# PHASE 5: Group Policy & Security Baselines – Hybrid Endpoint Hardening (On-Prem GPO + Intune)

This phase documents the security configuration of Windows endpoints for DipeshCorp (*Alias of **nxhz***) through both traditional on-premises Group Policy Objects (GPOs) and modern cloud-native Intune configuration profiles. These controls ensure enterprise-grade hardening across both domain-joined and Azure AD-joined systems, reflecting a hybrid security architecture.

This was executed in two coordinated tracks:

- 🧱 Track A: On-Premises GPOs (for domain-joined VMs)
- 🧱 Track B: Intune Baselines (for Autopilot and cloud-native devices)

---

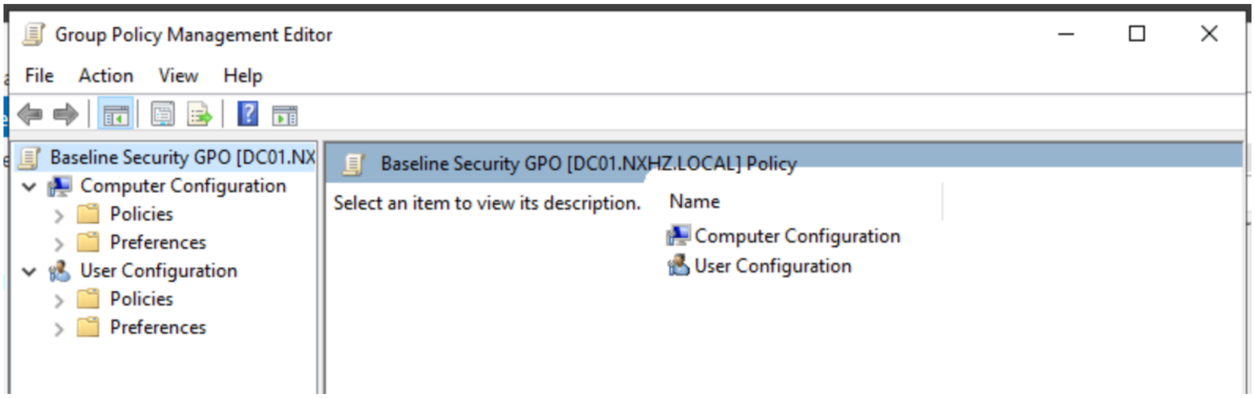
## TRACK A – On-Premises Group Policy Objects (GPOs) via DC01

Apply centralized security policies to on-premises domain-joined endpoints using Active Directory-based Group Policy.

Actions Completed:

Step A1: Create GPO in Group Policy Management

1. On DC01, opened Server Manager → Tools → Group Policy Management
2. Right-clicked domain: dipeshcorp.local → Created a new GPO
    - GPO Name: Baseline Security GPO
3. Right-clicked the GPO > Edit → Opened Group Policy Management Editor



Select an item to view its description.

Step A2: Configure Security Settings

A. Password Policy

Location: Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies

1. Minimum password length: 12
2. Password complexity: Enabled
3. Maximum password age: 90 days

B. Local Security Options

Location: Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options

1. Interactive logon: Message text for users attempting to log on: "Welcome to DipeshCorp. Unauthorized access is prohibited."
2. Accounts: Administrator account status: Disabled
3. User Account Control: Run all administrators in Admin Approval Mode: Enabled

C. Microsoft Defender Antivirus

Location: Computer Configuration → Administrative Templates → Windows Components → Microsoft Defender Antivirus

1. Turn on real-time protection: Enabled
2. Turn on behavior monitoring: Enabled
3. In Scan > Specify the day of the week to run a scheduled scan: Everyday

D. BitLocker Encryption

Location: Computer Configuration → Policies → Administrative Templates → Windows Components → BitLocker Drive Encryption → Operating System Drives

1. Require additional authentication at startup: Enabled
   - Allow BitLocker without compatible TPM: Uncheck
2. Choose how BitLocker-protected operating system drives can be recovered: Enabled
   - Save BitLocker recovery information to Active Directory Domain Services (AD DS): Enabled

E. Windows Update

Location: Computer Configuration → Administrative Templates → Windows Components → Windows Update

1. Configure Automatic Updates: Enabled
   - Auto-download and schedule the install
   - Scheduled install day: Everyday Scheduled install time: 3:00 AM
2. Specify active hours range for auto-restarts: Enabled
   - Active hours start: 9:00 AM
   - Active hours end: 5:00 PM

Step A3: Registry Edits via GPO

To disable Cortana:

1. Computer Configuration → Preferences → Windows Settings → Registry
2. New Registry Item:
   - Hive: HKEY_LOCAL_MACHINE

- Key Path: SOFTWARE\Policies\Microsoft\Windows\Windows Search
- Value Name: AllowCortana
- Type: REG_DWORD
- Value: 0

Step A4: Apply GPO to Workstations

1. Created new OU: “Workstations”
2. Moved domain-joined devices (e.g., Win11-VM01) to this OU
3. Link GPO to Workstations OU
    - On your domain controller (DC01), open:
        - Server Manager → Tools → Group Policy Management
    - In the left pane, expand:
        - Forest: dipeshcorp.local
        - Domains → dipeshcorp.local
        - You should see your created OU: Workstations
    - Right-click the Workstations OU → Click Link an Existing GPO...
    - In the dialog box that appears:
        - Select: Baseline Security GPO
        - Click OK

🧪 Testing Performed:

On domain-joined VM (Win11-VM01):

1. Ran: gpupdate /force
2. Verified password complexity prompt during change
3. Checked registry: HKLM...\AllowCortana = 0
4. Confirmed BitLocker encryption is on and recovery key stored in AD
5. Ran: gpresult /r to confirm GPO application

# TRACK B – Microsoft Intune-Based Security Configuration

Apply equivalent endpoint hardening policies to Azure AD-joined/Autopilot devices using Microsoft Intune.

Actions Completed:

Step B1: Deploy Microsoft Security Baselines via Intune

- Logged into: https://endpoint.microsoft.com
- Endpoint Security → Security Baselines > Microsoft Defender for Endpoint Baseline
    - Create Profile
    - Name: DipeshCorp Security Baseline
    - Configure settings as needed (e.g., SmartScreen ON, Defender Cloud Scan ON)
    - Assigned to group: All Cloud Devices

Step B2: Create Intune Configuration Profile for Equivalent GPO Settings

- Navigated to: Devices > Configuration → + Create Profile
- Platform: Windows 10 and later
- Profile Type: Settings Catalog
- Name: Hardening Policy (Intune)

Configured Settings:

A. Password Policy (Device Lock)

- Minimum length: 12
- Require uppercase letters: Yes
- Require special characters: Yes

B. BitLocker

- BitLocker required

- TPM required
- Backup recovery key to Azure AD: Yes

C. Microsoft Defender Antivirus

- Real-time protection: Enabled
- Cloud-delivered protection: Enabled

D. Windows Update

- Automatic updates: Enabled
- Active hours: 9:00 AM – 5:00 PM

E. Branding

- Organization Name: DipeshCorp
- Privacy URL: https://dipeshcorp.local/privacy

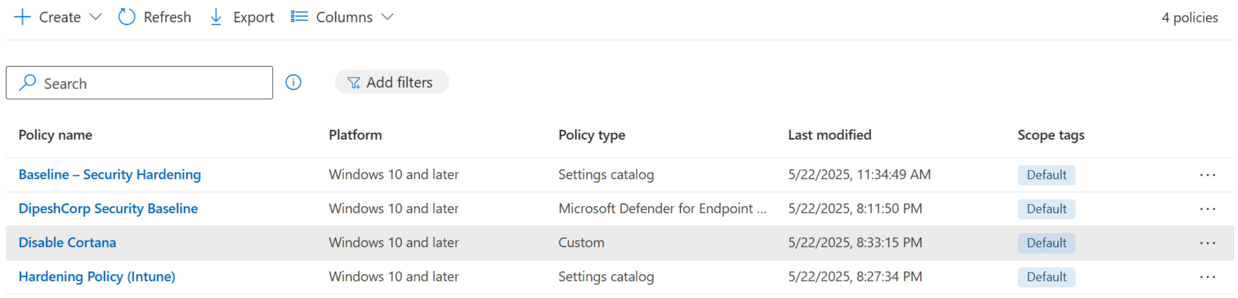
Assigned to group: All Devices

Step B3: Disable Cortana via Intune (OMA-URI Method)

- Devices > Configuration Profiles → + Create Profile
- Platform: Windows 10 and later
- Profile Type: Custom
- Name: Disable Cortana

OMA-URI Setting:

- Name: Disable Cortana
- OMA-URI: ./Device/Vendor/MSFT/Policy/Config/Experience/AllowCortana
- Data Type: Integer
- Value: 0
- Assigned to group: Cloud Devices



| Policy name | Platform | Policy type | Last modified | Scope tags | |
|---|---|---|---|---|---|
| Baseline – Security Hardening | Windows 10 and later | Settings catalog | 5/22/2025, 11:34:49 AM | Default | ··· |
| DipeshCorp Security Baseline | Windows 10 and later | Microsoft Defender for Endpoint ... | 5/22/2025, 8:11:50 PM | Default | ··· |
| Disable Cortana | Windows 10 and later | Custom | 5/22/2025, 8:33:15 PM | Default | ··· |
| Hardening Policy (Intune) | Windows 10 and later | Settings catalog | 5/22/2025, 8:27:34 PM | Default | ··· |

### 🧪 Testing Performed:

On an Azure AD-joined VM:

- Confirmed enrollment into Intune
- Verified policy sync in Device > Endpoint Manager
- BitLocker enabled → Recovery key verified in Azure AD
- Cortana setting disabled
- Defender protection levels enforced
- MDM profile confirmed in: Settings > Accounts > Access work or school

---

## V. Completion Outcome:

With the implementation of both on-premises GPOs and Microsoft Intune-based configuration profiles, DipeshCorp now enforces consistent security posture across hybrid environments. Domain-joined and cloud-native endpoints receive equivalent hardening controls including BitLocker, antivirus, update scheduling, and policy branding—ready for audit, compliance, and real-world operations.