# Create User Accounts with Data Access

Contents

[Create User Accounts with Data Access 1](#_Toc119606254)

[Lab Information 1](#_Toc119606255)

[Description 1](#_Toc119606256)

[Step 1: Create Folders, User Accounts, and User Groups 2](#_Toc119606257)

[Step 2: Set NTFS Folder Permissions for User Groups 3](#_Toc119606258)

[Permission Levels for Files and Folders 3](#_Toc119606259)

[Step 3: Test, Set Share Permissions, and Go Live 5](#_Toc119606260)

[Map a Network Drive and Network Printer 6](#_Toc119606261)

[Connect and Share a Printer 7](#_Toc119606262)

[Assignment Submission 7](#_Toc119606263)

Time required: 90 minutes

**How to Create Screenshots:** Please use the Windows Snip and Sketch Tool or the Snipping Tool. Paste a screenshot of just the program you are working on. If you are snipping a virtual machine, make sure your focus is outside the virtual machine before you snip.

1. Press and hold down the **Windows key** & **Shift**, then type **S.** This brings up the on-screen snipping tool.
2. Click and Drag your mouse around whatever you want to snip.
3. Release the mouse button. This places the snip into the Windows Clipboard.
4. Go into Word or wherever you want to paste the snip. Hold down **CTRL**, then type **V** to paste the snip.

## Lab Information

Nicole is responsible for a peer-to-peer network for a medical doctor’s office. Four computers are connected to the small company network; one of these computers acts as the file server for the network.

Nicole has created two classifications of data, Financial and Medical. Two workers (Nancy and Adam) require access to the Medical data, and two workers (Linda and Carlos) require access to the Financial folder. In addition, the doctor, Lucas, requires access to both categories of data.

## Description

Here is what Nicole must do to set up the users and data:

1. Create folders named Financial and Medical on the file server
2. Create five user accounts: Lucas, Nancy, Adam, Linda, and Carlos. All the accounts belong to the Windows standard user group.
3. Create two user groups: Financial and Medical.
4. Using NTFS permissions, set the permissions on the Financial and Medical folders so that only the members of the appropriate group can access each folder.
5. Test access to both folders using test data and then copy all real data into the two folders and subfolders.

# Step 1: Create Folders, User Accounts, and User Groups

Follow these steps to create the folders, user accounts, and user groups on the file server computer that is using Windows 11/10/8/7:

1. Sign in with an administrator level account.
2. On the C: drive: create these two folders: C:\Data\Medical and C:\Data\Financial.
3. Right Click on the Start Button 🡪 Open the Computer Management console.
4. Open Local Users and Groups 🡪 Users
5. Create new user accounts for Lucas, Nancy, Adam, Linda, and Carlos. The account types are automatically standard user accounts.
6. To create the Medical user group, right-click Groups under Local Users and Groups and select New Group in the shortcut menu.
7. The New Group box appears. Enter the name of the group (Medical) and its description (Users have access to the Medical folder).
8. Add all the users that need access to medical data (Lucas, Adam, and Nancy). To add members to the Medical group, click Add.
9. The Select Users box opens. Under Enter the object names to select, enter the name of a user and click OK. As each user is added, his or her name appears under Members in the New Group box. To create the group, click Create in the New Group box.
10. **Insert a screenshot of the Medical group showing the members:**

Click or tap here to enter text.

1. In the same way, create the Financial group. Add Lucas, Linda, and Carlos to the group.
2. **Insert a screenshot of the Financial group showing the members:**

Click or tap here to enter text.

1. Close the Computer Management console.

# Step 2: Set NTFS Folder Permissions for User Groups

Follow these steps to set the NTFS permissions for the two folders:

1. Open File Explorer  
   🡪 right-click the **Medical** folder  
   🡪 select **Properties** in the shortcut menu. The Properties box for the folder appears.
2. Click the **Sharing** tab 🡪 **Advanced Sharing** 🡪 Click **Share this folder**.
3. Click **Permissions** 🡪 Click **Full Control**.
4. Click OK twice to get back to Properties.
5. Click the **Security** tab.

Notice in the box that Authenticated Users, SYSTEM, Administrators, and Users all have access to the C:\Medical folder. When you select a user group, the type of permissions assigned to that group appears in the Permissions area. Table 17-1 explains the more significant types of permission. Note that the Administrators group has full control of the folder. Also notice the checks under Allow are dimmed. These permissions are dimmed because they have been inherited from the parent object. In this case, the parent object is Windows default settings.

### Permission Levels for Files and Folders

|  |  |
| --- | --- |
| **Permission Level** | **Description** |
| **Full control** | Can read, change, delete, and create files and subfolders, read file and folder attributes, read and change permissions, and take ownership of a file or folder. |
| **Modify** | Can read, change, and create existing files and subfolders. Can delete the folder or file but cannot delete subfolders and their files. Can read and change attributes. Can view permissions but not change them. Cannot take ownership. |
| **Read & execute** | Can read folders and contents and run programs in a folder. (Applies to both files and folders.) |
| **List folder contents** | Can read folders and contents and run programs in a folder. (Applies only to folders.) |
| **Read** | Can read folders and contents. |
| **Write** | Can create a folder or file and change attributes but cannot read data. This permission is used for a drop folder where users can drop confidential files that can only be read by a manager. For example, an instructor can receive student homework in a drop folder. |

1. To remove the inherited status from these permissions so you can change them, click Advanced. The Advanced Security Settings box appears.
2. Click **Disable inheritance**. The Block Inheritance box appears. To keep the current permissions, but remove the inherited status placed on them, click **Convert inherited permissions into explicit permissions on this object**. Click Apply.
3. Close the Advanced Security Settings box.
4. In the Medical Properties box, notice the permissions are now checked in black, indicating they are no longer inherited permissions and can be changed. Click Edit to change these permissions.
5. The Permissions box opens. Select the Authenticated Users group and click Remove. Also remove the Users group. Don’t remove the SYSTEM group, which gives Windows the access it needs. Also, don’t remove the Administrators group. You need to leave that group as is so that administrators can access the data.
6. To add a new group, click Add. The Select Users or Groups box opens. Under Enter the object names to select, type Medical, and click OK. The Medical group is added to the list of groups and users for this folder.
7. Using the check box under Permissions for Medical, check Allow under Full control to give that permission to this user group. Click OK twice to close the Properties box.
8. Change the permissions of the C:\Financial folder so that Authenticated Users and Users are not allowed access and the Financial group is allowed full control.

# Step 3: Test, Set Share Permissions, and Go Live

It’s now time to test your security measures. Do the following to test the NTFS permissions and implement your shared folders:

1. Test a user account in each user group to make sure the user can read, write, and delete in the folder he needs but cannot access the other folder. Put some test data in each folder. Then sign in to the system using an account you want to test and try to access each folder. When you click Continue, entering an administrator password in the resulting UAC box gives you access.
2. Now that NTFS permissions are set correctly for each local and network user, you are ready to allow access over the network. To do that, both NTFS and share permissions must allow network access. (Share permissions apply only to network access, not local access.) Best practice is to allow full access using share permissions and restrictive access using NTFS permissions. The most restrictive permissions apply. To allow full access using share permissions, click the Sharing tab of each folder’s properties box, and click Advanced Sharing.
3. In the Advanced Sharing box, if it is not already checked, check Share this folder. Then click Permissions. To add a new group, click Add. The Select Users or Groups box opens. Under Enter the object names to select, type Everyone and click OK. The Everyone group is added to the list of groups and users for this folder.
4. With Everyone selected, check Allow under Full control to give that permission to the Everyone user group. Click OK twice and then close the Properties box.
5. Now that you have the security settings in place for one computer, go to each computer on the network and create the user accounts that will be using this computer. Then test the security and make sure each user can access or cannot access the \Financial and \Medical folders as you intend.
6. When a user is denied access to a network resource, there is no opportunity to provide access from this screen
7. To access shared folders, you can drill down into the Network group in File Explorer or Windows Explorer. Another method is to type the computer name—as in \\Win8—in the address bar of the Explorer window.
8. After you are convinced the security works as you want it to, copy all the company data to subfolders in these folders. Check a few subfolders and files to verify that each has the permissions that you expect. And don’t forget to put in place on the file server the backup procedures you learned about in the chapter, “Maintaining Windows.”
9. **Insert a screenshot logged in as Carlos accessing the Financial folder:**

Click or tap here to enter text.

1. **Insert a screenshot logged in as Lucas accessing the Medical folder:**

Click or tap here to enter text.

# Map a Network Drive and Network Printer

To set up a network drive to a share, follow these steps:

1. On the remote computer that will use the network drive, open File Explorer. In the left pane, Right Click Network. Click Map network drive.
2. The Map Network Drive dialog box opens. Select a drive letter from the dropdown list.
3. Click the Browse button and locate the shared folder or drive on the host computer. Click OK to close the Browse For Folder dialog box, and click Finish to map the drive. The folder on the host computer now appears as one more drive in Explorer on your computer.
4. Use this method to map a network drive for Carlos to Financial.
5. **Insert a screenshot:**

Click or tap here to enter text.

1. Use this method to map a network drive for Lucas to Medical and Financial.
2. **Insert a screenshot:**

Click or tap here to enter text.

Note: When mapping a network drive, you can type the path to the host computer rather than clicking the Browse button to navigate to the host. To enter the path, in the Map Network Drive dialog box, use two backslashes, followed by the name of the host computer, followed by a backslash and the drive or folder to access on the host computer. For example, to access the Projects folder on the computer named Win8, enter \\Win8\Projects and then click Finish.

1. If a network drive does not work, go to the Network and Sharing Center, and verify that the network connection is good. You can also use the net use command to solve problems with mapped network drives.
2. A host computer might be in sleep mode or powered down when a remote computer attempts to make a mapped drive connection at startup. To solve this problem, configure the host computer for Wake-on-LAN.

# Connect and Share a Printer

Recall from the chapter, “Optimizing Windows,” that you can connect a network printer to a server and the server can share the printer on the network. The Print Management console can be used to manage all shared printers on the network from a single workstation. You can also map a network printer directly to your computer, eliminating a print server or printer sharing from the process. Here’s how:

Setup a fake printer for this part of the lab.

1. Open the Control Panel in Classic view and click **View Devices and Printers**. Click **Add a printer**. Click **The printer I want isn’t listed.**
2. Select **Add a local printer** and select **LPT1.** Choose any printer listed.
3. Right Click the printer, choose Printer Properties. Click the Sharing Tab. Click Share this printer.
4. **Insert a screenshot:**

Click or tap here to enter text.

1. On the other computer, Browse the Network to the other computer. Double click the shared printer. This should automatically install the printer.
2. **Insert a screenshot:**

Click or tap here to enter text.

1. You can remove the printer when you are done with the lab.

## Assignment Submission

Attach this completed document to the assignment in Blackboard.