Domain-Joined Windows 11 VM with Microsoft Edge Lockdown for Lab Use

Date: June 7, 2025
Category: Windows 11 / GPO / Domain Lab Hardening

Backlink: Bypassing TPM, Secure Boot, and Microsoft Account During Windows 11 VM Setup

---

Overview

This VM is domain-joined to `library.local` and intended to simulate a public-access or library-style machine for a generic user (`libraryuser`). Group Policy was used to lock down Microsoft Edge and restrict system-level access.

Environment

- **OS**: Windows 11 VM
- **Domain**: `library.local`
- **Domain Controller**: Windows Server 2022
- **OU**: `LibraryLabUsers`
- **User**: `libraryuser`
- **GPO**: `Library User Restrictions`
- **Template Type**: Classic ADM (no ADMX available at the time)

GPO Settings Applied

Control Panel & Program Access

- □□ Prohibit access to Control Panel and PC settings
- □□ Remove Add or Remove Programs

Microsoft Edge Configuration

- □□ Clear browsing data when Edge closes
- □□ Clear cached images and files on close
- □□ Disable saving browser history
- □ Enable Do Not Track
- ⚠ Enable insecure download warnings

Edge Extensions & Downloads

- □□ Block external extensions from being installed

Startup / Homepage Settings

- □□ Configure homepage URI `https://docs.natenetworks.com`
- □□ Action on Edge startup: Open list of URLs
- □□ Sites to open:
  - `https://docs.natenetworks.com`
  - `https://artash.io`
- □□ Set new tab page as homepage

Start Menu and Taskbar Restrictions

- □ Disable context menus in Start Menu
- □ Remove Run from Start Menu

Ctrl+Alt+Del Restrictions

- □ Remove Change Password
- □ Remove Lock Computer
- □ Remove Logoff
- □ Remove Task Manager

Results

Logging in as `libraryuser` now:

- Edge launches directly to the approved URLs

- All Edge settings and customization options are blocked
- Control Panel and system tweaks are locked down
- User cannot access Run, Task Manager, or make profile/system changes

---

Next Steps

1. **Prevent Edge Settings Access**
   - If not already enabled, locate:
     `Prevent access to the settings page in Microsoft Edge`
     → Set to **Enabled**
2. **Add AppLocker Rules**
   - Restrict `.exe` launches outside of `C:\Program Files` and `C:\Windows`
3. **Enable SmartScreen & SafeSearch Policies**
   - Protect against malicious or adult content
   - Optionally configure DNS-based content filtering (NextDNS/OpenDNS)
4. **Redirect Known Folders**
   - Use Folder Redirection to isolate documents and desktop paths per user
5. **Add User Logoff Timer / Idle Policy**
   - Use Task Scheduler or GPO to log off inactive users after X minutes

---

Revision #1
Created 7 June 2025 17:52:38 by Nate Nash
Updated 28 December 2025 20:31:02 by Nate Nash