U Drive / S Drive (Shared Drives)

How to set UDrive permissions

Setting Udrive Permissions

Introduction

In the interest of privacy, all Udrive directories have had their access permissions set to allow read and write access only by the owner of the directory. The new default setting will permit read and write access inside a user's home directory if the user chooses to change permissions on individual subdirectories and/or files. One obvious instance where this may be desirable is when the user has a web page that he/she wants others to see. Web pages are built within a subdirectory named "public_html."

The following sections describe how a user may change these permissions within his/her home directory. There is one section for changes made when logged into a UNIX machine (i.e., Sun or SGI) and another section for doing this when logged into a Windows computer. Changes made using either type of system will be reflected on both systems.

Changing File Permissions in a UNIX System

Permissions are the way you regulate access to your files. For instance, when setting up web pages, the main thing you'll be concerned with is making sure everyone can read the file while not letting them overwrite it. There may be some things that you don't want people to have access to at all.

How Do You Tell Which Permissions Are Set?

At a Unix prompt in a terminal window, type: ls -l The output might look like this (space=_):

_rwxr-xr-x1 usernamegroupname2525 Feb 18 09:17filename

The first set of letters, **rwxrwxr-x**, indicate the permissions set for the owner of the file, the group the file belongs to, and others who are neither the owner nor in the group.

The first three letters, **rwx**, indicate that the owner of the file can read, write, and exceute the file. The next three letters, **rwx**, indicate that the group can also read, write, and execute the file. The third set, **r-x**, indicate that other users (who are neither the owner nor in the group) can only read and execute the file. They cannot write to it. apply to everyone.

Following that is additional information about the file, including the username of the owner of the file and the group name that the file belongs to.

Notice that there are three user categories ("user," "group," and "other") and each user category has three permissions that can be set: "r," "w," and "x". To set permissions, you can use the chmod command. There are two ways to use chmod:

number or text.

Only the number method will be explained here.

Using the numbering scheme, the chmod command has three number places, for example 744, representing the three user types. The first number on the left side is for "user", the middle one is for "group" and the right hand one for "other." Here is what each 0 = --- = no access

1 = --x = execute
2 = -w- = write
3 = -wx = write and execute
4 = r-- = read
5 = r-x = read and execute
6 = rw- = read and write
7 = rwx = read write execute (full access)

To give a file named **foo** the same permissions as those in our example, you would type **chmod 775 foo**

For directories, rwx have these meanings:

read = list files in the directory
write = add new files to the directory
execute = access files in the directory

Additional information about the chmod and ls commands may be obtained from the UNIX manual pages by entering a "man chmod" or "man ls" command at the terminal prompt. On the Sun workstations, file permissions may also be set using the GUI-based FileManager.

Changing File Permissions in a Windows PC System

Currently, permissions can only be changed on PCs logging into the FLTECH domain with Windows 7 and 8.1. Users of other PC operating systems should follow the instructions for changing permissions in UNIX as detailed above.

To change permissions

1. Browse to the directory you want to change permissions on.
2. Click the right mouse button over the directory and choose properties from the drop-down menu that appears.
3. Select the Security tab from the next dialog box that appears.
4. On the Security page, press the button labeled permissions.
5. You will see three security categories assigned to your folder: (user (Unix User\{username}), group (Unix Group\{group name}, other (everyone))
6. Double-click the mouse button over the security category you want to change.

U Drive / S Drive (Shared Drives)

7. From the special access dialog box, select the desired permissions (read, write, execute) that you want applied to the security category.
8. Click OK to all remaining dialog boxes that are open.
9. Repeat steps 1-5 and verify that the permissions have been properly changed.

Unique solution ID: #1042
Author: Tech Support
Last update: 2015-03-30 15:19