

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 'dir.

Add Policy

☒ General

☒ **Blocked Categories**

☐ Scope

☐ Summary

Legal Liability

☒ Select all

☒ Child Abuse Images

☒ Criminal Activity

☒ Hacking

☒ Hate & Intolerance

☒ Illegal Drug

☒ Illegal Software

☒ School Cheating

☒ Self-Harm

☒ Weapons

Leisure

☐ Select all

☐ Chat

☒ Games

☐ Instant Messaging

☐ Professional Networking

☐ Web-based Email

☐ Social Networking

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 Security veya Business Premium lisansına sahip olması gerekir. Ayrıca kullanılan cihazın Windows 10 Enterprise, sürüm 1709 veya üstü olmasını gerekmektedir.

<input type="text" value="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:

Microsoft 365 Defender

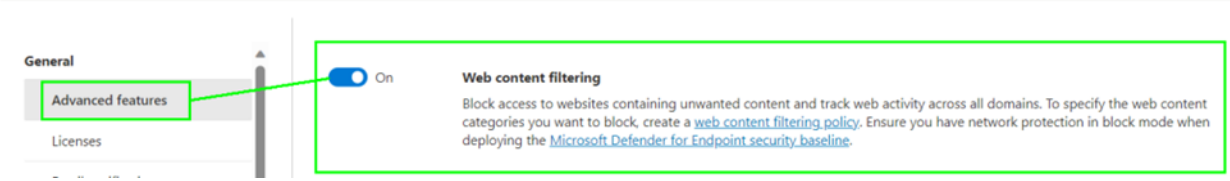
Search

Settings

Name	Description
Security center	General settings for the Microsoft 365 security center
Microsoft 365 Defender	General settings for Microsoft 365 Defender
Endpoints	General settings for endpoints
Email & collaboration	General settings for email & collaboration
Device discovery	Select your device discovery mode and customize standard discovery settings
Cloud Apps	General settings for cloud apps

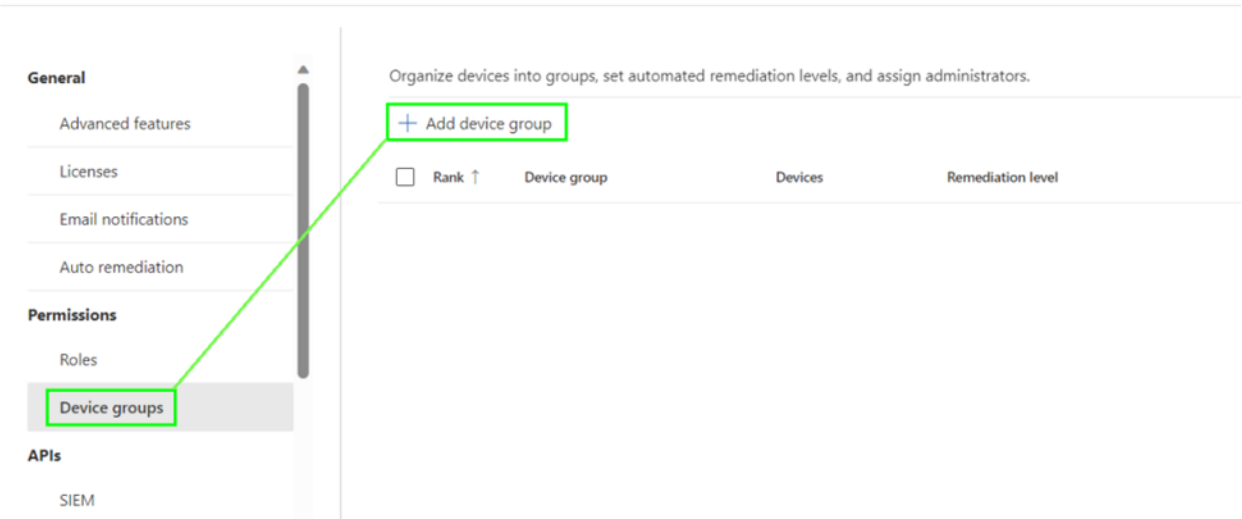
İlk olarak Advanced Features sekmesi altından Web Content Filter özelliğini aktif hale getiriyoruz.

Endpoints



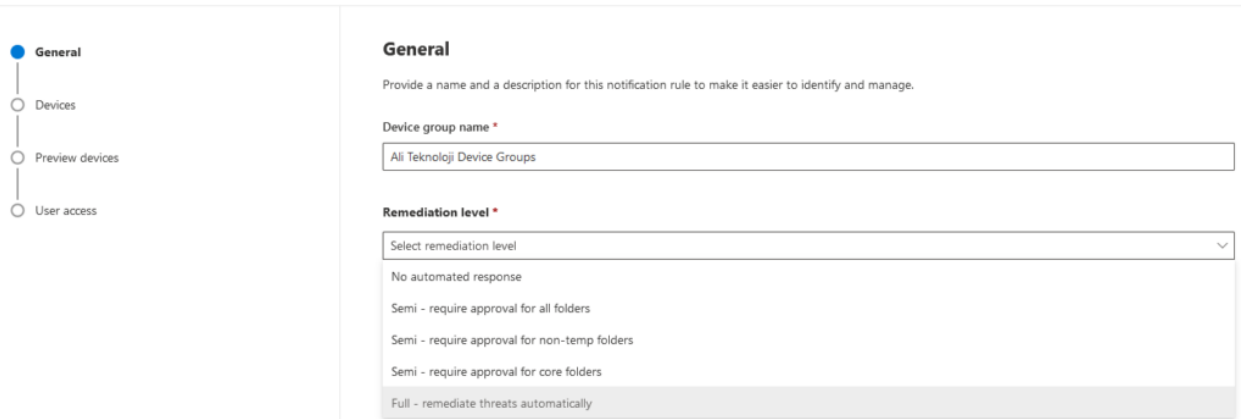
Şimdi politikayı kapsamak için bir cihaz grubu tanımlamamız gerekiyor. Ne yazık ki Security Center mevcut Entra ID bulunan gruplarını kullanmamaktadır, bunun yerine politikaları bir grup cihaza kapsamak için cihaz grupları oluşturmanız gerekmektedir.

Endpoints



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

Add device group



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.

Add device group

General

Devices

Preview devices

User access

Devices

Specify the matching rule that determines which devices belong to this group.

4 items

And/Or	Condition	Operator	Value	
	Name	Starts with	AKWIN	+
And	Domain	Starts with		+
And	Tag	Starts with		+
And	OS	In	Windows 11, Windows 10,...	

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.

Endpoints

Rules

Alert suppression

Indicators

Process Memory Indicators

Web content filtering

+ Add Policy

Delete Policy

Policy Name

Politikanın ismini belirliyoruz.

Add Policy

☒ General

☐ Blocked Categories

☐ Scope

☐ Summary

General details

Specify the policy name.

Policy name *

Ali Teknoloji Web Content Filter

Şimdi politika ile hangi kategorileri filtrelemek istediğimizi belirliyoruz.

Add Policy

General

Blocked Categories

Scope

Summary

Blocked Categories

Select the web content categories to block. You will continue to get data about access attempts to websites in all categories.

Adult Content

☐ Select all

☐ Cults

☒ Gambling

☒ Nudity

☒ Pornography/Sexually Explicit

☒ Sex Education

☒ Tasteless

☒ Violence

High Bandwidth

☐ Select all

☐ Download Sites

☐ Image Sharing

☐ Peer-to-Peer

☐ Streaming Media & Downloads

Legal Liability

☐ Select all

☐ Child Abuse Images

☐ Criminal Activity

☐ Hacking

☐ Hate & Intolerance

☐ Illegal Drug

☐ Illegal Software

☐ School Cheating

Back

Next

Cancel

Uncategorized

- ☒ Select all
- ☒ Parked domains
- ☒ Newly Registered Domains

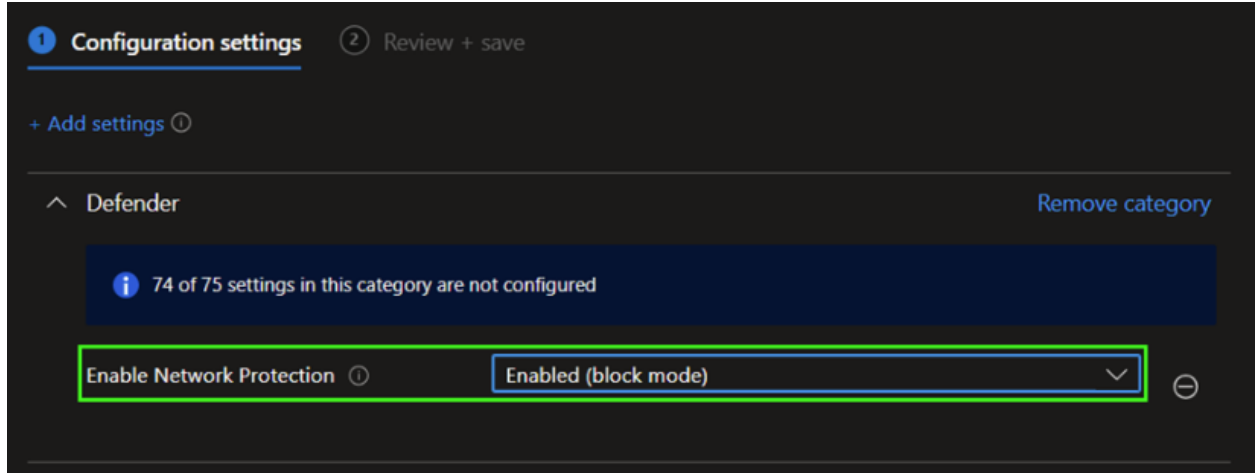
Engellenmesi gereken tüm kategorileri seçtikten sonra devam ediyoruz ve politikayı daha önce oluşturulan cihaz grubuna atıyoruz.

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

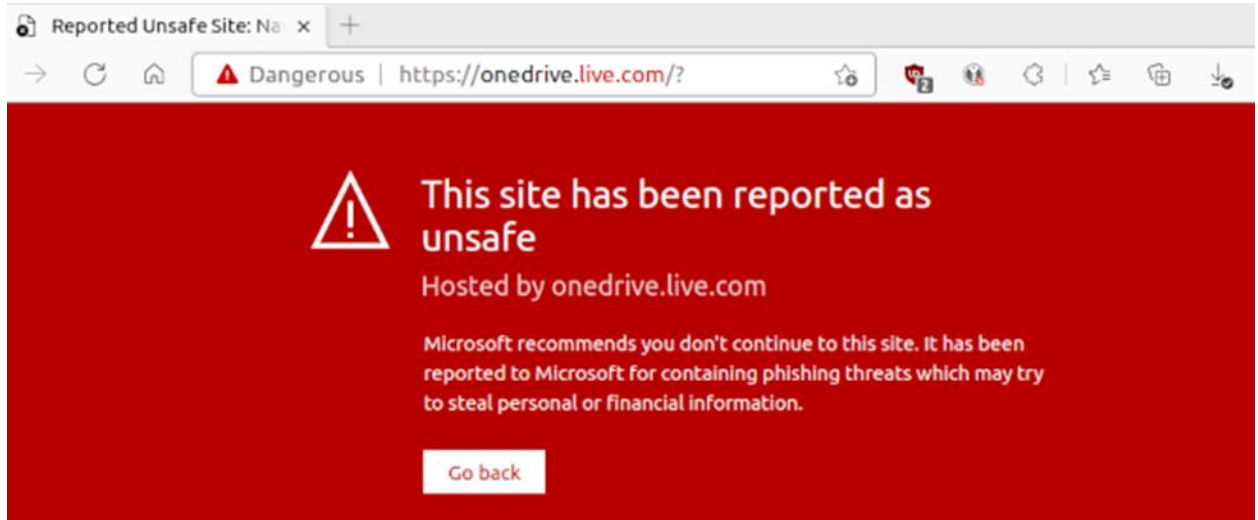
Device Configuration Profile ile Network Protection özelliğini devreye alıyoruz.

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 profili 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 ;

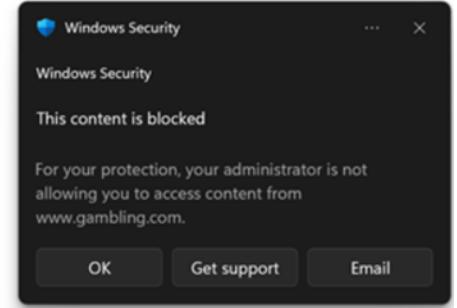


Access to www.gambling.com was denied

You don't have authorization to view this page.

HTTP ERROR 403

Reload



Web Content Filter özelliđi, iOS , Android ve macOS cihazlarda da etkinleřtirilebilir bir özelliktir. Farklı bir makalede bununla ilgili alıřmayı da inceleyeceđiz.