NCAPS Windows Autopilot Hardening Standard

Naming Convention, Windows Security Baseline, and Silent BitLocker with Entra Escrow

This build is organized by which lever each piece pulls: device naming, security baseline, and encryption. The single biggest operational risk is policy ownership of BitLocker, covered in the conflict section.

1. Naming Convention: NCAPS-%SERIAL%

The naming template lives in the **Autopilot deployment profile**, not in a configuration profile assigned to the Entra group.

> **Path** Devices > Enrollment > Windows > Deployment Profiles > your profile > Out-of-box experience (OOBE) > Apply device name template > Yes

Set the template to:

```
NCAPS-%SERIAL%
```

Constraints that bite if you ignore them

- **15 character maximum (NetBIOS limit).** `NCAPS-` consumes 6 characters, leaving 9 for the serial. If your Dell or Lenovo serials run longer than 9 characters, the name truncates and you can hit collisions. Use `%SERIAL%` only if serials fit. Otherwise switch to `%RAND:9%` or trim with a script.
- **Letters, numbers, and hyphens only.** No spaces or underscores. The template silently fails validation otherwise.
- **The name applies during OOBE** and triggers a reboot before the desktop appears.

Renaming already-enrolled devices

The deployment profile will not touch devices that are already enrolled. Use a proactive remediation instead.

Detection (flag devices not matching NCAPS-serial):

```
$serial = (Get-CimInstance Win32_BIOS).SerialNumber.Trim()
$expected = "NCAPS-$serial"
if ($expected.Length -gt 15) { $expected = $expected.Substring(0,15) }
if ($env:COMPUTERNAME -eq $expected) { exit 0 } else {
    Write-Output "Name drift: $env:COMPUTERNAME"; exit 1 }
```

Remediation:

```
$serial = (Get-CimInstance Win32_BIOS).SerialNumber.Trim()
$expected = "NCAPS-$serial"
if ($expected.Length -gt 15) { $expected = $expected.Substring(0,15) }
Rename-Computer -NewName $expected -Force
# Reboot happens at next maintenance window; or force:
# Restart-Computer -Force
exit 0
```

Run as SYSTEM, 64-bit. Skip the forced reboot in remediation unless you want surprise restarts. Let the rename apply on the next natural reboot.

2. Windows Security Baseline

Assign Microsoft's maintained baseline to the secure Entra group.

> **Path** Endpoint security > Security baselines > Security Baseline for Windows 10 and later > Create profile > assign to the group

Take the current published version. Review these settings before you assign, because the defaults are aggressive.

- **BitLocker settings inside the baseline.** The baseline includes its own BitLocker config. This collides with a standalone BitLocker config profile (see the conflict section). Decide which policy owns encryption.
- **Defender settings.** The baseline turns on most of what you want already: real-time protection, PUA, and network protection.
- **Attack Surface Reduction rules.** The baseline sets several to Block. Test these. ASR rules in Block mode can break legitimate line-of-business apps. Consider Audit first, review the event logs, then flip to Block.
- **Local admin and credential settings.** The baseline restricts a lot. Confirm your service accounts and management tooling still function.

Rollout approach

Roll it out in rings. Assign to a small static pilot ring first, watch for baseline conflict and error states under **Devices > Monitor > Configuration profiles**, then widen to the full dynamic group.

---

3. BitLocker: Silent Enablement with Entra Escrow

There are two clean ways to do this. **Pick one owner** to avoid CSP conflicts.

Option A (recommended): Let the Security Baseline own BitLocker

The baseline already carries BitLocker policy. Verify these values inside it:

- XTS-AES 256
- Silent enablement
- Recovery key backed up to Entra before encryption
- OS drive required

Option B: Standalone BitLocker config profile

Use this only if you strip BitLocker out of the baseline. Configure via Settings catalog or the Endpoint Protection template.

- **Require device encryption:** Yes
- **Encryption method:** XTS-AES 256-bit (OS and fixed drives)
- **Silent enablement:** Set "Warning for other disk encryption" to Block and "Allow standard users to enable encryption during Autopilot" to Yes, so it runs without prompting.

- **Recovery key:** "Save BitLocker recovery information to Microsoft Entra ID" = Yes, and "Do not enable BitLocker until recovery info is stored" = Yes. This guarantees escrow before encryption, the part people miss.

Hardware prerequisites

Silent enablement requires the hardware to support it: TPM 2.0 present and ready, and the device must be Entra joined or hybrid joined. If TPM is not ready, silent enablement quietly does nothing. Pair it with the detection remediation below as a safety net.

Detection (confirm encryption and escrow are both real):

```
$vol = Get-BitLockerVolume -MountPoint $env:SystemDrive
$key = $vol.KeyProtector |
    Where-Object KeyProtectorType -eq "RecoveryPassword"
if ($vol.VolumeStatus -eq "FullyEncrypted" -and
    $vol.ProtectionStatus -eq "On" -and $key) {
    exit 0
} else {
    Write-Output "BitLocker incomplete: Status=$($vol.VolumeStatus)"
    exit 1
}
```

Remediation:

```
$mp = $env:SystemDrive
$tpm = Get-Tpm
if (-not $tpm.TpmReady) {
    Write-Output "TPM not ready, cannot proceed"; exit 1 }
Enable-BitLocker -MountPoint $mp -EncryptionMethod XtsAes256 `
    -UsedSpaceOnly -RecoveryPasswordProtector -SkipHardwareTest `
    -ErrorAction SilentlyContinue
$key = (Get-BitLockerVolume -MountPoint $mp).KeyProtector |
    Where-Object KeyProtectorType -eq "RecoveryPassword"
if ($key) {
    BackupToAAD-BitLockerKeyProtector -MountPoint $mp `
        -KeyProtectorId $key.KeyProtectorId
    Resume-BitLocker -MountPoint $mp
    exit 0
} else { Write-Output "No recovery protector created"; exit 1 }
```

The One Conflict to Plan Around

The Security Baseline, a standalone BitLocker profile, and the BitLocker remediation can all try to own encryption settings. When two policies set the same CSP differently, the device lands in an error or conflict state and may not encrypt at all.

Clean separation

Component	Owns	Behavior
Security Baseline	BitLocker policy	Method, escrow requirement, and silent flag.
Remediation	Gap-fill only	Acts only when the baseline did not take (TPM timing, devices enrolled before the policy existed). Detects and fills gaps. Does not set competing policy.
Standalone profile	Nothing	Do not run a standalone BitLocker config profile if the baseline owns it.

Assignment Order on the Secure Entra Group

1. **Autopilot deployment profile (naming).** Targets the Autopilot device group, applies at OOBE.
2. **Windows Security Baseline.** Dynamic group, owns BitLocker, Defender, and ASR.
3. **Naming remediation.** Catches already-enrolled drift.
4. **BitLocker remediation.** Safety net for escrow and TPM gaps.
5. **Compliance policy.** Keys off BitLocker and Defender, which then feeds Conditional Access.