Active Directory Help Desk Simulation - L1 Report Project

Author: Mika Gellizeau

Date: 11/19/2025

A practical simulation of real-world Level 1 IT Help Desk identity, access, and ticketing operations in a Windows Server Directory environment.

Table of Contents

📄 Executive Summary

This report documents a complete Level 1 Help Desk simulation built in a controlled Windows Server Active Directory environment. The purpose of this project is to demonstrate practical, job-ready skills in identity and access management, troubleshooting, and ticket documentation—core responsibilities of an entry-level IT Support Technician.

The environment consists of a Windows Server 2022 domain controller and a Windows 11 workstation configured to replicate a small enterprise network. Within this setup, I implemented a realistic organizational structure, created user accounts, assigned security groups, applied group policy, and executed common L1 operational tasks such as password resets, account unlocks, onboarding, offboarding, and workstation domain joins.

To model real support workflows, a multi-ticket simulation was conducted, covering access issues, group modifications, file share troubleshooting, GPO application, and service account maintenance. Each ticket includes a clear problem statement, diagnosis, technical steps, resolution, and SLA considerations—mirroring professional help desk documentation standards.

By completing this project, I demonstrated proficiency in:

- Active Directory administration
- User and group lifecycle management
- Basic networking and DNS dependencies
- Windows client troubleshooting principles
- Ticketing workflows and documentation best practices

This simulation reflects the daily responsibilities of an L1 help desk technician and showcases the foundational skills necessary to support users in a modern Windows-based environment.

🖥️ Environment Overview

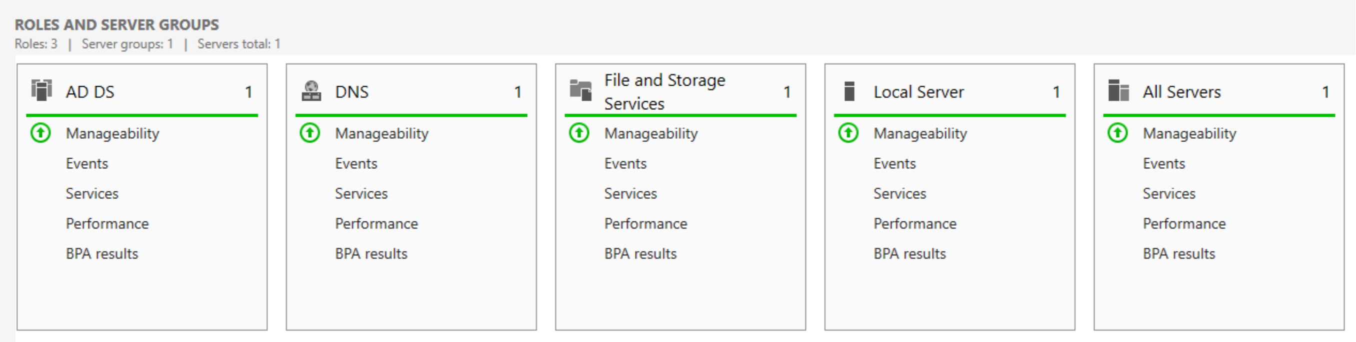
This project was built in a self-contained virtual lab designed to replicate a small enterprise Windows domain environment. The goal was to create a realistic foundation for performing user management, access control, domain joining, and troubleshooting activities commonly handled by Level 1 help desk technicians.

Domain Architecture

The lab uses a single-domain Active Directory forest to simulate a standard small to mid-sized organizational structure. The domain controller hosts Active Directory Domain Services (AD DS) and DNS, ensuring proper name resolution and authentication throughout the environment.

Key Components:

- Domain Name: **mikatech.com**
- Forest Functional Level: **Windows Server 2022**
- Services Used:
  - Active Directory Domain Services
  - DNS Server
  - Group Policy Management



ROLES AND SERVER GROUPS

Roles: 3 | Server groups: 1 | Servers total: 1

AD DS 1
Manageability
Events
Services
Performance
BPA results

DNS 1
Manageability
Events
Services
Performance
BPA results

File and Storage Services 1
Manageability
Events
Services
Performance
BPA results

Local Server 1
Manageability
Events
Services
Performance
BPA results

All Servers 1
Manageability
Events
Services
Performance
BPA results

Virtual Machines

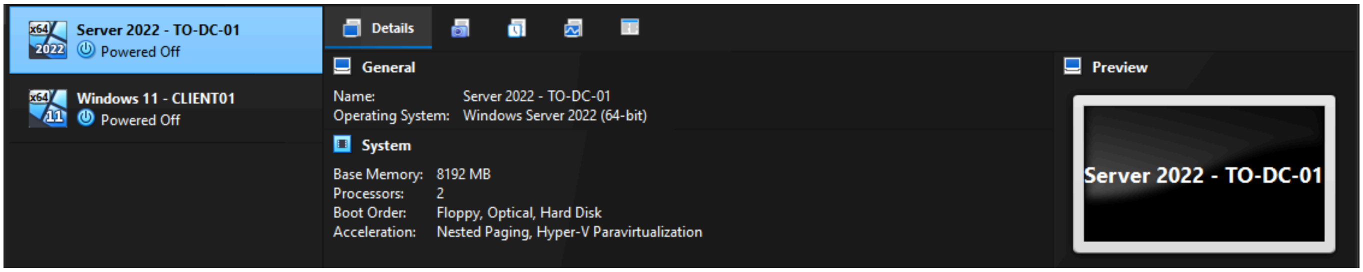
Two virtual machines were deployed to create the environment:

Domain Controller: TO-DC-01

- **OS**: Windows Server 2022
- **Role**: Primary Domain Controller
- **Functionality**:
  - User authentication
  - Group Policy processing
  - DNS resolution
  - Security group and OU management

Client Workstation: CLIENT01

- **OS**: Windows 11
- **Purpose**:
  - Domain join testing
  - User logon verification
  - GPO validation
  - Troubleshooting workflows



Server 2022 - TO-DC-01
Powered Off

Windows 11 - CLIENT01
Powered Off

General

Name: Server 2022 - TO-DC-01
Operating System: Windows Server 2022 (64-bit)

System

Base Memory: 8192 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization

Network Configuration

A host-only internal network was created to isolate the Active Directory environment from the host system and the internet. This ensures controlled testing conditions and prevents external dependencies from affecting the environment.

Domain Controller (TO-DC-01)

- IP Address: **192.168.56.101**
- Subnet Mask: **255.255.255.0**
- Default Gateway: *(Not required for isolated networks)*
- Preferred DNS: **192.168.56.101** *(self)*

Client Workstation (CLIENT01)

- IP Address: **192.168.56.102**
- Subnet Mask: **255.255.255.0**
- Default Gateway: *(Not required for isolated networks)*
- Preferred DNS: **192.168.56.101** *(must point to domain controller for domain join)*

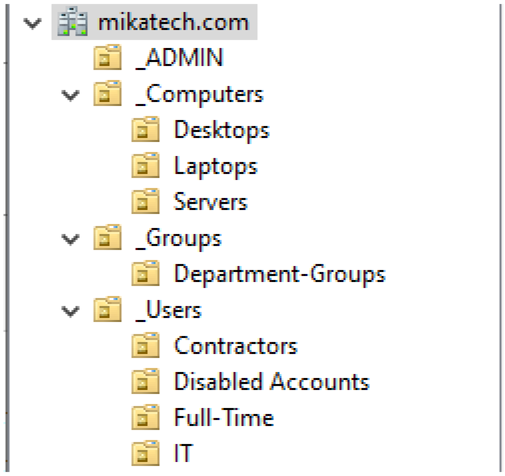
This configuration provides reliable name resolution and domain connectivity, both of which are essential for AD operations

---

OU & Group Structure

A clear and organized Active Directory structure was created to support user management, access control, and workstation administration within the mikatech.com domain. The layout follows common enterprise design principles, separating users, groups, and computer objects to maintain clarity and simplify administration.

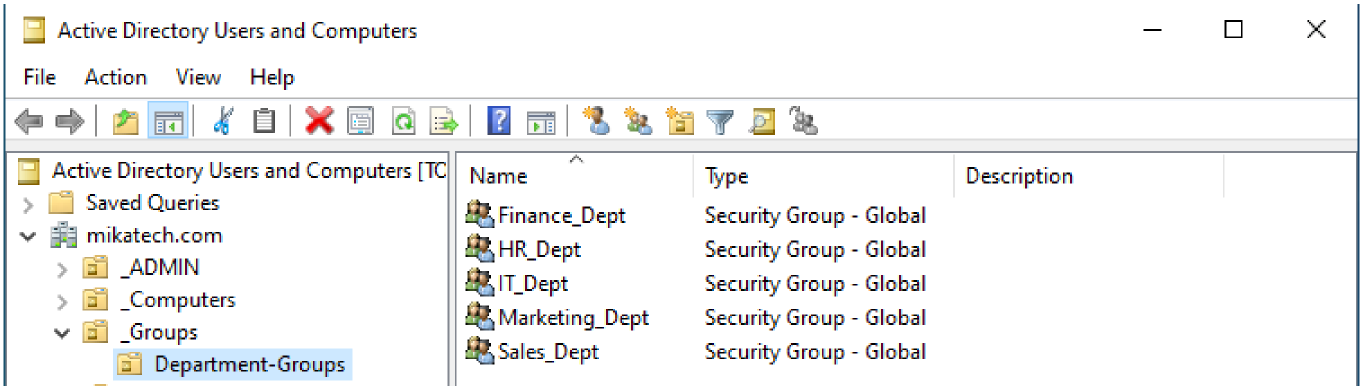
OU Structure (High-Level Overview)



- mikatech.com
  - _ADMIN
  - _Computers
    - Desktops
    - Laptops
    - Servers
  - _Groups
    - Department-Groups
  - _Users
    - Contractors
    - Disabled Accounts
    - Full-Time
    - IT

This structure allows for clean lifecycle management of accounts, logical grouping of permissions, and simplified navigation for day-to-day help desk tasks.

Security Groups (High-Level Overview)



Name	Type	Description
Finance_Dept	Security Group - Global	
HR_Dept	Security Group - Global	
IT_Dept	Security Group - Global	
Marketing_Dept	Security Group - Global	
Sales_Dept	Security Group - Global	

These groups enable consistent access provisioning and align with how permissions are typically managed in real enterprise environments.

👤 Identity & Access Operations

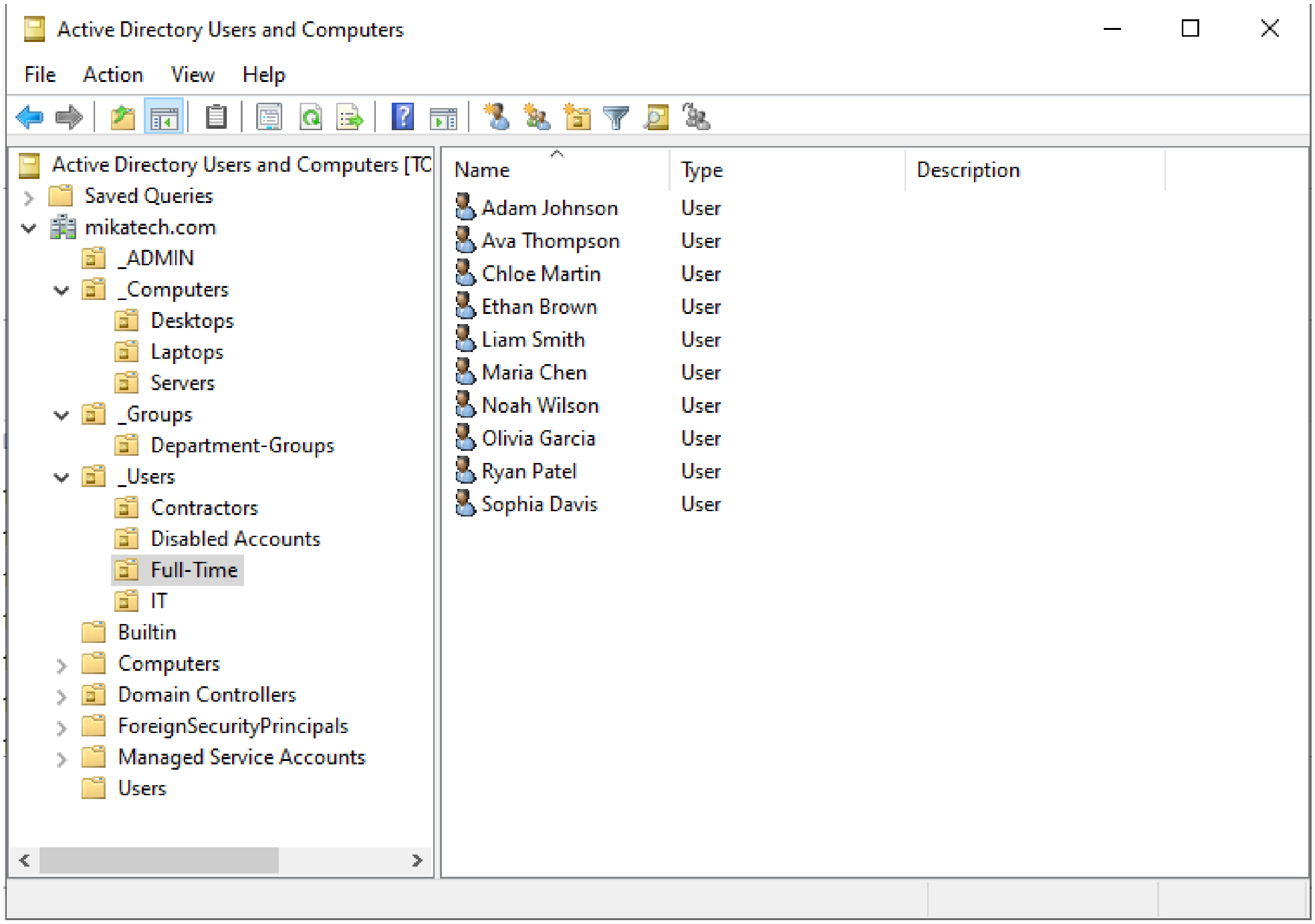
This phase involved performing realistic identity and access management tasks commonly handled by Level 1 help desk technicians. All work was completed using Active Directory Users and Computers (ADUC) and validated from the CLIENT01 workstation.

TASK 1 - User Creation

Ten realistic user accounts were created under **_Users** → **Full-Time**, each configured with:

- First and last name
- Standardized username (e.g., ajohnson)
- Temporary password (MikaTemp123!)
- “User must change password at next logon”
- Assigned department alignment

This establishes the standard identity lifecycle for new employees.



Name	Type	Description
Adam Johnson	User	
Ava Thompson	User	
Chloe Martin	User	
Ethan Brown	User	
Liam Smith	User	
Maria Chen	User	
Noah Wilson	User	
Olivia Garcia	User	
Ryan Patel	User	
Sophia Davis	User	

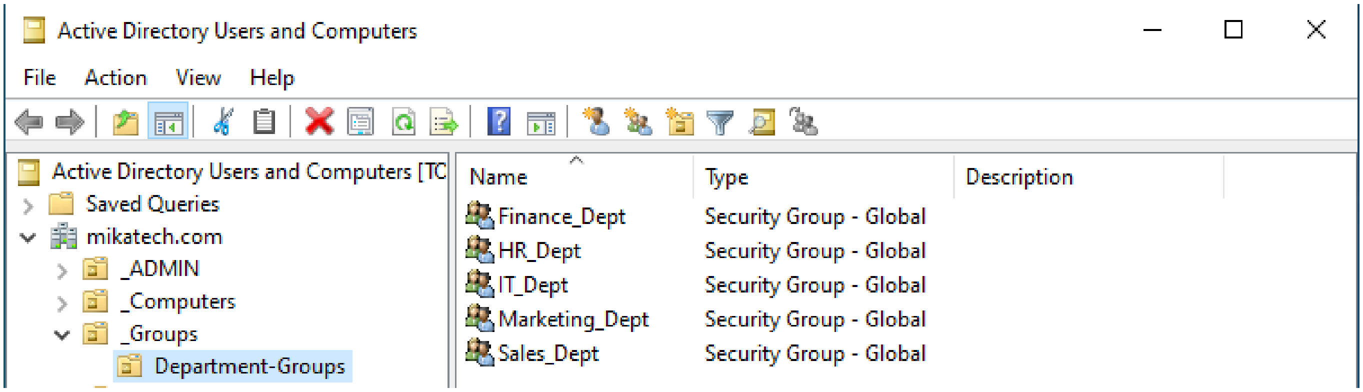
TASK 2 - Create Security Groups

Departmental security groups were created under **_Groups** → **Department-Groups** to support role-based access control.

Users were added to groups such as:

```
([Adam Johnson], [Ethan Brown]) -> Sales_Dept
([Maria Chen], [Chloe Martin]) -> HR_Dept
([Olivia Garcia], [Noah Wilson]) -> Finance_Dept
([Liam Smith], [Sophia Davis]) -> Marketing_Dept
([Ryan Patel], [Ava Thompson]) -> IT_Dept
```

This ensures permissions and file share access are granted based on department rather than per-user assignments.



Name	Type	Description
Finance_Dept	Security Group - Global	
HR_Dept	Security Group - Global	
IT_Dept	Security Group - Global	
Marketing_Dept	Security Group - Global	
Sales_Dept	Security Group - Global	

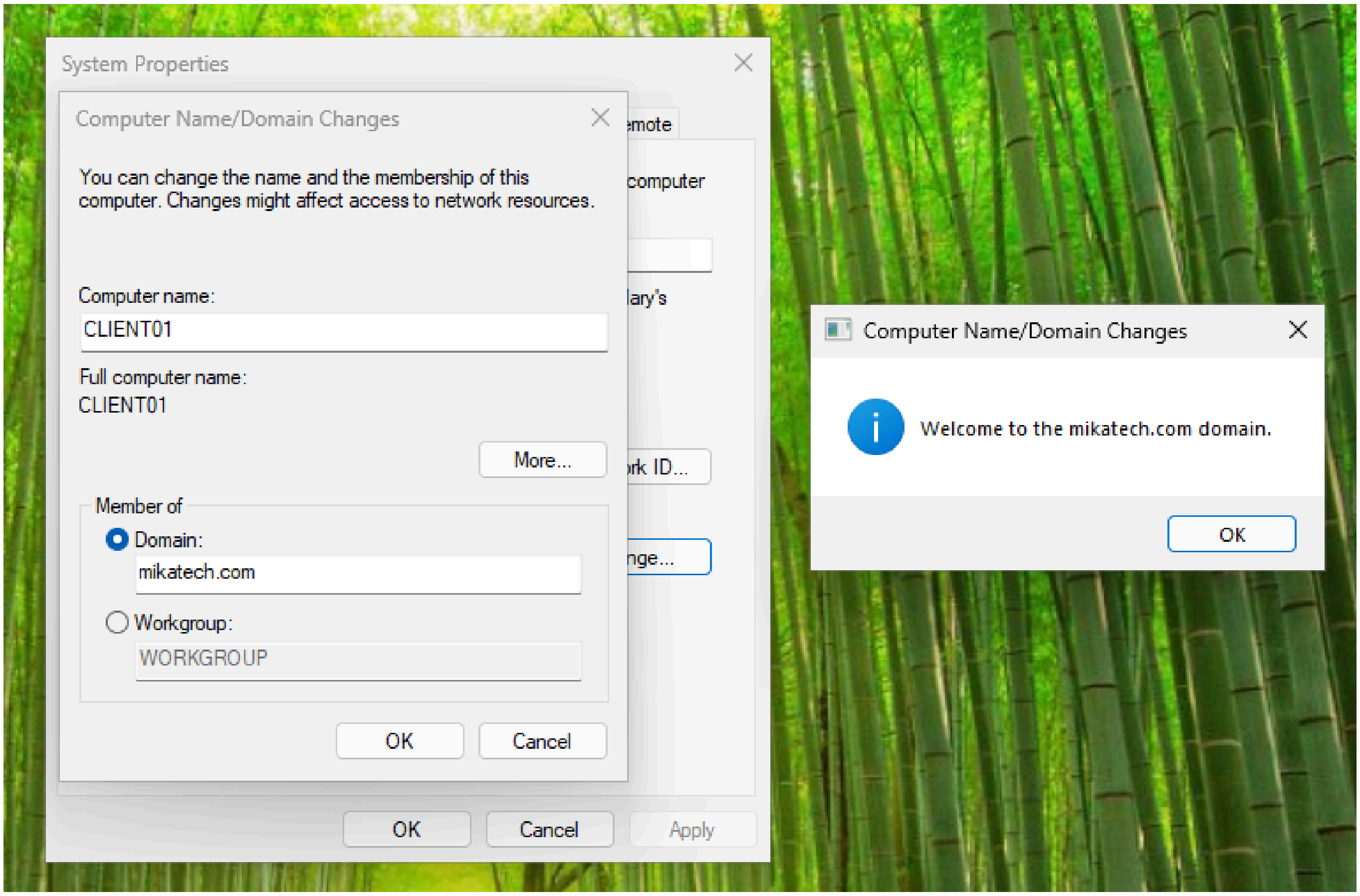
TASK 3 - Workstation Domain Join

The **CLIENT01** workstation was joined to the **mikatech.com** domain to validate authentication and workstation management.

Steps performed:

1. Renamed the PC to **CLIENT01**
2. Joined the domain: **mikatech.com**
3. Enter domain admin credentials
4. Restarted the system
5. Logged in as a standard domain user (**e.g. ajohnson**) to confirm profile creation

This confirms DNS, AD communication, and trust between the server and workstation.



System Properties

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
CLIENT01

Full computer name:
CLIENT01

Member of

● Domain:
mikatech.com

○ Workgroup:
WORKGROUP

Computer Name/Domain Changes

Welcome to the mikatech.com domain.

TASK 4 - Password Reset

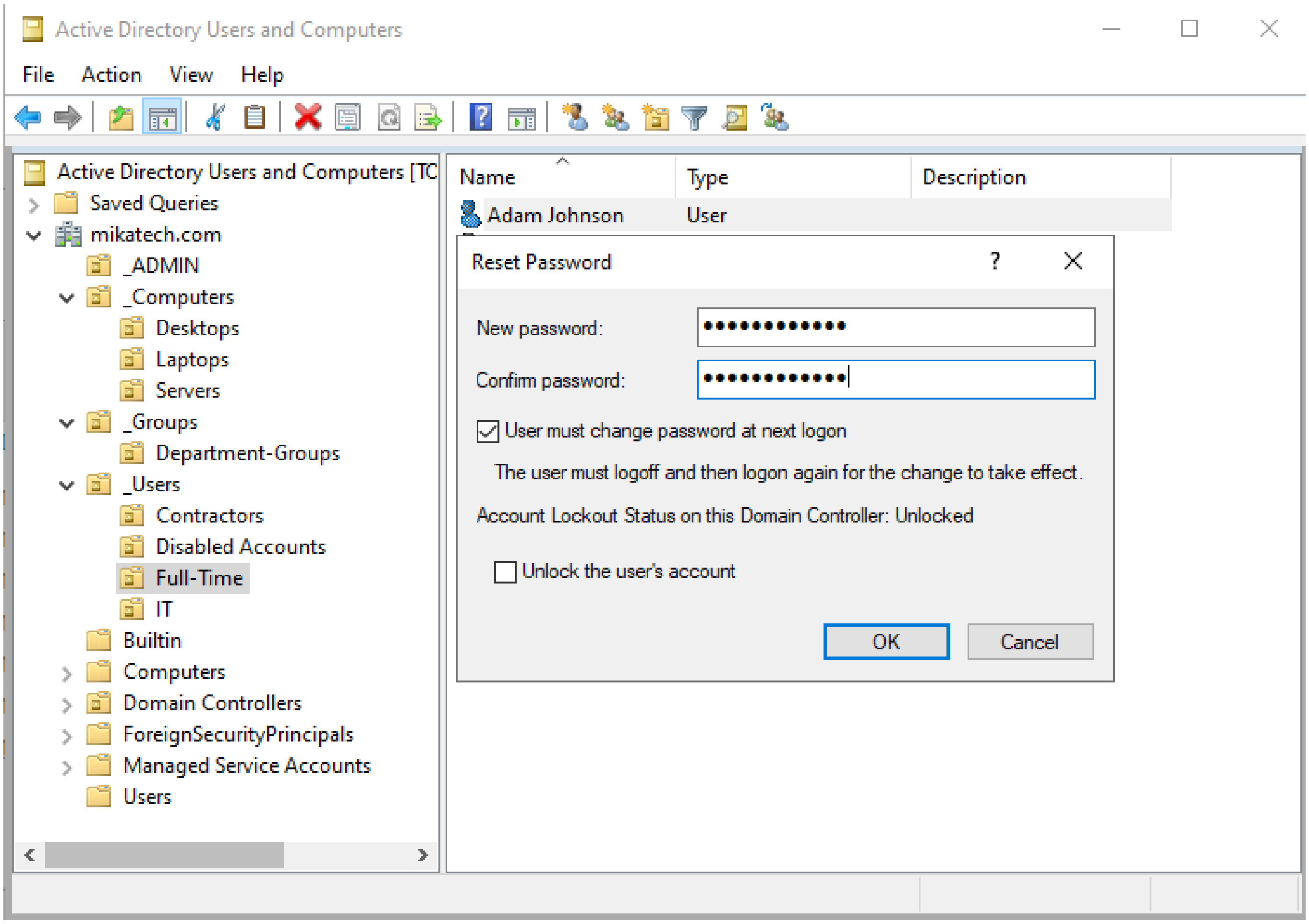
L1 Ticket Scenario:

> “A user, **Adam Johnson**, is unable to sign in because they forgot their password.”

Actions taken:

1. Located the user in ADUC
2. Reset password to a temporary value (e.g., `MikaTemp123!`)
3. Enabled “User must change password at next logon”
4. Instructed the user to sign in and set a new password.
5. Verified successful login on **CLIENT01**

This demonstrates secure password reset procedures common in L1 support.



Name	Type	Description
Adam Johnson	User	

Reset Password

New password: ••••••••••••

Confirm password: ••••••••••••

☑ User must change password at next logon

The user must logoff and then logon again for the change to take effect.

Account Lockout Status on this Domain Controller: Unlocked

☐ Unlock the user's account

TASK 5 - Account Lockout

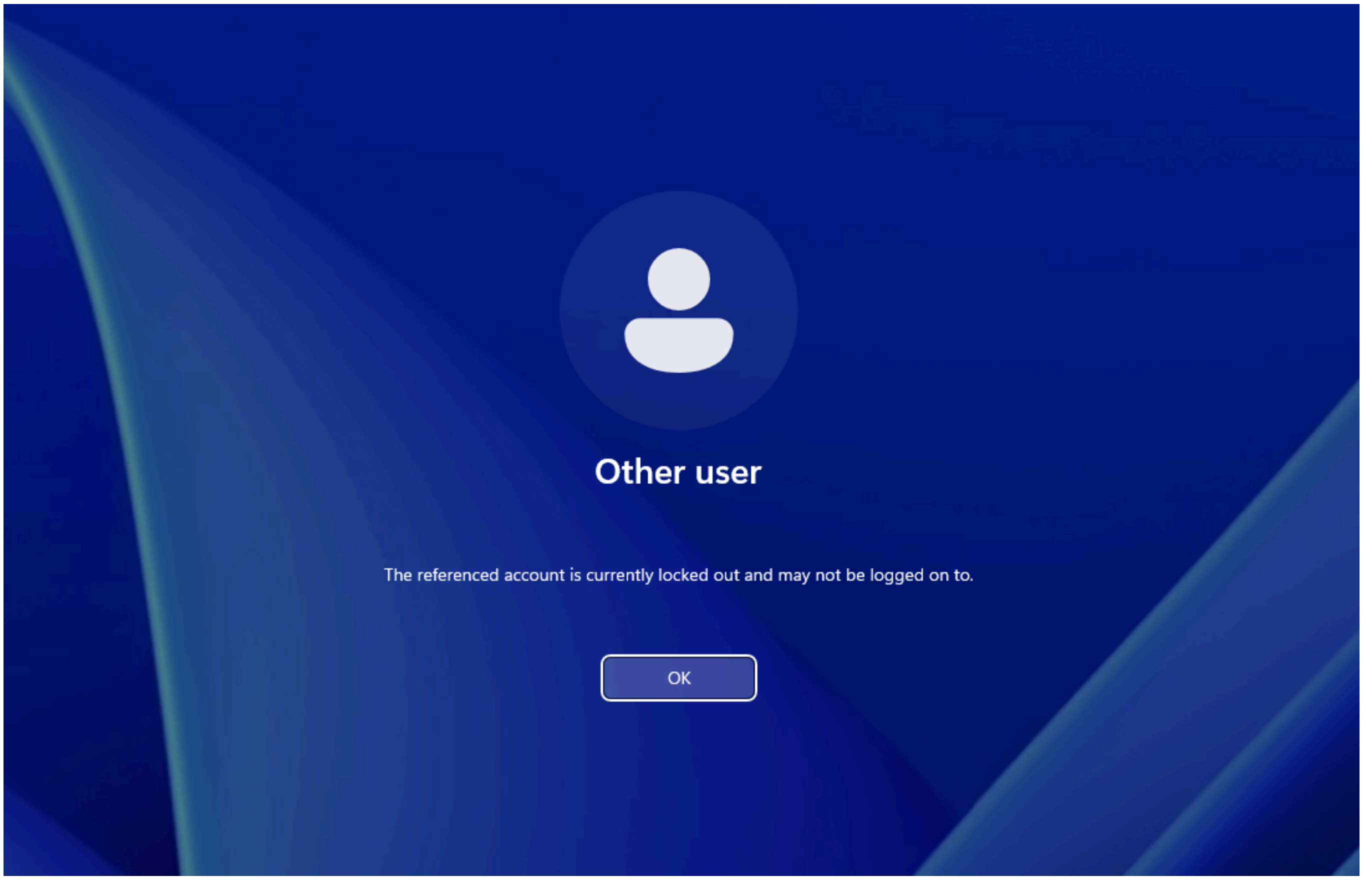
L1 Ticket Scenario:

> "A user, **Adam Johnson**, is locked out because they exceeded the permitted login attempts."

Actions taken:

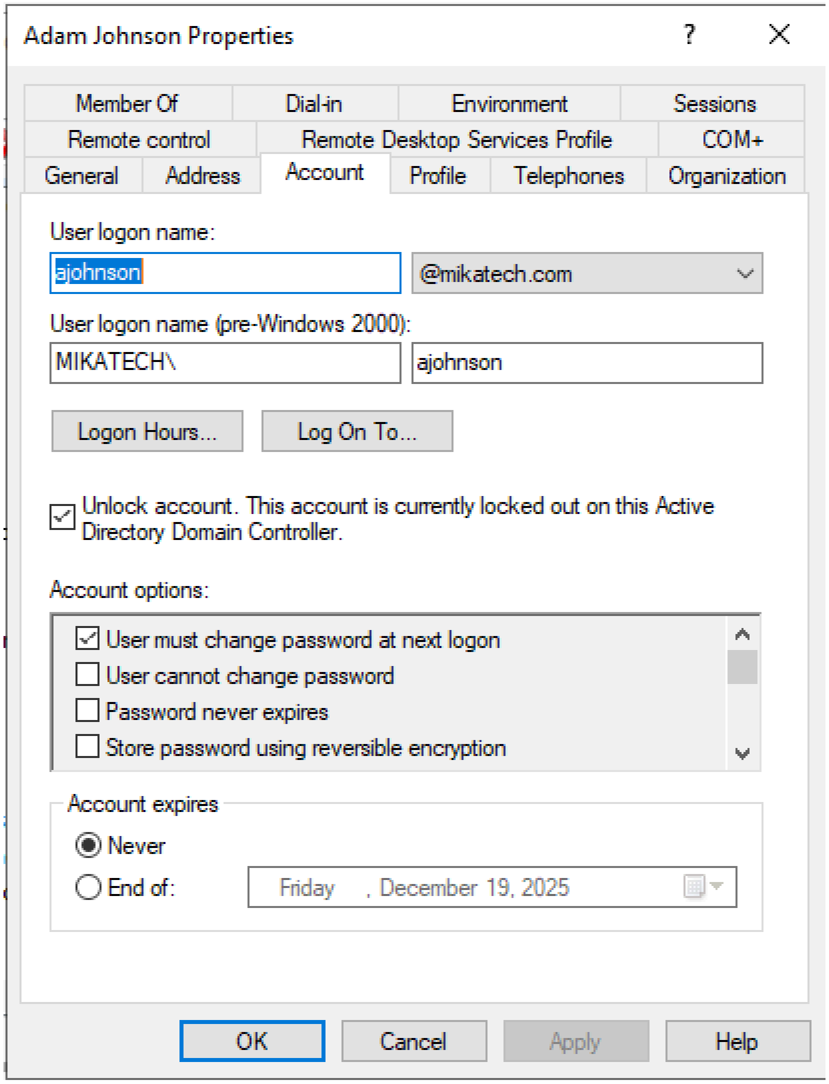
1. Located the account in ADUC
2. Verified lockout status
3. Used the **Unlock account** checkbox
4. Performed optional password reset
5. Confirmed the user could log in from CLIENT01

This reflects typical troubleshooting for account lockouts caused by cached credentials or repeated failed logins.



Other user

The referenced account is currently locked out and may not be logged on to.



User logon name: ajohnson @mikatech.com

User logon name (pre-Windows 2000): MIKATECH\ ajohnson

☑ Unlock account. This account is currently locked out on this Active Directory Domain Controller.

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: Friday , December 19, 2025

TASK 6 - Employee Onboarding

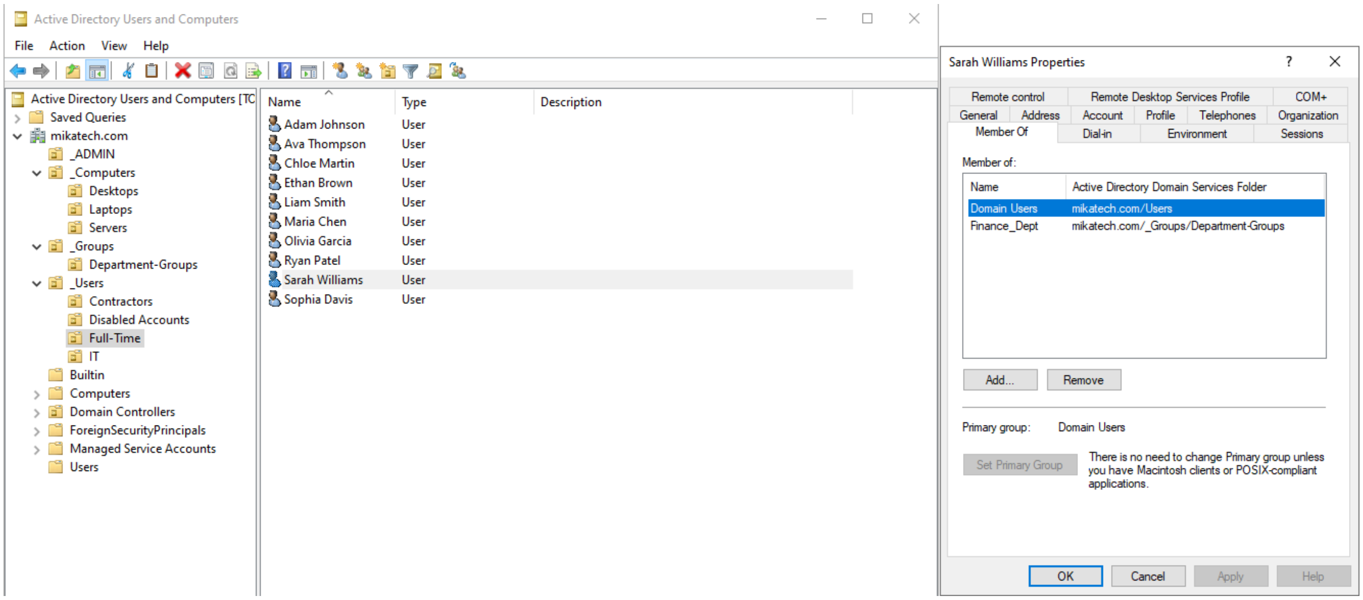
L1 Ticket Scenario:

> "A new employee, **Sarah Williams**, was onboarded as part of the Finance department."

Actions taken:

1. Created `swilliams` under `_Users → Full-Time`
2. Set temporary password with forced change at next logon
3. Added user to `Finance_Dept`
4. Completed user description with department and job title
5. Logged into CLIENT01 as `swilliams` to confirm:
    - New profile creation
    - Domain login success
    - Group-based access applied

This simulates a realistic new hire provisioning workflow.



- Active Directory Users and Computers [TC
  - Saved Queries
  - mikatech.com
    - _ADMIN
    - _Computers
      - Desktops
      - Laptops
      - Servers
    - _Groups
      - Department-Groups
    - _Users
      - Contractors
      - Disabled Accounts
      - Full-Time
      - IT
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Users

Name	Type	Description
Adam Johnson	User	
Ava Thompson	User	
Chloe Martin	User	
Ethan Brown	User	
Liam Smith	User	
Maria Chen	User	
Olivia Garcia	User	
Ryan Patel	User	
Sarah Williams	User	
Sophia Davis	User	

Member of:

Name	Active Directory Domain Services Folder
Domain Users	mikatech.com/Users
Finance_Dept	mikatech.com/_Groups/Department-Groups

Primary group: Domain Users

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

TASK 7 - Employee Offboarding

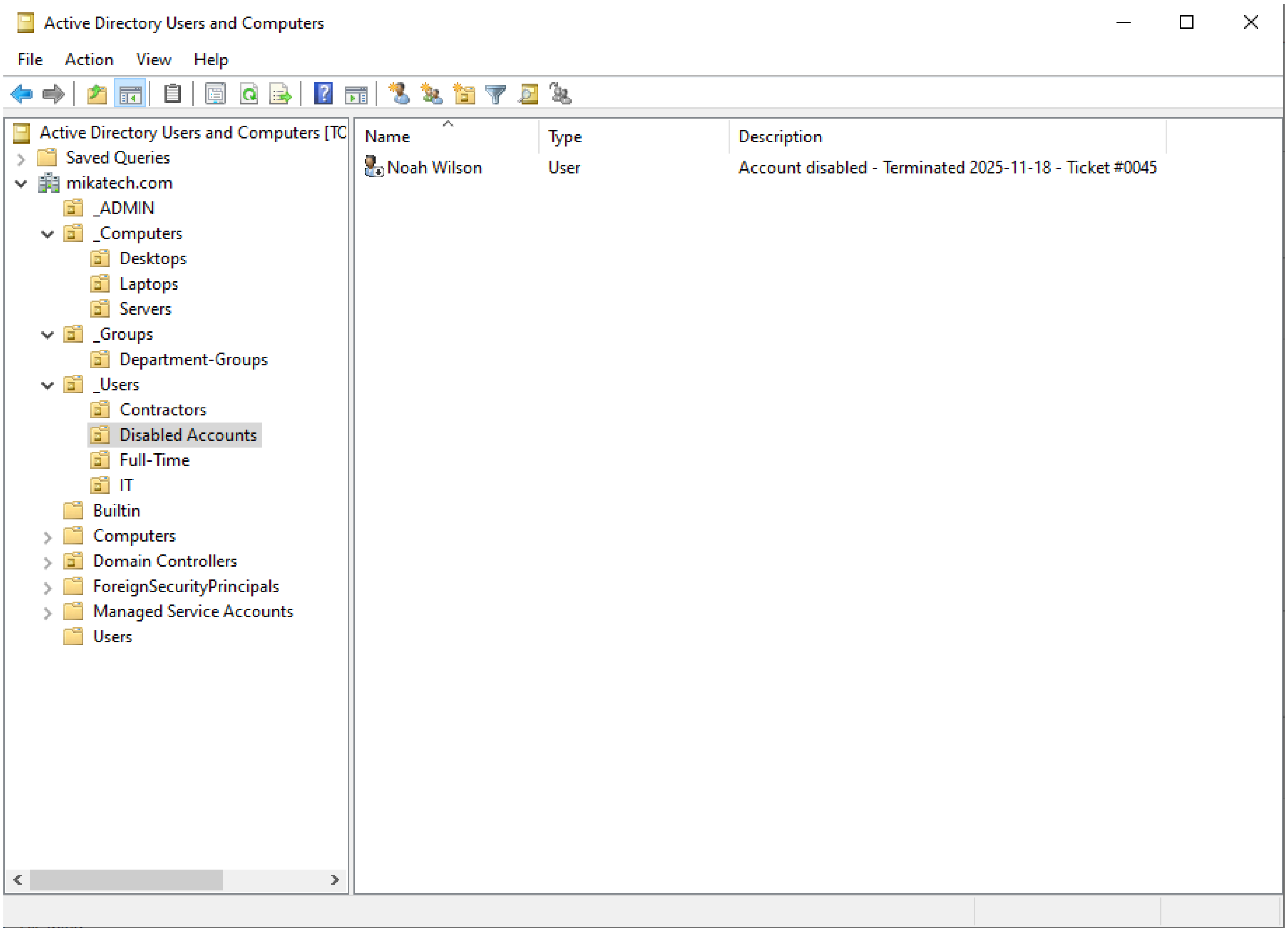
L1 Ticket Scenario:

> "The employee, **Noah Wilson**, is scheduled for termination at end of day."

Steps performed:

1. Located the user account in ADUC
2. Disabled the account to prevent further login
3. Moved the account to `_Users → Disabled Accounts`
4. Reset the password to a strong random value
5. Optionally removed non-essential group memberships
6. Updated the Description field, e.g., `"Terminated 2025-11-18"`

This reflects proper account lifecycle management and access revocation.



Name	Type	Description
Noah Wilson	User	Account disabled - Terminated 2025-11-18 - Ticket #0045

🎫 Ticketing Simulation

Ticket Workflow Overview

After establishing the environment and core identity workflows, the next step was to simulate the **daily ticket queue of an L1 help desk technician**.

For this phase:

- Eight realistic tickets were created
- Each ticket reflects a common enterprise request or incident
- Focus areas included **clear documentation**, **accurate diagnosis**, and **professional resolution notes**

Each ticket includes:

- Problem description
- Diagnosis
- Technical steps performed
- Final resolution
- Root cause
- SLA timing
- Customer confirmation

This mirrors what L1 technicians are expected to document in a real ticketing system.

Ticket Summary Table

Ticket #	Category	Affected Entity	Priority	Short Description
003218	Email / M365 Request	Olivia Garcia	Low	New email alias for vendor-facing communication
003219	Access / Groups	Adam Johnson	Medium	Add user to resource access group
003220	GPO / Restrictions	HR Department	Low	Apply GPO to restrict Control Panel
003221	File Share / Drive Mapping	Sophia Davis	Medium	Marketing drive not mapped to `M:`
003222	Identity / MFA Preparation	Ethan Brown	Medium	Add user to MFA pending group
003223	Service Account	svc_backup	High	Service account password reset
003224	HR Data Change	Chloe Martin	Low	Update job title, manager, and phone
003225	Security / Offboarding	Ryan Patel	High	Termination audit and access verification

> *The following tickets are presented in a “day in the life” style, reflecting how an L1 technician receives, diagnoses, and resolves issues throughout a typical workday.*

Ticket 003218 – Email Alias Request

User: Olivia Garcia (`ogarcia`) – Finance
Priority: Low

Problem:
“A user is unable to sign in because they forgot their password.”

User requested an additional email alias `accounts-payable@mikatech.com` to streamline communication with external vendors.

Diagnosis:
Verified identity and reviewed mailbox details. Confirmed alias request with Finance management.

Steps Performed:

- Opened simulated Microsoft 365 Admin Center
- Retrieved mailbox for `ogarcia`
- Added alias `accounts-payable@mikatech.com`
- Verified correct formatting and documented the change

Resolution:
Alias successfully added as a secondary address for `ogarcia`.

Root Cause:
Planned business request.

SLA:
27 minutes

Customer Confirmation:
User confirmed successful delivery to the alias.

Ticket 003219 – Add User to Resource Access Group

User: Adam Johnson (`ajohnson`) – Sales
Priority: Medium

Problem:
User unable to access Sales shared folder mapped to `\\TO-DC-01\SalesData`.

Diagnosis:
Checked AD group membership. User was not part of `Sales_Dept`.

Steps Performed:

1. Opened ADUC
2. Navigated to `_Groups → Department-Groups → Sales_Dept`
3. Added `ajohnson` to `Sales_Dept`
4. Instructed user to log off/on or ran `gpupdate /force`
5. Confirmed access to SalesData

Resolution:
Access restored.

Root Cause:
User not added to correct group during onboarding.

SLA:
18 minutes

Customer Confirmation:
User confirmed full access to all Sales files.

Ticket 003220 – Apply Control Panel Restriction via GPO

User: HR Department
Priority: Low (Scheduled Change)

Problem:
Management requested that HR users be prevented from accessing Control Panel.

Diagnosis:
Planned configuration change.

Steps Performed:

1. Opened Group Policy Management
2. Created GPO: `HR-ControlPanel-Restriction`
3. Enabled **Prohibit access to Control Panel**
4. Linked GPO to HR OU
5. Logged into CLIENT01 as HR test user and ran `gpupdate /force`
6. Tested Control Panel access

Resolution:
Control Panel successfully restricted for HR.

Root Cause:
Intentional configuration change.

SLA:
32 minutes

Customer Confirmation:
HR management confirmed expected behavior.

Ticket 003221 – Marketing Drive Mapping Issue

User: Sophia Davis (`sdavis`) – Marketing
Priority: Medium

Problem:
Marketing drive (`M:`) missing after login.

Diagnosis:
Verified membership in `Marketing_Dept`. Drive mapping script/GPO did not apply.

Steps Performed:

1. Opened File Explorer on CLIENT01
2. Selected “Map network drive”
3. Assigned drive letter **M:**
4. Used path `\\TO-DC-01\Marketing`
5. Confirmed file access
6. Flagged the missing auto-apply issue to L2

Resolution:
Drive manually mapped.

Root Cause:
Drive-mapping GPO or script not applying.

SLA:
14 minutes

Customer Confirmation:
User confirmed that `M:` appeared and worked normally.

Ticket 003222 – MFA Pending Group Assignment

User: Ethan Brown (`ebrown`) – Sales (temporary project)
Priority: Medium

Problem:
User must be placed into MFA enrollment workflow.

Diagnosis:
Reviewed HR/IT notes confirming requirement.

Steps Performed:

1. Navigated to `_Groups → MFA_Pending` in ADUC
2. Added `ebrown` to MFA_Pending
3. Documented usage of MFA group (simulated Azure AD sync)
4. Notified Cloud/IT team

Resolution:
User added to MFA_Pending.

Root Cause:
Planned onboarding change.

SLA:
11 minutes

Customer Confirmation:
User acknowledged the upcoming MFA enrollment process.

Ticket 003223 – Service Account Password Reset

Account: `svc_backup` – Service Account
Priority: High

Problem:
Backup scripts failing due to authentication errors.

Diagnosis:
Password expired for `svc_backup`.

Steps Performed:

1. Opened ADUC → `_Users → IT`
2. Located `svc_backup`
3. Reset password to strong value
4. Enabled **Password never expires**
5. Updated Description field
6. Notified infrastructure team

Resolution:
Service account restored.

Root Cause:
Password expired; account not set to non-expiring.

SLA:
9 minutes

Customer Confirmation:
Infrastructure team acknowledged and updated scripts.

Ticket 003224 – HR Attribute Update

User: Chloe Martin (`cmartin`) – HR
Priority: Low

Problem:
HR requested updates to job title, manager, and phone number.

Diagnosis:
Verified details with HR.

Steps Performed:

1. Opened `cmartin` properties
2. Updated Job Title, Manager, Telephone
3. Saved and verified

Resolution:
Attributes updated successfully.

Root Cause:
HR data maintenance.

SLA:
16 minutes

Customer Confirmation:
HR confirmed fields matched internal records.

Ticket 003225 – Termination Audit Verification

User: Ryan Patel (`rpatel`) – IT
Priority: High / Security

Problem:
End-of-day termination must be confirmed.

Diagnosis:
Account remained active at the time of review.

Steps Performed:

1. Opened user properties
2. Disabled account
3. Reset password
4. Moved to `_Users → Disabled Accounts`
5. Removed all non-default groups
6. Updated Description
7. Attempted login from CLIENT01

Resolution:
Account fully disabled and secured.

Root Cause:
Planned termination procedure.

SLA:
12 minutes

Customer Confirmation:
Security confirmed the account was inaccessible.

🧩 Skills Demonstrated

Throughout this Active Directory Help Desk Simulation, a wide range of foundational IT support skills were demonstrated. These skills align directly with the daily responsibilities of a Level 1 Help Desk Technician and reflect practical, real-world troubleshooting and identity management workflows.

Technical Skills

Active Directory Administration

- Created and managed user accounts in organizational OUs
- Performed password resets and account unlocks
- Managed department security groups and group membership
- Disabled, secured, and relocated terminated accounts
- Updated user attributes (title, phone, manager)

Group Policy Fundamentals

- Created and linked a GPO to restrict Control Panel access for HR
- Validated policy application using CLIENT01 and manual policy refresh
- Understood OU targeting and user-based configuration

Workstation Configuration

- Joined a Windows 11 workstation (CLIENT01) to the domain
- Performed login validation using standard domain accounts
- Mapped network drives and verified access to shared resources

Service Account Handling

- Located service accounts
- Reset service account passwords using secure practices
- Documented password resets and coordinated with infrastructure teams

---

Troubleshooting & Diagnostic Skills

Identity & Access Issues

- Identified group membership issues preventing file share access
- Diagnosed lockout events and resolved login failures
- Verified user permissions through ADUC and workstation testing

File Share & Drive Mapping

- Diagnosed missing mapped drives and validated share availability
- Differentiated between user error, missing group membership, and GPO/script issues
- Escalated environment-wide issues appropriately (L2 escalation)

Ticket Analysis & Root Cause Evaluation

- Distinguished planned changes from break/fix incidents
- Investigated underlying causes of access failures
- Provided clear, concise technical documentation for each ticket

Professional & Operational Skills

Ticket Documentation & Communication

- Logged issues using real help desk documentation structure
- Captured root cause, resolution steps, SLA timing, and confirmation notes
- Wrote user-friendly explanations and updates
- Simulated real communication flow with end users and internal teams

Prioritization & SLA Awareness

- Addressed high-priority service account outages first
- Completed routine HR changes within expected SLA windows
- Managed multiple ticket types across different departments

Change Management Awareness

- Properly documented scheduled changes (GPO application, alias additions)
- Ensured user confirmation before ticket closure
- Coordinated with HR and IT teams for onboarding/offboarding changes

🔚 Conclusion

This project successfully simulated a full Level 1 Help Desk workflow within a controlled Active Directory environment. By building a domain from the ground up, configuring users and groups, joining a workstation to the domain, and resolving realistic support tickets, this lab demonstrated the essential operational skills required to support users in a modern Windows-based organization.

Across all phases, the tasks performed reflected real help desk responsibilities, including identity lifecycle management, access troubleshooting, workstation validation, GPO application, and clear ticket documentation. Each ticket followed industry-standard practices for diagnosis, technical execution, SLA awareness, and user communication—mirroring the expectations of a professional support environment.

The experience reinforced practical competencies such as:

- Active Directory administration
- Account provisioning and deprovisioning
- Group-based access control
- Password resets and lockout resolution
- Workstation troubleshooting and domain validation
- Service account maintenance
- Ticket documentation and prioritization

Overall, this project provides a strong foundation in help desk operations and showcases the hands-on skills necessary for supporting users, maintaining account security, and contributing to efficient IT service delivery in an enterprise environment.