# MSAD Login V2

A Windows login process for Mac OS X

## User manual

## About MSAD Login

MSAD Login is a system that connects a Macintosh OS X machine to a Windows server running Active Directory.

This way of connecting to a Windows server allows OS X users to mount their home drive and get notifications when passwords are about to expire. This method of login is very different from the specified method documented by Apple in that accounts are not tied to the server, this means that when the computer is not connected to the network it can still be logged into, which is of particular use for PowerBooks or computers connected over the internet.

This method of logging in and mounting shares has a major benefit over using the 'Connect to server' method, as it will not lock your account if you use an incorrect password. You will also be told if your account has expired or has been locked out, something that is lacking (even in 10.4 and 10.5) when using Apple's 'Connect to server' method.

The way that MSAD Login connects to the server has other benefits, such as the fact that no changes are needed in the Active Directory schema (the database used to hold Windows user accounts).

The login procedure also allows passwords to be changed on both the server and the Macintosh.

One of the benefits of this system is that it checks with the Windows server to see if a password is about to expire, and warns up to 14 days before it actually expires.

For the latest news and information about MSAD Login, visit the website at http://www.pa-software.com/products/

## Minimum System Requirements

- Any G3 system
- Mac OS X version 10.2 or later
- 128 megabytes (MB) of random access memory (RAM)
- Microsoft Windows 2000 / 2003 server running Active Directory (AD)

To make sure you have the latest version of Mac OS X, choose System Preferences from the Apple menu, and then click Software Update. Click Update Now to retrieve updates for your system.

# Installation

### Installing and using MSAD Login

To install, mount the MSAD Login disk image and run the MSADLoginPro.pkg or for 10.4 or higher or Intel based Macintosh use MSADLoginProUB.pkg.

Note: If you have previously installed MSAD Login, then running MSAD Login installer will replace your previous installation.

If you receive a message that you do not have sufficient privileges to install this software, you will need to ask the current administrator of the machine to install the software. The administrator's name is shown in the User pane or Accounts of System Preferences depending on the version of OS X you are running. For more information, see Mac help, available in the Help menu.

# Setting up MSAD Login

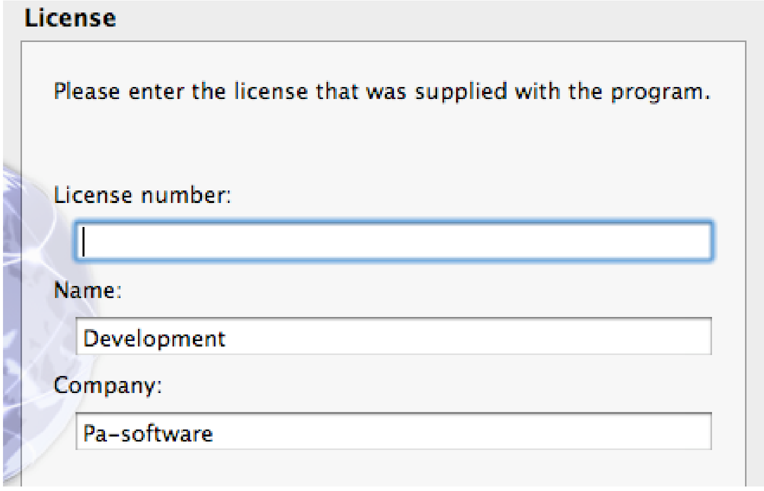
After installation the option is given to enter the network details using the Setup Assistant.

Note: If you need to change any of the network details given when MSAD Login was installed, then running 'Setup Assistant' (which is found in '/Applications/MSAD Login Setup Assistant') will allow you to enter your network settings or change your existing settings. It also allows you to add the login process to users after the installation.

## Running the Setup Assistant to enter the network settings

### *1. License*

This page allows you to enter your license (unless you are running the demo) and administrative details.
Note: The license is not case sensitive and must be in the format XXXX-XXXX-XXXX-XXXX-XXXX.



License

Please enter the license that was supplied with the program.

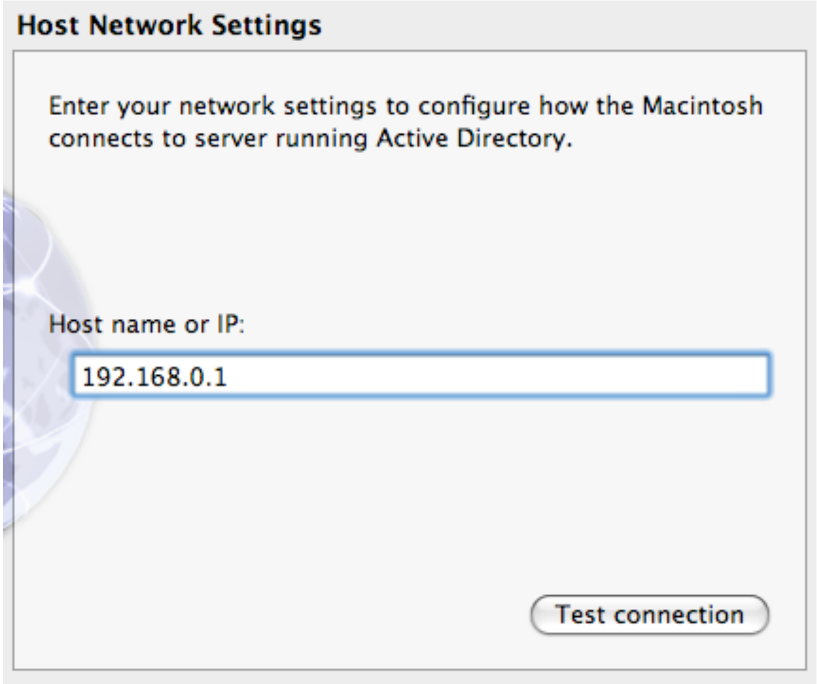
License number:

Name: Development

Company: Pa-software

### *2. Host Network Settings*

This page requires the host name or IP address of your Windows Active Directory server.
Note: To ensure no DNS issues occur it is recommended that an IP address is used, instead of a host name.



Host Network Settings

Enter your network settings to configure how the Macintosh connects to server running Active Directory.

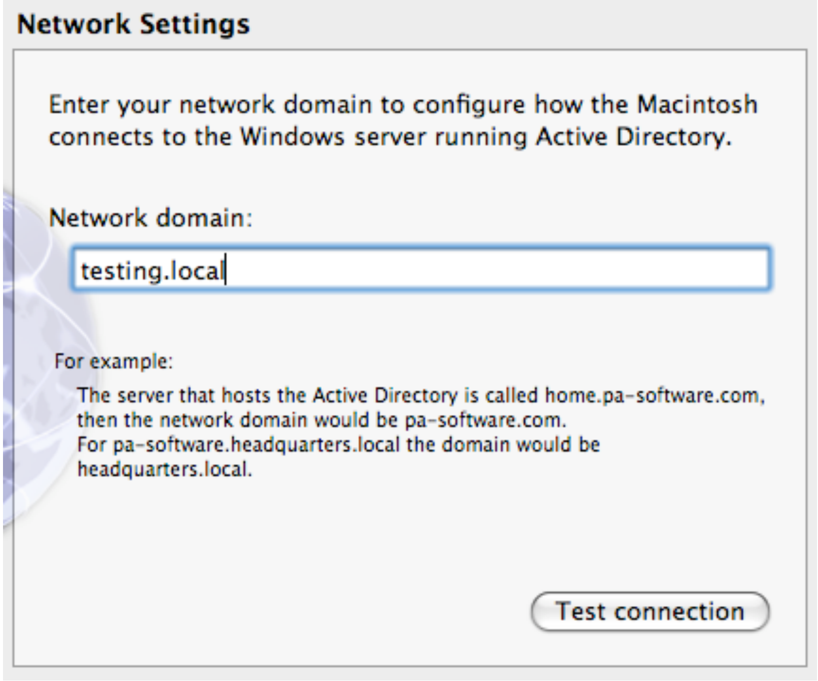
Host name or IP: 192.168.0.1

Click on ‘Test connection’, to ensure that the Mac OS X client can connect to the Windows Active Directory host server without any errors.

## 3. Network Settings

This page is where the Windows Active Directory server is checked to ensure that there are no network or permission errors when looking up the account details.

Note: It is recommended that a network administrator performs this check as the connection may require an administrator account to perform the check.



Network Settings

Enter your network domain to configure how the Macintosh connects to the Windows server running Active Directory.

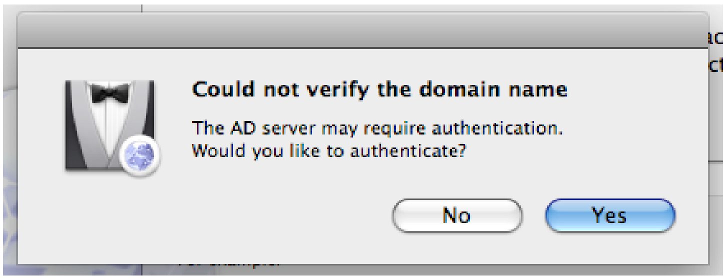
Network domain: testing.local

For example:
The server that hosts the Active Directory is called home.pa-software.com, then the network domain would be pa-software.com.
For pa-software.headquarters.local the domain would be headquarters.local.

In the network domain, enter your domain name, e.g. for a server with the

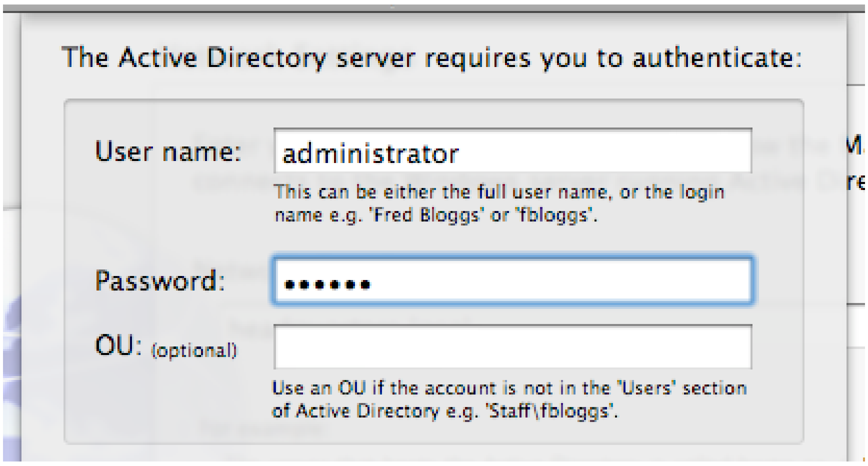
fully qualified name of server1.testing.local, the domain name would be testing.local.
Once entered, click test connection to check the server can be contacted and that the required details can be returned.

Note: It is common to get the error ‘Could not verify the domain name’ when testing the connection, as most Active Directory servers require a user name and password to perform the test. Click OK and on the next page enter a user name and password (and OU if used) for an account on the Active Directory server, then click OK to test the connection again.



**Could not verify the domain name**

The AD server may require authentication.
Would you like to authenticate?



The Active Directory server requires you to authenticate:

User name: administrator
This can be either the full user name, or the login name e.g. 'Fred Bloggs' or 'fbloggs'.

Password: ••••••

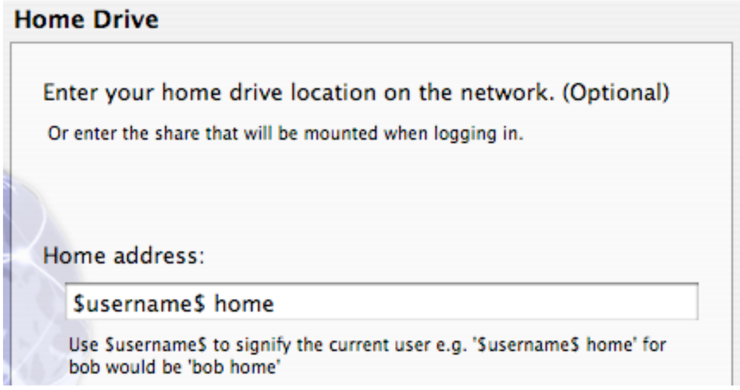
OU: (optional)
Use an OU if the account is not in the 'Users' section of Active Directory e.g. 'Staff\fbloggs'.

If you still get connection errors after entering a user name and password, see the troubleshooting section at the end of this guide

### 4. Home Drive (optional)

This page is where can optionally enter a share to be mounted when the user logs in.
This is either a shared volume on the server or a generic users volume e.g. the volume 'smb:\\server1.testing.local\shared' (where server1 is the name of the server) would be entered as 'shared', or for a generic user volume e.g. "smb:\\server1.testing.local\<a users login name> home' would be entered as '$username$ home', where when logging in the $username$ would be replace with the current users account login name as held on the Windows Active Directory server.

Note: As Samba currently cannot mount folders inside volumes (such as '/home/$username$/My documents'), it is suggested that either you enter only volume name.



Home Drive

Enter your home drive location on the network. (Optional)

Or enter the share that will be mounted when logging in.

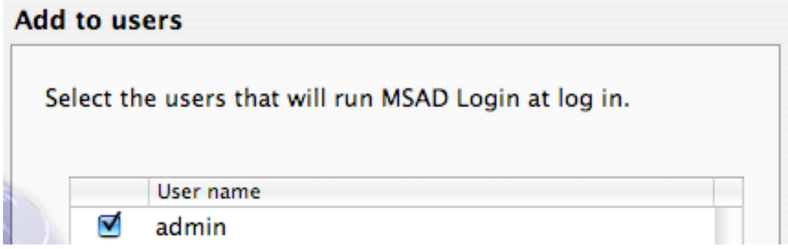
Home address: $username$ home

Use $username$ to signify the current user e.g. '$username$ home' for bob would be 'bob home'

### *5. Add To Users*

This page allows you the option of adding the login process to selected users only. This option can also be used afterwards when running the Setup Assistant to add the login system to other or new users.

Note: Un-checking a user does not mean it will remove the login process if it is already present. To do this you must use the 'Login items' or 'Startup items' depending on the operating system you are using.



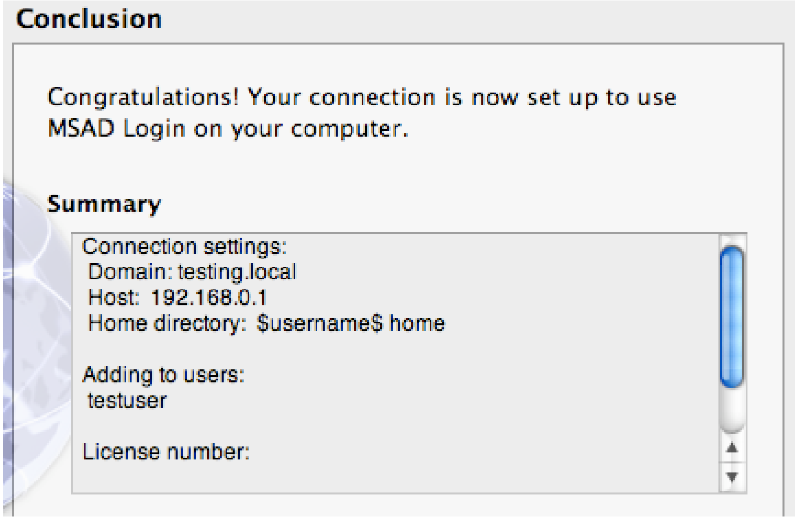
Add to users

Select the users that will run MSAD Login at log in.

| | User name |
|---|---|
| ☑ | admin |

### *6. Conclusion*

This page gives a summary of the settings you have chosen before they are saved, giving the opportunity to go back and make alterations.



Conclusion

Congratulations! Your connection is now set up to use MSAD Login on your computer.

Summary

```
Connection settings:
 Domain: testing.local
 Host:  192.168.0.1
 Home directory:  $username$ home

Adding to users:
 testuser

License number:
```

### *7. Finishing*

Once the settings have been successfully saved, you are given the option to run the login system. If you click OK you will then be directed to the user based Setup Assistant ready to configure your access to the Active Directory server (see *Running MSAD Login for the first time* for more details).

# Running MSAD Login for the first time

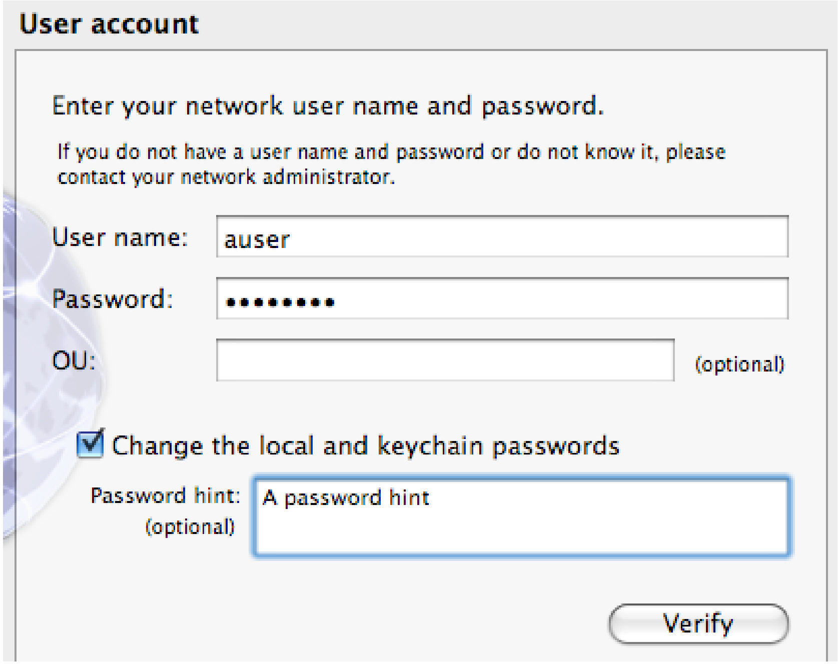
### Setting up the network password

The Windows Active Directory network password is stored in the default keychain and must be entered the first time the application is run.
This is done when you run the Setup Assistant in user mode (this is performed automatically the first time you login or straight after the network set up has finished).

1. *User Account*

   The user account requires the user name, password and optional OU of the account on the Active Directory server. Once entered you can ensure the details are correct by clicking on the Verify button.

   Note: If there are any problems they will be displayed in the log created by the verification process.



User account

Enter your network user name and password.

If you do not have a user name and password or do not know it, please contact your network administrator.

User name: auser

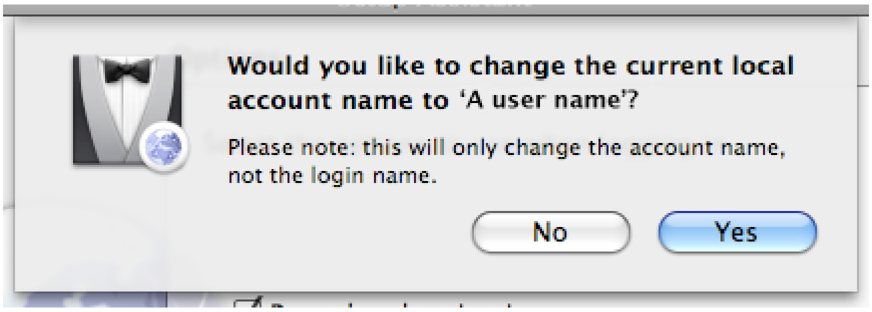
Password: ••••••••

OU: (optional)

☑ Change the local and keychain passwords

Password hint: (optional) A password hint

When creating the network password keychain item, you also have the option to change the current local password for both the local account and the default keychain.
This is performed by checking the ‘Change the local and keychain passwords’ checkbox.
This option also allows you to change the local account name to reflect the name used for your account on the server.



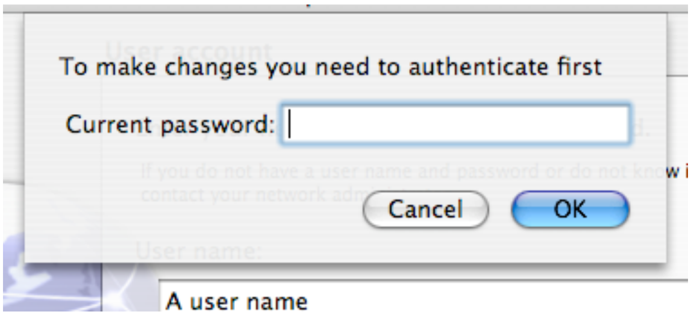
**Would you like to change the current local account name to 'A user name'?**

Please note: this will only change the account name, not the login name.

Note: If you are changing the local and default keychain password, then you will need to authenticate with the current local password.

## 2. Authenticating (to change the local password)

Before the Macintosh password can be changed, you will need to authenticate using your current Macintosh password (not you network account password).



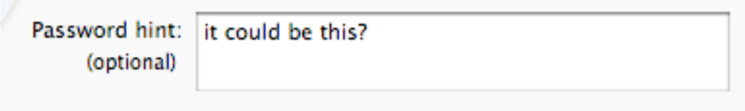
To make changes you need to authenticate first

Current password:

A user name

After authentication the application will store the password in the default keychain and use the key in the keychain to log into the Windows network each time you log into the Macintosh.

As an option, the local password hint can also be set or changed (this is only held locally as Windows does not have this feature without editing the Active Directory schema which is beyond the scope of this user guide).

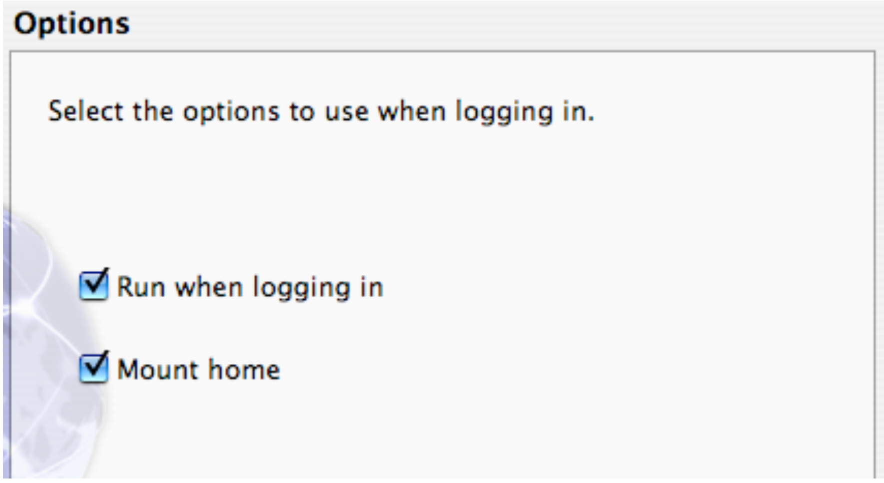


Password hint: (optional) it could be this?

Note: It is recommended that a hint is entered if more than one computer is used to connect to the Windows Active Directory account (this can only be set if the local password is changed).

## 3. Options

The options allow you to change the way MSAD Login runs on a user basis.



**Options**

Select the options to use when logging in.

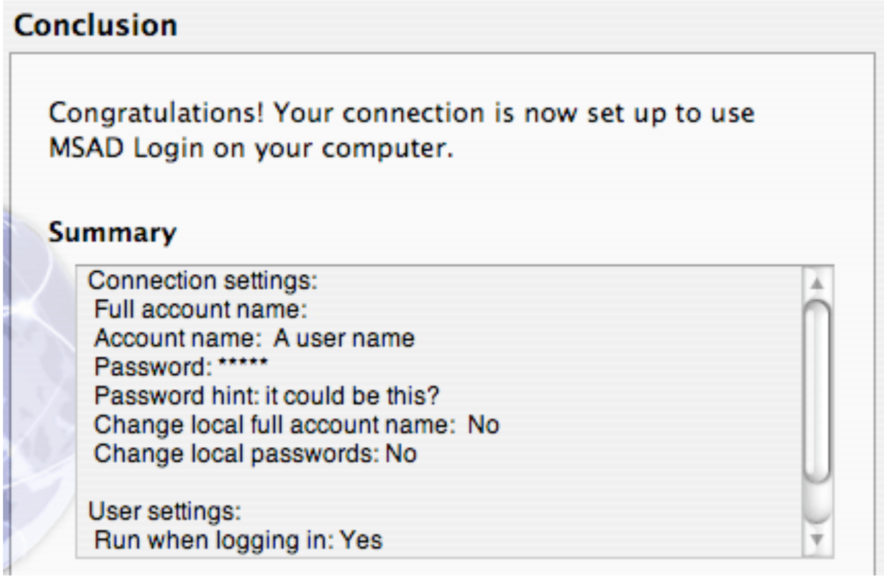
☑ Run when logging in

☑ Mount home

The first option controls if MSAD Login is started when you log into your Macintosh.
The second option allows a home share to be mounted when you log into your Macintosh.

### *4. Conclusion*

This page gives a summary of the settings you have chosen before they are saved, giving the opportunity to go back and make alterations.



**Conclusion**

Congratulations! Your connection is now set up to use MSAD Login on your computer.

**Summary**

```
Connection settings:
 Full account name:
 Account name:  A user name
 Password: *****
 Password hint: it could be this?
 Change local full account name:  No
 Change local passwords: No

User settings:
 Run when logging in: Yes
```

# Uninstalling MSAD Login

To remove MSAD Login from your system:

1. To remove MSAD Login, just put the folder 'Library/Application Support/Pa-software/MSAD Login' in the trash and delete the file 'MSAD Login.prefPane' in the folder 'Library/PreferencePanes/'.
2. You also need to remove the 'MSAD Login Setup Assistant.app' from '/Applications/Utilities/'.
3. If you have chosen to run MSAD Login at login, you should also remove MSAD Login from your login items in the accounts system preference.

For complete removal, delete the key ‘MSAD network password’ in the default keychain.

# Troubleshooting

## *Connection problems*

Connecting to the Windows server to validate the account requires that the port 389 is open and available.

If you are connecting to a Windows 2003 server, by default the network communications are encrypted which currently are not supported. To use the standard SMB communications, you will need to change the server's domain group policy (or get your network administrator to make the changes):
In the Active Directory Users and Computers, right-click on the domain icon and select Properties.
In the Properties window, select the Group Policy tab, select the Default Group Policy and click on Edit.
In the Policy Editor, navigate to Computer Configuration->Windows Settings->Local Polices->Security Options, find the entry Digitally sign communications and disable.

By default the network firewall is turned off on a Macintosh running OS X 10.3 or higher. If the firewall has been turned on, then it must be set to allow Windows sharing.
For 10.4 or higher, if the connection still fails, try un-checking the 'Enable stealth mode' option under the advanced firewall settings.
The firewall can be found in the sharing section of the system preferences.

## *Setup assistant issues*

If testing a connection under 'Network Settings' fails be sure that the account you are using has sufficient privileges and an OU is used if required e.g. if your account is not under the 'Users' section of Active Directory, then it would require an OU. Also, ensure that the correct domain name is used e.g. the server that hosts the Active Directory is called home.pa-software.com, then the network domain would be pa-software.com, for pa-software.server.local the domain would be server.local.

If there are still issues connecting, test the connection using Terminal by running the command (in one line):

```
ldapsearch -LLL -x -h 192.168.0.1 -D
"cn=administrator,cn=users,dc=testing,dc=local" -b
"dc=testing,dc=local" -W
```

Where 'administrator' is the full name of the account used, 192.168.0.1 is the IP address of your server, dc=testing and dc=local are the domain name of the Active Directory server e.g. for testing.local use dc=testing,dc=local.
Note: If the account is in an OU use ou=<name of ou> instead of cn=users.

## *Account errors*

The most common form of account error is when the network password is changed using a different computer. If this occurs, MSAD Login will show an authentication error and ask you if the password was changed using a different computer. If you select Yes, then you will need to enter your old password, and the new password (that was changed using the other computer).

If the account error is not due to changing the password on another computer and the network administrator has not reset the password, but you still receive authentication errors. There could be a problem with the password stored in your keychain. In this circumstance, you will need to delete the key 'MSAD network password' in your default keychain using Keychain Access which is found in `Applications:Utilities`.
Once the key is deleted, log out and log back in, you will then be presented with the Setup Assistant in order to create a new network key. For this you will need the password you used to log into your Macintosh and the password for you account on the Windows server.

Updated August 2009