

Lab 8.1.3 Securing Local Data and Transmitted Data

Objectives

- Use Windows New Technology File System (NTFS) permissions to secure local data on a Windows XP Professional edition computer.
- Use Internet Explorer 7 to access secure web sites.

Background / Preparation

This is a 2-part lab. The parts can be performed together or independently.

Part 1 – Securing local data

In part 1 you will secure data on a computer using the NTFS file system.

Scenario: A couple of users at a small business share a workstation. Confidential data is stored locally on the hard drive of the computer. You have been asked to help protect the data and secure it so that only one local user can access the data. Using NTFS permissions, you will secure that local data.

There are two local users, Bob and Joe. Bob will require Modify access to a folder called “Bob’s Files” located below a folder called “Local Data on the C drive.” Joe will not have access to “Bob’s Files.”

Part 2 – Identifying a secure communication channel when transmitting data over the Internet

In part 2 you will use Internet Explorer to identify secure and unsecure web sites.

Scenario: You are in charge of educating end users in a small business on secure access to web sites. You will need to educate the end users on how to recognize a legitimate secured website versus an illegitimate secured website.

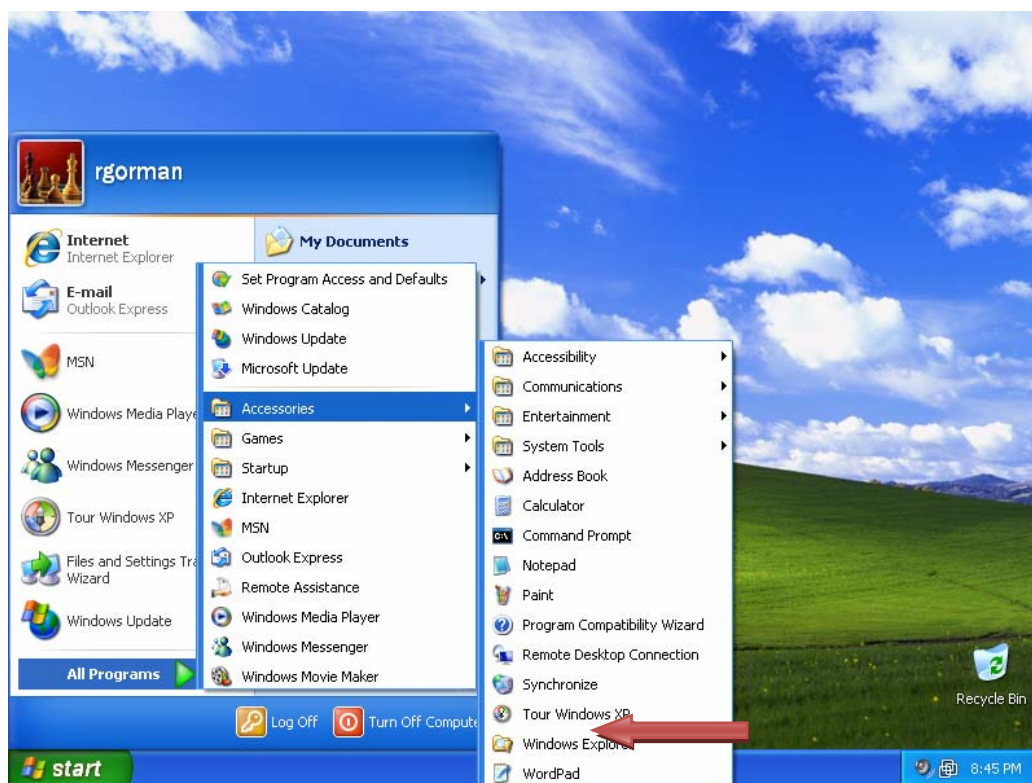
The following resources are required:

- Windows XP Professional computer with administrative access
- NTFS File System on the computer and Simple File Sharing turned off (under the Folder Options of Windows Explorer.)
- User accounts preconfigured for users Bob and Joe
- Internet connectivity

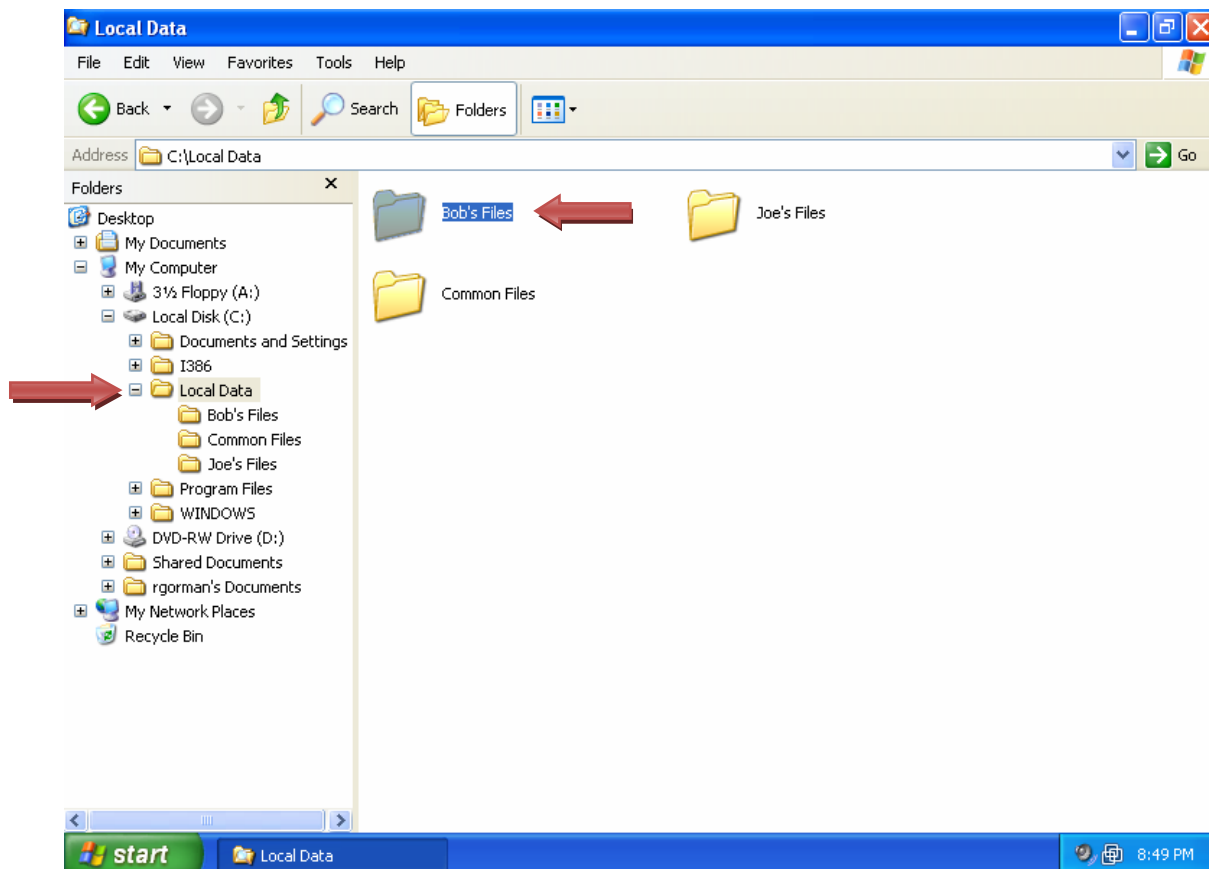
Part 1 – Securing local data

Step 1: Secure Bob's Files folder

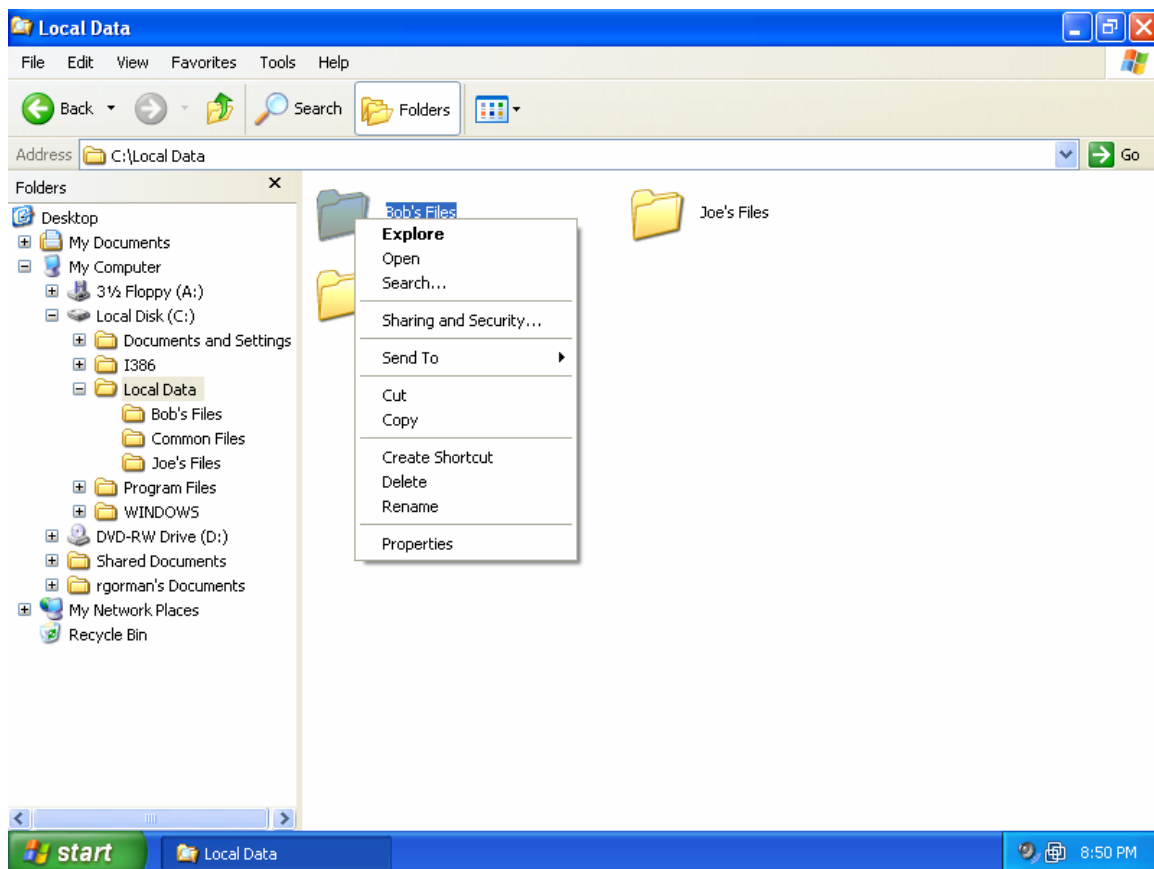
- Log in to the Windows XP computer as administrator.
- From the **Accessories** menu, launch Windows Explorer.



- c. Use Windows Explorer to create a folder on Local Disk (C:) called **Local Data**. From the **File** menu, click **New**, and then click **Folder**.
- d. Click the **Local Data** folder and then right-click in the open area at the right side of the screen. Click **New** and then click **Folder** and create a folder called **Bob's Files**. Repeat this process to create the folders **Common Files** and **Joe's Files**.
- e. Navigate to the **Local Data** folder, where you can see the **Bob's Files** folder.

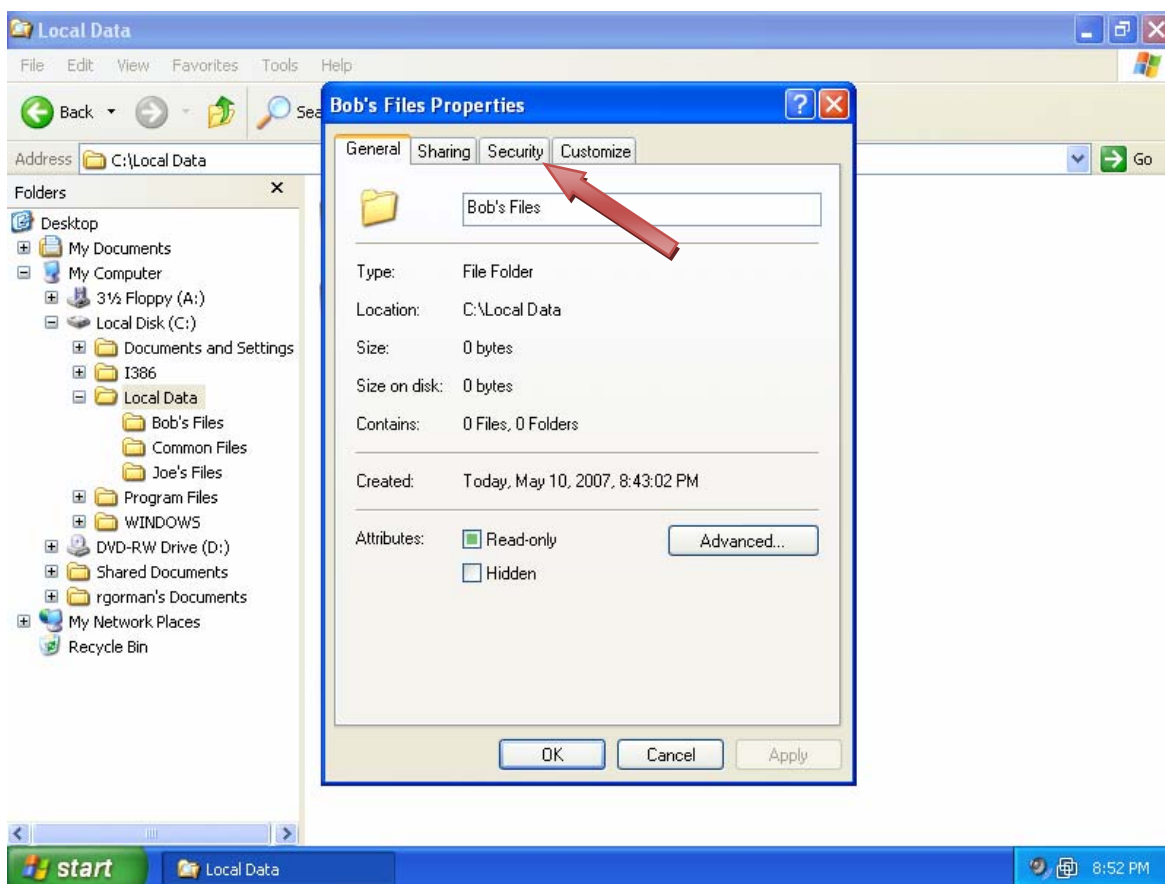


- f. Right-click the **Bob's Files** folder and choose **Properties**.

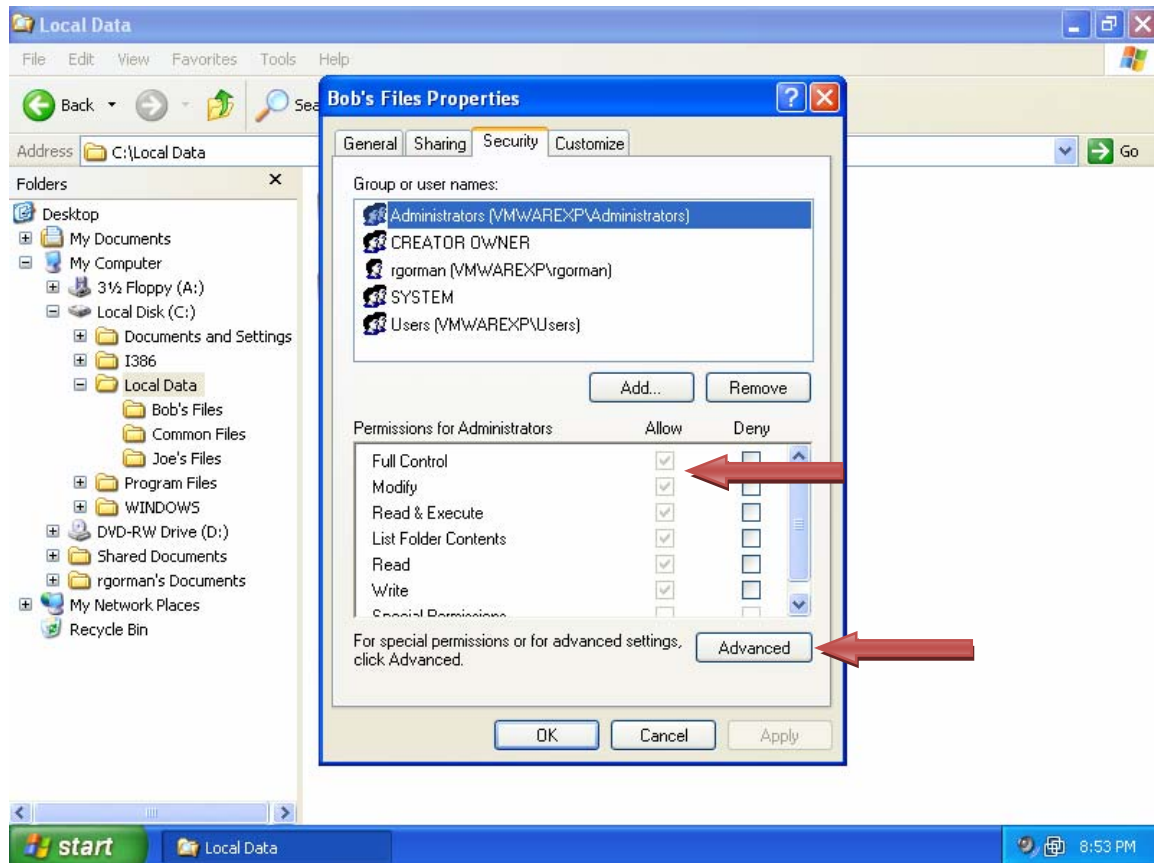


- g. From the **Bob's Files Properties** dialog box, click the **Security** tab.

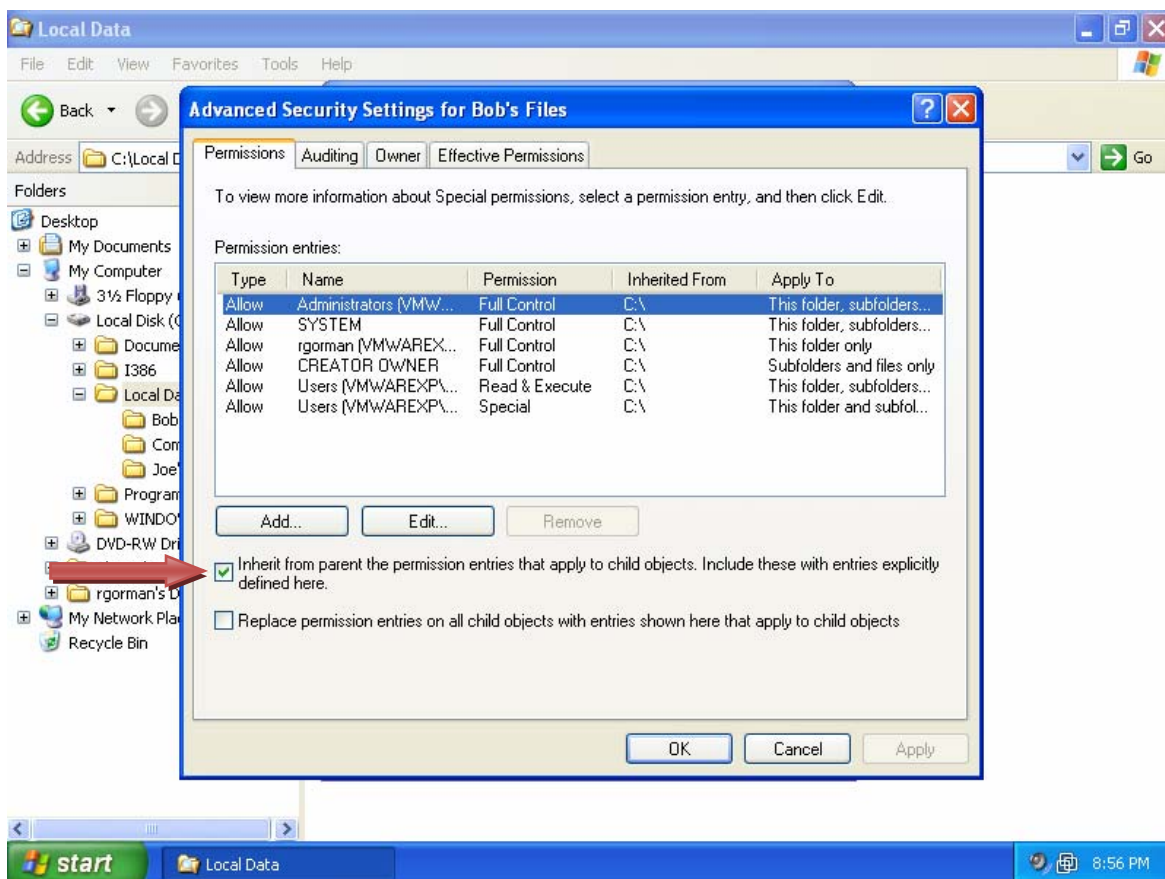
NOTE: You must be working on a drive that has the NTFS file system installed; otherwise, you will not see the **Security** tab.



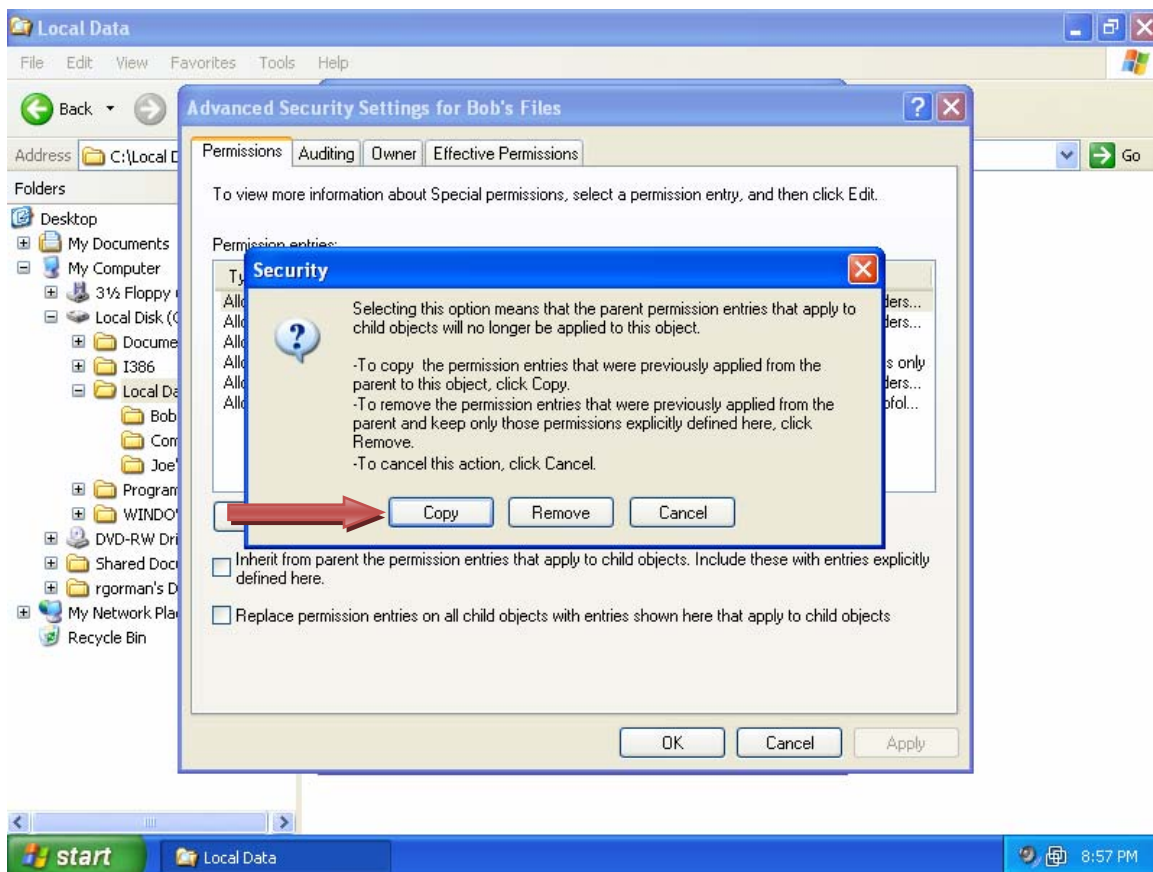
- h. Notice that the permissions are dimmed and not modifiable. This restriction is due to the permissions that were inherited from a parent folder. To secure the folder, you will need to disable the inherited permissions. From the **Security** tab, click the **Advanced** button.



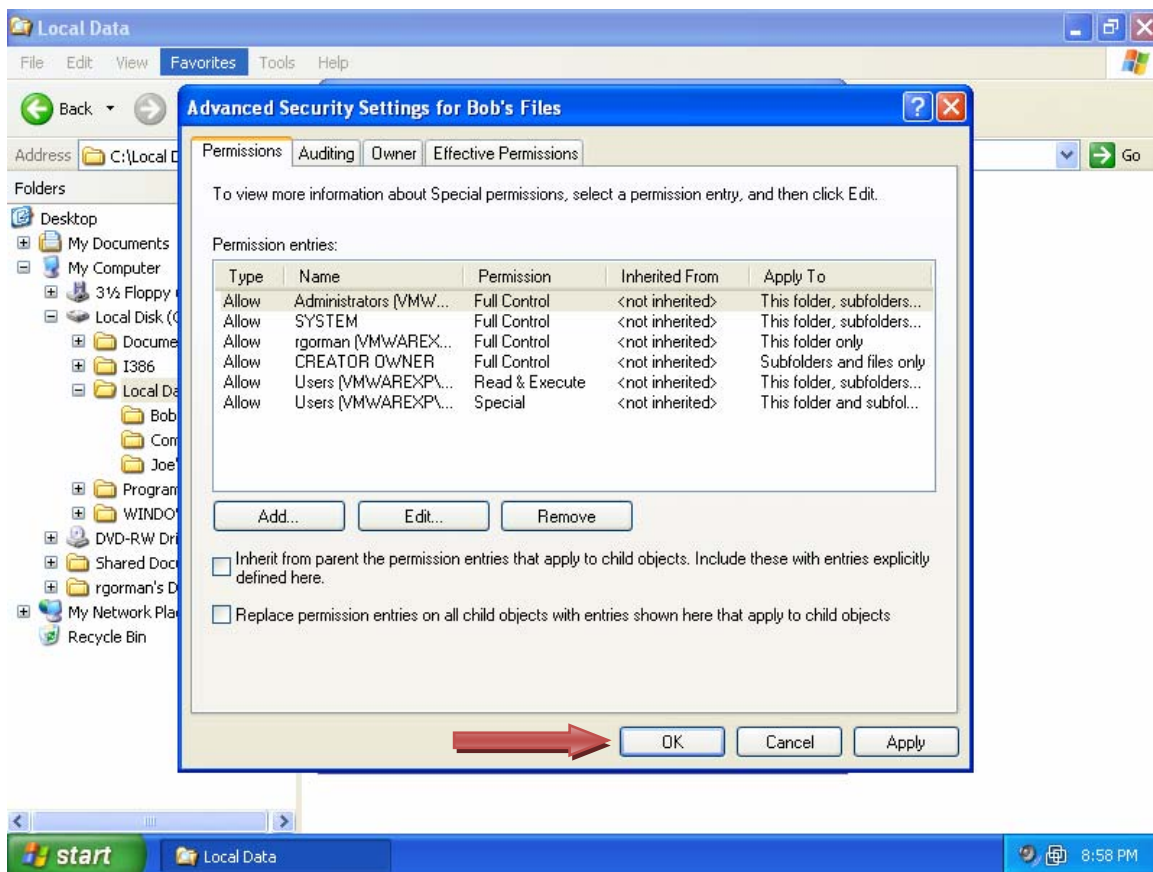
- i. Uncheck the check box next to **Inherit from parent the permission entries that apply to child objects.**



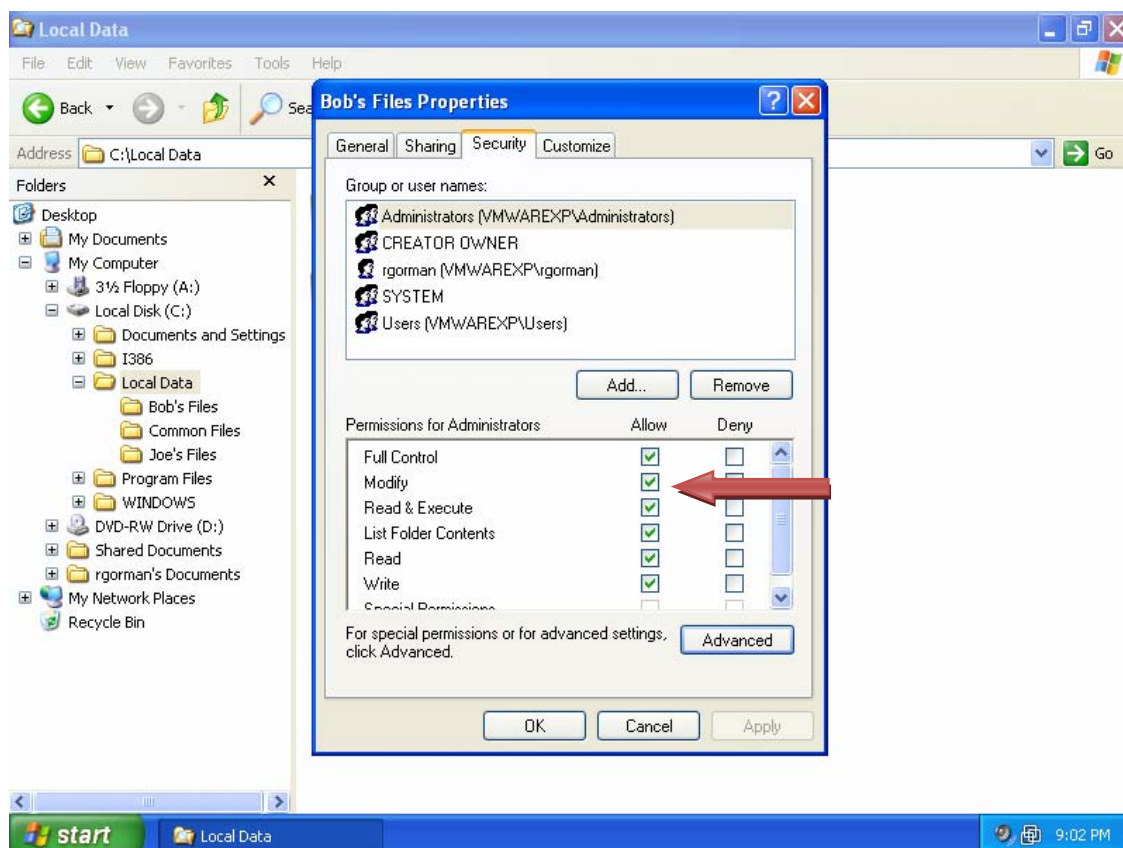
- j. Click **Copy** to retain the existing permissions.



k. Click **OK**.

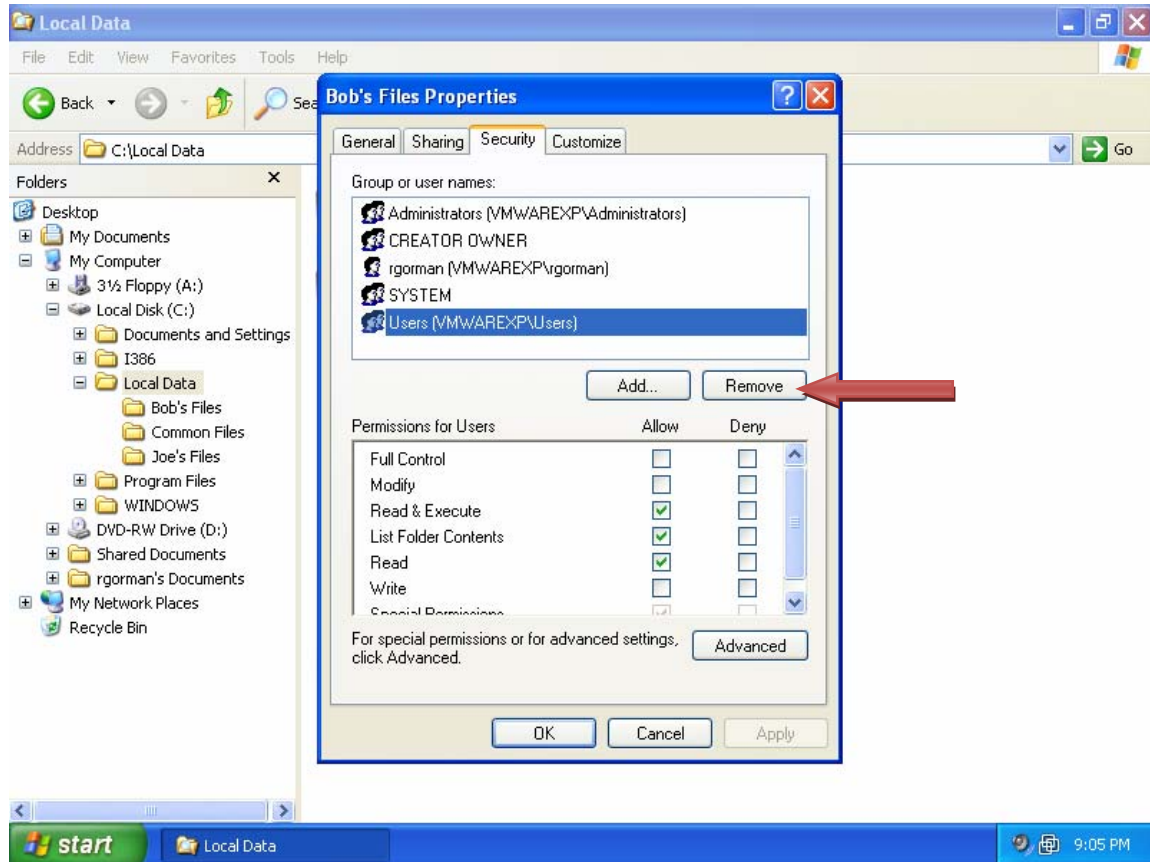


Now that inheritance is turned off, you are able to modify the permissions.

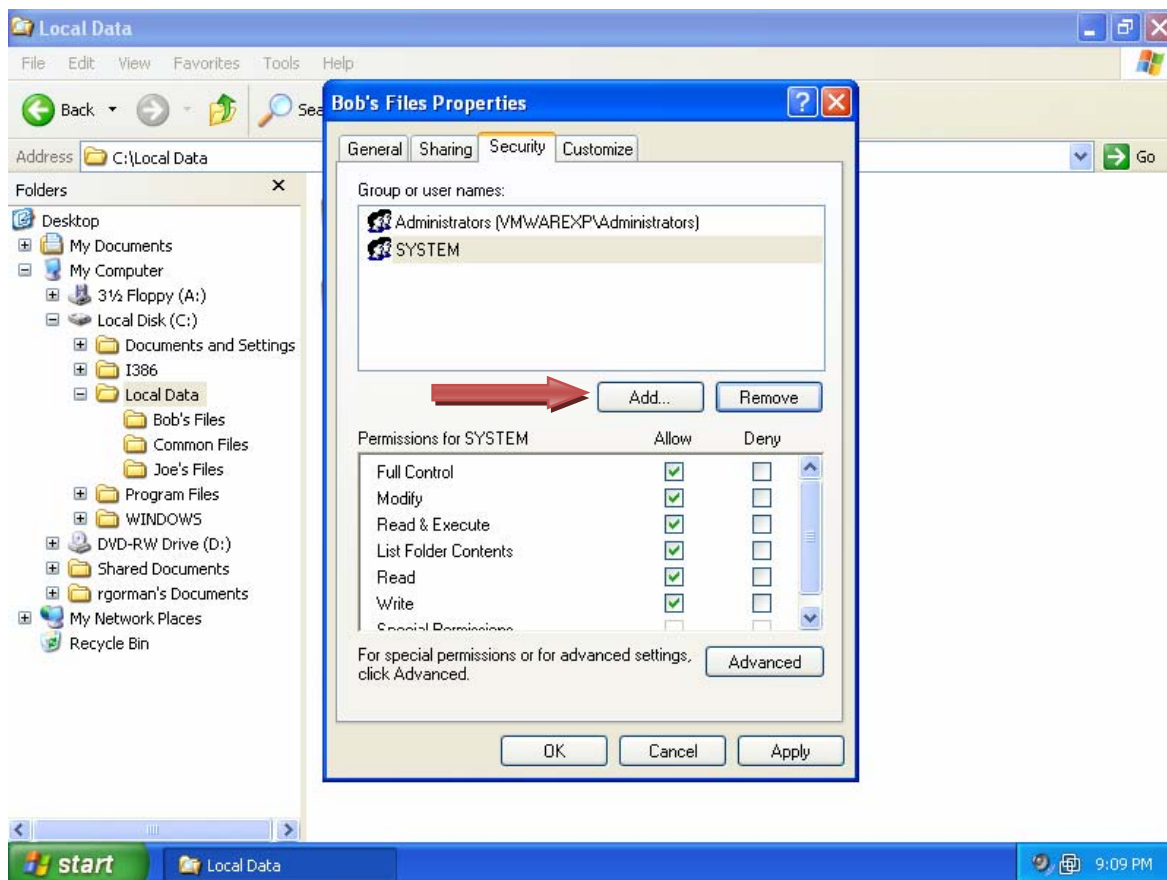


- I. Select the **Users** group and click **Remove**. Continue to select the other remaining users and groups, except for Administrators and SYSTEM, and click **Remove**.

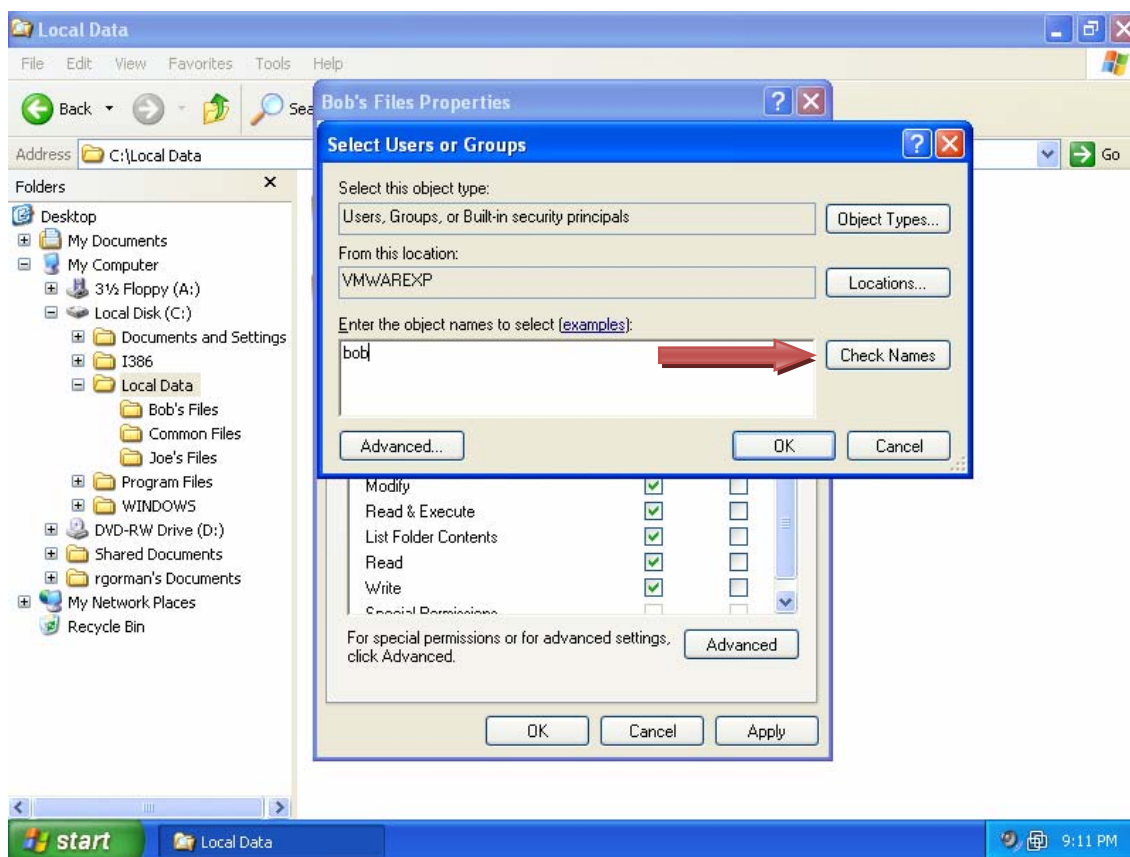
NOTE: Always grant the SYSTEM and Administrators groups Full Control access to directories and files to ensure that files can be backed up, recovered, and scanned properly by the computer system.



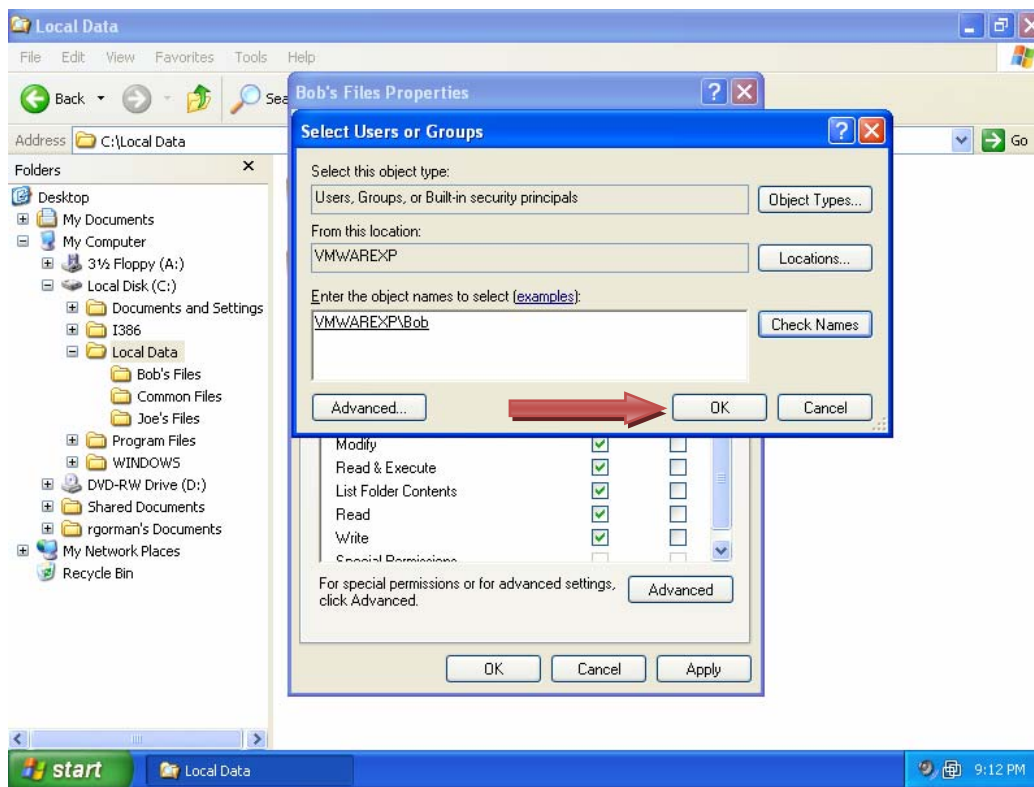
m. Now add Bob to the list. Click **Add**.



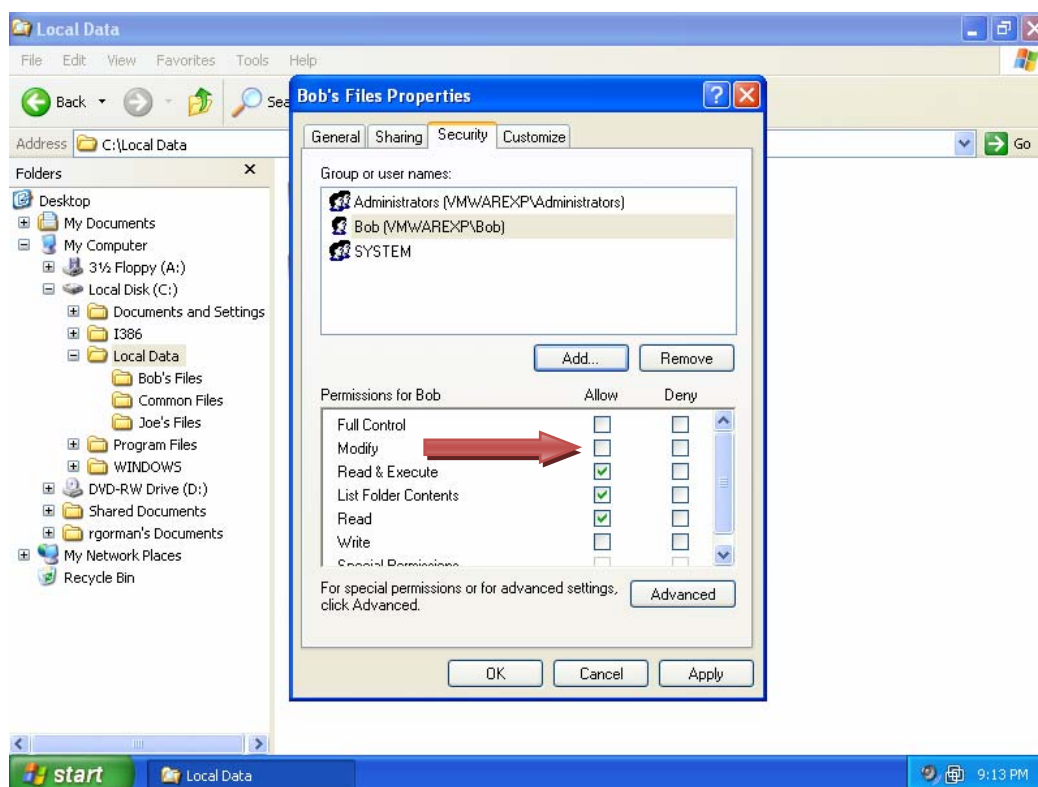
- n. Type **Bob** in the text box and click the **Check Names** button to verify his account.



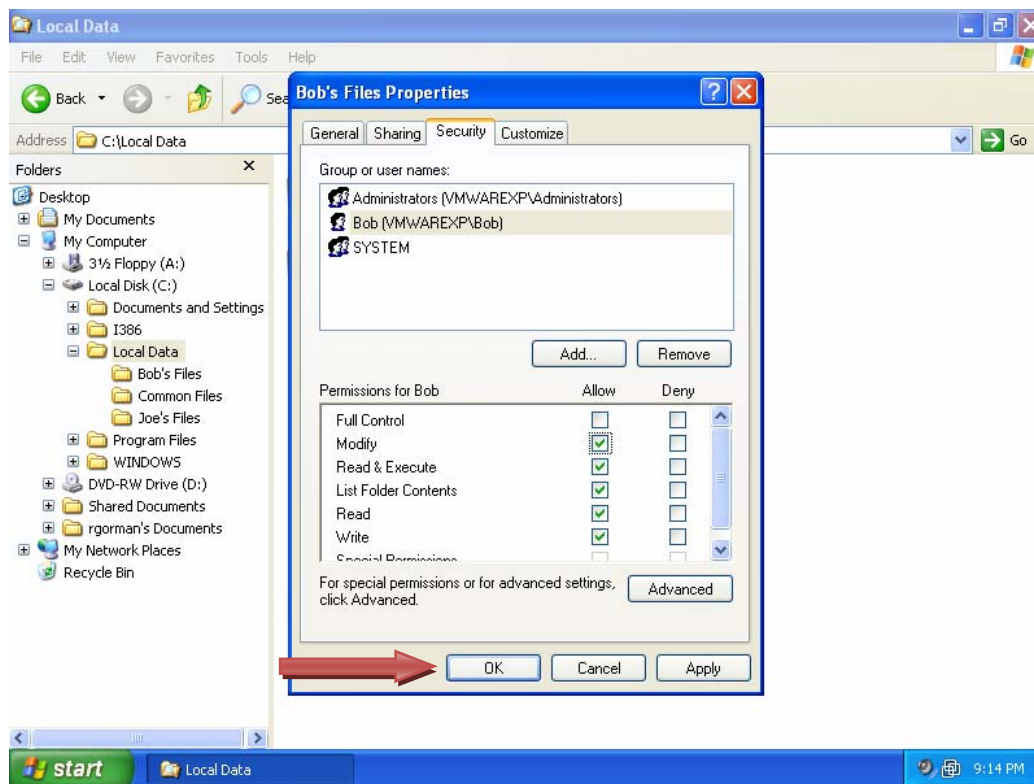
- o. Now that Bob has been verified, click **OK**.



- p. Bob is now added to the list. Notice that he currently has the Read & Execute, List Folder Contents, and Read permissions. Because Bob will need to write new files and delete existing files, grant Bob Modify permission. Check the check box in the **Allow** column next to **Modify**.

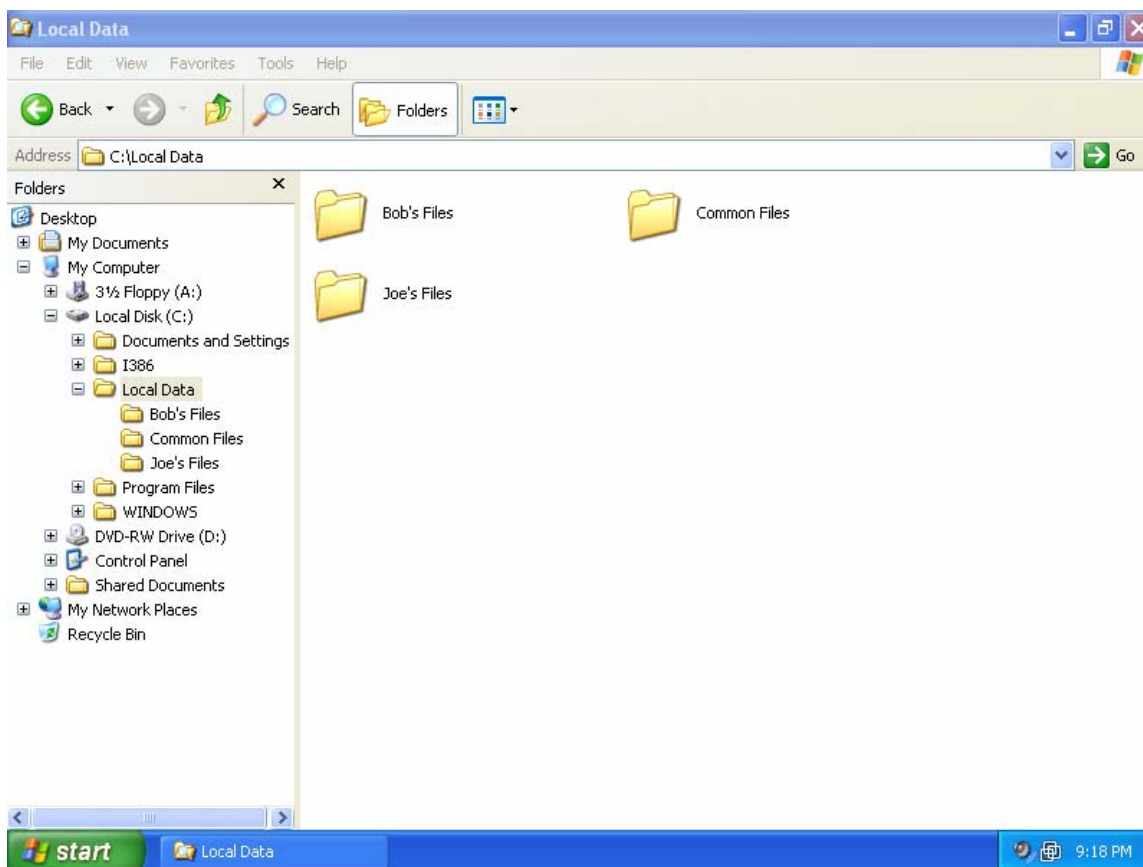


- q. Now that Bob has been granted Modify permission, click **OK** to set the security.

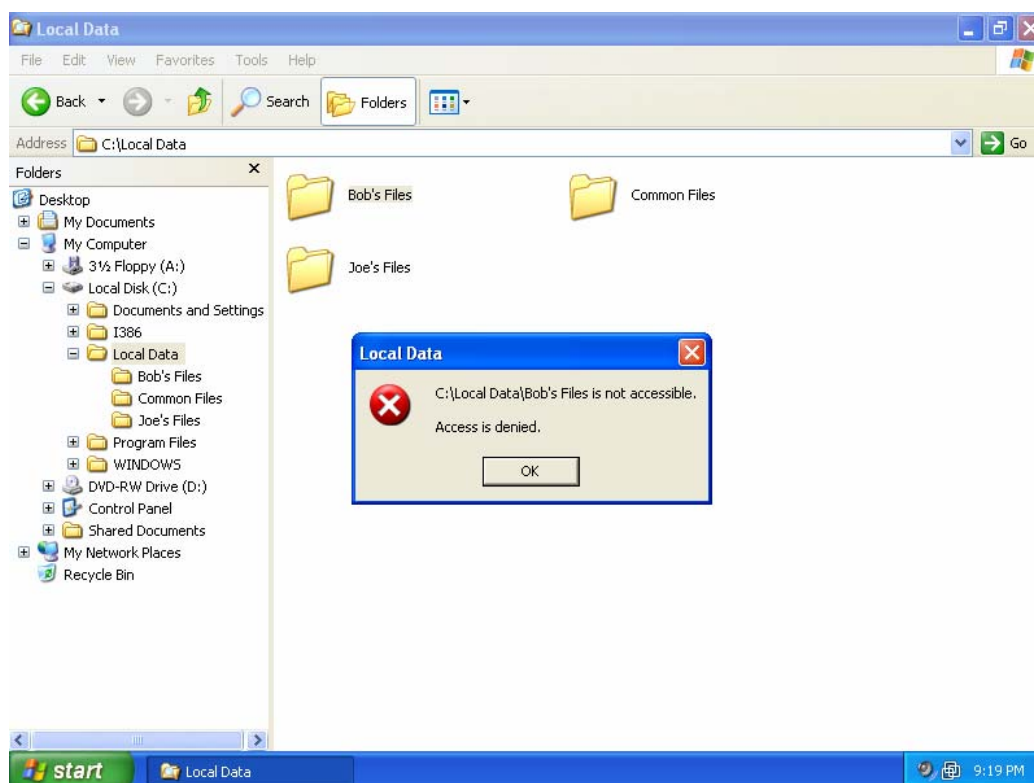


Step 2: Test Joe's access to Bob's Files

- a. Log in to the local PC as Joe and try to access the **Bob's Files** directory.



- b. Notice a popup dialog box indicating that Joe does not have permission to access these files. Because Joe does not have Administrative access to the PC, he is prevented from gaining access to **Bob's Files**.



Part 2 – Identifying a secure communication channel when transmitting data over the Internet

Step 1: Identify a secure web page

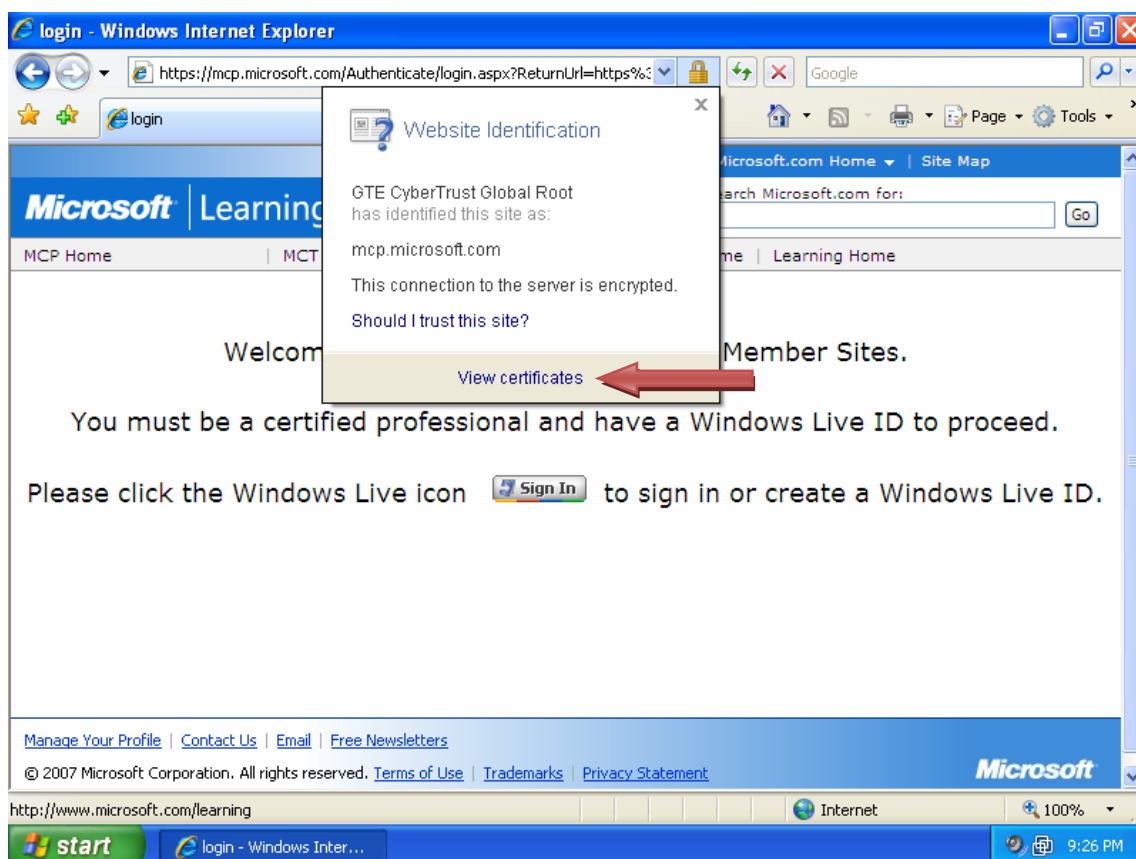
- a. Launch Internet Explorer and navigate to <http://www.microsoft.com/learning>. This site is a typical unsecured page. Click the **MCP Members Site** link.



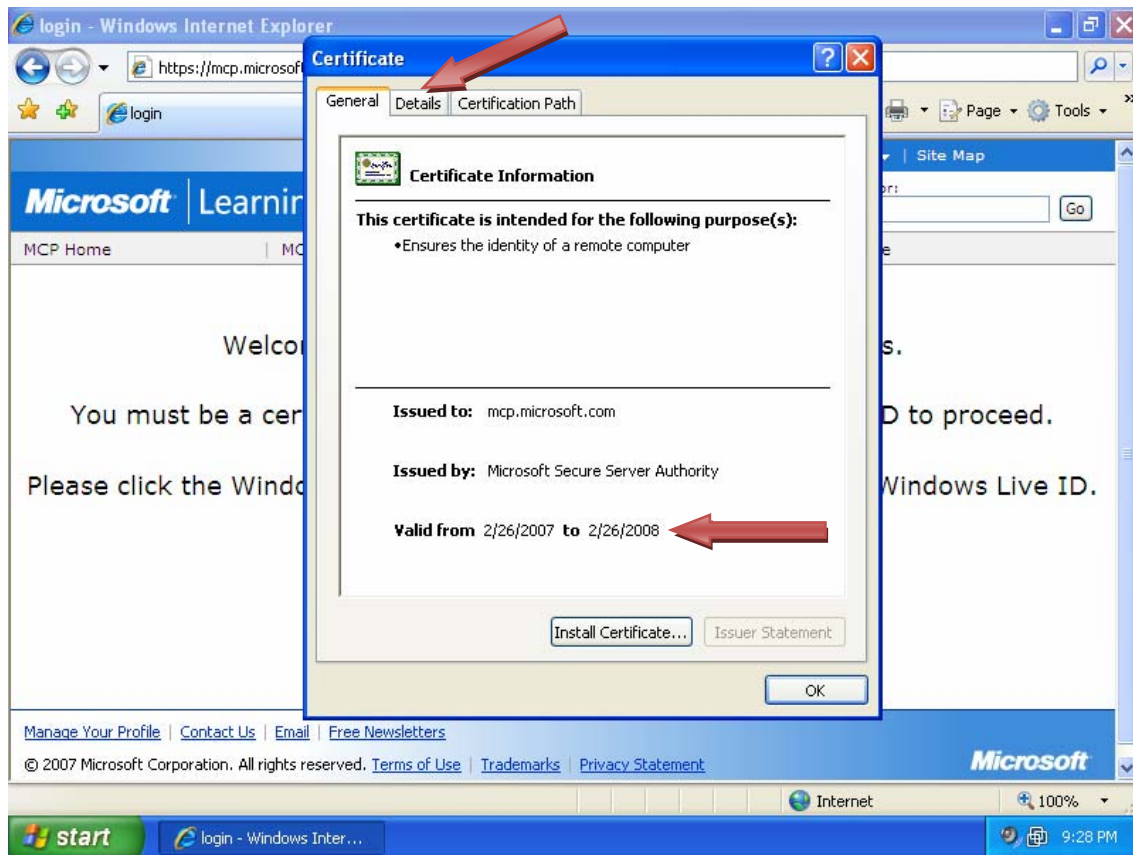
- b. Notice that the URL changed from HTTP to HTTPS. HTTPS is the secure version of HTTP and uses SSL for its security. Notice also that there is a **lock** icon located to the right of the URL. The presence of the **lock** icon indicates that the site is secure. Click the **lock** to see more information about the secure site.



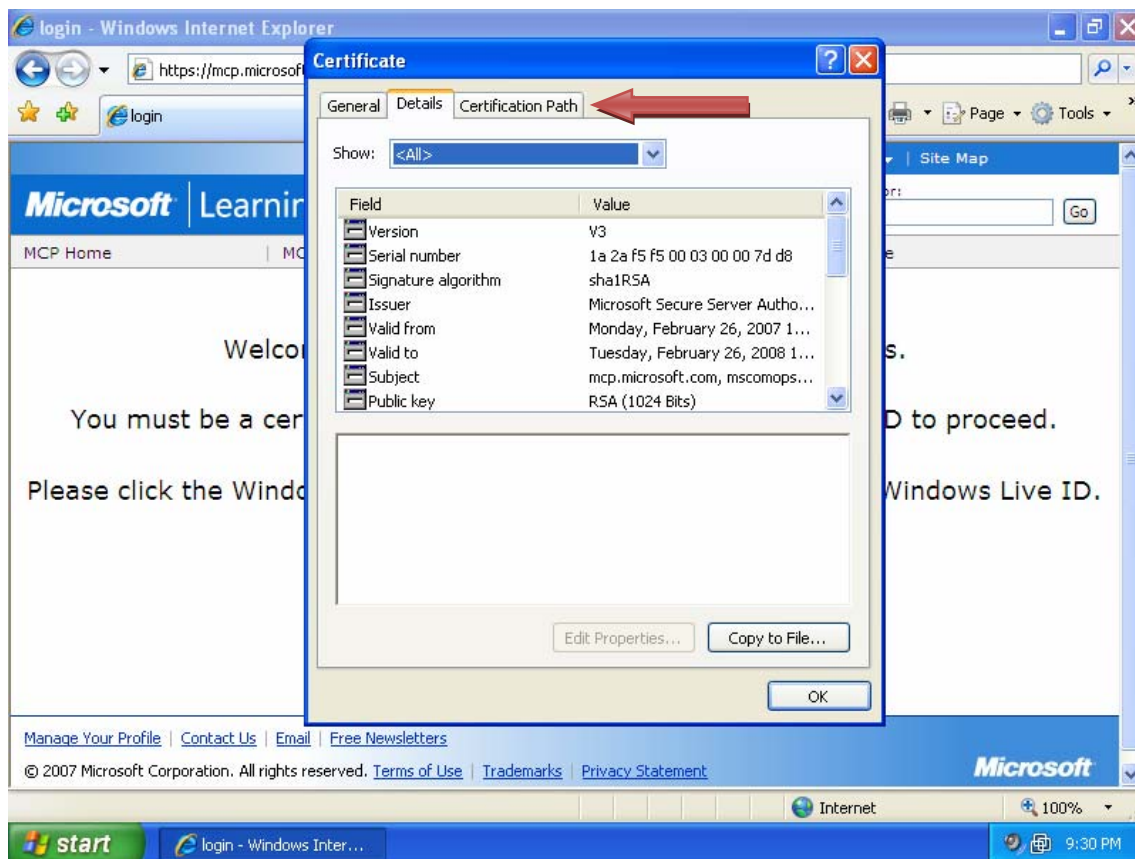
- c. The popup window displays information about the issuer of the security certificate for this website. It also indicates that the connection to that server is secure. Click the **View certificates** link at the bottom of the popup window.



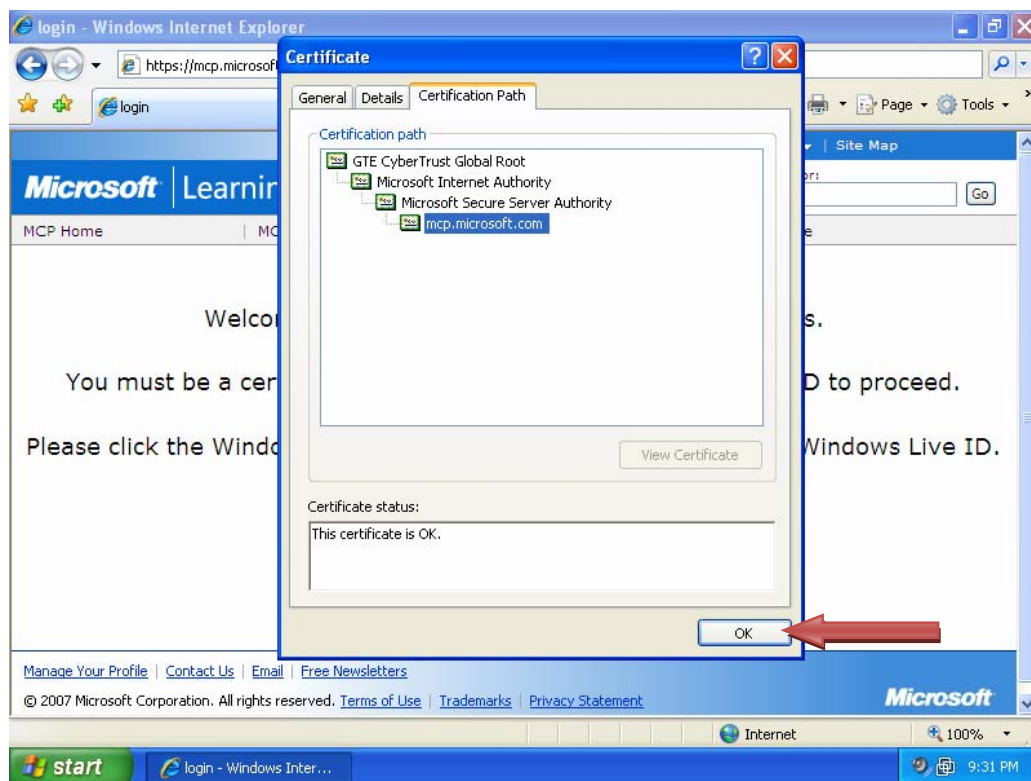
- d. The Certificate window opens and displays the certificate that has been installed on the web server to allow it to use SSL. Notice the **Valid from** date range at the bottom. Certificates are only valid for a specific period of time, and then they must be renewed. The renewal process ensures that web server administrators continually validate their servers with the certificate authority who issued the certificate. Click the **Details** tab for more information.



- e. The **Details** tab shows information about the certificate. Click the **Certification Path** tab.

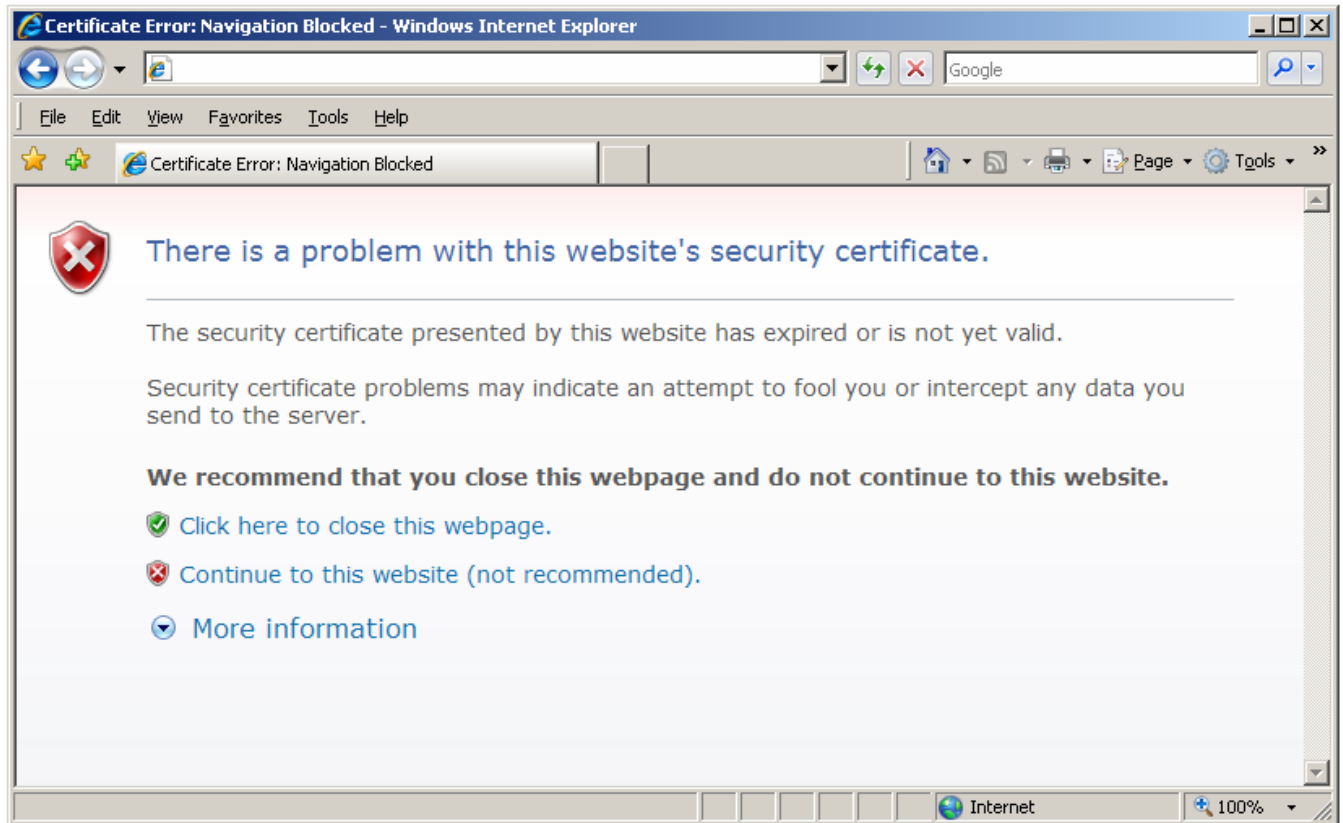


- f. The **Certification Path** tab displays a hierarchical list of certification authorities that have been authorized to issue the web server certificate. Click **OK** to close the Certificate window.



Step 2: Examine secure access to an untrusted source warning

- a. If the security certificate presented by a website is not from a trusted authority, Internet Explorer displays the screen shown below to alert you to the fact that there is a problem. It gives you options for closing the webpage or continuing to the website.



- b. Unless you know the website to be legitimate you may not be able to trust the server or the content it provides. If you navigate to the certification path, as previously described, you will not see a list of trusted certification authorities. You may be working with secure (HTTPS) website but one that is self-certified and not certified by approved authorities.