

Before You Begin

Welcome! The Virtual Security Cloud Labs are your opportunity to gain valuable hands-on experience with professional-grade tools and techniques as you work through the guided lab exercises provided in the on-screen lab manual. The use of virtualization enables you to perform all of the tasks in the lab manual in a live environment without putting your personal device or institution's assets at risk.

Before you begin the guided lab exercises, please review the following preparation checklist.

1. **Run the [System Checker](#).** The System Checker will confirm that your browser and network connection are ready to support virtual labs.
2. **Review the [Common Lab Tasks document](#).** This document provides an overview of the virtual lab environment and outlines several of the recurring tasks you may need to complete your lab exercise.
3. **When you've finished, use the Disconnect button to end your session and create a StateSave.** To end your lab session and save your work, click the Disconnect button in the upper-right corner of the Lab View toolbar. When prompted, assign a name for your StateSave (we recommend using the Section, Part, and Step number where you stopped) and click Continue. Please note that a StateSave will preserve any changes written to disk in your lab session. A StateSave will not preserve any open windows or active processes, similar to restarting your computer.
If you close your browser window without disconnecting, your lab session will automatically end after 5 minutes.
4. **[Technical Support](#) is here to help!** Our technical support team is available 24/7 to help troubleshoot common issues.
Please note that the 24/7 support team is Level 1 only, and cannot assist with questions about lab content or the array of software used in the labs. If you believe you've identified an error in the lab guide or a problem with the lab environment, your ticket will be escalated to the Jones & Bartlett Learning product team for review. In the meantime, we recommend resetting the lab (Options > Reset) or reaching out to your instructor for assistance.

Introduction

Computer security is accomplished using many different systems, but the fundamental concepts are all rooted in the security triad known as CIA (Confidentiality, Integrity and Availability). Confidentiality is preventing the disclosure of secure information to unauthorized individuals or systems. Integrity is maintaining and assuring the accuracy of data over its life-cycle. For information to be useful it must be available when needed: thus the need for Availability. This means the data may need to be in highly redundant, highly protected storage areas with adapted power and cooling.

Microsoft has developed their Active Directory Domain structure so that a central authority, the Domain Controller, is the central repository for all domain security records. It has several layers of authentication and authorization, including standard user/password, and several forms of two factor authentication. Two-factor authentication combines something you know (such as a password) with something you are (for instance, a fingerprint or retina scan) or something you possess (such as a smart card or USB stick). It can also employ a certificate system: either a self-signed or third-party certificate system that adds a distinct third layer to the authentication process. The domain can be a stand-alone entity, or can join with other domains in a forest with offices in several cities or countries. Administrators may have rights to their own city/domain, but in general, only the corporate IT administrators have access to the entire tree. This is a very common arrangement.

This lab will strive to demonstrate the Microsoft approach to securing the CIA triad. While Microsoft Windows Active Directory provides capabilities in all three of the CIA areas, the domain administrator will be called upon to implement two (Confidentiality and Integrity) roles most frequently. By creating users, assigning those users to groups, and then applying groups to resources in the domain, the administrator sets up both authentication using the Active Directory Domain authentication policies, and builds a series of nested Access Control Lists to control the access to domain resources. This system not only locks out unauthorized access, but it also can work to prevent changes to resources by internal users not qualified or authorized to have access.

Learning Objectives

Upon completing this lab, you will be able to:

1. Understand how Microsoft's Active Directory Domain Services can help implement an access control framework
2. Use Active Directory to create new user accounts and security groups
3. Implement a Windows file folder structure with custom permission rights
4. Augment an existing Group Policy to facilitate remote access

5. Create and verify access control lists to protect objects and folders from unauthorized access

Lab Overview

Each section of this lab is assigned at your instructor's discretion. Please consult your instructor to confirm which sections you are required to complete for your lab assignment.

SECTION 1 of this lab has four parts, which should be completed in the order specified.

1. In the first part of the lab, you will create new user accounts and security groups, and apply the new user accounts to the security groups.
2. In the second part of the lab, you will create nested folders on the remote server and assign unique file permissions using the new user accounts and security groups.
3. In the third part of the lab, you will set group policy to enable the use of remote desktop services for the new user accounts created in this lab.
4. In the fourth part of the lab, you will verify that the security configurations you modified are working properly.

SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will be introduced to a more robust way of creating users, groups, and permissions.

Finally, you will explore the virtual environment on your own in **SECTION 3** of this lab. You will answer questions and complete challenges that allow you to use the skills you learned in the lab to conduct independent, unguided work, similar to what you will encounter in a real-world situation.

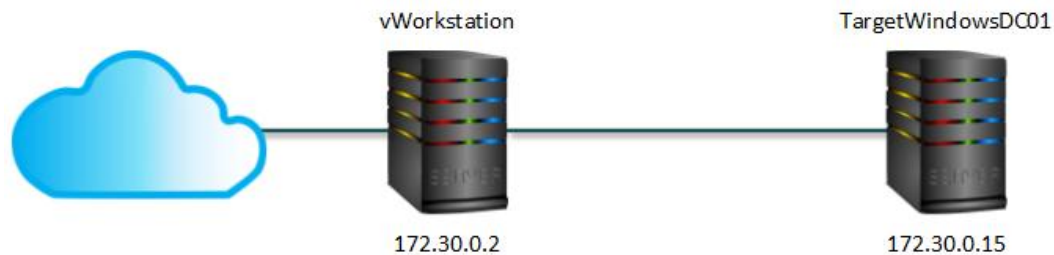
Topology

This lab contains the following virtual devices. Please refer to the network topology diagram below.

Enabling Windows Active Directory and User Access Controls

Fundamentals of Information Systems Security, Third Edition - Lab 03

- vWorkstation (Windows Server 2016)
- TargetWindowsDC01 (Windows Server 2016)



Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- Active Directory Domain Services
- Group Policy Object Editor
- PowerShell

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

SECTION 1:

1. Lab Report file including screen captures of the following;

- all new users and groups created in Active Directory;
- unsuccessful access error messages in the LabFiles folder for SFUser01 (2x);
- a file successfully created in the SFfiles folder for SFUser01;
- successful and unsuccessful results for HRUser01 and Manager01 (6x);

2. Files downloaded from the virtual environment:

- none;

3. Any additional information as directed by the lab:

- none;

4. Lab Assessment (worksheet or quiz - see instructor for guidance)

SECTION 2:

1. Lab Report file including screen captures of the following:

- all new users and groups created in Active Directory;
- PowerShell commands used to restrict the ENGfiles and MKTfiles folders;
- unsuccessful access error message in the LabFiles folder for ENGUser01;
- successful text file creation in the ENGfiles folder for ENGUser01;
- successful and unsuccessful results for MKTUser01 (2x);

2. Files downloaded from the virtual environment:

- none;

3. Any additional information as directed by the lab:

- none.

SECTION 3:

1. Analysis and Discussion
2. Tools and Commands
3. Challenge Exercise

Section 1: Hands-On Demonstration

Note: In this section of the lab, you will follow a step-by-step walk-through of the objectives for this lab to produce the expected deliverable(s).

1. On your local computer, **create** the **Lab Report file**.

Frequently performed tasks, such as how to create the Lab Report file, make screen captures, and download files from the lab, are explained in the Common Lab Tasks document. You should review these tasks before starting the lab.

2. **Proceed** with **Part 1**.

Part 1: User and Group Administration

Note: In the first part of this lab, you will use Microsoft's Active Directory and PowerShell to create three security groups on a remote server. You also will create several user accounts and apply them to the new security groups. Later in the lab, you will see how these objects are used to secure files and folders on the network.

Active Directory is the database that provides a centrally controlled and managed access and security management system for an organization's Windows computer systems. It is much easier and more manageable for an administrator to control user and resource access from one central location than to have to go to each machine on the network and make changes there. In many organizations, it would be impossible to physically access every machine, but Active Directory can virtually access all of the Windows machines in an organization. Machines not on the domain can still be accessed by users if they know the local machine name or IP Address, authorized user name, and password, however, this process is just much easier on Active Directory.

1. On the vWorkstation desktop, **double-click** the **Connections folder**.
2. In the Connections folder, **double-click** the **TargetWindowsDC01 RDP shortcut** to open a remote connection to the TargetWindowsDC01 machine, the Domain Controller for this lab.

If prompted, **type** the following credentials and **click OK**.

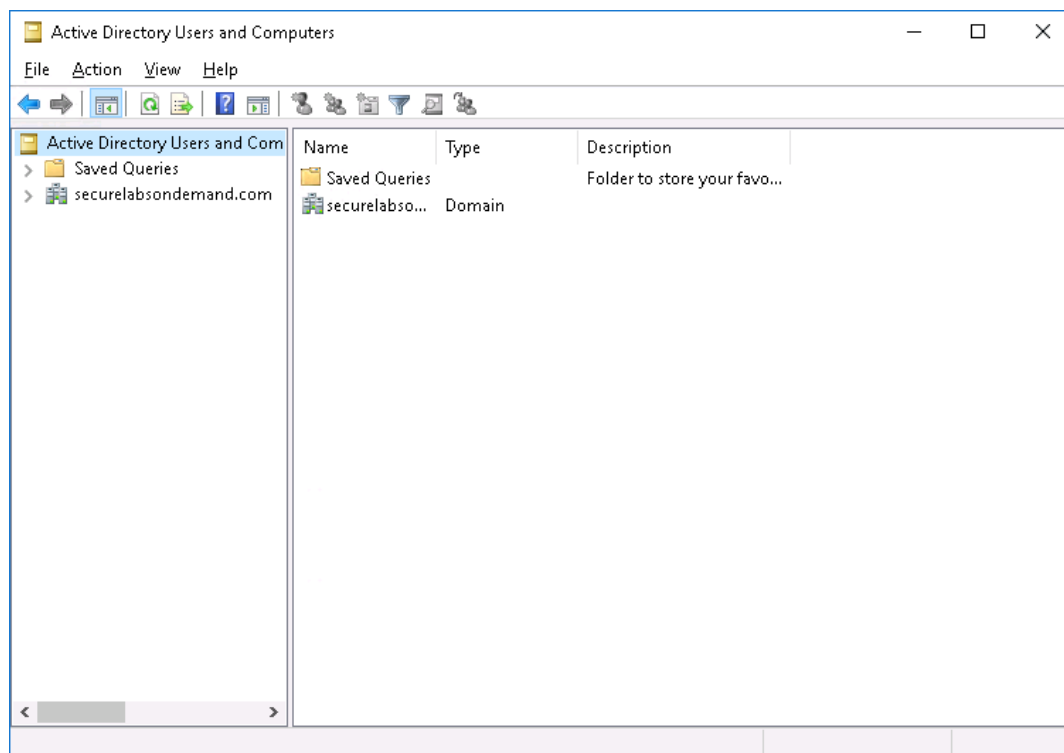
Enabling Windows Active Directory and User Access Controls

Fundamentals of Information Systems Security, Third Edition - Lab 03

- Username: **Administrator**
- Password: **P@ssw0rd!**

The remote desktop will open with the IP address of TargetWindowsDC01 (172.30.0.15) in the title bar at the top of the window.

3. On the TargetWindowsDC01 taskbar, **click** the **Windows Start menu**, then **click** the **Server Manager button** to open the Server Manager application.
4. From the Server Manager menu bar, **click Tools**, then **select Active Directory Users and Computers** to open the Active Directory Users and Computers window.



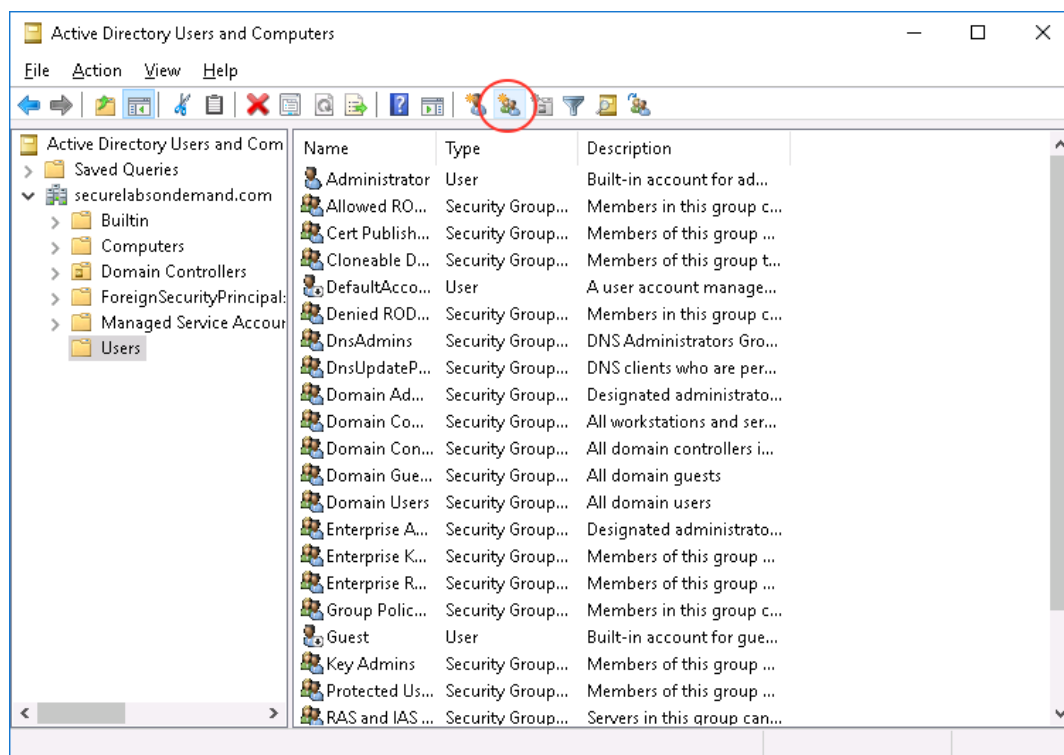
Active Directory Users and Computers

5. In left pane of the Active Directory Users and Computers window, **click** the arrow in front of **securelabsondemand.com** to view the folders in this domain.

Active Directory refers to these folders as Organizational Units.

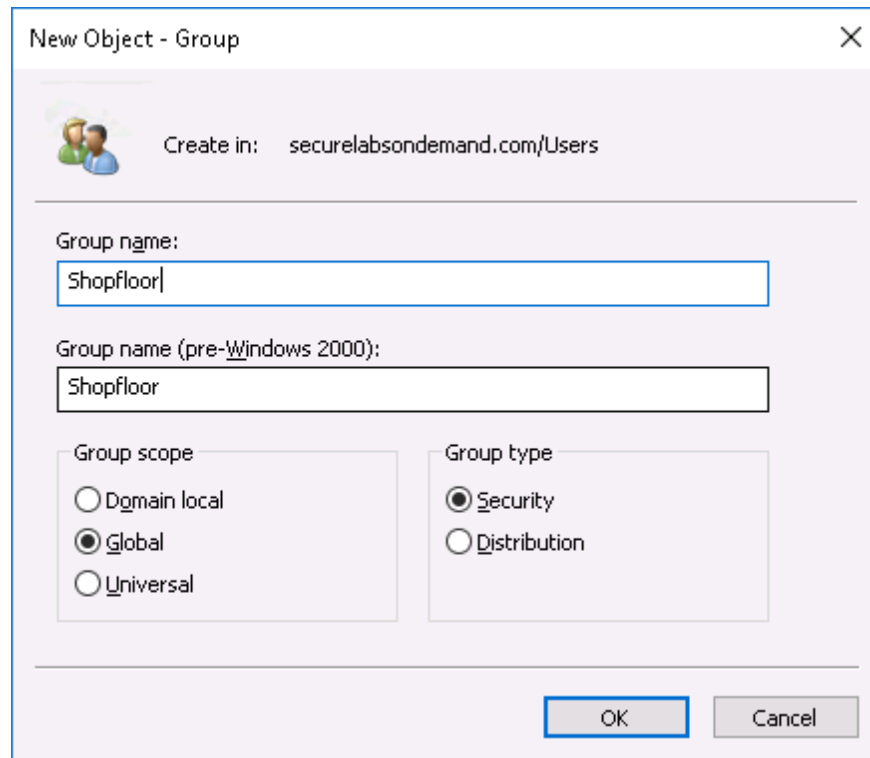
Note: In the next steps, you will use Active Directory to create two new groups in the securelabsondemand domain.

6. In the left pane of the Active Directory Users and Computers window, **click the Users folder** to open the Users Organization Unit.
7. On the Active Directory Users and Computers toolbar, **click the Create a new group in the current container icon** to open the New Object - Group dialog box.



Create a new group icon

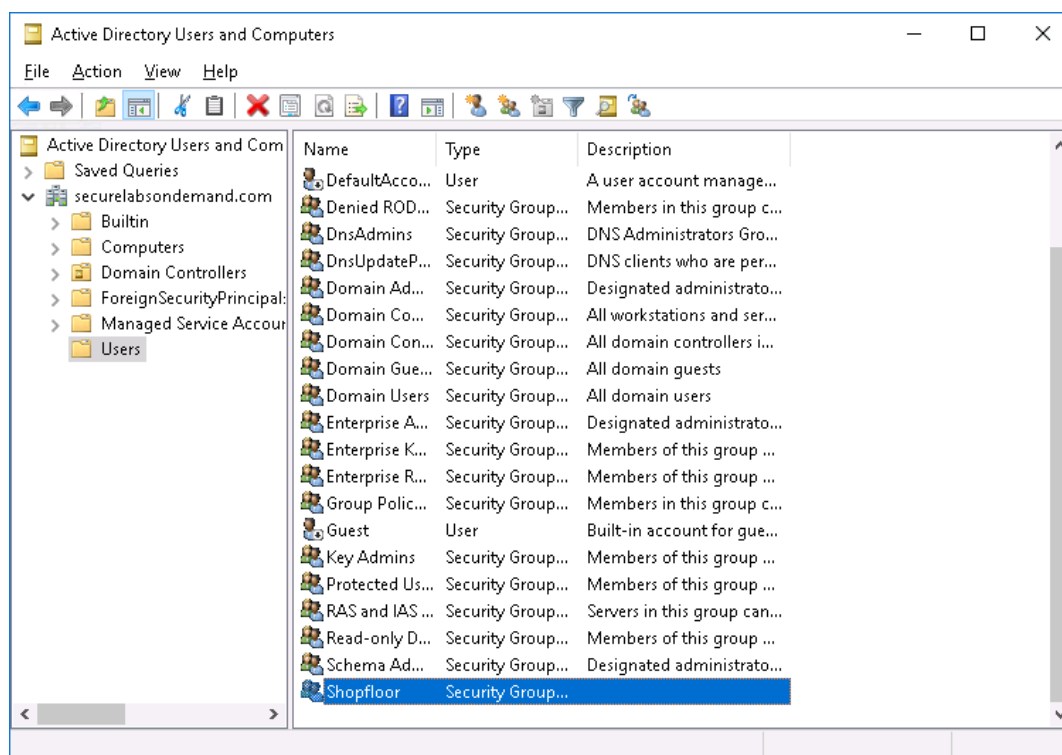
8. In the New Object - Group dialog box, **type Shopfloor** in the Group name box.



Name the new group object

9. In the New Object - Group dialog box, **click OK** to accept the defaults and create a new global security group.

The new group, Shopfloor, is added to the list of users and groups in the right-hand pane.



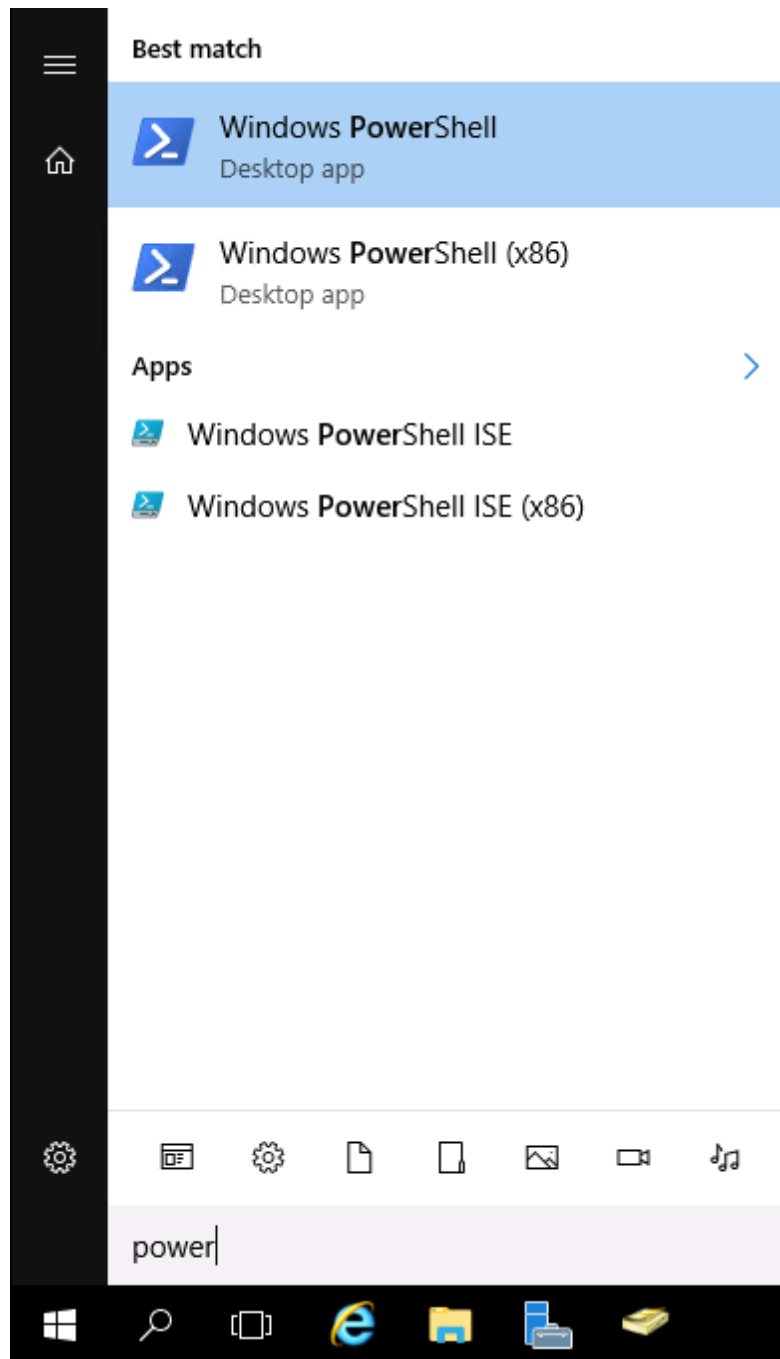
New group listed in Active Directory

10. Repeat steps 7-9 to create a new global security group entitled **Managers**.

11. Minimize the **Active Directory Users and Computers** window.

Note: In the next steps, you will use PowerShell to create another new group in the securelabsondemand domain. Many network administrators prefer to use command-line tools like PowerShell to save time.

12. On the TargetWindowsDC01 taskbar, click the **Windows Start** icon, then type **power** to retrieve the list of possible matches.



Search for PowerShell

13. From the list of matches, **right-click Windows PowerShell** and **select Run as administrator** from the context menu.

Enabling Windows Active Directory and User Access Controls

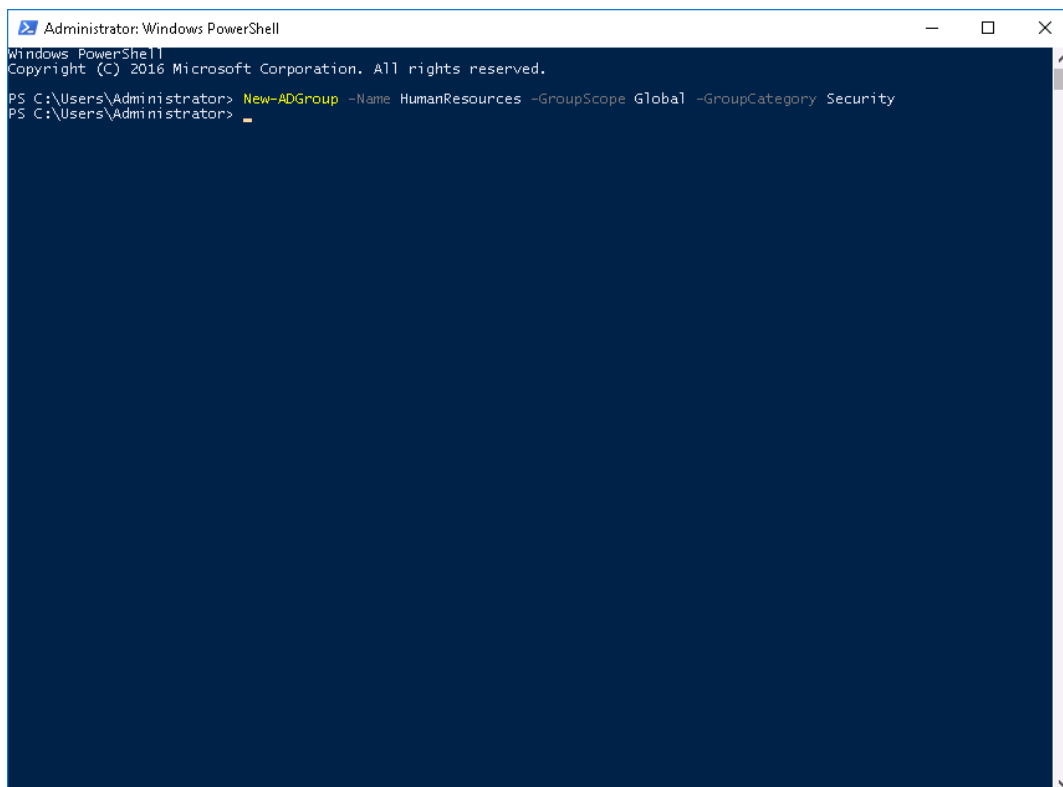
Fundamentals of Information Systems Security, Third Edition - Lab 03

Note: PowerShell uses the .NET framework in the power of a shell that allows for the automation and scripting of a Windows environment. To create a new global security group, you will use the command **New-ADGroup**. This command and the options used in this section are described below:

New-ADGroup -Name HumanResources -GroupScope Global -GroupCategory Security

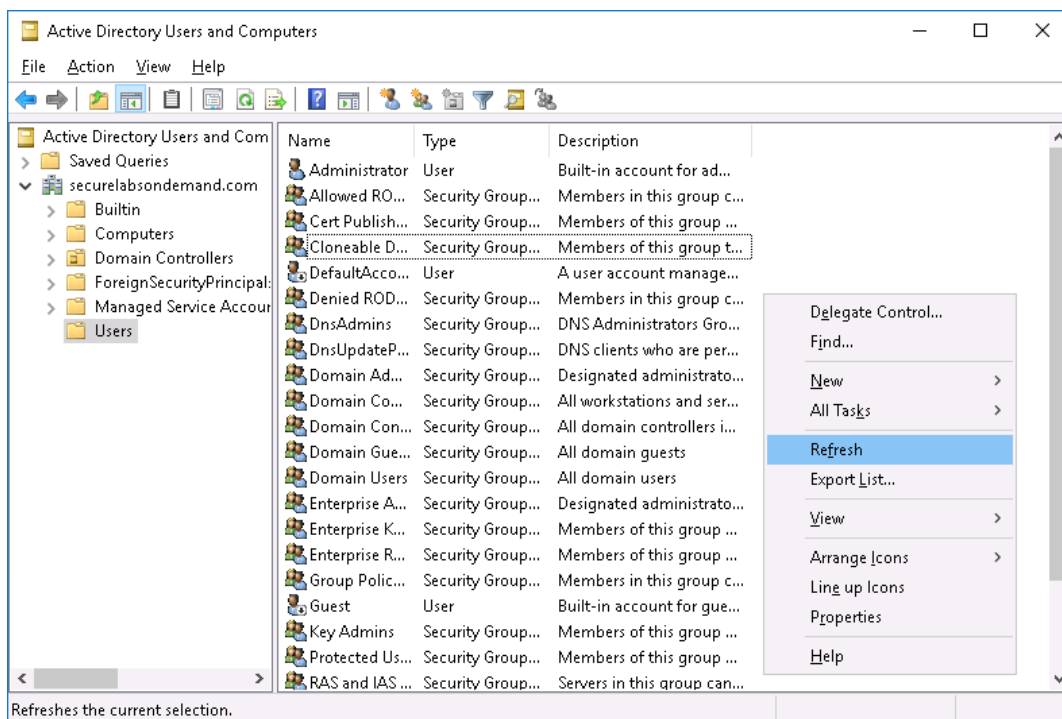
- **New-ADGroup** creates a new Active Directory group. By default, NewADGroup creates the group in the Users OU (Organizational Unit).
- **-Name** specifies the name of the group. This is a required field and the system will prompt you for a name if you do not specify it when issuing the command.
- **-GroupScope** specifies how the group is applied to the domain. There are three possible options for scope: Universal, Global, or Domain Local. This is a required field.
- **-GroupCategory** specifies the type of group. There are two possible options for category: Distribution (email) or Security.

14. At the PowerShell prompt, **type New-ADGroup -Name HumanResources -GroupScope Global -GroupCategory Security** and **press Enter** to create the new group.



Add an Active Directory Group in PowerShell

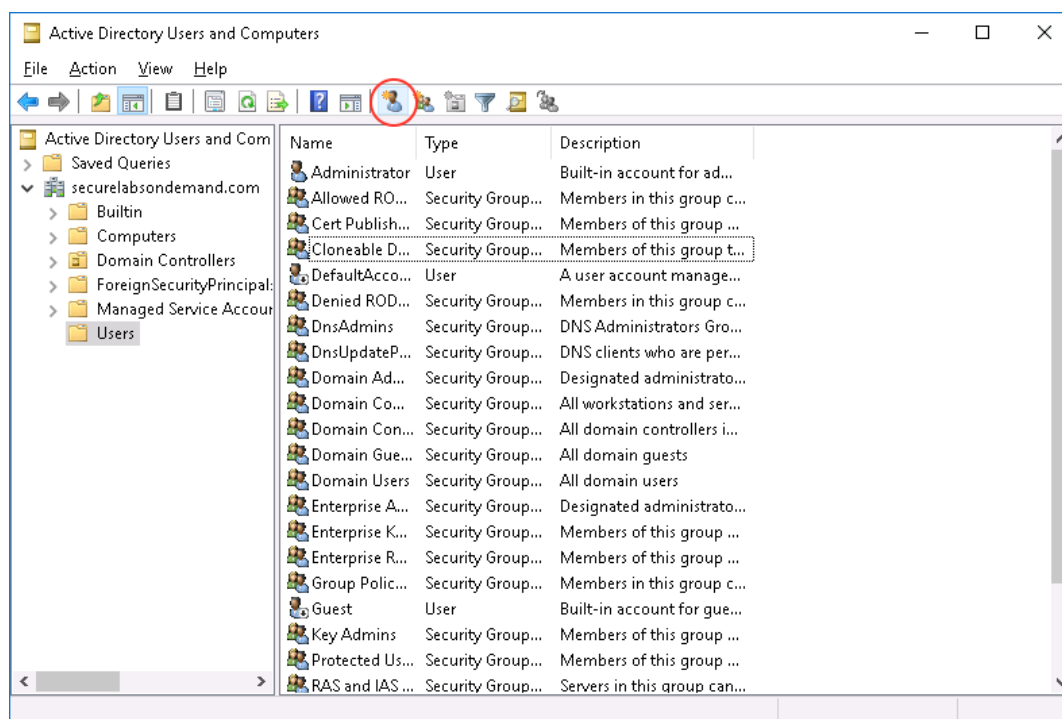
15. From the TargetWindowsDC01 taskbar, **restore** the **Active Directory Users and Computers** window.
16. In the right pane, **right-click** any empty area and **click Refresh** to verify that the new HumanResources group was added to the Users OU.



Refresh Active Directory Users and Computers

Note: In the next steps, you will use the Active Directory Users and Computers tool to create new users and add them to one of the global security groups you created in the previous steps.

17. On the Active Directory and Computers toolbar, **click** the **Create a new user in the current container** icon.



Create a new user icon

18. In the New Object – User dialog box, **type** the following information, then **click Next** to continue.

- First name: **SFUser**
- Last name: **01**
- User logon name: **SFUser01**

The Full name and User logon name (pre-Windows 2000) boxes will populate automatically.

New Object - User

Create in: securelabsondemand.com/Users

First name: SFUser Initials:

Last name: 01 Full name: SFUser 01

User logon name: SFUser01 @securelabsondemand.com

User logon name (pre-Windows 2000): SECURELABSONDEM\ SFUser01

< Back Next > Cancel

Name the new user object

19. In the New Object – User dialog box, **type** the following information.

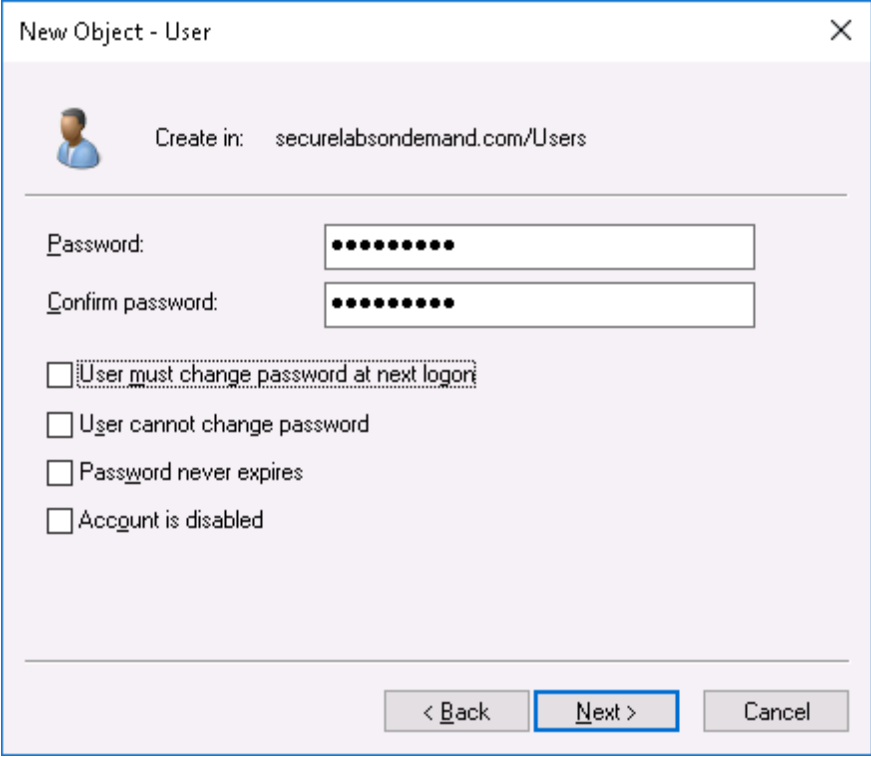
- Password: **P@ssw0rd!**
- Confirm password: **P@ssw0rd!**

Note: Here are some of the standard rules for secure password selection. These rules are not unique to this course, but used as guidelines for all passwords used in a production system:

- Never leave the Administrator account named Administrator
- Never use easily guessed passwords
- Do use a non-sequential set of letters, numbers, upper, lower, and special characters
- Change your passwords frequently
- Maintain your password policy; it's difficult, but necessary
- Wherever possible use two factor authentication (such as RSA Secure ID)

Another important password rule: never include any part of the account's username in a password. Typically, the username is easily discovered—the username is usually visible on the login screen and follow recognizable conventions within an organization. Including the username within the password gives the hacker half of the password and is poor security at best. The password used in this lab, *P@ssw0rd!*, follows many of these standard rules.

20. In the New Object – User dialog box, **click the User must change password at next logon checkbox** to remove the check and verify that all checkboxes are unchecked.

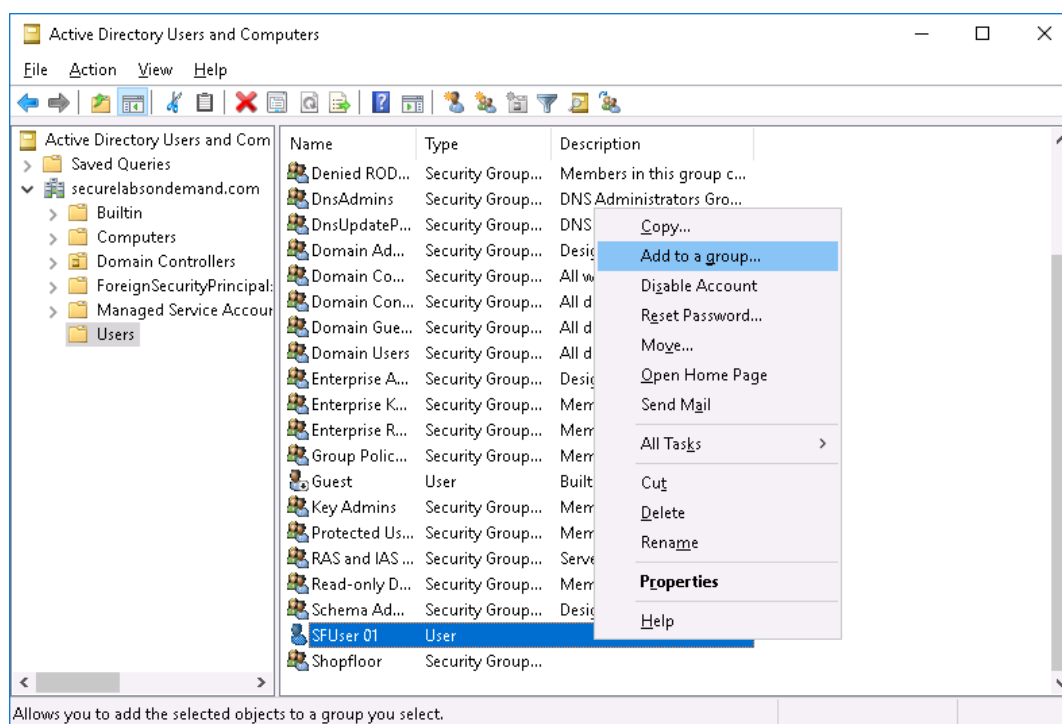


Create a password for a new user

21. In the New Object – User dialog box, **click Next** to continue.
22. In the New Object – User dialog box, **click Finish** to create the new user account.

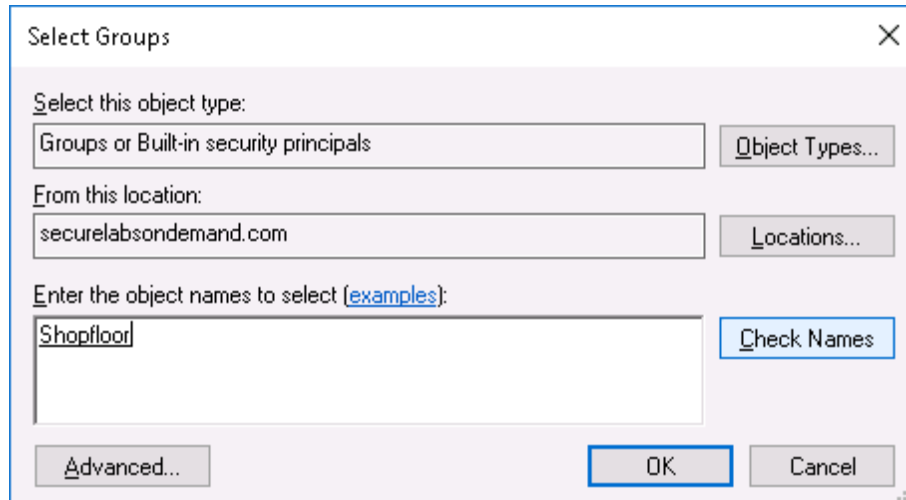
The new user will appear in the right pane with the groups you created earlier.

23. From the Users list, **right-click** the **SFUser01** user account and **select Add to a group** from the context menu.



Add user to a group

24. In the Select Groups dialog box, **type Shopfloor** in the Enter the object name to select textbox, then **click Check Names** to confirm that the group exists and is spelled correctly.



Add the user to an existing group

25. In the Select Groups dialog box, **click OK** to complete the process.

26. **Click OK** to close the success message.

27. **Repeat steps 17-22** to create the following new user.

- First name: **Manager**
- Last name: **01**
- User logon name: **Manager01**

28. **Repeat steps 24-27** to add Manager01 to the Shopfloor and Managers groups.

To add a user to more than one group in the same step, separate the group names with a semicolon before clicking the Check Names button.

29. **Restore the PowerShell window.**

Note: In the next steps, you will first use PowerShell to create another new user with the command *New-ADUser*. The command and its options are described below:

```
New-ADUser -Name HRUser01 -UserPrincipalName  
HRUser01@securelabsondemand.com -AccountPassword (ConvertTo-SecureString  
-AsPlainText "P@ssw0rd!" -Force) -GivenName HRUser -Surname 01 -Enabled  
$true
```

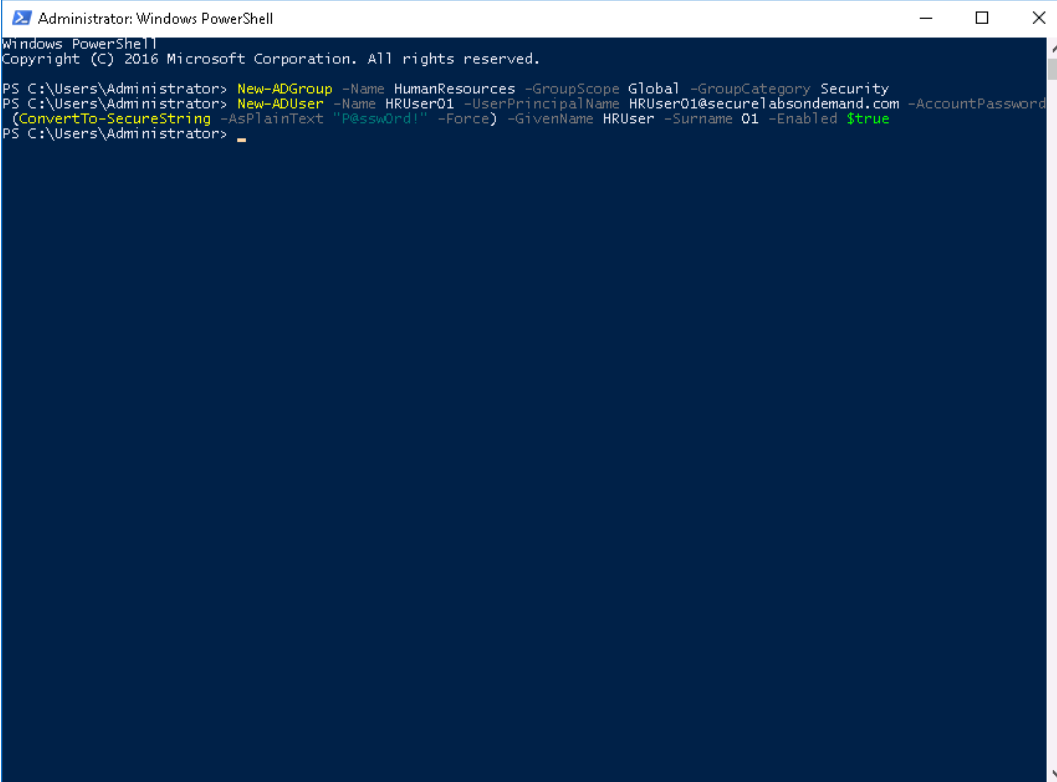
- **New-ADUser** creates a new user account in Active Directory.
- **-Name** specifies the name of the object in Active Directory.
- **-UserPrincipalName** determines the logon name for the new user.
- **-AccountPassword** specifies a password for the new user account. If you do not set a password when the account is created, it will be disabled until you set a password. A password can be set using the *Set-ADAccountPassword* command in a separate step.
- **-GivenName** sets the user's first name.
- **-Surname** specifies the user's last name.
- **-Enabled** enables the account (\$true) only if a password is set.

Next, you will add that new user to an existing global security group using the *New-ADUser* command described below:

```
Add-ADGroupMember -Identity HumanResources -Members HRUser01
```

- **Add-ADGroupMember** adds a user account to an Active Directory group.
- **-Identity** specifies the group to which you want to add user account(s).
- **-Members** identifies the user(s) that will be added to the group.

30. At the PowerShell prompt, **type** `New-ADUser -Name HRUser01 -UserPrincipalName HRUser01@securelabsondemand.com -AccountPassword (ConvertTo-SecureString -AsPlainText "P@ssw0rd!" -Force) -GivenName HRUser -Surname 01 -Enabled $true` and **press Enter** to create the HRUser01 account.

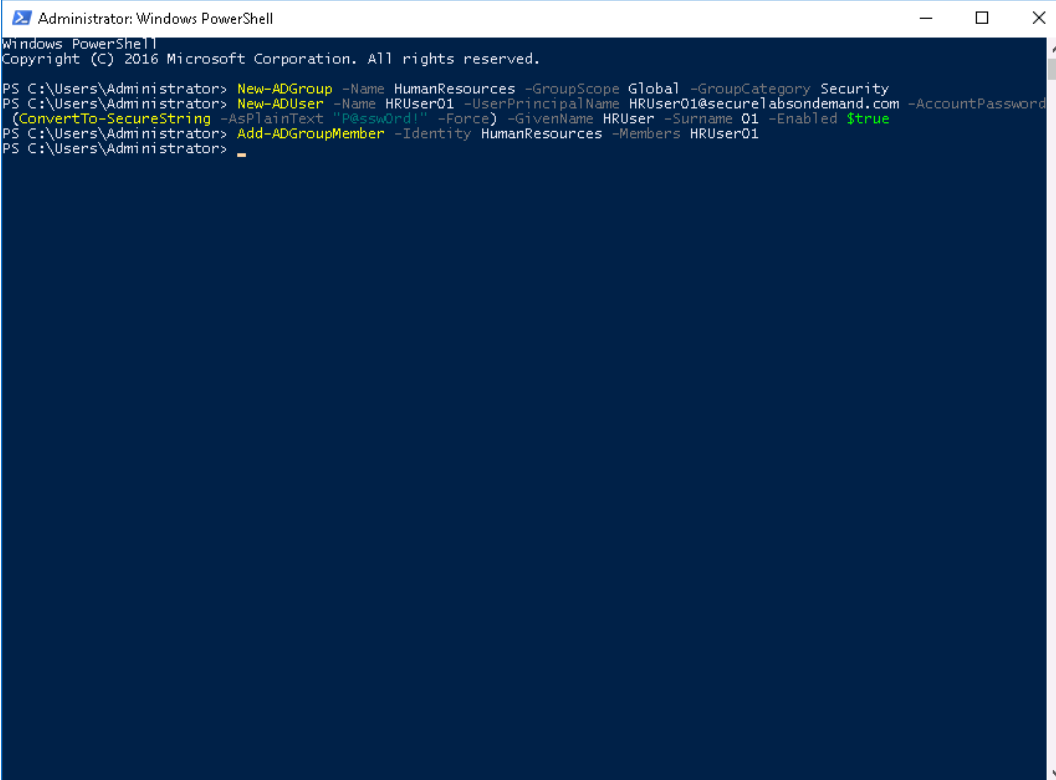


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> New-ADGroup -Name HumanResources -GroupScope Global -GroupCategory Security
PS C:\Users\Administrator> New-ADUser -Name HRUser01 -UserPrincipalName HRUser01@securelabsondemand.com -AccountPassword
(ConvertTo-SecureString -AsPlainText "Password!" -Force) -GivenName HRUser -Surname 01 -Enabled $true
PS C:\Users\Administrator> _
```

Create HRUser01

31. At the PowerShell prompt, **type** `Add-ADGroupMember -Identity HumanResources -Members HRUser01` and **press Enter** to add HRUser01 to the HumanResources group.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> New-ADGroup -Name HumanResources -GroupScope Global -GroupCategory Security
PS C:\Users\Administrator> New-ADUser -Name HRUser01 -UserPrincipalName HRUser01@securelabsondemand.com -AccountPassword
(ConvertTo-SecureString -AsPlainText "Password!" -Force) -GivenName HRUser -Surname 01 -Enabled $true
PS C:\Users\Administrator> Add-ADGroupMember -Identity HumanResources -Members HRUser01
PS C:\Users\Administrator>
```

Add HRUser01 to HumanResources

32. **Restore** the **Active Directory Users and Computers** window.
33. In the right pane, **right-click** any empty area and **click Refresh** to verify that the new HumanResources group was added to the Users OU.
34. **Make a screen capture** showing all of the **new users and groups** created in the previous steps and **paste** it into the Lab Report file.

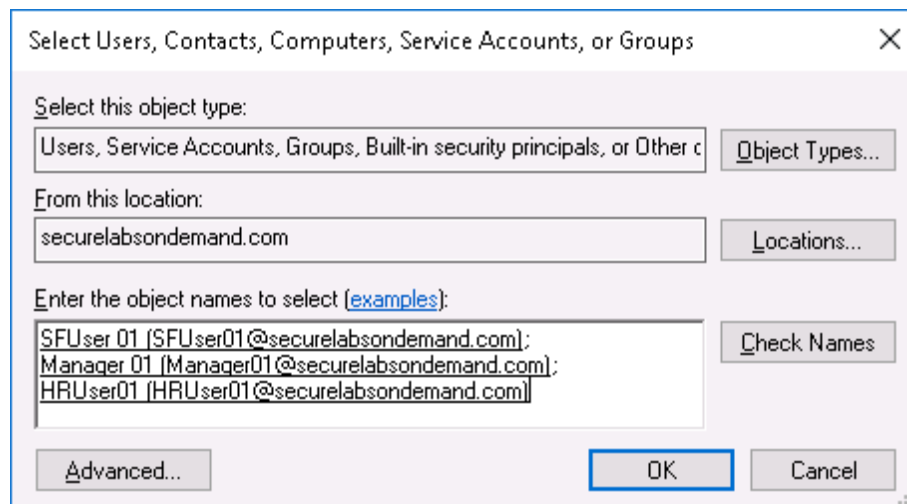
You may use multiple screen captures to view all of the new users and groups.

Note: In the next steps, you will use Active Directory to add the new user accounts to a Builtin (built-in) group called Remote Desktop Users. Members of this group are allowed to use the remote desktop services in the lab to connect to remote machines. You will need this access later in the lab.

35. In the left pane of the Active Directory Users and Computers window, **click** the **Builtin folder** to view the built-in Organizational Unit.
36. In the right pane, **double-click** the **Remote Desktop Users group object** to open the Remote Desktop Users Properties window.
37. In the Remote Desktop Users Properties dialog box, **click** the **Members tab** to see all of the members of this group.

By default, this group is empty.

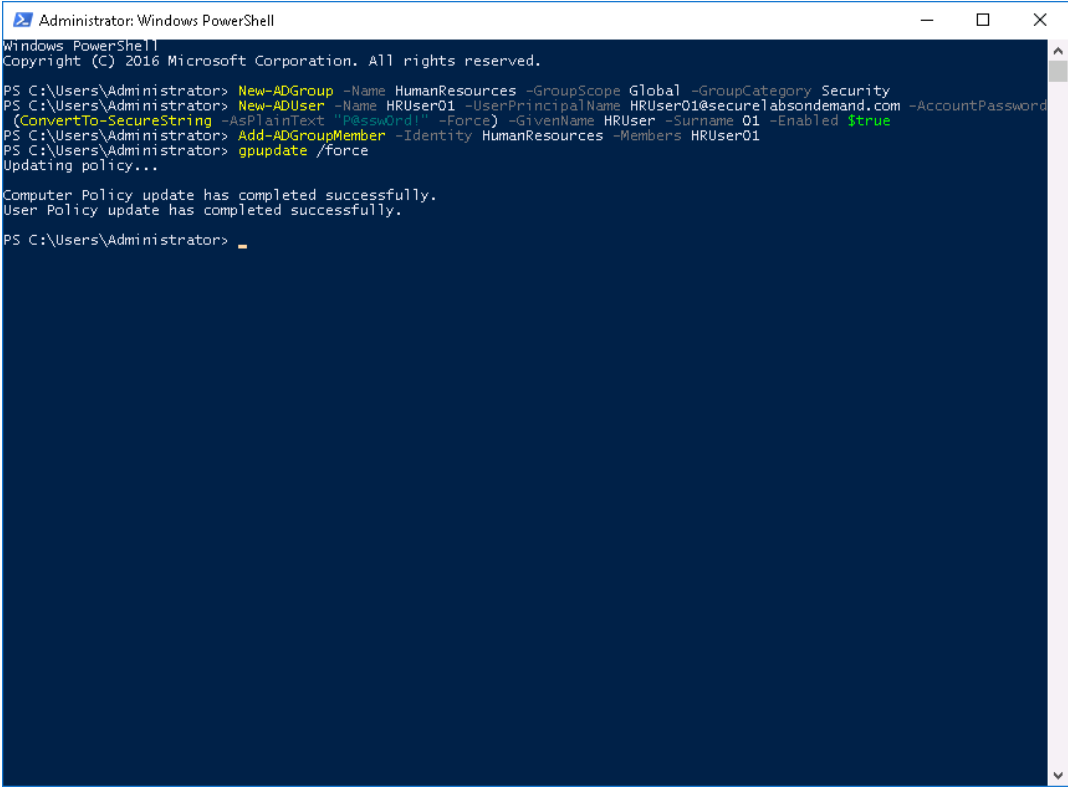
38. In the Remote Desktop Users Properties window, **click** the **Add button** to open the Select Users, Contacts, Computers, or Groups dialog box.
39. In the Enter the object names to select box, **type** **SFUser01; Manager01; HRUser01** and **click Check Names** to verify that the new users can be found.



Adding users to a built-in security group

40. **Click OK** to add the users and close the dialog box.
41. **Click OK** to close the Remote Desktop Users Properties window.
42. **Close** the **Active Directory Users and Computers** window.
43. **Close** the **Server Manager** window.
44. **Restore** the **PowerShell** window.
45. At the PowerShell prompt, **type `gpupdate /force`** and **press Enter** to force an immediate update of all Group Policies on the Domain Controller.

The system will generate a confirmation message indicating that the Computer and User Policy update has been updated successfully.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> New-ADGroup -Name HumanResources -GroupScope Global -GroupCategory Security
PS C:\Users\Administrator> New-ADUser -Name HRUser01 -UserPrincipalName HRUser01@securelabsondemand.com -AccountPassword
(ConvertTo-SecureString -AsPlainText "Password!" -Force) -GivenName HRUser -Surname 01 -Enabled $true
PS C:\Users\Administrator> Add-ADGroupMember -Identity HumanResources -Members HRUser01
PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator>
```

GPUPDATE

46. **Close the PowerShell window.**

Note: One of the biggest challenges faced by a Windows administrator is how to handle guest users, such as contract workers, auditors, or partners. Typically, best practices would dictate that a guest would be placed in a secure network, isolated from the production network by firewall barriers. If this is not practical, which is often the case with auditors, then clear and specific areas of access should be decided, making them as restrictive as possible. For CIA requirements, local, self-signed certificates are issued to guests who require a higher degree of access. These certificates expire on a specific date and limit the guest's access. Of course, Access Control Lists to strictly control the access is also mandatory and disabling the guest user in favor of creating short term user accounts will help as well. Creating guest user templates that have the USB ports and CD's disabled is a means of stopping the introduction of unwanted data, and the theft of company data. Using the newer system of Windows archiving makes restoring any compromised documents easier.

Part 2: Resource Management

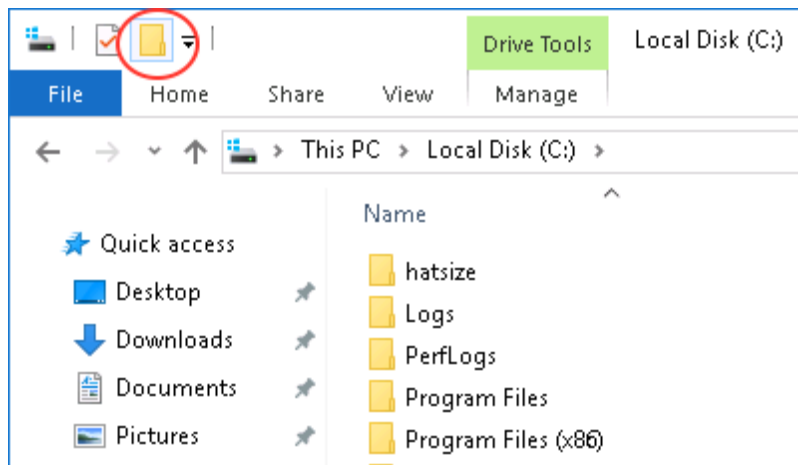
Note: In the next steps, you will use File Explorer and PowerShell to create a subfolder for each of the work teams in the lab: one for the employees on the shop floor, one for managers, and one for HR personnel. You will then assign explicit permissions for each folder as indicated in the following table.

Security Groups	Access to HRfiles	Access to MGRfiles	Access to SFfiles
Shopfloor			X
Managers		X	X
HumanResources	X		

Enabling Windows Active Directory and User Access Controls

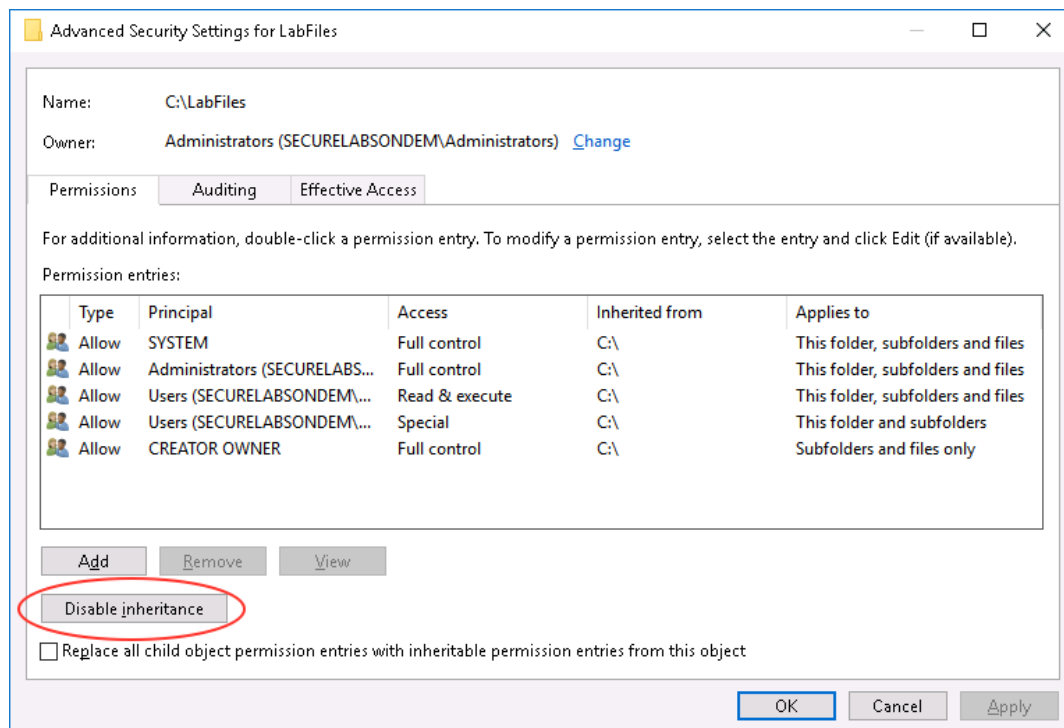
Fundamentals of Information Systems Security, Third Edition - Lab 03

1. On the TargetWindowsDC01 taskbar, **click the File Explorer icon** to open a File Explorer window.
2. In the File Explorer, **navigate** to the C: drive (**This PC > Local Disk (C:)**).
3. On the File Explorer Quick Access Toolbar, **click the New Folder button** to create a new folder.



Create a new folder

4. In the Folder Name field, **type LabFiles** and **press Enter** to name the new folder.
5. In the File Explorer, **right-click** the new **LabFiles folder**, and **select Properties** from the context menu to open the LabFiles Properties dialog box.
6. In the LabFiles Properties dialog box, **click the Security tab**.
7. In the LabFiles Properties dialog box, **click the Advanced button** to open the Advanced Security Settings for LabFiles dialog box.
8. In the Advanced Security Settings for LabFiles dialog box, **click the Disable Inheritance button** to disable inheritance to the sub-folders in the LabFiles folder.

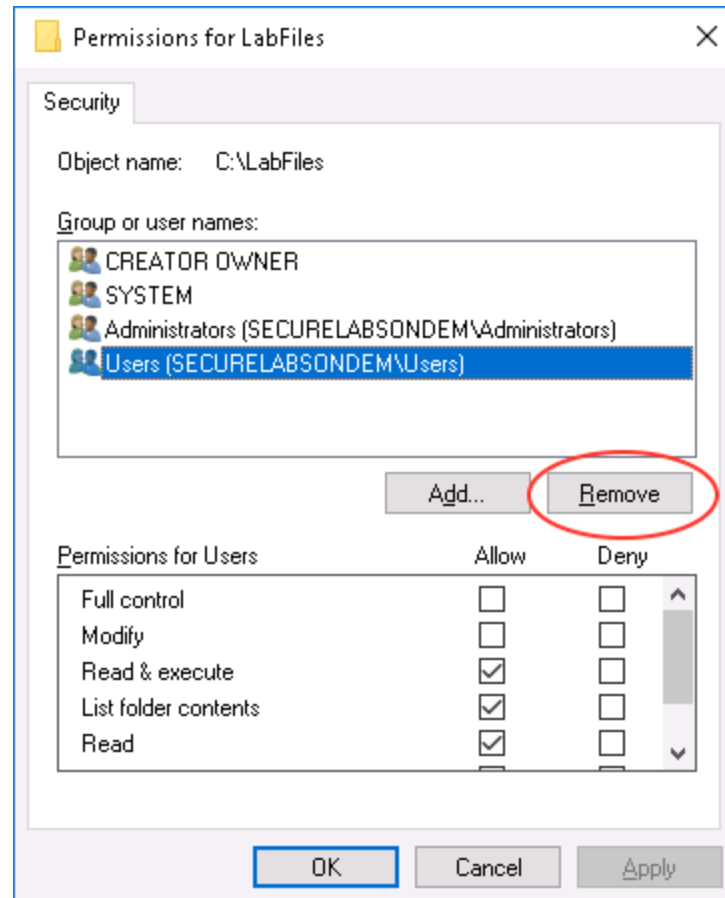


Advanced Security Settings

Note: By default, Windows will inherit the permissions of the parent folder so that all sub-folders will have the same permissions as the parent. Disabling inheritance now will enable you to specify permissions for each sub-folder.

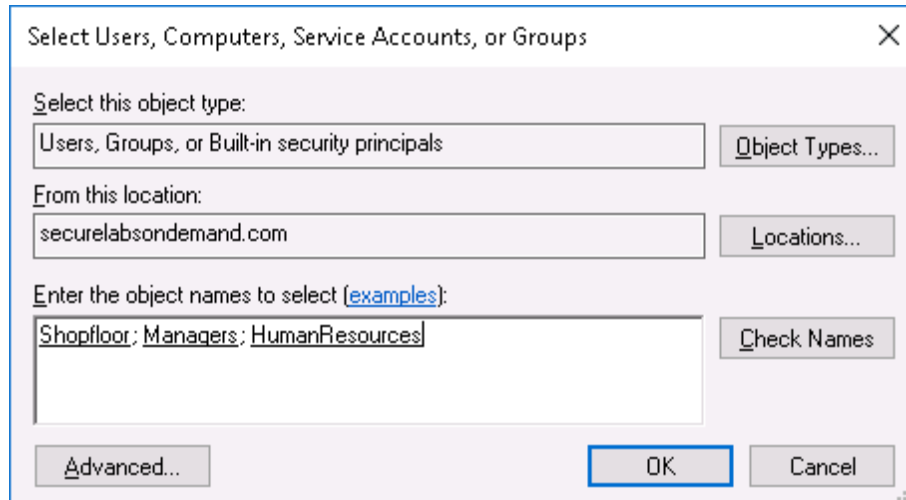
- When prompted, **click the Convert inherited permission into explicit permissions options button.**
- Click OK** to close the Advanced Security Settings for LabFiles dialog box.
- In the LabFiles Properties dialog box, **click Edit** to open the Permissions for LabFiles dialog box.
- In the Permissions for LabFiles dialog box, **click the Users (SECURELABSONDEM\Users) group and click Remove** to prevent everyone except the built-in administrative accounts (Administrators, SYSTEM, and CREATOR OWNER) from being able to access this folder and

its files.



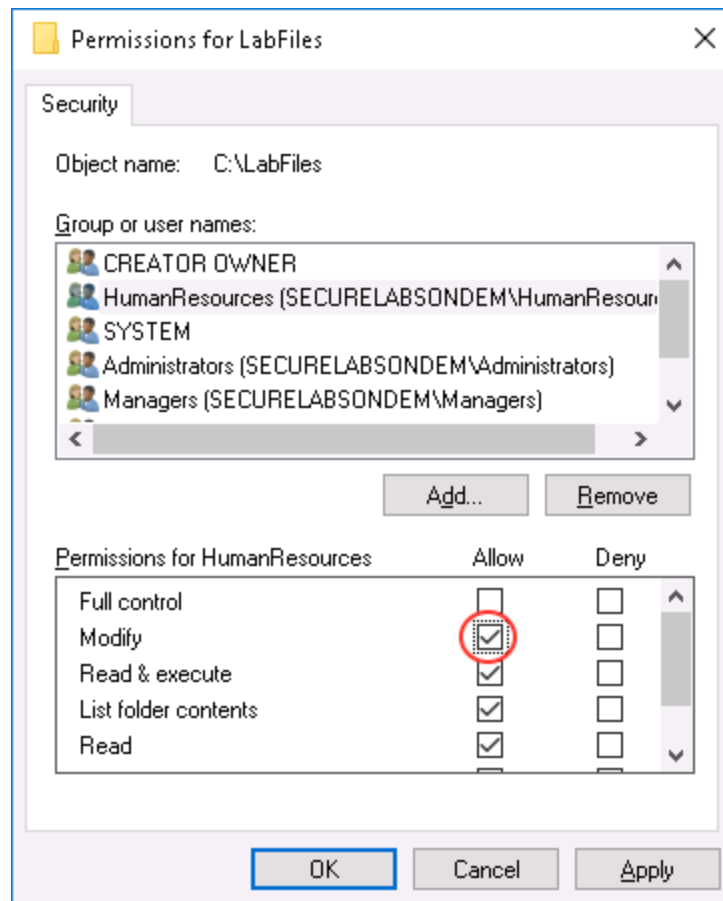
Remove domain users

13. In the Permissions for LabFiles dialog box, **click the Add button** to open the Select Users, Computers, Service Accounts, or Groups dialog box.
14. In the Enter the object names to select box, **type Shopfloor; Managers; HumanResources** and **click Check Names** to verify that the new users can be found.



Add security groups to a folder

15. **Click OK** to save the new settings.
16. In the Permissions dialog box, **click HumanResources**, then **click the Modify checkbox** in the Allow column to allow members of the HumanResources security group to modify files and folders within the LabFiles folder.



Edit a user's security permissions

Note: The Read and Execute option is used to allow users to view the folder's contents as well as execute scripts. The List folder contents option can be used as a means to traverse a folder but not open any of the files in an instance where you needed to give a user access to a file deeper in a set of folders. In that case, only that option would be checked, all other boxes would remain unchecked.

17. **Repeat step 16** for each of the new security groups.

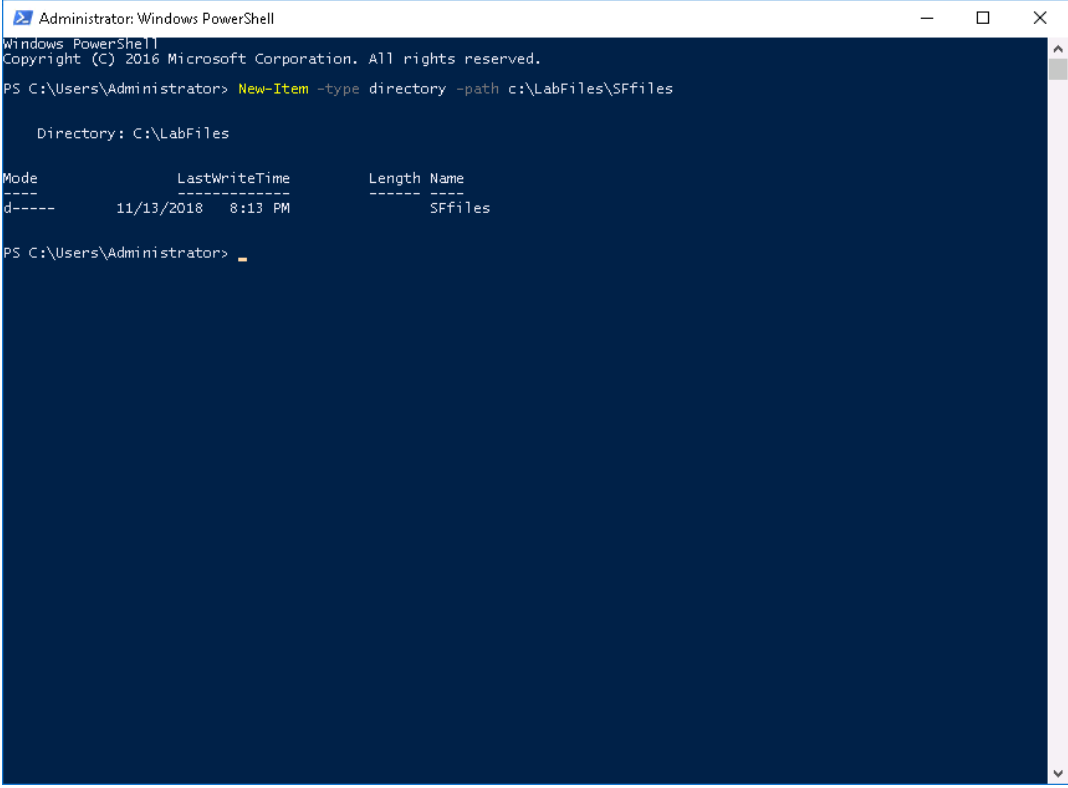
- **Managers**
- **Shopfloor**

18. **Click OK** to close the Permissions for LabFiles Properties dialog box.

19. **Click OK** to close the LabFiles Properties dialog box.
20. In the File Explorer, **double-click** the **LabFiles folder** to open it.
21. On the File Explorer Quick Access toolbar, **click** the **New Folder button** to create a new folder.
22. When prompted, **type HRfiles** to name a new folder.
23. **Repeat steps 21-22** to create a MGRfiles folder.
24. From the TargetWindowsDC01 taskbar, **click** the **Windows Start icon** and **type power** to retrieve the list possible matches.
25. In the list of matches, **right-click Windows PowerShell** and **click Run as administrator** from the context menu.

You will use the PowerShell application to create the final folder necessary to complete this activity.

26. At the PowerShell prompt, **type New-Item -type directory -path c:\LabFiles\SFfiles** and **press Enter** to create a new SFfiles directory under the LabFiles folder.



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt shows the execution of the command `New-Item -type directory -path c:\LabFiles\SFiles`. The output displays the directory path `Directory: C:\LabFiles` and a table of file system information.

Mode	LastWriteTime	Length	Name
d-----	11/13/2018 8:13 PM		SFiles

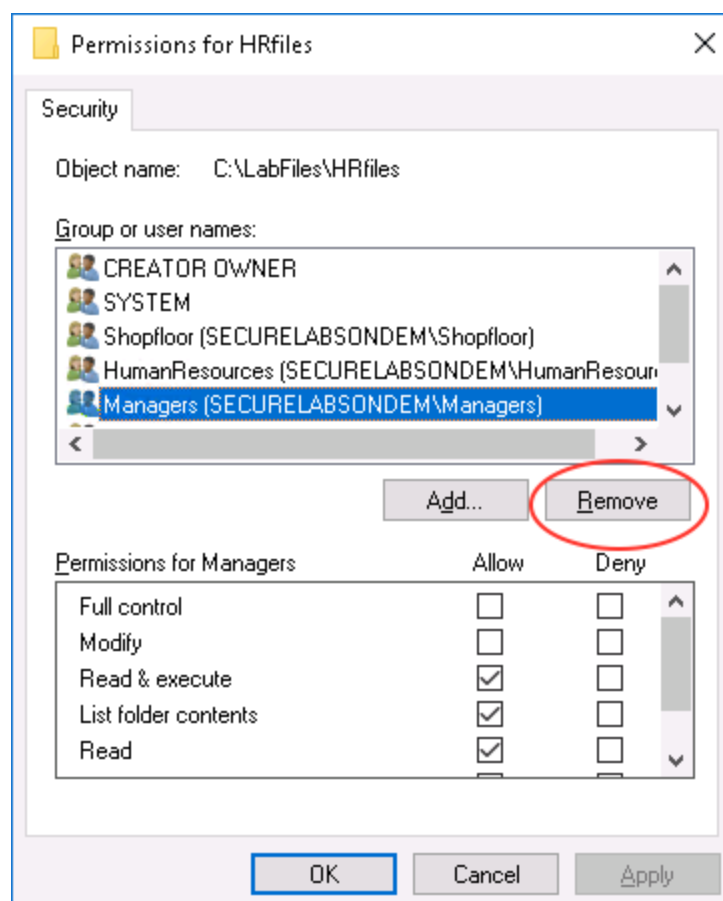
The PowerShell prompt is now at `PS C:\Users\Administrator>`.

Create SFiles directory

27. At the Powershell prompt, **type exit** and **press Enter** to close the PowerShell window, then **restore** the **File Explorer** window.
28. In the File Explorer, **right-click** the **HRfiles folder** and **select Properties** from the context menu to open the HRfiles Properties dialog box.
29. In the HRfiles Properties dialog box, **click** the **Security tab**.
30. In the HRfiles Properties dialog box, **click** the **Advanced button** to open the Advanced Security Settings for HRfiles dialog box.
31. In the Advanced Security Settings for HRfiles dialog box, **click** the **Disable Inheritance button** near the bottom of the dialog box.

Note: By default, Windows will inherit the permissions of the parent folder so that all subfolders will have the same permissions as the parent. Disabling inheritance now will enable you to specify permissions for each subfolder.

32. When prompted, **click the Convert inherited permission into explicit permissions options button.**
33. **Click OK** to close the Advanced Security Settings for HRfiles dialog box.
34. In the HRfiles Properties dialog box, **click Edit** to edit the security permissions for this folder.
35. In the Group or user names box, **click the Managers (SECURELABSONDEM\Managers) group** and **click Remove** to prevent members of this group from being able to access the HRfiles folder and its files.



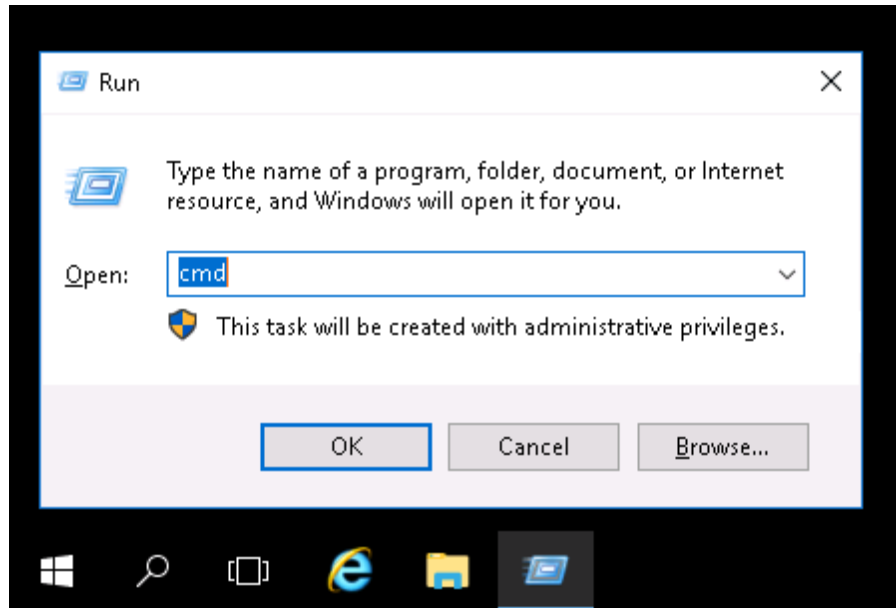
Remove Managers group from folder

36. **Repeat step 35** to prevent members of the Shopfloor group from accessing the HRfiles folder.
37. **Click OK** to close the Permission for HRfiles dialog box.
38. **Click OK** to close the HRfiles Properties dialog box.
39. **Repeat steps 28-38** to restrict the MGRfiles folder to the Managers group, removing the HumanResources and Shopfloor groups.
40. **Repeat steps 28-38** to restrict the SFfiles folder to the Shopfloor *and* the Managers groups, removing the HumanResources group.
41. **Close the File Explorer.**

Part 3: Group Policy

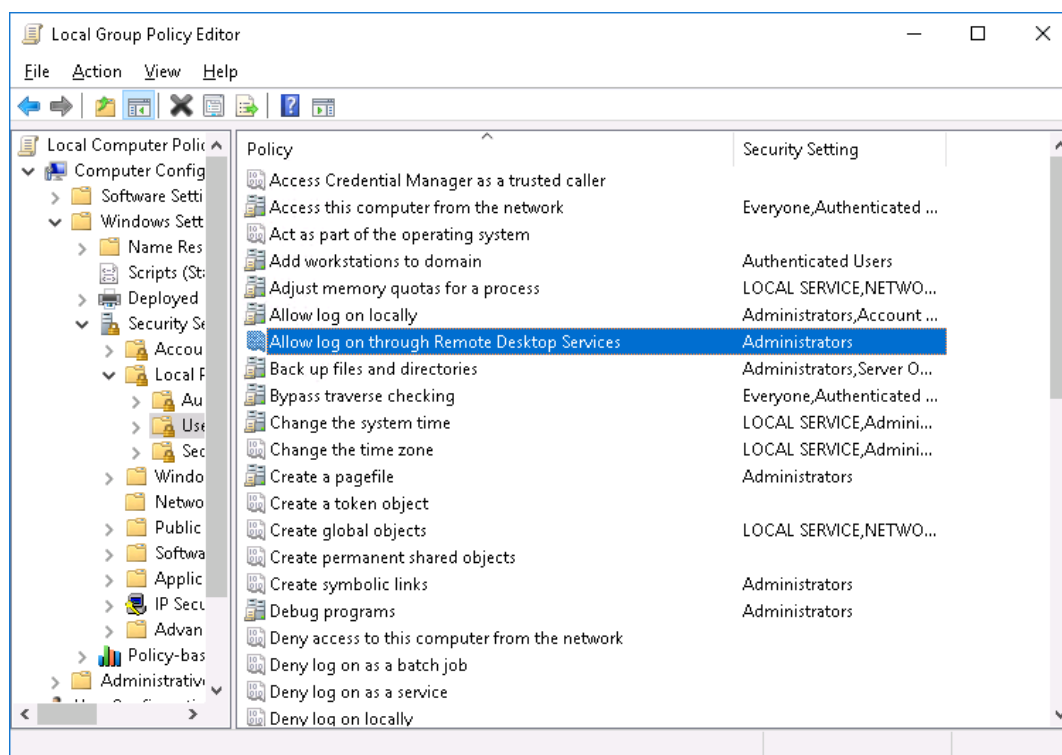
Note: In the next steps, you will use the Group Policy Object Editor to modify permissions on the TargetWindowsDC01 server to allow these new users to use the remote desktop services. Windows Group Policy is a very powerful, granular method of controlling machine and user access and experience on the Windows desktop and network. This tool is used on either a local or domain level to control access to many local computer and network resources such as drives, Internet access, kiosk mode, etc. It is a very powerful tool used by administrators frequently.

1. **Right-click the Windows Start icon** and **select Run** from the context menu.



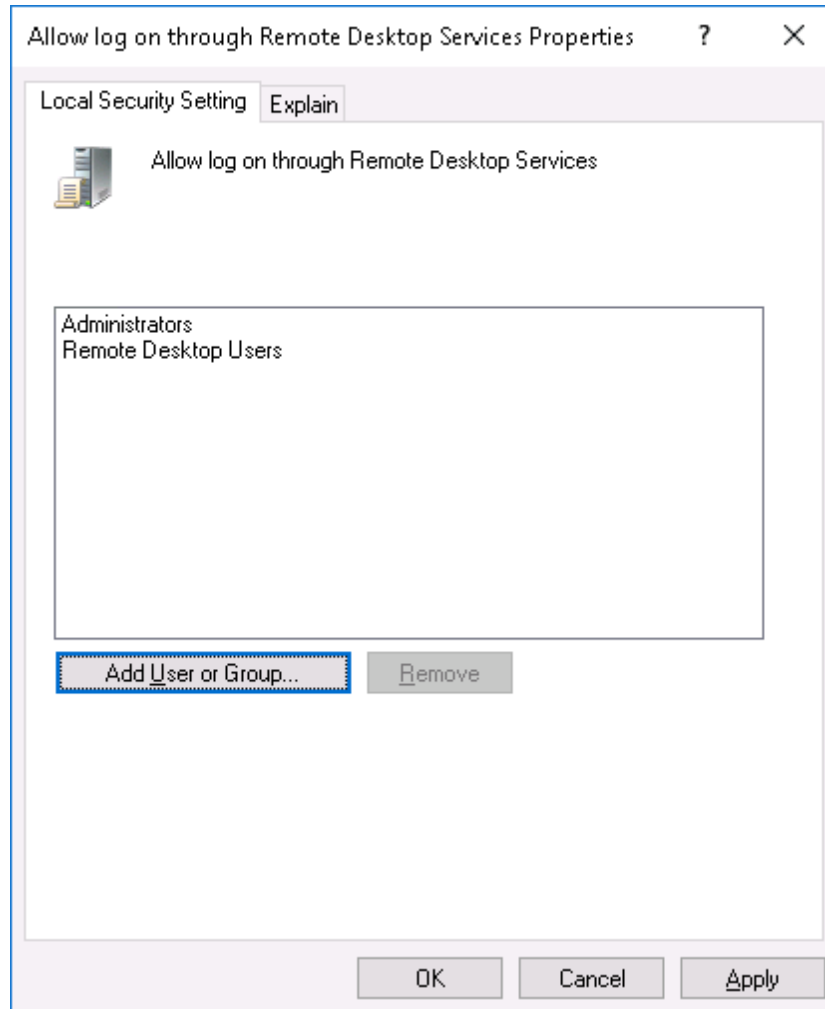
Run dialog box

2. In the Run dialog box, **type `gpedit.msc`** and **press Enter** to open the Local Group Policy Editor.
3. In the left pane of the Local Group Policy Editor, **navigate** to the User Rights Assignment folder (**Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment**).
4. In the right pane, **double-click** the **Allow log on through Remote Desktop Services policy** to open the Allow logon through Remote Desktop Services Properties dialog box.



Access the remote desktop services group policy

5. In the Allow logon through Remote Desktop Services Properties dialog box, **click the Add User or Group button** to open the Select Users, Groups, or Objects dialog box.
6. In the Enter the object names to select box, **type Remote Desktop Users** and **click Check Names** to validate the group name.
7. **Click OK** to save the changes and close the dialog box.



Properties for the remote desktop services policy

8. **Click OK** to close the Allow logon though Remote Desktop Services Properties dialog box.
9. **Close** the **Local Group Policy Editor** window.
10. **Close** the remote **TargetWindowsDC01** connection.

Part 4: Practical Application

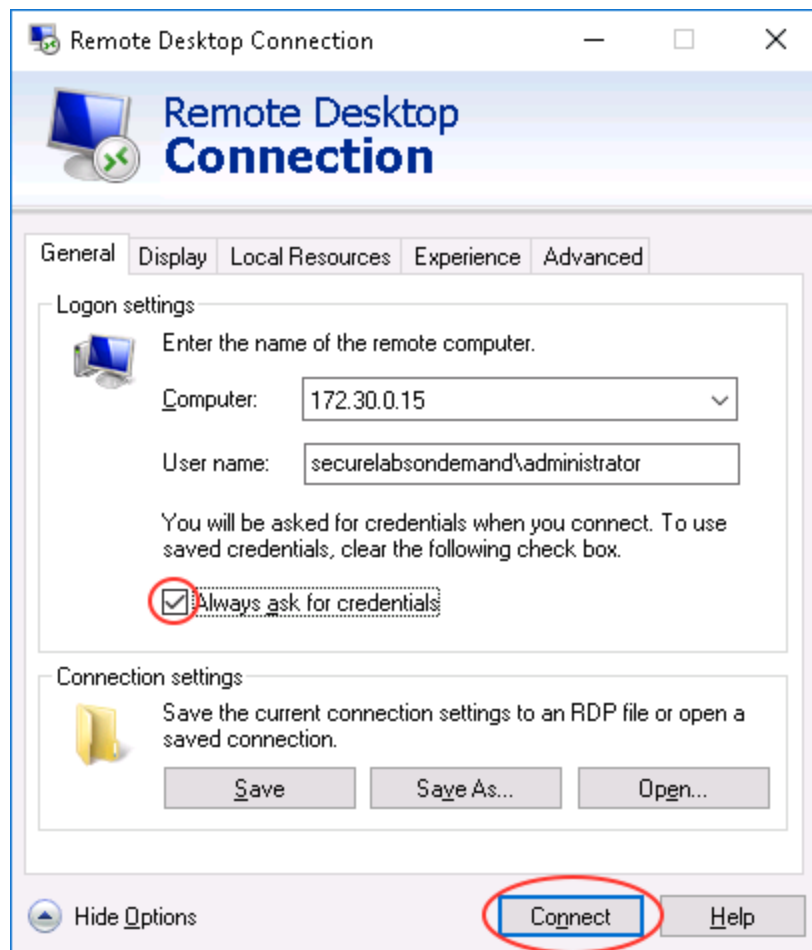
Note: In the next steps, you will conduct a test to verify that the new users can use the remote

desktop services to access the TargetWindowsDC01 server and modify the folder to which each account has access.

First, you will need to modify the shortcut to allow you to log in with a different user account, since the existing shortcut is pre-configured to automatically log in to the TargetWindowsDC01 machine using the Administrator account.

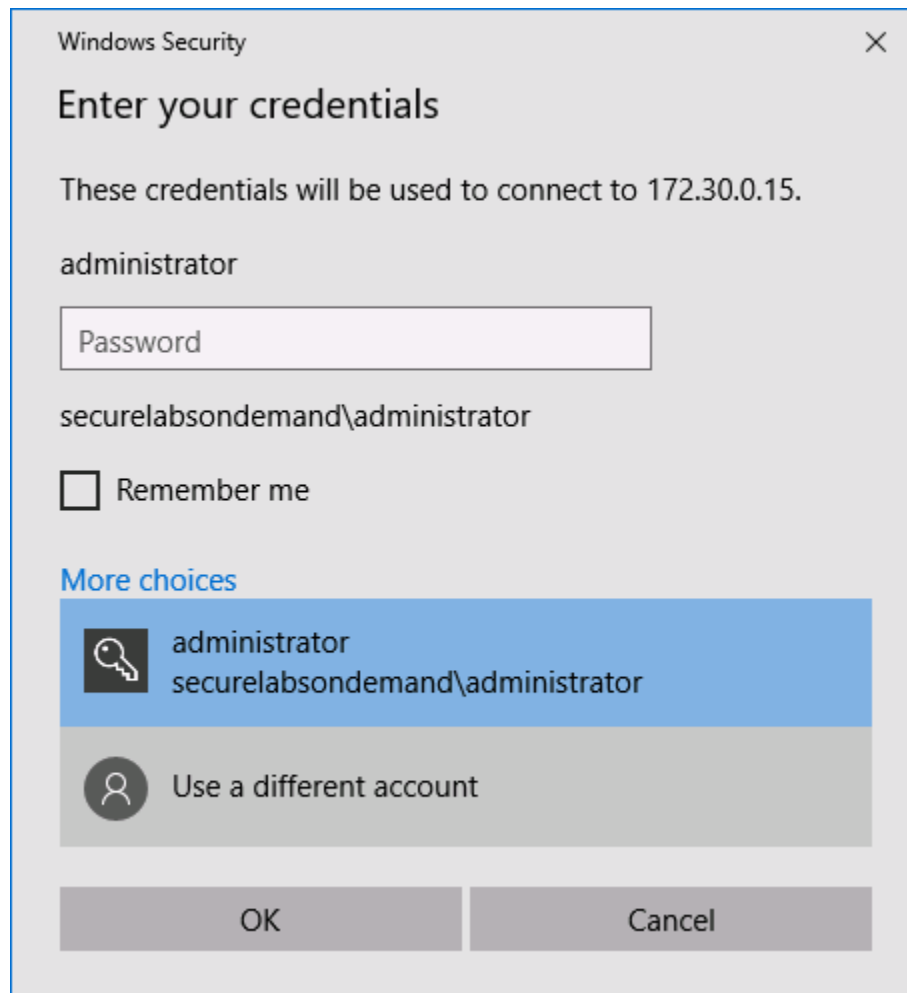
1. In the Connections folder on the vWorkstation, **right-click** the **TargetWindowsDC01 RDP shortcut** and **select Edit** to open the Remote Desktop Connection Properties dialog box.
2. In the Remote Desktop Connection Properties dialog box, **click** the **Always ask for credentials checkbox** and **click Connect**.

This option will prompt you for a username and password when you open the remote connection, giving you the opportunity to specify the user account you will use to log in.



Edit the remote desktop connection

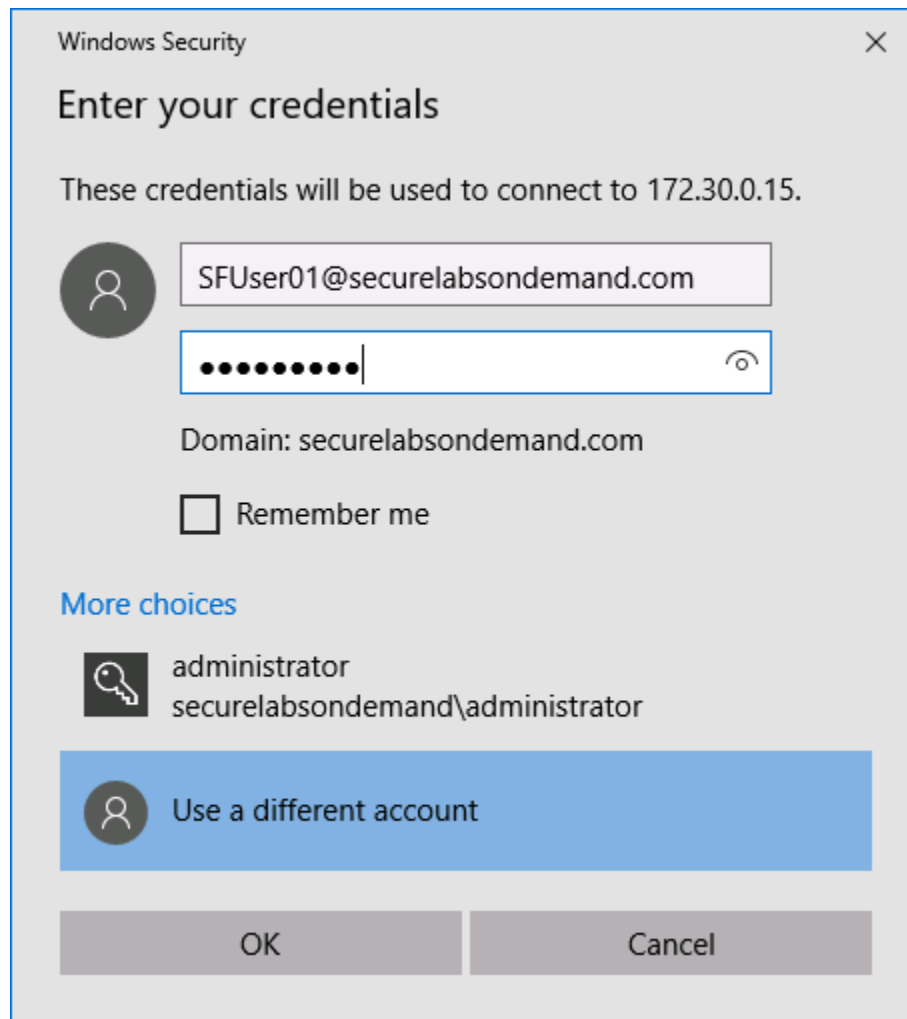
3. In the Windows Security dialog box, **click the More choices link**, then **click the Use a different account button**.



Enter credentials

4. When prompted, **type** the SFUser01 credentials and **press Enter** to open a remote connection to the TargetWindowsDC01 machine.
 - User name: **SFUser01@securelabsondemand.com**
 - Password: **P@ssw0rd!**

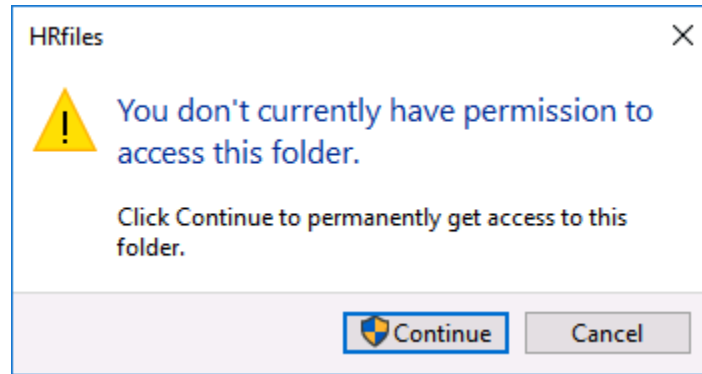
If you are prompted to reset the password, go back to Part 1, Step 20 to confirm you unchecked the checkbox.



Connect to TargetWindowsDC01 as SFUser01

5. From the TargetWindowsDC01 taskbar, **click the File Explorer icon** to open a new File Explorer window.
6. In the File Explorer, **navigate** to the HRfiles folder (**This PC > Local Disk (C:) > LabFiles > HRfiles**).

The SFUser01 account does not have permission to read or traverse this folder, so you will receive an error message.

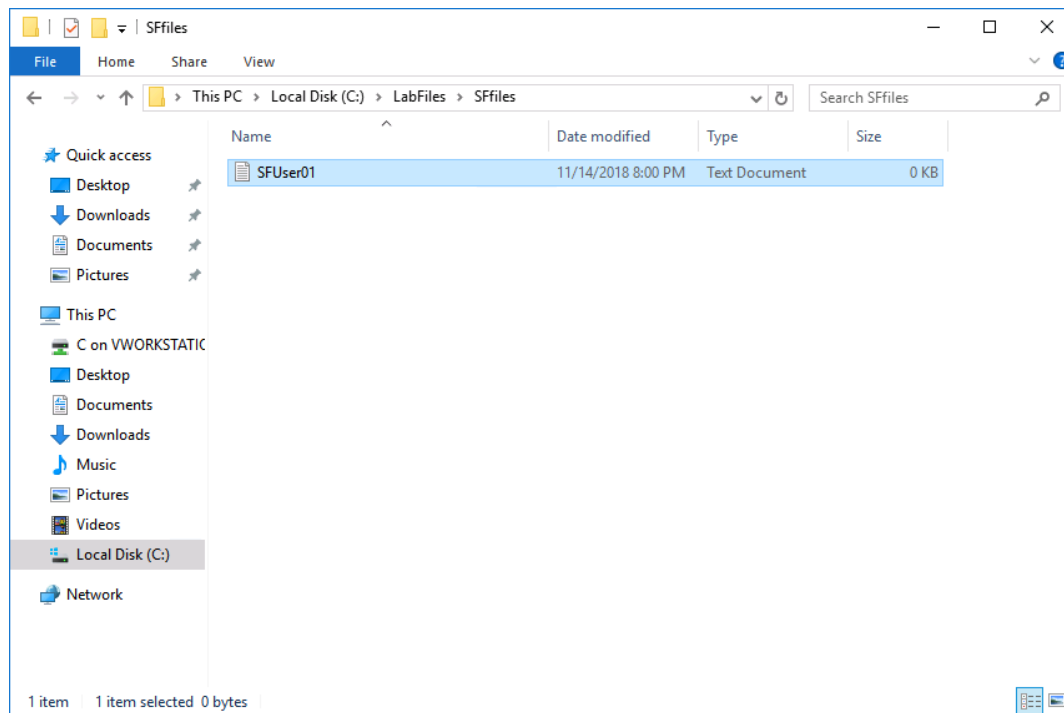


Unsuccessful access error message

7. **Make a screen capture** showing the **unsuccessful access error message**, the **LabFiles** folder, and the **TargetWindowsDC01** title bar and **paste** it into the Lab Report file.
8. **Click Cancel** to close the error message.
9. **Repeat steps 6-8** for the MGRfiles folder.
10. In the File Explorer, **navigate** to the SFfiles folder (**Local Disk (C:) > LabFiles > SFfiles**).
SFUser01 is a member of the Shopfloor security group and will be able to open the folder.
11. In the SFfiles folder, **right-click** anywhere and **select New > Text Document** from the context menu.
12. With *New Text Document* highlighted, **type SFUser01**, the logged on user's account name, and **press Enter** to name the new file.

Enabling Windows Active Directory and User Access Controls

Fundamentals of Information Systems Security, Third Edition - Lab 03



Successful file creation

13. **Make a screen capture** showing a **file successfully created in the SFfiles folder** and the **TargetWindowsDC01 title bar** and **paste** it into the Lab Report file.
14. **Close the remote TargetWindowsDC01 connection** to return to the vWorkstation.
15. **Repeat steps 1-14** using the **HRUser01** and **Manager01** user accounts and **document the successful and unsuccessful results of your tests** in the Lab Report file as indicated.

Remember that the Manager01 account should have access to both the SFfiles folder and the MGRfiles folder. You will have two successful screen captures for that account.

Note: This completes Section 1 of this lab. There are no deliverable files for this section.

Section 2: Applied Learning

Note: **SECTION 2** of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will be introduced to a more robust way of creating users, groups, and permissions.

Please confirm with your instructor that you have been assigned Section 2 before proceeding.

1. On your local computer, **create** the **Lab Report file**.
Frequently performed tasks, such as how to create the Lab Report file, make screen captures, and download files from the lab, are explained in the Common Lab Tasks document. You should review these tasks before starting the lab.
2. If you already completed Section 1 of this lab, you will need to reset the virtual environment before beginning Section 2. To reset the virtual environment, complete one of the following options.
 - a. **Click Options > Reset Lab** to restore all virtual machines to their base state. This will take several minutes to complete. If you do not see the vWorkstation desktop after five minutes, **click Options > Reload Lab** to reload your lab connection.
 - b. **Click Disconnect**, then **select Discard Changes** to end your lab session without creating a StateSave. If you previously created a StateSave, delete the StateSave at the launch page, then start a new lab session.
3. **Proceed with Part 1.**

Part 1: User and Group Administration

Note: In the first part of this lab, you will use Microsoft's Active Directory and PowerShell to create three security groups on a remote server. You also will create several user accounts and apply them to the new security groups. Later in the lab, you will see how these objects are used to secure files and folders on the network.

Active Directory is the database that provides a centrally controlled and managed access and security

Enabling Windows Active Directory and User Access Controls

Fundamentals of Information Systems Security, Third Edition - Lab 03

management system for an organizations Windows computer systems. It is much easier and more manageable for an administrator to control user and resource access from one central location than to have to go to each machine on the network and make changes there. In many organization's it would be impossible to physically access every machine, but Active Directory can virtually access all of the Windows machines in an organization. Machines not on the domain can still be accessed by users if they know the local machine name or IP Address, authorized user name, and password; however, this process is much easier on Active Directory.

1. **Open a remote connection** to the **TargetWindowsDC01** machine.

If prompted, **type** the following credentials and **click OK** to open the remote connection.

- Username: **Administrator**
- Password: **P@ssw0rd!**

2. From the TargetWindowDC01 Start menu, **launch PowerShell**.

Note: PowerShell uses the .NET framework in the power of a shell, which allows for automation and scripting of a Windows environment. To create a new global security group, you will use the command *New-ADGroup*. This command and the options used in this section are described below:

New-ADGroup -Name HumanResources -GroupScope Global -GroupCategory Security

- **New-ADGroup** creates a new Active Directory group. By default, NewADGroup creates the group in the Users OU (Organizational Unit).
 - **-Name** specifies the name of the group. This is a required field and the system will prompt you for a name if you do not specify it when issuing the command.
 - **-GroupScope** specifies how the group is applied to the domain. There are three possible options for scope: Universal, Global, or Domain Local. This is a required field.
 - **-GroupCategory** specifies the type of group. There are two possible options for category: Distribution (email) or Security.
3. At the PowerShell command prompt, **execute the command** to add the following two new Global Security groups in Active Directory:
 - **Marketing**
 - **Engineering**

Note: In the next steps, you will first use PowerShell to create another new user with the command *New-ADUser*. The command and its options are described below:

```
New-ADUser -Name HRUser01 -UserPrincipalName
HRUser01@securelabsondemand.com -AccountPassword (ConvertTo-SecureString
-AsPlainText "P@ssw0rd!" -Force) -GivenName HRUser -Surname 01 -Enabled
$true
```

- **New-ADUser** creates a new user account in Active Directory.
 - **-Name** specifies the name of the object in Active Directory.
 - **-UserPrincipalName** determines the logon name for the new user.
 - **-AccountPassword** specifies a password for the new user account. If you do not set a password when the account is created, it will be disabled until you set a password. A password can be set using the **Set-ADAccountPassword** command in a separate step.
 - **-GivenName** sets the user's first name.
 - **-Surname** specifies the user's last name.
 - **-Enabled** enables (\$true) the account only if a password is set.
4. At the PowerShell command prompt, **execute the command** to create a new user account (MKTUser01) using the the information below:

- Name: **MKTUser01**
- Principal name: **MKTUser01@securelabsondemand.com**
- Password: **P@ssw0rd!**
- Given name: **MKTUser**
- Surname: **01**

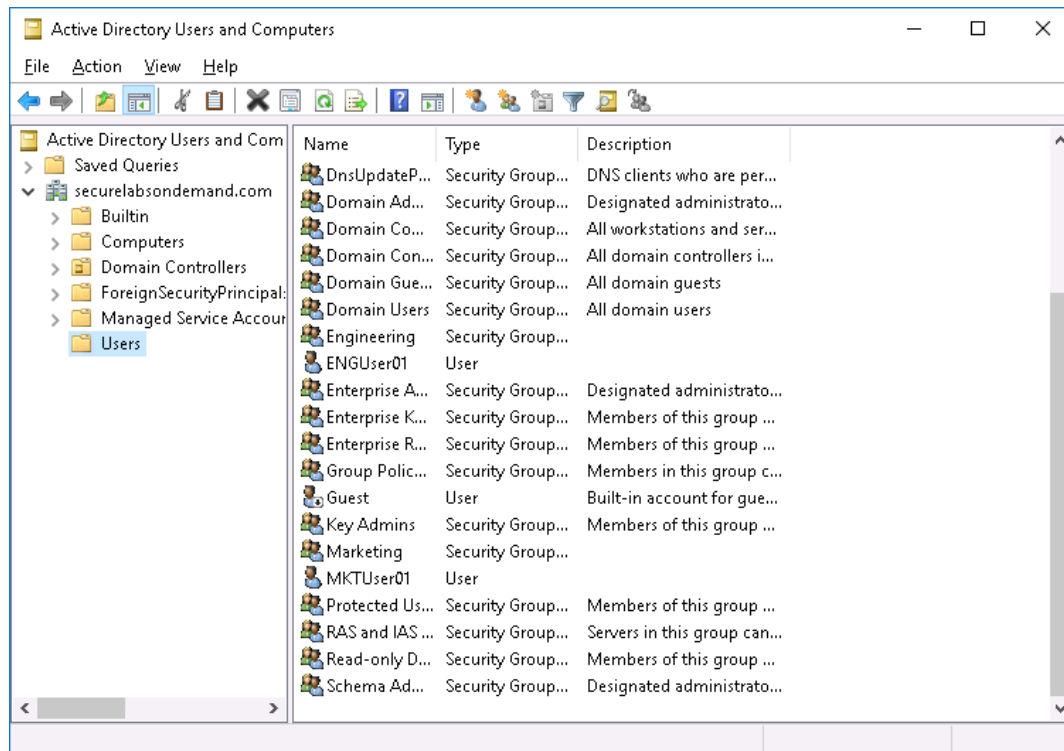
Note: Next, you will add the new user to an existing global security group using the *New-ADUser* command described below:

```
Add-ADGroupMember -Identity HumanResources -Members HRUser01
```

- **Add-ADGroupMember** adds a user account to an Active Directory group.
- **-Identity** specifies the group to which you want to add user account(s).
- **-Members** identifies the user(s) that will be added to the group.

5. At the PowerShell command prompt, **execute the command** to add the **MKTUser01** account to the **Marketing** group.
6. **Repeat steps 4-5** to create a new user (**ENGUser01**) and add that user account to the **Engineering** group.
7. **Launch the Server Manager**, then **open the Active Directory Users and Computers console**.
8. In the navigation pane, **expand securelabsondemand.com** and **navigate to the Users Organizational Unit**.
9. **Make a screen capture** showing the **new users and groups** created in this lab and **paste it** into the Lab Report file.

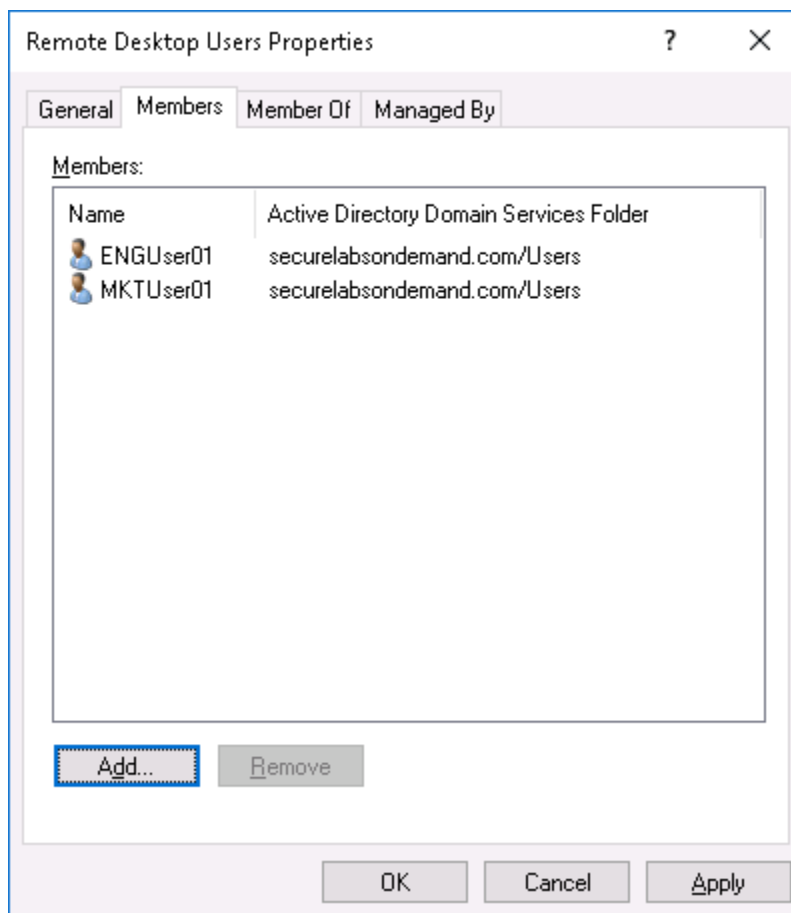
You may need to make multiple screen captures to display all new users and groups.



All Active Directory groups and user accounts

Note: In the next steps, you will use Active Directory Users and Computers console to add the new user accounts to a Builtin (built-in) group called Remote Desktop Users. Members of this group are allowed to use the remote desktop services in the lab to connect to remote machines. You will need this access later in the lab.

10. In the Active Directory console, **edit** the **Remote Desktop Users group** to add the two new users (MKTUser01 and ENGUser01) to the group.



Remote Desktop Users Properties

11. **Close** the **Active Directory Users and Computers** and **Server Manager** window.

12. **Restore** the **Powershell window** and **execute the command** to force an immediate update of all Group Policies on the Domain Controller.

Note: One of the biggest challenges faced by a Windows administrator is how to handle guest users, such as contract workers, auditors, or partners. Typically, best practices would dictate that a guest would be placed in a secure network, isolated from the production network by firewall barriers. If this is not practical, which is often the case with auditors, then clear and specific areas of access should be decided, making them as restrictive as possible. For CIA requirements, local, self-signed certificates are issued to guests who require a higher degree of access. These certificates expire on a specific date and limit the guest's access. Of course, Access Control Lists to strictly control the access is also mandatory and disabling the guest user in favor of creating short term user accounts will help as well. Creating guest user templates that have the USB ports and CD's disabled is a means of stopping the introduction of unwanted data, and the theft of company data. Using the newer system of Windows archiving makes restoring any compromised documents easier.

Part 2: Resource Management

Note: In the next steps, you will use PowerShell to create a subfolder for each of the work teams in the lab: one for engineering employees and one for marketing employees, then assign explicit permissions for each folder as indicated in the following table. The process using PowerShell is to get the current permission, modify the permissions, then set the permissions.

Security Groups	Access to ENGfiles	Access to MKTfiles
Engineering	X	
Marketing		X

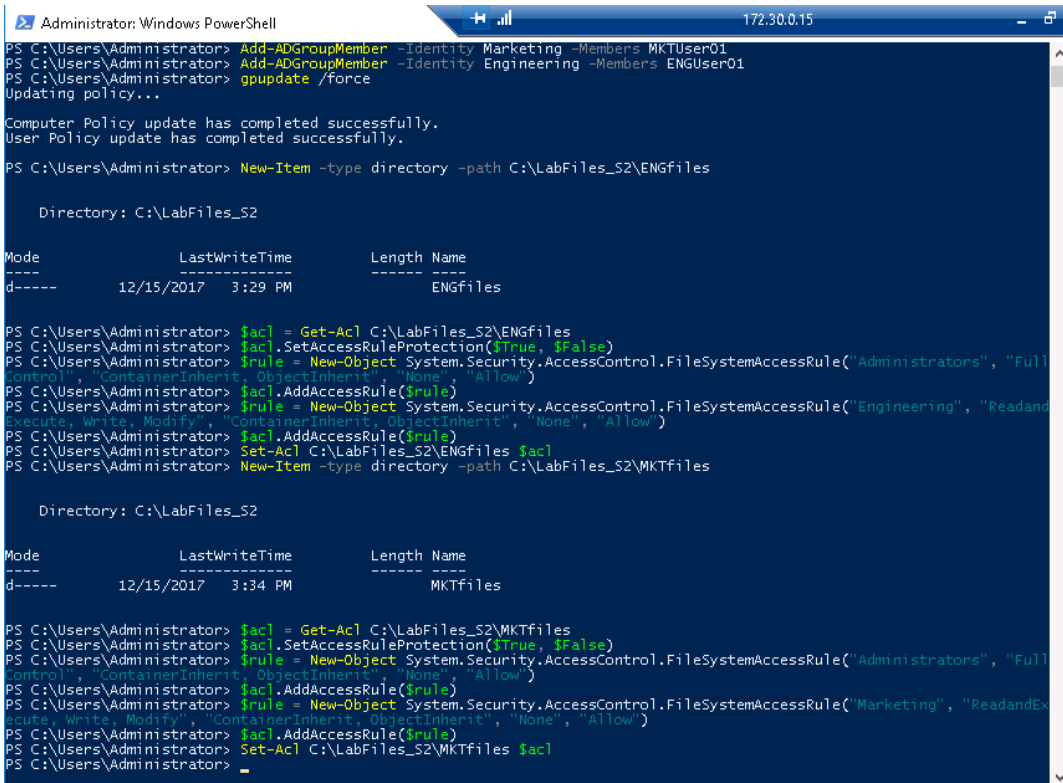
You will use the following commands and options to accomplish this task.

- **New-Item** creates a new file, folder, or registry item.
- **-type** identifies the type of item is being created: file, folder or registry object.
- **-path** sets the desired location of the new item.
- **Get-Acl** retrieves the current permissions.
- **SetAccessRuleProtection** sets inheritance on access rules.
- **New-Object** creates a new object.
- **AddAccessRule** adds the ACL to the file or directory.
- **Set-Acl** assigns the ACL to a file, directory, or registry key.

1. **Launch** the **File Explorer**.
2. **Navigate** to the Local Disk (C:) (**This PC > Local Disk (C:)**), then **create a new folder** titled **LabFiles_S2**.

3. **Right-click** the **LabFiles_S2** folder and **select Properties**.
 4. In the Properties dialog box, **click** the **Security tab** and **click** the **Edit button** to modify the security options for the LabFiles folder.
 5. **Click** the **Add button** and **add** the **Marketing and Engineering groups** to this folder.
 6. **Update the Permissions** to allow the Engineering and Marketing groups to modify files and folders within the LabFiles_S2 folder, then **close** the **dialog boxes**.
 7. **Restore** the **PowerShell window**.
 8. At the PowerShell command prompt, **execute** `New-Item -type directory -path C:\LabFiles_S2\ENGfiles` to create the ENGfiles folder.
 9. At the PowerShell command prompt, **execute** `$acl = Get-Acl C:\LabFiles_S2\ENGfiles` to allow the system to locate the current access control list (ACL) for the directory.
 10. At the PowerShell command prompt, **execute** `$acl.SetAccessRuleProtection($True, $False)` to remove inheritance from the folder.
- Note:** By default, Windows will inherit the permissions of the parent folder so that all subfolders will have the same permissions as the parent. Disabling inheritance now will enable you to specify permissions for each subfolder.
11. At the PowerShell command prompt, **execute** `$rule = New-Object System.Security.AccessControl.FileSystemAccessRule("Administrators", "FullControl", "ContainerInherit, ObjectInherit", "None", "Allow")` to create a rule that grants the Administrators group full access to the directory.
 12. At the PowerShell command prompt, **execute** `$acl.AddAccessRule($rule)` to apply the rule.

13. At the PowerShell command prompt, **execute** `$rule = New-Object System.Security.AccessControl.FileSystemAccessRule("Engineering", "ReadAndExecute, Write, Modify", "ContainerInherit, ObjectInherit", "None", "Allow")` to create a rule that grants the Engineering group modify permissions to the directory.
14. At the PowerShell command prompt, **execute** `$acl.AddAccessRule($rule)` to apply the rule.
15. At the PowerShell command prompt, **execute** `Set-Acl C:\LabFiles_S2\ENGfiles $acl` to set the new ACLs to C:\LabFiles_S2\ENGfiles.
16. **Repeat steps 8-15** to restrict the MKTfiles folder to the Marketing group.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Add-ADGroupMember -identity Marketing -Members MKTUser01
PS C:\Users\Administrator> Add-ADGroupMember -Identity Engineering -Members ENGUser01
PS C:\Users\Administrator> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator> New-Item -type directory -path C:\LabFiles_S2\ENGfiles

Directory: C:\LabFiles_S2

Mode                LastWriteTime         Length Name
----                -
d-----          12/15/2017   3:29 PM             ENGfiles

PS C:\Users\Administrator> $acl = Get-Acl C:\LabFiles_S2\ENGfiles
PS C:\Users\Administrator> $acl.SetAccessRuleProtection($true, $false)
PS C:\Users\Administrator> $rule = New-Object System.Security.AccessControl.FileSystemAccessRule("Administrators", "FullControl", "ContainerInherit, ObjectInherit", "None", "Allow")
PS C:\Users\Administrator> $acl.AddAccessRule($rule)
PS C:\Users\Administrator> $rule = New-Object System.Security.AccessControl.FileSystemAccessRule("Engineering", "ReadAndExecute, Write, Modify", "ContainerInherit, ObjectInherit", "None", "Allow")
PS C:\Users\Administrator> $acl.AddAccessRule($rule)
PS C:\Users\Administrator> Set-Acl C:\LabFiles_S2\ENGfiles $acl
PS C:\Users\Administrator> New-Item -type directory -path C:\LabFiles_S2\MKTfiles

Directory: C:\LabFiles_S2

Mode                LastWriteTime         Length Name
----                -
d-----          12/15/2017   3:34 PM             MKTfiles

PS C:\Users\Administrator> $acl = Get-Acl C:\LabFiles_S2\MKTfiles
PS C:\Users\Administrator> $acl.SetAccessRuleProtection($true, $false)
PS C:\Users\Administrator> $rule = New-Object System.Security.AccessControl.FileSystemAccessRule("Administrators", "FullControl", "ContainerInherit, ObjectInherit", "None", "Allow")
PS C:\Users\Administrator> $acl.AddAccessRule($rule)
PS C:\Users\Administrator> $rule = New-Object System.Security.AccessControl.FileSystemAccessRule("Marketing", "ReadAndExecute, Write, Modify", "ContainerInherit, ObjectInherit", "None", "Allow")
PS C:\Users\Administrator> $acl.AddAccessRule($rule)
PS C:\Users\Administrator> Set-Acl C:\LabFiles_S2\MKTfiles $acl
PS C:\Users\Administrator>
```

PowerShell commands

17. **Make a screen capture** showing the **commands used to restrict the ENGfiles and MKTfiles folders** and **paste** it into the Lab Report file.
18. **Close the PowerShell window.**

Part 3: Group Policy

Note: In the next steps, you will use the Group Policy Object Editor to modify permissions on the TargetWindowsDC01 server to allow these new users to use the remote desktop services. Windows Group Policy is a very powerful, granular method of controlling machine and user access and experience on the Windows desktop and network. This tool is used on either a local or domain level to control access to many local computer and network resources such as drives, Internet access, kiosk mode, etc. It is a very powerful tool used by administrators frequently.

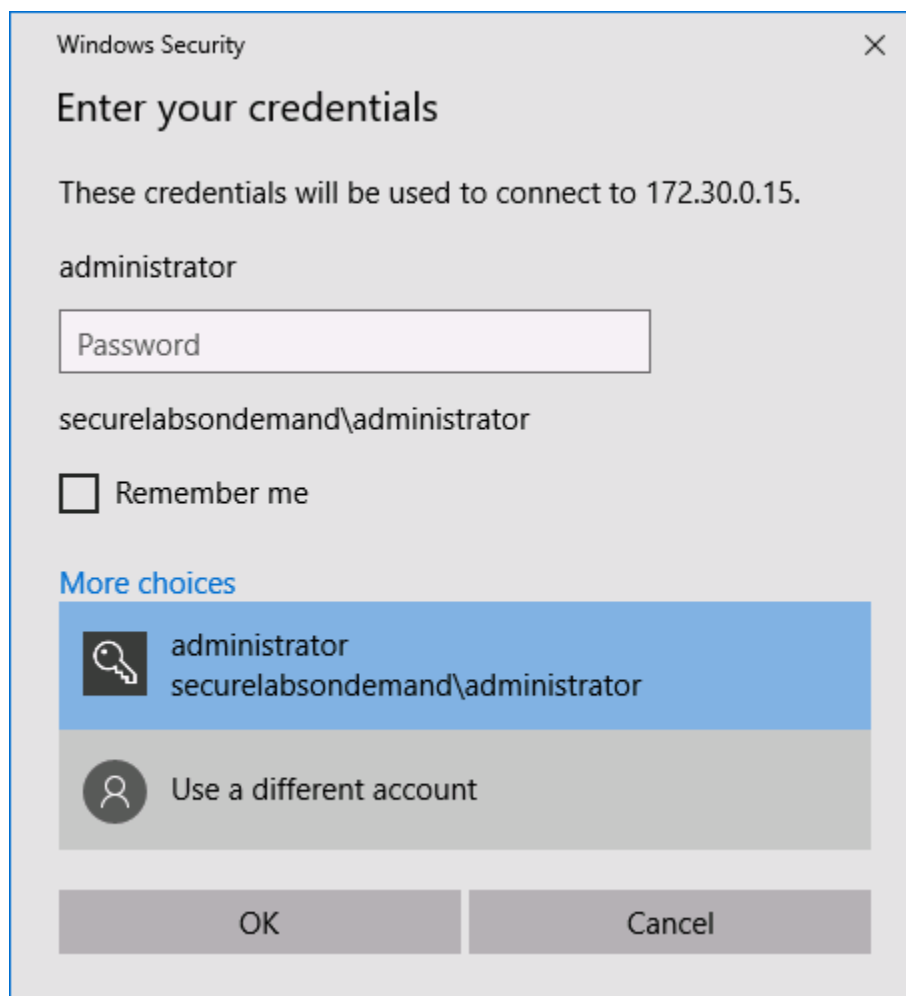
1. From the Windows Start menu, **run gpedit.msc** to open the Local Group Policy Editor.
2. In the left pane, **navigate** to the User Rights Assignment folder (**Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment**).
3. **Double-click** the **Allow log on through Remote Desktop Services policy** in the right pane and **add** the **Remote Desktop Users group** to the policy.
4. **Close** any **open windows**.
5. **Close** the **remote TargetWindowsDC01 connection**.

Part 4: Practical Application

Note: In the next steps, you will conduct a test to verify that the new users can use the remote desktop services to access the TargetWindowsDC01 server and modify the folder to which each account has access.

First, you will need to modify the shortcut to allow you to log in with a different user account since the existing shortcut is pre-configured to automatically log in to the TargetWindowsDC01 machine using the Administrator account.

1. In the Connections folder on the vWorkstation, **right-click** the **TargetWindowsDC01 shortcut** and **select Edit**.
2. **Click** the **Always ask for credentials checkbox** and **click Connect**.
3. In the Windows Security dialog box, **click More choices link** and **click Use a different account**.



Enter credentials

4. **Open a remote connection** to the **TargetWindowsDC01** machine with the **ENGUser01** credentials:

- User name: **ENGUser01**
- Password: **P@ssw0rd!**

5. **Launch** the **File Explorer**.

6. In the File Explorer, **navigate** to the MKTfiles folder (**This PC > Local Disk (C:) > LabFiles_S2 > MKTfiles**).

The ENGUser01 account does not have permission to read or traverse this folder, so you will receive an error message.

7. **Make a screen capture** showing the **unsuccessful access error message**, the **LabFiles_S2** folder, and the **TargetWindowsDC01** title bar and **paste** it into the Lab Report file.

8. **Close** the **error message**.

9. **Navigate** to the ENGfiles folder (**This PC > Local Disk (C:) > LabFiles_S2 > ENGfiles**).
ENGUser01 is a member of the Engineering security group and will be able to open the folder.

10. **Create** a new text document titled **ENGUser01**, the logged in user's account name, in the folder.

11. **Make a screen capture** showing a **file successfully created in the ENGfiles folder** and **include the TargetWindowsDC01 title bar** and **paste** it into the Lab Report file.

12. **Close** the **remote TargetWindowsDC01 connection**.

13. **Repeat steps 1-12** using the **MKTUser01** user account and **document the successful and unsuccessful results of your tests** in the Lab Report file as indicated.

Note: This completes Section 2 of this lab. There are no deliverable files for this section.

Section 3: Lab Challenge and Analysis

Note: The following questions are provided to allow you the opportunity for independent, unguided research, similar to what you will encounter in a real situation. Some questions will challenge you to find command line syntax for tasks you performed in the lab, others may ask you to extend your learning from the lab. Use screen captures where possible to illustrate your answers.

Part 1: Analysis and Discussion

In the lab, you learned that providing secure network access for guest users is a major challenge for Windows administrators. Give a brief summary of the challenges posed by guest access and identify tools or configuration methods that might solve the problem.

Part 2: Tools and Commands

What PowerShell commands could be used to create a new user, *ENGMGR01*, that is a member of both the *Engineering* and *Managers* Active Directory groups?

Part 3: Challenge Exercise

Design a user access control framework for your school's information technology department. You will need to design a folder structure, user/group accounts, and an access control table (similar to the one included in the note introducing Part 2 of this lab) that accounts for the following requirements. Use details from the lab and screen captures from your school's Web site to document your work.

- Each degree program within the department should have its own folder structure.
- Each student in the program will require a workspace folder.
- Each faculty member requires access to his students' workspace folders.
- Each faculty member requires his own workspace folder.
- The dean of the department will require a private workspace folder.
- The dean and staff members of the department will require a workspace folder to share materials with faculty members.
- Human Resources will require a workspace folder to share materials with all faculty and staff in the department.
- There is no requirement for remote desktop services.