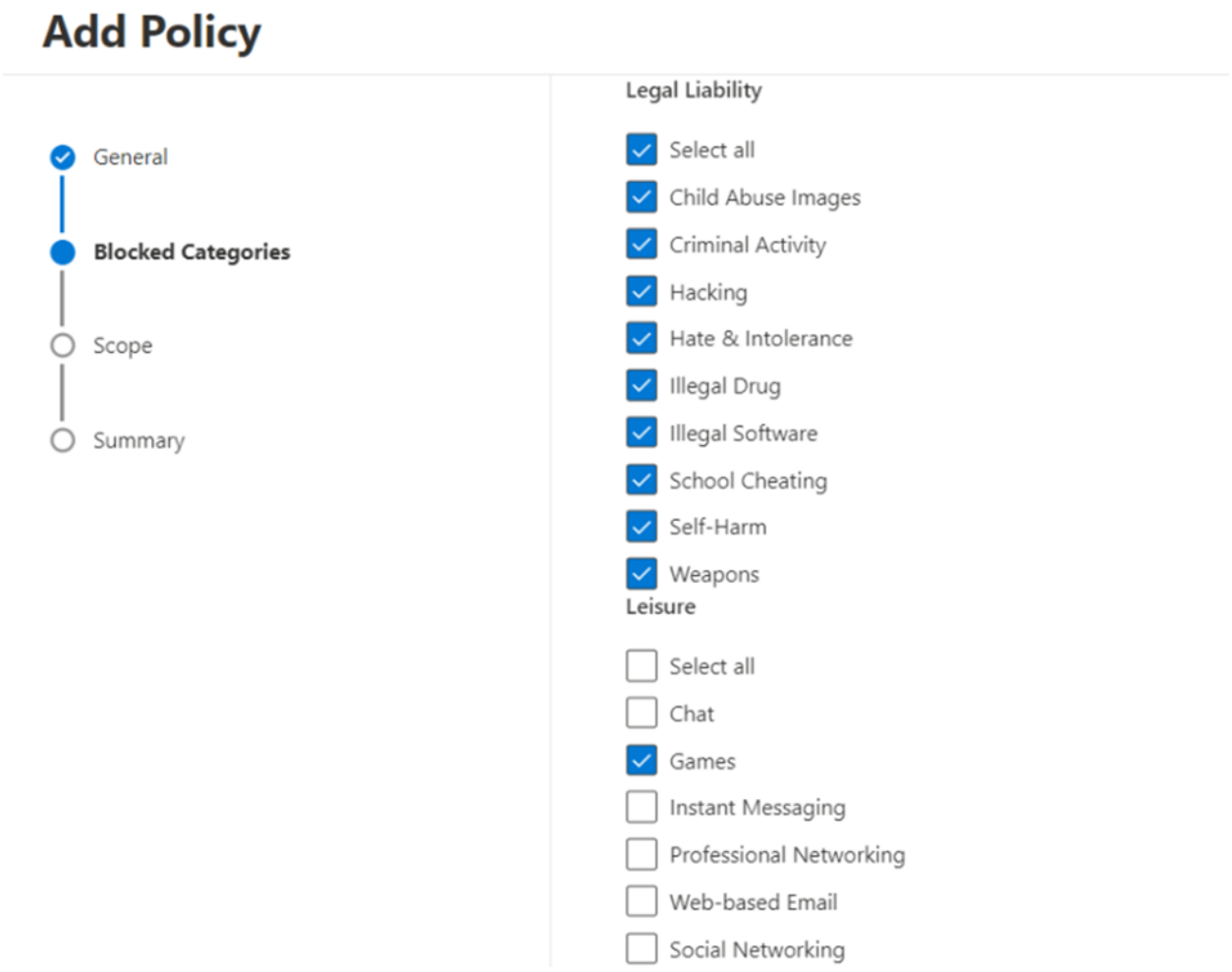
Microsoft Defender for Endpoint : Web Content Filter

Microsoft Defender for Endpoint, risk tabanlı güvenlik açığı yönetimi ve değerlendirmesi, saldırı yüzeyini azaltma, davranış tabanlı ve bulut destekli yeni nesil koruma, uç nokta algılama ve yanıtlama (EDR), otomatik araştırma ve düzeltme, yönetilen avcılık hizmetleri ve zengin API'ler içeren bütünsel, bulut tarafından sunulan bir uç nokta güvenlik çözümüdür. En önemli özelliklerinden biri Web Content Filter 'dır.



Web İçerik Filtresi, kullanıcıların erişebileceği web içeriğini kontrol ederek kuruluşun ağını korumaya yardımcı olan bir özelliktir. Önceden tanımlanmış kategorilere göre kötü amaçlı ve uygunsuz web sitelerini engeller. Bu, siber tehditlere karşı koruma sağlamak, üretkenliği artırmak ve yasal gerekliliklere uymak için güçlü bir araç olarak kullanılabilir. Windows SmartScreen motorunu kullanarak bir Windows uç noktasında çalışır.

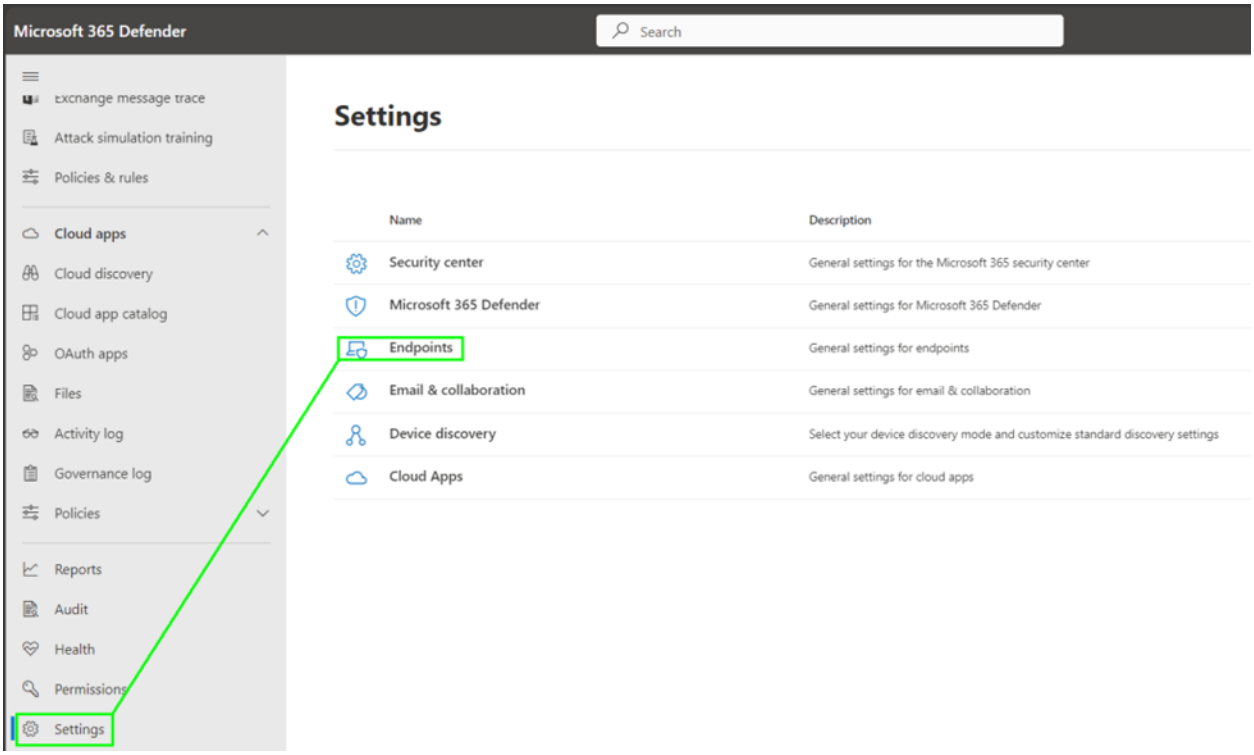
Ön Gereksinimler

Bu özelliği kullanmak için kurumların Microsoft 365 E5 , Microsoft 365 E5 Securty veya Business Premium lisansına sahip olması gerekir. Ayrıca kullanılan cihazın Windows 10 Enterprise, sürüm 1709 veya üstü olmasını gerekmektedir.

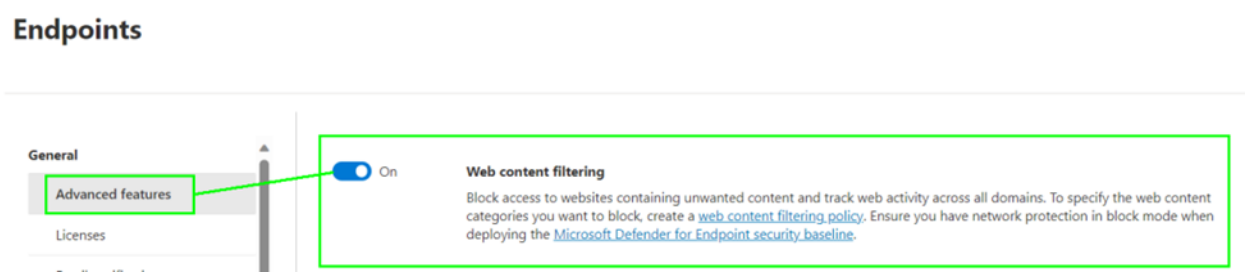
web con	Microsoft 365 Business	Microsoft 365 Frontline		Microsoft 365 Enterprise		Microsoft 365 Education	
Feature	Premium	F5 Security	F5 Sec+Comp	E5 Security	E5	A5 Security	A5
Office 365					E5		A5
Enterprise Mobility + Security					E5		A5
Windows	Business				E5		A5
> Web Content Filtering	✓	✓	✓	✓	✓	✓	✓

Web Content Filter 'ın Devreye Alınması

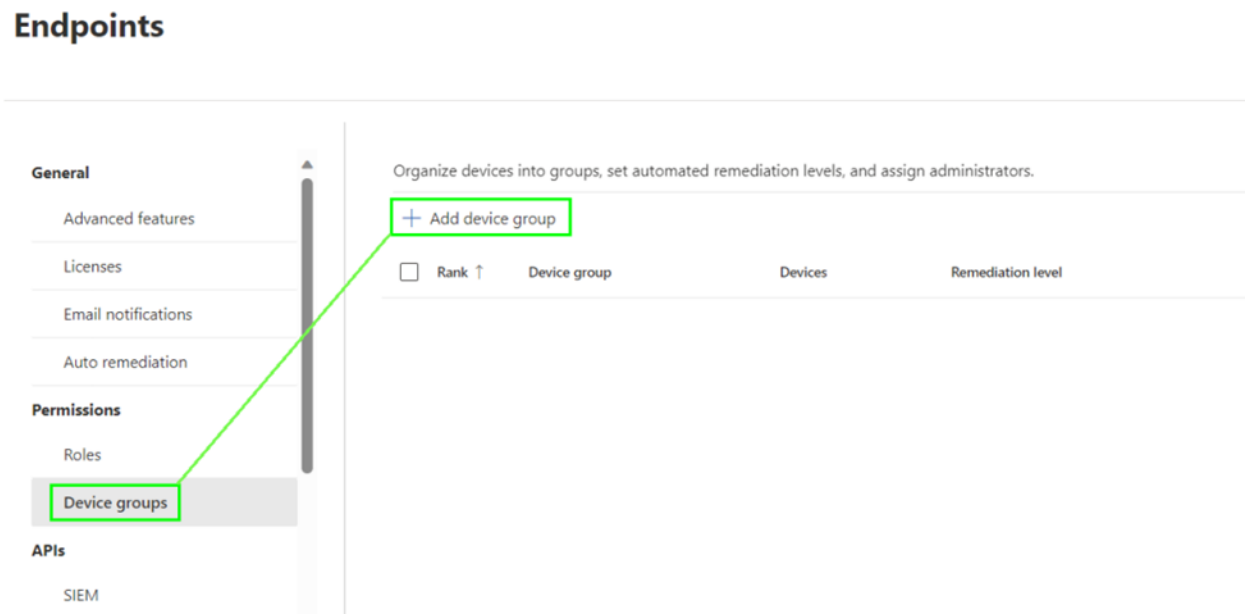
Web Content Filter'ı etkinleştirmek için https://security.microsoft.com adresine giriş yaparak Microsoft 365 Güvenlik Merkezi'nde Ayarlar bölümünden, Endpoint sayfasına giriyoruz:



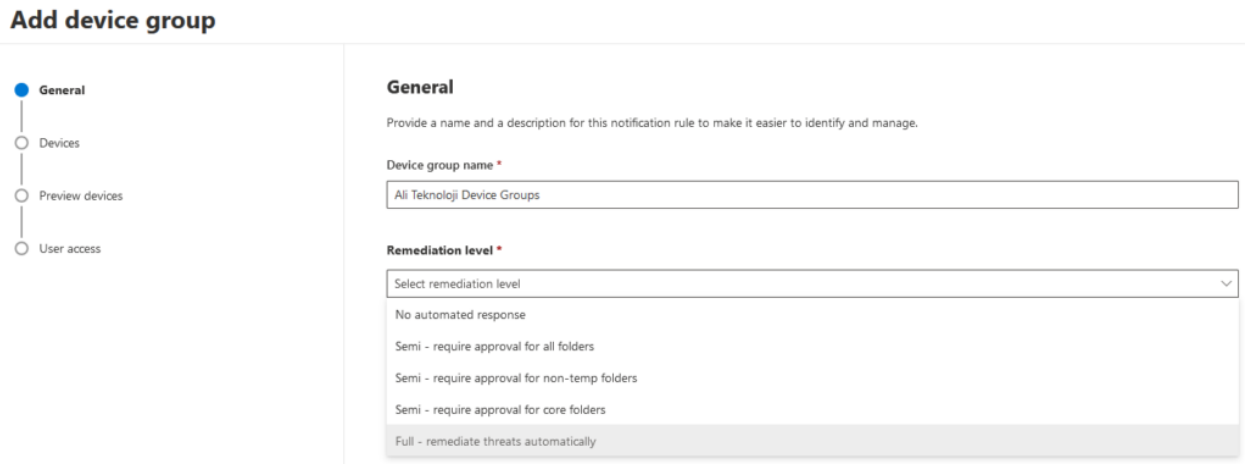
İlk olarak Advanced Features sekmesi altından Web Content Filter özelliğini aktif hale getiriyoruz.



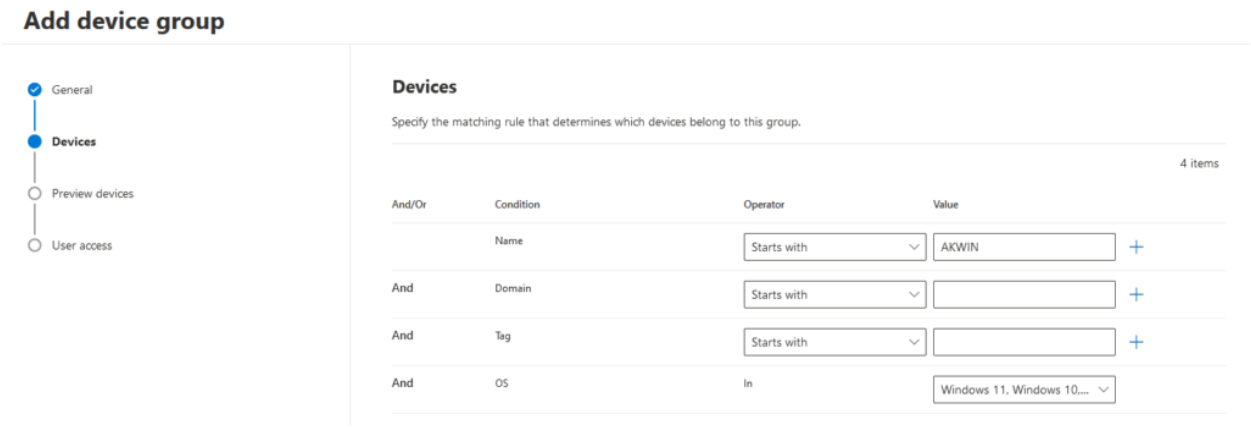
Şimdi politikayı kapsamak için bir cihaz grubu tanımlamamız gerekiyor. Ne yazık ki Security Center mevcut Entra ID bulunan gruplarını kullanmamaktadır, bunun yerine politikaları bir grup cihaza kapsamak için cihaz grupları oluşturmanız gerekmektedir.



Grubun adını ve Remediation level'ını belirliyoruz. Burada belirlediğimiz remedition level bizlere alacağı aksiyonun seviyesini belirtmektedir.

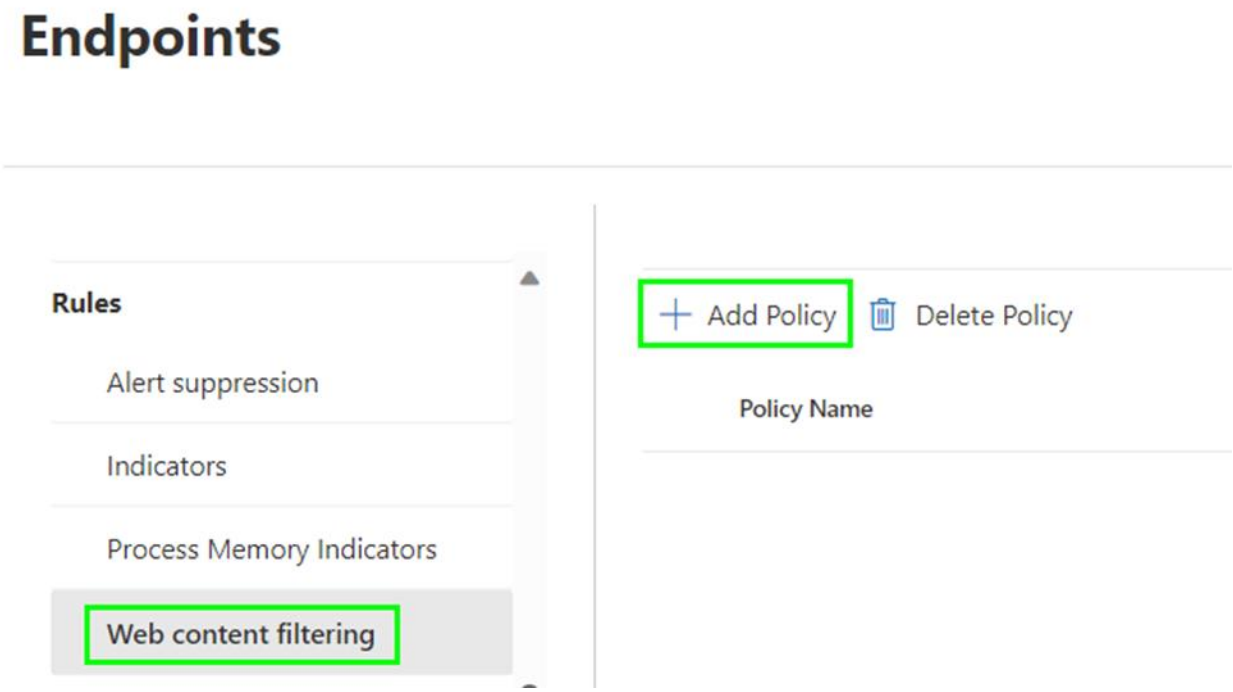


Cihazları belirli bir kapsam altına almak için filtreler eklememiz gerekir. Bu örnekte filtreyi, PC adının "AKWIN" ile başladığı ve işletim sistemi için Windows 10/11/AVD olması gereken her cihaza uygulanacak şekilde ayarlıyoruz.

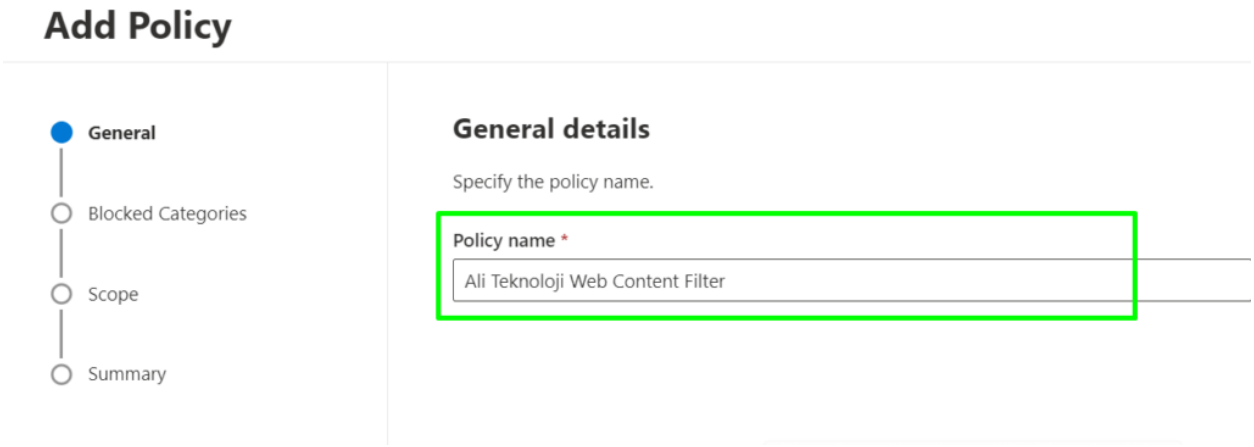


Cihaz grubunu oluşturduk.

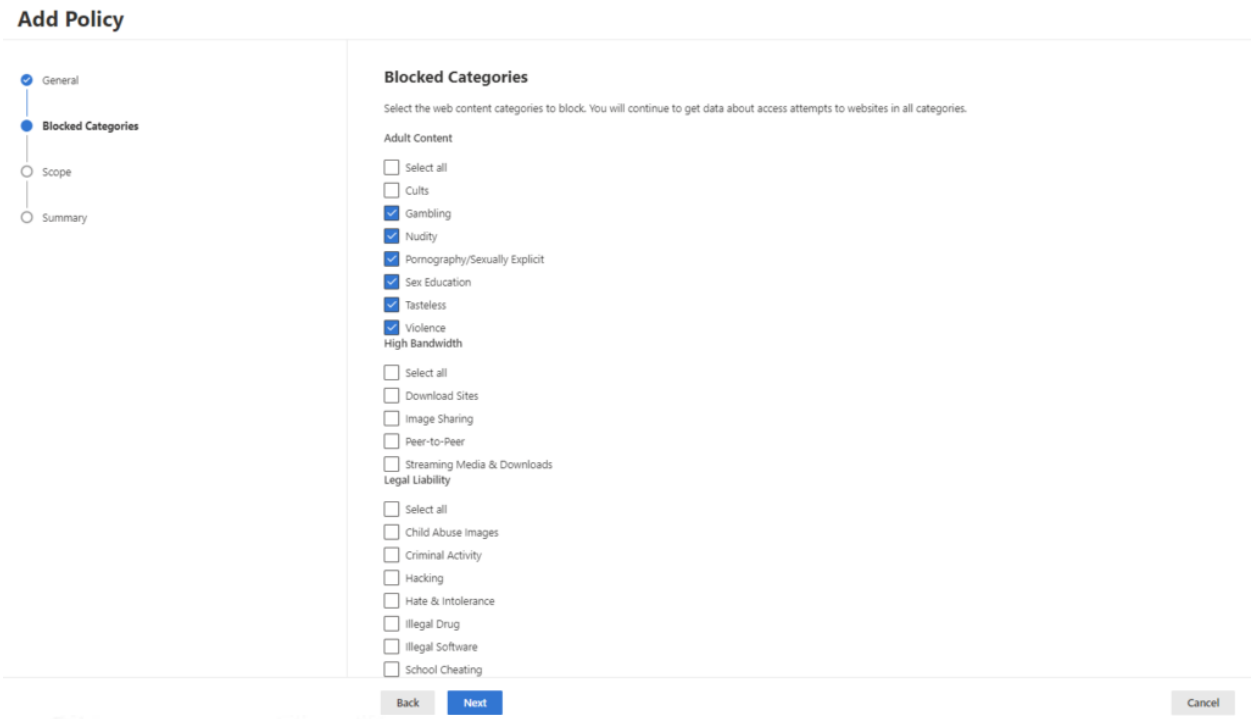
Daha sonra, hangi web içeriği kategorilerinin engellenmesi gerektiğini tanımladığımız bir kategori listesi oluşturmamız gerekiyor. Bu yüzden sol menüdeki "Kurallar" bölümünden "Web Content Filter "ye seçerek Add Policy seçeneğini seçiyoruz.

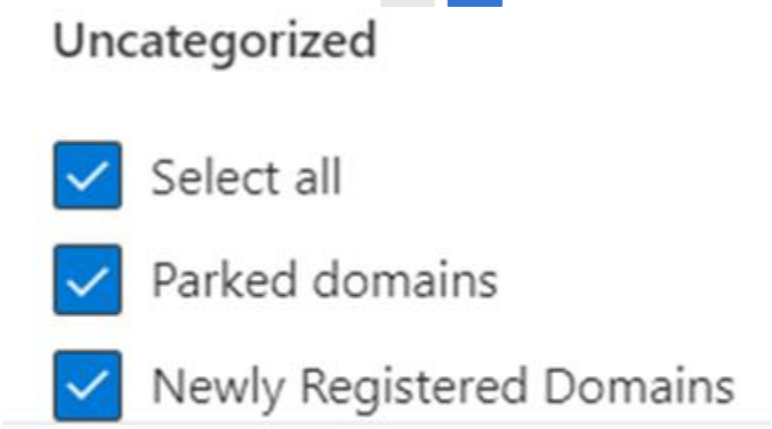


Politikanın ismini belirliyoruz.



Şimdi politika ile hangi kategorileri filtrelemek istediğimizi belirliyoruz.





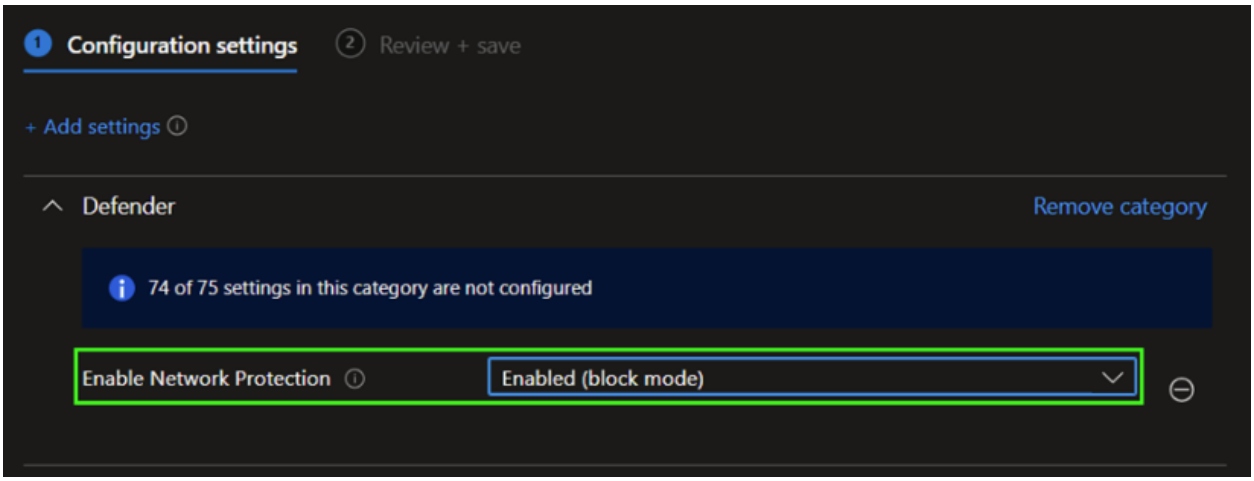
Engellenmesi gereken tüm kategorileri seçtikten sonra devam ediyoruz ve politikayı daha önce oluşturulan cihaz grubuna atıyoruz.

Artık Microsoft Güvenlik Merkezi'nde gerekli olan her şeyi yapılandırdınız.

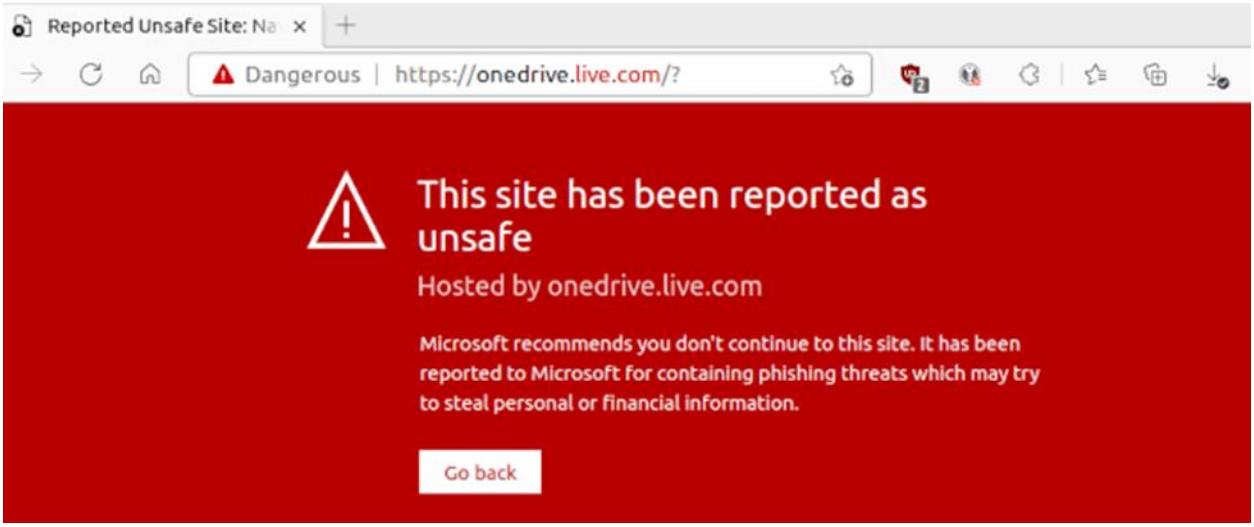
Device Configuration Profile ile Network Protection özelliğini devreye alıyoruz.

Bir Device Configuration Profile oluşturmak için https://endpoint.microsoft.com > Devices> Configuration Profile > Settings kataloğundan profil oluştur bölümüne gidin. Ardından arama yerine "Network Protection" yazabilirsiniz.

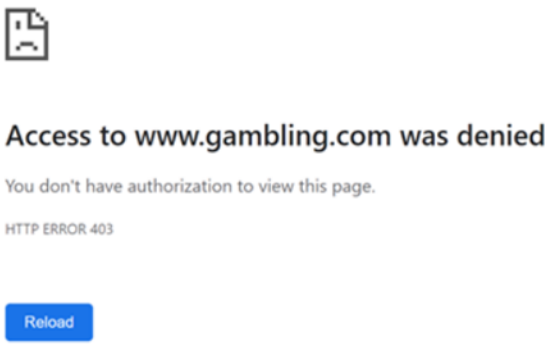
"Network Protection" için, aşağıdaki ekran görüntüsünde olduğu gibi özelliği blok modunda etkinleştirin:



Oluşan pofili cihaz grubuna atandıktan sonra kayıt edilmelidir.
Tüm yapılandırma oluşturulduktan, engellenmiş bir url'ye EDGE ile erişmeye çalışan bir kullanıcı aşağıdaki SmartScreen uyarısını görecektir:



Farklı tarayıcı ile ulaşmaya çalışan kullanıcı ise aşağıdaki "Access Denied" uyarısını görecektir ;



Web Content Filter özelliği, iOS , Android ve macOS cihazlarda da etkinleştirilebilir bir özelliktir. Farklı bir makalede bununla ilgili çalışmayı da inceleyeceğiz.