

Intune ile Cihaz Kontrolü

Neden cihaz kontrolüne ihtiyaç duyarız ?

Sistemizde, cihazlar ve bağlı oldukları işletim sistemi kaynaklı olarak güvenlik ve data güvenliği konusunda zafiyetler oluşabilir. Bu zafiyetleri azaltmak ve cihaz uyumluluğu ile güvenli ve takip edilebilir bir yapı kurulması ihtiyaç duyulmaktadır.

Device Control özelliğine ihtiyaç duyduğumuz çok fazla istek vardır.

Bazılarını sıralarsak;

- Kullanılmayan veya istenmeyen donanımların devre dışı bırakılması.
- Çıkarılabilir disklerin günlük yazma ve okuma verilerinin denetlenmesi.
- Envanter yetkisi ve kontrolünün yapılması.
- ...

Kuruluşların cihaz kontrolü konusunda net bir yönerge ile hareket etmeleri gerekmektedir. Son kullanıcı üzerinde yaratacağı etki ile farkındalığında artırılması hedeflenmelidir.

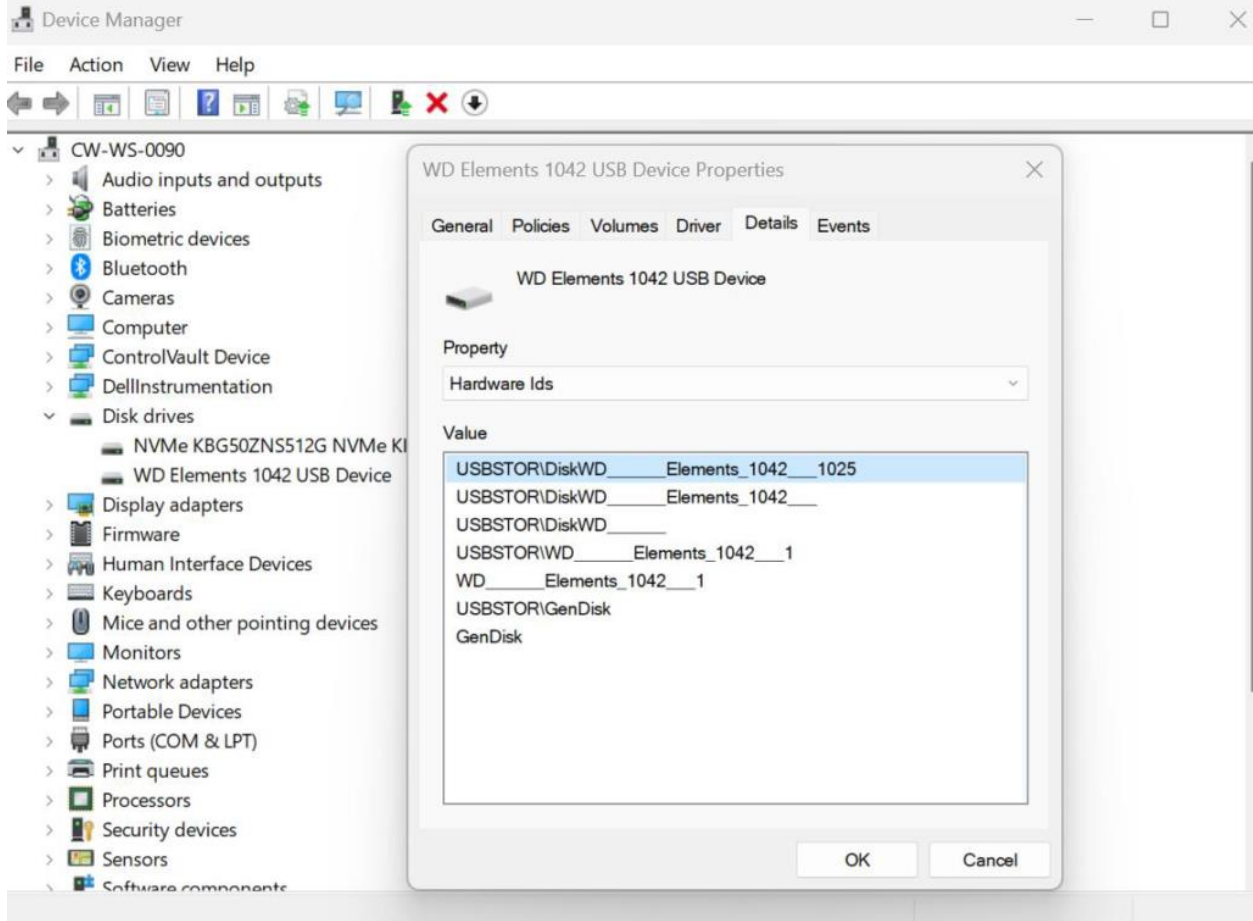
Identifying devices

Tüm donanımsal cihazların kendilerine has kimlikleri bulunmaktadır. Bu cihazların tanımlanması ve cihaz bazlı politikaların uygulanması gelen taleplerin detaylandırılması ve takip açısından da fayda sağlayacaktır. Cihazları tanımlamak için Device Manager 'dan yararlanabilirsiniz.

Bazı cihaz sınıfları kullanılmak istenmeyebilir ve gereksinimlerinize bağlı olarak tamamen engellenebilir.

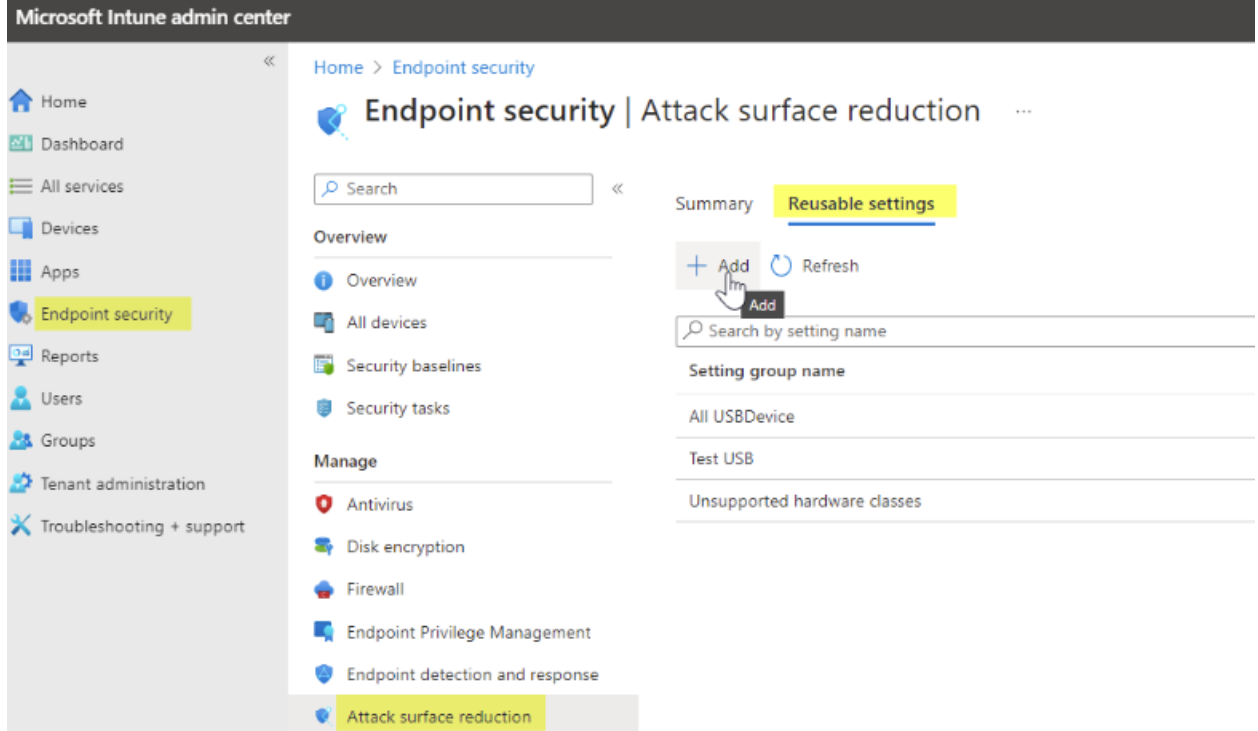
- CDROM
- FDC
- FloppyDisk
- SmartCardReader
- TapeDrive

Microsoft politikalarını uygularken, ClassGUID değeri kullanılması önerilmektedir

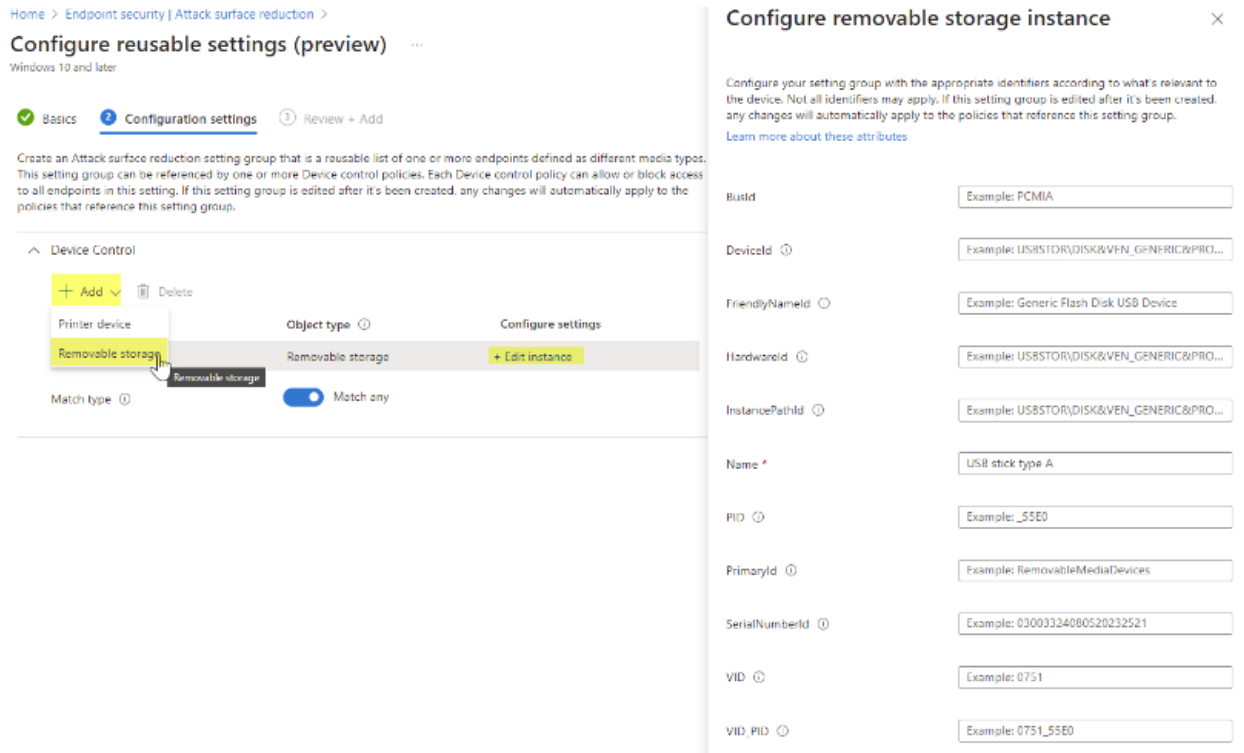


Reusable Settings

Reusable Settings grupları, birden fazla ilke için kullanılabilecek bir dizi cihaz attributelerini tanımlar ve yalnızca tek bir yerden yönetilebilir olduğu için kullanışlıdır. Bunu oluşturmak için: [Intune admin center](#)'a giriş yaptıktan sonra Endpoint Security>Attack surface reduction ve üst menüden Reusable settings seçeneğini seçiyoruz.



Ad ve açıklama belirtiyoruz ve **Device Control** bölümünden removable storage eklemesi gerçekleştiriyoruz. Burada birden fazla ekleme yapılabilir. **Edit Instance** seçeneği ile, düzenleme işlemlerini sağlayabilirsiniz.



Create Device control policy

Device Control Policy, Intune'da ve Endpoint Security başlığı altında **Saldırı Yüzeyini Azaltma (ASR)**'ın bir parçasıdır. Tüm ayar ve konfigürasyonları bu başlık altından yapılacaktır.

Home > Endpoint security

Endpoint security | Attack surface reduction

Search

Security baselines

Security tasks

Manage

Antivirus

Disk encryption

Firewall

Endpoint Privilege Management

Endpoint detection and response

App Control for Business (Preview)

Attack surface reduction

Account protection

Device compliance

Conditional access

Summary

Reusable settings

Attack surface reduction

+ Create Policy

Refresh

Search by profile name

Policy name

↑↓

Policy

E

L...

Create a profile

Platform

Windows 10 and later

Profile

Select a profile

Exploit Protection

Device Control

App and Browser Isolation

Web protection (Microsoft Edge Legacy)

Application control

Create

Create profile ...

Device Control

- ✓ Basics
- 2 Configuration settings**
- ③ Scope tags
- ④ Assignments
- ⑤ Review + create

^ Administrative Templates

System > Device Installation > Device Installation Restrictions



Apply layered order of evaluation for Allow and Prevent device installation policies across all device match criteria ⓘ	Enabled
Allow installation of devices that match any of these device IDs ⓘ	Not configured
Allow installation of devices that match any of these device instance IDs ⓘ	Not configured
Allow installation of devices using drivers that match these device setup classes ⓘ	Not configured
Prevent installation of devices not described by other policy settings ⓘ	Not configured
Prevent installation of devices that match any of these device IDs ⓘ	Not configured
Prevent installation of devices that match any of these device instance IDs ⓘ	Not configured
Prevent installation of devices using drivers that match these device setup classes ⓘ	Enabled

Prevented Classes


 Delete  Sort  Import  Export



<input type="checkbox"/>	{4d23232-d2e24-2323122e-213214-e21312-5114}	✓
<input type="checkbox"/>	{4d23232-d2e24-2323122e-213214-e13122-5114}	✓
<input type="checkbox"/>	{4d23232-d2e24-2323142e-213214-e21312-5114}	✓
<input type="checkbox"/>	{4d23232-d2e24-2323122e-213214-e21312-5514}	✓
<input type="checkbox"/>	{4d43232-d2e24-2323222e-213214-e21312-5114}	✓
<input type="checkbox"/>		

Also apply to matching devices that are already installed. ☒ True



Prevent installation of removable devices  Not configured 

System > Removable Storage Access



WPD Devices: Deny read access  Not configured 

WPD Devices: Deny read access (User)  Not configured 

WPD Devices: Deny write access  Not configured 

WPD Devices: Deny write access (User)  Not configured 

Defender

Allow Full Scan Removable Drive Scanning  Allowed. Scans removable drives. 

^ Data Protection

Allow Direct Memory Access ⓘ Block ▼

^ Dma Guard

Device Enumeration Policy ⓘ Not configured ▼

^ Storage

Removable Disk Deny Write Access ⓘ Not configured ▼

^ Connectivity

Allow USB Connection ⓘ Not configured ▼

Allow Bluetooth ⓘ Not configured ▼

Removable cihazların kontrolleri esas alındığında belirli cihazlara izin verilmesi veya belirli cihazların engellenmesi yönündeki talepleri, Cihaz ClassGUID değerleri baz alınarak politikaların oluşturulması en iyi yöntem olacaktır. Envanter Kontrolü için, özellikle depolama ve cihaz türlerinin listelenmesine izin vermek için, çoğunlukla HardwareID özelliği altında yer alan VID_PID (vendor and product ID) değerlerinin kullanılması önerilmektedir.

Microsoft Security Baseline'lar bizler için birer ölçek olarak görülebilir, ancak burada **Microsoft Security Configuration Framework'ler** referans alınmalıdır ve bu bağlamda değerlendirilmelidir.