Riferimenti e documenti utili:

- [http://search.cpan.org/~gbarr/perl-ldap/lib/Net/LDAP.pod|Net::LDAP]
- [http://markmail.org/message/mc3gjcb6fnsgtctr#query:net%3A%3Aldap%20user%20authentication%20perl+p
  Re: web user authentication using Net::LDAP]
- [http://www.perlmonks.org/?node=327902|Re: LDAP authentication with Net::LDAP]
- [http://www2.pluto.it/files/ildp/HOWTO/LDAP-HOWTO/index.html|LDAP HowTo (IT)]
- [http://www.sugarforge.org/screenshots/screenshot.php/60/150/fullsize/LDAP_Config.JPG|SugarCRM configu

Se lo scopo è solo autenticare la password di un utente dovrebbe bastare connettersi al server LDAP con le credenziali la connessione riesce allora l'utente è autenticato.

In questo modo bisogna comunque creare e gestire l'utente nel DB di IGSuite.

Per svincolarsi si potrebbe, credo, utilizzare il server LDAP per memorizzare le informazioni che normalmente sono m di IGSuite.

Lucas (08.05.2009): Quello che non so come gestire è proprio la sincronia tra i dati contenuti nel server LDAP e quelli un server LDAP in genere lo fa per accentrare i dati degli utenti sul server LDAP e non per doverli gestire sui vari softw LDAP, giusto? se è così dal momento che l'amministratore configurerà IGSuite per autenticarsi con LDAP dobbiamo f mantenendo i dati d'accesso a IGSuite (e lasciando la sincronia a senso unico: da LDAP a IG) sul server LDAP e quelli modificabili dal modulo "Personale". Ma chi crea gli utenti? LDAP al momento della prima richiesta di autenticazione?

Es.

```
sub autenticazione
 {
  if ( IG non trova abbinamento login e password in "users")
   {
    # prova con LDAP
    if ( ($login,$pwd,$NomeCognome) = interroga LDAP )
     {
      # LDAP dice OK
      if ( $login non esiste in "users")
       {
        inserisce_in_users( $login, $NomeCognome) # senza pwd
       }
      ok_sono_autenticato();
     }
   }
  else
   {
    ok_sono_autenticato();
   }

  non_sono_autenticato();
 }
```

TUTOS WAY www.tutos.org (configuration)

The way it works

To be able to authenticate your TUTOS users with a LDAP server, you will have first to configure the way to authentic
TUTOS users.

There's not one way of doing LDAP authentication, and you will need to know how LDAP is configured on your serve
TUTOS.

The scheme is always the same, you send the user name and password to the server, and it will accept or reject the con
doing that with a LDAP server :

Anonymous bind
: You connect as the anonymous user on the LDAP server, then you retrieve the user name and passwd, in order
;

User bind
: You try to connect the LDAP server directly with the given user name and passwd, and you will get an accept

Admin bind
: On some LDAP servers, you will have to connect as admin to be able to get the password info. Once connected
informations just as in the anonymous bind case.

Of course, for each of those cases, the password can be stored « as is » or encrypted.

How to configure it

After reading the first part, the config options should be easy to set up. So here are the parts of the config file to edit :

```
# LDAP configuration
#
# 0 = check standard database
# 1 = check ldauthserver for password verification
$tutos[ldapauth] = 0;

# encrypted passwords
# 1 = yes
$tutos[ldapauth_pw_enc] = 1;

$tutos[ldapauthserver]['host'] = "scd2ldap.siemens.net";
$tutos[ldapauthserver]['port'] = 389;

$tutos[ldapauthserver]['basedn'] =  "ou=mail,ou=user,o=cvf";
$tutos[ldapauthserver]['userdn'] = "uid";
```

LDAP paths, without such an info you can't find the user infos on the server. If you don't know those values, just ask y
the last part of the DN, in the example given we would find : uid=username,ou=mail,ou=user,o=cvf

We still have to separate those values because of the way LDAP search and binding works.

```
# use given user/passwd pair to bind the LDAP server
# 0 = no
# 1 = yes
```

```
$tutos[ldapauth_user] = 0;
```

If you set this option, we will use the user name and password to connect to the LDAP tree.

```
# do anonymous bind to ldpauthserver
# 1 = yes
# 0 = use tutos[ldapauthserver]['binddn']
#     and tutos[ldapauthserver]['passwd']
$tutos[ldapauth_anonymous] = 1;
```

Here you can choose to make an anonymous bind to the LDAP server...

```
$tutos[ldapauthserver]['binddn'] = "ou=adminprs,ou=ldap,ou=user,o=cvf";
$tutos[ldapauthserver]['passwd'] = "h4ckm3";
```

In the case you would have to bind the LDAP server as an admin, you will have to provide another LDAP path, wich c
privileged user) username. Then there is his password.

Adding the users to the tutos database

Now you have set up the authentication process, you still can't use TUTOS. In fact you can login, but nothing happens.
with the same login as the LDAP ones.

I've made a php script to do that, ldap_getdata.php in php/admin directory. As LDAP structure can be really different f
script is far from generic, but works well here !

You should make it fit with your own LDAP structure and then get all the wanted user to be created in TUTOS. If you
script generic, please feel free to contribute, by either sending us a patch, or telling us how to do that.

Simple Groupware WAY

LDAP / Active Directory

Normally Simple Groupware authenticates all users against a table in the database containing the usernames/password
"simple_sys_users".
But Simple Groupware can also use LDAP or Active Directory (AD) services for user authentication.

To enable LDAP, open your webbrowser with the Simple Groupware page and log in as super administrator (username
"/Workspace/System" and choose "Change setup settings". Choose "LDAP" as authentication mode and specify the IP
(secure connections use "ldaps://server/", unencrypted connections use "server"). By default, the connection is done to
"ldaps://server/", port 636 will be used instead.

Using Active Directory, you need to specify the windows domain which is added to the username for the authentication
to "mydomain.local", the username "administrator" is changed to "administrator@mydomain.local", note that this field

In order to handle authentication, an entry point in the LDAP directory tree is required. This entry point is called a base detect it automatically by using NamingContexts (this was successfully tested with openLDAP and Active Directory). working for you or you want to choose a different "base DN", then you can specify another value in the "base DN" fiel

Using LDAP you can use anonymous connections to resolve the DN of a user or provide the necessary credentials whi (user DN and password). The username is searched by default in the "uid" attribute within LDAP (can be changed in se this attribute is automatically set to "sAMAccountName".

Also every user still needs an account within Simple Groupware. You can create these accounts manually or check the creation" to let Simple Groupware create (or update) all accounts automatically. After making changes to setup settings Automatic creation uses these fields from LDAP/AD to create or update accounts in Simple Groupware:

```
LDAP / AD                          Simple Groupware
sAMAccountName /
```

Automatic user creation does not include group memberships. You can create these groups manually or (beginning wit option "Use LDAP Groups" together with "Enable automatic user creation" to let Simple Groupware create (or update) After making changes to Setup settings, click "Save" and you're done. When a user logs into Simple Groupware, his us automatically created (or updated) within Simple Groupware. The attribute used to identify group memberships is by d changed in setup settings.

Note: Nested groups (groups as member of other groups) are not replicated from LDAP/AD to Simple Groupware.

Note: The super administrator is not authenticated over LDAP/AD. It still uses the username and password defined dur username/password can also be changed using "Change setup settings".