



# SIMS Active Directory Service 7.0

## Installation- og Konfigurationsmanual

Version	Forfatter	Ændringer	Dato
7.0	Christian Tyllesen	Komplet revideret	22.10.2021
7.0.1	Christian Tyllesen	Præcisering af Azure AD DS understøttelse	01.09.2023

## Indhold

Beskrivelse.....	3
Adgangsniveauer gennem AD grupper .....	4
Områdegrupper gennem AD grupper .....	4
Adgangsniveauer gennem OU .....	4
Gyldighed.....	4
Funktioner.....	4
Forudsætninger og nødvendigheder .....	5
SIMS Active Directory Service installation .....	6
AD Service SQL bruger.....	7
Administration- og Konfigurationsinterface .....	8
Installation/Opstart .....	9
Bruger oprettelse .....	9
SQL Server konfiguration .....	10
SQL Config .....	10
AD Server konfiguration .....	11
AD Config .....	12
Service og Logs.....	13
Administration og konfiguration .....	14
Log ind .....	14
Dashboard (Oversigt) .....	14
Configuration (Konfigurationssiden).....	15
AD Config .....	16
AD <-> SQL Fieldmapping.....	16
AD <-> SIMS UserProfile ( <b>User</b> ).....	17
AD <-> SIMS UserProfile ( <b>Contact</b> ) .....	17
OU <-> SIMS UserProfile ( <b>User</b> ).....	18
OU <-> SIMS UserProfile ( <b>Contact</b> ) .....	18
AD <-> SIMS Area Group ( <b>User</b> ):.....	18
AD <-> SIMS Area Group ( <b>Contact</b> ): .....	19
Licensering .....	19
Generelt om konfigurationssiden .....	20
Checkliste .....	20

## Beskrivelse

Integrationen er udviklet til brug med On-premise Microsoft Active Directory Domain Services eller Microsoft Azure Active Directory Domain Services.

Integrationen benytter LDAP/LDAPS til opslag, og Kerberos, NTLM som verifikationsteknologi.

Andre AD/LDAP typer, samt verifikationsteknologier kan ikke garanteres at fungere 100% med denne integration.

SIMS integration med Microsoft Active Directory, er implementeret, via en mellemdatabase i MS SQL Serveren som også indeholder [NOX] databasen.

Løsningen består af en Windows Service som henter data fra AD og lagrer det i databasen [NOX], tabellen [UsersToSIMS] og nogle SQL Triggers som søger for at flytte data fra [UsersToSIMS] til [SIMSCodesAutoUpdate] tabellen.

Ud fra en forud defineret matrix mellem SIMS grupper og AD grupper, vil medarbejdere kunne oprettes med rettigheder i NOX Systemet, direkte.

Alternativt vil det være muligt at trække data over til en CardExchange software (Kort produktion) og først når der bliver tildelt et adgangskort, vil medarbejderen blive overført til SIMS og oprettet i NOX.

Når man vælger AD integration til SIMS, vil brugere som oprettes derigennem, blive taget således at de er lette at genkende og bliver styret igennem brugerens AD attributter. Det er stadig muligt at oprette brugere direkte i SIMS, disse brugere skal altid håndteres manuelt og direkte i SIMS.

### Adgangsniveauer gennem AD grupper

Der udformes en matrix som fortæller hvilke AD grupper der skal passe til hvilke profiler i SIMS. Vi anbefaler at der oprettes specifikke AD grupper som kan pares op med SIMS profilerne.

### Områdegrupper gennem AD grupper

Der udformes en matrix som fortæller hvilke AD grupper der skal passe til hvilke Områdegrupper i SIMS. Vi anbefaler at der oprettes specifikke AD grupper som kan pares op med SIMS Områdegrupper.

### Adgangsniveauer gennem OU

Det er muligt at pege på specifikke OU, som parres med en SIMS profil. Alle brugere indeholdt i denne OU vil så få samme SIMS profil.

### Gyldighed

En medarbejder er gyldig i SIMS/NOX, så længe at AD kontoen er aktiv. Hvis der er angivet udløbsdato på kontoen, eller den spærres, vil den også blive spærret i SIMS/NOX.

### Funktioner

SIMS Active Directory Service tilgår og understøtter følgende AD features:

- Fornavn-, og Efternavn
- Konto udløb (Account expires)
- Spærret bruger (Account is disabled)
- Initialer (SamAccount)
- Bestemt OU-container til AD grupper (scanner KUN valgte OU)
- Valgfrie attributter til opbevaring af kortnummer, PIN- og NOX-koder
- Yderligere attributter reserveret til fremtid brug

SIMS Active Directory Service installeres som en Windows Service, som synkroniserer data efter et forud defineret interval, standardtiden er sat til hvert 30. minut, det er naturligvis efter eget valg hvis der er andre ønsker.

Det er også muligt at synkronisere efter behov i Administrationsinterfacet.

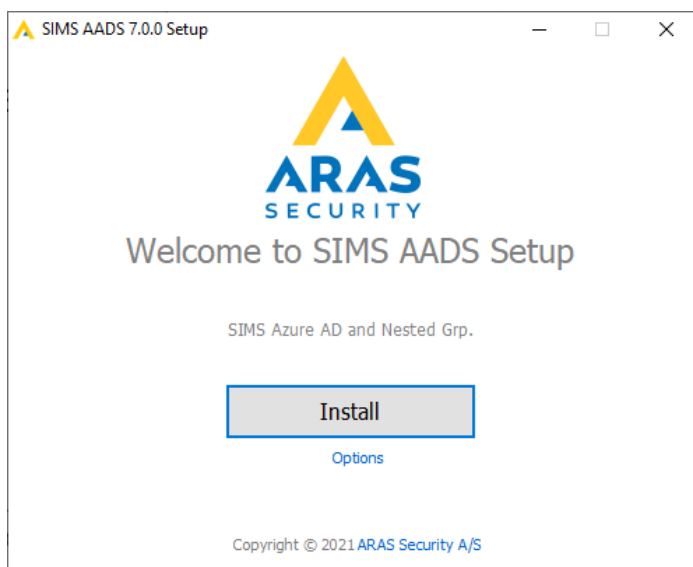
## Forudsætninger og nødvendigheder

- En SIMS Server installation
- En Microsoft© SQL Server
- Vi skal have en AD bruger
- Vi skal have et Hostname/IP-adresse på Domain Controlleren
- Vi skal have en SQL Bruger (db\_owner på [NOX] databasen)
- Vi skal kende SQL Server navn og evt. instans
- Eventuelt skal vi vide hvilken OU vi skal kigge i
- Hvilke Attributter vi skal kigge i (hvor er kortnummer, PIN-, NOX Kode)
- AD grupper -> SIMS profiler
- Hvor ofte skal SIMS synkroniseres med AD

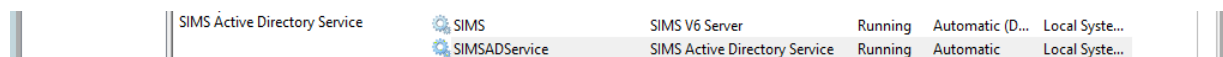
Konfiguration af ovenstående kan foretages af kunden selv, evt. i samarbejde med installatøren og/eller ARAS.

## SIMS Active Directory Service installation

SIMS Active Directory Service installations fil skal installeres på samme Windows Server som SIMS er installeret på. SIMS Active Directory Service installeres i samme folder under denne sti: C:\SIMSV6\AddOns\ADService

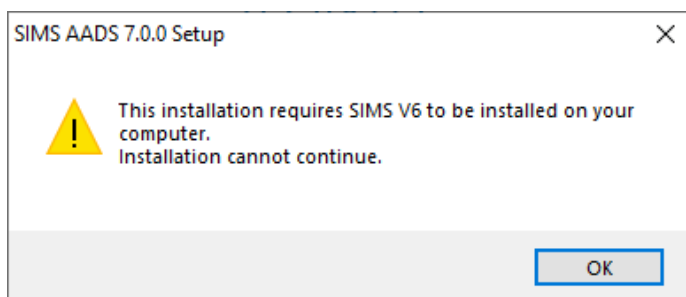


SIMS Active Directory Service installeres som en Windows Service, og vil køre helt standard som Local System.



### **NB!**

Det er IKKE muligt at installere SIMS Active Directory Service før SIMS, og det er ikke muligt at installere på en anden Server end SIMS Serveren, hvis det bliver nødvendigt, skal du kontakte ARAS.

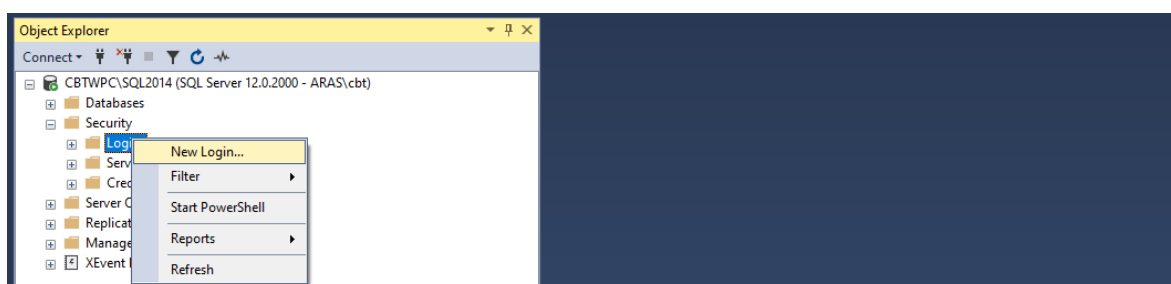


Hvis SIMS ikke er installeret endnu, henvises til SIMS Installationsmanualen for vejledning, kontakt egen installatør eller ARAS.

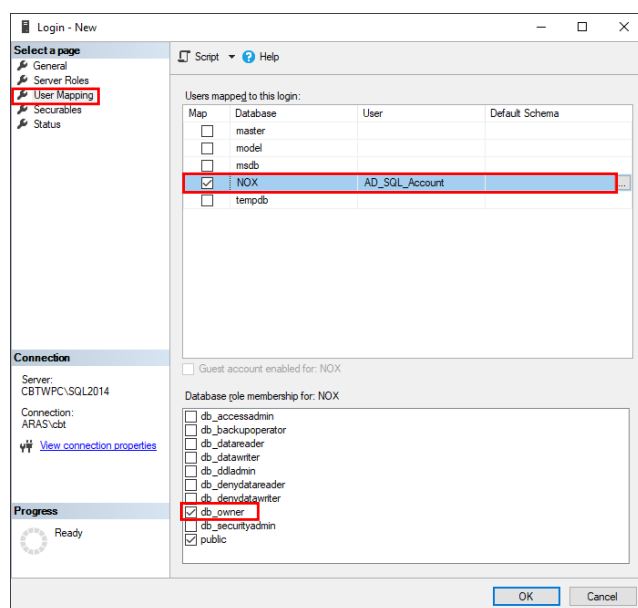
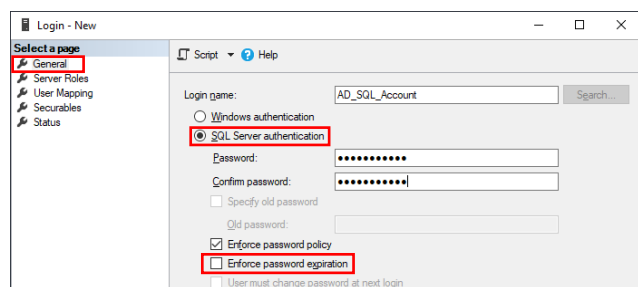
## AD Service SQL bruger

Du kan med fordel benytte den samme bruger til AD servicen, som er benyttet til SIMS Server SQL-forbindelsen.

Hvis du ønsker en separat bruger, oprettes denne på SQL Serveren, åbn Microsoft SQL Management Studio, vælg Security -> Logins, højreklik og klik New Login...



Opret nu brugeren med det ønskede navn, husk at vælge SQL Server authentication, fjerne Enforce password expiration og gøre brugeren til db\_owner på [NOX] databasen.



## Administration- og Konfigurationsinterface

Administration og Konfiguration af AD Servicen forgår gennem en webbrowser, ved at gå til <http://IPADRESSE:4545>

Det er anbefalet at benytte Google Chrome eller Microsoft Edge for bedste kompatibilitet, Internet Explorer er IKKE understøttet.

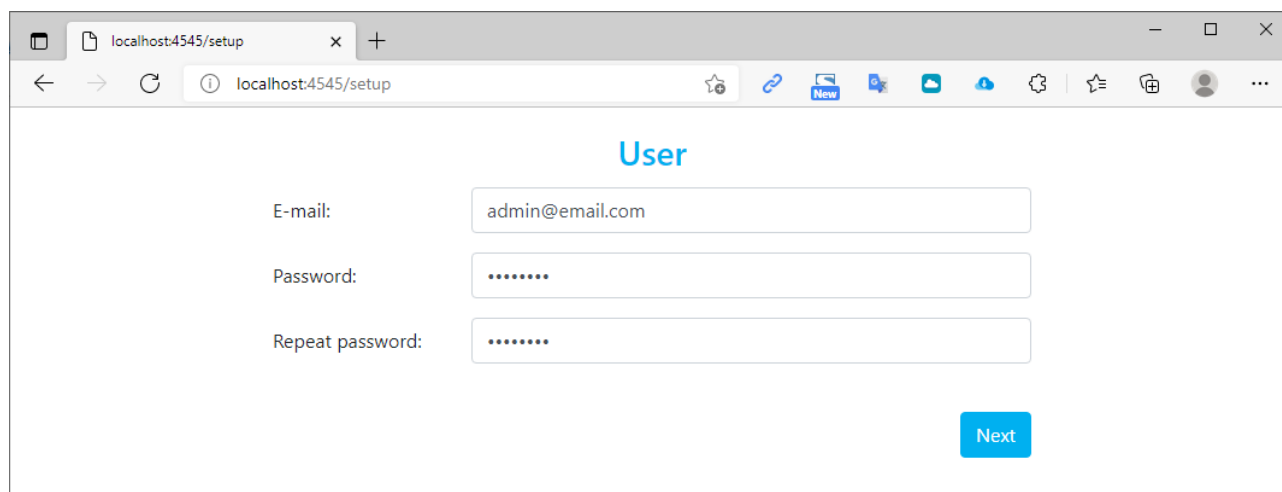
På de følgende sider er en trin-for-trin gennemgang af Administration- og Konfigurationsinterfacet.

Det er meningen at kunden selv skal være i stand til at administrere udvidelser og ændringer efter grundopsætningen af systemet.



## Installation/Opstart

### Bruger oprettelse



localhost:4545/setup

localhost:4545/setup

### User

E-mail:

Password:

Repeat password:

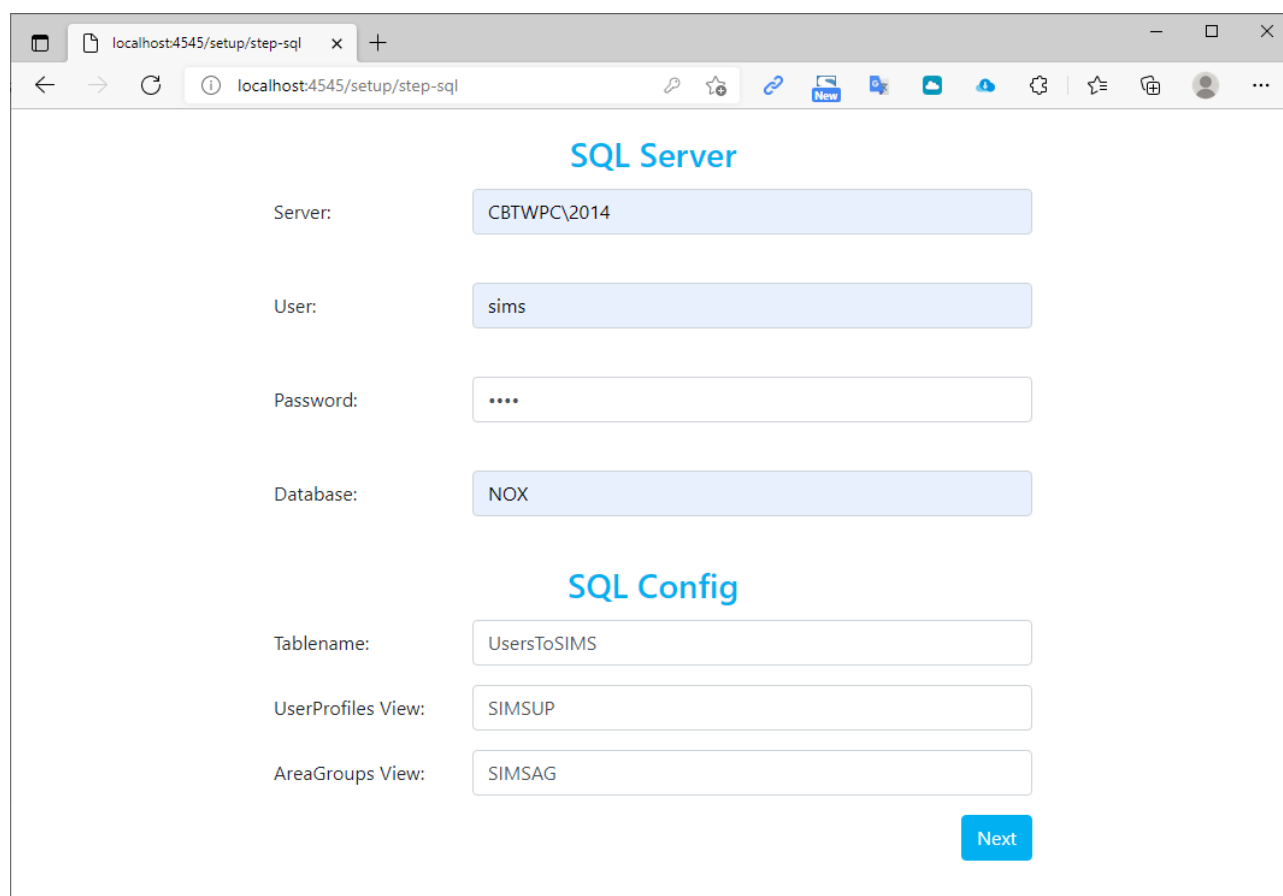
[Next](#)

Udfyld med E-mail og adgangskode.

OBS! Det er kun muligt at have én bruger.

Gå videre til næste side.

## SQL Server konfiguration



**SQL Server**

Server:

User:

Password:

Database:

**SQL Config**

Tablename:

UserProfiles View:

AreaGroups View:

[Next](#)

Udfyld Server feltet med SQL Server navn og evt. Instans

Udfyld User og Password med de SQL bruger oplysninger du har oprettet, eller fået oplyst af kunden.

Udfyld Database feltet med navnet på databasen som skal indeholde synkroniseringen, standardnavnet er NOX.

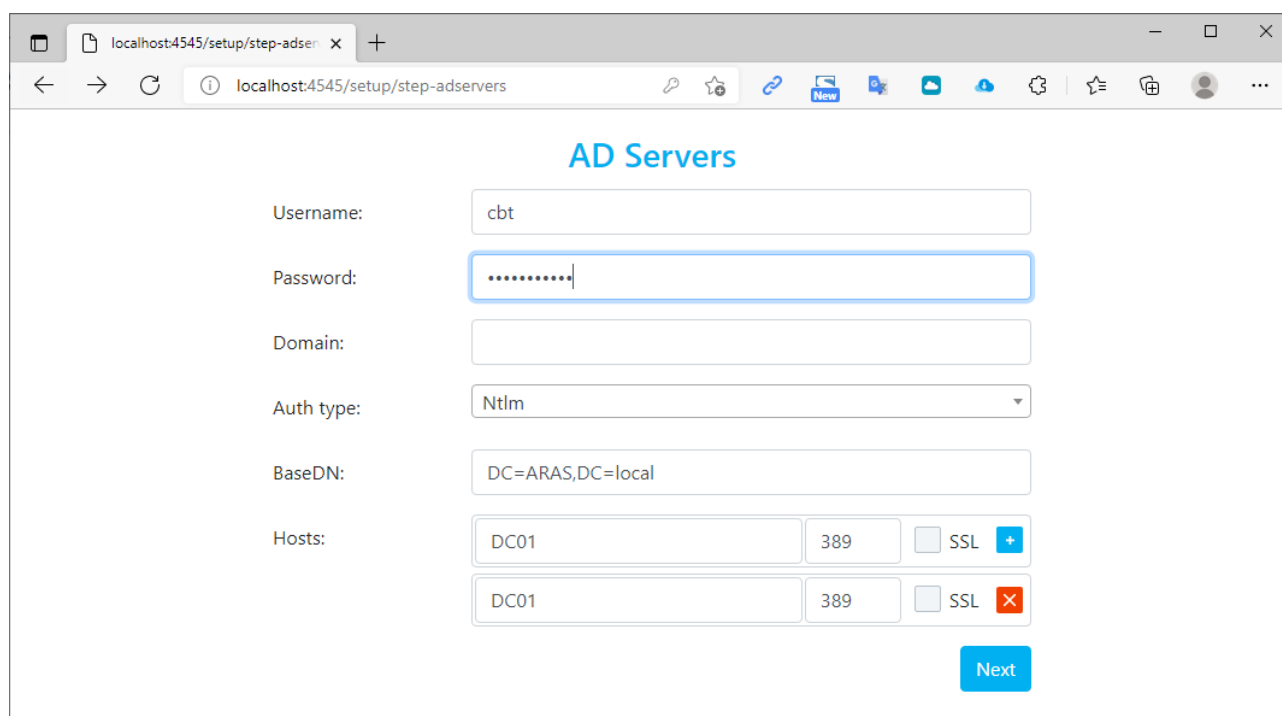
### SQL Config

Indeholder informationer om prædefinerede Views og tabelnavn

Felterne er foruddefinerede med værdier der passer til [NOX] databasen, værdierne skal normalt ikke ændres.

Gå videre til næste side.

## AD Server konfiguration



AD Servers

Username: cbt

Password: .....

Domain:

Auth type: Ntlm

BaseDN: DC=ARAS,DC=local

Hosts:

DC01	389	<input type="checkbox"/>	SSL	+
DC01	389	<input type="checkbox"/>	SSL	×

Next

Udfyld felterne Username og Password med de oplysninger du har fået udleveret, dette er din Service AD Bruger.

Udfyld Host med værtsnavn/IP på Domain Controlleren og klik på '+' for at tilføje den. Det er muligt at tilføje flere Domain Controllere, såfremt der er sekundære og tertiære Domain Controllere i virksomheden.

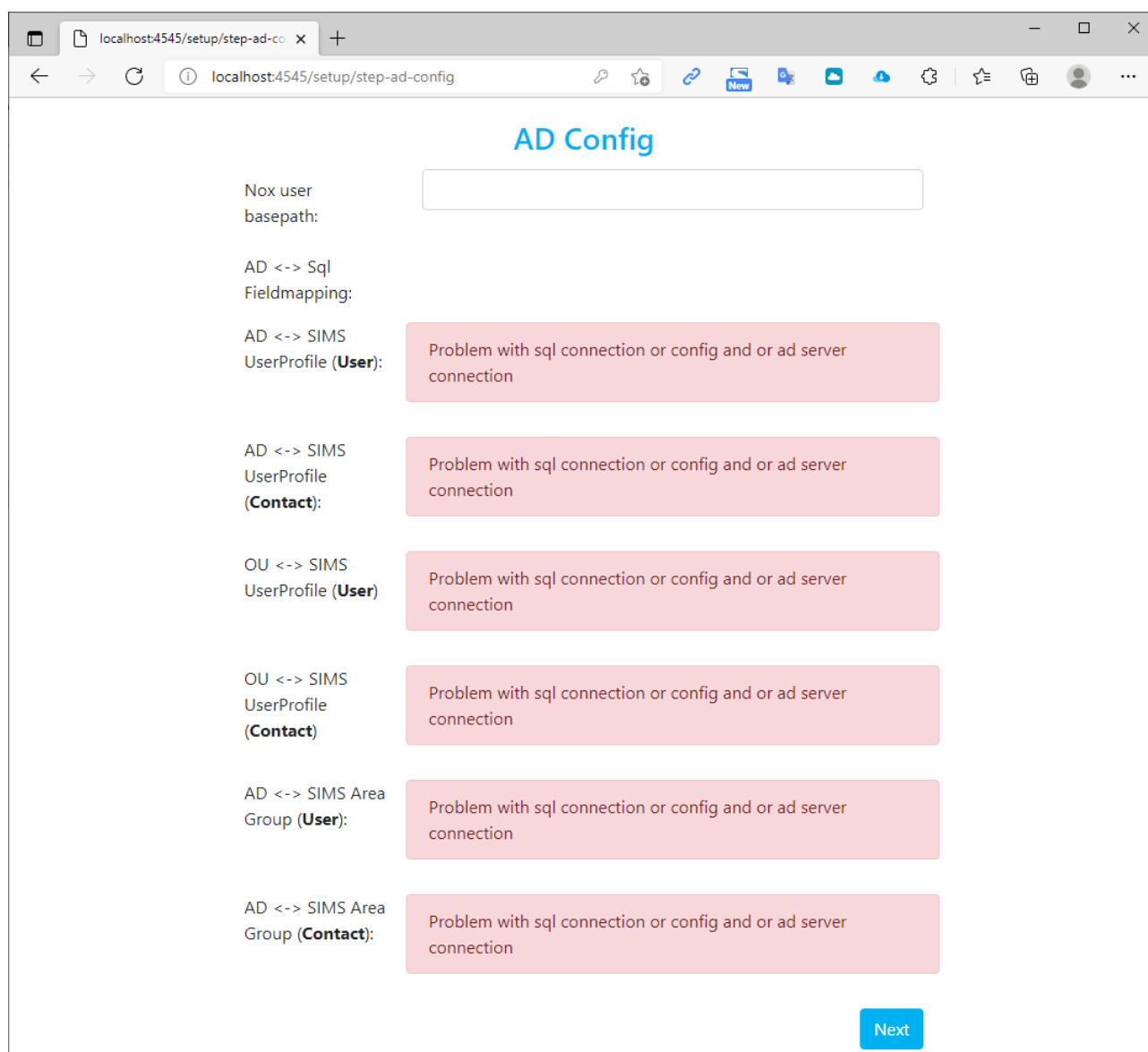
Standard port for LDAP er 389

Standard port for LDAPS er 636, husk flueben i SSL

Porten er frit definérbar, husk flueben i SSL der benyttes Secure LDAP (LDAPS)

Gå videre til næste side.

## AD Config



The screenshot shows a web browser window with the URL localhost:4545/setup/step-ad-config. The page title is "AD Config". It contains several configuration fields and error messages:

- Nox user basepath:** An empty text input field.
- AD <-> Sql Fieldmapping:** A label with no associated input field.
- AD <-> SIMS UserProfile (User):** A red error box containing the text: "Problem with sql connection or config and or ad server connection".
- AD <-> SIMS UserProfile (Contact):** A red error box containing the text: "Problem with sql connection or config and or ad server connection".
- OU <-> SIMS UserProfile (User):** A red error box containing the text: "Problem with sql connection or config and or ad server connection".
- OU <-> SIMS UserProfile (Contact):** A red error box containing the text: "Problem with sql connection or config and or ad server connection".
- AD <-> SIMS Area Group (User):** A red error box containing the text: "Problem with sql connection or config and or ad server connection".
- AD <-> SIMS Area Group (Contact):** A red error box containing the text: "Problem with sql connection or config and or ad server connection".

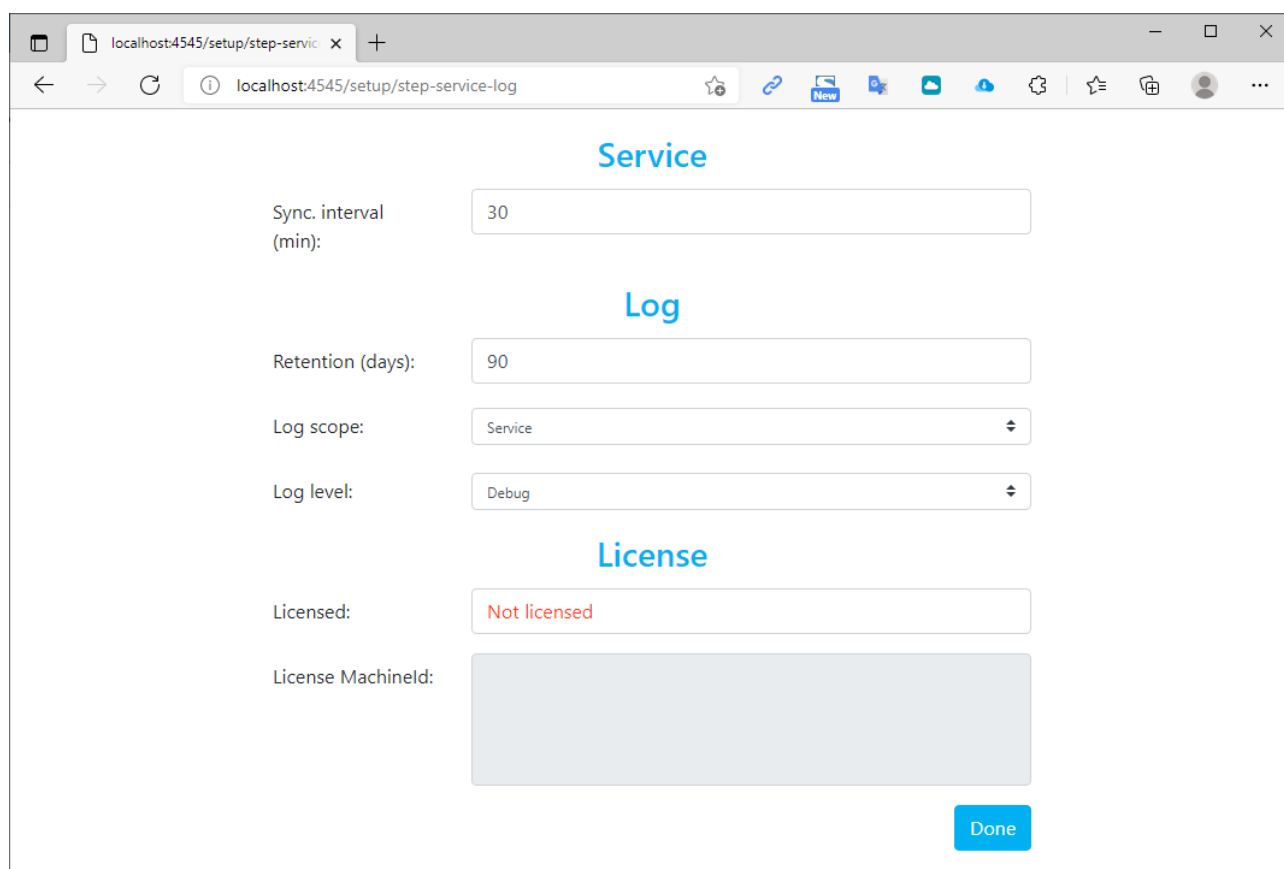
A blue "Next" button is located at the bottom right of the form area.

NOX User basepath kan udfyldes hvis du ønsker at låse AD udlæsningen til en bestemt sti, denne efterlades normalt tom.

Ofte vil det ikke være muligt at oprette Matrixen i dette step, og det er anbefalet at gå direkte videre til næste side, uden at lave ændringer.

Gå videre til næste side.

## Service og Logs



The screenshot shows a web browser window with the URL localhost:4545/setup/step-service-log. The page is divided into three sections: Service, Log, and License.

**Service**

Sync. interval (min):

**Log**

Retention (days):

Log scope:

Log level:

**License**

Licensed:

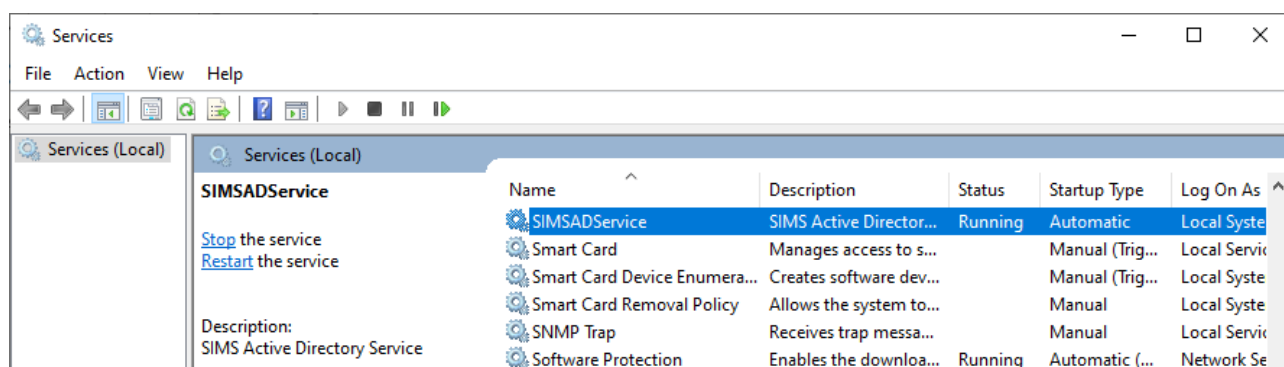
License MachineId:

Udfyld Sync. interval, hvor ofte skal der søges efter ændringer, standardtiden er 30 minutter.

Udfyld Retention, hvor længe skal logs opbevares, standard er 90 dage, Log scope bør efterlades på Service, og Log level sættes til Debug.

License MachineId bliver først synligt efter nyt login, klik på Done.

Du bliver nu sendt til Loginsiden. Bemærk at det kan være nødvendigt at genstarte SIMSADService før du kan påbegynde konfigurationen, gør det nu for en sikkerheds skyld.

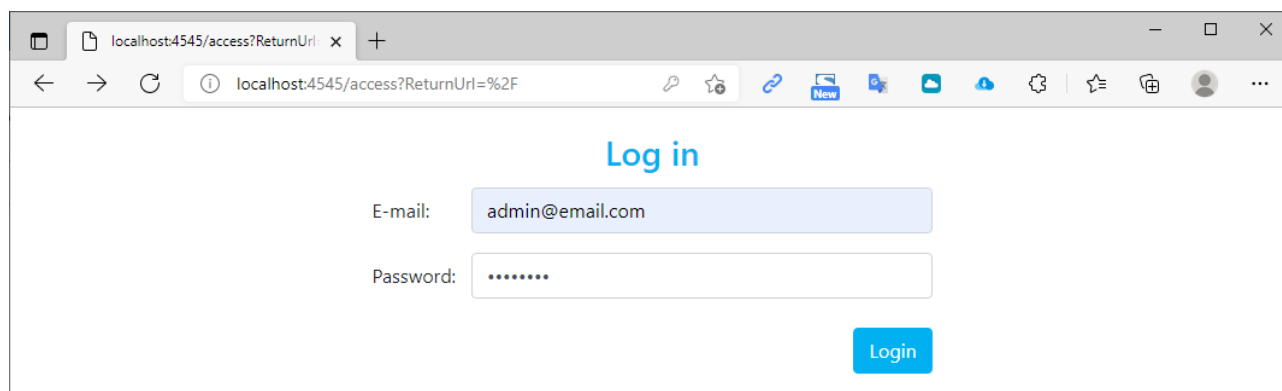


The screenshot shows the Windows Services console. The 'SIMSADService' is highlighted in the list.

Name	Description	Status	Startup Type	Log On As
SIMSADService	SIMS Active Director...	Running	Automatic	Local Syste...
Smart Card	Manages access to s...		Manual (Trig...	Local Servi...
Smart Card Device Enumera...	Creates software dev...		Manual (Trig...	Local Syste...
Smart Card Removal Policy	Allows the system to...		Manual	Local Syste...
SNMP Trap	Receives trap messa...		Manual	Local Servi...
Software Protection	Enables the downloa...	Running	Automatic (...)	Network Se...

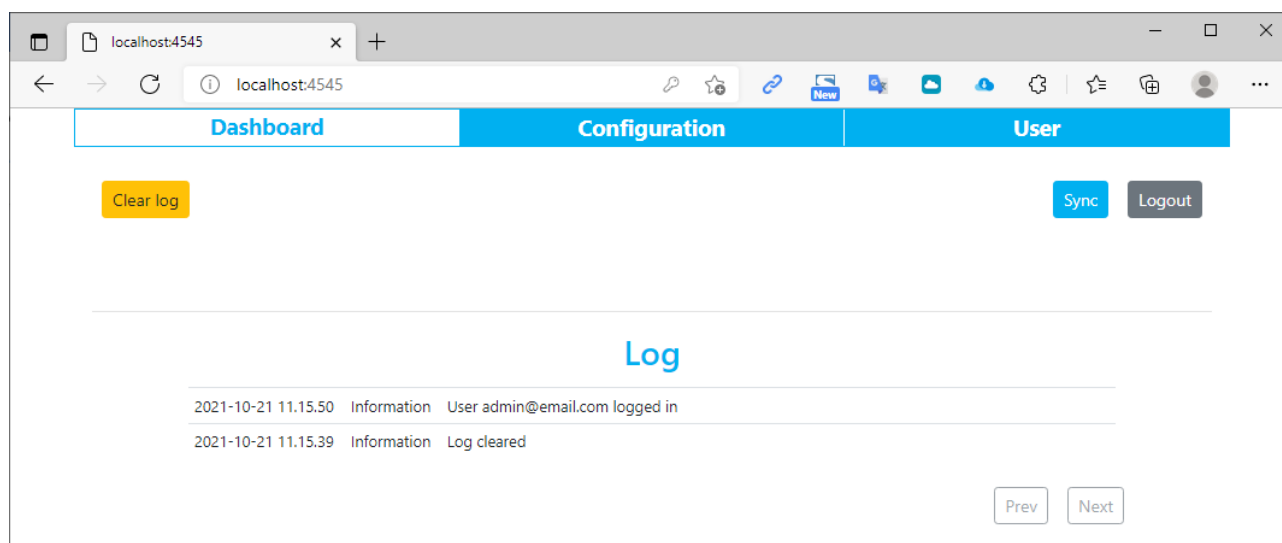
## Administration og konfiguration

### Log ind



### Log ind for at komme til Dashboard (Oversigtssiden)

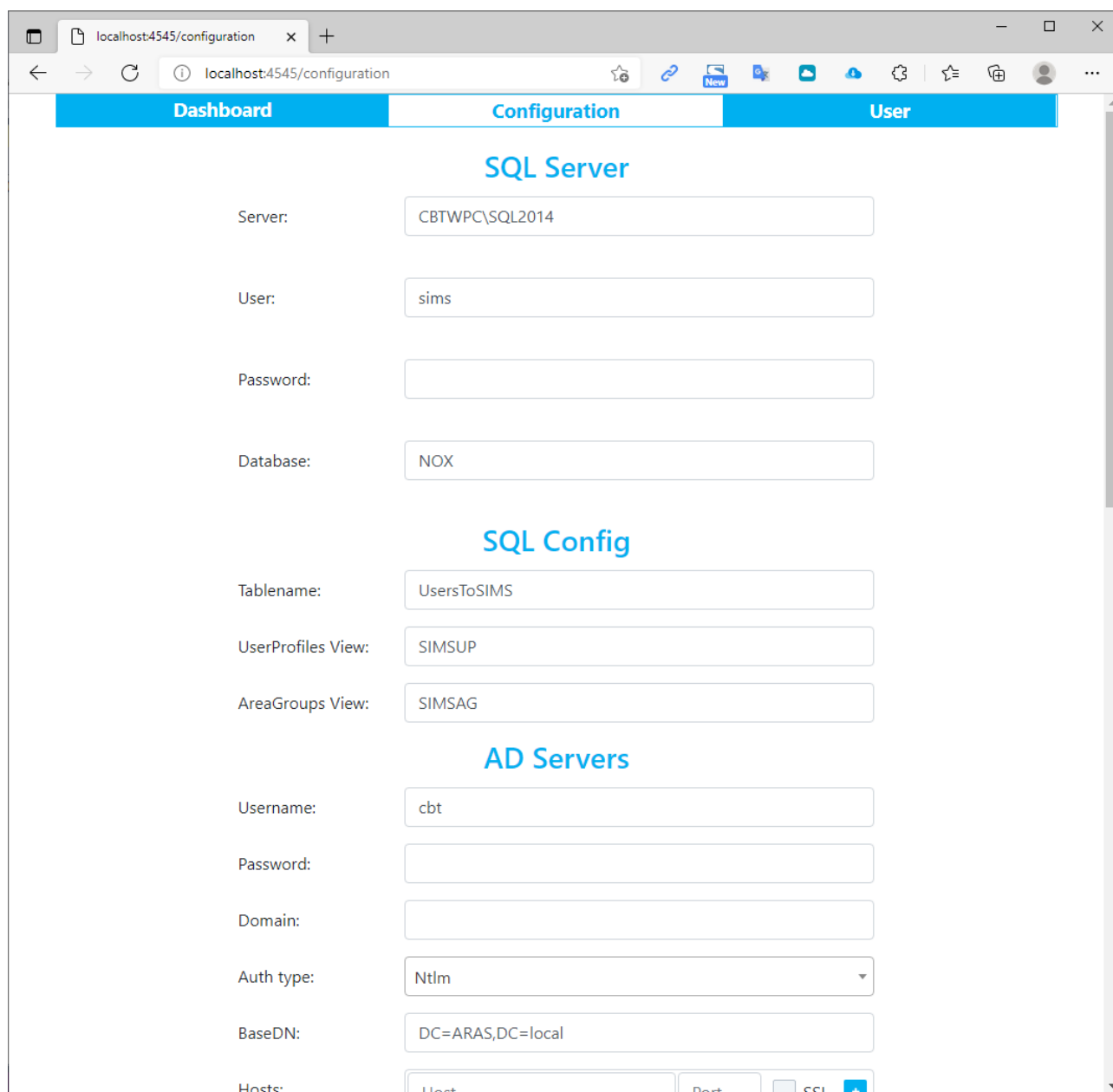
### Dashboard (Oversigt)



Her kan du manuelt starte synkronisering af brugere fra AD og se logs. Klik på Configuration, for at komme til konfigurationssiden.

## Configuration (Konfigurationssiden)

På konfigurationssiden findes alle de indstillinger der blev valgt under installationen.



The screenshot shows a web browser window with the URL localhost:4545/configuration. The page has a navigation bar with 'Dashboard', 'Configuration', and 'User' tabs. The 'Configuration' tab is active, showing three sections:

- SQL Server**
  - Server: CBTWPC\SQL2014
  - User: sims
  - Password: (empty)
  - Database: NOX
- SQL Config**
  - Tablename: UsersToSIMS
  - UserProfiles View: SIMSUP
  - AreaGroups View: SIMSAG
- AD Servers**
  - Username: cbt
  - Password: (empty)
  - Domain: (empty)
  - Auth type: Ntlm
  - BaseDN: DC=ARAS,DC=local
  - Hosts: (table with columns Host, Port, SSL)

Scroll ned ad siden, til Matrix opsætningen mellem AD og SIMS.

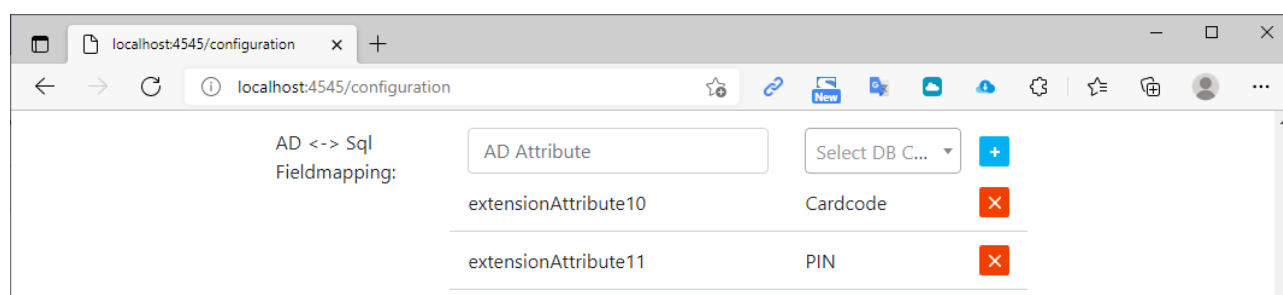
## AD Config

Under AD Config opsættes forholdet mellem AD grupper eller OU'er og SIMS profiler. Hvis der benyttes Områdegrupper, kan disse også opsættes her på samme måde som AD grupper og OU'er.

Det er også her du opsætter forholdet mellem AD attributter og felter i databasen.

## AD <-> SQL Fieldmapping


Det er her du linker AD Attributter til felter i databasen. F.eks. kunne man have kortnummer i extensionAttribute10 og PIN kode i extensionAttribute11, skriv attributtens værdi i feltet AD Attribute og vælg databasefeltet på drop down til højre, det vil se således ud:



Husk at klikke '+' for hver indstilling

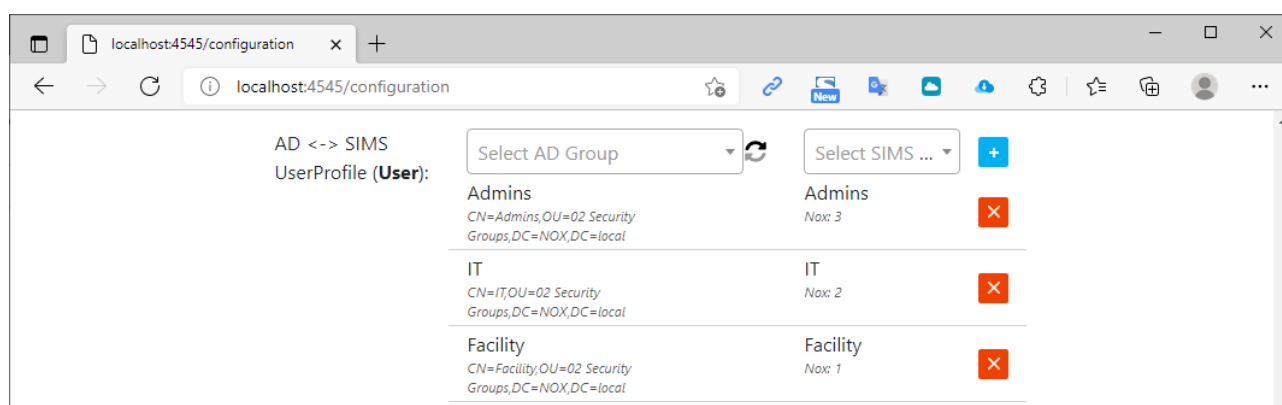


## AD <-> SIMS UserProfile (User)

Her oprettes link mellem AD grupper og SIMS Profiler, vælg AD gruppen i venstre drop down, og SIMS profilen i højre. Bemærk hvis der benyttes Nested AD Groups, skal du klikke på  således at animationen drejer rundt, som indikerer at der er tale om Nested AD Groups.

Vær opmærksom på at en bruger ikke må tilhøre mere end én AD -> SIMS Profil, hvis man skal have flere AD grupper -> SIMS profiler, skal man benytte Områdegrupper.

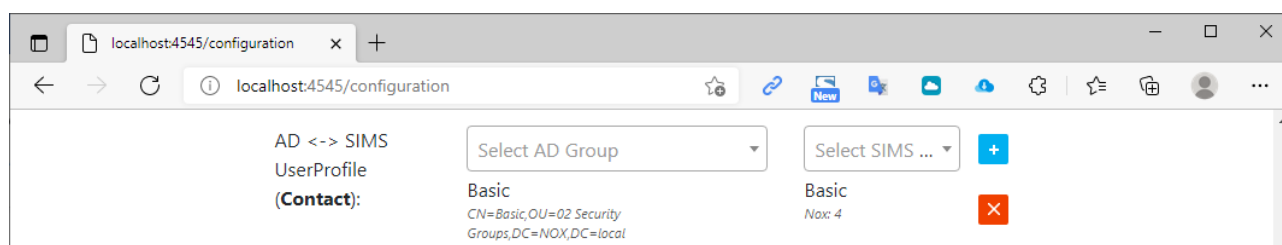
Hvis der benyttes CardExchange til at styre SIMS profil medlemskaber skal man altid linke AD brugere til SIMS profilen "Ingen adgang, NOX: 0"



## AD <-> SIMS UserProfile (Contact)

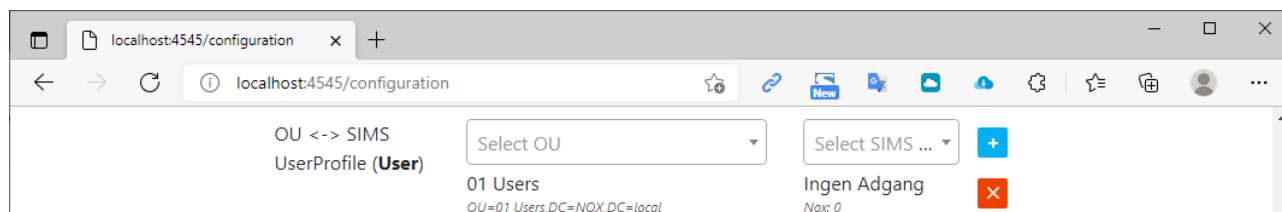
Ligesom det foregående punkt, men her vælges kontaktpersoner i AD, i stedet for brugere. Som erstatning for samAccountName er det E-mail som bliver den unikke faktor.

Bemærk at denne funktion ikke understøtter Nested AD Groups, og e-mail skal være udfyldt for at bruger bliver hentet.



## OU <-> SIMS UserProfile (User)

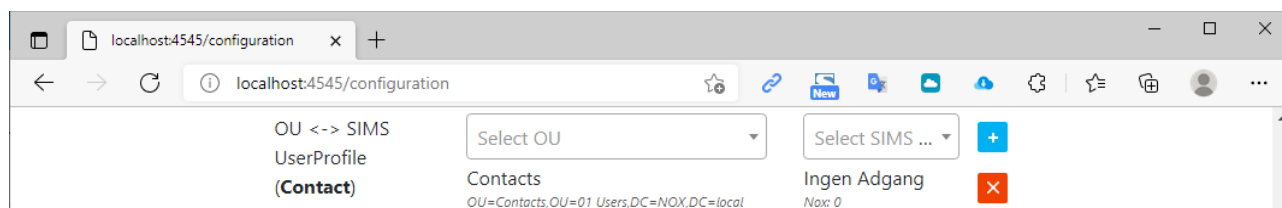
Det er muligt at udsøge alle brugere fra en bestemt OU, og tildele dem alle den samme SIMS profil.




Det kan eksempelvis give god mening hvis AD strukturen er lavet således, at man opbevarer sine medarbejdere i kategoriserede OU containere eller lignende.

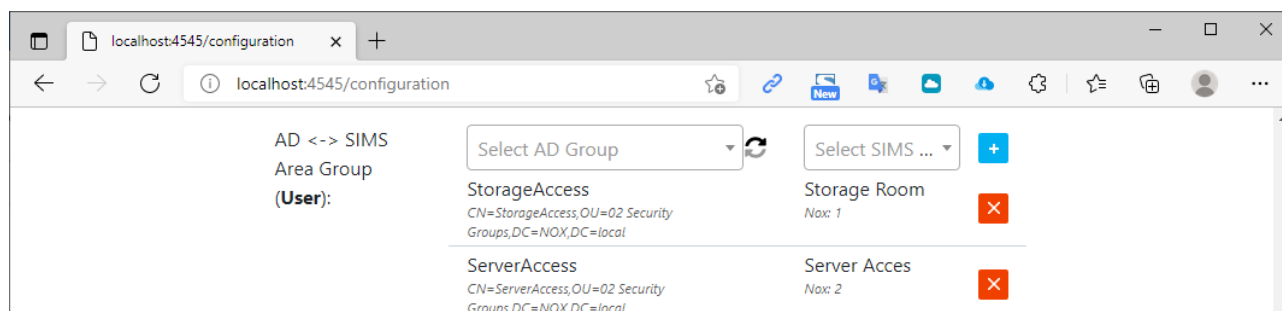
## OU <-> SIMS UserProfile (Contact)

Ligesom det foregående punkt, men her vælges kontaktpersoner i AD, i stedet for brugere. Som erstatning for samAccountName er det E-mail som bliver den unikke faktor.



## AD <-> SIMS Area Group (User):

I SIMS findes der mulighed for at lave grupper af områder og døre, det hedder områdegrupper, og kan tildeles som ekstra rettighed til brugere. Bemærk hvis der benyttes Nested AD Groups, skal du klikke på  således at animationen drejer rundt, som indikerer at der er tale om Nested AD Groups.

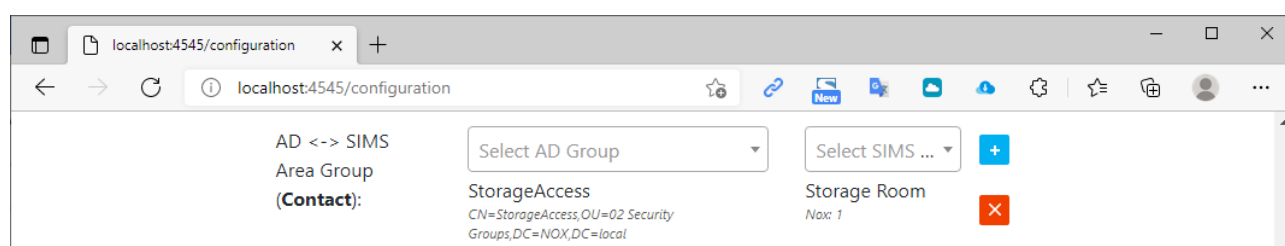


f.eks. kunne det være ekstra rettigheder til serverrum eller arkivrum.

## AD <-> SIMS Area Group (Contact):

Ligesom det foregående punkt, men her vælges kontaktpersoner i AD, i stedet for brugere. Som erstatning for samAccountName er det E-mail som bliver den unikke faktor.

Bemærk at denne funktion ikke understøtter Nested AD Groups, og e-mail skal være udfyldt for at bruger bliver hentet.

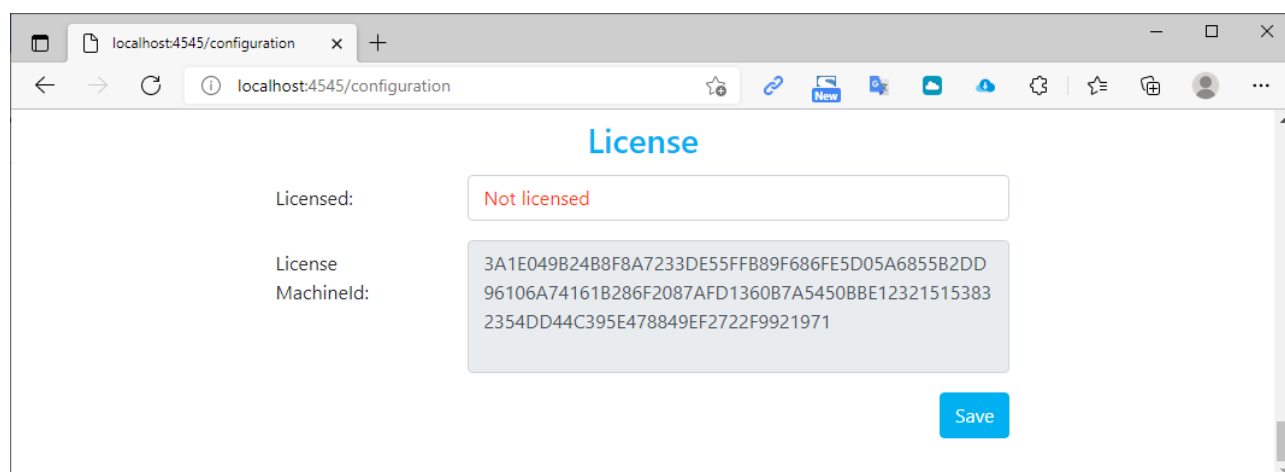


## Licensering

For at AD servicen kan fungere skal den licenseres.

Den ulicenserede udgave kan konfigureres fuldt ud, og kan teste om den kan forbinde korrekt til AD, den kan dog ikke synkronisere brugere.

Kopier License MachineId og send det til ARAS for få en licens.



## Generelt om konfigurationssiden

- Husk at klikke på '+' for at tilføje den valgte indstilling
- Husk at gå til bunden af siden og gemme indstillingerne
- Står du for længe på konfigurationssiden uden aktivitet, vil du automatisk blive logget ud.
- Husk loginoplysningerne! Hvis de mistes, skal alt konfigureres forfra! Vi har ikke mulighed for at genskabe koder eller konfiguration.
- Husk at SIMS/NOX ikke understøtter foranstillede 0 i kortnumre og koder, hvis der findes foranstillede 0 på brugere i AD vil de blive opdateret hver gang servicen skanner for ændringer.
- Husk kun én grundlæggende AD gruppe -> SIMS profil, er der brugere som er medlem af flere grupper vil der opstå en fejl på brugeren som kan ses i loggen.

## Checkliste

- SIMS Server er installeret og konfigureret
- SIMS Grupper er oprettet
- SIMS Områdegrupper er oprettet
- Base DN (f.eks. DC=aras,DC=local)
- Domain Controller IP/Hostname(s)
- LDAP eller LDAPS? (port 389, 636 eller selvvalgt)
- Service Account i AD (username/password)
- SQL Server name/instans
- SQL User/Pass (anbefaler at bruge den samme som SIMS benytter, skal være DB Owner eller SA)
- SIMS user/pass
- Evt. Attributter der benyttes til Kortnummer, PIN, og NOX kode
- Evt. Security Groups der skal overføres brugere fra, og hvilke(n) SIMS Gruppe(r) de passer til.
- Skal Områdegrupper styres fra AD, Evt. Security Groups der matche hvilke(n) SIMS Områdegrupper de passer til
- Evt. OU'er der skal overføres brugere fra, og hvilke(n) SIMS Gruppe(r) de passer til.
- Skal der benyttes flere kort pr. bruger? (Maks 3 ekstra kort)

Er du i tvivl, eller har du spørgsmål om noget i relation til ovenstående, eller SIMS Active Directory Service applikationen generelt, kan du kontakte ARAS på [support@aras.dk](mailto:support@aras.dk) eller pr. telefon.