Avast Business
On-Premise Console

Table of Contents

AVAST BUSINESS ON PREMISE MANAGEMENT CONSOLE

With Avast Business On Premise Management Console, adding critical protection to every PC, Mac, and server has never been easier. Flexible management provides the most convenient way to protect businesses.

Avast Business Management Console provides:

- Complete control over the behavior of antivirus on endpoint devices
- Centralized management of multiple devices - accessible anywhere
- Complete overview of current status of entire environment with immediate alerts
- Automatic and seamless updates

Avast Business Management Console integrates seamlessly with Avast Business Antivirus to:

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

When you install Avast Business Antivirus on devices through Avast Business Management Console, you can control Avast 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

Avast Business On Premise Management Console can be installed on Windows, Linux, and Mac devices.

Setting up Avast Business On Premise Management Console involves three steps:

- Installing the console
- Creating an account
- Uploading your license

From there, you can add devices to protect and manage them.

Requirements

Console (Windows version)

Minimum	Recommended
Operating System	
▪ Windows 10 ▪ Windows 8.x (Desktop) ▪ Windows 7 SP1 ▪ Windows Server 2008 R2 SP1 (64-bit) ▪ Windows Server 2012 and 2012 R2 (64-bit) ▪ Windows Server 2016 any Edition with latest Service Pack	▪ Windows 10 (64-bit) ▪ Windows 8.x Desktop (64-bit) ▪ Windows 7 SP1 (64-bit) ▪ Windows Server 2008 R2 SP1 (64-bit) ▪ Windows Server 2012 and 2012 R2 (64-bit) ▪ Windows Server 2016 any Edition with latest Service Pack (64-bit)
RAM	
2 GB	4 GB
Disk Space	
6 GB	6 GB
Processor	
2 GHz	2 GHz

Console (Docker version)

Minimum	Recommended
Operating System	
Any Linux, macOS, or Windows Operating System that can run Docker	Any 64 bit Linux, macOS, or Windows Operating System that can run Docker
Docker	
▪ Docker Engine 1.10.0 or higher ▪ Docker Compose 1.6.0 or higher	▪ Docker Engine, the most recent release ▪ Docker Compose, the most recent release

RAM	
2 GB	4 GB

CLIENT

WINDOWS	MACINTOSH
OS	**OS**
▪ Windows Server 2016 any Edition with latest Service Pack, excl. Server Core ▪ Windows Server 2012 R2 any Edition with latest Service Pack, excl. Server Core ▪ Windows Server 2008 R2 any Edition with latest Service Pack, excl. Server Core ▪ Windows 10 except Mobile and IoT Core Edition (32 or 64-bit) ▪ Windows 8.1 except RT and Starter Edition (32 or 64-bit) ▪ Windows 8 except RT and Starter Edition (32 or 64-bit) ▪ Windows 7 SP1 or higher, any Edition (32 or 64-bit) ▪ Windows Vista SP2 or higher, except Starter Edition (32 or 64-bit) ▪ Windows XP SP3, any Edition	▪ Snow Leopard (macOS 10.6.8) or newer
HARDWARE	**HARDWARE**
Windows fully compatible PC with Intel Pentium 4 or AMD Athlon 64 processor or above (must support SSE2 instructions)	Any Intel-based Mac with 250 MB free system disk space
RAM	
256 MB RAM or above	2 GB
RECOMMENDED	
Standard screen resolution 800 x 600 or higher	

SUPPORTED VIRTUALIZATION TOOLS

Avast Business On-Premise Console has been tested with the following virtualization tools:

- Oracle VirtualBox 5.1.18
- VMware Workstation for Windows
- Microsoft Hyper-V

DEFAULT PORTS

The default port is 8443. If no other application uses this port, you can accept the default during installation.

The default database server port is 5432.

Communication between Avast Business Management Console and Avast Business Antivirus uses the following ports:

- 8080
- 8090

SMTP SERVER

You can configure an SMTP server, which is used to send a wide variety of notifications, including when alerts are triggered, such as infected devices or out of date virus definitions. SMTP server is optional, but Avast highly recommends setting up an SMTP server.

SSL CERTIFICATE

Communication between the Avast Business Management Console and Avast update servers takes place over a secure SSL connection. Because of this, you need to set up an SSL certificate. If you have your own SSL certificate, you can use it. If not, the installation process generates a self-signed certificate. We recommend using your own SSL certificate.

POSTGRESQL

The database engine uses PostgreSQL. You don’t need to use a different database type for different connected workstations.

Installation creates a new PostgreSQL user account called “AvastMCpostgreSQL”

HTTPS CERTIFICATE

The Avast Business Management Console is accessed through a web browser. Communication between the management console and the Avast update servers takes place through a secure SSL connection. For this reason, a certificate is required, if a certificate is not available then it is possible to generate a self-signed certificate.

INSTALLATION LOGS

You can find the installation logs for the console and for PostgreSQL in the temp folder C:\users\<username>\AppData\local\temp. The installation generates the following logs:

- bitrock_installer.log
- Install-postgresql.log
- Setup Log <date lognumber>.txt

NOTE Bitrock_installer.log is related to the PostgreSQL installer itself. You only need this log if the installer is failing to launch or unpack. Most installation issues appear in the Setup Log.

Windows Installation

You can install Avast Business On Premise Management Console for Windows using the installer, which you can download here.

To install Avast Business On Premise Management Console for Windows

1 Download the installer here.
2 Run the installer.
3 Follow the instructions in the Wizard.

Linux and OS X Installation

You can install Avast Business On Premise Management Console on Linux and Mac devices using Docker. You will need to install Docker and then download and install the configuration files, which consist of a .YML file and a .ENV file.

To install Avast Business On Premise Management Console for Linux and Mac

1 Download and install Docker from https://www.docker.com/products/overview#/install_the_platform.
2 Once you have installed Docker, download and install the Avast Business On Premise Management Console configuration files https://artifactory.srv.int.avast.com/artifactory/webapp/#/artifacts/browse/tree/General/docker-local/avast/business-console/on-premise/.
3 Edit the .ENV file, changing the Host Name to match the name of the device that will run the Avast Business Management Console. Save the .ENV file.
4 In Docker, run the `docker-compose up` command from the terminal.

NOTE Once Avast Business services are running, you can run Avast Business On Premise Management Console.

To run Avast Business On Premise Management Console for Linux or Mac

1. Start a web browser.
2. Navigate to https://<hostname>:<port number> where <hostname> is the name of the host device and <port number> is the port number.

Creating an Account

The first time you run Avast Business On Premise Management Console, you will be prompted to create a new account and company. Each following time you run the console, you must log in.

Uploading your License

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

To upload your license

1. Once you have created your account, run the console and log in.

2. Click **Dashboard** 🏠.
3. Click **Upload license file**.
4. Type your license code.
5. Click **Activate license code**.

DASHBOARD

The Avast Business Dashboard provides you a complete overview of the health and status of your network. The Dashboard consists of three sections:

- Shortcuts—This section provides shortcuts to the things you need to do to get started with Avast Business, such as downloading antivirus software, activating devices, starting a scan, and uploading licenses.
- Network Security – Operating System—This section shows you how many devices you have on each platform.
- Threat Detection Statistics—This section displays a graph of recent threats detected.

SHORTCUTS

In the Shortcuts section, you add devices to Avast Business On Premise Management Console, scan your devices, activate devices, and upload license files.

ADDING DEVICES

To add devices so they can be managed by Avast Business On Premise Management Console, you create an installer from the console, which downloads Avast Business Antivirus to the devices and also allows the console to manage it. Once a device has Avast Business Antivirus installed, you can control all the features of Avast Business Antivirus remotely, from your Avast Business On Premise Management Console, such as:

- One-time or regularly scheduled tasks
- Setting up notifications of attacks on your network
- Restarting devices with or without user input
- Performing software upgrades at times that won't affect the user's workday

TO ADD A DEVICE REMOTELY

1. Do one of the following:

   - Download the installer, then send the installer to the device owner.
   - Send a link to the installer to the device owner.

2. Have the device owner run the installer on the device.
3. Follow the To activate a device procedure.

TO ADD A LOCAL DEVICE

1. Follow the To download the installer procedure.
2. Follow the To run the installer procedure.
3. Follow the To activate a device procedure.

TO DOWNLOAD THE INSTALLER

1. Click **Dashboard** 🏠.
2. In the **Shortcuts** section, click **Download antivirus**.

NOTE You can also download an installer from **Devices** 🖥.

3 Click the check box of the type of antivirus you want to download:

- Windows .EXE
- Windows .MSI
- Mac OS X .DMG

4 Click **Advanced settings**.
5 Do one of the following:

- To download an installer that doesn’t require the user to choose any options, click **Download the non-interactive installer**.
- To download an installer that lets users customize their options, click **Download the interactive installer** or go to the **Devices** section and click **Download antivirus**.

6 If your company uses a proxy server, select an option in the **Proxy** box.

TO RUN THE INSTALLER

1 If required, email the device owner a link to the downloaded .exe.
2 Do one of the following:

- Run the .exe on the device.
- Request that the device owner run the .exe on the device.

3 Follow the steps of the installation wizard.

ACTIVATING DEVICES

Before you can control Avast Business Antivirus on your devices, you must activate them.

By activating, you acknowledge the device belongs to your company, and you assign one of the seats of your license to that device.

Once you have activated the device, you have complete control Avast Business Antivirus on it.

TO ACTIVATE A DEVICE

1 Click **Dashboard** 🏠.
2 In the **Shortcuts** section, click **Activate now**.

NOTE You can also activate a device from **Devices** 🖥.

Once the device is activated, you can manage it using the Avast Business On Premise Management Console.

NETWORK SECURITY – OPERATING SYSTEM

The Network Security section on the Dashboard page displays the number of devices you have, by operating system.

TO REFRESH THE NETWORK SECURITY – OPERATING SYSTEM SECTION

1. Click **Dashboard** 🏠.
2. In the **Network Security – Operating System** section, click the **Refresh** button.

THREAT DETECTION STATISTICS

This section displays a graph that shows the number of threats detected. You can choose to display threats detected in the last:

- Week
- Two weeks
- Month

TO CHANGE THE TIME PERIOD OF THE THREAT DETECTION GRAPH

1. Click **Dashboard** 🏠.
2. In the **Threat Detection Statistics** section, click one of the following buttons:

- **Week**
- **2 Weeks**
- **Month**

TO REFRESH THE THREAT DETECTION STATISTICS SECTION

1. Click **Dashboard** 🏠.
2. In the **Threat Detection Statistics** section, click the **Refresh** button.

NOTIFICATIONS

Notifications are messages that keep you informed about the status of your network, providing a communication channel for important messages.

Notifications appear on the Notifications page in Avast Business Management Console, as well as being delivered to the email address you set up for your account.

On the Notifications page, you can turn off notification emails and define additional email addresses to send email notifications to.

You can also select options for e-mail notifications for each type of threat, which defines when e-mails are sent if the Admin doesn't read the in-app notification: instantly or in a batch at the end of the week. You can also turn email notifications off.

You can also turn in-app notification on or off for various security and network notifications. These notifications appear directly in the console.

TYPES OF NOTIFICATION

There are four types of notification:

- **Security**—Security messages notify you about threats detected and blocked and remind you to update your software.
- **Network**—These messages give you warnings and information about the status of devices in your network.
- **Billing**—Billing notifications inform you about your subscriptions and credit card status.
- **General**—General notifications are typically informational, covering subjects such as offers or scheduled maintenance.

Read and take action on new notifications in your email or by following the links on the Notification page.

SECURITY NOTIFICATIONS

- **Virus database out of date for more than 14 days**—Update your software now.
- **Virus database out of date for more than 21 days**—Update your software now. The warning will be resent if you take no action.
- **Threat blocked**—View blocked threats.
- **Threat detected**—View detected threats. Execute a full system scan.

NETWORK NOTIFICATIONS

- **Devices removed**—Verify the devices were removed intentionally.
- **New devices awaiting activation**—Activate new devices now.
- **Installation failed on a device**—View the install log to understand the issue. Resolve the issue and reinstall the software.
- **Device offline for 14 days**—Verify the device is switched on and connected to the network.
- **Devices awaiting activation for 21 days**—Activate new devices now.
- **Client software outdated for more than 21 days**—Update your software now. Make settings adjustments to update automatically on a regular schedule.

- **Devices awaiting activation more than 30 days–software expired**—Activate new devices now.
- **Device offline for 30 days**—Verify the device is switched on and connected to the network

BILLING NOTIFICATIONS

- **Payment received**—Download invoice if desired.
- **Trial will end in 7 days**—None. Unless you cancel, you will be automatically converted to the level of service of your trial and you will be billed.
- **Trial will end in 1 day**—You will be automatically converted to the level of service of your trial and billed.
- **Credit card expires in 30 days**—Supply new credit card information.
- **Credit card expired**—Supply new credit card information or risk late payments or subscription expiration.
- **Payment failed**—Supply new credit card information and pay balance owing.
- **Premium subscription expired – downgraded to free**—Supply new credit card information and pay outstanding balance.

FREQUENCY OF NOTIFICATIONS

Important notifications will be resent if the alert status persists and no action is taken. The time between repeat notifications is dependent on the severity level – a highly sensitive notification will be resent more quickly than a low sensitivity alert. However you can adjust the frequency of each notification type in the Notification settings.

NOTIFICATION EXPIRATION

Notifications will expire 30 days after the last time they are touched. “Touched” includes: delivered, read or action taken.

TO TURN IN-APP NOTIFICATIONS OFF

1. Click **Notification** 🔔.
2. Click **Notification settings**.
3. In a notification section, move the In-app notification slider to **Off**.

TO CHOOSE AN OPTION FOR E-MAIL NOTIFICATIONS

1. Click **Notification** 🔔.
2. Click **Notification settings**.
3. In a notification section, selection an option from the If not read send e-mail notification box:

   - **Instantly**—E-mails will be sent at the same time the notification is displayed in the app.
   - **Batched** – end of the week—E-mails will be sent at the end of each week.
   - **Never**—No e-mails will be sent.

TO CHOOSE WHO RECEIVES E-MAIL NOTIFICATIONS

1. Click **Notification** 🔔.
2. Click **Notification settings**.
3. Click the **Edit** link at the top of the window.
4. Select the check boxes of the names of the people you want to sent the notification to.

5. To send the email to other addresses, type the addresses, separated by commas, in the **Send a copy to the following email addresses** box.
6. Click **Update**.

DEVICES

The Devices page helps you manage your devices and groups. On this page, you can customize your device security to your environment.

On the Devices page, you see a list of all your devices and groups. This lets you view device status and drill down to the details of each device.

UNDERSTANDING THE STATUS OF DEVICES

The status of each device is displayed, with different statuses displayed in different colors.

- **Green**—Indicates the device is protected and safe. No action is required.
- **Orange**—Indicates the device is vulnerable. For example, a device might be orange if a scan hasn't been run in a long time, or if the device has been added within the last thirty days but hasn't been activated. If a device is orange, you should take the recommended action as soon as possible.
- **Red**—Indicates the device is in danger. For example, if a threat has been detected on the device. Take immediate action.
- **Grey**—Indicates the device is inactive or is in the process of being activated. Decide whether to activate the device or remove it from the network.

DEVICE STATUS MESSAGES

If your device message indicates one of the following statuses, please note the action to take to make a correction.

- **Virus definitions are out of date. New virus definitions are available.**
- **A threat was detected and is currently in the virus chest**.
  View the virus chest. You are taken to the virus chest where you can see entries filtered by the current device.
- **Your device has been out of communication for an extended period. The device may be unprotected.**
  Check why the device is not connected to the network and connect it.
- **Web shield is currently disabled on your device.**
  Check the status of your device settings and enable Web Shield as needed.
- **File shield is currently disabled on your device.**
  Check the status of your device settings and enable File Shield as needed.
- **The device software is out of date. A new software version is available.**
  Create and execute the program update task on the current device.
- **Mail shield is currently disabled on your device.**
  Check the status of your device settings and enable Mail Shield as needed.

TO SEARCH FOR A DEVICE

1. Click **Devices** 🖥.
2. In the **Device name** box, type part of the name of the device you're looking for.
3. Click **Search**.

TO FILTER THE DEVICE LIST

1. Click **Devices** 🖥.
2. Click **Filters**.

NOTE Skip Step 2 if you see the **Hide filters** button.

3. Select one or more of the following:
   - **Status**
   - **Operating system**
   - **Licenses**

ADDING AND ACTIVATING DEVICES

Your network contains all the devices that you want to protect from threats, regardless of the device location. Add devices when you first install the software and whenever you acquire a new device. Your device will be protected as soon as it is added to the network. If the device is not activated within 30 days however, it will become unprotected and remain so until you activate it.

After setting up your Avast Account and creating your company profile, you need to add your laptops, PCs, and Macs (devices) into your network. This enables you to manage the security and protection of all devices from the Avast Business Management Portal, accessible through any standard Web browser.

HOW TO ADD DEVICES

There are two ways to add a device to the network:

- Download the Avast Business app installer and execute it on all devices you want to protect.
- Send an email with a link to download the Avast Business installer to the device owner.

DOWNLOAD THE AVAST BUSINESS APP INSTALLER

1. Start your **Avast Business Management Console**.
2. On the **Dashboard** or **Network** page, click **Download the installer**.
3. Customize your installer.
4. When the installer is downloaded, run it on the devices you want to protect.

After a successful install, the program automatically scans and protects the device. The software then sends a message back to the Avast Business Management Console to indicate the device is ready for activation.

ACTIVATE YOUR ADDED DEVICES

Your device is protected as soon as it is added to the network. If the device is not activated within 30 days it becomes unprotected until you activate it.

It’s important that you activate all devices when you add them to your network to prevent your protection from lapsing. New devices will receive core, free protection for 30 days after the software is installed so you have time to activate the products you need.

If the devices are not activated, a follow-up notification is sent to you after 21 days if the devices are not activated.

TO ACTIVATE YOUR ADDED DEVICES

1. Click **Dashboard** 🏠.
2. Click **Activate now**.
3. Choose the type of protection subscription - premium or free.

You will be able to see and manage the protection status of each of these devices in your dashboard.

NOTE If devices are not activated, their protection terminates after 30 days.

REMOVING AND UNINSTALLING DEVICES

You can remove and uninstall a device remotely from the Avast Business On Premise Console using the following procedure. You can also uninstall a device locally using the Windows Control Panel procedure for uninstalling the Avast Business Antivirus application.

TO REMOVE AND UNINSTALL A DEVICE REMOTELY

You can only remove and uninstall devices that are online.

When the process is complete, Avast Business Antivirus is uninstalled from the device and the device is removed from Avast Business On Premise Console.

1. Click **Devices** 🖥.
2. Click the check boxes of the devices you want to uninstall.
3. Do one of the following:
   - Click **Actions**, **Unselect all**.
   - Click the three dots icon ⋮ next to the device.
4. Click **Remove and Uninstall**.
5. Click Yes.

NOTE You may have to wait a while for the process to complete.

UPDATE MIRRORING

You can set up a device to act as an update mirror for other devices. An update mirror stores identical copies of update files that reside on Avast's update servers. Other devices that you manage through Avast Business On Premise Management Console can download update files from the update mirror instead of contacting the Avast update server.

Update mirroring is only available for Windows workstation, Windows server, and macOS devices.

Once you select a device to be an update mirror, that device receives program updates and virus definitions over the web. You can then define which devices and groups use the device to update by selecting that mirror in any Settings Template.

Ideally, the device you choose to be an update mirror should be accessible to other devices on the network and be available at all times other workstations need to update.

Only one device can be an update mirror at a time. If you have an update mirror and you set another device to be an update mirror, mirroring is turned off on the first device.

NOTE The devices and the management console will still communicate in relation to licensing, usage date, and threat notifications.

TO SELECT A DEVICE TO BE AN UPDATE MIRROR

1. Click **Devices** .
2. Click the device.
3. Move the **Update mirror** slider to **On**.
4. Make a note of the **IP Address/Host name** of the device for future use.
5. To decide how other devices will update if they can't reach the update mirror, select one of the following options:
    - **Other devices won't download updates from Update mirror but from Avast servers**
    - **Other devices won't download updates at all (Not recommended)**
6. Click **Continue**.
7. Click the check boxes of the settings templates you want to use this update mirror.
8. Click **Turn on Update** mirror.

NOTE All your existing settings templates are updated with the IP address of the mirror device.

TO DEFINE WHICH DEVICES AND GROUPS USE AN UPDATE MIRROR

Which devices and groups update from an update mirror device are defined in the settings template applied to those devices and groups.

If a settings template doesn't have an IP address in the Updates via mirror section, the devices and groups with that settings template applied do not update from a mirror, they update directly from Avast servers.

1. Click **Device settings** .
2. Click a template.
3. Click one of the following tabs:
    - **Windows Workstation**
    - **Windows Server**
    - **Mac OS X**
4. Click the **General settings** tab.
5. Click the **Use mirror on this setting template** check box.
6. Select the IP address of the mirror device.

NOTE If there is no IP address in the box, no mirror will be used for updating.

7. For Windows Workstation or Windows Server, click a check box to define how devices and groups update when the update mirror is offline:
    - **Other devices won't download updates from Update mirror but from Avast servers**
    - **Other devices won't download updates at all (Not recommended)**

8. Click **Apply changes**.
9. Apply the template to the devices and groups you want to update from the update mirror device by following the To apply a template to a device or device group procedure.

GROUPS

Groups are a convenient tool to help you manage your devices. If you have multiple devices that you want to apply the same settings to, you can create a group of those devices and give it a name. Then you can apply settings templates to the group instead of to each device individually, which will save you time. Groups will appear in the groups panel.

VIEWING AND CREATING DEVICE GROUPS

To view or create a group, go to the Devices menu and click the group icon on the top left of the title bar. This exposes tools to help you manage device groups.

THE DEFAULT DEVICE GROUP

A default group is provided for you. This is the parent group and, although you can rename it, you can't delete it. All new devices are placed in the default group when you add them to your network, unless you specifically add the device from within another group you have created. As soon as a device is added to a group, it assumes the protection of the settings template for that group. You can change the name of the default group and the settings template that applies to it by selecting the configuration icon next to the group name.

CREATE A NESTED DEVICE GROUP

If you want to set up a device group hierarchy, you can create a device group as a subset of another group. This can help you mirror a detailed device organizational structure and apply program settings at a granular level.

TO ADD A GROUP

1. Click **Devices** 🖥.
2. If required, click the **Groups** panel.
3. Click **Add group**.
4. Type a group name.
5. Choose a parent group.
6. To choose a settings template, do one of the following:

   - Click the **Use settings template from the parent group** box.
   - Choose an option from the box.

7. Click **Add group**.

TO ADD A SUB-GROUP

1. Click **Devices** 🖥.
2. If required, click the **Groups** panel.

3. Click the three dots icon ⋮ next to a group, then click **Add sub-group**.
4. Type a group name.
5. Choose a parent group.
6. To choose a settings template, do one of the following:

   - Click the **Use settings template from the parent group** box.
   - Choose an option from the box.

7. Click **Add group**.

TO EDIT A GROUP

1. Click **Devices** 🖥.
2. If required, click the **Groups** panel.
3. Click the three dots icon ⋮ next to a group, then click **Edit group**.
4. Make your changes.
5. Click **Save group**.

TO ADD A DEVICE TO A GROUP

When you add a device to a group, the device will assume the settings of the group that it's added to. If the group uses a settings template, the added device also uses that settings template. If you move the device to a different group, it changes to use the settings template of the group you moved it to.

1. Click **Devices** 🖥.
2. Click the check boxes of the devices you want to move.
3. Click **Actions**, **Move to group**.
4. Click the group to add the device to.
5. Click **Move devices**.

NOTE You can also add a device to a group by dragging the device to any group in the Groups panel on the Devices page.

ACTIONS ON THE DEVICE PAGE

On this page, you can also perform certain actions, such as:

- Changing the settings template
- Changing the license edition
- Activating the device
- Unselecting devices
- Removing and uninstalling the device

You can perform these actions on single devices or on multiple devices at once.

TO CHANGE THE SETTINGS TEMPLATE OF A DEVICE

NOTE This procedure may require the device to restart.

1. Click **Devices** 🖥.
2. Click the check boxes of the devices you want to move.

3. Click **Actions**, **Change settings template**.
4. Do one of the following:
   - To use the settings template from the parent group, select **Use settings template from the parent group**.
   - To choose a different settings template, clear the check box, then select a settings template.
5. Click **Change settings template**.

TO CHANGE THE LICENSE EDITION OF A DEVICE

NOTE This procedure requires the device to restart.

1. Click **Devices** 🖥.
2. Click the check boxes of the devices.
3. Click **Actions**, **Change license edition**.

TO ACTIVATE A SELECTED DEVICE

NOTE This procedure requires the device to restart.

1. Click **Devices** 🖥.
2. Click the check boxes of the devices.
3. Click **Actions**, **Activate selected devices**.

TO UNSELECT A DEVICE

1. Click **Devices** 🖥.
2. Click **Actions**, **Unselect all**.

REMOVING AND UNINSTALLING DEVICES

The To remove and uninstall a device procedure removes the device from your device list, but the Avast software is not yet removed from the device. The status of the device appears as “Uninstalling” until the uninstall is complete, when the device no longer appears in the console.

The second step in the process occurs the next time your removed device connects to the internet:

- The device receives the 'remove' message and uninstalls the security software.
- When the uninstall concludes, a message is sent back to your management console confirming the device is removed.

TO REMOVE AND UNINSTALL A DEVICE

1. Click **Devices** 🖥.
2. Click the check boxes of the devices.
3. Click **Actions**, **Remove and uninstall**.
4. Click **Yes**.

PERMANENTLY REMOVING A DEVICE THAT CANNOT CONNECT TO THE NETWORK

If your device is lost or cannot connect to the network (for example, it has no internet connection), it may never receive the message to perform the uninstall. If this is the case, you can permanently delete the device from within the management console and, if possible, manually uninstall the software from the device.

To delete the device from the management portal, first follow the To remove an uninstall a device procedure. Then:

1 Find the device by filtering for deleted devices.
2 Delete the device again.

The device is fully removed from the network. If you have access to the device, but it cannot access the network, manually uninstall the Avast software from the device.

CREATING TASKS ON THE DEVICE PAGE

You can create tasks on the Device page, or on the Tasks page. The difference is that when you create tasks on the Device page, you can choose the devices that the task runs on. If you create a task on the Tasks page, the task will run on all devices.

TO SCAN A DEVICE

1 Click **Devices** 🖥.
2 Click the check boxes of the devices you want to include in the task.
3 Click **Actions**, **Create a task**.
4 Click **Scan device**.
5 Select a type of scan:

- **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.

6 Choose the options for your scan.
7 Click **Start Scan**.

TO SEND A MESSAGE TO A DEVICE

1 Click **Devices** 🖥.
2 Click the check boxes of the devices you want to include in the task.
3 Click **Actions**, **Create a task**.
4 Click **Send a message to the device**.
5 Type a message to your users.
6 Type a Custom name for the Send a message to the device task.
7 Do one of the following:

- To send the message now, leave the **Schedule the message** check box unchecked. Click **Send message**.
- To schedule the message for a later time or make the message repeat on a regular basis, click the **Schedule the message** check box, then choose your scheduling options. Click **Schedule message**.

TO UPDATE A DEVICE

1. Click **Devices** 🖥.
2. Click the check boxes of the devices you want to include in the task.
3. Click **Actions**, **Create a task**.
4. Click **Update device**.
5. Do one of the following:
    - To update Avast Business Antivirus, click the **Program update** check box.
    - To update virus definitions, click the **Virus definition update** check box.
6. Type a Custom name for the Update device task.
7. Do one of the following:
    - To update now, leave the **Schedule the message** check box unchecked. Click **Update**.
    - To update later or repeat the update on a regular basis, click the **Schedule the update** check box, then choose your scheduling options. Click **Schedule update**.

TO SHUT DOWN A DEVICE

1. Click **Devices** 🖥.
2. Click the check boxes of the devices you want to include in the task.
3. Click **Actions**, **Create a task**.
4. Click **Shutdown device**.
5. Click one of the following check boxes:
    - **Restart device**
    - **Shutdown device**
6. Type a message that will notify your users before the restart or shutdown.
7. Choose an option in the **Specify when the message is displayed** box.
8. Type a Custom name for the restart or shutdown task.
9. Do one of the following:
    - To update now, leave the **Schedule the message** check box unchecked. Click **Update**.
    - To update later or repeat the update on a regular basis, click the **Schedule the update** check box, then choose your scheduling options. Click **Schedule update**.

VIEWING DEVICE DETAILS

When you click a device, you are taken to a device details page that shows you more information about the device. This page includes four tabs:

- Overview
- Components
- Tasks
- Threats detected

On each of these tabs, you can perform certain actions.

TO VIEW DEVICE DETAILS

1. Click **Devices** 🖥.
2. Click a device.

On the **Overview tab**, you can view information such as device alias, device IP address, domain, and operating system. The actions you can perform on this tab are:

- Edit the device alias.
- Turn on the update mirror.
- Change the license edition.
- Change and edit the settings template.
- Remove this device from your network.

On the **Components tab**, you can view the status of your antivirus and identity protection. You can also turn the components of your protection on or off. For more information about each component, see the documentation that comes with Avast Business Antivirus.

The **Tasks tab** displays the progress of recent, current, and scheduled tasks, along with a description, the time started, and the last results, if any. On this tab, you can stop and delete tasks. You can also create tasks. For more information about creating tasks, see the help for the Tasks page.

TO STOP OR DELETE A TASK FROM THE TASKS TAB OF THE DEVICES PAGE

1. Click **Devices** 🖥.
2. Click a device.
3. Click the **Tasks** tab.
4. Click the three dots icon ⋮ next to a task, then click **Stop** or **Delete**.

The **Threats detected tab** shows details of the threats detected on devices. This tab shows the threat status, name, file name and location, how it was detected, and the date of detection. From this tab, you can open the Virus chest, where you can restore and delete files.

TO RESTORE AND DELETE INFECTED FILES FROM THE THREATS DETECTED TAB OF THE DEVICES PAGE

1. On the **Threats detected** tab, click **Virus chest**.
2. Select the infected file.
3. Click one of the following:

- **Restore files**
- **Delete files**

TASKS

The Tasks page shows you the progress of tasks on devices, a description of tasks, the schedules of tasks, as well as the results of tasks, if any. The Tasks page displays completed, in-progress, and scheduled tasks. You can click any task to see more details, including which devices the task has been completed on and the devices where the task isn't complete.

Through this page, you can create tasks for all devices, such as device scans, messages to devices, device updates, and device shutdowns. You can create these tasks to happen as soon as possible, or you can schedule them for at a future point in time and schedule them to recur on a regular basis.

TASK HISTORY

The Task History pane shows you details of executed tasks, including the number of devices where the task is completed, and the number where the task isn't done. Click anywhere in a task to see exactly which devices are in each state. Tasks will only run on their assigned devices when the device is turned on and will only report status when they are connected to the network.

In the Task History pane, you can stop tasks that are in progress and delete tasks.

NOTES

- If you want to create a task that applies only to certain devices, and not all the devices you manage, create your task on the Device page.
- Tasks from deleted devices are displayed until deleted.

VIEWING TASKS

Double-clicking any task lets you see the details of that task.

Filtering tasks helps you find the tasks you're looking for when you have a lot of tasks completed, in progress, or scheduled.

TO SEE THE DETAILS OF A TASK

1. Click **Tasks** 🔍.
2. Double-click a task.

NOTE If you want to delete the task, scroll to the bottom of the page and click the Delete task link.

TO FILTER TASKS

1. Click **Tasks** 🔍.
2. If the **Filters** button displays, click it.
3. Do any of the following:

   - Select an interval.
   - Select a task type.

TO UNSELECT TASKS

1. Click **Tasks** 🔍.

2. Click the check boxes of the tasks you want to stop or delete.
3. Click **Actions**.
4. Do one of the following:

   - To stop the tasks, click **Stop**.
   - To delete the tasks, click **Delete**.

EDITING TASKS

Once you have set up a task, you can't edit it. If you need to change a task, you must delete the current task and create a new one.

TO STOP OR DELETE A TASK

1. Click **Tasks** 🔍.
2. Click the check boxes of the tasks you want to stop or delete.
3. Click **Actions**.
4. Do one of the following:

   - To stop the tasks, click **Stop**.
   - To delete the tasks, click **Delete**.

CREATING TASKS ON THE TASKS PAGE

You can create tasks on the Device page or on the Tasks page. The difference is that when you create tasks on the Device page, you can choose the devices that the task runs on. If you create a task on the Tasks page, the task will run on all devices.

SCANNING DEVICES

You can create the following types of scans:

- **Quick scan**—This is fastest and scans the most vulnerable areas of your device.
- **Full system scan**—This can cover all data, programs and storage but will take longer to run.
- **Removable media scan**—CD/DVD, external drive or USB drive - that you have attached to your device.
- **Custom scan**—This option provides the capability to create and save scans based on a range of scan parameters specific to your devices and environment.
- **Boot-time scan**—This option scans Windows Workstations when they boot up.

WHEN TO RUN SCANS

The more often your users download files from the web or install software, the more often you should perform scans. The more often you do scans, the more likely you will catch malicious threats before they do damage to your devices and networks.

You can create a task to run regularly scheduled scans that will run on your network at non-peak times so that your users' work will not be interrupted.

TO SCAN ALL MANAGED DEVICES

1. Click **Tasks** 🔍.

2. Click **Create a task**.
3. Click **Scan device**.
4. Select a type of scan:

    - **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 if compressed files are included.
    - **Boot-time Scan (MS Windows only)**—Run a scan when the device boots up.

5. Choose the options for your scan.
6. Click **Start Scan**.

UPDATING DEVICE SOFTWARE

Both Avast Business Antivirus threat detection software and the threat database that Avast Business Antivirus uses are updated on a frequent basis. New threats are discovered every day and it is important to keep your device up to date to maximize the protection of your device and networks.

HOW TO UPDATE ANTIVIRUS SOFTWARE AND VIRUS DEFINITIONS

You can create a task to update the Avast Business Antivirus application or update the virus definition file for Avast Business Antivirus.

When the task runs, the software updates on each device the next time that device is turned on and connected to the internet. The task history shows you when the task has completed successfully for each device.

NOTE You can also set your settings template to update Avast Business Antivirus and virus definition updates automatically. For more information, see Using settings templates to keep antivirus up to date.

TO UPDATE ANTIVIRUS ON ALL MANAGED DEVICES

1. Click **Tasks** 🔍.
2. Click **Create a task**.
3. Click **Update device**.
4. Do one of the following:

    - To update Avast Business Antivirus, click the **Program update** check box.
    - To update virus definitions, click the **Virus definition update** check box.

5. Type a Custom name for the Update device task.
6. Do one of the following:

    - To update now, leave the **Schedule the message** check box unchecked. Click **Update**.
    - To update later or repeat the update on a regular basis, click the **Schedule the update** check box, then choose your scheduling options. Click **Schedule update**.

SENDING A MESSAGE TO ALL MANAGED DEVICES

You can send a message to all devices whenever you want to share important information with users, for example, to warn them in advance of an upcoming shutdown. The message appears in a small pop-up window on users' devices.

TO SEND A MESSAGE TO ALL MANAGED DEVICES

1. Click **Tasks** 🔍.
2. Click **Create a task**.
3. Click **Send a message to the device**.
4. Type a message to your users.
5. Type a Custom name for the Send a message to the device task.
6. Do one of the following:

   - To send the message now, leave the **Schedule the message** check box unchecked. Click **Send message**.
   - To schedule the message for a later time or make the message repeat on a regular basis, click the Schedule the message check box, then choose your scheduling options. Click Schedule message.

SHUTTING DOWN ALL MANAGED DEVICES

From the Tasks page, you can create a task to shut down or restart all managed devices. When you create the task, you choose an option for when the warning message to users is displayed and decide if the shutdown happens immediately, is scheduled to happen later, and if it recurs on a regular basis.

TO SHUT DOWN ALL MANAGED DEVICES

1. Click **Tasks** 🔍.
2. Click **Create a task**.
3. Click **Shutdown device**.
4. Click one of the following check boxes:

   - **Restart device**
   - **Shutdown device**

5. Type a message that will notify your users before the restart or shutdown.
6. Choose an option in the **Specify when the message is displayed** box.
7. Type a Custom name for the restart or shutdown task.
8. Do one of the following:

   - To update now, leave the **Schedule the message** check box unchecked. Click **Update**.
   - To update later or repeat the update on a regular basis, click the **Schedule the update** check box, then choose your scheduling options. Click **Schedule update**.

DEVICE SETTINGS

On the Settings page, you can view and manage your settings templates.

A settings template is a group of security rules. You can create a group of settings, save it as a template and then apply it to a device or device group. A settings template contains settings for multiple operating systems—Windows, Windows Server, and Mac—and consists of a set of security preferences that you can apply to devices and device groups.

If you change a settings template that is applied to devices and device groups, once you save the settings they will be applied to all those devices and groups. The changes are also applied to any future devices and device groups you apply the template to.

DEFAULT TEMPLATE

Avast Business Management Console includes a default template that has already been set up for you, 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. You can also change templates at any time.

USING SETTINGS TEMPLATES TO KEEP ANTIVIRUS UP TO DATE

In the General tab of the settings template, there are two settings that help you keep your Avast software and the threats library updated. By default, both of these settings are configured to update automatically. This will ensure updates are always applied as they become available, without you having to remember.

These settings are available on all three tabs of settings templates:

- Windows workstation
- Windows server
- Mac OS X

WINDOWS WORKSTATION SETTINGS

For Windows Workstation, the areas you can configure are:

- **Active protection**—Antivirus, Data, and Identity protection.
- **General**—Common settings such as password protection, program updates, and virus definition updates.
- **Antivirus**—DeepScreen, CyberCapture and Hardened mode. You can also exclude file paths and URLs and identify file paths to exclude from DeepScreen and Hardened mode.
- **Troubleshooting**—Enable self-defense mode and hardware-assisted virtualization as well as identify Web and Mail ports.

WINDOWS SERVER SETTINGS

For Windows Server, you can configure settings that will be applied only to Windows Servers.

MAC OS X SETTINGS

For Mac OS X, you can configure:

- **Active protection**—File Shield, Mail Shield, and Web Shield.
- **General settings**—Automatic and streaming updates.

TO CREATE A SETTINGS TEMPLATE

1. Click **Device settings** 🔧.
2. Do one of the following:
   - To duplicate a template, click the three dots icon ⋮ at the right of a template and click **Duplicate**.
   - Click **Add a settings template**.
3. Type a name for the setting.
4. Click **Create**.

TO EDIT A TEMPLATE

1. Click **Device settings** 🔧.
2. Click a template.
3. Make your changes.
4. Click **Apply changes**.

NOTE If you change the name of the settings template, click **Save name**.

TO DELETE A TEMPLATE

1. Click **Device settings** 🔧.
2. Click the three dots icon ⋮ at the right of a template and click **Delete**.
3. Click **Delete**.

TO APPLY A TEMPLATE TO A DEVICE OR DEVICE GROUP

If you apply a settings template to a device, it overrides the settings template applied to the parent group. The device continues to use the assigned settings template until you change the settings template, which means that the device continues to use the settings template even if you move it to a new group.

1. Click **Device settings** 🔧.
2. If required, click the **Groups** panel.
3. Click the check boxes of the device or device group to apply the template to.
4. Click **Actions**, then **Change Settings** template.
5. Do one of the following:
   - Click the **Use settings template from the parent group** check box.
   - Clear the **Use settings template from the parent group** check box, then select a new settings template.
6. Click **Change settings template**.

TO SEE THE DEVICES AND DEVICE GROUPS THAT HAVE THE SETTINGS TEMPLATE APPLIED

1. Click **Device settings** 🔧.
2. Do one of the following:
   - To see the devices and device groups that have the template applied to them directly, click the **Directly assigned column** of the settings template.
   - To see the devices and device groups that have the template applied to them directly, in addition to the devices and device groups that inherit the template, click the **Settings used column** in the settings template.

NOTE You can change the settings template the group or device by clicking **Change settings**.

LICENSES

On the licenses page, you can see an overview of your current licenses, how many licenses are currently assigned, start a trial of another level of protection, and buy additional licenses.

TO START A LICENSE TRIAL

1. Click **Licenses** .
2. Under one of the Antivirus tiers, click **Start Trial**.

TO BUY LICENSES

1. Click **Licenses** .
2. Do one of the following:
   - To buy licenses for additional devices, under one of the Antivirus tiers, click **Buy more devices**.
   - To buy or renew a license, click **Buy now**.

REPORTS

The Reports page displays a visual representation of data for:

- Threats
- Tasks
- Devices

You can change the timeframe of the report, and you can also change the regional settings for the report. Regional settings include the first day of the week and your time zone.

NOTE When you change the time zone, the new time zone is applied everywhere times and dates appear in the console. For example, the last time your devices were synched and the date when the last threat was blocked.

TO CHANGE THE REPORTING PERIOD

1. Click **Reports**.
2. Choose an option in the **Show report for** box.

TO CHANGE REGIONAL SETTINGS

1. Click **Reports**.
2. Click the **UTC** link in the top right of the window.

NOTE You can also click **Settings** to change the regional settings.

3. Choose the day your week starts on.
4. Choose your time zone.
5. Click **Update**.

THREATS REPORT

This area displays external threats to devices and data, and how you have been protected from them.

THREAT OVERVIEW AND THREATS OVER TIME

Displays how many threats were detected by each shield. It counts threats that were resolved as well as those that were not resolved for any reason.

THREAT TYPES

Displays a breakdown of threat categories. It counts all detected threats.

TOP 10 THREATS

Displays how many times a particular threat was detected by any shield, no matter if it was resolved or not. If the same threat was detected on more devices that might mean an infected source has spread across your devices.

HOW THREATS WERE RESOLVED

Displays a breakdown of actions that were taken in order to resolve the threats. It counts only successful actions.

TOP 10 INFECTED DEVICES

Displays the devices that have the most threats detected. Both resolved and unresolved threats are counted.

TASKS REPORT

This area displays information on failed tasks.

TASKS OVERVIEW

One-time tasks refer to tasks that weren’t scheduled and tasks that were scheduled to run just once. Automatic recurring task runs refer to every task that was executed during the selected time period on each of your devices. For example, if you selected Last 30 days as your time-range and you have one recurring task that runs on all five of your devices on a daily basis, your Task overview will show 150 automatic recurring task runs from one recurring task (1 task x 30 runs on 5 devices = 150 runs in total).

The number of failed task runs is calculated based on every task run on each of your devices. Therefore, you may have multiple failed task runs even with only one device.

DEVICES REPORT

This area displays information on devices. The number of devices removed and the number of devices added are displayed.

TOP 10 DEVICES WITH FAILED TASKS

This section displays the number of times each task has failed on each of your devices. If an automatic recurring task fails multiple times, each failure is recorded as a new task failure.

DEVICE OVERVIEW

Device removed refers to the number of times you uninstalled antivirus from a device, regardless of whether you uninstalled antivirus from the console or directly from the device.

Devices added refers to the number of devices you have installed and activated Avast Business Antivirus on. If you install Avast Business Antivirus on a device but do not activate it from the console, the device is not counted.

If you reinstall Avast Business Antivirus on a device, the device won’t be included in the count for devices removed or devices added.

COMPANY PROFILE

When you create your Avast Account, we recommend you set up your company profile, including information such as company name, industry, size, and contact information. Provide the information as completely as possible and click the Save button at the bottom of the page. You can return and edit company details whenever information changes within the company.

CLOSE YOUR AVAST ACCOUNT

If needed, you can also close your account from the company profile page. When you close your account, Avast Business Management Portal and Avast Business Antivirus immediately uninstall from your devices so they are unprotected. You lose access to the Management Portal and all your settings and customizations.

NOTE If you are subscribed to Premium or any paid add-ons, a final invoice will be sent to the e-mail address of the account holder and you will be charged for your last month's usage.

TO SET UP OR EDIT YOUR COMPANY PROFILE

1. Click your profile icon in the top right corner of the browser window, then click **Edit company profile**.
2. Make your changes.

NOTE Company name and Industry are required fields.

3. Click **Save**.

USER MANAGEMENT

The User Management area is provided so that you can:

- Invite other users in your company to help you manage the portal.
- View who has access to your portal.
- Restrict access of existing users to the portal (i.e. block access or remove access).

Once you've added a user, you can edit the following information:

- Name
- Surname
- Email
- Role

You can also change your password at any time. Avast Business enforces a strong password policy. The minimum length for a password is eight characters and must use at least one letter, one number, and one special character.

TO ADD A USER

1. Click your profile icon in the top right corner of the browser window, then click **User management**.
2. Click **Create new user**.
3. Type the following:

   - **Name**
   - **Surname**
   - **Email**
   - **Password**
   - **Retype password**

4. Select a **Role**.
5. Click **Create**.

TO EDIT A USER

1. Click your profile icon in the top right corner of the browser window, then click **User management**.
2. Click a user.
3. Make your changes.
4. Click **Save**.

TO CHANGE A PASSWORD

1. Click your profile icon in the top right corner of the browser window, then click **User management**.
2. Click a user.

3 Click **Change password**.
4 Type a new password that is at least eight characters long and uses at least one letter, one number, and one special character.
5 Type the password again.
6 Click **Save**.
7 Click **Save**.

TROUBLESHOOTING

In this section, you can find answers to the most common troubleshooting questions.

WHERE CAN I FIND LOGS?

If you used the default installation path, the Avast Business On Premise Management Console logs will be located in C:\Program Files\Avast Software\Management Console\Console\Log.

When troubleshooting using logs, you will find most common issues in main.log

CAN I TURN ON DEBUG LOGGING?

You can turn on debug logging, but it isn’t recommended since it creates a large number of logs.

WHERE ARE THE POSTGRESQL LOGS?

You can find PostgreSQL log information in the Windows Events logs.

MY DEVICE IS INSTALLED BUT DOESN’T APPEAR IN THE CONSOLE

This may be because the device doesn’t support IPv6 hostnames.

WHY ISN’T UPDATE MIRRORING WORKING?

If update mirroring isn’t working, confirm the settings are applied correctly. If you find the settings are correct, then you may find that a firewall or network issue is keeping updates from being transferred from the update mirror to the client device.

CAN I SUPPORT DEVICES THAT USE PROXY SERVERS?

Avast Business On Premise Management Console doesn’t currently support devices that use proxy servers.

CAN I USE AVAST BUSINESS MANAGEMENT CONSOLE ON AN OFFLINE NETWORK?

Avast Business Management Console requires access to the internet.

INDEX