



APPLICATION NOTE

Centralized Mac Home Directories with ExtremeZ-IP

Published: July 2009

Abstract

Organizations wanting to integrate Mac OS X systems into their Windows-based enterprise network will most likely want to also centralize the storage of user home directories on a Windows server to ensure proper data security and backup policies are applied. While Mac OS X provides support for using SMB to access Windows shares, the native AFP protocol has many advantages for Mac OS X systems, and Group Logic's ExtremeZ-IP Server enables a Windows server to fully support AFP clients such as Mac OS X.

This application note describes how to configure both DirectControl and ExtremeZ-IP to enable users to log in to an OS X system with their Active Directory user ID and password to gain access to their home directory stored on a Windows server. The latest version of Extreme Z-IP provides integration with Windows Server's Distributed File System (DFS). This paper will also explain how to setup a Mac to support a DFS hosted home directory. The integration of Centrify DirectControl and ExtremeZ-IP combine to provide IT administrators the tools and services they need to fully integrate Mac OS X systems into both the centralized administration and management that Active Directory provides as well as the centralized network storage that Windows Server provides, further reducing the cost of managing OS X systems in a Windows-centric enterprise.

Contents

1	Introduction	2
2	Set Up the Windows Server and ExtremeZ-IP	3
3	Install and Configure Centrify DirectControl on the Mac	5
	3.1 Steps to Install Centrify DirectControl and Join the Active Directory Domain ..	6
	3.2 Configuring centrifydc.conf for Network Home Directories:.....	7
4	Testing the Solution	7
5	Using Centrify DirectControl with DFS	10
	5.1 Configure ExtremeZ-IP on the Windows Server to support DFS:	10
	5.2 ExtremeZ-IP DFS Configuration	12
	5.3 ExtremeZ-IP AFP Volume Creation	13
	5.4 Group Logic DFS Macintosh Software Installation.....	15
	5.5 Testing the Configuration	16
6	Summary	17
	6.1 For More Information.....	17
	6.2 Legal Notices	17

1 Introduction

A common question that all IT administrators consider when planning any desktop deployment is: where to store the user's home directory – on the local hard disk or on a central server? Mac OS X provides the flexibility to enable administrators to use either of these methods to store the user's home directory. When they choose to store the home directory on a network file server, there are even further choices, such as SMB (Server Message Block), AFP (Apple Filing Protocol) or DFS (Distributed File System). It is also possible to combine these methods and maintain a master home directory on the server while providing offline access with a local cached copy of the network home directory; Apple calls this a Portable Home Directory. DirectControl extends the integration of OS X systems into Active Directory for user authentication and authorization as well as Group Policy enforcement, which enables Windows administrators to easily manage OS X user and system settings in the same way that they manage Windows systems.

This application note describes how to configure both DirectControl and ExtremeZ-IP to enable users to log in to an OS X system with their Active Directory user ID and password to gain access to their home directory stored on a Windows server. DirectControl joins the OS X system to Active Directory and provides the user authentication, manages the user's UNIX identity, sets up the Kerberos environment for SSO, and manages the home directory path and mounting of network home directories. In this scenario, we will use

the AFP protocol to enable the user to access a Windows server for the home directory since it offers many advantages over using the SMB protocol.

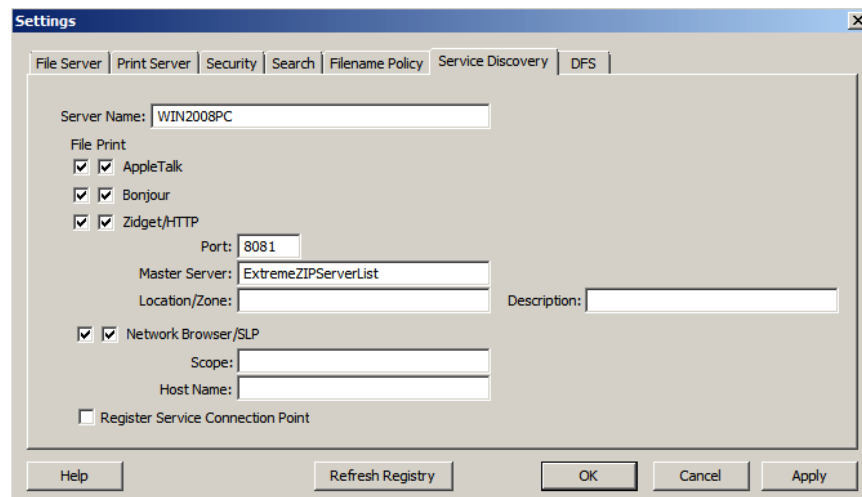
2 Set Up the Windows Server and ExtremeZ-IP

The Windows Server and Mac workstation must be joined into the same Active Directory forest. This server does not have to be configured as a file server in order to serve a file system to Mac systems, but if you want to also provide home directory services to Windows computers, then you should configure this system to also be a file server.

ExtremeZ-IP provides support for Kerberos-based user authentication, which enables a Windows home directory to be mounted at the time that the user logs in without needing to store a user ID and password anywhere on the system. This ensures that the user's Active Directory password is protected and the resulting Kerberos environment can be used to authenticate the user to the AFP-based home directory provided by ExtremeZ-IP.

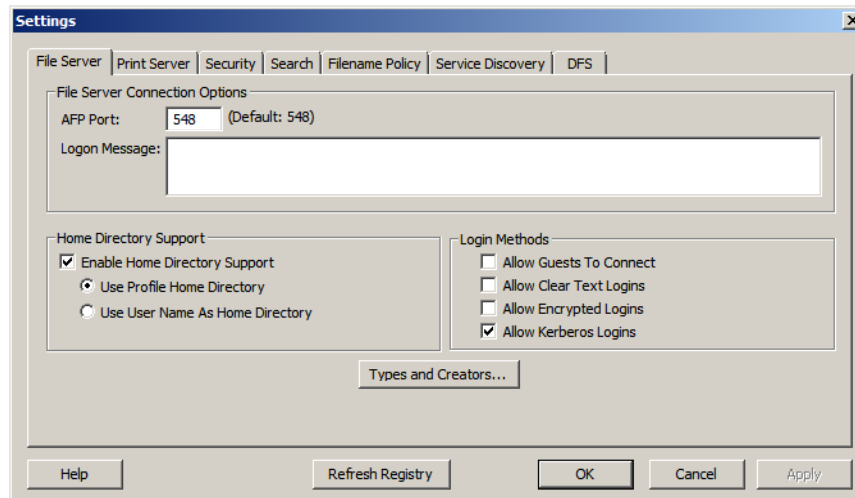
In this document, we will be using examples from ExtremeZ-IP 6.0, the most recent version as of this writing, which supports DFS described later in this document.

We can optionally setup ExtremeZ-IP Server's Settings to define the name that the server will be known to AFP-based client workstations. Typically, this is only necessary to support Mac OS 9, but in some cases it may be helpful for Mac OS X clients. Choose the Settings/Service Discovery tab. In this case, we will use the same name for the AFP Server Name as the Windows name so that DNS will resolve to the same computer.

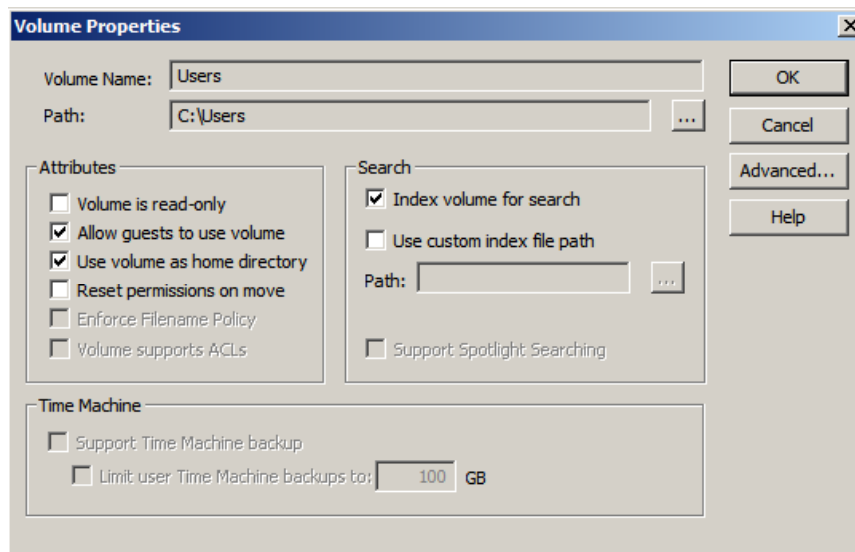


Choose the Settings/File Server tab and check "Enable Home Directory Support" and the "Use Profile Home Directory Support", a feature of ExtremeZ-IP that hides all other directories in a share point from the user except for his specified home directory, thus eliminating the user's ability to see all other users' home directories (which he should not be able to access). However, if you want users to be able to access directories other than just the user's home directory, you can leave "Enable Home Directory Support" unchecked.

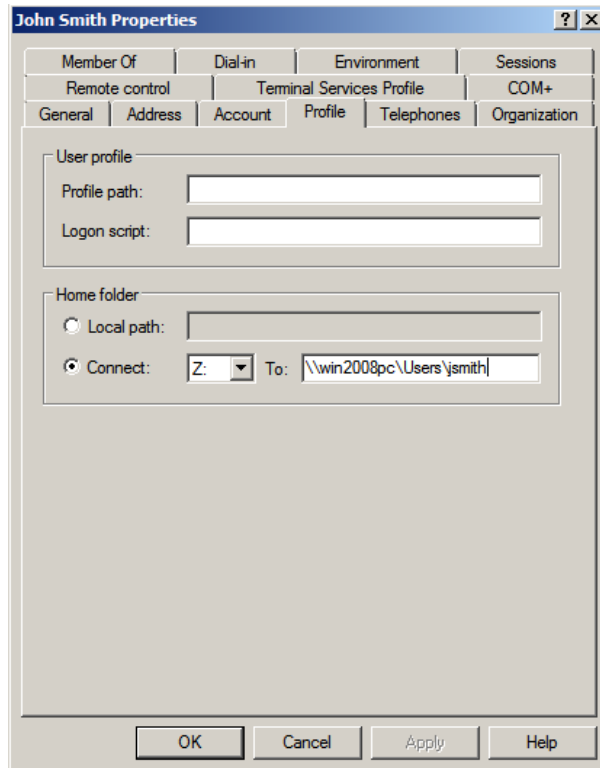
Also ensure that “Allow Kerberos Logins” is checked to enable users to gain access to the server without having to type their user ID and password once they have logged in with their Active Directory credentials (single sign-on feature).



Next, we need to define the volume that will be shared via AFP. Click the “Volumes” button at the bottom of the ExtremeZ-IP window, and choose the directory containing the user’s home directory. In this example we will share “C:\Users” and give it the ExtremeZ-IP Volume Name of “Users.” If we want to hide this ExtremeZ-IP volume from users who do not have a home directory on it and hide all directories from the user except for the user’s own home directory, check “Use volume as a home directory.”



In the Profile tab of their Active Directory Users and Computers user account properties, define a network home directory share path by selecting the “Connect” option button and choosing an appropriate drive letter, and then entering a valid path. When the “Apply or “OK” button is clicked, a home directory is automatically created for the user at the specified path.



Before proceeding to the Macintosh configuration, it is best to log in from a Windows client machine with the Active Directory user account to verify that the user can log in and that their network home directory is automatically mounted in Windows.

3 Install and Configure Centrify DirectControl on the Mac

DirectControl provides centralized management of all UNIX, Linux and Mac user attributes, including their identity and home directory path. These new user attributes can be managed using the Active Directory Users and Computers MMC console on the Centrify Profile tab, or through the DirectControl Administrator Console. DirectControl supports a user that might need to have more than one independent set of UNIX or Linux or Mac user account properties using a "Zone," which is a logical grouping of computer systems) has been created for the Mac and users.

However, for the purposes of this document, we will use a new, simplified mode, called "Workstation Mode," which only requires DirectControl to be installed on the Macintosh computer. It does not require any Centrify software to be installed on the server, and Centrify Zones do not need to be defined or configured.

Before the user can log in, we need to install DirectControl on the Mac workstation, and join the Mac to Active Directory in Workstation Mode.

3.1 Steps to Install Centrify DirectControl and Join the Active Directory Domain

Before starting, ensure that your Mac operating system is supported. DirectControl currently supports Mac OS X 10.4 and 10.5 on both PPC and Intel processors.

1. Download the DirectControl for Mac DMG file.

This is a Mac “disk image” that, once downloaded, will automatically mount a volume containing the Centrify DirectControl for Mac installer and relevant Mac utilities and documentation to your Mac desktop.



2. In the DMG, double-click to launch the ADCheck utility.



The ADCheck utility can alert you to any network issues that would prevent your Mac from reaching a Windows domain controller. Resolve any issues before going to the next step (you may need assistance from your Windows administrator).

3. Double-click the installer package, CentrifyDC-4.3.0.



This launches a standard Mac installer that leads you through the steps to install DirectControl on your Mac.

When the installation finishes, the Centrify ADJoin utility will launch so you can join your Mac to an Active Directory domain.

4. In ADJoin, type the name of your Active Directory domain, and select the Workstation Mode radio button. Then click the Join Domain button.

3.2 Configuring centrifydc.conf for Network Home Directories:

In Workstation Mode, without installing additional Centrify software on the Windows Domain controller, you will need to use a text editor to configure two items in the `/etc/centrifydc.conf` file.

First, `auto.schema.remote.file.service` should be set to "AFP". For example:

```
auto.schema.remote.file.service: AFP
```

Second, `auto.schema.use.adhomedir` should be set to "true". For example:

```
auto.schema.use.adhomedir: true
```

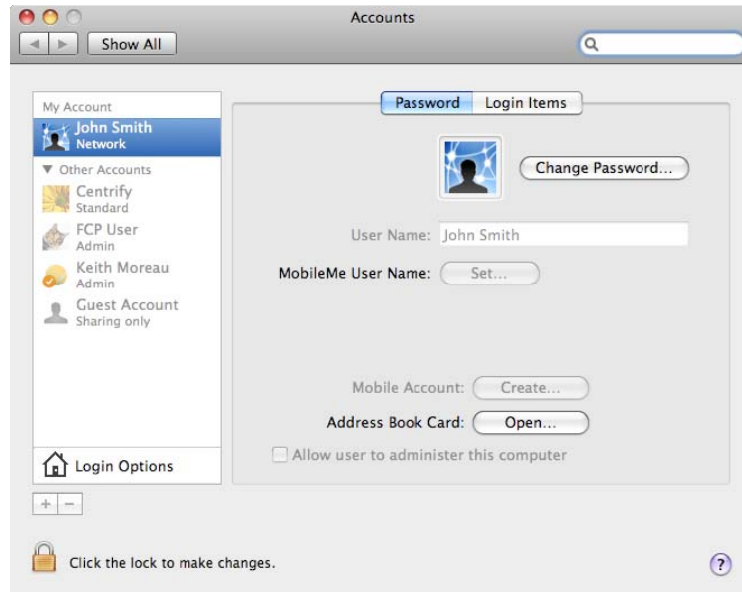
After these settings, you will need to either reboot the Macintosh computer or run these two Centrify command-line commands in the Macintosh terminal app as an admin user:

```
adflush  
adreload
```

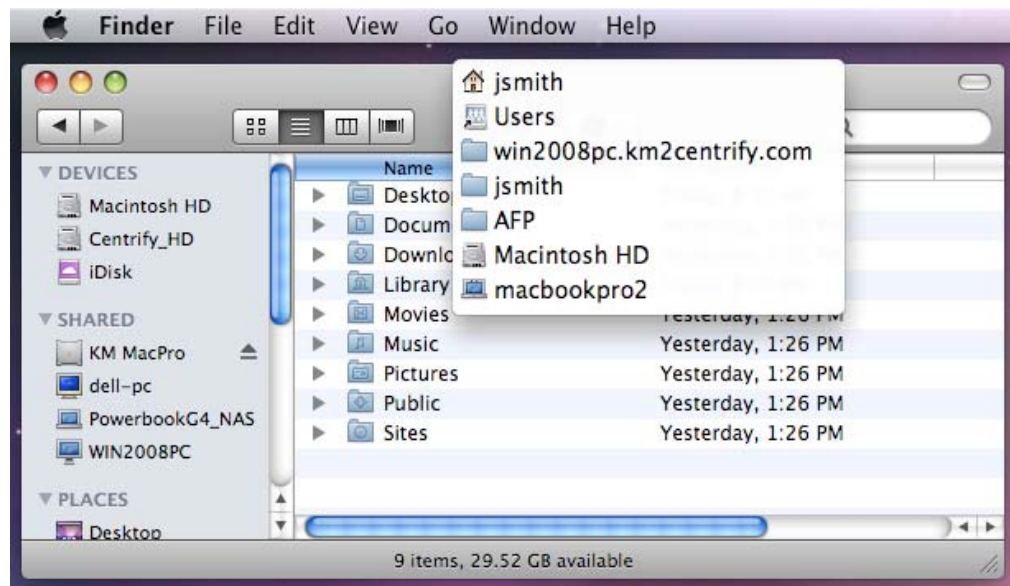
4 Testing the Solution

Once a computer is joined to Active Directory, any user who has a valid Active Directory user account and is using a Mac that is joined the Active Directory domain will be able to log in without any further user configuration required on the system. DirectControl enables the Mac to be treated just like any other Windows workstation; user authentication policies and login methods are supported and modeled after an XP workstation in an Active Directory environment.

Logging in to this Mac for the first time with the user's Active Directory user ID and password results in the network home directory being populated with the default set of Mac user files and folders on the Windows server. We can see in the Accounts panel within the System Preferences that the user's account, "John Smith," is a network account that was defined in Active Directory.



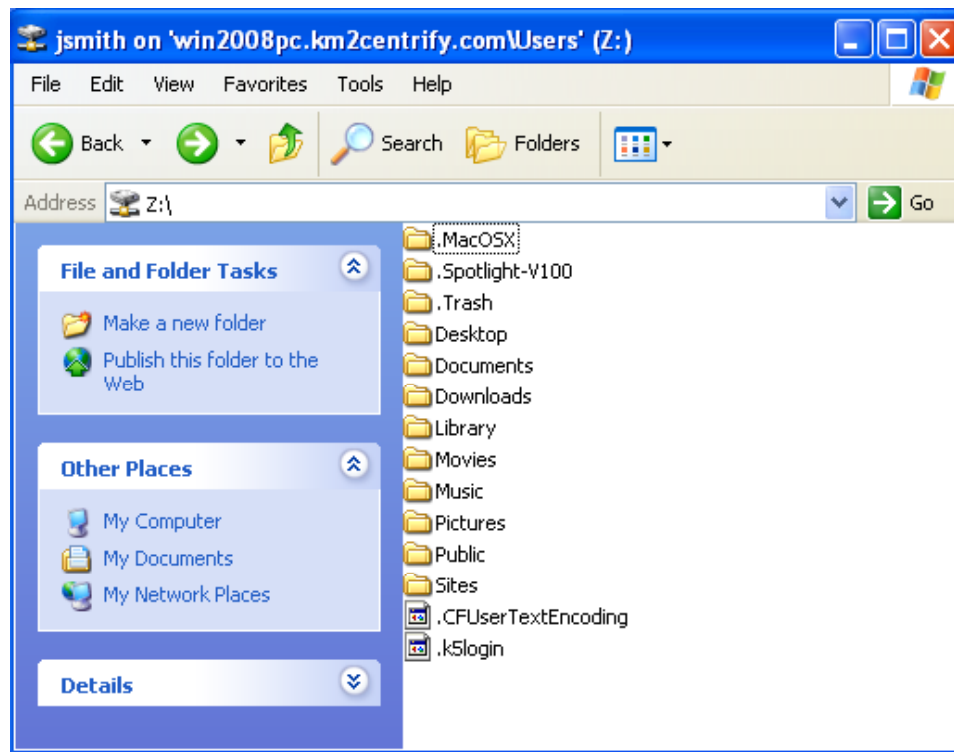
Opening Finder and going to the Home directory will show that the Home Directory path is mounted to the AFP network share that we previously defined.



We can also see on the Windows server that the home directory was properly populated with the default home directory contents for a Mac workstation on the server.

Kerberos-based authentication from the Mac to the Windows server also ensures that proper permissions are enforced as the user accesses files and folders on the server in addition to providing the user with single sign-on to the file server. By using Kerberos to authenticate to the server, the file server will enforce proper security regardless of the user's local UNIX identity on the Mac workstation, meaning that a user may have a UID of 10000 on a laptop and a different UID of 15000 on a Mac in a lab environment, and yet the user will still be able to access his network home directory from both workstations

based upon his Kerberos-based authentication to the server. File permissions will be reported back to the user so that he can read and write the files, while on the server it will show that his Active Directory account is the owner of the files.



Now that the user has a home directory he can access from a networked workstation, he will be able to use either a Mac or Windows computer to get to his home directory using the platform's native network file access protocol for the best platform compatibility.

5 Using Centrify DirectControl with DFS

Microsoft Distributed File System (DFS) is a set of technologies used to present a single virtual namespace to a collection of file servers and manage replication of data between those servers. Microsoft DFS consists of two technologies:

- DFS Replication (DFS-R): provides facilities for replicating file server data between locations and servers.
- DFS Namespaces (DFS-N): allows administrators to group file server shares on disparate machines into a single virtual namespace so end-users can access files without needing to know where the files are located.

Using DFS provides numerous benefits, including allowing administrators to relocate share points to other locations or servers without having to change the network paths that clients use to access the share.

To use DFS with a Macintosh client, the Macintosh and ExtremeZ-IP need to be configured to use DFS. For the purpose of this document, we will use the ExtremeZ-IP DFS Client application on the client Macintosh, and assume the Client Macintosh is running Mac OS 10.5 Leopard, which currently is the only method to support DFS home directories on a Macintosh.

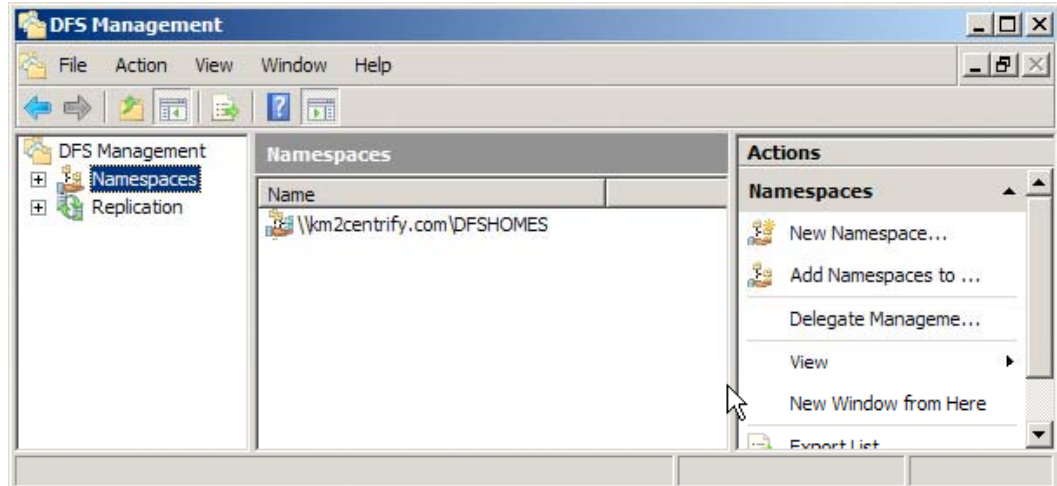
In the following example, for clarity, we have used a different Windows directory and ExtremeZ-IP volume than described in the previous section, but there is nothing preventing non-DFS and DFS Macintosh clients from using the same home directory.

5.1 Configure ExtremeZ-IP on the Windows Server to support DFS:

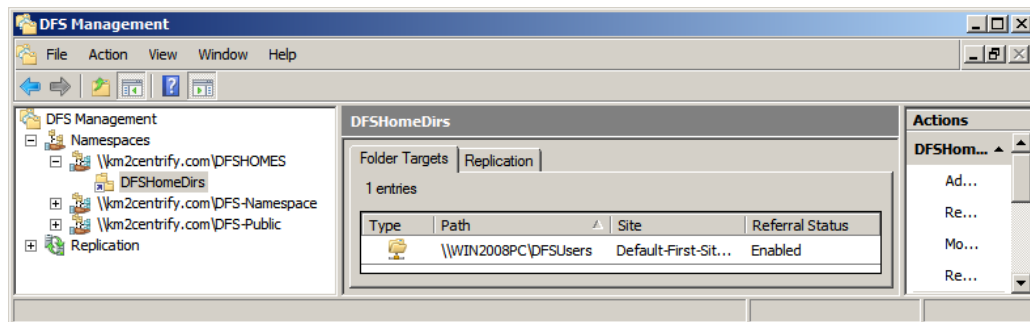
Here is a summary of the steps to use DFS home directories with ExtremeZ-IP:

- Configure your Windows server and Active Directory users to support DFS and DFS home directories.
- Configure ExtremeZ-IP to use the DFS namespace.
- Set up an ExtremeZ-IP volume on the target server for the folder containing the user home directories
- Set up an ExtremeZ-IP volume on the DFS Root Emulator for the DFS Home Directory
- Download and Install the Group Logic DFS Client Application from the ExtremeZ-IP Web Server onto your Mac
- Edit the Group Logic DFS configuration file `/etc/dfs/servers.conf` file on the Mac client, adding the IP address or hostnames of your ExtremeZ-IP DFS root server(s)

If you do not already have an appropriate namespace, you should configure a DFS Namespace on a Windows Server, using the Windows DFS Management Application. In our case we created a namespace called DFSHOMES on a single server that is our Domain Controller, DFS Root Server, and DFS Target Server.

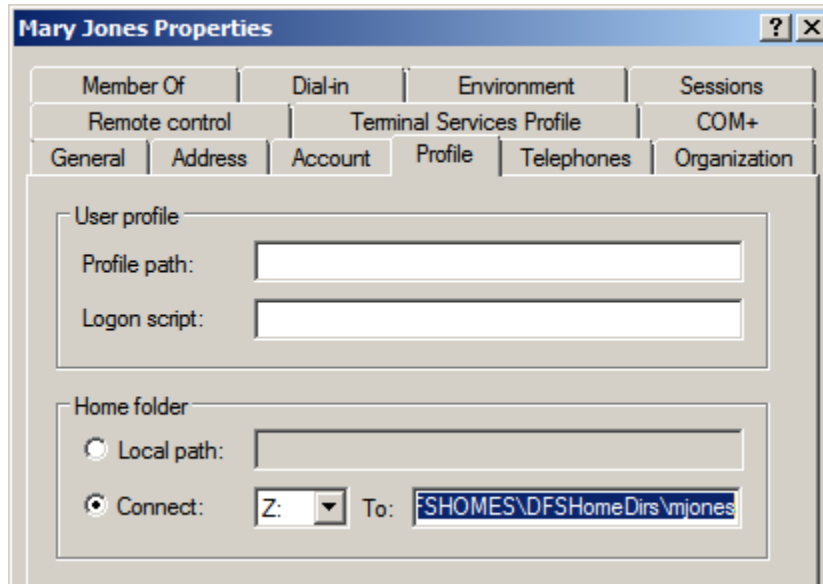


Add a target to your DFS namespace for the directory containing your user home directories. In this case the user home directories reside on the Windows domain controller local file system, but they would usually point to a network share. We've called our DFS folder "DFSHomeDirs" and it is targeting an actual directory, "C: \DFSUsers", which contains the home directories of our users. Please note that the target directory (in this case "DFSUsers") needs to be shared and accessible with the correct permissions on the network. In other words, in our simplistic single server example the DFS link \\km2centrify.com\DFSHomes\DFSHomeDirs resolves to a target share of \\Win2008PC\DFSUsers, which happens to be the same server.



Make sure your Active Directory user profile points to the new DFS namespace, rather than an actual path. In this example, the user "Mary Jones" home folder path is:

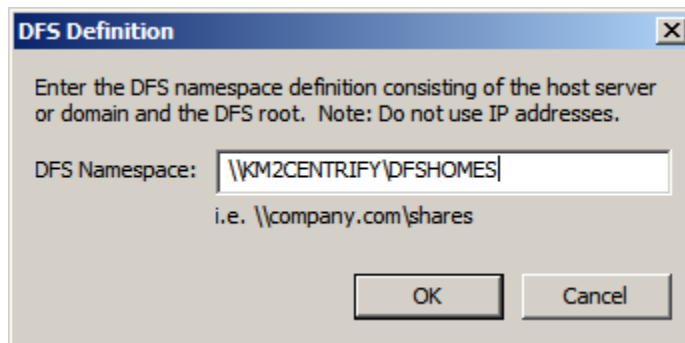
\\win2008pc.km2centrify.com\DFSHOMES\DFSHomeDirs\mjones



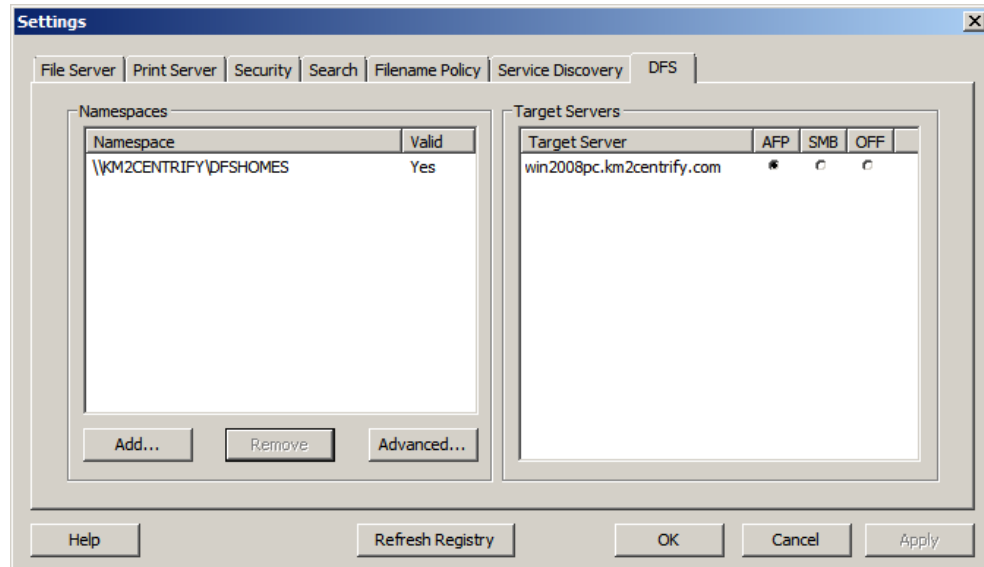
At this point you may want to validate the Windows DFS configuration by logging in this user with a Windows client. If they can log in and their network home folder is mounted, even though their home folder profile uses a DFS namespace, then proceed with this setup for Mac users.

5.2 ExtremeZ-IP DFS Configuration

In the ExtremeZ-IP application in Windows, click the “Settings” Button and select the “DFS” tab. Click the “Add” button and enter the path to the DFS namespace you defined in the Microsoft DFS Management Application. In this case it’s \\KM2CENTRIFY\DFSHOMES.



ExtremeZ-IP will validate the path and will put up the namespace and the corresponding target server. You’ll need to check the AFP option button and click “OK”.



5.3 ExtremeZ-IP AFP Volume Creation

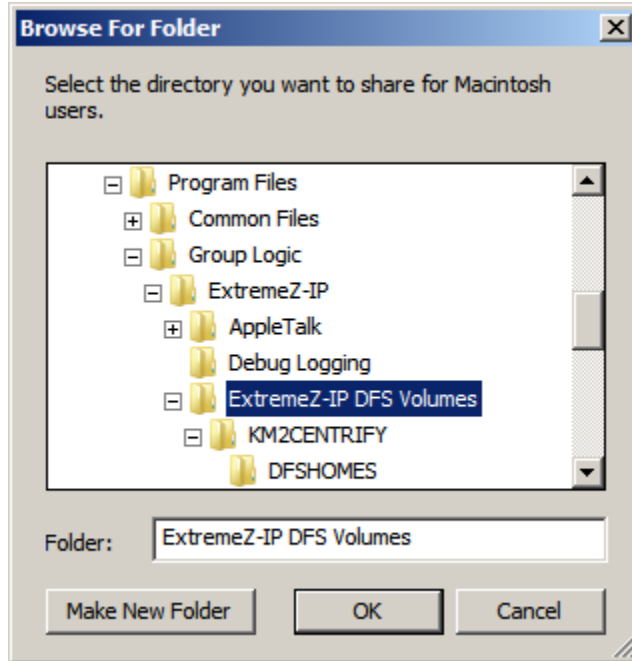
You'll need to create ExtremeZ-IP AFP volumes for each of the following paths:

- On the DFS target server, the directory containing the actual users' home directories, which was targeted above using the Windows DFS Management Application
- On the DFS root emulator, the ExtremeZ-IP DFS Root Path Home Directory

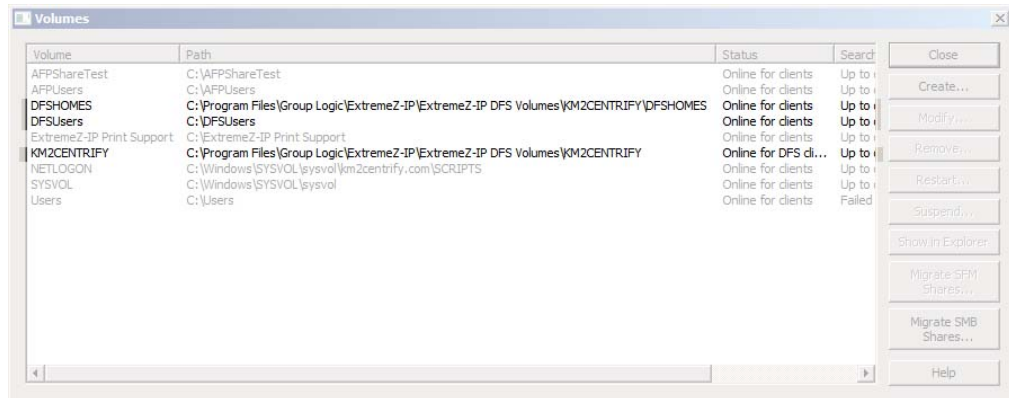
Within the "Volumes" window of ExtremeZ-IP, create an AFP volume from the Directory containing the actual Users' Home Directories. In this example it is "DFSUsers."

ExtremeZ-IP's DFS configuration creates special directories on your file server in C:\Program Files\Group Logic\ExtremeZ-IP DFS Volumes\. The automatically created ExtremeZ-IP volumes contained in this folder allow a Macintosh with the appropriately installed Group Logic software to use symbolic links contained in these AFP shares to properly resolve the DFS namespace. In this example, C:\Program Files\Group Logic\ExtremeZ-IP DFS Volumes\KM2CENTRIFY is the automatically created volume. The automatically created volumes in this directory will work for normal DFS browsing, but in the case of home directories we will need to manually share out a subdirectory.

Create **ExtremeZ-IP** subvolumes for the home directory folders located inside of **C:\Program Files\Group Logic\ExtremeZ-IP DFS Volumes**. In this example the path is **C:\Program Files\Group Logic\ExtremeZ-IP DFS Volumes\KM2CENTRIFY\DFSHomes**.

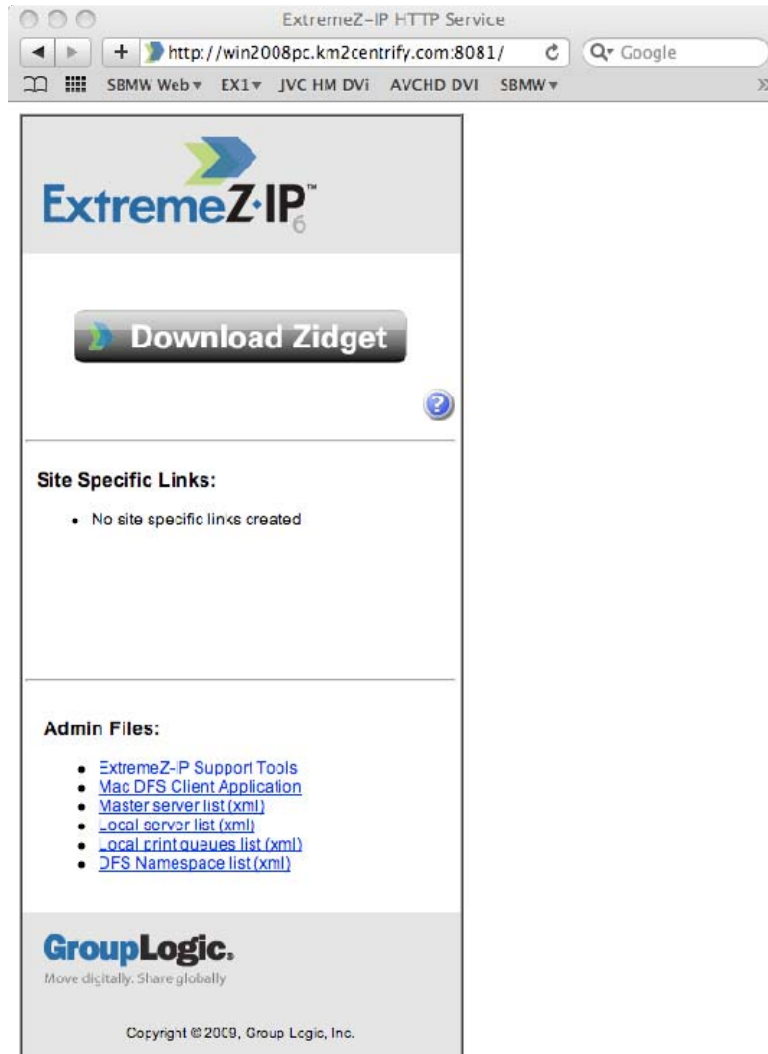


These volumes will be added to the ExtremeZ-IP volume list.



5.4 Group Logic DFS Macintosh Software Installation

On the Macintosh, which has been successfully joined to your domain using Centrify DirectControl, go to a web browser and point to the ExtremeZ-IP web server running on your domain controller using the domain name or IP address:



Click the “Mac DFS Client Application” link to download the installer. You’ll need to enter your Mac’s administrator user name and password for the install.

Once the Mac DFS Client Application is installed, you’ll need to edit the file `/etc/dfs/servers.conf`, which was created when the Group Logic Mac DFS Client Application was installed.

Add the fully qualified domain name and the port as the last line of this file. In this example, we added the line “win2008pc.km2centrify.com:8081” to this file.

```
/etc/dfservers.conf:

#####
# This file is used by Group Logic, Inc.'s
# DFS client application. It should contain the
# fully qualified domain name and port for the
# ExtremeZ-IP DFS root servers to be contacted
# to allow the Mac to browse your DFS namespace(s)
#
# example: bookers.gliilabs.com:8081
#
# the default port for use with ExtremeZ-IP is 8081
#
#####

#add server(s) below, one per line
win2008pc.km2centrify.com:8081
```

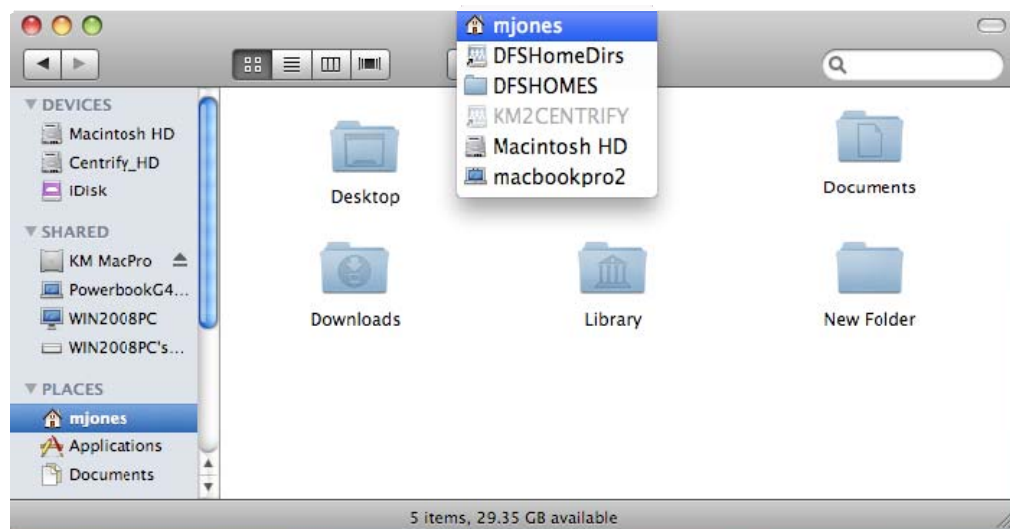
In /etc/CentrifyDC/centrifydc.conf, ensure that you have the settings “auto.schema.remote.file.service” set appropriately to AFP. For example:

```
auto.schema.remote.file.service: AFP
```

Note: You can also take advantage of the DirectControl Group Policy in order to centrally manage this dfservers.conf file by using the File Copy Group Policy to distribute a common file to all systems to which the policy applies.

5.5 Testing the Configuration

After installing and configuring the Group Logic DFS Client Application, reboot the Macintosh. At the login screen, log in as the user. The DFS network home directory user has logged in on the Mac, and if this is the first login from the Mac, the remote home directory will be populated with the default set of Mac user files and folders.



6 Summary

Enterprise organizations that want to integrate and embrace Mac users into their environment can fully integrate these users with the combination of Centrify DirectControl and Group Logic ExtremeZ-IP. DirectControl ensures that the workstations enforce the company's security policies through Active Directory authentication and password policies, and Group Policy will also enforce the enterprise security configuration policy standards. ExtremeZ-IP ensures that Mac users can securely access their network home directories via AFP and store Mac files properly on a Windows server with the advantages of DFS.

6.1 For More Information

For more information on DirectControl for Mac OS X, check out our web site at:

<http://www.centrify.com/mac>

For more information on ExtremeZ-IP, visit the Group Logic web site at:

<http://www.grouplogic.com/products/extremeZ-IP/>

Also see the Group Logic's Knowledge Base article titled "How does ExtremeZ-IP map the Windows security model to Macintosh-style folder permissions?"

<http://support.grouplogic.com/?p=1556>

6.2 Legal Notices

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of the Enterprise Desktop Alliance

Centrify may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Centrify, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2009 Centrify Corporation. All rights reserved.

Centrify and DirectControl are trademarks of Centrify Corporation in the United States and/or other countries. Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.