**1. PowerShell Script: Login Script**

**File:** Login\_Script.ps1  
**Purpose:** Map a network drive and connect a shared printer during user login.

Powershell:

# PowerShell Login Script Example

# Map a network drive to the Shared folder

New-PSDrive -Name "S" -PSProvider FileSystem -Root "\\corp.local\Shared" -Persist

# Connect to a shared network printer

Start-Process -FilePath "rundll32.exe" -ArgumentList "printui.dll,PrintUIEntry /in /n \\corp.local\HP\_LaserJet"

📝 **Usage:**  
This script is assigned via Group Policy:

* GPMC > User Configuration > Windows Settings > Scripts (Logon) > Add script

**2. Command-line Steps to Set Up Windows Server & Active Directory**

You can execute these commands in **PowerShell** or use the GUI tools as described.

**Install Active Directory Domain Services (AD DS)**

Powershell:

# Install AD DS role

Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

**Promote Server to Domain Controller**

Powershell:

# Create a new forest and domain

Install-ADDSForest -DomainName "corp.local" -DomainNetbiosName "CORP" -SafeModeAdministratorPassword (ConvertTo-SecureString -AsPlainText "Admin@123" -Force) -Force

**Create Organizational Units (OUs)**

Powershell:

# Create OUs for departments

New-ADOrganizationalUnit -Name "IT" -Path "DC=corp,DC=local"

New-ADOrganizationalUnit -Name "HR" -Path "DC=corp,DC=local"

New-ADOrganizationalUnit -Name "Sales" -Path "DC=corp,DC=local"

**Create Users Within OUs**

Powershell:

# Create users in each OU

New-ADUser -Name "John IT" -SamAccountName "john.it" -UserPrincipalName "john.it@corp.local" -AccountPassword (ConvertTo-SecureString "Welcome@123" -AsPlainText -Force) -Enabled $true -Path "OU=IT,DC=corp,DC=local"

New-ADUser -Name "Alice HR" -SamAccountName "alice.hr" -UserPrincipalName "alice.hr@corp.local" -AccountPassword (ConvertTo-SecureString "Welcome@123" -AsPlainText -Force) -Enabled $true -Path "OU=HR,DC=corp,DC=local"

**Set Group Policies (GPO) via Group Policy Management Console (GUI)**

No direct PowerShell shown here, but typically set:

* Password Policy (Minimum length, complexity)
* Desktop Restrictions (e.g., hide Control Panel)
* Login Banner

You can use:

Powershell:

# Force group policy update

gpupdate /force

**Enable Remote Desktop (Optional)**

Powershell:

# Enable RDP via registry

Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal Server" -Name "fDenyTSConnections" -Value 0

# Allow RDP through firewall

Enable-NetFirewallRule -DisplayGroup "Remote Desktop"