

# Active Directory Integrated Home Directories

## Overview

This document explains how to configure home directories in Active Directory and how to configure the Mac OS X client to use use them. The instructions are divided into the following areas.

- Setting up the folder hierarchy on the Windows server with appropriate permissions.
- Configuring ExtremeZ-IP to host home directories.
- Adding the home directory path to the users' profiles.
- Binding the client computer to the domain using the Directory Setup application.

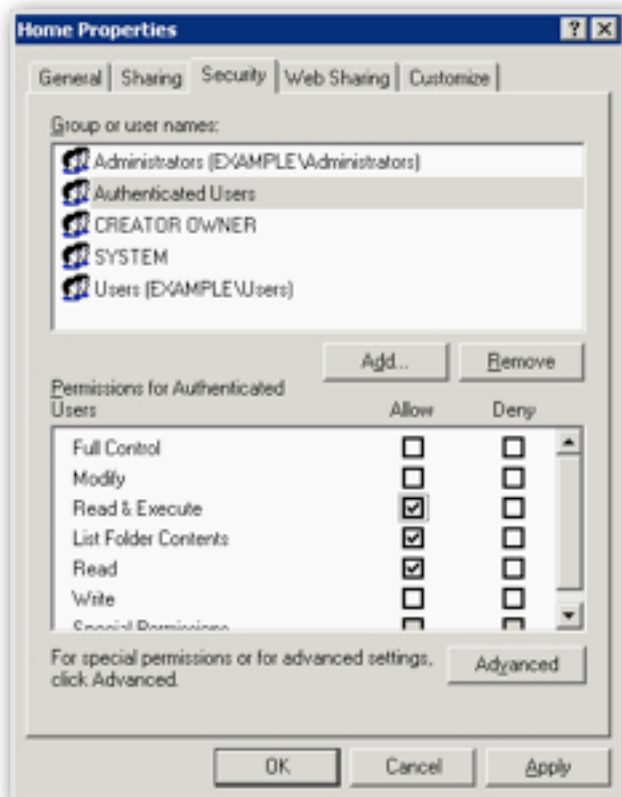
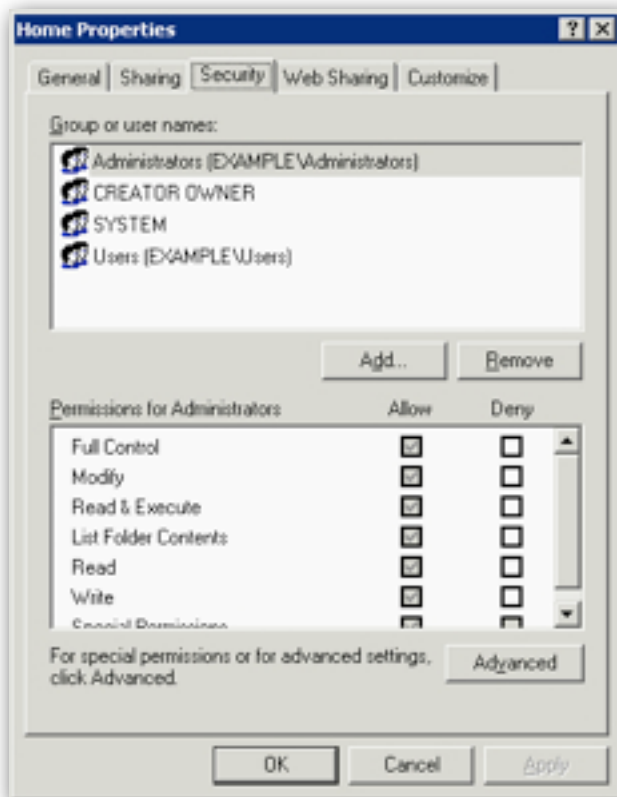
For best results you should be using the latest version of ExtremeZ-IP. A link to the latest version of ExtremeZ-IP can be obtained from Group Logic support or found on the [Latest Releases](#) page of the Group Logic website.

In addition to using the latest version of ExtremeZ-IP, it is important that you upgrade to at least the latest version of Mac OS X Tiger (10.4.11 as of this writing). The screenshots and steps below describe the process for configuring Mac OS X Tiger. The configuration for Max OS X Leopard are similar, though some of the names and GUIs of the utilities have changed. Apple has provided many fixes in each successive version of Mac OS X, that make the mounting of network home directories much more reliable.

## Creating Home Directories for Windows and Macintosh Computers

1. On the server where the home directories will be stored, create a folder to store your users home directories, for example, "H:/Home".
2. Right-click the folder and select Sharing and Security.

3. Grant the LOCAL administrators group (usually displayed as SERVERNAME\Administrators)"FULL CONTROL" (and thus the Domain Admins because they're automatically made a member of the LOCAL Administrators group when the server was joined to the domain).
4. Grant "Authenticated Users" the following permissions: Read & Execute, List Folder Contents and Read.
5. Click Advanced.
6. Apply permissions for "Authenticated Users" to "This folder only".
7. Uncheck "Allow inheritable permissions from parent to propagate to this object and all child objects. Include these with entries explicitly defined here."
8. Choose to copy the existing permissions.
9. Click Apply.
10. Close all of the Security Settings windows.
11. Share your home directory under both Windows sharing (SMB) and ExtremeZ-IP (AFP) and give "Everyone" full control permissions for Windows files sharing (permissions will be enforced through NTFS). It is very important that the paths for the SMB and AFP shares be identical.



# ExtremeZ-IP Home Directory Configuration

## Overview

This section describes the process for enabling the ExtremeZ-IP home directory support feature. This feature allows volumes to be designated as home directory volumes, presenting the user with a filtered view of the volume that shows only their assigned home directory folder.

When a volume is designated as a home directory volume, a user will only be given the option to mount the volume if it contains their individual home directory. When browsing that volume, the user will only see their home directory folder. All other folders on the volume will be hidden.

Client Macs that are configured to use an ExtremeZ-IP network based home directory will continue to function properly, regardless of whether the ExtremeZ-IP server's home directory support is enabled or disabled. If the server's home directory feature is disabled, the user will simply be presented with the entire contents of the volume rather than a filtered view.

## Home Directory Support Setup

To enable the home directory feature on your ExtremeZ-IP File Server, check the Enable Home Directory Support option, found in the Settings dialog of the ExtremeZ-IP Administrator. You will configure specific volumes on the server as home directory volumes in the next step. Additionally, you must choose the type of home directory support you would like:

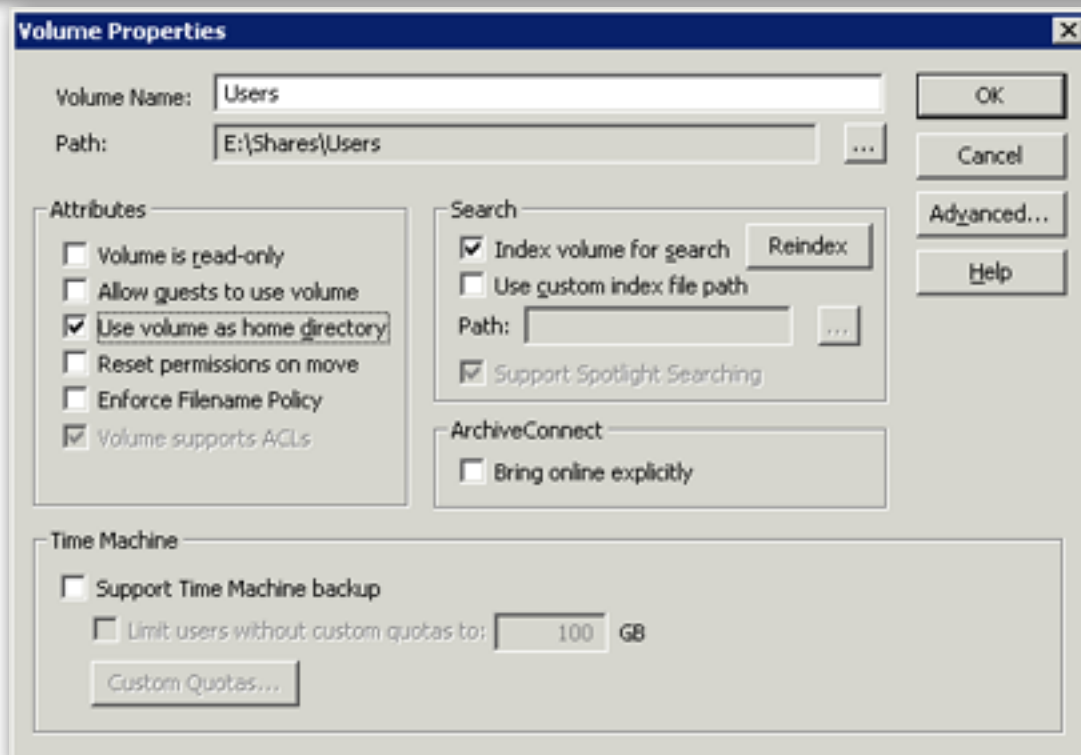
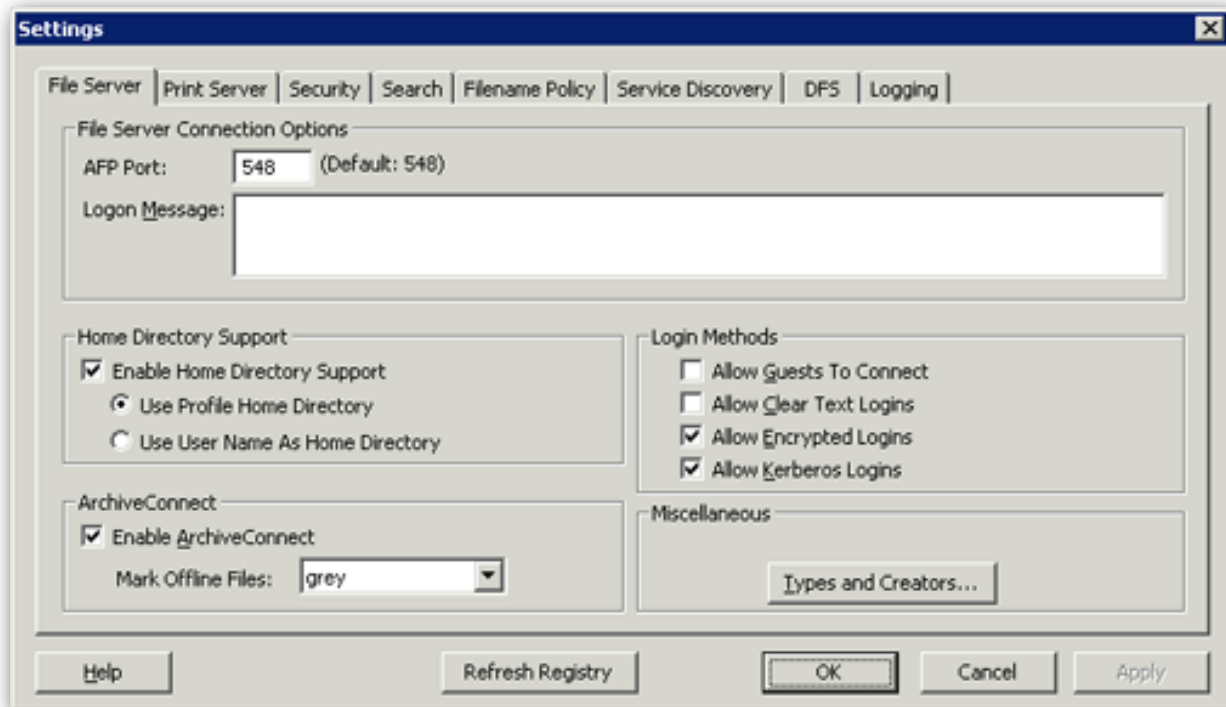
**Use Profile Home Directory** – This option assigns a user's home directory based on the Home folder path specified in their Active Directory account profile. The profile home directory option will use the path specified in the Connect option of the Home folder configuration, shown below. The drive letter assigned in the profile does not apply to Mac home directories.

**Use User Name as Home Directory** – If the volume being mounted is a home directory volume and contains a directory with a name matching the user's user name, that directory will be assigned as their home directory.

To configure an individual volume as a home directory, simply create a new volume or select an existing volume in the Volumes dialog of ExtremeZ-IP

Administrator and choose Modify. On the Volume Properties dialog, check the Use volume as home directory option.

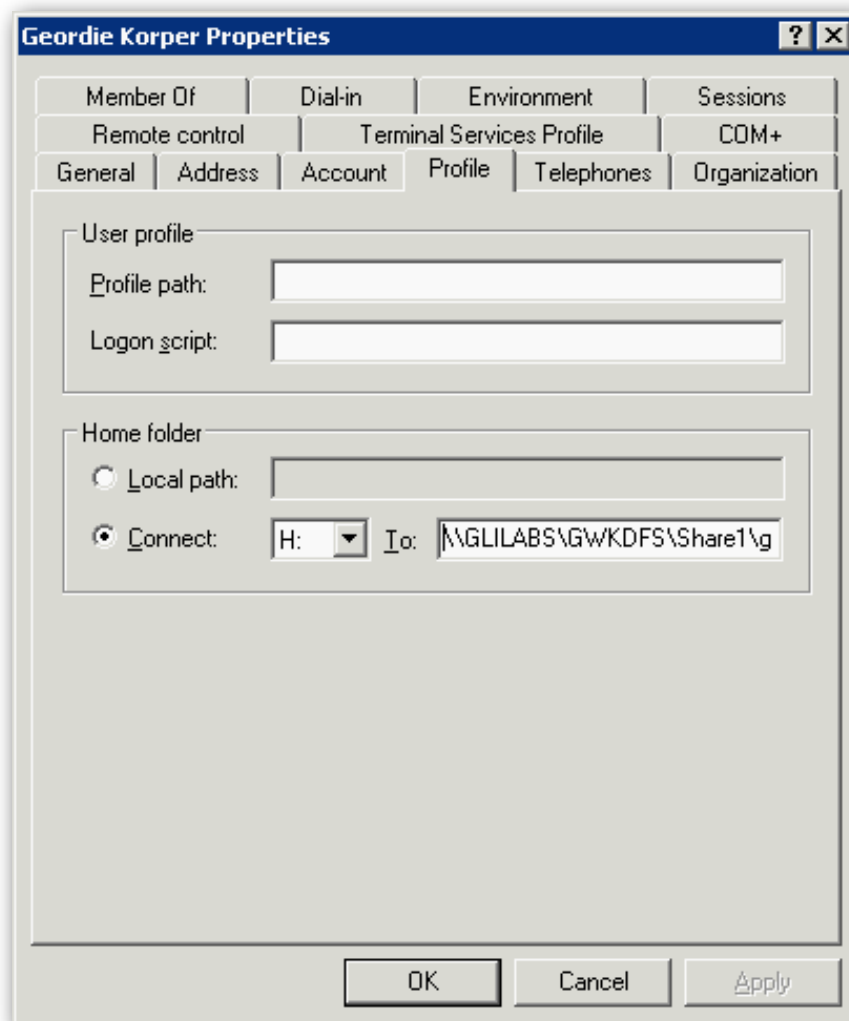
After completing these steps, home directory support will be active on your server.



## Assigning User Home Directories

The following step will create the home directory for the user. Because of the permissions set above users will have "Full control" over the newly created folder, and the Local Administrators group will have "Full control" through the inherited permissions. You then have a home directory that a user can do whatever they want with and local administrators can access/backup/restore copy files to.

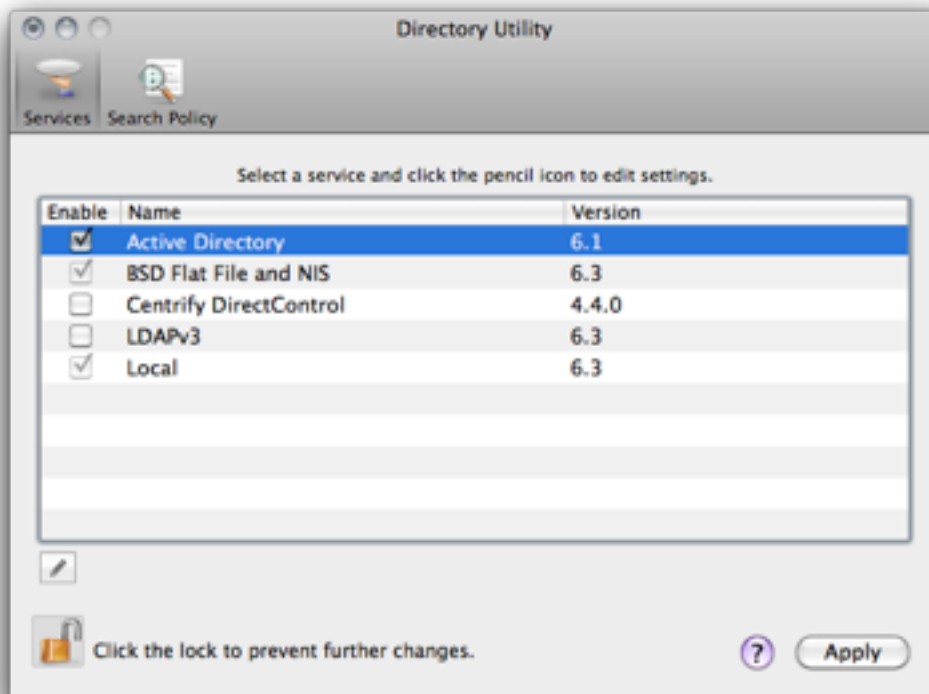
1. Open the Active Directory Users and Computers on the Domain Controller.
2. Add a user or select an existing user.
3. Go to the users PROFILE tab, click connect under the home folder, select a drive letter (H: is the most common) and type \\servername\home \username in the To: field.



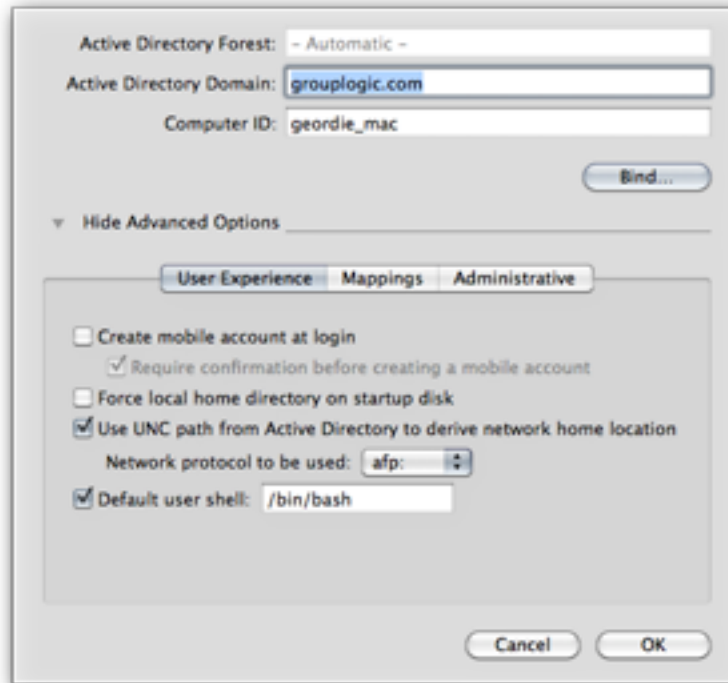
## Binding your Mac to Active Directory

Now that you have set up the home directory profile on the server you will now need to bind the Mac OS X clients to Active Directory. The steps below are for configuring Mac OS X Tiger.

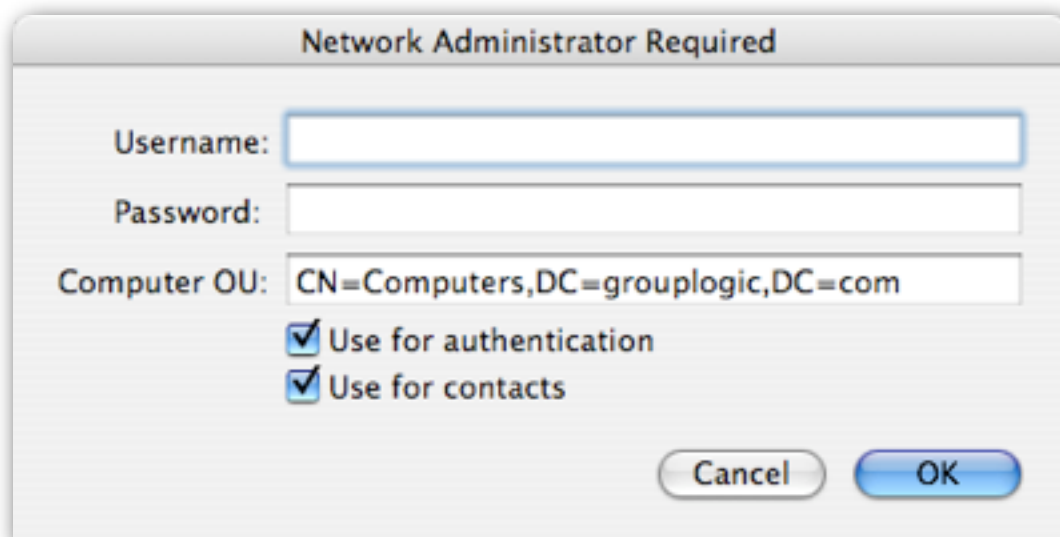
1. Launch the Directory Utility configuration tool, which you can find in `/SystemLibrary/CoreServices/`.
2. Authenticate to unlock Directory Utility, if needed.
3. Check the Active Directory checkbox and click Configure.



4. Enter your domain name in the Active Directory Domain field.
5. Enter the computer name in the Computer ID field.
6. Click the disclosure triangle to Show Advanced Options.



7. Verify that that Network protocol to be used is set to afp:.
8. Click the Bind button.
9. Provide a Domain user name and password. The pre-populated Computer OU settings should work, in most cases.



10. Click the OK button (if necessary Click OK to agree to Join existing account).
11. Click the OK button, Apply and close Directory Access configuration tool.
12. Restart the Macintosh client and login to it with an AD account.

Your Windows home directory should be now mounted automatically as a network drive.

## Verifying the Configuration

To verify that the configuration is correct, restart the client computer and login using an Active Directory account. If everything is configured correctly, the user's home directory will be mounted over the network, and the Mac will have copied the default set of Mac OS X user folders (Library, Documents, etc.) to the server. If you navigate up to the parent directory, you should only see the folder for the logged in user.

Because configuration is required on both the client and the server, there are many potential pitfalls in setting up Active Directory integrated home directories. The key is to verify that each individual component is working properly. If the parts work correctly they will work when correctly when combined.

To test that you can properly see the users' home folder from the Mac, you can manually connect to the file server and mount the HOME directory. To verify that the computer is properly bound to the Active Directory domain, you can use the 'dsconfigad -show' command. In Tiger (Mac OS X 10.4), you can check that the ActiveDirectory plug-in is properly getting the home directory from the user's profile with 'lookupd -q user -a name *username*' (replace username with the name of the user). In Leopard and above (Mac OS X 10.5), the 'lookupd' command has been replaced with 'dscacheutil', but the syntax is the same (dscacheutil -q user -a name *username*).