A Guide for Department Shared Folder Access Controllers

Does the staff in your department have documents that they need to share with each other and collaborate on?

Are you concerned about the security of important department files that are now saved on your computer?

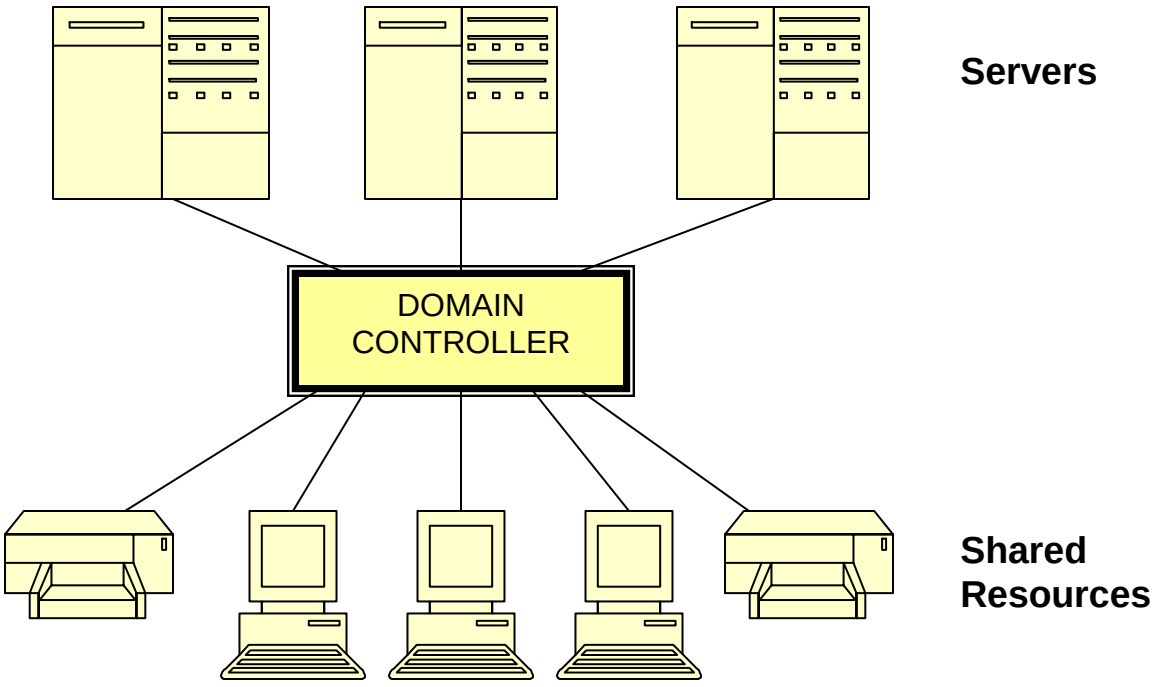
Would you like to be able to access these department files when you are not in your office?

What Is A Domain? 3
Advantages of Department Shared Folders 4
Important Things You and Your Users Should Know 4
How to Request a New Department Shared Folder 5
Viewing Your Access Groups 6
  Viewing group members 7
Searching for a NetID 8
Adding Users 9
Removing Access 10
Inform the Users 11

What Is A Domain?

A ***domain*** is an internal network of computers where the users can share space on a server for storing files and sharing access to printers. ***Sunysb.edu*** is an example of the domain that many of our users belong to. It consists of a series of servers – Admin01, Admin02, Admin03, etc.- and a Domain Controller.

The sunysb.edu domain:



The domain is maintained by **DoIT Windows Admin**.

To access the domain you must log on using your **NetID** and **NetID password**. This lets you use the resources on the domain for which your account has permissions.

Many departments utilize shared folders on the domain servers to store and share important files.

Advantages of Department Shared Folders

- **A secure, more reliable environment.** Important files containing "sensitive" data should not be stored on your computer. If these files are stored on the server they will not be affected if your computer crashes or is stolen. Also, files stored on the server are backed up nightly.
- **An effective way of sharing information and resources.** You may have a database or spreadsheet that users in different areas of the department may need information from for various purposes. The file can be accessed in the shared folder whenever they need it. You may even want more than one user to maintain data on a spreadsheet or database. They can do so easily when it is in the shared folder.
- **Can be accessed at any time from anywhere when you need them.** You can access your shared folder from another computer.

Important Things You and Your Users Should Know

- Resources on the server are limited. Department shared folders are allocated 1 gigabyte of storage by default. If necessary, this can be increased.
- Servers are monitored by DoIT Windows Admin.
- This folder should be used to store files for work purposes only. Storage of other file types like executable files used to install programs, personal music, screensavers or photos is not recommended.
- Virus infected files will be deleted.
- When you delete files from these folders they do not go to the *Recycle Bin* on your computer. DoIT Windows Admin must restore the files from backup.
- In most cases, more than one person can access a file at the same time but only one person can edit the file.

Reminder:

Access to Data Policy D 100
The University's Division of Information Technology ("DoIT") is committed to minimizing vulnerabilities that may result from compromised operating system integrity or application security problems, as well as protecting against the unauthorized disclosure or misuse of any information stored on any device connected to the University's network infrastructure. To ensure the continued integrity of its information technology resources, the University may audit, inspect and/or monitor them, at any time.

How to Request a New Department Shared Folder

Two people are responsible for maintaining the access group for the department's shared folder. This maintenance includes:

- Giving staff access
- Removing access when staff are terminated, retire or leave the department

Access Controllers will use the **Active Directory Users and Computers** software to do this.

1. Access Controller completes the ***Department Shared Folder Request Form*** online
   http://naples.cc.sunysb.edu/doit/sharereq.nsf/share+request

2. DoIT Windows Admin creates the shared folder and the access control groups

3. DoIT Windows Admin emails the shared folder information to both Access Controllers, Client Support and the department's computer support technician. This includes:
   - the shared folder name
   - the path (server name, etc.) where the folder is located
   - the access group names

4. Client Support or the department's computer support technician installs the *Active Directory Users and Computers* software on both Access Controllers computers

5. Client Support trains the Access Controllers

6. Access Controllers begin adding/removing users to the access groups

You must submit a **Department Shared Folder Request Form** for every folder that requires its own separate access group.

If the Access Controllers change you must send an email to "**DoIT Windows Admin**".

Viewing Your Access Groups

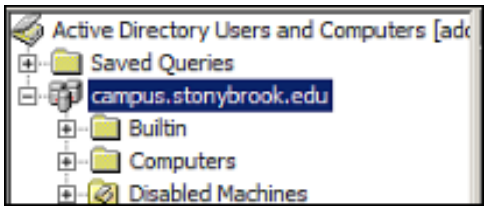
The **Active Directory Users and Computers** software must be installed on the Access Controllers' computer in order for them to maintain their shared folder access groups. Contact Client Support or your department's computer support technician if this hasn't been done yet.

Each shared folder will have at least 3 access groups associated with it:

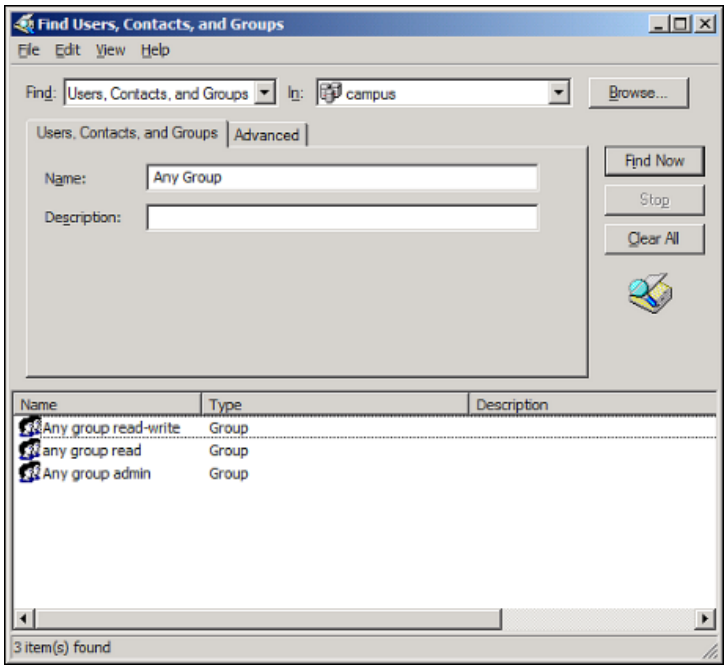
- **An admin group** – this group contains the names of the shared folder Access Controllers. Only DoIT Windows Admin can add/remove names to this group.
- **A read group** – the people in this group have "read only" access to the files in this shared folder. Share Access Controllers can add or remove people to this group.
- **A read-write group** – the people in this group have "read/write" access to the files in this shared folder. This allows them to create, modify and delete folders and files within this folder. Share Access Controllers can add or remove people to this group.

Double click the **Active Directory Users and Computers** shortcut on your desktop to open it

Search for the folder or access group name:



Right click *campus.stonybrook.edu* and choose **Find**



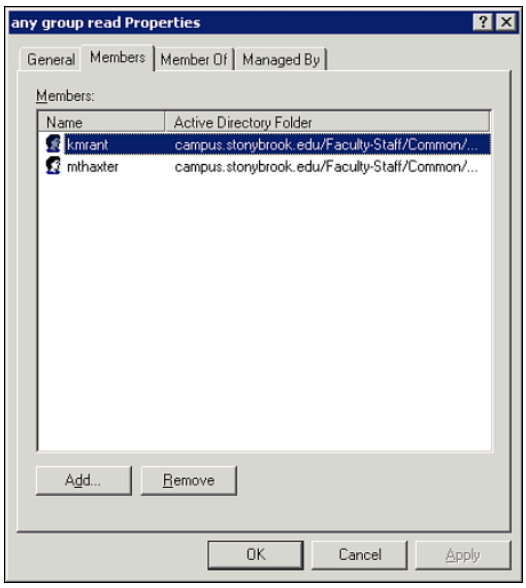
Enter the folder or access group **name**

Click **Find Now**

The **Description** field will include information about the group and the type of access.

Viewing group members

- Double click the access group name
- Click the **Members** tab



Group members are identified by their **NetID** in the Active Directory.

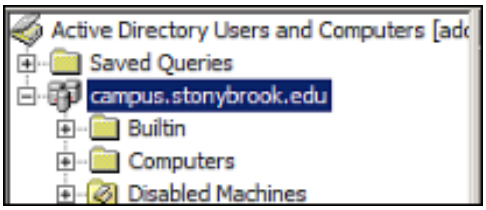
Searching for a NetID

Users are identified in the Active Directory by their **NetID**. It will be easier to add/remove a user to an access group if you know their **NetID** ahead of time.

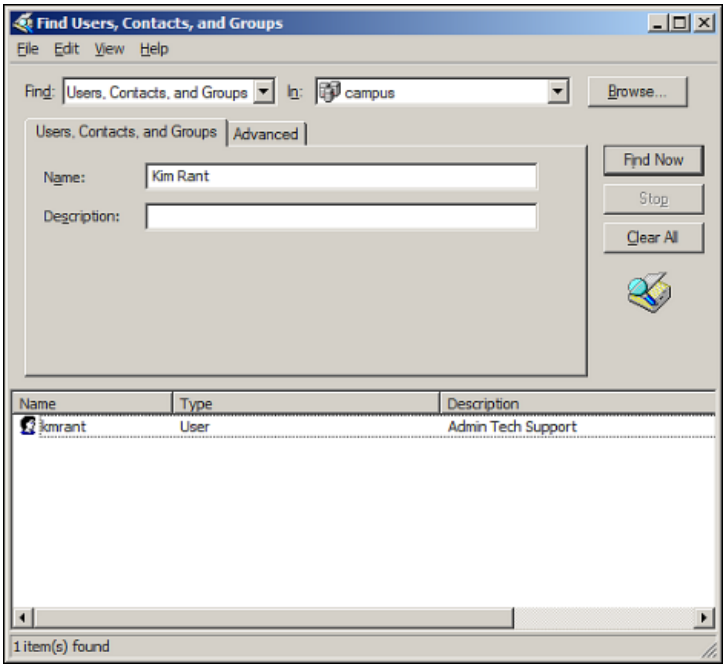
- New staff members are assigned a **NetID** upon hire
- New students are assigned a **NetID** when they are admitted to the University
- The **NetID** is inactivated upon termination

Users can obtain their **NetID** and **NetID Password** by logging in to SOLAR and following the **NetID** links.

If you do not know the **NetID** you can search for it in the Active Directory.



Right click *campus.stonybrook.edu* and choose **Find**



In the **Name** field, enter the person's **first name and last name**

Click **Find Now**

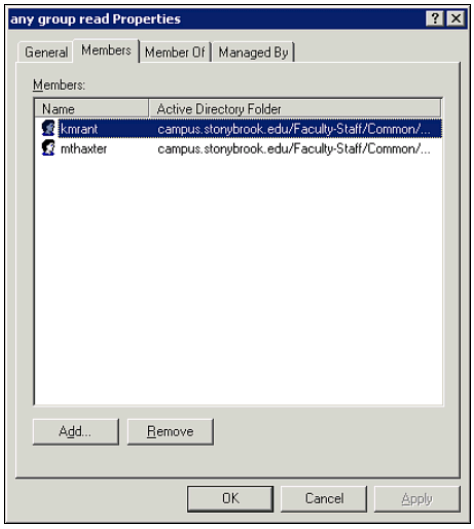
The **NetID** will be displayed below

It's possible that you will see more than one name match. If you are unsure, ask the user.

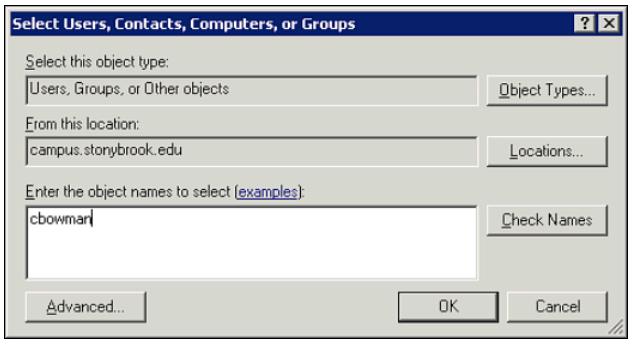
Adding Users

When a staff member requires access to the department shared folder you must add them to the appropriate access group:

- Double click the access group name to open it
- Click the **Members** tab. Group members are identified by their **NetID**.

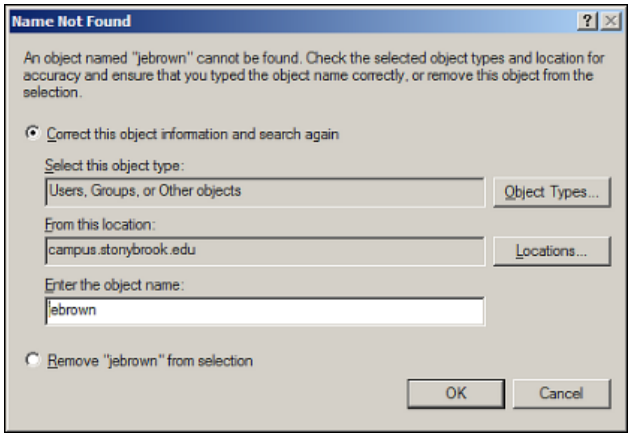


Click the **Add** button



Enter the person's **NetID** and click **Check Names**

If the person is found in the Active Directory click **OK**



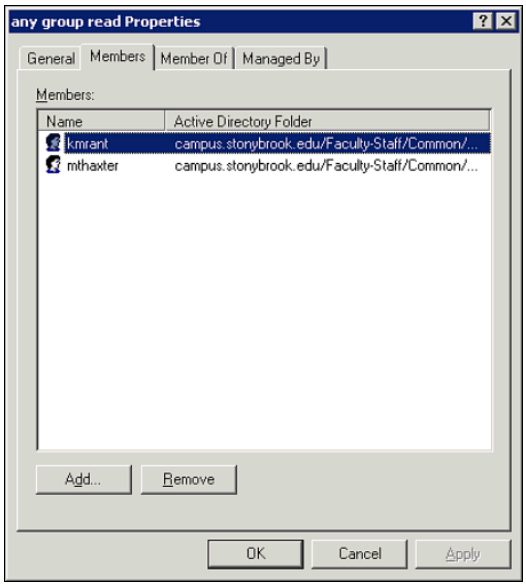
If the person is not found, the ***Name Not Found*** dialog box will be displayed.

In this case, click **Cancel** and check the NetID again to make sure it is correct. ***Users cannot be added if they do not have a valid NetID in the Active Directory.***

Removing Access

When staff terminate, retire or transfer to another department and no longer require access to the department shared folder you must remove them from the access group.

- Double click the access group name to open it
- Click the **Members** tab. Group members are identified by their **NetID**.



Click once to select the name

Click the **Remove** button

Click **Yes** to confirm the deletion

Click **OK** to complete the removal

Inform the Users

Access Controllers must notify new users when they are given access to the department shared folder. Domain users will see the shortcut the next time that they log in.

New users need to know the following:

- What the folder is used for
- How to log on to the Stony Brook domain (if they don't do this already) or authenticate using their NetID and NetID Password
- How to access the shared folder
- How to create a shortcut and/or map a drive to the shared folder
- How to access files in the shared folder
- How to save files to the shared folder
- How to create a subfolder
- How to access files in the shared folder when they are not in the office
- How to restore files that were deleted from the shared folder

All of this information can be found in the "**Using Your Department Shared Folder**" document which is available on the Client Support website. Make sure your users have a copy.

http://it.cc.stonybrook.edu/site_documents/networking/using_your_share.pdf