

Independent Tests of Anti-Virus Software



Parental Control Certification

Kaspersky Safe Kids for Windows

TEST PERIOD: MAY 2023

LAST REVISION: 1ST JUNE 2023

WWW.AV-COMPARATIVES.ORG

Introduction

Amongst other things, parental control software allows parents to restrict which websites their children can see, in order to avoid the children being exposed to materials the parents consider unsuitable.

Parental Control Certification

AV-Comparatives provides certification for parental control software. In order to be certified, a product must block at least 98% of pornographic websites, have zero false alarms on child-friendly websites, and have no severe unresolved bugs (or design flaws) discovered during the review. A certification is valid for one year and vendors can apply for certification once a year. Only products which were submitted for the Parental Control Test, and which passed the test, are published. Five vendors submitted their products for certification in 2023, of which only two reached the requirements.

Parental Control Test

We tested the effectiveness of the parental control software against 1,000 websites with inappropriate content for children, such as sites displaying pornographic images and text. We chose the appropriate settings for blocking pornography. We additionally tested 100 obviously child-friendly websites, such as lego.com, to check for false positives.



Test Results

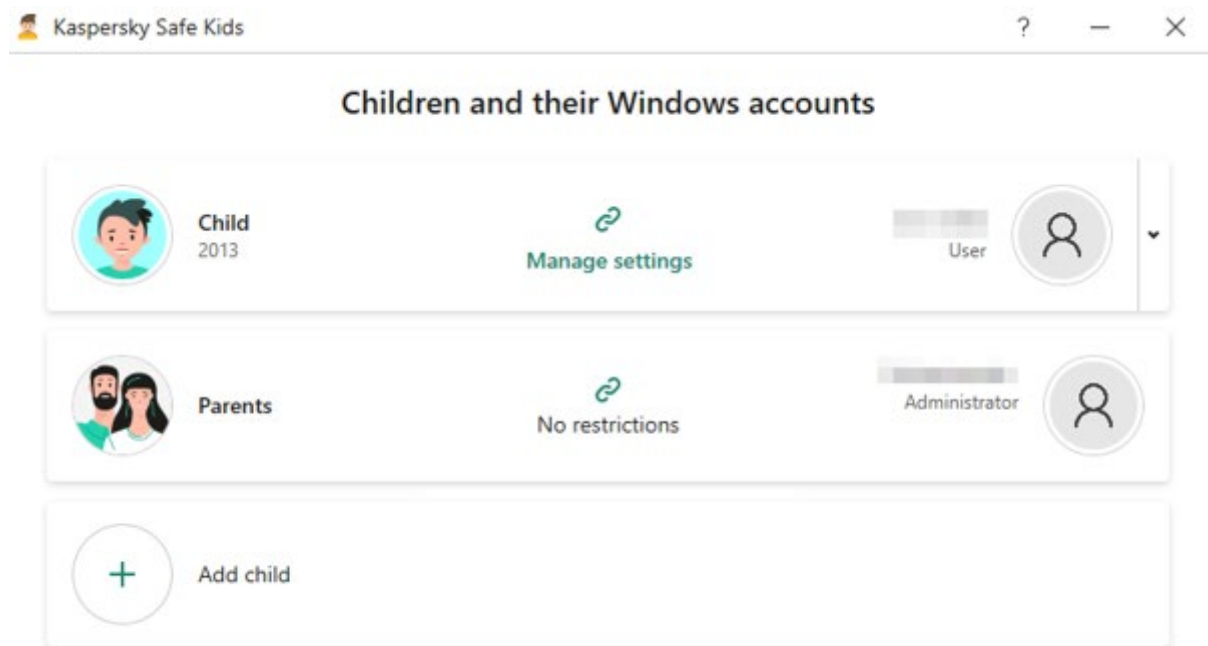
	Block Rate
Adult	98.0%
False-Positives	0

Kaspersky Safe Kids for Windows blocked 98.0% of pornographic websites.

Review

We have included a short review of the product in this report, so that parents have an idea of what the product is like to use and what other features it has.

Kaspersky Safe Kids for Windows



Summary

Kaspersky Safe Kids for Windows is straightforward to install, and very easy to configure using the cloud console. There is a wide range of monitoring and control functions available. We were impressed with the speed at which settings applied in the console are activated on the child's device, as this was virtually instantaneous.

About the product

Kaspersky Safe Kids is a standalone parental control program. It comes in a free and a premium version; the latter includes some additional features, such as scheduled time limits. There is a free trial of the premium version available. We have reviewed the premium version here.

Which versions of Windows are supported?

Windows 7, 8.1, 10, 11

What parental control features does it have?

The product includes web-content filtering; website blacklisting and whitelisting; daily device-usage time limits; application control; safe search (including in YouTube); YouTube history; precise scheduling of computer and application usage times. For mobile devices, there is also battery-level monitoring and location reporting.

Which Windows browsers are supported?

Google Chrome; Mozilla Firefox; Microsoft Edge; Internet Explorer; Opera; Yandex.

What categories of material does it block?

The categories that can be controlled are shown below, together with the default settings for a 7-year-old child:

RESTRICTIONS FOR WEBSITE CATEGORIES

Adult content ⓘ	Forbidden ▼	Electronic commerce ⓘ	Allowed ▼
Job search ⓘ	Allowed ▼	Video games ⓘ	Allowed ▼
Anonymizers ⓘ	Forbidden ▼	Religions, religious associations ⓘ	Warning ▼
Software, audio, video ⓘ	Warning ▼	News media ⓘ	Allowed ▼
Gambling, lotteries, sweepstakes ⓘ	Forbidden ▼	Violence ⓘ	Forbidden ▼
Internet communication ⓘ	Warning ▼	Profanity, obscenity ⓘ	Warning ▼
Alcohol, tobacco, drugs ⓘ	Forbidden ▼	Weapons, explosives, pyrotechnics ⓘ	Forbidden ▼

ADD EXCLUSIONS
Use this list to allow or block access to websites regardless of their categories.

For example: www.example.com
Allowed ▼

How is access to the program and its configuration controlled?

On Windows computers, Kaspersky Safe Kids provides different parental control settings for each Windows user account. This means that you should have an administrator account for yourself, and a non-administrator account for the child, on every computer that the child uses. You have to set up a “My Kaspersky” online account to install the product, and to make changes to the configuration later on.

Installing the product

It is best to first create a My Kaspersky account, and then install the software on the device the child will use, although it’s possible to do it the other way around. In the My Kaspersky web console, you can create profile for each child; this requires you to add a name, year of birth, and select an avatar or use a photo to identify the child. Next, you need to download the installer file for Windows, and run it on the PC that your child uses. Installing the software on the child’s device is very quick and easy; the wizard notes that you should have different Windows accounts for parents and children on the PC. The wizard includes an advice section for parents on how to talk to their children about the program’s restrictions and monitoring functions. You are then prompted to assign the child profiles to one the Windows accounts on the PC.

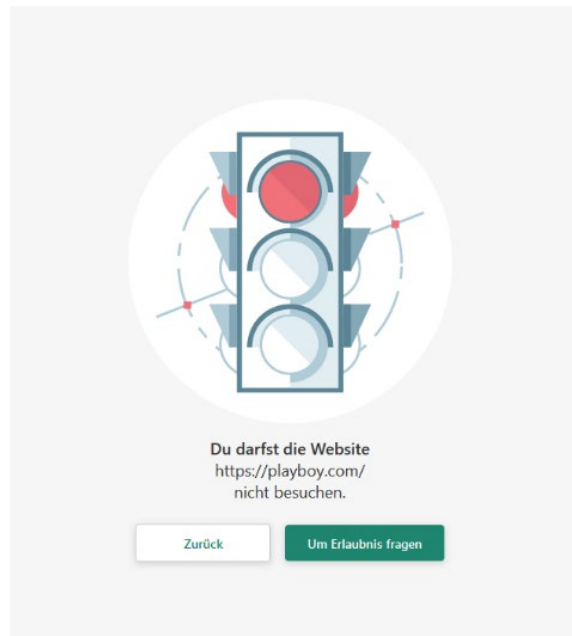
Configuring web-content filtering

Categories for filtering can be set under the settings of the internet section in the Kaspersky Kids web console. The available categories are shown in the screen shot above. There are three settings for each category: Forbidden, Warning, and Allowed, which can be changed using each category's drop-down menu. We note that you have to click Save at the bottom of the page for changes to take effect.

Blacklisting/whitelisting individual sites

Blacklists and whitelists can be configured by adding a websites URL into the box in the *Exclusions* section (shown above), selecting *Forbidden* or *Allowed* as appropriate, and then clicking *Add*. There is also a option *Block all websites except exclusions*, this means the child can only see specifically whitelisted sites. In our functionality test, we found that changes made in the console were applied on the child's device almost instantly.

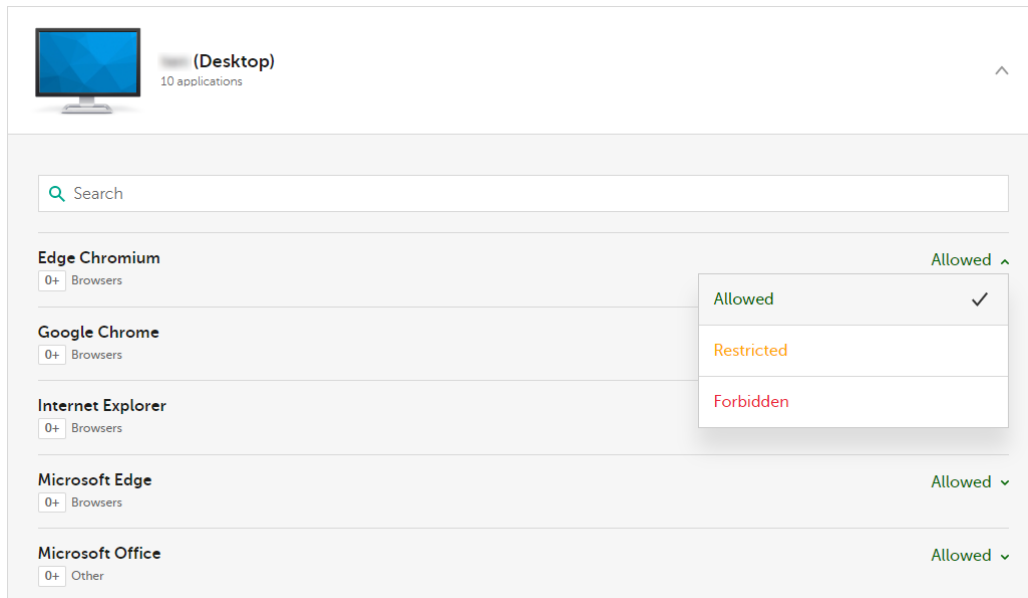
What does the child see when a page is blocked?



Clicking *Back* goes back to the previous page shown in the browser, while *Ask for Permission* sends a message to the child's parents via the web console, saying that the child has requested access.

Configuring Application Monitoring

On the *Settings* tab of the *Applications* page, you will see a device-specific list of applications that you can control. A drop-down menu for each app lets you set permissions to *Allowed*, *Blocked* or *Restricted*. If you select *Restricted*, you can control the number of hours per day the child can use the app, with separate settings for each day of the week.

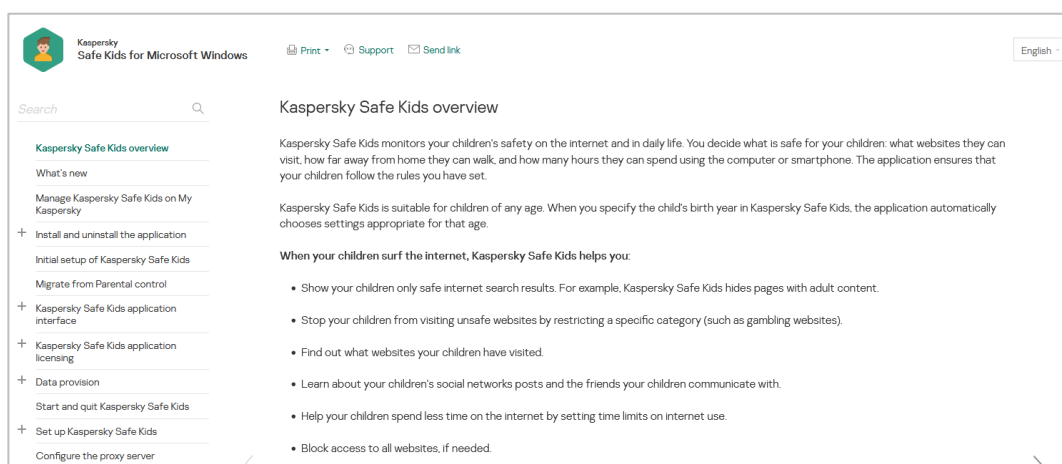


Configuring Time Limits

These are configured on the *Device use* page of the console, *Settings* tab. You can limit the total number of hours per day the child can use a particular device. You can also state whether the device should be blocked outside of the permitted times, or if the child should just be sent a warning instead. You can specify particular times of day when the device cannot be used. The specific times option is very flexible; you can have individual settings for each day of the week, or for weekdays on the one hand and weekends on the other. It's possible to specify multiple use periods each day. We found both the daily usage and the schedule options very easy to configure.

Help

Clicking the ? symbol in the program window (or Help in the System Tray context menu) opens a comprehensive online manual for the product. This provides straightforward text instructions for installing and configuring the program, but unfortunately almost no screenshots.



General advice to parents on choosing and installing parental control software

When it comes to choosing and installing parental control software, it's important to remember that no program can replace the value of talking to your children about adult or disturbing topics they may encounter. Even with parental control software installed, it's possible for children to access inappropriate content through mobile devices borrowed from friends or by using technical workarounds like a proxy server. In essence, parental control software can be most effective in preventing accidental exposure to inappropriate content for younger children.

Before purchasing parental control software, it's important to ensure that it meets your specific needs. Standard features include web content filtering that blocks categories of websites like pornography or weapons. Other features to consider are setting time limits on device usage or Internet access. You may want to restrict usage to certain hours or empower your child to manage their usage themselves. If you have a shared family computer, check that the program allows you to use it without restrictions. To be sure that the program meets your requirements, it's recommended to try a trial version and test it out. Don't hesitate to seek expert assistance if needed.

When installing parental control software on a Windows or macOS computer, it's crucial to prevent children from easily disabling or uninstalling the software. There are two ways to achieve this: either use parental control software with password protection or ensure that your child's account does not have administrator rights. In either case, use a password that your child cannot guess. To properly configure the software for your child, log on to their account when installing the program, and use your administrator credentials to authorize the installation. After installation, check that the software works as expected by testing it with various browsers and websites. Make sure that it prevents computer usage outside of permitted hours and cannot be uninstalled without a password. If you encounter any issues, contact the vendor's support service. Remember not to save the password when configuring the software via a web browser.

Copyright and Disclaimer

This publication is Copyright © 2023 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(June 2023)