Disabling USB Storage Access via GPO

Environment: Windows Server 2022 (Domain Controller), Windows Enterprise Clients

---

Objective

Prevent unauthorized access or data theft via USB/removable storage devices on all domain-joined client machines using centralized Group Policy.

Technology Stack

- Group Policy Management via Windows Server 2022
- Domain-Joined Clients (Windows 10/11 Enterprise)
- Administrative Templates (Group Policy Editor)

Step-by-Step Implementation

1. Create a New GPO

- Open the **Group Policy Management Console (GPMC)**
- Right-click your domain root (e.g., `kali.local`)
- Select: **Create a GPO in this domain and link it here**
- Name it: `Removable Storage Access`

2. Edit the GPO

- Right-click `Disable USB Storage` → Click **Edit**

3. Navigate to the Policy Path

`Computer Configuration → Policies → Administrative Templates → System → Removable Storage Access`

4. Configure the Policy

- Find: **All Removable Storage classes: Deny all access**
- Double-click it

- Set to: **Enabled**
- Click **Apply**, then **OK**

Configuration Summary

Setting Name	Value
GPO Name	Disable USB Storage
Scope	Computer Configuration
Policy Path	System → Removable Storage Access
Policy Applied	All Removable Storage classes
Policy Value	Deny all access
Enforced	Yes

Security Benefits

- Prevents introduction of **unauthorized software** via USB
- Blocks potential **data leaks** or **ransomware infections**
- Aligns with **CIS Benchmarks** and **Zero Trust Architecture**
- Ideal for government, healthcare, finance, and education IT

Skills Demonstrated

- Secure endpoint configuration using Group Policy
- Computer-level policy enforcement
- Compliance-focused IT administration
- Preventative security design

Final Notes

- Combine with **Device Installation Restrictions** for even stronger security
- Test GPO on **OU-level before domain-wide rollout**

- Document GPOs in a version-controlled **policy change log**