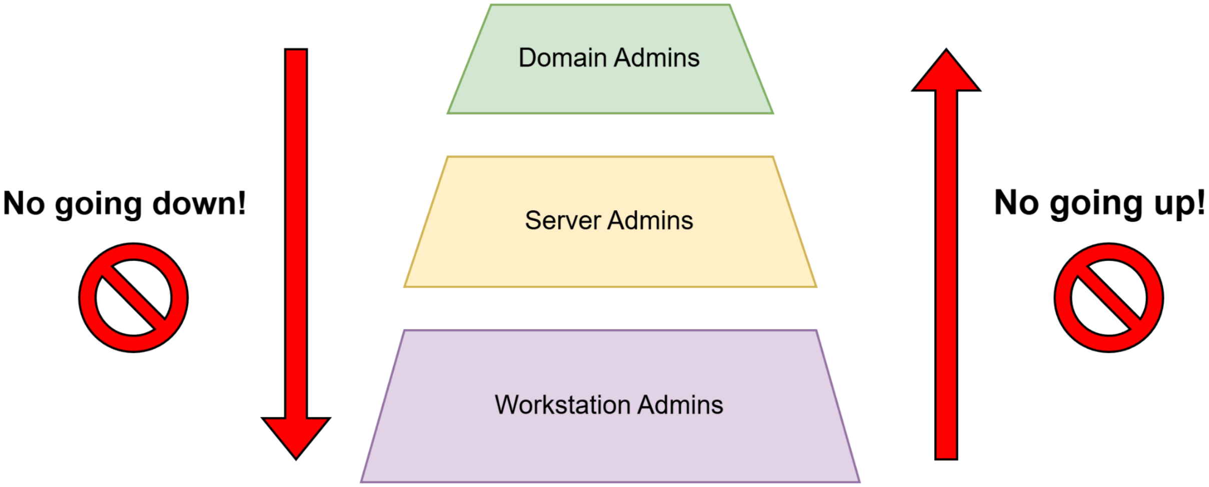
# Active Directory Tiered Access Model Lab
## By Michael Ambeguia

**Purpose:** Active Directory domains are vast and are composed of many different devices and user accounts with varying security risks and requirements. Domains are typically made up of Domain Controllers, servers, and workstations. These three device types each have their own security risks and must be protected from unauthorized logons. A great way to secure an AD domain is to implement a tiered access model in which privileged access to these device types is limited to only administrators associated with them. This access control model can prevent hackers from moving laterally within a domain, prevents unauthorized access to sensitive data, and helps organizations enforce separation of duties. In this lab I will implement the tiered access model in my home lab Active Directory environment.

## Sections:

## Section #1 Introduction



The tiered access model is a vital secure policy to enforce for an Active Directory domain. The basic premise of this model is to prevent the misuse of privileged users within the domain. This model has three tiers which are domain admins, server admins, and workstation admins. Domain admins can only access and work on domain controllers, server admins can only work on non DC servers, and workstation admins can only access and work on workstations.

Why is this model even important to enforce?

1. Prevent lateral movement: If a malicious actor were to perform a privilege escalation attack successfully they will be stuck at the level they escalated in. For instance, if they escalated in the workstation level they would not be able to move up to the server or Domain Controller level.

2. Protect sensitive data: Sensitive data is protected since only administrators with the privilege to access and work with it are allowed. This prevents accidental mishaps and exposure of data by unauthorized individuals.

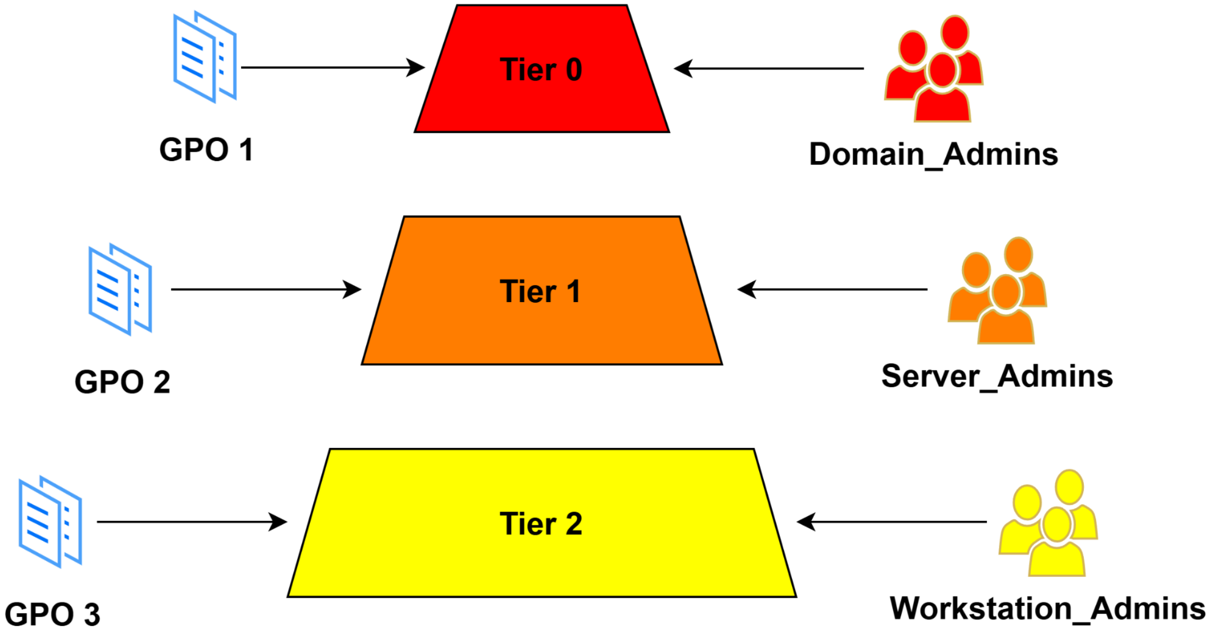
3. Enforce principle of least privilege: Since administrators will only have permissions to work at their assigned level the principle of least privilege is enforced. Workstation admins only have access to the user workstations they are responsible for administering, they cannot administer the servers. Server admins will not be able to work on workstations or DCs. No one will be able to do more than what they were assigned to do!

4. Segregation of duties: Segregation of duties is implemented since each level of administrator can only "stay in their lane". Lower level IT workers will only have workstation admin permissions and won't be able log onto a file server or the domain controller.

What are the limitations of this model?

***The main limitation of the tiered access model is that it will not prevent privilege escalation on a tier!*** If a hacker were to breach the network and land on a workstation they will have the ability to escalate privileges if there are vulnerabilities on the system that will allow it. The good thing is that they will be stuck at tier 2 and won't be able to move to tier 1 or tier 0. Limiting the scope of a breach is a vital ability for organizations.

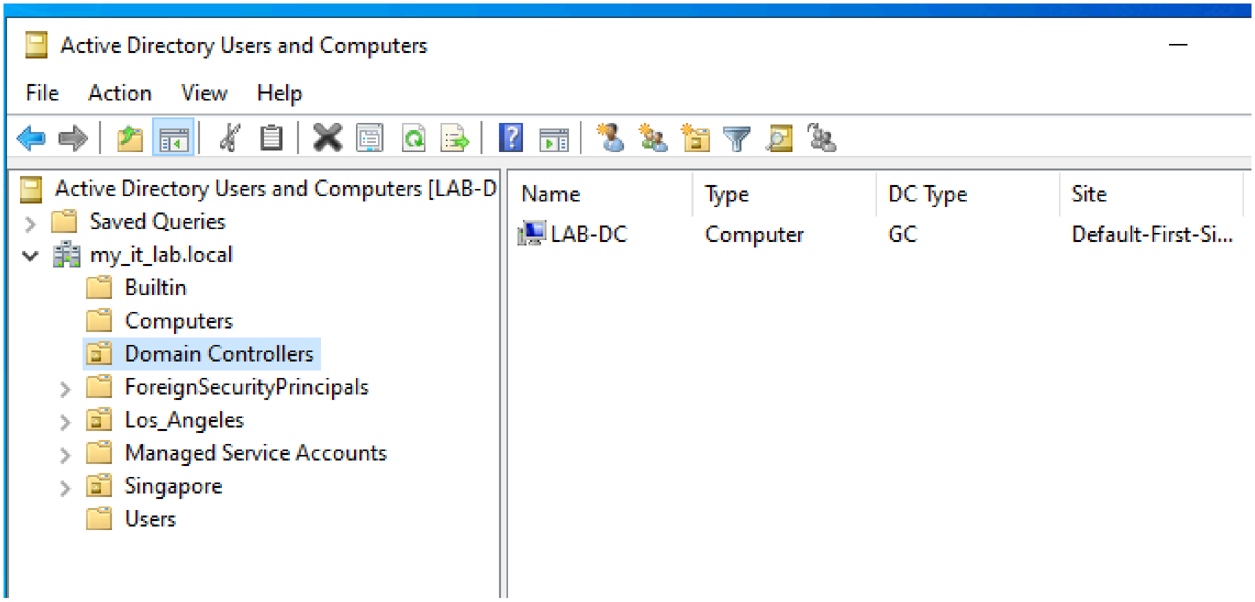
How can this model be implemented?



1. Devices must be separated into Organizational Units based on device type.
2. Each tier needs its own administrator group that is delegated control over it.
3. There needs to be GPOs for each tier's OU to prevent logins from lower and higher tiers.

# Section #2 Separate devices into OUs

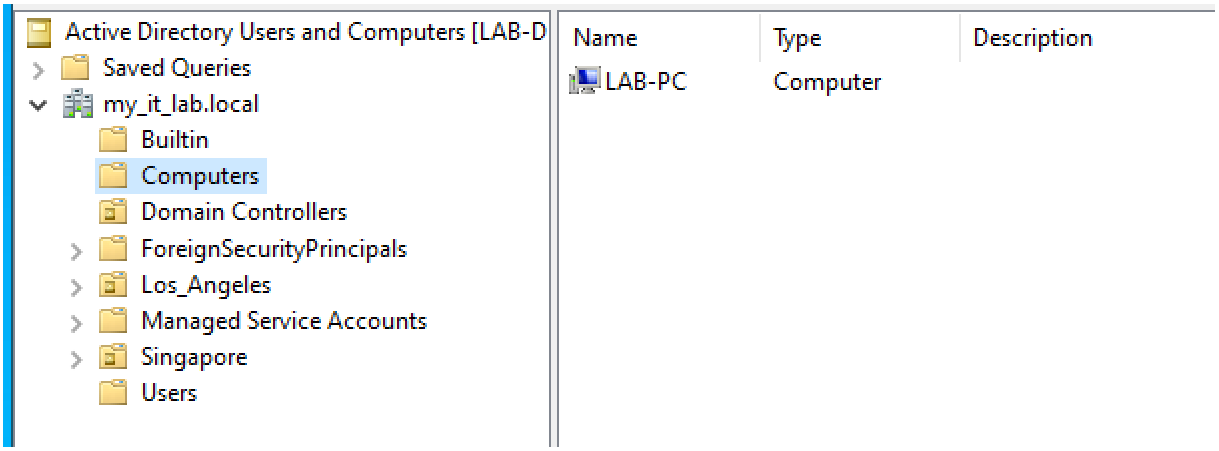
2.1 Verify there is a a Domain Controllers OU:



| Name | Type | DC Type | Site |
|---|---|---|---|
| LAB-DC | Computer | GC | Default-First-Si... |

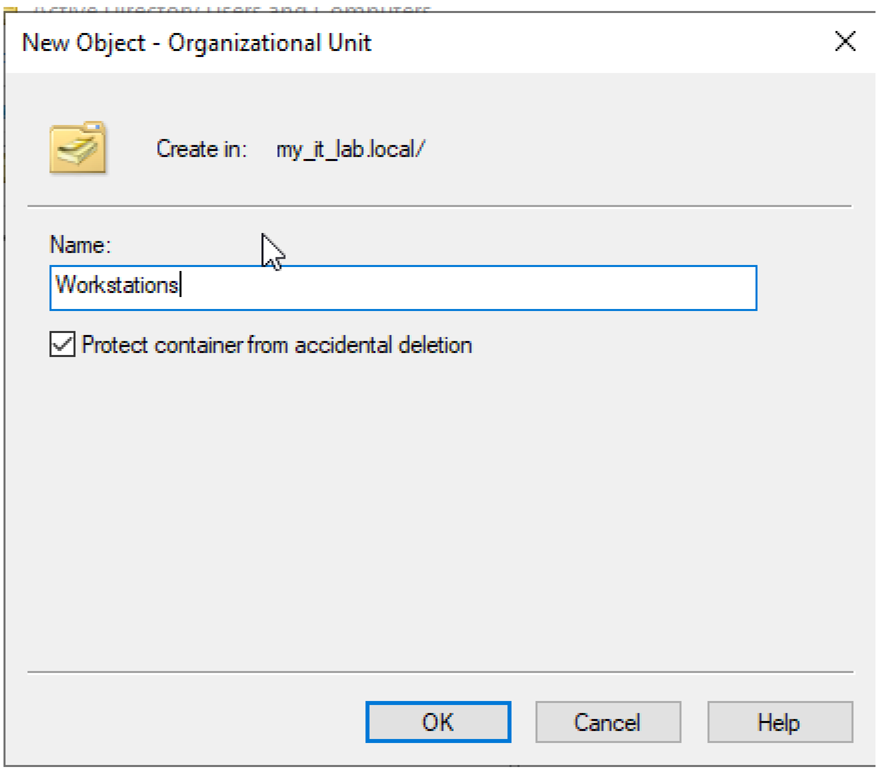
My domain controller is already in the Domain Controllers OU.  This OU is created by Active Directory by default, even putting domain controllers in the OU automatically.

2.2 Create a workstation OU:



| Name | Type | Description |
|---|---|---|
| LAB-PC | Computer | |

Currently a workstation PC is only in the default Computers OU. I will create a workstation OU now to enforce separation since there is no default workstation OU.

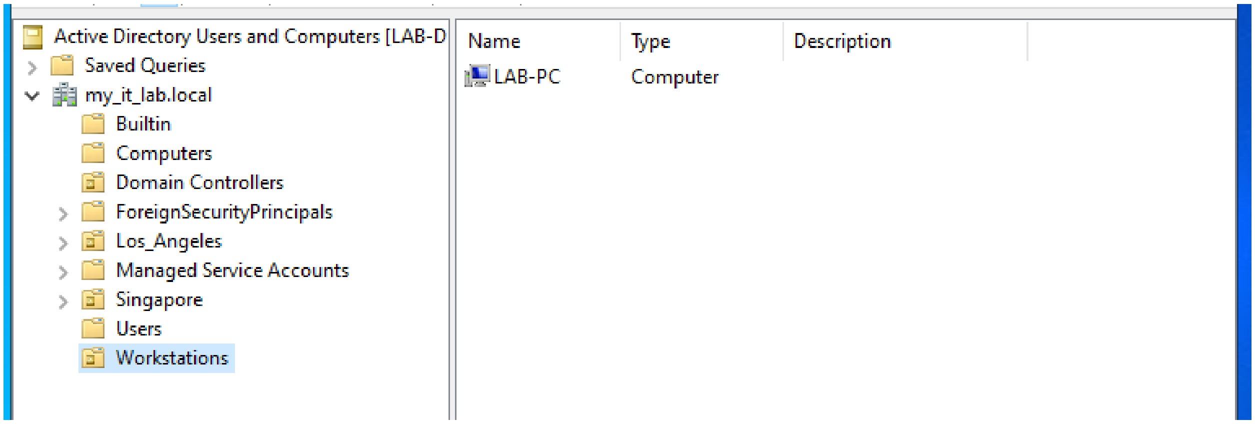


Create in: my_it_lab.local/

Name: Workstations

☑ Protect container from accidental deletion

Giving the new OU a name, Workstations.

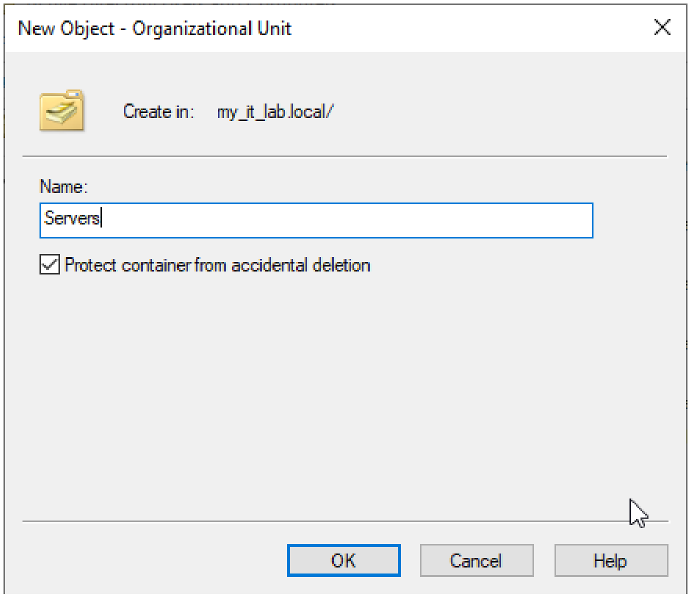


| Name | Type | Description |
|---|---|---|
| LAB-PC | Computer | |

Moved the LAB-PC workstation to the proper OU. Now the LAB-PC workstation is in the Workstations OU.

2.3 Create a server OU:

I do not have any extra Windows Server devices but I will still create an OU for this tier.



Create in: my_it_lab.local/

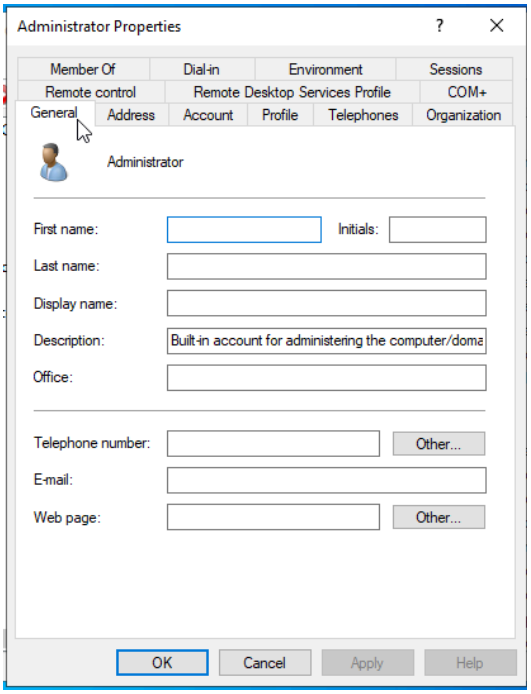
Name:
Servers

☑ Protect container from accidental deletion

Since I do not have any extra server devices I don’t have any to move to this OU.

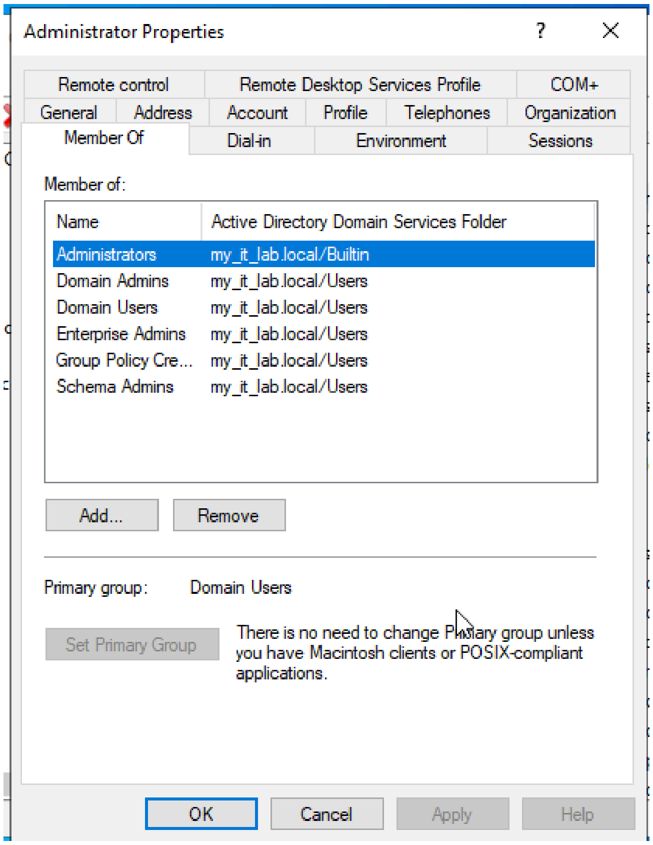
# Section #3 Create tiered admin accounts

3.1 Verify that a domain admin account is already created:



Administrator

First name:
Initials:
Last name:
Display name:
Description: Built-in account for administering the computer/doma
Office:
Telephone number:
E-mail:
Web page:

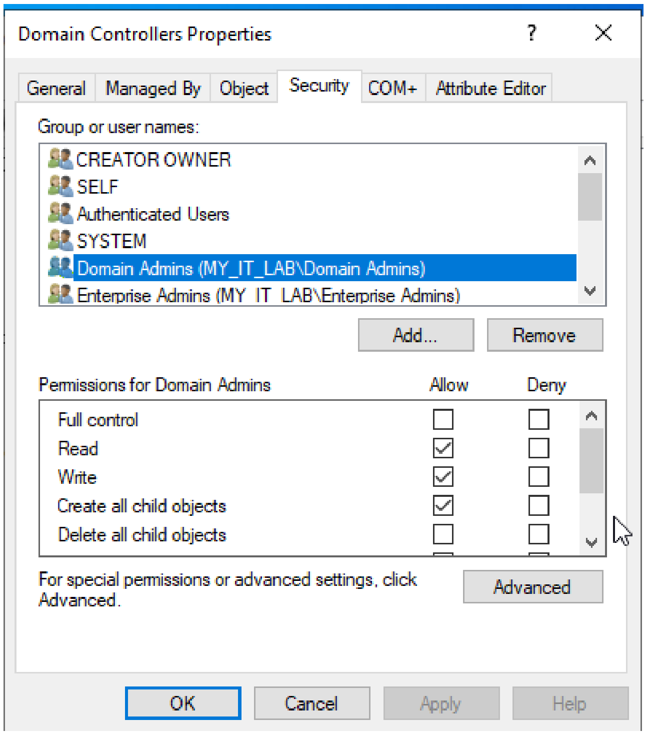


Member of:

| Name | Active Directory Domain Services Folder |
|---|---|
| Administrators | my_it_lab.local/Builtin |
| Domain Admins | my_it_lab.local/Users |
| Domain Users | my_it_lab.local/Users |
| Enterprise Admins | my_it_lab.local/Users |
| Group Policy Cre... | my_it_lab.local/Users |
| Schema Admins | my_it_lab.local/Users |

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.



Group or user names:

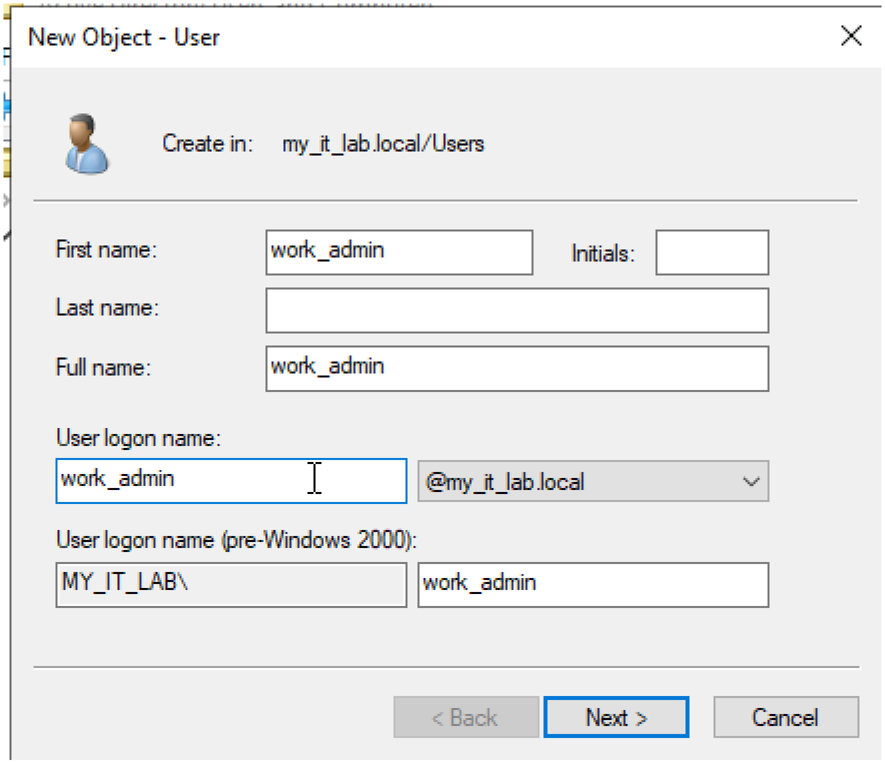
- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- Domain Admins (MY_IT_LAB\Domain Admins)
- Enterprise Admins (MY_IT_LAB\Enterprise Admins)

| Permissions for Domain Admins | Allow | Deny |
|---|---|---|
| Full control | □ | □ |
| Read | ☑ | □ |
| Write | ☑ | □ |
| Create all child objects | ☑ | □ |
| Delete all child objects | □ | □ |

For special permissions or advanced settings, click Advanced.

There already is a domain administrator account created named Administrator.

3.2 Create  a workstation admin account:
Creating a new user named work_admin.



New Object - User

Create in: my_it_lab.local/Users

First name: work_admin

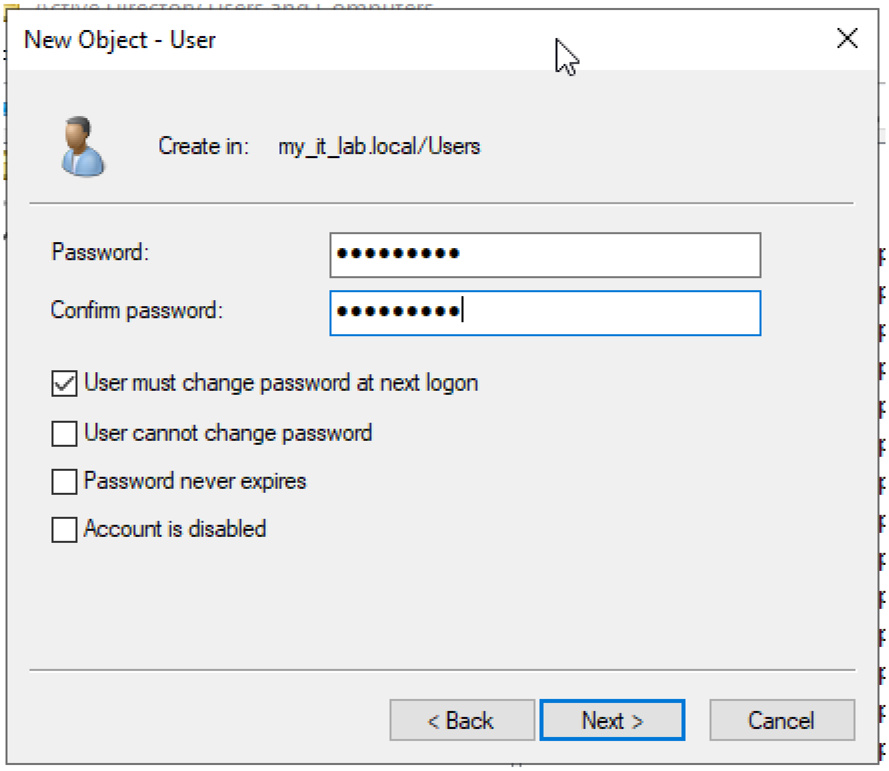
Initials:

Last name:

Full name: work_admin

User logon name: work_admin @my_it_lab.local

User logon name (pre-Windows 2000): MY_IT_LAB\ work_admin



New Object - User

Create in: my_it_lab.local/Users

Password: ••••••••••

Confirm password: ••••••••••

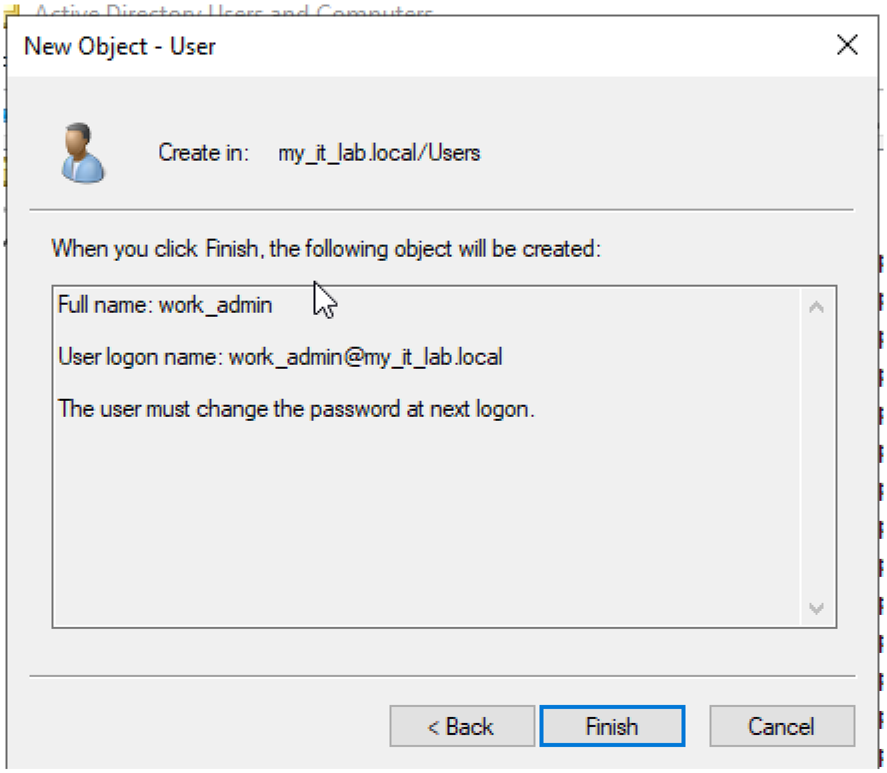
☑ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

Setting a password for the work_admin user ( it will need to be changed upon initial logon).



New Object - User

Create in: my_it_lab.local/Users

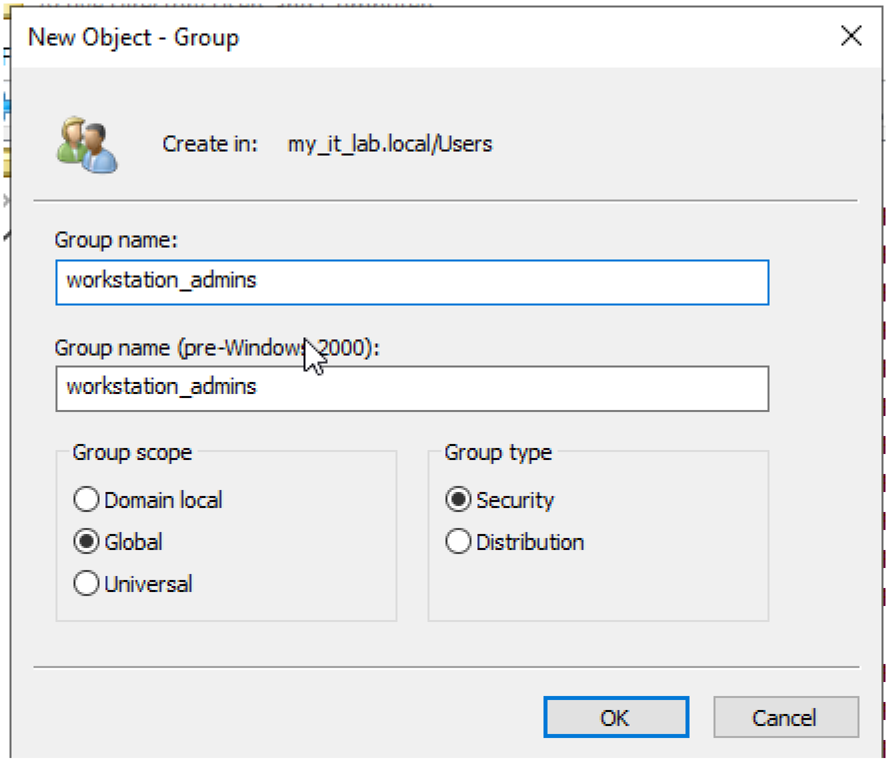
When you click Finish, the following object will be created:

Full name: work_admin

User logon name: work_admin@my_it_lab.local

The user must change the password at next logon.

Creating a new group named workstation_admins.



New Object - Group

Create in: my_it_lab.local/Users

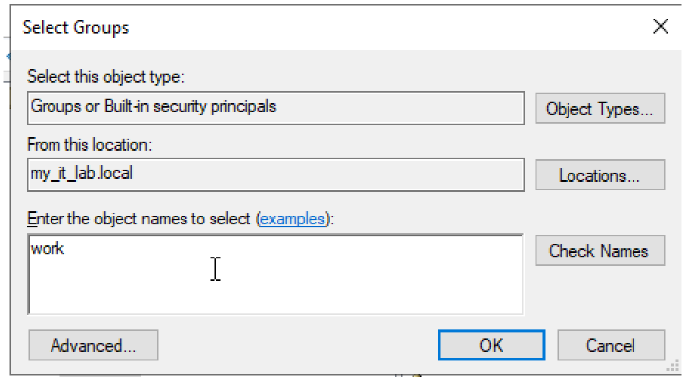
Group name: workstation_admins

Group name (pre-Windows 2000): workstation_admins

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

The group is a global security group. That means that the group is a domain group that can have security permissions set on it.

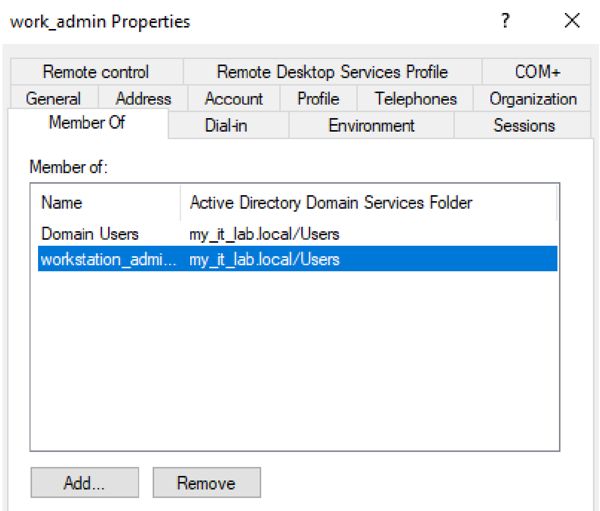


Select this object type:
Groups or Built-in security principals

From this location:
my_it_lab.local

Enter the object names to select (examples):
work

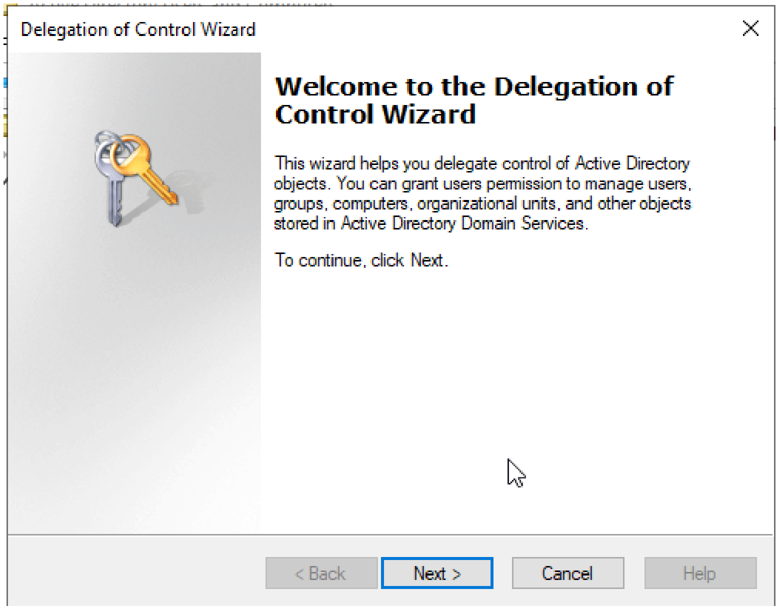
Adding the work_admin user to the group.



Member of:

| Name | Active Directory Domain Services Folder |
|---|---|
| Domain Users | my_it_lab.local/Users |
| workstation_admi... | my_it_lab.local/Users |

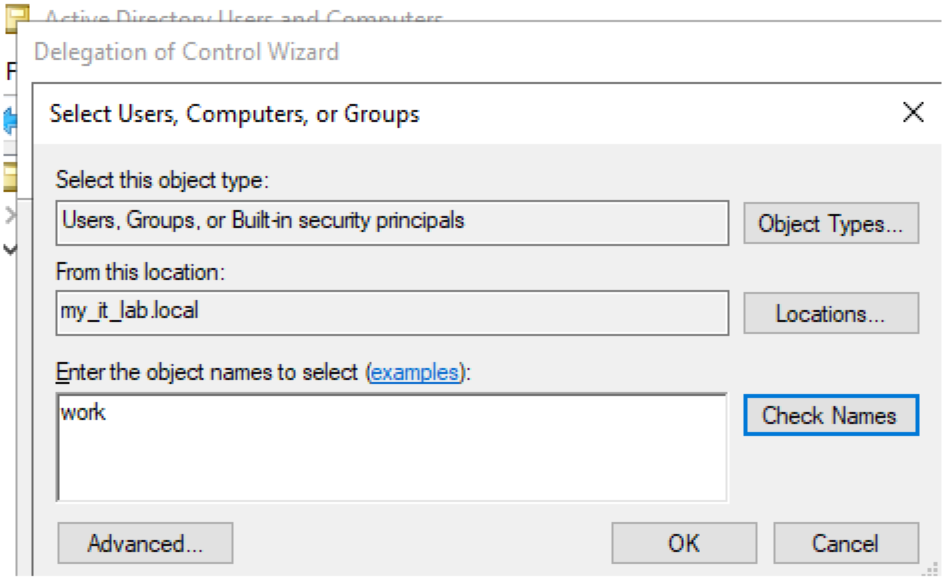
Now I will grant the workstation_admins group delegation control over the Workstations OU.



**Welcome to the Delegation of Control Wizard**

This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.

To continue, click Next.


Active Directory Users and Computers

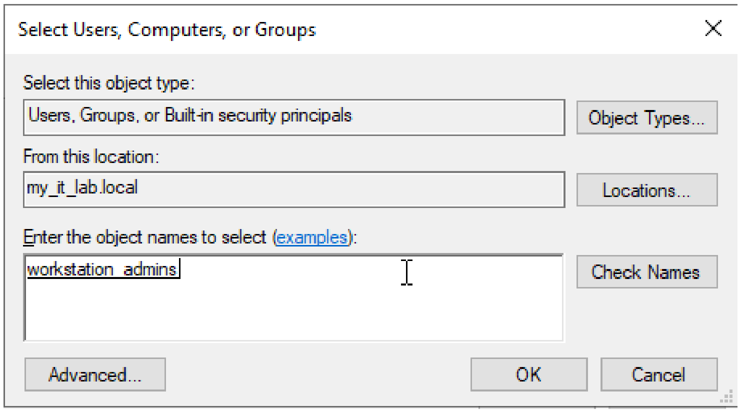
Delegation of Control Wizard

Select Users, Computers, or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
my_it_lab.local

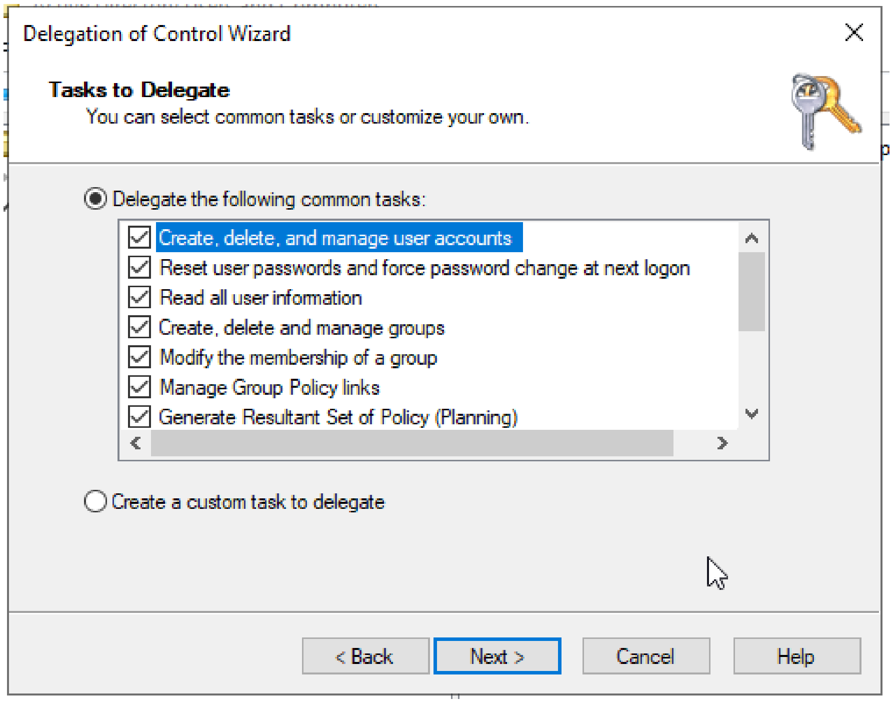
Enter the object names to select (examples):
work


Select Users, Computers, or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
my_it_lab.local

Enter the object names to select (examples):
workstation_admins


Delegation of Control Wizard

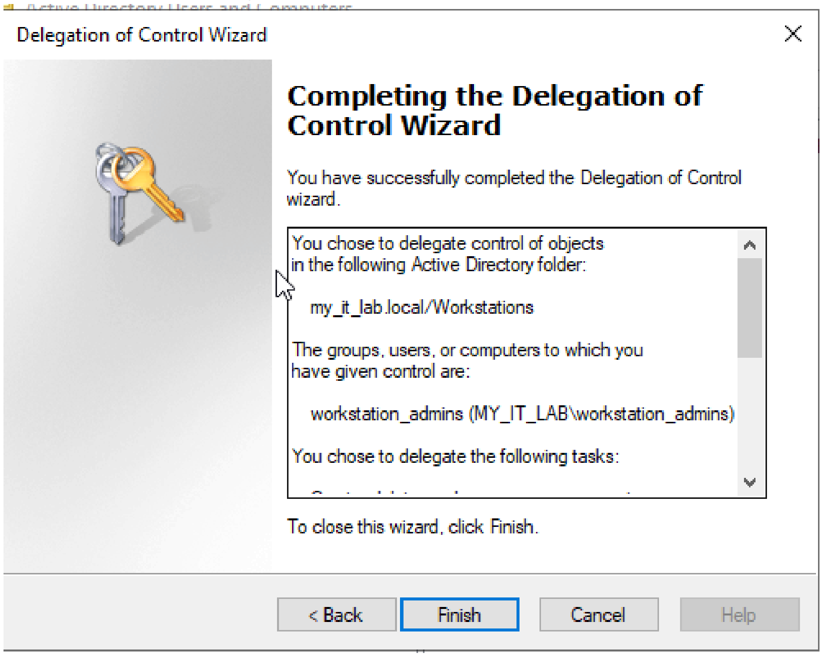
**Tasks to Delegate**
You can select common tasks or customize your own.

● Delegate the following common tasks:

- ☑ Create, delete, and manage user accounts
- ☑ Reset user passwords and force password change at next logon
- ☑ Read all user information
- ☑ Create, delete and manage groups
- ☑ Modify the membership of a group
- ☑ Manage Group Policy links
- ☑ Generate Resultant Set of Policy (Planning)

○ Create a custom task to delegate

Gave the group full permissions for the OU. That means that workstation_admins members have control over AD objects for the OU.



Delegation of Control Wizard

Completing the Delegation of Control Wizard

You have successfully completed the Delegation of Control wizard.

You chose to delegate control of objects in the following Active Directory folder:

my_it_lab.local/Workstations

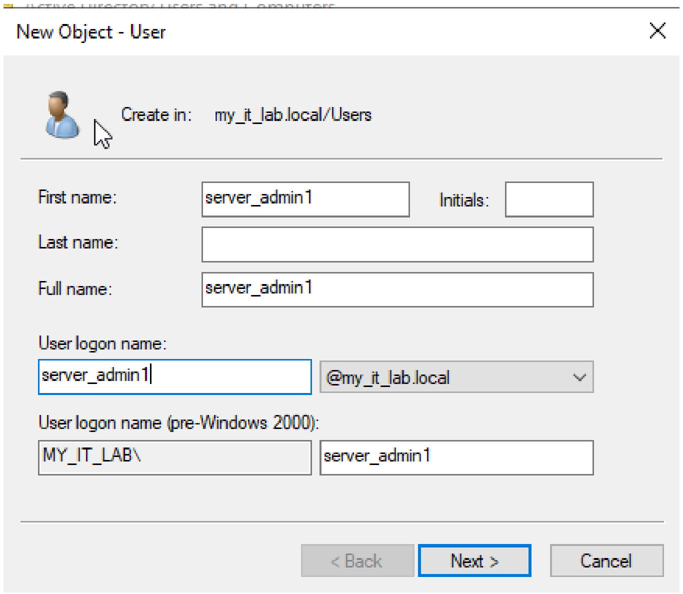
The groups, users, or computers to which you have given control are:

workstation_admins (MY_IT_LAB\workstation_admins)

You chose to delegate the following tasks:

To close this wizard, click Finish.

3.2 Create a server admin account:



New Object - User

Create in: my_it_lab.local/Users

First name: server_admin1

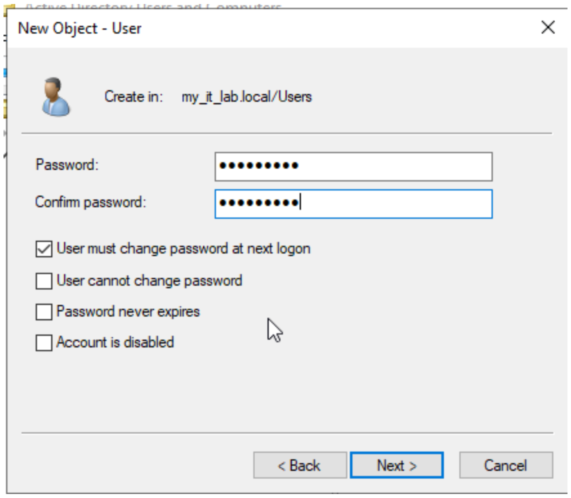
Initials:

Last name:

Full name: server_admin1

User logon name: server_admin1 @my_it_lab.local

User logon name (pre-Windows 2000): MY_IT_LAB\ server_admin1



New Object - User

Create in: my_it_lab.local/Users

Password: •••••••••

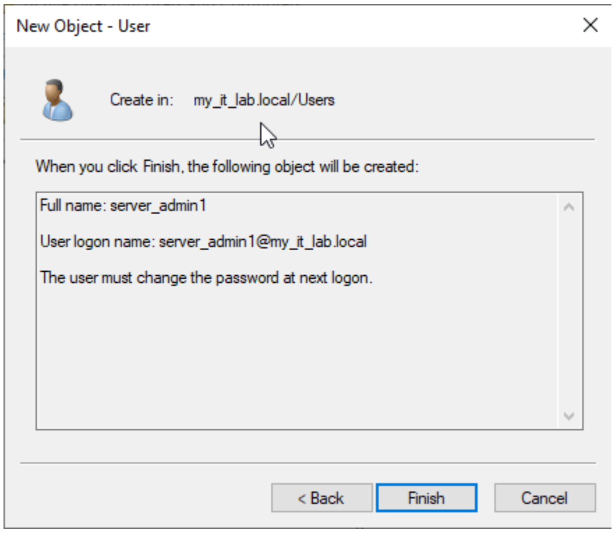
Confirm password: •••••••••

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled



New Object - User

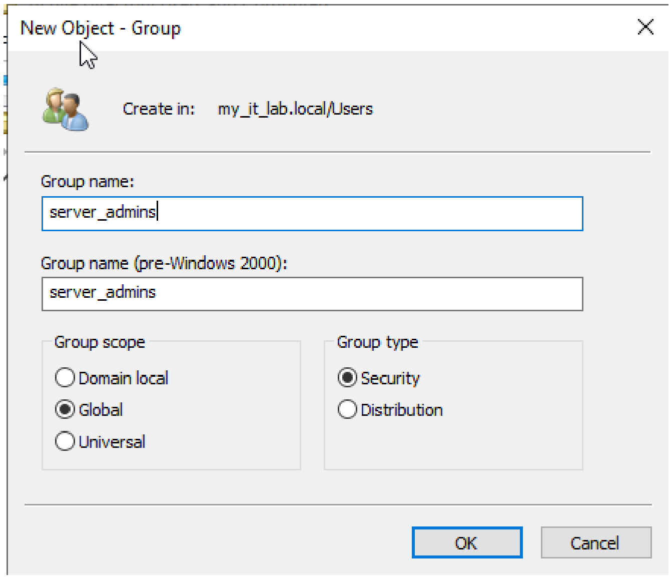
Create in: my_it_lab.local/Users

When you click Finish, the following object will be created:

Full name: server_admin1

User logon name: server_admin1@my_it_lab.local

The user must change the password at next logon.



New Object - Group

Create in: my_it_lab.local/Users

Group name: server_admins

Group name (pre-Windows 2000): server_admins

Group scope

○ Domain local

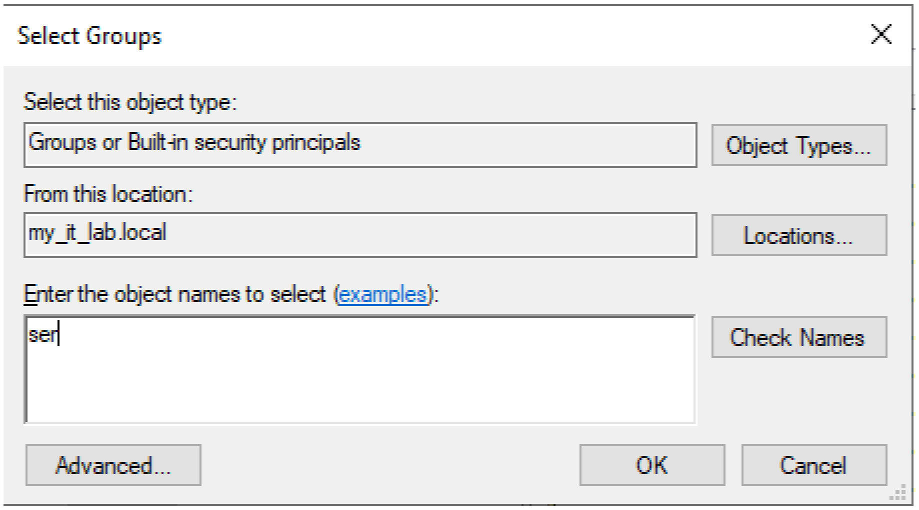
● Global

○ Universal

Group type

● Security

○ Distribution



Select Groups

Select this object type:

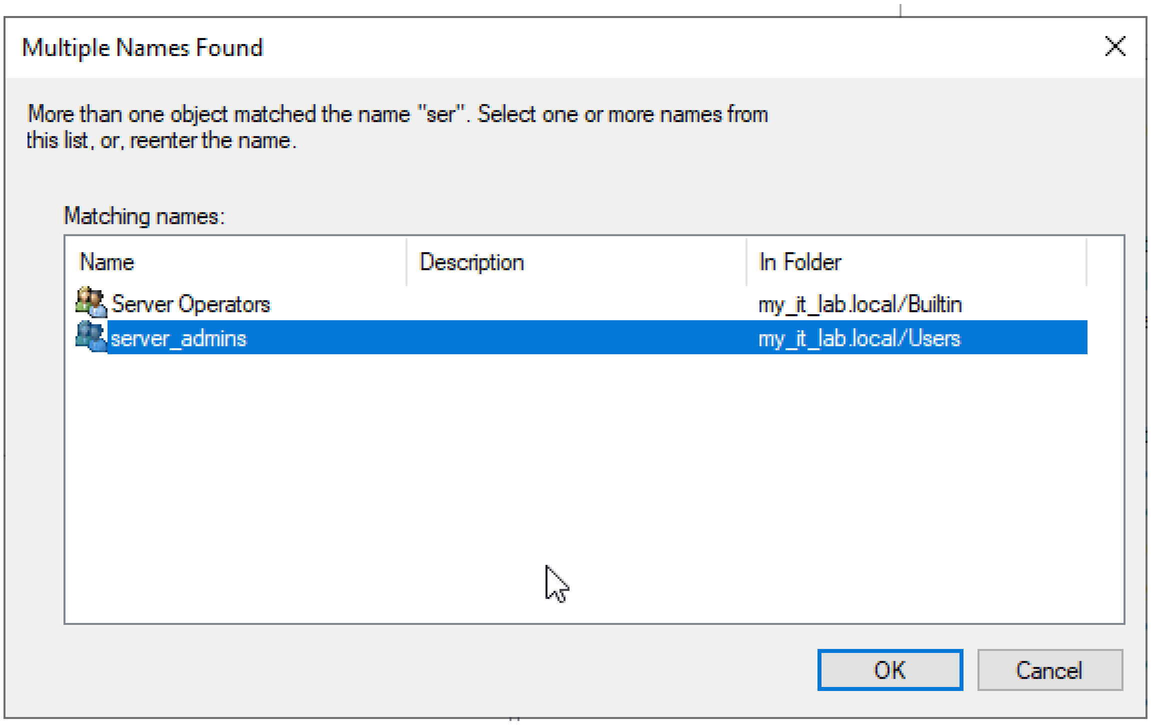
Groups or Built-in security principals

From this location:

my_it_lab.local

Enter the object names to select (examples):

ser

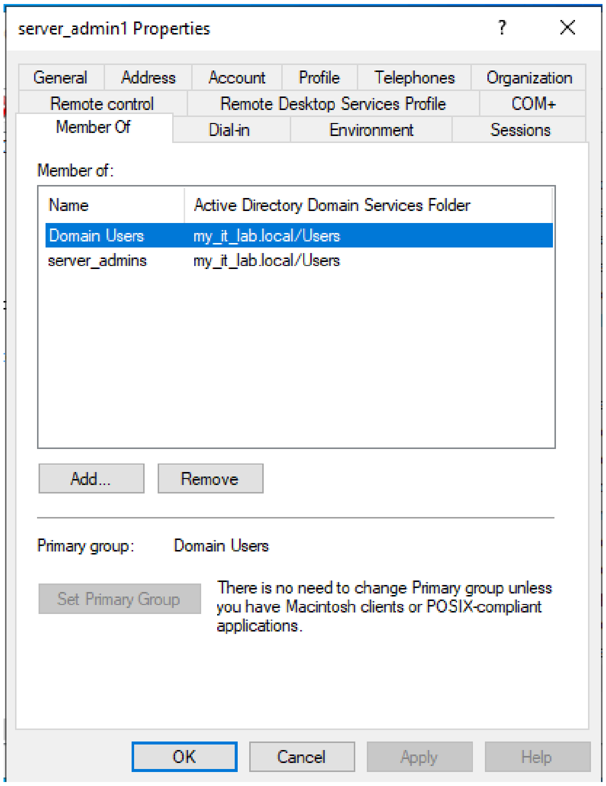


Multiple Names Found

More than one object matched the name "ser". Select one or more names from this list, or, reenter the name.

Matching names:

| Name | Description | In Folder |
|---|---|---|
| Server Operators | | my_it_lab.local/Builtin |
| server_admins | | my_it_lab.local/Users |


server_admin1 Properties

Member of:

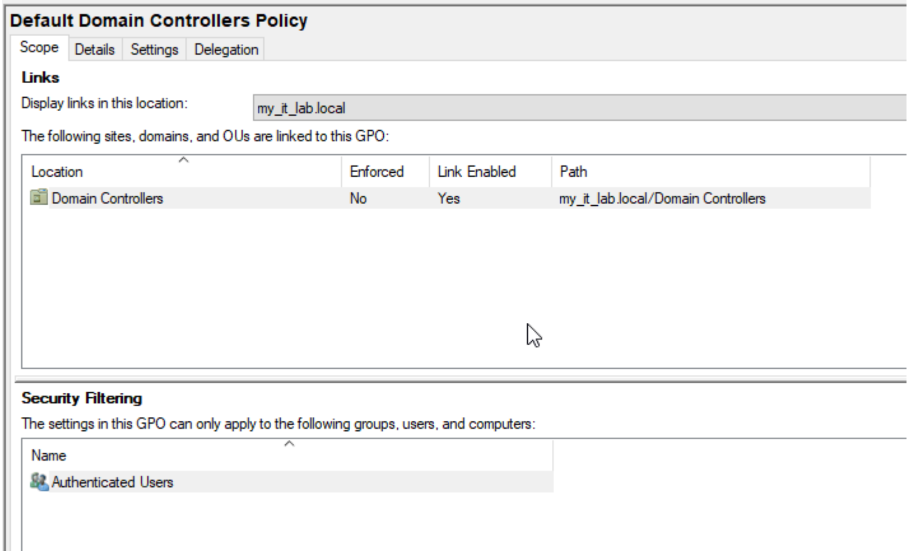
| Name | Active Directory Domain Services Folder |
|---|---|
| Domain Users | my_it_lab.local/Users |
| server_admins | my_it_lab.local/Users |

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

# Section #4 Apply Access Restrictions

4.1 Edit GPO for Domain Controller OU:
Creating a GPO to block logins using workstation_admin or server_admin accounts onto the DC. This setting will be configured on the default domain controller GPO.


Default Domain Controllers Policy

Links

Display links in this location: my_it_lab.local

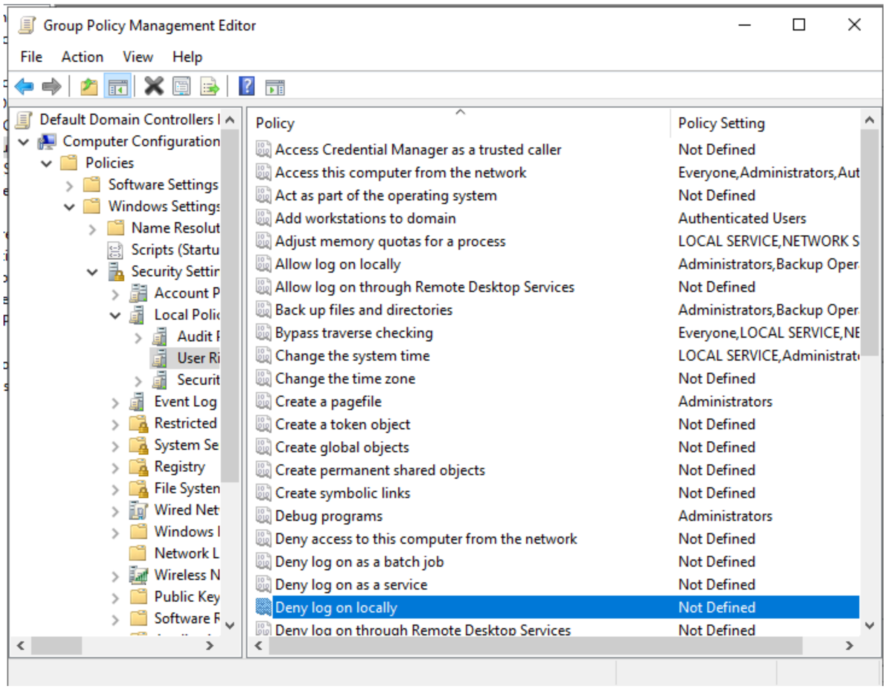
The following sites, domains, and OUs are linked to this GPO:

| Location | Enforced | Link Enabled | Path |
|---|---|---|---|
| Domain Controllers | No | Yes | my_it_lab.local/Domain Controllers |

Security Filtering

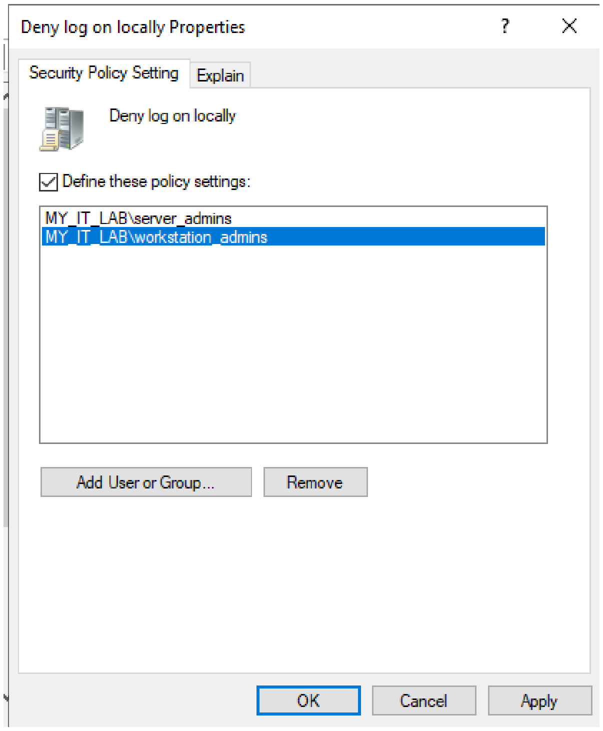
The settings in this GPO can only apply to the following groups, users, and computers:

| Name |
|---|
| Authenticated Users |



| Policy | Policy Setting |
|---|---|
| Access Credential Manager as a trusted caller | Not Defined |
| Access this computer from the network | Everyone,Administrators,Aut |
| Act as part of the operating system | Not Defined |
| Add workstations to domain | Authenticated Users |
| Adjust memory quotas for a process | LOCAL SERVICE,NETWORK S |
| Allow log on locally | Administrators,Backup Oper |
| Allow log on through Remote Desktop Services | Not Defined |
| Back up files and directories | Administrators,Backup Oper |
| Bypass traverse checking | Everyone,LOCAL SERVICE,NE |
| Change the system time | LOCAL SERVICE,Administrat |
| Change the time zone | Not Defined |
| Create a pagefile | Administrators |
| Create a token object | Not Defined |
| Create global objects | Not Defined |
| Create permanent shared objects | Not Defined |
| Create symbolic links | Not Defined |
| Debug programs | Administrators |
| Deny access to this computer from the network | Not Defined |
| Deny log on as a batch job | Not Defined |
| Deny log on as a service | Not Defined |
| Deny log on locally | Not Defined |
| Deny log on through Remote Desktop Services | Not Defined |

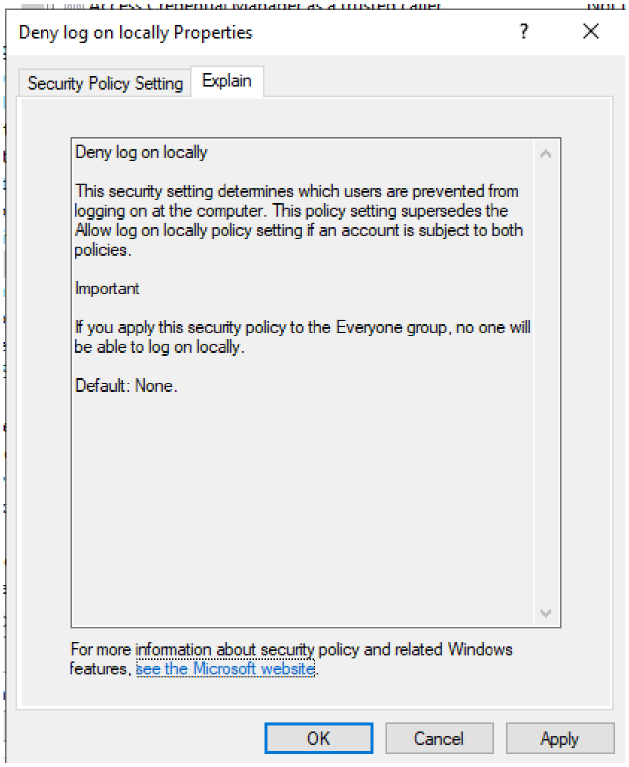
The specific GPO setting is Computer Configuration/ Policies/ Windows Settings/ Security Settings/ User Rights / Deny Log on locally.



Deny log on locally

☑ Define these policy settings:

MY_IT_LAB\server_admins
MY_IT_LAB\workstation_admins



Deny log on locally

This security setting determines which users are prevented from logging on at the computer. This policy setting supersedes the Allow log on locally policy setting if an account is subject to both policies.

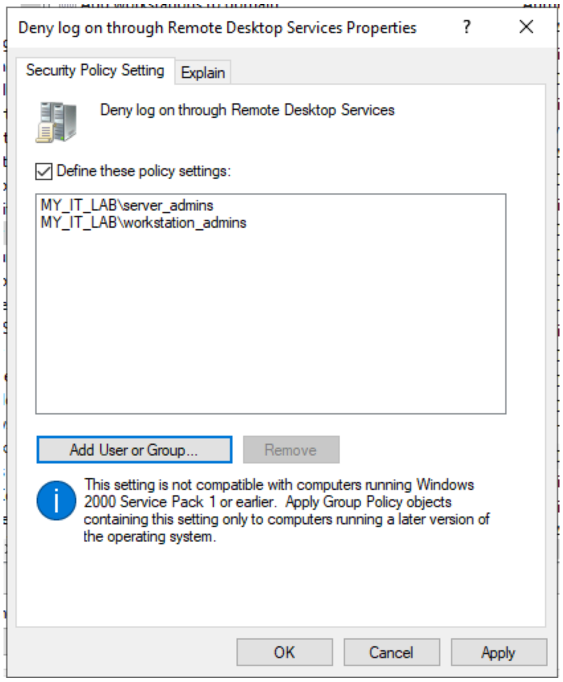
Important

If you apply this security policy to the Everyone group, no one will be able to log on locally.

Default: None.

For more information about security policy and related Windows features, see the Microsoft website.

I added the proper groups to be blocked for this setting.



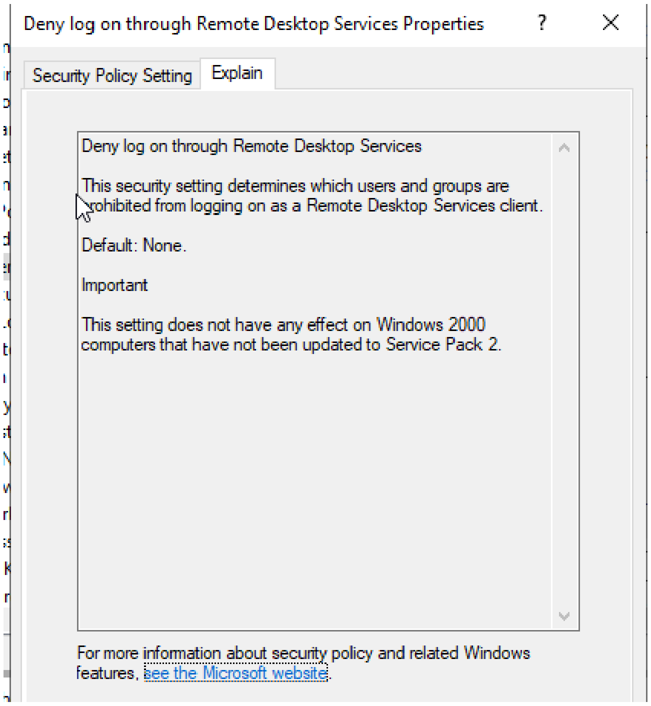
Deny log on through Remote Desktop Services Properties

Deny log on through Remote Desktop Services

☑ Define these policy settings:

MY_IT_LAB\server_admins
MY_IT_LAB\workstation_admins

This setting is not compatible with computers running Windows 2000 Service Pack 1 or earlier. Apply Group Policy objects containing this setting only to computers running a later version of the operating system.



Deny log on through Remote Desktop Services Properties

Deny log on through Remote Desktop Services

This security setting determines which users and groups are prohibited from logging on as a Remote Desktop Services client.

Default: None.

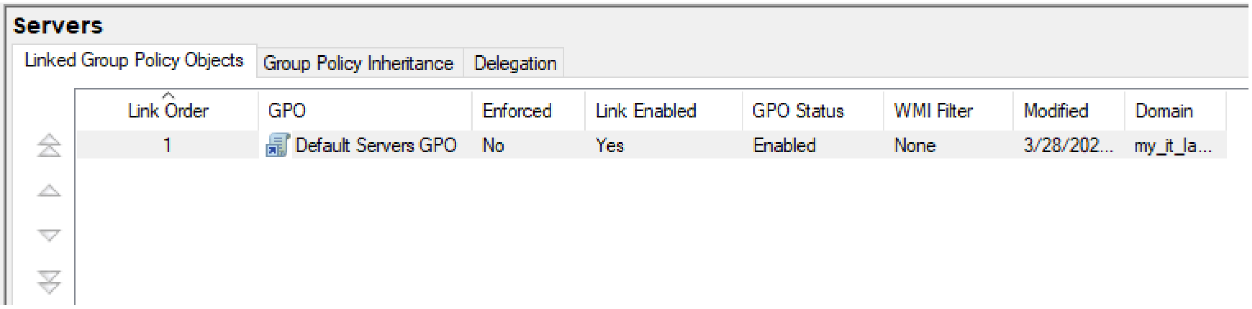
Important

This setting does not have any effect on Windows 2000 computers that have not been updated to Service Pack 2.

For more information about security policy and related Windows features, see the Microsoft website.

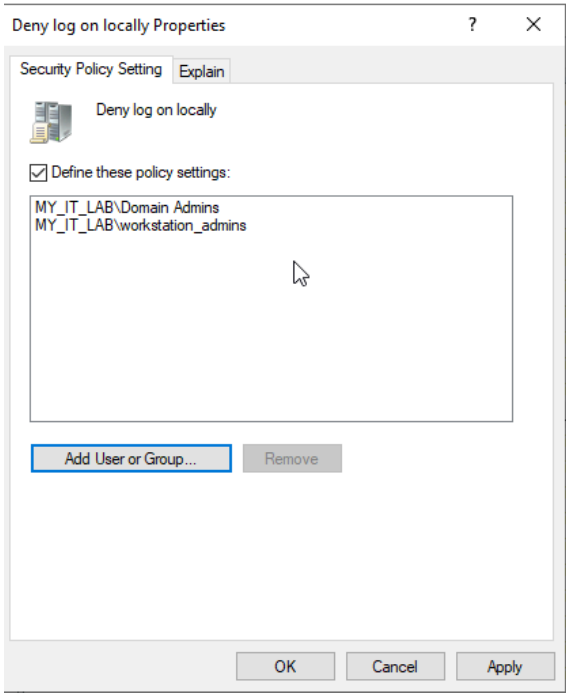
Additionally, I also blocked remote logons for these groups.

4.2 Create GPO for Servers OU and configure it:
I created a new GPO for the Servers OU called Default Servers GPO.



Servers

| Link Order | GPO | Enforced | Link Enabled | GPO Status | WMI Filter | Modified | Domain |
|---|---|---|---|---|---|---|---|
| 1 | Default Servers GPO | No | Yes | Enabled | None | 3/28/202... | my_it_la... |



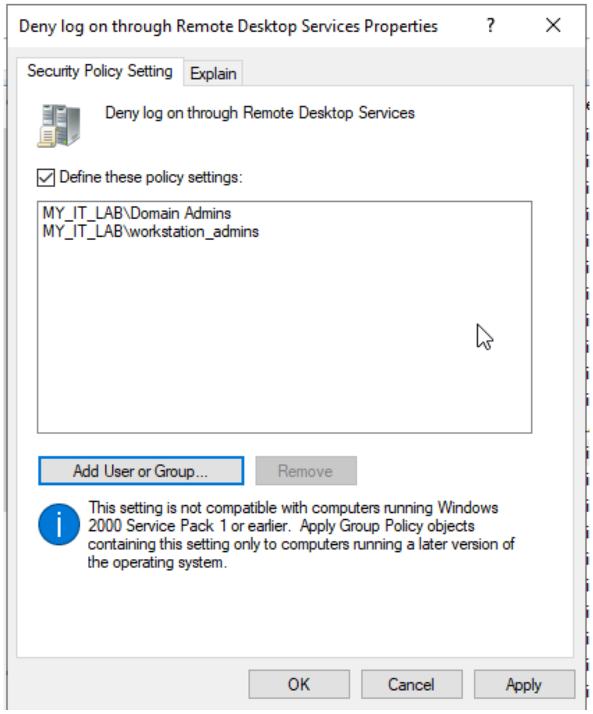
Deny log on locally Properties

Security Policy Setting | Explain

Deny log on locally

☑ Define these policy settings:

MY_IT_LAB\Domain Admins
MY_IT_LAB\workstation_admins



Deny log on through Remote Desktop Services Properties

Security Policy Setting | Explain

Deny log on through Remote Desktop Services

☑ Define these policy settings:

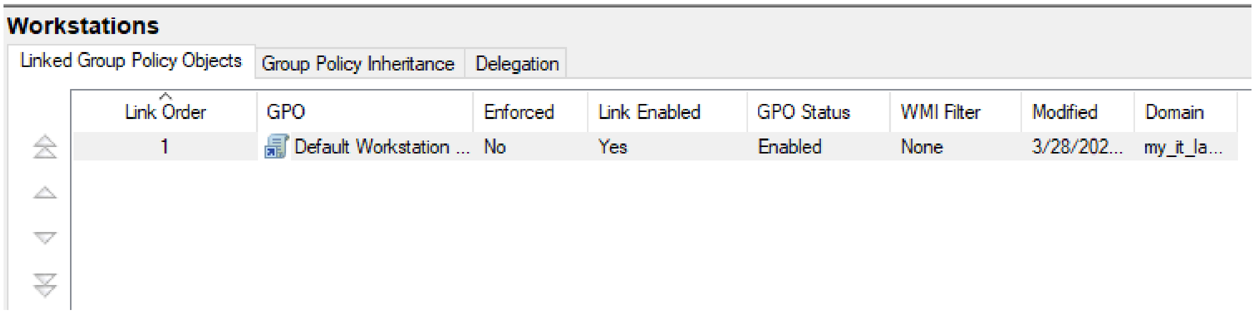
MY_IT_LAB\Domain Admins
MY_IT_LAB\workstation_admins

This setting is not compatible with computers running Windows 2000 Service Pack 1 or earlier. Apply Group Policy objects containing this setting only to computers running a later version of the operating system.

Again, I configured “Deny log on locally” and remotely to block the proper groups. In this case, I am blocking Domain_Admins and workstation_admins from logging onto servers.

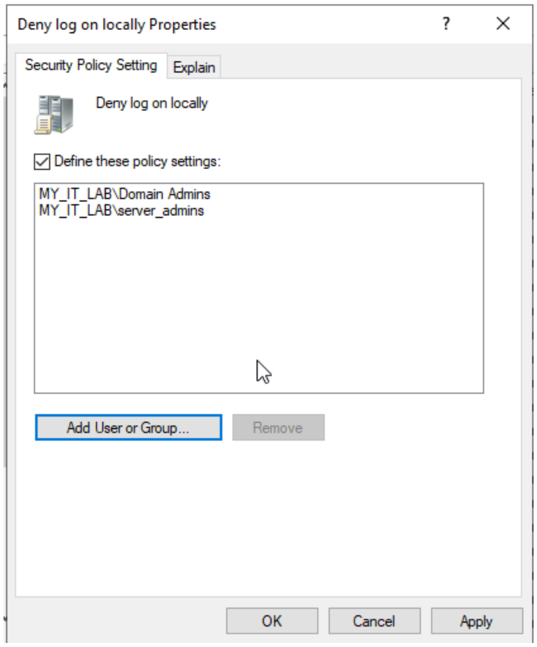
## 4.3 Create a workstation GPO and configure it

I created a GPO for the Workstations OU named Default Workstation GPO



**Workstations**

| Link Order | GPO | Enforced | Link Enabled | GPO Status | WMI Filter | Modified | Domain |
|---|---|---|---|---|---|---|---|
| 1 | Default Workstation ... | No | Yes | Enabled | None | 3/28/202... | my_it_la... |

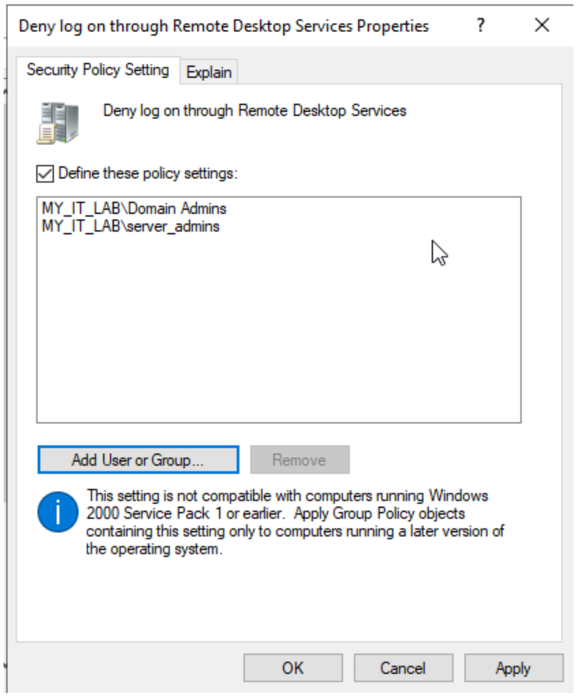


Deny log on locally Properties

Deny log on locally

☑ Define these policy settings:

MY_IT_LAB\Domain Admins
MY_IT_LAB\server_admins



Deny log on through Remote Desktop Services Properties

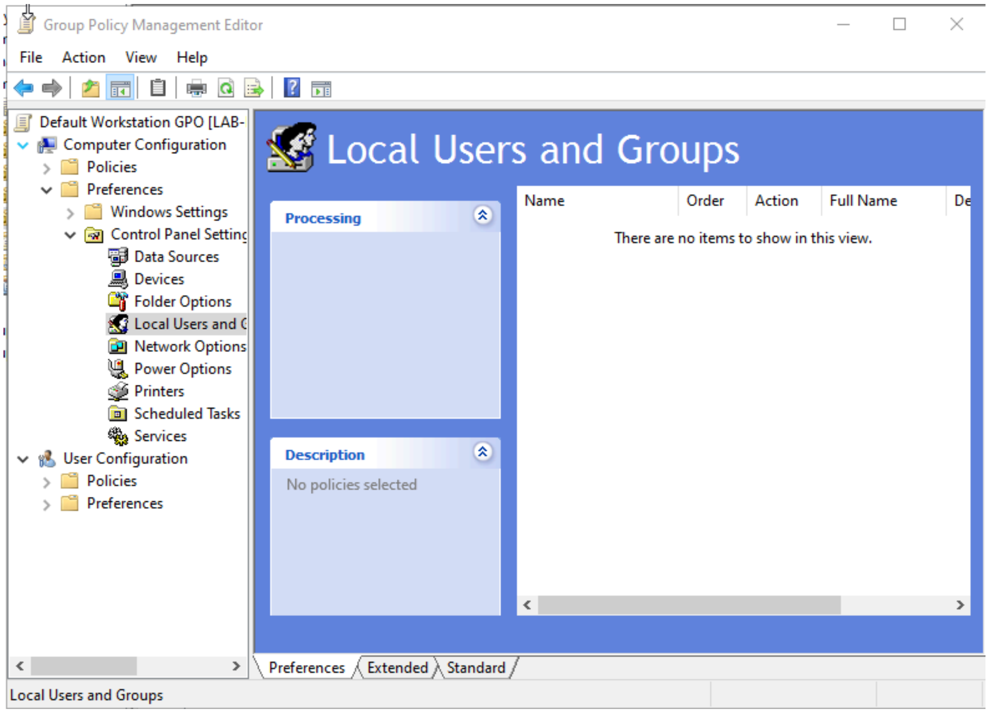
Deny log on through Remote Desktop Services

☑ Define these policy settings:

MY_IT_LAB\Domain Admins
MY_IT_LAB\server_admins

This setting is not compatible with computers running Windows 2000 Service Pack 1 or earlier. Apply Group Policy objects containing this setting only to computers running a later version of the operating system.

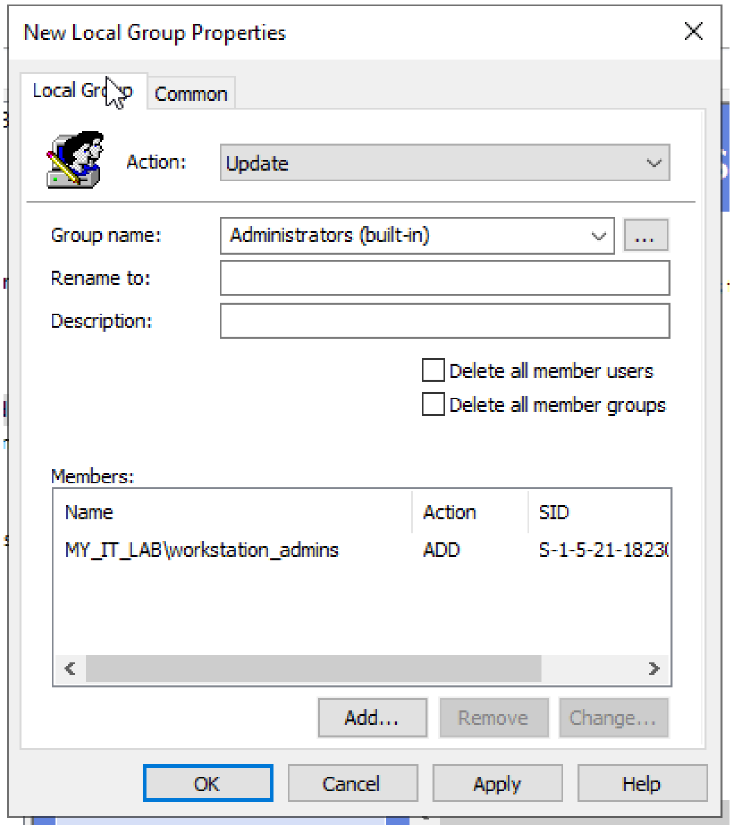
I blocked server_admins and Domain_admins from logging into workstations remotely and in person.



There are no items to show in this view.

No policies selected

One additional GPO I need to configure is granting the workstation_admins local admin rights on workstations. This setting can be configured under the  Computer Configuration/ Preferences/ Windows Settings/ Local Users and Groups.



Action: Update

Group name: Administrators (built-in)

Rename to:

Description:

□ Delete all member users

□ Delete all member groups

Members:

| Name | Action | SID |
|---|---|---|
| MY_IT_LAB\workstation_admins | ADD | S-1-5-21-1823( |

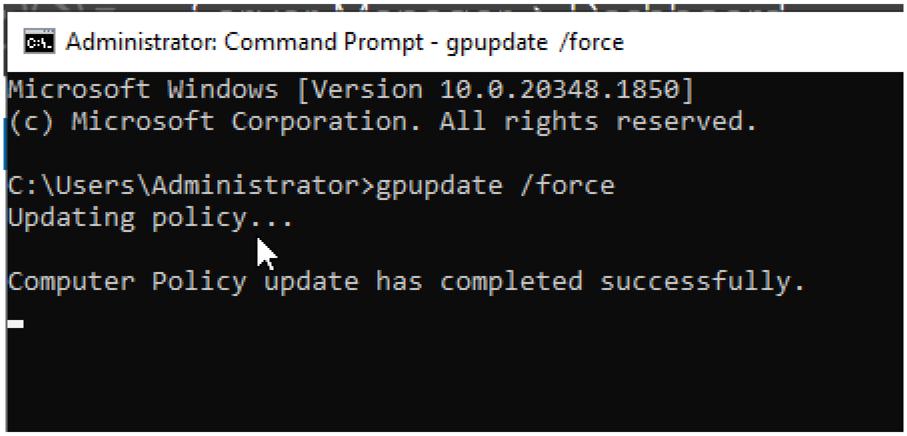
Now the workstation_admins group has local admin privileges on workstations.

If I had an extra server for this lab I would have to do the same thing for the server_admins group. OU delegations are different from having local admin privileges. They only grant control over an OU's AD objects while local admin privileges will allow accounts to perform admin tasks.

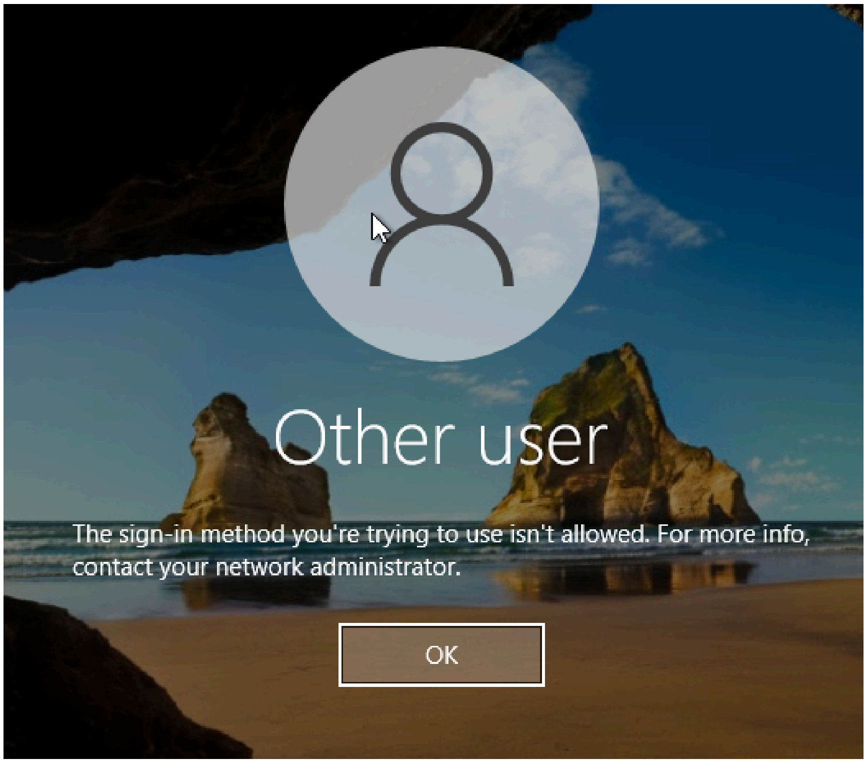
# Section #5 Test and Validate Tiered Access

5.1 Try logging into Domain Controller using server admin/ workstation admin account:

I will try to sign into the domain controller using the server_admin1 and work_admin accounts.

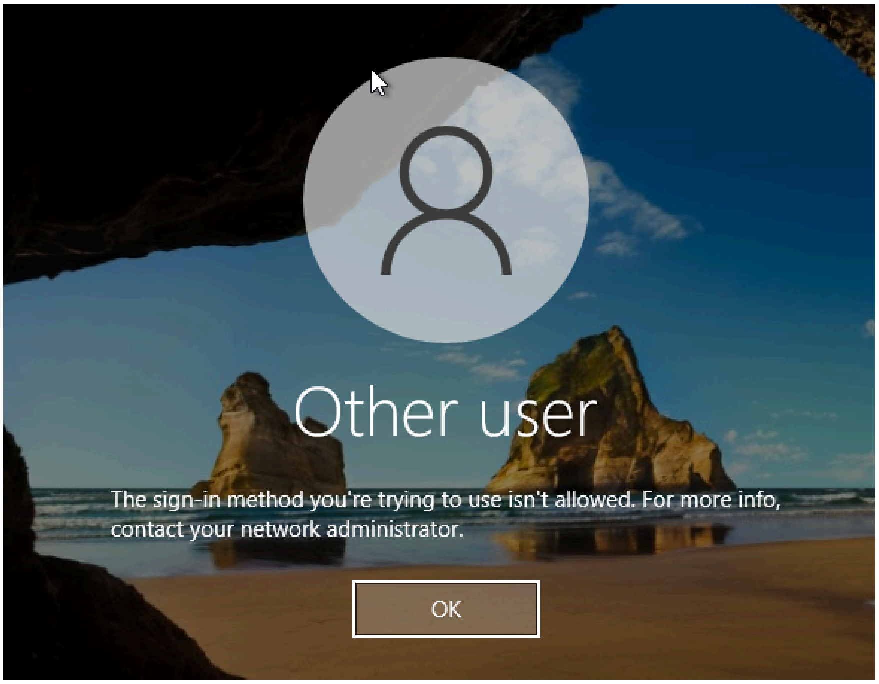


```
Microsoft Windows [Version 10.0.20348.1850]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
```



The sign-in method you're trying to use isn't allowed. For more info, contact your network administrator.

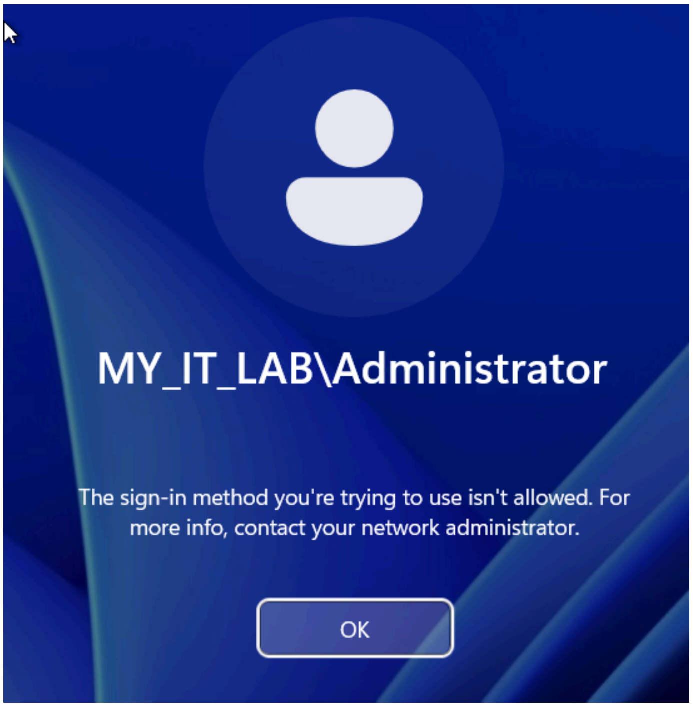
Work_admin was blocked!


Other user

The sign-in method you're trying to use isn't allowed. For more info, contact your network administrator.

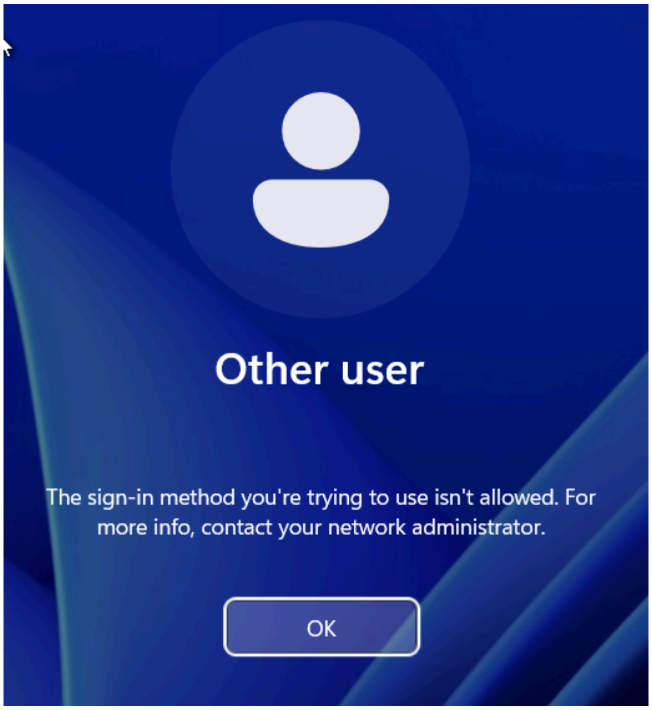
Server_admin1 was blocked as well!

5.1 Try logging into the LAB-PC workstation with the domain admin account and the server admin account:


MY_IT_LAB\Administrator

The sign-in method you're trying to use isn't allowed. For more info, contact your network administrator.

The domain administrator is blocked!

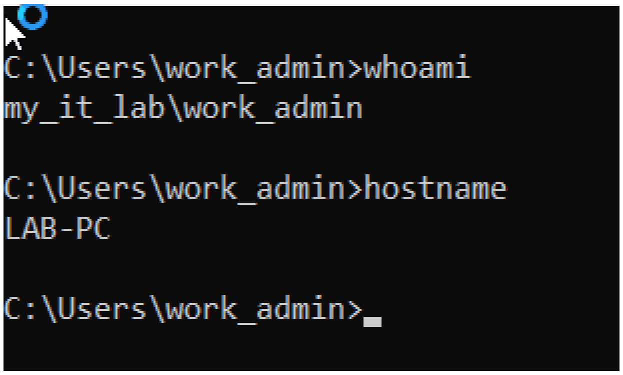


Other user

The sign-in method you're trying to use isn't allowed. For more info, contact your network administrator.

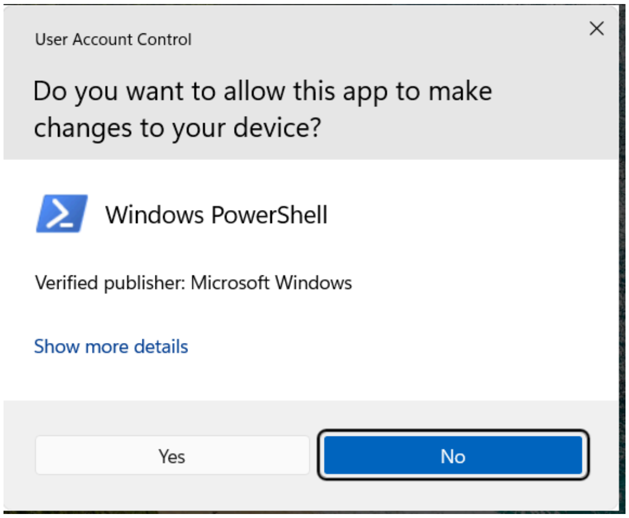
Server-admin1 was blocked as well.

Now I will test to make sure workstation_admin members can perform administrative tasks on workstations



```
C:\Users\work_admin>whoami
my_it_lab\work_admin

C:\Users\work_admin>hostname
LAB-PC

C:\Users\work_admin>
```

I am logged into the LAB-PC workstation as work-admin.



User Account Control

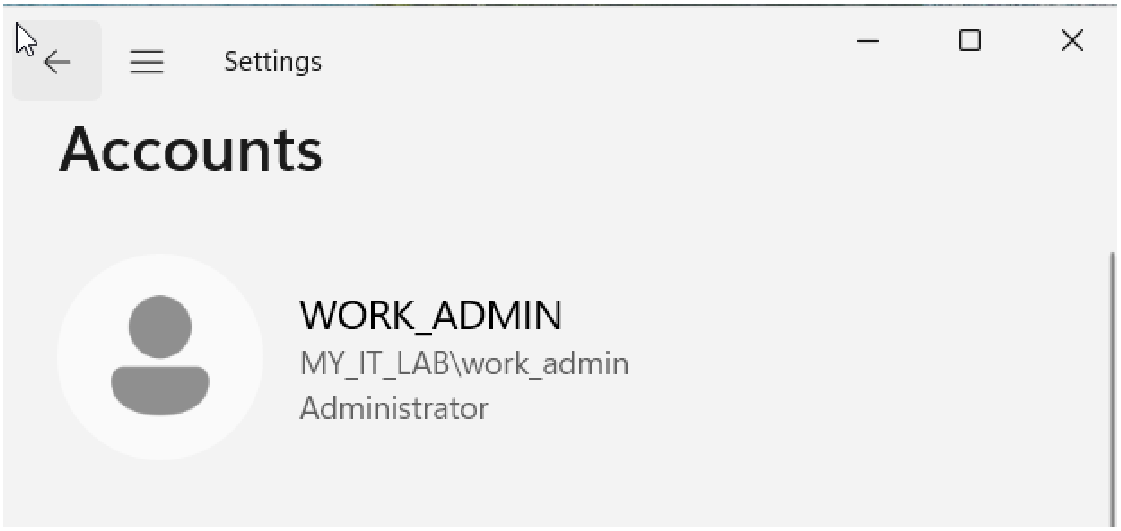
Do you want to allow this app to make changes to your device?

Windows PowerShell

Verified publisher: Microsoft Windows

Show more details

UAC worked.



Accounts

WORK_ADMIN
MY_IT_LAB\work_admin
Administrator

Also checking the info for my work_admin you can see work_admin has administrator privileges on the workstation.