

Active Directory Structure Expansion

Part 3: Active Directory Expansion and Management



1 Active Directory Blueprint	3
1.1 Introduction	3
1.2 The blueprint	3
1.2.1 Blueprint for Users	4
1.2.2 Blueprint for Computers	5
1.2.3 Blueprint for Groups	6
1.2.4 Blueprint for ServiceAccounts	7
1.2.5 Blueprint for Projects	8
1.2.6 Blueprint for Administrators	8
2. Expanding the Active Directory	9
2.1 PowerShell Script	9
3.1 Users OU	12
3.1.1 Regions	12
3.1.1.1 Sales	12
3.1.1.2 HR	13
3.1.1.3 IT	13
3.1.2 Final Structure	14
3.2 Computers OU	14
3.3 Groups OU	15
3.3.1 Security Groups	15
3.3.2 Distribution Groups	16
3.3.3 Printers	16
3.4 ServiceAccounts OU	17
3.5 Projects OU	17
3.5.1 Completed	17
3.5.2 Active	18
3.6 Administrators OU	18

4 Setting up All Objects	19
4.1 Setting up Objects in Administrator	19
4.2 Setting up Objects in Company Computers	21
4.3 Setting up Objects in Company Users	23
4.4 Setting up Objects in Groups	23
4.4.1 Group Domains	25
4.5 Setting up Objects in Projects	27
4.6 Setting up Objects in Service Accounts	28
5 Active Directory Management	32
5.1 Finding Objects	32
5.2 Password Reset	33
5.3 Editing User Profiles	35
5.4 Moving Objects to Different OU	37
5.5 Advanced View Features	38
5.6 Asset Reviews	40
5.7 Onboarding / Offboarding Users	41
6 Conclusion	43

1 Active Directory Blueprint

1.1 Introduction

Expanding our home-lab Active Directory (AD) to a more business-level structure will provide valuable insights into real-world IT management and operations. This enhancement aims to deepen our understanding of key AD components and processes, preparing us for more complex, enterprise environments.

1. **Organisational Units (OUs):** Structuring OUs will help us manage and delegate administrative tasks efficiently, replicating the organisational hierarchy of a business.
2. **Groups:** Implementing various Security and Distribution Groups will improve our grasp of user permissions, access control, and communication strategies within a business context.
3. **Contacts:** Adding external contacts will teach us how to manage interactions with non-domain entities, such as vendors and partners.
4. **Printers:** Integrating printers into the AD structure will demonstrate how to manage and deploy network printers in a business environment.
5. **Users and Service Accounts:** Expanding user and service account management will provide insights into handling diverse user roles and services across an organisation.
6. **Onboarding and Offboarding Processes:** Setting up these processes will help us understand how to efficiently integrate and remove employees, ensuring smooth transitions and maintaining security.

By refining our AD setup, we will gain practical experience with enterprise-level practices and enhance our skills in managing a business-grade IT environment.

1.2 The blueprint

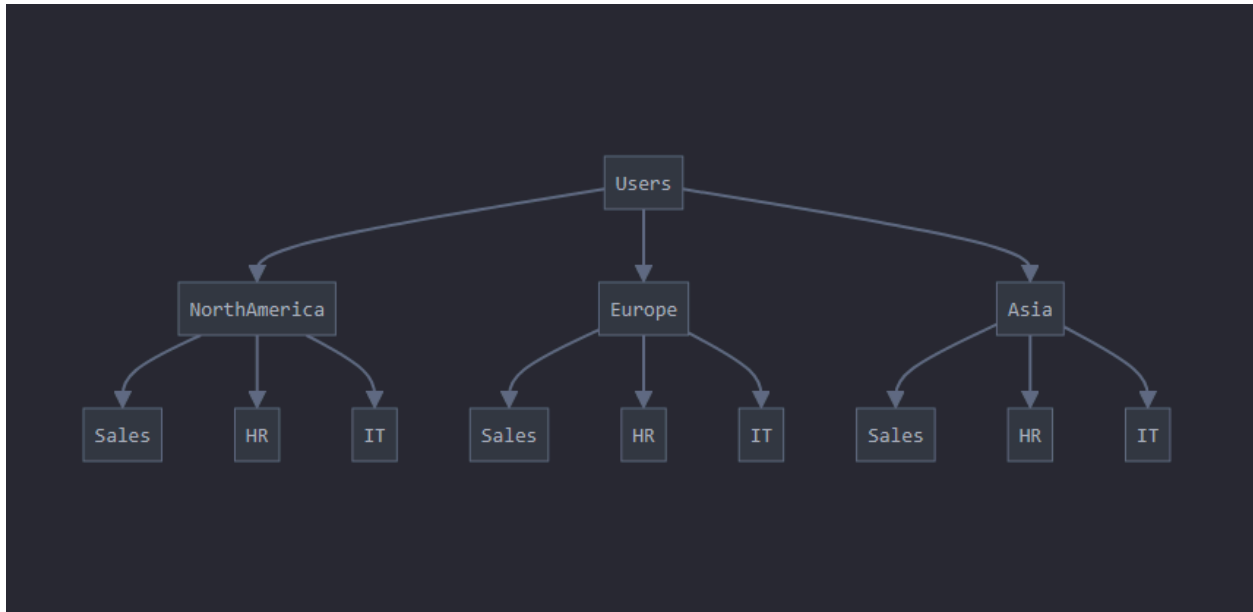
The blueprint will have several organisational units. The primary OU's will be as follows

- Users
- Computers
- Groups
- ServiceAccounts
- Projects
- Administrators

The root of our Active Directory (AD) structure will be "ActiveDomain.com". While changing this name would be ideal, the complexities involved mean we will retain the current name.

The structure will be organised into primary Organisational Units (OUs), each further subdivided to reflect various components of our AD. Below are the blueprints for the primary OUs.

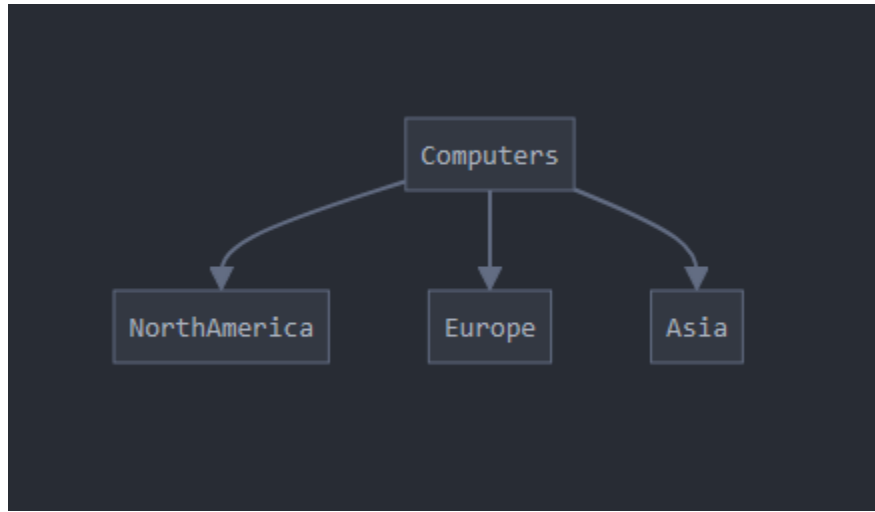
1.2.1 Blueprint for Users



Users

- NorthAmerica
 - Sales
 - HR
 - IT
- Europe
 - Sales
 - HR
 - IT
- Asia
 - Sales
 - HR
 - IT

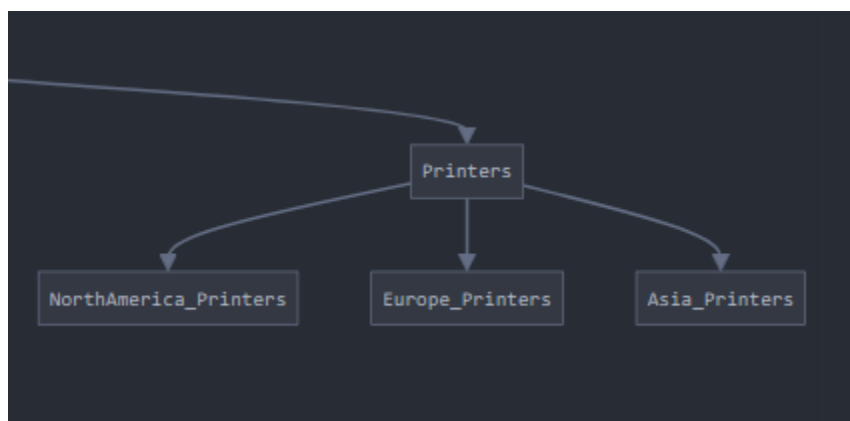
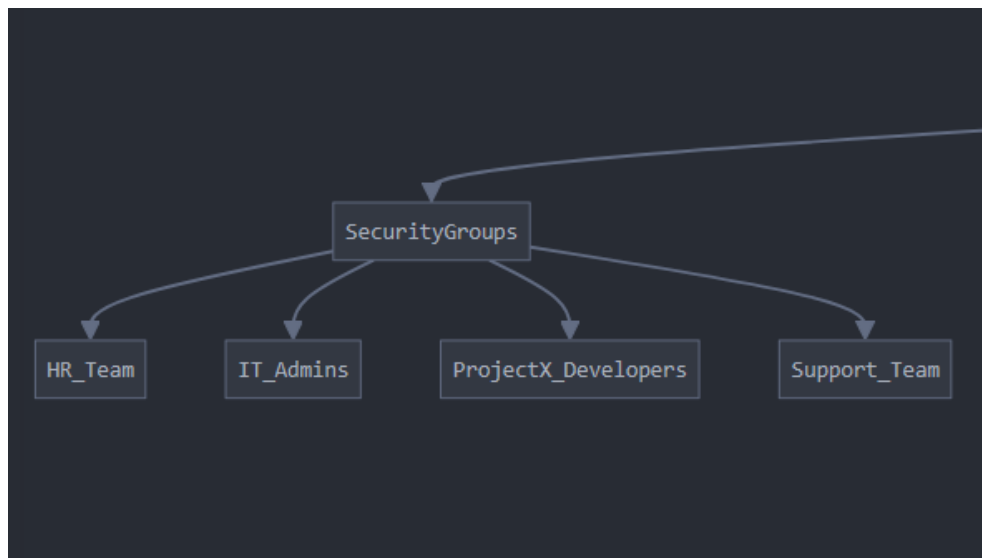
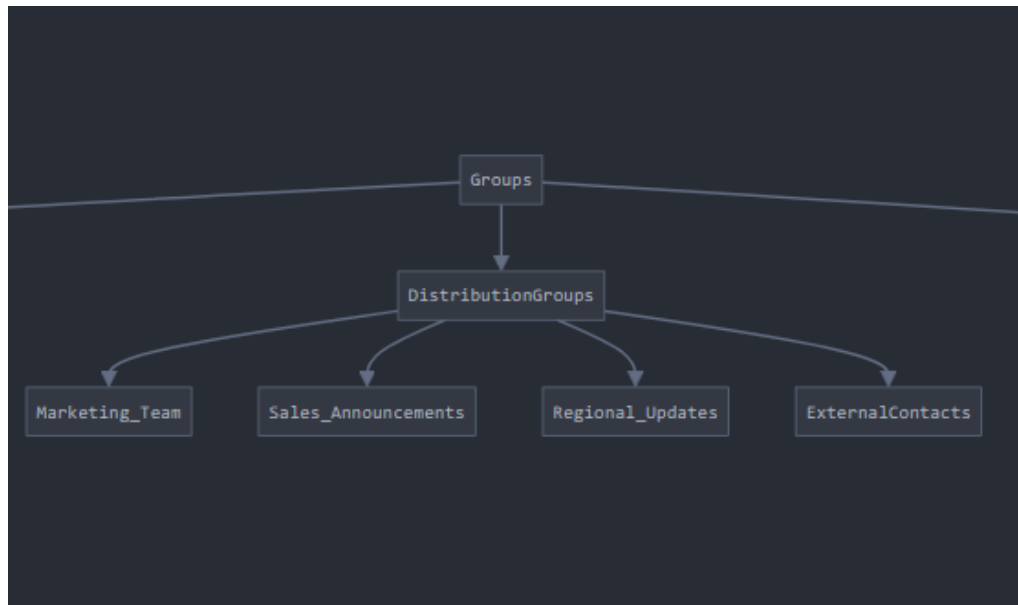
1.2.2 Blueprint for Computers



Computers

- NorthAmerica
- Europe
- Asia

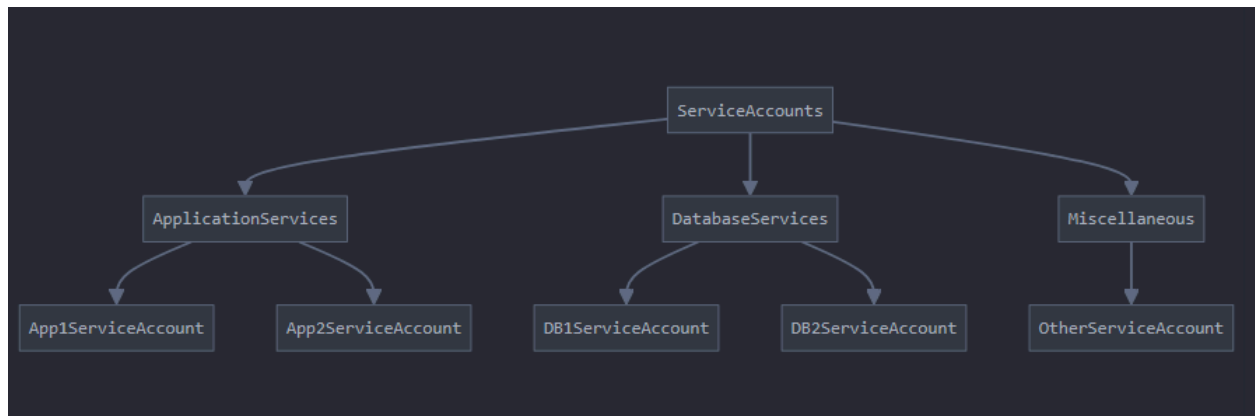
1.2.3 Blueprint for Groups



Groups

- SecurityGroups
 - HR_Team
 - IT_Admins
 - ProjectX_Developers
 - Support_Team
- DistributionGroups
 - Marketing_Team
 - Sales_Announcements
 - Regional_Updates
 - ExternalContacts
- Printers
 - NorthAmerica_Printers
 - Europe_Printers
 - Asia_Printers

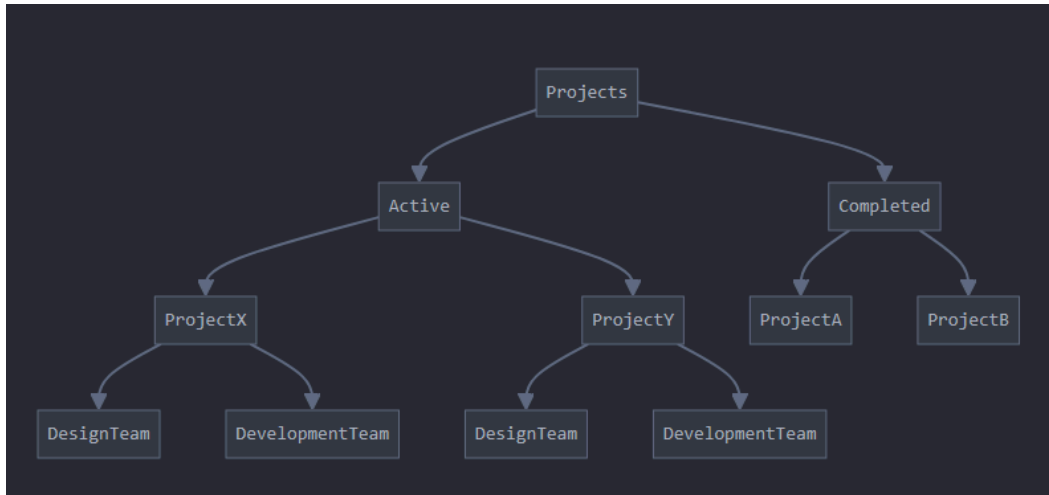
1.2.4 Blueprint for ServiceAccounts



ServiceAccounts

- ApplicationServices
 - App1ServiceAccount
 - App2ServiceAccount
- DatabaseServices
 - DB1ServiceAccount
 - DB2ServiceAccount
- Miscellaneous
 - OtherServiceAccount

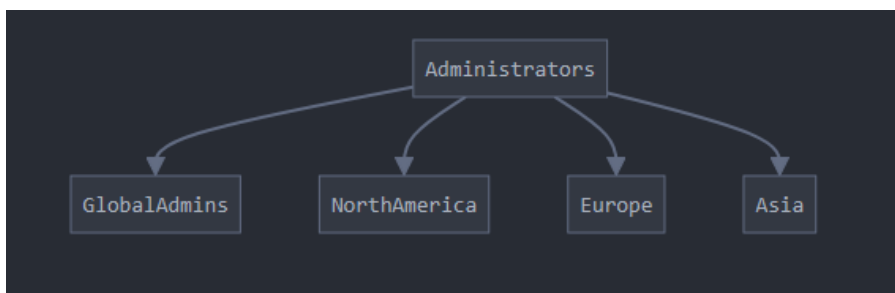
1.2.5 Blueprint for Projects



Projects

- Active
 - ProjectX
 - DesignTeam
 - DevelopmentTeam
 - ProjectY
 - DesignTeam
 - DevelopmentTeam
- Completed
 - ProjectA
 - ProjectB

1.2.6 Blueprint for Administrators



Administrators

- GlobalAdmins
- NorthAmerica
- Europe
- Asia

2. Expanding the Active Directory

The Active Directory structure is designed to facilitate efficient management and organisation of users, computers, groups, and resources within the domain. Below is the detailed breakdown of the primary Organisational Units (OUs) and their respective components.

To do this, we'll create a PowerShell script to reduce the manual work of creating all of these OU's. This will save us time and allow us to focus on the more important areas instead.

2.1 PowerShell Script

We'll be running a PowerShell Script I made. This script will essentially make us all of the Organisational Units we need. There are a few steps needed to ensure it'll work. First we have to check to see if we have the Active Directory Module.

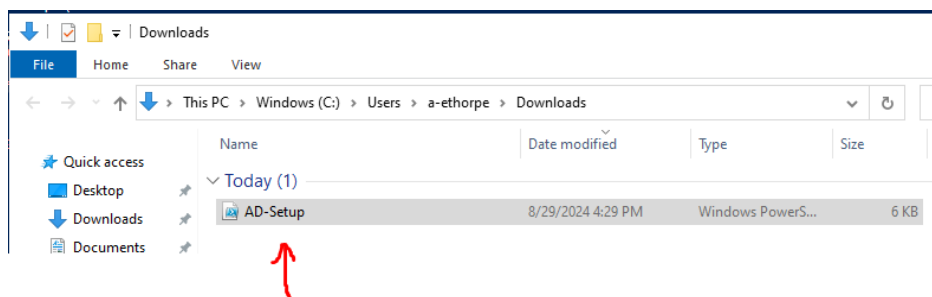


- First we want to type "Import-Module ActiveDirectory"
- Next we'll check to see if the module "ActiveDirectory" has been added
- In this case, it has worked

Next we'll use a PowerShell script I made which can be found on my Google Drive:

<https://drive.google.com/file/d/1OasFXCibhGIAAny1qkg7YTPGzuUOhj/view?usp=sharing>

This will generate all of the Organisational Units.



After downloading the file, you'll have to go back to PowerShell ISE as administrator

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
PS C:\Windows\system32> cd C:\Users\A-ethorpe\Downloads
PS C:\Users\A-ethorpe\Downloads> .\AD-Setup.ps1
.\AD-Setup.ps1 : File C:\Users\A-ethorpe\Downloads\AD-Setup.ps1 cannot be loaded. The file C:\Users\A-ethorpe\Downloads\AD-Setup.ps1 is not digitally signed. You cannot
run this script on the current system. For more information about running scripts and setting execution policy, see about_Execution_Policies at
https://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\AD-Setup.ps1
+ ~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess
PS C:\Users\A-ethorpe\Downloads>
```

- First you'll change to the directory of where the PowerShell script is set
 - `cd C:\Users\A-ethorpe\Downloads.`
- Second you'll run the command
 - `“.AD-Setup.ps1”`
- Then you'll get an error as shown. The reason for this is because our script is not digitally signed. This is a security feature that helps prevent dangerous scripts from being run.

For this lab, we'll be temporarily avoiding this security halt by temporarily disabling it. In a real world environment, we would NOT do this. Although it wouldn't cause any issues, it's bad practice. Accidentally opening the wrong script or not knowing what you're doing could cause serious damage. However, for this scenario we will do it just to speed up the process.

```
PS C:\Windows\system32> cd C:\Users\A-ethorpe\Downloads
PS C:\Users\A-ethorpe\Downloads> .\AD-Setup.ps1
.\AD-Setup.ps1 : File C:\Users\A-ethorpe\Downloads\AD-Setup.ps1 cannot be loaded. The file C:\Users\A-ethorpe\Downloads\AD-Setup.ps1 is not digitally signed. You cannot
run this script on the current system. For more information about running scripts and setting execution policy, see about_Execution_Policies at
https://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\AD-Setup.ps1
+ ~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess
PS C:\Users\A-ethorpe\Downloads> Set-ExecutionPolicy RemoteSigned -Scope Process
```

Execution Policy Change

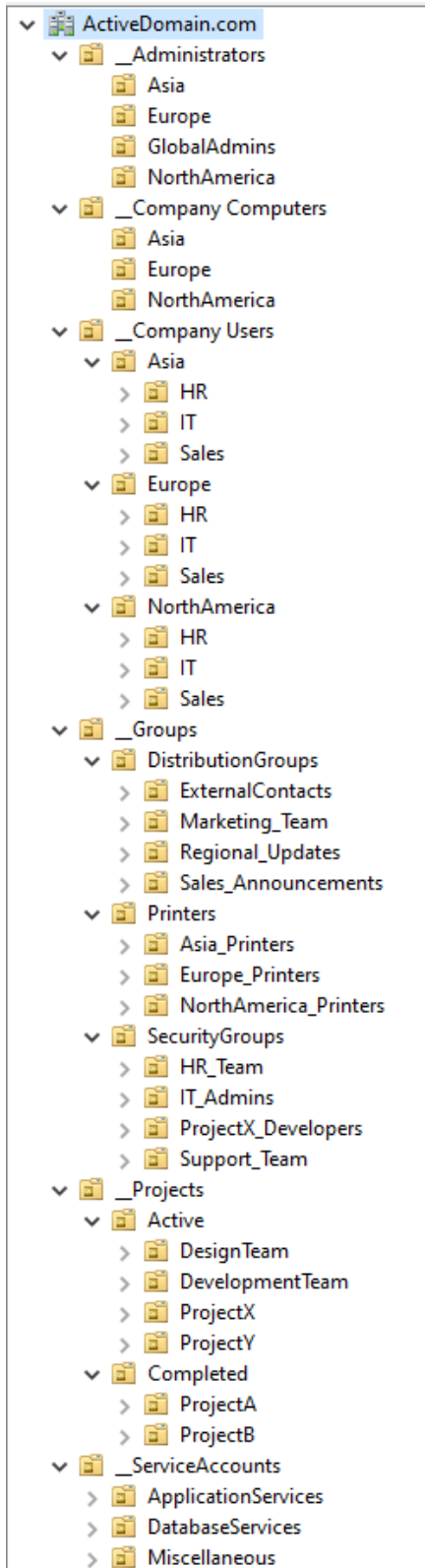
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic at https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?

Yes Yes to All No No to All Suspend

- Type `"Set-ExecutionPolicy RemoteSigned -Scope Process"`
 - This will lower the policy for the current PowerShell session
- Select "Yes"

```
PS C:\Users\A-ethorpe\Downloads> Unblock-File -Path "C:\Users\A-ethorpe\Downloads\AD-Setup.ps1"
```

- If this doesn't work. Type this instead. This will unblock the file.



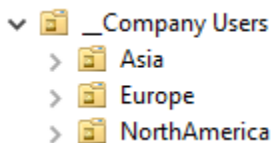
- After this, everything should be made! Now we'll be going through each one to explain its purpose and use.

3.1 Users OU

The "Users" OU is essential for managing user accounts across different regions. By organising users based on their geographical location and departmental role, it simplifies administrative tasks and the application of group policies. Users will also be called "Company Users". This is to differentiate from the already made Users OU (this OU holds a lot of important Security Groups that are best not to be deleted unless certain of knowing how it works)

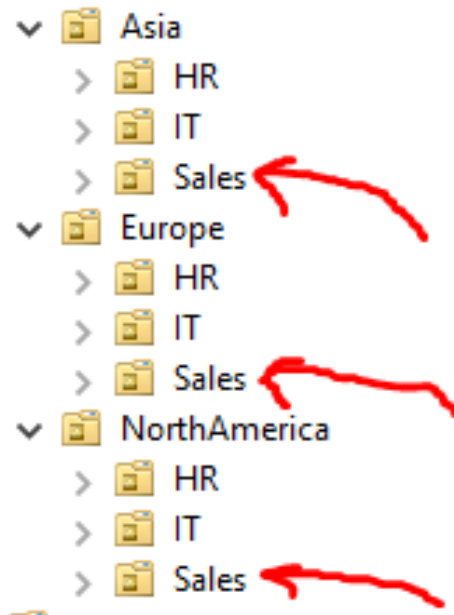
3.1.1 Regions

Each region within the "Users" OU—"NorthAmerica," "Europe," and "Asia"—has sub-OU's representing the core departments within the organisation.



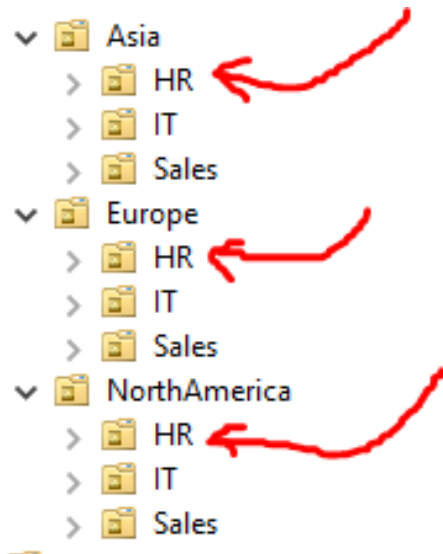
3.1.1.1 Sales

Houses user accounts for sales team members, such as John.Doe in North America or Carlos.Martin in Europe. These users are often subject to specific policies that support their sales functions.



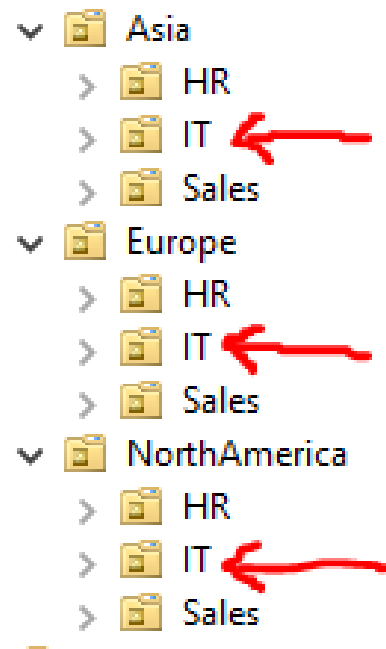
3.1.1.2 HR

Contains HR personnel like Jane.Smith from North America and Elena.Moreno from Europe. This structure ensures that HR users are managed separately, with access to sensitive employee data controlled and restricted as needed.



3.1.1.3 IT

IT staff across regions, like Tech.James in North America and Dev.Raj in Asia, are included here. This allows IT policies, such as software deployment or security settings, to be applied uniformly within the department.

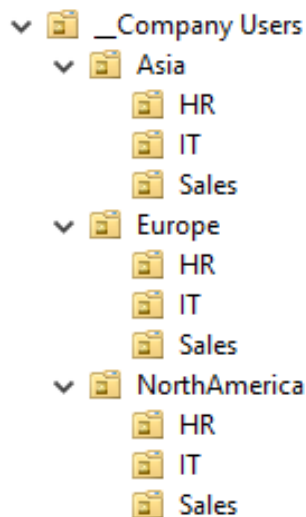


3.1.2 Final Structure

The final structure under the "Users" OU ensures a clear hierarchy:

- "NorthAmerica" > "Sales," "HR," "IT"
- "Europe" > "Sales," "HR," "IT"
- "Asia" > "Sales," "HR," "IT."

This setup allows for streamlined management and policy application across the company's global workforce.



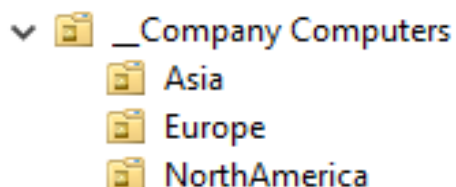
3.2 Computers OU

The "Computers" OU organises all computer objects by region, providing a logical structure for managing and applying policies to devices.

"NorthAmerica": Includes computers such as NA-LAPTOP-01 and NA-DESKTOP-02, enabling the application of region-specific policies like software updates or security configurations.

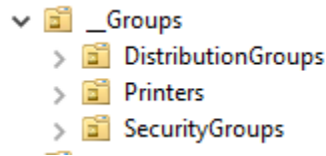
"Europe": Houses computers like EUROPE-WORKSTATION-01, ensuring that devices in European offices are managed according to local requirements.

"Asia": Includes devices such as ASIA-PC-05, facilitating efficient management and compliance with regional IT standards.



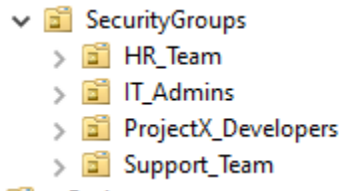
3.3 Groups OU

The "Groups" OU is divided into "Security Groups," "Distribution Groups," and "Printers," each serving distinct purposes.



3.3.1 Security Groups

"Security Groups" control access to resources by assigning permissions based on team roles.



HR Team

- Grants HR staff across regions, such as Susan.Wright from North America, access to HR-related files and systems.

IT Admins

- Includes users like Admin.James, who require administrative privileges to manage IT infrastructure.

ProjectX Developer

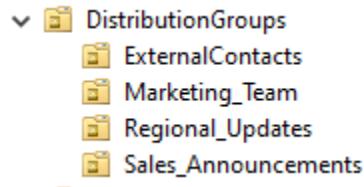
- Contains developers working on Project X, allowing controlled access to project-specific resources.

Support Team

- Includes users who provide technical support, ensuring they have the necessary permissions to assist users across the company.

3.3.2 Distribution Groups

"Distribution Groups" are used for email communication, enabling messages to be sent to multiple recipients simultaneously.



Marketing Team

- Allows the marketing department to communicate with all its members across different regions.

Sales Announcement

- Enables sales leaders to send important updates to all sales personnel.

Regional Updates

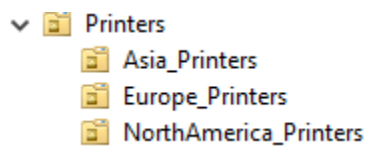
- Facilitates region-specific communications, such as Europe_Updates for European staff.

External Contacts

- Contains external partners or vendors, allowing them to be included in relevant communications without giving them network access.

3.3.3 Printers

The "Printers" OU manages printer objects by region, simplifying the deployment and management of network printers.



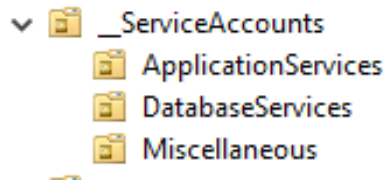
"NorthAmerica_Printers": Includes printer objects like NA-OFFICE-PRINTER-01.

"Europe_Printers": Manages printers in European offices, such as EUROPE-OFFICE-PRINTER-02.

"Asia_Printers": Contains printers like ASIA-OFFICE-PRINTER-03 used in Asian offices.

3.4 ServiceAccounts OU

The "ServiceAccounts" OU is designed to manage dedicated user accounts that run services within the organisation.



Application Services

- "App1ServiceAccount" and "App2ServiceAccount" are used by applications to operate with the necessary permissions, ensuring security and stability.

Database Services

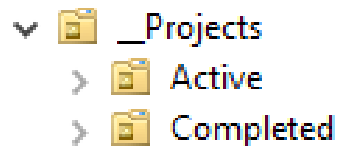
- "DB1ServiceAccount" and "DB2ServiceAccount" are specifically for database operations, allowing databases to function securely.

Miscellaneous

- "OtherServiceAccount" is used for any services that do not fall under application or database categories, such as backup systems.

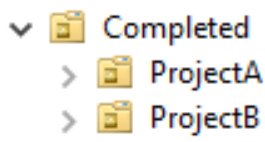
3.5 Projects OU

The "Projects" OU helps manage resources related to ongoing and completed projects.



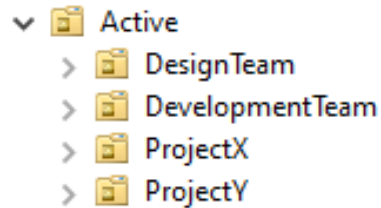
3.5.1 Completed

"ProjectA" and "ProjectB" store data and resources from past projects, ensuring they remain accessible for future reference.



3.5.2 Active

"ProjectX" and "ProjectY" represent ongoing projects, each with sub-OUs for "Design Team" and "Development Team," allowing for focused management of project resources.



Design Team

- Houses users involved in the design phase of projects, ensuring they have the necessary resources.

Development Team

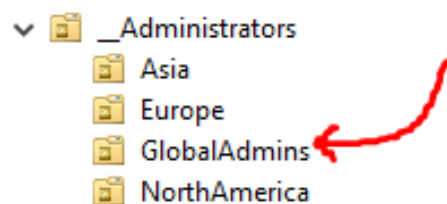
- Includes users working on the development aspect, allowing for efficient project management.

3.6 Administrators OU

The "Administrators" OU manages administrative accounts, providing control over various levels of the domain.

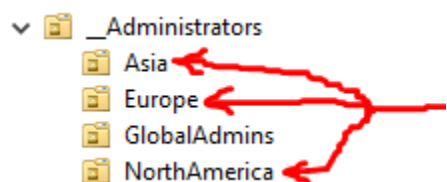
Global Admins

- GlobalAdmins contains accounts with domain-wide privileges, such as Admin.Global, who can manage the entire Active Directory.



Regional Admins

- Regional OUs like "NorthAmerica," "Europe," and "Asia" house admins with specific regional responsibilities, ensuring targeted and secure administrative control.

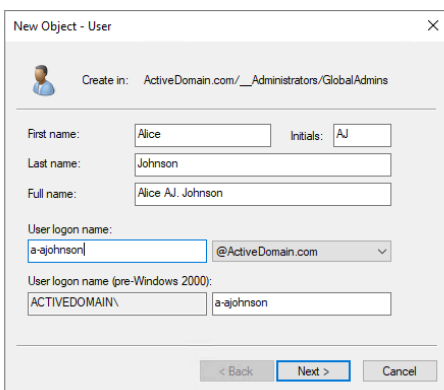


4 Setting up All Objects

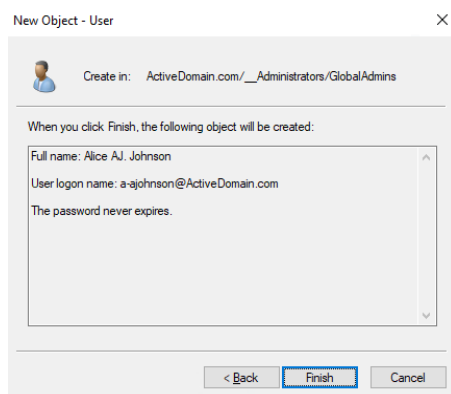
4.1 Setting up Objects in Administrator

This section covers the configuration of the "Administrators" Organisational Unit (OU) within Active Directory. The "Administrators" OU is critical for managing administrative accounts with domain-wide or regional control. Key objects in this OU include:

- **GlobalAdmins:** Contains domain-wide administrators responsible for overarching management and policy enforcement. These accounts have full access to all domain resources.
- **NorthAmerica, Europe, Asia:** Regional administrator accounts tailored for specific geographic regions. These accounts manage domain activities and policies within their respective regions.



- Here we're making a New User Object. In this case, this is an Admin for GlobalAdmins



- After this we would set a password that would never expire and finish.

In order to give this more detail, we right click the new object, and select properties

Alice AJ. Johnson Properties

Member Of: Remote control, Dial-in, Environment, Sessions, Remote Desktop Services Profile, COM+

General | Address | Account | Profile | Telephones | Organization

Alice AJ. Johnson

First name: Alice Initials: AJ

Last name: Johnson

Display name: Alice AJ. Johnson

Description: A global admin for all regions

Office: Global Administrator

Telephone number: Other...

E-mail:

Web page: Other...

OK Cancel Apply Help

- Here we've given it a description and an office

Select Groups

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

From this location: ActiveDomain.com

Enter the object names to select (examples): Administrators

Object Types... Locations... Check Names

Advanced... OK Cancel

Alice AJ. Johnson Properties

Remote control | Remote Desktop Services Profile | COM+ | General | Address | Account | Profile | Telephones | Organization | Member Of | Dial-in | Environment | Sessions

Member of:

Name	
Active Directory Domain Services Folder	
Domain Users	ActiveDomain.com/Users

Add... Remove

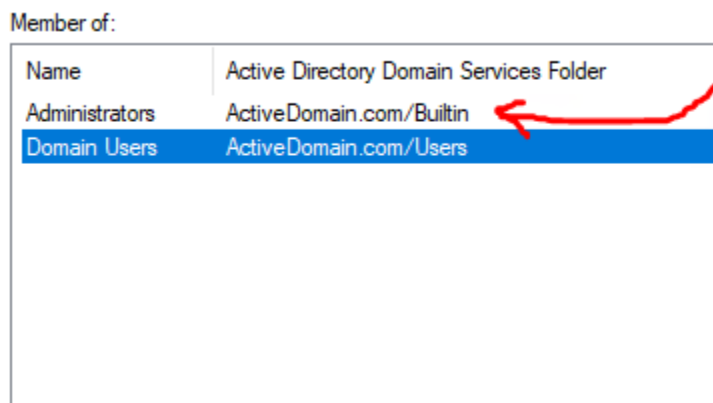
Primary group: Domain Users

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

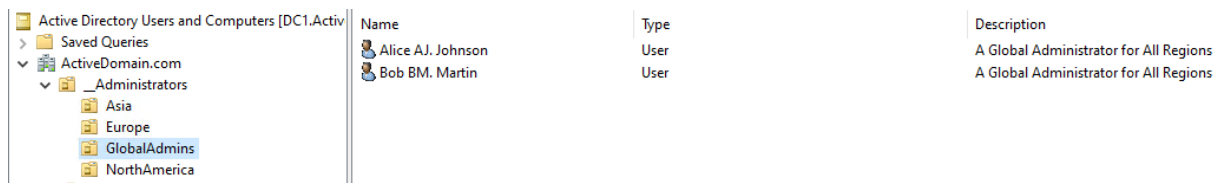
OK Cancel Apply Help

- To make this user an admin, we have to go to "Member Of"
- Then select "Add..."
- Then type in "Administrators"
- Then select "Check Names"
- Then select "OK"

What we have done here is looked for a group called “Administrators” and in this group, there are a number of different restrictions made specifically for admins. By giving this user this group, we make this user have all the privileges this group has.



We can repeat this for all the other administrators in the different OU's



4.2 Setting up Objects in Company Computers

This section details the setup of the "Company Computers" OU, designed to organize computer objects by region. This structure supports efficient device management and policy application. Key components include:

- **NorthAmerica:** Computer objects for devices used in North American offices. Examples include laptops and desktops specific to this region.
- **Europe:** Computer objects for European offices, ensuring region-specific management and compliance.
- **Asia:** Computer objects for devices in Asian offices, facilitating targeted administration and support.

New Object - Computer

Create in: ActiveDomain.com/_Company Computers/Asia

Computer name:
AS-PC-05

Computer name (pre-Windows 2000):
AS-PC-05

The following user or group can join this computer to a domain.

User or group:
Default: Domain Admins Change...

☐ Assign this computer account as a pre-Windows 2000 computer

OK Cancel Help

- Create a new object, select computer
- Give it a name you'd like

AS-PC-05 Properties

Location Managed By Dial-in

General Operating System Member Of Delegation LAPS

AS-PC-05

Computer name (pre-Windows 2000): AS-PC-05

DNS name:

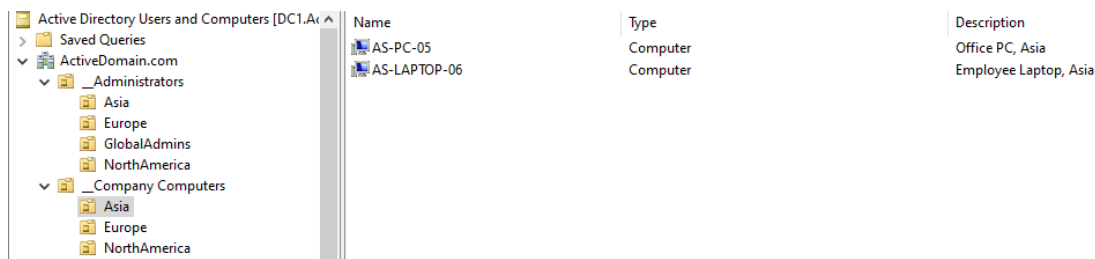
DC Type: Workstation or server

Site:

Description: Office PC, Asia

OK Cancel Apply Help

- Give it a Description
- Press Apply and OK



- Then set it up for the other OUs

4.3 Setting up Objects in Company Users

The "Company Users" OU is structured to manage user accounts based on geographical regions and departmental roles. This section outlines:

- **NorthAmerica, Europe, Asia:** Each region includes sub-OUs for departmental roles such as Sales, HR, and IT. This hierarchical organisation helps in applying region-specific policies and managing user accounts efficiently.
- **Sales, HR, IT:** Within each region, these sub-OUs manage users based on their departmental function, ensuring appropriate access controls and policy application.

This section is very similar to Administrators. You simply add a new User and give the necessary details. In this case, we won't need to add them to the group Administrator.

4.4 Setting up Objects in Groups

The "Groups" OU is used for managing various group objects, including security and distribution groups. Printer has been included here but it may be best to give printers its own OU. Regardless, this section includes:

- **SecurityGroups:** Manages access control groups such as HR_Team, IT_Admins, ProjectX_Developers, and Support_Team. These groups control permissions and access to resources.
- **DistributionGroups:** Facilitates communication through groups like Marketing_Team, Sales_Announcements, Regional_Updates, and ExternalContacts, enabling efficient email distribution.
- **Printers:** Organises printer objects by region, including NorthAmerica_Printers, Europe_Printers, and Asia_Printers, to manage network printers effectively.

New Object - Group

Create in: ActiveDomain.com/___Groups/DistributionGroups

Group name:

ExternalContacts

Group name (pre-Windows 2000):

ExternalContacts

Group scope

☐ Domain local

☒ Global

☐ Universal

Group type

☐ Security

☒ Distribution

OK

Cancel

Name	Type
ExternalContacts	Distribution Group - Universal
Marketing_Team	Distribution Group - Universal
Regional_Updates	Distribution Group - Universal
Sales_Announcements	Distribution Group - Universal

- Here we're making a Group Distribution. These are used for email communication, enabling messages to be sent to multiple recipients simultaneously

New Object - Group

Create in: ActiveDomain.com/___Groups/SecurityGroups

Group name:

HR_Team

Group name (pre-Windows 2000):

HR_Team

Group scope

☐ Domain local

☒ Global

☐ Universal

Group type

☒ Security

☐ Distribution

OK

Cancel

Name	Type
HR_Team	Security Group - Global
IT_Admins	Security Group - Global
ProjectX_Developers	Security Group - Global
Support_Team	Security Group - Global

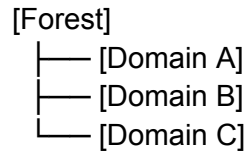
- Here we're making a Security Group. These are to control access to resources by assigning permissions based on team roles.

Printers will be empty as we have no physical or virtual printers to create the object. If we did, we could and it's as simple as finding the link to that specific printer and adding it.

4.4.1 Group Domains

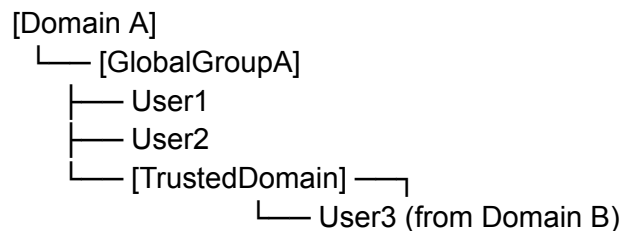
Another note about groups is the Group Scope. There are differences between Domain Local, Global and Universal.

Imagine this is your forest and domains:



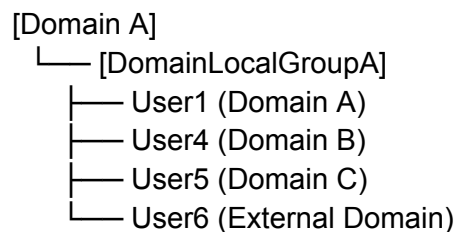
Global groups are limited to their own domain but can include members from other domains through trusts. They are primarily used to group users within the same domain and can be assigned permissions in other domains via Domain Local groups.

- **Scope:** Limited to the domain they are created in but can include members from other trusted domains.
- **Usage:** Useful for grouping users within the same domain.
- **Example:**



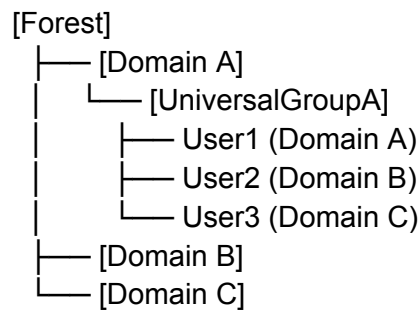
Domain Local groups are confined to the domain where they are created but can include members from any domain in the forest, as well as from external forests if trusts are set up. They are ideal for managing permissions on resources within their own domain.

- **Scope:** Restricted to the domain they are created in but can include members from any domain, including trusted and external domains.
- **Usage:** Ideal for assigning permissions to resources within their own domain.
- **Example:**



Universal groups have a broader scope, encompassing members from any domain in the forest. They are suitable for assigning permissions to resources across the entire forest, making them versatile for cross-domain resource access.

- **Scope:** Can include members from any domain within the forest and can be used across the entire forest.
- **Usage:** Suitable for assigning permissions across domains in the forest.
- **Example:**



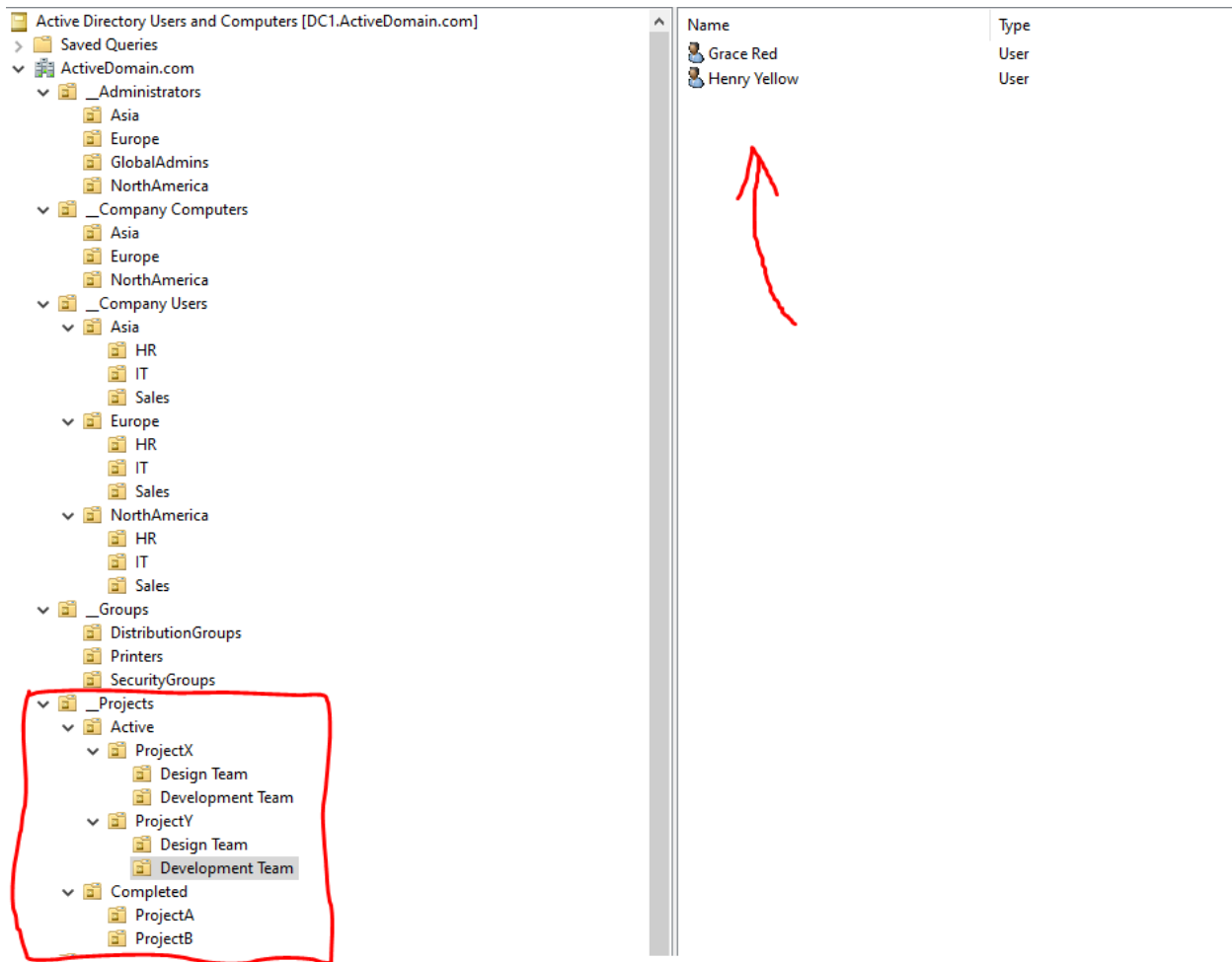
Summary:

- Global Groups are specific to their domain but can be used in other domains indirectly through Domain Local groups.
- Domain Local Groups are restricted to their domain for permissions but can include members from any domain within the forest or external domains.
- Universal Groups can span across all domains in the forest, making them suitable for cross-domain permissions and membership.

4.5 Setting up Objects in Projects

This section details the "Projects" OU, designed to manage resources and tasks related to ongoing and completed projects. Key components include:

- **Active:** Contains sub-OUs for ongoing projects such as ProjectX and ProjectY, each with DesignTeam and DevelopmentTeam sub-OUs. This structure helps manage active project resources and team members.
- **Completed:** Houses resources and records for completed projects like ProjectA and ProjectB, ensuring that historical project data remains accessible for future reference.



- With these, it's as simple as adding a user. Like before.

4.6 Setting up Objects in Service Accounts

The "Service Accounts" OU is used to manage dedicated accounts for various services within the organisation. This section includes:

- **ApplicationServices:** Contains service accounts like App1ServiceAccount and App2ServiceAccount, used for application-specific operations.
- **DatabaseServices:** Includes service accounts such as DB1ServiceAccount and DB2ServiceAccount, which handle database operations securely.
- **Miscellaneous:** Manages other service accounts not covered by the application or database categories, such as backup system accounts.

Services are made as USER accounts, but they're not actual users, rather they're services that can be used. Something like display monitors for fast food restaurants:



Or even security monitors for security cameras:



To help differentiate between regular users and services, it's often best practice to use a symbol or some kind of recognition for a service account.

Sales

- Europe
- NorthAmerica

_Groups

- DistributionGroups
- Printers
- SecurityGroups

_Projects

- Active
 - ProjectX
 - Design Team
 - Development Team
 - ProjectY
 - Design Team
 - Development Team
- Completed
 - ProjectA
 - ProjectB

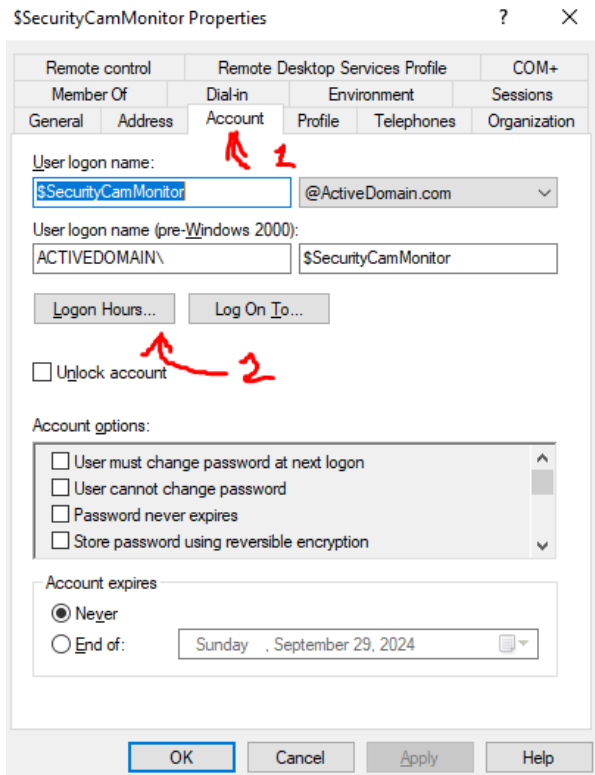
_ServiceAccounts

- Application Services
- Database Services
- Miscellaneous

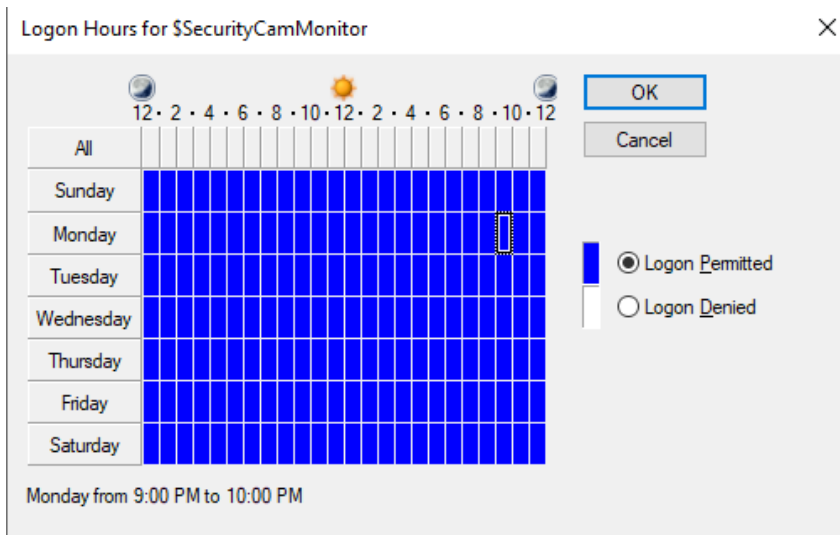
Name	Type	Description
\$SecurityCamMonitor	User	Operates security monitoring systems.
\$MenuDisplayControl	User	Controls restaurant display monitors.

- As shown here, we've added a "\$" at the start to tell us that this is a service account.

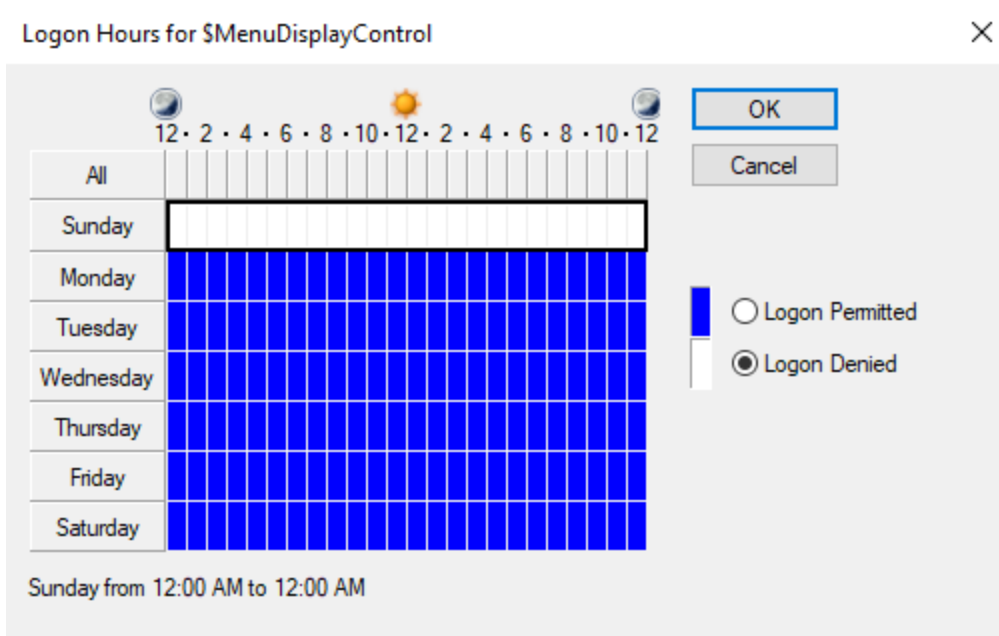
Something we can also do for both users and service accounts is to have logon hours.



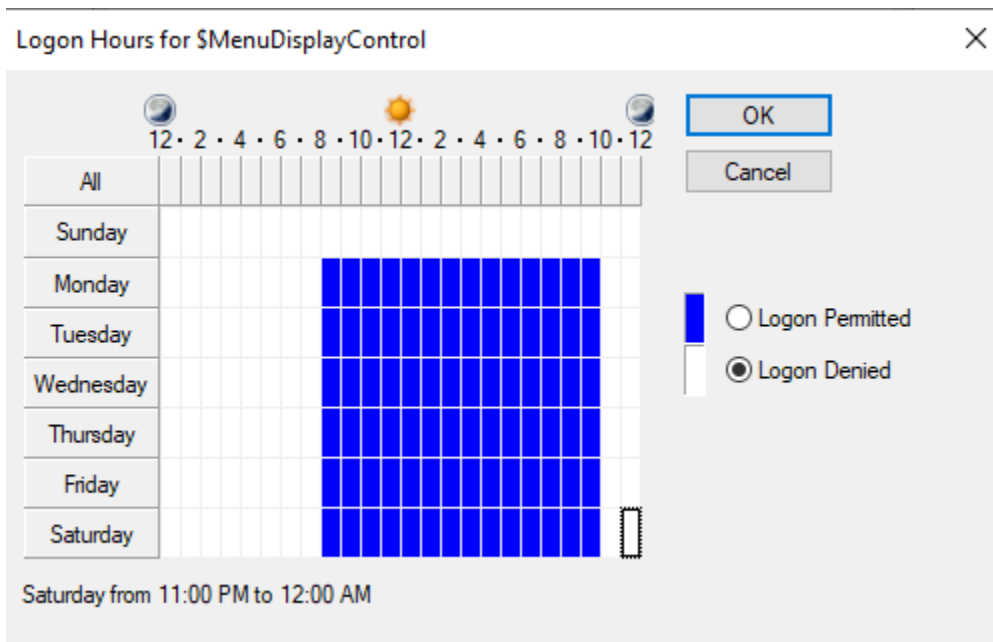
- Select Properties > Account > Logon Hours...



- Here we can see all the logon hours for this service. For this case, we're going to assume we have a restaurant business. For the security camera monitor, we're going to keep this running 24/7 so we won't touch this.



- We will make changes to our Menu Display Controller. As we don't need this service to be open 24/7.
- In this case, we've highlighted all of Sunday and denied login. The click and drag feature makes this much easier to manage.



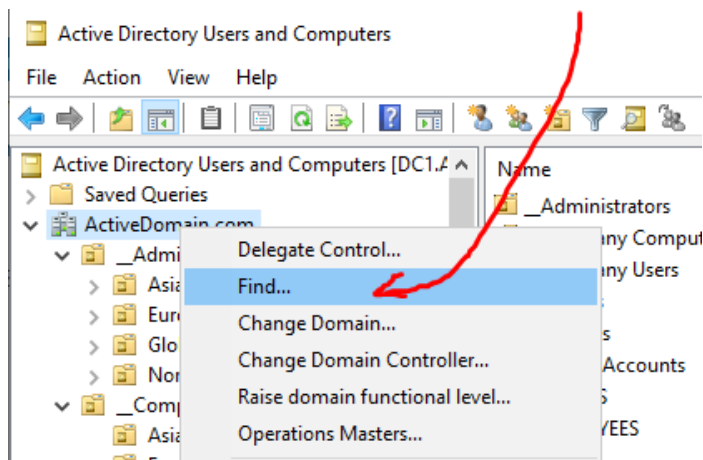
- We've now updated it to replicate when the display monitors need to be online. This can be adjusted anytime. So if it needs to be earlier, or later, it can be done.

5 Active Directory Management

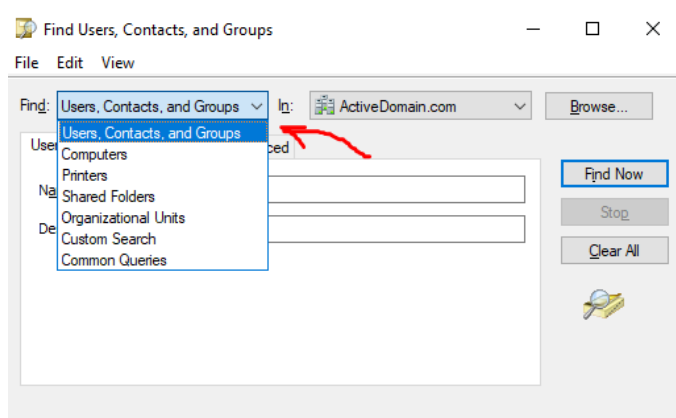
In this section, we will cover essential tasks for managing Active Directory in a work environment. From finding and managing objects to handling user onboarding and offboarding, these tasks are crucial for maintaining an efficient and secure directory service.

5.1 Finding Objects

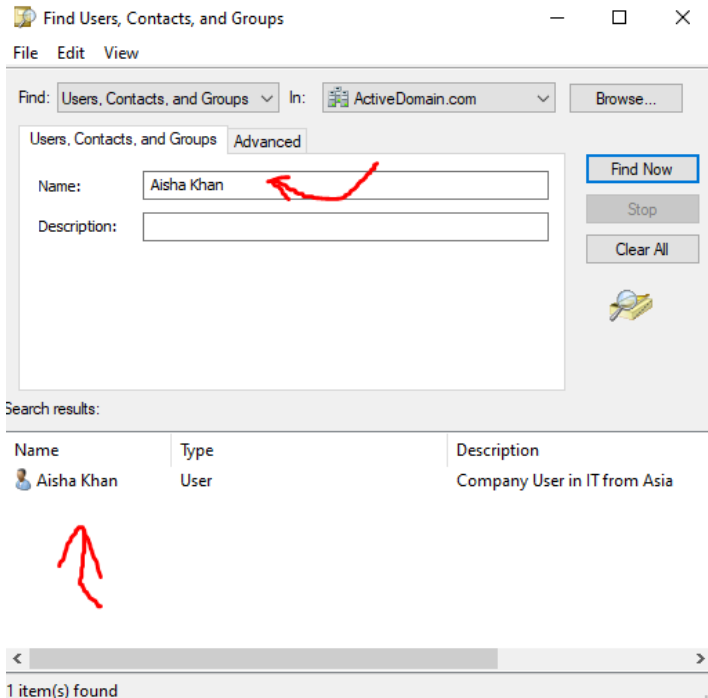
Learn how to locate specific objects within Active Directory using various search methods. This includes finding users, groups, computers, and other objects based on different criteria.



- Right click on the created Domain
- Select Find...



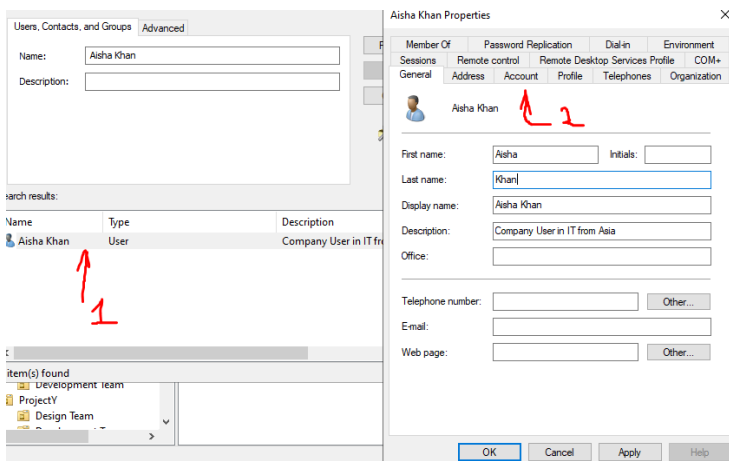
- Here we can be selective on what we want to choose. We can select Users, Contact and Groups here as we want to find a user.



- Type the name and we can find the user. This is especially useful for needing to make changes to a user. Whether it's editing their profile, moving them to a different OU, or, more commonly, password resets.

5.2 Password Reset

Discover the steps to reset passwords for users within Active Directory. This section covers the procedures for handling password recovery and ensuring account security.



- If you click on the account, you'll get the general information on the account
- Click on "Account"

Aisha Khan Properties

Member Of Password Replication Dial-in Environment
Sessions Remote control Remote Desktop Services Profile COM+

General Address Account Profile Telephones Organization

User logon name: Aisha.Khan @ActiveDomain.com

User logon name (pre-Windows 2000): ACTIVEDOMAIN\ Aisha.Khan

Logon Hours... Log On To...

☐ Unlock account

Account options:

☐ User must change password at next logon
☐ User cannot change password
☐ Password never expires
☐ Store password using reversible encryption

Account expires

☒ Never
☐ End of: Sunday, September 29, 2024

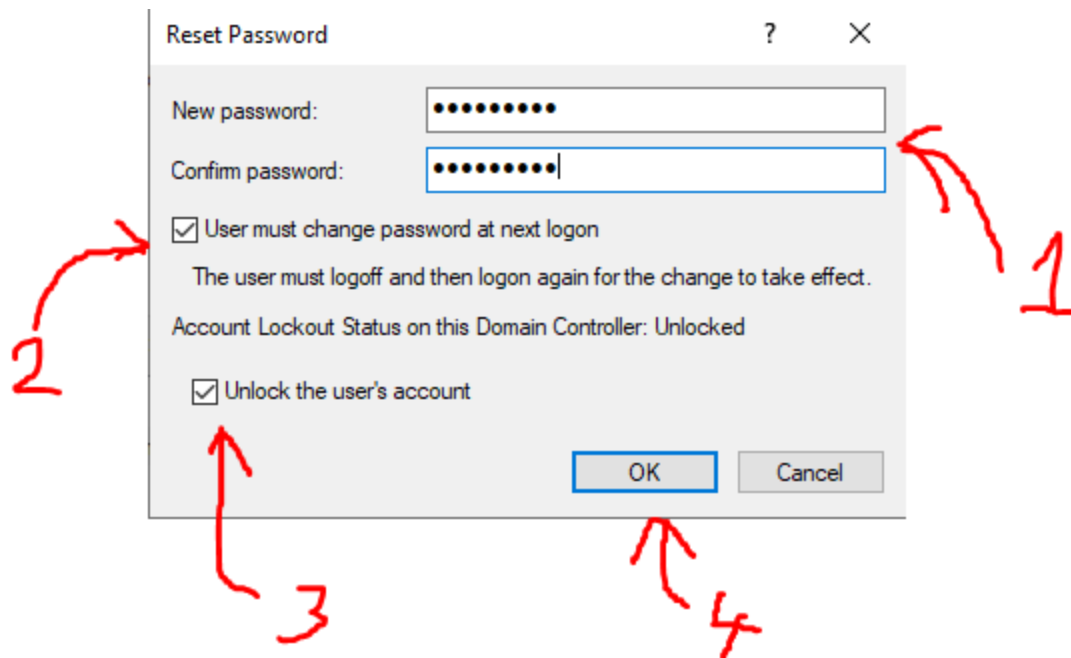
OK Cancel Apply Help

- In some cases, the user has had their account locked due to many failed attempts but they may remember their password. We can unlock their account by clicking on 1 to tick the box.
- Then click on 2 to apply then 3 to confirm the change.

Name	Type	Description
Aisha Khan	User	Company User in IT from Asia

Rename
Delete
Add to a group...
Disable Account
Reset Password...
Move...
Open Home Page
Send Mail
Properties

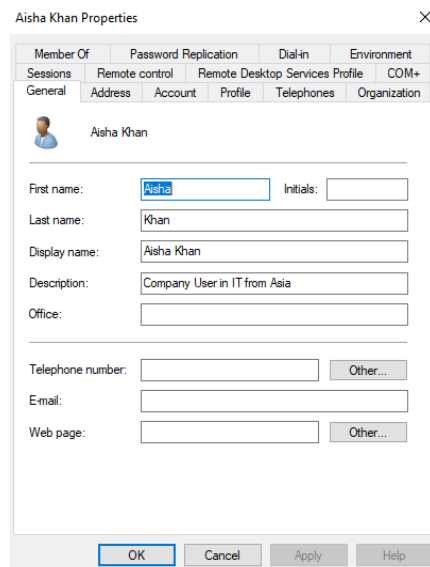
- Sometimes the password does need to be reset, in order to do this we'd just right click the name, select "Reset Password..."



- We would then add the new password
- Make sure that the user must change the password at next logon
- Unlock the users account if it's blocked
- Then press OK

5.3 Editing User Profiles

Understand how to update and manage user profiles in Active Directory. This involves modifying user attributes, contact information, and other relevant details.



- In this case, we're going to make changes to Aisha, as she's needs more details of her
- She has also been promoted to Administrator, so we'll need to make those adjustments

Aisha Khan Properties

Member Of	Password Replication	Dial-in	Environment
Sessions	Remote control	Remote Desktop Services Profile	COM+
General	Address	Account	Profile
	Telephones	Organization	

Aisha Khan

First name: Aisha Initials:

Last name: Khan

Display name: Aisha Khan

Description: Company User in IT from Asia

Office: Asia IT Administrator

Telephone number: 53024567890 Other...

E-mail: a-akhan@activedirectory.com

Web page: Other...

OK Cancel Apply Help

- We've now given her more details.
- We will now want to give her the permissions of an Admin

Aisha Khan Properties

Member Of	Password Replication	Dial-in	Environment
Sessions	Remote control	Remote Desktop Services Profile	COM+
General	Address	Account	Profile
	Telephones	Organization	

Member of

Name Active Directory Domain Service

Domain Users ActiveDomain.com/Users

Add... Remove

Primary group: Domain Users

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

OK Cancel Apply Help

Select Groups

Select this object type:

Groups or Built-in security principals Object Types...

From this location:

ActiveDomain.com Locations...

Enter the object names to select (examples):

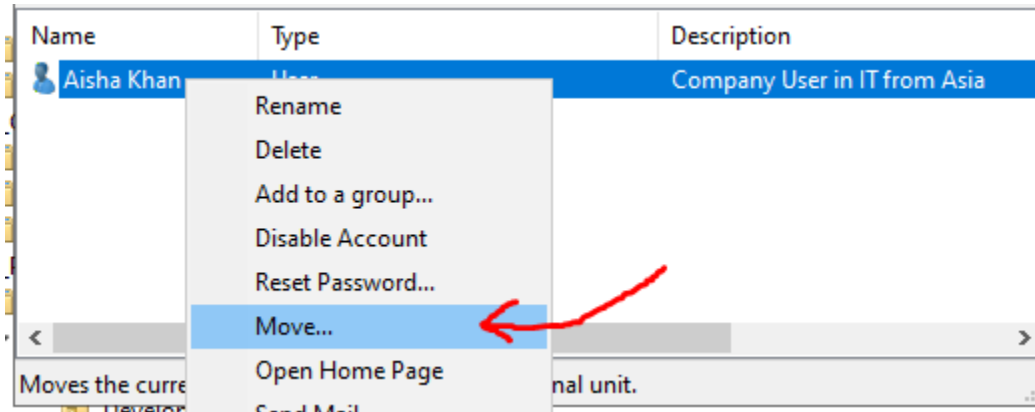
Administrators Check Names

Advanced... OK Cancel

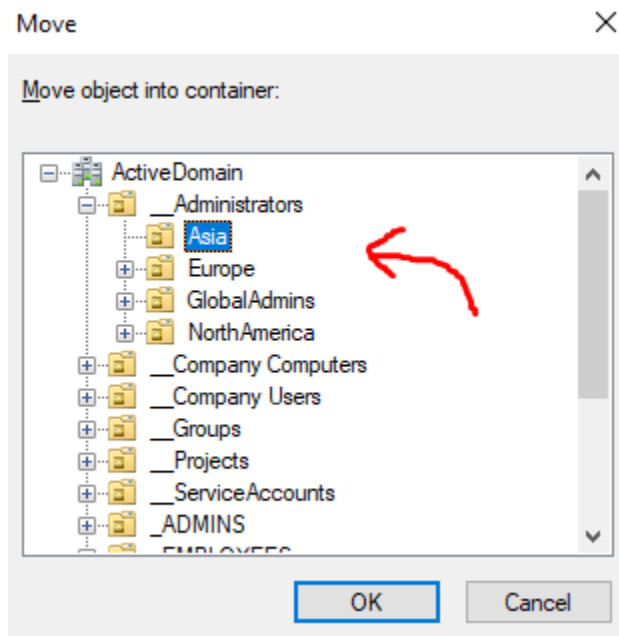
- We are now giving her administration privileges
- Go to Member Of > Add > Type Admin > Check Names > OK > Apply > OK

5.4 Moving Objects to Different OU

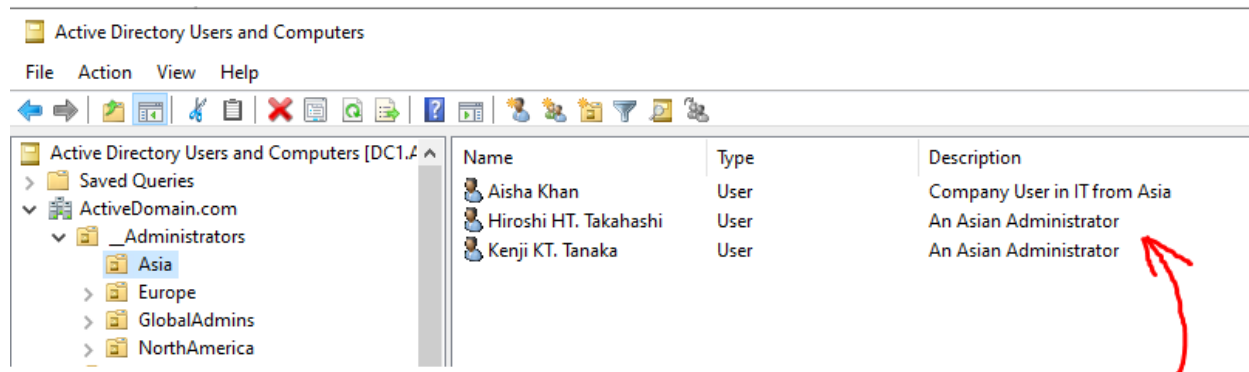
Explore the process of moving objects between Organisational Units (OUs). This section explains how to reorganise directory structure and manage object placement efficiently.



- Since Aisha is now an IT Administrator, we can move her to the correct location
- Right click her name > Move



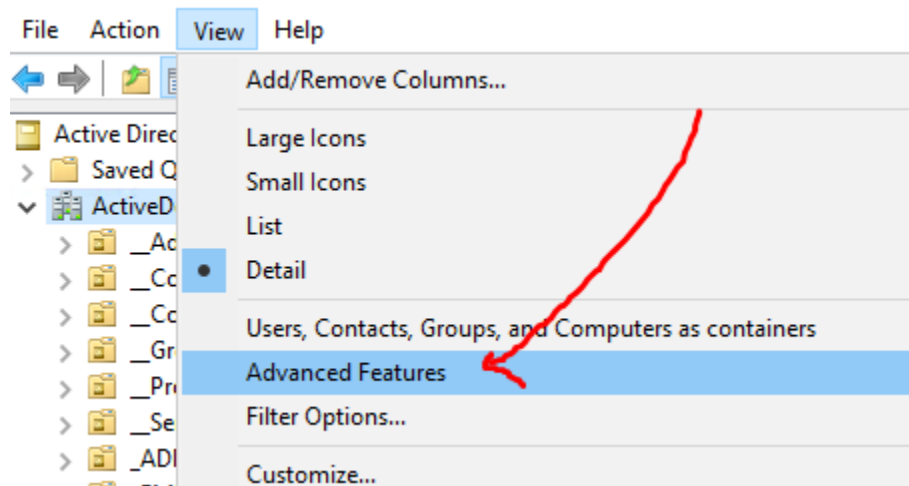
- Select the correct location
- Press OK



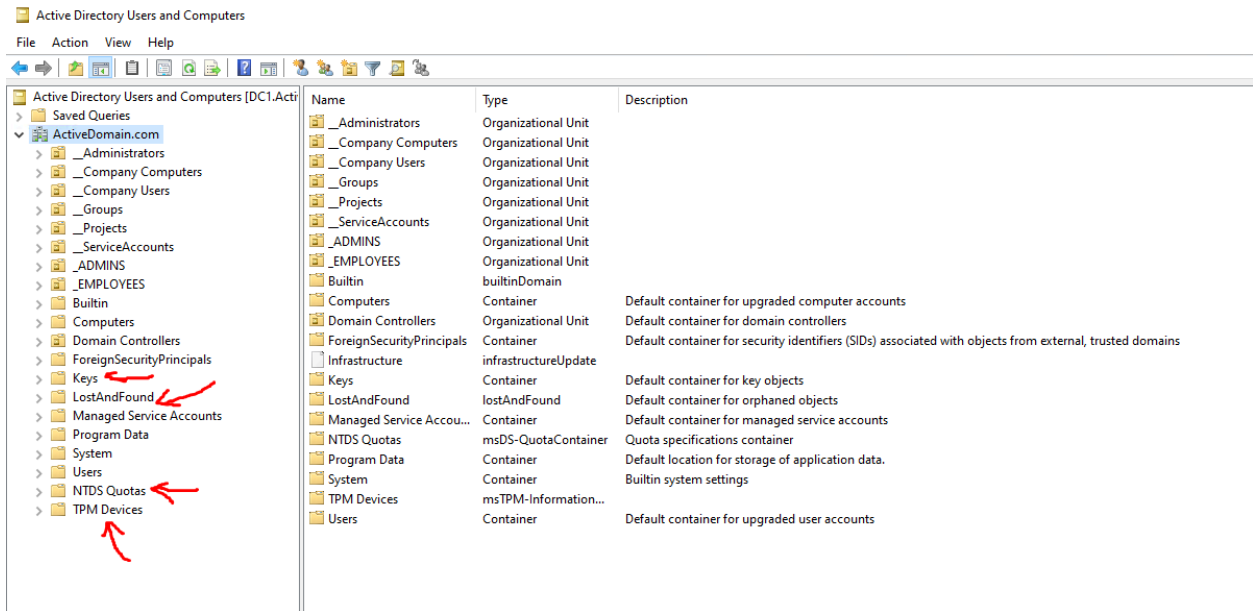
- We can now see she has been moved
- If you cannot see this, you'd simply refresh it and the move should be seen

5.5 Advanced View Features

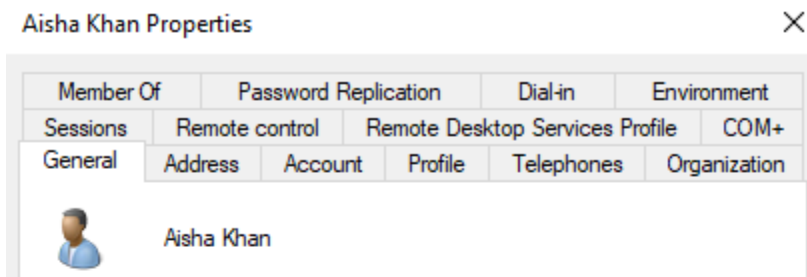
Advanced features and views in Active Directory provides deeper insights and control over your directory environment.



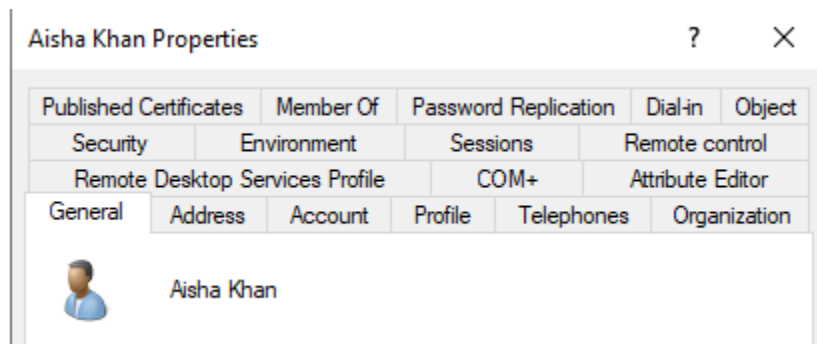
- To get to it, you go to View > Advanced Features



- Here we can see there's been more OUs that are shown.
BEFORE:



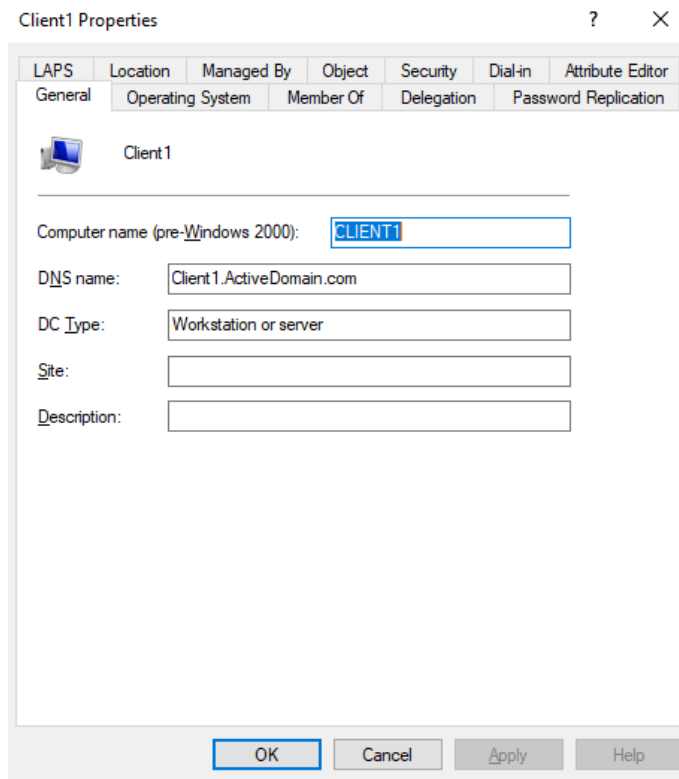
AFTER:



Also when looking through the properties of an object, we can see significantly more from the properties.

5.6 Asset Reviews

Discovering the options that asset properties can provide for us and what we can change.



The screenshot shows the 'Client1 Properties' dialog box with the 'General' tab selected. The 'Computer name (pre-Windows 2000):' field contains 'CLIENT1'. The 'DNS name:' field contains 'Client1.ActiveDomain.com'. The 'DC Type:' field is set to 'Workstation or server'. The 'Site:' and 'Description:' fields are empty. The 'Member Of' tab is also visible in the tab bar.

LAPS	Location	Managed By	Object	Security	Dial-in	Attribute Editor
General	Operating System	Member Of	Delegation	Password Replication		

Client1

Computer name (pre-Windows 2000): CLIENT1

DNS name: Client1.ActiveDomain.com

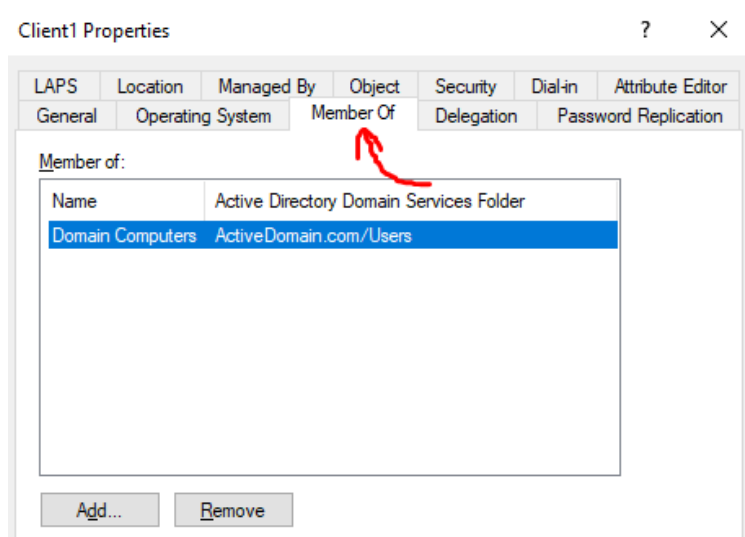
DC Type: Workstation or server

Site:

Description:

OK Cancel Apply Help

- Computers are considered an Asset and here we can make some changes. Whether it's the description



The screenshot shows the 'Client1 Properties' dialog box with the 'Member Of' tab selected. A red arrow points to the 'Member Of' tab. The 'Member of:' section shows a list of domain objects. The 'Domain Computers' object is selected, and its path 'ActiveDomain.com/Users' is displayed. The 'Add...' and 'Remove' buttons are at the bottom.

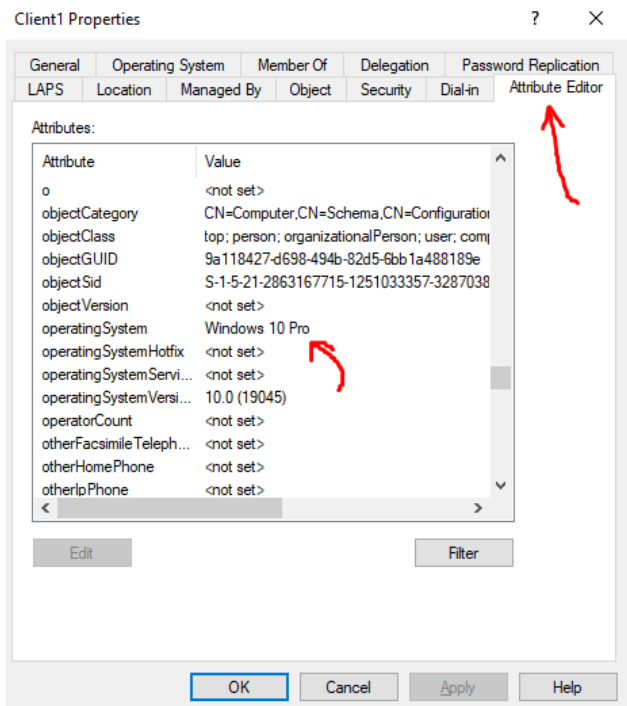
LAPS	Location	Managed By	Object	Security	Dial-in	Attribute Editor
General	Operating System	Member Of	Delegation	Password Replication		

Member of:

Name	Active Directory Domain Services Folder
Domain Computers	ActiveDomain.com/Users

Add... Remove

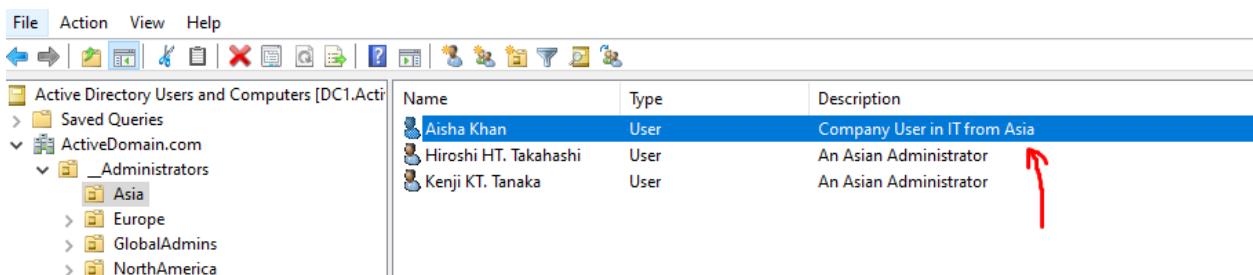
- Or we can add a member in the Member Of section



- We can also look at the attribute editor
- This will tell us everything about the asset. In this case, we know that this uses the operating system of Windows 10 Pro

5.7 Onboarding / Offboarding Users

Procedures for onboarding new users and offboarding departing ones. This section details the steps to efficiently add new accounts and remove outdated ones.



- After moving Aisha to Administrators for Asia, we still need to update the description and more. A simple way I would do this would be to open up an existing member that has the correct privileges that the new admin user would now have.

Hiroshi HT. Takahashi Properties

Published Certificates

Member Of

Password Replication

Dial-in

Object

Security

Environment

Sessions

Remote control

Remote Desktop Services Profile

COM+

Attribute Editor

General Address Account Profile Telephones Organization

Hiroshi HT. Takahashi

First name: Hiroshi Initials: HT

Last name: Takahashi

Display name: Hiroshi HT. Takahashi

Description: An Asian Administrator

Office: Asia Administrator

Telephone number: Other...

Email:

Web page: Other...

OK Cancel Apply Help

Aisha Khan Properties

Published Certificates

Member Of

Password Replication

Dial-in

Object

Security

Environment

Sessions

Remote control

Remote Desktop Services Profile

COM+

Attribute Editor

General Address Account Profile Telephones Organization

Aisha Khan

First name: Aisha Initials:

Last name: Khan

Display name: Aisha Khan

Description: Company User in IT from Asia

Office: Asia IT Administrator

Telephone number: 63024567890 Other...

Email: a-akhan@activedirectory.com

Web page: Other...

OK Cancel Apply Help

- We can now update the description to match Hiroshi

Hiroshi HT. Takahashi

First name: Hiroshi Initials: HT

Last name: Takahashi

Display name: Hiroshi HT. Takahashi

Description: An Asian Administrator

Office: Asia Administrator

Telephone number: Other...

Email:

Web page: Other...

OK Cancel Apply Help

Aisha Khan

First name: Aisha Initials:

Last name: Khan

Display name: Aisha Khan

Description: An Asian Administrator

Office: Asia IT Administrator

Telephone number: 63024567890 Other...

Email: a-akhan@activedirectory.com

Web page: Other...

OK Cancel Apply Help

- Update has been made

Hiroshi HT. Takahashi Properties

Security

Environment

Sessions

Remote control

Remote Desktop Services Profile

COM+

Attribute Editor

General Address Account Profile Telephones Organization

Published Certificates Member Of Password Replication Dial-in Object

Member of:

Name	Active Directory Domain Services Folder
Administrators	ActiveDomain.com/Builtin
Domain Users	ActiveDomain.com/Users
RDS Remote Ac...	ActiveDomain.com/Builtin
Remote Desktop ...	ActiveDomain.com/Builtin
Remote Manage...	ActiveDomain.com/Builtin

Add... Remove

Primary group: Domain Users

Set Primary Group

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

OK Cancel Apply Help

Aisha Khan Properties

Security

Environment

Sessions

Remote control

Remote Desktop Services Profile

COM+

Attribute Editor

General Address Account Profile Telephones Organization

Published Certificates Member Of Password Replication Dial-in Object

Member of:

Name	Active Directory Domain Services Folder
Administrators	ActiveDomain.com/Builtin
Domain Users	ActiveDomain.com/Users

Add... Remove

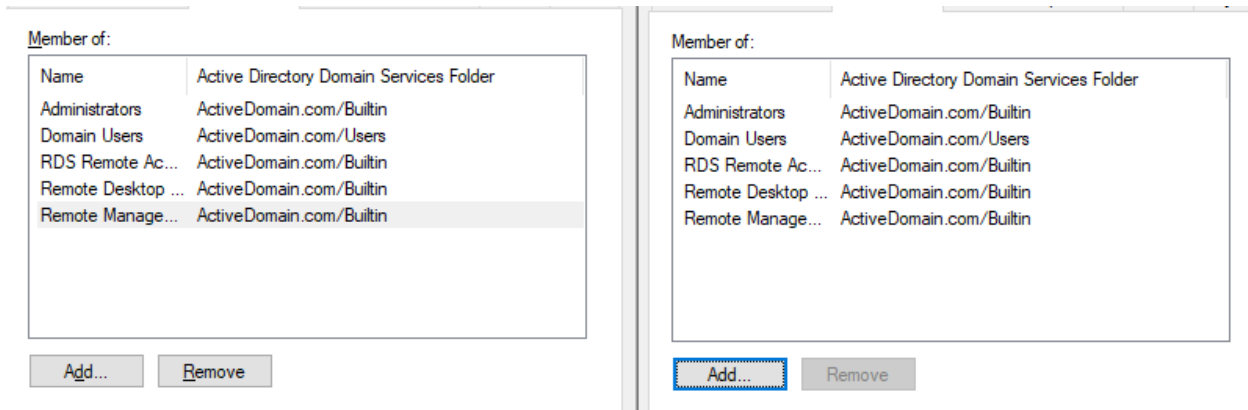
Primary group: Domain Users

Set Primary Group

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

OK Cancel Apply Help

- The permissions also have to be changed. Aisha is now a member of more groups.
- All I would do here is copy the name of the groups that Aisha are not yet a part of, Go to Aisha's Window > Add > paste the name > Check Names > Apply > OK > And repeat for the rest



Now it's done.

To offboard, we would simply do the same, but in reverse. Remove all of the groups they should no longer be a part of and continue.

6 Conclusion

In this third part of the Active Directory Structure Expansion project, we successfully expanded and managed an Active Directory (AD) environment tailored to business-level requirements. By implementing a comprehensive blueprint for Organisational Units (OUs) encompassing users, computers, groups, service accounts, and projects, we have structured a scalable and efficient AD framework.

The deployment of PowerShell scripts to automate the creation of these OUs not only streamlined the setup process but also demonstrated the value of scripting in reducing manual administrative overhead. Additionally, the configuration of various objects within the AD, from user and computer accounts to service accounts and security groups, has enhanced our understanding of resource management and policy enforcement in a complex IT environment.

Through this expansion, we have gained practical experience in managing a business-grade AD setup, including essential tasks such as password resets, user profile management, and the onboarding/offboarding process. This project has equipped us with the skills necessary to handle advanced AD management tasks in a real-world enterprise context, laying a strong foundation for further exploration and professional growth in IT management.