Quick Start: AVG Business Management Consoles

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

Table of Contents

Introduction to the AVG Business Management Consoles

With the AVG Business Management Consoles, adding critical protection to every PC and server has never been easier. Flexible management provides the most convenient way to protect businesses. The Management Consoles provide:

- Complete control over the behavior of Antivirus on endpoint devices
- Centralized management of multiple devices, either accessible anywhere in the Cloud or situated locally with the On-Premise Console
- A complete overview of the current status of entire environment with immediate alerts
- Automatic and seamless updates

AVG Business Management Consoles integrate seamlessly with AVG Business Antivirus to:

- Leverage virtualization to protect confidential information
- Protect multiple platforms - PCs and servers
- Update to the latest version automatically or manually
- Add extra firewall protection for remote endpoints
- Provide complete server protection
- Secure your e-mail client

When you install AVG Business Antivirus on devices through the AVG Business Management Consoles, you can control AVG Business Antivirus on those devices remotely. You can change and apply settings to each device individually, without having to visit each device or recall them from the field.

Setting Up the Management Console

Verify Console System Requirements

AVG Business Cloud Console

Browsers (latest versions recommended):

- Google Chrome
- Firefox
- Safari
- Microsoft Edge
- Internet Explorer

AVG Business On-Premise Console

Windows:

- 7 SP1 or higher, 8.x, 10
- Server 2008 R2 SP1, 2012 and 2012 R2, 2016, 2019 any edition
- Small Business Server 2008, 2011 (64 bit only)
- Exchange Server 2003 x86 (up to 18.8), 2007, 2010, 2013, 2016, 2019 (64 bit only)
- SharePoint Server 2003, 2007, 2010, 2012, 2016, 2019 (64 bit only)

AVG Business Antivirus Endpoints

Windows:

- 7 SP1 or higher, 8.x except RT and Starter Edition, 10 except Mobile and IoT Core Edition
- Server 2008 R2, 2012 R2, 2016, 2019, all any edition with latest service pack excluding Server Core
- Microsoft Exchange Server 2010 SP2, 2013, 2016, 2019
- Microsoft SharePoint Services 3.0 and SharePoint Server 2010 and higher

AVG Business Patch Management

Windows Only:

- 7 SP1 or higher, 8.x, 10
- Server 2008 R2 with latest service pack excluding Server Core, 2012, 2016, 2019
- Exchange Server 2010 SP2, 2013, 2016

Verify Console Firewall Requirements

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

Ports

TCP & UDP:

- 80 – Internet vulnerability checks and feature updates
- 443 – FFL Encryption Key negotiation
- 8080, 8090 – Communication between console and clients within local network (only for On-Premise Console)
- 4158 – Mirror, for local updates within local network
- 7074 – Remote Deployment within local network

URLs

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

Setting Up the Console

Cloud Console

1. Navigate to https://console.avg.com/
2. Click **Register** and fill in all required information to set up access

On-Premise Console

1. Navigate to https://www.avg.com/en-us/installation-files-business
2. Under the Business tab, click **Download** beside the AVG On-Premise Management Console

For the On-Premise Console, follow the installation process for your operating system as detailed in On-Premise Console Management.

Activating Licenses in the Management Console

An activation code is part of your confirmation of purchase. It contains information about the edition you purchased. Your code is the license used to activate your software.

1. When running the Console for the first time, the screen will prompt you to enter your license code.
2. Enter your license code.
3. Click **Activate license code**.

Activating Additional Licenses

1. Navigate to the *Subscriptions* page
2. Do one of the following:
   - If you have a license code, click **Got activation code?**, enter the code, then click **Activate**
   - Beside the subscription you would like to purchase, click **Buy**, then complete the transaction

Assigning Licenses to Devices

You can only perform this action after you have added a device to your network.

This procedure requires the device to restart.

1. On the *Devices* page, do one of the following:
   - To include all devices in a group, click the **More** button next to the group name. Then click **Edit group**.

- To include multiple devices, select the check boxes of the devices. Then click **Actions ▸ Change subscription**.
- For a single device, click the **More** button next to a device, then click **Change subscription**.

2. Select the license you would like to use from the drop-down menu(s).
3. Click **Apply** for the license you want to change to, or **Save group** if you are changing the subscription for an entire group of devices.

Adding Devices via the Installer File or Shareable Link

Cloud Console and On-Premise Console

Downloading Installer

1. Select which type of installer you need:
    - Windows .exe (for workstations and servers)
    - Windows .msi (for deployment using GPO)
2. Select the subscription products
3. Click **Advanced Settings** to view the following options
4. Choose the Group and Policy the device will use
    - **If desired, you can activate your devices and select the subscriptions to use after installation by checking the box with that option.**
5. Choose whether to automatically remove competitive antivirus products on the device
    - **The option to remove competitive antivirus products is checked by default. We recommend that you leave this option checked when installing the Antivirus service.**
6. Select the installer size (Light vs Full)
    - **If you select Light, the other services will be downloaded upon installation of the Antivirus agent. This option is not recommended if you are installing Antivirus on multiple devices at the same, as each machine will individually contact AVG servers to download the other services.**
7. Ensure you have defined the correct Proxy Server, if any, in the policy you are applying to the device
8. Click **Download now** and specify where to save the installation package–such as on a flash drive or network drive

You can also send a download link from this page by clicking **Share download link** beneath the *Download now* button. You can then copy and send the private download URL to any desired recipients.

On-Premise Console Only

Sending Download Link via Email

Before you can send download links from the On-Premise Console, you will need to define your SMTP server.

1. Enter the email addresses for the target users in the *Send To* box, separated by commas
2. If desired, alter the *Subject* line of the email that will be sent
3. To configure the message you send in the email, check *Include your custom message* and type a message in the space provided
4. Select the subscription products
5. Click **Advanced Settings** to view the following options
6. Choose the Group and Policy the device will use
    - **If desired, you can activate your devices and select the subscriptions to use after installation by checking the box with that option.**
7. Choose whether to automatically remove conflicting antivirus products on the device
    - **The option to remove competitive antivirus products is checked by default. We recommend that you leave this option checked when installing the Antivirus service.**
8. Select the installer size (Light vs Full)
    - **If you select Light, the other services will be downloaded upon installation of the Antivirus agent. This option is not recommended if you are installing Antivirus on multiple devices at the same, as each machine will individually contact AVG servers to download the other services.**
9. Ensure you have defined the correct Proxy Server, if any, in the settings template you are applying to the device
10. Click **Send**

Installing on the Local Client

Once you have an installer file or download link from the AVG Business Management Console, you need to install AVG Business Antivirus to the end device(s).

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. Wait while AVG Business Antivirus is installed on the device
5. When prompted, restart the device
6. The device should now be visible in your Console

Adding Devices via Remote Deployment

Remote Deployment Requirements

- Administrator credentials to the computer or Windows domain. If using domain credentials, include the domain name: (e.g., YOUR_DOMAIN\username).
- Network information about the devices you are deploying to. You need this information to locate the devices on your network.
- Prepare computers for the client installation. Uninstall any other Antivirus software if installing Avast Business Antivirus.

Configure the following on each device:

Windows Vista/7/8.x/10

Enable WMI Traffic

- Execute NETSH command: netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes

Enable ADMIN Share

- Open Regedit
- Navigate to: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Create a new DWORD "LocalAccountTokenFilterPolicy" with Value of 1

Enable Printer and File Sharing

- In Control Panel ▸ Network and Internet ▸ Network and Sharing Center

- Click Change Advanced Sharing Settings, then enable File Printer Sharing

Firewall

1. Open Firewall settings
2. Go to Settings ▸ Profiles ▸ Directly connected to the Internet ▸ Applications ▸ Generic Host Process - and Generic Host Process 2
3. Allow:
    - DCOM server data
    - Microsoft DCOM Server
    - DCOM Client Data (should be allowed by default)
    - Microsoft DCOM Client (should be allowed by default)

Enable DCOM

1. Run dcomcnfg
2. Navigate to Component Services ▸ Computers
3. Right-click on My Computer ▸ Properties
4. Click the Default Properties tab
5. Click *Enable Distributed COM on this Computer* checkbox

Enable RPC

1. Run services.msc
2. Navigate to and enable "Remote Procedure Call (RPC)"

Remote Deployment Details

The Remote Deployment option is only available after you have added at least one device to your network using another install method. You must also designate a Master Agent thus, it is best if the first device you add to your network is the device you will use as the Master Agent. Below is a summary of the remote deployment process:

Device Detection

The device detection process uses Address Resolution Protocol (ARP) to ping all IP addresses within the subnet in order to get their MAC address. This process can take up to 15 minutes, possibly longer depending on the network.

If a response is received with a MAC address, a reverse DNS lookup occurs to get the host name for the IP. If a host name is received, a device record is created and stored in a list—which is transmitted to the web service when detection is complete.

Once the initial authentication is completed, the process will scan for host devices periodically and compare it to the list already stored. From this point on, the process will only add new host devices and will not delete any.

Authentication

During remote deployment, a list of administrator credentials—e.g., YOUR_DOMAIN\user_name and password—are passed to the remote deployment process until one successfully provides access to the target computer. If none of the credentials work, the process will quit and return an error message.

The client waits for changes made to the devices/login tables to see if anything is marked for deployment—based upon the host computer's MAC address.

Requirements

To automatically deploy Antivirus to multiple devices remotely, you must have:

- Cloud Console or On-Premise Console 6.0 or higher
- Antivirus 18.6 or higher
- At least one device installed and activated
- A working Master Agent
- File and Printer Sharing for Microsoft Networks enabled
- A Microsoft Windows operating system supported by Active Directory
- Valid Credentials for Active Directory with Administrator rights
- All necessary ports open (7074)

Deploying Installers Remotely

Network Scanning

1. Click **Begin Deployment Process**
    - If you do not have a Master Agent available, click **Add new Master Agent** and follow the process for setting a Master agent.
    - If you do have a Master Agent or Agents available, select the one you would like to use
2. In the Active Directory Credentials section, enter the following information:

- Domain
- Username
- Password

3. Click **Scan your network** and wait until the device detection process is complete

Network Deployment

1. In the *Active Directory Groups* section, navigate to a folder that contains unprotected devices and select the check boxes next to the devices you would like to deploy to
2. Click **Define installer settings**
3. In the *Select a license* section, choose one of your available Antivirus subscriptions
4. In the *Deploy to a group in AVG Business Console* section, do any of the following:
   - Select a group
   - Select **Copy Active Directory group structure into the selected group** in order to use your Active Directory's existing group structure
   - Select a policy
5. Choose whether to automatically remove conflicting antivirus programs on the device
6. Click **Start deployment to devices**
   - **Wait while Antivirus is deployed to devices. You can navigate to other pages during this process and use the Remote Deployment button on the navigation menu to return and view the progress of your Remote Deployment.**
7. Click **Finish Remote Deployment**

Policy Configuration and Components

The main way you manage your devices is through policies, which are groups of security rules for multiple operating systems (Windows Workstation, Windows Server, and MacOS X) that determine how AVG Business Antivirus works on the endpoints. Any changes to a policy are applied to the devices and groups assigned to it.

The AVG Business Management Consoles include a default template that has already been set up with the suggested configuration. You can apply this template, or create your own by duplicating the default to customize it or by creating a new template altogether. The default template cannot be deleted until another policy has been created.

A single policy contains settings for Windows Workstations and Windows Servers so you do not need to create separate policies for each operating system. This enables you to configure settings for a device group that contains multiple OS types at once. You can create policies by clicking **Add Policy** on the *Policies* page. You will then have a chance to name the policy before configuring your settings for the various components.

Antivirus Components by Product License

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

Enabling and Disabling Components

Nearly all the shields and tools available in AVG Business Antivirus can be enabled or disabled in the policy. 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.

1. In the policy you are configuring, select the *Active Protection* tab
2. Select the relevant OS tab (Windows Workstation, Windows Server)
3. Beside the components 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**

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 policy.

1. In the policy you are configuring, select the *Active Protection* tab
2. Select the relevant OS tab (Windows Workstation, Windows Server)
3. Beside the components you want to alter, do one of the following:
    - If the component is not yet installed, click **Install this component**. Then click **I understand, install component**
    - If the component is already installed, click the **More** button beside the component, then click **Uninstall this component**. Then click **I understand, uninstall component**

For more details on configuring the various components available in the Policies of the AVG Business Management Consoles, see Configuring Settings and Policies in the AVG Business Management Consoles.

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:** `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 AVG Business Antivirus in the *Antivirus Settings* tab of your policies.

Any changes made to exclusions within policies will propagate across your network every 5-10 minutes. Console policies override local settings.

1. Navigate to the *Antivirus Settings* tab for the desired OS
2. In the *Exclusions* section, do one of the following:
   - Click **File paths**, enter a file path you would like to exclude, then click **Add**
   - Click **URL addresses**, enter a URL you would like to exclude, then click **Add**
3. Click **Apply changes** when you are finished

If you have multiple OS types using the same policy, be sure to add the exclusions to this section under the Windows Workstation and/or Windows Server tabs.

Configuring Automatic Updates

You can set your devices to automatically update the AVG Business Antivirus program and virus definitions.

Configuring Updates

Updates are sent either directly via AVG servers or any configured Master Agents/Local Update Servers on your network. If you have selected manual updates, you will need to

manually update via the *Devices* page to ensure all devices on your network remain up to date with the latest protection.

Creating and Configuring Scans

You can configure the types of files and programs that are scanned by AVG Business Antivirus when you set up the scan task, assuming you selected an Advanced Scan type (Custom, Boot-time). Therefore, the main details for what will be scanned are not configured in policies, though exclusions are.

Types of Scans

- **Quick Scan—**Scan for common threats
- **Full System Scan—**Run a detailed scan of every file on the device
- **Removable Media Scan—**Scan USBs and portable media connected to the device
- **Custom Scan—**Run a scan where you choose the file types, sensitivity of the scan, performance, actions, and whether compressed files are included.
- **Boot-time Scan (MS Windows only)—**Run a scan when the device boots up.

Cloud Console

Creating Scheduled Scans

You can only create scheduled Quick or Full System Scans.

1. Navigate to the *Policies* page
2. Click the policy you would like to add scheduled scans to
3. Click the **Service Settings** tab
4. Expand the **Antivirus Scans** section
5. Configure the following for both **Quick Scan** and **Full System Scan**:
    - **Frequency:** choose between Daily, Weekly, and Monthly
    - **Day of the week/month:** choose which day you would like the scan to run
    - **Start time:** select which time of day you would like the scan to run
6. When you are finished, click **Apply**

Creating One-Time Scans

1. Navigate to the *Devices* page, then do one of the following:
    - For a single device, click the **More** button to the right of the device name
    - For multiple devices, check the boxes of all devices you would like included, then click **Actions**
2. Hover over **Antivirus Scans**
3. Click the type of task you would like to create:
    - Quick Antivirus Scan
    - Full System Antivirus Scan
    - Advanced Antivirus Scans
4. Fill in the details and settings for the task, then click **Create**

On-Premise Console

1. Click **Scan device**.
2. Select a type of scan:
    - **Quick Scan—**Scans for common threats
    - **Full System Scan—**Runs a detailed scan of every file on the device
    - **Removable Media Scan—**Scans USBs and portable media connected to the device
    - **Custom Scan—**Runs a scan where you choose the file types, sensitivity of the scan, performance, actions, and whether compressed files are included.
    - **Boot-time Scan (MS Windows only)—**Runs a scan when the device boots up.
    - **If you chose Custom or Boot-time Scan, select the additional configuration options for your scan.**
3. If you would like the task to be recurring, select *Schedule the scan* and set the Frequency (one-time, daily, weekly, or monthly) and Schedule start date and time.
4. Type a Custom name for the scan.
5. Click **Start Scan**.

Any threats that are detected during this scan are usually sent to the device's Virus Chest. You can view and manage these detections in Device Details.

Scan Configuration

Configuring Boot-Time Scans

Boot-time scans are only available for Microsoft Windows devices, and will scan your device when it is just beginning to "boot up".

Windows locations to scan: you can select preset locations to scan from the drop-down menu, which are then added to the list. If desired, you can also type the path to a specific location to be included in the scan. Any locations you do not want included in the scan can be removed from the list by clicking the delete button.

Restart the device now: immediately restart the device in order to perform a boot-time scan. If you do not check this, the boot-time scan will run the next time the device restarts.

Notify users with a message before the restart: enter a message to be displayed to the end user notifying them the device will restart shortly

Specify when the above message will be displayed: select when the message will be displayed, between 1 minute, 10 minutes, 30 minutes, or 1 hour before restart.

Heuristics: heuristics enable Antivirus to detect unknown malware by analyzing code for commands that may indicate malicious intent. The default setting is Normal. With higher sensitivity, Antivirus is more likely to detect malware, but also more likely to make false-positive detections that incorrectly identify files as malware.

PUP and suspicious files: choose whether or not to scan for Potentially Unwanted Programs (PUPs)

Unpack archive files: choose whether or not to unpack archive file types during scanning, which is slower but more extensive

When a threat is found: choose what action AVG takes when a threat is detected, between Clean automatically, move to chest, repair, delete, or no action.

Cancel the scan on the workstation: choose whether or not the scan can be canceled on the workstation while it is running

Configuring Custom Scans

Custom scans provide the most control over what specific types of files, folders, programs, and processes are included in the AVG Business Antivirus scan. You can select different scan options for Windows Workstations, Windows Servers, and MacOS X Devices within the same scan task.

Configuring Locations

You can select preset locations to scan from the drop-down menu, which are then added to the list. If desired, you can also type the path to a specific location to be included in the scan. Any locations you do not want included in the scan can be removed from the list by clicking the delete button.

File Types Tab

You can choose whether or not to scan all files (or just the most common areas for threats). Additionally, you can configure the scan to recognize file types by their content, which requires scanning the entire file, or by their name extension which will only scan the files with the extensions you enter in the text box that appears when that option is selected.

Sensitivity Tab

Heuristics Sensitivity: Heuristics enable Antivirus to detect unknown malware by analyzing code for commands that may indicate malicious intent. The default setting is Normal. With higher sensitivity, Antivirus is more likely to detect malware, but also more likely to make false-positive detections that incorrectly identify files as malware. Code emulations unpack and test suspected malware in an emulated environment where the file cannot cause damage to devices. *Use code emulation* is enabled by default.

Sensitivity: choose to test whole files, which will cause the scan to be slower but more extensive.

PUP and suspicious files: choose whether or not to scan for Potentially Unwanted Programs (PUPs)

Links: choose whether any links within files are followed during the scan, which will cause the scan to be slower but more extensive.

Performance Tab

Priority: choose the priority of the scan on the end device(s). A higher priority will lead to a quicker scan, but will use more resources.

Persistent cache: choose whether to speed up the scan by using the persistent cache, and/or to store data about scanned files in the persistent cache which will slow down the scan.

File access: choose whether to speed up the scan by reading files in the order they are stored on the disk, which is only effective on NTFS volumes.

Actions Tab

Apply an action: choose whether or not actions are automatically taken during the scan when a virus, potentially unwanted program (PUP), or suspicious file is detected. The options are Clean Automatically, Move to chest, Repair, Delete, and No Action.

If, for whatever reason, AVG cannot complete the main action, it will attempt the action selected under *If the action fails, use*

Options: choose whether to perform the selected action upon restart.

Processing of infected archives: choose whether to only remove the packed file from the archive (and if that fails, do nothing), remove the packed file from the archive (and if that fails, remove the entire archive), or to remove the entire archive.

Packers Tab

Choose whether or not to extract all archive files for scanning.

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