# Your Challenge: Configuring F-Response Universal to use Active Directory Authentication

*Note: This guide assumes you have an active F-Response Universal™ instance and that you have network access to this instance. In addition this guide recommends certain 3rd party applications to obtain LDAP/AD configuration details, Internet access will be required to download and install these applications.*

## Step 1: Determine the overall complexity of your LDAP/Active Directory environment

It's important to have a good understanding of your domain environment and where your examiners are located prior to beginning the LDAP/Active Directory configuration process. At a minimum you will need to know the following:

**What domain are my examiners in? Are they all in the same domain or are they in different domains?**

In short, if you have examiners who login to the Active Directory network using different domains, i.e. CHICAGO, TAMPA, etc. then you will need to use the "alternative ldap servers" configuration settings. If all users login to the same domain take a big sigh of relief, as your configuration should be shorter.

**Is there a single-level group I can have my examiners added to?**

In other words, examiner user accounts will need to be directly added to a security group, at this time F-Response Universal does not support nested group memberships.

## Step 2: Determine your local Domain Controller

Unless you are lucky enough to know your domain controller hostname or IP address by heart you will need to determine that information now. You may have the appropriate value provided by your network administration team, however if not you can always determine your Primary Domain Controller (PDC) using the following command line.

```
C:\netdom query /d:<YOURDOMAIN> PDC
```

This should return the Primary Domain Controller for your user account and gives you the first step toward determining your LDAP configuration.

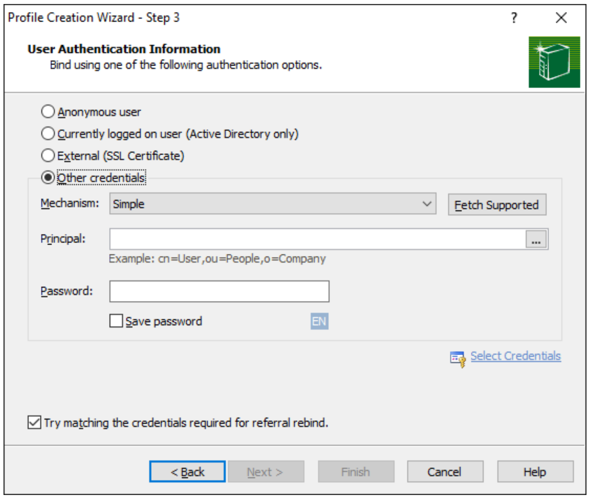
## Step 3: Download and install Softerrra Ldap Browser

In order to get a good feel for the LDAP/Active Directory environment and to confirm your settings as you collect them we recommend installing a simple freeware LDAP Browser. For this task we have found Softerra LDAP Browser to be an excellent application. You'll find the application at http://www.ldapbrowser.com/download.htm .

## Step 4: Use Softerra LDAP Browser to obtain F-Response Universal LDAP Configuration details (Simplified)

After installing Softerra LDAP Browser you will want to open the application and create a new profile. You'll use the afore determined Primary Domain Controller or PDC as your LDAP Server. The port and ssl options may be provided to you, however if not, you may have to experiment with both. The standard non-ssl port for LDAP is 389, the standard ssl port is 636.

When prompted for authentication, use the <YOURDOMAIN>\<YOURUSERNAME> format for the Principal value, and of course your password.



Profile Creation Wizard - Step 3

**User Authentication Information**
Bind using one of the following authentication options.

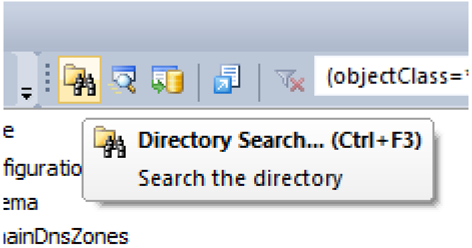
○ Anonymous user
○ Currently logged on user (Active Directory only)
○ External (SSL Certificate)
● Other credentials

Mechanism: Simple
Principal:
Example: cn=User,ou=People,o=Company
Password:
□ Save password

☑ Try matching the credentials required for referral rebind.

After successfully logging into the LDAP Server you will need to locate the defaultNamingContext for your LDAP Server. Typically, this is the "ldap_dn" for your F-Response Universal configuration. Copy this value to a notepad instance for the future.

Next we will need to use the Directory Search feature to locate an examiner account and make sure that account is a member of the group that controls access to F-Response Universal.



When you open the Directory Search dialog you will need to start by populating the Search DN. Think of this as the overall set of records you wish to search through. In this case we need to use the defaultNamingContext from above. Next, for the filter we need to locate a single user account. The fastest way to do this is the use the following filter syntax:

```
(sAMAccountName=<YOURUSERNAME>)
```

```
Ex. (sAMAccountName=joeuser)
```

After locating the user account in question you will want to double click on that account to retrieve all the details for that user. Specifically, we are focused on the "memberOf" values. You'll want to locate the "memberOf" entry matching the previously defined Security Group that you have designated to control access to F-Response Universal.

Once you locate that value it's time to do some basic subtraction. You will need to remove from that string value the "defaultNamingContext" or "ldap_dn" you located earlier. Let's try an example.

```
memberOf = CN=univ_users,CN=Users,DC=tampa,DC=abcompany,DC=com
```

```
defaultNamingContext = DC=tampa,DC=abcompanny,DC=com
```

Resulting "group_dn":

```
CN=univ_users,CN=Users
```

## Step 5: Configure the F-Response Universal Application with the newly gained information

Armed with the following information we are ready to get onto the F-Response Universal Appliance and configure it for LDAP/Active Directory Authentication.

ldap_server -> Provided by Step 2 and netdom query

ldap_port -> Determined in Step 4 using Softerra LDAP Browser

ldap_ssl -> Same as above.

ldap_dn -> Provided in Step 4 from the defaultNamingContext.

ldap_group -> Calculated in Step 4 from the memberOf value and the defaultNamingContext.

You must now add this information to the F-Response Universal configuration file. In order to do this you must have shell access to the appliance (either via SSH or through the terminal) and be proficient in a text editor. Both the "vi" and "nano" editors are available on the appliance for your use. Novice users should use "nano". The configuration file that must be edited is "/etc/fswitch/fswitch.cfg"

Using the following example values we will indicate what must be set in the configuration file.

**Domain Controller (PDC) ->** **`pdc.abcompany.com`**

**LDAP Port ->** **`636`**

**LDAP SSL ->** **`Yes`**

**LDAP Group ->** **`CN=univ_users,CN=Users`**

**LDAP DN ->** **`DC=tampa,DC=abcompanny,DC=com`**

How the configuration file should look:

```
{ldap_server,"pdc.abcompany.com"}.

{ldap_group,"CN=univ_users,CN=Users"}.

{ldap_dn,"DC=tampa,DC=sbcompany,DC=com"}.

{ldap_ssl,true}.

{ldap_port,636}.

{authtype,ldap}.
```

After completing your changes to the configuration file you'll want to save and exit the text editor and restart the F-Response Universal Appliance software using the following command.

```
service fswitchbasic restart
```

## Step 5b: Handling complex domain configurations

Up to this point we have only had to deal with LDAP/AD Configurations that encompass a single domain. In many organizations this level of simplification is not possible. For these instances we have developed an alternate LDAP configuration.

This configuration allows you the setup separate settings for each Windows Domain you need to support. In fact, if you look closely you'll see the configuration process uses all the same pieces of information as the simplified process, however it does this for each configured domain.

Let's take the prior example and add a second domain, so you now have both the "Tampa" and "Chicago" domains at abcompany.com, each with a univ_users group and each with a different defaultNamingContext or ldap_dn.

**Tampa (ex. TAMPA\jilluser)**

**Domain Controller (PDC) ->** `tampa.abcompany.com`

**LDAP Port ->** `636`

**LDAP SSL ->** `Yes`

**LDAP Group ->** `CN=univ_users,CN=Users`

**LDAP DN ->** `DC=tampa,DC=abcompanny,DC=com`

**Chicago (ex. CHICAGO\joeuser)**

**Domain Controller (PDC) ->** `chicago.abcompany.com`

**LDAP Port ->** `636`

**LDAP SSL ->** `Yes`

**LDAP Group ->** `CN=univ_users,CN=Users`

**LDAP DN ->** `DC=chicago,DC=abcompanny,DC=com`

**Important note, in order to properly configure multiple domains, each domain must have a predefined security group to place user accounts in. They do NOT need to be the same name.*

How the configuration file should look:

```
{ldap_alternate_servers,[{"tampa",[{server,"tampa.abcompany.com"},{port,636},{ssl,true
},{ldap_dn,"DC=tampa,DC=abcompany,DC=com"},{ldap_group,"CN=univ_users,CN=Users"}]},{"c
hicago",[{server,"chicago.abcompany.com"},{port,636},{ssl,true},{ldap_dn,"DC=chicago,D
C=abcompany,DC=com"},{ldap_group,"CN=univ_users,CN=Users"}]}]}.

{authtype,ldap}.
```

After completing your changes to the configuration file you'll want to save and exit the text editor and restart the F-Response Universal Appliance software using the following command.

```
service fswitchbasic restart
```

## Step 6: Testing your configuration

The F-Response Universal Appliance contains a command line tool for testing your LDAP configuration. Simply use the following syntax to determine if you configuration is correct before attempting to use the F-Response Universal Console.

```
/usr/sbin/fswitchadm testldap --username=”YOURUSERNAME” --password=”YOURPASSWORD” --domain=”YOURDOMAIN”
```

The tool will then walk through each step attempting to connect, bind, locate the user account, and determine if the user is a member of that group.

## Troubleshooting

Sadly LDAP configuration can be quite challenging and there really isn’t a one size fits all solution to troubleshooting issues that might arise. As such we recommend you reach out to F-Response Sales and Support and request assistance if you run into difficulties beyond what is covered in this document. Our engineers are happy to help and will most likely ask to join you on a GoToMeeting troubleshooting session to walk through the issue you are having. If possible, please take the time to create a generic user account “univtest” or the like as the F-Response engineer will see that account’s password during the testing process.