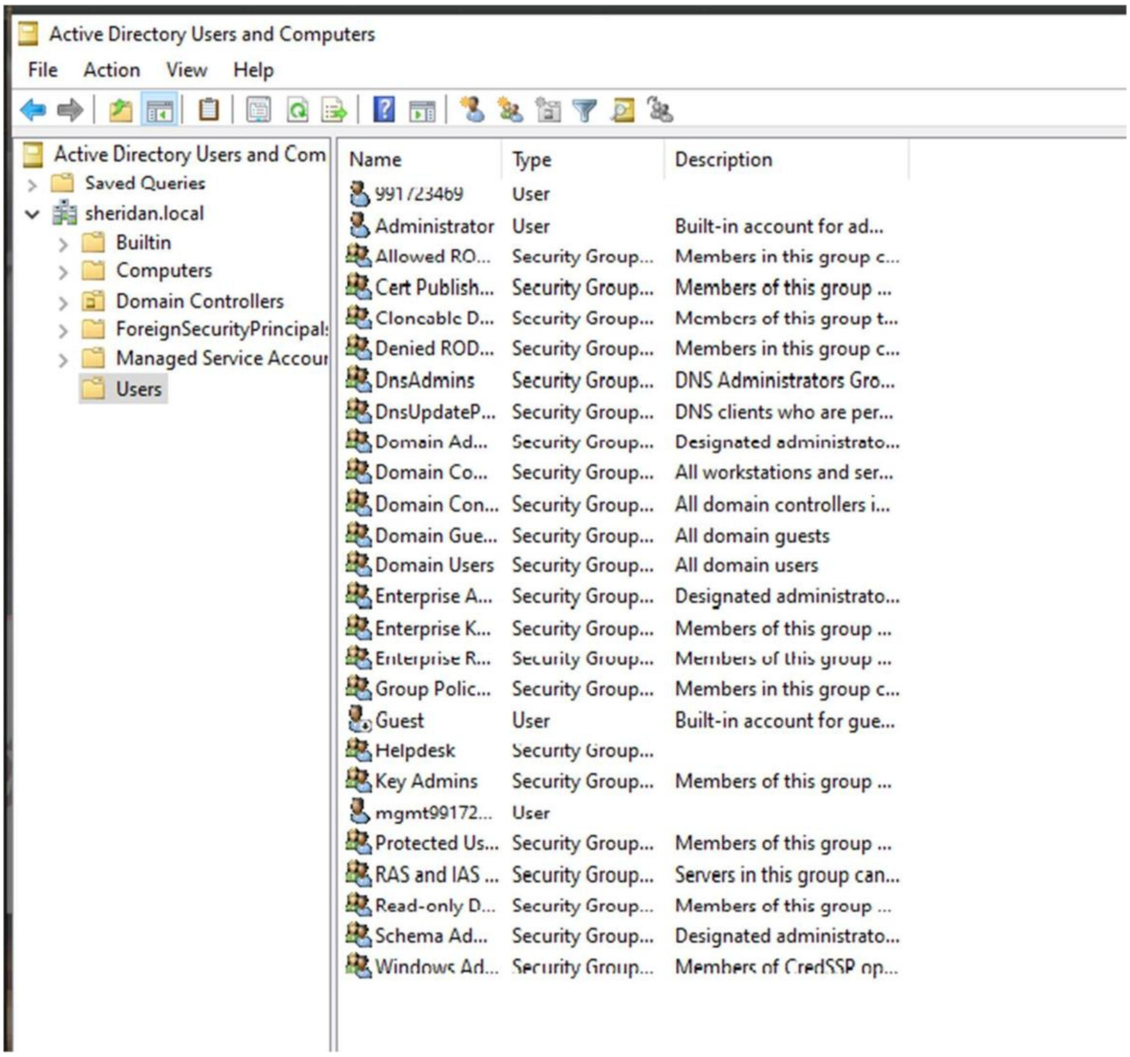
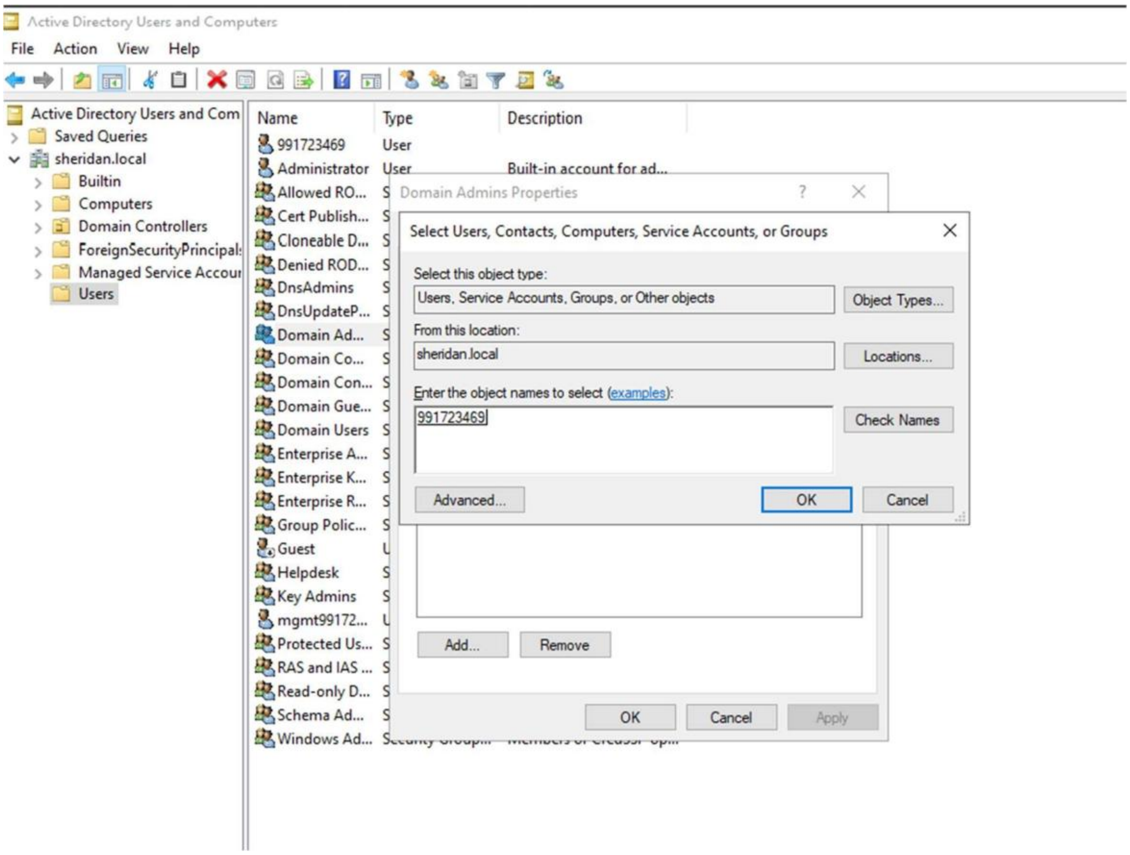
Name: Mahimaa Vardini Balaji Ramathaal

PART A – USER CREATION



Name	Type	Description
991723469	User	
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Helpdesk	Security Group...	
Key Admins	Security Group...	Members of this group ...
mgmt99172...	User	
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...
Windows Ad...	Security Group...	Members of CredSSP op...

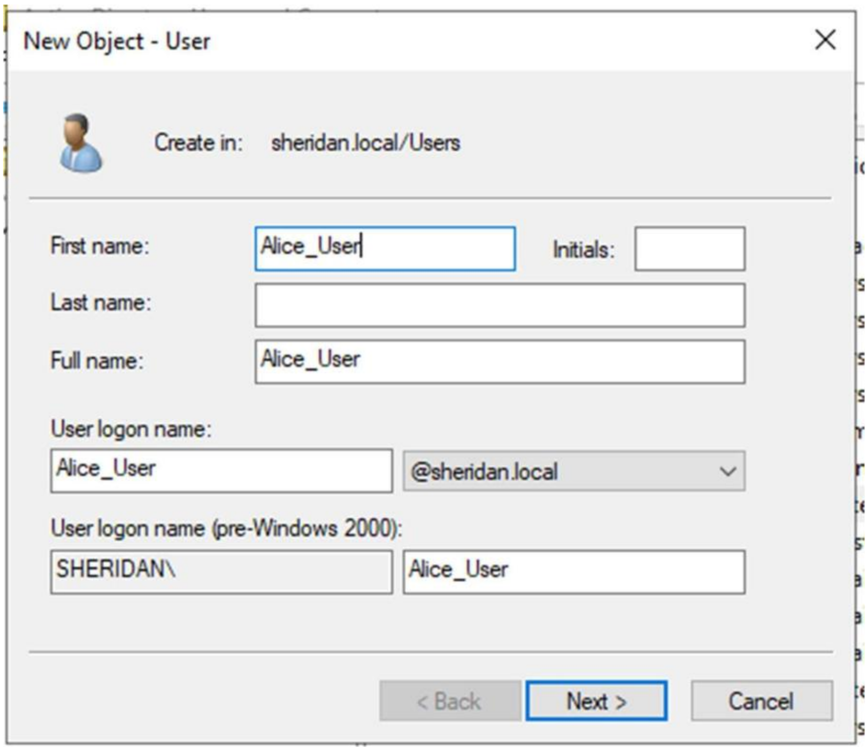


Name	Type	Description
991723469	User	
Administrator	User	Built-in account for ad...
Allowed RO...	S	
Cert Publish...	S	
Cloneable D...	S	
Denied ROD...	S	
DnsAdmins	S	
DnsUpdateP...	S	
Domain Ad...	S	
Domain Co...	S	
Domain Con...	S	
Domain Gue...	S	
Domain Users	S	
Enterprise A...	S	
Enterprise K...	S	
Enterprise R...	S	
Group Polic...	S	
Guest	U	
Helpdesk	S	
Key Admins	S	
mgmt99172...	U	
Protected Us...	S	
RAS and IAS ...	S	
Read-only D...	S	
Schema Ad...	S	
Windows Ad...	Security Group...	Members of Ullussr up...

Select this object type:
Users, Service Accounts, Groups, or Other objects

From this location:
sheridan.local

Enter the object names to select (examples):
991723469



Create in: sheridan.local/Users

First name: Alice_User

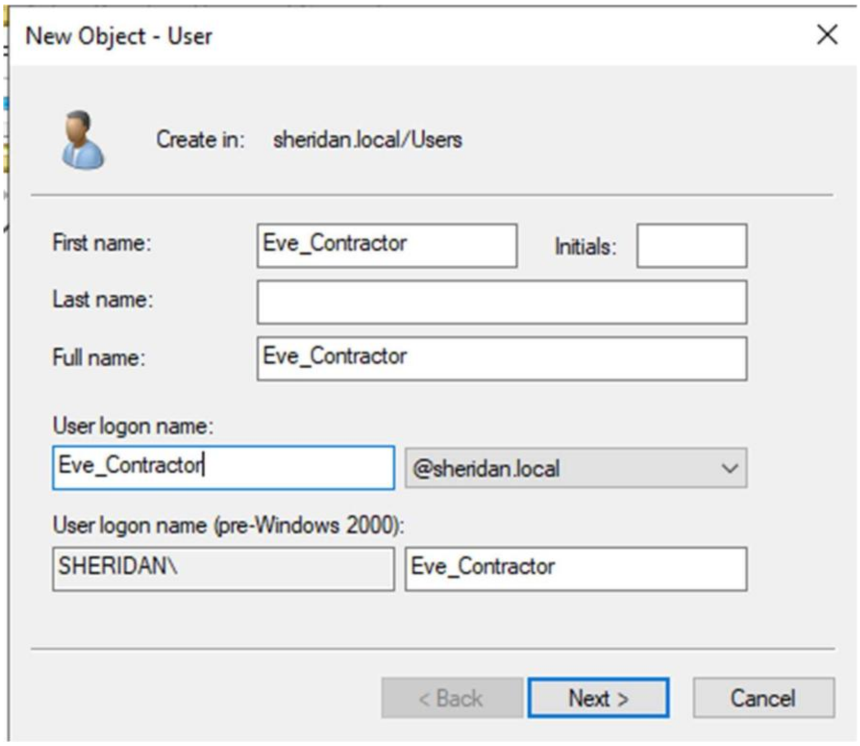
Initials:

Last name:

Full name: Alice_User

User logon name:
Alice_User @sheridan.local

User logon name (pre-Windows 2000):
SHERIDAN\ Alice_User



New Object - User

Create in: sheridan.local/Users

First name: Eve_Contractor

Initials:

Last name:

Full name: Eve_Contractor

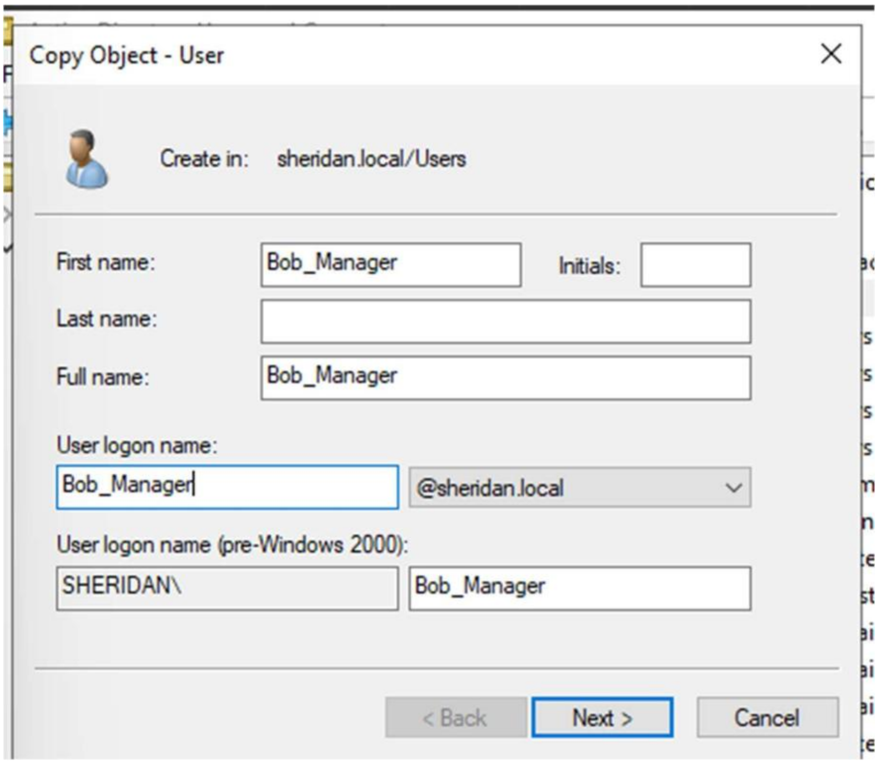
User logon name:

Eve_Contractor @sheridan.local

User logon name (pre-Windows 2000):

SHERIDAN\ Eve_Contractor

Building a user template for standard users



Copy Object - User

Create in: sheridan.local/Users

First name: Bob_Manager

Initials:

Last name:

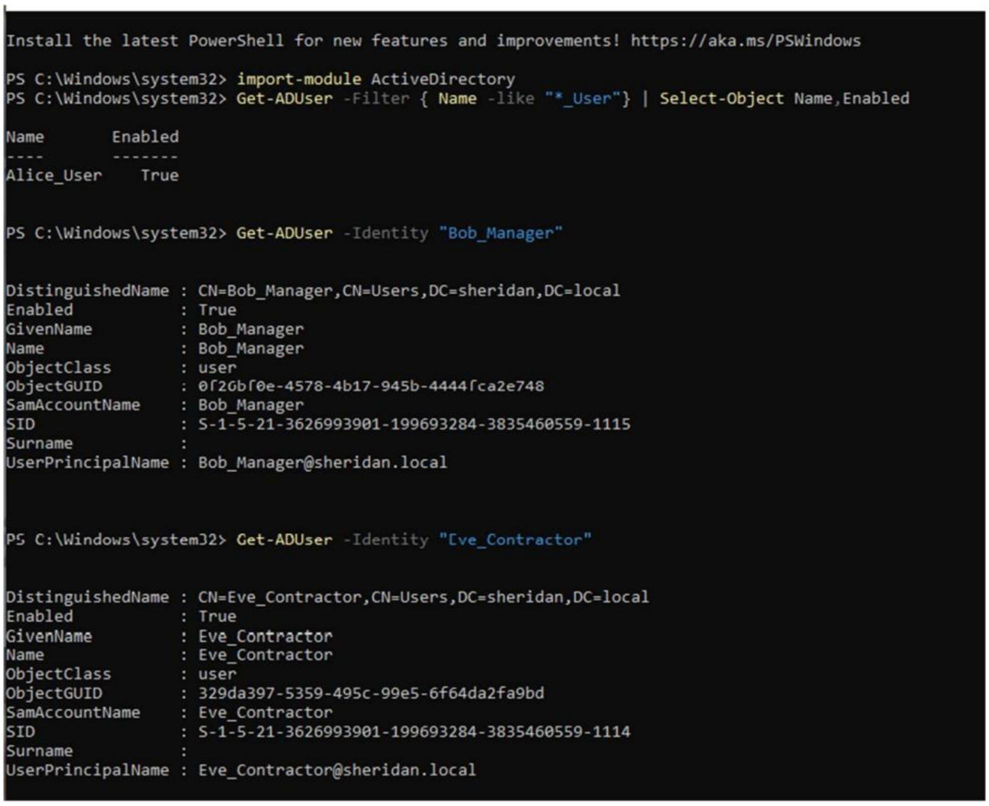
Full name: Bob_Manager

User logon name:

Bob_Manager @sheridan.local

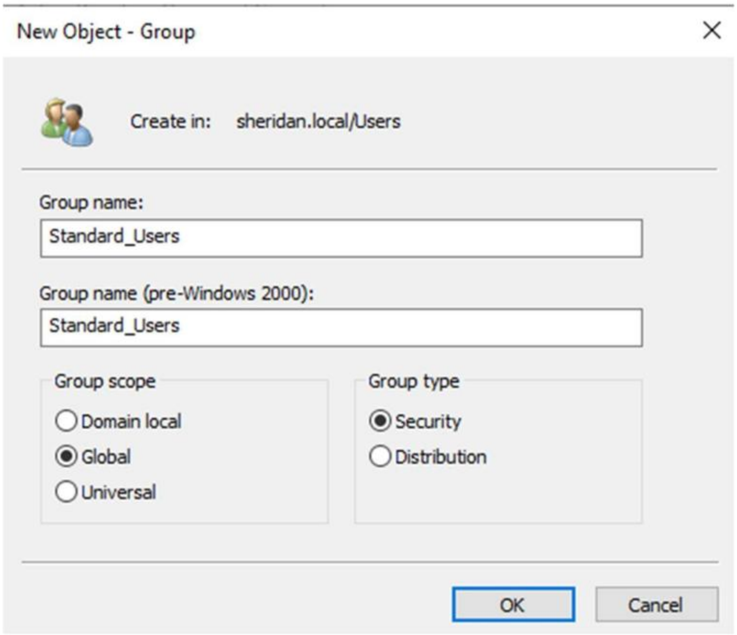
User logon name (pre-Windows 2000):

SHERIDAN\ Bob_Manager



```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> import-module ActiveDirectory
PS C:\Windows\system32> Get-ADUser -Filter { Name -like "*_User"} | Select-Object Name,Enabled

Name       Enabled
----       -------
Alice_User    True


PS C:\Windows\system32> Get-ADUser -Identity "Bob_Manager"


DistinguishedName : CN=Bob_Manager,CN=Users,DC=sheridan,DC=local
Enabled           : True
GivenName         : Bob_Manager
Name              : Bob_Manager
ObjectClass       : user
ObjectGUID        : 0f26bf0e-4578-4b17-945b-4444fca2e748
SamAccountName    : Bob_Manager
SID               : S-1-5-21-3626993901-199693284-3835460559-1115
Surname           :
UserPrincipalName : Bob_Manager@sheridan.local



PS C:\Windows\system32> Get-ADUser -Identity "Eve_Contractor"


DistinguishedName : CN=Eve_Contractor,CN=Users,DC=sheridan,DC=local
Enabled           : True
GivenName         : Eve_Contractor
Name              : Eve_Contractor
ObjectClass       : user
ObjectGUID        : 329da397-5359-495c-99e5-6f64da2fa9bd
SamAccountName    : Eve_Contractor
SID               : S-1-5-21-3626993901-199693284-3835460559-1114
Surname           :
UserPrincipalName : Eve_Contractor@sheridan.local
```

PART B – GROUP MANAGEMENT



New Object - Group

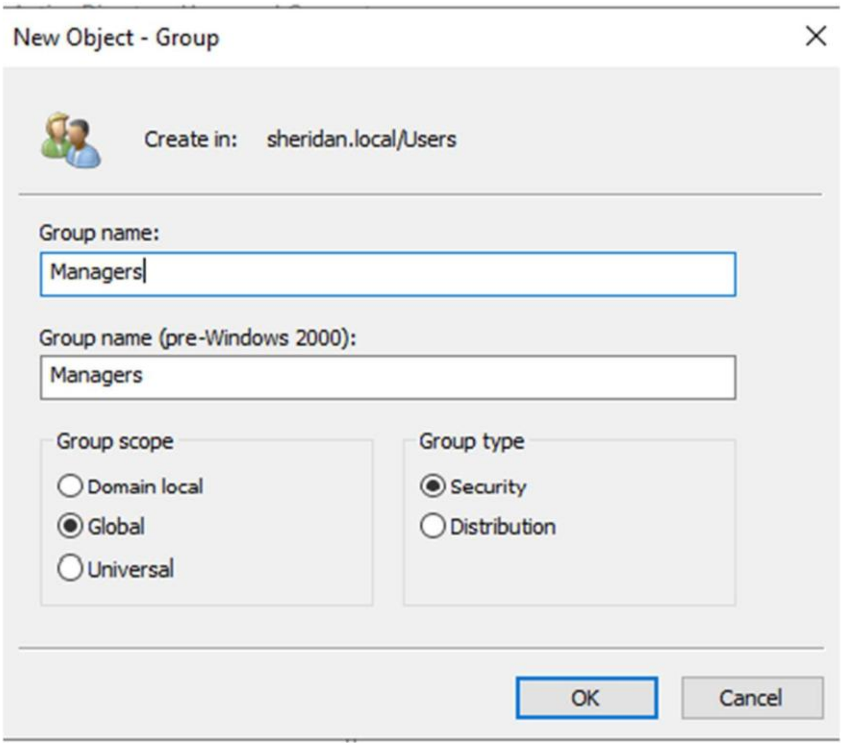
Create in: sheridan.local/Users

Group name:
Standard_Users

Group name (pre-Windows 2000):
Standard_Users

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution



New Object - Group

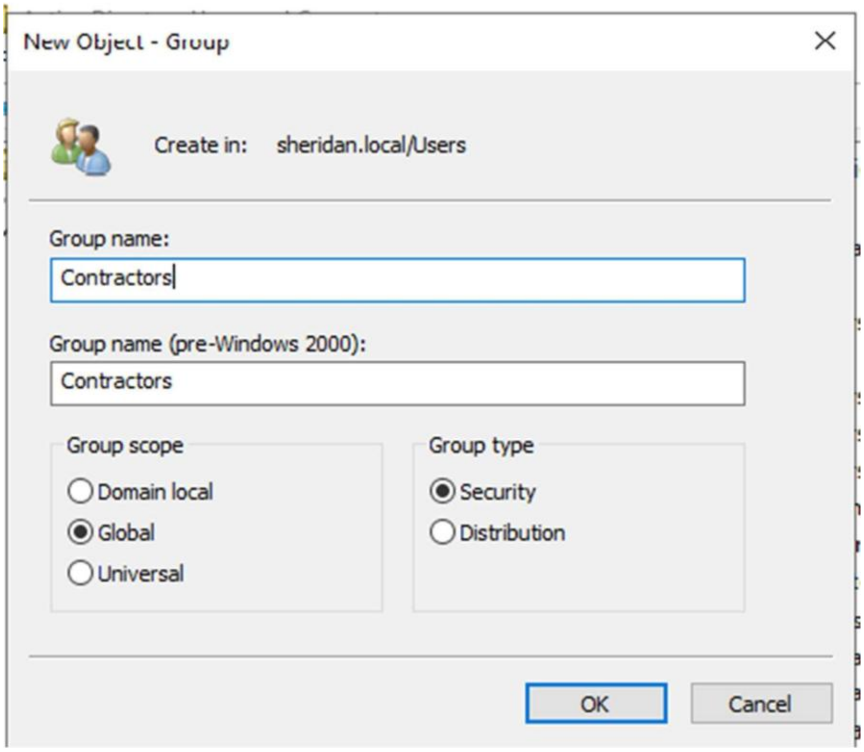
Create in: sheridan.local/Users

Group name:
Managers

Group name (pre-Windows 2000):
Managers

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution



New Object - Group

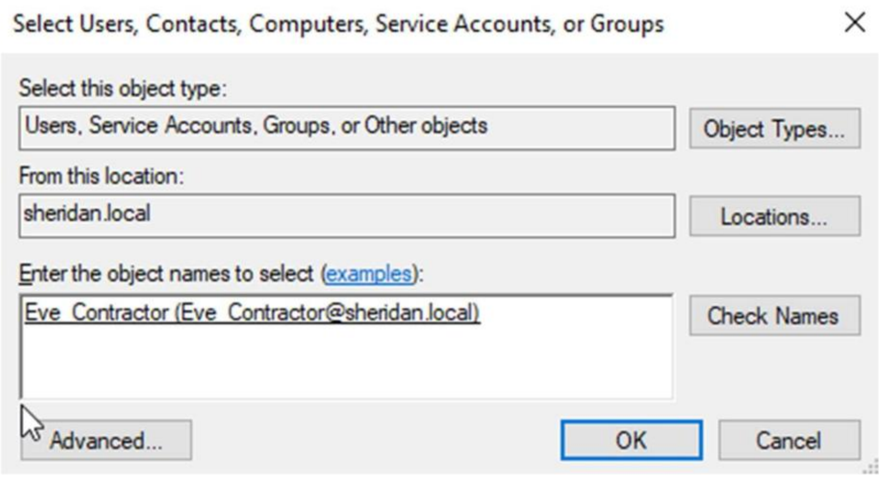
Create in: sheridan.local/Users

Group name:
Contractors

Group name (pre-Windows 2000):
Contractors

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution



Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type:

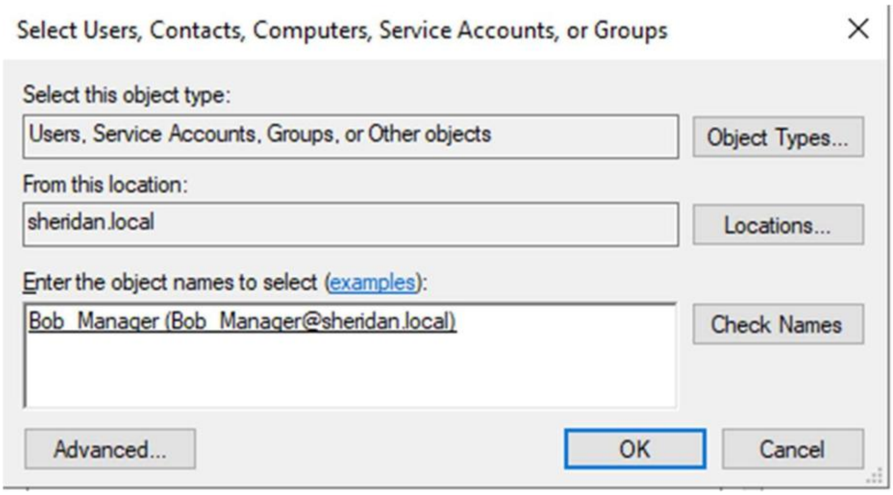
Users, Service Accounts, Groups, or Other objects

From this location:

sheridan.local

Enter the object names to select (examples):

Eve_Contractor (Eve_Contractor@sheridan.local)



Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type:

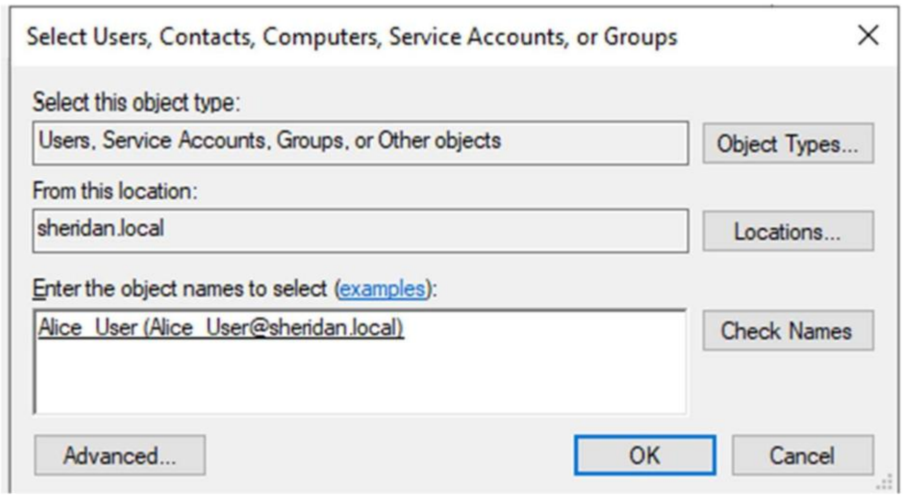
Users, Service Accounts, Groups, or Other objects

From this location:

sheridan.local

Enter the object names to select (examples):

Bob_Manager (Bob_Manager@sheridan.local)



Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type:

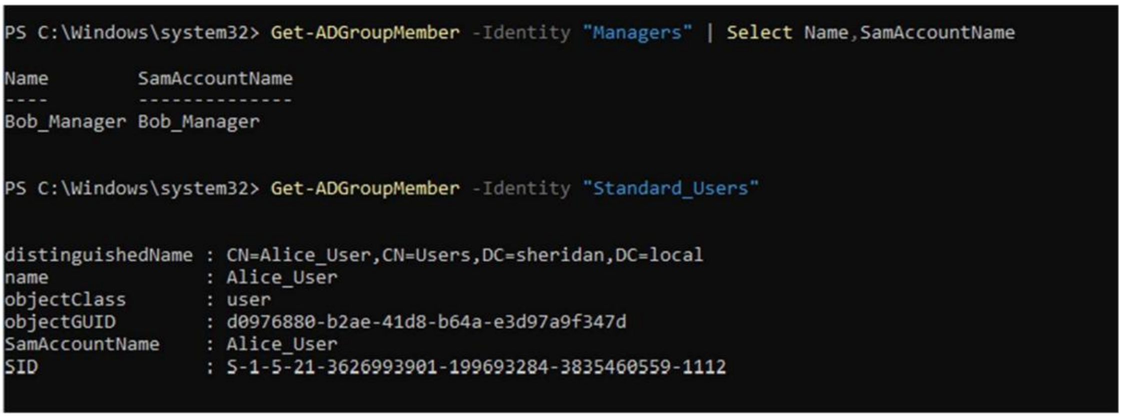
Users, Service Accounts, Groups, or Other objects

From this location:

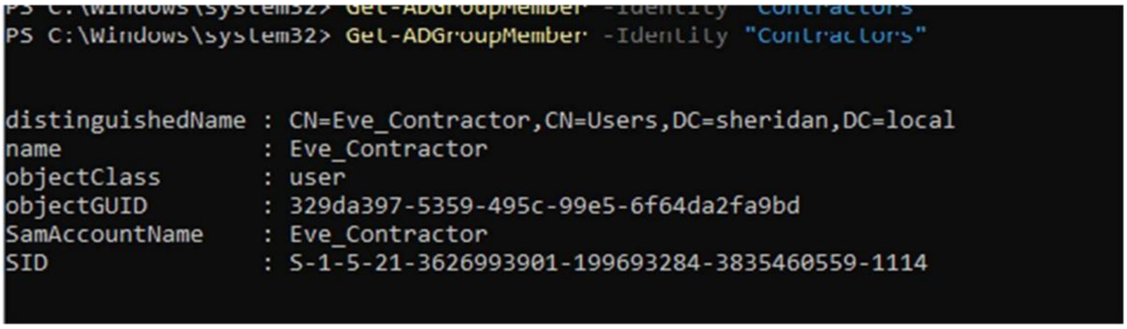
sheridan.local

Enter the object names to select (examples):

Alice_User (Alice_User@sheridan.local)

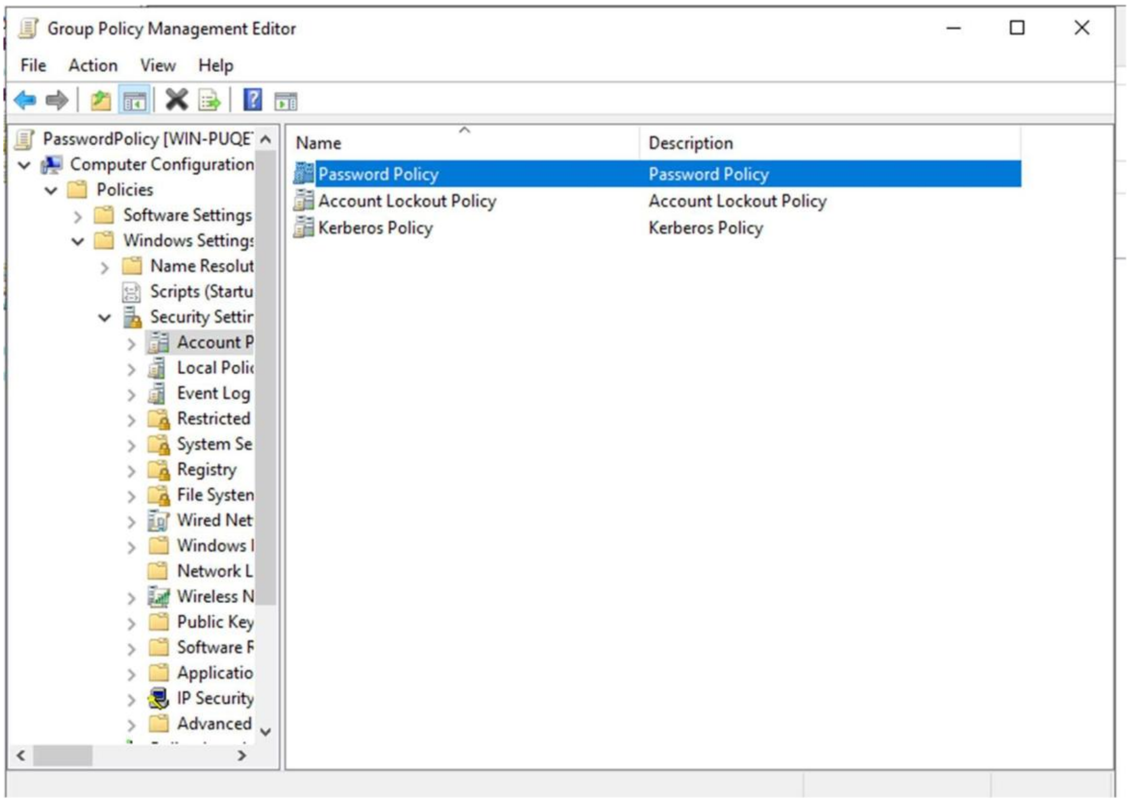


```
PS C:\Windows\system32> Get-ADGroupMember -Identity "Managers" | Select Name,SamAccountName

Name        SamAccountName
----        --------------
Bob_Manager Bob_Manager


PS C:\Windows\system32> Get-ADGroupMember -Identity "Standard_Users"


distinguishedName : CN=Alice_User,CN=Users,DC=sheridan,DC=local
name              : Alice_User
objectClass       : user
objectGUID        : d0976880-b2ae-41d8-b64a-e3d97a9f347d
SamAccountName    : Alice_User
SID               : S-1-5-21-3626993901-199693284-3835460559-1112
```

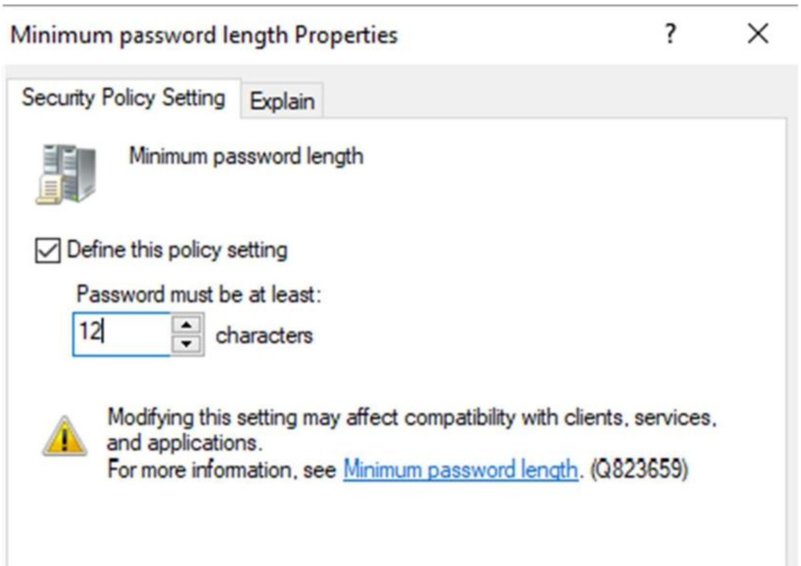


```
PS C:\Windows\system32> Get-ADGroupMember -Identity "Contractors"
PS C:\Windows\system32> Get-ADGroupMember -Identity "Contractors"


distinguishedName : CN=Eve_Contractor,CN=Users,DC=sheridan,DC=local
name              : Eve_Contractor
objectClass       : user
objectGUID        : 329da397-5359-495c-99e5-6f64da2fa9bd
SamAccountName    : Eve_Contractor
SID               : S-1-5-21-3626993901-199693284-3835460559-1114
```

PART C – SECURITY POLICIES



Name	Description
Password Policy	Password Policy
Account Lockout Policy	Account Lockout Policy
Kerberos Policy	Kerberos Policy



Minimum password length Properties

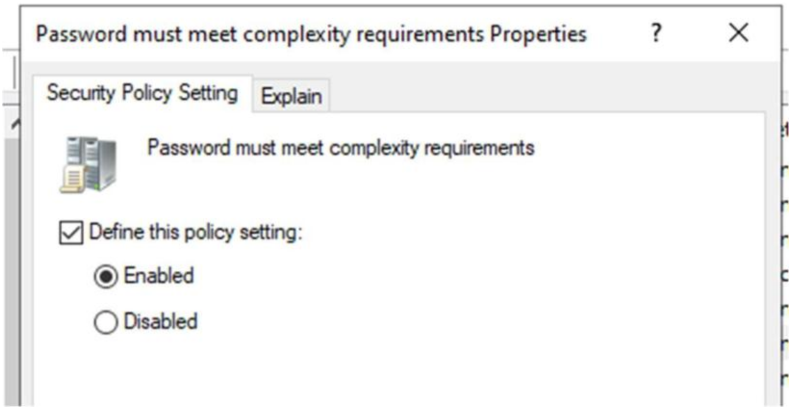
Minimum password length

☑ Define this policy setting

Password must be at least:

12 characters

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Minimum password length. (Q823659)



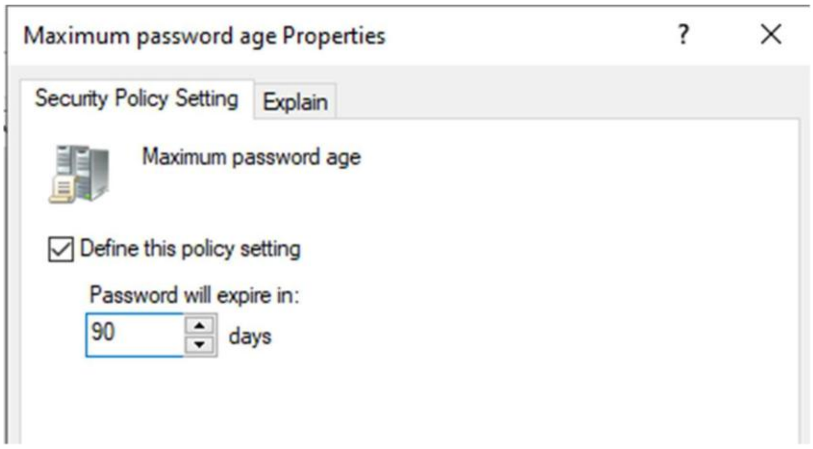
Password must meet complexity requirements Properties

Password must meet complexity requirements

☑ Define this policy setting:

● Enabled

○ Disabled



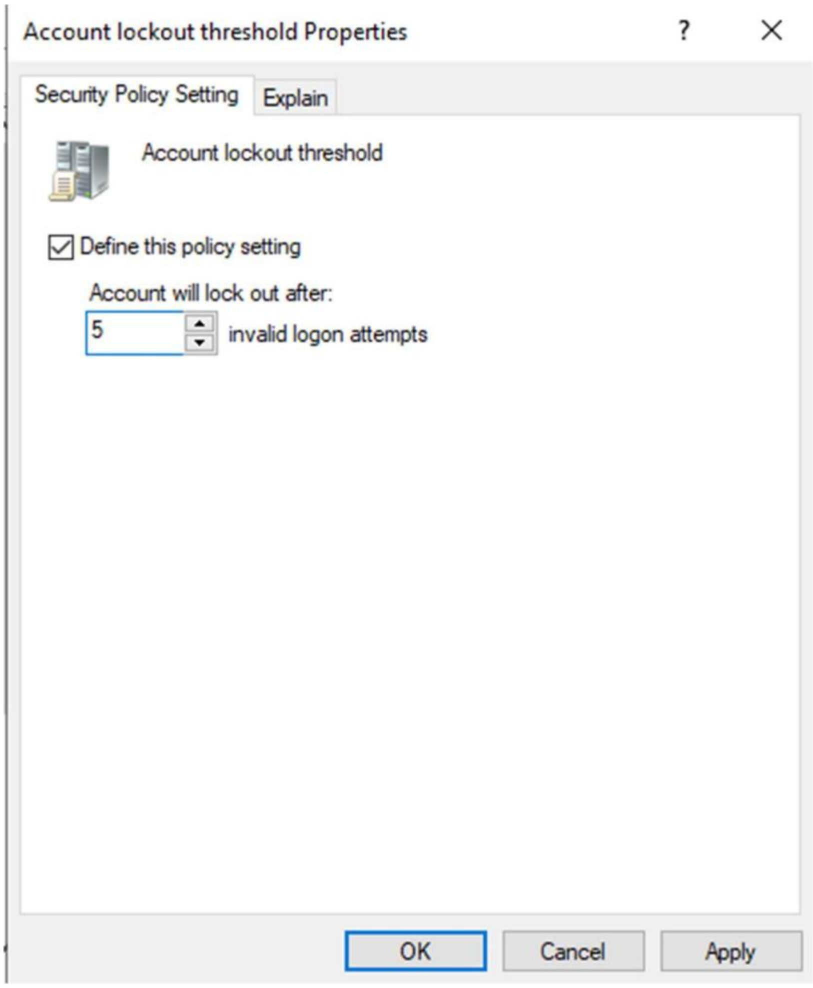
Maximum password age Properties

Maximum password age

☑ Define this policy setting

Password will expire in:

90 days



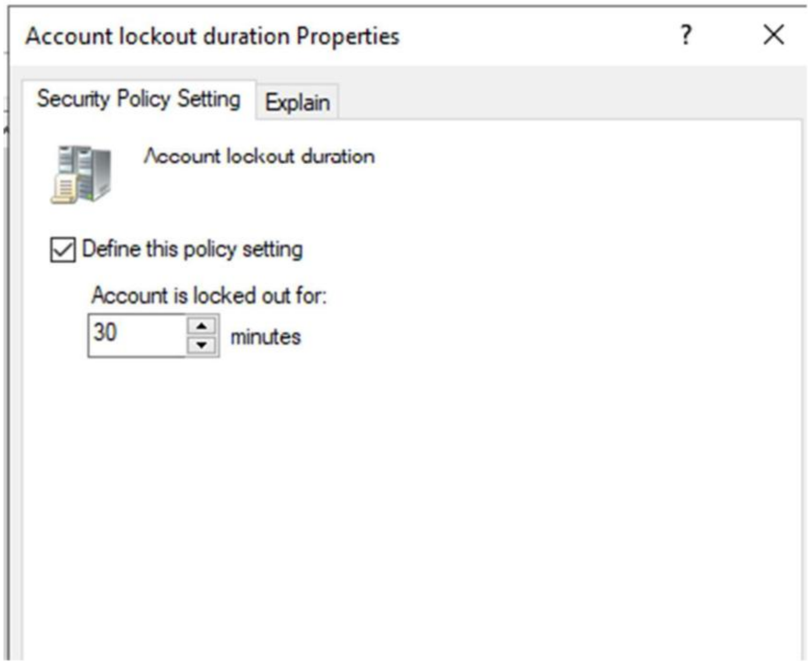
Account lockout threshold Properties

Account lockout threshold

☑ Define this policy setting

Account will lock out after:

5 invalid logon attempts



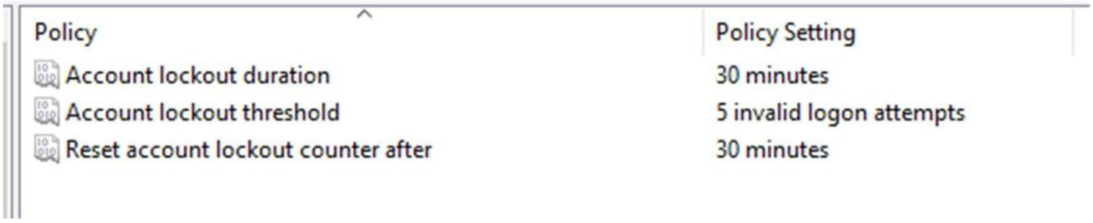
Account lockout duration Properties

Account lockout duration

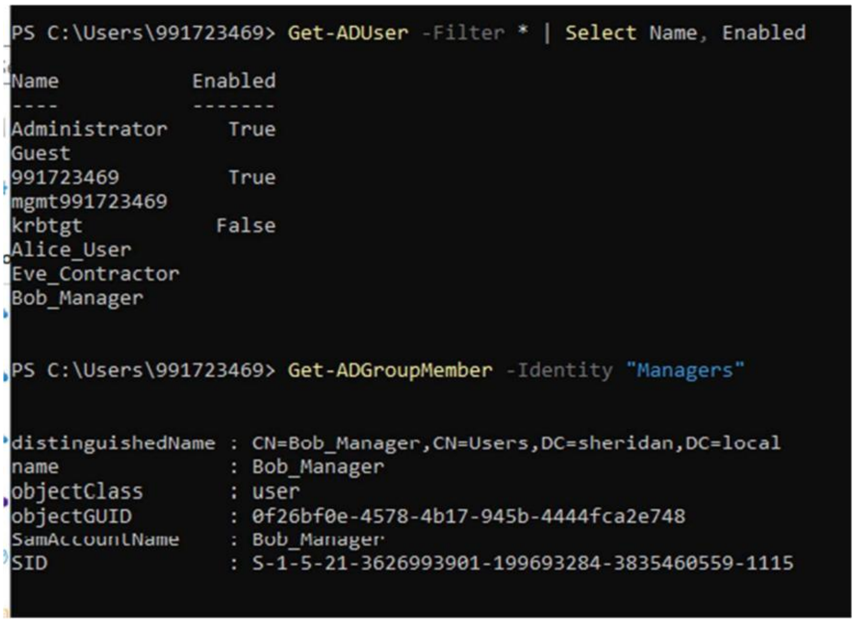
☑ Define this policy setting

Account is locked out for:

30 minutes

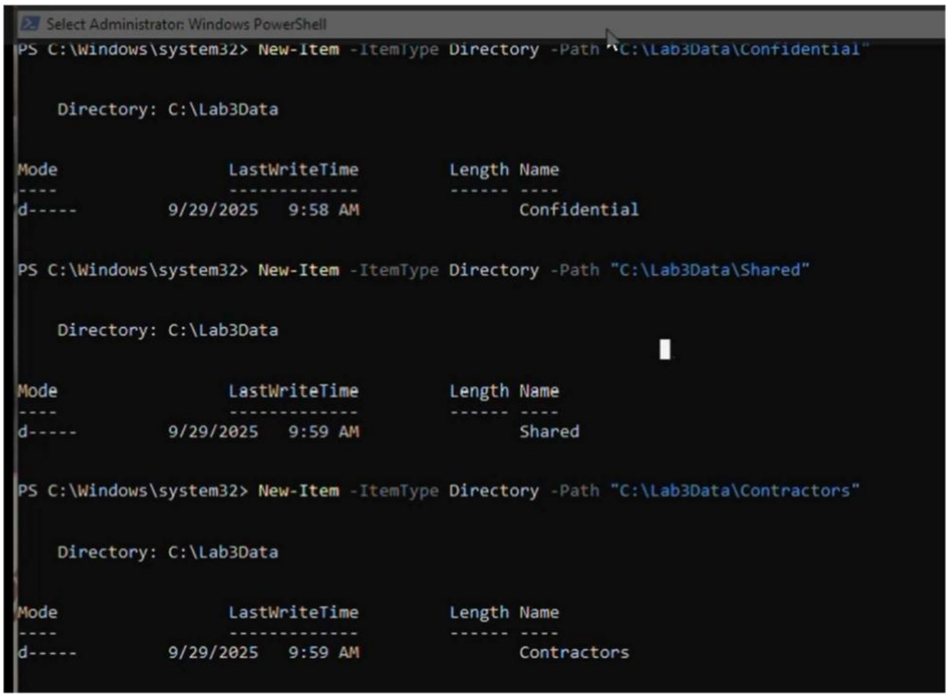


Policy	Policy Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes



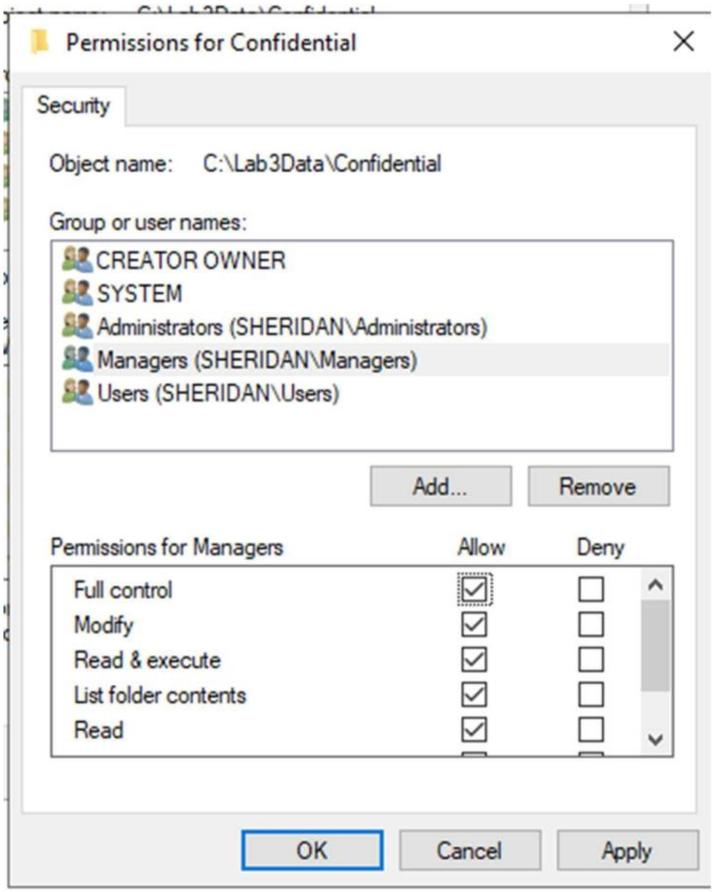
```
PS C:\Users\991723469> Get-ADUser -Filter * | Select Name, Enabled

Name           Enabled
----           -------
Administrator     True
Guest
991723469         True
mgmt991723469
krbtgt           False
Alice_User
Eve_Contractor
Bob_Manager


PS C:\Users\991723469> Get-ADGroupMember -Identity "Managers"


distinguishedName  : CN=Bob_Manager,CN=Users,DC=sheridan,DC=local
name               : Bob_Manager
objectClass        : user
objectGUID         : 0f26bf0e-4578-4b17-945b-4444fca2e748
SamAccountName     : Bob_Manager
SID                : S-1-5-21-3626993901-199693284-3835460559-1115
```

PART D – FOLDER STRUCTURE



```
PS C:\Windows\system32> New-Item -ItemType Directory -Path "C:\Lab3Data\Confidential"


    Directory: C:\Lab3Data


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/29/2025   9:58 AM                Confidential


PS C:\Windows\system32> New-Item -ItemType Directory -Path "C:\Lab3Data\Shared"


    Directory: C:\Lab3Data


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/29/2025   9:59 AM                Shared


PS C:\Windows\system32> New-Item -ItemType Directory -Path "C:\Lab3Data\Contractors"


    Directory: C:\Lab3Data


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/29/2025   9:59 AM                Contractors
```

PART E – NTFS PERMISSIONS



Permissions for Confidential

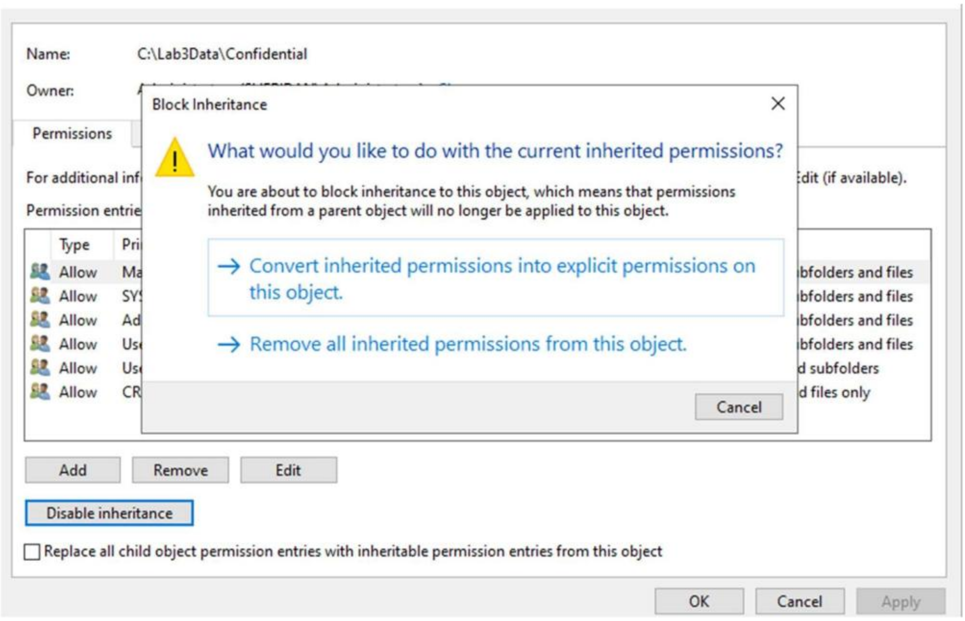
Security

Object name: C:\Lab3Data\Confidential

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (SHERIDAN\Administrators)
- Managers (SHERIDAN\Managers)
- Users (SHERIDAN\Users)

Permissions for Managers	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□



Name: C:\Lab3Data\Confidential

Owner:

Permissions

For additional inf

dit (if available).

Permission entrie

Type	Pri	
Allow	Ma	bfolders and files
Allow	SY	bfolders and files
Allow	Ad	bfolders and files
Allow	Us	bfolders and files
Allow	Us	d subfolders
Allow	CR	d files only

Block Inheritance

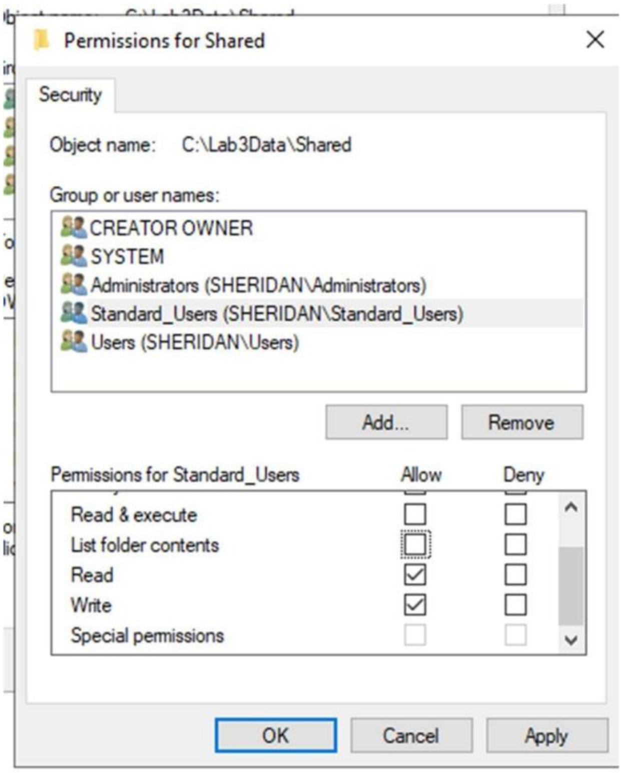
What would you like to do with the current inherited permissions?

You are about to block inheritance to this object, which means that permissions inherited from a parent object will no longer be applied to this object.

→ Convert inherited permissions into explicit permissions on this object.

→ Remove all inherited permissions from this object.

□ Replace all child object permission entries with inheritable permission entries from this object



Permissions for Shared

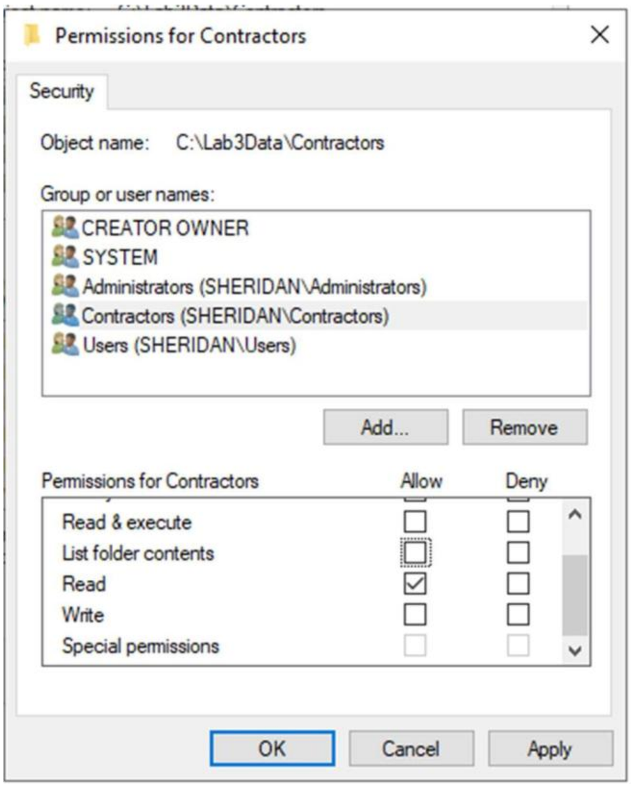
Security

Object name: C:\Lab3Data\Shared

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (SHERIDAN\Administrators)
- Standard_Users (SHERIDAN\Standard_Users)
- Users (SHERIDAN\Users)

Permissions for Standard_Users	Allow	Deny
Read & execute	□	□
List folder contents	□	□
Read	☑	□
Write	☑	□
Special permissions	□	□



Permissions for Contractors

Security

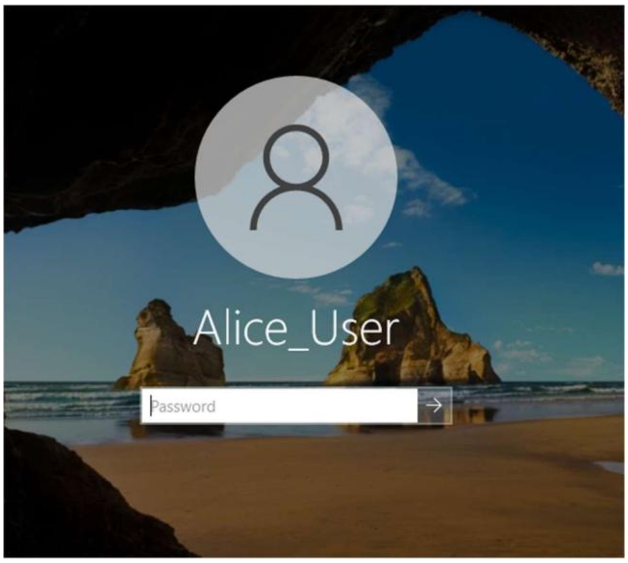
Object name: C:\Lab3Data\Contractors

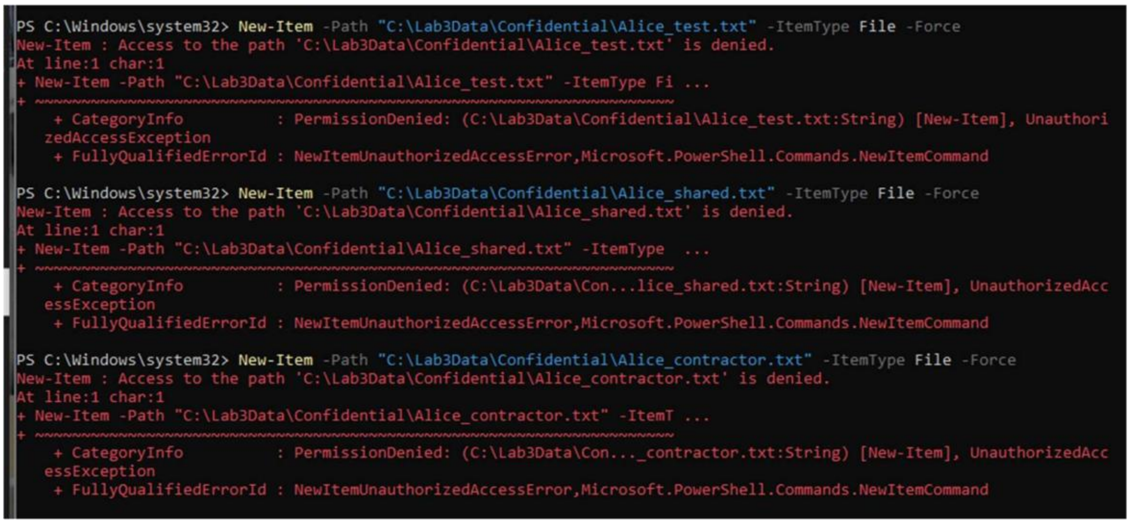
Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (SHERIDAN\Administrators)
- Contractors (SHERIDAN\Contractors)
- Users (SHERIDAN\Users)

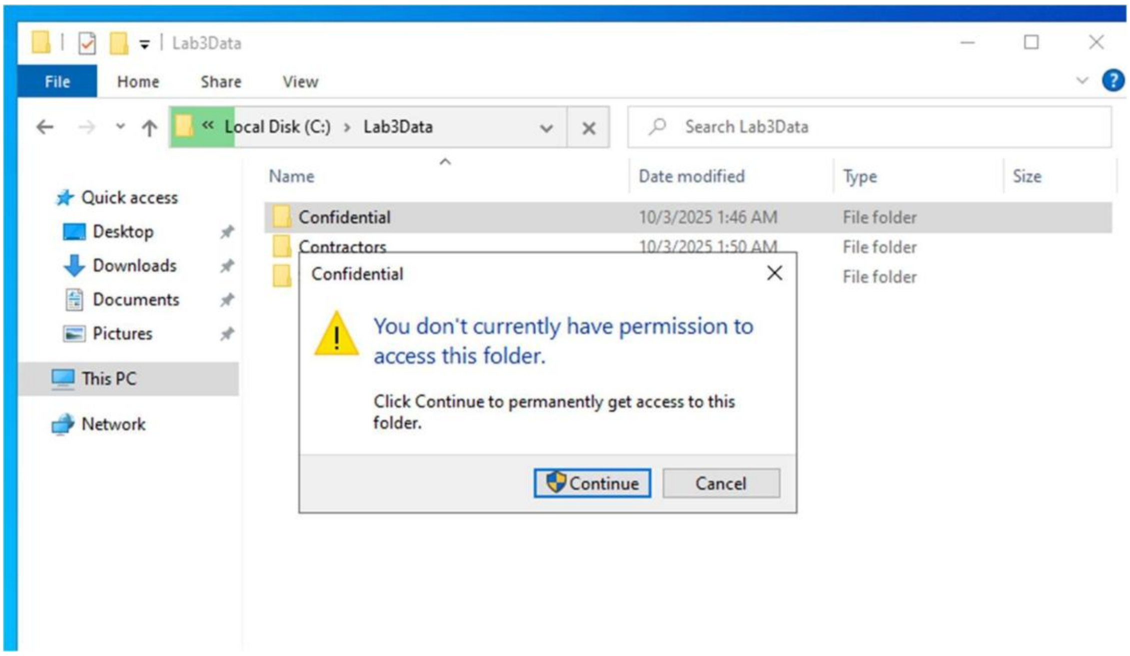
Permissions for Contractors	Allow	Deny
Read & execute	□	□
List folder contents	□	□
Read	☑	□
Write	□	□
Special permissions	□	□

PART F – TESTING PERMISSIONS



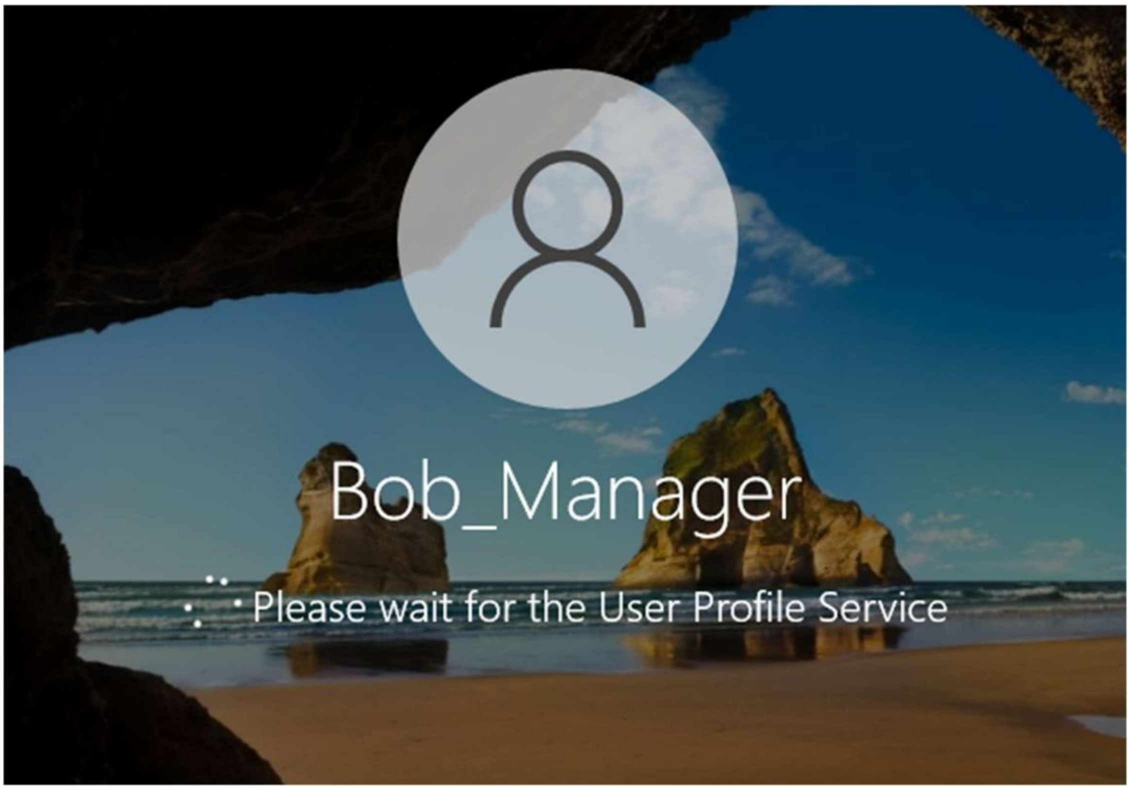


```
PS C:\Windows\system32> New-Item -Path "C:\Lab3Data\Confidential\Alice_test.txt" -ItemType File -Force
New-Item : Access to the path 'C:\Lab3Data\Confidential\Alice_test.txt' is denied.
At line:1 char:1
+ New-Item -Path "C:\Lab3Data\Confidential\Alice_test.txt" -ItemType Fi ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Lab3Data\Confidential\Alice_test.txt:String) [New-Item], Unauthori
   zedAccessException
    + FullyQualifiedErrorId : NewItemUnauthorizedAccessError,Microsoft.PowerShell.Commands.NewItemCommand

PS C:\Windows\system32> New-Item -Path "C:\Lab3Data\Confidential\Alice_shared.txt" -ItemType File -Force
New-Item : Access to the path 'C:\Lab3Data\Confidential\Alice_shared.txt' is denied.
At line:1 char:1
+ New-Item -Path "C:\Lab3Data\Confidential\Alice_shared.txt" -ItemType  ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Lab3Data\Con...lice_shared.txt:String) [New-Item], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : NewItemUnauthorizedAccessError,Microsoft.PowerShell.Commands.NewItemCommand

PS C:\Windows\system32> New-Item -Path "C:\Lab3Data\Confidential\Alice_contractor.txt" -ItemType File -Force
New-Item : Access to the path 'C:\Lab3Data\Confidential\Alice_contractor.txt' is denied.
At line:1 char:1
+ New-Item -Path "C:\Lab3Data\Confidential\Alice_contractor.txt" -ItemT ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Lab3Data\Con..._contractor.txt:String) [New-Item], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : NewItemUnauthorizedAccessError,Microsoft.PowerShell.Commands.NewItemCommand
```



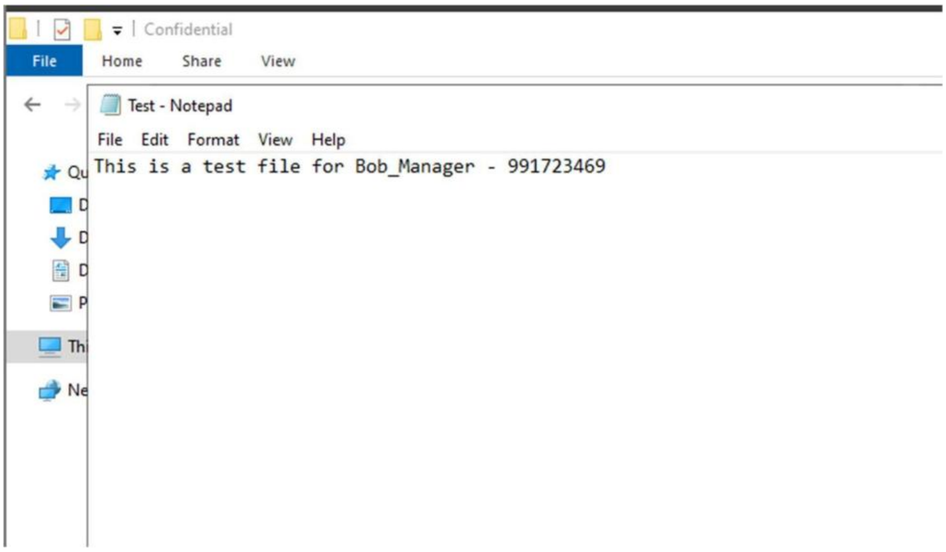
You don't currently have permission to access this folder.

Click Continue to permanently get access to this folder.



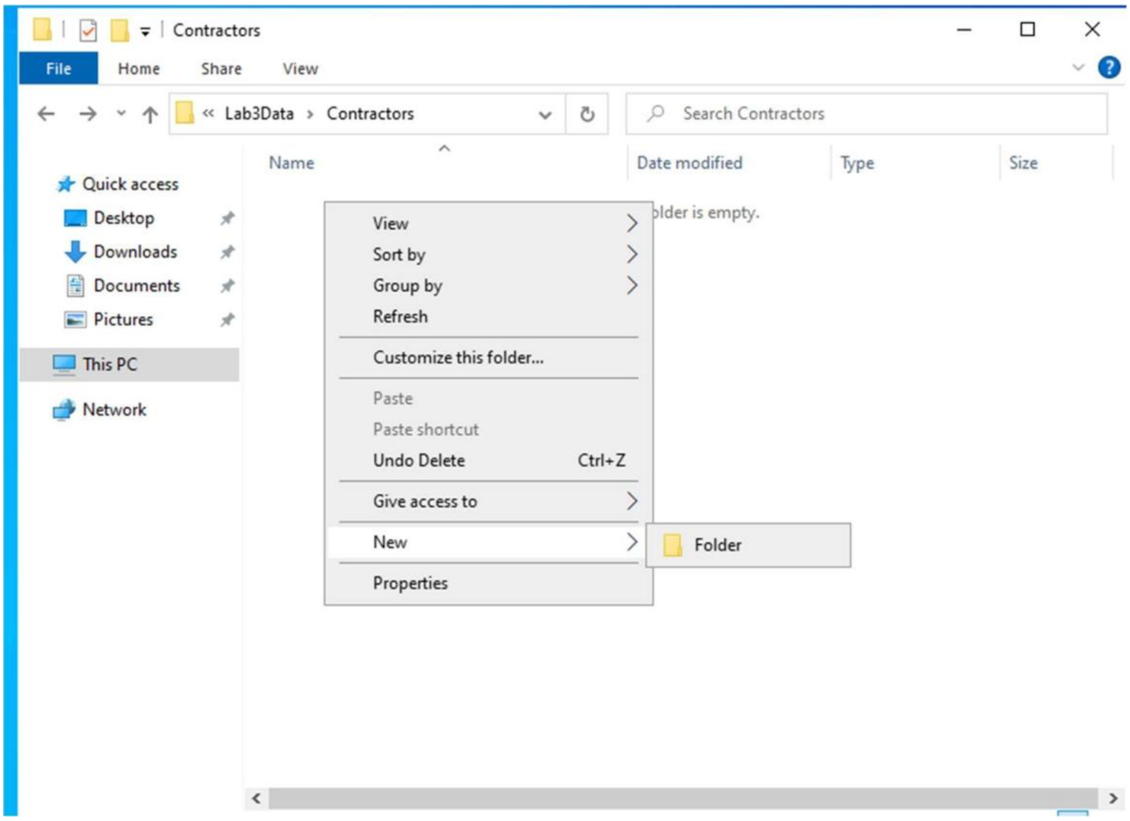
Bob_Manager

Please wait for the User Profile Service

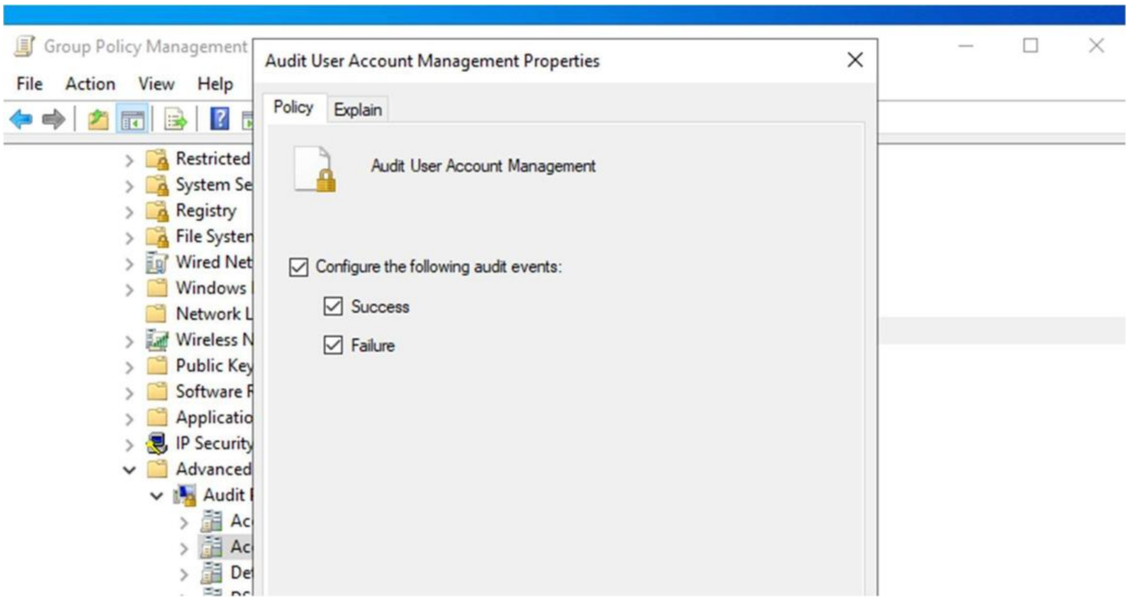


This is a test file for Bob_Manager - 991723469

Eve_Contractors cannot create a file in the contractors folder



PART G – AUDITING



Audit User Account Management Properties

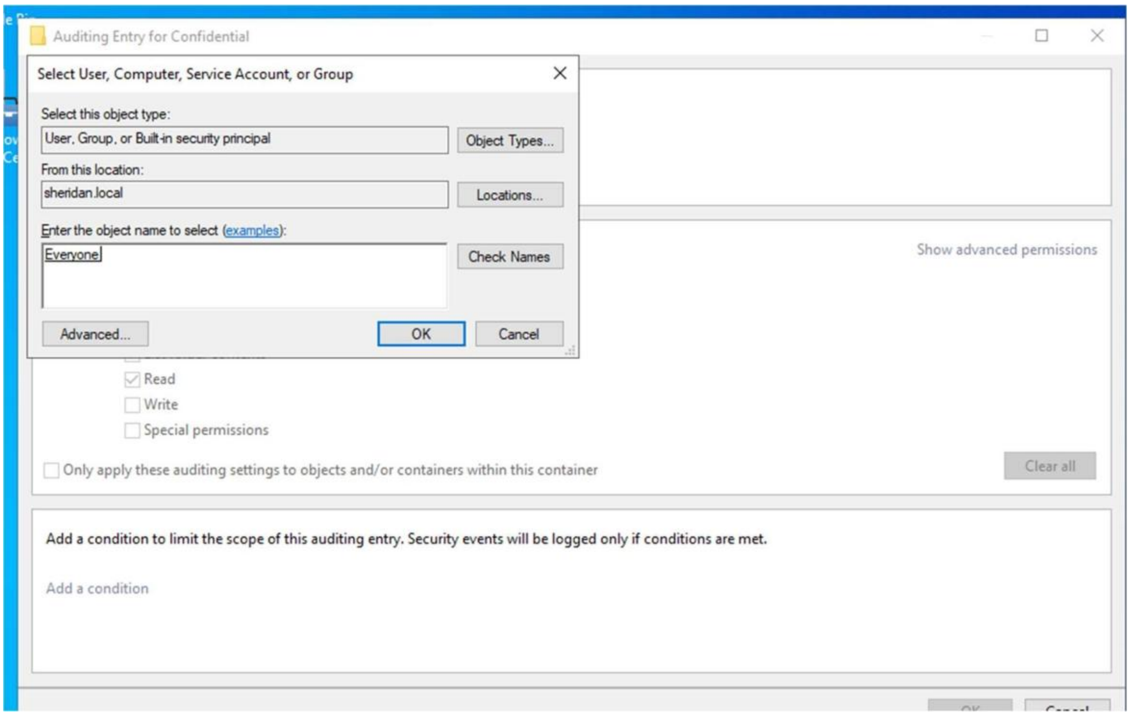
Policy | Explain

Audit User Account Management

☑ Configure the following audit events:

☑ Success

☑ Failure



Auditing Entry for Confidential

Select User, Computer, Service Account, or Group

Select this object type:
User, Group, or Built-in security principal
Object Types...

From this location:
sheridan.local
Locations...

Enter the object name to select (examples):
Everyone
Check Names

Advanced... OK Cancel

Show advanced permissions

☑ Read

☐ Write

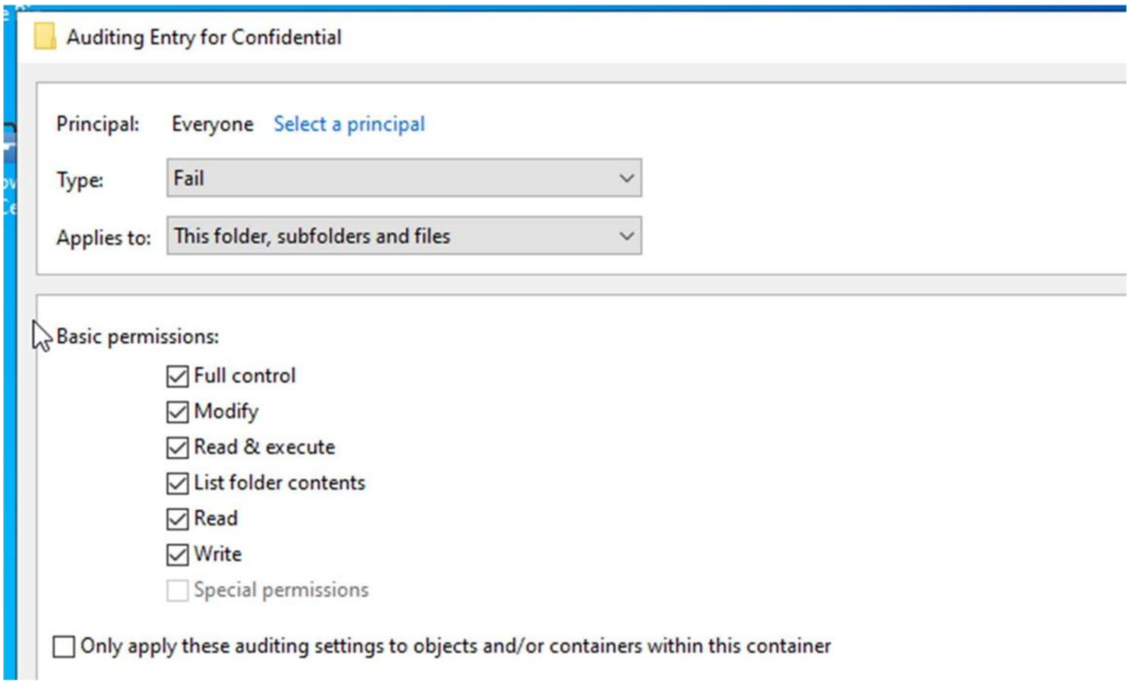
☐ Special permissions

☐ Only apply these auditing settings to objects and/or containers within this container

Clear all

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

Add a condition



Auditing Entry for Confidential

Principal: Everyone

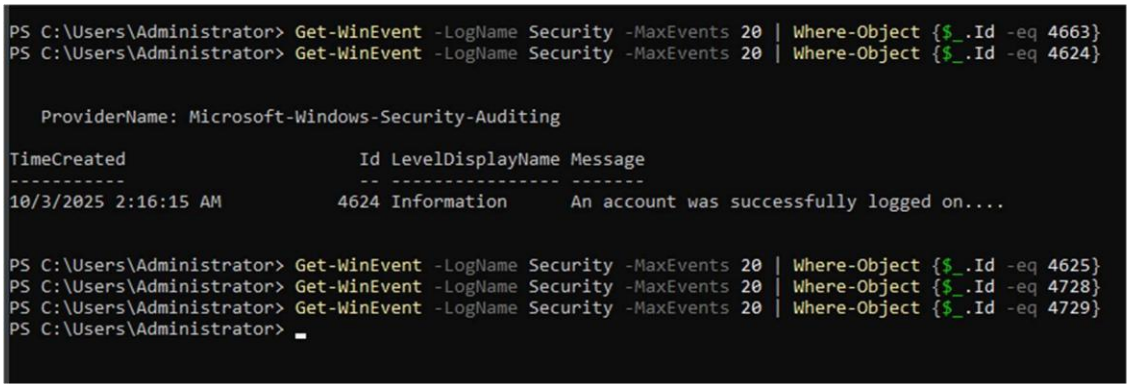
Type: Fail

Applies to: This folder, subfolders and files

Basic permissions:

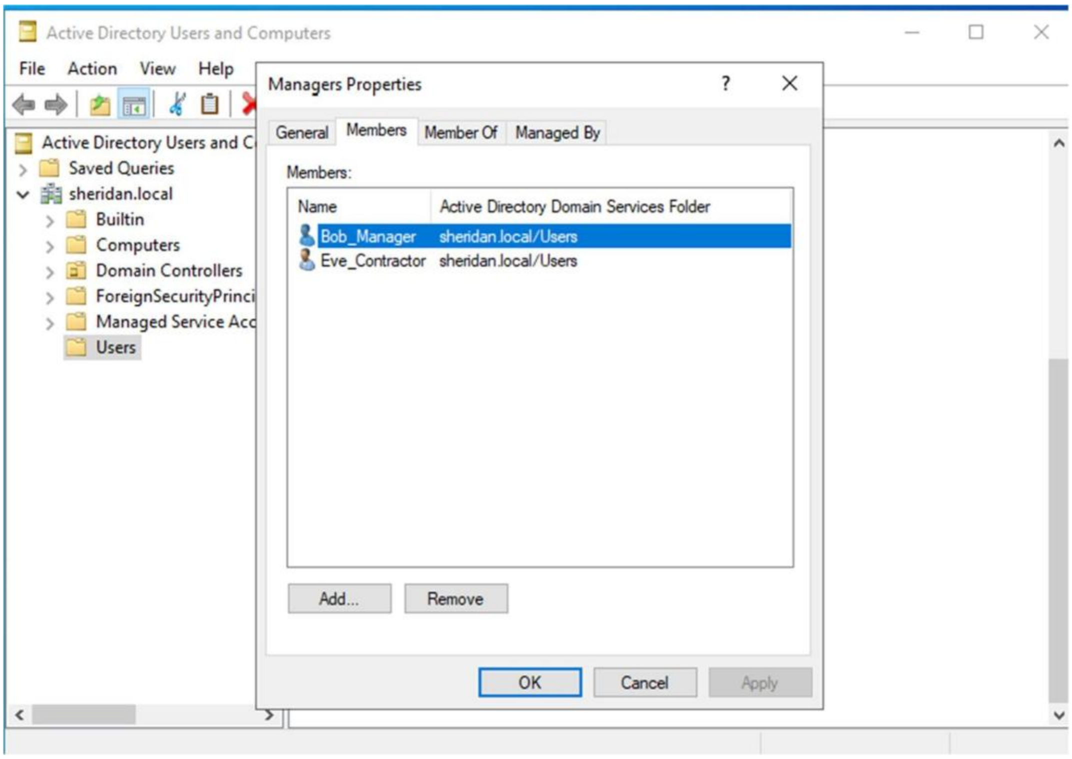
☑ Full control
☑ Modify
☑ Read & execute
☑ List folder contents
☑ Read
☑ Write
□ Special permissions

□ Only apply these auditing settings to objects and/or containers within this container



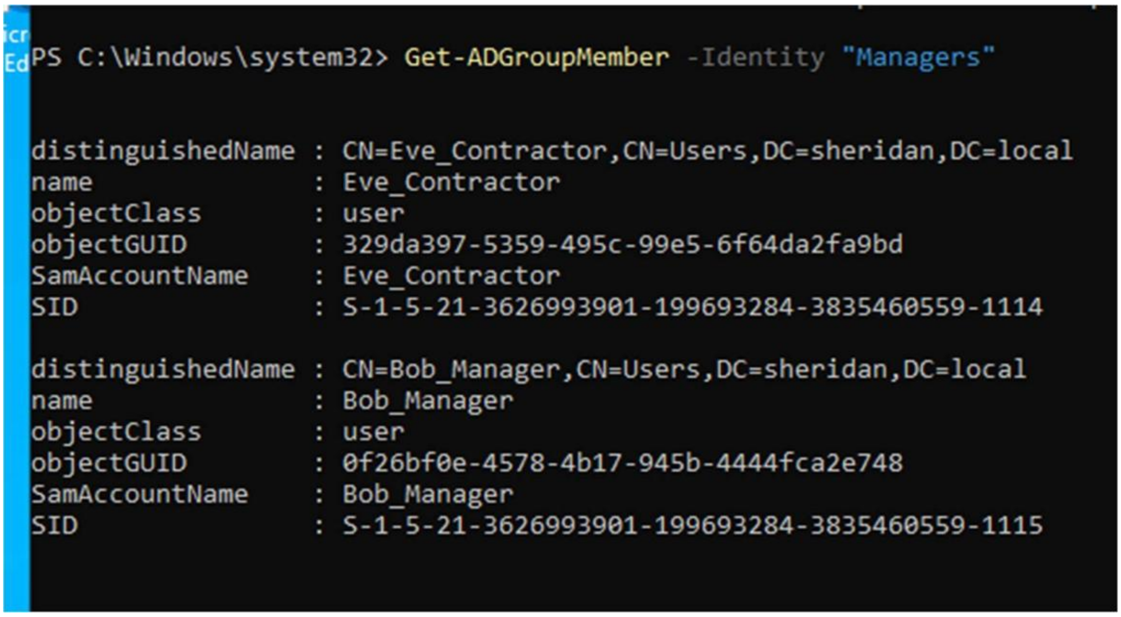
```
PS C:\Users\Administrator> Get-WinEvent -LogName Security -MaxEvents 20 | Where-Object {$_.Id -eq 4663}
PS C:\Users\Administrator> Get-WinEvent -LogName Security -MaxEvents 20 | Where-Object {$_.Id -eq 4624}


   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
10/3/2025 2:16:15 AM          4624 Information      An account was successfully logged on....


PS C:\Users\Administrator> Get-WinEvent -LogName Security -MaxEvents 20 | Where-Object {$_.Id -eq 4625}
PS C:\Users\Administrator> Get-WinEvent -LogName Security -MaxEvents 20 | Where-Object {$_.Id -eq 4728}
PS C:\Users\Administrator> Get-WinEvent -LogName Security -MaxEvents 20 | Where-Object {$_.Id -eq 4729}
PS C:\Users\Administrator>
```

PART H – MISCONFIGURATION SIMULATION

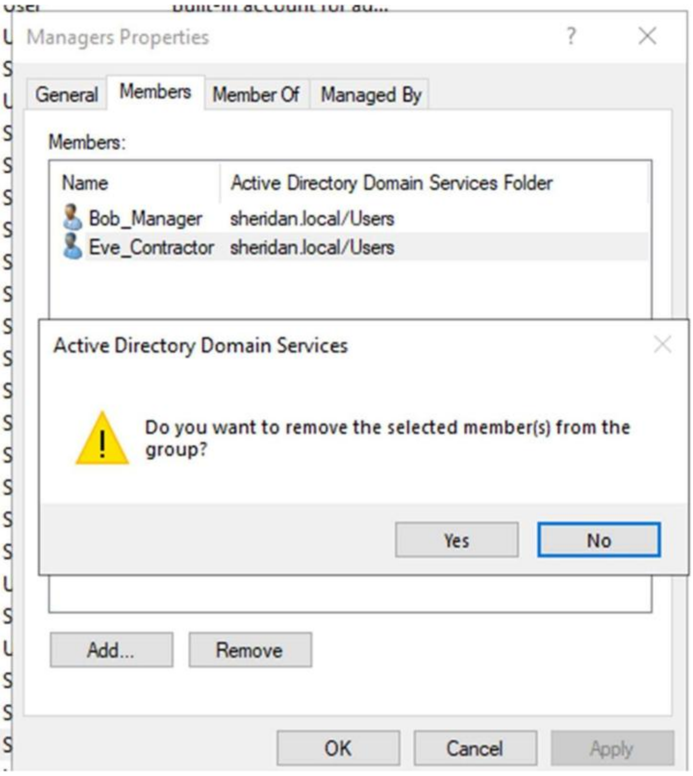


Members:

Name	Active Directory Domain Services Folder
Bob_Manager	sheridan.local/Users
Eve_Contractor	sheridan.local/Users



```
PS C:\Windows\system32> Get-ADGroupMember -Identity "Managers"


distinguishedName : CN=Eve_Contractor,CN=Users,DC=sheridan,DC=local
name              : Eve_Contractor
objectClass       : user
objectGUID        : 329da397-5359-495c-99e5-6f64da2fa9bd
SamAccountName    : Eve_Contractor
SID               : S-1-5-21-3626993901-199693284-3835460559-1114

distinguishedName : CN=Bob_Manager,CN=Users,DC=sheridan,DC=local
name              : Bob_Manager
objectClass       : user
objectGUID        : 0f26bf0e-4578-4b17-945b-4444fca2e748
SamAccountName    : Bob_Manager
SID               : S-1-5-21-3626993901-199693284-3835460559-1115
```



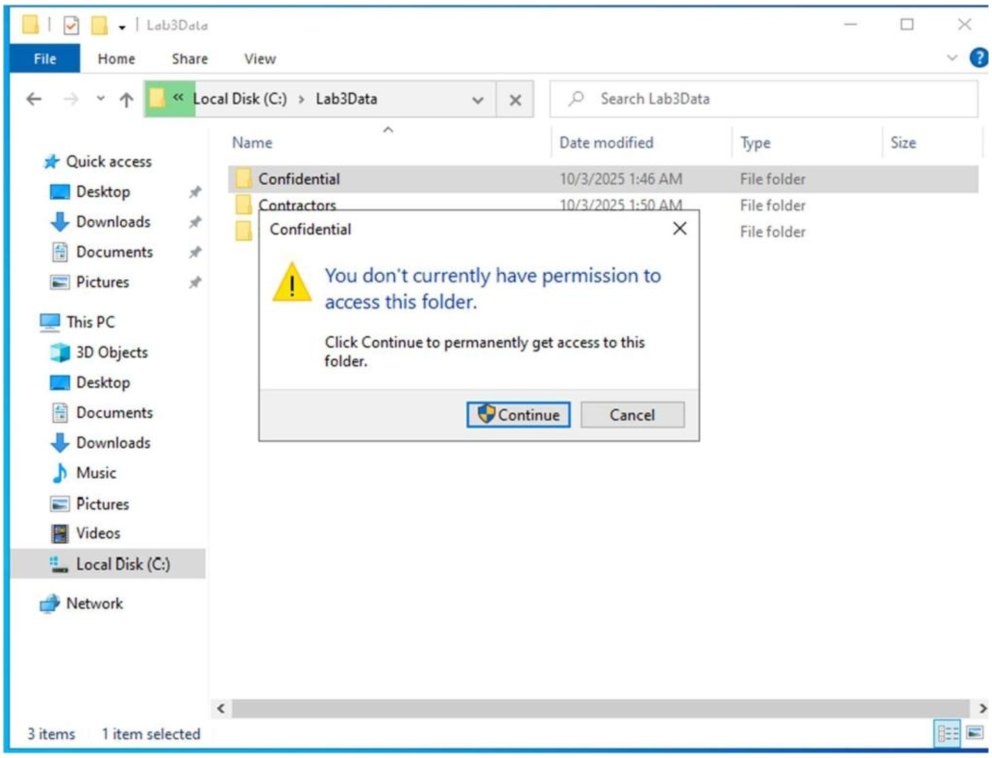
Managers Properties

Members:

Name	Active Directory Domain Services Folder
Bob_Manager	sheridan.local/Users
Eve_Contractor	sheridan.local/Users

Active Directory Domain Services

Do you want to remove the selected member(s) from the group?



Lab3Data

Name	Date modified	Type	Size
Confidential	10/3/2025 1:46 AM	File folder	
Contractors	10/3/2025 1:50 AM	File folder	
		File folder	

Confidential

You don't currently have permission to access this folder.

Click Continue to permanently get access to this folder.

3 items 1 item selected

Reflection

How do AD policies and NTFS permissions work together to enforce security? What risks arise if one is misconfigured?

Active directory policies and NTFS permissions create a strong, layered security defense. AD controls who can log in and which security groups they belong to, while NTFS dictates what files and folders those groups are allowed to use. A misstep in either setting can result in a data leak or privilege escalation. When Group Policy enforcement is combined with properly configured folder permissions and regular auditing, organizations gain the power to effectively prevent, spot, and react to unauthorized access.