Kako sinkronizirati Microsoft Active Directory s LDAP imenikom ustanove?

Prvi korak - kreiranje certifikata za Microsoft Active Directory

Da bi se mogao realizirati sustav koji drži u sinkronizaciji osnovne podatke u LDAP-u i Microsoft Active Directory-ju potrebno je najprije konfigurirati Microsoft Active Directory tako da koristi SSL (port 636), odnosno imati certifikat za server. Active Directory ne dozvoljava promjenu zaporke ako komunikacija nije zaštićena SSL-om.

Uporabom alata `makecert.exe` kreirajte certifikat za Active Directory:

```
makecert -n "CN=CA_FQDN" -r -sv ca_key.pvk ca_cert.cer
```

pri čemu vrijednost parametra `CA_FQDN` treba odgovarati FQDN vrijednosti vašeg poskužitelja.

Izvršavanjem gore navedene naredbe kreirat će se dvije datoteke:

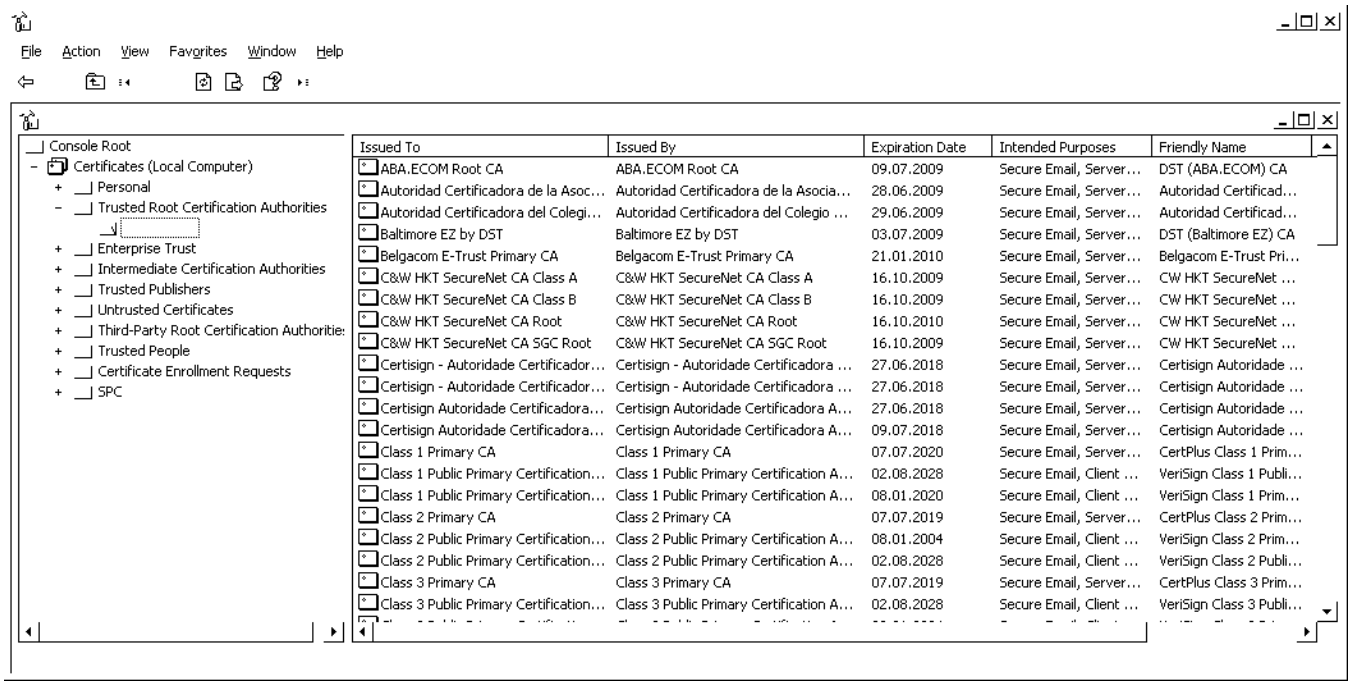
- **`ca_key.pvk`** - sadrži privatni ključ CA;
- **`ca_cert.cer`** - generirani certifikat CA;

Uporabom konzole za manipuliranje certifikatima generirani CA certifikat potrebno je dodati u spremište certifikata kojima vjerujemona sljedeći način:

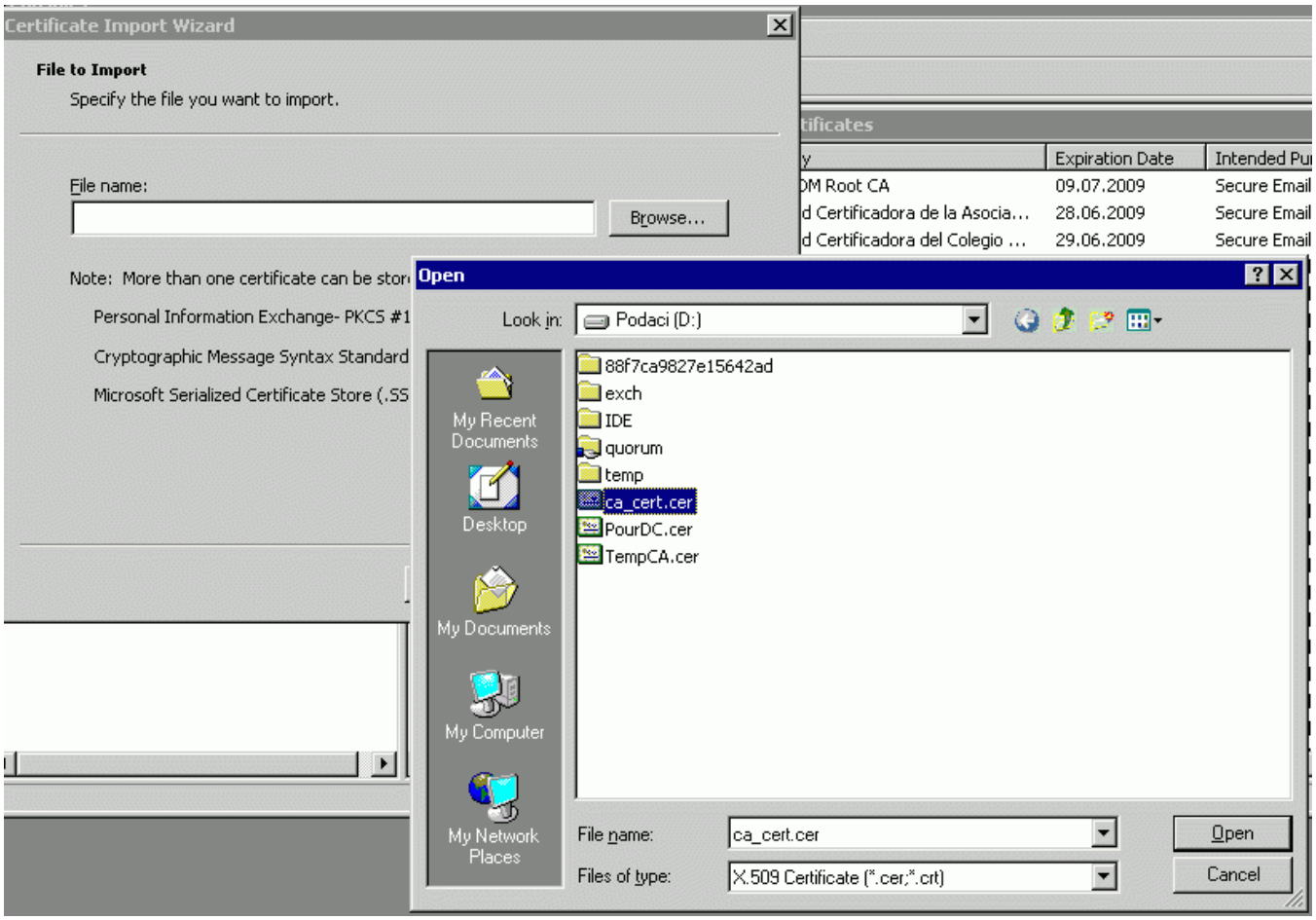
1.Pokrenite MMC: **`Start -> Run -> mmc`**

2.Iz izbornika **File** odabere se **Add/Remove Snap in** i nakon odabira komande **Add** iz izbornika odabere se **Certificates** tipa **Computer Account**:

3.U stablu je popis certifikata kojima vjerujemo **Certificates / Trusted Root Certificate**. U kontekstonom izborniku (desni gumb miša) za tu stavku odabere se **Import**:



4.Potrebno je odabrati CA certifikat koji se u našem slučaju nalazi u datotecica_cert.cer :

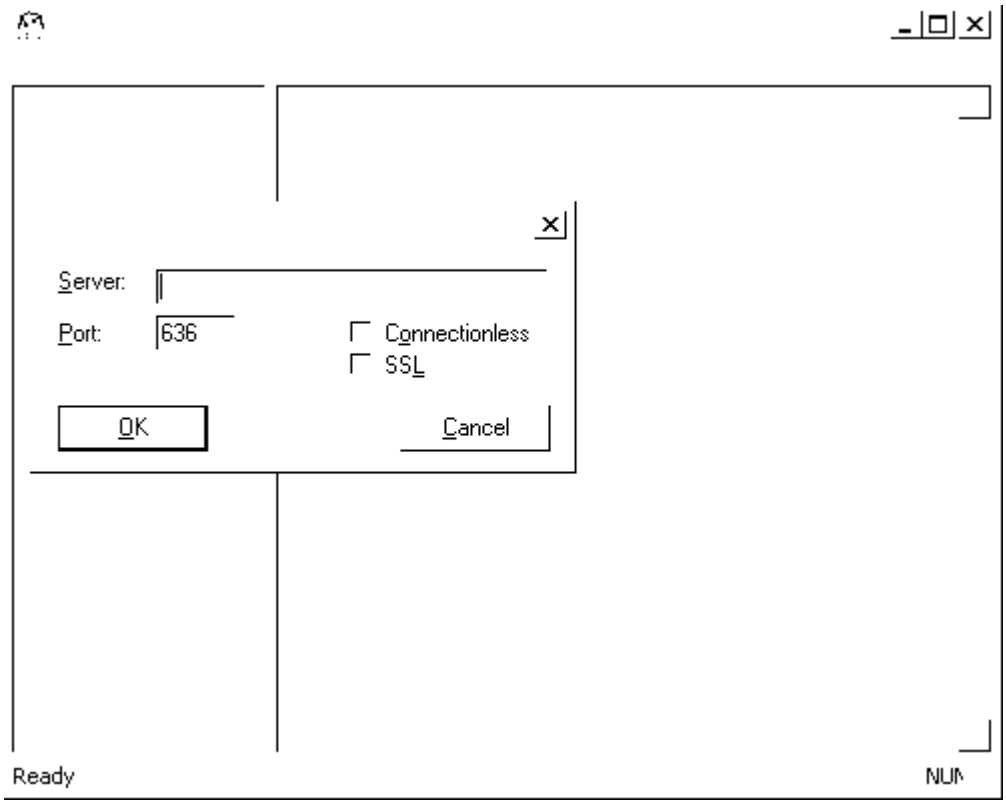


5.Sada se može kreirati certifikat za autentikaciju poslužitelja i potpisati ga od strane CA (naredba se piše u jednom retku, no zbog preglednosti je svaka opcija prikazana u svom retku):

```
makecert -sk ServerName
         -iv  ca_key.pvk
         -n  "CN=FQDN_posluzitelja"
         -ic  ca_cert.cer ServerName.cer
         -eku 1.3.6.1.5.5.7.3.1
         -ss  my
         -sr  localMachine
         -sky  exchange
         -sp  "Microsoft RSA SChannel Cryptographic Provider"
         -sy   12
```

U navedenoj naredbi potrebno je **FQDN_posluzitelja** zamijeniti stvarnom FQDN vrijednošću poslužitelja te opcionalno **ServerName** i **ServerName.cer** zamijeniti imenom kojim želimo nazvati generirani certifikat (npr. AD_cert i AD_cert.cer).

Za kraj preostaje provjeriti je li moguće Active Directory-ju pristupit LDAPS protokolom. To se može provjeriti alatom **ldp.exe** koji je dio Microsoft Support Tools(link is external)-a. Pod **Server** se upisuje poslužitelj koji provjerava dok je LDAPS port 636.



Ako se **ldp.exe** uspješno spoji na poslužitelj LDAPS protokolom, ispisat će se poruka s prva dva retka:

```
ld = ldap_open("posluzitelj", 636);
Established connection to poslužitelj
```

Drugi korak - inicijalna sinkronizacija

U drugom koraku potrebno je sinkronizirati MS Active Directory bazu s već postojećim podacima u LDAP imeniku:

1. Za sve korisnike koji već imaju račun u MS Active Directory-ju provjerite imaju li u LDAP imeniku **uid** jednak korisničkom računu u MS Active Directory bazi (odnosno je li [LDAP] **uid** = [MSAD] **sAMAccountName**);
2. Provjerite imaju li svi korisnici iz LDAP-a račun u MS AD, ako nemaju potrebno ih je inijeti u MS AD:

   a. Eksportirajte korisničke podatke iz LDAP imenika u .ldif datoteku:

   ```
   ldapsearch -LLL -H ldap://server:389/ -b "dc=domena,dc=hr" -x -D "cn=admin,dc=domena,dc=hr" -s sub -
   W "objectClass=hreDuPerson" uid givenName sn cn mail o ou hrEduPersonUniqueId
   hrEduPersonPrimaryAffiliation > backup.ldif
   ```

   b. Datoteku **backup.ldif** prebacite na poslužitelj na kojem se nalazi MS Active Directory;
   c. U isti direktorij odkomprimirajte program za uvoz korisnika iz LDIF datoteke
   d. Pokrenite program za import korisnika iz .ldif datoteke:

   ```
   USERIMPORT backup.ldif
   ```

   Program će preskočiti korisnike čiji **uid**-i se već nalaze u MS AD. Korisnici se ubacuju u **OU** naziva **Import-AAI** i kao **description** imaju vrijednost atributa **hrEduPersonPrimaryAffiliation**.

3. Instalirajte AOSI web klijent (AOSI-WWW) inačicu 1.6 ili noviju:

```
#apt-get install aosi-aai-www
```

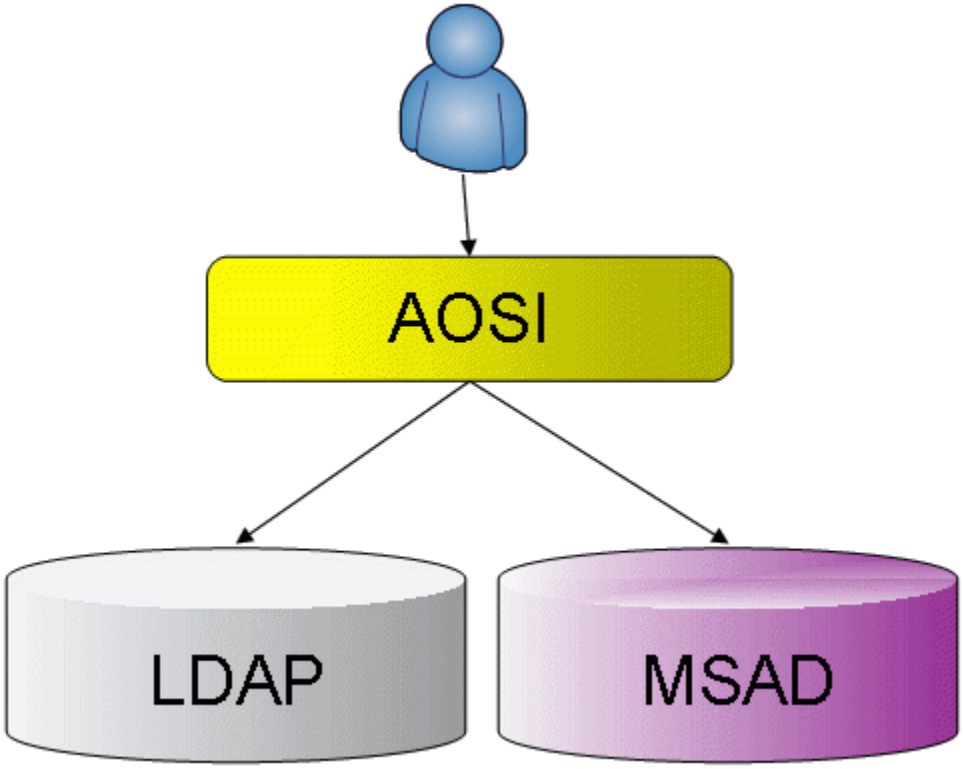
4. Instalirajte AOSI web servis (AOSI-WS) s podrškom za plug-inove (inačica 2.1 ili novija):

```
#apt-get install aosi-aai
```

Napomena: prilikom instalacije AOSI web klijenta 1.6+ će se automatski instalirati odgovarajuća verzija AOSI web servisa.

5. Instalirajte MSAD plug-in za AOSI web servis koji održava LDAP i MS AD u sinkronom stanju:

```
#apt-get install libmsad-aosi-aai
```



6.Na MS AD serveru potrebno je kreirati dva korisnika (zapamtite njihove lozinke):

- AOSIRO - korisnik koji ima samo mogućnost dohvaćanja podataka iz AD;
- AOSIWRT - korisnik koji ima mogućnost stvaranja i brisanja unosa u AD;

7. Potrebno je pravilno konfigurirati AOSI plug-in u datoteci **`/usr/lib/aosi/Plugins/MSAD.conf`** (napomena: nemojte koristiti Perl specijalne znakove u stringovima!):

`<base_dn dc=ustanova,dc=hr>` - upisati BASE_DN ustanove;

`AD_base` - base DN od AD-a (primjer: `AD_base = DC=ADDomena,DC=local`);

`AD_hostname` - DNS naziv poslužitelja ili IP adresa na kojoj se nalazi AD (primjer: `AD_hostname = 161.53.233.233`);

`AD_port` - port na kojemu sluša AD s certifikatom - podrazumijevani je 636 (primjer: `AD_port = 636`);

AD_aosiro_dn - Distinguished Name korisnika koji ima pravo čitanja iz AD-a. (primjer: `AD_aosiro_dn = CN=AOSIRO, CN=Users,${AD_base},` ovdje je prikazan način kako iskoristiti već definirane vrijednosti - `AD_base`);

AD_aosiro_pwd - zaporka AOSIRO računa (primjer: `AD_aosiro_pwd = aosiropwd`);

AD_aosiwrt_dn - Distinguished Name korisnika koji ima pravo pisanja u AD (primjer: `AD_aosiro_dn = CN=AOSIWRT, CN=Users,${AD_base},` ovdje je prikazan način kako iskoristiti već definirane vrijednosti - `AD_base`);

AD_aosiwrt_pwd - `zaporka` AOSIWRT računa (primjer: `AD_aosiro_pwd = aosiwrtpwd`);

AD_new_dn - inicijalno će svi korisnici biti kreirani kreirati u ovoj grupi. AD administratori mogu kasnije premjestiti korisnike u druge grupe (primjer: `AD_new_dn = CN=Users`);

users_ou - korisnici će biti kreirani u navedenim grupama ovisno o vrijednosti atributa hrEduPersonPrimaryAffiliation, npr:

```
<users_ou hrEduPersonPrimaryAffiliation>
default = CN=Users
student = OU=Studenti
</users_ou>
```

AD_new_users_disabled - `odreuje` hoće li novostvoreni računi biti onemogućeni: 1 - da, 0 - ne (primjer: `AD_new_users_disabled = 0`);

AD_new_users_pne - `odreuje` hoće li zaporka novostvorenih računa biti bez vremenskog ograničenja: 1 - da, 0 - ne (primjer: `AD_new_users_pne = 1`);

AD_new_users_pwd_exp - određuje hoće li zaporka novostvorenih računa odmah biti nevažeća (kako bi korisnici morali postaviti novu zaporku): 1 - da, 0 - ne (primjer: `AD_new_users_pwd_exp = 0`);

use_custom_suffix - ako se AD_base razlikuje od domene (realm) ustanove, upisuje se realm u `userPrincipalName` (primjer: `use_custom_suffix = 1`);

AD_custom_suffix - ako se AD_base razlikuje od domene (realm) ustanove, ovdje se upiše realm ustanove koji će se upisivati u `userPrincipalName`, kako bi korisnici mogli kao naziv računa pisati `korisnik@domena.hr` (primjer: `AD_custom_suffix = domena.hr`);

custom_filter - `ako je potrebno` sinkronzirati samo određenu grupu ljudi (odn. identitete koji imaju određeni atribut postavljen na određenu vrijednost, npr. djelatnike), tada se ova vrijednost postavlja na oblik `atribut=vrijednost` (primjer: `custom_filter = hrEduPersonPrimaryAffiliation=djelatnik`). **Ako želite sinkronizirati sve identitete, ovaj parametar nemojte upisivati u konfiguracijsku datoteku!**

custom_filter_operator - ako parametar `custom_filter` sadrži više filtera, primejnjuje se operator naveden u ovom retku (primjer: `custom_filter_operator = and`);

panic_on_errors - `treba` li plug-in prekinuti osnovnu operaciju za LDAP imenik: 1 - da, 0 - ne;

show_warnings_as_errors - treba li plug-in sva upozorenja koje pošalje AD proslijediti kao pogrešku: 1 - da, 0 - ne;

m_attributes - popis atributa koji se smiju mijenjati u AD (izmjena ostalih atributa se ne proslijeđuje AD-u), npr:

```
<m_attributes>
userPassword
</m_attributes>
```

admin_users - popis uid-a koji smiju unositi promjene u AD - najčešće su to isti uid-i kao i u `/etc/aosi/valid_user` datoteci. Korisnici smiju mijenjati samo neke atribute, npr:

```
<admin_users>
u100
u200
</admin_users>
```

exclude_users - popis uid-a za koje se neće obavljati sinkronizacija, npr:

```
<exclude_users>
    ne_windows_racun
</exclude_users>
```

Primjer konfiguracije:

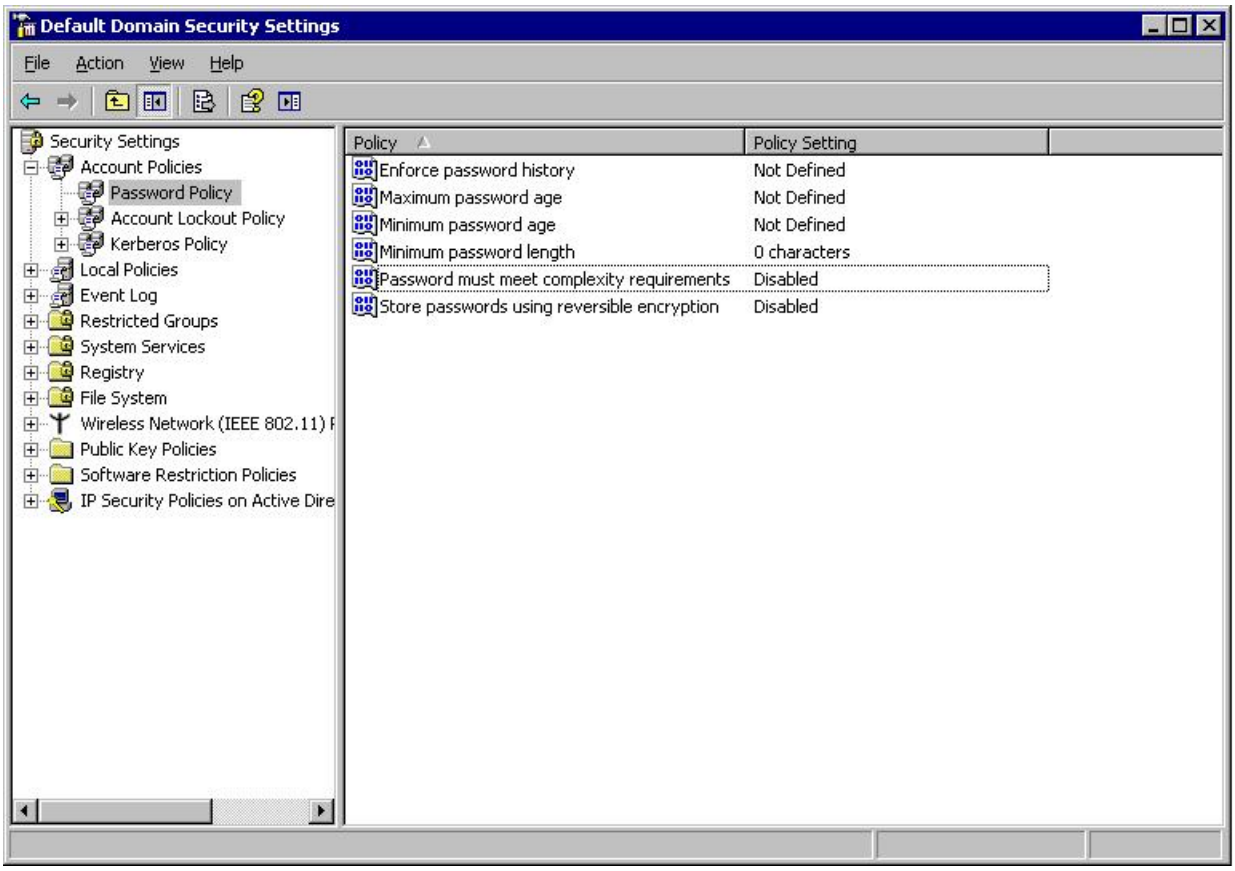
```
# WARNING: Do not use special Perl characters in strings (e.g. names, passwords etc)
<base_dn dc=domena,dc=hr>
AD_base                 = DC=ADDomena,DC=local
AD_hostname             = 161.53.233.233
AD_port                 = 636
AD_aosiro_dn            = CN=AOSIRO,CN=Users,${AD_base}
AD_aosiro_pwd           = aosiropwd
AD_aosiwrt_dn           = CN=AOSIWRT,CN=Users,${AD_base}
AD_aosiwrt_pwd          = aosiwrtpwd
AD_new_dn               = CN=Users
<users_ou hrEduPersonPrimaryAffiliation>
  default = OU=Ostali
  student = OU=Studenti
  djelatnik = OU=Djelatnici
<users_ou>
AD_new_users_disabled   = 0
AD_new_users_pne        = 1
AD_new_users_pwd_exp    = 0
use_custom_suffix       = 1
AD_custom_suffix        = domena.hr
panic_on_errors         = 0
show_warnings_as_errors = 0
<m_attributes>
  userPassword
</m_attributes>
<admin_users>
     u100
     u200
</admin_users>
<base_dn>
```

8. Potrebno je provjeriti je li aktiviran MSAD plug-in, odn. u datoteci **`/etc/aosi/plugins.conf`** provjeriti postoji li redak u kojemu piše **`MSAD`** (ne smije ispred pisati znak #).

9. Da bi zaporke u obje baze (LDAP imenik i MS Active Directory) bile sinkronizirane, nakon uspostave operativne veze LDAP - Active Directory korisnici moraju postaviti zaporku u oba repozitorija. Da bi se to izvršilo, potrebno je obavijestiti korisnike da postave zaporku kroz AOSI web sučelje.

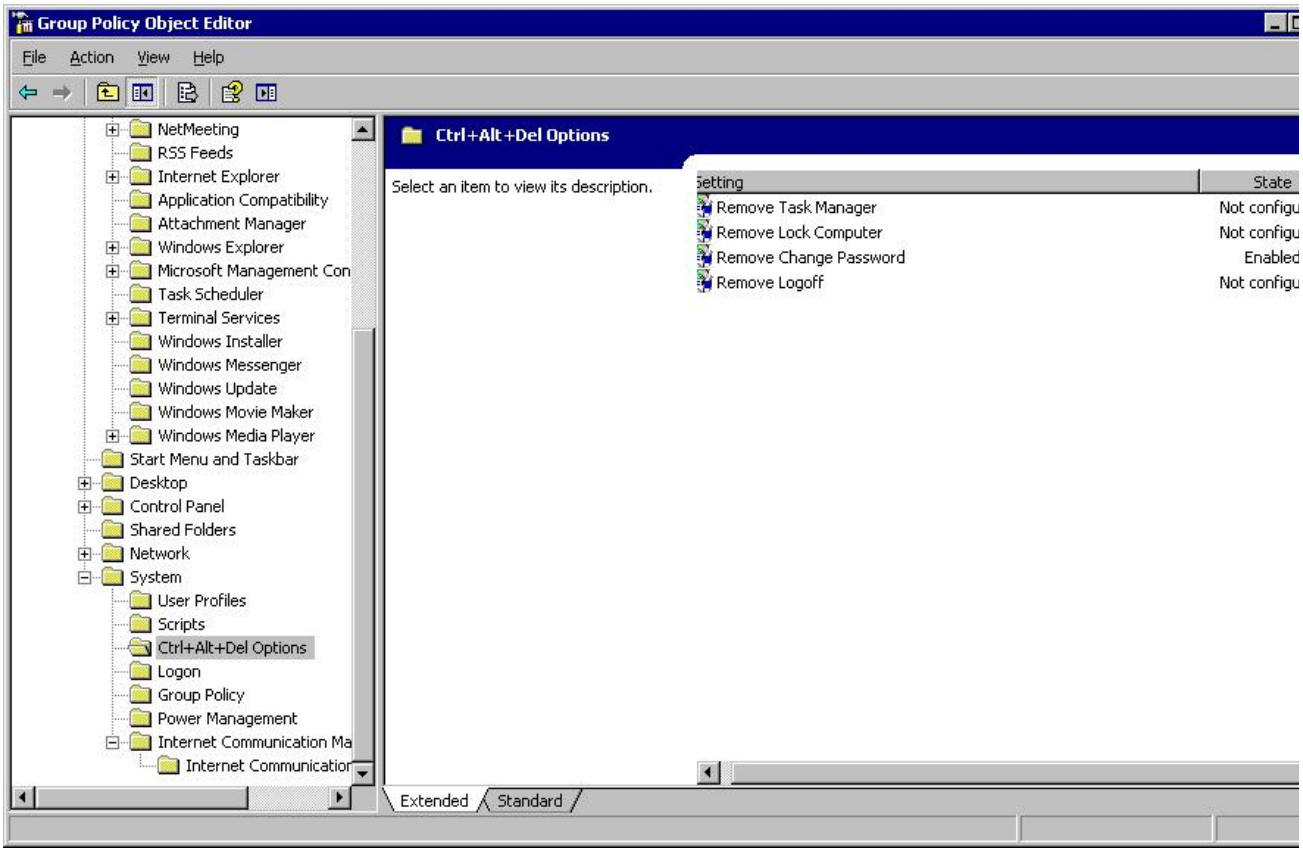
10. Na strani MS AD u **`Domain Security Policy`** -> **Account Policies** -> **Password Policy** potrebno je postaviti odgovarajući *Password Policy* za zaporke:

Enforce Password Histry=Not Defined
Maximum Password age=Not Defined
Minimum Password age=Not Defined
Minimum Password length=0
Password must meet complexity requirements=Disabled
Store Password using Reversible encryption=Disabled



11.Sprječavanje korisnika da mijenjaju zaporku u MS AD - kroz **`Group Policy Editor`** potrebno je za korisničke račune postaviti:

User Configuration/
Administrative Template/
System/
Ctrl+Alt+Del Options/
Remove Change Password=Enabled



Sinkronizacija više Active Directory-ja

Ako ustanova ima npr. odvojene MS AD domene za djelatnike i studente moguće ih je odvojeno sinkronizirati.

Predradnje

Da bi se mogao postaviti sustav koji drži u sinkronizaciji osnovne podatke u LDAP imeniku i više Microsoft Active Directory-ja, potrebno je prema gore navedenim uputama instalirati MSAD ASOI plug-in (**`libmsad-aosi-aai`**).

Filteri

Prilikom konfiguracije plug-in-a vrijednost parametra **`custom_filter`** mora se postavti na jednu od vrijednosti za određeni atribut (npr. **`custom_filter = hrEduPersonPrimaryAffiliation=djelatnik`**).

Umnožavanje

U sljedećim koracima će se kopirati postojeće MSAD plug-in datoteke u nove:

1. Pozicionirajte se u direktorij s plug-inovima:

   ```
   cd /usr/lib/aosi/Plugins
   ```

2. Napravite kopiju MS AD plug-in modula:

   ```
   cp MSAD.pm MSAD_student.pm
   ```

3. Napravite kopiju MS AD plug-in konfiguracijske datoteke:

   ```
   cp MSAD.conf MSAD_student.conf
   ```

4. Otvorite datoteku plug-in modula (`MSAD_student.pm`) u vašem omiljenom editoru i napravite sljedeće:

    1. Pronađite redak **package plugins::MSAD;** i prepravite ga u **package plugins::MSAD_student;**

    2. Redak **my $plugin_name = 'MSAD';** promijenite u **my $plugin_name = 'MSAD_student';**

5. Otvorite novu konfiguracijsku datoteku (`MSAD_student.conf`) u vašem omiljenom editoru i promijenite vrijednosti sljedećih parametara:

    1. **AD_base**;

    2. **AD_hostname**;

    3. Ako je potrebno **AD_aosiro_dn** i **AD_aosiro_pwd**;

    4. Ako je potrebno **AD_aosiwrt_dn** i **AD_aosiwrt_pwd**;

    5. **custom_filter** (npr. custom_filter = hrEduPersonPrimaryAffiliation = student);

6. datoteci **`/usr/lib/aosi/Plugins/plugins.conf`** dodajte novi plug-in:

```
MSAD
MSAD_student
LDIFSync
```

7. Restartajte AOSI web servis:

```
/etc/init.d/aosi restart
```

8. Da biste provjerili je li se novi plug-in učitao, provjerite sadržaj datoteke **`/var/log/aos/aosi.log`** u kojoj bi se trebali nalaziti otprilike ovakvi zapisi:

```
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD: getting admin list: u100, u200
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD: getting exclusion list: Administrator
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD: users disabled=0
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD: users password never expires=1
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD: users password expires now=0
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD: use custom suffix=1
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD: custom suffix=realm.hr
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD: panic on errors=1
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD: custom
filter=hrEduPersonPrimaryAffiliation=djelatnik
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD: filters=hrEduPersonPrimaryAffiliation =>
[djelatnik];
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD_student: getting admin list: u100, u200
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD_student: getting exclusion list:
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD_student: users disabled=0
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD_student: users password never expires=1
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD_student: users password expires now=0
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD_student: use custom suffix=1
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD_student: custom suffix=realm.hr
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD_student: panic on errors=1
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD_student: custom
filter=hrEduPersonPrimaryAffiliation=student
Apr 26 06:25:04 aosi-dev aosi[9836]: -=- Plugins::MSAD_student: filters=hrEduPersonPrimaryAffiliation =>
[student];
```

Ako je potrebno, prethodno opisani postupak možete ponoviti više puta uz poštivanje jedinstvenosti naziva datoteka.