

# Controlling Access to a Network Shared Drive Folder

---

August 2011

Most likely your office maintains space on a DHS shared network drive. Your office controls access to its portion of the shared drive through a folder-based security mechanism. Typically, access to your main folder is restricted to the staff on your office's main email distribution list.

If you want to restrict access to a particular folder within your shared drive, here's what to do:

1. Create/identify the folder you want to control.
2. Find the full path to that folder by:
  - a. Clicking on My Computer on your desktop.
  - b. Finding your network shared drive and right clicking it.
  - c. In the left NAV under "Details", the network drive path will appear, for example:
    - \\ZZA1CE-0350\dhs-g\DHS\Your Office\Your Folder
3. Create the name of an email distribution list that you'd like to use to govern access to the folder. Use something like "officename [folder]". Keep it short, simple, easy to recognize in the GAL. This email list becomes your security group, and as the manager of this group, you have the ability to add and remove names of users, as needed. To do this [once the email list is created], open the security list in the GAL, click "modify members", then add or remove users.
4. Identify who you want to have access to that folder – you will need full DHS email addresses.
5. Email IT Support and tell them you want to:
  - a. Restrict access to a folder. Send them the full path (step 2).
  - b. Create an email distribution list with the names you picked (step 3); and
  - c. Add all the names/email addresses to that distribution list and give each of those individuals "owner" rights to the distribution list – this way anyone in that list can change the list if you want to add/remove names. You can also pick one person and give them ownership rights to add/remove people from the distribution list. However you do it, it's key that someone you know can edit that list of names – this will give you control over who can access the folder.
  - d. Restrict access to that folder so that only users on the distribution list can access it. You can make this a little more complex by changing the tiers of control over the folder.
    - i. Full restriction/access – only those on the list can open the folder and once they're in they can do anything they want.
    - ii. Read only – you can allow anyone to read files in that folder – they cannot edit/delete anything – then only people on the distribution list can change.
6. Then get confirmation from IT Support, and conduct a test –
  - a. See if someone outside your new group can open the folder.
  - b. See if someone inside your group can open the folder and change stuff in it.
  - c. See if someone on your list can change the names on the list.