

GLOBETEAM



Central Brugerstyring:

Brugervejledning til administrati-
onsløsning

DSML-udtræk fra Active Directory,
version 1.21



Indledning

Dette dokument beskriver, hvordan man etablerer et korrekt DSML-formatteret udtræk fra Active Directory, som kan anvendes af administratoren for partnerorganisationen til automatiseret oprettelse af brugere via det centrale brugerstyrings-administrationsprogram.

Hvis du ønsker at øge automatiseringsgraden, eksportere fra et andet directory end Active Directory eller blot gøre tingene på en anderledes måde end beskrevet her, så vil vi anbefale at du søger hjælp hos nogen, der allerede har erfaring med DSML.

Alternativt anbefales det at konsultere DSMLv2-standarden (se fx <http://www.oasis-open.org/committees/dsml/docs/DSMLv2.doc>), studere beskrivelserne af attributterne i Appendix A (med speciel vægt på alle de påkrævede attributter) samt at du sætter dig ind, hvordan man sætter passwords. Erfaringsmæssigt vil du i reglen blive i stand til at luge de første – og værste – begynderfejl ud ved at generere en DSML-fil som beskrevet i vejledningen og sammenligne med din DSML-fil.

Indhold

1. Installation af DSDE-applikation på den lokale maskine.....	3
2. Etablering af DSML-udtræk til brugeroprettelse fra Active Directory	5
3. Efterbehandling af DSML-udtræk til brugeroprettelse.....	7
4. Import i administratorapplikationen af brugeroprettelsesfil	9
5. Etablering af DSML-udtræk til tilmelding til organisationens egen gruppe.....	11
6. Efterbehandling af DSML-udtræk til tilmelding til organisationens egen gruppe	13
7. Tilmelding til organisationens egen gruppe i administratorapplikationen.....	14
Appendix A. Beskrivelse af de relevante attributter.	16



1. Installation af DSDE-applikation på den lokale maskine

Det er nødvendigt at installere en kommandolinje-applikation – Directory Services Data Exchange (DSDE) – for at etablere det nødvendige DSML-udtræk.




DSDE er en del af DSML Service for Windows-installationspakken, som p.t. kan findes på:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=37df79b8-6f2b-4c04-9744-49816baee8ae&displaylang=en>

eller direkte på:

<http://download.microsoft.com/download/7/8/D/78DB44EF-1DB7-4D19-AB75-7455E3983FE8/DSfW.msi>

DSML Service for Windows kan installeres på Windows 2000, Windows Server 2003 eller Windows XP.

<p>Start installationen af DSML Service for Windows (DSFW.MSI) og tryk OK til sikkerhedsadvarslen</p>	
<p>Tryk Next</p>	
<p>Accepter licensaftalen og tryk Next.</p>	
<p>Vælg installationsmappe og tryk Next</p>	



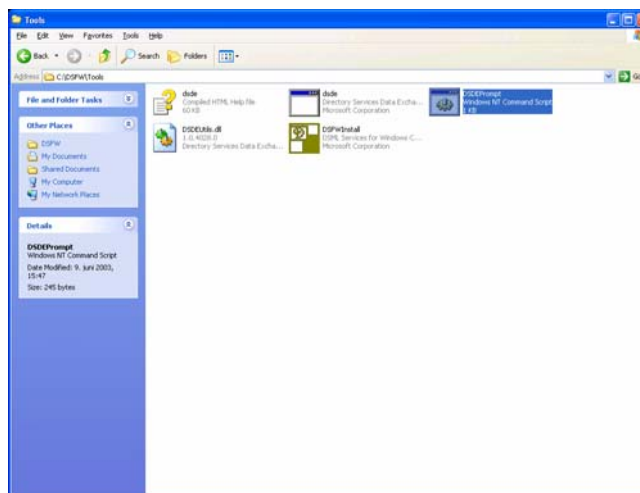
<p>Accepter installation ved at trykke Next</p>	
<p>Når installationen af DSML Service for Windows er gennemført med succes bliver følgende meddelelse vist.</p> <p>Tryk Next.</p>	
<p>Installationen afsluttes.</p> <p>Tryk Next.</p>	



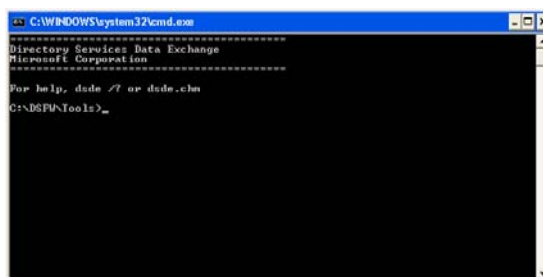
2. Etablering af DSML-udtræk til brugeroprettelse fra Active Directory

DSDE-kommandolinjeapplikationen bliver placeret i DSML Service for Windows' Tools-mappe (ved default installation af DSML Service for Windows er den fulde sti: c:\DSFW\Tools). Bemærk i øvrigt, at der medfølger en hjælpefil, som er placeret i samme mappe.

Tryk på "DSDEPrompt" i Tools-mappen



Brug kommandolinje-prompt'en til at udføre det ønskede query i Active Directory



Er den lokale maskine allerede tilsluttet den ønskede DC, skal du udføre følgende DSDE query, for at alle Active Directory-brugere fra OU'en Miljo (der i nedenstående eksempler er placeret i brugere OU'en i Active Directory-domænet gentofte.dk) bliver skrevet over i filen userimport.xml:

```
DSDE /query (objectClass=user) /baseDN OU=miljo,OU=brugere,DC=gentofte,DC=dk /scope oneLevel
/output userimport.xml /replace OU=miljo,OU=brugere,DC=gentofte,DC=dk
OU=19438414,OU=Kommune,OU=Offentlig,OU=Brugere,DC=mbsdkint,DC=dk /outRequest /attributes
objectClass,sAMAccountName,displayName,givenName,sn,mail,company,distinguishedName,userPrincipal
Name,title,department
```

Ønsker du at hente alle Active Directory-brugere fra OU'en Miljo (der er placeret i OU'en ved navn brugere) fra DC'en test, skal du udføre følgende DSDE query, for at få alle brugerne skrevet over i filen userimport.xml:



```
DSDE /query (objectClass=user) /baseDN OU=miljo,OU=brugere,DC=gentofte,DC=dk /scope oneLevel
/output userimport.xml /replace OU=miljo,OU=brugere,DC=gentofte,DC=dk
OU=19438414,OU=Kommune,OU=Offentlig,OU=Brugere,DC=mbsdkint,DC=dk /outRequest /attributes
objectClass,sAMAccountName,displayName,givenName,sn,mail,company,distinguishedName,userPrincipal
Name,title,department /prot ldap /server ldap://dc=test,dc=gentofte,dc=dk
```

Bemærk, at de to instanser af strengen "OU=miljo,OU=brugere,DC=gentofte,DC=dk" skal erstattes med det korrekte DistinguishedName (DN) i jeres eget Active Directory, samt at den ene instans af strengen "OU=19438414,OU=Kommune,OU=Offentlig,OU=Brugere,DC=mbsdk,DC=dk" skal erstattes af det DistinguishedName (DN), som jeres organisation er blevet tildelt i administratorløsningen.



3. Efterbehandling af DSML-udtræk til brugeroprettelse

Forud for import af DSML-udtrækket fra det lokale Active Directory udføres følgende tilpasninger:

- Indsætning af organisationens CVR-nummer:

Den simpleste metode er at åbne filen i en editor og gennemføre en Search and Replace operation	
Search skal være:	<attr name="distinguishedName">
Replace skal være:	<attr name="CVR-Nummer"><value>19438414</value></attr><attr name="distinguishedName">

- Indsætning af userAccountControl-attributten med værdien 544:

Den simpleste metode er at åbne filen i en editor og gennemføre en Search and Replace operation	
Search skal være:	<attr name="distinguishedName">
Replace skal være:	<attr name="userAccountControl"><value>544</value></attr><attr name="distinguishedName">

- Indsætning af organisationens forkortelse i employeeNumber-attributten. Husk at ændre det nuværende id (157) til organisationens forkortelse:

Den simpleste metode er at åbne filen i en editor og gennemføre en Search and Replace operation	
Search skal være:	<attr name="distinguishedName">
Replace skal være:	<attr name="employeeNumber"><value>157</value></attr><attr name="distinguishedName">

- Ændring til korrekt brugernavn (dvs. tilføjelse af prefix) i addRequest og distinguishedName. Husk at ændre det nuværende id (157) til organisationens forkortelse:

Den simpleste metode er at åbne filen i en editor og gennemføre en Search and Replace operation	
Search skal være:	CN=
Replace skal være:	CN=157

- Ændring til korrekt brugernavn (dvs. tilføjelse af prefix) i displayName. Husk at ændre det nuværende prefix (157) til organisationens forkortelse:

Den simpleste metode er at åbne filen i en editor og gennemføre en Search and Replace operation	
Search skal være:	<attr name="displayName"><value>
Replace skal være:	<attr name="displayName"><value>157



- Ændring til korrekt brugernavn (dvs. tilføjelse af prefix) i samAccountName. Husk at ændre det nuværende prefix (157) til organisationens forkortelse:

Den simpleste metode er at åbne filen i en editor og gennemføre en Search and Replace operation	
Search skal være:	<attr name="sAMAccountName"><value>
Replace skal være:	<attr name="sAMAccountName"><value>157

- Ændring til korrekt brugernavn (dvs. tilføjelse af prefix) i userPrincipalName. Husk at ændre det nuværende prefix (157) til organisationens forkortelse:

Den simpleste metode er at åbne filen i en editor og gennemføre en Search and Replace operation	
Search skal være:	<attr name="userPrincipalName"><value>
Replace skal være:	<attr name="userPrincipalName"><value>157

- Ændring til korrekt suffix i userPrincipalName. Husk at ændre det nuværende suffix (gentofte.dk) til organisationens forkortelse:

Den simpleste metode er at åbne filen i en editor og gennemføre en Search and Replace operation (bemærk at det vil være nødvendigt at lave en mere avanceret search and replace, såfremt der er navnesammenfald mellem organisationens eget Active Directory-domæne og maildomænet)	
Search skal være:	@gentofte.dk
Replace skal være:	@mbsdk.dk

Hvis søgningen ikke fungerer som ventet, skyldes det typisk, at du har benyttet et "forkert" anførelselstegn (dvs. et tegn, der har en anden Unicode-værdi), end det der benyttes i XML-dokumentet.

Der bør ikke være behov for yderligere tilpasninger, medmindre organisationen anvender p-nummer eller har behov for at angive IP-adresser (se appendix A). Men det kan naturligvis forekomme alafhængig af den konkrete Active Directory-implementering. Som regel vil det dog højst være nødvendigt at fjerne overflødige eller vildledende attributinformationer.

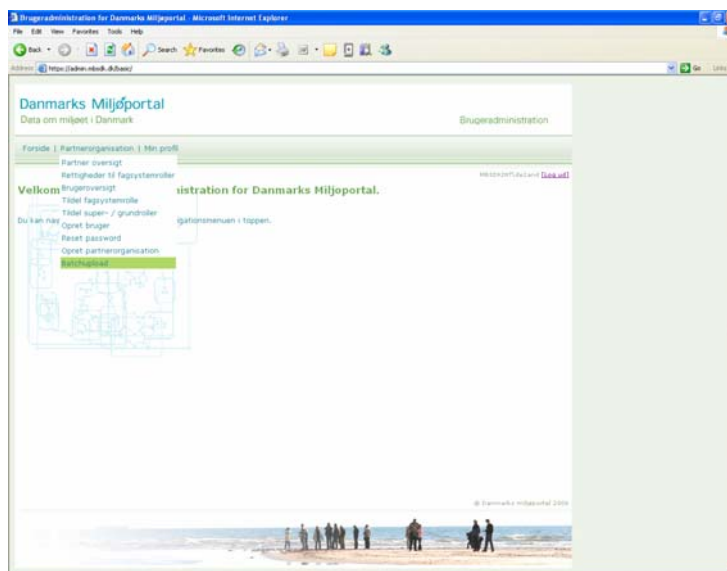


4. Import i administratorapplikationen af brugeroprettelsesfil

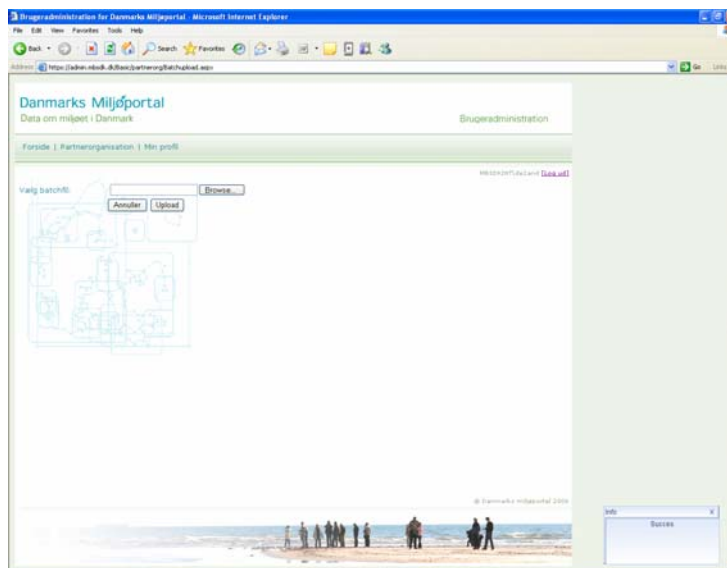
Når den DSML-formatterede fil er klargjort, importeres den i administratorapplikationen (vælg Batchupload i Partnerorg.-menuen).

Logget ind som partnerorganisations-administrator

Vælges "Batchupload"



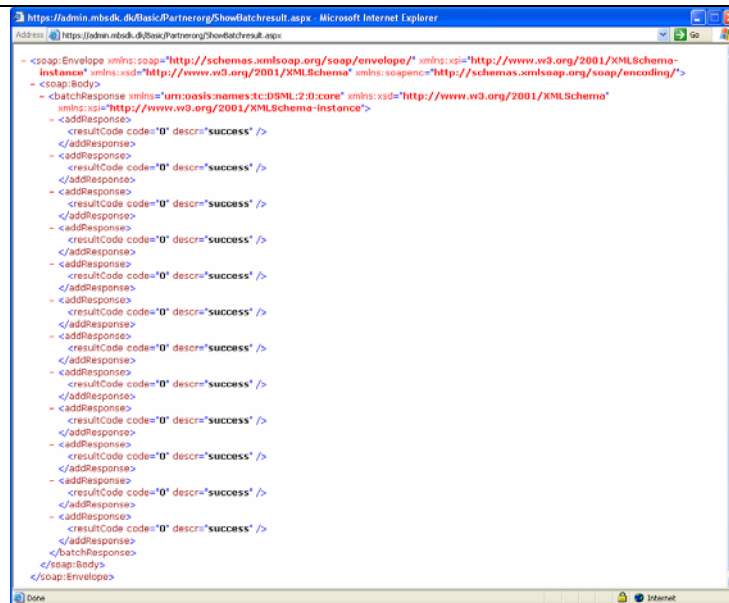
Herefter kan DSML filen lokaliseres og uploades fra den lokale maskine.





Når filen er blevet importeret vil resultatet af operationen (DSML response filen) blive vist i et separat vindue.

Hvis du har fulgt vejledningen og operationen fejler så tidligt at der ikke bliver genereret en responsfil, så skyldes det typisk at filen er gemt i et andet format end ASCII (fx Unicode eller RTF-8).



Det er i øvrigt også muligt at aflevere DSML-formattede filer via administratorapplikationens web service.

Bemærk, at brugerens konto som udgangspunkt er låst og uden password. Kontoen kan enten låses op manuelt i administratorapplikationen af partnerorganisationsadministrator, eller også kan der etableres en DSML-fil, som ændrer password'et.

Ønsker du at tilføje et nyt password via DSML, tager det sig således ud i DSML:

```
<modifyRequest
dn="CN=brugernavn,OU=19438414,OU=Kommune,OU=Offentlig,OU=Brugere,DC=mbsdkint,DC=dk">
  <modification name="unicodePwd" operation="replace">
    <value xsi:type="xsd:base64Binary">IjEyMzQ1Njc4OSI=</value>
  </modification>
</modifyRequest>
```

Bemærk, at password'et skal Base64-kodes samt at der skal sættes gåseøjne (") omkring selve passwordet.

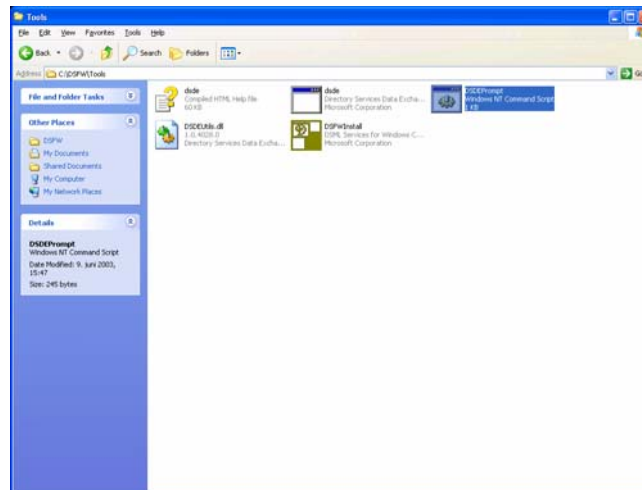
Bemærk yderligere, at det i dette tilfælde er administratorens ansvar, at brugeren bliver informeret om, at han nu er oprettet, og hvad hans password er sat til (samt at hans normale brugernavn er blevet "genbrugt", men dog har fået tilføjet et prefix).

Alternativt kan man bede den centrale administrator om at autoudsende nye passwords til alle brugere i en partnerorganisation. Bemærk dog at dette i givet fald vil gælde for **alle** brugere i den pågældende partnerorganisation (herunder den juridiske administrator og partnerorganisationsadministratorer).

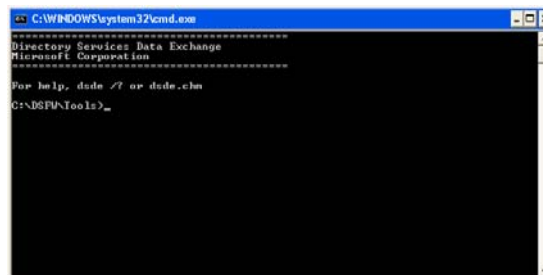


5. Etablering af DSML-udtræk til tilmelding til organisationens egen gruppe

Tryk på "DSDEPrompt" i Tools-mappen



Brug kommandolinje-prompt'en til at udføre det ønskede query i Active Directory



Er den lokale maskine allerede tilsluttet den ønskede DC, skal du udføre følgende DSDE query, for at alle Active Directory-brugere fra OU'en Miljo (der er placeret i OU'en brugere i Active Directory-domænet gentofte.dk) bliver skrevet over i filen gruppe.xml:

```
DSDE /query (objectClass=user) /baseDN OU=miljo,OU=brugere,DC=gentofte,DC=dk /scope oneLevel
/output groupimport.xml /replace OU=miljo,OU=brugere,DC=gentofte,DC=dk
OU=19438414,OU=Kommune,OU=Offentlig,OU=Brugere,DC=mbsdkint,DC=dk /outRequest /attributes
no_attribute
```

Ønsker du at hente alle Active Directory-brugere fra OU'en Miljo (der er placeret i OU'en brugere) fra DC'en test, skal du udføre følgende DSDE query, for at få alle brugerne skrevet over i filen use-rimport.xml:

```
DSDE /query (objectClass=user) /baseDN OU=miljo,OU=brugere,DC=gentofte,DC=dk /scope oneLevel
/output groupimport.xml /replace OU=miljo,OU=brugere,DC=gentofte,DC=dk
OU=19438414,OU=Kommune,OU=Offentlig,OU=Brugere,DC=mbsdkint,DC=dk /outRequest /attributes
no_attribute /prot ldap /server ldap://dc=test,dc=gentofte,dc=dk
```



Bemærk, at de to instanser af strengen "OU=miljo,OU=brugere,DC=gentofte,DC=dk" skal erstattes med organisationens eget DistinguishedName (DN), samt at den ene instans af strengen "OU=19438414,OU=Kommune,OU=Offentlig,OU=Brugere,DC=mbsdk,DC=dk" skal erstattes af organisationens DistinguishedName (DN) i administratorløsningen.



6. Efterbehandling af DSML-udtræk til tilmelding til organisationens egen gruppe

Forud for import af DSML-udtrækket fra det lokale Active Directory vil der skulle udføres følgende tilpasninger:

- Ændring til gruppe(dvs. tilføjelse af prefix) i samAccountName:

Den simpleste metode er at åbne filen i en editor og gennemføre en Search and Replace operation	
Search skal være:	<addRequest dn="
Replace skal være:	<modification name="member" operation="add"><value>

- Ændring til korrekte brugernavn (dvs. tilføjelse af prefix) i samAccountName:

Den simpleste metode er at åbne filen i en editor og gennemføre en Search and Replace operation	
Search skal være:	DC=dk" />
Replace skal være:	DC=dk</value></modification>

- Ændring til korrekte brugernavn (dvs. tilføjelse af prefix) i addRequest og distinguishedName. Husk at ændre det nuværende prefix (157) til organisationens forkortelse:

Den simpleste metode er at åbne filen i en editor og gennemføre en Search and Replace operation	
Search skal være:	CN=
Replace skal være:	CN=157

- Tilføjelse af modifyrequest for den korrekte gruppe. Husk at erstatte strengen "OU=19438414,OU=Kommune,OU=Offentlig,OU=Brugere,DC=mbsdk,DC=dk" med organisationens DistinguishedName (DN) og erstatte strengen "CN=19438414" med "CN=<organisationens cvr-nummer>" (hvor <organisationens cvr-nummer> bør være det samme som det tal, der er angivet i den første OU= i DN'en):

Den simpleste metode er at åbne filen i en editor og gennemføre en Search and Replace operation	
Search skal være:	core">
Replace skal være:	core"><modifyRequest dn="CN=19438414,OU=19438414,OU=Kommune,OU=Offentlig,OU=Brugere,DC=mbsdk,DC=dk">

- Ændring til korrekte afslutning af DSML-filen:

Den simpleste metode er at åbne filen i en editor og gennemføre en Search and Replace operation	
Search skal være:	</batchRequest>
Replace skal være:	</modifyRequest></batchRequest>

Såfremt search ikke fungerer som ventet så skyldes det typisk at man har brugt et "forkert" anførelstegn (dvs. et tegn, der har en anden Unicode-værdi) end det, der benyttes i XML-dokumentet.

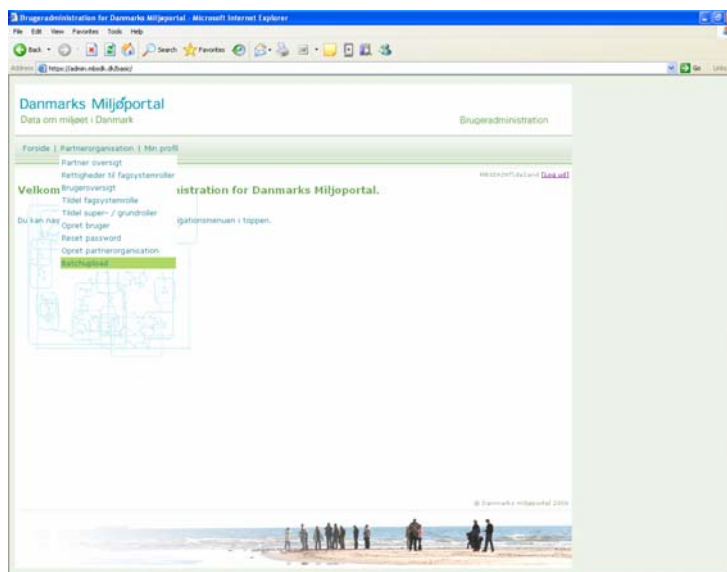


7. Tilmelding til organisationens egen gruppe i administratorapplikationen

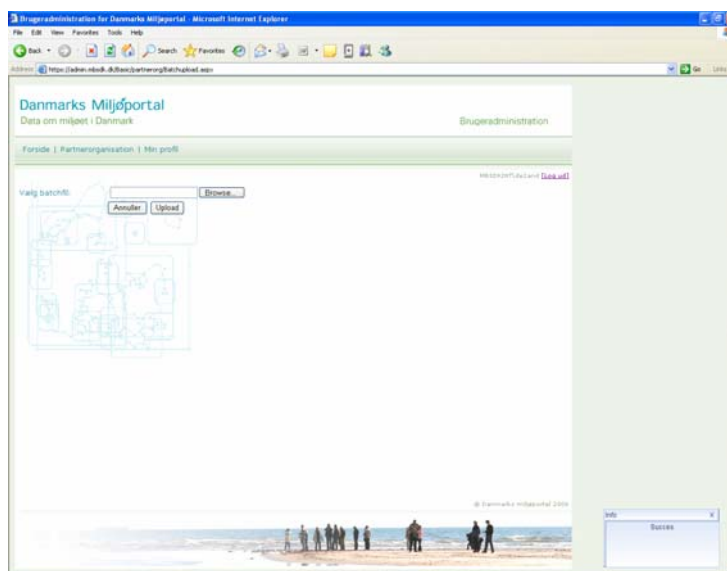
Når den DSML-formatterede fil er klargjort, importeres den i administratorapplikationen (vælg Batchupload i Partnerorg. menuen).

Logget ind som partnerorganisations-administrator

Vælges "Batchupload"



Herefter kan DSML-filen lokaliseres og uploades fra den lokale maskine.



Når filen er blevet importeret vil resultatet af operationen (DSML response filen) blive vist i et separat vindue.



Det er i øvrigt også muligt at aflevere DSML-formattede filer via administratorapplikationens web service.



Appendix A. Beskrivelse af de relevante attributter.

Såfremt organisationen besidder erfaring med LDAP-baserede directories er det naturligvis også muligt at frembringe de nødvendige brugerinformationer på en mere fuldautomatisk måde. Dette appendix beskriver kravene til attributter på brugerne med henblik på at muliggøre en sådan løsning.

Attributnavn	Påkrævet (Ja/Nej)	Beskrivelse	Syntaks	Eksempel	Kommentar	Syntaks
sAMAccountName	J	Brugerens traditionelle logonnavn (NT-logonnavnet)	Kun engelske bogstaver og tal. Dannes som en kombination af et unikt prefix, der henviser til organisationen, og brugerens nuværende loginnavn.	cfksaa		Unicode String (0 til 256)
userPrincipalName	J	Brugerens fulde navn (inkl. "@domain")	RFC 822-baseret navn: Dvs. <i>samAccountName@mbsdk.dk</i>	cfksaa@mbsdk.dk		Unicode String
givenName	J	Brugerens fornavn og evt. mellemnavn	Alle tegn i Western Europe character set [ISO 8859-1]	Sten Aabo		Unicode String (1 til 64)
sn	J	Brugerens efternavn	Alle tegn i Western Europe character set [ISO 8859-1]	Hansen		Unicode String (1 til 64)
userPassword	J	Brugerens password	Min. 9 tegn. Kun engelske bogstaver og tal.	Pass12345	Opbevares i UTF-8 format. Write-only attribut.	Objekt (1 til 128)



title	N	Brugerens titel	Alle tegn i Western Europe character set [ISO 8859-1]	Konsulent		Unicode String (1 til 64)
mail	J	Brugerens e-mail adresse	Kun engelske bogstaver og tal samt "@" og "."	saa@cfk.dk		Unicode String (0 til 256)
userCertificate (eller X509Cert)	N	Brugerens certifikater	DER-kodede X.509v3-certifikater		<i>Tager kun imod DER-kodede certifikater</i>	Objekt
company	N	Navnet på den virksomhed, hvor brugeren er ansat	Alle tegn i Western Europe character set [ISO 8859-1]	Center for Koncernforvaltning		Unicode String (1 til 64)
department	N	Navnet på afdelingen, hvor brugeren er ansat	Alle tegn i Western Europe character set [ISO 8859-1]	IT-afdelingen		Unicode String (1 til 64)
employeeNumber	J	Unik virksomhedsidentificer	Alle tegn i Western Europe character set [ISO 8859-1]	CFK		Unicode String (1 til 512)
streetAddress	N	Postadresse	Alle tegn i Western Europe character set [ISO 8859-1]	Rentemestervej 8		Unicode String (1 til 1024)
l	N	By	Alle tegn i Western Europe character set [ISO 8859-1]	København NV		Unicode String (1 til 128)
postalCode	N	Postnr.	Alle tegn i Western Europe character set [ISO 8859-1]	2400		Unicode String (1 til 40)
telephoneNumber	N	Telefonnr.	Alle tegn i Western Europe character set [ISO 8859-1]	72307000		Unicode String (1 til 64)



userAccountControl	J	Indeholder en række flag, der kontrollerer brugerkontos opførelse	Styring på bits (se http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/a_useraccountcontrol.asp for udtømmende information)	Benyttes typisk til disable/enable af bruger	<i>Skal ændres i forbindelse med brugeroprettelsen for at stå korrekt</i>	DWORD (4 bytes)
cn (eller Common-Name) & name (eller RDN)	J	Brugerens directorynavn (dvs. det, der bliver vist i AD Users and Computers).	<i>samAccountName</i>	cfksaa		Unicode String (hvv. 1 til 64 og 1 til 255)
displayName	J	Brugerens fulde navn	<i>samAccountName</i>	cfksaa		Unicode String (0 til 256)
altSecurityIdentities	N	Skal være udfyldt når brugeren kan logge ind med et certifikat	Se http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/security_properties.asp	X509<I>DC=dk,DC=mbsdk,CN=Users,CN=user01,E=user01@mb.sdk.dk.		Unicode String
CVR-Nummer	J	Organisationens CVR-nummer	8-cifret tal (evt. med landekode foran)	12854358		Unicode String (multi-valued)
P-Nummer	N	Organisationens P-nummer	10-cifret tal Hver IP-adresse skal se således ud: <Tal mellem 0 og 255>.<Tal mellem 0 og 255>.<Tal mellem 0 og 255>.<Tal mellem 0 og 255>. Hvis der er flere IP-adresser skal de separeres med et ";".			Unicode String
url	N	En eller flere IPv4-adresser i formatet separeret med ";"		10.100.1.1;10.100.1.4		Unicode String



Derudover skal brugeren som tidligere nævnt gøres til medlem i organisationens egen gruppe (se også afsnittet "Efterbehandling af DSML-udtræk til tilmelding til organisationens egen gruppe").