UniLock.

Active Directory 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 Active Directory, hvorfra andre systemer automatisk kan hente personers stamdata, login, mailadresse, grupperettigheder mv. Personers placering og grupperettigheder i Active Directory 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 Active Directory med medlemskab af gruppen for receptionister, så kan Julia automatisk oplåse døre og frakoble tyverialarmer i kontorområ-

det styret af UniLock og anvende UniLock pc-programmet med begrænsede operatørrettigheder.

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

Beskrivelse

Med denne import mulighed kan Active Directory 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 Active Directory 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 Active Directory, 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 Active Directory.

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 Active Directory, og en kanal som henter lokalebookinger fra Outlook (Exchange Server).

1.3 Program-moduler

Import er mulig, når der er tegnet licens til import-modulet, eller programmet er i demo-mode.

2. Operatør-vejledning

2.1 Personers adgangsrettigheder

Aktiveres synkronisering af personers adgangsrettigheder fra Active Directory, vil personers medlemskab af grupper i UniLock blive styret udelukkende fra AD, hvor eventuelle operatørændringer automatisk overskrives ved næste AD-synkronisering.

Operatører vil altid have mulighed for at overstyre personers adgangsrettigheder tildelt fra AD (medlemskab af persongrupper) med direkte adgangsrettigheder til k-punkter, hvis operatøren har operatørrettigheder til dette.

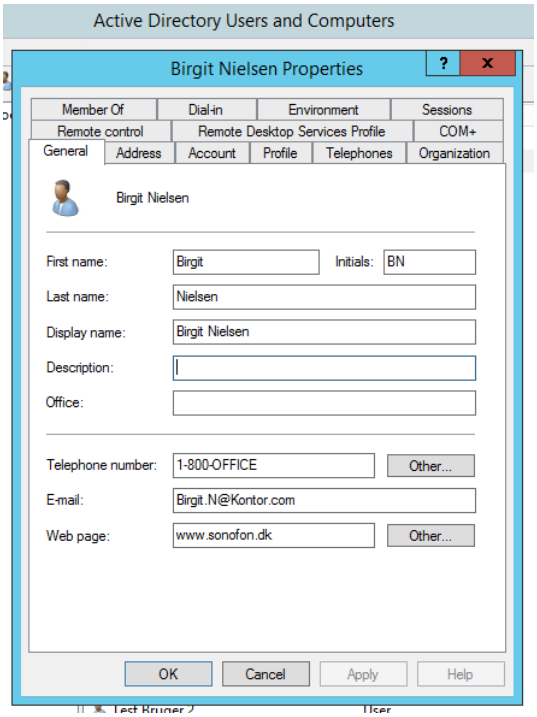
2.2 Operatørers adgangsrettigheder

Aktiveres synkronisering af operatører fra Active Directory, vil de importerede operatørers medlemskab af operatørgruppe i UniLock blive styret udelukkende fra AD, hvor eventuelle operatørændringer automatisk overskrives ved næste AD-synkronisering.

2.3 Active Directory

2.3.1 Personer i Active Directory

AD personer kan have tilknyttet en række attributter, hvor en oversigt over de mest almindelige kan findes i afsnit 4.
Nedenstående er et eksempel på hvordan en person kan ses/editeres i AD:



I AD kan personer placeres i en organisatorisk enhed (OU) og have medlemskab af flere grupper.

2.3.2 Grupper

I AD 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. Installations-vejledning

3.1 Active Directory (AD)

Active Directory er et meget udbredt IT-værktøj til at styre rettigheder mv. i Windows og lignende IT-miljøer.

3.1.1 Formål med AD og LDAP

Active Directory (AD) er en indførelse af Lightweight Directory Access Protocol (LDAP) i Windows miljøer.

LDAP får en række forskelligartede systemer til at anvende en fælles kilde for brugeroplysninger. Dette reducerer besværet ved den daglige administration af virksomhedens systemer væsentligt. Dette gælder både for administratorerne og brugerne der ikke skal huske mange forskellige brugernavne og kodeord.

AD's vigtigste opgave er at sørge for at godtgøre ægtheden og adgangstilladelse af tjenesterne for Windows baserede computere. Active Directory giver også administrationen mulighed for at tildele politikker, udrulle software, og anbringe kritiske opdateringer til en organisation. Active Directory opbevarer informationer og indstillinger i en central database.

AD er en hierarkisk opbygget struktur af objekter. Objekterne er inddelt i 3 kategorier:

- Ressourcer (fx printere)
- Tjenester (fx e-mail)
- Brugerne (bruger konti og grupper)

AD kan inddeles i forskellige organisatoriske enheder (OU) for at lette administration af disse enheder. Populært sagt kan OU sammenlignes med, at man på en harddisk (AD) opretter filmapper (OU) til at placere filer (personer, printere mv.) i.

3.1.2 Login og adgang

I Active Directory oprettes det login, som UniLock skal anvende for at logge ind i Active Directory og læse data.

Det anbefales at anvende sikret kommunikation (SSL/TLS) ved hjælp af LDAPS. Det anvendte LDAPS-certifikat skal installeres på UniLock installations-pc, så denne har tillid (trust) til Active Directory serveren.

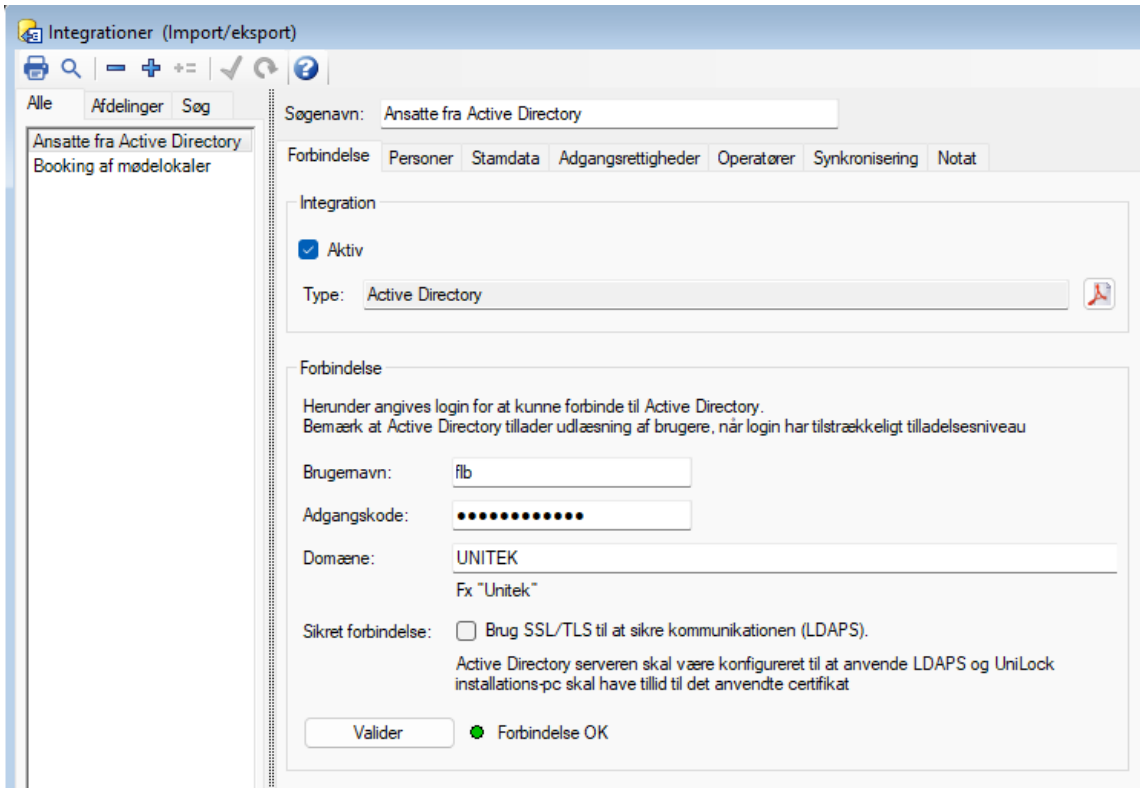
Forbindelsen kan testes med Windows værktøjet LDP.exe, som i Windows 11 tilføjes via [Settings], [System], [Optional feature], [View features] ”RSAT: Active Directory Certificate Services Tools”.

3.1.3 Grupper

I AD 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 [Import/Eksport]. Her oprettes et nyt objekt af typen [Active Directory].



3.2.1 Forbindelse

Angiv brugernavn og adgangskode med adgang til at læse informationer fra Active Directory domænet.

Er Active Directory serveren konfigureret til sikret forbindelse med LDAPS, så aktiveres dette her også her.

[Valider] knappen validerer om det er muligt at hente listen af grupper i Active Directory med det angivne login.

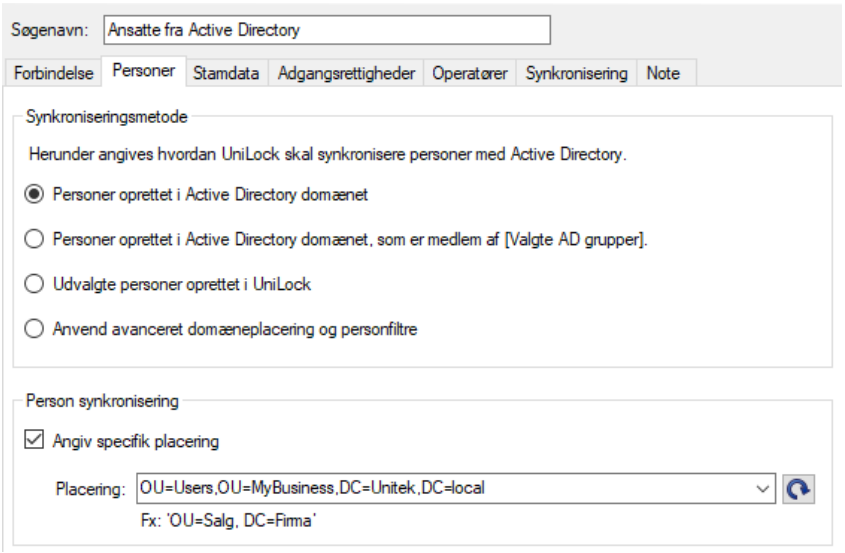
3.2.2 Personer

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

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

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

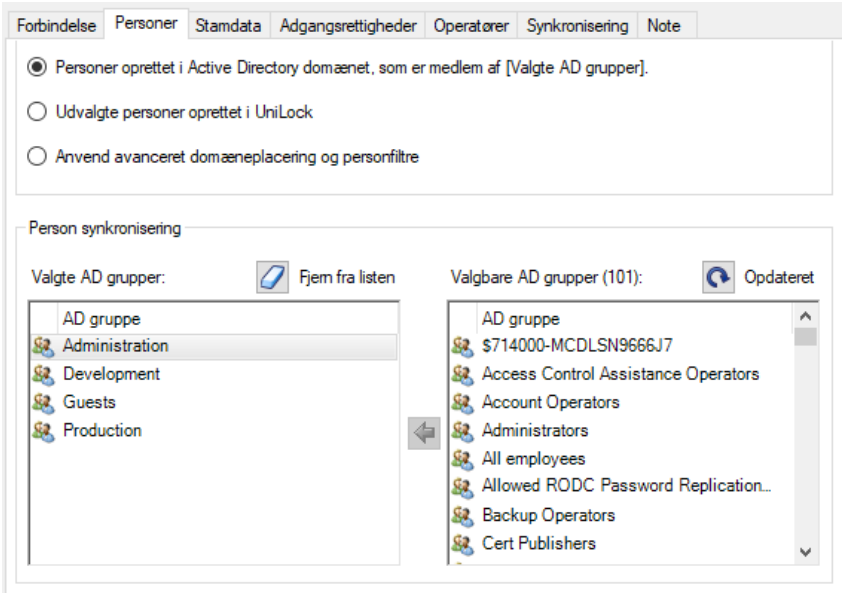
Personer oprettet i domænet



Her hentes alle personer oprettet i AD domænet. Det er endda muligt at vælge en specifik organisatorisk enhed (OU) i Active Directory at hente alle personer fra, hvilket kan sammenlignes med at hente filer (personer) fra en bestemt mappe (OU) på harddisken (AD).

knappen indlæser muligheder for placering fra AD.

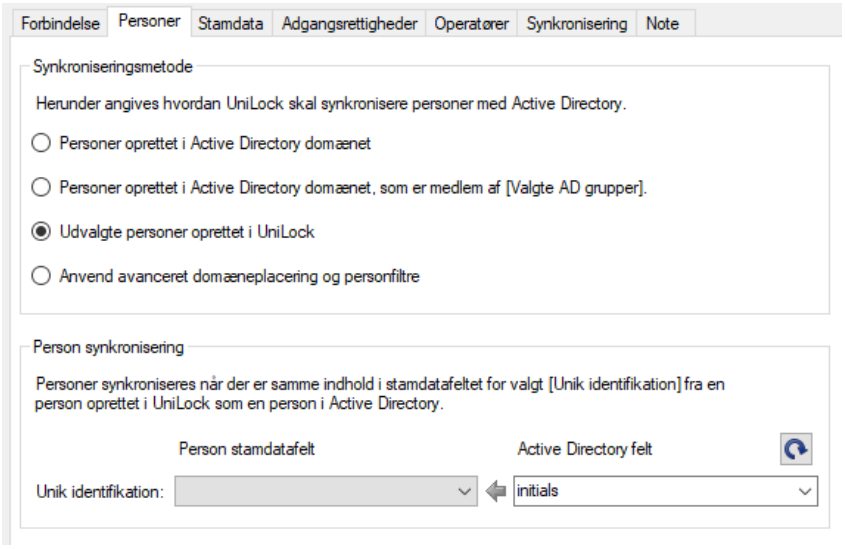
Personer oprette i domænet fra udvalgte grupper



Her hentes alle personer oprettet i AD domænet, som er medlem af valgte AD grupper og deres undergrupper (nested groups).

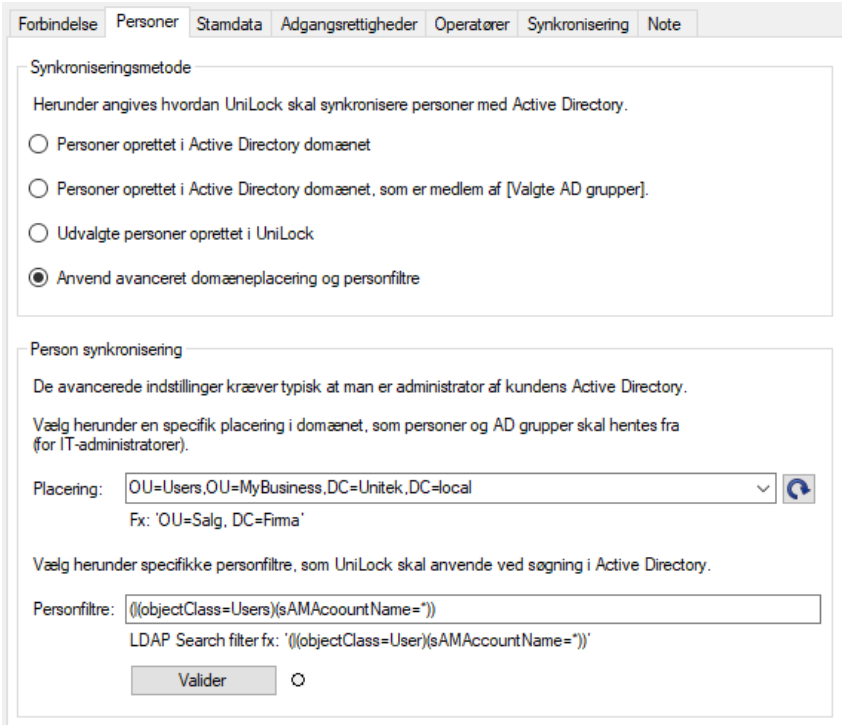
[Opdater liste] knappen indlæser tilgængelige AD-grupper, som herefter kan vælges for synkronisering.

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 AD ud fra [Unik identifikation], indlæses personens øvrige data fra AD til UniLock.

Avanceret

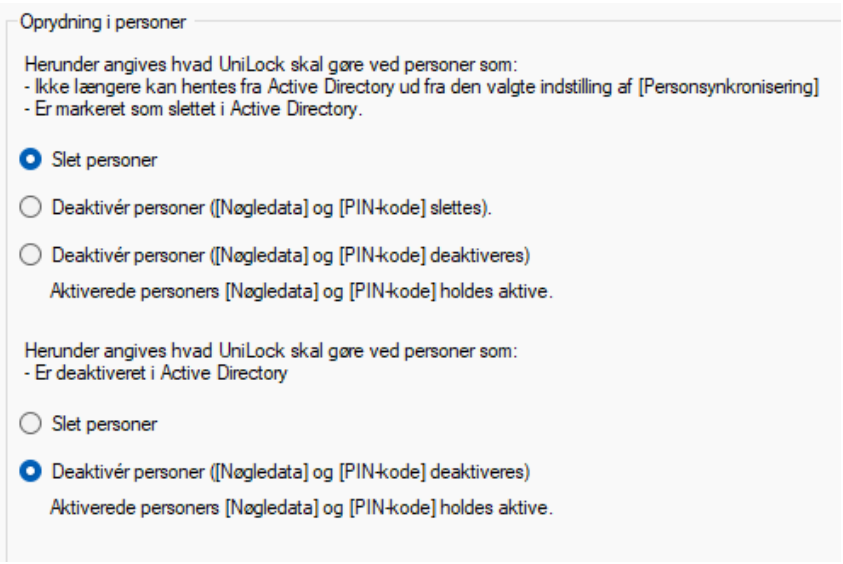


Her har IT-administratoren af Active Directory mulighed for at specificere den placering personer skal hentes fra og hvilke personfiltre der anvendes ved søgning efter personer. Personfilteret skrives jf. LDAP Search filter syntax.

knappen indlæser muligheder for placering fra AD.

[Valider] knappen validerer, om det indtastede personfilter er muligt at anvende i AD.

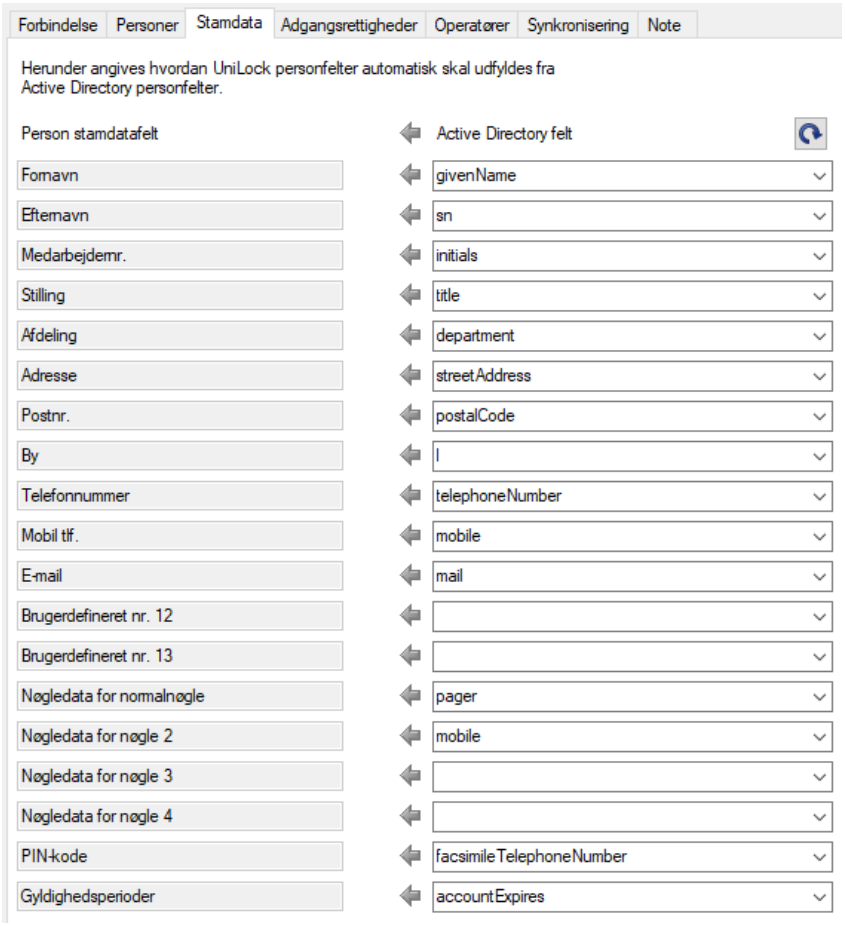
Oprydning i personer



Når personer deaktiveres/fjernes eller personers rettigheder fjernes i AD, 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 AD. Hvis operatører tilføjer personers nøgle i UniLock, vil denne indstilling også sikre at personers nøgler ikke slettes, hvis personer fejlagtigt flyttes/slettes i AD.

3.2.3 Stamdata

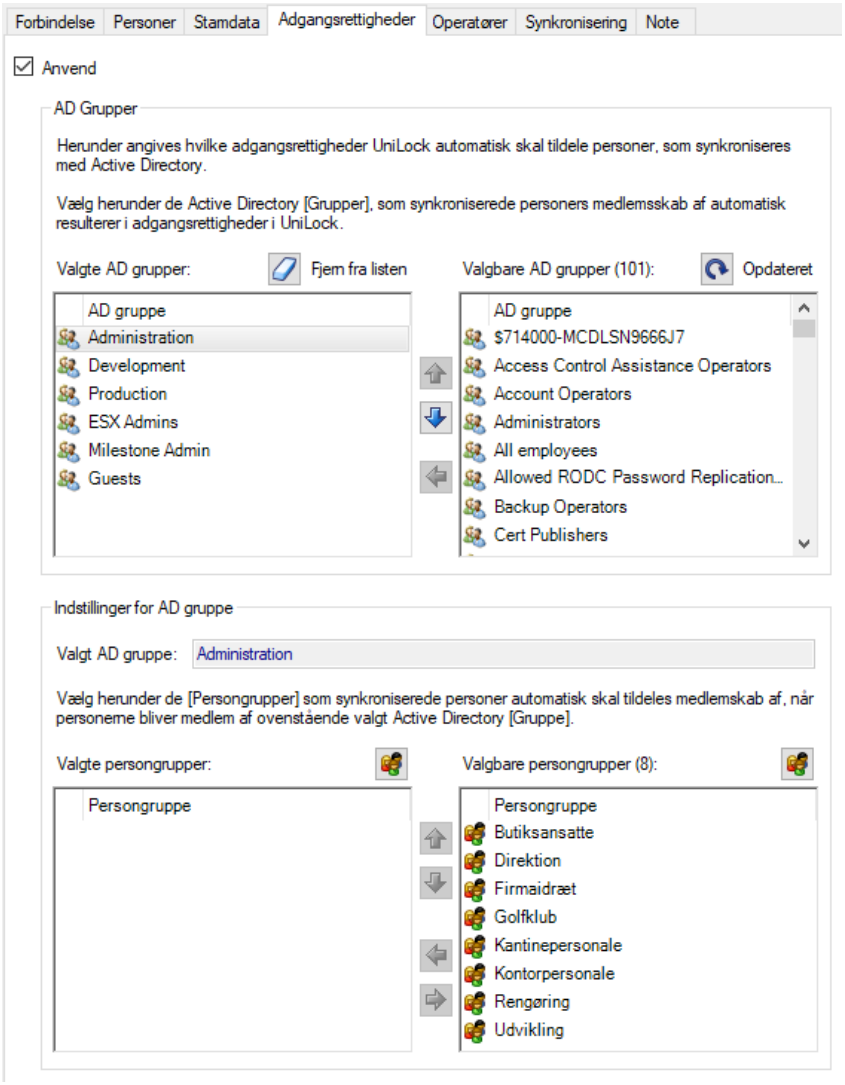


Her indstilles hvordan personers data skal overføres fra Active Directory til UniLock.

knappen indlæser valgmuligheder for [Active Directory felt], som en hjælp til at finde de respektive felter.

I det viste eksempel hentes fx personers Nøgledata fra AD feltet [Pager] og PIN-kode fra AD feltet [Fax] som begge typisk er ubrugte. Nøgledata og PIN-kode kan udfyldes i UniLock af operatøren, hvis UniLock ikke er indstillet til at synkronisere felterne.

3.2.4 Adgangsrettigheder



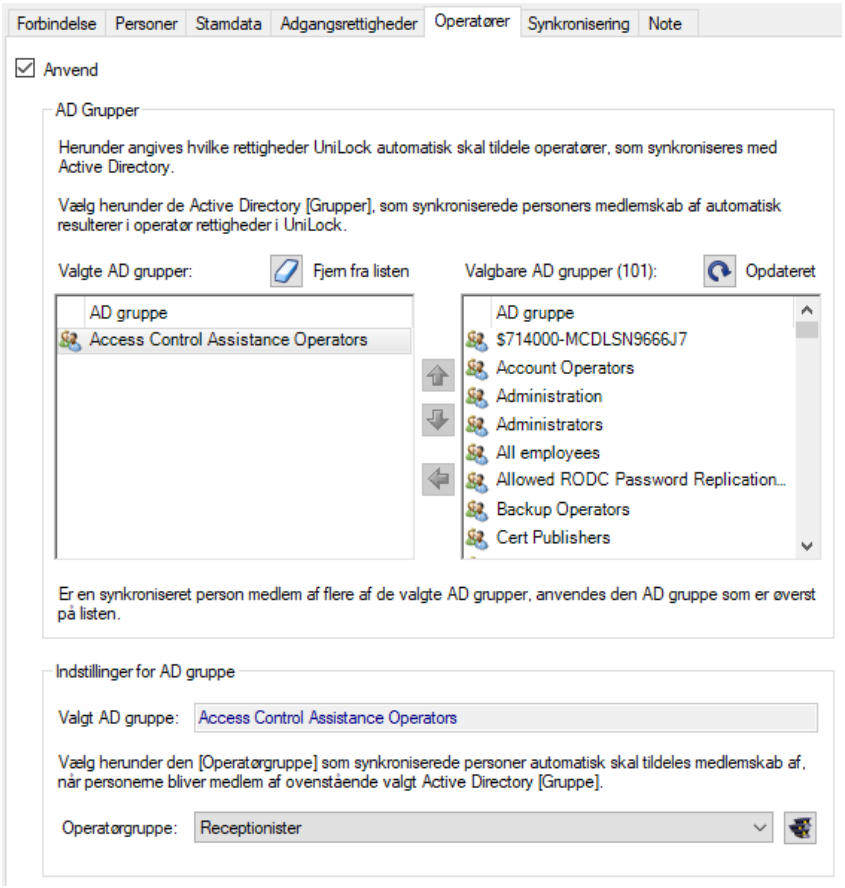
Her indstilles eventuelt hvordan personer automatisk tildeles adgangsrettigheder i UniLock ud fra hvilke AD-grupper og deres undergrupper (nested groups) personer er medlem af.

Aktiveres synkronisering af adgangsrettigheder, vil personers medlemskab af grupper i UniLock blive styret udelukkende fra AD, hvor eventuelle operatørændringer automatisk overskrives ved næste AD-synkronisering. Operatører vil altid have mulighed for at overstyre personers adgangsrettigheder tildelt fra AD (medlemskab af persongrupper) med direkte adgangsrettigheder til k-punkter.

En persons nøgle aktiveres når personen er medlem af en af de valgte AD grupper. En persons nøgle deaktiveres, når personen ikke er medlem af en af det valgte AD grupper.

Både [Valgte AD 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 AD automatisk oprettes som UniLock operatører og tildeles adgangsrettigheder i UniLock ud fra hvilke AD-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 AD.

Operatørers søgenavn opbygges af ”det indtastede domæne i AD synkronisering” og Active Directory attributten ”name” som fx ”Unitek\Hans Peder Jensen. Loginnavnet er Active Directory attributten “sAMAccountName” som er samme login som når personen skal logge ind i Windows.

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

Logge ind

En AD importeret operatør kan logge ind i UniLock så længe vedkommende er aktiv i AD (og ikke ’expired’ eller ’disabled’ i AD).

3.2.6 Synkronisering

UniLock henter automatisk de nyeste informationer fra AD én gang i timen.

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

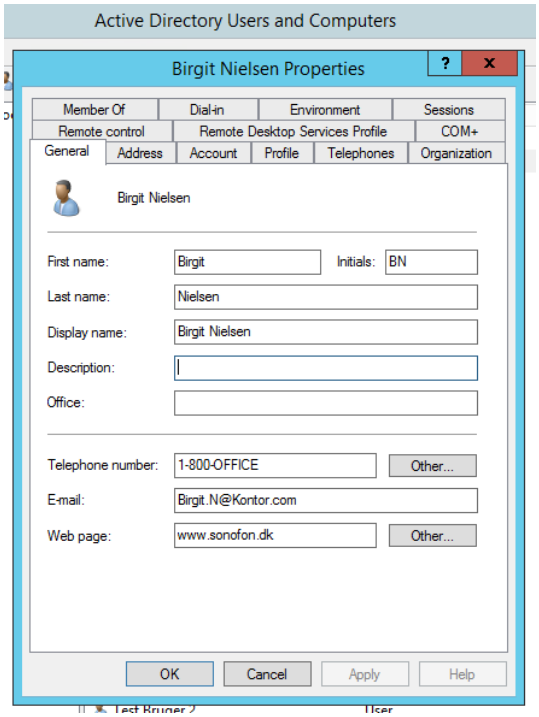
3.2.7 Logfiler

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 AD.

4. Personattributter i Active Directory

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

Den fuldstændige liste over personattributter i Active Directory kan pt. findes hos Microsoft via dette link: https://msdn.microsoft.com/en-us/library/ms677979(v=vs.85).aspx eller hos kouti via dette link: http://www.kouti.com/tables/userattributes.htm



Attribut	Beskrivelse	AD felt
givenName	First name	[General], [First name]
sn	Surname (family- or last name)	[General], [Last name]
middleName	Middle Name	
displayName	Name displayed in address book (usual first, inital, last names)	[General], [Display name]
initials	Initial parts of full name	[General], [Initials]
description	Description of user	[General], [Description]
telephoneNumber	Primary telephone number place of business	[General], [Telephone number]
otherTelephone	Alternate telephone numbers place of business	[General], [Telephone number], [Other]
mail	SMTP address	[General], [E-mail]
wWWHomePage	Primary webpage	[General], [Web page]
physicalDeliveryOfficeName	Office location in place of business	[General], [Office]
l	User address town or city	[Address], [City]
postalAddress	Postal address	
postalCode	Postal code or ZIP code	[Address], [Zip/Postal Code]
st	State or province in user address	[Address], [State/province]
streetAddress	Street address of place of businness	[Address], [Street]
userPrincipalName	Logon name	[Account], [User logon name]
sAMAccountName	Logon name supporting previous Windows versions	[Account], [User logon name (pre-Windows)]
accountExpires	Specifies when an account expires	[Account], [Account expires]
facsimileTelephoneNumber	Business fax machine number	[Telephones], [Fax]
otherFacsimileTelephoneNumber	Alternate fax machine numbers	[Telephones], [Fax], [Other]
homePhone	Home telephone number	[Telephones], [Home]
ipPhone	IP Phone number	[Telephones], [IP phone]
otherIpPhone	Alternate IP Phone numbers	[Telephones], [IP phone], [Other]
Mobile	Primary cellular telephone number	[Telephones], [Mobile]
otherMobile	Alternate cellular telephone numbers	[Telephones], [Mobile], [Other]
pager	Primary pager telephone number	[Telephones], [Pager]
otherPager	Alternate pager telephone numbers	[Telephones], [Pager], [Other]
title	Jobtitle	[Organization], [Job title]
department		[Organization], [Department]