Summary **Files** **Support** **Report Spam** **Log in** **Create account**

Active Directory Integration

From itop

iTop can be configured to have users authenticated against an existing Active Directory (AD) server.

The Active Directory Authentication in iTop is based on the LDAP protocol, therefore you must have PHP's LDAP extension installed when you install iTop for the AD authentication to be possible.

In iTop, the choice of the authentication method is per-user. This means that you can have User A that relies on iTop's built-in authentication mechanism and User B relying on the LDAP/AD authentication. this can be useful for example if User A is going to be used for some automation/scripting usage and User B being a real person using her/his AD account.

In this case, for each user that will be authenticated with Active Directory, a 'LDAP User' record must be created in iTop. This record defines the "rights" of the user (based on its set of profiles) but the authentication (password) is managed by Active Directory.

Contents

Configuring iTop to use Active Directory Authentication

Once iTop has been installed, adjust the configuration in the file 'config-itop.php' (at the root of the installation).

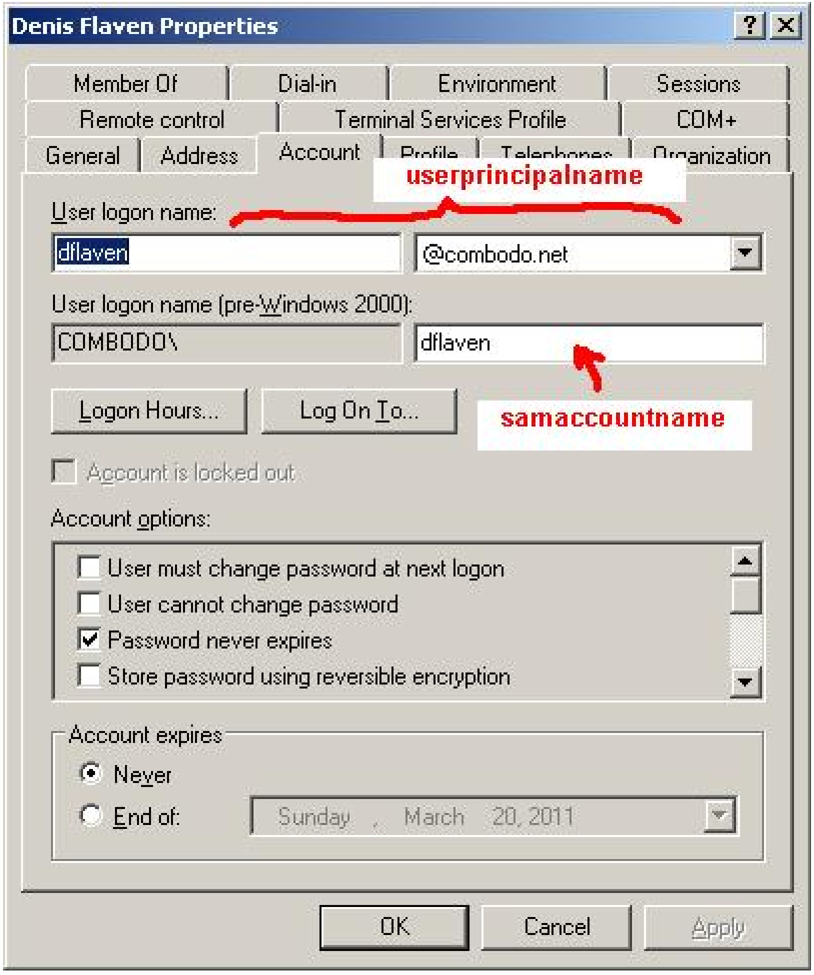
Look for the section 'authent-ldap' inside the $MyModuleSettings array.

```
$MyModuleSettings = array(
        'authent-ldap' => array (
                'host' => 'your_ad_server',
                'port' => 389,
                'default_user' => 'default_login',
                'default_pwd' => 'default_pwd',
                'base_dn' => 'DC=yourcompany,DC=com',
                'user_query' => '(&(samaccountname=%1$s)(objectCategory=User))',
                'options' => array (
  17 => 3,
  8 => 0,
),
```

- host is the IP address of FQDN of your active directory server
- post is 389 unless the AD server is using a different one (LDAPS uses 636)
- default_user and default_pwd indetify a generic user that has enough rights in the active directory to be able to retrieve the list of users as defined by the user_query
- user_query is a LDAP query string that defines how to retrieve the users in the LDAP/Active Directory tree.

There are several possibilities for the user_query depending how your AD has been implemented, since two attributes can be used to identify a Windows user in Active Directory: 'samaccountname' and 'userprincipalname'.

For example, the user listed on the screenshot below, as a samaccountname='dflaven' and userprincipalname='dflaven@combodo.net'.



Denis Flaven Properties

User logon name: dflaven @combodo.net

User logon name (pre-Windows 2000): COMBODO\ dflaven

☐ Account is locked out

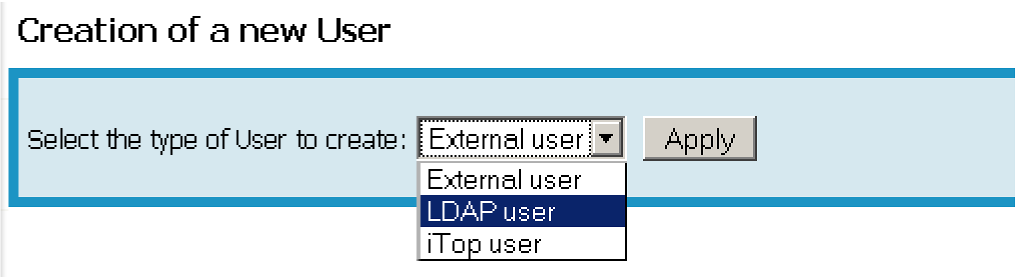
Account options:

☐ User must change password at next logon
☐ User cannot change password
☑ Password never expires
☐ Store password using reversible encryption

Account expires

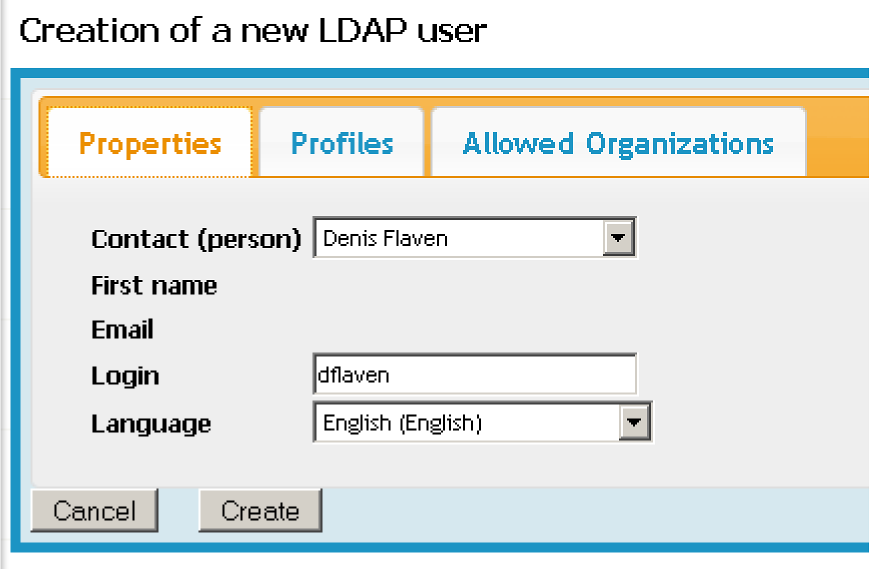
● Never
○ End of: Sunday , March 20, 2011

So if I create a user whose login is 'dflaven' in iTop (as shown below - don't forget to assign a profile to the account):



Creation of a new User

Select the type of User to create: External user



Creation of a new LDAP user

Contact (person) Denis Flaven

First name

Email

Login dflaven

Language English (English)

I can use the following two queries to retrieve the user from Active Directory:

```
'user_query' => '(&(samaccountname=%1$s)(objectCategory=User))',
```

or

```
'user_query' => '(&(userprincipalname=%1$s@combodo.net)(objectCategory=User))',
```

the later will work if all users are part of the 'combodo.net' domain.

On the other end I can decide to create a user with the login 'dflaven@combodo.net' in iTop and to use the following query in the configuration file:

```
'user_query' => '(&(userprincipalname=%1$s)(objectCategory=User))',
```

You can also adjust the ldap_query to force the users to be members of a particular AD group. For example the following query will only allow the members of the AD group "iTop Users" (CN=iTop Users,CN=Users,DC=combodo,DC=net) to log into iTop:

```
'user_query' => '(&(samaccountname=%1$s)(objectCategory=User)(memberOf=CN=iTop Users,CN=Users,DC=
```

Advantage of this method: if the person is removed from the specified AD group, then her/his access to iTop is immediately revoked.

Troubleshooting

Once you've setup the iTop configuration to work with AD and created your first 'LDAP' user, try to connect to iTop using this newly created account.

If the login fails, have a look at the file "error.log" located at the root of the iTop installation folder, at the end of the file you should see something like:

```
2011-02-18 15:04:44 | Error | ldap_authentication: no entry found with the query '(samaccountname
```

If the message is "User not found in LDAP", check that:

1. The user exists in AD. (names are not case sensitive)
2. The default account (default_user/default_pwd) has enough rights to list the existing users in AD.
3. The LDAP query is correct...

If the error message is "wrong password for user..." check that the password is correct (the password IS case sensitive)

If the error message is "several (xx) entries match the query ", check that your user_query is correct and actually contains %1$s in its definition.

Importing users from Active Directory

It is possible to import/synchronize users from an Active Directory to an iTop instance using the sample script below.

The script performs the following tasks:

1. Extract the information from the Active Directory, based on a given LDAP query
2. For each LDAP record found, search for the corresponding iTop user accounts and either

    If a match is found (based on the login name) the script synchronizes the profiles of the iTop user with the AD information
    Else the script creates a new iTop user (and if needed also a Person) based on the AD information

Download the following script, and copy it in the "webservices" folder of iTop: AD_import_accounts.php (http://www.combodo.com/documentation/AD_import_accounts.txt)

Script's configuration

Edit the configuration array at the beginning of the script to tailor it to your needs:

```
///////////////////////////////////////////////////////////////////////////////
// Configuration parameters: adjust them to connect to your AD server
// And configure the mapping between AD groups and iTop profiles
$aConfig = array(

        // Configuration of the Active Directory connection
        'host'  => 'localhost', // IP or FQDN of your domain controller
        'port'  => '389', // LDAP port, 398=LDAP, 636= LDAPS
        'dn'            => 'DC=combodo,DC=net', // Domain DN
        'username'      => 'ad_user', // username with read access
        'password'      => 'ad_password', // password for above

        // Query to retrieve and filter the users from AD
        // Example: retrieve all users from the AD Group "iTop Users"
        'ldap_query' => '(&(objectCategory=user)(memberOf=CN=iTop Users,CN=Users,DC=combodo,DC=ne
        // Example 2: retrieves ALL the users from AD
        // 'ldap_query' => '(&(objectCategory=user))', // Retrieve all users

        // Which field to use as the iTop login samaccountname or userprincipalname ?
        'login' => 'samaccountname',
        //'login' => 'userprincipalname',

        // Mapping between the AD groups and the iTop profiles
        'profiles_mapping' => array(
                //AD Group Name => iTop Profile Name
                'Administrators' => 'Administrator',
                ),

        // Since each iTop user must have at least one profile, assign the profile
        // Below to users for which there was no match in the above mapping
        'default_profile' => 'Portal user',

        'default_language' => 'EN US', // Default language for creating new users

        'default_organization' => 2, // ID of the default organization for creating new contacts
);
// End of configuration
////////////////////////////////////////////////////////////////////////////////
```

Where:

- '**ldap_query'** defines the LDAP query to be used to retrieve the list of users from the Active Directory. It is possible to use this query to limit the list of users to the members of a particular AD group (in our example the group named 'iTop Users'). You can of course use this query to limit the export at will: only active users, only users of a specific organization, etc...
- '**login'** defines which field of the Active Directory has to be used as the 'login' for the iTop user. Make sure that this setting is consistent with the configuration of the LDAP authentication, as explained in #Configuring iTop to use Active Directory Authentication.
- '**profiles_mapping'** defines the mapping between the Active Directory groups membership and the iTop profiles. For example if the Active Directory account is a member of the group 'Administrators' then it will be assigned the profile 'Administrator' (notice there is no 's' at the end) in iTop. Caution: the name of the iTop profiles are case sensitive, and must be spelled exactly as in iTop.
- '**default_profile'** if a user is a member of none of the 'mapped' groups, it would end-up with no profile at all in iTop. Which is not allowed (the account creation would fail). In this case the script will assign the 'default_profile' to this user. Caution: the profile 'User portal' (lowercase 'p') has precedence over all other profiles in iTop.

running the script

The script can be run only by an iTop administrator.

When your configuration is done, run the script either by pointing your web browser to it (http://your_itop_server/webservices/AD_import_accounts.php) or by using the following command line:

```
cd \Inetpub\wwwroot\itop\webservices
php.exe -q AD_import_accounts.php --auth_user=<iTop_admin_user> --auth_pwd=<iTop_admin_pwd>
```

By default the script runs in simulation mode (i.e no change is made in the iTop database).

Check the output, and once everything looks fine, run the script for real by passing it the flag "simulation=0" e.g.: http://your_itop_server/itop/webservices/AD_import_accounts.php?simulation=0

or (using the command line):

```
cd \Inetpub\wwwroot\itop\webservices
php.exe -q AD_import_accounts.php --auth_user=<iTop_admin_user> --auth_pwd=<iTop_admin_pwd> --sim
```

Note

The command line examples above are given for iTop running on Windows/IIS, but the synchronization script car run as well if iTop is installed on a Unix/Linux/Mac system, as long as the LDAP connection to the Active Directory server is available.

Similarly the synchronization script can be tailored to synchronize iTop with any LDAP server, not only Active Directory, but in this case, the LDAP queries must be tailored to the LDAP appropriate schema.

Retrieved from "http://sourceforge.net/apps/mediawiki/itop/index.php?title=Active_Directory_Integration"

- This page was last modified on 19 February 2011, at 09:01.

© 2013 SourceForge. All Rights Reserved. SourceForge is a Dice Holdings, Inc. company Terms of Use - Privacy Policy - Cookies/Opt Out