



**Avast Business
Cloud Console**

TABLE OF CONTENTS

Introduction to Avast Business Cloud Management Console.....	1
Setting up.....	2
Requirements.....	2
Windows installation	3
Creating an account	3
Uploading your license.....	4
Logging in to Avast Business Cloud Management Console for Windows.....	4
Navigation and General Settings	5
Minimizing and maximizing the Navigation bar	5
Submitting a ticket to Avast Technical Support.....	5
Setting time and date options	7
Setting up Master Agents	7
Migrating from Enterprise Administration or Small Office Administration.....	11
Dashboard.....	12
Shortcuts.....	12
Adding and activating devices	12
Automatically Deploying Avast Antivirus to Multiple Devices Remotely	14
Network Security – Operating System.....	16
Threat Detection Statistics.....	16
Notifications.....	17
Devices.....	20
Understanding the status of devices	20
Assigning a settings template to devices.....	21
Removing and uninstalling devices.....	22
Groups.....	22
Actions on the Device page.....	24
Removing and uninstalling devices.....	25
Viewing device details.....	28
Tasks.....	30
Task history	30
Viewing tasks	30

Creating tasks on the Tasks page	31
Scanning devices	32
Sending a message to all managed devices	32
Updating device software	33
Shutting down all managed devices	33
Device Settings.....	35
Default template	35
Configuring Avast Business Antivirus with settings templates.....	35
Reports.....	100
Threats report	100
Tasks report	101
Device report	101
Licenses	102
Company profile.....	104
Close your Avast account.....	104
Personal profile	105
User management	106
Troubleshooting.....	108
Where can I find logs?.....	108
Can I turn on debug logging?	108
Where are the PostgreSQL logs?	108
My device is installed but doesn't appear in the console.....	108
Why aren't Master Agents working?	108
Can I support devices that use proxy servers?	108
Can I use Avast Business Cloud Management Console on an offline network?.....	108
Index.....	109

CHAPTER ONE:

INTRODUCTION TO AVAST BUSINESS CLOUD MANAGEMENT CONSOLE

With Avast Business Cloud 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 Cloud Management Console provides:

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

Avast Business Cloud 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 e-mail client

When you install Avast Business Antivirus on devices through Avast Business Cloud 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.

CHAPTER TWO:

SETTING UP

Setting up Avast Business Cloud Management Console involves three steps:

- Creating an account
- Logging in to the console
- Uploading your license

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

REQUIREMENTS

Connecting to Avast Business Cloud Management Console requires:

- A Windows or Mac device
- A web browser

SUPPORTED VIRTUALIZATION TOOLS

Avast Business Cloud Console has been tested with the following virtualization tools:

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

DEFAULT PORTS

Ensure the following ports are open:

	PORT NUMBER
Default port	▪ 8443
Default database server port	▪ 5432
Ports used for communication between Avast Business Cloud Management Console and Avast Business Antivirus	▪ 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. Using an SMTP server is optional, but Avast highly recommends doing so.

SSL CERTIFICATE

Communication between the Avast Business Cloud 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 Cloud 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 the installation process lets you 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\\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

The first time you access Avast Business Cloud Management Console, you are prompted to create a new account and company. Each following time you access the console, you must log in. If you have your own SSL certificate, you can use it. If not, Avast can generate one for you.

TO ACCESS AVAST BUSINESS CLOUD MANAGEMENT CONSOLE

- 1 Using a web browser, navigate to <https://business.avast.com>.
- 2 Click **Register**.
- 3 Follow the Wizard to set up access.


CREATING AN ACCOUNT

The first time you run Avast Business Cloud 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**.

LOGGING IN TO AVAST BUSINESS CLOUD MANAGEMENT CONSOLE FOR WINDOWS

- 1 On a Windows computer, using an internet browser, navigate to <https://business.avast.com>.
- 2 Log in with your username and password.

CHAPTER THREE:

NAVIGATION AND GENERAL SETTINGS

The navigation menu on the left side of the Avast Business window lets you go to the different pages in the application. To save space on your screen, you can minimize the navigation bar.

The navigation bar also lets you:

- Submit a ticket to Avast technical support
- Set the local date and time
- Set up e-mail so you can send download links
- Migrate from other consoles
- Update the console

MINIMIZING AND MAXIMIZING THE NAVIGATION BAR

TO MINIMIZE THE NAVIGATION BAR

- Click .

TO MAXIMIZE THE NAVIGATION BAR


- Click .

SUBMITTING A TICKET TO AVAST TECHNICAL SUPPORT

Before contacting Technical Support, you can try any of the following steps:

- Restarting your computer
- Checking that your computer's internet access is working
- Updating to the latest version of Avast for Business Cloud Console
- Reading the [Troubleshooting](#) page of this manual
- Looking for the answer to your technical questions on the [Avast forum](#) and in the [knowledgebase](#)

TO UPDATE THE AVAST BUSINESS CLOUD CONSOLE

Updating the Avast Business Cloud Console can sometimes solve technical issues, as well as give you new features to manage devices. If there is a new version available, you'll see this icon at the bottom left corner of the console, next to the version number: 

If the icon doesn't appear next to the version number, then you have the current version, however, you can always check if your version is up to date by clicking the version number link. The dialog that pops up tells you if you need to update.

TO CHECK FOR UPDATES

- Click the version number link at the bottom left corner of the console.

NOTE To see the product roadmap, what's in development, and what was introduced in previous versions, click the link, then click the tab of the information you'd like to see.

TO UPDATE THE CONSOLE

- 1 Click the version number link at the bottom left corner of the console.
- 2 In the dialog box, click **Download**.
- 3 Open the downloaded file.
- 4 Follow the installer instructions.

SUBMITTING A TICKET TO AVAST TECHNICAL SUPPORT

You can submit a ticket to Avast Technical Support directly from the left navigation menu or [on this page](#).

NOTE All fields are mandatory.


PRIORITY

Select a priority that reflects the severity of your issue:

- **High**—The product isn't usable. For example, users can't log in to the console, or a newer version has failed to install.
- **Medium**—The product has lost significant functionality or performance and some users can't perform their normal functions. For example, a feature is failing or service is interrupted.
- **Low**—Any issue that doesn't have a significant impact. Also used for product feature requests and how-to questions. For example, if you want to request an enhancement to the product or can't find what you need to accomplish a task.

NOTE Avast responds to submitted tickets within 24 hours. Selecting a higher priority doesn't affect ticket response time.

TO SUBMIT A TICKET TO AVAST TECHNICAL SUPPORT

- 1 Click **Submit a ticket** .
- 2 Type the following:
 - **Company**
 - **Contact Name**
 - **Email**
 - **Phone**
 - **Subject**
 - **Description**
- 3 Select a **Priority**.
- 4 Select your **Product**.
- 5 Select the **I'm not a robot** check box.
- 6 Click **Submit**.

SETTING TIME AND DATE OPTIONS

The time and date options you can set on the Regional settings tab affect how reports are generated and displayed.


FIRST DAY OF THE WEEK

When you choose the first day of the week, [weekly reports](#) begin on that day of the week. For example, if you choose Saturday, all weekly reports begin on Saturdays. If you choose Monday, all weekly reports begin on Mondays.

TIME ZONE

The time zone displays on the top right corner of reports. You can change your time zone at any time.

TO SET TIME AND DATE OPTIONS

- 1 Click **General Settings** .
- 2 Click the **Regional settings** tab.
- 3 In the **First day of week** box, select a day.
- 4 In the **Time zone** box, select a time zone.
- 5 Click **Save**.

SETTING UP MASTER AGENTS

You can set up devices to act as Master Agents for other devices. Master Agents store identical copies of update files that reside on Avast's update servers. Other devices that you manage through Avast Business Cloud Management Console can download update files from Master Agents instead of contacting the Avast update server.

Once you select a device to be a Master Agent, 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 devices you choose to be Master Agents should be accessible to other devices on the network and be available at all times other workstations need to update. If you set up multiple Master Agents, your devices can update from another even if one is unavailable.

NOTE Devices and the management console still communicate directly for licensing, usage data, and threat notifications.



MASTER AGENT REQUIREMENTS

The device you use as a Master Agent must:

- Be online all the time
- Have a static IP address

We highly recommend you choose a server device for your Master Agent.

MASTER AGENTS AND DEVICES RUNNING AVAST ANTIVIRUS VERSION 18.4 AND OLDER


You cannot use Master Agents with devices that run Avast Antivirus version 18.4 and older.

IMPORTANT Avast recommends updating your devices to a newer version, and using a Master Agent.

If you cannot update the device, you can download updates from Local Update Servers instead of Avast Update Servers, which will reduce the bandwidth you use to download updates.

See [To update devices with Avast Antivirus 18.4 and older using Local Update Servers](#).

TO SET UP A DEVICE AS A MASTER AGENT


- 1 Click **General Settings** .
- 2 Click the **Master Agents** tab.
- 3 Click **Add new Master Agent**.
- 4 (Optional) Select an operating system in the **Filter devices** list and type a device name in the **Search** box.
- 5 Click a device.
- 6 Click **Select**.

Once you finish this procedure, it may take a while for the Master Agent to activate on the device.

TO DEFINE WHICH DEVICES AND GROUPS USE A MASTER AGENT

Master Agents can be used by devices use to download updates instead of downloading them from the Avast servers, which can take longer.

Which devices and groups update from a Master Agent are defined in the settings template applied to those devices and groups.

- 1 Click **Device settings** .
- 2 Click a template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **General settings** tab.
- 5 If required, click the **Advanced update settings for devices with AV version 18.4 and older** link to expand it.
- 6 In the Virus definitions updates and Program updates section, select the **Via available Local Update Servers** button.
- 7 Click **Apply Changes**.
- 8 Apply the template to the devices and groups you want to update from the Master Agent device by following the [To apply a template to a device or device group](#) procedure.


TURNING MASTER AGENTS ON AND OFF

You can turn Master Agents on or off:




- for a device
- for one or more device groups
- for all devices and groups

NOTE Turning a Master Agent on or off only affects devices and device groups that are configured to use the Master Agent to update.

TO TURN A MASTER AGENT ON OR OFF FOR A DEVICE



- 1 Click **Devices** .
- 2 Click a device.
- 3 Click the **Overview** tab.
- 4 Do one of the following:
 - To turn a Master Agent on, select the **Always update from Avast servers** check box.
 - To turn a Master Agent off, clear the **Always update from Avast servers** check box.
- 5 Click **Save**.

TO TURN A MASTER AGENT ON OR OFF FOR A DEVICE GROUP



- 1 Click **Devices** .
- 2 If the **Groups** panel is not expanded, click **Expand Groups** .
- 3 Click the **More** button  next to the group, then click **Edit group**.
- 4 Do one of the following:
 - To turn the Master Agent on, select the **Always update from Avast servers** check box.
 - To turn the Master Agent off, clear the **Always update from Avast servers** check box.
- 5 Click **Save group**.

TO TURN A MASTER AGENT ON

This procedure turns on a Master Agent for devices and device groups that are assigned to use the Master Agent.



- 1 Click **General Settings** .
- 2 Move the slider  next to the Master Agent to **On**.
- 3 Select the IP address of your Master Agent device in the **Select mirror IP address** list.
- 4 Click **Turn ON**.

TO TURN A MASTER AGENT OFF

- 1 Click **General Settings** .
- 2 Move the slider  next to the Master Agent to **Off**.
- 3 Click **Turn OFF**.

TO UPDATE DEVICES WITH AVAST ANTIVIRUS 18.4 AND OLDER USING LOCAL UPDATE SERVERS

If the devices cannot communicate with your Local Update Server, they will update from Avast's Update Servers.

- 1 Click **General Settings** .
- 2 Move the slider  next to the Master Agent to **On**.
- 3 Click the Advanced update settings for devices with AV version 18.4 and older link.
- 4 Select the **Use Local Update Server for devices with Program version 18.4 and older** check box.
- 5 Select the IP address of your Local Update Server in the **Select mirror IP address** list.
- 6 Click **Turn ON**.


MIGRATING FROM ENTERPRISE ADMINISTRATION OR SMALL OFFICE ADMINISTRATION

When you import Enterprise Administration and Small Office Administration products, they are replaced with Avast Business Antivirus or Avast Business Antivirus Pro licenses, depending on which editions you had in your old console. Please note that the term “edition” is replaced with “license”.

If you have more than one license or licenses from multiple editions, you may need to [activate devices](#) manually.

NOTE Settings/Policies are transferred along with the devices.

TO MIGRATE FROM ENTERPRISE ADMINISTRATION OR SMALL OFFICE ADMINISTRATION

- 1 Click **General Settings** .
- 2 Click **Import file**.
- 3 Navigate to the `export.xml` file on the device where your console is installed:
 - EA console: `C:\Program Files\AVAST Software\Enterprise Administration\DATA\log`
 - SOA console: `C:\ProgramData\AVAST Software\Administration Console2`
- 4 Click **Open**.

You will see an overview of how many groups and devices you're able to transfer.

- 5 Click the **Devices** page.

Devices from the EA/SOA console appear in this console in the **Devices** section, with the status of Pending. This may take a while.

- 6 Select the groups or devices you want to transfer.
- 7 Click **Transfer**.


As they transfer, the status of the devices change from Pending to Transferring.

Once devices are fully transferred they have the status Safe, Vulnerable, or In Danger, depending on the health of the device.

CHANGING THE LANGUAGE

TO CHANGE THE LANGUAGE

You can choose from eight languages.

- 1 Click your profile icon  in the top right corner of the browser window, then click **Language**.
- 2 Select a language.
- 3 Click **Change Language**.

CHAPTER FOUR:

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 seeing threat reports.
- 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 Cloud Management Console, scan your devices, activate devices, and upload license files.

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 is 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 three ways to add a device to the network:

- [Download the Avast Business app installer](#) and execute it on all devices you want to protect.
- [E-mail an Avast Business download link](#) to the device owner.
- [Use a remote installer to automatically add multiple remote devices.](#)

TO DOWNLOAD THE AVAST BUSINESS APP INSTALLER

- 1 Start the **Avast Business Cloud Management Console**.
- 2 On the **Dashboard** page, click **Download antivirus**.
- 3 Click **Download the installer**.
- 4 Select the operating system the installer is for:
 - **Windows .EXE (For workstations and servers)**
 - **Windows .MSI**
 - **Mac OS X .DMG**
- 5 Select the product **License**.
- 6 (Optional) Click **Advanced Settings** and select the following options:
 - **The group to add the managed device to**
 - **The settings template to use on the managed device**
 - **Installer size**
 - **Proxy server**
- 7 When the installer is downloaded, run it on the devices you want to protect.

NOTE If a restart is required, a notification displays after the install.

TO SEND AN ANTIVIRUS INSTALL LINK BY E-MAIL

- 1 Start your **Avast Business Cloud Management Console**.
- 2 On the **Dashboard** or **Devices** page, click **Download antivirus**.
- 3 Click **share download link**.
- 4 Click **Copy URL**.
- 5 Send the URL to the target device.

After a successful install through the installer or a download link, the application automatically scans and protects the device. The software then sends a message back to the Avast Business Cloud 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 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.


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.

AUTOMATICALLY DEPLOYING AVAST ANTIVIRUS TO MULTIPLE DEVICES REMOTELY

Avast Business Cloud Management Console makes it easy to automatically find devices in your Active Directory that aren't already protected by Avast Antivirus. Once you've found the devices, you can choose which ones you want to deploy Avast Antivirus to, and deploy Avast Antivirus to them remotely, with only a few clicks.

While you are going through the procedure of automatically deploying Avast Antivirus remotely, the

Remote Deployment  button is available on the Navigation menu so you can navigate to the Remote Deployment pages.

REQUIREMENTS

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

- Avast Business Cloud Management Console 6.0 or higher
- Avast Business 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)

RESTRICTIONS



Automatically deploying to multiple devices remotely works only for devices that do not have Avast Antivirus currently installed. To use automatic remote deployment for devices that already have Avast Antivirus installed, you must first uninstall Avast Antivirus. Then, when your Active Directory is scanned, the Remote Installer automatically finds the devices that don't have Avast Antivirus installed and deploys Avast Antivirus, through your Master Agent.

TO AUTOMATICALLY DEPLOY AVAST ANTIVIRUS TO DEVICES IN YOUR ACTIVE DIRECTORY REMOTELY

Deploying Avast Antivirus automatically to devices in your Active Directory involves four steps:

- Scanning your network
- Selecting the devices
- Defining installer settings
- Deploying to devices

1 (Optional) Remove and uninstall Avast Antivirus from existing devices.

2 Click **Devices** , then the **Plus**  button.

3 Click **Deploy installers remotely**.

4 Click **Begin deployment process**.

- If you don't have a Master Agent available, click the **Add new Master Agent** link and follow the [To set up a device as a Master Agent](#) procedure.
- If you do have Master Agents available, select the one you want to use.

5 In the **Active Directory credentials** section, enter the following:

- **Domain**
- **Username**
- **Password**

6 Click **Scan your network**.

NOTE Wait while the network is scanned.

7 In the **Active Directory Groups** section, navigate to a folder that contains unprotected devices and select the check boxes next to the devices you want to deploy to.

8 Click **Define installer settings**.

9 In the **Select a license** box, select one of your available antivirus licenses.


10 In the **Deploy to a group in Avast Business console** section, do any of the following:

- Select a group.
- (Optional) Select the **Remove other conflicting antivirus products during deployment** check box.
- Select a settings template.

11 Click **Start deployment to devices**.

NOTE Wait while antivirus is deployed to devices.

12 Click **Finish Remote Deployment**.

NOTE Some devices may require a restart for changes to take effect. You can create this task easily by navigating to the **Devices** page  and clicking the **Create a Restart task** link next to any device that has one.

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.

CHAPTER FIVE:

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 Cloud Management Console, as well as being delivered to the e-mail address you set up for your account.

On the Notifications page, you can turn off notification e-mails and define additional e-mail addresses to send e-mail 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 e-mail 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 two types of notification:

- **Security**—Security messages notify you about detected and blocked threats and remind you to update your software.
- **Network**—These messages give you warnings and information about the status of devices in your network.

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

SECURITY NOTIFICATIONS

- **Threat was blocked**—Threat was blocked before it accessed the device. Investigate the blocked threat.
- **Threat was blocked and moved to the chest**—Threat was blocked before it accessed the device and moved to the virus chest. View the virus chest to identify the threat.
- **Threat was found while scanning**—Threat was found on the device during a scan. Investigate the threat.
- **Threat was found and moved to the chest**—Threat was found on the device during a scan and moved to the virus chest. View the virus chest to identify the threat.
- **Virus database is out of date**—Update Avast Antivirus.

NETWORK NOTIFICATIONS

- **Antivirus application is outdated**—Update Avast Antivirus.
- **Device offline for an extended period**—Verify the device is switched on and connected to the network.
- **Devices are awaiting activation**—Activate devices now.
- **Device was removed**—Verify the devices were removed intentionally.
- **Newly added device is awaiting activation**—Activate new devices now.
- **Other technical issues**—Investigate the issue.

TO MARK ALL NOTIFICATIONS AS READ

- 1 Click **Notification** .
- 2 Click **Mark all as read**.

NOTIFICATION DELIVERY



You can turn on and off notifications within the application. They appear on the Notifications page.

You can also receive batch notifications at e-mail addresses. If in-app notifications are turned on, you will only receive a batched e-mail notification if notifications are not read in the app. You can receive batch e-mail notifications daily or weekly.


Notifications expire after 30 days of inactivity. Activity includes:

- Delivery of the notification.
- Reading the notification.
- Any action being taken on the notification.


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 SETTINGS FOR E-MAIL NOTIFICATIONS

- 1 Click **Notification** .
- 2 Click **Notification settings**.
- 3 In each of the sections, do one of the following:
 - If in-app notifications are turned off, select an option from the **Send e-mail notification** list.
 - If in-app notifications are turned on, select an option from the **If not read send e-mail notification list**.

TO CHOOSE WHO RECEIVES E-MAIL NOTIFICATIONS

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

CHAPTER SIX:

DEVICES

The Devices page helps you manage your devices and groups. On this page, you can configure 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.**
Update your virus definitions.
- **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 **Show Filter Panel** .

NOTE Skip Step 2 if you see the **Reset all filters and hide filter panel** button.



- 3 To find devices, select one or more of the following:
 - The status of the device.
 - The operating system of the device.
 - The tier of license the device has
 - If the device is a Master Agent or local update server.
 - When the device was last seen.
- 4 To find devices that are running certain tasks, select one or more of the following:
 - The type of task the device is running.
 - The interval of the task the device is running.


ASSIGNING A SETTINGS TEMPLATE TO DEVICES

You can assign a settings template to an individual device, or to a group of devices.



Settings templates control the level of active protection, data protection, and identity protection that devices get from Avast Antivirus, and additional settings. For more information, see [Device Settings](#).

TO ASSIGN A SETTINGS TEMPLATE TO A DEVICE

- 1 Click **Devices** .
- 1 Select the check boxes of the devices you want to assign a new settings template to.
- 2 Do one of the following:
 - Click **Actions, Change Settings Template**.
 - Click the **More** button  next to the device, then click **Change Settings Template**.
- 3 Select a settings template.
- 4 Click **Change Settings Template**.

NOTE You can also change a device's settings template using the Groups panel. If the Groups panel is not expanded, click **Expand panel** .

TO ASSIGN A SETTINGS TEMPLATE TO A GROUP OF DEVICES

- 1 Click **Devices** .
- 2 If the **Groups** panel is not expanded, click **Expand panel** .
- 3 Select the check box of a group.
- 4 Click **Actions, Change Settings Template**.
- 5 Select a settings template.
- 6 Click **Change Settings Template**.



REMOVING AND UNINSTALLING DEVICES

You can remove and uninstall a device remotely from the Avast Business Cloud 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 Cloud Console.

- 1 Click **Devices** .
- 2 Select the check boxes of the devices you want to uninstall.
- 3 Do one of the following:
 - Click **Actions**.
 - Click the **More** button  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.

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 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 Select an option in the **Group settings** list.
- 7 (Option) To update devices in the group from Avast servers, even if the settings template gets virus definitions and program updates from local servers, select the **Always update from Avast servers** check box.
- 8 Click **Add group**.

TO ADD A SUB-GROUP



Sub-groups inherit the properties of their parent groups by default, but you can edit the group at any time.

- 1 Click **Devices** .
- 2 If required, click the **Groups** panel.
- 3 Click the **More** button  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 **More** button  next to a group, then click **Edit group**.
- 4 Make your changes.
- 5 Click **Save group**.

TO DELETE A GROUP

- 1 Click **Devices** .
- 2 If required, click the **Groups** panel.
- 3 Click the **More** button  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 assumes 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 Do one of the following:
 - To include multiple devices, select the check boxes of the devices you want to add. Then click **Actions, Move to group**.
 - For a single device, click the **More** button  next to a device, then click **Move to group**.
- 3 Click the group to add the device to.
- 4 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 the same time.



TO CHANGE THE SETTINGS TEMPLATE OF A DEVICE

NOTE This procedure may require the device to restart.

- 1 Click **Devices** .
- 2 Do one of the following:
 - To include multiple devices, select the check boxes of the devices. Then click **Actions, Change Settings Template**.
 - For a single device, click the **More** button  next to a device, then click **Change Settings Template**.
- 3 Select a template.
- 4 Click **Change settings template**.


TO CHANGE THE LICENSE EDITION OF A DEVICE

NOTE This procedure requires the device to restart.

- 1 Click **Devices** .
- 2 Do one of the following:
 - To include multiple devices, select the check boxes of the devices. Then click **Actions, Change license**.
 - For a single device, click the **More** button  next to a device, then click **Change license**.
 - Barcelona, Spain Click **Apply** for the license you want to change to.

TO ACTIVATE A SELECTED DEVICE

NOTE This procedure requires the device to restart.

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

TO UNSELECT DEVICES

- On the Devices page, 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 Do one of the following:
 - To include multiple devices, select the check boxes of the devices you want to uninstall, then click **Actions, Remove and uninstall**.
 - For a single device, click the **More** button  next to a device, then click **Remove and uninstall**.
- 3 Click **Yes**.



CREATING TASKS ON THE DEVICE PAGE

You can create tasks on the Device page, or on the Tasks page. When you create tasks on the Device page, you can choose the devices that the task runs on; when you create a task on the Tasks page, the task will run on all devices.



TO SCAN A DEVICE

- 1 Click **Devices** .
- 2 Do one of the following:
 - To include multiple devices, select the check boxes of the devices you want to include in the task, then click **Actions, Create a task**.
 - For a single device, click the **More** button  next to a device, then 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 whether 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 (Optional) Select **Schedule the scan** and set the **Frequency** and **Schedule start date and time**.
- 7 (Optional) Type a **Custom name** for the scan.
- 8 Click **Start Scan**.



TO SEND A MESSAGE TO A DEVICE

- 1 Click **Devices** .
- 2 Do one of the following:
 - To include multiple devices, select the check boxes of the devices you want to include in the task, then click **Actions, Create a task**.
 - For a single device, click the **More** button  next to a device, then click **Create a task**.
- 3 Click **Send a message to the device**.
- 4 Type a message to your users.
- 5 (Optional) Select **Schedule the message** and set the **Frequency** and **Schedule start date and time**.
- 6 (Optional) Type a **Custom name**.
- 7 Click **Send message**.

TO UPDATE A DEVICE

- 1 Click **Devices** .
- 2 Do one of the following:
 - To include multiple devices, select the check boxes of the devices you want to include in the task, then click **Actions, Create a task**.
 - For a single device, click the **More** button  next to a device, then click **Create a task**.
- 3 Click **Update device**.
- 4 Do one of the following:
 - To update Avast Business Antivirus, select the **Program update** check box.
 - To update virus definitions, select the **Virus definition update** check box.
- 5 (Optional) Select **Schedule the update** and set the **Frequency** and **Schedule start date and time**.
- 6 (Optional) Type a **Custom name** for the update.
- 7 Click **Update**.

TO SHUT DOWN OR RESTART A DEVICE

- 1 Click **Devices** .
- 2 Do one of the following:
 - To include multiple devices, select the check boxes of the devices you want to include in the task, then click **Actions, Create a task**.
 - For a single device, click the **More** button  next to a device, then click **Create a task**.
- 3 Click **Shutdown device**.
- 4 Select one of the following check boxes:
 - **Restart device**
 - **Shutdown device**
- 5 (Optional) 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 (Optional) Select **Schedule the shutdown** and set the **Frequency** and **Schedule start date and time**.
- 8 (Optional) Type a **Custom name** for the shutdown task.
- 9 Click **Shutdown**.


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.
- Override the local update server.
- Change the license edition.
- 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 [Configuring Avast Business Antivirus with settings templates](#) section.

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 [Tasks](#).

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 **More** button  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**

CHAPTER SEVEN:

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.

On 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 only run on their assigned devices when the device is turned on and 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.
- 3 Click any of the following tabs:
 - **Overview**
 - **Devices**
 - **Settings**


TO SEARCH FOR A TASK

- 1 Click **Tasks** .
- 2 In the **Task name** box, type part of the name of the task you're searching for.


The Task list updates as you type.

NOTE To clear the search, click  in the search box.


TO FILTER TASKS

- 1 Click **Tasks** .
- 2 If the **Filters** button displays, click it.
- 3 Select any of the following:
 - An interval.
 - A task type.
 - The status of the device the task runs on.
 - The operating system of the device the task runs on.
 - If the device the task runs on is a Master Agent or local update server.
 - When the device the task runs on was last seen.

TO UNSELECT TASKS

- 1 Click **Tasks** .
- 2 With at least one task selected, click **Actions, Unselect all tasks**.

TO STOP OR DELETE A TASK

- 1 Click **Tasks** .
- 2 Select 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.

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**—Scans the most vulnerable areas of your device.
- **Full system scan**—Covers all data, programs and storage but will take longer to run.
- **Removable media scan**—Scans CDs/DVDs, external drive or USB drives that you have attached to your device.
- **Custom scan**—Provides the capability to create and save scans based on a range of scan parameters specific to your devices and environment.
- **Boot-time scan**—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 run on your network at non-peak times so that your users' work is not 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 (Optional) Select **Schedule the scan** and set the **Frequency** and **Schedule start date and time**.
- 6 (Optional) Type a **Custom name** for the scan.
- 7 Choose the options for your scan.
- 8 Click **Start Scan**.

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 (Optional) Select **Schedule the message** and set the **Frequency** and **Schedule start date and time**.
- 6 (Optional) Type a **Custom name**.
- 7 Click **Send message**.

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 devices 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, select the **Program update** check box.
 - To update virus definitions, select the **Virus definition update** check box.
- 5 (Optional) Select **Schedule the update** and set the **Frequency** and **Schedule start date and time**.
- 6 (Optional) Type a **Custom name** for the update.
- 7 Click **Update**.

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.

This procedure shuts down all devices managed by the Avast Business Cloud Console. If you want to shut down individual devices, [create a task from the Devices page](#).

TO SHUT DOWN ALL MANAGED DEVICES

- 1 Click **Tasks** .
- 2 Click **Create a task**.
- 3 Click **Shutdown device**.
- 4 Select one of the following check boxes:
 - **Restart device**
 - **Shutdown device**
- 5 (Optional) Type a message to notify your users before the restart or shutdown.
- 6 Choose an option in the **Specify when the message is displayed** box.
- 7 (Optional) Select **Schedule the shutdown** and set the **Frequency** and **Schedule start date and time**.
- 8 (Optional) Type a **Custom name** for the shutdown task.
- 9 Click one of the following:
 - **Restart**
 - **Shutdown**
 - **Schedule restart**
 - **Schedule shutdown**

CHAPTER EIGHT:

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 settings 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 Cloud 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 settings tab of the settings template, you can choose to keep your Avast software and the threats library updated either automatically or manually.

By default, these settings are configured to update automatically, ensuring 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

CONFIGURING AVAST BUSINESS ANTIVIRUS WITH SETTINGS TEMPLATES

To control Avast Business Antivirus on your devices:

- Create a settings template
- Apply a template to device groups

A settings template is a group of system settings that determines how Avast Business Antivirus is configured on devices. Once you have configured the settings in the settings template, you then apply the template to a device or device group.

A single settings template contains settings for Workstations, Servers, and Mac OS X. You don't need to create separate Windows Workstation, Windows Server, and Mac OS X policies.

Different shields and tools are available for Windows Workstations, Windows Servers, and Mac OS X devices. The following table shows which shields and tools are available for each:

SHIELD/TOOL	WORKSTATION	SERVER	MAC OS X
FILE SHIELD	X	X	X
MAIL SHIELD	X	X	X
WEB SHIELD	X	X	X
REAL SITE	X	X	
ANTI-SPAM	X	X	
FIREWALL	X		
BEHAVIOR SHIELD	X		
WEBCAM SHIELD	X		
SECURITY BROWSER EXTENSION	X		
EXCHANGE		X	
SHAREPOINT		X	
BROWSER CLEANUP	X		
DATA SHREDDER	X	X	
SANDBOX	X	X	
SECURELINE VPN	X		
WI-FI INSPECTOR	X	X	
RESCUE DISK	X	X	
PASSWORDS	X		
SOFTWARE UPDATER	X		

INSTALLING AND UNINSTALLING ACTIVE PROTECTION COMPONENTS


Active protection components are the Avast Business Antivirus features that protect you in real-time. Most of these features are installed with Avast Business Antivirus, but others you need to install before use. You can uninstall them at any time, and install any missing features that you need.

Mac OS X protection components cannot be installed or uninstalled, but can be turned off.

- 1 Click **Device Settings**, then click the name of a settings template.
- 2 Click any of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 3 Click the **Active Protection** tab.
- 4 Click the **Install this component link** next to the component you want to install.
- 5 Click **I understand, install component**.
- 6 Click **Apply Changes**.

TO UNINSTALL AN ACTIVE PROTECTION COMPONENT

- 1 Click **Device Settings**, then click the name of a settings template.
- 2 Click any of the following tabs:

- **Windows Workstation**
 - **Windows Server**
- 3 Click the **Active Protection** tab.
 - 4 Click  next to the component you want to uninstall, then click **Uninstall this component**.
 - 5 Click **I understand, uninstall component**.
 - 6 Click **Apply Changes**.


TO CREATE A SETTINGS TEMPLATE

- 1 Click **Device Settings**, then click the name of a settings template.
- 2 Click any of the following tabs:
 - **Windows Workstation**
 - **Server Settings**
- 3 Click the **Active Protection** tab, then any of the following:
 - [Configuring settings templates: Enabling and configuring File Shield for Windows Workstations and Windows Servers](#)
 - [Configuring settings templates: Enabling and configuring Mail Shield for Windows Workstations and Windows Servers](#)
 - [Configuring settings templates: Enabling and configuring Web Shield for Windows Workstations and Windows Servers](#)
 - [Configuring settings templates: Protecting Against DNS Hijacking with Real Site for Windows Workstations and Windows Servers](#)
 - [Configuring settings templates: Enabling and configuring Anti-spam for Windows Workstations and Windows Servers](#)
 - [Configuring settings templates: Enabling and configuring Data Shredder for Windows Workstations and Windows Servers](#)
 - [Configuring settings templates: Configuring Sandbox for Windows Workstations and Windows Servers](#)
 - [Configuring settings templates: Wi-Fi Inspector for Windows Workstations and Windows Servers](#)
 - [Configuring settings templates: Rescue Disk for Windows Workstations and Windows Servers](#)
- 4 On the **Antivirus settings** tab, follow the [Configuring settings templates: Configuring Antivirus Settings for Windows Workstations and Windows Servers](#).
- 5 On the **Troubleshooting** tab, follow the [Configuring settings templates: Configuring Troubleshooting Settings for Windows Workstations and Windows Servers](#).
- 6 Follow the [Configuring settings templates: Configuring General Settings](#) procedure.
- 7 Click the **Windows Workstation** tab, then do any of the following:
 - [Configuring settings templates: Enabling and configuring Firewall for Windows Workstations](#)
 - [Configuring settings templates: Enabling Behavior Shield for Windows Workstations](#)
 - [Configuring settings templates: Enabling and configuring Webcam Shield for Windows Workstations](#)
 - [Configuring settings templates: Enabling Security Browser Extension for Windows Workstations](#)
 - [Configuring settings templates: Enabling Browser Cleanup for Windows Workstations](#)

- [Configuring settings templates: SecureLine VPN for Windows Workstations](#)
 - [Configuring settings templates: Password Protection for Windows Workstations](#)
 - [Configuring settings templates: Software Updater for Windows Workstations](#)
- 8 Click the **Windows Server** tab, then do any of the following:
- [Configuring settings templates: Enabling and configuring Exchange Server Protection for Windows Servers](#)
 - [Configuring settings templates: Enabling SharePoint Server Protection for Windows Servers](#)
- 9 Click the **Mac OS X** tab, then do any of the following:
- [Configuring settings templates: Enabling and configuring File Shield for Mac OS X](#)
 - [Configuring settings templates: Enabling and configuring Mail Shield for Mac OS X](#)
 - [Configuring settings templates: Enabling and configuring Web Shield for Mac OS X](#)
 - [To Configure Settings Template General Settings for Mac OS X](#)
- 10 Click **Close**.



After you configure your settings template, the next step is [Assigning a settings template to a device or group of devices](#).

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 **More** button  at the right of a template and click **Delete**.
- 3 Click **Delete**.

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

You can't change the groups or devices assigned to a template from the Device settings page. If you want to assign a group or device, visit the [Devices page](#).

- 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, select a check box and click **Change settings**.

CONFIGURING SETTINGS TEMPLATES: ENABLING AND CONFIGURING FILE SHIELD FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS



File Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X


For Mac OS X settings, see [Configuring settings templates: Enabling and configuring File Shield for Mac OS X](#).

File Shield is the main layer of active protection in Avast Business Antivirus. It scans programs and files saved on devices for malicious threats in real-time before allowing them to be opened, run, modified, or saved. If malware is detected, File Shield prevents the program or file from infecting devices.

We strongly recommend you keep this shield turned on at all times and only make configuration changes if you have an advanced understanding of malware protection principles.

- 1 Click **Device settings** .
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 In the **Shields** section, move the slider  to enable **File Shield**.
- 6 Click **Apply Changes**.

TO CONFIGURE WHEN FILE SHIELD SCANS FILES

- 1 Click **Device settings** .
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **File Shield** section.
- 6 Click the **Scan behavior** tab.
- 7 In the **Scan when executing** section, select any of the following:
 - **Scan programs when executing**
 - **Scan scripts when executing**
 - **Scan libraries when executing**
- 8 In the **Scan when opening** section, select any of the following:
 - **Scan documents when opening**
 - **Scan documents with custom extensions**, then type the custom extensions to scan.

NOTE You can use wildcard characters. For information on using wildcard characters, see [About file paths in Settings Templates](#).

- **Scan all files**
- 9 In the **Scan when attaching** section, click any of the following:
 - **Scan auto-run items when removable media is attached**
 - **Scan diskette boot sectors on access**
 - 10 In the **Scan when writing** section, click any of the following:
 - **Scan files when writing**
 - **Scan files with default extensions**
 - **Scan all files**
 - **Scan files with custom extensions**, then type the custom extensions to scan.

NOTE You can use wildcard characters. For information on using wildcard characters, see [About file paths in Settings Templates](#).

- **Do not scan files on remote shares**
 - **Do not scan files on removable media**
- 11 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: EXCLUDING FILES, FILE TYPES, AND LOCATIONS FROM FILE SHIELD

File Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring File Shield for Mac OS X](#).

You can modify the list of locations that are not scanned. Exclusions are files and locations that will not be scanned. Enable the check boxes to define when the file is not scanned: when the file is read, written to, or executed. You can use wildcards in file names, paths, and extensions, such as ? to represent a single character, and * to represent a character string.


Exclusions that you specify on this screen only apply to File Shield and do not affect any other scans or Shields. To exclude a location from all Avast Business Antivirus scans, see [Configuring settings templates: Excluding Files, Folders, or URLs from Scans and Shields for Windows Workstations and Windows Servers](#).

For information on how to use file paths, see [About File Paths in Settings Templates](#).

TO EXCLUDE FILES, FILE TYPES, AND LOCATIONS FROM FILE SHIELD

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **File Shield** section.
- 6 Click the **Exclusions** tab.
- 7 Select any of the following check boxes:
 - **R**—Read
 - **W**—Write
 - **X**—Execute
- 8 Type a file name, path, or extension, then click **Add**.
- 9 Repeat step 8 until all your chosen file names, paths, and extensions are excluded.
- 10 Click **Apply Changes**.

TO REMOVE A FILE SHIELD EXCLUSION

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **File Shield** section.
- 6 Click the **Exclusions** tab.
- 7 Next to the exclusion you want to remove, click .
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING ACTIONS TO TAKE WHEN FILE SHIELD FINDS A VIRUS, POTENTIALLY UNWANTED PROGRAMS, OR SUSPICIOUS FILE

File Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring File Shield for Mac OS X](#).

You can specify what actions to take when a virus, potentially unwanted programs, or suspicious file is detected.

TO CONFIGURE ACTIONS TO TAKE WHEN FILE SHIELD FINDS A VIRUS, POTENTIALLY UNWANTED PROGRAMS, OR SUSPICIOUS FILE

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **File Shield** section.
- 6 Click the **Actions** tab.
- 7 Click one of the following tabs:
 - **Virus**
 - **PUP**
 - **Suspicious**
- 8 Select an option in the **Choose what action Avast will perform after finding a virus** box.
- 9 If applicable, select an option in the **if the action fails, use** box.
- 10 In the **Options** section, select any of the following check boxes:

- **Show notifications for actions**
- **Perform the selected action when the system restarts**

11 In the **Processing Infected Archives** section, select one of the following check boxes:

- **Try to remove only the packed file from the archive; if it fails, do nothing**
- **Try to remove only the packed file; if it fails, remove the whole containing archive**
- **Always remove the whole archive**

12 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING WHICH ARCHIVE FILES AVAST TRIES TO UNPACK DURING A FILE SHIELD SCAN

File Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring File Shield for Mac OS X](#).

You can choose which archive (packer) files Avast Business Antivirus should attempt to unpack during the scanning process.

File Shield is better able to analyze files for malware when files are unpacked. Unpacking a file is the same as extracting a file from an archive. Original archives, including the files contained within, remain intact when being processed by File Shield.

To configur which archive files Avast tries to unpack during a File Shield scan

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **File Shield** section.
- 6 Click the **Packers** tab.
- 7 Do one of the following:
 - Select **All packers**.
 - Select the check boxes of individual packers.
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING AVAST ANTIVIRUS FILE SHIELD SENSITIVITY

File Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring File Shield for Mac OS X](#).

You can define the following settings for File Shield:

Heuristics enable Avast Business Antivirus to detect unknown malware by analyzing code for commands that may indicate malicious intent. Specify your preferences for the following options:

- Indicate your preferred level of heuristic sensitivity. The default setting is Normal. With higher sensitivity, Avast Business 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.

Enable the **Test whole files** check box if you want the scan to analyze entire files rather than only the parts typically affected by malicious code. When this option is enabled, the scan is slower but more thorough.

Enable the **Scan for potentially unwanted programs (PUPs)** check box if you want the scan to look for programs that are stealthily downloaded with other programs and typically perform unwanted activity.

NOTE The more options you enable and the higher the sensitivity you set, the more thoroughly File Shield scans your devices. With higher sensitivity, false-positive detections are more likely and more resources are consumed.

TO CONFIGURE AVAST ANTIVIRUS FILE SHIELD SENSITIVITY

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **File Shield** section.
- 6 Click the **Sensitivity** tab.
- 7 Select an option in the **Heuristics Sensitivity** box.
- 8 Select any of the following check boxes:
 - **Use code emulation**
 - **Test whole files**
 - **Scan for potentially unwanted programs (PUPs)**

- 9 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: GENERATING AND CONFIGURING FILE SHIELD REPORTS

File Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring File Shield for Mac OS X](#).

You can generate a report of scans and customize the content of the report.

Report files are saved in one of the following locations:

- Windows 10, Windows 8.1, Windows 8, Windows 7, or Windows Vista:
C:\ProgramData\Avast Software\Avast\report
- Windows XP: C:\Documents and Settings\All Users\Application Data\Avast Software\Avast\report

TO GENERATE AND CONFIGURE FILE SHIELD REPORTS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **File Shield** section.
- 6 Click the **Report File** tab.
- 7 Select the **Generate Report File** check box.
- 8 Type a name in the **File Name** box.
- 9 Select the **File Type**.
- 10 Select an option in the **If File Exists** box.
- 11 Select any of the **Reported Items** you want to include in the report:
 - **Infected items**
 - **Hard errors**
 - **Soft errors**
 - **OK items**
 - **Skipped items**
- 12 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: ENABLING AND CONFIGURING MAIL SHIELD FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS


Mail Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Mail Shield for Mac OS X](#).

Mail Shield checks incoming and outgoing email messages for viruses and links to malicious websites. This only applies to messages handled by mail management software installed on your computer, such as MS Outlook. If you access your web-based email account via an Internet browser, your devices are protected by other Shields.

TO ENABLE MAIL SHIELD FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 In the **Shields** section, move the slider  to enable **Mail Shield**.
- 6 Click **Apply Changes**.

TO IDENTIFY WHICH MESSAGES MAIL SHIELD PROTECTS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Mail Shield** section.
- 6 Click the **Main Settings** tab.
- 7 Select any of the following check boxes:
 - **Scan inbound mail (POP3, IMAP4)**
 - **Scan outbound mail (SMTP)**
 - **Scan newsgroup messages (NNTP)**
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING NOTES AND WARNINGS FOR EMAILS SCANNED BY MAIL SHIELD

Mail Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Mail Shield for Mac OS X](#).

Configuring behavior settings of Mail Shield lets you add notes and warnings to emails. You can also customize certain settings for Microsoft Outlook only.

The following settings attach notes to the bottom of incoming or outgoing emails:

- **Insert note into clean message (incoming)**—Informs you that the email you received does not contain malware.
- **Insert note into infected message (incoming)**—Informs you that the email you received likely contains malware.
- **Insert note into clean message (outgoing)**—Informs recipients that the email you sent does not contain malware. This option is enabled by default.

The following settings attach notes to the subject line of emails:

- **Mark in subject of mail containing a virus**—Tags emails with the subject line ****VIRUS**** if the email contains malware. You can also specify your own tag in the text box.

TO CONFIGURE NOTES AND WARNINGS FOR EMAILS SCANNED BY MAIL SHIELD

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Mail Shield** section.
- 6 Click the **Behavior** tab.
- 7 Select any of the following check boxes:
 - **Insert note into clean message (incoming)**
 - **Insert note into infected message (incoming)**
 - **Insert note into clean message (outgoing)**
 - **Add a warning to the subject line of infected e-mails.** If you want a custom message, type the warning to add.
- 8 In the **MS Outlook only** section, select any of the following check boxes:
 - **Show splash screen**
 - **Scan files when attaching to e-mail**

- **Scan archived messages when opening**
- **Unread messages only**

9 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: SCANNING SSL CONNECTIONS WITH MAIL SHIELD

Mail Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Mail Shield for Mac OS X](#).

You can enable scanning of emails sent or received using SSL/TLS encrypted connection. If disabled, only emails sent or received via unsecured connections are scanned.

TO SCAN SSL CONNECTIONS WITH MAIL SHIELD

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Mail Shield** section.
- 6 Click the **SSL Scanning** tab.
- 7 Select the **Scan SSL connections** check box.
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CHOOSING THE ACTION TO TAKE WHEN MAIL SHIELD FINDS A VIRUS, POTENTIALLY UNWANTED PROGRAM, OR SUSPICIOUS FILE

Mail Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Mail Shield for Mac OS X](#).

TO CHOOSE THE ACTION TO TAKE WHEN MAIL SHIELD FINDS A VIRUS, POTENTIALLY UNWANTED PROGRAM, OR SUSPICIOUS FILE

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Mail Shield** section.
- 6 Click the **Actions** tab.
- 7 Click one of the following tabs:
 - **Virus**
 - **PUP**
 - **Suspicious**
- 8 Select an option in the **Choose what action Avast will perform after finding a virus** box.
- 9 If applicable, select an option in the **if the action fails, use** box.
- 10 If you want a notification that a virus, PUP, or suspicious file has been dealt with, select the **Show a notification window when action is taken** check box.
- 11 In the **Processing of Infected Archives** section, select one of the following:
 - **Try to remove only the packed file from the archive; if it fails, do nothing**
 - **Try to remove only the packed file; if it fails, remove the whole containing archive**
- 12 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING WHICH ARCHIVE FILES MAIL SHIELD TRIES TO UNPACK

Mail Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Mail Shield for Mac OS X](#).

You can choose which archive (packer) files Avast Business Antivirus tries to unpack during the Mail Shield process. Mail Shield is better able to analyze files for malware when files are unpacked. Unpacking a file is the same as extracting a file from an archive. Original archives, including the files contained within, remain intact when being processed by Mail Shield.

TO CONFIGURE WHICH ARCHIVE FILES MAIL SHIELD TRIES TO UNPACK

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Mail Shield** section.
- 6 Click the **Packers** tab.
- 7 Do one of the following:
 - Click **All packers**.
 - Clear the **All packers** check box, then select the check boxes of individual packers.
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING MAIL SHIELD SCANNING SENSITIVITY

Mail Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Mail Shield for Mac OS X](#).

You can adjust the sensitivity of the Avast Business Antivirus Mail Shield scan.

Heuristics enable Avast Business Antivirus to detect unknown malware by analyzing code for commands which may indicate malicious intent. Specify your preferences for the following options:

- Indicate your preferred level of heuristic sensitivity. The default setting is Normal. With higher sensitivity, Avast Business Antivirus is more likely to detect malware, but also more likely to make false-positive detections (incorrectly identify files as malware).
- Code emulations unpack and test any suspected malware in an emulated environment where the file cannot cause damage to devices. The Use code emulation option is enabled by default.

Enable the **Test whole files** check box if you want the scan to analyze entire files rather than only the parts typically affected by malicious code. When this option is enabled, the scan is slower but more thorough.

Enable the **Scan for potentially unwanted programs (PUPs)** check box if you want the scan to look for programs that are stealthily downloaded with other programs and typically perform unwanted activity.

The more options you enable and the higher the sensitivity you set, the more thoroughly the Shield scans your devices. With higher sensitivity, false-positive detections are more likely and more resources are consumed.

TO CONFIGURE MAIL SHIELD SCANNING SENSITIVITY

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Mail Shield** section.
- 6 Click the **Sensitivity** tab.
- 7 Select an option in the **Heuristics Sensitivity** box.
- 8 Select any of the following check boxes:
 - **Use code emulation**
 - **Test whole files**
 - **Scan for potentially unwanted programs (PUPs)**
- 9 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: GENERATING AND CONFIGURING A MAIL SHIELD REPORT

Mail Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Mail Shield for Mac OS X](#).

You can generate a report of Mail Shield behavior and customize the content of the report.

TO GENERATE AND CONFIGURE MAIL SHIELD REPORTS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Mail Shield** section.
- 6 Click the **Report File** tab.
- 7 Select the **Generate Report File** check box.
- 8 Type a name in the **File Name** box.
- 9 Select the **File Type**.
- 10 Select an option in the **If File Exists** box.
- 11 Select any of the **Reported Items** you want to include in the report:
 - **Infected items**
 - **Hard errors**
 - **Soft errors**
 - **OK items**
 - **Skipped items**
- 12 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: ENABLING AND CONFIGURING WEB SHIELD FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

Web Shield is available for:


- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Web Shield for Mac OS X](#).

Web Shield protects your system from threats while browsing the web. It also prevents malicious scripts from running, even when you are offline.

In Web Shield, you can enable and configure web, HTTPS, and script scanning.

TO ENABLE AND CONFIGURE WEB SHIELD FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 In the **Shields** section, move the slider  to enable **Web Shield**.
- 6 Click **Apply Changes**.

TO CONFIGURE WEB SHIELD SETTINGS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Click the **Main settings** tab.
- 7 In the **Web Scanning** section, select **Enable**, then select any of the following check boxes:
 - **Warn when downloading files with poor reputation**—Sends an alert message when a file with a bad rating or no rating with reputation services is being downloaded.
 - **Scan traffic from well-known browser processes only**—Resolves conflicts with less-known browsers and other web applications that you trust if they are blocked by the Shield while trying to access the Internet. If you enable this option, data traffic from these less-known web applications is authorized and is not scanned for malware by the Shield.
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING THE FILE TYPES WEB SHIELD SCANS

Web Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Web Shield for Mac OS X](#).

You can define which items should be scanned while they are being downloaded from the web. Both file types and MIME types can be scanned.

File types and MIME-types can include wildcard characters * or ?. The asterisk replaces zero or more characters, whereas the question mark replaces a single character. For example:

- To scan both HTM and HTML file types, type htm* into the text box.
- To scan all file types with two characters in a file extension, type ?? into the text box.

IMPORTANT For information on how to use file paths, see [About File Paths in Settings Templates](#).

TO CONFIGURE THE FILE TYPES WEB SHIELD SCANS


- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Click the **Web Scanning** tab.
- 7 To scan every file when downloaded, select the **Scan all files** check box.
- 8 To choose file types to scan, select the **Scan selected file types only** check box, then select one or both of the following:
 - **Scan files with specified extensions**, then type an extension and click **Add**.
 - **Scan files with specified MIME-types**, then type a MIME type and click **Add**.
- 9 Repeat step 8 until all extensions are added.
- 10 (Optional) To not unpack archives even if they have trusted digital signatures, select the **Do not unpack archives with valid digital signatures** check box.
- 11 Click **Apply Changes**.

TO REMOVE A FILE TYPE OR MIME-TYPE FROM WEB SHIELD SCANS

Web Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Web Shield for Mac OS X](#).

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Click the **Web Scanning** tab.
- 7 Next to the file type or MIME-type you want to remove, click  .
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: EXCLUDING URLS, MIME-TYPES, AND PROCESSES FROM WEB SHIELD

Web Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Web Shield for Mac OS X](#).

You can modify the URLs, MIME-types, and processes excluded from scanning.

NOTE Exclusions that you specify on this screen only apply to Web Shield and do not affect any other scans or Shields. To exclude a location from all Avast Business Antivirus scans, see [Configuring settings templates: Excluding Files, Folders, or URLs from Scans and Shields for Windows Workstations and Windows Servers](#).

IMPORTANT For information on how to use file paths, see [About File Paths in Settings Templates](#).

TO EXCLUDE URLS, MIME-TYPES, AND PROCESSES FROM WEB SHIELD

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**


- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Click the **Exclusions** tab.
- 7 Do any of the following:
 - To exclude a URL, in the **Use URLs to Exclude** section, select the **Enable** check box, then type the URL and click **Add**.
 - To exclude a MIME type, in the **Use MIME-types to Exclude** section, select the **Enable** check box, then type the URL and click **Add**.
 - To exclude a process, in the **Use Processes to Exclude** section, select the **Enable** check box, then type the URL and click **Add**.
- 8 Repeat step 7 until all your chosen URLs, MIME-types, and processes are excluded.
- 9 Click **Apply Changes**.

TO REMOVE AN EXCLUSION FROM A FILE, FILE TYPE, OR LOCATION IN WEB SHIELD

Web Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Web Shield for Mac OS X](#).

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Click the **Exclusions** tab.
- 7 Next to the exclusion you want to remove, click  .
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING ACTIONS PERFORMED WHEN WEB SHIELD FINDS A VIRUS, POTENTIALLY UNWANTED PROGRAM, OR SUSPICIOUS FILE

Web Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Web Shield for Mac OS X](#).

You can specify what actions to take when a virus, a potentially unwanted program or a suspicious file is detected.

TO CONFIGURE ACTIONS PERFORMED WHEN WEB SHIELD FINDS A VIRUS, POTENTIALLY UNWANTED PROGRAM, OR SUSPICIOUS FILE

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Click the **Actions** tab.
- 7 Click one of the following tabs:
 - **Virus**
 - **PUP**
 - **Suspicious**
- 8 Select an option in the **Choose what action Avast will perform after finding a virus** box.
- 9 To show a notification when a virus, PUP, or suspicious file is dealt with, select the **Show a notification window when action is taken** check box.
- 10 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING WHICH ARCHIVE FILES WEB SHIELD TRIES TO UNPACK

Web Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Web Shield for Mac OS X](#).

You can choose which archive (packer) files Avast Business Antivirus tries to unpack during the scanning process. Unpacking a file is the same as extracting a file from an archive. Original archives, including the files contained within, remain intact when being processed by the Shield.

TO CONFIGURE WHICH ARCHIVE FILES WEB SHIELD TRIES TO UNPACK

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Click the **Packers** tab.
- 7 Do one of the following:
 - Select **All packers**.
 - Clear the **All packers** check box, then select the check boxes of individual packers.
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING WEB SHIELD SCANNING SENSITIVITY

Web Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Web Shield for Mac OS X](#).

You can adjust the sensitivity of the Avast Business Antivirus Web Shield.

Heuristics enable Avast Business Antivirus to detect unknown malware by analyzing code for commands that may indicate malicious intent. Specify your preferences for the following options:

- Indicate your preferred level of heuristic sensitivity. The default setting is Normal. With higher sensitivity, Avast Business Antivirus is more likely to detect malware, but also more likely to make false-positive detections (incorrectly identify files as malware).
- Code emulations unpack and test any suspected malware in an emulated environment where the file cannot cause damage to your devices. The Use code emulation option is enabled by default.

Enable the **Test whole files** check box if you want the scan to analyze entire files rather than only the parts typically affected by malicious code. When this option is enabled, the scan is slower but more thorough.

Enable the **Scan for potentially unwanted programs (PUPs)** check box if you want the scan to look for programs that are stealthily downloaded with other programs and typically perform unwanted activity.

NOTE The more options you enable and the higher the sensitivity you set, the more thoroughly the Shield scans your devices. With higher sensitivity, false-positive detections are more likely and more resources are consumed.

TO CONFIGURE WEB SHIELD SCANNING SENSITIVITY

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Click the **Sensitivity** tab.
- 7 Select an option in the **Heuristics Sensitivity** box.
- 8 Select any of the following check boxes:
 - **Use code emulation**
 - **Test whole files**
 - **Scan for potentially unwanted programs (PUPs)**

- 9 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: BLOCKING URLS WITH WEB SHIELD

Web Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Web Shield for Mac OS X](#).


Site blocking lets you create a custom list of URLs that users can't visit. This can be useful to prevent users from accessing certain content on the web.

IMPORTANT For information on how to use file paths, see [About File Paths in Settings Templates](#).

TO BLOCK URLS WITH WEB SHIELD

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Click the **Site Blocking** tab.
- 7 Select the **Enable site blocking** check box.
- 8 Type a **URL** and click **Add**.
- 9 Repeat step 8 until you have added all the URLs you want to block.
- 10 Click **Apply Changes**.

TO REMOVE A SITE BLOCK IN WEB SHIELD

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Click the **Site Blocking** tab.
- 7 Next to the block you want to remove, click .
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: EXCLUDING URLS FROM WEB SHIELD SCRIPT SCANNING

Web Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Web Shield for Mac OS X](#).

Script scanning prevents browsers and other applications from running potentially malicious scripts. This includes remote threats from the web and outside sources, local threats downloaded to your hard drive or in the browser cache, and scripts that come from encrypted connections.

NOTES


- Use exclusions only if you are sure the website you want to exclude from scanning is safe.
- Exclusions that you specify on this screen only apply to Web Shield Script Scanning and do not affect any other scans or Shields. To exclude a location from all Avast Business Antivirus scans, see [Configuring settings templates: Excluding Files, Folders, or URLs from Scans and Shields for Windows Workstations and Windows Servers](#).

TO EXCLUDE URLS FROM WEB SHIELD SCRIPT SCANNING

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Click the **Script Exclusions** tab.
- 7 Select the **Enable** check box.
- 8 Type a URL and click **Add**.
- 9 Repeat step 8 until you have added all the URLs you want to exclude.
- 10 Click **Apply Changes**.

TO REMOVE A URL EXCLUSION FROM WEB SHIELD SCRIPT SCANNING

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Click the **Script Exclusion** tab.

- 7 Next to the exclusion you want to remove, click .
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: GENERATING AND CONFIGURING A WEB SHIELD REPORT

Web Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Mac OS X settings, see [Configuring settings templates: Enabling and configuring Web Shield for Mac OS X](#).

You can generate a report of Web Shield scans, and configure the content of the report.

Report files are saved in one of the following locations:

- Windows 10, Windows 8.1, Windows 8, Windows 7, or Windows Vista:
C:\ProgramData\Avast Software\Avast\report
- Windows XP: C:\Documents and Settings\All Users\Application Data\Avast Software\Avast\report

TO GENERATE AND CONFIGURE A WEB SHIELD REPORT

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Click the **Report File** tab.
- 7 Select the **Generate Report File** check box.
- 8 Type a name in the **File Name** box.
- 9 Select the **File Type**.
- 10 Select an option in the **If File Exists** box.
- 11 Select any of the **Reported Items** you want to include in the report:
 - **Infected items**
 - **Hard errors**
 - **Soft errors**
 - **OK items**
 - **Skipped items**
- 12 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: PROTECTING AGAINST DNS HIJACKING WITH REAL SITE FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS


Real Site is available for:

- Windows Workstations
- Windows Servers

Real Site protects against DNS (Domain Name System) hijacking to ensure you get to the actual website you want to visit.

Real Site doesn't have any configurable options, but is available to users in Avast Business Antivirus.

TO PROTECT AGAINST DNS HIJACKING WITH REAL SITE FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 In the **Shields** section, move the slider  to enable **Real Site**.
- 6 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: ENABLING AND CONFIGURING ANTI-SPAM FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

Anti-spam is available for:


- Windows Workstations
- Windows Servers

Anti-spam ensures that the inbox in your mail management software is free from unwanted spam, junk emails, and phishing scams. This feature applies to email clients installed on your devices.

You can configure the active Anti-spam settings in settings templates with features such as:

- the sensitivity of the scan
- the subject line added to suspected spam and phishing messages
- whitelisting domains or recipients of outbound emails
- when to retrieve new rules
- enabling LiveFeed
- Microsoft Outlook features

TO ENABLE ANTI-SPAM FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 In the **Shields** section, move the slider  to enable **Anti-spam**.
- 6 Click **Apply Changes**.

TO CONFIGURE ACTIVE ANTI-SPAM SETTINGS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Anti-spam** section.
- 6 Click the **Main Settings** tab.
- 7 Select an option in the **Sensitivity** box.
- 8 To include a message of the Subject line of spam emails, select the **Mark** check box, then type a message.
- 9 To include a message of the Subject line of phishing emails, select the **Mark** check box, then type a message.
- 10 To whitelist recipients of outbound emails automatically, select one of the following check boxes:
 - **Add recipients of outbound emails to whitelist automatically**
 - **Add only domains of the recipients**
- 11 To update anti-spam rules at regular intervals, select the **Retrieve new rules** check box. In the **Period (in sections)** box, type an interval, in seconds.
- 12 To check all incoming emails against a database of global spam messages before carrying out other checks, select the **Enable LiveFeed** box.
- 13 To change MS Outlook-specific settings, do any of the following:
 - **Automatically move spam messages to the junk folder**
 - **Add entries from address book to whitelist automatically**
- 14 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: ADDING EMAIL ADDRESSES TO THE ANTI-SPAM WHITE LIST

Anti-spam is available for:

- Windows Workstations
- Windows Servers

The White List is a list of senders whose emails are never treated as spam and are always delivered as normal.


TO ADD EMAIL ADDRESSES TO THE ANTI-SPAM WHITE LIST

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Anti-spam** section.
- 6 Click the **White List** tab.
- 7 Type an email address in the **White List** box and click **Add**.

NOTE Type the full email address. Wildcard characters aren't permitted.

- 8 Repeat step 7 until all email addresses are added.
- 9 Click **Apply Changes**.

TO REMOVE AN EMAIL ADDRESS FROM THE ANTI-SPAM WHITE LIST

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Anti-spam** section.
- 6 Click the **White List** tab.
- 7 Next to the exclusion you want to remove, click .
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: ADDING EMAIL ADDRESSES TO THE ANTI-SPAM BLACK LIST

Anti-spam is available for:

- Windows Workstations
- Windows Servers

The Black List is a list of senders whose emails are always treated as spam.


TO ADD EMAIL ADDRESSES TO THE ANTI-SPAM BLACK LIST

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Anti-spam** section.
- 6 Click the **Black List** tab.
- 7 Type an email address in the **Black List** box and click **Add**

NOTE Type the full email address. Wildcard characters aren't permitted.

- 8 Repeat step 7 until all email addresses are added.
- 9 Click **Apply Changes**.

TO REMOVE AN EMAIL ADDRESS FROM THE ANTI-SPAM BLACK LIST


- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Anti-spam** section.
- 6 Click the **Black List** tab.
- 7 Next to the exclusion you want to remove, click .
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: ENABLING AND CONFIGURING FIREWALL FOR WINDOWS WORKSTATIONS

Firewall is available for Windows Workstations.

Firewall monitors all network traffic between devices and the outside world to protect you from unauthorized communication and intrusions.

TO ENABLE FIREWALL

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 In the **Shields** section, move the slider  to enable **Firewall**.
- 6 Click **Apply Changes**.

TO ASSIGN A PROFILE TO A DEFINED NETWORK

The two profiles you can assign to defined networks are:

- Private (Trusted)—Provides a lower level of security
- Public (Not trusted)—Provides a higher level of security

We recommend you apply the Public profile to all networks that are not your private network, such as when you connect to the Internet in a café or at an airport.

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Firewall** section.
- 6 Click the **Networks** tab.
- 7 Select a default profile for undefined networks in the **Default profile for undefined network** box.

NOTE If you select **Users can choose profile**, then end users can set their own profile for the network.

- 8 If applicable, select the **Override the profile of every network which was already set by the user with** check box.

NOTE This option is available if you chose Private (Trusted) or Public (Not trusted), and lets you override network profiles that end users have defined, replacing their choice with the default profile you chose.

- 9 To define a network, click **Add network**, then type a network name and the MAC address of the network router. Select a profile, then click **Add**.
- 10 Repeat step 9 for all networks you want to add.
- 11 Click **Apply Changes**.

TO DEFINE A NETWORK FOR FIREWALL

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Firewall** section.
- 6 Click the **Networks** tab.
- 7 Click **Add network**.
- 8 In the **Network name** box, type a name for the network.
- 9 In the **MAC address of network router** box, type the network box's MAC address.
- 10 In the **Profile** box, select a profile.
- 11 Click **Apply Changes**.

TO OVERRIDE USER-DEFINED FIREWALL RULES

Selecting this option lets you control all Firewall rules from Avast Business Console.

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Firewall** section.
- 6 Click the **Rules** tab.
- 7 Select the **Control all rules via the web console** check box.
- 8 Click **Apply Changes**.

TO DEFINE FIREWALL PROFILE SYSTEM RULES

We recommend you only change system rules if you have advanced knowledge of firewall concepts or for troubleshooting purposes. Firewall is already configured to provide the appropriate firewall protection for most uses.

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Firewall** section.
- 6 Click the **Rules** tab.
- 7 Click the **System Rules** tab.
- 8 In each of the following sections, select **Enabled**, **Disabled**, or **Decide based on packet rules**:
 - **Allow Windows File and Printer Sharing**—Authorizes other devices in the network to access shared folders and printers on devices.
 - **Allow remote desktop connections to this computer**—Authorizes other devices in the network to remotely access and control devices when the Remote Desktop service is enabled.
 - **Allow incoming ping and trace requests (ICMP)**—Authorizes incoming Internet Control Message Protocol messages. ICMP is typically used by system tools, such as ping or tracert commands, for diagnostic or control purposes when troubleshooting connectivity issues.

- **Allow outgoing ping and trace requests (ICMP)**—Authorizes outgoing Internet Control Message Protocol messages. ICMP is typically used by system tools, such as ping or tracert commands, for diagnostic or control purposes when troubleshooting connectivity issues.
- **Allow IGMP traffic**—Authorizes multicast communication using the Internet Group Management Protocol, which is required by some media streaming services for more efficient use of resources during activities such as video streaming and gaming.
- **Allow multicast traffic**—Authorizes applications and services for media streaming when distributing content to groups of multiple recipients in a single transmission, which is necessary for activities such as video-conferencing.
- **Allow DNS**—Authorizes communication with Domain Name Servers which enables devices to recognize the IP addresses of the websites you visit.
- **Allow DHCP**—Authorizes communication using the Dynamic Host Configuration Protocol to automatically provide network devices and devices with IP addresses and other related configuration information such as the subnet mask and default gateway.
- **Allow VPN connections via PPTP**—Authorizes connections to Virtual Private Networks based on the Point-to-Point Tunneling Protocol. This protocol is known to present numerous security risks.
- **Allow VPN connections via L2TP-IPSec**—Authorizes connections to Virtual Private Networks based on a more secure combination of the Layer 2 Tunneling Protocol and Internet Protocol Security in comparison with the older Point-to-Point Tunneling Protocol.
- **Allow stealth mode for public networks**—prevents attackers from uncovering information about devices and running services when your Firewall is in Public mode, which is the Network profile you should set when you are connected to a public network, such as in a cafe or at an airport.

9 Click **Apply Changes**.

TO DEFINE FIREWALL APPLICATION RULES

Firewall is available for Windows Workstations.

IMPORTANT We recommend you only change application rules if you have advanced knowledge of firewall concepts or for troubleshooting purposes. Firewall is already configured to provide the appropriate firewall protection for most uses.

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Firewall** section.
- 6 Click the **Application Rules** tab.

TO DEFINE A DEFAULT FIREWALL RULE FOR APPLICATIONS

You can define a default rule for applications that don't have a specific rule defined. The default rule is applied to any application that doesn't appear in the list on this page.

- 1 On the **Application Rules** tab, select an option in **For applications with no defined rules, allow the following:**
 - **Auto-decide**—Firewall allows connections with verified applications, but blocks connections from unknown or suspicious applications.
 - **All connections**—Firewall allows all connections automatically.
 - **No connections**—Firewall blocks all connections automatically.
 - **Ask user**—Firewall asks the end user if they want to allow or block the connection.
- 2 Click **Apply Changes**.

TO APPLY A FIREWALL CONNECTION RULE FOR AN APPLICATION

You can apply one of the existing Firewall connection rules to an application. If you want to define a custom connection, follow the [To create a custom Firewall connection rule for an application](#) procedure.

- 1 On the **Application Rules** tab, click **Add application rule**.
- 2 In **Application name** box, type a name for the rule.
- 3 In the **Application path** box, type the path to the application, including the application's file extension. For example, `C:\Program Files\app.exe`.

NOTE To see variables you can use in the application path, click **Show system path variables**.

- 4 Select one of the following options in **Allow Connections:**
 - **All connections**—Allows all incoming and outgoing connections.
 - **Internet out only**—Allows only outgoing connections to the internet.
 - **No connections**—Does not allow any connections.
- 5 Click **Save application rule**.

TO CREATE A CUSTOM FIREWALL CONNECTION RULE FOR AN APPLICATION

When you create a custom Firewall connection rule for an application, three default rules are provided for you:

- **Internet Out**—Allows TCP and UDP protocols out.
- **Internet In**—Allows TCP and UDP protocols in.
- **Default Rule**—Blocks all protocols, out and in, unless a specific rule allows the protocol to communicate. For example, this rule is applied to ICMPv6 by default, blocking ICMPv6 from communicating either in or out. TCP and UDP would be blocked by this rule, however, the other two rules supersede this rule and allow them to communicate.


You can edit or disable any of these three rules, and you can also create additional rules for other protocols.

- 1 On the **Application Rules** tab, click **Add application rule**.
- 2 In **Application name** box, type a name for the rule.
- 3 In the **Application path** box, type the path to the application, including the application's file extension. For example, `C:\Program Files\app.exe`.

NOTE To see variables you can use in the application path, click **Show system path variables**.

- 4 In **Allow connections**, select **Custom**.
- 5 To add a new rule, click **Add new rule** and do the following:
 - Select the **Enabled** check box.
 - In the **Name** box, type a name.
 - In the **Action** box, select an action.
 - In the **Protocol** box, select a protocol.
 - In the **Direction** box, select a direction.
 - In the **Address** box, type an address.
 - In the **Local Port** box, type a port number.
 - In the **Remote Port** box, type a port number.
 - In the **ICMP Type** box, type the ICMP type.
 - In the **Profile** box, select a profile.
- 6 Click **Save**.
- 7 To edit any of the existing rules, click a rule, make your changes, then click **Save**.
- 8 To disable a rule, click a rule. In the **Enabled** column, clear the check box, then click **Save**.
- 9 Click **Save application rule**.
- 10 Click **Apply Changes**.

NOTE A disabled rule be enabled at any time.

NOTE To delete a rule, next to the rule, click  .

TO DEFINE FIREWALL ADVANCED PACKET RULES

Firewall is available for Windows Workstations.

By default, packet rules are applied in the order they appear on the Advanced packet rules page. You can also reorder these rules to change the order in which they are applied.

IMPORTANT We recommend you only change packet rules if you have advanced knowledge of firewall concepts or for troubleshooting purposes. Firewall is already configured to provide the appropriate firewall protection for most uses.

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Firewall** section.
- 6 Click the **Rules** tab.
- 7 Click the **Advanced packet rules** tab.

TO ADD A NEW PACKET RULE

New packet rules are added to the bottom of the list, giving them the lowest priority.

To change the precedence of a new rule, follow the [To change the order of a Packet Rule](#) procedure.

- 1 Click **Add new rule**.
- 2 Do the following:
 - In the **Enabled** column, select the **Enabled** check box.
 - In the **Name** column, type a name.
 - In the **Action** column, select an option.
 - In the **Protocol** column, select a protocol.
 - In the **Direction** column, select a direction.
 - In the **Address** column, type an address.
 - In the **Local Port** column, type a port number.
 - In the **Remote Port** column, type a port number.
 - In the **ICMP Type** column, type the ICMP type.
 - In the **Profile** column, select a profile.
- 3 Click **Update**.
- 4 Click **Apply Changes**.


TO EDIT A PACKET RULE

You can edit the custom rules you've created. Default packet rules are not available to edit.

- 1 On the **Advanced packet rules** tab, click any custom rule you have created.
- 2 Do any of the following:
 - In the **Enabled** column, select the **Enabled** check box.
 - In the **Name** column, type a name.
 - In the **Action** column, select an option.
 - In the **Protocol** column, select a protocol.
 - In the **Direction** column, select a direction.
 - In the **Address** column, type an address.
 - In the **Local Port** column, type a port number.
 - In the **Remote Port** column, type a port number.
 - In the **ICMP Type** column, type the ICMP type.
 - In the **Profile** column, select a profile.
- 3 Click **Update**.
- 4 Click **Apply Changes**.

TO CHANGE THE ORDER OF A PACKET RULE


You can change the order that custom packet rules are applied. Default packet rules are applied in the order they appear on the Advanced Packet Rules tab.

- 1 On the **Advanced packet rules** tab, click and drag the  button next to any custom rule you have created.
- 2 Drop the rule in a new location in the list.
- 3 Click **Apply Changes**.

TO DISABLE A PACKET RULE

- 1 On the **Advanced packet rules** tab, click any custom rule you have created.
- 2 In the **Enabled** column, clear the check box.
- 3 Click **Save**.
- 4 Click **Apply Changes**.

TO DELETE A PACKET RULE


- 1 On the **Advanced packet rules** tab, click **Delete**  next to any custom rule you have created.
- 2 Click **Save**.
- 3 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: ENABLING BEHAVIOR SHIELD FOR WINDOWS WORKSTATIONS

Behavior Shield is available for Windows Workstations.

Behavior Shield is an additional layer of active protection in Avast Business Antivirus. It monitors all processes on devices in real-time for suspicious behavior that may indicate the presence of malicious code. Behavior Shield works by detecting and blocking suspicious files based on their similarity to other known threats, even if the files are not yet added to the virus definitions database.

TO ENABLE BEHAVIOR SHIELD FOR WINDOWS WORKSTATIONS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 In the **Shields** section, move the slider  to enable **Behavior Shield**.
- 6 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: DEFINING WHAT BEHAVIOR SHIELD DOES WITH SUSPICIOUS PROGRAMS

Behavior Shield is available for Windows Workstations only.

You can configure how Behavior Shield deals with suspicious files that it encounters. You can also set up file locations that are excluded from Behavior Shield.

TO DEFINE WHAT BEHAVIOR SHIELD DOES WITH SUSPICIOUS PROGRAMS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Behavior Shield** section.
- 6 In the **Main Settings** section, select a check box to define how to deal with suspicious programs:
 - **Always ask**
 - **Automatically move detected threats to the Chest**
 - **Automatically move known threats to the Chest**
- 7 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: EXCLUDING LOCATIONS FROM BEHAVIOR SHIELD

Behavior Shield is available for Windows Workstations.

Exclusion paths can include wildcard characters * or ?. The asterisk replaces zero or more characters, whereas the question mark replaces a single character. For example:


- To block all subdomains and domains of a particular website, add *. to the beginning and /* to the end of the website domain, type *.example.com/* into the text box.
- To block any website containing triple "x" anywhere in the URL, type *xxx* into the text box.
- To block all html pages with the filename containing a single character in domain of a particular website, type example.com/? .html into the text box.

NOTE Exclusions that you specify on this screen only apply to Behavior Shield and do not affect any other scans or Shields. To exclude a location from all Avast Business Antivirus scans, see [Configuring settings templates: Excluding Files, Folders, or URLs from Scans and Shields for Windows Workstations and Windows Servers](#).

IMPORTANT For information on how to use file paths, see [About File Paths in Settings Templates](#).

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Behavior Shield** section.
- 6 Type a file location to exclude and click **Add**.
- 7 Repeat step 6 until all locations are added.
- 8 Click **Apply Changes**.

TO REMOVE AN EXCLUSION FROM BEHAVIOR SHIELD

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Behavior Shield** section.
- 6 Next to the exclusion you want to remove, click .
- 7 Click **Apply Changes**.


CONFIGURING SETTINGS TEMPLATES: ENABLING WEBCAM SHIELD FOR WINDOWS WORKSTATIONS

Webcam Shield is available for Windows Workstations.

Webcam Shield prevents applications and malware from accessing webcams without the consent of the user. With Webcam Shield enabled, untrusted applications cannot capture images or videos and send the content to computers to compromise privacy.

NOTE Webcam Shield determines trusted applications based on Avast Reputation Services, which reviews the application's certification information and analyzes how many users have the application installed.

TO ENABLE WEBCAM SHIELD FOR WINDOWS WORKSTATIONS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 In the **Shields** section, move the slider  to enable **Webcam Shield**.
- 6 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING WEBCAM SHIELD FOR WINDOWS

Webcam Shield is available for Windows Workstations.

The settings for Webcam Shield consist of two parts:

- **Mode**—Settings that are applied to all applications
- **Applications**—A list of applications that are blocked or allowed individually. This list is used in Smart and Strict modes, but No mercy mode blocks all applications.

The end user of the device the AV policy is applied to can also configure settings for Webcam Shield. They can choose a mode and create an application permission list.

When you create your AV policy, the mode you choose overrides the mode the user chooses. You also have the option to replace the user's application permission list with your own, which means that the user's application permission list is ignored. However, in No mercy mode, no applications are allowed, not even the applications on the application permission list.

TO SET THE WEBCAM SHIELD MODE

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Webcam Shield** section.
- 6 Select one of the following modes:
 - **Smart** automatically allows trusted applications to access the webcam. If an untrusted application attempts to access the webcam, a notification appears, asking the user to block

or allow the application. After selecting an option, the application appears on the Webcam Shield Settings screen, where the user can view its status and select additional actions.

- **Strict** notifies the user each time any application attempts to access the webcam and allows the user to decide if the application is blocked or allowed. After blocking or allowing an application, the application appears on the Webcam Shield Settings screen where the user can view its status and select additional actions.
- **No mercy** blocks all applications from accessing the webcam. If you choose No mercy, both the user's and AV policy application permission lists are disabled. No applications are allowed to use the webcam.

7 Click Apply Changes.

TO DISABLE USERS' WEBCAM ACCESS LIST

Webcam application permission lists are only valid in Smart and Strict modes.

End users with Avast Antivirus can set up their own list to block and allow certain applications access to their webcam. Administrators can also set up a list. If you want to disable user lists and use the one you configure, select the **Overwrite the application list which was already set by the user** check box.

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Webcam Shield** section.
- 6 Select **Overwrite the application list which was already set by the user**.
- 7 Click **Apply Changes**.

TO CREATE A WEBCAM ACCESS LIST

Webcam access lists are valid in Smart and Strict modes.

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Webcam Shield** section.
- 6 Do either of the following in the **Applications** section:
 - To block webcam access for a specific application, type the path to the application in the box, select the **Blocked** check box, then click **Add**.
 - To allow webcam access for a specific application, type the path to the application in the box, select the **Allowed** check box, then click **Add**.
- 7 Repeat step 6 until you have added all the applications you want to block and allow.

NOTE When you type the path to your application, include the application name and its file extension.

- 8 To remove the setting for a blocked or allowed application, click the **Delete** button next to the application. Once the permission is removed, the application is subject to the mode you chose in the main settings.

NOTE To help you enter the application path, you can use the environment variables in the Application section.

- 9 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: ENABLING SECURITY BROWSER EXTENSION FOR WINDOWS WORKSTATIONS

Security Browser Extension is available for Windows Servers.

Security Browser Extension is a web browser extension designed to improve online security and overall experience when browsing the Internet.


Security Browser Extension doesn't have any configurable options, but is available to users in Avast Business Antivirus.

CONFIGURING SETTINGS TEMPLATES: ENABLING AND CONFIGURING EXCHANGE SERVER PROTECTION FOR WINDOWS SERVERS

Exchange Server protection is available for Windows Servers.

Exchange Server protection protects your Exchange Server from threats.

TO ENABLE EXCHANGE SERVER PROTECTION FOR WINDOWS SERVERS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Server** tab.
- 4 Click the **Active Protection** tab.
- 5 In the **Shields** section, move the slider  to enable **Exchange**.
- 6 Click **Apply Changes**.

TO CONFIGURE EXCHANGE SERVER SCANNING

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Server** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Exchange** section.
- 6 Click the **Scanning** tab.
- 7 Select any of the following check boxes:
 - **Scan messages on-access**
 - **Scan messages in the background**
 - **Enable proactive scanning**
 - **Scan at transport level**
 - **Scan RTF message bodies**
 - **Try to clean infected objects**
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING ACTIONS TO TAKE WHEN EXCHANGE SERVER PROTECTION FINDS UNTESTABLE OR INFECTED ITEMS

Exchange Server protection is available for Windows Servers.

TO CONFIGURE ACTIONS TO TAKE WHEN EXCHANGE SERVER PROTECTION FINDS UNTESTABLE OR INFECTED ITEMS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Server** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Exchange** section.
- 6 Click the **Actions** tab.
- 7 In the **Untestable Items** area, select any of the following check boxes:
 - **Allow full access to the item**
 - **Overwrite the item with a warning**
 - **Delete the whole message**
 - **If possible, change object icon**
- 8 In the **Infected Items** area, select any of the following check boxes:
 - **Allow full access to the item**
 - **Overwrite the item with a warning**
 - **Delete the whole message**
 - **If possible, change object icon**
- 9 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: BLOCKING EMAIL ATTACHMENTS ON EXCHANGE SERVERS

Exchange Server protection is available for Windows servers.

You can choose to block attachments with certain filename masks. Hackers can mask filenames to make malicious files appear to be safe.

TO BLOCK EMAIL ATTACHMENTS ON EXCHANGE SERVERS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Server** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Exchange** section.
- 6 Click the **Blocking** tab.
- 7 Select the **Enable attachment blocking by name** check box.
- 8 Type a filename mask and click **Add**.
- 9 Repeat step 8 until you have added all the attachment filenames you want to block.
- 10 To configure the file that replaces the attachment, type in the following boxes:
 - **Filename replacement**
 - **Replace with**
- 11 Click **Apply Changes**.


CONFIGURING SETTINGS TEMPLATES: ENABLING SHAREPOINT SERVER PROTECTION FOR WINDOWS SERVERS

SharePoint server protection is available for Windows servers.

SharePoint server protection protects your SharePoint Server from threats.

SharePoint server protection doesn't have any configurable options, but is available to users in Avast Business Antivirus.

TO ENABLE SHAREPOINT SERVER PROTECTION FOR WINDOWS SERVERS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Server** tab.
- 4 Click the **Active Protection** tab.
- 5 In the **Shields** section, move the slider  to enable **SharePoint**.
- 6 Click **Apply Changes**.


CONFIGURING SETTINGS TEMPLATES: ENABLING BROWSER CLEANUP FOR WINDOWS WORKSTATIONS

Browser Cleanup is available for Windows Workstations.

Browser Cleanup removes unwanted browser add-ons and toolbars.

Browser Cleanup doesn't have any configurable options, but is available to users in Avast Business Antivirus.

TO ENABLE BROWSER CLEANUP FOR WINDOWS WORKSTATIONS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 In the **Tools** section, move the slider  to enable **Browser Cleanup**.
- 6 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: ENABLING AND CONFIGURING DATA SHREDDER FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS


Data Shredder is available for:

- Windows Workstations
- Windows Servers

Data Shredder lets you irreversibly erase your files or whole drives so that there is no way for anyone to restore and misuse your data.

Random overwrite overwrites your data with random patterns.

TO ENABLE DATA SHREDDER

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 In the **Tools** section, move the slider  to enable **Data Shredder**.
- 6 Click **Apply Changes**.

TO CONFIGURE DATA SHREDDER

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Data Shredder** section.
- 6 Select an option in the **Algorithm Settings** box.
- 7 Type the number of passes you want to perform for random overwrite.
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING SANDBOX FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

Sandbox is available for:

- Windows Workstations
- Windows Servers

Sandbox lets you run applications in a safe virtual environment, isolated from the rest of your device's system. This feature is useful when you want to run suspicious or untrusted applications without risk.

Sandbox storage is a file space completely isolated from the rest of your system and other Sandboxes.

When you run an application in Sandbox, all necessary files are always copied to Sandbox storage where they can be modified as needed without affecting the original files. Any new files created during virtualization are also saved to Sandbox storage.

By default, Sandbox storage is created in the same drive as the original file. If there is insufficient space on the pre-selected drive or you encounter disk performance issues, you may need to select a different drive or browse for another location.

CONFIGURING THE LOCATION OF SANDBOX STORAGE

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Sandbox** section.
- 6 Click the **Sandbox Storage** tab.
- 7 Select a drive by doing one of the following:
 - Select the **The same drive as the modified file** check box.
 - Select the drive check box, then select a drive from the drop box.
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING SANDBOX WEB BROWSER OPTIONS

Sandbox is available for:

- Windows Workstations
- Windows Server

Enabling the **Save trusted downloaded files** setting saves files downloaded while browsing the web inside the virtualized window onto your device. This only applies to download processes that are identified as safe. If you clear this box, downloaded files are deleted when you close the Sandboxed browser.

Enabling exclusions options excludes your personalized data in web browsers from being deleted when you close Sandbox. Enable each box according to your preferences, or enable **All settings and components** to exclude all listed components plus browser extensions and add-ons.

In the **Maintenance** section, you can manage storage settings.

Enabling **Cache web browser files (Sandbox will not be automatically deleted)** saves only the virtualized files for web browsers, improving the browser's performance in Sandbox.

Enabling **Automatically cleanup Sandbox storage** lets you specify how often cached contents are deleted.

TO CONFIGURE SANDBOX WEB BROWSER OPTIONS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Sandbox** section.
- 6 Click the **Web Browsers** tab.
- 7 To save trusted downloaded files outside the Sandbox location, select the **Save trusted downloaded files outside the sandbox** check box.
- 8 To choose settings and components that will not be virtualized when the web browser runs in the Sandbox, select any of the following check boxes:
 - **All settings and components (extensions, add-ons, etc.)**
 - **Bookmarks**
 - **History**
 - **Cookies**

NOTE Excluded settings and components are not deleted when you end the session.

- 9 To save virtualized web browser files, select the **Cache web browser files (sandbox will not be automatically deleted)** check box.
- 10 To clean up Sandbox storage on a recurring basis, with the **Cache web browser files (sandbox will not be automatically deleted)** check box selected, select the **Automatically cleanup sandbox storage** check box, then do one of the following:
 - Select **Once every** and type the number of days between cleanups.
 - Select **Once every** and select a day of the week.

- Select **Every first** and select a day of the week.

NOTE If you select **Every first**, the Sandbox is cleaned up the first of the month, on the first occurrence of the day that you choose in the box. So, if you chose Tuesday in that box, the Sandbox storage is cleaned up the first Tuesday of every month.

11 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: SETTING WHICH APPLICATIONS ARE VIRTUALIZED IN SANDBOX

Sandbox is available for:

- Windows Workstations
- Windows Servers

Virtualizing processes is useful when you want to regularly run questionable applications in Sandbox. You can configure Sandbox to always virtualize a specific application, or any applications contained in a specific folder.


NOTE If Avast Business Antivirus marks a file as suspicious after scanning but you need to use the file regularly, we recommend that you exclude the file from all scans and shields using the [Configuring settings templates: Excluding Files, Folders, or URLs from Scans and Shields for Windows Workstations and Windows Servers](#) procedure, then set the file to be started in Sandbox automatically each time it runs using the [Configuring settings templates: Setting which Applications Are Virtualized in Sandbox](#) procedure.

IMPORTANT For information on how to use file paths, see [About File Paths in Settings Templates](#).

TO SET WHICH APPLICATIONS ARE VIRTUALIZED IN SANDBOX

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Sandbox** section.
- 6 Click the **Virtualized Processes** tab.
- 7 Do any of the following:
 - To automatically virtualize an application, type the path to the application and click **Add**.
 - To automatically virtualize any application in a folder, type the path to the folder and click **Add**.
- 8 Repeat step 7 until all applications and folders are added.
- 9 Click **Apply Changes**.

TO STOP VIRTUALIZING A PROCESS IN SANDBOX

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Sandbox** section.
- 6 Click the **Virtualized Processes** tab.
- 7 Next to the process you want to stop virtualizing, click  .
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: SPECIFYING LOCATIONS THAT CAN'T BE ACCESSED BY VIRTUALIZED APPLICATIONS

Sandbox is available for:

- Windows Workstations
- Windows Servers


Harmful applications running in Sandbox can attempt to capture sensitive data copied to the virtualized environment. To prevent malware from accessing this data, a list of common system locations is blocked by default. Enable the Allowed check box next to any file or program that you want to access during virtualization.

You can also add your own locations to block or allow. Type the folder location manually into the text box or click Browse, click the relevant folder, then click OK.

TO SPECIFY LOCATIONS THAT CAN'T BE ACCESSED BY VIRTUALIZED APPLICATIONS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Sandbox** section.
- 6 Click the **Privacy** tab.
- 7 In the **Private Pre-set Locations** select one of the following for each location:
 - **Blocked**
 - **Allowed**
- 8 For user-defined locations, type a file path, click select either **Blocked** or **Allowed**, then click **Add**.
- 9 Repeat step 8 until all locations are defined.
- 10 Click **Apply Changes**.

TO REMOVE A BLOCK FROM A LOCATION SO IT CAN BE ACCESSED BY VIRTUALIZED APPLICATIONS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Sandbox** section.
- 6 Click the **Privacy** tab.
- 7 Next to the process you want to stop virtualizing, click  .
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: SPECIFYING LOCATIONS THAT WON'T BE VIRTUALIZED

Sandbox is available for:

- Windows Workstations
- Windows Servers

All files acquired during a Sandbox session are deleted when you close the sandboxed application. If you want to keep certain files, you can save them to a specified folder. We recommend using caution when saving files from sandboxed applications to excluded locations. If the application running in Sandbox is malicious, saving a file to a location on a device could be harmful.


Consider the options you have set up for your Sandbox when you add exclusion locations. For example, if you set your options to delete the contents of folders on exit, you might want to exclude the folder where you save files you download from the Internet.

IMPORTANT For information on how to use file paths, see [About File Paths in Settings Templates](#).

TO SPECIFY LOCATIONS THAT WON'T BE VIRTUALIZED

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Sandbox** section.
- 6 Click the **Exclusions** tab.
- 7 Type a file path and click **Add**.
- 8 Repeat step 7 until you have added all the paths you want to exclude.
- 9 Click **Apply Changes**.

TO REMOVE AN EXCLUSION FROM A VIRTUALIZED LOCATION

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Sandbox** section.
- 6 Click the **Exclusions** tab.
- 7 Next to the exclusion you want to remove, click .
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: ALLOWING VIRTUALIZED APPLICATIONS TO ACCESS THE INTERNET


Sandbox is available for:

- Windows Workstations
- Windows Servers

You can control which applications can access the Internet when they are running in the Sandbox or are automatically virtualized by CyberCapture.

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Sandbox** section.
- 6 Click the **Internet access** tab.
- 7 To give all applications the same access, select one of the following :
 - **Allow all virtualized applications to access the internet**
 - **Block internet access for all virtualized applications**
- 8 To configure which applications can access the Internet, select **Allow certain virtualized applications to access the internet**, then do either of the following:
 - If you want to let all web browsers access the Internet, select the **Web browsers** check box.
 - To let another application access the Internet, type its file path, then click **Add**. Repeat this step until you've identified all the applications you want to access the Internet.
- 9 Repeat step 8 until you have added all the paths you want to exclude.
- 10 Click **Apply Changes**.

TO REMOVE PERMISSION FOR A VIRTUALIZED APPLICATION TO ACCESS THE INTERNET

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click the **Windows Workstation** tab.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Sandbox** section.
- 6 Click the **Internet Access** tab.
- 7 Next to the application you want to prevent from accessing the Internet, click  .
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: SECURELINE VPN FOR WINDOWS WORKSTATIONS

SecureLine VPN is available for Windows Workstations.

SecureLine VPN is a Virtual Private Network (VPN). A VPN functions as a private tunnel through the Internet which encrypts your data and secures your connection when using public Wi-Fi connections such as those in cafes or airports.

SecureLine VPN has servers in several locations which means you can bypass geolocation restrictions as well as access your favorite content while traveling.

SecureLine VPN doesn't have any configurable options, but is available to users in Avast Business Antivirus.

CONFIGURING SETTINGS TEMPLATES: WI-FI INSPECTOR FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

Wi-Fi Inspector is available for:

- Windows Workstations
- Windows Servers

Wi-Fi Inspector scans your network for vulnerabilities and identifies potential security issues that open the door to threats. This feature checks the status of your network, devices connected to the network, and router settings. Wi-Fi Inspector helps you secure your network to prevent attackers from accessing it and misusing your personal data.

Wi-Fi Inspector doesn't have any configurable options, but is available to users in Avast Business Antivirus.

CONFIGURING SETTINGS TEMPLATES: RESCUE DISK FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

Rescue Disk is available for:

- Windows Workstations
- Windows Servers

If you suspect your devices are infected with malware and all other antivirus scans (including the Boot-time scan) were unable to resolve the issue, you can use Rescue Disk.

Rescue Disk enables you to scan devices when your system is not running. This method significantly increases your chances of detecting and removing malware because the malware is unable to counteract.

Rescue Disk doesn't have any configurable options, but is available to users in Avast Business Antivirus.

CONFIGURING SETTINGS TEMPLATES: PASSWORD PROTECTION FOR WINDOWS WORKSTATIONS

Password protection is available for Windows Workstations.

Passwords is a password manager that allows you to use one Master Password to quickly and safely log into your online accounts and complete web forms. Passwords encrypts and securely stores your sensitive information, and enables you to synchronize your data across all your devices.

Using Avast Business Antivirus to store your passwords is a safer alternative to storing passwords in your browser. The passwords you save in your browser are stored on your device along with the information necessary to decrypt them. Avast Business Antivirus stores your passwords with a much more secure level of encryption, and protects all your data with a password known only by you.

IMPORTANT To ensure your privacy, we do not store your Master Password locally or on any server. This means that nobody, including Avast Business Antivirus representatives, can access your Passwords data and recover or reset your Master Password if you forget it.

Passwords doesn't have any configurable options, but is available to users in Avast Business Antivirus.

CONFIGURING SETTINGS TEMPLATES: SOFTWARE UPDATER FOR WINDOWS WORKSTATIONS

Software Updater is available for Windows Workstations.

Software Updater helps keep commonly used third-party software up to date to eliminate potential security risks. Malicious threats or attackers often use leaks in outdated software to access devices. This feature displays the most popular programs installed on devices and allows you to easily update them.

Software Updater doesn't have any configurable options, but is available to users in Avast Business Antivirus.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING GENERAL SETTINGS

General settings let you control how you access and get notifications from Avast Business Antivirus, as well as how you update programs and virus definitions. You can also set your proxy, if you use one, enable or disable debug logging, and show or hide the Avast Business Antivirus icon in your toolbar tray.

Follow the links for:

- [General Settings for Windows Workstations and Windows Servers](#)
- [General Settings for Mac OS X](#)

TO CONFIGURE SETTINGS TEMPLATE GENERAL SETTINGS FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **General Settings** tab.
- 5 Select any of the following:
 - **Password Protection**—Password protect access to the Avast Business Antivirus UI.
 - **Silent Mode**—No messages/notifications are displayed.
 - **Debug logging**—Records operations, processes, and errors that occur.
 - **Avast tray icon**—Displays an icon in the tray.
- 6 Choose automatic or manual updates for the following:
 - **Program Updates**
 - **Virus Definition Updates**
- 7 In the Proxy Settings section, do one of the following:
 - Select **Direct connection (no proxy)**.
 - Select **HTTP Proxy**, then select an address, port, and authentication method.
- 8 Click **Apply Changes**.

TO CONFIGURE SETTINGS TEMPLATE GENERAL SETTINGS FOR MAC OS X

For the most up-to-date protection, choose to update automatically.

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click **Mac OS X**.
- 4 Click the **General Settings** tab.
- 5 In the **Virus Definition Updates** section, select one of the following:
 - **Automatically when new update is available**
 - **Manually**
- 6 In the **Program Updates** section, select one of the following:

- **Automatically when new update is available**
 - **Manually**
- 7 If required, click **Advanced update settings for devices with older AV version**.
 - 8 In the **Virus definitions updates and Program updates** section, choose your options:
 - **Via available Local Update Servers (Recommended to reduce bandwidth)**
 - **Directly from Avast Update Servers**
 - 9 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING ANTIVIRUS SETTINGS FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

The Antivirus settings of settings templates include:

- **DeepScreen**—Enable to run suspicious programs that aren't known to core antivirus technologies in the Sandbox, where it is compared to malicious behavior patterns, giving you the chance to allow or block it.
- **CyberCapture**—Enable the CyberCapture cloud-based smart file scanner to isolate suspicious files in a safe environment and automatically establish a two-way communication channel with Avast Threat Labs for immediate analysis.
- **Hardened Mode**—Enable to evaluate files is based on their reputation coming from the cloud.
- **Exclusions**—Identify paths and URLs excluded from scanning and shield protection.

TO CONFIGURE ANTIVIRUS SETTINGS FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Antivirus Settings** tab.
- 5 To run unknown suspicious programs in the Sandbox, in the **DeepScreen** section, select the **Activate** check box.
- 6 To isolate suspicious files and send info to Avast Threat Labs, in the **CyberCapture** section, select the **Activate** check box, then select a suspicious files check box.
- 7 Select an option in the **Hardened Mode** box:
 - **Disabled**
 - **Moderate**—Blocks files that have bad or no ratings
 - **Aggressive**—Only chosen executable files with known good ratings are allowed
- 8 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: EXCLUDING FILES, FOLDERS, OR URLS FROM SCANS AND SHIELDS FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

You can exclude certain files, folders, or URLs from scanning. While it is generally not recommended, you may want to exclude certain files or websites from scanning, for example if you want to speed up your scans or to avoid false positive detections.

Exclusions created in the File paths and URL Addresses sections apply globally to all manual scans and Shields. To exclude files only from a specific scan or Shield, use the Exclusions section in the settings of that particular scan or Shield.


NOTE Set exclusions only if you know that the files and websites you want to exclude are not infected.

TO EXCLUDE FILES, FOLDERS, OR URLS FROM SCANS AND SHIELDS FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Antivirus Settings** tab.
- 5 Do any of the following:
 - To exclude a file path, click the **File Paths** tab, then type the file path and click **Add**.
 - To exclude a URL, click the **URL Addresses** tab, then type the URL and click **Add**.
 - To exclude a file path from DeepScreen, click the **DeepScreen** tab, then type the file path and click **Add**.
 - To exclude a file path from Hardened Mode, click the **Hardened Mode** tab, then type the file path and click **Add**.
- 6 Repeat step 5 until you have added all your exclusions.
- 7 Click **Apply Changes**.

TO REMOVE AN EXCLUSION FROM A FILE, FILE TYPE, OR LOCATION FOR SCANS AND SHIELDS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Antivirus Settings** tab.
- 5 In the **Exclusions** section, click one of the following tabs:
 - **File Paths**
 - **URL Addresses**
 - **DeepScreen**
 - **Hardened Mode**

- 6 Next to the exclusion you want to remove, click .
- 7 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: CONFIGURING TROUBLESHOOTING SETTINGS FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

The Troubleshooting settings of settings templates include:

- **Enable anti-rootkit monitor**—Normally Avast Business Antivirus scans for rootkits when the operating system starts to detect viruses that cannot be detected after startup. Unchecking this box disables the scan for quicker startup, but an active virus may not be detected.
- **Avast self-defense Module**—Avast Business Antivirus contains self-defense features to prevent virus attacks from modifying or deleting critical antivirus files. Clearing this box turns off the self-defense module and allows Avast Business Antivirus files to be deleted.
- **Enable Hardware-Assisted Virtualization**—This is a more secure way to launch virtualized processes. If this box is checked, potential threats opened in Sandbox cannot modify your computer or files.

TO CONFIGURE TROUBLESHOOTING SETTINGS FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click one of the following tabs:
 - **Windows Workstation**
 - **Windows Server**
- 4 Click the **Troubleshooting** tab.
- 5 Select **Activate** for any of the following check boxes:
 - **Enable anti-rootkit monitor**
 - **Avast self-defense module**
 - **Enable hardware-assisted virtualization**
- 6 In the **Mail** section, do any of the following:
 - Type port numbers in any of the ports boxes.

NOTE To add multiple ports, separate them with a comma.

- Type a server address or port in the **Ignored addresses** box.
 - Select the **Ignore local communication** check box.
- 7 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: ENABLING AND CONFIGURING FILE SHIELD FOR MAC OS X

File Shield is available for:


- Windows Workstations
- Windows Servers
- Mac OS X

For Windows Workstations and Windows Servers settings, see [Configuring settings templates: Enabling and configuring File Shield for Windows Workstations and Windows Servers](#).

File Shield is the main layer of active protection in Avast Business Antivirus. It scans programs and files saved on devices for malicious threats in real-time before allowing them to be opened, run, modified, or saved. If malware is detected, File Shield prevents the program or file from infecting devices.

By default, File Shield is configured to provide optimal protection when switched on. We strongly recommend you keep this shield turned on at all times and only make configuration changes if you have an advanced understanding of malware protection principles.

TO ENABLE FILE SHIELD FOR MAC OS X

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click **Mac OS X**.
- 4 Click the **Active Protection** tab.
- 5 In the **Shields** section, move the slider  to enable **File Shield**.
- 6 Click **Apply Changes**.

TO CONFIGURE FILE SHIELD

You can specify what actions to take when viruses, potentially unwanted programs, or suspicious files are detected.

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click **Mac OS X**.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **File Shield** section.
- 6 In the **Settings** section, select any of the following:
 - **Report potentially unwanted programs (PUP)**
 - **Move infected files to chest**
- 7 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: EXCLUDING FILES, FILE TYPES, AND LOCATIONS FROM FILE SHIELD FOR MAC OS X

You can modify the files and locations that are not scanned, by excluding them. Enable the check boxes to define when the file is not scanned—when the file is read, written to, or executed.


NOTE Exclusions that you specify on this screen only apply to File Shield and do not affect any other scans or Shields. To exclude a location from all Avast Business Antivirus scans, see [Configuring settings templates: Excluding Files, Folders, or URLs from Scans and Shields for Windows Workstations and Windows Servers](#).

IMPORTANT For information on how to use file paths, see [About File Paths in Settings Templates](#).

TO EXCLUDE FILES, FILE TYPES, AND LOCATIONS FROM FILE SHIELD FOR MAC OS X

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click **Mac OS X**.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **File Shield** section.
- 6 In the **Exclusion** list, type a file name, path, or extension and click **Add**.
- 7 Repeat step 6 until all your chosen file names, paths, and extensions are excluded.
- 8 Click **Apply Changes**.

TO REMOVE A FILE SHIELD EXCLUSION FOR MAC OS X

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click **Mac OS X**.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **File Shield** section.
- 6 Next to the exclusion you want to remove, click .
- 7 Click **Apply Changes**.

CONFIGURING SETTINGS TEMPLATES: ENABLING AND CONFIGURING MAIL SHIELD FOR MAC OS X


Mail Shield is available for:

- Windows Workstations
- Windows Servers
- Mac OS X

For Windows Workstations and Windows Servers settings, see [Configuring settings templates: Enabling and configuring Mail Shield for Windows Workstations and Windows Servers](#).

Mail Shield checks incoming and outgoing email messages for viruses and links to malicious websites. This only applies to messages handled by mail management software installed on your computer, such as MS Outlook. If you access your web-based email account through an Internet browser, your devices are protected by other Shields.

TO ENABLE MAIL SHIELD FOR MAC OS X

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click **Mac OS X**.
- 4 Click the **Active Protection** tab.
- 5 In the **Shields** section, move the slider  to enable **Mail Shield**.
- 6 Click **Apply Changes**.


TO CONFIGURE MAIL SHIELD SETTINGS FOR MAC OS X

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click **Mac OS X**.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Mail Shield** section.
- 6 Select any of the following check boxes:
 - **Enable IPv6**
 - **Scan secured connections**
 - **Report potentially unwanted programs (PUP)**
 - **Mark mail headers**
 - **Remove infected attachments**
- 7 Click **Apply Changes**.

TO EXCLUDE MAIL SERVICES AND HOST NAMES FROM MAIL SHIELD FOR MAC OS X

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click **Mac OS X**.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Mail Shield** section.
- 6 In the **Exclusion** list, do the following
 - Select a mail service.
 - Type a host name.
 - Click **Add**.
- 7 Repeat step 6 until the list of exclusions is complete.
- 8 Click **Apply Changes**.

TO REMOVE A MAIL SHIELD EXCLUSION FOR MAC OS X

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click **Mac OS X**.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Mail Shield** section.
- 6 Next to the exclusion you want to remove, click .
- 7 Click **Apply Changes**.


CONFIGURING SETTINGS TEMPLATES: ENABLING AND CONFIGURING WEB SHIELD FOR MAC OS X

Web Shield is available for both Windows Workstations and Windows Servers, as well as OS X. For Windows Workstations and Windows Servers settings, see [Configuring settings templates: Enabling and configuring Web Shield for Windows Workstations and Windows Servers](#).

Web Shield protects your system from threats while browsing the web. It also prevents malicious scripts from running, even when you are offline.

In Web Shield, you can enable and configure web, HTTPS, and script scanning.

TO ENABLE WEB SHIELD FOR MAC OS X

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click **Mac OS X**.
- 4 Click the **Active Protection** tab.
- 5 In the **Shields** section, move the slider  to enable **Web Shield**.
- 6 Click **Apply Changes**.


TO CONFIGURE WEB SHIELD SETTINGS FOR MAC OS X

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click **Mac OS X**.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Click the **Main Settings** tab.
- 7 Do any of the following:
 - To enable scanning on devices using Internet Protocol version 6, select the **Enable** check box in the **Enable IPv6** section.
 - To enable scanning of sites that are accessed over secured connections, select the **Enable** check box in the **Scan secured connections** section. To only scan secured connections from browsers, and not other applications, select the **Scan secured connections from browsers only** check box.
 - To list background programs such as spyware, that could potentially be downloaded, select the **Report potentially unwanted programs (PUP)** check box in the **PUP** section.
- 8 Click **Apply Changes**.

TO EXCLUDE SAFE URLs FROM THE WEB SHIELD SCAN FOR MAC OS X

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click **Mac OS X**.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 In the **Exclusion** list, do the following
 - Select **http** or **https**.
 - Type a host name.
 - Click **Add**.
- 7 Repeat step 6 until the list of exclusions is complete.
- 8 Click **Apply Changes**.

TO REMOVE A WEB SHIELD EXCLUSION FOR MAC OS X

- 1 Click **Device settings**.
- 2 Click the name of a settings template.
- 3 Click **Mac OS X**.
- 4 Click the **Active Protection** tab.
- 5 Click the **Customize** link in the **Web Shield** section.
- 6 Next to the exclusion you want to remove, click .
- 7 Click **Apply Changes**.

ABOUT FILE PATHS IN SETTINGS TEMPLATES

In certain elements of Settings templates, wildcard characters can help you when you don't 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.

CHARACTER	MEANING
?	Replaces a single character For example, <code>ab?.html</code> matches the files <code>abc.html</code> , <code>abd.html</code> , and <code>abe.html</code> . It will not match the file <code>abc.htm</code> .
*	Replaces zero or more characters For example <code>*.html</code> matches the files <code>abc.html</code> and <code>d.txt</code> . The pattern <code>*txt</code> matches the files <code>abc.txt</code> , <code>x.txt</code> , and <code>xyztxt</code> .

Under certain circumstances, you will not get the expected result without using wildcards. For example:

- To exclude all HTML files, type `*.htm*` into the text box. Typing `.html` or `.htm` into the text box will not include any files because no full file name is represented.
- To exclude a folder and its sub-folders, add `*` to the end of the folder name, for instance `C:\example*`.
- To exclude all files labeled in a certain way on any of your hard drives, include `?:\` in front of the path, for instance `?:\example.exe`.

NOTE Not all file paths allow the use of wildcards.

CHAPTER NINE:

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.

NOTE To change the day of the week that weekly reports start on, see [First day of the week](#).

TO CHANGE REGIONAL SETTINGS

- 1 Click **Reports** .
- 2 Click the **UTC** link in the top right of the window.
- 3 Choose the day your week starts on.
- 4 Choose your time zone.
- 5 Click **Save**.

NOTE You can also click **Settings**  to [change regional settings](#).

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 the threat categories of 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 taken 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 displayed.

TASKS REPORT

This area displays information on tasks that have completed and tasks that have failed.

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 daily on all five of your devices, your Task overview shows 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.

DEVICE 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 different task failure.

DEVICE OVERVIEW

Device removed refers to the number of times you uninstalled Avast Business Antivirus from a device, regardless of whether you uninstalled Avast Business 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.


CHAPTER TEN: LICENSES

The Licenses page displays valuable information about your licenses, and gives you the tools to manage your protection.

On this page, you can see:

- What level of protection you have
- How many devices you have protected
- When your protection expires
- Whether your protection is set to auto-renew
- When you last updated your license status

TO VIEW INFORMATION ABOUT PROTECTION AND LICENSES

- 1 Click **Licenses** .
- 2 View any of the following:
 - To see what level of protection you have, identify which boxes on the page are highlighted.
 - To see how many devices are protected, identify the number of devices in each of the highlighted boxes. You can also see the number of licenses you have for devices. For example, if a box displays “Devices 3/10,” this indicates that you have 3 assigned devices out of 10 licenses that you own.
 - To see when your protection expires, see the date next to **Expiration** in the boxes. Your protection expires after this date.
 - To see your auto-renewal status, see the status next to **Auto-renewal**.
 - To see when you last updated your license status, see the time and date next to **Latest update** at the bottom of the page.

MANAGE LICENSE TASKS

The tasks you can perform on this page are:


- Buy additional devices for your license
- Manage your auto-renewal status
- Extend your license expiry date
- Start a new trial or a trial of another level of protection
- Buy Avast Business Antivirus licenses
- Update license status
- Compare the level of protection in Avast Business Antivirus products

NOTE If you are using the Avast Business Antivirus as a trial, the license page lets you turn your trial into a subscription.


TO CHANGE AUTO-RENEWAL STATUS

If your auto-renewal status is On, your licenses automatically renew for one year on the expiration date. If not, your protection expires on that date and you must renew manually. If Unknown is displayed, the autorenewal status can't be retrieved.


NOTE Auto-renewal requires that your Avast Business user profile is complete and has a valid credit card that can be charged.

- 1 Click **Licenses** .
- 2 Under an Antivirus tier that you have a license for, click the link next to **Auto-renewal**.


TO EXTEND THE EXPIRY DATE OF YOUR LICENSE

- 1 Click **Licenses** .
- 2 Under an Antivirus tier that you have a license for, click **Extend expiration**.

TO START A LICENSE TRIAL

- 1 Click **Licenses** .
- 2 Under an Antivirus tier that you don't have a license for, click **Start Trial**.

TO BUY LICENSES

- 1 Click **Licenses** .
- 2 Do one of the following:
 - To buy licenses for additional devices for an Antivirus tier that you already have a license for, click **Buy more devices**.
 - To buy or renew a license for an Antivirus tier that you don't have a license for, click **Buy now**.

TO UPDATE LICENSE STATUS

License statuses include:

- Trial
- Paid
- Expired

You may need to update your license status when you convert from an expired or trial license to paid.

- 1 Click **Licenses** .
- 2 Click the **Update now** link at the bottom of the page.

TO COMPARE THE PROTECTION LEVEL OF ANTIVIRUS PRODUCTS


- 1 Click **Licenses** .
- 2 Click the **business products** link at the bottom of the page.

CHAPTER ELEVEN:

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.

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**.

CLOSE YOUR AVAST ACCOUNT

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


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

CHAPTER TWELVE:


PERSONAL PROFILE

You can change the name and your password on your personal profile.


TO EDIT YOUR NAME

- 1 Click your profile icon  in the top right corner of the browser window, then click **Edit personal profile**.
- 2 Type your **Name** and **Surname**.
- 3 Click **Save**.

TO CHANGE YOUR PASSWORD

- 1 Click your profile icon  in the top right corner of the browser window, then click **Edit personal profile**.
- 2 Click the **Change your password** link.
- 3 Type the following:
 - **Current password**
 - **New password**
 - **Retype new password**
- 4 Click **Save**.

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**.

CHAPTER THIRTEEN:

USER MANAGEMENT

The User Management area is provided so that you can:

- Invite other users to be administrators.
- 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
- E-mail
- 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. Passwords must use at least one letter, one number, and one special character.

TO INVITE ADMINISTRATORS

You can invite other users to be administrators for the console. Other administrators have the same level of access as you, with the ability to add devices, set up settings templates, and add additional administrators.

The user receives an invitation by e-mail, which they can accept or reject.

TO INVITE A NEW USER AS AN ADMINISTRATOR

- 1 Click your profile icon  in the top right corner of the browser window, then click **User management**.
- 2 Click **Invite Administrators**.
- 3 Type the following:
 - **E-mail**
 - **Subject**
- 4 To configure the message you send in the email, select the **Include your custom message** check box and type a message.
- 5 To receive an email when the user logs in as an administrator, select the **Notify me by email after user login** check box.
- 6 Click **Send**.

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**.

CHAPTER FOURTEEN:

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 Cloud 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 AREN'T MASTER AGENTS WORKING?

If a Master Agent 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 Master Agent to the client device.

CAN I SUPPORT DEVICES THAT USE PROXY SERVERS?

Avast Business Cloud Management Console doesn't currently support devices that use proxy servers.

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

Avast Business Cloud Management Console requires access to the internet.

INDEX

account	
creating	3
activating	
devices	13, 25
adding	
devices, e-mailing the install link	13
devices, using the installer	13
groups	23
sub-groups	23
administrators, inviting	106
Anti-rootkit monitor, enabling for Windows ...	93
Anti-spam	
adding email addresses to the white list	65
blocking spam email addresses	66
configuring for Windows	63
enabling for Windows	63
Antivirus	
configuring	35
configuring settings templates for Windows	
.....	91
configuring settings templates for Windows,	
troubleshooting	93
deploying to multiple remote devices ...	14, 15
excluding files, folders, or URLs from scans	
and shields for Windows	92
installing by e-mail	13
installing components	36
keeping up to date	35
uninstalling components	36
updating on devices	27
using the installer	13
Antivirus components	37
Avast	
closing account	104
keeping Avast Business Antivirus up to date	
.....	35
updating on all devices	33
Behavior Shield	
defining how to deal with suspicious files ...	74
enabling for Windows	74
excluding locations from	75
BitRock log	3
boot time scan	32
Browser Cleanup	
configuring for Windows	81
enabling for Windows	81
buying licenses	103
calling tech support	5
changing	
password	105
regional settings	100
checking for updates	5
closing	
Avast account	104
company profile	104, 105
Components tab	
about	28
configuring	
Anti-Spam Shield for Windows	63
Antivirus	35
Antivirus for Windows	91
Antivirus for Windows, excluding files,	
folders, and URLs from scans and shields	92
Antivirus for Windows, troubleshooting	93
Browser Cleanup for Windows	81
CyberCapture for Windows	91
Data Shredder for Windows	81
DeepScreen for Windows	91
Exchange Server protection for Windows ...	78
File Shield for Mac OS X	94
File Shield for Windows	39
Firewall for Windows	67
Hardened Mode for Windows	91
Mail Shield for Mac OS X	95
Mail Shield for Windows	46
Web Shield for Mac OS X	97
Web Shield for Windows	53
Webcam Shield for Windows	76
Configuring settings templates	
excluding items from File Shield, Mac OS X.	95
console	
doesn't display installed device	108
using while offline	108
creating	

account.....	3	status	20
groups	22	uninstalling	22, 26
settings templates.....	37, 39	unselecting.....	25
custom scan	32	updating.....	27
CyberCapture, configuring settings templates		updating with a Master Agent.....	9
for Windows.....	91	viewing details	28
dashboard	12	downloading	
network security section.....	16	device installer.....	13
shortcuts section.....	12	editing	
threat detection statistics	16	company profile.....	104, 105
Data Shredder		groups	24
configuring for Windows.....	81	personal profile.....	105
enabling for Windows.....	81	settings templates	38
day, setting.....	7	tasks	31
debug logs, turning on	108	email	
DeepScreen		adding addresses to the white list.....	65
configuring settings templates for Windows		blocking spam email addresses	66
.....	91	enabling	
default group	23	anti-rootkit monitor for Windows	93
default ports.....	2	Anti-spam Shield for Windows	63
default settings template.....	35	Behavior Shield for Windows	74
deleting		Browser Cleanup for Windows.....	81
files from the Threats detected tab.....	29	Data Shredder for Windows	81
groups	24	DNS protection for Windows.....	63
settings templates.....	38	Exchange Server protection for Windows...	78
tasks	31	File Shield for Mac OS X.....	94
details, seeing task.....	30	File Shield for Windows	39
Device report	101	Firewall for Windows.....	67
devices	20	hardware-assisted virtualization for Windows	
activating.....	13, 25	93
adding by e-mailing install link.....	13	Mail Shield for Mac OS X	95
adding to a group.....	24	Mail Shield for Windows.....	46, 63
adding using the installer.....	13	Security Browser Shield for Windows	78
assigning settings templates to.....	21	Self-Defense module for Windows.....	93
changing licenses	25	SharePoint Server Protection for Windows.	80
changing settings template.....	25	Web Shield for Mac OS X.....	97
don't appear in console	108	Web Shield for Windows	53
downloading installer	13	Webcam Shield for Windows	76
filtering.....	21	Enterprise Administration,migrating from	11
removing	22, 26	Exchange Server protection	
restarting.....	28	blocking email attachments	80
scanning	26	configuring actions to deal with suspicious	
scanning all managed.....	32	items	79
searching for	21	configuring for Windows	78
sending a message to.....	27	enabling for Windows.....	78
sending messages to all	33	file paths, using wildcards in Settings Templates	
shutting down	28	99
shutting down all	34	File Shield	

actions taken when virus found.....	42	hardware-assisted virtualization, enabling for	
archive files	43	Windows	93
configuring for Mac OS X	94	help, getting.....	5
configuring for Windows.....	39	history, viewing task	30
enabling for Mac OS X.....	94	HTTPS certificate.....	3
enabling for Windows.....	39	installation	
excluding items from, Mac OS X	95	viewing logs	3
excluding items from, Windows	41	Windows	3
reports.....	45	installing	
sensitivity	44	Antivirus by e-mail	13
filtering		Antivirus components.....	36
device list	21	Antivirus through the installer.....	13
tasks	31	inviting administrators.....	106
Firewall		language,setting the	11
adding new packet rules	72	licenses	
applying connection rules.....	70	buying	103
assigning a profile to a network.....	67	starting a trial.....	103
changing the order of packet rules.....	73	uploading	4
configuring for Windows.....	67	logging in.....	4
creating custom connection rules.....	71	logs	
defining advanced packet rules	72	location of PostgreSQL	108
defining application rules.....	69	location of troubleshooting	108
defining default rules	70	turning on debug	108
defining networks for Windows.....	68	Mac OS X	
defining system rules	68	configuring File Shield.....	94
deleting packet rules.....	73	configuring general settings of settings	
disabling packet rules.....	73	templates.....	90
editing packet rules.....	73	configuring Mail Shield	96
enabling for Windows.....	67	configuring Web Shield.....	97
overriding user-defined rules.....	68	enabling File Shield	94
full system scan.....	32	enabling Mail Shield	95
general settings.....	5	enabling Web Shield	97
configuring settings template	90	excluding items from File Shield.....	95
configuring settings template for Mac OS	90	Mail Shield	
getting help	5	actions taken when virus found	49
groups		archive files.....	50
adding	23	configuring for Mac OS X.....	95
adding devices to	24	configuring for Windows	46
assigning settings templates to.....	22	configuring notes in emails.....	47
creating	22	enabling for Mac OS X	95
default group	23	enabling for Windows.....	46
deleting	24	reports	52
editing	24	scanning SSL connections	48
sub-groups	23	sensitivity	50
viewing	22	master agents	
Hardened Mode		troubleshooting	108
configuring settings templates for Windows		Master Agents	
.....	91	requirements	8

setting up	7	Mail Shield	52
turning off	10	start date of weekly	7
turning off for a device	9	Tasks report	101
turning off for a group	10	Threat report	100
turning on.....	10	Web Shield.....	62
turning on for a device.....	9	requirements	2
turning on for a group.....	10	Master Agents	8
messages, sending to devices	27	Rescue Disk, enabling	89
migrating		restarting devices	28
from Enterprise Administration	11	restoring, files on the Threats detected tab....	29
from Small Office Administration	11	Sandbox	
navigation bar	5	configuring location of.....	82
maximizing	5	configuring web browsers	83
minimizing.....	5	selecting locations that can't be accessed by	
network security section.....	16	virtualized applications.....	85
notifications		selecting which applications are virtualized in	
about.....	17	84
configuring	18	selecting which locations are not virtualized	
expiration	18	in	86
marking as read.....	18	selecting which virtualized applications can	
network.....	18	access the web.....	87
security.....	17	scanning	
selecting recipients	19	all managed devices.....	32
turning off in-app	18	at boot time	32
types.....	17	custom	32
passwords		devices	26
changing your.....	105	full system.....	32
enabling password protection for Windows	89	quickly.....	32
protect access to Avast Antivirus with.....	90	removable media.....	32
personal profile.....	105	tasks	32
PostgreSQL.....	3	script scanning, excluding URLs from	61
logs	3	searching	
PostgreSQL, location of logs	108	for devices.....	21
proxy servers, support of	108	tasks	31
quick scan.....	32	SecureLine VPN	
Real Site		selecting which virtualized applications can	
enabling for Windows.....	63	access the web.....	88
regional settings.....	100	Security Browser Shield, enabling for Windows	
remote deployment		78
antivirus	14, 15	Self-Defense module, enabling for Windows..	93
requirements	14	sending messages	
removable media scan	32	to all devices	33
removing		to devices.....	27
devices	22, 26	sensitivity	
reports		of File Shield.....	44
changing the reporting period	100	of Mail Shield	50
Device report	101	of Web Shield.....	59
File Shield	45	setting the language	11

setting up	
company profile	104, 105
Master Agents	7
settings	
general	5
settings templates	
assigning to devices	21
assigning to groups	22
changing for devices	25
configuring Anti-spam Shield	63
configuring Browser Cleanup	81
configuring Data Shredder	81
configuring Exchange Server protection	78
configuring File Shield	39
configuring File Shield for Mac OS X	94
configuring Firewall	67
configuring general settings	90
configuring general settings for Mac OS	90
configuring how Behavior Shield deals with suspicious files	74
configuring location of Sandbox	82
configuring Mail Shield	46
configuring Mail Shield for Mac OS X	95
configuring Sandbox web browsers	83
configuring Web Shield	53
configuring Web Shield for Mac OS X	97
configuring Webcam Shield	76
creating	37
default	35
deleting	38
editing	38
enabling anti-rootkit	93
enabling Anti-spam Shield	63
enabling Avast Self-Defense module for Windows	93
enabling Behavior Shield	74
enabling Browser Cleanup	81
enabling Data Shredder	81
enabling DNS protection	63
enabling Exchange Server protection	78
enabling File Shield	39
enabling File Shield for Mac OS X	94
enabling Firewall	67
enabling hardware-assisted virtualization for Windows	93
enabling Mail Shield	46
enabling Mail Shield for Mac OS X	95
enabling password protection	89
enabling Real Site	63
enabling Rescue Disk	89
enabling SecureLine VPN	88
enabling Security Browser Shield	78
enabling SharePoint Server Protection	80
enabling Software Updater	89
enabling Web Shield	53
enabling Web Shield for Mac OS X	97
enabling Webcam Shield	76
enabling Wi-Fi Inspector	88
seeing the devices and groups where applied	39
selecting locations that can't be accessed by virtualized applications	85
selecting which applications are virtualized in Sandbox	84
selecting which locations are not virtualized in Sandbox	86
selecting which Sandbox applications can access the web	87
using to keep Antivirus up to date	35
using wildcards in file paths	99
setup log	3
SharePoint Server Protection	
enabling for Windows	80
shortcuts section	12
shutting down	
all devices	34
devices	28
Small Office Administration, migrating from	11
SMTP server	2
Software Updater	
enabling	89
SQL, location of logs	108
SSL	
certificates	2
scanning connections with Mail Shield	48
starting a license trial	103
status messages, devices	20
status, devices	20
stopping tasks	31
sub-groups	
about	23
adding	23
deleting	24
editing	24
tasks	
boot-time scan	32

custom scan	32	virus software on all devices	33
deleting from the Tasks page.....	31	updating the console	5
deleting from the Tasks tab	29	uploading	
details.....	30	license	4
editing	31	URLs, blocking with Web Shield	60
filtering.....	31	user management, about	106
full system scan.....	32	users	
history	30	adding new	106
quick scan.....	32	editing existing.....	107
removable media scan	32	viewing	
scanning	32	device details	28
searching.....	31	groups.....	22
stopping	31	tasks.....	30
stopping from the Tasks tab	29	virus	
unselecting.....	31	File Shield action against	42
viewing.....	30	Mail Shield action against.....	49
Tasks report	101	Web Shield action against	57
Tasks tab		virus software, updating on all devices	33
about.....	29	warnings	
stopping or deleting tasks from the.....	29	configuring Mail Shield	47
tech support.....	5	Web Shield	
threat detection statistics section	16	actions taken when virus found	57
Threat report.....	100	archive files.....	58
Threats detected tab		blocking URLs with.....	60
about.....	29	configuring file types scanned.....	54, 55
deleting files from the.....	29	configuring for Mac OS X.....	97
restoring files from the	29	configuring for Windows	53
time, setting.....	7	enabling for Mac OS X	97
troubleshooting, FAQ.....	108	enabling for Windows.....	53
turning on		excluding URLs from script scanning	61
Master Agents, for a device	9	reports	62
Master Agents, for a group.....	10	sensitivity.....	59
uninstalling		Webcam Shield	
Antivirus components.....	36	configuring for Windows	76
devices	22, 26	enabling for Windows.....	76
unselecting		Wi-Fi Inspector	
devices	25	enabling	88
tasks	31	wildcards, using in Settings Templates file paths	99
updating		Windows installation	3
Antivirus on devices.....	27		
Avast on all devices.....	33		