CNT 4603: System Administration Spring 2011

Project Eight – Configuring Folder Permissions And Account Auditing

Instructor :　　　Dr. Mark Llewellyn
　　　　　　　　markl@cs.ucf.edu
　　　　　　　　HEC 236, 4078-823-2790
　　　　　　　　http://www.cs.ucf.edu/courses/cnt4603/spr2011

Department of Electrical Engineering and Computer Science
University of Central Florida

Project Eight

- **Title:** "Project Eight: Configuring Folder Permissions And Account Auditing"

- **Points:** 30 points

- **Due Date:** April 25th by 11:55 pm WebCourses time.

- **Objectives:** This project focuses on configuring folder permissions on the `savn.local` file server `Server02` (this might be `Server01` depending on what you did for Project Seven). You will create a folder and assign users various permissions to files in the folder and then audit the user's interactions with the folder.

- **Deliverables:** Screen shots as shown on pages 14, 21, 30, and 37.

Project Eight – Background

- In Project Seven you created a couple of files and compressed and encrypted them.

- Start your file server running (again, mine will be on `Server02`).

- Now create a folder and move copies of these files into the folder. I named my folder `Group 1`.

- The next step is to configure the permissions that various user's of the folder will have to the folder's contents.

- Follow the steps on the following pages to configure the permissions for the new folder.
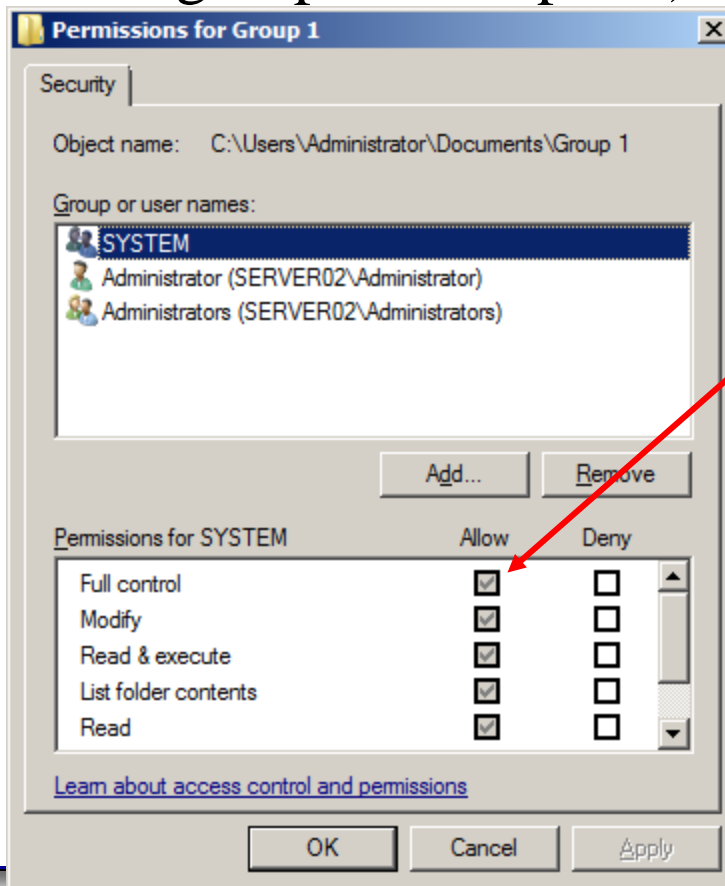
Project Eight – Configuring Folder Permissions

- Right click on the folder Group 1, then click Properties, and then click the Security tab and you should see the screen as shown below:
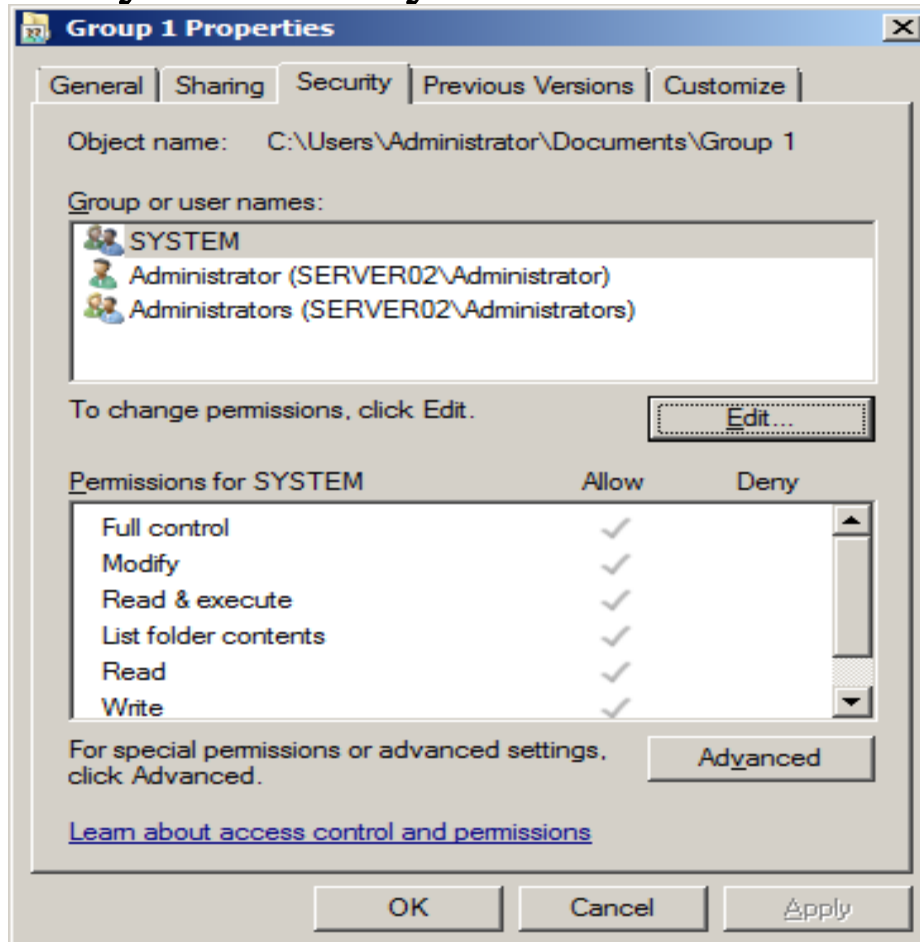
Project Eight – Configuring Folder Permissions

- Click the Edit button and look at the permissions that are currently assigned to the various users (there may only be two or three user groups at this point).
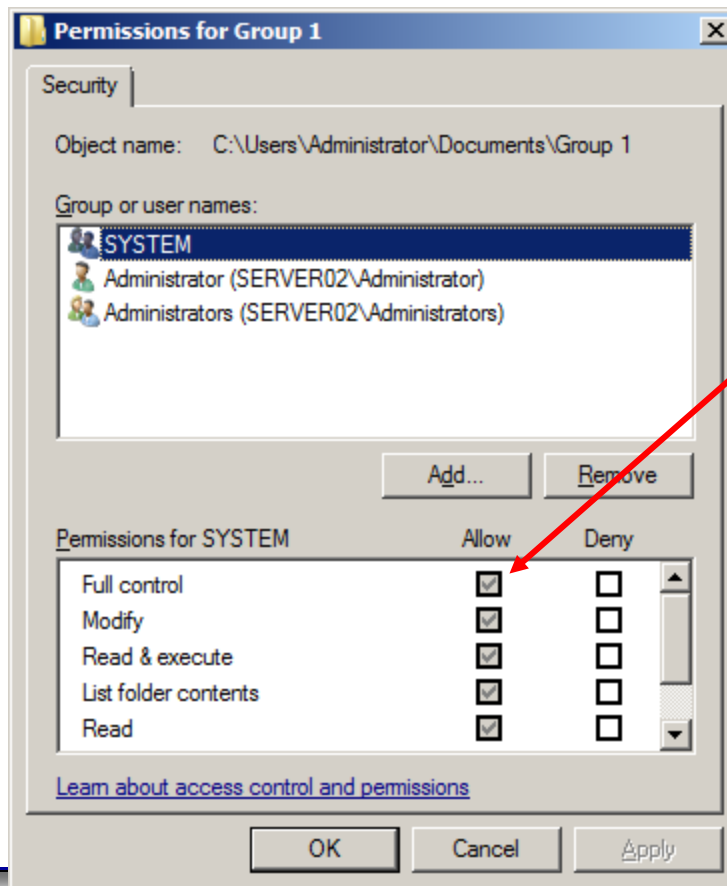

The system has all permissions at this point.

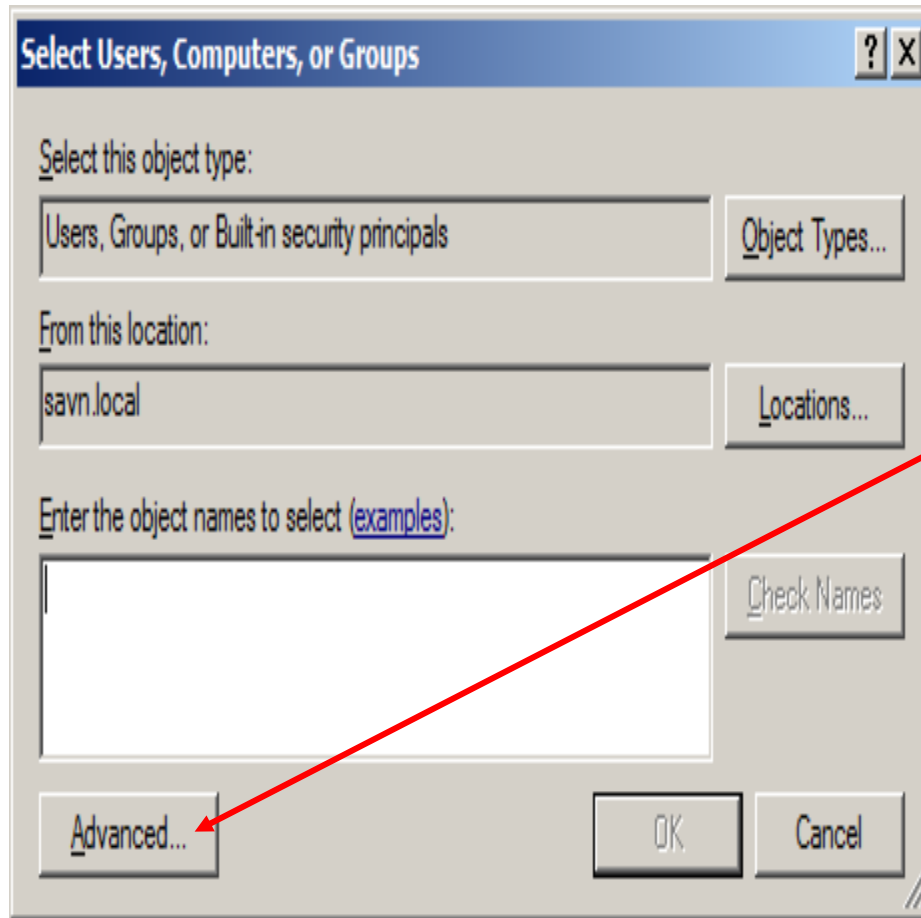# Project Eight – Configuring Folder Permissions

- Click the Add button and then click the Advanced button in the Select Users, Computers or Groups dialog box that appears.

The system has all permissions at this point.

Project Eight – Configuring Folder Permissions

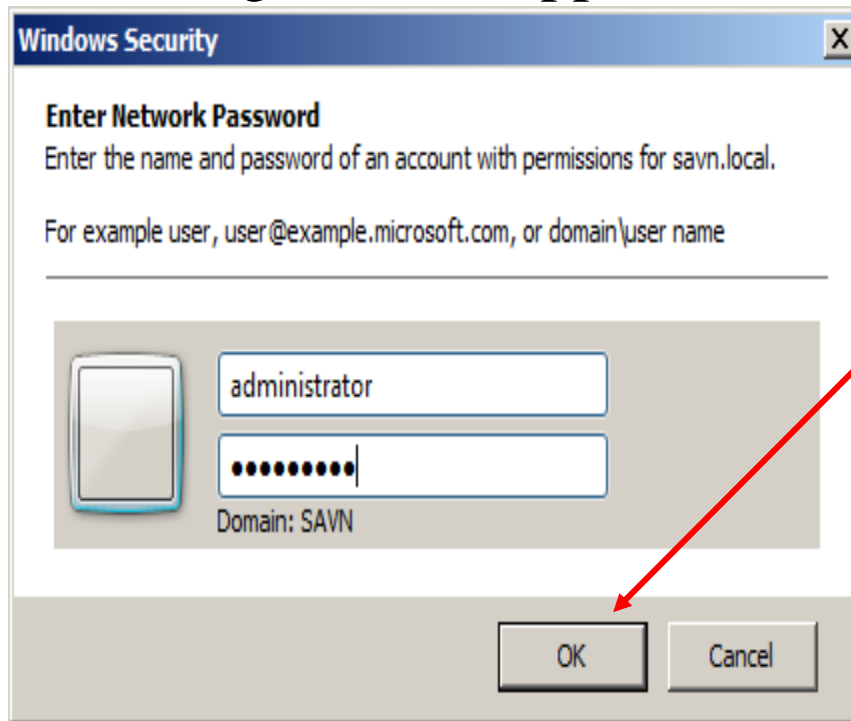Click Advanced, and the Select Users, Computers, or Groups dialog box will appear.
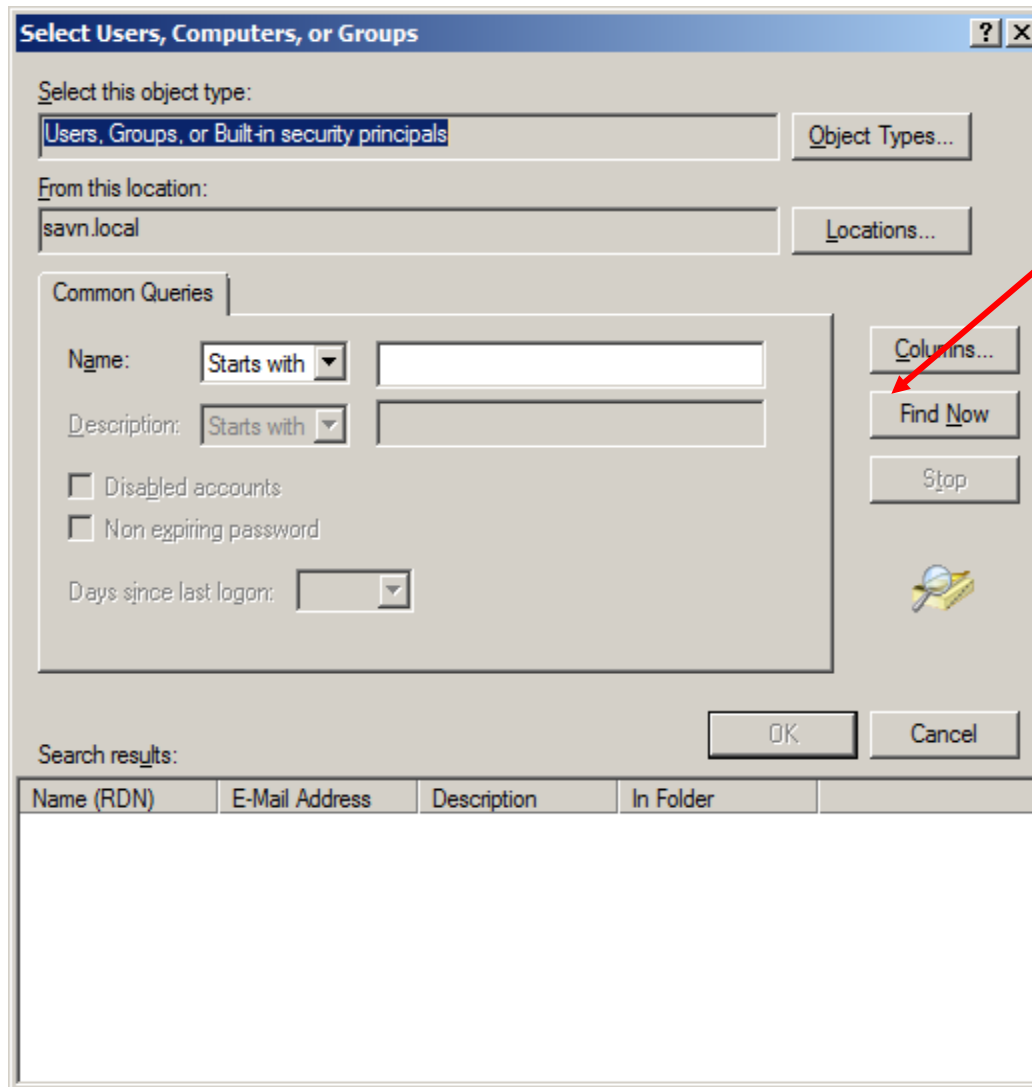
Project Eight – Configuring Folder Permissions

- When you click the Advanced button, since we are in a network controlled by a domain controller, you will need to enter the administrator's information for the domain controller server in the dialog box that appears.

Enter the `savn.local` administrator credentials and click OK

Project Eight – Configuring Folder Permissions

Select Users, Computers, or Groups

Select this object type:

Users, Groups, or Built-in security principals   [Object Types...]

From this location:

savn.local   [Locations...]

Common Queries

Name: Starts with ▼   [   ]   [Columns...]

Description: Starts with ▼   [   ]   [Find Now]

☐ Disabled accounts   [Stop]

☐ Non expiring password

Days since last logon: [▼]

[OK]   [Cancel]

Search results:

Name (RDN)	E-Mail Address	Description	In Folder

In the Select Users, Computers, or Groups dialog box, click Find Now

Project Eight – Configuring Folder Permissions

- In the search results window of the Select Users, Computers, or Groups dialog box scroll down until you find the `savn.local` user that you created in Project Six.

- I've created a few other users for demonstration purposes here, you might want to do the same in order to gain some practice in this area of system administration.

- In this example, I'm using the user named Candice. Find the user in the search result window and double click on the listing.

- This will reset the dialog box so that it appears as on the next page.

Project Eight – Configuring Folder Permissions

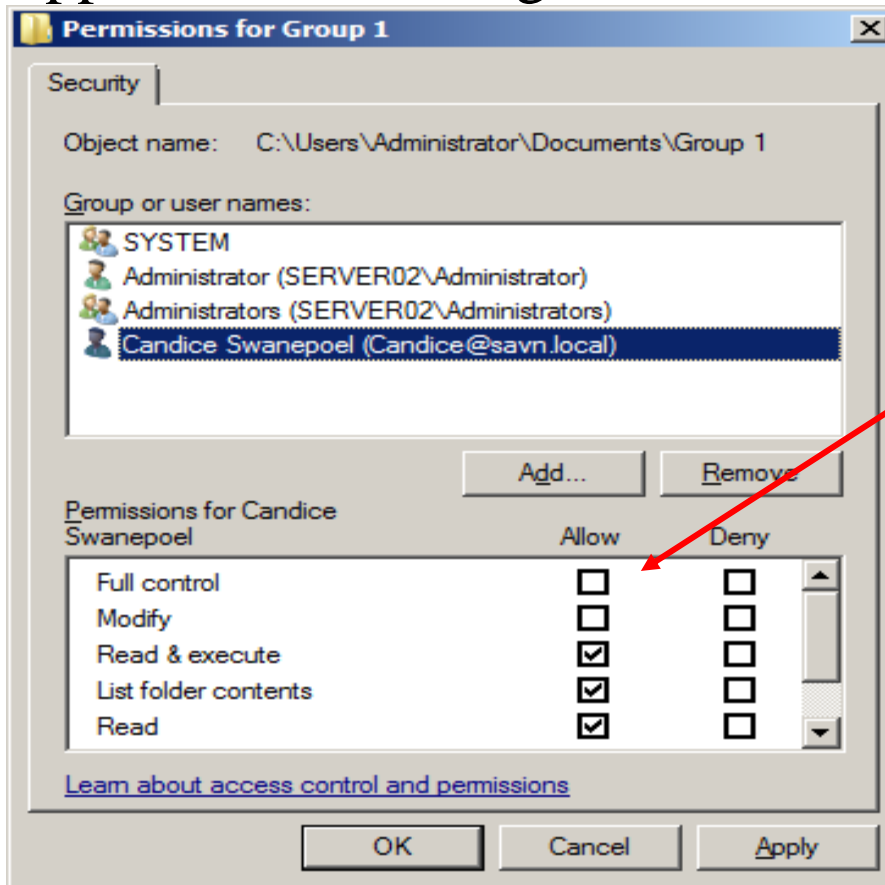- When the user's name is in the reset dialog box, click OK.
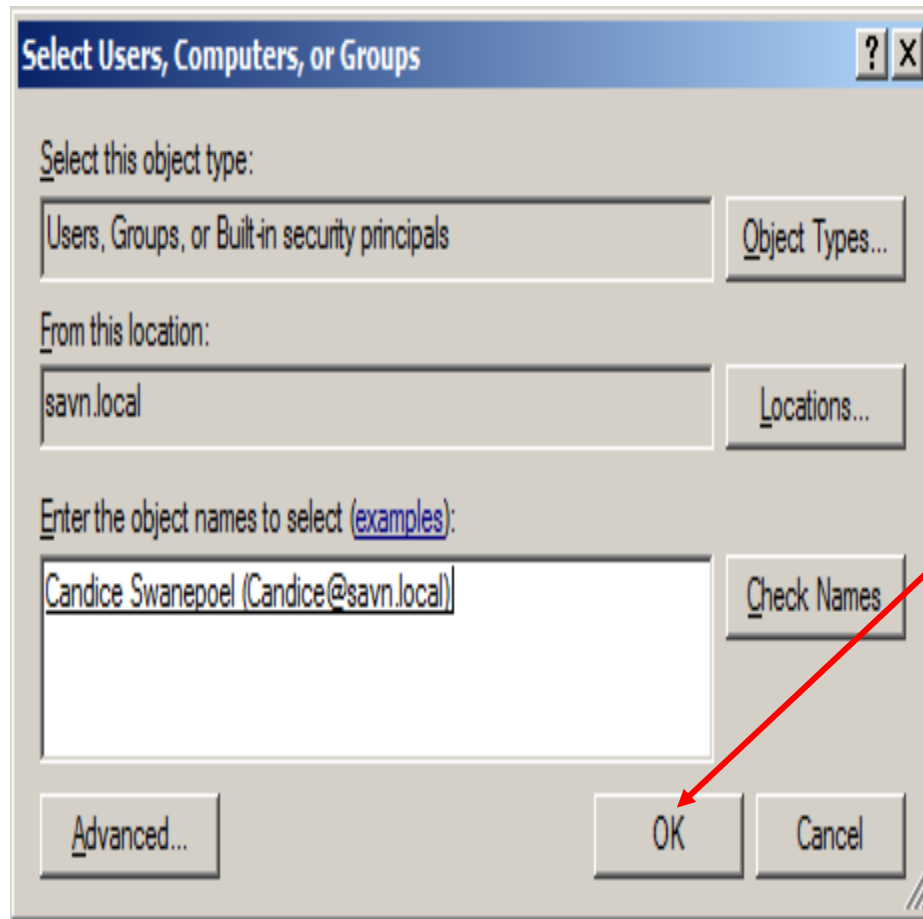
Candice is now in the object name list, so click OK

Project Eight – Configuring Folder Permissions

- When you click OK in the previous dialog box you are returned to the Permissions for Group 1 dialog box and now Candice appears in the listing.

Highlight the entry for Candice and see the permissions that she now has on the folder Group 1.

Project Eight – Configuring Folder Permissions

- Notice that the default permissions to the Group 1 folder that are assigned to Candice involve only reading the folder and executing applications within it. No write/modification or full control permissions are set.

- Check the box to allow Candice the ability to modify the folder Group 1.

- Then click Apply.

- Then click OK.

Project Eight – Configuring Folder Permissions
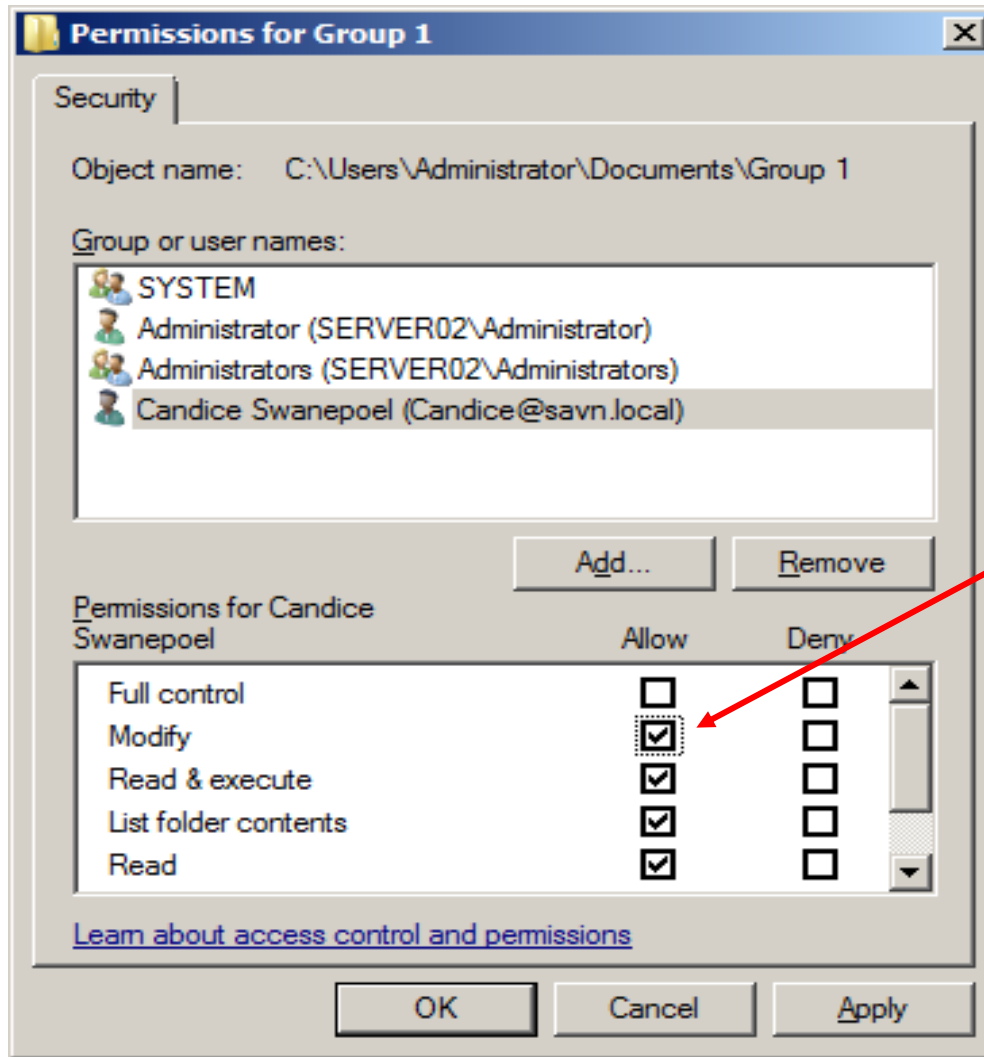
Give Candice modify permission on the Group 1 folder then click Apply.

Do a screen capture of this dialog box. This is deliverable #1 for this project.

Then click OK.

Project Eight – Dealing With Inherited Permissions

- If you examine the permissions box for Administrators more closely in the previous slide you'll notice that some of the allow boxes for permissions are checked and deactivated. These are inherited permissions.

- An inherited permission means that the same permission on a parent object, such as the root folder in this case, apply to the child objects such as files and folders within the parent folder.

- If you want to change inherited permissions that cause Allow or Deny boxed to be deactivated (and checked), you can do so by removing the inherited permissions.

- We'll practice this next.

Project Eight – Dealing With Inherited Permissions

- Once again start Server02 running, if it isn't already, and go to the Group 1 folder.

- Right click the folder and click Properties.

- Select the Security tab.

- Click the Advanced button.

- You'll see the screen as shown on the next page when you've done all this.

Project Eight – Dealing With Inherited Permissions

Advanced Security Settings for Group 1

Permissions | Auditing | Owner | Effective Permissions

To view or edit details for a permission entry, select the entry and then click Edit.

Object name: C:\Users\Administrator\Documents\Group 1

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Candice (SAVN\Candice)	Modify	<not inherited>	This folder, subfolders and…
Allow	Administrator (SERVER02…	Full control	C:\Users\Administr…	This folder, subfolders and…
Allow	SYSTEM	Full control	C:\Users\Administr…	This folder, subfolders and…
Allow	Administrators (SERVER0…	Full control	C:\Users\Administr…	This folder, subfolders and…

Click Edit

Edit…

☑ Include inheritable permissions from this object's parent

Managing permission entries

OK   Cancel   Apply

Project Eight – Dealing With Inherited Permissions

Advanced Security Settings for Group 1

Permissions

To view or edit details for a permission entry, select the entry and then click Edit.

Object name: C:\Users\Administrator\Documents\Group 1

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Candice (SAVN\Candice)	Modify	<not inherited>	This folder, subfolders a...
Allow	Administrator (SERVER0...	Full control	C:\Users\Administr...	This folder, subfolders a...
Allow	SYSTEM	Full control	C:\U...	
Allow	Administrators (SERVER...	Full control	C:\U...	

Add...   Edit...   Remove

☑ Include inheritable permissions from this object's parent

☐ Replace all existing inheritable permissions on all descendants with inheritable permissions from this object
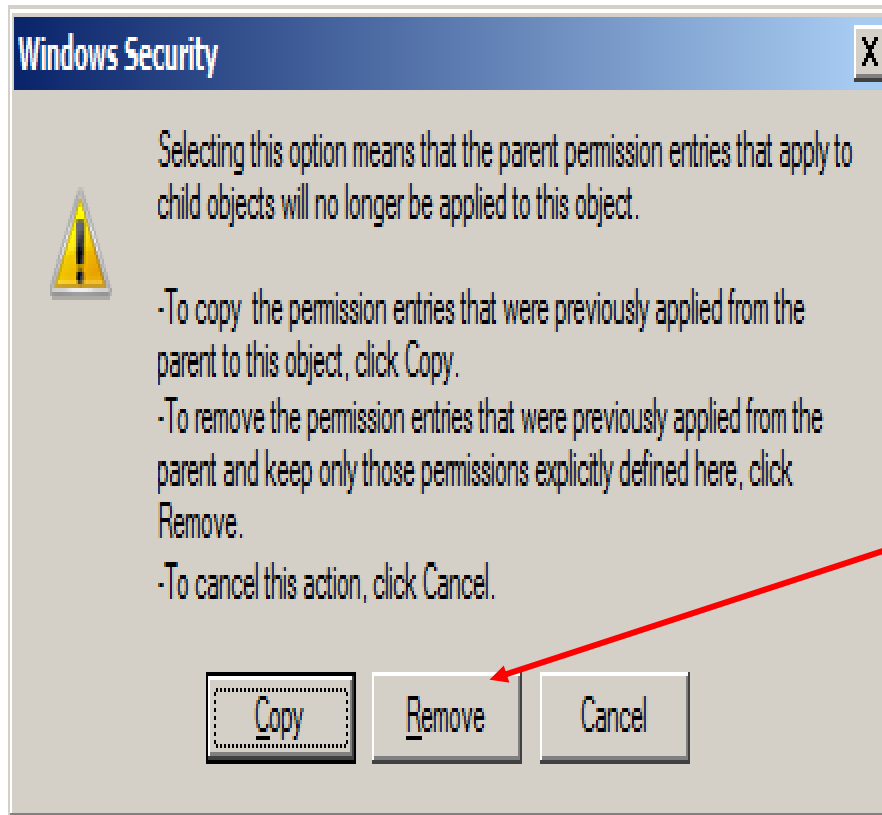
Managing permission entries

OK   Cancel   Apply

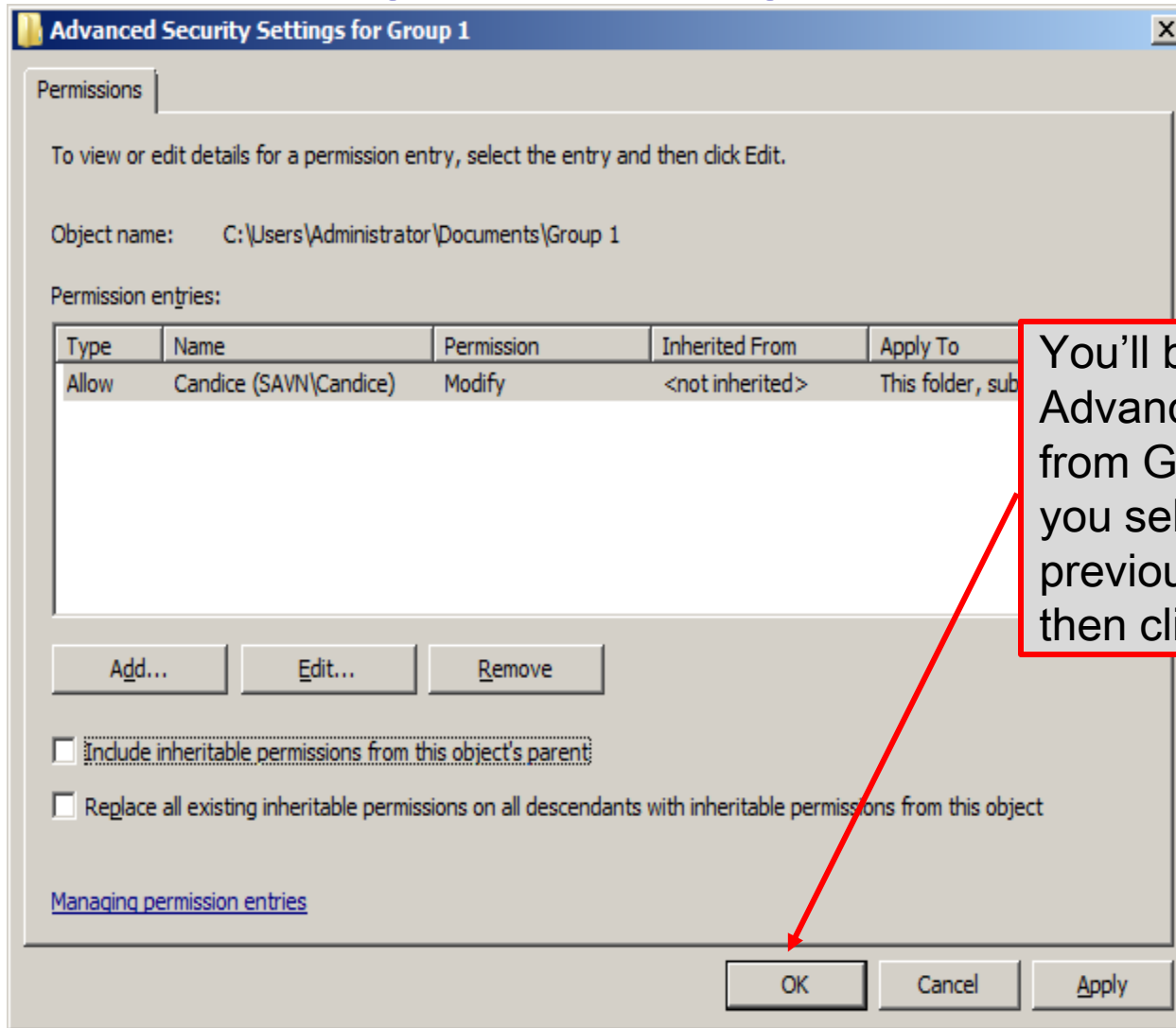> Remove the check from the Include inheritable permissions from this object's parent

Project Eight – Dealing With Inherited Permissions

Windows Security

Selecting this option means that the parent permission entries that apply to child objects will no longer be applied to this object.

-To copy the permission entries that were previously applied from the parent to this object, click Copy.

-To remove the permission entries that were previously applied from the parent and keep only those permissions explicitly defined here, click Remove.

-To cancel this action, click Cancel.

[Copy]   [Remove]   [Cancel]

When you remove the check in the previous dialog box, the Windows Security dialog box will appear. Notice that there are three options from which to choose. One is to copy back the inherited permission (if you have removed them already), one is to removed the inherited permissions, and one is to cancel the operation. Click Remove.

Project Eight – Dealing With Inherited Permissions

Advanced Security Settings for Group 1   ✕

Permissions

To view or edit details for a permission entry, select the entry and then click Edit.

Object name: C:\Users\Administrator\Documents\Group 1

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Candice (SAVN\Candice)	Modify	<not inherited>	This folder, sub

[Add...]   [Edit...]   [Remove]

☐ Include inheritable permissions from this object's parent

☐ Replace all existing inheritable permissions on all descendants with inheritable permissions from this object

Managing permission entries

[OK]   [Cancel]   [Apply]

You'll be returned to the Advanced Security Settings from Group 1 dialog box when you select Remove in the previous dialog. Click OK, then click OK again.

Project Eight – Dealing With Inherited Permissions
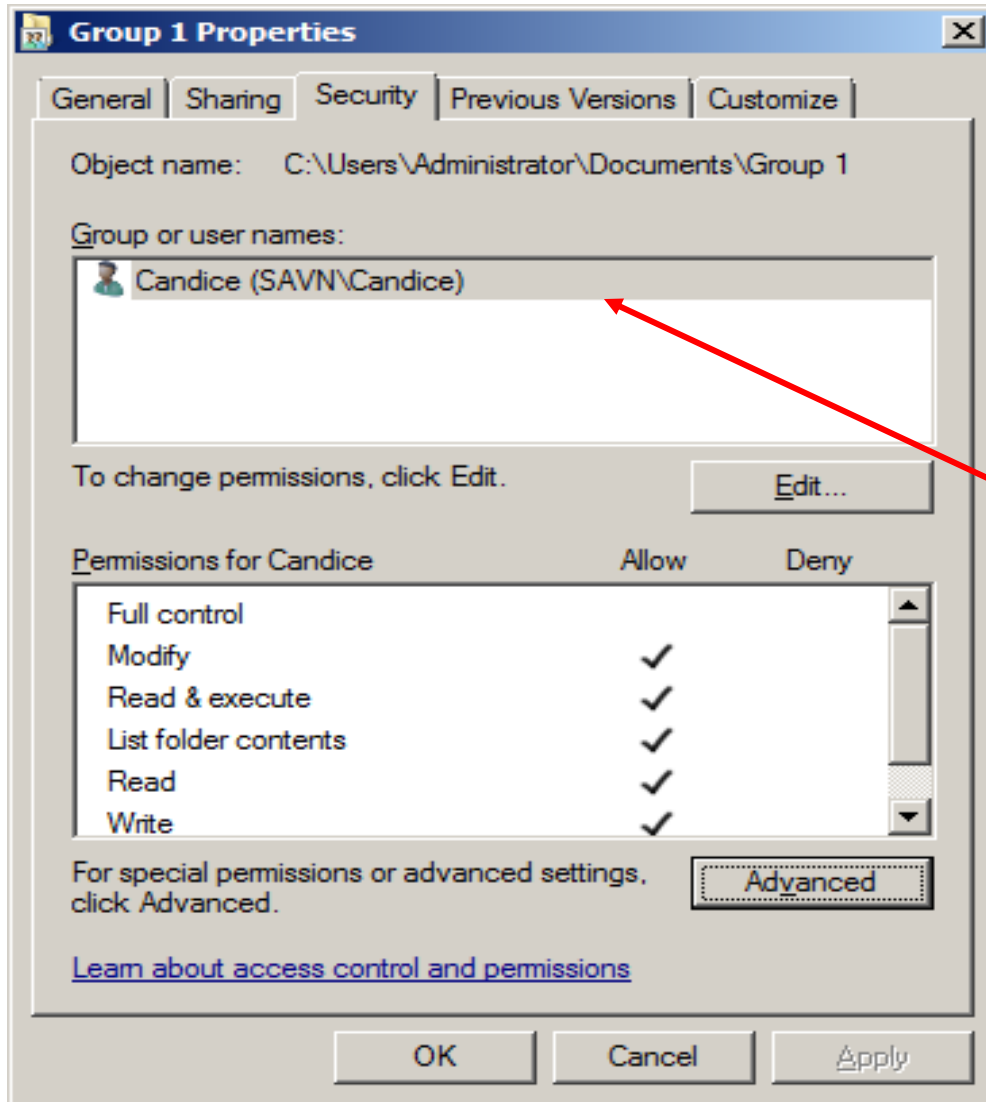
When you finally return to the Group 1 Properties dialog box, notice that Candice is now the only user who has any permissions on the folder. Specifically, those with inherited permissions have disappeared, since you've now removed them from the list.

Take a screen shot of this dialog box. This is deliverable #2 for this project.

Project Eight – Dealing With Special Permissions

- If you have the need to customize permissions, you have the option to set up special permissions for a particular group or user.

- The screen shot on the next page illustrates some of the special permissions that you can set up.

- The meanings of these special permissions are explained in the table on the next page.

Project Eight – Dealing With Special Permissions

Permission	Description	Applies to
Full control	Can read, add, delete, execute, and modify files, plus change permissions and attributes, and take ownership	Folders and files
Traverse folder/execute file	Can list the contents of a folder and run program files in that folder; keep in mind that all users are automatically granted this permission via the Everyone and Users groups, unless it is removed or denied by you	Folders and files
List folder / read data	Can list the contents of folders and subfolders and read the contents of files	Folders and files
Read attributes	Can view folder and file attributes (read-only and hidden)	Folders and files
Read extended attributes	Enables the viewing of extended attributes (archive, index, compress, and encrypt)	Folders and files
Create files / write data	Can add new files to a folder and modify, append to, or write over file contents	Folders and files
Create folders / append data	Can add new folders and add new data at the end of files, but otherwise cannot delete, write over, or modify data	Folders and files
Write attributes	Can add or remove the read-only and hidden attributes	Folders and files
Write extended attributes	Can add or remove the archive, index, compress, and encrypt attributes	Folders and files
Delete subfolders and files	Can delete subfolders and files (the following Delete permission is not required)	Folders and files
Delete	Can delete the specific subfolder or file to which this permission is attached	Folders and files
Read permissions	Can view the permissions (ACL information) associated with a folder or file (but does not imply you can change them)	Folders and files
Change permissions	Can change the permissions associated with a folder or file	Folders and files
Take ownership	Can take ownership of the folder or file (read permissions and change permissions automatically accompany this permission)	Folders and files

Project Eight – Dealing With Special Permissions

- When the regular NTFS permissions do not enable you to create exactly the type of access you want to allow on a folder, you will use the special permissions to configure the access permissions.

- To start this part of the project. Create a new folder, I named mine Reports, and copy the files you created earlier into this new folder.

- Follow the steps on the next couple of pages to configure the special permissions on the Reports folder.
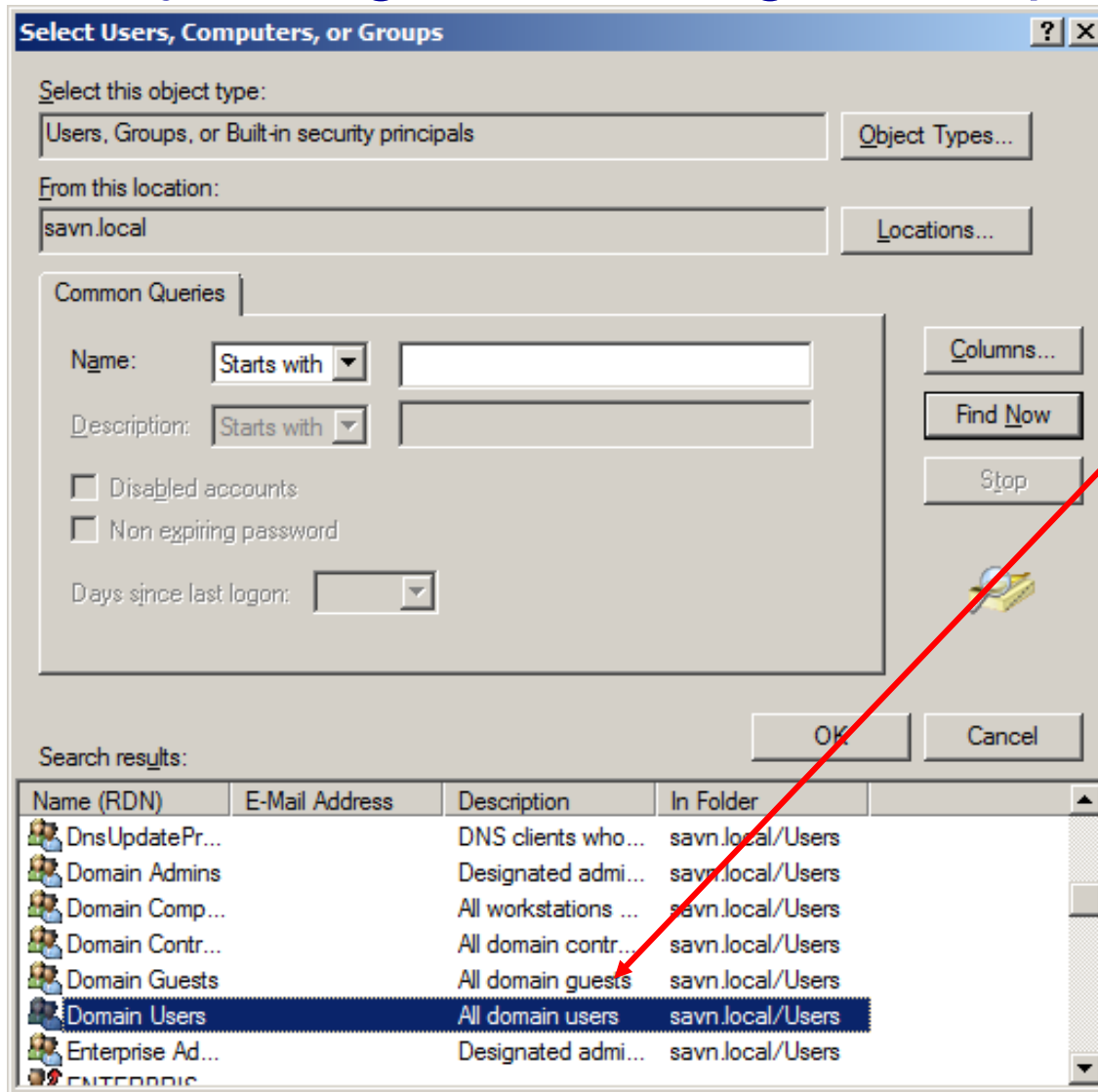
Project Eight – Dealing With Special Permissions

- Right click the Reports folder, then click Properties.

- Click the Security tab.

- Click Edit.

- Click Add.

- Click Advanced in the Select Users, Computer, or Groups dialog box.

- Click Find Now.

- Enter the administrator credentials for the domain controller in the Windows Security dialog box.

- Click Find Now.

Project Eight – Dealing With Special Permissions

In the search results window, find the Domain Users name and double click it.
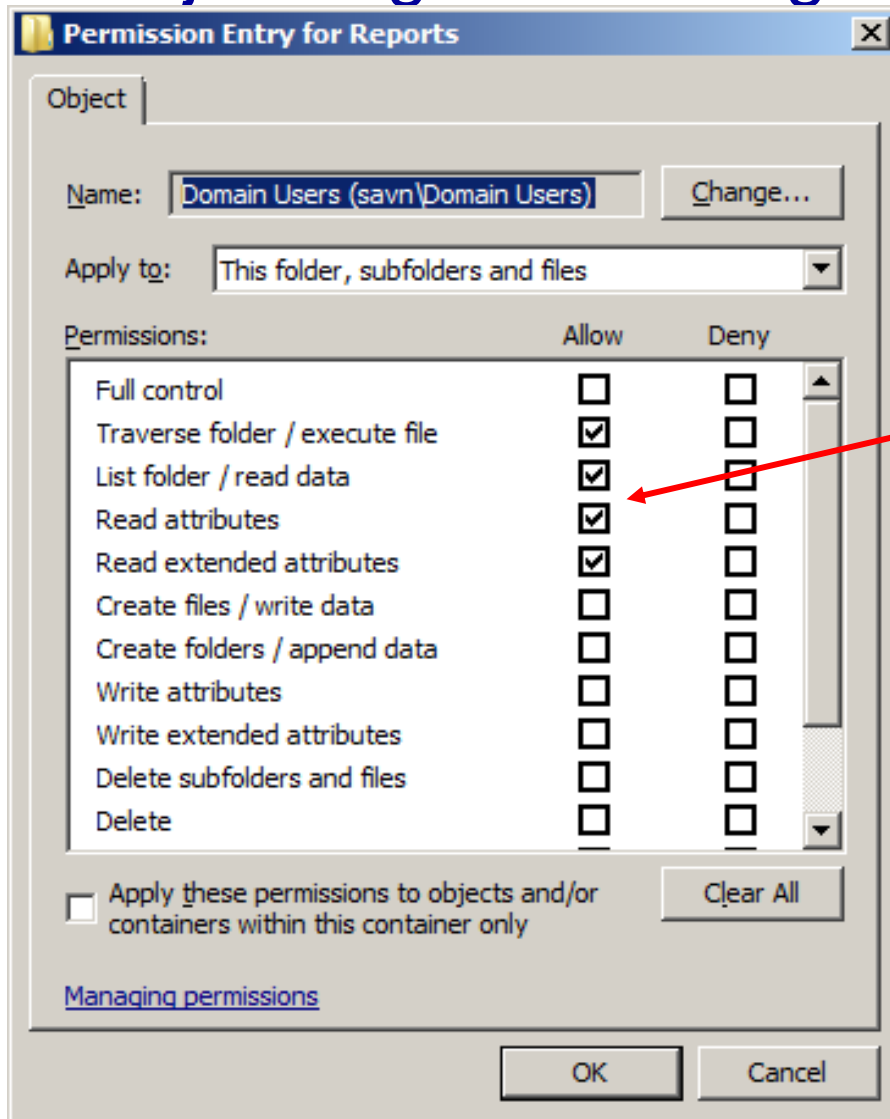
Project Eight – Dealing With Special Permissions

- Click OK in the Select Users, Computer, or Groups dialog box.

- Click Apply in the Permissions for Reports dialog box.

- Click OK in the Permissions for Reports dialog box.

- Click Domain Users under Group or user names in the Properties dialog box.

- Click Advanced.

- Ensure that Domain Users is selected under Permission entries and click Edit.

- Again make sure that the Domain Users group is still selected and click the Edit button in the Advanced Security Settings for Reports dialog box. You'll see the dialog box on the next page.
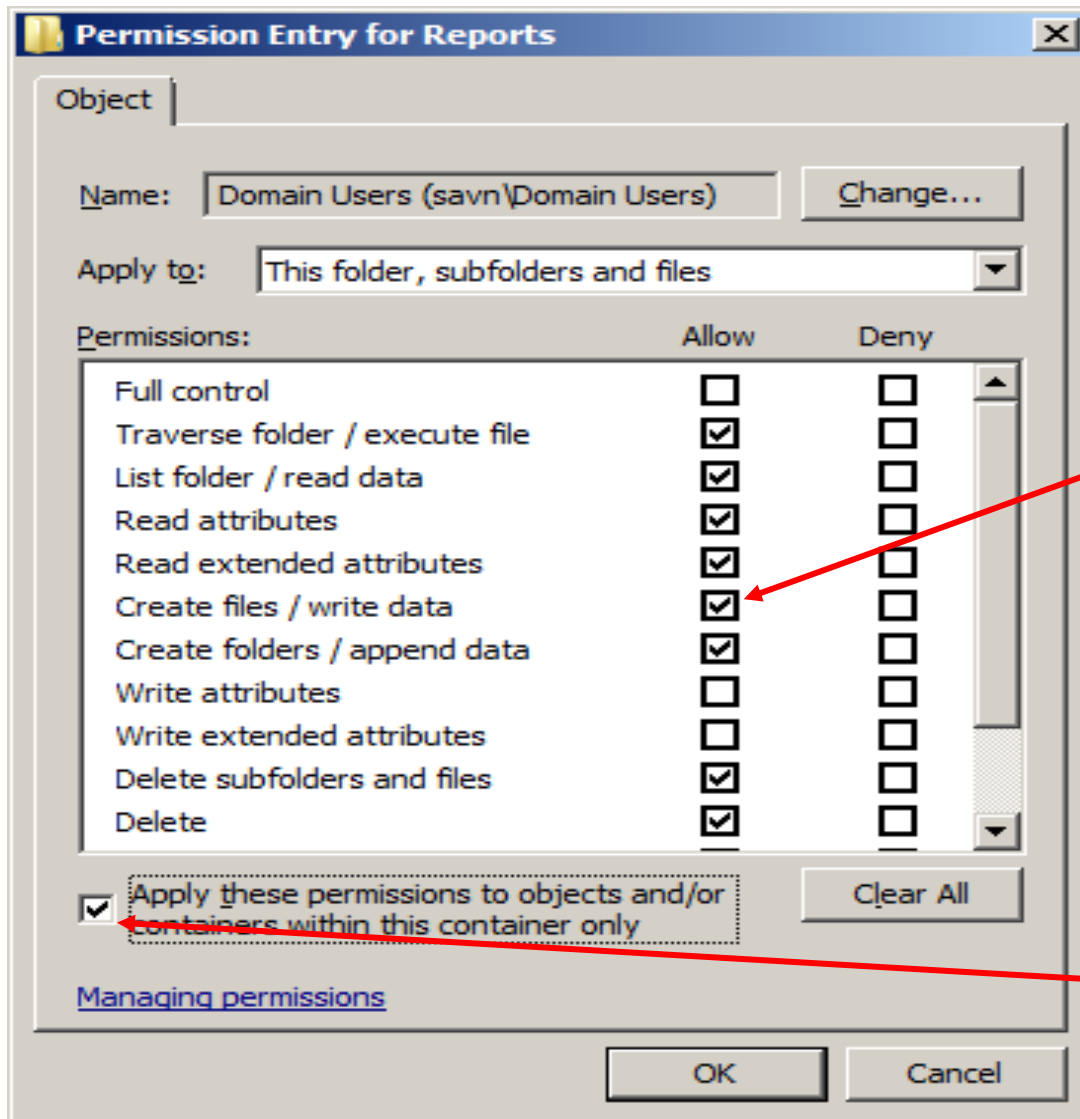
Project Eight – Dealing With Special Permissions

Note the permissions that are set by default for the Domain Users group.

Project Eight – Dealing With Special Permissions

Permission Entry for Reports

Object

Name: Domain Users (savn\Domain Users)   Change...

Apply to: This folder, subfolders and files

Permissions:	Allow	Deny
Full control	☐	☐
Traverse folder / execute file	☑	☐
List folder / read data	☑	☐
Read attributes	☑	☐
Read extended attributes	☑	☐
Create files / write data	☑	☐
Create folders / append data	☑	☐
Write attributes	☐	☐
Write extended attributes	☐	☐
Delete subfolders and files	☑	☐
Delete	☑	☐

☑ Apply these permissions to objects and/or containers within this container only

Clear All

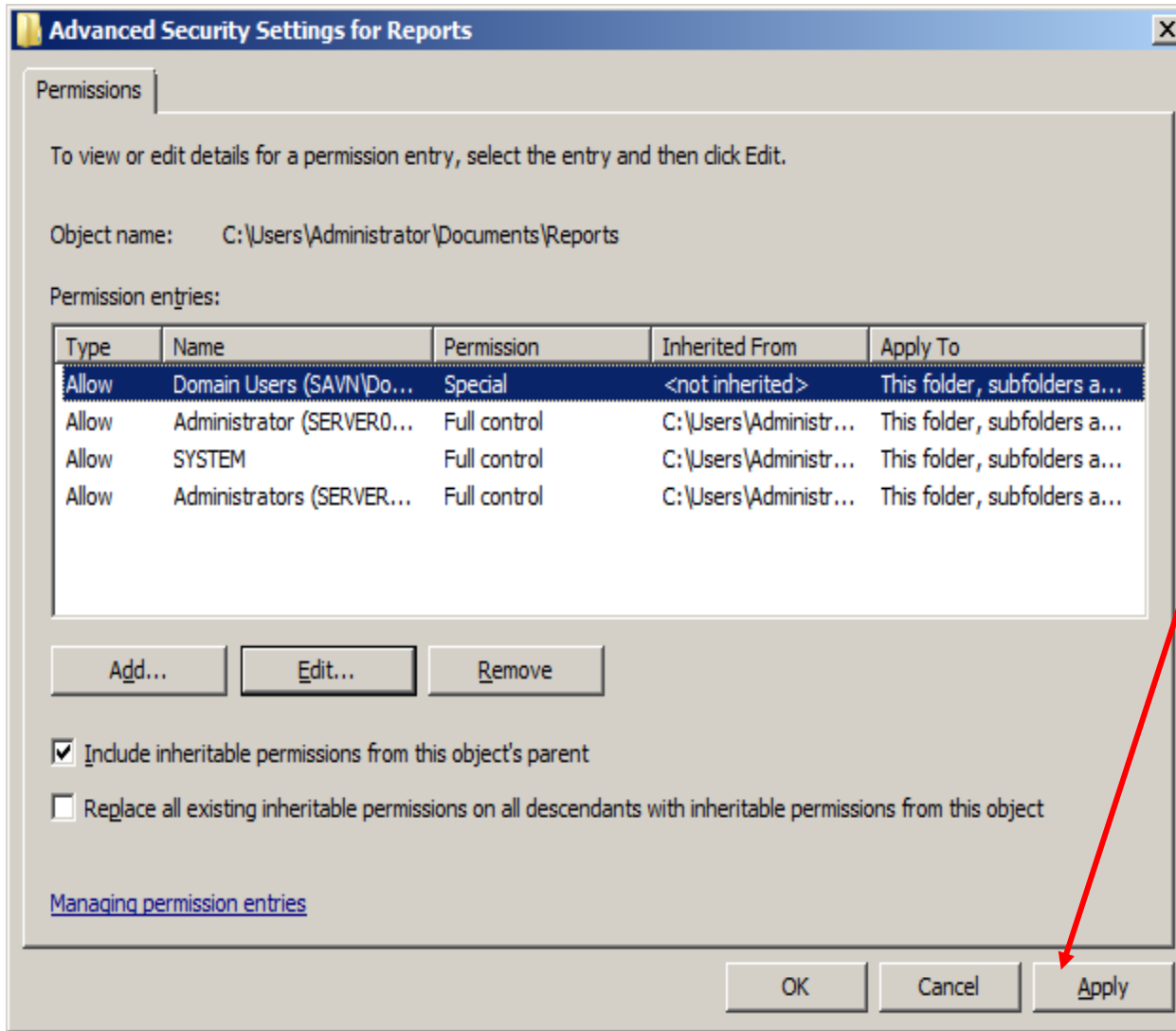Managing permissions

OK   Cancel

Click the allow box for each of the following permissions entries: Create files/write data, Create folders/append data, Delete subfolders and files, and Delete.

Also check the box for apply these permissions…

Then click OK.

Project Eight – Dealing With Special Permissions

Advanced Security Settings for Reports

Permissions

To view or edit details for a permission entry, select the entry and then click Edit.

Object name: C:\Users\Administrator\Documents\Reports

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Domain Users (SAVN\Do...	Special	<not inherited>	This folder, subfolders a...
Allow	Administrator (SERVER0...	Full control	C:\Users\Administr...	This folder, subfolders a...
Allow	SYSTEM	Full control	C:\Users\Administr...	This folder, subfolders a...
Allow	Administrators (SERVER...	Full control	C:\Users\Administr...	This folder, subfolders a...

Add...   Edit...   Remove

☑ Include inheritable permissions from this object's parent

☐ Replace all existing inheritable permissions on all descendants with inheritable permissions from this object

Managing permission entries

OK   Cancel   Apply

Take a screen shot of this dialog box. This is deliverable #3 for this project.

Then click Apply. Then back out of everything by repeatedly clicking OK.

Project Eight – Auditing A Folder

- Accessing folders and files can be tracked by setting up auditing, which in Windows Server 2008 enables you to track activity on a folder or a file, such as read and/or write activity.

- Windows Server 2008 NTFS folders and files enable you to audit a combination of any or all of the activities listed as special permissions in the table on page 23.

- When you set up auditing, the options for each type of access are to track successful and unsuccessful attempts.

- You'll practice setting up an audit on a folder in the next section of this project.

- Follow the steps on the next page to get started.

Project Eight – Auditing A Folder

- We'll set up audit properties on the newly created Reports folder. So, as before, go to the folder, right click it, then select Properties.

- Click the Security tab.

- Click the Advanced button.

- Click the Auditing button.

- Click the Edit buttons.

- Click Add.

- Click the Advanced button in the Select Users, Computer, or Groups dialog box.

Project Eight – Auditing A Folder

- Enter the administrator credentials for the `savn.local` domain controller administrator in the Windows Security dialog box.

- Then click the Find Now button.

- Search down the list in the search results window until you find the listing for Everyone and double click this entry.

Project Eight – Auditing A Folder

Project Eight – Auditing A Folder

Notice in the Auditing Entry for Reports dialog box the Successful and Failed boxes that you can check for each permission.

Project Eight – Auditing A Folder

Click the Successful box for each of the following permissions:
Traverse folder/execute file
List folder / read data
Create files/ write data
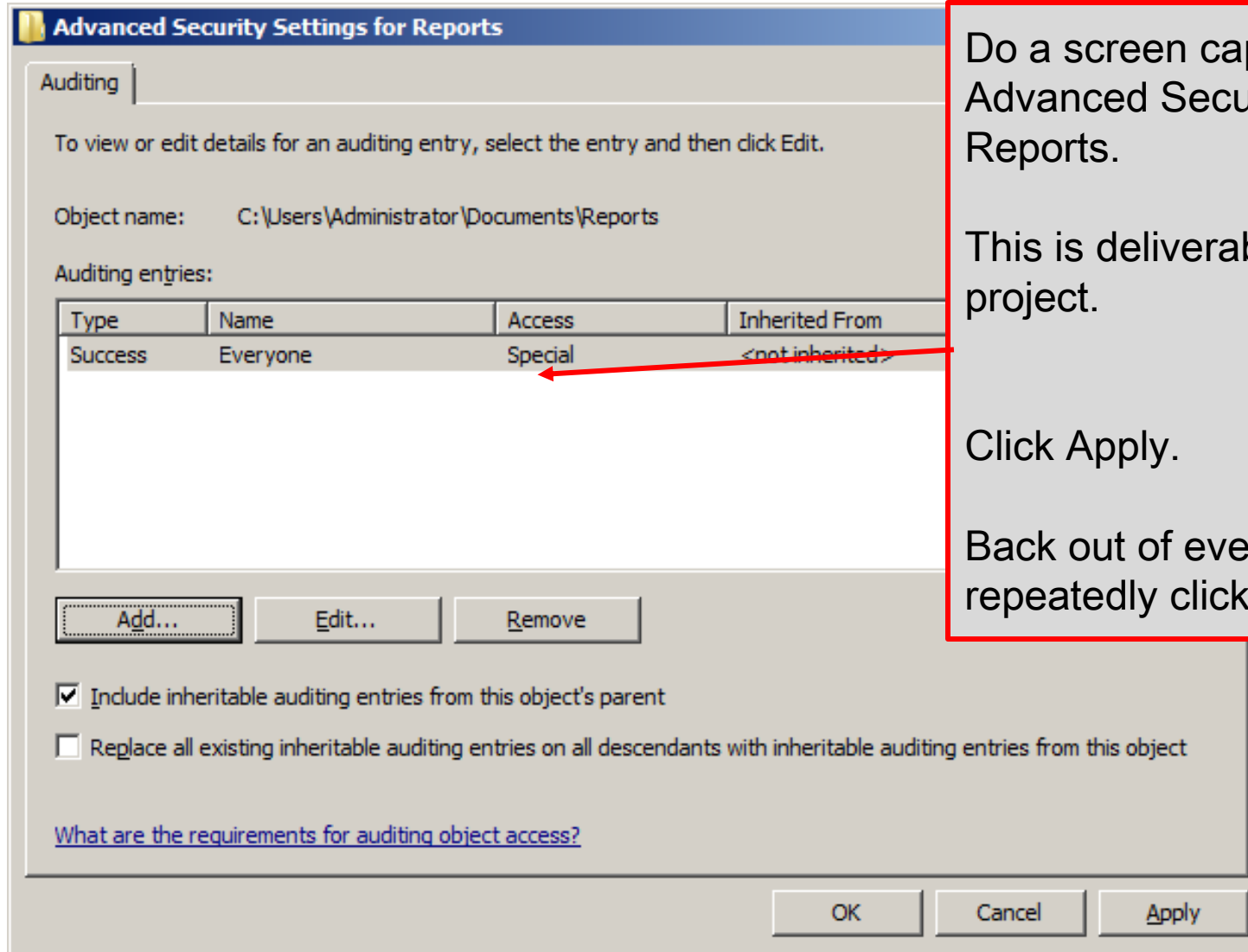Create folders / append data
Delete subfolders and files

Then click OK.

Project Eight – Auditing A Folder

Advanced Security Settings for Reports

Auditing

To view or edit details for an auditing entry, select the entry and then click Edit.

Object name: C:\Users\Administrator\Documents\Reports

Auditing entries:

Type	Name	Access	Inherited From
Success	Everyone	Special	<not inherited>

Add...   Edit...   Remove

☑ Include inheritable auditing entries from this object's parent

☐ Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object

What are the requirements for auditing object access?

OK   Cancel   Apply

Do a screen capture of the Advanced Security Settings for Reports.

This is deliverable #4 for this project.

Click Apply.

Back out of everything by repeatedly clicking OK.