

Microsoft Defender for Endpoint: Web Content Filter

Microsoft Defender for Endpoint is a holistic suite that includes risk-based vulnerability management and assessment, attack surface reduction, behavior-based and cloud-enabled next-generation protection, endpoint detection and response (EDR), automated investigation and remediation, managed hunting services, and rich APIs. is an endpoint security solution delivered by the cloud. One of its most important features is the Web Content Filter.

Web Content Filter is a feature that helps protect an organization's network by controlling the web content users can access. Blocks malicious and inappropriate websites based on predefined categories. This can be used as a powerful tool to protect against cyber threats, increase productivity and comply with legal requirements. It runs on a Windows endpoint using the Windows SmartScreen engine.

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

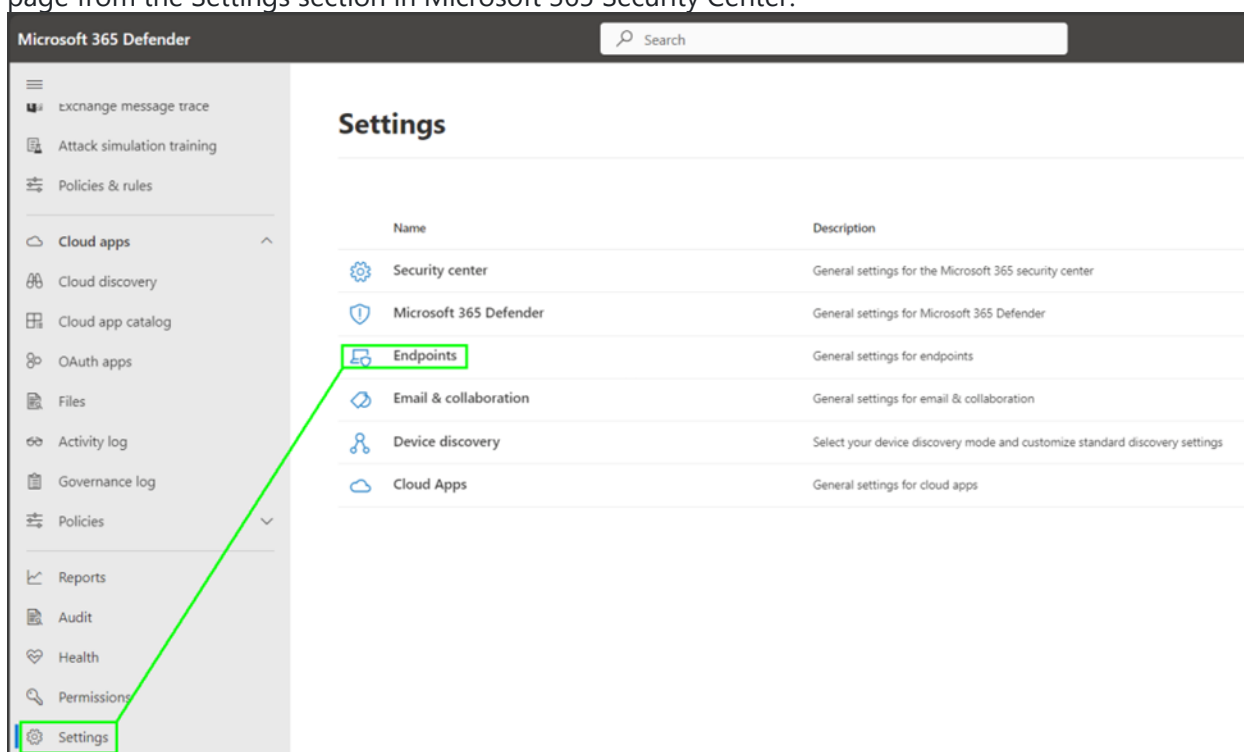
Prerequisites

To use this feature, organizations must have a Microsoft 365 E5, Microsoft 365 E5 Security or Business Premium license. Additionally, the device used must be Windows 10 Enterprise, version 1709 or higher.

<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	✓	✓	✓	✓	✓	✓	✓	

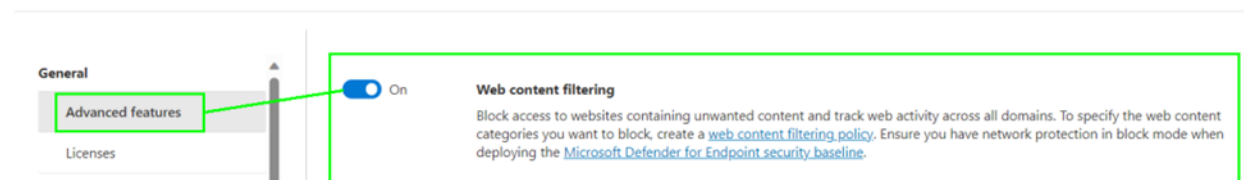
Activating the Web Content Filter

To enable Web Content Filter, we log in to <https://security.microsoft.com/> and enter the Endpoint page from the Settings section in Microsoft 365 Security Center:



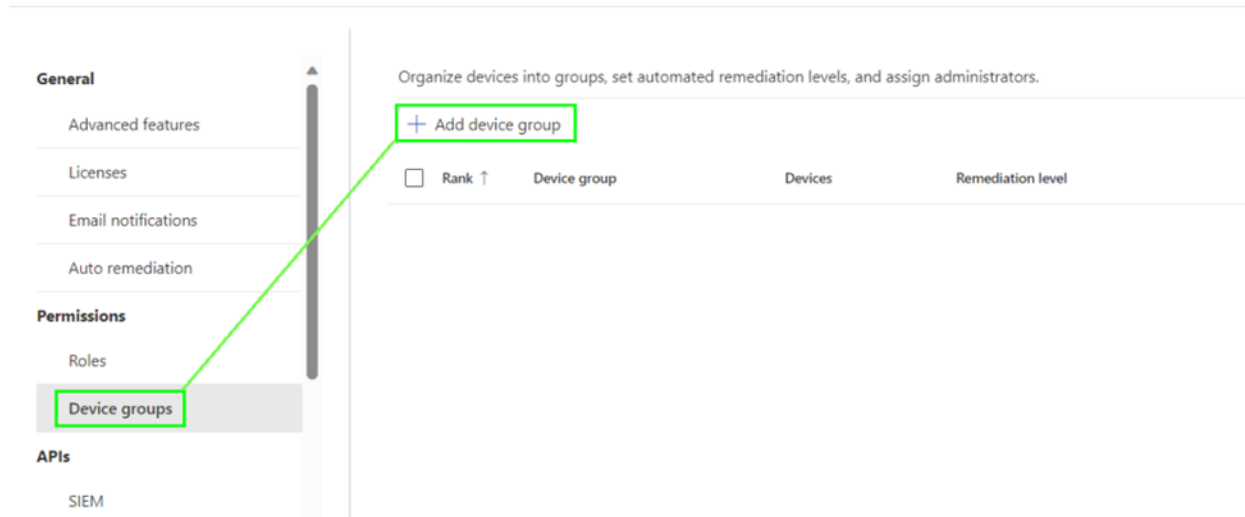
First, we activate the Web Content Filter feature under the Advanced Features tab.

Endpoints



Now we need to define a device group to cover the policy. Unfortunately, Security Center does not use existing Entra ID groups; instead, you must create device groups to extend policies to a group of devices.

Endpoints



We determine the name of the group and the Remediation level. The remediation level we determine here tells us the level of action it will take.

Add device group

General

Devices

Preview devices

User access

General

Provide a name and a description for this notification rule to make it easier to identify and manage.

Device group name *

Ali Teknoloji Device Groups

Remediation level *

Select remediation level

No automated response

Semi - require approval for all folders

Semi - require approval for non-temp folders

Semi - require approval for core folders

Full - remediate threats automatically

We need to add filters to get devices under a certain scope. In this example, we set the filter to apply to every device where the PC name starts with "AKWIN" and the operating system must be Windows 10/11/AVD.

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,...	

We created the device group.

Next, we need to create a category list in which we define which categories of web content should be blocked. Therefore, from the "Rules" section on the left menu, we select "Web Content Filter" and select the Add Policy option.

Endpoints

Rules

Alert suppression

Indicators

Process Memory Indicators

Web content filtering

+ Add Policy

Delete Policy

Policy Name

We determine the name of the policy.

Add Policy

General

Blocked Categories

Scope

Summary

General details

Specify the policy name.

Policy name *

Ali Teknoloji Web Content Filter

Now we determine which categories we want to filter by policy.

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

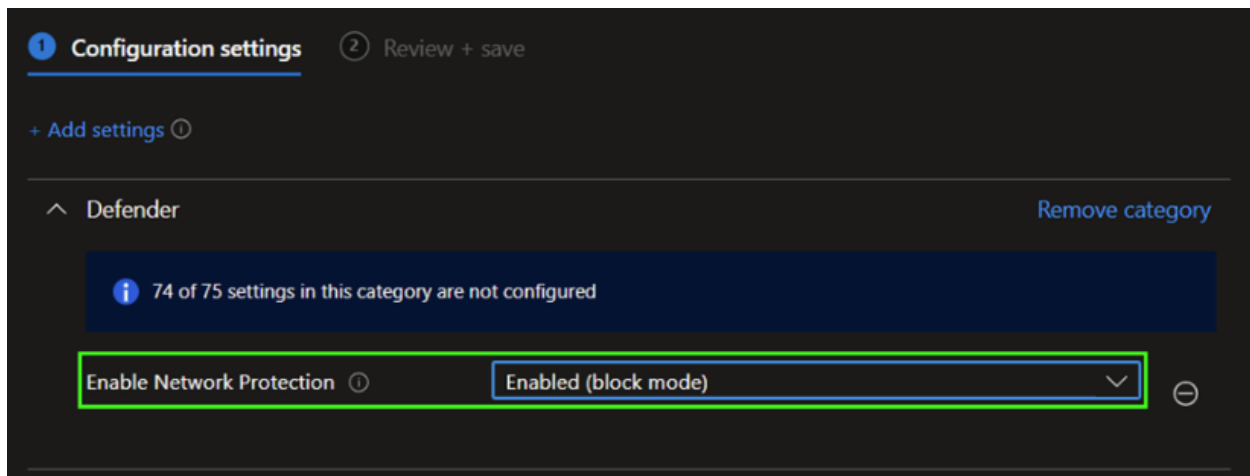
Once we have selected all the categories that need to be blocked, we go ahead and assign the policy to the device group created earlier.

You have now configured everything necessary in Microsoft Security Center.

We activate the Network Protection feature with the Device Configuration Profile.

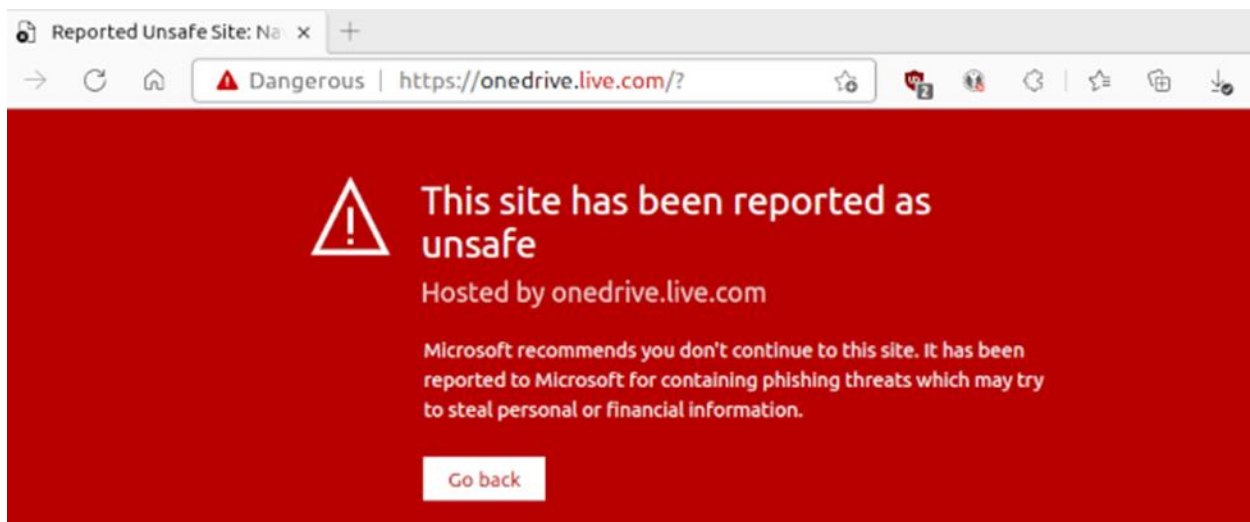
To create a Device Configuration Profile, go to <https://endpoint.microsoft.com> > [Devices](#) > [Configuration Profile](#) > [Create profile from the Settings catalog](#). Then you can type "Network Protection" in the search field.

For "Network Protection", enable the feature in block mode as in the screenshot below:



The resulting profile must be registered after being assigned to the device group.

Once all the configuration has been created, a user trying to EDGE access a blocked url will see the following SmartScreen warning:



The user who tries to access with a different browser will see the following "Access Denied" warning;

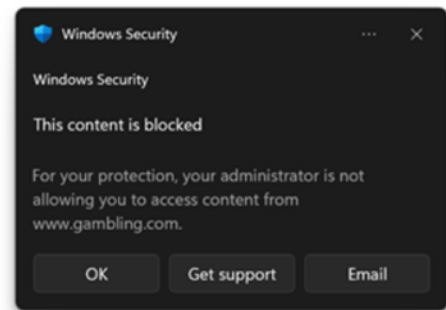


Access to www.gambling.com was denied

You don't have authorization to view this page.

HTTP ERROR 403

Reload



The Web Content Filter feature is also an enableable feature on iOS, Android and macOS devices. We will also examine the study on this in a different article.