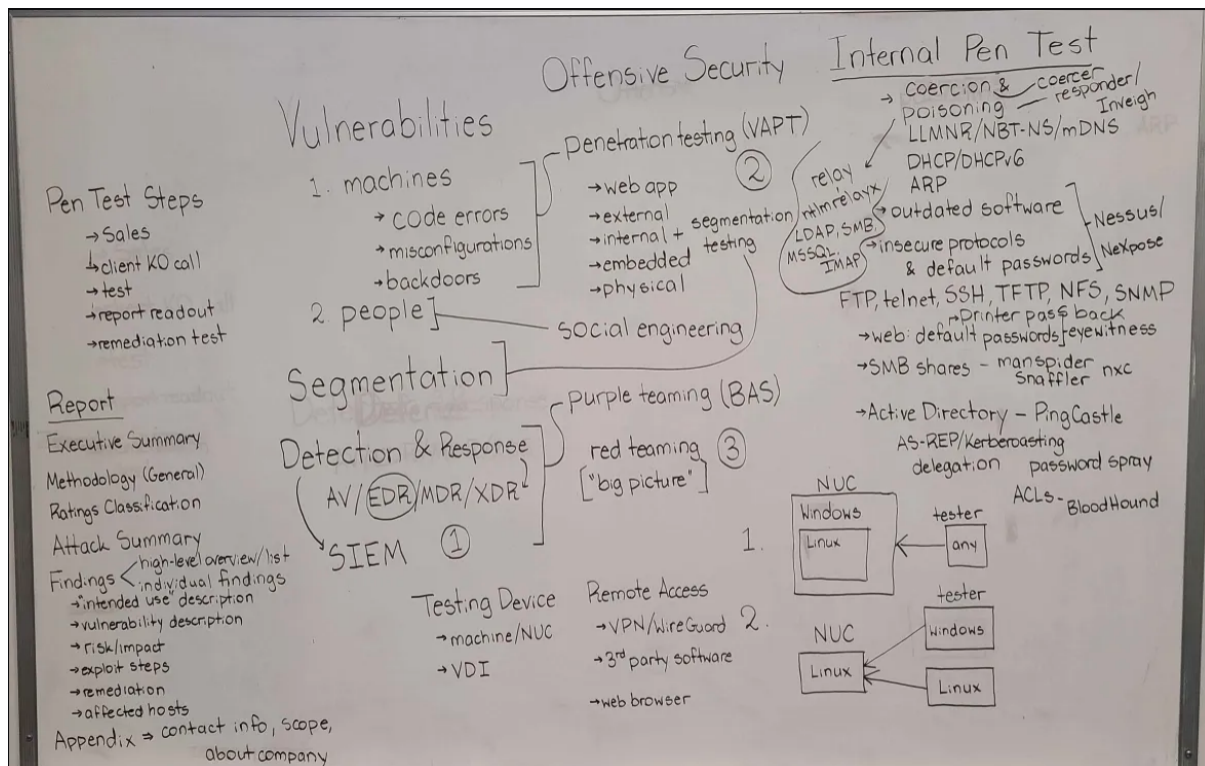


# Collegiate Penetration Testing Competition



## Pentest Steps

- Client Kick off call
- Test + peer review
- report readout
- remediation test + peer review

Sysreptor tool to write reports

- 90 % of tests are done on poisoning.
- Hacker recipes.
- TCM security.
- CDN. what is CDn ?
- change prox mox pass.
- change kali pass.
- set pass for windows machine.

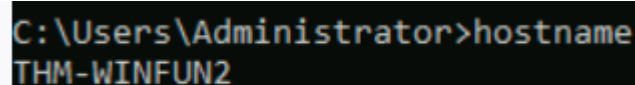
LdapRelayScan , PKINITtools, statistically-likely-usernames

- To access local users and groups using the run dialog box from windows logo start button use **lusrmgr.msc**
- to open system configuration using run dialog prompt use: msconfig
- to open windows system management open: msinfo32
- to open windows command prompt use cmd

Note: windows command prompt and powershell are not case sensitive.

## Windows command prompt

1. To know the computer name we use "hostname" as command.



```
C:\Users\Administrator>hostname
THM-WINFUN2
```

2. To know the logged-in user: we use whoami command

The command **whoami** will output the name of the logged-in user.

```
C:\Users\Administrator>whoami  
thm-winfun2\administrator
```

3. A command used often is **ipconfig**. This command will show the network address settings for the computer.

```
C:\Users\Administrator>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet:  
  
    Connection-specific DNS Suffix  . : eu-internal  
    Link-local IPv6 Address . . . . . : fe80::6486:c81a:3db5:a0ed%7  
    IPv4 Address. . . . . : 10.10.  
    Subnet Mask . . . . . : 255.255.0.0  
    Default Gateway . . . . . : 10.10.  
  
C:\Users\Administrator>
```

4. A command to retrieve the help manual for a command is **/?**.

```

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : THM-WINFUN2
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : eu-west-1.ec2-utilities.amazonaws.com
                                   eu-west-1.compute.internal

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : eu-west-1.compute.internal
Description . . . . . : AWS PV Network Device #0
Physical Address. . . . . : 02-45-EB-96-31-E5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::fd01:ae01:5a9d:37ba%7(Preferred)
IPv4 Address. . . . . : 10.10.159.6(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Lease Obtained. . . . . : Sunday, September 15, 2024 8:12:29 PM
Lease Expires . . . . . : Sunday, September 15, 2024 10:42:29 PM
Default Gateway . . . . . : 10.10.0.1
DHCP Server . . . . . : 10.10.0.1
DHCPv6 IAID . . . . . : 117897266
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-0B-D3-93-00-0C-29-49-2A-7E
DNS Servers . . . . . : 10.0.0.2
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrator>_

```

5. To clear the command prompt screen, the command is `cls`.
6. netstat: The next command is `netstat`. as per the help manual, this command will display protocol statistics and current TCP/IP network connections.

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP    10.10.159.6:3389        ip-10-100-2-58:53234    ESTABLISHED

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : eu-west-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::fd01:ae01:5a9d:37ba%7
    IPv4 Address. . . . . : 10.10.159.6
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.10.0.1

C:\Users\Administrator>
```

```
C:\Users\Administrator>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
        /renew [adapter] | /release [adapter] |
        /renew6 [adapter] | /release6 [adapter] |
        /flushdns | /displaydns | /registerdns |
        /showclassid adapter |
        /setclassid adapter [classid] |
        /showclassid6 adapter |
        /setclassid6 adapter [classid] ]

where
    adapter          Connection name
                     (wildcard characters * and ? allowed, see examples)

Options:
    /?              Display this help message
    /all            Display full configuration information.
    /release        Release the IPv4 address for the specified adapter.
    /release6       Release the IPv6 address for the specified adapter.
    /renew          Renew the IPv4 address for the specified adapter.
    /renew6         Renew the IPv6 address for the specified adapter.
    /flushdns       Purges the DNS Resolver cache.
    /registerdns     Refreshes all DHCP leases and re-registers DNS names
    /displaydns     Display the contents of the DNS Resolver Cache.
    /showclassid    Displays all the dhcp class IDs allowed for adapter.
    /setclassid     Modifies the dhcp class id.
    /showclassid6   Displays all the IPv6 DHCP class IDs allowed for adapter.
    /setclassid6    Modifies the IPv6 DHCP class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig          ... Show information
```

7. The `net` command is primarily used to manage network resources. This command supports sub-commands.

8. if you wish to see the help information for `net user` , the command is `net help user` .

```
C:\Users\Administrator>net help
The syntax of this command is:
```

```
NET HELP
command
    -or-
NET command /HELP
```

Commands available are:

NET ACCOUNTS	NET HELPMSG	NET STATISTICS
NET COMPUTER	NET LOCALGROUP	NET STOP
NET CONFIG	NET PAUSE	NET TIME
NET CONTINUE	NET SESSION	NET USE
NET FILE	NET SHARE	NET USER
NET GROUP	NET START	NET VIEW
NET HELP		

NET HELP NAMES explains different types of names in NET HELP syntax lines.  
NET HELP SERVICES lists some of the services you can start.  
NET HELP SYNTAX explains how to read NET HELP syntax lines.  
NET HELP command | MORE displays Help one screen at a time.

```

C:\Users\Administrator>net help user
The syntax of this command is:

NET USER
[username [password | *] [options]] [/DOMAIN]
    username {password | *} /ADD [options] [/DOMAIN]
    username [/DELETE] [/DOMAIN]
    username [/TIMES:{times | ALL}]
    username [/ACTIVE: {YES | NO}]

NET USER creates and modifies user accounts on computers. When used
without switches, it lists the user accounts for the computer. The
user account information is stored in the user accounts database.

username      Is the name of the user account to add, delete, modify, or
               view. The name of the user account can have as many as
               20 characters.
password      Assigns or changes a password for the user's account.
               A password must satisfy the minimum length set with the
               /MINPWLEN option of the NET ACCOUNTS command. It can have as
               many as 14 characters.
*             Produces a prompt for the password. The password is not
               displayed when you type it at a password prompt.
/DOMAIN       Performs the operation on a domain controller of
               the current domain.
/ADD          Adds a user account to the user accounts database.
/DELETE       Removes a user account from the user accounts database.

Options       Are as follows:

  Options      Description
  -----
  /ACTIVE:{YES | NO}  Activates or deactivates the account. If
                       the account is not active, the user cannot
                       access the server. The default is YES.
  /COMMENT:"text"    Provides a descriptive comment about the
                       user's account. Enclose the text in
                       quotation marks.

```

Here's a list of basic and commonly used commands in the Windows Command Prompt (cmd):

1. `dir` - Lists the contents of a directory.
2. `cd` - Changes the directory.
3. `cls` - Clears the command prompt screen.
4. `copy` - Copies files from one location to another.
5. `move` - Moves files from one location to another.
6. `del` - Deletes one or more files.
7. `md` or `mkdir` - Creates a new directory.
8. `rd` or `rmdir` - Deletes a directory.
9. `type` - Displays the contents of a text file.
10. `echo` - Displays messages or turns command echoing on or off.



11. `exit` - Exits the command prompt or batch file.
12. `ren` or `rename` - Renames a file or files.
13. `find` - Searches for a text string in a file or files.
14. `xcopy` - Copies files and directories, including subdirectories.
15. `path` - Displays or sets a search path for executable files.
16. `attrib` - Displays or changes file attributes.
17. `chkdsk` - Checks a disk and displays a status report.
18. `diskpart` - Displays or configures Disk Partition properties.
19. `tasklist` - Displays all currently running tasks including services.
20. `taskkill` - Kills or stops a running process or application.
21. `ipconfig` - Displays all current TCP/IP network configuration values and refreshes DHCP and DNS settings.
22. `netstat` - Displays active connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6).
23. `ping` - Sends ICMP Echo Request messages to test network connectivity.
24. `tracert` - Traces the route that packets take to a specified host or destination.

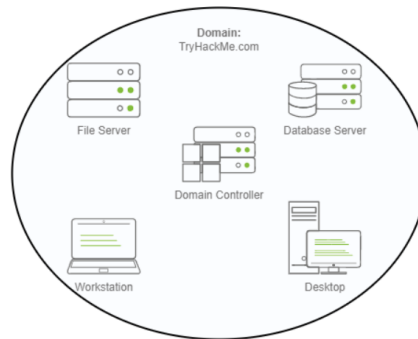
These commands form the foundation for interacting with the Windows operating system via the command line, enabling file management, network diagnostics, and system performance analysis.

To use a text editor in windows command prompt, we can use: `notepad <filename.txt>`

- Command to open the Windows Defender Firewall is `WF.msc`.

## Active Directory

To overcome these limitations, we can use a Windows domain. Simply put, a **Windows domain** is a group of users and computers under the administration of a given business. The main idea behind a domain is to centralise the administration of common components of a Windows computer network in a single repository called **Active Directory (AD)**. The server that runs the Active Directory services is known as a **Domain Controller (DC)**.



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

## 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.

```

graph TD
    A["Domain"] --> B["Domain Controller"]
    B --> C["Active Directory Domain Services"]

    C --> D["User Management"]
    C --> E["Group Policy"]
    C --> F["Authentication"]
    C --> G["Resource Access Control"]

    %% Additional components can be added as needed
    D --> H["User Accounts"]
    D --> I["User Groups"]

    E --> J["Security Policies"]
    E --> K["Software Deployment"]

    F --> L["Kerberos"]
    F --> M["LDAP"]

    G --> N["File Permissions"]
    G --> O["Network Resource Access"]

```

This Mermaid diagram illustrates the hierarchical structure of a domain, domain controller, and Active Directory Domain Services (AD DS). It shows how AD DS manages various aspects of network administration, including user management, group policies, authentication, and resource access control. The diagram also includes some key subcomponents and protocols associated with each main function of AD DS.

## 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. You could say that a security principal is an object that can act upon resources in the network.

Users can be used to represent two types of entities:

- **People:** users will generally represent persons in your organisation that need to access the network, like employees.
- **Services:** you can also define users to be used by services like IIS or MSSQL. Every single service requires a user to run, but service users are different from regular users as they will only have the privileges needed to run their specific service.

### **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 principals" 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.

**Note:** Machine Account passwords are automatically rotated out and are generally comprised of 120 random characters.

Identifying machine accounts is relatively easy. They follow a specific naming scheme. The machine account name is the computer's name followed by a dollar sign. For example, a machine named `DC01` will have a machine account called `DC01$`.

## 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.

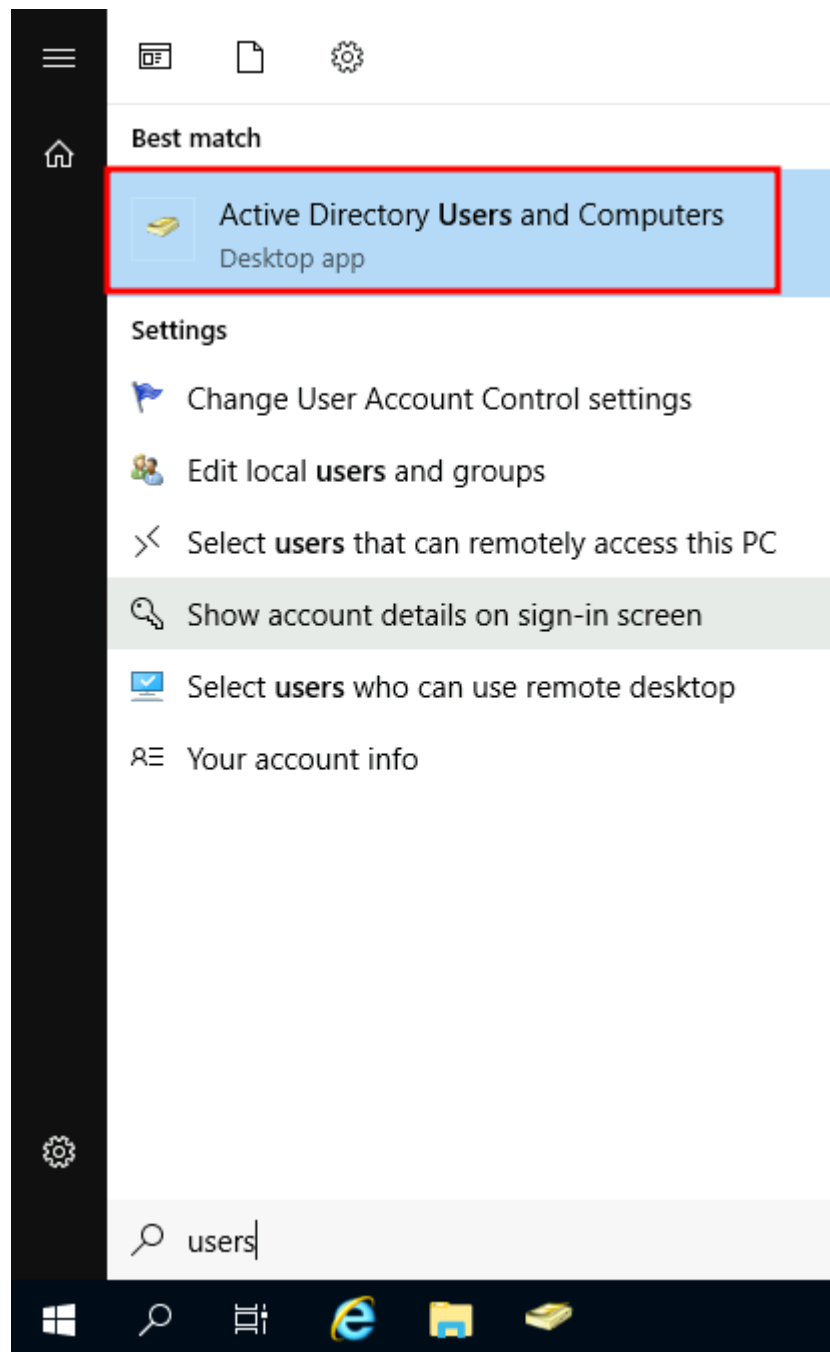
Several groups are created by default in a domain that can be used to grant specific privileges to users. As an example, here are some of the most important groups in a domain:

Security Group	Description
Domain Admins	Users of this group have administrative privileges over the entire domain. By default, they can administer any computer on the domain, including the DCs.
Server Operators	Users in this group can administer Domain Controllers. They cannot change any administrative group memberships.
Backup Operators	Users in this group are allowed to access any file, ignoring their permissions. They are used to perform backups of data on computers.
Account Operators	Users in this group can create or modify other accounts in the domain.
Domain Users	Includes all existing user accounts in the domain.
Domain Computers	Includes all existing computers in the domain.
Domain Controllers	Includes all existing DCs on the domain.

You can obtain the complete list of default security groups from the [Microsoft documentation](#).

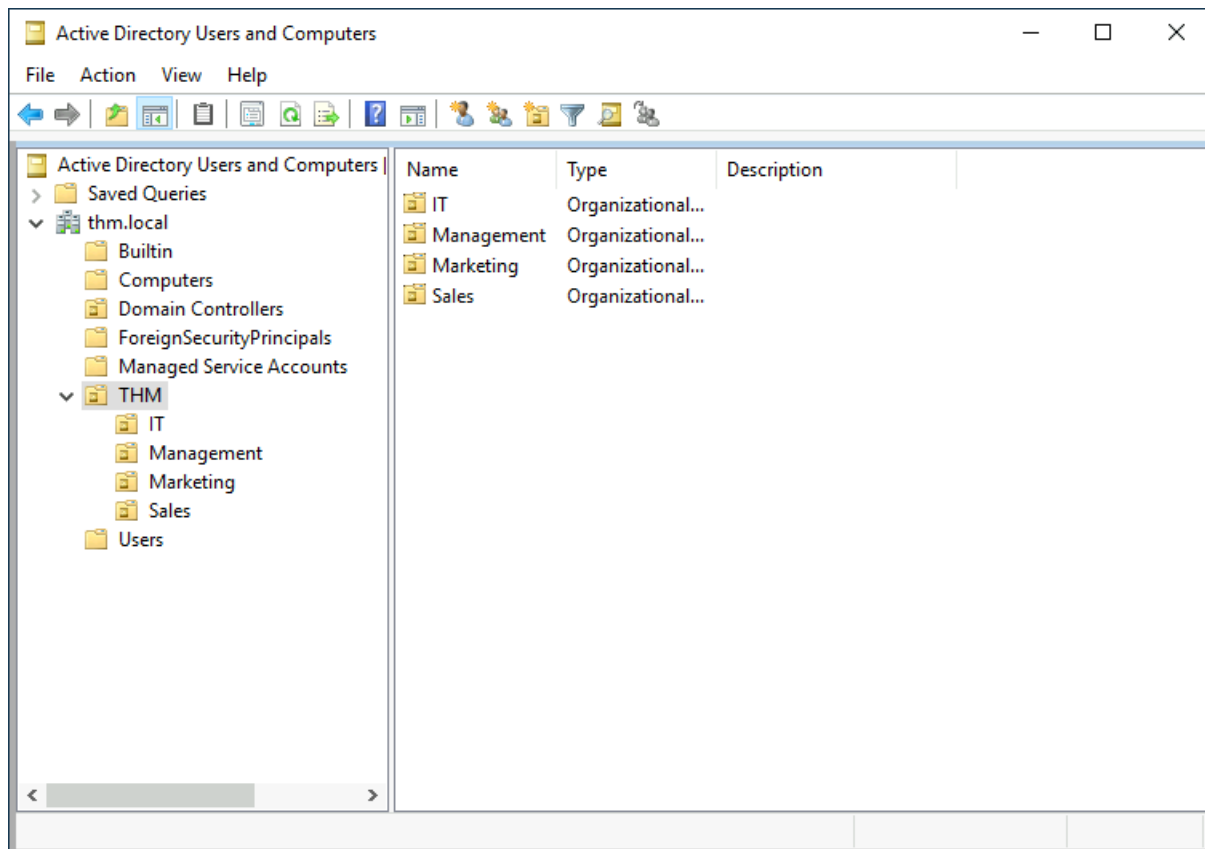
## Active Directory Users and Computers

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:

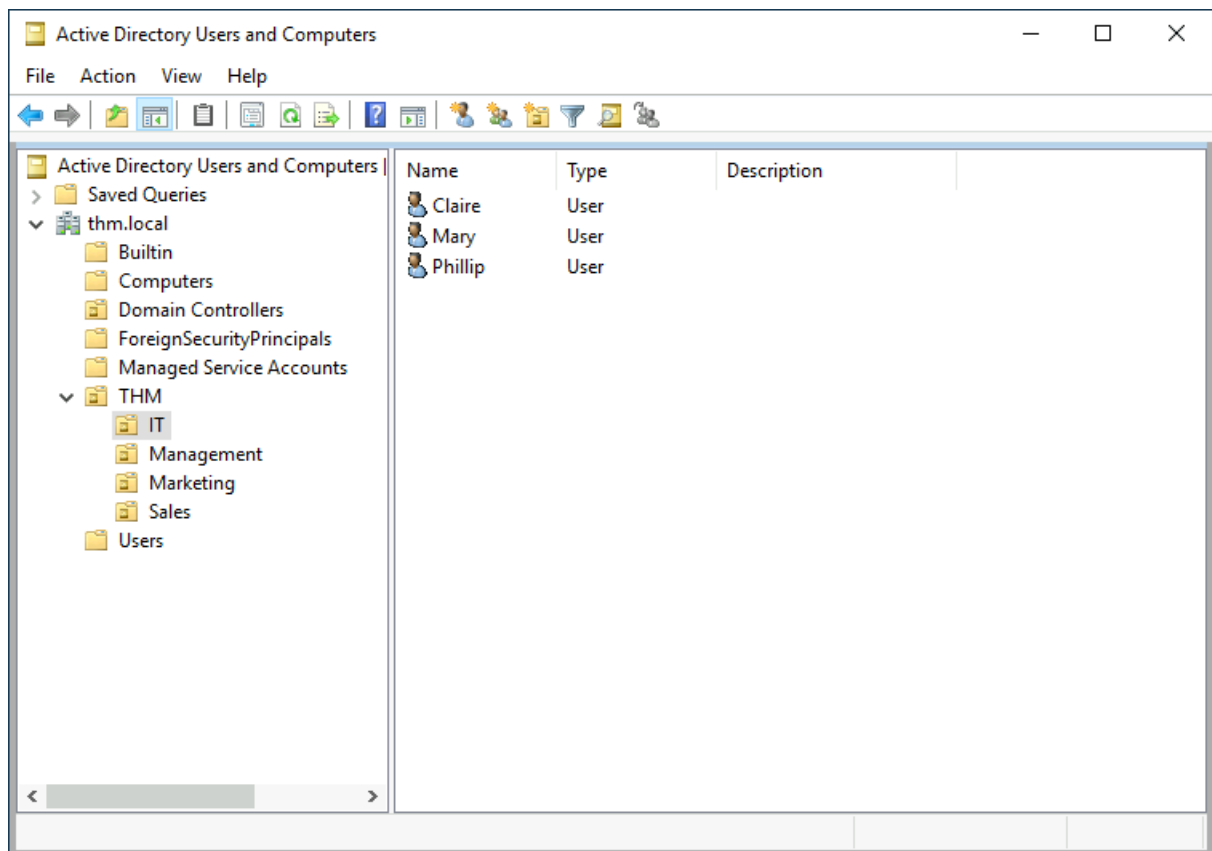


This will open up a window where you can see the hierarchy of users, computers and groups that exist in the domain. These objects are organised in **Organizational Units (OUs)** which are container objects that allow you to classify users and machines. OUs are mainly used to define sets of users with similar policing requirements. The people in the Sales department of your organisation are likely to have a different set of policies applied than the people in IT, for example. Keep in mind that a user can only be a part of a single OU at a time.

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. Feel free to right-click the **THM** OU and create a new OU under it called **Students** just for the fun of it.



If you open any OUs, you can see the users they contain and perform simple tasks like creating, deleting or modifying them as needed. You can also reset passwords if needed (pretty useful for the helpdesk):



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

You are probably wondering why we have both groups and OUs. While both are used to classify users and computers, their purposes are entirely different:

- **OUs** are handy for **applying policies** to users and computers, which include specific configurations that pertain to sets of users depending on their

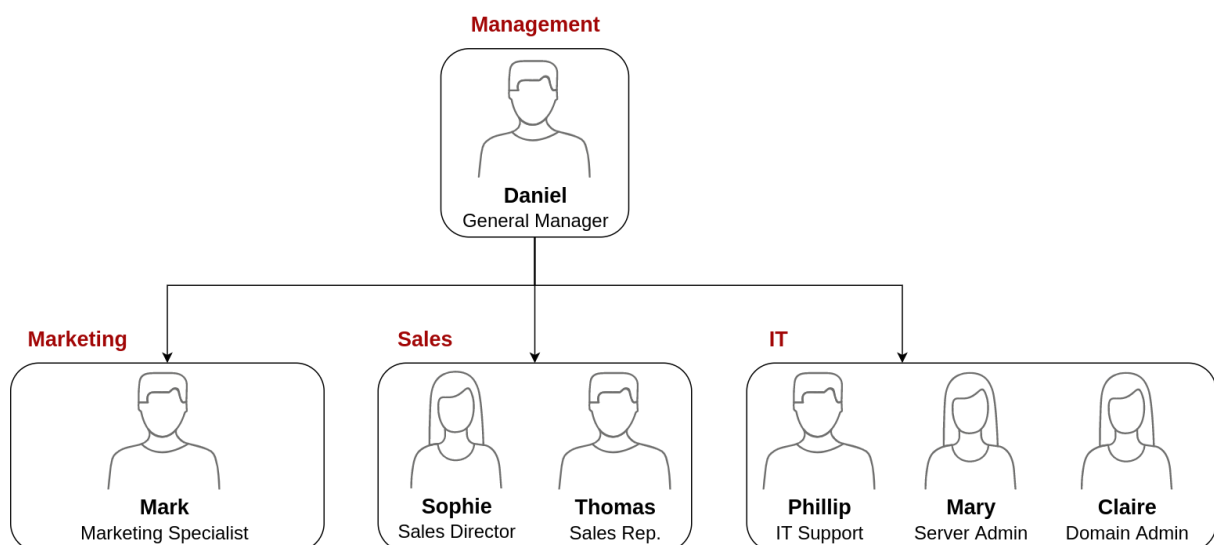


particular role in the enterprise. Remember, a user can only be a member of a single OU at a time, as it wouldn't make sense to try to apply two different sets of policies to a single user.

- **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 groups in AD

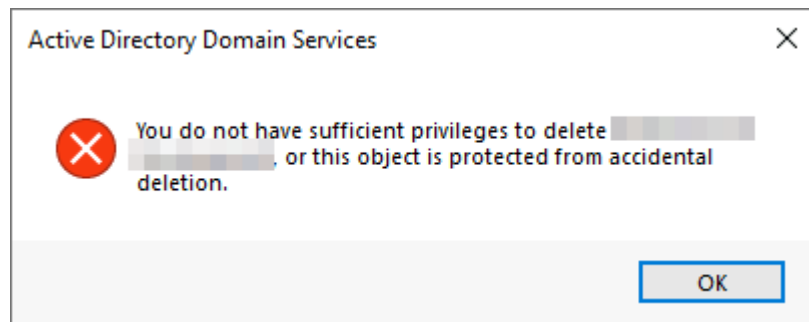
Your first task as the new domain administrator is to check the existing AD OUs and users, as some recent changes have happened to the business. You have been given the following organisational chart and are expected to make changes to the AD to match it:



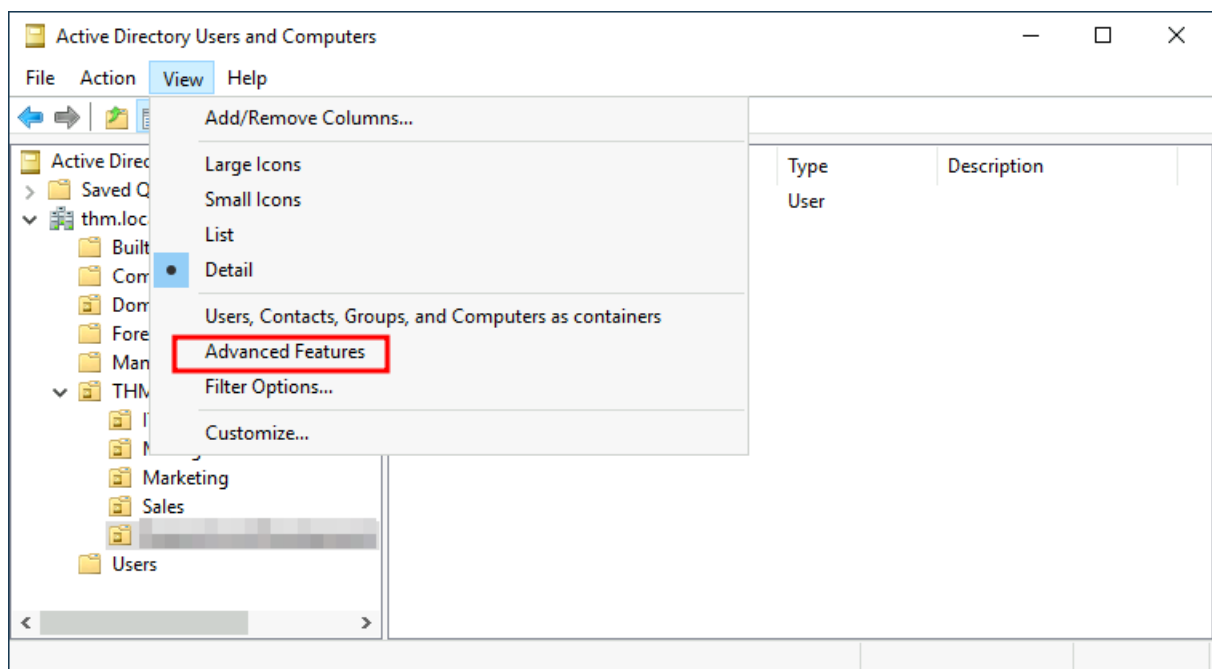
## Deleting extra OUs and users

The first thing you should notice is that there is an additional department OU in your current AD configuration that doesn't appear in the chart. We've been told

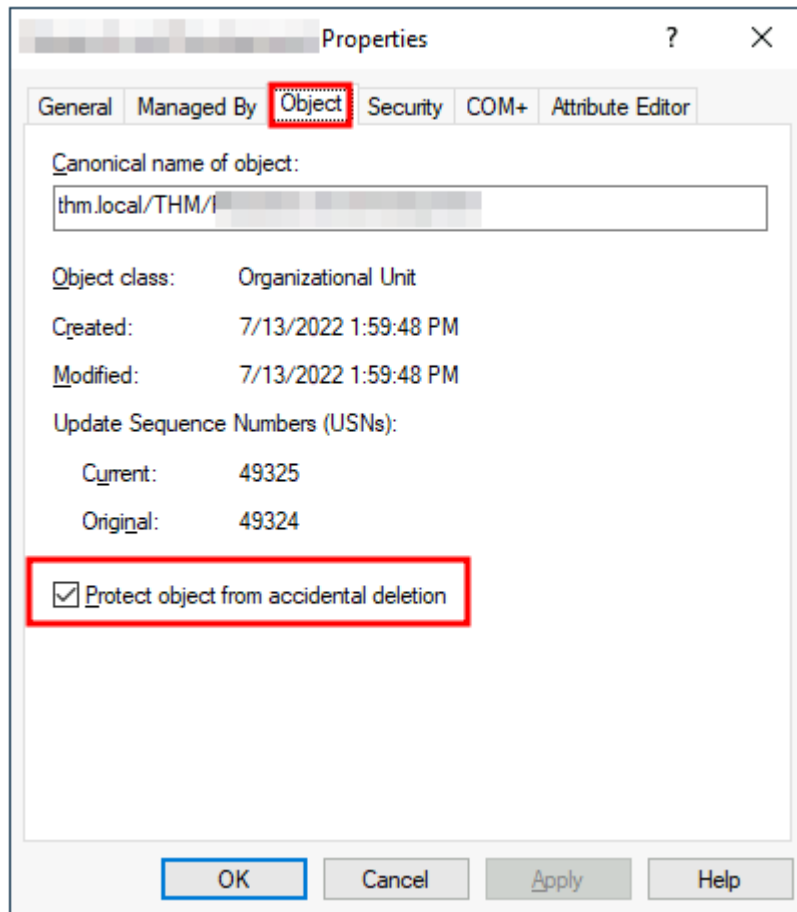
it was closed due to budget cuts and should be removed from the domain. If you try to right-click and delete the OU, you will get the following error:



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.

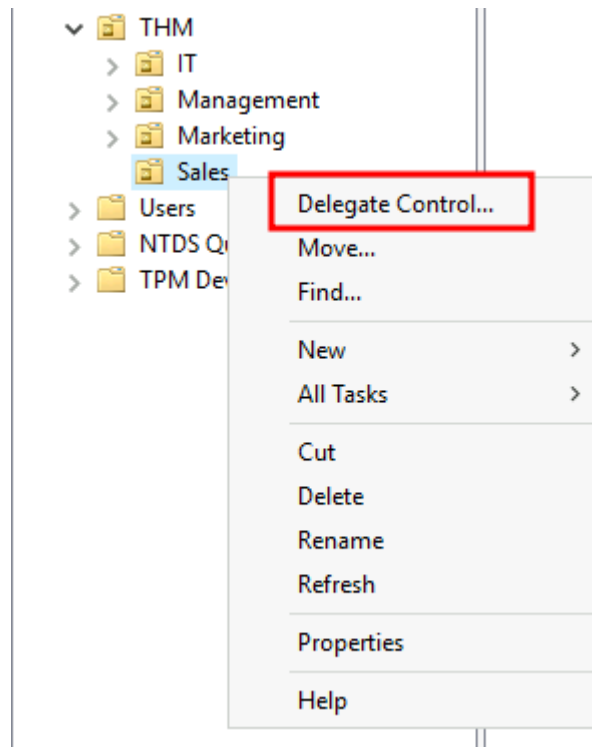
## Delegation

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 the

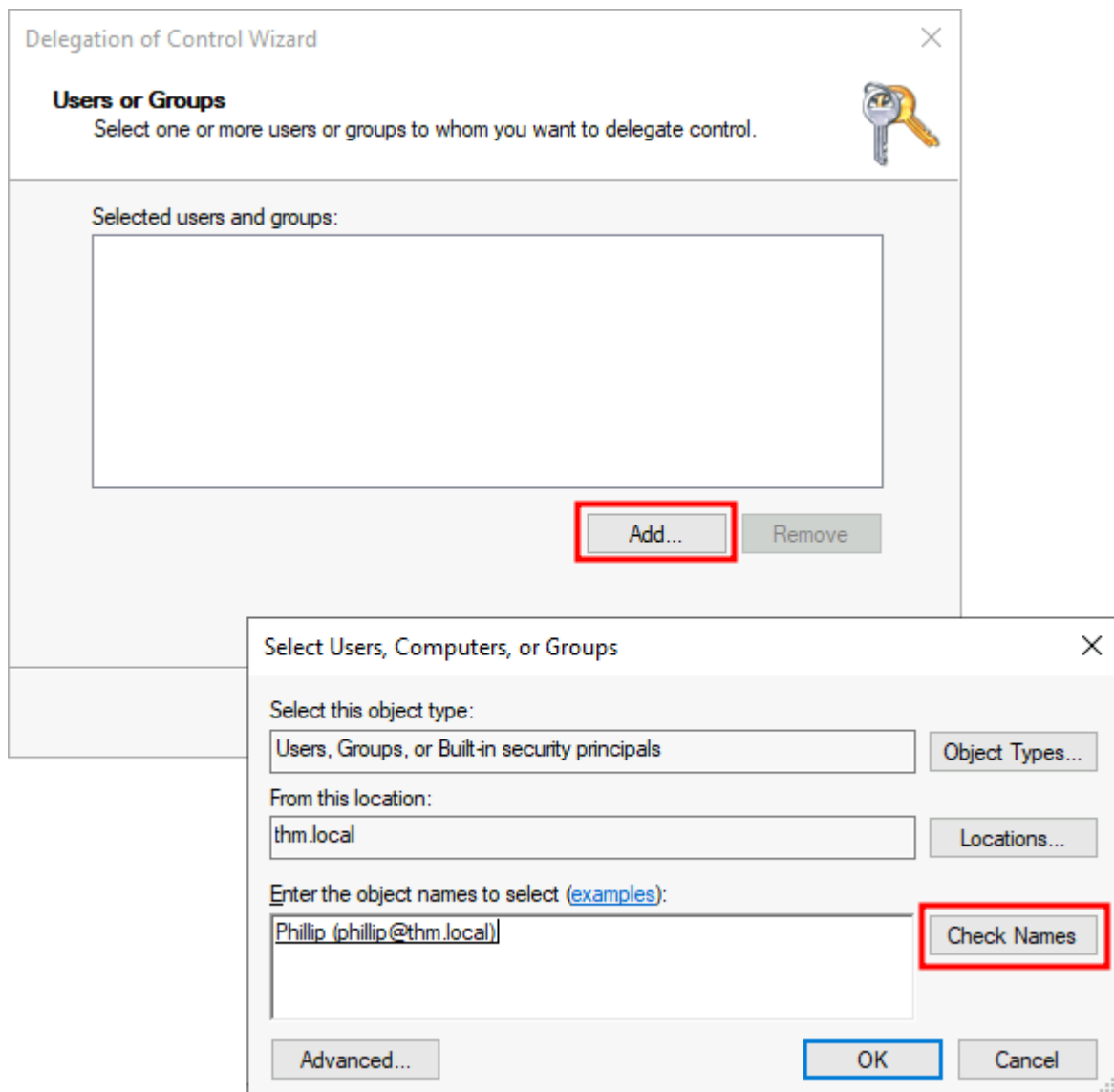
control of resetting passwords over the Sales, Marketing and Management OUs to him.

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**:

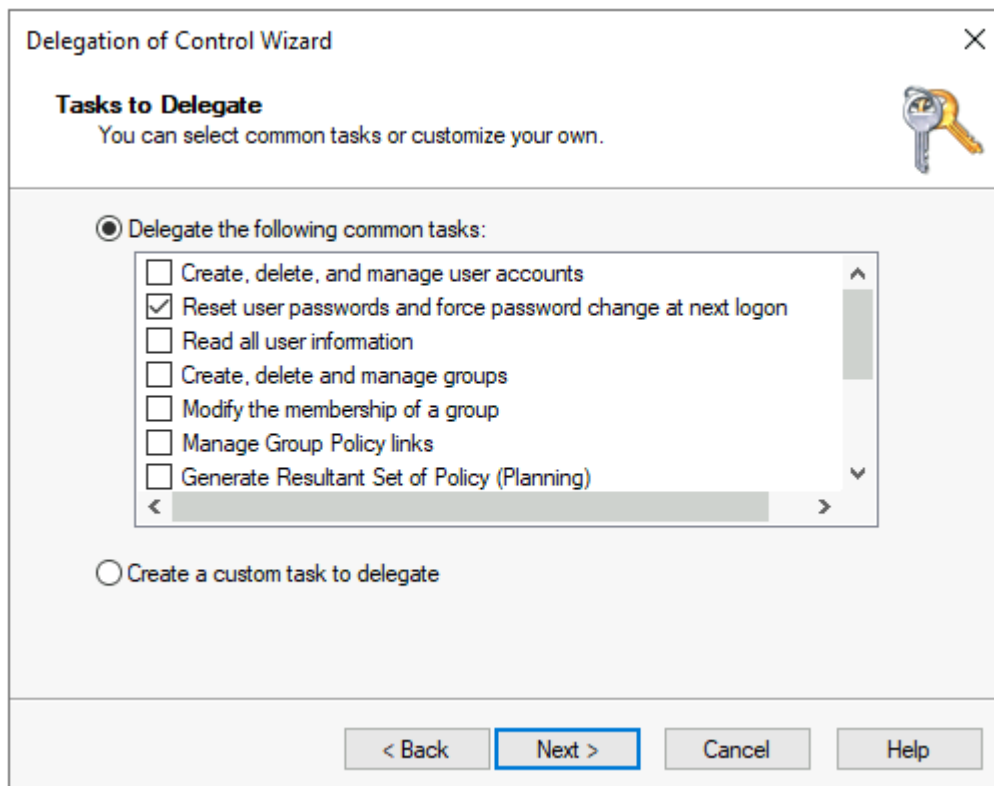


This should open a new window where you will first be asked for the users to whom you want to delegate control:

**Note:** To avoid mistyping the user's name, write "phillip" and click the **Check Names** button. Windows will autocomplete the user for you.



Click OK, and on the next step, select the following option:



Click next a couple of times, and now Phillip should be able to reset passwords for any user in the sales department. While you'd probably want to repeat these steps to delegate the password resets of the Marketing and Management departments, we'll leave it here for this task. You are free to continue to configure the rest of the OUs if you so desire.

Now let's use Phillip's account to try and reset Sophie's password. Here are Phillip's credentials for you to log in via RDP:



<b>Username</b>	phillip
<b>Password</b>	Claire2008

**Note:** When connecting via RDP, use `THM\phillip` as the username to specify you want to log in using the user `phillip` on the `THM` domain.

While you may be tempted to go to **Active Directory Users and Computers** to try and test Phillip's new powers, he doesn't really have the privileges to open it, so you'll have to use other methods to do password resets. In this case, we will be using Powershell to do so:

WindowsPowerShell(As Phillip)

```
PS C:\Users\phillip> Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host -AsSecureString -Prompt 'New Password') -Verbose
```

```
New Password: *****
```

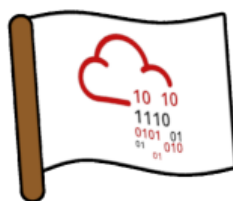
```
VERBOSE: Performing the operation "Set-ADAccountPassword" on target "CN=Sophie,OU=Sales,OU=THM,DC=thm,DC=local".
```

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:

WindowsPowerShell(as Phillip)

```
PS C:\Users\phillip> Set-ADUser -ChangePasswordAtLogon $true -Identity sophie -Verbose
```

```
VERBOSE: Performing the operation "Set" on target "CN=Sophie,OU=Sales,OU=THM,DC=thm,DC=local".
```



Log into Sophie's account with your new password and retrieve a flag from Sophie's desktop.

**Note:** When connecting via RDP, use `THM\sophie` as the username to specify you want to log in using the user `sophie` on the `THM` domain.

In Windows Command Prompt, the equivalent of the `su` command (used in Unix-based systems to switch users) is the `runas` command. The `runas` command allows you to run a program as another user.

Here's an example of how to use it:

```
runas /user:Administrator cmd
```

This command will prompt you for the password of the `Administrator` user and then open a new Command Prompt window as that user.

Make sure you have the appropriate permissions to switch users or run commands as another user.

## Scenario

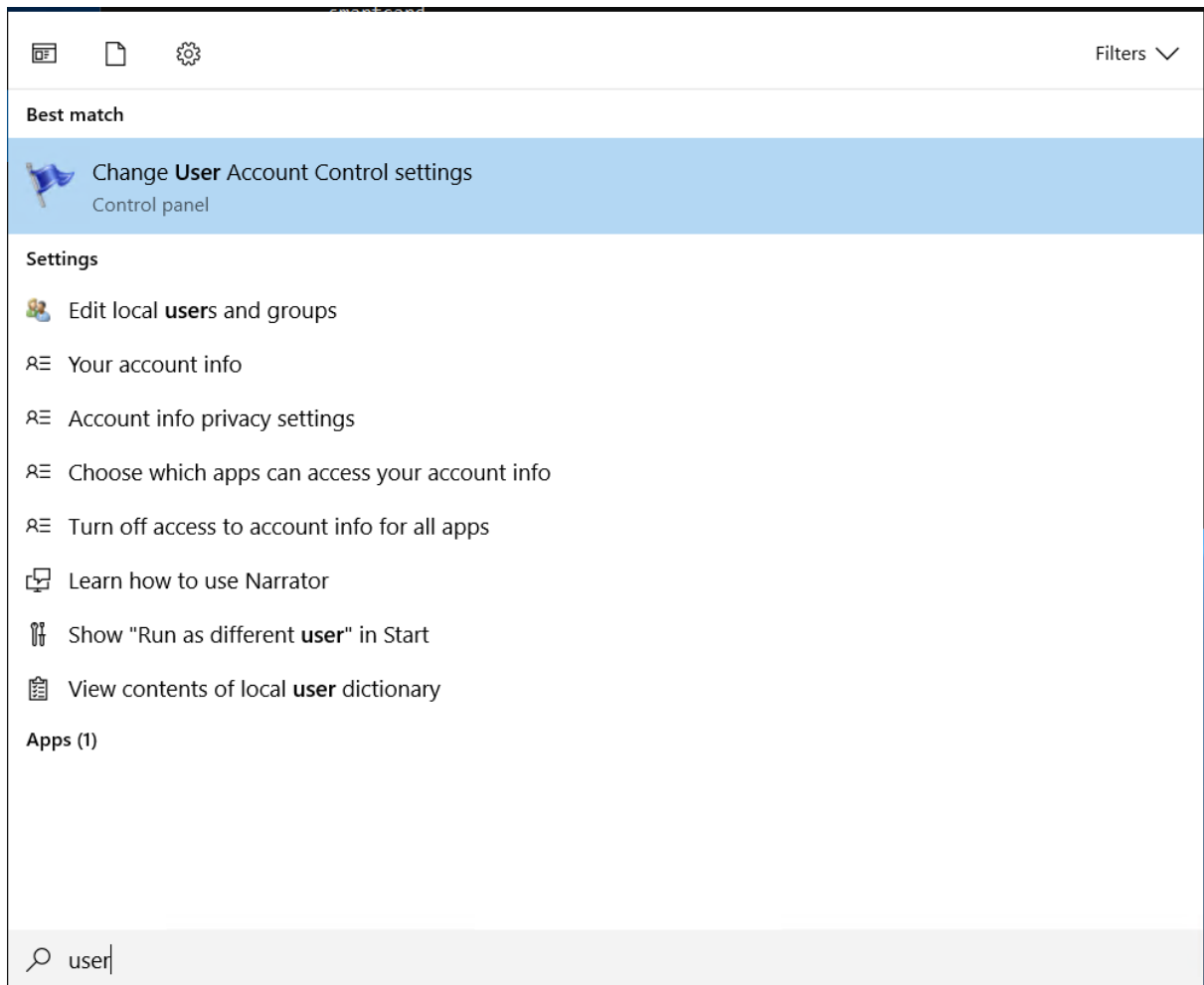
Scenario: I am a standard user `phillip`, who wants to access Active Directory Domain Service, but I am not a domain admin.

The thing is I know administrator user is the domain admin and he is part of `Domain Admin group`

I am trying to access the ADDS by being a standard user which is impossible if you do not know the Administrator's creds.

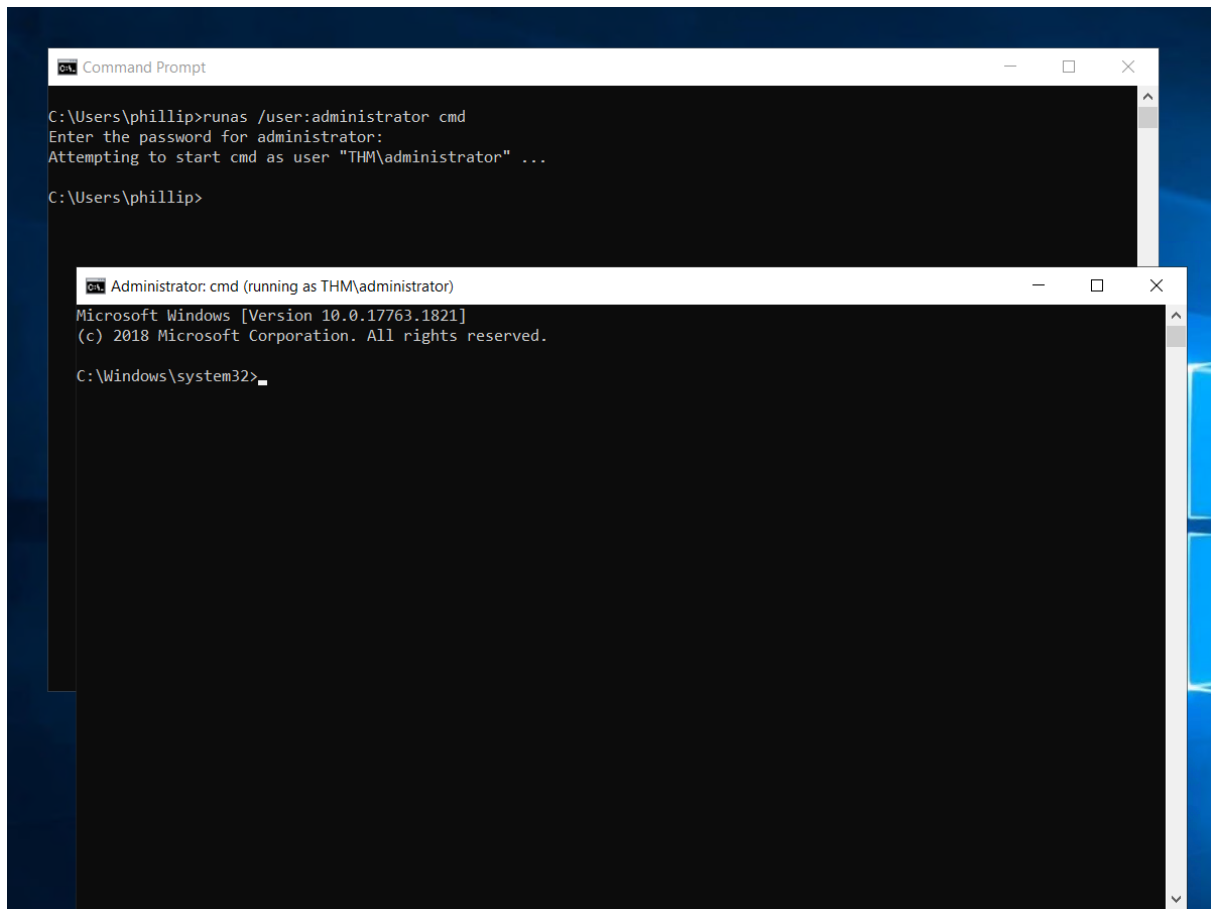
lets do it





See, I am a standard user "phillip" and when I tried searching for user, it did not show me AD DS.

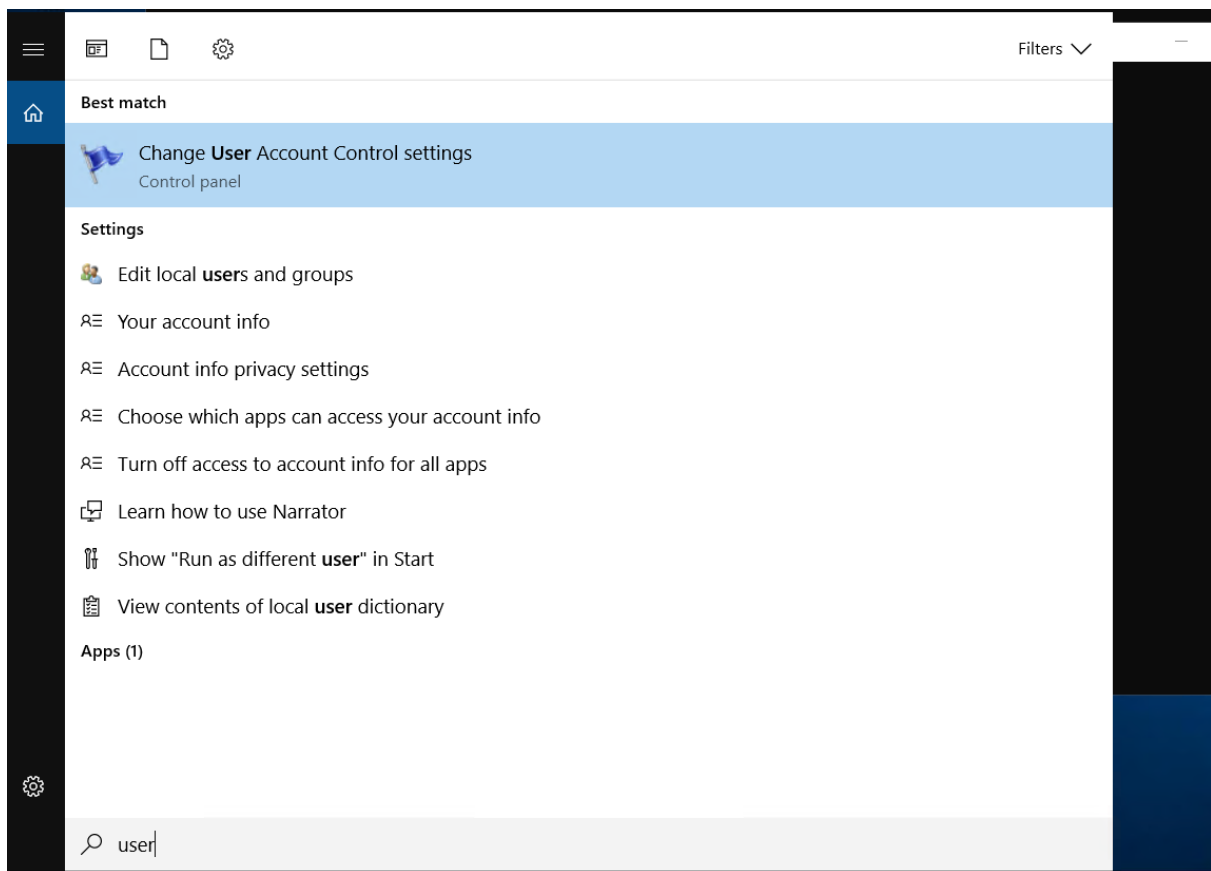
Step 1: We will utilize administrator users creds to get admin access.



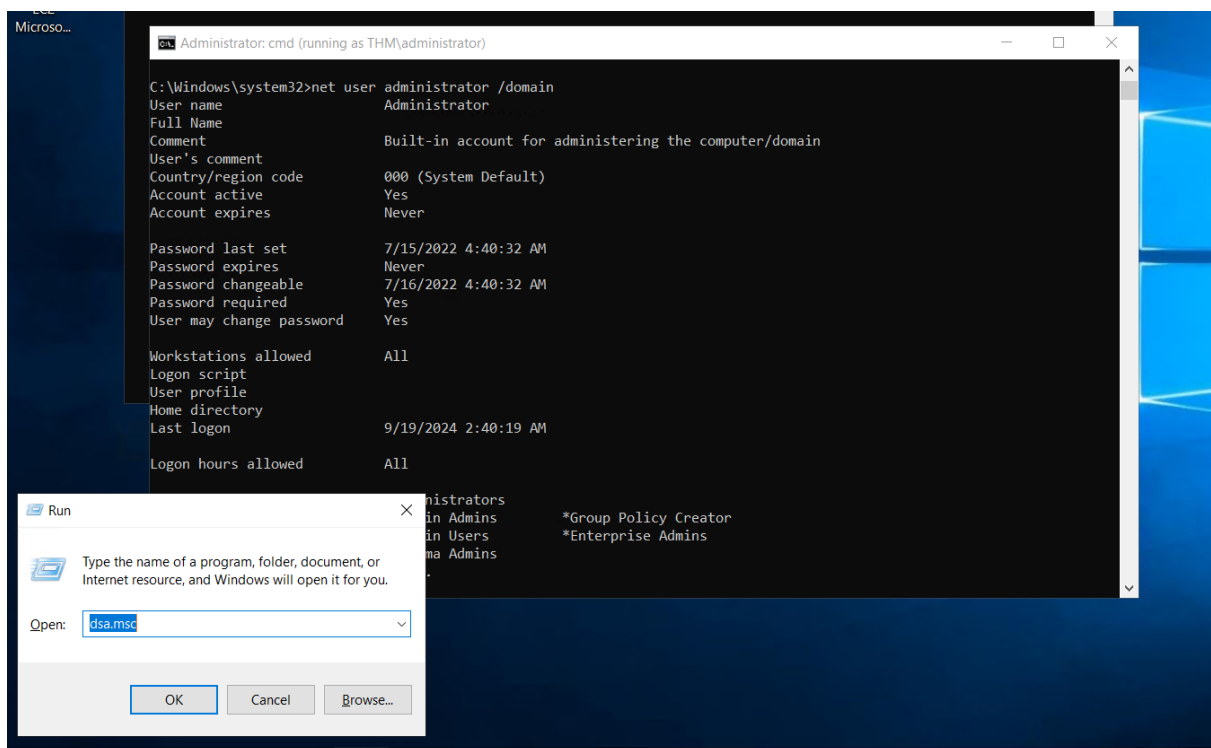
- We are now an admin user.

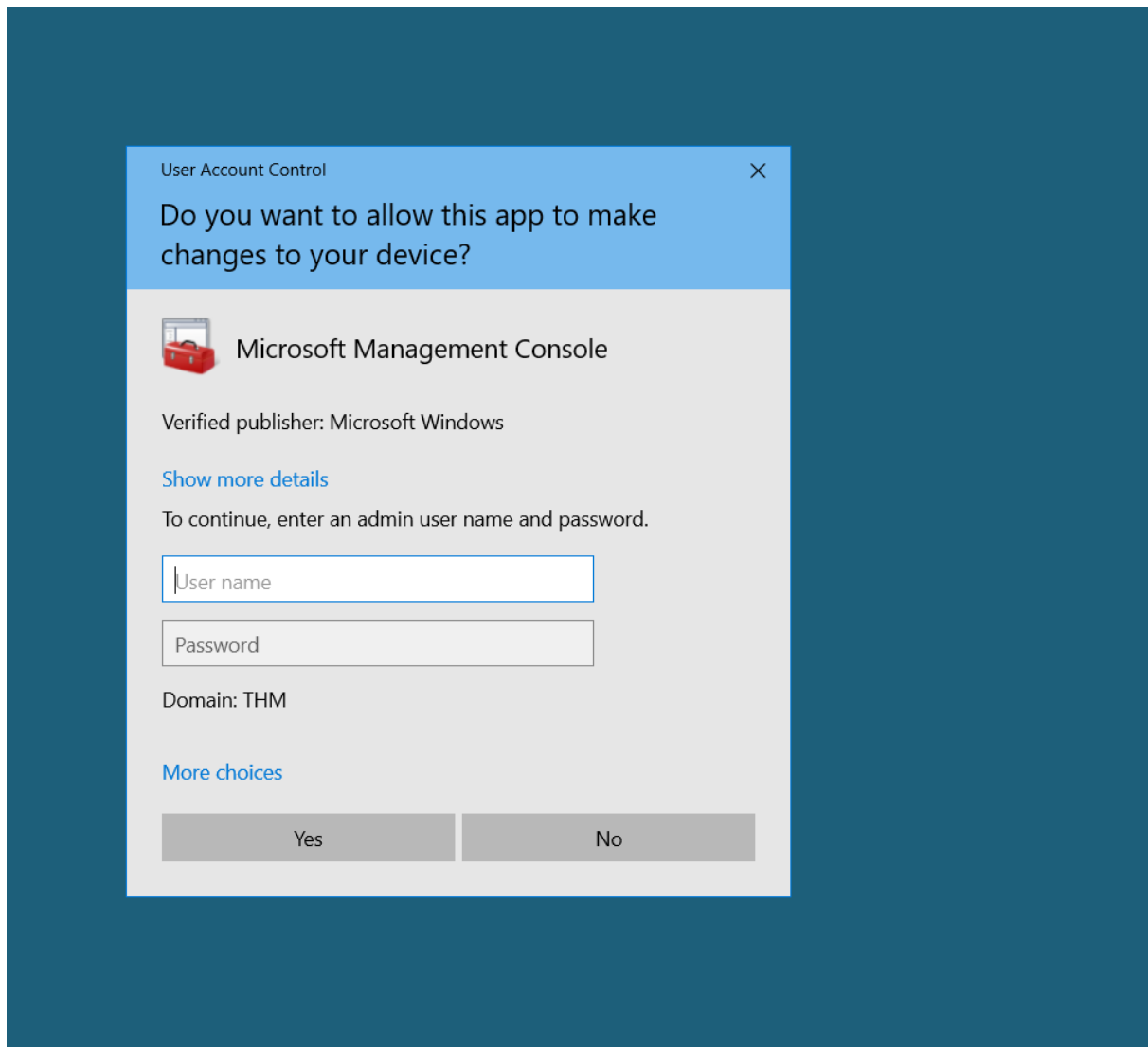
Step 2: To be a **Domain Admin** for accessing AD DS, you need to be a part of **Local Group Memberships** group.

- We can see administrator is part of Local Group Memberships group.
- So we can access AD DS. But we still cannot access AD DS using search I II just screenshot it.

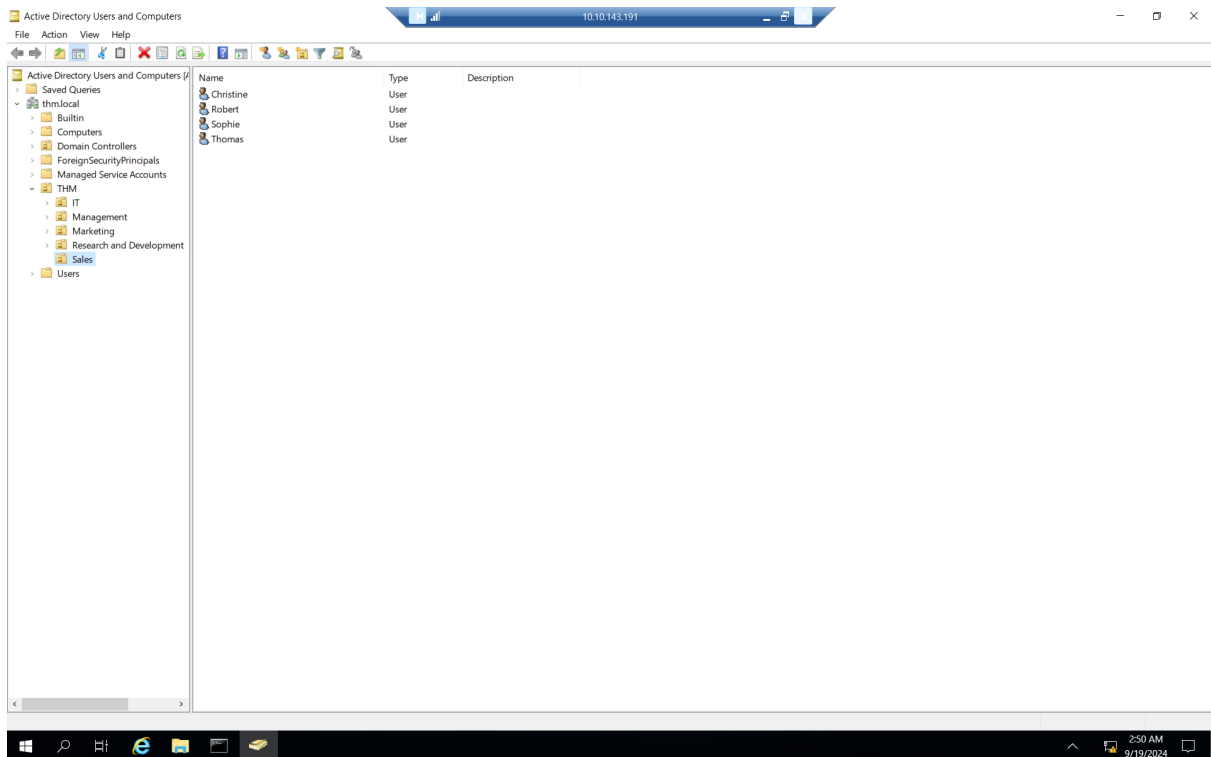


- We are an administrator user, we are part of local group membership group, but we cannot still access the AD DS, here's how we can do now
- By running a **dsa.msc in a dialog box**





- It will prompt for UAC and we need to again enter Admin creds and we are good to go.



- Hurray, we have admin access, we will try something crazy now I will add phillip to the local group membership and see whether I can access to the AD DS

```
Administrator: cmd (running as THM\administrator)

C:\Windows\system32>net user phillip /domain
User name                phillip
Full Name                Phillip
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        7/11/2022 1:39:41 PM
Password expires         Never
Password changeable      7/12/2022 1:39:41 PM
Password required        Yes
User may change password No

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               9/19/2024 1:48:43 AM

Logon hours allowed      All

Local Group Memberships
Global Group memberships *Domain Users
The command completed successfully.
```

- see its not a part of the local group memberships group.

```
Administrator: cmd (running as THM\administrator)
C:\Windows\system32>net group

Group Accounts for \\ADBASICS

-----
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Key Admins
*Protected Users
*Read-only Domain Controllers
*Schema Admins
The command completed successfully.
```

```
Administrator: cmd (running as THM\administrator)
C:\Windows\system32>net group "Domain Admins" phillip /add /domain
The command completed successfully.

C:\Windows\system32>net user phillip /domain
User name          phillip
Full Name          Phillip
Comment
User's comment
Country/region code 000 (System Default)
Account active      Yes
Account expires     Never

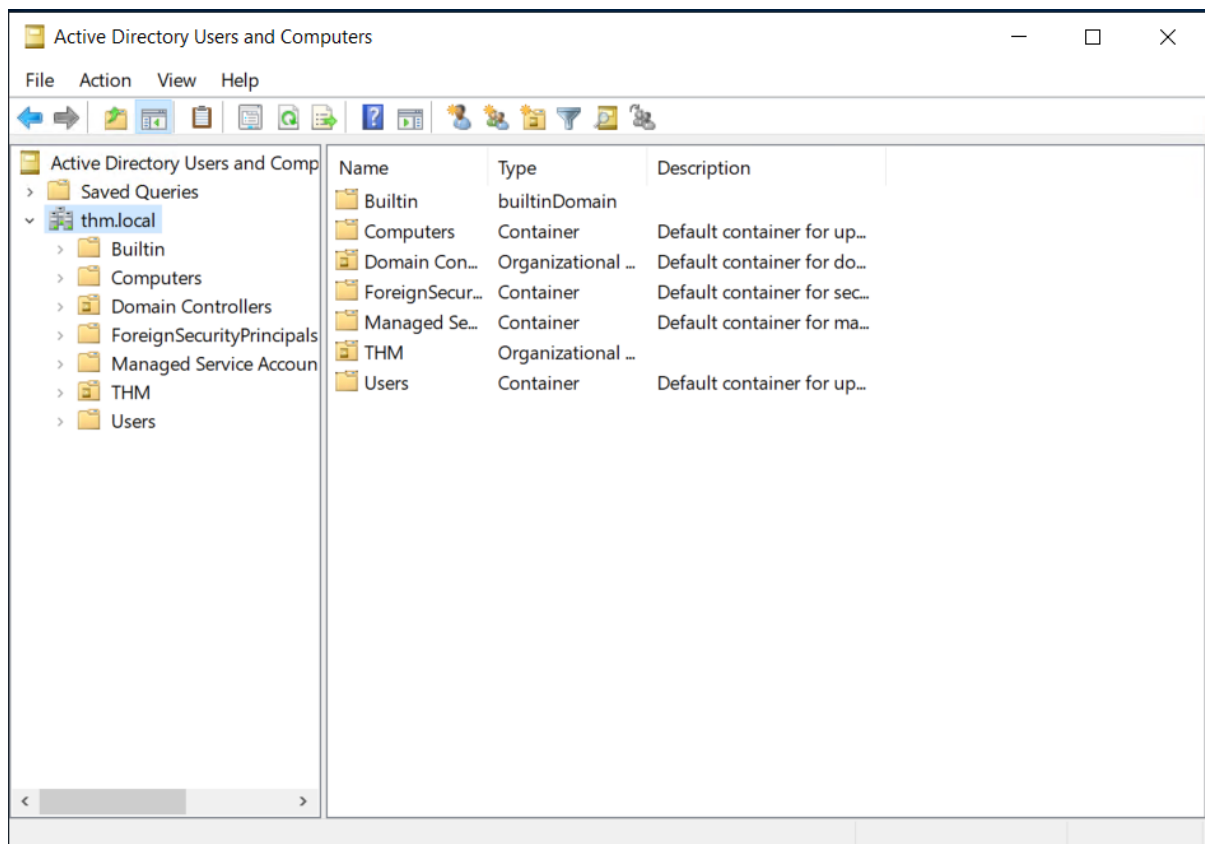
Password last set   7/11/2022 1:39:41 PM
Password expires    Never
Password changeable 7/12/2022 1:39:41 PM
Password required   Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon          9/19/2024 1:48:43 AM

Logon hours allowed All

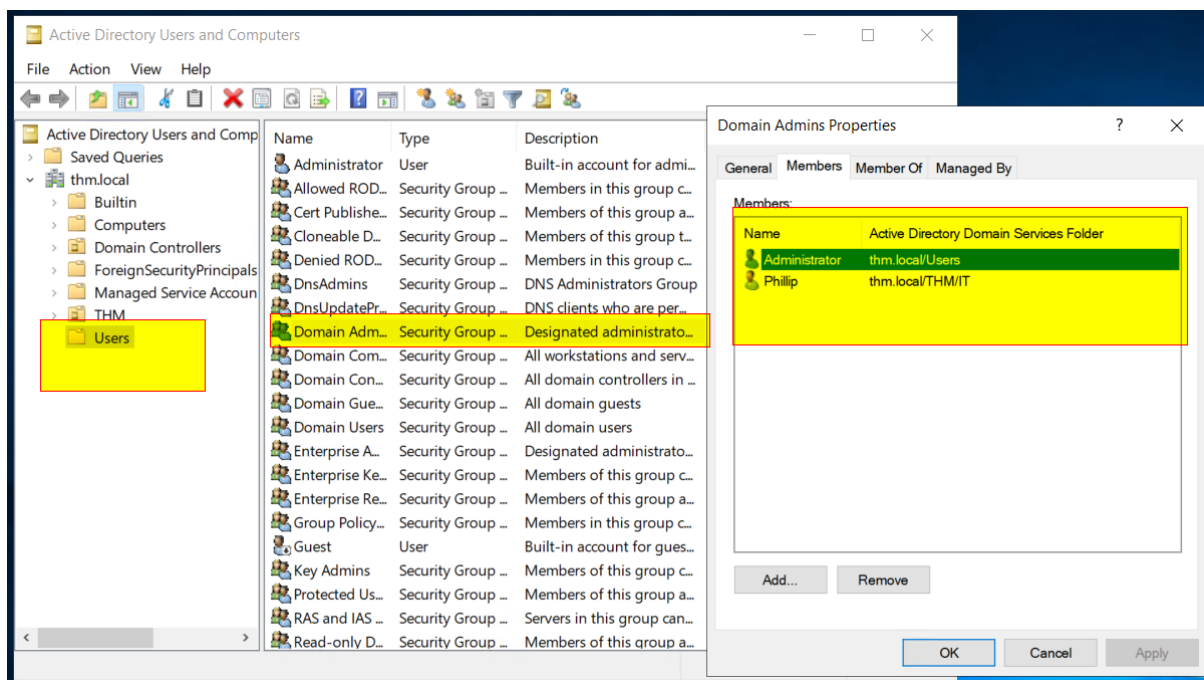
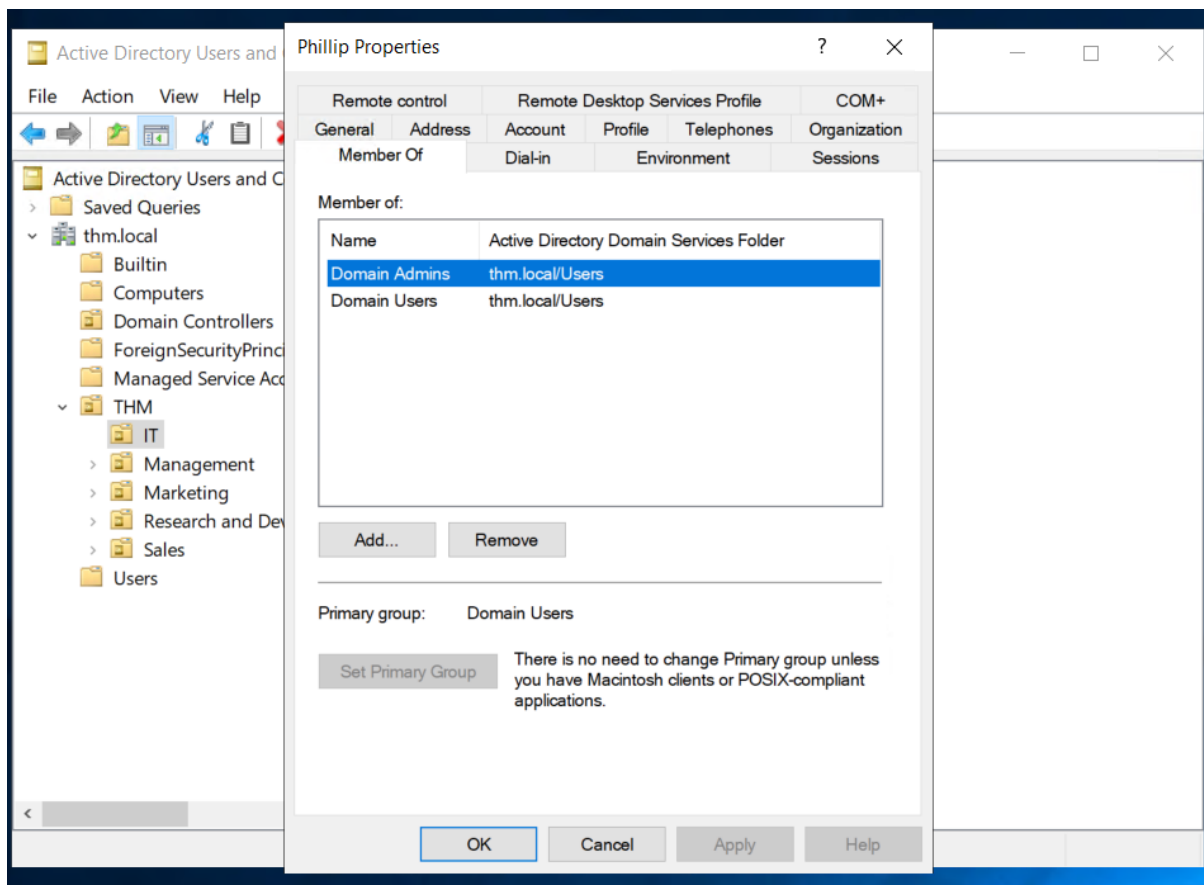
Local Group Memberships
Global Group memberships *Domain Admins *Domain Users
The command completed successfully.
```

now we can directly search for users and get to the AD DS being phillip.



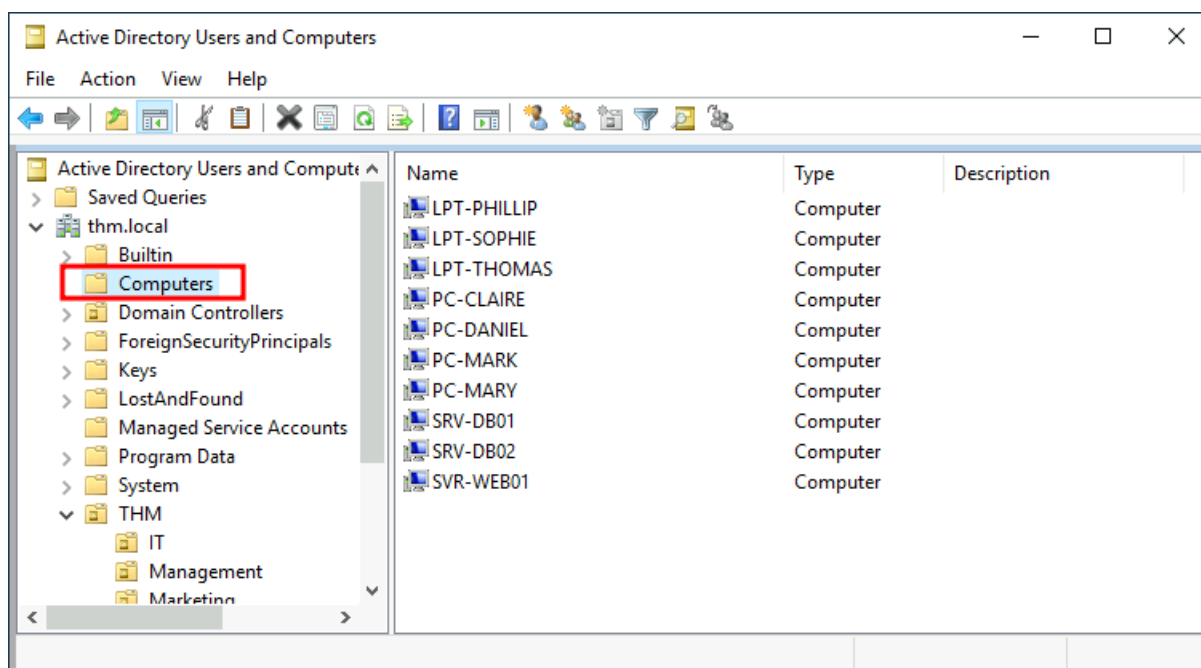
- Used run dialog box and typed dsa.msc
- entered creds of philip and we are not domain controllers





# 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.

While there is no golden rule on how to organise your machines, an excellent starting point is segregating devices according to their use. In general, you'd expect to see devices divided into at least the three following categories:

## 1. 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.

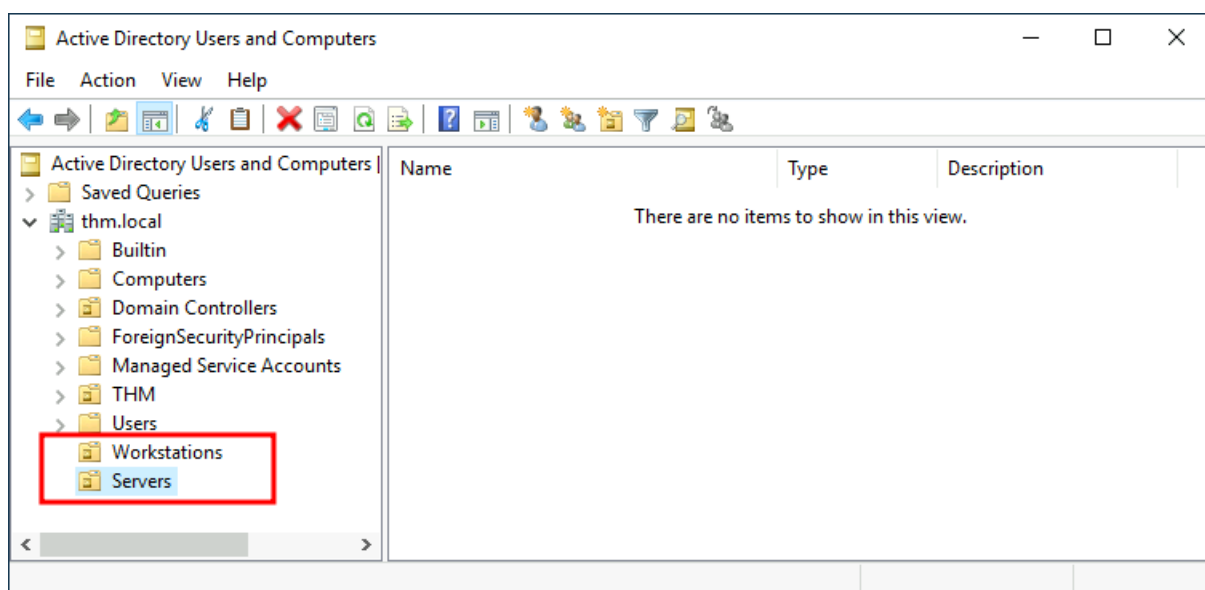
## 2. Servers

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

## 3. 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.

Since we are tidying up our AD, let's create two separate OUs for **Workstations** and **Servers** (Domain Controllers are already in an OU created by Windows). We will be creating them directly under the **thm.local** domain container. In the end, you should have the following OU structure:



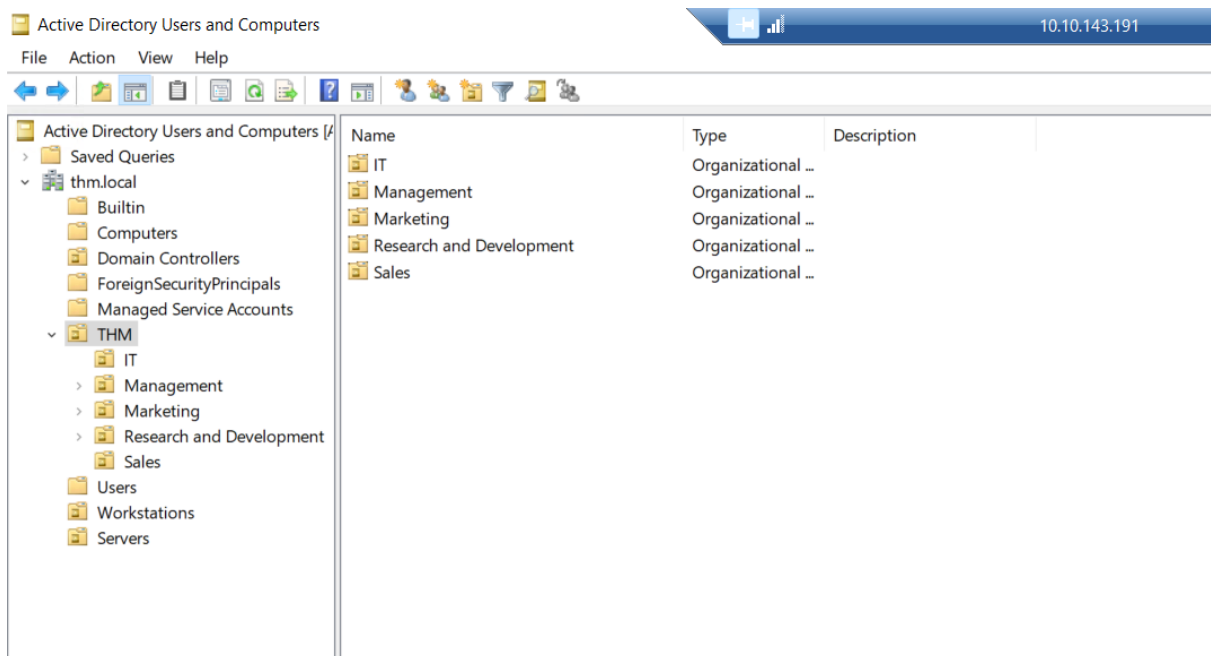
Now, move the personal computers and laptops to the Workstations OU and the servers to the Servers OU from the Computers container. Doing so will allow us to configure policies for each OU later.

Scenario: To check whether, which folder is Organisational unit and which one's container here's how we can do that

## To Confirm:

To verify if these folders are **OUs** or **Containers**:

1. Right-click on the folder (like **Users**, **Workstations**, or **Servers**).
2. Check if there is an option to **link a GPO**. If you can apply a GPO, it's an OU.
3. If it's a system container (like the default **Users** container), you won't be able to apply GPOs directly to it.



Based on the screenshot:

- **Containers:**
  - **Builtin**
  - **Computers**

- **ForeignSecurityPrincipals**
- **Managed Service Accounts**

These are default system containers, not OUs, and cannot have Group Policies applied to them.

- **Organizational Units (OUs):**
  - **IT**
  - **Management**
  - **Marketing**
  - **Research and Development**
  - **Sales**

These are custom OUs where Group Policies can be applied to manage users, groups, and computers.

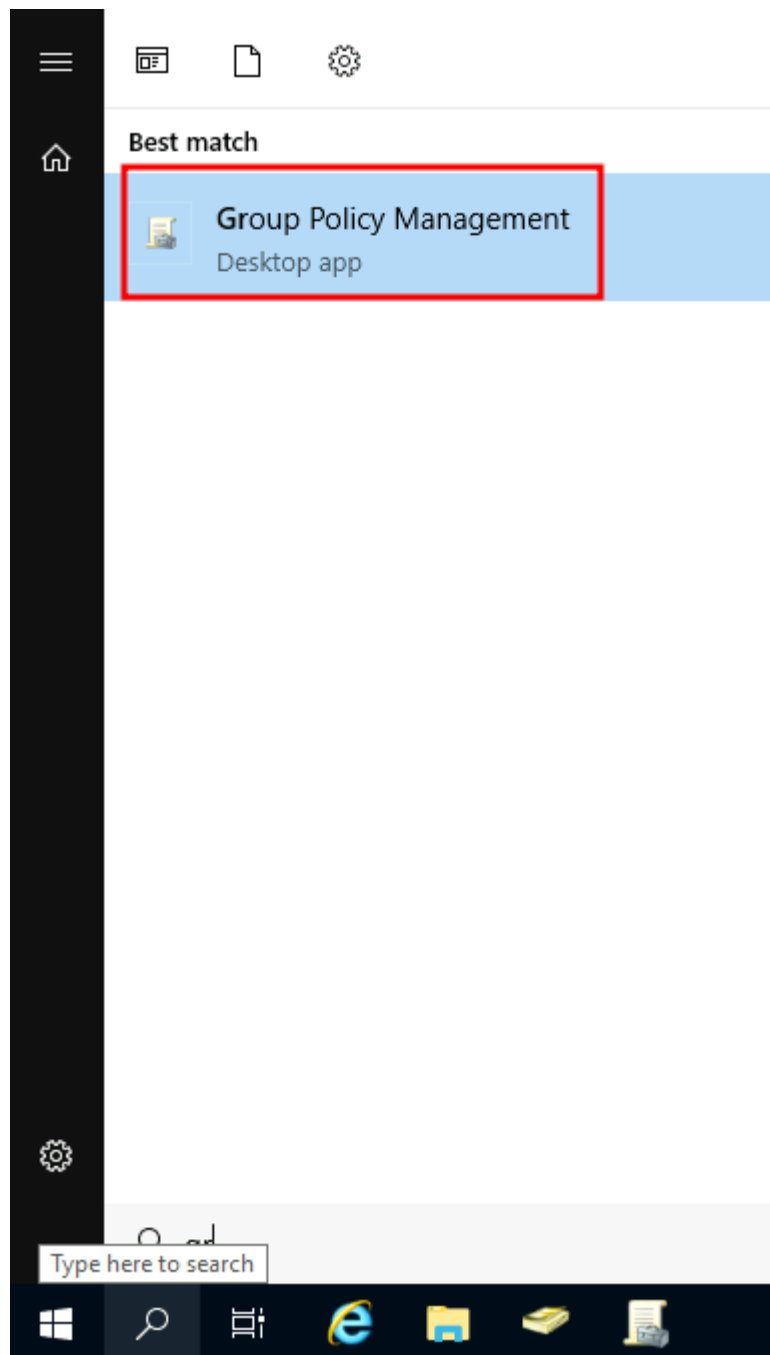
You'll need to verify whether **Users**, **Workstations**, and **Servers** are also OUs or system containers, as they could be either depending on how they were set up.

## Group Policies

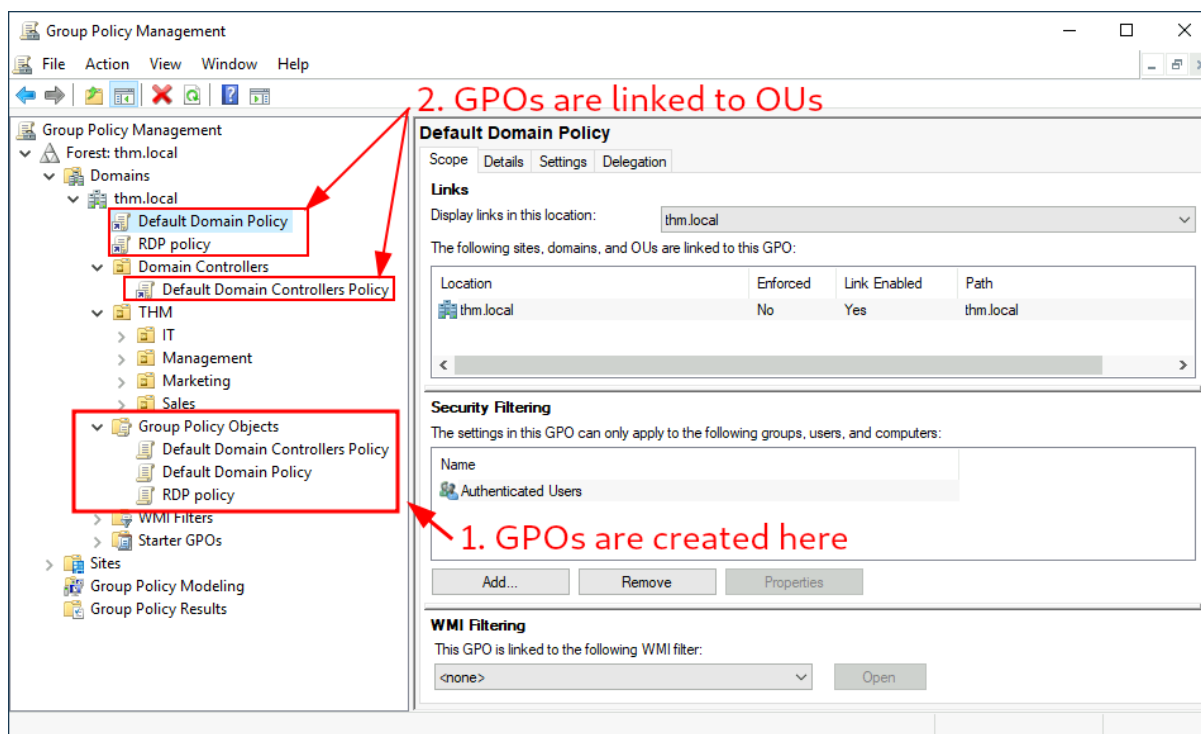
So far, we have organised users and computers in OUs just for the sake of it, but the main idea behind this is to be able to deploy different policies for each OU individually. That way, we can push different configurations and security baselines to users depending on their department.

Windows manages such policies through **Group Policy Objects (GPO)**. GPOs are simply a collection of settings that can be applied to OUs. GPOs can contain policies aimed at either users or computers, allowing you to set a baseline on specific machines and identities.

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

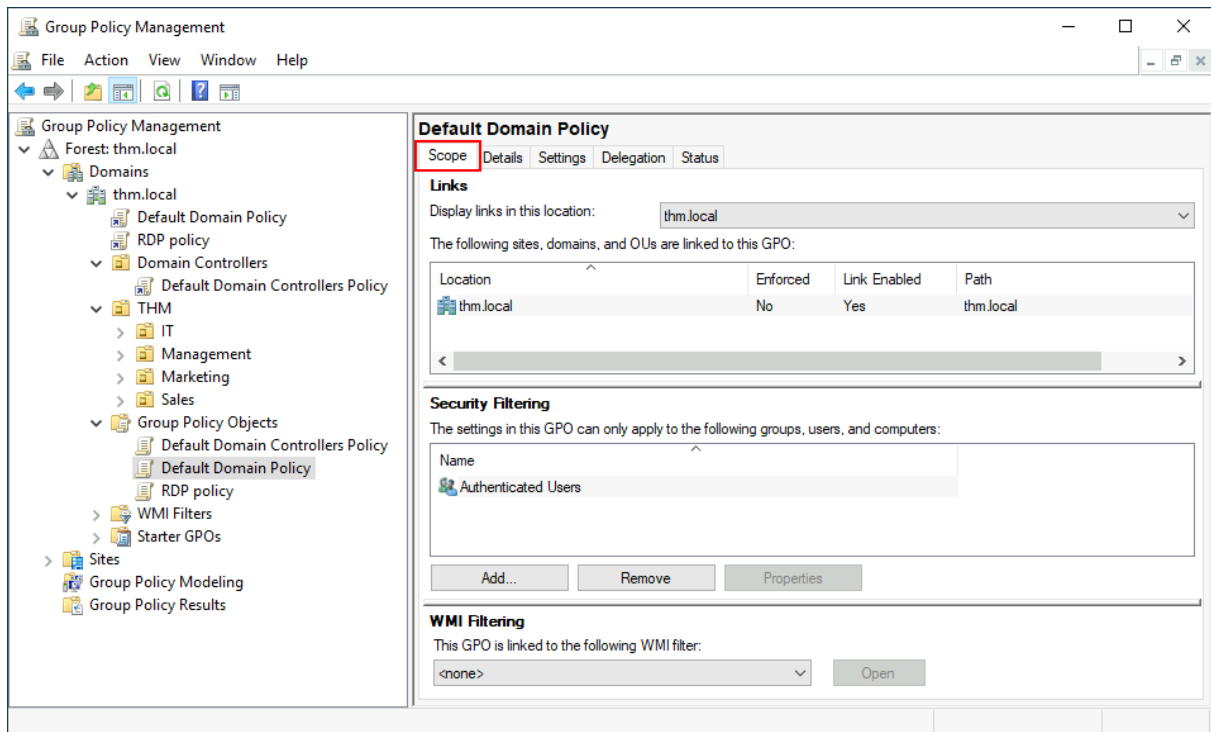


The first thing you will see when opening it is your complete OU hierarchy, as defined before. To configure Group Policies, you first create a GPO under **Group Policy Objects** and then link it to the OU where you want the policies to apply. As an example, you can see there are some already existing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

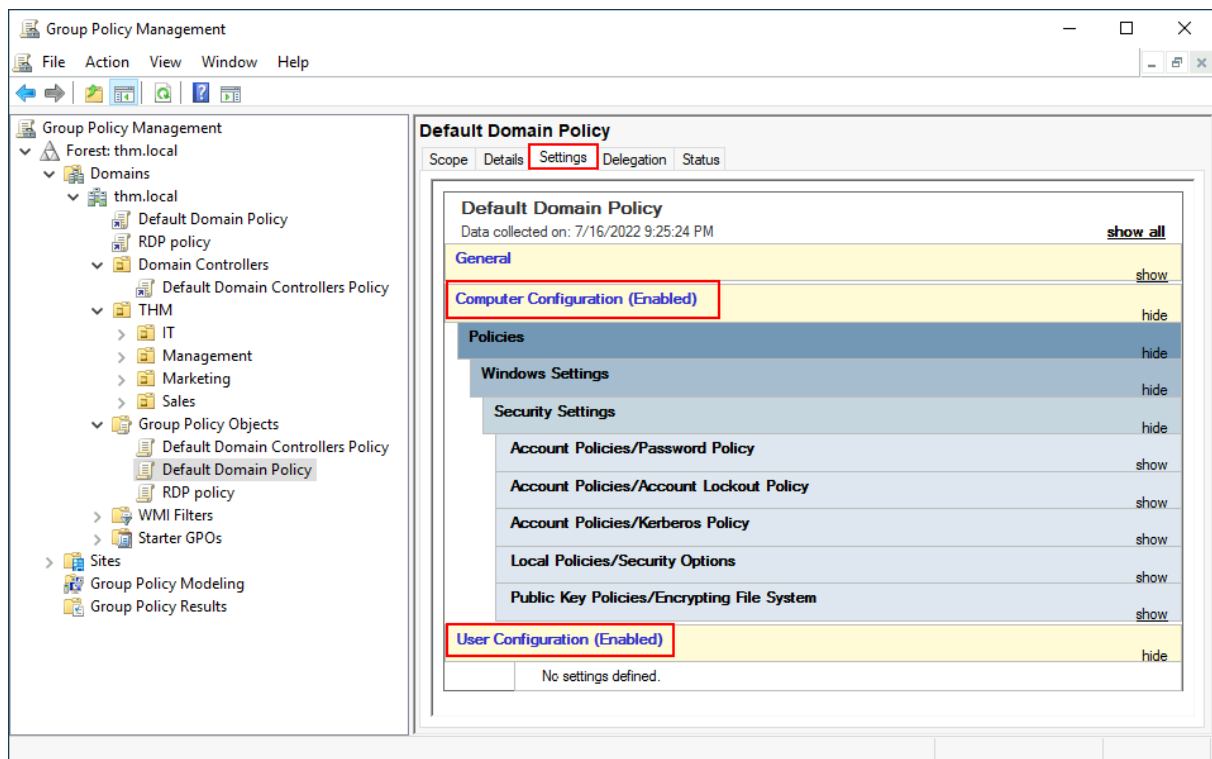
Let's examine the **Default Domain Policy** to see what's inside a GPO. The first tab you'll see when selecting a GPO shows its **scope**, which is where the GPO is linked in the AD. For the current policy, we can see that it has only been linked to the **thm.local** domain:



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:

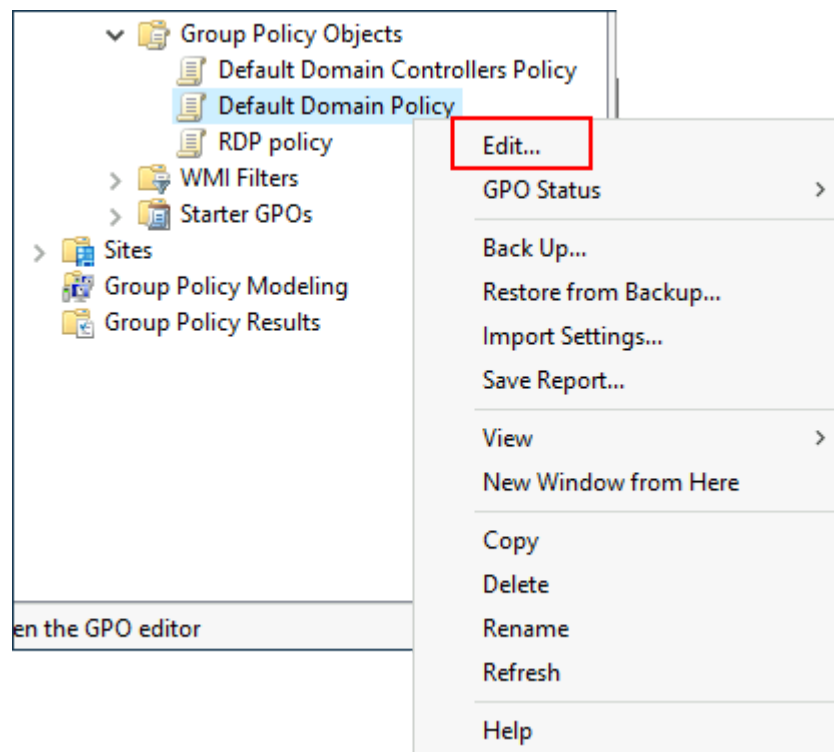




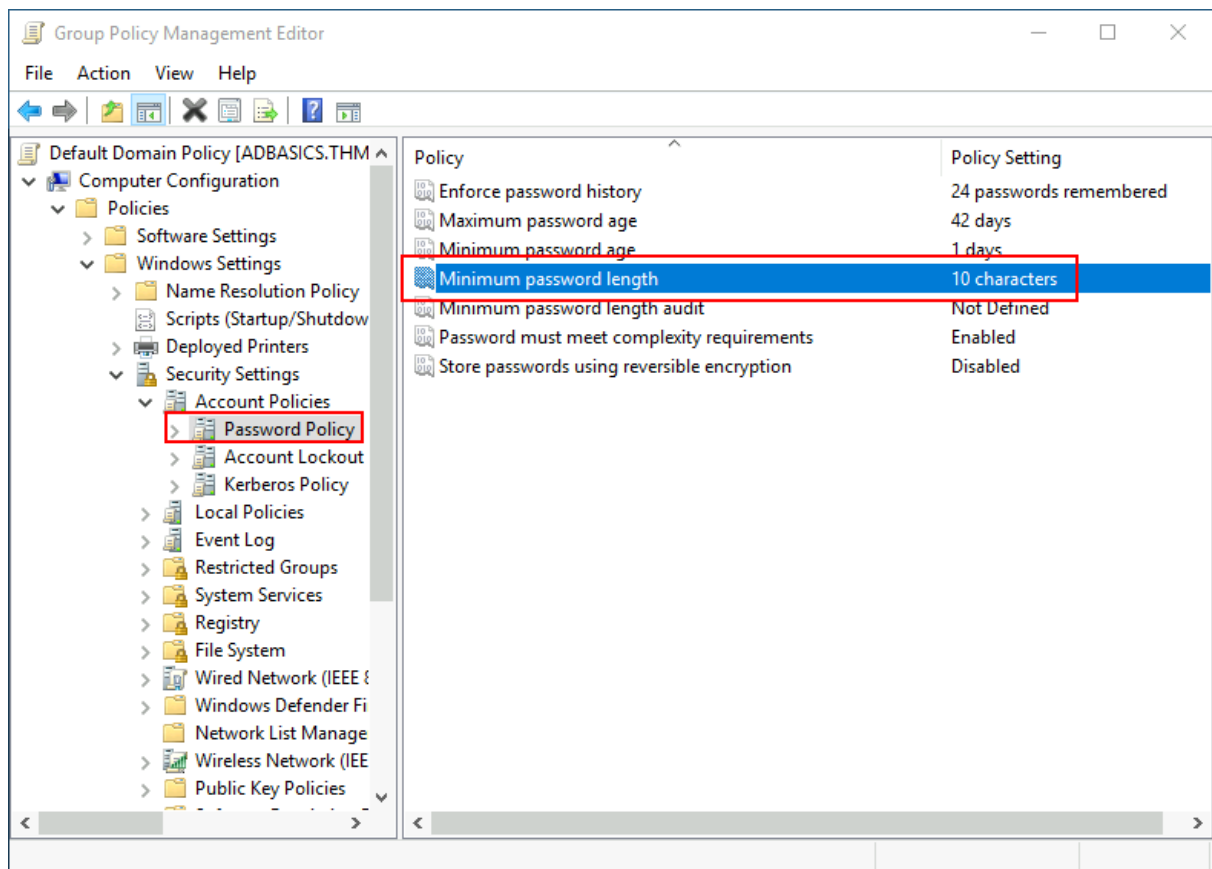
Feel free to explore the GPO and expand on the available items using the "show" links on the right side of each configuration. In this case, the **Default Domain Policy** indicates really basic configurations that should apply to most domains, including password and account lockout policies:

<b>Computer Configuration (Enabled)</b>		hide
<b>Policies</b>		hide
<b>Windows Settings</b>		hide
<b>Security Settings</b>		hide
<b>Account Policies/Password Policy</b>		hide
<b>Policy</b>	<b>Setting</b>	
Enforce password history	24 passwords remembered	
Maximum password age	42 days	
Minimum password age	1 days	
Minimum password length	7 characters	
Password must meet complexity requirements	Enabled	
Store passwords using reversible encryption	Disabled	
<b>Account Policies/Account Lockout Policy</b>		hide
<b>Policy</b>	<b>Setting</b>	
Account lockout threshold	0 invalid logon attempts	

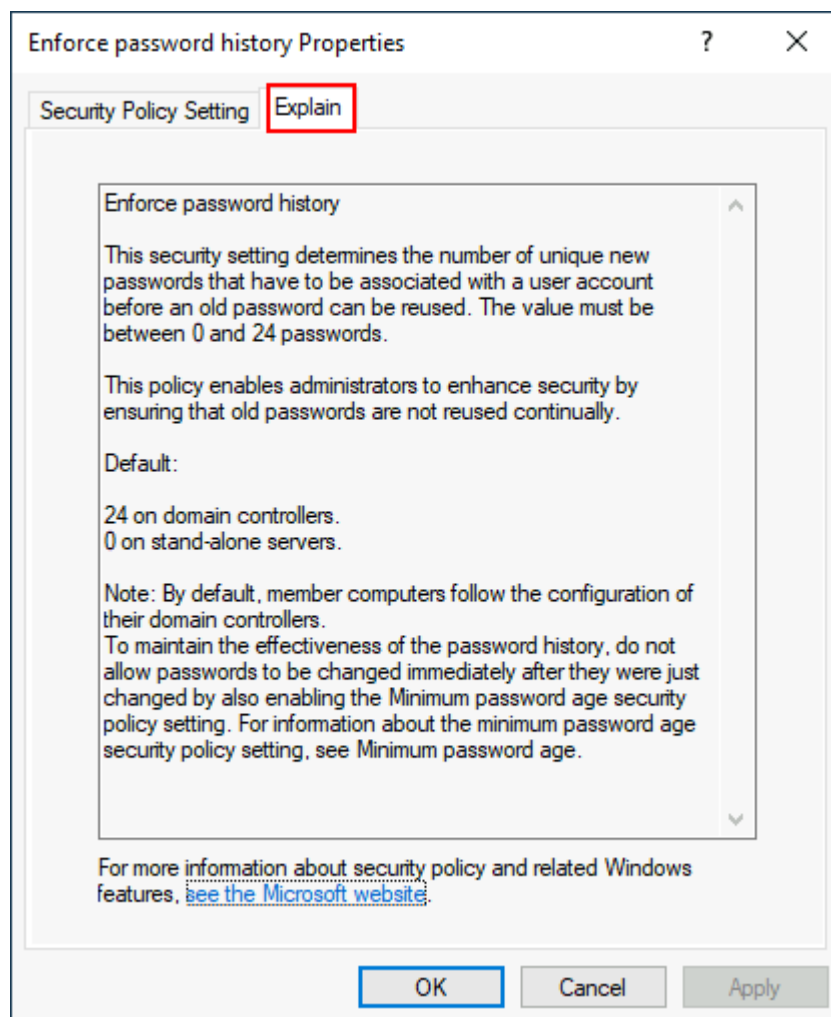
Since this GPO applies to the whole domain, any change to it would affect all computers. Let's change the minimum password length policy to require users to have at least 10 characters in their passwords. To do this, right-click the GPO and select **Edit**:



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:



As you can see, plenty of policies can be established in a GPO. While explaining every single of them would be impossible in a single room, do feel free to explore a bit, as some of the policies are straightforward. If more information on any of the policies is needed, you can double-click them and read the **Explain** tab on each of them:



## 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:

WindowsPowerShell

```
PS C:\> gpupdate /force
```

# Creating some GPOs for THM Inc.

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

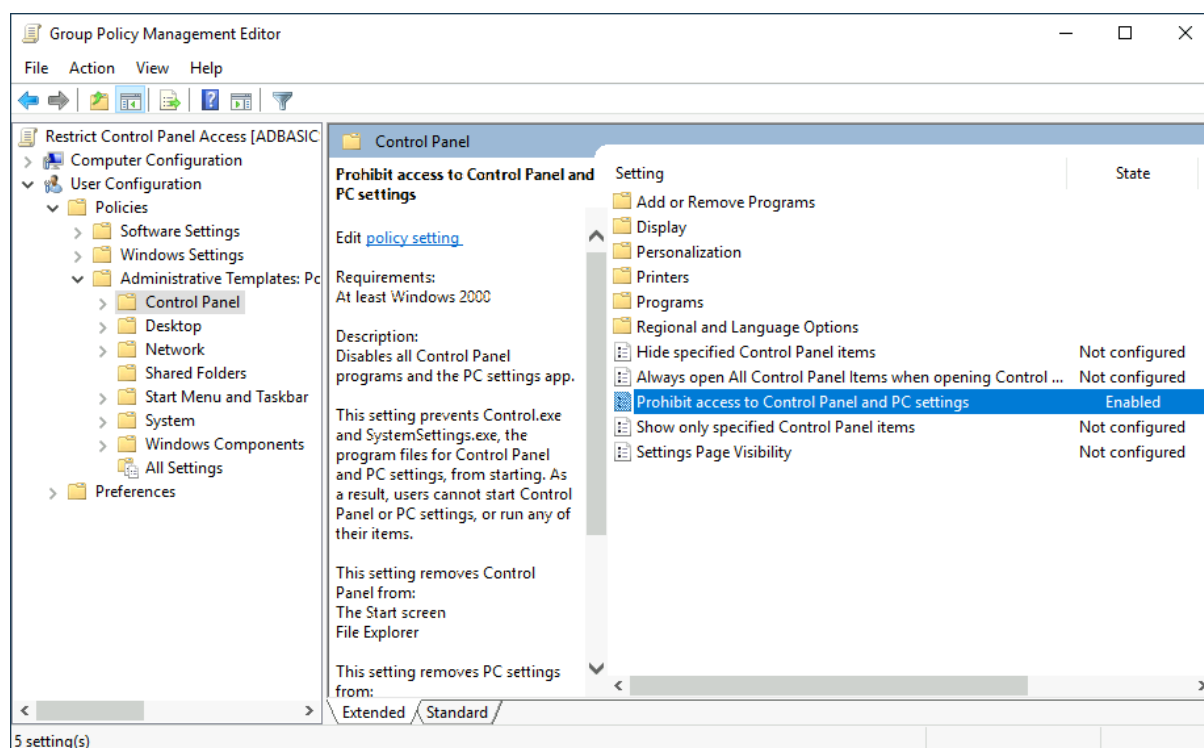
1. Block non-IT users from accessing the Control Panel.
2. Make workstations and servers lock their screen automatically after 5 minutes of user inactivity to avoid people leaving their sessions exposed.

Let's focus on each of those and define what policies we should enable in each GPO and where they should be linked.

## ***Restrict Access to Control Panel***

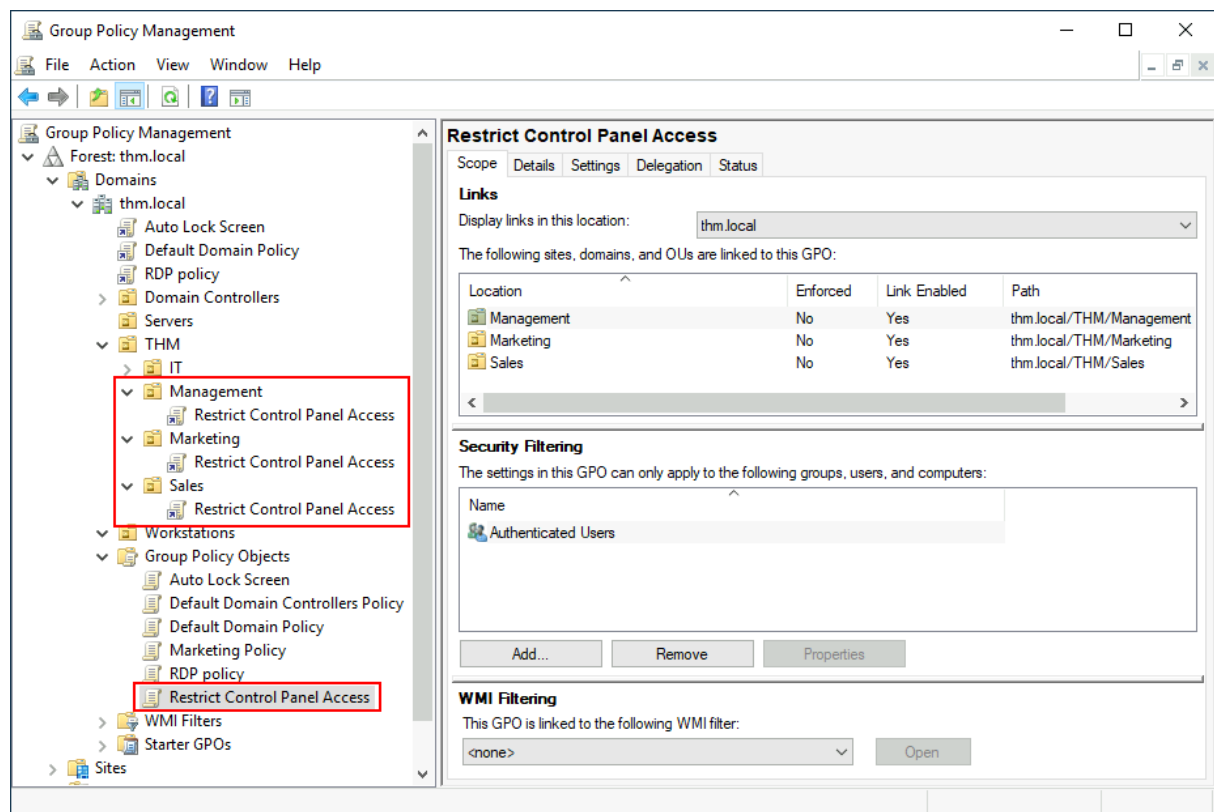
We want to restrict access to the Control Panel across all machines to only the users that are part of the IT department. Users of other departments shouldn't be able to change the system's preferences.

Let's create a new GPO called **Restrict Control Panel Access** and open it for editing. Since we want this GPO to apply to specific users, we will look under **User Configuration** for the following policy:



Notice we have enabled the **Prohibit Access to Control Panel and PC settings** policy.

Once the GPO is configured, we will need to link it to all of the OUs corresponding to users who shouldn't have access to the Control Panel of their PCs. In this case, we will link the **Marketing** , **Management** and **Sales** OUs by dragging the GPO to each of them:



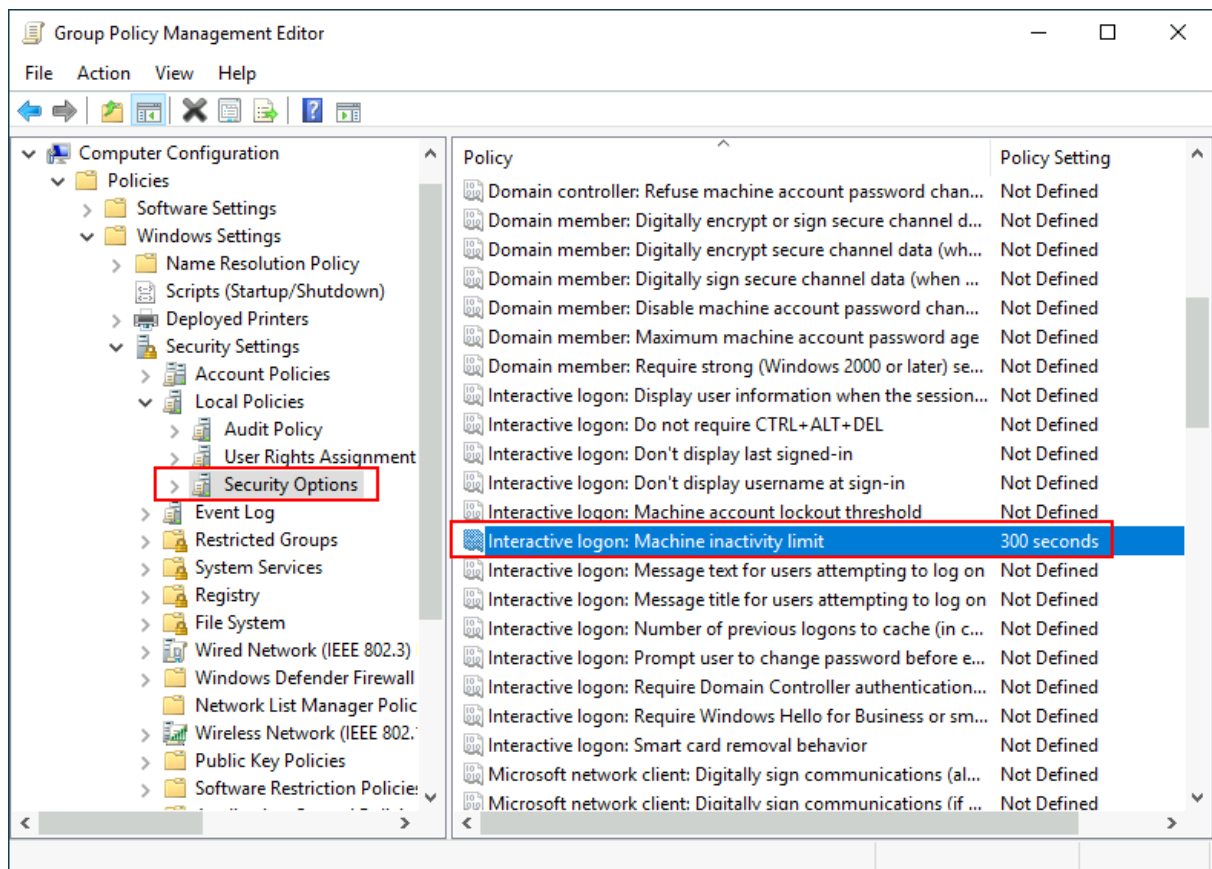
## Auto Lock Screen GPO

For the first GPO, regarding screen locking for workstations and servers, we could directly apply it over the **Workstations** , **Servers** and **Domain Controllers** OUs we created previously.

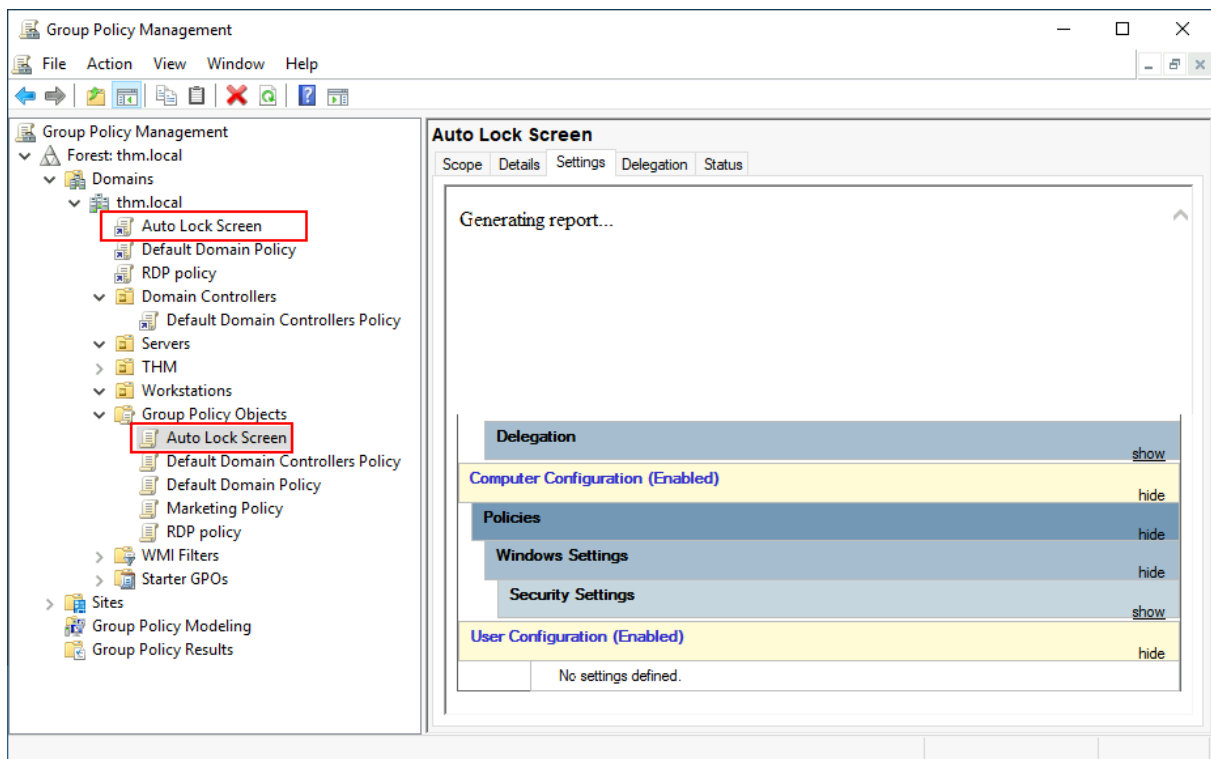
While this solution should work, an alternative consists of simply applying the GPO to the root domain, as we want the GPO to affect all of our computers. Since the **Workstations** , **Servers** and **Domain Controllers** OUs are all child OUs of the root domain, they will inherit its policies.

**Note:** You might notice that if our GPO is applied to the root domain, it will also be inherited by other OUs like **Sales** or **Marketing** . Since these OUs contain users only, any Computer Configuration in our GPO will be ignored by them.

Let's create a new GPO, call it **Auto Lock Screen** , and edit it. The policy to achieve what we want is located in the following route:



We will set the inactivity limit to 5 minutes so that computers get locked automatically if any user leaves their session open. After closing the GPO editor, we will link the GPO to the root domain by dragging the GPO to it:



Once the GPOs have been applied to the correct OUs, we can log in as any users in either Marketing, Sales or Management for verification. For this task, let's connect via RDP using Mark's credentials:



<b>Username</b>	Mark
<b>Password</b>	M4rk3t1ng.21

Note: When connecting via RDP, use `THM\Mark` as the username to specify you want to log in using the user `Mark` on the `THM` domain.

If we try opening the Control Panel, we should get a message indicating this operation is denied by the administrator. You can also wait 5 minutes to check if the screen is automatically locked if you want.

Since we didn't apply the control panel GPO on IT, you should still be able to log into the machine as any of those users and access the control panel.



**Note:** If you created and linked the GPOs, but for some reason, they still don't work, remember you can run `gpupdate /force` to force GPOs to be updated.

## Authentication Methods

When using Windows domains, all credentials are stored in the Domain Controllers. Whenever a user tries to authenticate to a service using domain credentials, the service will need to ask the Domain Controller to verify if they are correct. Two protocols can be used for network authentication in windows domains:

- **Kerberos:** Used by any recent version of Windows. This is the default protocol in any recent domain.
- **NetNTLM:** Legacy authentication protocol kept for compatibility purposes.

While NetNTLM should be considered obsolete, most networks will have both protocols enabled. Let's take a deeper look at how each of these protocols works.

## Kerberos Authentication

Kerberos authentication is the default authentication protocol for any recent version of Windows. Users who log into a service using Kerberos will be assigned tickets. Think of tickets as proof of a previous authentication. Users with tickets can present them to a service to demonstrate they have already authenticated into the network before and are therefore enabled to use it.

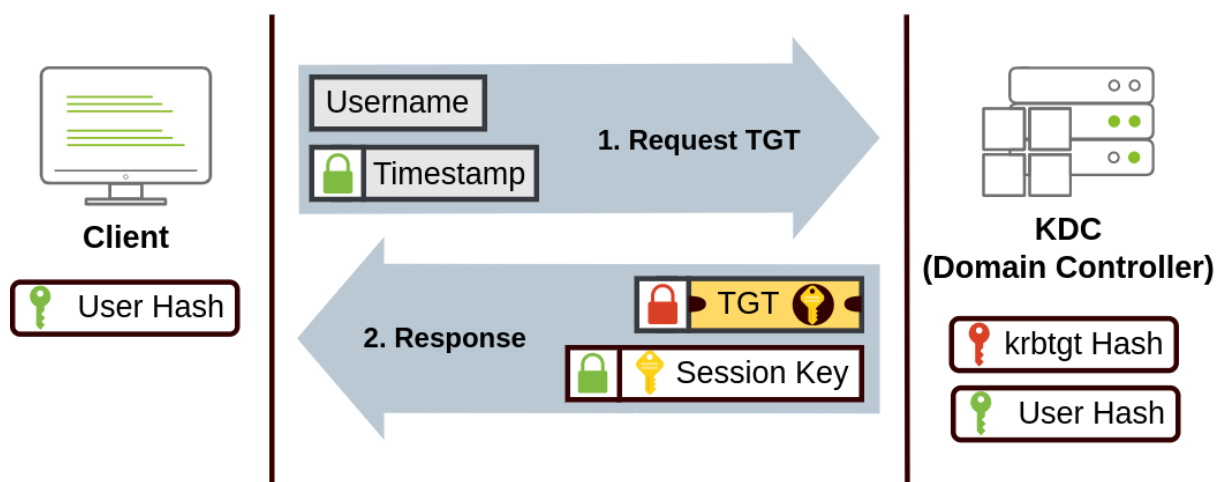
When Kerberos is used for authentication, the following process happens:

1. The user sends their username and a timestamp encrypted using a key derived from their password to the **Key Distribution Center (KDC)**, a service usually installed on the Domain Controller in charge of creating Kerberos tickets on the network.

The KDC will create and send back a **Ticket Granting Ticket (TGT)**, which will allow the user to request additional tickets to access specific services.

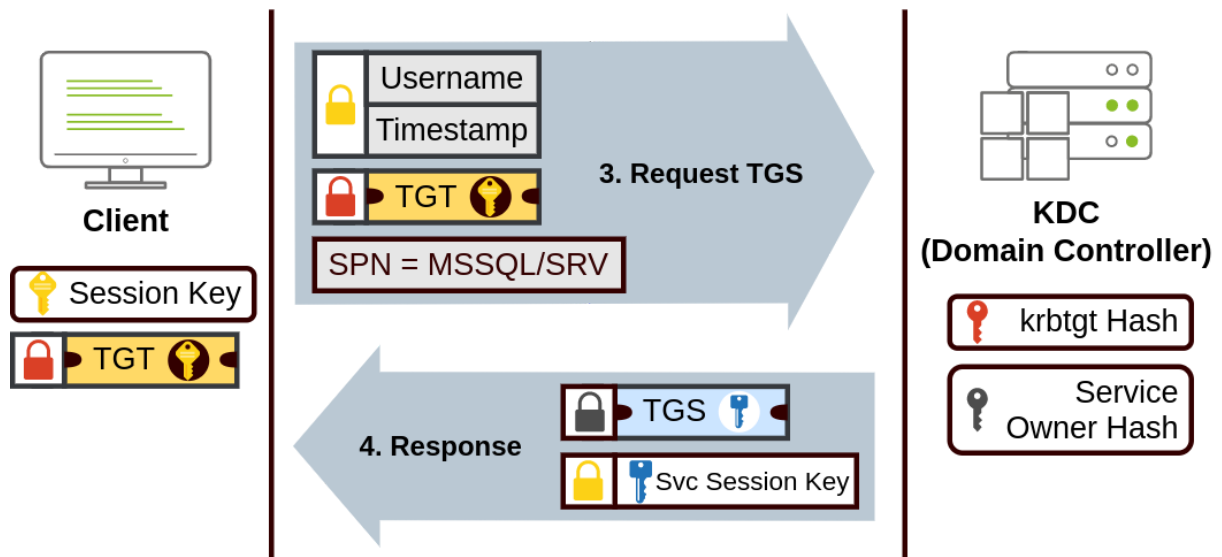
The need for a ticket to get more tickets may sound a bit weird, but it allows users to request service tickets without passing their credentials every time they want to connect to a service. Along with the TGT, a **Session Key** is given to the user, which they will need to generate the following requests.

Notice the TGT is encrypted using the **krbtgt** account's password hash, and therefore the user can't access its contents. It is essential to know that the encrypted TGT includes a copy of the Session Key as part of its contents, and the KDC has no need to store the Session Key as it can recover a copy by decrypting the TGT if needed.

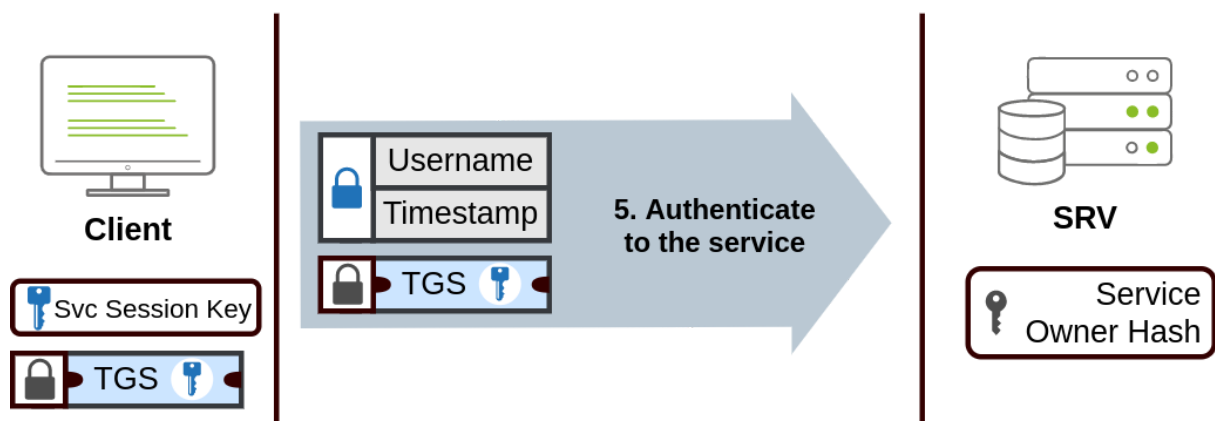


1. When a user wants to connect to a service on the network like a share, website or database, they will use their TGT to ask the KDC for a **Ticket Granting Service (TGS)**. TGS are tickets that allow connection only to the specific service they were created for. To request a TGS, the user will send their username and a timestamp encrypted using the Session Key, along with the TGT and a **Service Principal Name (SPN)**, which indicates the service and server name we intend to access.

As a result, the KDC will send us a TGS along with a **Service Session Key**, which we will need to authenticate to the service we want to access. The TGS is encrypted using a key derived from the **Service Owner Hash**. The Service Owner is the user or machine account that the service runs under. The TGS contains a copy of the Service Session Key on its encrypted contents so that the Service Owner can access it by decrypting the TGS.

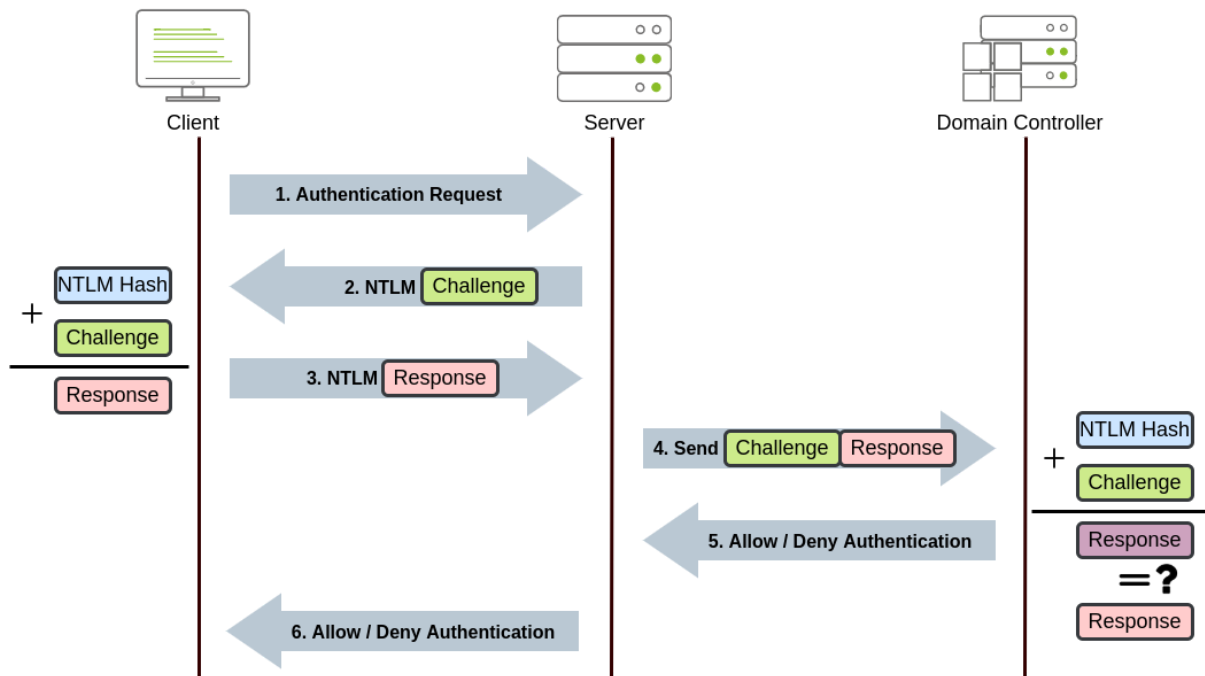


1. The TGS can then be sent to the desired service to authenticate and establish a connection. The service will use its configured account's password hash to decrypt the TGS and validate the Service Session Key.



## NetNTLM Authentication

NetNTLM works using a challenge-response mechanism. The entire process is as follows:



1. The client sends an authentication request to the server they want to access.
2. The server generates a random number and sends it as a challenge to the client.
3. The client combines their NTLM password hash with the challenge (and other known data) to generate a response to the challenge and sends it back to the server for verification.
4. The server forwards the challenge and the response to the Domain Controller for verification.
5. The domain controller uses the challenge to recalculate the response and compares it to the original response sent by the client. If they both match, the client is authenticated; otherwise, access is denied. The authentication result is sent back to the server.
6. The server forwards the authentication result to the client.

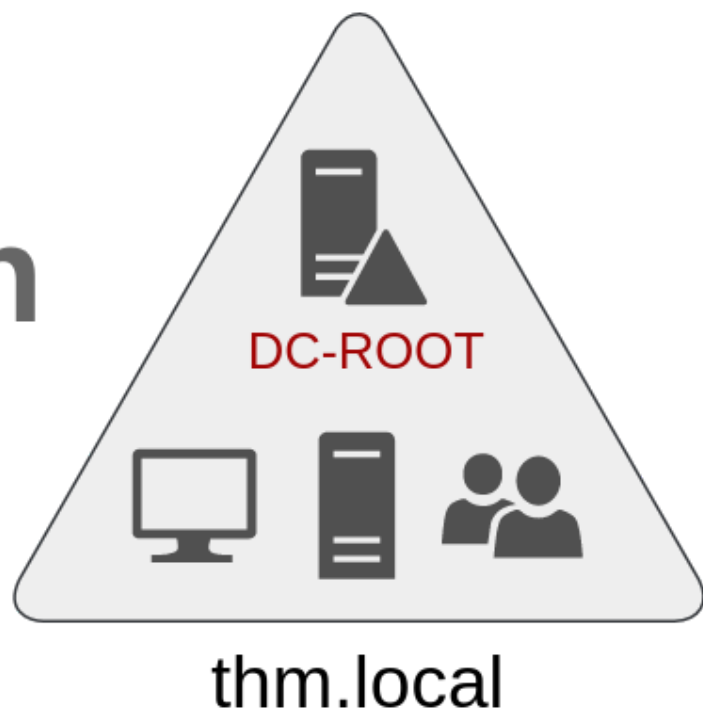
Note that the user's password (or hash) is never transmitted through the network for security.

**Note:** The described process applies when using a domain account. If a local account is used, the server can verify the response to the challenge itself without requiring interaction with the domain controller since it has the password hash stored locally on its SAM.

# Trees & Forests

So far, we have discussed how to manage a single domain, the role of a Domain Controller and how it joins computers, servers and users.

# Domain



As companies grow, so do their networks. Having a single domain for a company is good enough to start, but in time some additional needs might push you into having more than one.

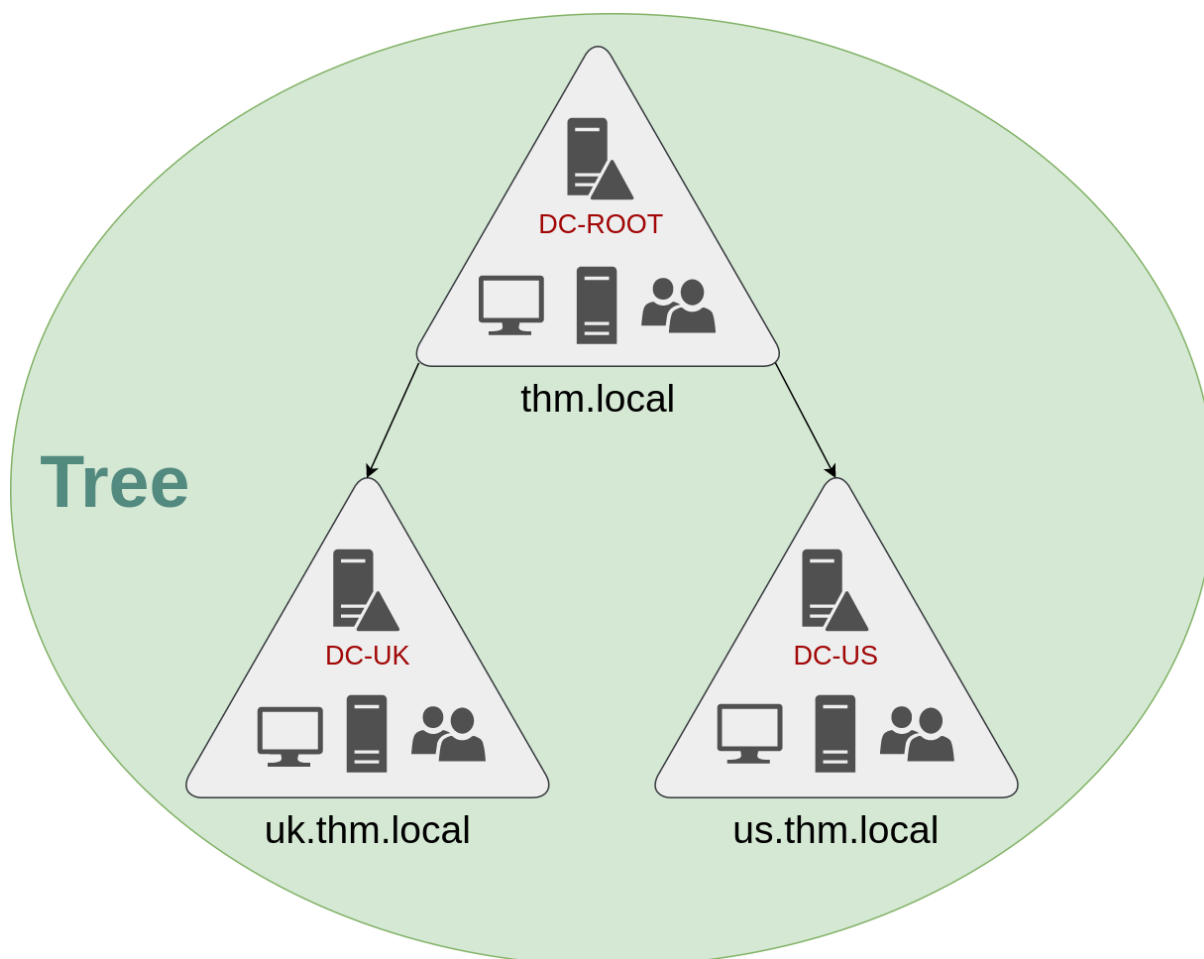
## Trees

Imagine, for example, that suddenly your company expands to a new country. The new country has different laws and regulations that require you to update your GPOs to comply. In addition, you now have IT people in both countries, and each IT team needs to manage the resources that correspond to each country without interfering with the other team. While you could create a

complex OU structure and use delegations to achieve this, having a huge AD structure might be hard to manage and prone to human errors.

Luckily for us, Active Directory supports integrating multiple domains so that you can partition your network into units that can be managed independently. If you have two domains that share the same namespace ( `thm.local` in our example), those domains can be joined into a **Tree**.

If our `thm.local` domain was split into two subdomains for UK and US branches, you could build a tree with a root domain of `thm.local` and two subdomains called `uk.thm.local` and `us.thm.local`, each with its AD, computers and users:

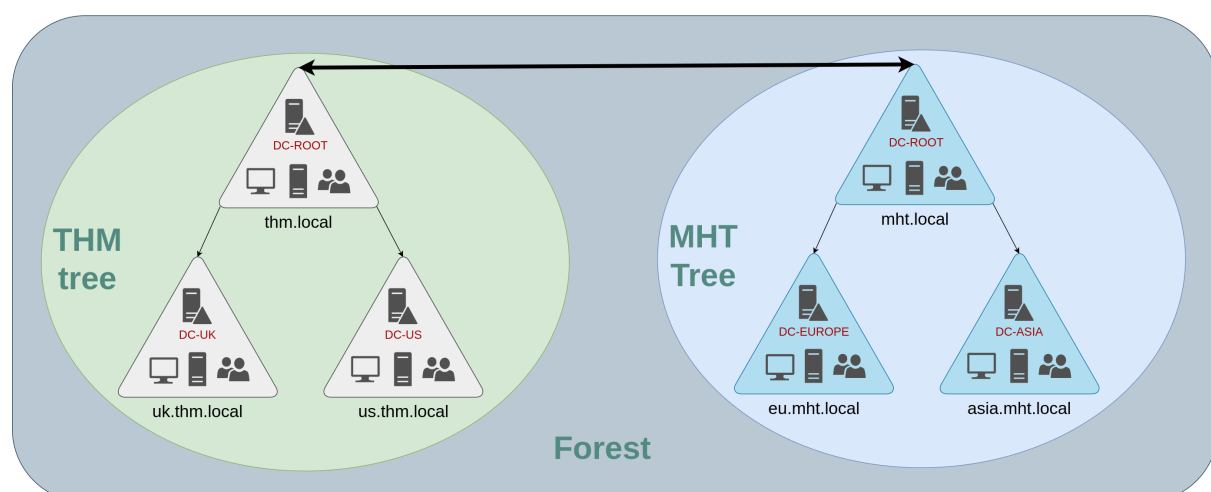


This partitioned structure gives us better control over who can access what in the domain. The IT people from the UK will have their own DC that manages the UK resources only. For example, a UK user would not be able to manage US users. In that way, the Domain Administrators of each branch will have complete control over their respective DCs, but not other branches' DCs. Policies can also be configured independently for each domain in the tree.

A new security group needs to be introduced when talking about trees and forests. The **Enterprise Admins** group will grant a user administrative privileges over all of an enterprise's domains. Each domain would still have its Domain Admins with administrator privileges over their single domains and the Enterprise Admins who can control everything in the enterprise.

## Forests

The domains you manage can also be configured in different namespaces. Suppose your company continues growing and eventually acquires another company called **MHT Inc.** When both companies merge, you will probably have different domain trees for each company, each managed by its own IT department. The union of several trees with different namespaces into the same network is known as a **forest**.



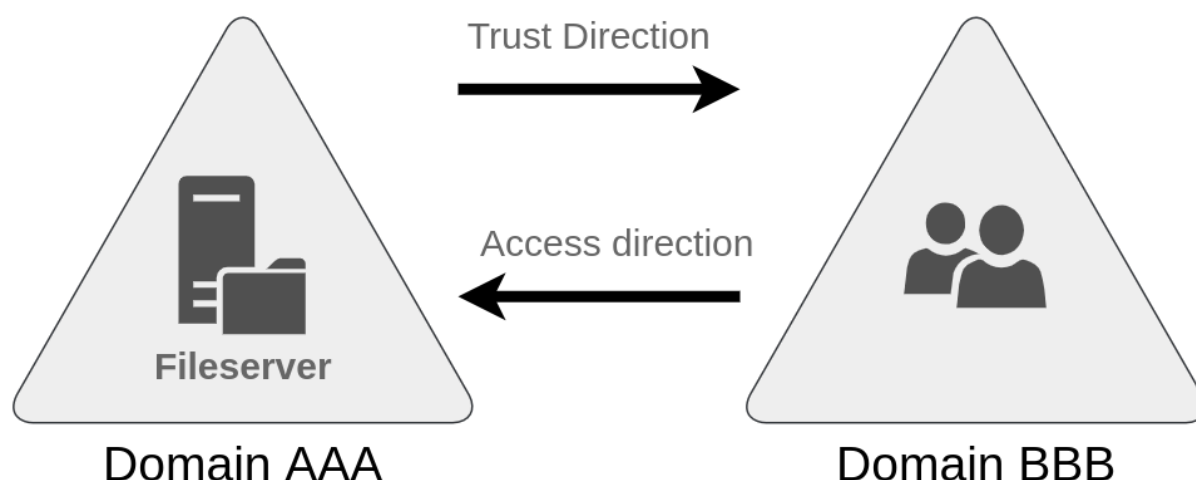
## Trust Relationships

Having multiple domains organised in trees and forest allows you to have a nice compartmentalised network in terms of management and resources. But at a certain point, a user at THM UK might need to access a shared file in one of MHT ASIA servers. For this to happen, domains arranged in trees and forests are joined together by **trust relationships**.

In simple terms, having a trust relationship between domains allows you to authorise a user from domain **THM UK** to access resources from domain **MHT EU**.

The simplest trust relationship that can be established is a **one-way trust relationship**. In a one-way trust, if **Domain AAA** trusts **Domain BBB**, this means that a

user on BBB can be authorised to access resources on AAA:



The direction of the one-way trust relationship is contrary to that of the access direction.

**Two-way trust relationships** can also be made to allow both domains to mutually authorise users from the other. By default, joining several domains under a tree or a forest will form a two-way trust relationship.

It is important to note that having a trust relationship between domains doesn't automatically grant access to all resources on other domains. Once a trust relationship is established, you have the chance to authorise users across different domains, but it's up to you what is actually authorised or not.

## Conclusion:

In this room, we have shown the basic components and concepts related to Active Directories and Windows Domains. Keep in mind that this room should only serve as an introduction to the basic concepts, as there's quite a bit more to explore to implement a production-ready Active Directory environment.

If you are interested in learning how to secure an Active Directory installation, be sure to check out the Active Directory Hardening Room (To be released soon). If, on the other hand, you'd like to know how attackers can take advantage of common AD misconfigurations and other AD hacking techniques, the [Compromising Active Directory module](#) is the way to go.



Breaching Active Directory.

Hacking Active Directory for Beginners (TCM Security).

Octoer

25th Sept 2024

Oct 2 2024

Oct 9th

October 16 - Web

October 19th

Active Directory Certificate Services.

MS-EVEN Forced Authentication Attack Path.