# **Active Directory Infrastructure Setup – CYBERTOUCH SOLUTIONS**

This project involves setting up a **Windows Server Domain Controller** using **Active Directory** for the company **CYBERTOUCH SOLUTIONS**.

The purpose of this deployment is to create a centralised and secure IT infrastructure that supports identity management, device control, and access permissions across the organisation.

---

### ## **Company Structure**

**Cybertouch Solutions** is a small-scale IT services firm that operates within a structured domain environment to support its core departments.

The current infrastructure includes:

* **1 x Windows Server** configured as an **Active Directory (AD) Domain Controller**. This server manages authentication, user accounts, organisational units (OUs), group policies, and network-wide access control.
* **2 x Windows 8 Client PCs** assigned to the:
  + **Human Resources Department** – for administrative and employee data management tasks.
  + **IT Department** – for system maintenance, support, and technical operations within the domain.

The company is structured to allow for future scalability, with Organisational Units and Group Policy Objects already designed to accommodate additional departments or users such as **Sales** and **Audit**, even though they currently operate without assigned PCs (see justification in the OU section).

---

### ## **Project Objectives**

The primary goal of this project is to simulate a functional, centralised IT environment for **Cybertouch Solutions** using Microsoft’s Active Directory services. The project objectives are as follows:

* **Set up and configure an Active Directory Domain Controller** on a Windows Server to serve as the core of network management and authentication.
* **Join client PCs to the domain** to enable centralised control, user authentication, and access management.
* **Create Organisational Units (OUs)** to logically structure departments and user accounts, simplifying administration and applying specific policies.
* **Implement basic Group Policies** to control user access, enforce security settings, and ensure consistent desktop environments across the organisation.
* **Simulate a centralised IT environment** that reflects how small-to-medium businesses manage users, devices, and resources within a domain-based network.

---

## **Network Design**

```

Internet

↓

Router (Gateway: 10.0.5.1)

↓

Switch

┌──────┬─────────────┬──────────────┐

│ │ │ │

Server PC1 (Win 8) PC2 (Win 8)

```

| Device | IP Address | Role |

|---------------|----------------|-----------------------------|

| Windows Server| 10.0.5.7 | AD Domain Controller (DC) |

| Windows 8 PC | DHCP | Client (Human Resource |

| Windows 8 PC | DHCP | IT |

---

## **Domain Configuration**

- \*\*Domain Name\*\*: `CYBERTOUCH. Local`

- \*\*Server Name\*\*: `CYBERTOUCH`

- \*\*Static IP\*\*: `10.0.5.7`

- \*\*AD Roles Installed\*\*: AD DS, DNS (DHCP)

---

### ## **Organisational Units (OUs)**

Using **Active Directory Users and Computers**, four users were created and placed into their respective Organisational Units (OUs). Out of the four users, only the **HR** and **IT** departments were assigned computers, while **Sales** and the **Audit Department** were not.

This was intentional and based on the following valid operational reason:

HR and IT departments require dedicated workstations for daily administrative tasks, data management, and system operations. In contrast, users in Sales and Audit either operate in a mobile or hybrid capacity, often accessing resources through shared devices, remote access, or personal laptops with secure VPN access. As a result, no permanent computer assignment was necessary for those departments at this stage of the deployment.

```

CYBERTOUCH.Local

├── OU: HR Department

│ └── Users: Tope.HR

├── OU: IT Department

│ └── Users: Timothy.IT

├── OU: Sales

│ └── Users:

├── OU: Audit

│ └── Users:

---

## Group Policy (GPO)

Created and linked using \*\*Group Policy Management Console (gpmc.msc) \*\*:

- \*\*GPO Name\*\*: `DisableRemovableDrives,

- \*\*Linked to\*\*: OU: HR Department

- \*\*Policy Configured\*\*:

- `Computer Configuration` > `Administrative Templates` > `System` > `Removable Storage Access`

- Set \*\*"All Removable Storage classes: Deny all access"\*\* to \*\*Enabled\*\*

Result: USB and external drives are disabled for all users in the \*\*Accounts OU\*\*.

---

## Group Policy (GPO)

Created and linked using \*\*Group Policy Management Console (gpmc.msc) \*\*:

- \*\*GPO Name\*\*: `DisableRemovableDrives, Disable Restart Access, and Authentic Poweroff Disabling

- \*\*Linked to\*\*: OU: IT Department

- \*\*Policy Configured\*\*:

- `Computer Configuration` > `Administrative Templates` > `System` > `Removable Storage Access`

- Set \*\*"All Removable Storage classes: Deny all access"\*\* to \*\*Enabled\*\*

## Screenshots

- AD Domain Structure

- GPO Editor Screenshot

- PC joined to domain

- Result of denied USB access

---

### ## **Key Takeaways**

* **Hands-on experience with Windows Server**: Successfully configured and deployed core Windows Server roles, including setting up a functional Active Directory Domain Controller.
* **Centralised access control with Group Policy**: Learned how to implement and manage Group Policy Objects (GPOs) to enforce security settings and user restrictions across the domain.
* **Organisational Unit (OU) structuring**: Gained insight into designing a scalable directory structure by logically organising users and departments into OUs.
* **Applied Identity and Access Management (IAM) principles**: Applied IAM concepts in a real-world simulated environment, emphasising secure access and user role management within a domain.

---

## **Author**

\*\*Ogunbayeje Dare\*\*

Cybersecurity Analyst