

The AVG Business logo, consisting of a colorful graphic of overlapping shapes in orange, blue, green, and red, followed by the text 'AVG Business' in a bold, black, sans-serif font, and 'by avast' in a smaller, orange, lowercase, sans-serif font below it.

AVG Business
by avast

Remote Administration Use Cases

Performing Tasks in the New AVG Consoles

Author: **Kira John**

Brand: **AVG**

Date of update: **May 13, 2020**

Status: **Internal**

Table of Contents

Console Migration Introduction	3
Console Use Cases	3
Remote Deployment	3
Configuring Settings for Groups and Devices	5
Configuring Firewall Settings	6
Handling Threats	7
Server Settings	8
Device States	9
Installation Scripts	10
VPS Updates	11
Update Proxies vs Local Update Servers	13
Installing in Offline/Isolated Networks	13

Console Migration Introduction

With the migration of the AVG Remote Administration Console to the new AVG Business On-Premise and Cloud Console(s,) the Business Technical Support team would like to ensure our partners and customers know how to perform their usual tasks in the new Console. The other benefit of this migration is that the AVG Business Protection and Consoles will no longer be in maintenance mode, but will be actively improved upon with regular feature releases.

This document is meant to cover the most common uses as determined by our Technical Support team. You can read about other tasks and options in the Consoles by accessing our [Knowledge Base](#).

Console Use Cases

Remote Deployment

Remote Deployment allows customers to install AVG Business Protection (Antivirus, Internet Security Business, File Server Edition, Email Server Edition) on computers within their domain/network straight from the Console.

In Remote Administration Console

You can remotely install from the Remote Administration Console using the **Install AVG on stations** wizard in the Tools menu. This would use the Console device to scan your devices by Active Directory, IP range, or domain, and install AVG on whatever stations did not have it already.

In AVG Business Console(s)

You must designate a Master Agent to scan your Active Directory and deploy AVG Business Protection to your network. In order to designate a Master Agent you must install the AVG client on a device in your network through another method, such as the installer file. We recommend you use a server device for a Master Agent.

1. Click **General Settings** in the bottom-left corner
2. Click the *Master Agents* tab and review the displayed information
3. Click **Add new Master Agent**
4. Select a device to promote as Master Agent
5. Click **Select**
6. Wait until the Master Agent's status changes from *Pending* to *Active*.

Once you have a Master Agent, you may begin the Remote Deployment process.

1. In the Dashboard, click **Download installer**
2. Click **Deploy installers remotely** and review the Deploy remotely in four steps section
3. Click **Begin deployment process**
4. Insert your full domain (such as int.domain.com or domain.local) displayed in Control Panel → System, and domain administrator credentials
5. Click **Scan your network**

The device detection process also uses Address Resolution Protocol (ARP) to ping all IP addresses. This process can take up to 15 minutes, possibly longer depending on the network. If a response is received, a reverse DNS lookup occurs.

After a successful scan, you will see the folder structure of your Active Directory displayed in Remote Deployment Step 2/4, including devices that may no longer exist in your network.

1. Select the devices in the list that you wish to deploy Antivirus to
2. Click **Define installer settings**
 - Select your subscription, group, settings template, and check the *Remove other conflicting antivirus products during deployment* (Recommended) box
 - If you would like to copy your Active Directory's group structure, check the *Copy Active Directory group structure* into the selected group box
3. Click **Start deployment to devices**
4. After the deployment completes, click the **Finish Remote Deployment** button

Please allow several minutes to several hours to deploy (depending upon network bandwidth, device quantity, etc). Once the status changes to Deploying in the Management Console, you should see an AVG setup installer and other AVG services start in Task Manager on the devices.

All deployed devices will be asked to reboot, which the end user can either confirm or postpone. All deployed devices will be activated automatically.

Download installer


Download the installer


Deploy installers remotely

Deploy remotely in four steps

- 1 **Designate a master agent, and scan your Active Directory**
The Master Agent will perform the deployment to save you bandwidth. You'll need to login to your Active Directory and start a scan.
- 2 **Select which devices to deploy to**
Choose from the available devices in your Active Directory.
- 3 **Define installer settings**
Choose a group, license, schedule and define whether to remove a competitor's antivirus.
- 4 **View deployment progress**
See the deployment status on each device. Wait until all the devices complete their deployment, and then you're done.

[Begin deployment process](#)

The  **Remote Deployment** shortcut will be available in the left menu while the deployment is in progress.

Configuring Settings for Groups and Devices

Customers can configure the settings for AVG Business Protection to be personalized for their network and needs, including the ability to enable or disable specific components.

In Remote Administration Console

Devices are grouped in this Console and settings are configured directly for each group, meaning creating multiple groups with the same settings requires manual work. These can be configured in the **Shared settings for stations** section, which will allow you to choose components, schedule tasks such as scans, exceptions, and update proxies. Additionally, settings for stations (devices) and servers are separated, and Firewall settings for stations are not included in the base settings.

In AVG Business Console(s)

Devices generally use the settings template or policy applied to the group they are in, though you can change the settings template or policy of specific devices if you so choose. For example, you may want a settings template or policy for a group of server devices, and if one server in the group needs specialized settings you can change the template for that one device within the group.

You can configure settings for Windows workstations, Windows servers, and Mac OS X devices within the same settings template or policy.

1. Click **Device settings**
2. Click the name of the template you wish to configure
3. Make your changes, bearing in mind that each Antivirus component has further configuration options if you click **Customize** in the *Active Protection* tab
4. When you are done, click **Apply changes**

Policy

Policy name*

 Windows Workstation
 Windows Server
 Patch Management

Select your preferred configuration for the following areas to control how the AVG software interacts with your network and devices.

Active protection	General settings	Antivirus settings	Troubleshooting
Antivirus protection			
 File Shield ?		Customize	<input checked="" type="checkbox"/> ON <small>OFF</small>
 Behavior Shield ?		Customize	<input checked="" type="checkbox"/> ON <small>OFF</small>
 Mail Shield ?		Customize	<input checked="" type="checkbox"/> ON <small>OFF</small>
 Web Shield ?		Customize	<input checked="" type="checkbox"/> ON <small>OFF</small>
 Firewall ?		Customize	<input checked="" type="checkbox"/> ON <small>OFF</small>
Data protection			

Configuring Firewall Settings

The Firewall is one of the most important components of AVG Business Protection as it manages web traffic, blocking potentially dangerous connections to and from your devices. Configuration is sometimes necessary to prevent necessary traffic from being blocked.

In Remote Administration Console

The Remote Administration Console has very few configuration options for the **Firewall in the Shared Firewall settings for stations** menu. You can only configure system and application rules.

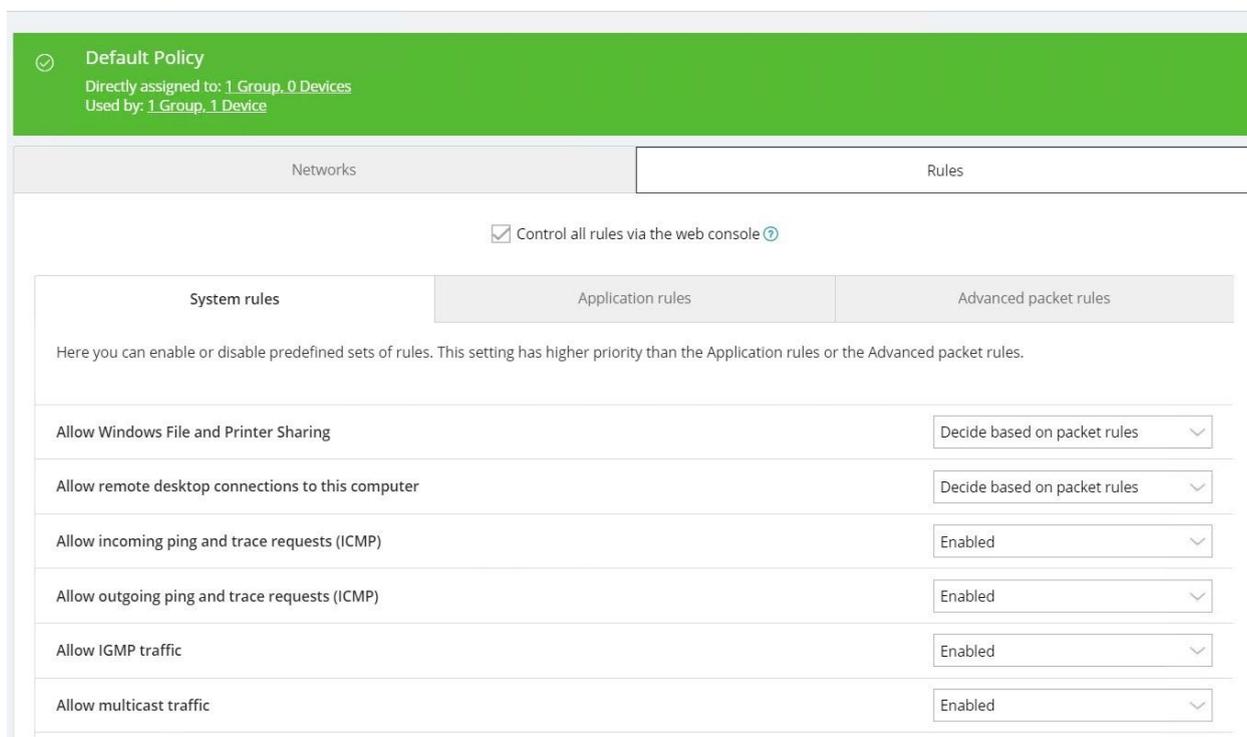
In AVG Business Console(s)

The AVG Business Firewall is an Active Protection component that can be configured with manual rules for the system, applications, and packets.

1. Click **Device settings**
2. Click the name of the template you wish to configure
3. On the *Active Protection* tab, click **Customize** beside the Firewall component
4. On the *Networks* tab, you can select the default profile (public or private) for undefined networks, create a list of defined networks and their profiles, and enable or disable additional advanced settings
5. On the *Rules* tab, you can create and configure System, Application, and Advanced Packet rules

- a. **System:** the highest tier of rules, configuration for various types of web traffic
 - b. **Application:** the middle tier of rules, configuration for specific applications on your devices and what types of connections are allowed
 - c. **Advanced Packet:** the lowest tier of rules, configuration for specific packets based on protocol, port, ICMP type, etc
6. When you are done, click **Apply changes**

Policy > Windows Workstation > Firewall



System rules	Application rules	Advanced packet rules
Here you can enable or disable predefined sets of rules. This setting has higher priority than the Application rules or the Advanced packet rules.		
Allow Windows File and Printer Sharing		Decide based on packet rules
Allow remote desktop connections to this computer		Decide based on packet rules
Allow incoming ping and trace requests (ICMP)		Enabled
Allow outgoing ping and trace requests (ICMP)		Enabled
Allow IGMP traffic		Enabled
Allow multicast traffic		Enabled

Handling Threats

When threats are detected by AVG Business Protection, they must be handled quickly to ensure devices are kept safe and secure.

In Remote Administration Console

Threat notifications in this Console are listed in the Notifications and Scan results pages. Customers can push a threat removal command from the Console itself if the Antivirus has not been configured to deal with certain threats automatically.

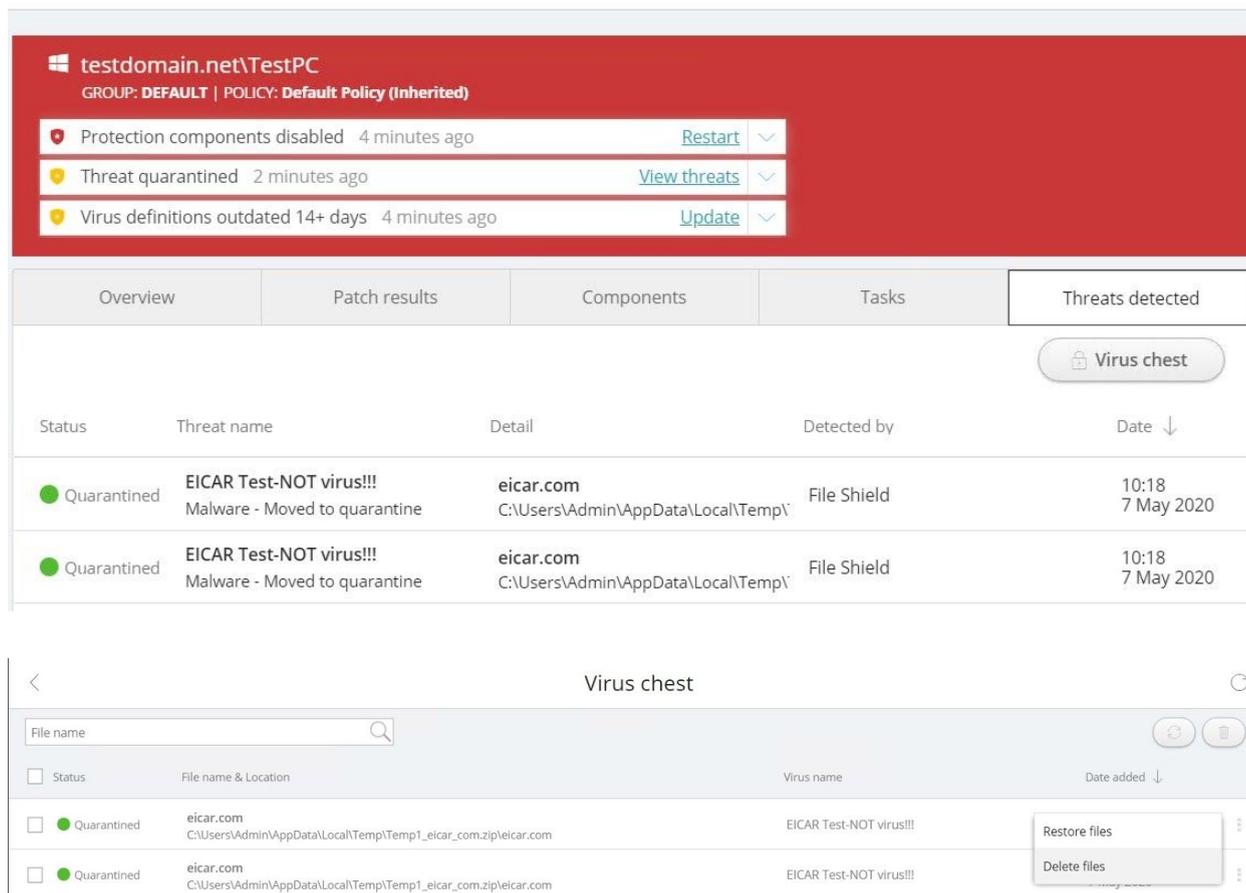
In AVG Business Console(s)

Threat notifications in the AVG Business Consoles are provided on the Dashboard, Notifications, and Devices pages. Threats are listed under 3 categories:

- Viruses
- Potentially Unwanted Programs (PUPs)
- Suspicious Files

You can configure what actions AVG Business Protection takes automatically when these threats are detected in the settings templates. If a threat has been located and moved to the Virus Chest on the device, you can view the Chest from your Console and either delete or restore the file.

Device



The screenshot shows the AVG Business Protection console for a device named 'testdomain.net\TestPC'. The device is in a 'Protection components disabled' state. A 'Virus chest' is visible, containing two quarantined threats: 'EICAR Test-NOT virus!!!' (Malware - Moved to quarantine) detected by File Shield on 10:18 7 May 2020. The console also shows tabs for Overview, Patch results, Components, Tasks, and Threats detected.

Status	Threat name	Detail	Detected by	Date ↓
Quarantined	EICAR Test-NOT virus!!! Malware - Moved to quarantine	eicar.com C:\Users\Admin\AppData\Local\Temp\	File Shield	10:18 7 May 2020
Quarantined	EICAR Test-NOT virus!!! Malware - Moved to quarantine	eicar.com C:\Users\Admin\AppData\Local\Temp\	File Shield	10:18 7 May 2020

The Virus chest view shows a search bar and a table with columns for Status, File name & Location, Virus name, and Date added. A context menu is open over the first entry, showing 'Restore files' and 'Delete files' options.

Server Settings

Servers often require specialized settings, especially for Antivirus programs, to ensure web traffic is protected but not interfered with unnecessarily.

In Remote Administration Console

Settings for servers must be configured in the **Shared settings for application servers** section, which will allow you to choose components, schedule tasks such as scans, exceptions, and update proxies.

In AVG Business Console(s)

Settings for servers can be configured in the same settings templates or policy as settings for workstations. You may still wish to have a separate settings template or policy for your server devices.

1. Click **Device settings**
2. Click the name of the template you wish to configure
3. Click the Windows Server tab

4. Make your changes, bearing in mind that each Antivirus component has further configuration options if you click **Customize** in the *Active Protection* tab
5. When you are done, click **Apply changes**

Policy

Policy name*

 Windows Workstation
 Windows Server
 Patch Management

Select your preferred configuration for the following areas to control how the AVG software interacts with your network and devices.

Active protection	General settings	Antivirus settings	Troubleshooting
<i>Antivirus protection</i>			
 File Shield ?			Customize ON ⋮
 Mail Shield ?			Install this component
 Web Shield ?			Install this component
<i>Data protection</i>			
 Data Shredder ?			Customize ⋮
 Exchange ?			Install this component

Device States

Devices have different levels of safety — called states — based on the various detected threats across your network.

In Remote Administration Console

The levels of safety for stations are listed as non-compliance states. This can be caused by unhealed high severity detections, unhealed medium severity detections, rootkits not removed, excess time since the last scan or synchronization, a restart needed, and/or need updates to the virus definitions/program versions.

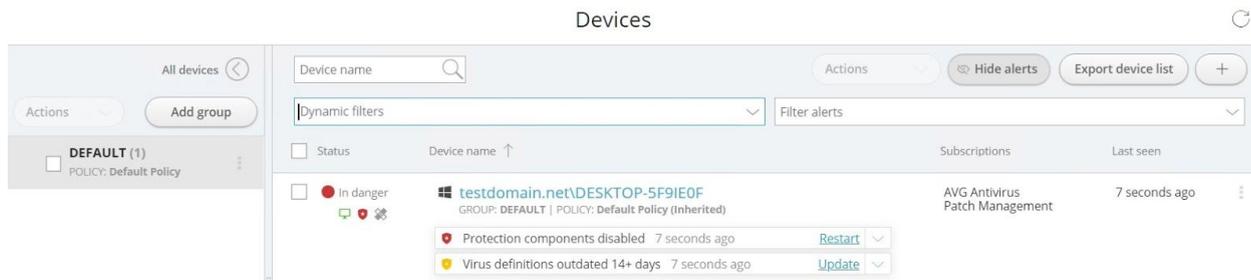
In AVG Business Console(s)

Devices fall under one of three states, visible in the *Dashboard* and on the *Devices* page.

- **Safe:** your device has no active alerts and the Antivirus program and virus definitions are up to date
- **Vulnerable:** your device has some minor active alerts, such as missing patches

- **In Danger:** your device has one or more major active alerts, such as virus definitions out of date

The *Notifications* page will list alerts as they come up, along with actions required to resolve them. You can also see them on the *Devices* page, and they fall under two types: Security and Network.



The screenshot shows the 'Devices' page in the Avast console. At the top, there's a search bar for 'Device name' and buttons for 'Actions', 'Hide alerts', and 'Export device list'. Below this is a table of devices. The first device is 'testdomain.net\DESKTOP-5F91E0F' with a status of 'In danger'. It has two alerts: 'Protection components disabled' (7 seconds ago) with a 'Restart' button, and 'Virus definitions outdated 14+ days' (7 seconds ago) with an 'Update' button. The device is subscribed to 'AVG Antivirus Patch Management' and was last seen '7 seconds ago'.

Installation Scripts

Installation scripts can help users install AVG Business Protection on many devices with minimal effort, particularly if Remote Deployment is not an option.

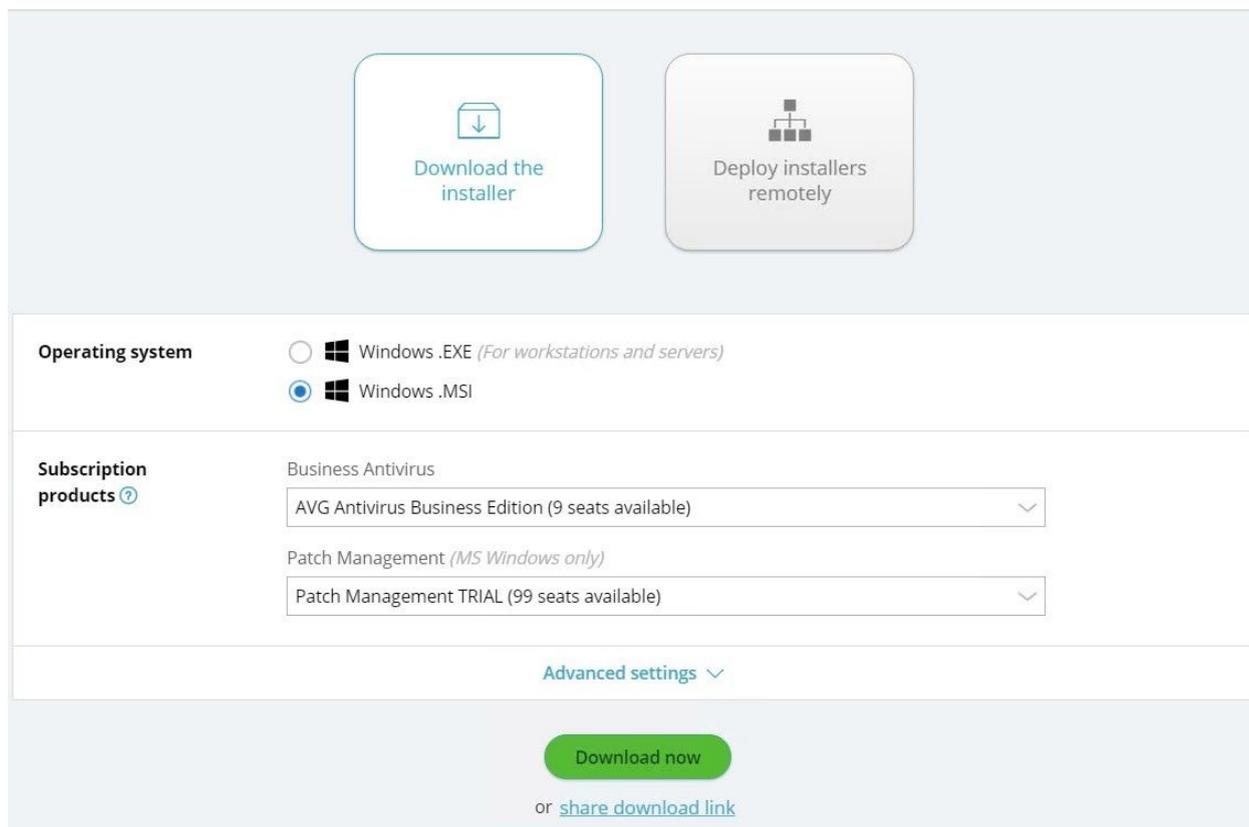
In Remote Administration Console

You can create custom installation scripts using the AVG Network Installer Wizard to then deploy to multiple devices across your network without using the remote deployment option.

In AVG Business Console(s)

While the AVG Business Console does not support the creation of installation scripts, you can create a .msi installer file for deployment through GPO.

Download installer



The screenshot shows the Avast download installer interface. At the top, there are two buttons: "Download the installer" (highlighted in light blue) and "Deploy installers remotely" (greyed out). Below these are two sections for configuration. The "Operating system" section has two radio buttons: "Windows .EXE (For workstations and servers)" and "Windows .MSI" (selected). The "Subscription products" section has two dropdown menus: "Business Antivirus" (selected) and "AVG Antivirus Business Edition (9 seats available)", and "Patch Management (MS Windows only)" (selected) and "Patch Management TRIAL (99 seats available)". Below these is an "Advanced settings" link with a dropdown arrow. At the bottom, there is a green "Download now" button and a link "or [share download link](#)".

VPS Updates

Virus databases must be updated regularly to ensure AVG Business Protection can detect newer threats. These updates are generally done automatically by the Antivirus program.

In Remote Administration Console

The Remote Administration Console receives notifications when virus definition updates are released, so you can ensure your devices are up to date.

In AVG Business Console(s)

As configured in the default policy, VPS updates occur automatically when devices are connected to the internet, and you will receive notifications if devices' virus definitions are out of date. You can also set the updates to manual so you have control over when to update your devices, at which point you will need to use the Tasks tab to send update commands.

Policy

Windows Workstation		Windows Server	Patch Management
Select your preferred configuration for the following areas to control how the AVG software interacts with your network and devices.			
Active protection	General settings	Antivirus settings	Troubleshooting
Password protection ?	<input type="checkbox"/> Enable		
Silent Mode ?	<input type="checkbox"/> Use Silent Mode		
Reputation services ?	<input checked="" type="checkbox"/> Enable Reputation services		
When to update	Virus definitions updates ? <input checked="" type="radio"/> Automatically when new update is available. <i>(Strongly recommended for an up-to date protection)</i> <input type="radio"/> Manually ?		
	Program updates ? <input checked="" type="radio"/> Automatically when new update is available. <i>(Strongly recommended for an up-to date protection)</i> <input type="radio"/> Manually ?		

Create new task

You are creating a task for all your devices
 How to select specific devices? ?

 Scan device	 Send a message to the device	 Update device	 Shutdown device
Update device	<input checked="" type="radio"/> Program update ? <input type="radio"/> Virus definitions update ?		
Create update schedule ?	<input type="checkbox"/> Schedule the update		
Custom name ?	<input type="text" value="Program update 6 May 2020 10:58"/>		

Update

Update Proxies vs Local Update Servers

Update proxies are URLs used to update devices that may be different from the standard URL. The AVG Business Consoles do not use update proxies, but rather devices on the network host and push out updates to other managed devices.

In Remote Administration Console

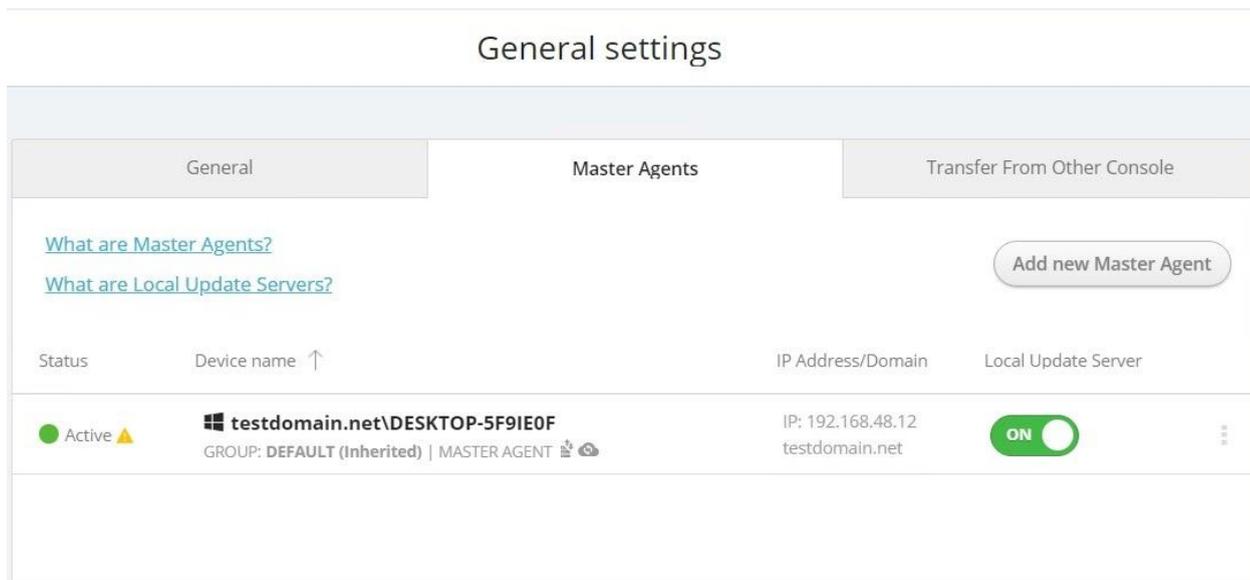
You can set a custom update URL proxy during the installation of end devices, or in the **Shared settings for stations** section.

In AVG Business Console(s)

The AVG Business Console uses devices marked as Master Agents / Local Update Servers to push updates through your network. These devices should have a fixed IP address, be online at all times, and ideally be server devices.

1. Click **General Settings** in the bottom-left corner
2. Click the *Master Agents* tab and review the displayed information
3. Click **Add new Master Agent**
4. Select a device to promote as Master Agent
5. Click **Select**
6. Wait until the Master Agent's status changes from *Pending* to *Active*
7. On the *Master Agents* tab, ensure the slider under Local Update Server is **On**

General settings



General settings			
General	Master Agents	Transfer From Other Console	
What are Master Agents? What are Local Update Servers?	<input type="button" value="Add new Master Agent"/>		
Status	Device name ↑	IP Address/Domain	Local Update Server
Active	testdomain.net\DESKTOP-5F91E0F <small>GROUP: DEFAULT (Inherited) MASTER AGENT </small>	IP: 192.168.48.12 testdomain.net	<input checked="" type="checkbox"/> ON

Installing in Offline/Isolated Networks

Certain networks have limited or no internet access and therefore require an Antivirus solution that does not require access to the internet.

In Remote Administration Console

With the option for update proxies, the Remote Administration Console can be installed and used in an offline or isolated environment with minimal configuration.

In AVG Business Console(s)

The AVG Business Management (On-Premise) Console can be installed in an offline or isolated environment, but requires some specialized configuration during the installation of the Console itself. For details on the configuration, see the Knowledge Base article [Offline Networks in Avast and AVG Business On-Premise Console](#).

