

Active Directory SIMS Plugin

SIMS integration med Microsoft Active Directory, er implementeret, via en mellemdatabase.

Løsningen består af en Windows Service som henter data fra AD og lagrer det i en mellemdatabase, ud fra en forud defineret matrix mellem SIMS grupper og AD grupper.

I denne integration er det AD der er den styrende part.

På denne måde vil det være muligt at oprette brugere gennem SIMS sideløbende, uden at de forskellige oprettelser vil influere på hinanden. Det er muligt helt at slå bruger håndteringen helt fra hvis det er ønsket udelukkende at benytte AD styring.

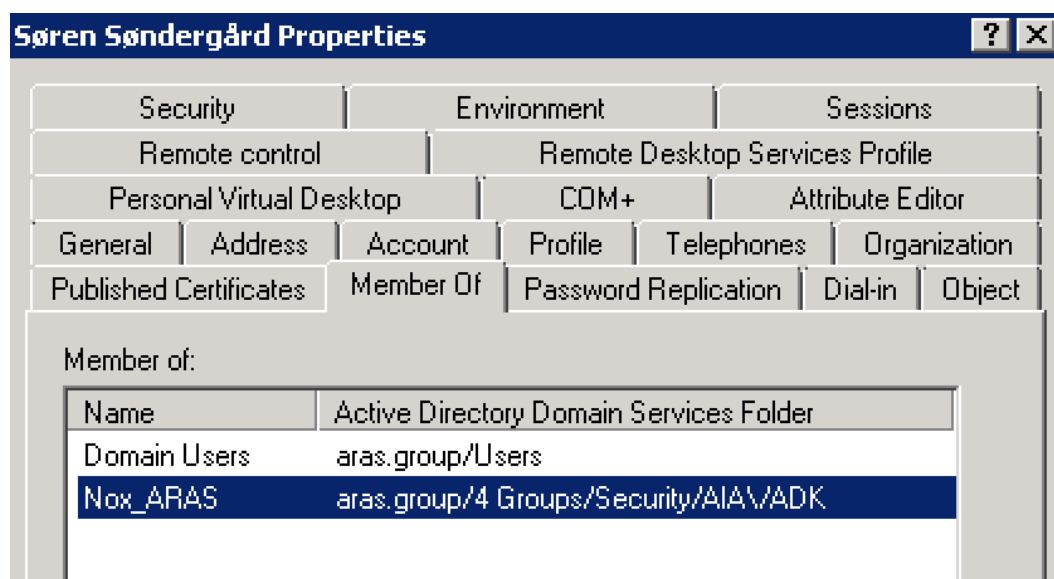
Matrix

Der skal udformes en matrix som fortæller hvilke AD medlemmer der skal have hvilke profiler i SIMS systemet. Vi anbefaler at der oprettes nye grupper i AD som kan pares op med profilerne i SIMS.

Et eksempel på matrix kunne være følgende:

AD gruppe	SIMS grp.	AD Sti til gruppe
Nox_User	1	CN=Nox_User,OU=AIA/ADK,OU=Security,OU=4 Groups,DC=aras,DC=group
Nox_Admin	2	CN=Nox_Admin,OU=AIA/ADK,OU=Security,OU=4 Groups,DC=aras,DC=group
Nox_Cleaner	3	CN=Nox_Cleaner,OU=AIA/ADK,OU=Security,OU=4 Groups,DC=aras,DC=group
Nox_ARAS	4	CN=Nox_ARAS,OU=AIA/ADK,OU=Security,OU=4Groups,DC=aras,DC=group

Brugere oprettes i AD og gives medlemskab af ønsket gruppe som vist herunder



Kortnummer, PIN- og evt. NOX-kode skal angives i AD, under hver sin valgfri attribut.

Vi anbefaler at benytte attributter som ikke bliver vist i generelle LDAP-opslag til at lagre kort- og kode data.

Benyt f.eks. exchangeattribute13 eller anden attribut der ikke er umiddelbar synlig i et LDAP-opslag (gennem Global adressebog i AD)

På baggrund af data i AD, oprettes/slettes/ændres/deaktiveres brugere i SIMS.

Vi kombinerer Fornavn, Efternavn og SamAccount name for at sikre alle brugere er unikke i NOX.

Funktioner

SIMS AD Plugin tilgår og understøtter følgende features:

- Fornavn-, og Efternavn
- Konto udløb (Account expires)
- Spærret bruger (Account is disabled)
- Initialer (SamAccount)
- Bestemt OU-container til AD grupper (hvis ikke valgt, bliver hele AD-træet gennemført)
- Valgfrie attributter til opbevaring af kortnummer, PIN- og NOX-koder
- To disponible attributter til fremtidig brug

SIMS AD Plugin installeres på SIMS serveren og er en selvstændig service.

SIMS AD Plugin indeholder en lokal database som indeholder Matrixen og alle indstillinger.

Hvis der ikke findes en relevant gruppe eller der ikke er nogen kortdata på en bruger i AD, vil brugeren blive ignoreret.

Integrationen kører som en Windows Service, og synkroniserer data efter et forud defineret interval, standardtiden er sat til hvert 30. minut, det er naturligtvis efter eget valg hvis der er andre ønsker.

Det er også muligt at køre jobbet "on-demand" igennem webinterfacet.

Krav og forudsætninger

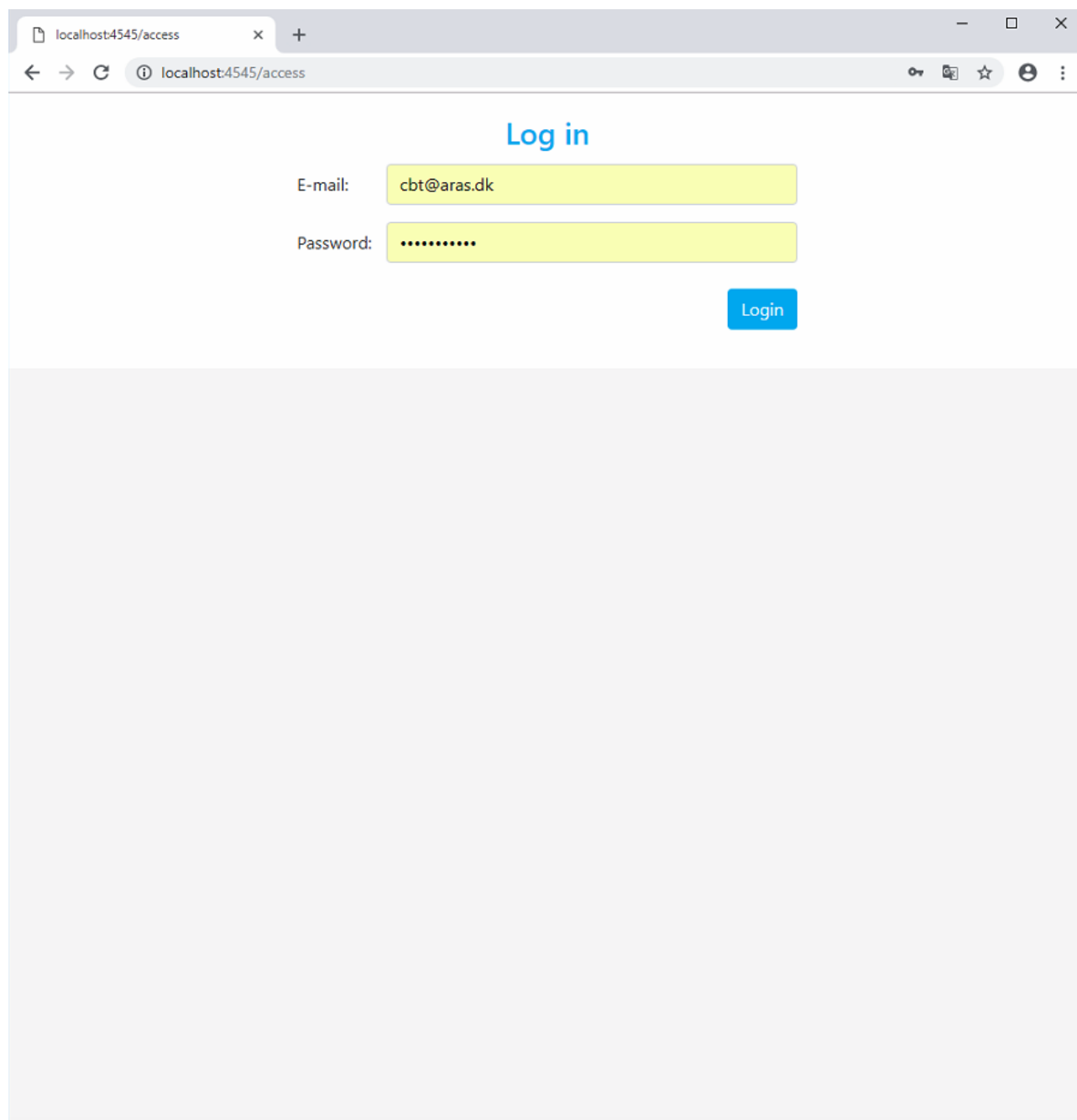
- Vi skal have en AD bruger (Brugernavn/Password)
- Vi skal have et hostname/IP-adresse på Domain Controlleren
- Eventuelt skal vi vide hvilken OU vi skal kigge i (ingen OU = Vi skanner hele træet)
- Hvilke Attributter vi skal kigge i (hvor gemmer i kortnummer, PIN-, NOX Kode)
- Vi skal vide hvilke AD grupper der skal spejles over i SIMS Grupper (det kan man selv tilføje mere af senere)
- Vi skal vide hvor ofte vi skal synkronisere med AD
- Vi skal have en SQL Bruger med fuld adgang til vores mellemdatabase
- Vi skal kende SQL Server navn og evt. instans
- Vi skal kende Databasens navn (den bør vi kende da vi leverer databasen)

SIMS AD Plugin, Administrations interface

Administration og configuration af AD servicen forgår gennem en webbrowser, på de følgende sider vises dette interface. Det er meningen at slutbrugeren selv kan administrere udvidelser og ændringer efter grundopsætning af systemet.

Login siden:

Log ind med den e-mailadresse og adgangskode som blev oprettet under grundopsætningen.

A screenshot of a web browser window showing a login page. The browser's address bar displays "localhost:4545/access". The page has a white background with a blue "Log in" heading. Below the heading are two input fields: "E-mail:" with the value "cbt@aras.dk" and "Password:" with a masked password of nine dots. A blue "Login" button is positioned to the right of the password field. The bottom half of the browser window is a solid light gray area.

localhost:4545/access

Log in

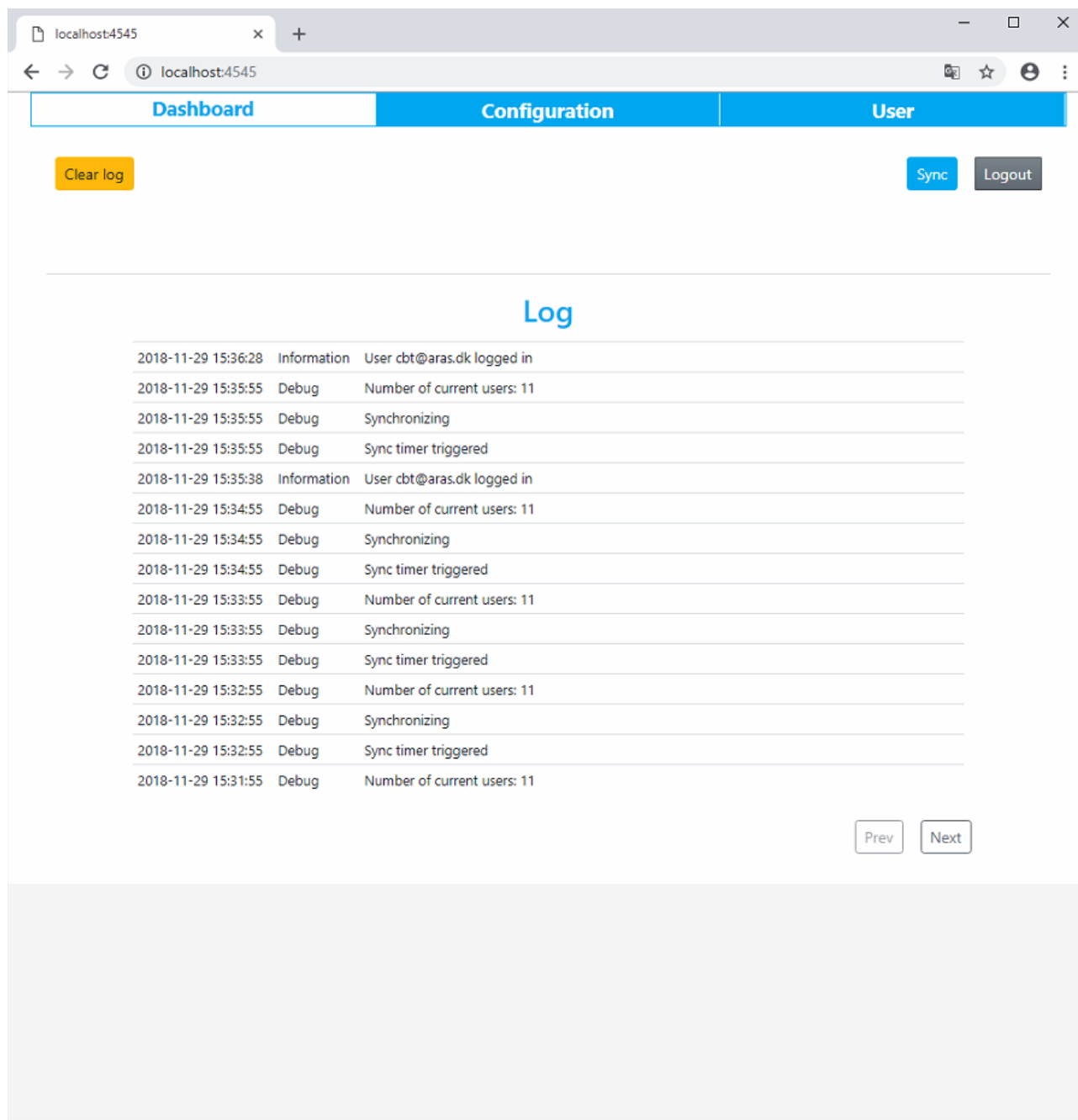
E-mail:

Password:

Login

Dashboard (Log- og synkronisering)

Under denne side kan man se historisk log, og har mulighed for at køre en manuel synkronisering efter behov.



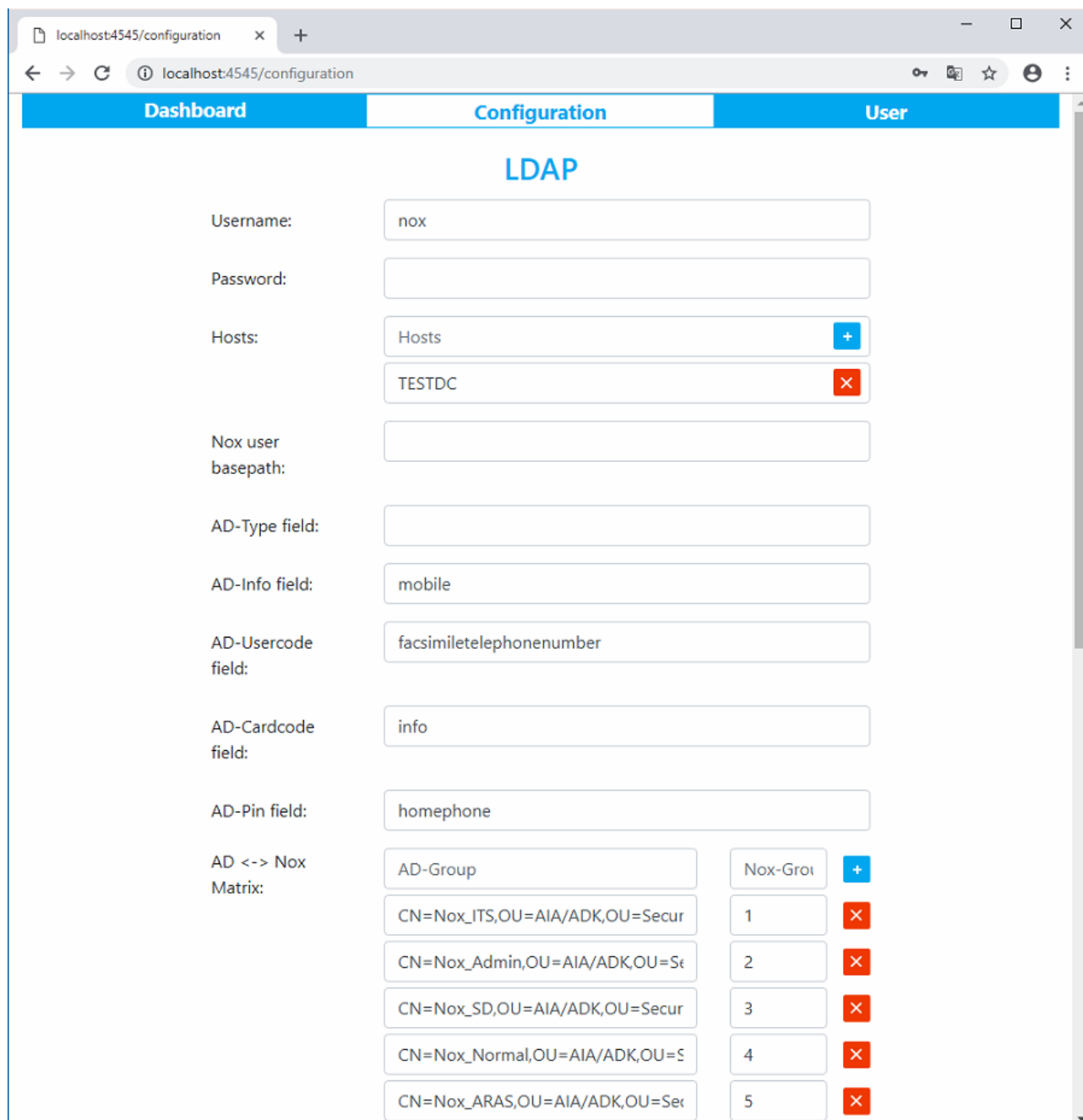
The screenshot shows a web browser window with the URL localhost:4545. The dashboard has three tabs: Dashboard (selected), Configuration, and User. In the top right corner, there are buttons for 'Clear log', 'Sync', and 'Logout'. The main content area is titled 'Log' and displays a list of log entries. The log entries are as follows:

2018-11-29 15:36:28	Information	User cbt@aras.dk logged in
2018-11-29 15:35:55	Debug	Number of current users: 11
2018-11-29 15:35:55	Debug	Synchronizing
2018-11-29 15:35:55	Debug	Sync timer triggered
2018-11-29 15:35:38	Information	User cbt@aras.dk logged in
2018-11-29 15:34:55	Debug	Number of current users: 11
2018-11-29 15:34:55	Debug	Synchronizing
2018-11-29 15:34:55	Debug	Sync timer triggered
2018-11-29 15:33:55	Debug	Number of current users: 11
2018-11-29 15:33:55	Debug	Synchronizing
2018-11-29 15:33:55	Debug	Sync timer triggered
2018-11-29 15:32:55	Debug	Number of current users: 11
2018-11-29 15:32:55	Debug	Synchronizing
2018-11-29 15:32:55	Debug	Sync timer triggered
2018-11-29 15:31:55	Debug	Number of current users: 11

At the bottom right of the log list, there are 'Prev' and 'Next' buttons.

Configuration (konfiguration af Active Directory og database indstillinger)

Under denne side opsættes Matrix mellem AD og SIMS, samt database indstillinger og log niveau. Desuden er det også her man indstiller synkroniseringsintervallet.



The screenshot shows a web browser window at localhost:4545/configuration. The page has three tabs: Dashboard, Configuration (selected), and User. The main heading is 'LDAP'. The configuration fields are as follows:

- Username: nox
- Password: (empty)
- Hosts:
 - Hosts (with a blue '+' button)
 - TESTDC (with a red 'x' button)
- Nox user basepath: (empty)
- AD-Type field: (empty)
- AD-Info field: mobile
- AD-Usercode field: facsimiletelephonenumber
- AD-Cardcode field: info
- AD-Pin field: homephone
- AD <-> Nox Matrix:

AD-Group	Nox-Group	Action
CN=Nox_ITS,OU=AIA/ADK,OU=Secur	1	Red 'x' button
CN=Nox_Admin,OU=AIA/ADK,OU=Sec	2	Red 'x' button
CN=Nox_SD,OU=AIA/ADK,OU=Secur	3	Red 'x' button
CN=Nox_Normal,OU=AIA/ADK,OU=Sec	4	Red 'x' button
CN=Nox_ARAS,OU=AIA/ADK,OU=Sec	5	Red 'x' button

Fortsætter på næste side

Service

Sync. interval (min):

SQL Database

Tablename:

Server:

Database:

User:

Password:

Log

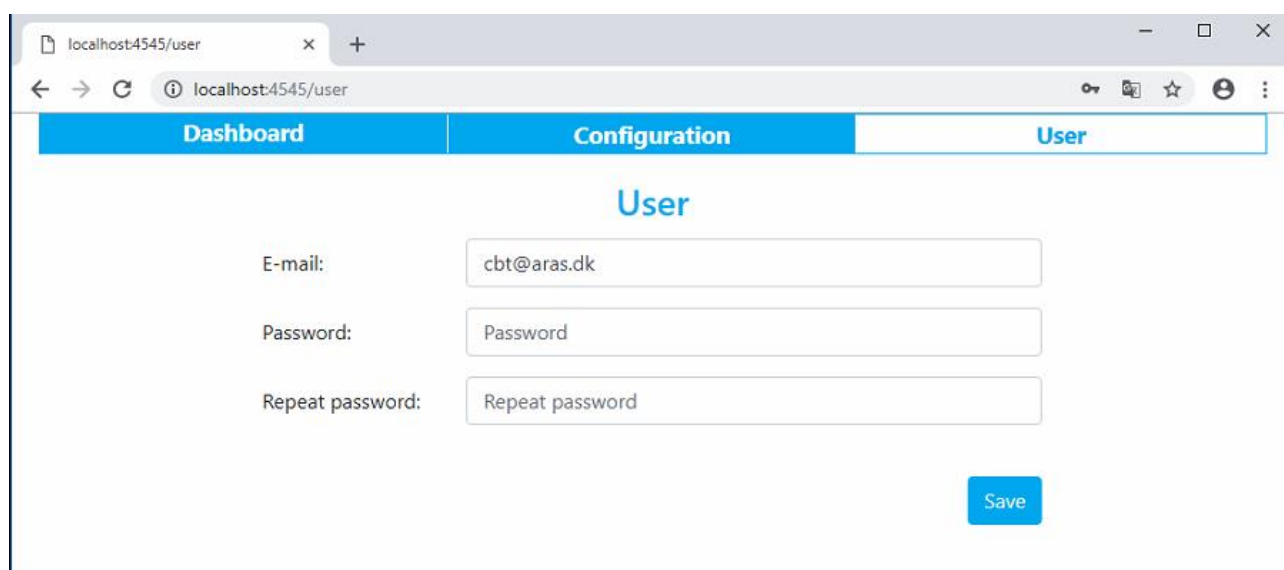
Retention (days):

Log scope:

Log level:

User (Bruger/kode ændring)

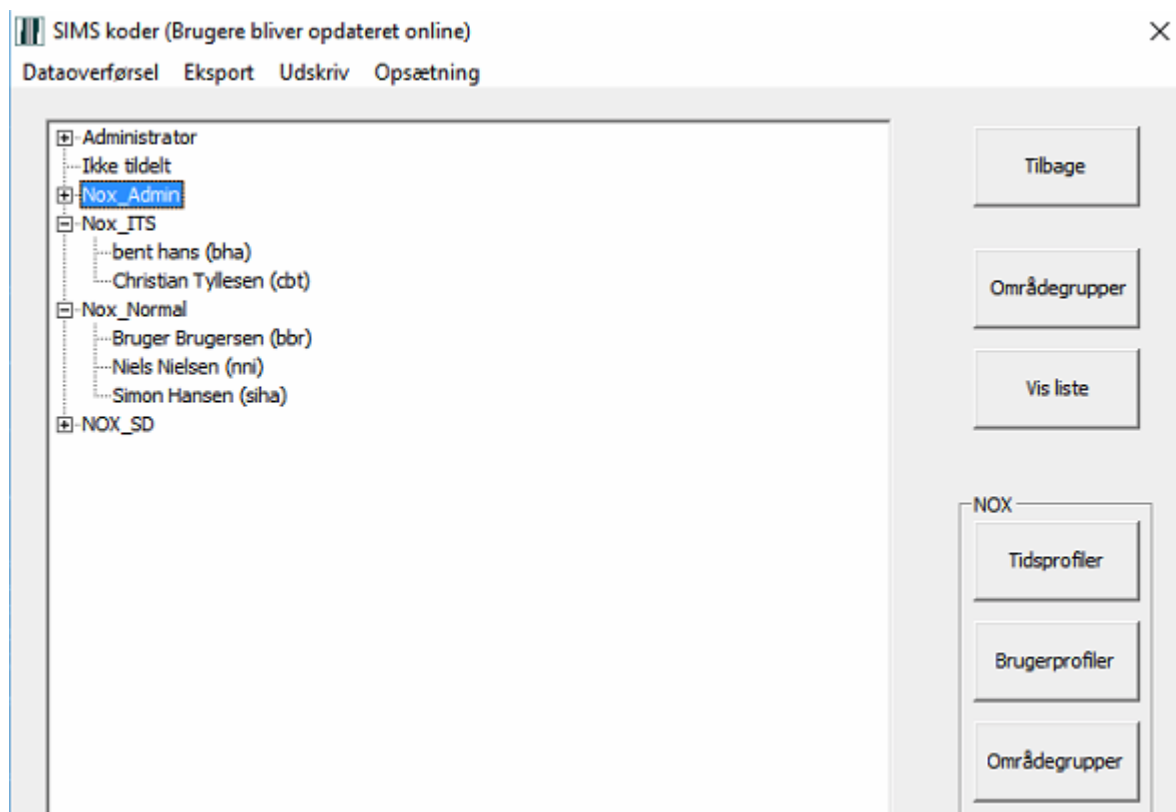
På denne side kan man ændre sine brugeroplysninger



The screenshot shows a web browser window with the URL localhost:4545/user. The page has a navigation bar with three tabs: Dashboard, Configuration, and User. The User tab is active. The main content area is titled "User" and contains three input fields: "E-mail" with the value "cbt@aras.dk", "Password" with the value "Password", and "Repeat password" with the value "Repeat password". A blue "Save" button is located at the bottom right of the form.

SIMS Grupper, til brug i Matrix

Der skal oprettes SIMS bruger grupper som kan linkes med AD grupper, disse oprettes under Bruger Administration.



Når SIMS bruger grupperne er oprettet kan de med fordel udlæses direkte i CEUsers databasen igennem det SQL View vi har oprettet til formålet.

