

# IT MANAGER GUIDE: AGNET ENTERPRISE FILE SERVER

This document provides overview and guidance for departmental IT managers regarding the utilization and operation of their AGNET Enterprise File Server.

# Contents

---

- Overview ..... 2
- File Server Acquisition and Requirements ..... 3
  - How to obtain your File Server .....3
  - Site Requirements .....3
  - IT Manager Software and Workstation Requirements .....3
  
- How to Manager your Enterprise File Server ..... 4
  - How to Grant Access to the File Server ..... 4
  - Enterprise File Server Directory Structure ..... 5
  - How to Create and Map User Personal Directories ..... 7
  - How Users access the Enterprise File Server .....8
  - How to Recover Deleted Files .....9
  
- Using your File Server as a Print Server ..... 9

# Overview

---

As a component of the AgriLife Enterprise venture Enterprise File services offers redundant local and off-site storage capabilities to facilitate the need to meet University and System IT requirements. Additionally each enterprise file server provides the following features:

- Redundant Power Supplied 2U Rack mounted HP File Server
- Quota Management per folder with email alerts to IT Managers and End users
- Replicated Offsite and Non-Replicated Shares
- Right-Sized Capacity for departmental Business Needs
- Automated Workstation failover utilizing DFSR Technology (AD Joined systems only)

Operations management of enterprise file servers is provided by AgriLife IT. Management tasks performed by AIT consist specifically of the following:

- Hardware replacement, maintenance and upgrades
- Patch management for Operating system and applications
- Remote System Monitoring
- Overall Disk Array Quota Monitoring
- Initial Networking and installation

IT Managers within Units and Centers are responsible for the following tasks:

- Creation of individual user personal directories and quota settings
- Creation of workgroup shared directories, access controls and quota settings
- Cleanup of "shared" folder space when quota limits are obtained
- General usage oversight (i.e. policing the storage of personal non-business files)
- General usage oversight of replicated and non-replicated shares use.
- Addition of network shared printers and queues (if utilized)

# File Server Acquisition and Requirements

---

## How to Obtain an Enterprise File Server

If you have not yet obtained your Enterprise File Server please contact your AgriLife IT coordinator (Tom Lyster or Jim Segers) to begin the process. Once your server has been configured AIT will schedule a brief planning meeting to prepare for the site installation of your server. Various details regarding networking connectivity, UPS availability and rack space will be discussed.

## Site Requirements

General site requirements\* include the following:

- Minimum 2 Network Ports (Minimum 100MB recommended)
- 2U of 19" 4-post rack space
- Environmentally controlled and secured location
- Access to an Uninterruptable Power Supply (if not available AIT will provide)

*\*AgriLife IT will provide the above for AgriLife Extension and Research centers around the state.*

## IT Manager Software and Workstation Requirements

By default your server will automatically be ready for service the day it is installed. The only requirement to begin use of your server as an IT manager is to have installed the Remote Server Administration Tools on a 64-Bit Windows 7 workstation that is joined to the AGNET.TAMU.EDU Active directory domain. (Please refer to the "[Managing Users & Computers – Instructions](#)" guide for installation instructions) You will not be able to manage your server or setup user shares until these requirements are met.

# How to Manage your Enterprise File Server

---

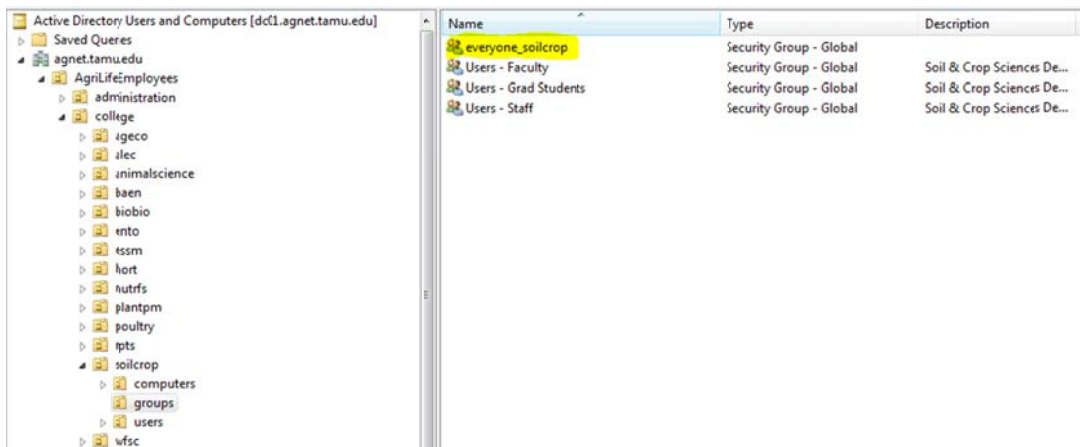
By default your enterprise file server is fully prepared and operational once it has been installed at your local site. All of the following services have been setup and tested:

- Burn-in testing
- Server Naming
- Active Directory Join
- Active Directory Group Permission Configuration
- DFS Replication Configuration and Testing
- DFS Naming Application
- Quota Management with email alerting
- Volume Shadow Copy (Facilitates Previous Version Recovery Feature)
- Default Replicated and Non-Replicated Shares
- Default group, public and personal directory folders

## How to Grant Access to Your Enterprise File Server

By default the only user with access to your server is the unit IT manager and the AIT engineering team. In order for a user to have access to your enterprise file server you must add them to a pre-established group that has been created in your OU/GROUPS folder. This group is named “**everyone\_XXX**” where XXX is the name of your departmental or unit OU.

As you create user accounts, each of your users that need access to the file server should be added to this group to enable them the correct permissions to use your enterprise file server.



# Enterprise File Server Directory Structure

The standard directory structure for all AgriLife enterprise file servers contains two top level folders **temp** and **protect**. The protect folder contains 3 subfolders: **group**, **share** and **user**.

**/temp**

**/protect**

**/group**

**/share**

**/user**

**temp** is a local-only folder, meaning it is not replicated to the AgriLife core datacenter or protected via backups. It is meant as a temporary file storage area for use by the OU administrator. Suggested use of this folder includes:

- Storage of ISO's
- Temporary transfer location for files (i.e. during a workstation rebuild)
- Transient Large File Transfers (workstation to workstation)

The temp folder is set to a default 100GB size on all enterprise IT servers.

**protect** is a replicated folder, meaning that all folders and content within the **protect** folder are replicated to the AgriLife core data center and backed up. This directory is also presented redundantly by the core data center, meaning that if your file server should become unavailable, for some reason, data within the protect folder will still be available via the core enterprise storage system. Access to the core enterprise storage system, in such a situation, is transparent meaning the path remains unchanged and will still be [\\agnet\files\your-org-abbreviation](#).

**It is HIGHLY RECOMMENDED not to store or place large transient files anywhere within this folder or subfolders within the “protect” directory. Large files create sizeable delays in the network based DFS Replication service potentially creating a backlog for more important business files being replicated to the core enterprise storage server. AIT recommends that IT Managers should coach users on best use of this space as not to adversely affect the service for others users within the unit. The “temp” directory should be used as a large transient file swapping area if required.**

**/protect/group** is intended for special groups of users who need a common folder to share documents, etc. It is recommended as a best practice that you should set up each of these groups as needed by creating a group in Active Directory with those users as members, creating a folder for that group and then applying the Active Directory group to the permissions of that folder.

The default quota size for the /protect/group folder is 200GB. IT Managers will receive email alerts at 85%, 95%, and 100% of quota capacity on this folder. This quota limit can also be increased by the IT managers if required.

Alternatively the shared folder could be created and permissions to the folder added for each user that needs access. This method would work best when few users are accessing the folder and that group of users is not used elsewhere for any other purposes; negating the need to create an Active Directory group.

**/protect/share** is intended as an area for all users within your organization to create their own folders, content, etc. to share with each other. This folder is set with a default quota of 100GB and quota warnings are sent to the unit IT manager at 85%, 95% and 100% levels. Individual users who trigger one of these thresholds are also notified at these quota levels via email.

**/protect/user** is the top-level folder for all of your users' home directories which you set up through Active Directory (See Section 2 above). Default quotas are set to 10GB and can be altered with the File Server Resource Manager (FSRM) Server tool (See <http://agrillife.org/it/migrate/> for information on how to change and manage quotas).

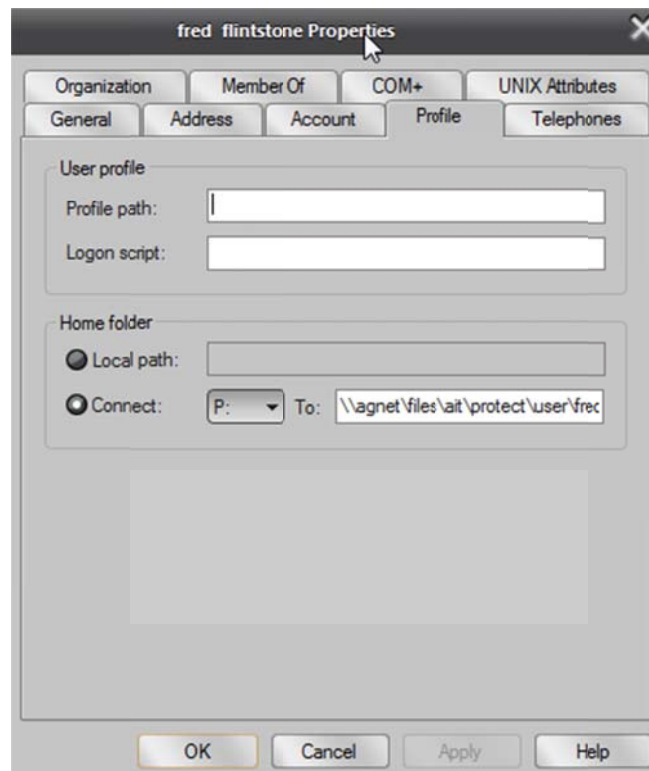
Both IT managers and end users will receive quota warning emails at 85%, 95%, and 100% of quota level.

## How to Create and Map User Personal Directories in a One Step Process

Users' personal directories on your enterprise file server should not be created manually. They will automatically be created with the correct permissions and default quota policies applied by using the following method.

*NOTE: This step shouldn't be performed until your file server is in place and configuration has been completed. Users who have had their profile "home folder" set before your file server is ready will need to be revisited in order to automatically create and map their personal directory on the file server.*

To automatically create and map a user's personal directory, locate them in Active Directory using the Active Directory and Computers RSAT tool and open the user's properties dialog box, then select the "Profile" tab.



Under the "Home folder" section, select the "Connect:" radio button, select a drive letter to map, (P: Drive is recommended as a standard) and enter the path to their folder in the "To:" box. The path format is:

[\\agnet\files\xxx\protect\user\firstname.lastname](#)

In the above example, the user is part of AgriLife IT, so their path is

[\\agnet\files\ait\protect\user\firstname.lastname](#)

As long as your organization's file server is in place and configured, this step will automatically create their folder with the proper permissions set – as well as map the drive for them when they log on to their domain-joined workstation and automatically apply the 10GB quota limit and quota warnings policy to their personal folder.

This process saves a considerable amount of time setting up permissions manually, configuring quotas and alerts.

## **How Users Access the Enterprise File Server**

There are two scenarios to explain when discussing browsing of the file shares on your file server.

1. A computer joined to the AGNET domain
2. A computer not joined to the domain

When a computer is joined to the AGNET domain, users may access their organization's file shares by accessing the DFS namespace. This is done by opening a Windows file system browsing window and entering [\\agnet\files](#). A list of servers will be provided. The user should select the appropriate departmental file server they have access to. While other file servers may be listed they will not have access to them. Alternatively they can link directly to their file server. For example, the namespace for the Department of Soil and Crop Sciences could be accessed by entering [\\agnet\files\soilcrop](#). Once there, you will see the standard file server directory structure with top level folders **protect** and **temp**.

When a computer is *not* joined to the AGNET domain, users must connect directly to the file server using the UNC path example below, which requires knowing the AFSXX name of your organization's file server. Example: [\\afs14.tamu.edu\soilcrop](#) this name is labeled on the front of your file server, or can be obtained by contacting AIT.

Users can also map local drives on their workstations using these UNC paths by using the appropriate commands offered by their version of operating system.

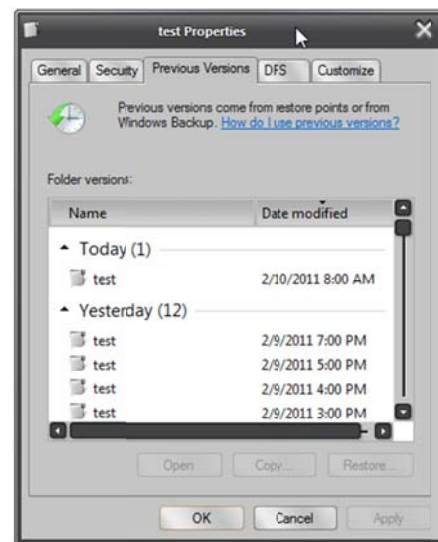
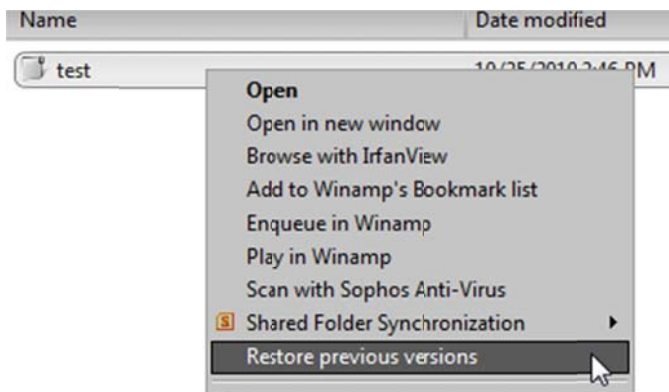
## How to Recover Deleted Files

By default each enterprise IT file server has been enabled with Volume Shadow Copy services. This service provides for the ability to recover files that have been recently deleted.

Between the hours of 8am and 6pm (Mon-Fri) each enterprise file server makes a snapshot of all files on the server each hour and creates a version of the file. Each file must be in existence before the Volume Shadow copy makes the version copy. (i.e. Files that existed less than an hour on the server and were not in existence at the top of any hour between 8am and 6pm cannot be recovered if deleted by the user.)

Up to 64 copies are kept which allows recovery of files that were captured back approximately 6 full business days.

Users can access the “previous versions” by going to any file or folder on the enterprise file server and right-clicking. They will see an option called “**Restore previous Version**”. This will bring up a window displaying all the available versions of that file or folder.



## Using your File Server as a Print Server

By default all enterprise IT Servers are not configured with print services. During the planning meeting you should request this service option if required.