Active Directory

[Windows Domain: 2](#_Toc197013484)

[A Real-World Example: 2](#_Toc197013485)

[Active Directory 3](#_Toc197013486)

[Users 3](#_Toc197013487)

[Machines 3](#_Toc197013488)

[Security Groups 3](#_Toc197013489)

[Active Directory Users and Computers 3](#_Toc197013490)

[Security Groups vs Ous 4](#_Toc197013491)

[Managing Users in AD 5](#_Toc197013492)

[Deleting extra OUs and users 5](#_Toc197013493)

[Delegation 7](#_Toc197013494)

[Managing Computers in AD 10](#_Toc197013495)

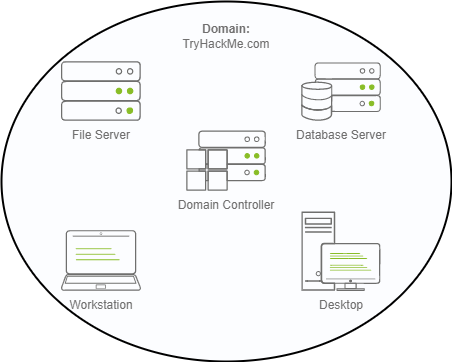
[Workstations 10](#_Toc197013496)

[Servers 11](#_Toc197013497)

[Domain Controllers 11](#_Toc197013498)

[Group Policies 13](#_Toc197013499)

# Windows Domain:



The main advantages of having a configured Windows domain are:

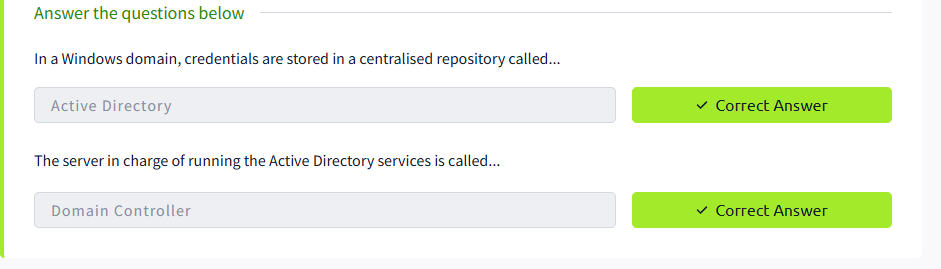
* **Centralised identity management:** All users across the network can be configured from Active Directory with minimum effort.
* **Managing security policies:** You can configure security policies directly from Active Directory and apply them to users and computers across the network as needed.

## A Real-World Example:

If this sounds a bit confusing, chances are that you have already interacted with a Windows domain at some point in your school, university or work.

In school/university networks, you will often be provided with a username and password that you can use on any of the computers available on campus. Your credentials are valid for all machines because whenever you input them on a machine, it will forward the authentication process back to the Active Directory, where your credentials will be checked. Thanks to Active Directory, your credentials don't need to exist in each machine and are available throughout the network.

Active Directory is also the component that allows your school/university to restrict you from accessing the control panel on your school/university machines. Policies will usually be deployed throughout the network so that you don't have administrative privileges over those computers.



# Active Directory

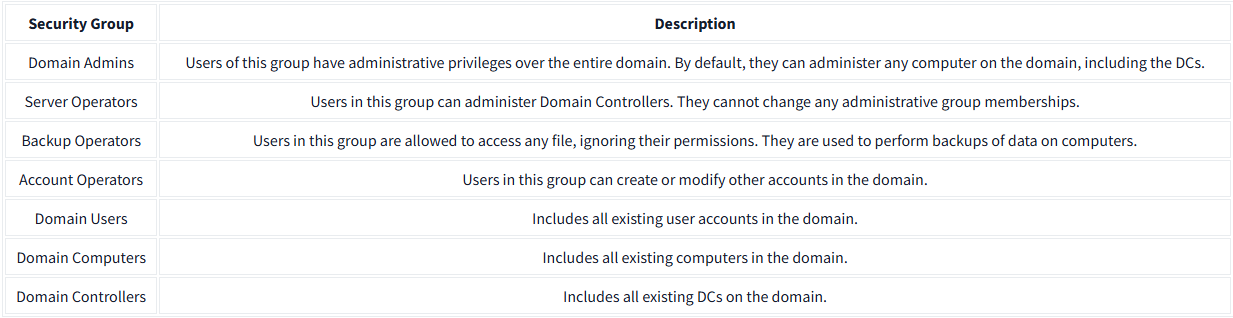
The core of any Windows Domain is the **Active Directory Domain Service (AD DS)**. This service acts as a catalogue that holds the information of all of the "objects" that exist on your network. Amongst the many objects supported by AD, we have users, groups, machines, printers, shares and many others. Let's look at some of them:

Users: Users are one of the most common object types in Active Directory. Users are one of the objects known as **security principals**, meaning that they can be authenticated by the domain and can be assigned privileges over **resources** like files or printers.

Machines**:** Machines are another type of object within Active Directory; for every computer that joins the Active Directory domain, a machine object will be created. Machines are also considered "security principles" and are assigned an account just as any regular user. This account has somewhat limited rights within the domain itself. The machine accounts themselves are local administrators on the assigned computer, they are generally not supposed to be accessed by anyone except the computer itself, but as with any other account, if you have the password, you can use it to log in.

Security Groups: If you are familiar with Windows, you probably know that you can define user groups to assign access rights to files or other resources to entire groups instead of single users. This allows for better manageability as you can add users to an existing group, and they will automatically inherit all of the group's privileges. Security groups are also considered security principals and, therefore, can have privileges over resources on the network.

Groups can have both users and machines as members. If needed, groups can include other groups as well.



## Active Directory Users and Computers

To configure users, groups or machines in Active Directory, we need to log in to the Domain Controller and run "Active Directory Users and Computers" from the start menu:

A screenshot of a computer

AI-generated content may be incorrect.

This will open up a window where you can see the hierarchy of users, computers and groups that exist in the domain. These objects are organised in **Organizational Units (OUs)** which are container objects that allow you to classify users and machines. OUs are mainly used to define sets of users with similar policing requirements

Checking our machine, we can see that there is already an OU called THM with four child OUs for the IT, Management, Marketing and Sales departments. It is very typical to see the OUs mimic the business' structure, as it allows for efficiently deploying baseline policies that apply to entire departments. Remember that while this would be the expected model most of the time, you can define OUs arbitrarily.

A screenshot of a computer

AI-generated content may be incorrect.

You probably noticed already that there are other default containers apart from the THM OU. These containers are created by Windows automatically and contain the following:

**Builtin:** Contains default groups available to any Windows host.

**Computers:** Any machine joining the network will be put here by default. You can move them if needed.

**Domain Controllers:** Default OU that contains the DCs in your network.

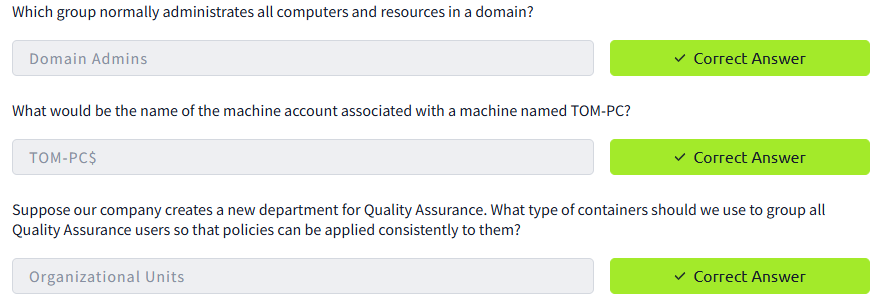
**Users:** Default users and groups that apply to a domain-wide context.

**Managed Service Accounts:** Holds accounts used by services in your Windows domain.

## Security Groups vs Ous

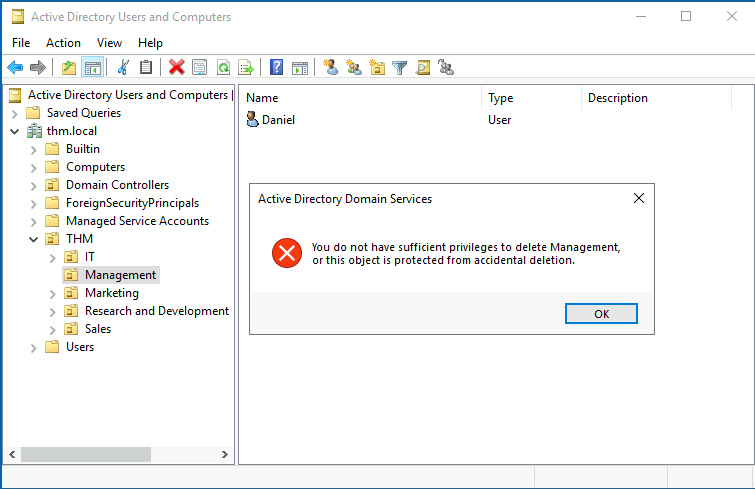
**OUs** are handy for **applying policies** to users and computers, which include specific configurations that pertain to sets of users depending on their particular role in the enterprise. Remember, a user can only be a member of a single OU at a time, as it wouldn't make sense to try to apply two different sets of policies to a single user.

**Security Groups**, on the other hand, are used to **grant permissions over resources**. For example, you will use groups if you want to allow some users to access a shared folder or network printer. A user can be a part of many groups, which is needed to grant access to multiple resources.

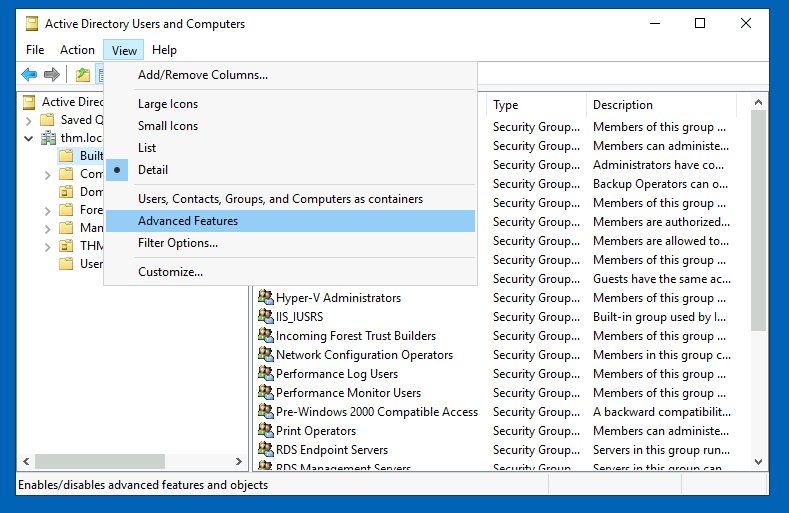


# Managing Users in AD

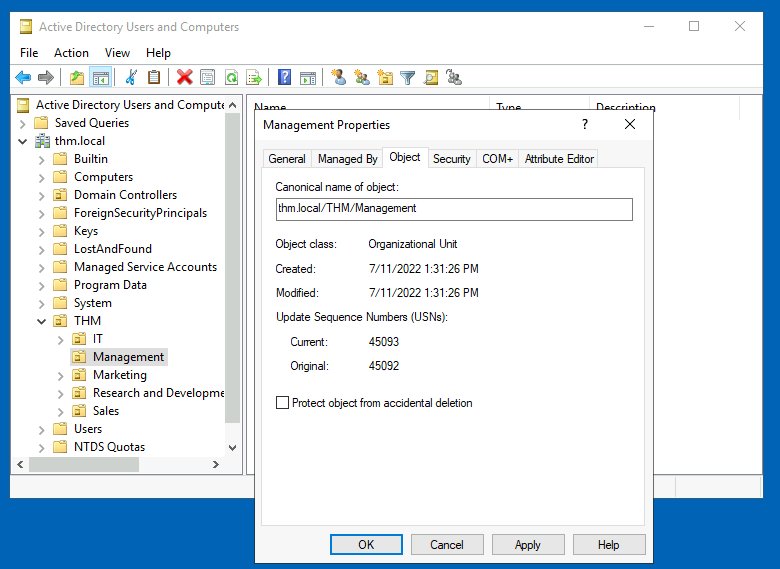
## Deleting extra OUs and users



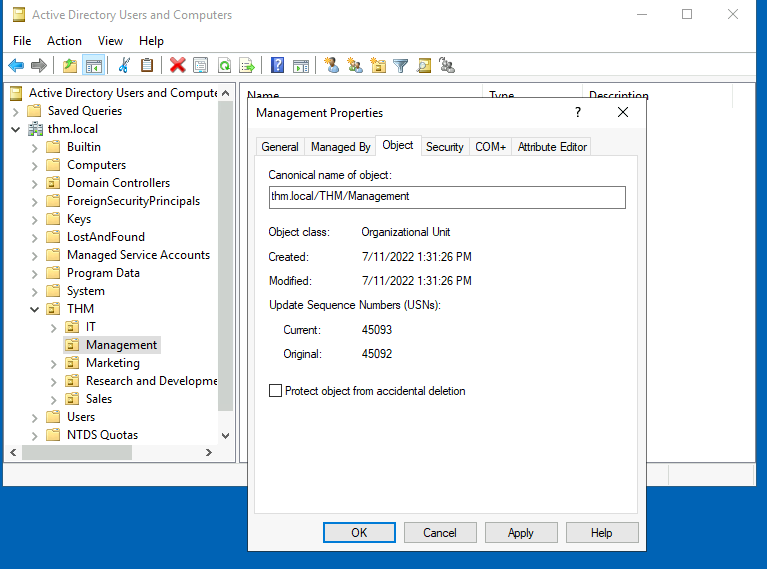
By default, OUs are protected against accidental deletion. To delete the OU, we need to enable the **Advanced Features** in the View menu:

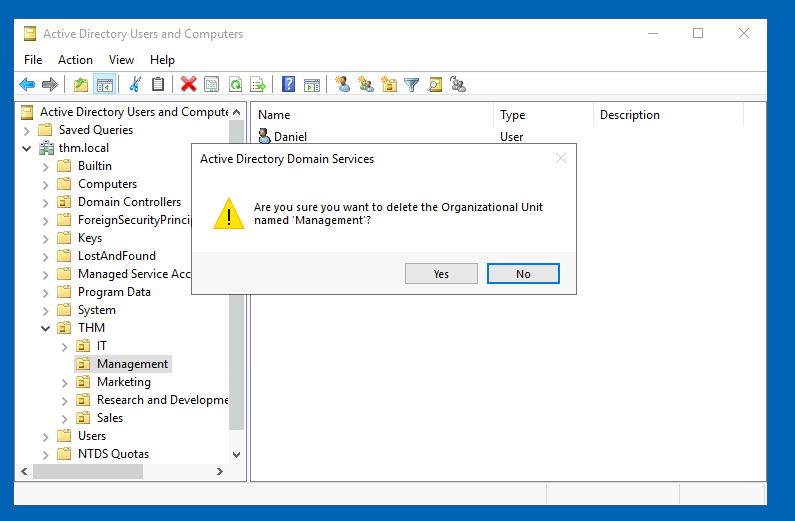


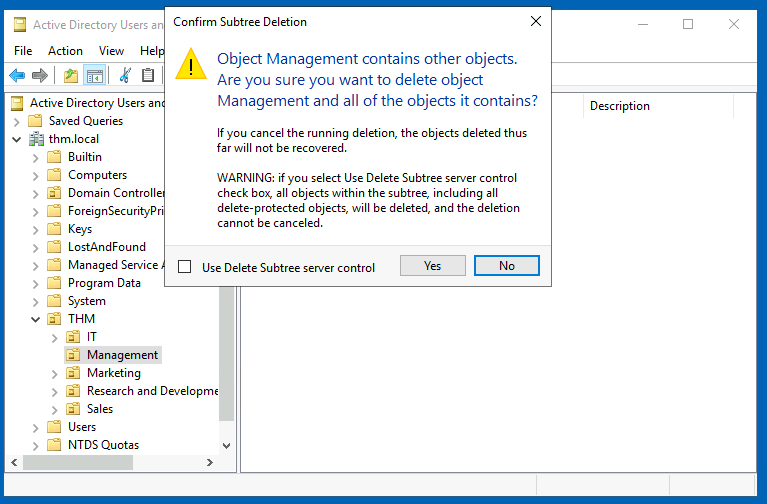
This will show you some additional containers and enable you to disable the accidental deletion protection. To do so, right-click the OU and go to Properties. You will find a checkbox in the Object tab to disable the protection:



Be sure to uncheck the box and try deleting the OU again. You will be prompted to confirm that you want to delete the OU, and as a result, any users, groups or OUs under it will also be deleted.







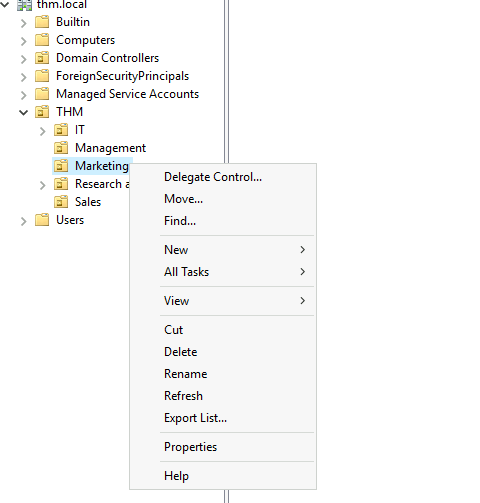
After deleting the extra OU, you should notice that for some of the departments, the users in the AD don't match the ones in our organisational chart. Create and delete users as needed to match them.

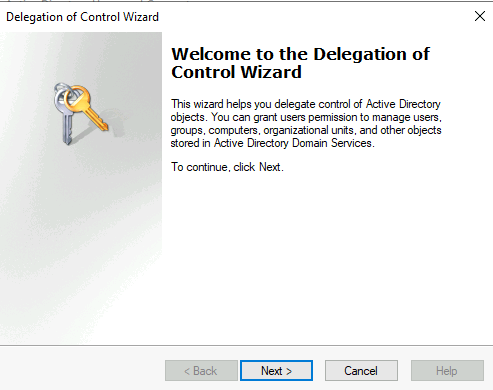
## Delegation

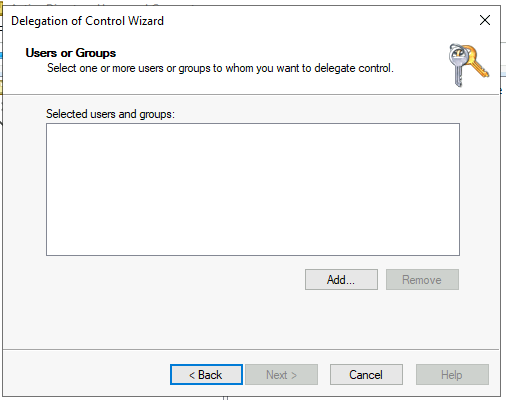
One of the nice things you can do in AD is to give specific users some control over some OUs. This process is known as **delegation** and allows you to grant users specific privileges to perform advanced tasks on OUs without needing a Domain Administrator to step in.

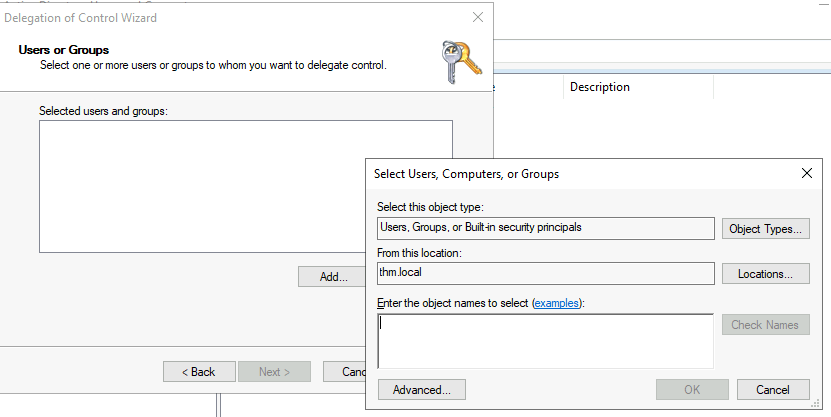
One of the most common use cases for this is granting IT support the privileges to reset other low-privilege users' passwords. According to our organisational chart, Phillip is in charge of IT support, so we'd probably want to delegate control of resetting passwords over the Sales, Marketing and Management OUs to him.

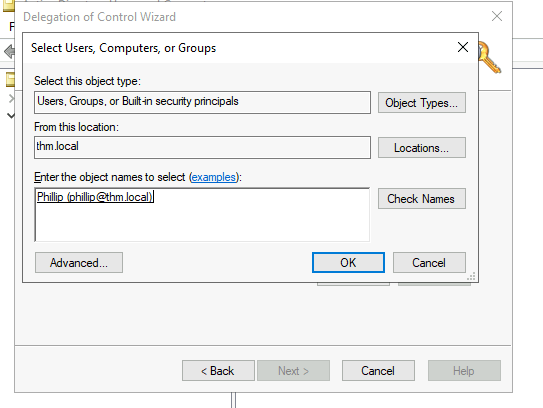
For this example, we will delegate control over the Sales OU to Phillip. To delegate control over an OU, you can right-click it and select **Delegate Control**:



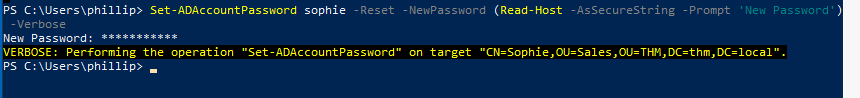






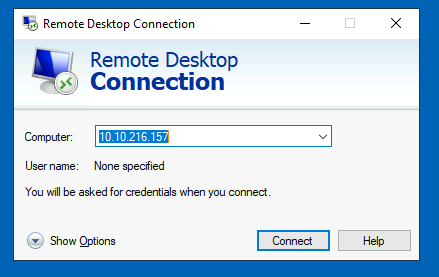


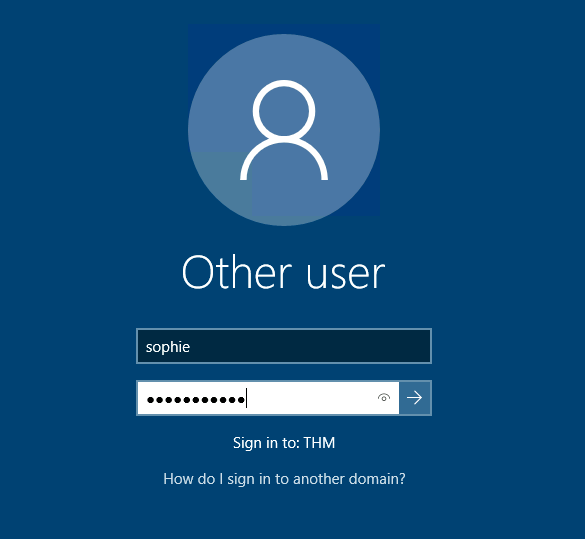
**Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host -AsSecureString -Prompt 'New Password') -Verbose**



Since we wouldn't want Sophie to keep on using a password we know, we can also force a password reset at the next logon with the following command:

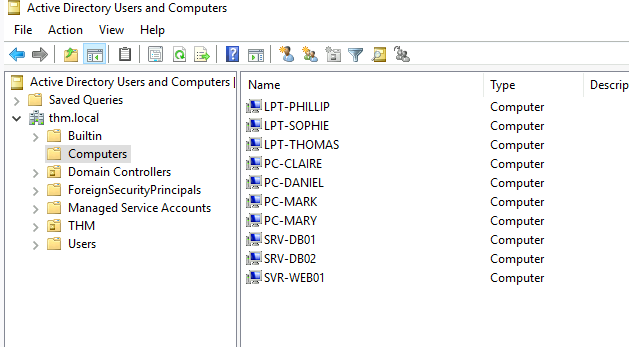
**Set-ADUser -ChangePasswordAtLogon $true -Identity sophie -Verbose**





# Managing Computers in AD

By default, all the machines that join a domain (except for the DCs) will be put in the container called "Computers". If we check our DC, we will see that some devices are already there:



We can see some servers, some laptops and some PCs corresponding to the users in our network. Having all of our devices there is not the best idea since it's very likely that you want different policies for your servers and the machines that regular users use on a daily basis.

## Workstations

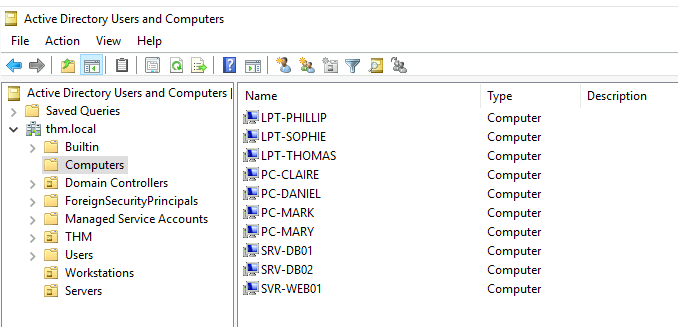
Workstations are one of the most common devices within an Active Directory domain. Each user in the domain will likely be logging into a workstation. This is the device they will use to do their work or normal browsing activities. These devices should never have a privileged user signed into them.

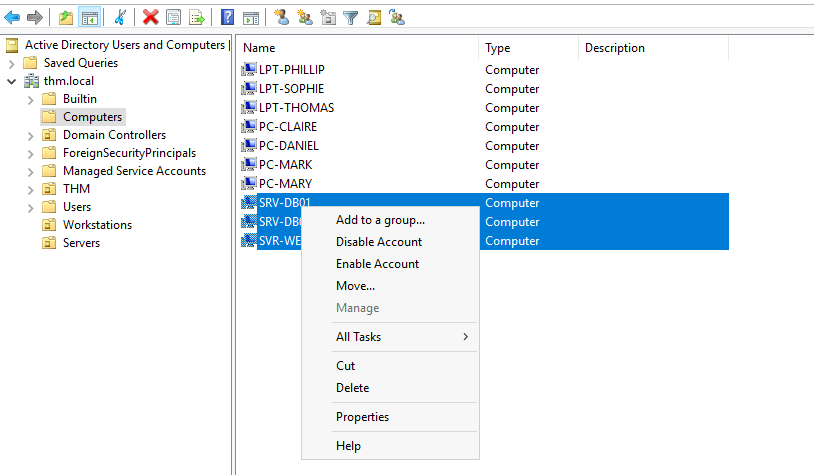
## Servers

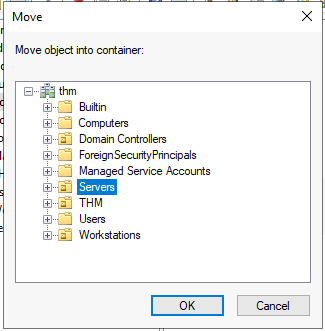
Servers are the second most common device within an Active Directory domain. Servers are generally used to provide services to users or other servers.

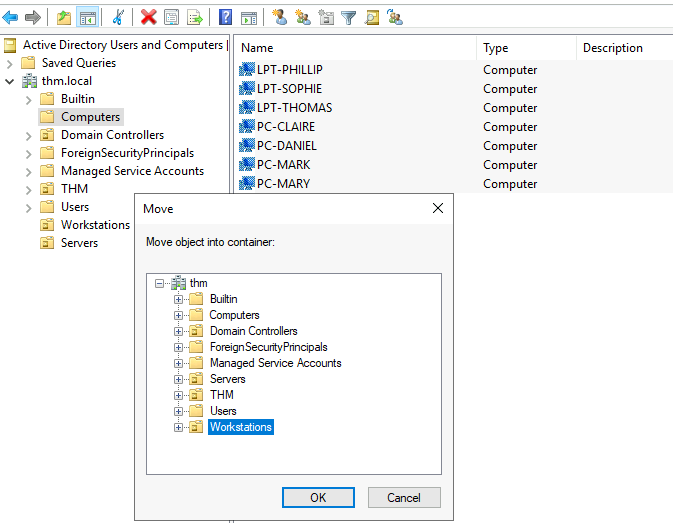
## Domain Controllers

Domain Controllers are the third most common device within an Active Directory domain. Domain Controllers allow you to manage the Active Directory Domain. These devices are often deemed the most sensitive devices within the network as they contain hashed passwords for all user accounts within the environment.





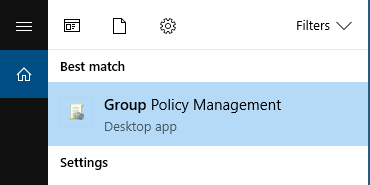




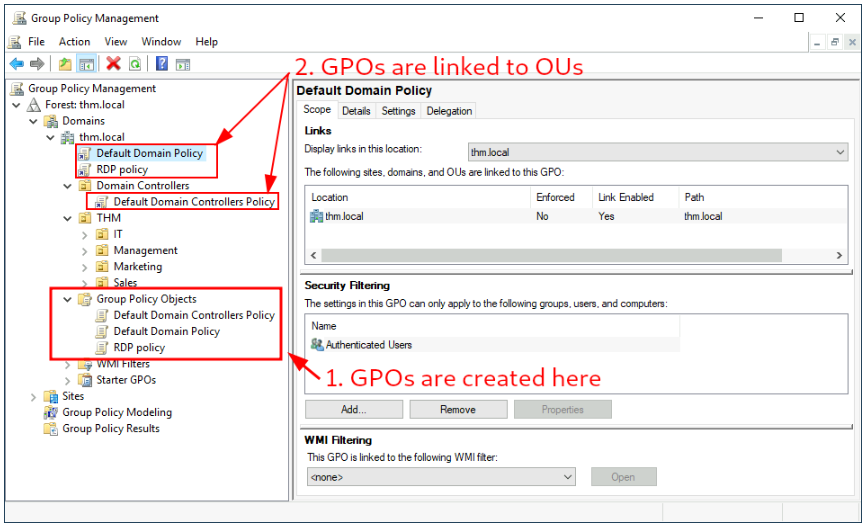
# Group Policies

So far, we have organised users and computers in OUs just for the sake of it, but the main idea behind this is to be able to deploy different policies for each OU individually. That way, we can push different configurations and security baselines to users depending on their department.

To configure GPOs, you can use the **Group Policy Management** tool, available from the start menu:

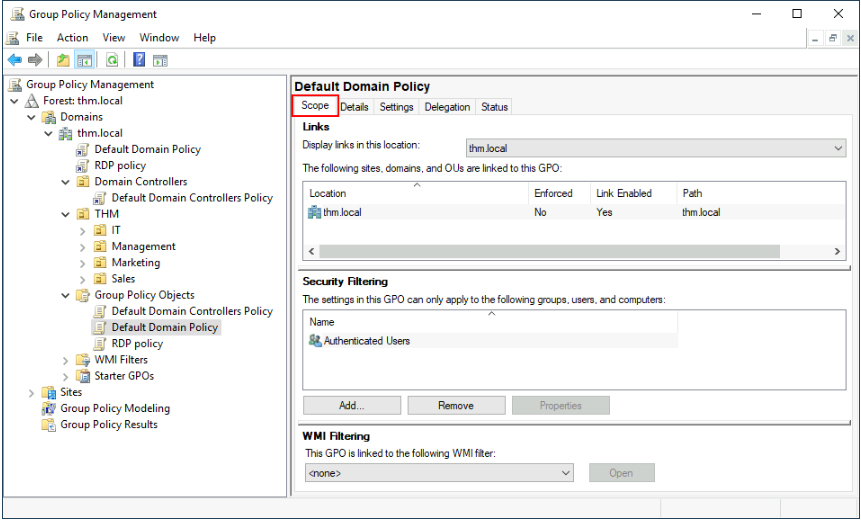


The first thing you will see when opening it is your complete OU hierarchy, as defined before. To configure Group Policies, you first create a GPO under **Group Policy Objects** and then link it to the OU where you want the policies to apply. As an example, you can see there are some already existing GPOs in your machine:



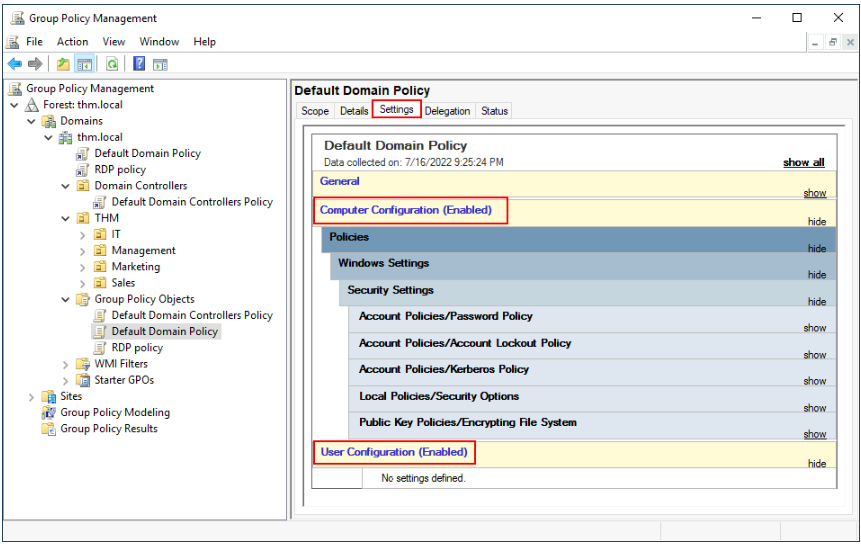
We can see in the image above that 3 GPOs have been created. From those, the Default Domain Policy and RDP Policy are linked to the thm.local domain as a whole, and the Default Domain Controllers Policy is linked to the Domain Controllers OU only. Something important to have in mind is that any GPO will apply to the linked OU and any sub-OUs under it. For example, the Sales OU will still be affected by the Default Domain Policy.

Let's examine the Default Domain Policy to see what's inside a GPO. The first tab you'll see when selecting a GPO shows its **scope**, which is where the GPO is linked in the AD. For the current policy, we can see that it has only been linked to the thm.local domain:

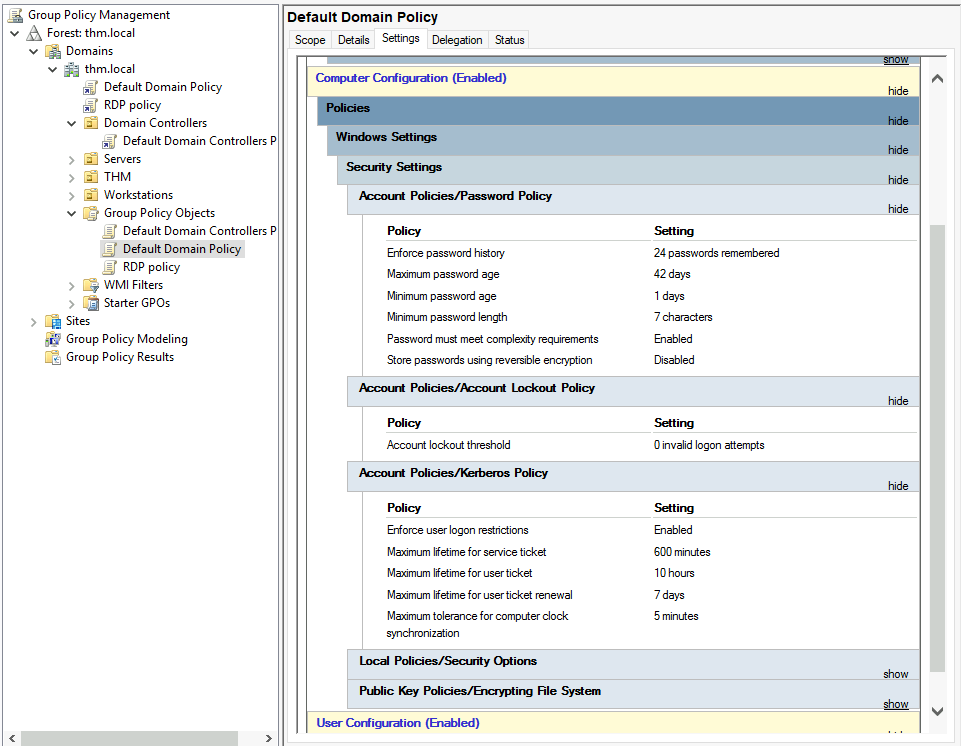


As you can see, you can also apply **Security Filtering** to GPOs so that they are only applied to specific users/computers under an OU. By default, they will apply to the **Authenticated Users** group, which includes all users/PCs.

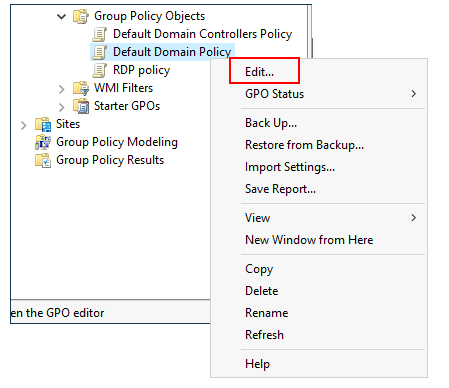
The **Settings** tab includes the actual contents of the GPO and lets us know what specific configurations it applies. As stated before, each GPO has configurations that apply to computers only and configurations that apply to users only. In this case, the Default Domain Policy only contains Computer Configurations:



 In this case, the Default Domain Policy indicates really basic configurations that should apply to most domains, including password and account lockout policies:

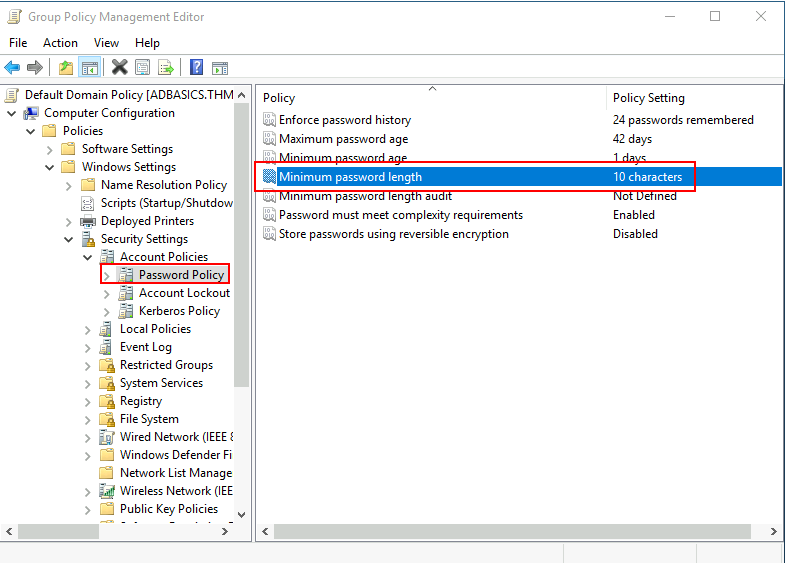


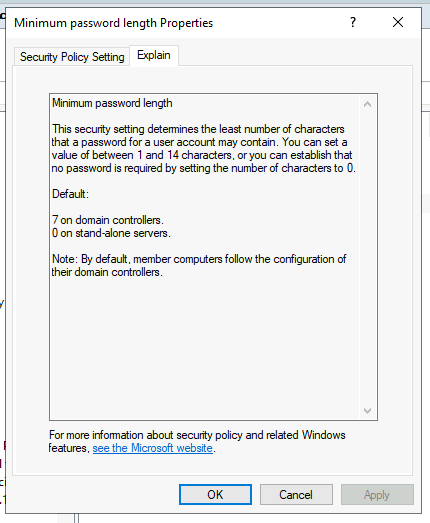
Let's change the minimum password length policy to require users to have at least 10 characters in their passwords. To do this, right-click the GPO and select **Edit**:



This will open a new window where we can navigate and edit all the available configurations. To change the minimum password length, go to

Computer Configurations -> Policies -> Windows Setting -> Security Settings -> Account Policies -> Password Policy and change the required policy value:

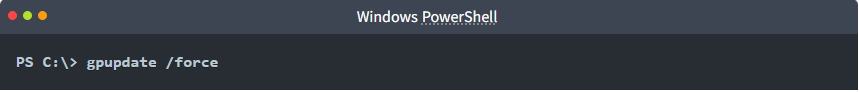




## GPO distribution

GPOs are distributed to the network via a network share called SYSVOL, which is stored in the DC. All users in a domain should typically have access to this share over the network to sync their GPOs periodically. The SYSVOL share points by default to the C:\Windows\SYSVOL\sysvol\ directory on each of the DCs in our network.

Once a change has been made to any GPOs, it might take up to 2 hours for computers to catch up. If you want to force any particular computer to sync its GPOs immediately, you can always run the following command on the desired computer:



Creating some GPOs for THM Inc.

As part of our new job, we have been tasked with implementing some GPOs to allow us to:

1. Block non-IT users from accessing the Control Panel.
2. Make workstations and servers lock their screen automatically after 5 minutes of user inactivity to avoid people leaving their sessions exposed.