



Avast Business

Quick Start: AVG Business Antivirus

For more help or troubleshooting, please visit our online documentation:

<https://businesshelp.avast.com/>

Table of Contents

Quick Start: AVG Business Antivirus	1
Table of Contents	2
Antivirus Setup	5
Setting Up your Device	5
Verify System Requirements	5
AVG Business Antivirus Endpoints	5
Verify Firewall Requirements	5
Geoblocking	6
Ports (TCP & UDP)	6
URLs	6
Installing AVG Business Antivirus on Devices	6
Customizing Installation	6
Recommended Components for Servers and Workstations	7
Recommended for Business Environments	7
Recommended for Servers	7
Activating Licenses on your Device	8
Configuring Settings	9
Settings Configuration and Components	9
Antivirus Components by Product License	9
Enabling and Disabling Components	9
Installing and Uninstalling Components	10

Configuring Exclusions	11
Wildcards	11
Exclusions	11
Adding Exceptions	11
Configuring Automatic Updates	12
Configuring Automatic Updates	12
Creating and Configuring Scans	12
Types of Scans	13
Customizing Deep Scans	13
Sensitivity	13
Scan Areas	14
Packers and Archives	14
File Types	14
Exceptions	15
Customizing File or Folder Scans	16
Sensitivity	16
Packers and Archives	16
File Types	16
Customizing Explorer Scans	17
Sensitivity	17
Packers and Archives	18
File Types	18
Customizing Boot-time Scans	19

Sensitivity	19
Scan Areas	19
Glossary	21

Antivirus Setup

Setting Up your Device

Verify System Requirements

AVG Business Antivirus Endpoints

Windows:

- 11 – x64, x86
- 10 – all versions except Mobile and IoT Core Edition – x64, x86
- 8/8.1 – all versions except RT and Starter Edition – x64, x86
- 7 SP1 – requires KB3033929requiresKB3033929 – x64, x86
- Server 2022, 2019, 2016, 2012 – any edition with latest service pack excluding Server Core – x64
- Server 2008 R2 – requires KB3033929requiresKB3033929 – x64
- Small Business Server 2011 – x64

Supported applications:

- Exchange Server 2022, 2019, 2016, 2013, 2010
- SharePoint Server 2019, 2016, 2012, 2010
- SharePoint Services 3.0 and higher

Verify Firewall Requirements

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

Geoblocking

AVG web services are hosted in many countries around the world. Therefore, we do not recommend geoblocking in your firewall settings.

If geoblocking is necessary, we recommend you set URL Allow rules to supercede geoblocking, so AVG traffic can still be allowed.

Ports (TCP & UDP)

- 80 - Internet Vulnerability Checks and Feature Updates

URLs

- *.avast.com
- *.avg.com
- *.avcdn.net

Installing AVG Business Antivirus on Devices

For unmanaged AVG Business Antivirus, you can download the installer from <https://www.avg.com/en-us/installation-files-business>. On the Business tab, select the installer for the Antivirus version you have. When the installer is downloaded, you can run it on the 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 Email Shield
 - Select **Custom protection** so you can check and uncheck the specific components you would like to install.
5. Click **Install** and wait while AVG Business Antivirus 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 AVG Business Antivirus.

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.

Recommended for Servers

The following components should be uninstalled completely or disabled on servers by setting the sliders to **Off** or by not installing them on the device entirely:

- Web Shield
- Mail Shield

Activating Licenses on your Device

You can activate your AVG Business Antivirus subscription after you have installed the program on your device(s).

1. Open the AVG Business Antivirus UI on the device
2. Click **MyAVG** or **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

Configuring Settings

Settings Configuration and Components

There are many components that come along with AVG Business Antivirus, both in the baseline Antivirus and in the additional versions.

Antivirus Components by Product License

Component	AVG Email Server Business	AVG File Server Business	AVG Antivirus Business	AVG Internet Security Business
File Shield	X	X	X	X
Web Shield			X	X
Email Shield			X	X
Anti-Spam	X	X		X
Enhanced Firewall			X	X
Behavior Shield			X	X
Data Safe			X	X
Exchange	X	X		X
Sharepoint	X	X		X
Data Shredder			X	X

Enabling and Disabling Components

Many of the shields and tools available in AVG Business Antivirus 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.

1. Open the AVG Business Antivirus client UI
2. Click on the proper button for the component you are trying to enable or disable:
 - **Computer:** File Shield, Behavior Shield
 - **Web & Email:** Web Shield, Email Shield
 - **Hacker Attacks:** Enhanced Firewall
3. 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**
4. If required, confirm your choice

Installing and Uninstalling Components

Most Active Protection features are installed with AVG Business Antivirus, but these components can be uninstalled and reinstalled as needed via the Troubleshooting menu.

1. Open the AVG Business Antivirus 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 AVG Business Antivirus, see [Configuring Settings in AVG Business Antivirus](#).

Configuring Exclusions

Wildcards

Many of the Shields and other components included in AVG Business Antivirus, 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: <code>ab?.html</code> matches the files <code>abc.html</code> , <code>abd.html</code> , <code>abe.html</code> , etc. It will not match the file <code>abc.htm</code> .
*	Replaces zero or more characters For example: <code>*mtl</code> matches the files <code>abc.html</code> and <code>d.html</code> . <code>*txt</code> matches the files <code>abc.txt</code> , <code>x.txt</code> , and <code>xyztxt</code> .

Exclusions

You can configure exclusions that will propagate across all of the various Shields and components of AVG Business Antivirus in the *Exceptions* tab of the **Settings** ▶ **General** page.

Adding Exceptions

1. Open the AVG Business Antivirus 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 AVG Business Antivirus 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 AVG Business Antivirus](#).

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

You can configure the types of files and programs that are scanned by AVG Business Antivirus in the 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

- **Deep Scan**—Run an in-depth scan of your system, checking all hard drives, rootkits, and auto-start programs
- **File or Folder 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**—Run 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 Deep 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 AVG to scan for programs that are stealthily downloaded with other programs and can perform unwanted activity

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

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

Scan priority: determines how many resources can be utilized by AVG 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 AVG 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 AVG to scan applications that launch automatically when you insert a USB or other removable device into your PC

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

UEFI BOOT: enables AVG to scan the main firmware interfaces during boot-up

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

Modules loaded in memory: enables AVG 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 AVG 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 AVG 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 AVG to repair the infected file. If repair is not possible, the file is moved to Quarantine, and if that fails the file is deleted
- **Move file to Quarantine:** the infected file will not be repaired automatically, but will be moved to Quarantine
- **Delete File:** AVG will not try to repair the infected file or move it to Quarantine, instead the file will be deleted automatically

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

Generate report file: enables AVG 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 Standard Antivirus Exceptions](#).

Customizing File or Folder 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 AVG to scan for programs that are stealthily downloaded with other programs and can perform unwanted activity

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

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

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

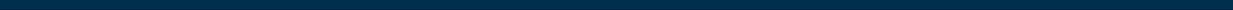
Packers and Archives

In the Packers and Archives section you can specify the compressed file types that you want AVG 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 AVG 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 AVG to repair the infected file. If repair is not possible, the file is moved to Quarantine, and if that fails the file is deleted
- **Move file to Quarantine:** the infected file will not be repaired automatically, but will be moved to Quarantine
- **Delete File:** AVG will not try to repair the infected file or move it to Quarantine, instead the file will be deleted automatically

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

Generate report file: enables AVG 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 AVG to scan for programs that are stealthily downloaded with other programs and can perform unwanted activity

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

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

Scan priority: determines how many resources can be utilized by AVG 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 AVG 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 AVG 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 AVG to repair the infected file. If repair is not possible, the file is moved to Quarantine, and if that fails the file is deleted

- **Move file to Quarantine:** the infected file will not be repaired automatically, but will be moved to Quarantine
- **Delete File:** AVG will not try to repair the infected file or move it to Quarantine, instead the file will be deleted automatically

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

Generate report file: enables AVG 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 AVG to scan for programs that are stealthily downloaded with other programs and can perform unwanted activity

Unpack archive files: enables AVG 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 AVG 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 AVG 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 AVG 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:** AVG will not try to repair the infected file or move it to the Virus Chest, instead the file will be deleted automatically

There are many more features and options available in AVG Business Antivirus. For more information, please see our Knowledge Base at <https://businesshelp.avast.com/>.

Glossary

A

Anti-spam

Antivirus component designed to scan outgoing and incoming emails for threats.

Antivirus

A service which keeps devices safe from viruses and other threats. Requires regular virus definition updates to be effective.

av

A service which keeps devices safe from viruses and other threats. Requires regular virus definition updates to be effective.

Avast Business Antivirus

A service which keeps devices safe from viruses and other threats. Requires regular virus definition updates to be effective.

AVG Business Antivirus

A service which keeps devices safe from viruses and other threats. Requires regular virus definition updates to be effective.

D

Device

Personal computers, laptops, or server devices you would like to add to your network.

E

Exception

Individual or uncategorized websites, files, etc allowed or blocked by Antivirus.

Exclusion

Individual or uncategorized websites, files, etc allowed or blocked by Antivirus.

F

Firewall

Antivirus component which scans all outgoing and incoming traffic to a device for threats.

G

Group

Organizational structure used for managing numbers of devices on a network. Your Console comes with a default group which can be renamed, but cannot not be deleted.

L

License

The type of subscription you have for a specific, paid Avast or AVG product.

Local Update Server

Device(s) in your network designated by your Console to download, deploy to, or scan other networked machines.

M

Master Agent

Device(s) in your network designated by your Console to download, deploy to, or scan other networked machines.

P

Policy

A set of settings applied to device(s) from your Console to automate client-side Antivirus processes.

Potentially Unwanted Program

Programs which sometimes act similarly to malware or spyware, usually installed as part of another installation.

PUP

Programs which sometimes act similarly to malware or spyware, usually installed as part of another installation.

Q

Quarantine

Component of Antivirus which quarantines potentially infected files until it has been determined that it is safe to permanently delete them, either manually or according to a schedule.

R

Remote Deployment

Method of installing Antivirus from your Console to all chosen devices on the local network, only available when a device on the network already has Antivirus

installed through a different method.

S

Subscription

The type of subscription you have for a specific, paid Avast or AVG product.

V

Virus Chest

Component of Antivirus which quarantines potentially infected files until it has been determined that it is safe to permanently delete them, either manually or according to a schedule.