# Windows Server Intro – Users and Groups

# Section 1 – Domain Users

Machines:

* 1 Windows Server 2016
* 1 Windows 10 Client Machine

## Part 1: Domain User Accounts

In order **to access Active Directory network resources,** and computers that are members of an Active Directory domain, **users must authenticate** (prove their identity) **with a domain controller** that holds their account information. This means they must provide a username and the appropriate password for that username or they can’t access domain computers and their resources. The usernames must be the usernames associated with domain user accounts held in the domain controller’s Active Directory database. Local user accounts, even if they exist on domain joined computers, are not stored in Active Directory and therefore cannot be used to authenticate with a domain controller or access resources within the network.

Domain user accounts are created on domain controllers and are held within that domain. A user can log in at any computer in any domain in the forest, but the user account authentication information must be accepted and approved by a domain controller in the user’s home domain. This makes the domain the Authentication Boundary in Active Directory.

Domain user accounts are created by authorized administrative accounts and can be done manually or automated such as a PowerShell script. In this exercise you’ll use the manual method of account creation. While a username can be anything, it is common practice to have a naming policy convention in place. One very common naming policy is for a username to be a concatenation of the user’s first initial and last name. This is by no means required, nor is it the only useful naming convention, but is the one that will be used throughout these labs.

In the next steps you will examine the domain accounts that were converted from local account during promotion to a domain controller.

* If not already logon to **the server** with the **Administrator** account. When Server Manager starts, click on the Tools menu at the top and select Computer Management. Look for Local Users and Computers to verify that the SAM database has been disabled and that the Active Directory database must be used for user accounts.
* Close Computer Management.
* Click on the Tools menu again and select Active Directory Users and Computers (ADUC)
* Expand the name of your domain in the left pane, then left click once on Users.

In the right pane you should be able to find your JDoe account and the Student accounts that you created as local users. These accounts were converted to domain accounts in the promotion process.

* Right click on the **jdoe** account and select Properties (or double click on it).

Graphical user interface, text, application

Description automatically generated

* In **jdoe Properties**, click on the **Member of** tab and record what groups the account is a member of.

**Name Active Directory Domain Services Folder**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Now check the membership of the **client local** account and record what you see.

**Name Active Directory Domain Services Folder**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

In the next section you will create a new, personal administrative account that you will use for most of the work in the rest of this and the following guides.

* Still in **Active Directory Users and Computers (ADUC)** right click on the **Users icon** in the left panel and select **New** and then **User** from the cascading menus.
* Put in your first and last name and give yourself a logon name. It is suggested that you use your first initial and last name for the logon name, but you don’t have to.

Graphical user interface, text, application, email

Description automatically generated

* You should record the password below for reference in case you forget it later. Be sure to UNCHECK ‘[ ] User much change password at next login’ and also CHECK ‘ [X] Password never expires’.

**Username:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Password**:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* After the account has been created, locate it in the right pane in ADUC and double click on it.
* Click on the Member of tab and add **Domain Admins** to the membership. This will give you complete administrative control of the domain. When you have finished with this you should see that your new account is a member of two groups. Fill in the lines below.

**Name Active Directory Domain Services Folder**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Log off as Administrator and log on with your new personal administrative account.

Unless specified otherwise, you should always log onto your server with your personal domain admin account.

In the next steps you will set your new Domain Controller to allow other computers on the network to see it and access it.

* On **your server** in Server Manager use the Tools menu to select Services.
* Locate **Function Discovery Resource Publication**, double click on it and set it to **Automatic** startup type and then **Start** it. (There are two different Function Discovery services, be sure you have selected the correct one.)
* Repeat this process of setting Automatic startup and starting the SSDP Discovery service and the UPnP Device Host service.

Next you will verify that you can browse your network and see both of your computers.

* On your client, open File Explorer there and verify you can see both your server and the client PC under Network. *Do not continue until you can browse to both machines.*

In the next steps you will join the WIN10 computer to the domain

* On **the client** open the IP properties for the network adapter as you did when you set the static IP address.
* Change the Preferred DNS server address to the IP address of **the server**.
* Delete any Alternate DNS server entry.
* Close all the open windows.
* Open File Explorer, right click on This PC in the left pane and select Properties

Graphical user interface, application

Description automatically generated

* In the System windows, click on Advanced system settings in the left pane.
* Click on the Computer Name tab, then click on the Change button
* In the Computer Name/Domain Changes windows, select the More button
* Put your domain name in the box for Primary DNS suffix for this computer. You are doing this so that when you try to join this computer to the domain, it will try to register with the correct DNS zone..
* Click OK and close the windows. You may be required to reboot **your client** after changing the DNS suffix.
* If, after rebooting, log back onto **your client** as your original local account.
* Return to the Computer Name windows (This PC / Properties / Advanced System Settings / Computer Name / Change).
* Click the radio button for Domain under Member of and put in your domain name, then click OK

Graphical user interface, text, application, email

Description automatically generated

* You will then be asked for domain credentials that have the rights to add a computer to the domain. If you correctly added your personal account to the SRV16 Domain Admins group, you can use those credentials. A few seconds after entering the credentials you should get a screen welcoming you to the domain. After you click OK you will have to reboot again.
* After restarting, the system will offer to allow you to log into the client with a local account. If you do this you will not be able to access the domain properly. You can tell it is offering a local logon by the NetBIOS name of your computer rather than the domain at the logon screen.

Graphical user interface, application

Description automatically generated

* Click on the arrow, select Other User and then log on with your personal domain admin account. Notice that just below the password box you will see a Sign in to field.

Once you have logged into **the client** with domain credentials you will see that the very first logon takes longer because Windows 10 realizes this account hasn’t logged into this computer before.

* Go to the Desktop and open File Explorer (folder icon on the Taskbar).
* If you get the message about Network Discovery, Click to change

Graphical user interface, text, application

Description automatically generated

* After you have **turned on Network Discovery**, go to the Network icon and click on the **the server.**
* Open the **<ServerName>-Share** folder, open the TestData file, add the date and save the document.

Creating User Accounts

* Now on the Server, create domain user accounts (using Active Directory Users and Computers on the server) for each of these employees of your organization and use a consistent naming convention of first initial and last name; ex: **FLastName**. You will use these accounts in later labs. For simplicity, give them all the same password, requiring them to create a new one that meets complexity on their first login.

Here is an example list. This can be entered into a spreadsheet for use as a CSV file in powershell to expedite the process.

**Full Name Username Description**

Florence Horvath FHorvath HR Manager

Cotton Malone CMalone HR Staff

John Rebus JRebus HR Staff

Gabriel Allon GAllon Accounting Department Manager

Jeffrey Archer JArcher Accounting Department Staff

Jesse Stone JStone Accounting Department Staff

Steve Berry SBerry Marketing Department Manager

David Baldacci DBaldacci Marketing Department Staff

Jack Reacher JReacher Marketing Department Staff

Jeffrey Deaver JDeaver MIS Senior Administrator

Linda Fairstein LFairstein MIS Administrator

Virgil Flowers VFlowers MIS Help Desk Staff

Emma Peale EPeale MIS Help Desk Staff

Robert Parker Rparker Senior Editor

Claudia Plum CPlum Editorial Staff

Ian Rankin IRankin Editorial Staff Intern

Cassiopeia Vit CVit Editorial Staff Intern

## Part 2: Preparing Global Groups

As previously demonstrated, users gain access to the Active Directory network by authenticating with valid domain user accounts. Once a user authenticates, the user will need to access resources within the domain such as files, folders and even applications. To provide security in the domain, these resources are protected by Permissions which are held in Access Control Lists on each protected resource. While it is possible to provide access to resources by entering individual user account information into each Access Control List, this would be prohibitively inefficient except in the smallest of Active Directory network. To make access control efficient, permissions are granted to entities called Groups with have user accounts as members. As will be seen, it is far simpler to grant a specific level of access (permission) to a large number of users by employing groups than assigning permissions to each individual account.

While the concept of groups is very simple (containers holding membership lists) the proper use of different types and scopes of groups can be confusing. The two different types of groups (Security and Distribution) are easily dealt with: Only Security groups can be used for assigning permissions, so those are they only type we will consider here. The real difficulty come in the understanding and proper use of the three scopes that are possible within the Security group type, Global groups, Domain Local groups and Universal groups.

* **Domain Local** Groups

Protects resources within the local domain with **permissions**

* **Global** Groups

Collect **users** within the local domain

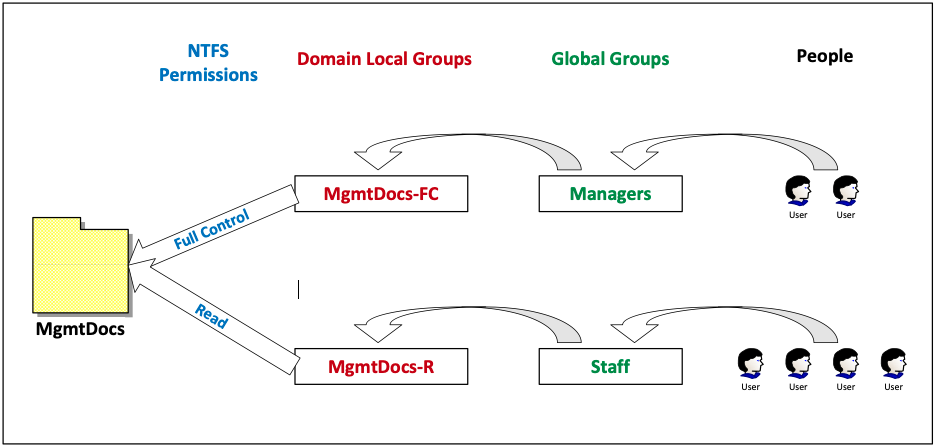
* **Universal** Groups

Collect **global groups** from different domains in the forest

* **System** Groups (Special Identities)

Collect **users** based on authentication method or status

Microsoft’s recommended best practice for using groups is represented by the acronyms **A->G->DL->P** and **A-G-U-DL-P**. For single domain forests and even many multiple domain forests, the A-G-DL-P is the only form needed. User Accounts (A) are members of Global groups (G) which are members of Domain Local groups (DL). Permissions (P) to access resources are given only to Domain Local Groups. In larger forests where Universal Groups may be employed, Global groups are members of Universal groups (U) which are members of Domain Local groups.



**Global** groups contain membership lists of user accounts (and computer accounts) from the local domain that have similar security access requirements and restrictions. The membership list that a Global group contains can only include users and computers that are members of the domain where that Global group exists. While the membership list of a Global group is very restricted, a Global group can be a member of a Domain Local group in any domain in the forest. It can also be used to access resources in any domain in the forest directly, although that is not the preferred method.

Creating Global groups for Widgets will be fairly simple; you can organize users into Global groups based on their departments or titles. Plan your groups below. One example is provided to give you guidance. You will not need to use all the spaces provided.

**Group Scope Group Name Members/Description**

Global HRManagers Managers in the HR Department

Global HRStaff Staff Members in the HR Department

Global AcctDeptMan Managers in the Accounting Department

Global AcctDeptStaff Staff Members in the Accounting Department

Global MarkDeptMan Managers in the Marketing Department

Global MarkDeptStaff Staff Members in the Marketing Department

Global MISDeptMan Managers/Admin of the MIS department

Global MISDeptStaff Staff Members of the MIS Department

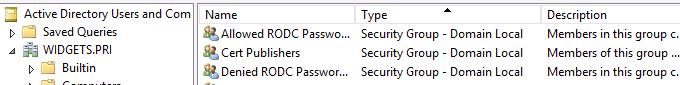
Global EditDeptMan Manager/Senior of the Editorial Department

Global EditDeptStaff Staff Members of the Editorial Department

Global EditDeptIntern Intern Staff Members of the Editorial Department

In the next section you will create Global groups for your domain as you described on the previous page. The groups and users from the examples will be used here.

* Start **your server** and log on with your personal administrative account.
* Using the Tools menu in Server Manager, open Active Directory Users and Computers (ADUC).
* In the left pane **expand** your domain to show the subfolders.
* Left click on the **Users** folder (container) and examine the contents in the right pane.
* Expand the width of the Type column header so you can read the full names of the types of objects, then click on the Type column header to sort the entries by type.



What different types of group scopes do you find in the Users container?

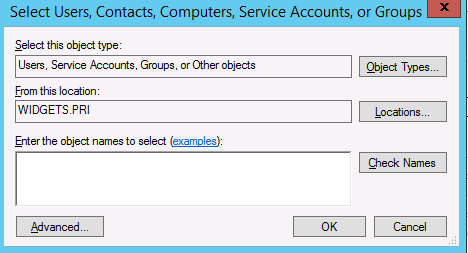
* Right click on the Users container in the left pane and select New then Group from the cascading menus.
* Give the group the name of HRManagers that will be a Global security group.

What are the default radio button settings for Group Scope and Type?

**Scope**:

**Type**:

* Now create another Global security group for **HRStaff**.
* In the right pane of ADUC **now double click on the HRManagers group** to open the Properties page for this group.
* Click on the Members tab at the top.
* In the Members section, click the Add button. This will take you to the place where you can put users (or other groups) into this group.
* This window has three main sections, Object Type, Locations and Check Names.



* Click on the Object Types button and examine the options
* **Uncheck all the boxes except for the Users box and click OK.**
* Rather than try to remember the usernames, click on the **Advanced** button at the bottom of the window.
* Although you could perform a detailed search, just click on **Find Now** for a simple search.
* You should now see a list of all the users in your domain. **Locate** the **user** who is the **HRManager**, click on the name and then click OK.

What is this user’s full object name entry shown in the Enter the object names field?

* Click OK to return to the Members tab of the **HRManagers** Properties window and click OK.

**As you can tell, if you examine the options in various screens there are variations on how you can search for and add users to groups. In the next step you will see a variation of the process.**

* In the Users container, locate the account for Cotton Malone and double click on it to open the user’s properties window.
* Click on the **Member Of** tab.
* Click the Add button.
* This time, instead of using the Advanced button, type in HRStaff in the Enter field and click on Check Names.
* When you do this, if the name is found the system will underline the name of the group for you to verify the spelling and existence of the group, then click OK.
* Click OK again to save the change to the account.
* You have just learned two different ways to add users to group. Now using any method you prefer, Create the remaining Global Groups and add the appropriate uses from the previous lab to those groups.

## Part 2: Domain Local Groups

A **Domain Local** group is used to control access (assign permissions) to resources within the local domain that contains that particular Domain Local group. A Domain Local group cannot be used to access resources outside its own domain. Domain Local Groups have membership lists that can contain accounts or groups from any domain in the forest. A given resource (such as a file or folder) may have multiple Domain Local groups in its Access Control list. It is a common practice to include and abbreviation of the permission level in the name of a Domain Local group. This will be demonstrated later.

The Human Resources (HR) Department at Widgets is responsible for administering corporate policies and benefits. The HR Department routinely publishes company policy information and information on benefits such as vacation, overtime and healthcare policies. To accomplish this, they post documents on corporate servers that all employees can access. While all employees need to be able to read the documents, only HR managers are allowed to modify the documents, while HR staff can only read them. MIS Department members need to have full control of the folder. To simplify the control of these documents the documents are put in a folder called Corporate Policies that will be protected by permissions. To simplify the application of permissions, Domain Local groups will be used. Following are the groups that the MIS department will create for this purpose.

Resource (Folder) Name: **\HRDept\CorpPolices**

**Scope Permission Group Name Membership**

DL Full Control CorpPolicies-FC Domain Admins (built-in Global group)

DL Modify CorpPolicies-M HRManagers (Global group)

DL Read CorpPolicies-R HRStaff (Global group)

**In the next steps you will create these Domain Local groups and then put the appropriate Global groups into them.**

* On **your server** in ADUC create a group in the Users container called CorpPolicies-FC and give it the Domain Local Scope and Security Type.

Graphical user interface, text, application, email

Description automatically generated

* After the DL group has been created, click the Members tab and add the Domain Admins group.
* Now create DL security groups that will have the Modify permission and the Read permission as shown above. Then add the appropriate Global groups to them.

**Creating an example folder structure on your server system.**

Text

Description automatically generated

\Corporate-Documents

\AcctDept

\ExecBonuses

\Payroll

\EditorialDept

\EdDocs

\HRDept

\CorpPolicies

\MarketingDept

\Literature

* On **your server**, **create the folder structure shown above.** First create the **Corporate-Documents** folder directly under the C:\ drive, then create the four departmental folders under the **Corporate-Documents** folder. Finally, create the appropriate departmental subfolders as shown.

In the following sections you will use the indicated security requirements to create a series of domain local groups to protect the resources (folders) described. For simplicity use only four different permission levels.

**FC** for Full Control

**M** for Modify

**R** for Read

**RW** for Read and Write

You can use the special built-in Everyone group instead of a Domain Local group if appropriate.

Editorial Dept **EdDocs** folder. [EditorialDept\**EdDocs**]

* Editorial Staff need Modify, Senior Editors needs **Full Control**, Interns need **Read and Write** permission. Everyone in the MIS Dept needs **Full Control.**
* Marketing Managers and staff need to be able to **read** Editorial department documents.

Marketing Department **Literature** folder [MarketingDept\**Literature**]

* **Everyone** (specialidentity group) in the company needs to be able to **read** the contents.
* Marketing department managers need **full control** and staff need to be able to **modify** literature.
* MIS administrators need **full control** of the contents

Accounting Department **AcctDept** folders. [AcctDept\**Payroll** & AcctDept\**Executive Bonuses**]

* Accounting Managers need to have **full control** of all documents in the **AccDept** folders.
* Accounting Staff need to be able to **modify** [AcctDept\**Payroll]** data but should not have any access to Executive bonus documents
* MIS Domain Administrators should have **full control** of all [AcctDept\**Payroll]** documents but not [AcctDept\**Executive Bonuses]**. They should have no access to bonus information.
* MIS Senior Administrators need **full control** of all Accounting information including [AcctDept\**Executive Bonus]** information

You should plan one Domain Local group for each permission level that will be needed.

Resource (Folder) Name: [EditorialDept**\EdDocs**]

**Scope Permission Group Name Membership (Global Group Name)**

DL FC EdDocs-FC Senior Editors, MIS

DL M EdDocs-M Editorial Staff

DL RW EdDocs-RW Editorial Staff Interns

DL R EdDocs-R Marketing Managers

* Continue by designing the necessary domain local groups on the following page

**Note: When you use System groups like Everyone, Authenticated Users or Creator Owner, you set permissions for those groups directly on the resource; you don’t put system groups into Domain Local groups.**

Resource (Folder) Name: \**MarketingDept**

**Scope Permission DL Group Name Membership (Global Group Name)**

DL FC MarketingDept-FC Marketing Dept Manger, Domain Admins

DL M MarketingDept-M Marketing Department Staff

DL R MarketingDept-R Everyone

Resource (Folder) Name: \**AcctDept**

**Scope Permission DL Group Name Membership (Global Group Name)**

DL FC AcctDept-FC Acct Managers, MIS Senior Admins

Resource (Folder) Name: \AcctDept\**Payroll**

**Scope Permission DL Group Name Membership (Global Group Name)**

DL M AcctDept-Payroll-M Accounting Staff

DL FC AcctDept-Payroll-FC MIS Domain Admins

DL

Resource (Folder) Name:\HRDept**\CorpPolices**

**Scope Permission DL Group Name Membership (Global Group Name)**

DL Full Control CorpPolicies-FC Doman Admins

DL Modify CorpPolicies-M HRManagers

DL Read CorpPolicies-R HRStaff

## Part 3 Controlling Access

Controlling access to resources such as files and folders is called **Authorization.** We use Permissions to protect these resources from both access at the local computer and access from across the network. There are two kinds of permissions we can assign.

**NTFS permissions** are settings applied to a file or folder using the file system on the storage medium such as a hard disk drive. In order for NTFS permissions to be used, the drive must be formatted with the NTFS file system. Because NTFS permissions are applied at the file system level, they are always in effect. This applies to any access to the file or folder whether the user is accessing the resource from the local keyboard or from another computer in the network.

There are 6 standard folder permissions and 5 standard file permissions. Each standard permission is in turn made up of more granular permissions called Special or Advanced permissions.

Standard or Basic Permissions

For Folders For Files

Graphical user interface, application

Description automatically generated Graphical user interface, application

Description automatically generated

Special or Advanced Permissions for Folders

Graphical user interface

Description automatically generated with medium confidence

**Share permissions** control access to folders that are accessed from other computers in the network. They have no effect on a user who is using the local computer that contains the shared folder.

There are only three standard or basic Share permissions which are shown by different names depending on whether you are doing basic or advanced sharing. It is strongly recommended that you only use advanced sharing because basic sharing also modifies the underlying NTFS permissions can easily lead to errors and security holes.

Basic Sharing Advanced Sharing

Text

Description automatically generated with low confidence Background pattern

Description automatically generated with low confidence

What leads to confusion with basic sharing is that if you give a user or group either the Owner or Read/Write basic share permission, the NTFS permission for that user or group is set to Full Control for that folder. Any files or sub folders will inherit the Full Control permission for that security principle. If you give a security principle the Read basic share permission, the NTFS permission for that principle is given the Read and Execute NTFS permissions.

**Combined permissions**: When a user connects to a shared folder and then accesses files or subfolders though that share, both the share permissions and any NTFS permissions are used to determine the users effective level of access. In such a case, whichever permission (share or NTFS) is the most restrictive is the permission that sets the maximum level of access. For example if a user has the Full Control permission at the Share, but only Read permission set on the NTFS file system, the user is only have the Read permission. Neither NTFS nor Share permissions take precedence over the other. Whichever is set to the most restrictive level of access is the maximum permission the user is allowed.

It is common practice to set Share permissions (using Advanced Sharing permissions) very open and use NTFS permissions as the primary means of securing folders and files since the NTFS permissions are always in effect wither the resource is access locally or from across the network. Typically this would involve giving the Everyone system group the Full Control share permissions.

In the next steps you will examine the default NTFS permissions, the permissions interface and permission inheritance from parent to child object.

* Start **your server** if it isn’t already running and log on with your personal administrative account.
* Open File Explorer and **create a new folder** under your C: drive called **PermTest**.
* After creating the folder, right click on it and select Properties. You will see several tabs including the Sharing tab for configuring sharing and the Security tab for NTFS settings.
* Click on the Security tab to view the Discretionary Access Control List.

Graphical user interface, text, application

Description automatically generated

* Under Group or user names you will see all the groups or users that currently have permissions defined for them. These entries are called the Access Control Entries or ACEs.
* When you click on one of the ACEs you will see the standard permissions below with check marks for the current permissions. You may see some that only have a checkmark for Special Permissions which just means you have to dig deeper to find out exactly what permissions they have.
* Click on the Advanced button and you will see more information. Note that some entries may be listed more than once. If so, look under that Applies to column and you will see differences.
* At the top of the Advanced Security Settings window, you will see an entry for the Owner of this resource (folder).
* Click Cancel twice to close the Properties windows.
* Create a folder under the **PermTest** folder call **Sub1** and a folder under **Sub1** called **Sub2**.
* Ensure that the hierarchy looks like **PermTest > Sub1 > Sub2** as shown.

Text

Description automatically generated with low confidence

* Check the NTFS permissions on **Sub1** and **Sub2**. You should find that they have inherited the NTFS permissions from their parent folders (Sub1 from PermTest and Sub2 permissions from Sub1).
* Create a New Text Document in Sub2 called Test1. This file will inherit NTFS permissions from its parent folder.
* Right click on Test1.txt and select Properties.
* You will notice that while there are several tabs on a file, there is no Sharing tab. That is because you can only share folders, not files. Files are accessed from within the shared folders when you connect to the share. Click on the Security tab.

In the next steps you will stop inheritance and examine the effects on object permissions.

* Open the NTFS permissions access control list for **Sub1** (security tab in properties).
* Click the Edit button and then click on the ACE for the Administrators group.

Table

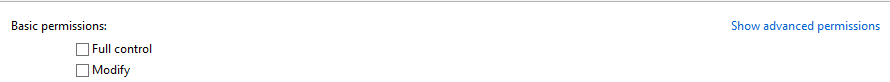
Description automatically generated with low confidence

* Click the Advanced button.
* Click on the button for Disable inheritance.
* Select to convert to explicit permissions and then click OK to return to the Security tab in the properties window.
* Click Edit and then select the Users group.
* Uncheck the Read & Execute permission then click to check it again. Now that there are all explicit permissions, you can change them any way you want.
* You should see that you still can’t change the Special permissions check box. To examine the special permissions, you will need to click Cancel to return to the Properties window then click the Advanced button
* Highlight the row that contains **Special** under the **Access** column, then click the **Edit** button.

Graphical user interface, text, application

Description automatically generated

* Locate the link on the right side of the widows that says Show advanced permissions and then click on the link.



* Return to the main Security tab window in Properties and click Edit.
* Remove the Administrator group from the list and click OK, then continue to click OK until the widows have closed.
* Check the NTFS permissions on the Sub2 folder and verify the permissions were not inherited.
* Check the NTFS permissions on the Test1 file verify the permissions were not inherited.

In the next steps you will see how an Administrator can use membership on other groups to access resources

* Log on as the **built in Administrator** account.

Keep in mind that any an account not only gets permissions from the groups it is a direct member of, but of any groups those groups are member of. So even though the Administrator isn’t a member of the Users group, the Administrator gets User group permissions from membership in the Domain Users group.

* Still logged in as the Administrator, open the Test1 file, add the date and try to save the file. Verify that you are unable to.
* Open the Test1.txt Properties and click on Security, then Edit.
* Verify you are unable to change the permissions in this window.

In the next section you will see how an administrator can gain access to a resource even without any permission initially.

* Log off **SRV16** and log back on as your personal administrative account.
* Use File Explorer to navigate to Sub1 and remove the Users group from the NTFS access control list.

Graphical user interface, text, application

Description automatically generated

* Log off and log on as the **built in Administrator** account
* Use File Explorer to navigate to the Sub1 folder. You should not be able to.
* Go to the Properties of Sub1 and click on **Security**, then click the **Advanced** button.
* Click on Change next to the Owner message
* Type in Administrators and click on **Check Name** to make sure you spelled it correctly, then click OK.
* If you want this to apply to child objects (and you do) you will need to check the box to Replace owner on sub containers and objects, then click OK. (Remember that the Owner of an object can always change the permissions on the object.)

Graphical user interface, text, application

Description automatically generated

* Close the Security tab and reopen it.
* Click Edit to add your personal account to the list and give your account Full Control.
* Click on the Advanced button and check the box to Replace all child object permissions …. And then click OK.
* Still logged in as Administrator, open the Test1 file to verify you are able to save changes.

Earlier you created a folder structure for some of the company’s departments. You also designed a number of Domain Local groups for assigning permissions to those folders. Now it is time to actually set the permissions.

* Use File Explorer to navigate to the HR Dept folder then down to the CorpPolicies folder and open the NTFS permissions access control list.
* Remove all groups from the access control list [Hint: **stop inheritance**]
* Add the three domain local groups you created in Lab 3 for this folder.
* Set each group to the permission indicated in the name of the DL group.

Graphical user interface, text

Description automatically generated

* In a similar fashion, configure permissions for the other DL groups you created at the appropriate folders in the Corporate Documents structure. *Be sure to remove any unnecessary groups from the Access Control Lis*t. Leave the Administrators group in the ACL so the administrator (you) will always have control.

In the next steps you will see how to determine the effective permissions (or effective access) for a user or group. Effective access is a good way to check to see if your permissions will have the effect you want.

* At this point you have finished setting permissions for the CorpPolicies folder. In the Security tab of the CorpPolicies Properties, click on Advanced and then click on the Effective Access tab

Graphical user interface

Description automatically generated

* Click on Select a User and select Cotton Malone

Graphical user interface, text, application, email

Description automatically generated

* Click the **View effective access** button and you will be able to see what permissions Cotton Malone has to this folder based on his group memberships and the permissions you set for those groups. You will see a red X at every permission that is not available to the user and a green check mark for every permission that the use has.
* Examine the effective access for several different users for different folders to see if your permissions are set correctly.
* Close all tabs for the CorpPolicies folder.

## Part Four – Share Permissions

* In the next few steps you will see how to use the basic sharing button and you will also see why it can lead to unexpected results because it not only sets sharing permissions, but also sets NTFS permissions.
* Using File Explorer navigate to the **\PermTest\Sub1** folder.
* Open the **Sub1** Properties and click on the Security tab.
* Remove any users or groups except for your personal administrative account which should have the Full Control NTFS permission.
* Click the Share button

Graphical user interface, text, application

Description automatically generated

* In the blank input box type in **Everyone** and click Add
* Next, add the **Authenticated Users** group
* In the Permissions level, set the **Everyone group to Read** and **the Authenticated Users group to Read/Write,** then click the Share button at the bottom of the File Sharing window.

A picture containing table

Description automatically generated

* You should then get a screen saying that the folder is shared.
* Click Done
* Now open the Security tab for **Sub1** and examine the NTFS permissions.

Note the highest permission for the Everyone group.

Note the highest permission for the Authenticated Users group.

You should now see that using this basic sharing mode causes an opening of NTFS permissions which could lead to errors or even security lapses. The advantage of this method is that an inexperienced user can share a folder without having to add groups and permissions at the NTFS level. While simple, it has potential problems.

In the next steps you will see how to stop sharing a folder.

* Return to the Sharing tab of Sub1 and click on the Advanced Sharing button.
* Uncheck the box for Share this folder to remove the share, then click OK.
* Now go to the Security tab to examine the NTFS permissions.
* When you stopped sharing, note how the NTFS permissions did not revert back to where they were before you used the basic sharing option?

You should now realize another reason that the basic sharing is not desirable. Not only does it change NTFS permissions, but stopping the sharing does not restore the NTFS permissions to the pre-shared state.

In the next steps you will use the Advanced Sharing option.

* Close any windows that might still be open for the Sub1 folder.
* Navigate to the **CorpPolicies** folder and open the Properties windows.
* Just as a reminder, examine the Security tab to confirm the groups that have permissions set. Note the group names.
* Now open the Sharing tab and click on Advanced Sharing.
* Click to check the box to Share this folder then click the Permissions button

Graphical user interface, text, application, email

Description automatically generated

* What is the default group and what permission does this group have?

**Group:**

**Permission:**

* Add the Authenticated Users group and give this group the Full Control permission.
* Remove the Everyone group so that the only share permission is for the Authenticated Users group then click OK twice to finish setting up the share.
* Close the Properties window.
* With **your server** running, start **your client** if it isn’t already running and log on with the Florence Horvath account (she is the HR Manager). Since this user hasn’t logged onto **a client** before, the initial logon will take a little time as the new user profile is prepared. Subsequent logons by the same user will not require this setup.
* Go to the Desktop and open File Explorer as Florence Horvath on **the client.**
* Expand the Network tab in the left pane and then expand the **server’s** icon.

Take note of what the FHorvath account can see based on it’s permissions.

* Click on the CorpPolicies share and in the right pane create a new text document called HR Policies. Open the text file, put in the date and save the changes.

Graphical user interface, application

Description automatically generated

* Log off **the client** and log on as Cotton Malone who is an HR staff member. Once again you will have to wait for the new user profile to be created since this user has not used **the client** before.
* Navigate to the HR Polices text document on the server share and open the file.
* Add some content to the file and try to change save the changes.

Note CMalone’s inability to modify the file due to access restriction.

* Log off and log on with the Jack Reacher account which is not a member of the HR department.

Note JReacher’s inability to access the CorpPolicies folder due to access restriction.

* Log off and log on to **the client** with your personal administrative account.
* Navigate to the HR Polices file, make a change to the file and save the changes.

-END