

6105 Windows Server og datanett

Leksjon 5b Brukeradministrasjon i AD

- Brukeradministrasjon
- Lokale brukerkontoer og domenekontoer
- Pålogging i domene og lokalt
- Brukerkontoer i domene
- Hjemmekataloger og brukerprofiler
- Kommandofiler og logon skripts

Pensum

- Kvisli: Windows Server og nettverk, kapittel 7 Brukeradministrasjon

Nyttige linker

- [Wikipedia: User profiles in Microsoft Windows](#)
- [Microsoft Technet: Manage User Accounts in Windows Server Essentials](#)

Brukeradministrasjon

- **Hva er brukeradministrasjon?**
- **Hvorfor brukeradministrasjon?**
 - Autentisering = identifisere brukeren
 - Autorisering = styre hva brukeren har lov til
- **Hvem utfører brukeradministrasjon?**
 - Sentral nettverksadministrator / IT-avdeling
 - Delegering til flere lokale administratorer (store organisasjoner)
 - Maskinell registrering / import av brukerkontoer
 - Selvbetjening / egenregistrering
 - » Jfr. webapplikasjoner / nettsteder på Internett
 - » Aktivering av studentkonto

Brukerkontoer i Windows

- **Lokale brukerkontoer kan finnes på**

- Klientmaskiner
- Medlemstjenere
- Frittstående (stand-alone) tjenere

- **I domener brukes *domenekontoer***

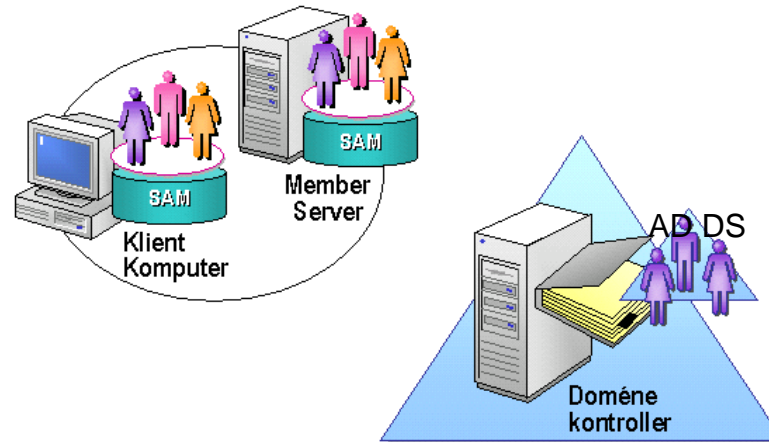
- Alle kontoer i AD DS er domenekontoer

- **Innebygde brukerkontoer**

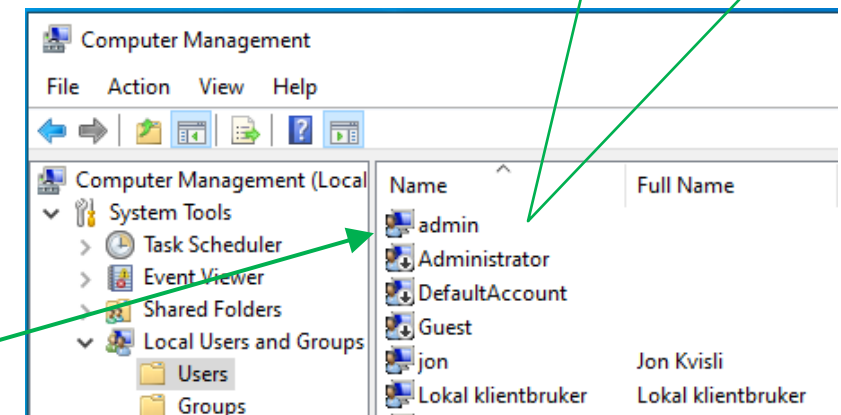
- Opprettes automatisk under installasjon av Windows
 - » *Administrator* Medlem av gruppen *Administrators* som har alle rettigheter lokalt på maskinen
 - » *Guest* Uten passord !
 - » *DefaultAccount* Brukes "internt" av Windows-systemet

- **I Windows 10 opprettes en lokal bruker ved installasjon**

- Denne brukeren er medlem i gruppen *Administrators*
- Den som installerer bestemmer navn på brukeren



I Windows 10 er innebygde brukere sperret / deaktivert etter installasjon !



Lokale kontoer og domenekontoer

Lokale brukerkontoer	Domenekontoer
<ul style="list-style-type: none">• Opprettes på lokal maskin• Lagres i lokal brukerdatabase (SAM Security Account Manager)• Brukernavn og passord kontrolleres mot lokal brukerdatabase• Kan bare gis tilgang til ressurser på denne maskinen• Brukere må ha en brukerkonto på hver maskin de skal benytte	<ul style="list-style-type: none">• Opprettes på domenekontrolleren• Lagres i sentral brukerdatabase (Active Directory)• Brukernavn og passord kontrolleres mot AD på domenekontroller• Kan gis tilgang til alle ressurser på alle maskiner i domenet• Hver bruker kan ha én brukerkonto for alle maskiner i domenet• Replikeres (kopieres) til andre domenekontrollere i domenet (i store nett med flere lokasjoner)

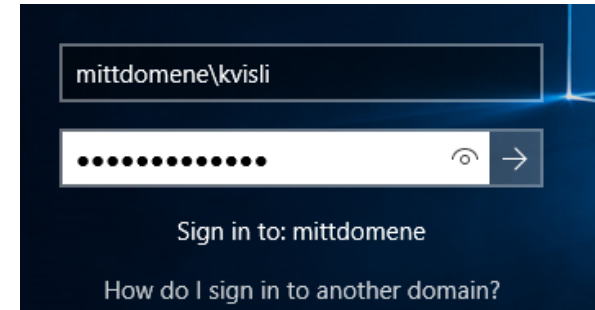
Pålogging i domene og lokalt

Login med domenebruker:

User name: *domenenavn\brukernavn*

Eksempel: *mittdomene\jon*

Maskinen du logger på fra må være medlem i domenet

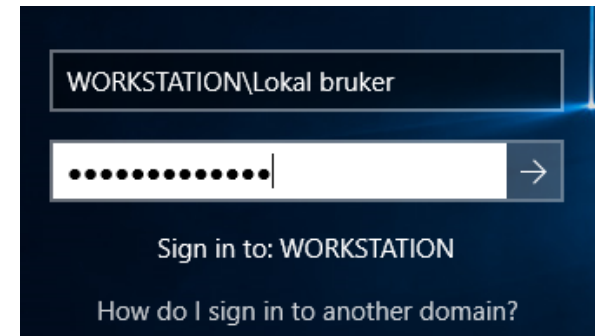


Login med lokal bruker:

User name: *maskinnavn\brukernavn*

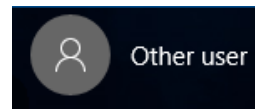
Eksempel: *workstation\admin*

Maskinen kan være medlem i domene eller arbeidsgruppe



For å bytte bruker må du først velge:

Other User



Brukerkontoer i Windows domene

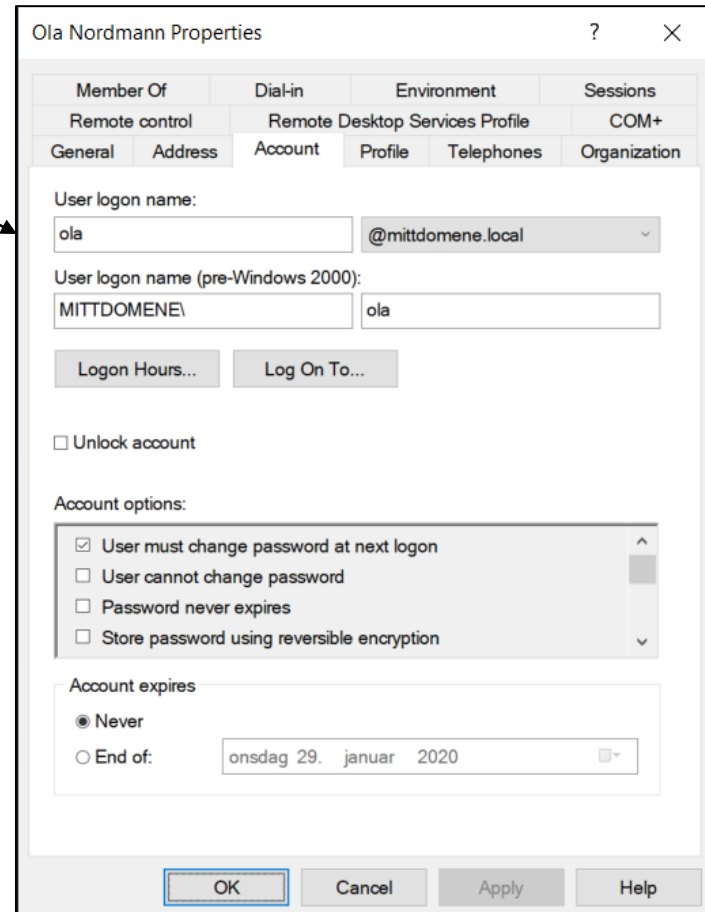
- **Regler for kontonavn (User logon name)**

- Max. 20 tegn
 - » Ikke tillatte tegn: " / \ [] : ; | = , + * ? < >
- Lokale brukerkontoer
 - » Navnet må være entydige på maskinen
- Domenekontoer
 - » Navnet må være entydige i hele domenet

- **Strategier for passordbytte**

- Bruker kan ikke endre passord
- Bruker endrer passord fritt
- Bruker må endre med faste intervaller
- Passord utløper aldri

- **Se pensumbok for omtale av flere egenskaper til domenekontoene**



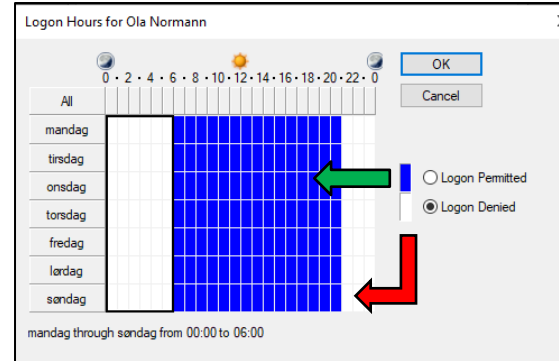
Komplekse passord i Windows domener

- **Domenebrukere må følge regler for komplekse passord (complex requirements)**
 - Passordet kan ikke inneholde hele, eller deler av kontonavnet.
 - Passordet må være minst seks tegn langt
 - Passordet må inneholde tegn fra minst tre av følgende kategorier:
 - » store bokstaver i det engelske alfabetet
 - » små bokstaver i det engelske alfabetet
 - » siffer fra 0-9
 - » ikke-alfabetiske tegn, for eksempel: !, \$, #, %
- **Complex requirements kan skrus av.**
 - Windows vil da tillate enklere / kortere passord
 - Anbefales ikke!

Begrensninger på domenekontoer

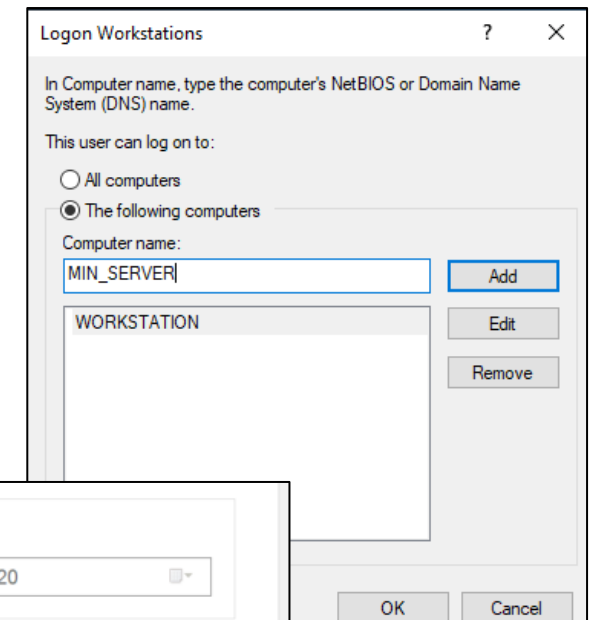
- **Begrense tidsrom for pålogging**

- Ukedager
- Klokketimer



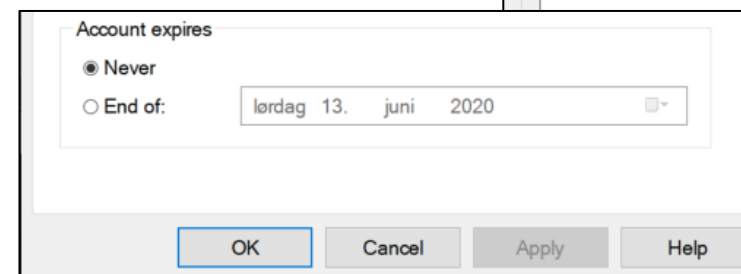
- **Begrense hvilke maskiner brukeren kan logge inn fra**

- Alle maskiner i domenet
- Bare navngitte maskiner

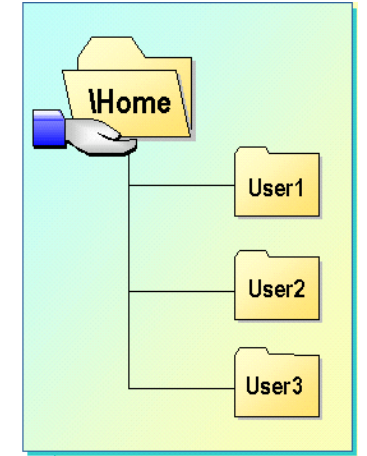


- **Begrense kontoens levetid / utløpsdato**

- kontoen stenges automatisk etter utløpt levetid



Hjemmekatalog (Home Folder)

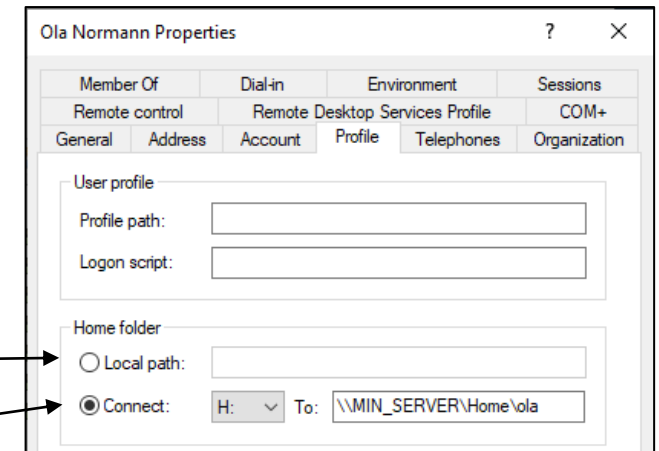


- **Brukerens "private" katalog (mappe)**

- Én mappe knyttet til hver brukerkonto
 - » Brukeren har alle rettigheter på mappen
 - » Andre brukere har ingen tilgang
- Kan ligge på lokal maskin, eller på en filtjener
 - » Bør samles under én felles mappe på filtjener
 - » Obs! Sørg for nok diskplass!

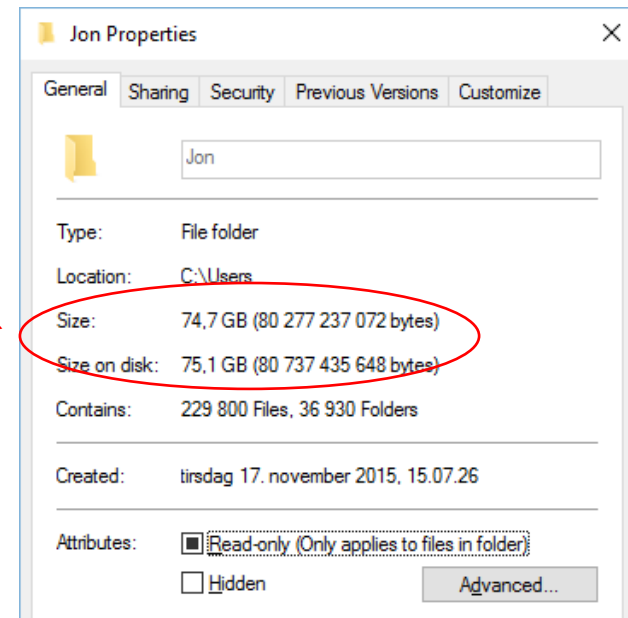
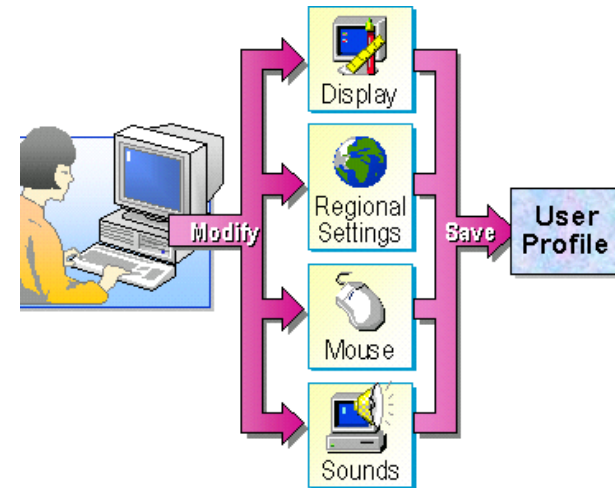
- **To alternative plasseringer**

- Local path
 - » Hjemmekatalogen plasseres på lokal disk på klientmaskin
- Connect
 - » Hjemmekatalogen legges under delt mappe på server, f.eks. mapper under en delt mappe **Home**
 - » Diskbokstaven kobles automatisk til hjemmekatalogen ved pålogging
 - » Koblingen settes opp i konfigureringsbildet for brukerinformasjon (domenebrukere)

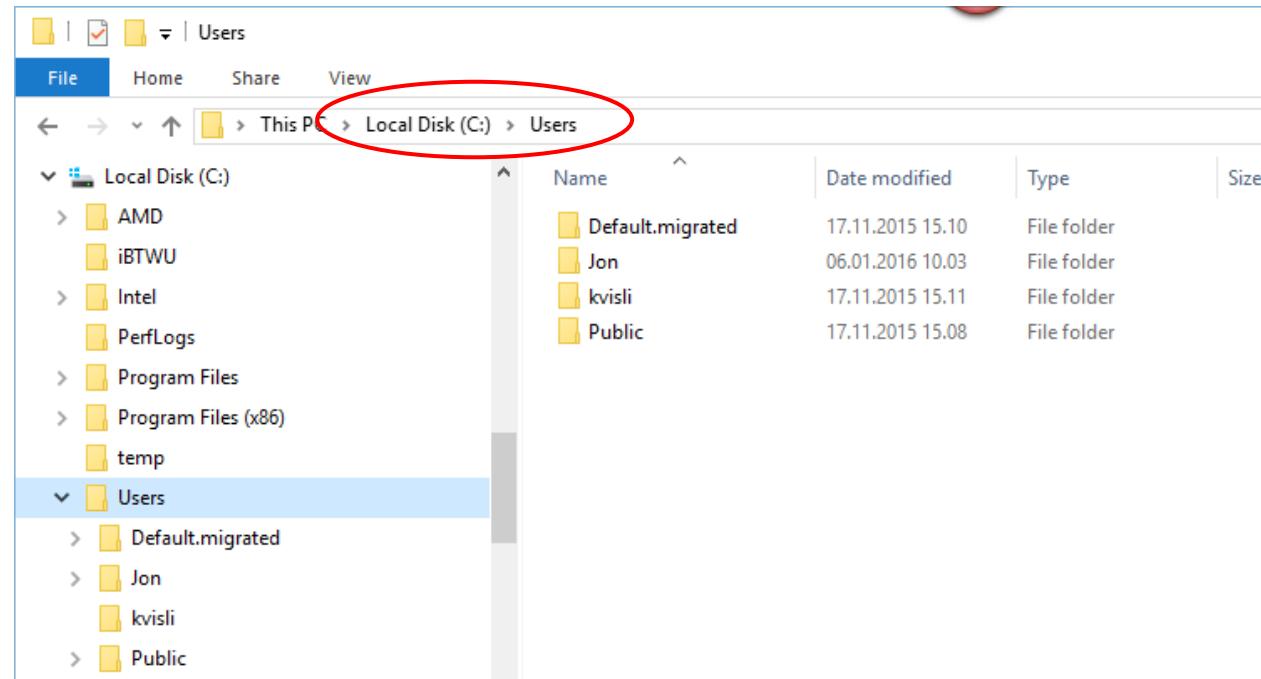


Brukerprofil

- **Lagrer brukeravhengige innstillinger:**
 - Utseende, farger, ikoner på skrivebordet (desktop'en)
 - Tilkoblinger til delte nettressurser (disker / skrivere)
 - Konfigurasjon og data for programmer
 - Brukerdefinerte innstillinger
 - m.m.
- **Både Windows og applikasjoner kan lagre data i brukerprofilen**
 - Dette kan medføre at profilen tar mye diskplass!
 - Dataene i profilen lagres og endres "automatisk" av programmene



Lokal brukerprofil



- **Lagres i en mappe på lokal disk**
 - C:\Users*brukernavn* (C:\Users*brukernavn* i norsk versjon)
 - Profilmappen opprettes første gang bruker logger inn!
- **Spesielle (skjulte) profiler i Windows**
 - *Default* mal for nye brukerprofiler
 - *Public* felles profil-elementer for alle brukere

Noe av innholdet i brukerprofilen

- **Den skjulte filen NTUSER.DAT**

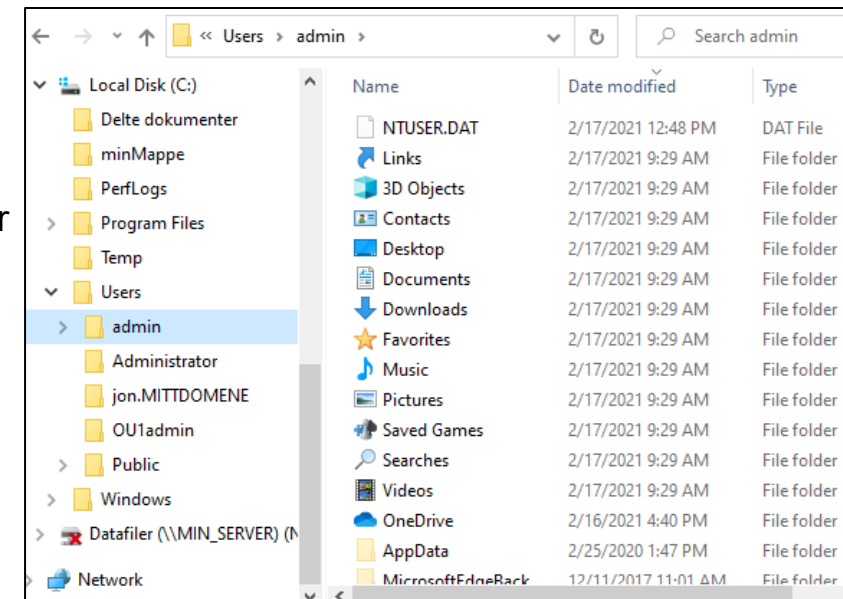
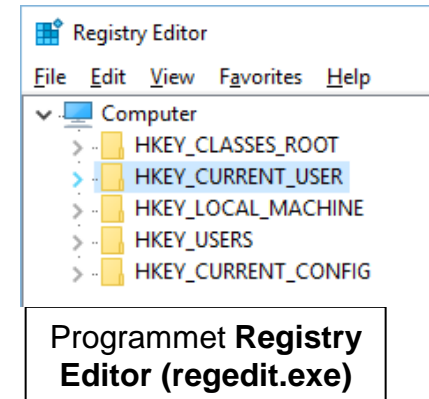
- Inneholder **brukerdelen** av *Windows Registry* (**HKEY_CURRENT_USER**)
 - » Database med brukerens "Windows-innstillinger", bl.a. fargevalg
- Filen holdes åpen og låst så lenge bruker er pålogget !

- **Mapper i den lokale brukerprofilen:**

- Contacts Brukerens kontakter
- Desktop Filer og snarveier på brukerens skrivebord
- Documents, Brukerens dokumenter
- Downloads Brukerens nedlastede filer
- Favorites Brukerens favoritter i Internet Explorer / Edge
- Music, Pictures, Videos Brukerens musikk-, bilde- og videofiler

- **Skjulte og beskyttede systemmapper i profilen:**

- AppData Beregnet for lagring av "midlertidige data" fra applikasjoner
- Cookies Cookier for Internet Explorer
- Local Settings Brukes som Application data, men innholdet kopieres ikke til tjener ved bruk av "roaming profile"
- Nethood, PrintHood Snarveier til delte mapper og skrivere som brukes
- Recent Snarveier til nylig brukte filer
- SendTo Snarveier som vises i "Send to" menyen
- Start Menu Snarveier som vises i startmenyen



Brukerprofil i nettverk

- **Vandrende (roaming) brukerprofil**

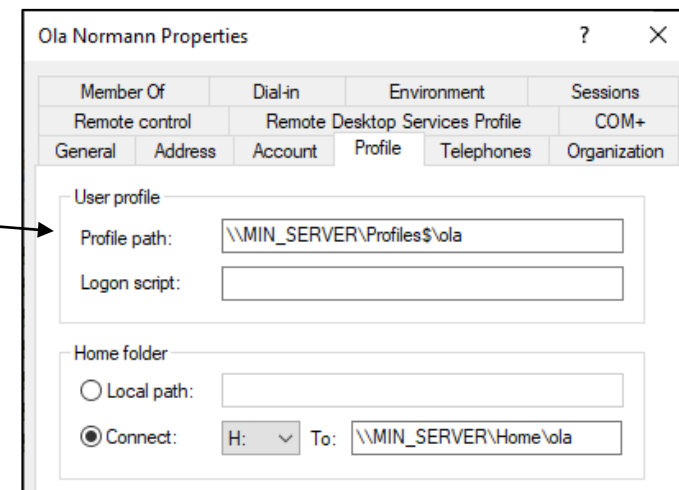
- Profilen lagres på en filtjener, f.eks. i brukerens hjemmekatalog, eller i en egen katalog for profiler
 - » Nettverksadministrator bestemmer plassering (*Profile Path*)
 - » Profilmappen opprettes **ved første pålogging**
- Profilen kopieres til lokal profil på systemdisken (C:\Users) når brukeren logger på lokal maskin med en domenebruker
- Alle endringer skjer i den lokale profilen
- Endringene skrives tilbake til filtjener når bruker logger ut
- Dette gir brukeren tilgang til den samme profilen fra alle maskiner i nettet!

- **Standard (default) brukerprofil**

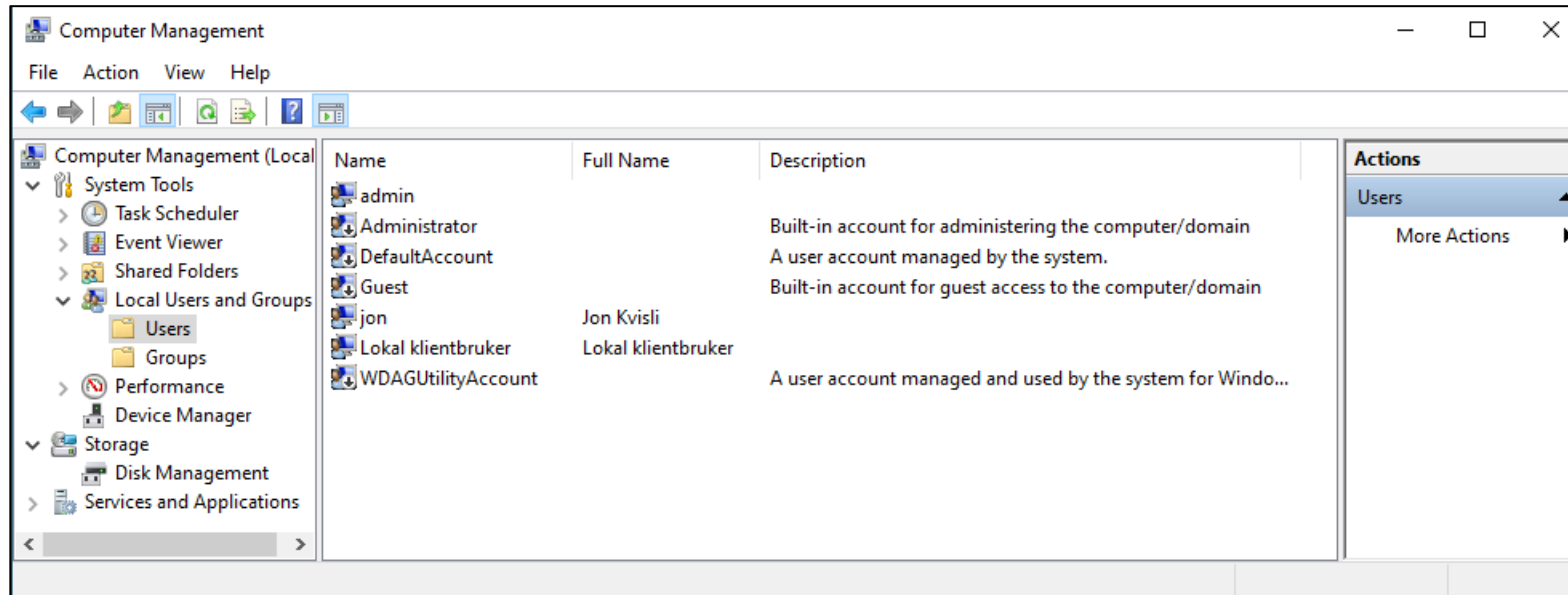
- En felles ”profilmal” som alle nye bruker får kopi av
- Kan endres fritt av bruker etter første pålogging

- **Påtvunget (mandatory) brukerprofil**

- Felles profil som ikke kan endres av brukere
- Egnet for å gi alle brukere samme skrivebord / oppsett
- NTUSER.DAT døpes om til NTUSER.MAN
- Kan være lokal eller roaming



Administrasjonsverktøy (demo)



- **Computer Management – for å administrere lokal maskin**
 - Lokale brukere (og grupper)
 - Delte mapper lokalt på maskinen (Shared Folders)
 - Maskinvare (Device Manager)
 - m.m.
- **Obs! Kan ikke administrere domener / domenekontoer!**

Administrasjonsverktøy (demo)

Active Directory Users and Computers

- **For å administrere domener**

- Domenebrukere
- Domenegrupper
- Datamaskiner / domenekontrollere
- OU'er
- m.m.

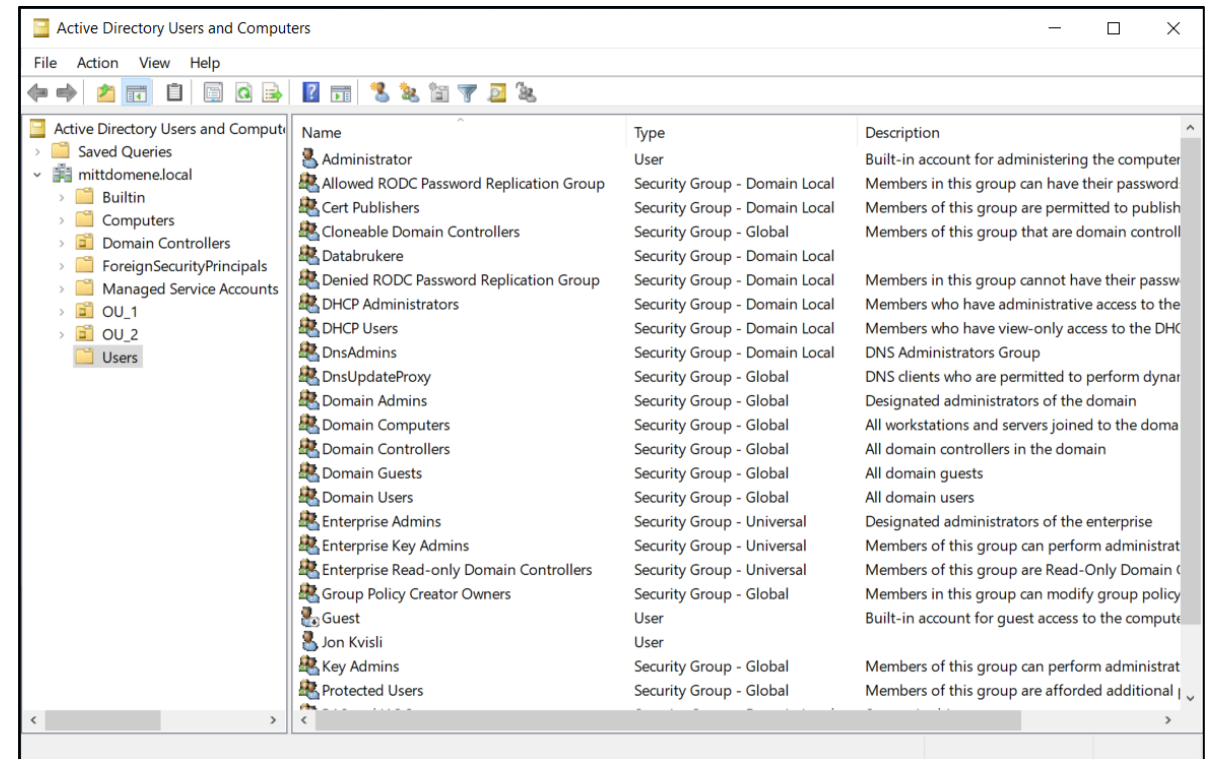
- **Egenskaper**

- Kan brukes fra alle datamaskiner i domenet
 - » eller via terminaltjener / remote desktop
- Må kjøres som bruker med administrative rettigheter i domenet
 - » Medlem av gruppen Domain Admins.

- **Installeres automatisk på domenekontroller**

- **På medlemstjener:**

- Må installeres som en del av funksjonen (*feature*) Active Directory Domain Controller Tools.



Kommandofiler og logon skript

- **Kommandofil (batchfil / skriptfil)**

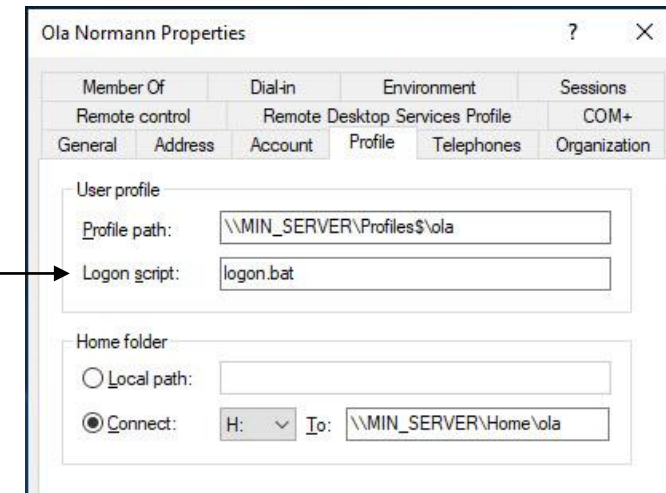
- Tekstfil som inneholder Windows kommandoer (tilsvarer shellskript i Linux)
- Filtype: .BAT
- Når filen kjøres utføres alle kommandoene i filen
- Eksempel: kommandofil som sletter alle Word og Excel filer

```
del *.doc*
del *.xls*
```

- **Logon script**

- Kommandofil som kjøres hver gang bruker logger på
- Lagres på filtjener / domenekontroller
I mappen: C:\WINDOWS\SYSTEM32\sysvol\domenenavn\SCRIPTS
- Kan f.eks. brukes for å koble til nettverksdisker automatisk ved pålogging:

```
net use P: /delete
net use P: \\MIN_SERVER\prog
net use H: /delete
net use H: \\MIN_SERVER\Users\%username%
```



Windows-kommandoen NET

Kommandoen NET kan bl.a. brukes for å utføre brukeradministrasjon i Windows

- kan skrives i kommandovindu, eller kjøres fra kommandofiler / logon skript.
- har flere opsjoner og bruksområder:

net share	deling av ressurser
net use	tilkobling av ressurser
net user	behandling av brukere
net group	behandling av domenegrupper
net localgroup	behandling av lokale grupper
net help	hjelp til net kommandoene. Se: net help <kommando>

NET kommandoen er ikke pensum i dette emnet!