# AD Project - Test Cases & Configuration Guide

## HR & IT Department Only

## 1. GPO CONFIGURATION (4 GPOs Only)

### GPO 1: Domain-PasswordPolicy

Where to apply: corp.local (root domain)

Settings to configure:

Computer Configuration > Policies > Windows Settings >
Security Settings > Account Policies > Password Policy

- Minimum password length: 10 characters
- Password must meet complexity requirements: Enabled
- Enforce password history: 3 passwords
- Maximum password age: 90 days
- Account lockout threshold: 5 invalid logon attempts
- Account lockout duration: 30 minutes
- Reset account lockout counter after: 30 minutes

How to verify: On a client, run `gpupdate /force`, then check settings in `gpedit.msc`

Screenshot needed: Show the Password Policy settings window

### GPO 2: Domain-WindowsFirewall

Where to apply: corp.local (root domain)

Settings to configure:

Computer Configuration > Policies >
Windows Settings > Security Settings >
Windows Defender Firewall with Advanced Security

Domain Profile: ON (inbound: block, outbound: allow)
Private Profile: ON
Public Profile: ON

How to verify: On client, go to Windows Security → Firewall & Network Protection. All should show "ON"

Screenshot needed: Show Windows Security with Firewall status

### GPO 3: Domain-ScreenLockPolicy

Where to apply: corp.local (root domain)

Settings to configure:

```
Computer Configuration > Policies >
Windows Settings > Security Settings > Local Policies >
Security Options

- Interactive logon: Require smartcard: No
- Interactive logon: Require sign-in using Ctrl+Alt+Delete: Yes
- Interactive logon: Machine inactivity limit: 900 seconds (15 minutes)
```

How to verify: Leave workstation idle for 15 minutes. It should lock automatically.

Screenshot needed: Screenshot of locked screen after inactivity

### GPO 4: Domain-DriveMapping

Where to apply: OU=Users,DC=corp,DC=local

Settings to configure:

```
User Configuration > Preferences >
Windows Settings > Drive Maps

Drive Z: \\FileServer\Common (Map for All Users)
Drive H: \\FileServer\HR (Map only if user in GRP-HR-Users group)
Drive I: \\FileServer\IT (Map only if user in GRP-IT-Users group)
```

How to verify: Log in as HR user. Open File Explorer. You should see Z: and H: drives.

Screenshot needed: File Explorer showing mapped drives (Z:, H: for HR user)

## 2. SIMPLE TEST CASES (10 Tests)

### Test 1: Domain User Logon

What: HR user logs into domain workstation

Steps:

1. At login screen, enter: corp\hr.staff.1
2. Enter password
3. Click Sign In

Expected: User logs in successfully, desktop appears

Proof: Take screenshot of desktop

### Test 2: Failed Logon + Event Log

What: Intentionally fail login 5 times to trigger account lockout

Steps:

1. At login screen, try wrong password
2. Repeat 4 more times
3. On 6th attempt, should say "Account locked"
4. Check Event Viewer on DC for Event ID 4740

Expected: Account gets locked after 5 failures

Proof: Screenshot of "Account locked" message + Event ID 4740 in Event Viewer

### Test 3: HR Access to HR Share

What: HR user should access \\FileServer\HR successfully

Steps:

1. Log in as hr.staff.1
2. Open File Explorer

3. Go to \\FileServer\HR

Expected: Folder opens successfully

Proof: Screenshot showing folder contents

### Test 4: HR Cannot Access IT Share

What: HR user should be denied access to \\FileServer\IT

Steps:

1. Log in as hr.staff.1
2. Open File Explorer
3. Try to go to \\FileServer\IT

Expected: "Access Denied" message appears

Proof: Screenshot of access denied error

### Test 5: IT Access to IT Share

What: IT user should access \\FileServer\IT successfully

Steps:

1. Log in as it.admin
2. Open File Explorer
3. Go to \\FileServer\IT

Expected: Folder opens successfully

Proof: Screenshot showing folder contents

### Test 6: IT Cannot Access HR Share

What: IT user should be denied access to \\FileServer\HR

Steps:

1. Log in as it.admin
2. Open File Explorer
3. Try to go to \\FileServer\HR

Expected: "Access Denied" message appears

Proof: Screenshot of access denied error

### Test 7: All Users Access Common Share

What: Both HR and IT users should access \\FileServer\Common
Steps:
1. Log in as hr.staff.1
2. Open File Explorer → \\FileServer\Common → success
3. Log in as it.admin
4. Open File Explorer → \\FileServer\Common → success

Expected: Both users can access Common share
Proof: Screenshots showing access granted for both users

### Test 8: Drive Mapping for HR User

What: HR user should see Z: and H: mapped automatically
Steps:
1. Log in as hr.staff.1
2. Open File Explorer
3. Look at left sidebar under "This PC"

Expected: Z: (Common) and H: (HR) appear automatically
Proof: Screenshot of File Explorer showing mapped drives

### Test 9: Drive Mapping for IT User

What: IT user should see Z: and I: mapped automatically
Steps:
1. Log in as it.admin
2. Open File Explorer
3. Look at left sidebar under "This PC"

Expected: Z: (Common) and I: (IT) appear automatically
Proof: Screenshot of File Explorer showing mapped drives

### Test 10: Firewall Status

What: Firewall should be ON on all domain clients
Steps:

1. Log in to workstation
2. Open Windows Security (search "Windows Security")
3. Click "Firewall & Network Protection"

Expected: Shows "ON" for all three profiles (Domain, Private, Public)
Proof: Screenshot of Windows Security showing firewall ON

## 3. USERS TO CREATE

### HR Department Users

Username: hr.manager
Full Name: HR Manager
Department: HR
Group Membership: GRP-HR-Users, GRP-All-Users

Username: hr.staff.1
Full Name: HR Staff One
Department: HR
Group Membership: GRP-HR-Users, GRP-All-Users

Username: hr.staff.2
Full Name: HR Staff Two
Department: HR
Group Membership: GRP-HR-Users, GRP-All-Users

### IT Department Users

Username: it.admin
Full Name: IT Administrator
Department: IT
Group Membership: GRP-IT-Users, GRP-All-Users

Username: it.support
Full Name: IT Support
Department: IT
Group Membership: GRP-IT-Users, GRP-All-Users

### Test User (for permission testing)

Username: test.user
Full Name: Test User
Department: None
Group Membership: GRP-All-Users only (no department access)

## 4. SECURITY GROUPS TO CREATE

### Global Groups (for users)

Name: GRP-HR-Users
Type: Global / Security
Members: hr.manager, hr.staff.1, hr.staff.2
Purpose: Contains all HR staff

Name: GRP-IT-Users
Type: Global / Security
Members: it.admin, it.support
Purpose: Contains all IT staff

Name: GRP-All-Users
Type: Global / Security
Members: hr.manager, hr.staff.1, hr.staff.2, it.admin, it.support, test.user
Purpose: Contains everyone (for common share access)

### Domain Local Groups (for file share permissions)

Name: DL-HR-Share
Type: Domain Local / Security
Members: GRP-HR-Users
Purpose: Applied to \\FileServer\HR with Modify permissions

Name: DL-IT-Share
Type: Domain Local / Security
Members: GRP-IT-Users
Purpose: Applied to \\FileServer\IT with Modify permissions

Name: DL-Common-Share
Type: Domain Local / Security
Members: GRP-All-Users
Purpose: Applied to \\FileServer\Common with Read/Write permissions

## 5. FILE SHARE PERMISSIONS

### Share 1: HR

UNC Path: \\FileServer\HR
NTFS Permissions:

- DL-HR-Share: Modify (Read, Write, Delete)
- Domain\Domain Admins: Full Control
- Everyone: Remove / Deny (except above)

Share Permissions:

- DL-HR-Share: Change
- Domain\Domain Admins: Full Control

Result: Only HR staff can access; IT staff get "Access Denied"

### Share 2: IT

UNC Path: \\FileServer\IT
NTFS Permissions:

- DL-IT-Share: Modify (Read, Write, Delete)

- Domain\Domain Admins: Full Control
- Everyone: Remove / Deny (except above)

Share Permissions:

- DL-IT-Share: Change
- Domain\Domain Admins: Full Control

Result: Only IT staff can access; HR staff get "Access Denied"

### Share 3: Common

UNC Path: \\FileServer\Common
NTFS Permissions:

- DL-Common-Share (GRP-All-Users): Modify
- Domain\Domain Admins: Full Control
- Everyone: Remove / Deny (except above)

Share Permissions:

- DL-Common-Share: Change
- Domain\Domain Admins: Full Control

Result: All domain users can read and write; non-domain users blocked

## 6. AUDIT EVENTS TO TRACK

### Enable These Audit Policies

Go to: Group Policy Management Editor → Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies

| Category | Subcategory | Success | Failure | Event IDs |
|---|---|---|---|---|
| Logon/Logoff | Logon | ✓ Yes | ✓ Yes | 4624, 4625 |
| Logon/Logoff | Account Lockout | ✓ Yes | ✓ Yes | 4740 |

| | | | | |
|---|---|---|---|---|
| Logon/Logoff | Group Membership | ✓ Yes | ✗ No | 4628 |
| Account Management | User Account Management | ✓ Yes | ✗ No | 4720, 4722 |
| Account Management | Security Group Management | ✓ Yes | ✗ No | 4728, 4756 |
| Privilege Use | Sensitive Privilege Use | ✓ Yes | ✓ Yes | 4673 |

### What Event IDs Mean

- 4624: Successful logon (good login)
- 4625: Failed logon (wrong password)
- 4740: Account locked out (too many wrong passwords)
- 4720: User account created
- 4722: User account enabled/disabled
- 4728/4756: User added to group
- 4673: Sensitive privilege used (admin action)

## 7. FINAL DELIVERABLES CHECKLIST

### Documentation

- Architecture diagram (DC, File Server, Clients)
- Screenshot showing OU structure in ADUC
- List of all users and their groups
- List of all security groups and members
- File share permissions table

### GPO Screenshots

- Password policy settings
- Firewall status (Windows Security)
- Mapped drives in File Explorer
- Group Policy Management showing 4 GPOs linked

### Test Results (with screenshots)

- Test 1: Domain user logon successful
- Test 2: Account lockout + Event ID 4740 in Event Viewer

- Test 3: HR user access HR share (allowed)
- Test 4: HR user access IT share (denied)
- Test 5: IT user access IT share (allowed)
- Test 6: IT user access HR share (denied)
- Test 7: Both users access Common share (allowed)
- Test 8: HR user sees Z: and H: drives
- Test 9: IT user sees Z: and I: drives
- Test 10: Firewall ON on client

## Event Viewer Screenshots

- Screenshot showing Event ID 4624 (successful logon)
- Screenshot showing Event ID 4625 (failed logon)
- Screenshot showing Event ID 4740 (account lockout)
- Screenshot showing Event ID 4728 (user added to group)

## Final Report

- All documents combined into one PDF or Word file
- Professional formatting with clear sections
- Conclusion explaining what was learned