

## Title

Setting up basic authentication to an Active Directory Server

## Summary

This article explains how to set up a Mac OS X client machine to authenticate against an Active Directory Server without implementing any schema extensions to the AD server.

## Discussion

First you will need to get the following information from your Network Administrator:

- The address of your active directory server and its search base suffix
- The search base they would like you to use to access user records
- A fully qualified distinguished name and password that has read access to the user records of your domain. Often AD administrators have a generic user account created solely for this purpose.
- The name of the attribute fields in the AD that hold:
  - RecordName (this is the short name, for example, "mjones")
  - RealName (this is the full name, for example, "Mary Jones")
  - UniqueID (this is an integer value unique to each user)
- It may also be helpful to have a printout of any user's AD record.
- Whether you will need to access the global catalog or use SSL encryption, and, if so, the custom port required

Configure Directory Services to look to the AD server for authentication information

1. Open the Directory Access application located in the Utilities folder.
2. Click on "LDAPv3" and click on "Configure". You may need to click on the lock in the lower left corner first to allow changes.
3. Uncheck the "Use DHCP supplied LDAP server" checkbox and click on the disclosure triangle next to "Show Options".
4. Create a new configuration by clicking on the "New..." button and provide the appropriate information, for example:
  - name: Active Directory
  - server name: ad.apple.com
  - LDAP mappings: Active Directory
  - Search base suffix: dc=apple,dc=com
5. Click on the "Edit..." button to edit the configuration
6. Set the timeouts to 10 seconds each
7. Click on the check box to use authentication and provide the distinguished name and password that you obtained from your Network Administrator. For example,
  - Distinguished Name: cn=apple test,cn=users,dc=apple,dc=com

Password: testapple

8. If you require access to the global catalog or SSL support, check the appropriate boxes and indicate the custom port required.

### Configure Search and Mappings

1. Click on the "Search & Mappings" tab
2. In the "Record Types and Attributes" table, click on the "Groups" item then click on the "Delete" button. Do this for the "Mounts" item as well.
3. Click on the "Users" item (not the disclosure triangle). The assumed search base will be filled in for you. Verify that this matches the search base for user records recommended by your Network Administrator. An example value is "cn=Users,dc=apple,dc=edu". "organizationalPerson" and "user" should appear in the column to the right.
4. Click on the disclosure triangle next to Users. Now we'll set the mappings for each user attribute to correspond to the appropriate field on the AD server. If the field does not exist on the AD server, we will assign a static value by using the "#" symbol. To change the value of the field that an attribute is mapped to, click on the attribute (in the left column), then double-click on the value in the right column. Additional "Map to" values can be removed. The following are examples of valid entries:
  - RecordName: sAMAccountName
  - UniqueID: uSNCreated
  - RealName: displayName
  - Password:
  - PrimaryGroupID: #20
  - NFSHomeDirectory: #/Users/default
5. Delete the HomeDirectory, EMailAddress, PhoneNumber, and Comment attributes under "Users".
6. Click on OK to save the custom settings for the Active Directory configuration, then click on OK to save the configuration in the LDAPv3 settings panel. Provide a local administrator's username and password if prompted.
7. Click on the Authentication tab.
8. Select "Custom Path" from the Search popup button.
9. Click on the "Add..." button, choose the LDAPv3 configuration you just created and click on the Add button.
10. Repeat the last two steps for the Contacts tab.
11. Click on the Apply button and quit Directory Access.
12. If SSL encryption is required and your AD server is using a self-signed certificate, you will need to follow the instructions in Kbase article number 107178 before proceeding.

## Create a default home directory for AD users

1. Launch the Terminal application. You will copy a user home directory template to the Users directory and allow anyone to read/write to that directory:

```
% sudo ditto /System/Library/User\ Template/English.lproj /Users/default
% sudo chmod -R a+rwX /Users/default
```

2. It is recommended that you implement a login hook to set the ownership of the default user directory to the user logging in and to refresh the default user home directory to a pristine state. You can also use this opportunity to customize the environment a user encounters when logging in. (Need another Kbase article for this)

## Verify that you can obtain user information from the Active Directory

1. Restart the computer.
2. When the computer boots up, log in as a local admin user
3. Launch the Terminal application
4. Type "lookupd -d" and hit return. At the new prompt, type:

```
userWithName appletest
```

Replacing "appletest" with the RecordName of a user you know to exist in the Active Directory. This should return a list with attributes mapped to the appropriate fields.

Example:

```
[demo:~] apple% lookupd -d
lookupd version 272 (root 2002.07.27 09:40:39 UTC)
Enter command name, "help", or "quit" to exit
> userWithName: appletest
Dictionary: "DS: user appletest"
_lookup_agent: DSAgent
_lookup_validation: 1036726157
home: /Users/default
gid: 20
name: appletest
passwd: *****
uid: 13945539
+ Category: user
+ Time to live: 43200
+ Age: 0 (expires in 43200 seconds)
+ Negative: No
+ Cache hits: 0
+ Retain count: 3
```

Next confirm that you can perform lookups by id:

```
> userWithNumber: 13945539
Dictionary: "DS: user appletest"
_lookup_agent: DSAgent
_lookup_validation: 1036726157
home: /Users/default
gid: 20
mail: appletest@apple.com
name: appletest
passwd: *****
uid: 13945539
+ Category: user
+ Time to live: 43200
+ Age: 0 (expires in 43200 seconds)
+ Negative: No
+ Cache hits: 0
+ Retain count: 3
```

You should now be able to authenticate to the machine as any AD user.