Quick Start: Avast Small Office Protection

For more help or troubleshooting, please visit our online documentation:
https://businesshelp.avast.com/

Table of Contents

Quick Start: Avast Small Office Protection 1
Table of Contents 2
Setting Up your Device 5
Verify System Requirements 5
Small Office Protection Endpoints 5
Verify Firewall Requirements 5
Ports 5
URLs 6
Installing Small Office Protection on Devices 6
Windows Workstations 6
Customizing Installation 6
Recommended Components for Servers and Workstations 6
Recommended for Business Environments 7
MacOS X Devices 7
Android Devices 8
iOS Devices 8
Activating Licenses on your Device 8
Windows Workstations 8
Android Devices 9
Activating with Activation Code 9
Activating with Avast Account 9
iOS Devices 9
Settings Configuration and Components 10
Components by Operating System 10
Enabling and Disabling Components 11

Installing and Uninstalling Components....11
Configuring Exclusions....12
Wildcards....12
Exclusions....13
Adding Exceptions....13
Configuring Automatic Updates....13
Configuring Automatic Updates....13
Creating and Configuring Scans....14
Windows Workstations....14
Types of Scans....14
Customizing Full Virus Scans....14
Sensitivity....14
Scan Areas....15
Packers and Archives....15
File Types....15
Exceptions....16
Customizing Targeted Scans....16
Sensitivity....16
Packers and Archives....17
File Types....17
Customizing Explorer Scans....18
Sensitivity....18
Packers and Archives....18
File Types....19
Customizing Boot-time Scans....19
Sensitivity....19
Scan Areas....20
Android Devices....20

Scan of Internal Memory.....20
iOS Devices.....21

Setting Up your Device

Avast's new Small Office Protection differs from Avast Business Antivirus in the following ways:

- license limit of 10, as it is meant for small businesses with limited devices
- *cannot* be installed on server operating systems
- can be installed on Android/iOS devices
- contains many different components
- only available for *unmanaged* devices

For more information on the different components available for Avast Business Antivirus versus Small Office Protection, see Component Overview.

Verify System Requirements

Small Office Protection Endpoints

Windows:

- 7 SP2 or higher, 8.x except RT and Starter Edition, 10 except Mobile and IoT Core Edition

Mac:

- MacOS 10.10 (Mavericks or later with at least 500MB free disk space)

Android:

- Android 4.1 (Jelly Bean) or higher

iPhone/iPad:

- iOS 12.0 or higher

Verify Firewall Requirements

For overall functionality, and to enable the Small Office Protection clients to authenticate/update, you must allow certain ports and URL addresses through your Firewall or Proxy Server.

Ports

TCP & UDP:

- 53 – Secure DNS services (only if using Real Site component)
- 80 – Internet Vulnerability Checks and Feature Updates
- 443 – FFL Encryption Key Negotiation (only if using Real Site component)

URLs

- *.avast.com
- *.avcdn.net
- *.mailshell.net (only if using Anti-Spam)

Installing Small Office Protection on Devices

Windows Workstations

For unmanaged Small Office Protection, you can download the installer from here. When the installer is downloaded, you can run it on the Windows device you would like to install Antivirus on.

Customizing Installation

1. Copy the installer file to a location accessible by the end device
2. Double-click on the installer file to run it
3. If asked to allow the application to make changes to your device, click **Yes**
4. Click **Customize**, then do one of the following:
    - Select **Recommended protection** to install all components
    - Select **Minimal protection** to install only File, Web, and Mail Shield
    - Select **Custom protection** so you can check and uncheck the specific components you would like to install.
5. Click **Install** and wait while Small Office Protection is installed on your device
6. When prompted, restart the device

Recommended Components for Servers and Workstations

A Business environment has different needs than those of consumers, and therefore certain components are not recommended for use in such a network even though they are available in Small Office Protection.

Recommended for Business Environments

The following components should be uninstalled completely or disabled by setting the sliders to **Off**:

- Real Site
- Wi-Fi Inspector

If these components are not removed, you may encounter instability in the network, slower computer operation, or errors.

MacOS X Devices

For unmanaged Small Office Protection, you can download the installer from here. When the installer is downloaded, you can run it on the MacOS X device you would like to install Antivirus on.

1. Copy the installation file (.dmg) to a location accessible by your device, and ensure no other application or antivirus software is running
2. Double-click the downloaded setup file
3. Double-click the Small Office Protection icon, then close the window
4. Click **Continue** in the pop-up, review the Privacy Policy, then click **Continue**
5. Click **Continue** to confirm you have read the *End User License Agreement* and click **Agree** to confirm you accept the terms
6. If you would like to make changes to the default setup, click **Customize**. Otherwise, click **Install**
7. If prompted, use your Touch ID or Administrator Password to grant permission for the installation, then click **Install Software**
8. Click Ok to allow Small Office Protection to access your downloads folder
9. When the *System Extension Blocked* notification appears, click **Open Security Preferences**, then do the following:
    1. Click the lock icon, enter your Administrator Password and click **Unlock**, then click **Allow**
    2. Select **Privacy** and enable *Full Disk Access* for Small Office Protection. When prompted, click **Quit Now**, then close the **Security & Privacy** window
10. Optionally, uncheck the box if you do not want Google Chrome installed as your default browser, then click **Continue**

11. Click **Close** when the installation is complete, then click **Move to Trash**
12. Click **Ok** to allow the Small Office Protection installer to access your downloads folder

Android Devices

You can download Small Office Protection for your Android phone from the Google Play store.

1. Open the Play Store app
2. Search for "Avast"
3. Select **Avast Antivirus - Mobile Security & Virus Cleaner** from the list
4. Click **Install**
5. If necessary, click **Accept** to allow the download to begin

iOS Devices

You can download Small Office Protection for your iOS device from the App Store.

1. Open the App Store
2. Search for "Avast Mobile Security"
3. Select **Avast Security & Privacy** from the list
4. Tap the download icon
5. Once the app is downloaded, tap **Open**
6. If prompted, tap **Allow** to give Avast Security & Privacy to send you notifications

Activating Licenses on your Device

You can activate your Small Office Protection subscription after you have installed the program on your device(s). Your purchase of Small Office Protection should come with a subscription code you can use to activate your devices, which should also be tied to your Avast account. The number of devices you can activate depends on the subscription you purchased.

Windows Workstations

1. Open the Small Office Protection UI on the device
2. Click **Menu**

3. Click **Enter activation code**
4. Type in your activation code/wallet key, then click **Enter**
5. If necessary, confirm the details of your subscription and the involved components

Android Devices

Activating with Activation Code

1. Tap the *Avast Mobile Security* icon on your device to open the app
2. Tap **Menu** ▸ **Remove ads**
3. Tap the **three dots** in the top right, then tap **Already purchased**
4. Select **Redeem an activation code**
5. Type or paste your activation code into the text box, including hyphens
6. Tap **Use This Code** to complete activation

Activating with Avast Account

1. Tap the *Avast Mobile Security* icon on your device to open the app
2. Tap **Menu** ▸ **Remove ads**
3. Tap the **three dots** in the top right, then tap **Already purchased**
4. Select **Restore from Avast Account**
5. Select **Email**
6. Enter your Avast Account credentials
7. Tap **Log In Avast Account**

iOS Devices

1. Tap the *Avast Security & Privacy* icon on your device to open the app
2. Tap Upgrade
3. Tap **Already purchased**
4. Select **Enter Avast subscription code**
5. Type or paste your activation code into the text box, including hyphens
6. Tap **Ok** to complete activation

Settings Configuration and Components

There are many components that come along with Small Office Protection, both for workstations and mobile devices.

Components by Operating System

Component	Windows Workstations	MacOS X	Android	iOS
File Shield	X	X		
Web Shield	X	X	X	
Mail Shield	X	X		
Behavior Shield	X			
Ransomware Shield	X	X		
Remote Access Shield	X			
Wi-Fi Inspector	X	X		
Real Site	X			
Firewall	X			
Sandbox	X			
Anti-Spam				
Exchange				
Sharepoint				
Webcam Shield	X			
Sensitive Data Shield	X			
SecureLine VPN				
Data Shredder	X			
Passwords	X			
Password Protection	X			
Software Updater	X			
Browser Cleanup	X			
Do Not Disturb Mode	X			
Rescue Disk	X			
File Scanner			X	
Photo Vault			X	X
Identity Protection				X
App Lock			X	
Anti-Theft			X	
Camera Trap			X	

Component	Windows Workstations	MacOS X	Android	iOS
Last Known Location			X	
SIM Security			X	
Call Blocker			X	
Power Save			X	
RAM Boost			X	
Junk Cleaner			X	
Wi-Fi Speed Test			X	
Wi-Fi Security			X	X
App Insights			X	
VPN Standalone App			X	X

Enabling and Disabling Components

Many of the shields and tools available in Small Office Protection can be enabled or disabled on the device. This is especially useful if you are trying to install only a few of the components on a server, or just keeping your number of tools to a minimum. Some tools, however, can only be installed or uninstalled entirely, such as Sandbox and Rescue Disk.

1. Open the Small Office Protection client UI
2. Click on the proper tab for the component you are trying to enable or disable:
    - **Protection:** File Shield, Web Shield, Mail Shield, Behavior Shield, Sandbox, Wi-Fi Inspector, Real Site, Firewall
    - **Privacy:** Passwords, Anti-Spam, Data Shredder, Webcam Shield
    - **Performance:** Software Updater
3. Click on the button for the component
4. Beside the component you want to alter, do one of the following:
    - To enable the component, move the slider to **On**
    - To disable the component, move the slider to **Off**
5. If required, confirm your choice

Installing and Uninstalling Components

Most Active Protection features are installed with Small Office Protection, but these components can be uninstalled and reinstalled as needed via the Troubleshooting

menu. MacOS X protection components cannot be installed or uninstalled but can be turned off.

1. Open the Small Office Protection client UI
2. Navigate to **Menu** ▸ **Settings** ▸ **General** ▸ **Troubleshooting**
3. Click **Add/Modify Components**
4. Beside the components you want to alter, do one of the following:
    - If the component is not yet installed, check the box beside it
    - If the component is already installed, uncheck the box beside it
5. Click **Change** to confirm once you are finished making your edits

For more details on configuring the various components available in the settings of Small Office Protection, see Configuring Settings in Small Office Protection.

Configuring Exclusions

Wildcards

Many of the Shields and other components included in Small Office Protection, as well as the main Antivirus itself, enable you to configure exclusions or block specific paths. Wildcards help when you do not know the exact file path or file name of files you want to include or exclude, or if you want to indicate multiple files in one path. Not all file paths allow the use of wildcards.

Character	Meaning
?	Replaces a single character **For example:** `ab?.html` matches the files `abc.html`, `abd.html`, `abe.html`, etc. It will **not** match the file `abc.htm`.
*	Replaces zero or more characters **For example:** `*mtl` matches the files `abc.html` and `d.html`. `*txt` matches the files `abc.txt`, `x.txt`, and `xyztxt`.

Exclusions

You can configure exclusions that will propagate across all of the various Shields and components of Small Office Protection in the *Exceptions* tab of the **Settings** ▸ **General** page.

Adding Exceptions

1. Open the Small Office Protection client UI
2. Click **Menu** in the top-right, then **Settings**
3. In the **General** ▸ **Exceptions** section, click **Add Exception**, then do one of the following:
    - Enter or browse to a file path you would like to exclude
    - Enter or browse to a folder path you would like to exclude
    - Enter a URL you would like to exclude
4. Click **Add Exception** when you are finished

Configuring Automatic Updates

You can automatically update the virus definitions and Small Office Protection program version on your device(s) when new updates are available. You can also set your device(s) to update manually. For more information, see Updating Small Office Protection.

Configuring Automatic Updates

1. Click **Menu** in the top-right of the UI
2. Click **Settings**
3. In the *General* section, navigate to the **Update** tab
4. Beside the two **Check for Updates** buttons, click **More options**
5. Select **Automatic Update**

Creating and Configuring Scans

Windows Workstations

You can configure the types of files and programs that are scanned by Small Office Protection in the Virus Scans settings. Therefore, the main details for what will be scanned are configured in the scan settings, while exclusions are configured in the General section.

Types of Scans

- **Full Virus Scan—**Run an in-depth scan of your system, checking all hard drives, rootkits, and auto-start programs
- **Targeted Scan—**Scans only the folders you select when you initiate the scan
- **Explorer Scan—**Performs a scan of folders or drives that you specify, but is only available in the Windows context menu when you right-click on a file, folder, or drive
- **Boot-time Scan (MS Windows only)—**Runs a scan when the device boots up

You can access the settings for the various scan types by clicking Menu ▸ Settings, then navigating to Protection ▸ Virus Scans.

Customizing Full Virus Scans

Sensitivity

You can determine the sensitivity of the scan by adjusting the scan sensitivity settings. The higher the sensitivity, the higher the protection and potential for false positive malware detections. Reducing the sensitivity reduces the chance of false positive detections, but may also reduce the effectiveness of the scans. Scan sensitivity can be adjusted to Medium, High, or Low sensitivity by dragging the slider.

Scan for potentially unwanted programs (PUPs): enables Avast to scan for programs that are stealthily downloaded with other programs and can perform unwanted activity

Follow links during scan: enables Avast to scan other files used by the files being scanned for potentially harmful content

Test whole files (very slow for big files): enables Avast to scan entire files rather than only the parts typically affected by malicious code

Scan priority: determines how many resources can be utilized by Avast during the scan. Higher priority means a faster scan, but may slow down other processes on the device

Scan Areas

Select or tick the boxes beside the listed areas to include them in your scan. The main area options are:

- **All harddisks:** enables Avast to scan all hard drives on your PC
- **System drive:** the options in this section apply to data that is stored on physical devices such as hard drives and USB sticks

The following options for scanning will be applied to the area specified above.

All removable media: enables Avast to scan applications that launch automatically when you insert a USB or other removable device into your PC

Rootkits: enables Avast to scan for hidden threats in the system

UEFI BIOS: enables Avast to scan the main firmware interfaces during boot-up

CD-ROM & DVD drives: enables Avast to scan CD and DVD drives for malicious content

Modules loaded in memory: enables Avast to scan applications and processes that launch after system startup or run in the background

Packers and Archives

In the Packers and Archives section you can specify the compressed file types that you want Avast to unpack during the scan.

- **Scan only common installers:** scans the contents of executable files utilized when installing applications
- **Scan all archives:** scans all archive file contents, which may slow down the scan considerably
- **Don't scan archives:** disables Avast from scanning archive files

File Types

Specify the file types that are prioritized when scanning your PC for malware:

- **Content based types (slow):** scans files that are typically most vulnerable to malware attacks
- **Name extension based types (fast):** scans files with only risky extensions, such as .exe, .com, .bat
- **Scan all files (very slow):** scans all files on your PC for malware

Perform automatic actions during this scan: enable this option and define the automatic action when an infected file is found:

- **Fix automatically:** enables Avast to repair the infected file. If repair is not possible, the file is moved to the Virus Chest, and if that fails the file is deleted
- **Move file to Virus Chest:** the infected file will not be repaired automatically, but will be moved to the Virus Chest
- **Delete File:** Avast will not try to repair the infected file or move it to the Virus Chest, instead the file will be deleted automatically

Shut down computer after scan finishes: enables Avast to shut down your computer after the scan completes

Generate report file: enables Avast to create and store a report file automatically. The report file location is listed beneath this option.

Exceptions

Although it is not recommended to exclude any files or folders from a scan, you can define certain exceptions to temporarily exclude particular files or folders from a scan for troubleshooting purposes. At the bottom of the scan settings page, click **View exceptions**. From there you can follow the steps in **Configuring Exclusions**.

Customizing Targeted Scans

Sensitivity

You can determine the sensitivity of the scan by adjusting the scan sensitivity settings. The higher the sensitivity, the higher the protection and potential for false positive malware detections. Reducing the sensitivity reduces the chance of false positive detections, but may also reduce the effectiveness of the scans. Scan sensitivity can be adjusted to Medium, High, or Low sensitivity by dragging the slider.

Scan for potentially unwanted programs (PUPs): enables Avast to scan for programs that are stealthily downloaded with other programs and can perform unwanted activity

Follow links during scan: enables Avast to scan other files used by the files being scanned for potentially harmful content

Test whole files (very slow for big files): enables Avast to scan entire files rather than only the parts typically affected by malicious code

Scan priority: determines how many resources can be utilized by Avast during the scan. Higher priority means a faster scan, but may slow down other processes on the device

Packers and Archives

In the Packers and Archives section you can specify the compressed file types that you want Avast to unpack during the scan.

- **Scan only common installers:** scans the contents of executable files utilized when installing applications
- **Scan all archives:** scans all archive file contents, which may slow down the scan considerably
- **Don't scan archives:** disables Avast from scanning archive files

File Types

Specify the file types that are prioritized when scanning your PC for malware:

- **Content based types (slow):** scans files that are typically most vulnerable to malware attacks
- **Name extension based types (fast):** scans files with only risky extensions, such as .exe, .com, .bat
- **Scan all files (very slow):** scans all files on your PC for malware

Perform automatic actions during this scan: enable this option and define the automatic action when an infected file is found:

- **Fix automatically:** enables Avast to repair the infected file. If repair is not possible, the file is moved to the Virus Chest, and if that fails the file is deleted
- **Move file to Virus Chest:** the infected file will not be repaired automatically, but will be moved to the Virus Chest
- **Delete File:** Avast will not try to repair the infected file or move it to the Virus Chest, instead the file will be deleted automatically

Shut down computer after scan finishes: enables Avast to shut down your computer after the scan completes

Generate report file: enables Avast to create and store a report file automatically. The report file location is listed beneath this option.

Customizing Explorer Scans

Sensitivity

You can determine the sensitivity of the scan by adjusting the scan sensitivity settings. The higher the sensitivity, the higher the protection and potential for false positive malware detections. Reducing the sensitivity reduces the chance of false positive detections, but may also reduce the effectiveness of the scans. Scan sensitivity can be adjusted to Medium, High, or Low sensitivity by dragging the slider.

Scan for potentially unwanted programs (PUPs): enables Avast to scan for programs that are stealthily downloaded with other programs and can perform unwanted activity

Follow links during scan: enables Avast to scan other files used by the files being scanned for potentially harmful content

Test whole files (very slow for big files): enables Avast to scan entire files rather than only the parts typically affected by malicious code

Scan priority: determines how many resources can be utilized by Avast during the scan. Higher priority means a faster scan, but may slow down other processes on the device

Packers and Archives

In the Packers and Archives section you can specify the compressed file types that you want Avast to unpack during the scan.

- **Scan only common installers:** scans the contents of executable files utilized when installing applications
- **Scan all archives:** scans all archive file contents, which may slow down the scan considerably
- **Don't scan archives:** disables Avast from scanning archive files

File Types

Specify the file types that are prioritized when scanning your PC for malware:

- **Content based types (slow):** scans files that are typically most vulnerable to malware attacks
- **Name extension based types (fast):** scans files with only risky extensions, such as .exe, .com, .bat
- **Scan all files (very slow):** scans all files on your PC for malware

Perform automatic actions during this scan: enable this option and define the automatic action when an infected file is found:

- **Fix automatically:** enables Avast to repair the infected file. If repair is not possible, the file is moved to the Virus Chest, and if that fails the file is deleted
- **Move file to Virus Chest:** the infected file will not be repaired automatically, but will be moved to the Virus Chest
- **Delete File:** Avast will not try to repair the infected file or move it to the Virus Chest, instead the file will be deleted automatically

Shut down computer after scan finishes: enables Avast to shut down your computer after the scan completes

Generate report file: enables Avast to create and store a report file automatically. The report file location is listed beneath this option.

Customizing Boot-time Scans

Sensitivity

You can determine the sensitivity of the scan by adjusting the scan sensitivity settings. The higher the sensitivity, the higher the protection and potential for false positive malware detections. Reducing the sensitivity reduces the chance of false positive detections, but may also reduce the effectiveness of the scans. Scan sensitivity can be adjusted to Medium, High, or Low sensitivity by dragging the slider.

Scan for potentially unwanted programs (PUPs): enables Avast to scan for programs that are stealthily downloaded with other programs and can perform unwanted activity

Unpack archive files: enables Avast to extract ('unpack') files and folders from archives for scanning

Scan Areas

Select or tick the boxes beside the listed areas to include them in your scan. The main area options are:

- **All harddisks:** enables Avast to scan all hard drives on your PC
- **System drive:** the options in this section apply to data that is stored on physical devices such as hard drives and USB sticks

The following options for scanning will be applied to the area specified above.

Auto start programs: enables Avast to check all auto-start programs

Perform automatic actions during this scan: enable this option and define the automatic action when an infected file is found:

- **Fix automatically:** enables Avast to repair the infected file. If repair is not possible, the file is moved to the Virus Chest, and if that fails the file is deleted
- **Move file to Virus Chest:** the infected file will not be repaired automatically, but will be moved to the Virus Chest
- **Delete File:** Avast will not try to repair the infected file or move it to the Virus Chest, instead the file will be deleted automatically

Android Devices

The Scan option enables you to scan all applications installed on your device and informs you about security risks caused by changes in default Android settings. The virus definitions used by the scan are updated automatically.

1. Tap the *Avast Mobile Security* icon on your device to open the app
2. Tap **Scan** on the main screen

Once the scan finishes, the app either displays that everything is fine or lists the found issues and offers possibilities to resolve them. You can tap **Resolve** or **Enable** if these actions are available.

Scan of Internal Memory

By default, the scan of Internal Memory is turned off. If you would like your device's internal storage to be included in the scans, you can turn it on in the Settings.

1. Tap the *Avast Mobile Security* icon on your device to open the app
2. Tap **Menu ▸ Settings**

3. Tap **Protection**
4. Click the slider to enable *Internal storage scanning*

iOS Devices

The Scan option enables you to scan all applications installed on your device and informs you about security risks caused by changes in default iOS settings. The virus definitions used by the scan are updated automatically.

1. Tap the *Avast Security & Privacy* icon on your device to open the app
2. Tap **Scan** on the main screen

Once the scan finishes, the app either displays that everything is fine or lists the found issues and offers possibilities to resolve them. You can tap **Resolve** or **Enable** if these actions are available.

There are many more features and options available in Small Office Protection. For more information, please see our Knowledge Base at https://businesshelp.avast.com/.