Avast Business
Cloud Console

Console Version 7.19

TABLE OF CONTENTS

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 (Google Chrome, Firefox, Safari, Microsoft Edge, Internet Explorer, etc.)

NOTE Avast recommends using the latest version of Google Chrome for optimal performance, compatibility, and security of Avast Business Cloud Management Console.

DEFAULT PORTS

The default ports used by Avast Business Cloud Management Console should be open in your network firewall for optimal performance of your Console and the Avast Business Antivirus software.

- Communication between Console and Clients—TCP/UDP 443, 8080, and 8090
- For Internet vulnerability checks and feature updates—TCP/UDP 80
- DCOM—TCP/UDP 135
- Mirror, for local updates—TCP/UDP 4158
- Secure Domain Name Resolution Services—TCP/UDP 53
- For Remote Deployment—TCP/UDP 7074
- Network Time Protocol, for time synchronization—UDP 123
- Gamification—TCP 8742

NOTE Another port you should have open is 8443, which used to be the default for communication and has been replaced by port 443. However, if 443 is already in use in your network such as for a hosted web server, your console will not work.

ANTIVIRUS AND MANAGEMENT CONSOLE URLS

The following URLs should be whitelisted in your Internet settings.

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

TO REGISTER FOR YOUR 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.

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 your company's 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 **Company Profile**.
2. Make your changes.
3. Click **Save**.

NOTE Company name and Industry are required fields.

CLOSE YOUR AVAST ACCOUNT

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

NOTE This option only closes your console account. You cannot close your personal Avast account from the company profile page.

YOUR 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 **Your 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 **Your profile**.
2. Click the **Change your password** link.
3. Type the following:
   - **Current password**
   - **New password**
   - **Retype new password**
4. Click **Save**.

NOTE Avast Business enforces a strong password policy. The minimum length for a password is eight characters. Passwords must use a combination of capital and lowercase letters, as well as numbers. We also recommend you use special characters for maximum password security.

MANAGE COMPANIES

The Manage companies section is provided to allow a single Avast account to manage multiple companies, eliminating the need for multiple logins to the Cloud Console.

TO ADD COMPANIES

1. Click your profile icon  in the top right corner of the browser window, then click **Your profile**.
2. Click **Create another company**.
3. Enter the Company Name and its location/language.
4. Click **Create**.

TO SWITCH BETWEEN COMPANIES

1. Beside the profile icon, click the Account Switching icon  .
2. Select the company you would like to switch to.

Users can manage their companies on the Your profile section, or by clicking Manage Companies in the Account Switching menu.

USER MANAGEMENT

The User Management section is provided so that you can:

- Invite other users to be administrators.
- View who has access to your console.
- Restrict access of existing users to the console (i.e. block access or remove access).

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

- Name
- Surname
- E-mail
- Role

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 invite e-mail, select the **Include your custom message** check box and type a message.
5. To receive an e-mail when the user logs in as an administrator, select the **Notify me by e-mail 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.

NOTIFICATION SETTINGS

The Notification settings section enables you to choose the types of notifications Avast Business Cloud Management Console displays. The different types of notifications are covered in further detail in Chapter Five: Notifications.

From the Notification settings section, you can turn in-app notifications on or off for various security and network notifications. These notifications appear directly in the console. You can also select options for e-mail notifications for each type of threat, which defines when e-mails are sent if the Administrator does not read the in-app notification: instantly or in a batch at the end of the week. You can also turn e-mail notifications off.

TO TURN IN-APP NOTIFICATIONS OFF

1. Click your profile icon in the top right corner of the browser window, then click **Notification settings**.
2. In a notification section, move the In-app notification slider 

to **Off**.

TO CHOOSE SETTINGS FOR E-MAIL NOTIFICATIONS

1. Click your profile icon in the top right corner of the browser window, then click **Notification settings**.
2. 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**.

The options for e-mail notifications are instantly, batched at the end of the week, batched at the end of the day, or never.

TO CHOOSE WHO RECEIVES E-MAIL NOTIFICATIONS

1. Click your profile icon  in the top right corner of the browser window, then click **Notification settings**.
2. Click the **Edit** link at the top of the window.
3. Select the check boxes of the names of the people you want to send the notification to.
4. To send the e-mail to other addresses, type the addresses, separated by commas, in the **Send a copy to the following e-mail addresses** box.
5. Click **Update**.

LANGUAGE

The Language section enables you to choose in which language to display your Avast Business Cloud Management Console. The current options are Deutsch, English, Español, Français, Italiano, Português, Русский, and Norsk.

TO CHANGE THE LANGUAGE

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**.

LOGGING OUT

The Logout section immediately logs you out of the Avast Business Cloud Management Console without any confirmation prompts.

TO LOG OUT

1. Click your profile icon  in the top right corner of the browser window.
2. Click **Logout**.

CHAPTER THREE:

NAVIGATION

The navigation menu on the left side of the Avast Business Cloud Management Console window allows you to navigate to the different pages in the application. To save space on your screen, you can minimize the navigation bar.

You can minimize the navigation menu by clicking the  button and maximize it by clicking the  button.

NAVIGATION MENU

The pages of the navigation menu allow you to add and manage devices remotely, view or change device settings, schedule and create reports, and receive notifications on changes or risks to your devices.

Below is a brief overview of each page and the actions you can perform on them:

- **Dashboard**—Review general statistics for your managed devices and pertinent information from all the menu pages.
- **Notifications**—Receive notifications on changes or threats to your devices.
- **Devices**—Add devices to your console, view all managed devices and their current statuses, and create and configure groups.
- **Tasks**—Schedule scans, updates, and shut downs and/or restarts of your devices or send messages to devices.
- **Patches**—View all patches for the software on your devices, and determine which patches need to be applied.
- **Device settings**—View all settings templates and which devices and groups are using them and create new templates.
- **Reports**—Compile reports based on the devices, tasks, and threats occurring across your managed devices.
- **Subscriptions**—View your current license type, number of devices in use versus number available, and expiration date, and purchase more devices or enter updated license codes.
- **Help & Support**—View helpful links to Avast product pages and the Knowledge Base and contact the technical support team.
- **General Settings**—Choose your date and time preferences, set up Master Agents, and migrate from other consoles.

The status and version links at the bottom of the navigation bar also allow you to:

- View the status of the Avast Business Cloud Management database
- View the version number for your Console
- See a roadmap for future updates to the Console

CHAPTER FOUR:

DASHBOARD

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

- **Shortcuts**—This section provides quick access 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.
- **Patch Management – Devices Summary**—This section shows you the percentage of your devices that are in danger, vulnerable, or safe related to software patches.
- **Patch Management – Patch Summary**—This section shows you the number of failed and missing patches along with the number of affected devices.

You can also configure your Dashboard to include or exclude the *Network and Threat Overview* and *Patch Management* widgets. To do so, click **Configure** at the bottom of the page, then click the sliders beside the widget categories.

SHORTCUTS

In the Shortcuts section, you add devices to Avast Business Cloud Management Console, scan your devices, activate devices, and see threat reports.

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, which occurs when you install Avast Business Antivirus on it. 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 Cloud Management Console, 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.

NOTE The remote installation option is not available unless you have already added at least one device to your network through another installation method and designated that device as a Master Agent.

TO DOWNLOAD THE AVAST BUSINESS APP INSTALLER

1. On the **Dashboard** or **Devices** page, click **Download installer** or the plus sign button to add a device.
2. Click **Download the installer**.
3. Select the operating system the installer is for:
   - **Windows .EXE (For workstations and servers)**
   - **Windows .MSI**
   - **Mac OS X .DMG**
4. Select the product **License**.
5. 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**
   - **Whether to remove competitive antivirus products**
   - **Installer size (Light or Full)**
   - **Proxy server**
6. 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. On the **Dashboard** or **Devices** page, click **Download installer**.
2. Click **Send download link via e-mail**.
3. In the **Send to** box enter the target e-mail address. If you would like to send the link to multiple e-mails, enter them separated by commas.
4. Alter the **Subject** line of the e-mail that will be sent.
5. To configure the message you send in the e-mail, select the **Include your custom message** check box and type a message.
6. Select the product **License**.
7. 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**
   - **Whether to remove competitive antivirus products**
   - **Installer size (Light or Full)**
   - **Proxy server**
8. Click **Send** to e-mail an install link to the selected e-mail addresses.

NOTE For both the installer package and the download e-mail link, the Full installer contains all necessary files to install Avast Business Antivirus on the device and can be used in an offline environment if necessary. The Light installer does not have all the files and requires internet access, as it contacts Avast servers to retrieve the installation details and files. Adding multiple

devices using the Light installer may have negative effects on the speed of your network until the installation process is complete.

After a successful install through the installer or a download e-mail link, the Avast Business Antivirus 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.

How to activate your added devices

Your device is protected as soon as it is added to the network. 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 you have purchased a license and still have devices available under it, your added devices will be automatically activated.

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

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.

How to deploy Avast Antivirus to multiple devices remotely

Avast Business Cloud Management Console makes it easy to automatically find devices in your Active Directory that are not already protected by Avast Antivirus. Once you have 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 from the sidebar.

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 do not 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. Remove and uninstall Avast Antivirus from existing devices.
2. On the **Dashboard** or **Devices** page, click **Download installer**.
3. Click **Deploy installers remotely**.
4. Click **Begin deployment process**.

   - If you do not have a Master Agent available, click the **Add new Master Agent** link and follow the Setting Up Master Agents 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. This may take a while.

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 **Subscription products** section, click **Change subscription**, then select one of your available Antivirus licenses and your Patch Management license, if you have one.
10. In the **Deploy to a group in Avast Business console** section, do any of the following:

    - Select a group.
    - If you would like to copy your Active Directory's group structure, select the **Copy Active Directory group structure into the selected group** check box.
    - Select a settings template.

11. If you would like Avast Business to remove any conflicting antivirus programs during installation, select the **Remove other conflicting antivirus products during deployment** check box.
12. Click **Start deployment to devices**.

NOTE Wait while Antivirus is deployed to devices. You can navigate to other pages during this process and use the Remote Deployment button on the navigation menu to return to view the progress of your Remote Deployment.

13 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. Please see the To Shut Down or Restart a Device section for more details.

How to migrate from Enterprise Administration or Small Office Administration

If you are trying to migrate your protection from Enterprise Administration or Small Office Administration, the Avast Business Cloud Management Console provides the tools to import your devices and settings.

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 the **Transfer From Other Console** tab.
3 Click **Import file**.
4 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

5 Click **Open**. You will see an overview of how many groups and devices you are able to transfer.
6 Click the **Devices** page.

NOTE Devices from the EA/SOA console appear in your Avast Business Cloud Management Console in the **Devices** section, with the status of Pending. This may take a while.

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

As they transfer, the status of the devices changes 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.

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 across your devices over a chosen time period.

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.

Patch Management – Devices Summary

This section only shows on your Dashboard if you have it enabled. If you do not have a subscription for Patch Management, there will be a link to Start Trial if you have not completed one for Patch Management. Nothing will show if you already completed a trial.

The main graph is a Devices Summary so you can easily see how the percentage of your devices that are in danger or vulnerable due to missing patches, or safe and therefore up to date. This section gives you a quick snapshot of the devices across your network and how protected they are.

Patch Management – Patch Summary

This section only shows on your Dashboard if you have it enabled. If you do not have a subscription for Patch Management, there will be a link to a video detailing the usage and benefits of Patch Management. This section displays a count of *Failed to deploy patches* listing the number of patches and number of affected devices, and a count of *Missing Patches* with the number of patches and affected devices.

This section will only be filled in with information if you have a Patch Management subscription and both of the following enabled:

- Patch scanning. To schedule a recurring patch scan, see the To configure patch scanning procedure.
- Automatic patch deployment. To set up automatic patch deployment, see the To configure automatic patch deployment procedure.

NOTE You can view a break-down of the patches and apply a variety of filters to search for them on the Patches page.

CHAPTER FIVE:

NOTIFICATIONS

Notifications are important messages that keep you informed about the status of your network. Notifications appear on the Notifications page in Avast Business Cloud Management Console and are also delivered to the e-mail address you set up for your account.

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 **Notifications**  .
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:

- Clicking on the notification.
- Any action being taken on the notification.

TO TURN IN-APP NOTIFICATIONS OFF

1. Click **Notifications**  .
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 **Notifications**  .
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 e-mail addresses** box.
6. Click **Update**.

CHAPTER SIX:

DEVICES

The Devices page displays a list of all your devices and groups. This lets you view device status and drill down to the details of each device to configure your device security to your environment.

UNDERSTANDING THE STATUS OF DEVICES

The status of each device is displayed next to its name, with different statuses displayed in different colors.

- **Green**—Indicates the device is protected and safe. No action is required.
- **Yellow**—Indicates the device is vulnerable. For example, a device might be yellow if a scan has not been run in a long time. If a device is yellow, 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 ALERT MESSAGES

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

- Device Management
  - **Offline 21+ days.** Your device has not synced in more than 21 days. Check why the device is not connected to the network and connect it.
  - **Offline 14+ days.** Your device has not synced in more than 14 days. Check why the device is not connected to the network and connect it.
  - **Obsolete OS.** Your device is using an obsolete version of the operating system. Consider updating the device to a more recent OS to resolve this vulnerability.
  - **Restart needed.** Your device needs to be restarted for one or more reasons. Create a restart task for affected devices.
  - **Agent outdated 21+ days.** The device management agent is out of date by more than 21 days. Check why the device is not updating.
  - **Device has been reinstalled.** The device has been reinstalled by the user on the device. No further action is needed.
  - **Device has been migrated.** The device has been properly migrated to your Console.
- Antivirus
  - **Antivirus subscription expired.** Device is using an expired Avast Antivirus subscription. Choose a new subscription with remaining available seats or purchase new seats.
  - **Some OS drivers missing.** MacOS drivers are missing or need to be approved on the device.
  - **Agent outdated 21+ days.** The Antivirus agent is out of date by more than 21 days. Create a task to update the agent.
  - **Virus definitions outdated 21+ days.** The virus definitions in the database are out of date by more than 21 days. Create a task to update the virus definitions.

- **Virus definitions outdated 14+ days.** The virus definitions in the database are out of date by more than 14 days. Create a task to update the virus definitions.
- **Protection components disabled.** Some of the core protection components have been disabled manually by the end user. Create a task to restart the device and its components.
- **Threat unresolved.** One or more threats have been found by one of the Shields but could not be resolved. You should inspect the Device Settings configuration or examine the threat and resolve it manually from the Threats list in Device Details.
- **Threat quarantined.** One or more threats have been found by one of the Shields and automatically moved to quarantine. You should examine the threat and either delete or restore the threat manually from quarantine.
- **Threat found and resolved.** One of more threats have been found by one of the Shields and has been resolved automatically. No further action is needed.

- Patch Management
  - **Patch subscription expired.** Device is using an expired Patch Management subscription. Choose a new subscription with remaining available seats or purchase new seats.
  - **Patches failed to deploy.** One or more patches have failed to deploy to the device. View the patch itself to see possible reasons.
  - **Critical patches missing.** One or more critical/important patches are missing on the device. You should deploy them via the Patches page.
  - **Patches missing.** One or more low severity patches are missing on the device. You should deploy them via the Patches page.
  - **Patch scan failed.** Scan for missing patches has failed on the device. Create a task to scan the device again.

DEVICE LIST ACTIONS

TO SEARCH FOR A DEVICE

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

TO FILTER THE DEVICE LIST

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

NOTE Ensure you have selected the proper group to filter.

3. To filter devices, select one or more options from the following choices in the **Dynamic filters** menu:

   - **Device Status**: Activated devices, Safe, Vulnerable, In danger, Activating, Awaiting activation, Uninstall pending, Expired.
   - **Operating System**: Windows Workstation, Windows Server, Mac OS X.
   - **Superpowers**: Local Update Server, Master Agent.
   - **Last seen more than**: Week ago, Month ago.

4. To remove a filter, do one of the following:

- Click the small button in the top right corner of the filter name.
- Click into the **Dynamic filters** menu and backspace to remove the filter(s).

TO FILTER THE DEVICE LIST BY ALERTS

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

NOTE Ensure you have selected the proper group to filter.

3. To filter devices, select one or more options from the following choices in the **Filter alerts** menu:
   - Any alerts
   - Any muted alerts
   - **Device Management:** Offline 21+ days, Offline 14+ days, Obsolete OS, Restart needed, Agent outdated 21+ days, Device has been reinstalled, or Device has been migrated
   - **Antivirus:** Antivirus subscription expired, Some OS drivers missing, Agent outdated 21+ days, Virus definitions outdated 21+ days, Virus definitions outdated 14+ days, Protection components disabled, Threat unresolved, Threat quarantined, or Threat found and resolved
   - **Patch Management:** Patch subscription expired, Patches failed to deploy, Critical patches missing, Patches missing, or Patch scan failed
4. To remove a filter, select a different filter from the list or click **reset filter**.

NOTE Filters will only appear for alerts that have been triggered on your devices.

HIDING ALL ALERTS

1. Click **Devices**  .
2. Click **Hide alerts**.

TO EXPORT THE DEVICE LIST

You can export the complete list of the devices in your network from the Devices page. The list will include various details for each device, such as its IP address, Operating System, Group, and Subscriptions.

1. Click **Devices**  .
2. Click **Export device list**.

MANAGING ALERTS

Alerts are visible across your devices on the list to provide you insight on the current state of the devices across your network.

DISMISSING ALERTS

This option will dismiss an alert for a time, which will update your device status as well. You will not be able to view your dismissed alerts; however, the next time a risk check is run on the device, the alert may reappear.

1. Click **Devices**  .
2. Click the drop-down arrow beside an alert in the devices list.

3 Click **Dismiss**.

MUTING ALERTS

This option will mute an alert for the selected length of time, which will update your device status as well.

1 Click **Devices**  .
2 Click the drop-down arrow beside an alert in the devices list.
3 Select one of the following:

- Mute for one day
- Mute for one week
- Mute for two weeks
- Mute for one month
- Mute for one year
- Mute for the next century

4 To unmute an alert, click the crossed-out bell symbol beside the alert in the devices list, then click either **Unmute** or **Unmute this alert on all devices**.

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 OR SELECT DEVICES WITHIN MULTIPLE GROUPS

1 Click **Devices**  .
2 Select the check boxes of the devices you want to assign a new settings template to.

NOTE You can select devices from multiple groups by clicking the group names and selecting the check boxes of the chosen devices in each group.

3 Do one of the following:

- Click **Actions**, **Change Settings Template**.
- Click the **More** button next to the device, then click **Change Settings Template**.

4 Select a settings template.
5 Click **Change Settings Template**.

TO ASSIGN A SETTINGS TEMPLATE TO A GROUP OF DEVICES

1 Click **Devices**  .
2 Select the check box of a group.
3 Click **Actions**, **Change Settings Template**.
4 Select a settings template.
5 Click **Change Settings Template**.

REMOVING AND UNINSTALLING DEVICES

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

You can only remove and uninstall devices that are online. 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.

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

TO REMOVE AND UNINSTALL A DEVICE REMOTELY

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**, **Remove and Uninstall**.
   - For a single device, click the **More** button next to a device, then click **Remove and Uninstall**.
3. Click **Yes**.

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

TO PERMANENTLY REMOVE A DEVICE THAT CANNOT CONNECT TO THE NETWORK

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

To delete the device from the Management Console, first follow the To remove and uninstall a device procedure. Then:

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

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

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 to the left of the device list.

VIEWING AND CREATING DEVICE GROUPS

To view or create a group, go to the **Devices** menu and look at the Groups panel. If the Groups panel is not expanded, click **Expand panel** .

THE DEFAULT DEVICE GROUP

A default group is provided for you. This is the parent group and, although you can rename it, you cannot 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. Click **Add group**.
3. Type a group name.
4. Choose a parent group.
5. Select a settings template option in the **Group settings** list.
6. To update devices in the group from Avast servers, even if the settings template gets virus definitions and program updates from local update servers, select the **Always update from Avast servers** check box.
7. 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. Click the **More** button next to a group, then click **Add sub-group**.
3. Type a group name.
4. Choose a parent group.
5. To choose a settings template, do one of the following in **Group settings**:
   - Select the **Use settings template from the parent group** check box.
   - Choose an option from the list.
6. Click **Add group**.

TO EDIT A GROUP

1. Click **Devices**  .
2. Click the **More** button ⋮ next to a group, then click **Delete group**.
3. When asked to confirm, click **Delete**.

TO DELETE A GROUP

NOTE Any devices in the group need to be removed from it before the group can be deleted.

1. Click **Devices**  .
2. Click the **More** button ⋮ next to a group, then click **Edit group**.
3. Make your changes.
4. 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 is 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**.
- 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 with at least one device selected, click **Actions, Unselect all**.

CREATING TASKS ON THE DEVICE PAGE

You can create tasks on the **Devices** page or on the **Tasks** page. When you create tasks on the Devices 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 Select **Schedule the scan** and set the **Frequency** and **Schedule start date and time**.
7 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 Select **Schedule the message** and set the **Frequency** and **Schedule start date and time**.
6 Type a **Custom name** for the message.
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 Select **Schedule the update** and set the **Frequency** and **Schedule start date and time**.
6 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 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 Select **Schedule the shutdown** and set the **Frequency** and **Schedule start date and time**.
8 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
- Patch results
- 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 including build number. 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.

The **Patch results** tab details all the detected security and feature patches available for the device. The patches will display whether they have been installed on the device, or if there was an issue with deployment of the patch. See Patch Management for more information.

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/or delete files.

TO RESTORE OR 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**

VIEWING INFORMATION ON INDIVIDUAL ITERATIONS OF DEVICE TASKS

You can see additional information on the specific instances of repeating tasks, for example:

- Task progress.
- Time the task started.
- The results of the task.
- The next time the task is scheduled to run.

1. Click **Devices**  .
2. Click a device.
3. Click the **Tasks** tab.
4. Click a task.
5. Click an iteration of a task.

NOTE You can click the **More** button next to a task iteration to either **Stop** or **Delete** that iteration of the task.

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 has not been completed.

On this page, you can create tasks for all devices at once, 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 page shows you details of executed tasks, including the number of devices where the task is completed, and the number where the task is not 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 page, 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

Clicking any task lets you see the details of that task in three tabs: Overview, Devices, and Settings.

Filtering tasks helps you find the tasks you are looking for when you have many tasks scheduled, in progress, or completed.

TO SEE THE DETAILS OF A TASK

1. Click **Tasks**  .
2. Click a task.
3. Click any of the following tabs:

   - **Overview—**shows the overall results of the task, its schedule, and how many devices are running the chosen task.
   - **Devices—**displays a list of devices running the chosen task, task progress, and the last result separated by device.
   - **Settings—**displays the settings for the chosen task that were applied when the task was created.

TO SEARCH FOR A TASK

1. Click **Tasks**  .

2 In the **Task name** box, type part of the name of the task you are 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 Click the **Filters** button.
3 Click the **Dynamic** filters menu, then select one or more options from the following choices:

- **Task types**: Scan, Send message, Software update, Shutdown & Restart.
- **Task intervals**: One-time task, Recurring task.

4 To remove a filter, do one of the following:

- Click the small × button in the top right corner of the filter name.
- Click into the **Dynamic filters** menu and backspace to remove the filter(s).

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 cannot 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 **Devices** page or on the **Tasks** page. The difference is that when you create tasks on the Devices 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.

IMPORTANT Scheduled tasks will not run on devices added to the network after the creation of the task. Any scheduled tasks would have to be deleted and re-created to include the new devices.

SCANNING DEVICES

You can create the following types of scans:

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

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 perform 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 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**
   - **Full System Scan**
   - **Removable Media Scan**
   - **Custom Scan**
   - **Boot-time Scan (MS Windows only)**.
5. Select **Schedule the scan** and set the **Frequency** and **Schedule start date and time**.
6. Type a **Custom name** for the scan.
7. 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. Select **Schedule the message** and set the **Frequency** and **Schedule start date and time**.
6. Type a **Custom name** for your message.
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(s) 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. Select **Schedule the update** and set the **Frequency** and **Schedule start date and time**.
6. Type a **Custom name** for the update.
7. Click **Update**.

SHUTTING DOWN OR RESTARTING 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 Management Console. If you want to shut down individual devices, create a task from the Devices page.

TO SHUT DOWN OR RESTART 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 Type a message to notify your users before the shut down or restart.
6 Choose an option in the **Specify when the message is displayed** box.
7 Select **Schedule the shutdown** and set the **Frequency** and **Schedule start date and time**.
8 Type a **Custom name** for the shut down or restart task.
9 Click one of the following:

- **Restart**
- **Shutdown**
- **Schedule restart**
- **Schedule shutdown**

CHAPTER EIGHT:

PATCHES

On the Patches page, you can view and manage all the software patches for your devices.

Patch Management allows you to keep all your devices up to date with the latest feature and security patches for over 150 software vendors. This not only gives endpoint users all the latest features of their software, but also addresses the newest security threats. The Cloud Management Console makes it easy to identify and deploy patches from a central dashboard.

PATCH MANAGEMENT

Patch Management provides the following features:

- **Patches direct from vendor**—Automatically retrieves patches for Windows and 3rd-party applications to keep your devices up-to-date.
- **Flexible deployment schedules**—Schedule and deploy patches at your preferred times, or manually deploy on-demand to groups and individual devices.
- **Intuitive dashboard**—Manage all patches and view summaries of applied, missing, and failed patches.
- **Customizable patches**—Select which software vendors, products, and severity of patches you would like to scan and install and create exclusions for applications you do not want to patch.
- **Patch scan results**—Learn more about missing patches including specific updates, bulletin links, release dates, descriptions, and more.
- **Reports**—Determine the health and security of device software and applications.
- **Patch notifications**—Receive notifications when a new patch is found to be missing from your device(s) or has failed to deploy.

As part of the Patch Management process, you will need to decide when to scan, patch, and restart your devices, which devices to update, how to install patches, and which patches to install.

PREPARING DEVICES FOR PATCH MANAGEMENT

For uninterrupted patching, check these items before setting up patch management on devices:

- Ensure the user profile of the device's group policy in Active Directory allows program installations and upgrades.
- Ensure the device's hard drive has enough space for patches to be received and stored.
- Ensure that if the device's policy is set up to download patches from a local update server, the server is in the same network.
- Ensure the device is online at the time of patching.
- Ensure the device's Firewall settings allow patch installation.

PATCH SCANNING

A scan must be done to check devices for what patches they need. Scanning devices for missing patches is essential to patch management to identify what patches should be installed.

Patch scanning is a free feature available to all Avast Business Console users. By default, all devices that have a settings template are scanned once a day, and the result displayed on the Patches page. To change the frequency and time the scan runs, edit your settings template by following the To configure patch scanning procedure.

Patch scanning is a prerequisite for Patch Management, which is a paid feature and requires an additional license. Please see the Subscriptions section for details.

Choosing Devices to Update

Choosing the devices you want to update is a key part of determining how to set up patch deployment.

If you are updating all your devices, or a short list of devices, on a one-time basis, you may want to complete an ad hoc patch deployment from the Patches page.

If you are updating groups of devices, you may want to establish recurring patch management using a settings template. You can apply different settings templates to different device groups. For example, you could put all Windows Workstations into a group and apply a settings template that updates Windows the second and fourth Tuesday of every month. Leaving your Mac devices out of that group would reduce the time it takes for the updates to be applied.

Because each device can only have a single settings template applied to it, you may have to set up multiple settings templates that have the same settings for patch scanning and deployment. Patching using settings templates is discussed in further detail in the Patch Management via Settings Templates section.

NOTE All devices you want to patch must have a settings template with patch management enabled applied to them, even if you only want to do ad hoc installs.

Recurring versus Ad Hoc Patching

Missing patches can be installed on managed devices either through a one-time ad hoc deployment from the Patches page, or through a recurring deployment using a settings template. It may be necessary to apply patches through different methods depending on your network needs and the device. For example, there may be a critical patch for a server device that has patch deployment scheduled for the following week. In this instance, you may want to push the critical patch immediately rather than waiting for the scheduled deployment.

Patch via a settings template when:	Patch via the Patches page when:
You want to install on a regular basis	You want to install on a one-time basis
You want to apply a patch schedule to a group of devices	You want to patch most devices, or only a few specific devices
You want to set up a recurring patch schedule	You want to install patches immediately, or soon
You want to automatically deploy patches that meet certain criteria	You want to select patches to deploy from a list
You want to exclude patches from specific vendors or applications	You want to install patches that have been excluded from an automated install

Recurring Patches

Installing patches through settings templates lets you set up recurring installs of patches. Using a settings template, you can choose the patches you want to install and set up the time you want the install to start. With installation through settings templates, you set up your patching options, and then choose the effected devices by applying the settings template to a device group.

Using a settings template to install patches is best for setting up a recurring, ongoing patching schedule. You can even use multiple settings templates to arrange patches to be installed on different schedules according to their severity and importance. The schedule repeats with no actions from you, keeping your devices up to date and taking the work of patch management off your task list.

Ad hoc Patches

Doing an ad hoc deployment via the Patches page gives you the same options for choosing and installing patches. You can sort by the same options and set up the install and restart for time when users won't be interrupted. However, with ad hoc installs, you also choose the devices the patches are installed on from a list of devices instead of a device group.

Ad hoc installs are best for doing one-time patch installs. For example, if a high-profile security vulnerability is found in popular software that effects most of your users, you could do an ad hoc install to start the patching process right away, without worrying about scheduling the patch for a convenient time.

NOTE Please note that even if you're doing an ad hoc, one-time patch deployment, all devices you are patching must have a settings template with patch scanning applied to them.

Patching via the Patches page

When you select patches to deploy on the **Patches** page, the patches are added to the next deployment as scheduled in the applicable settings template. Patches you select are deployed only to the devices you select, not all devices that have the settings template applied to them.

You should use a one-time patch deployment if you want to deploy patches to individual devices instead of to all the devices that have a certain settings template applied to them. For example, if a patch has some risk associated with it, you may want to update only one device to see what the affect the patch has before deploying that patch to all devices. You can select multiple devices to deploy to. If you select multiple devices that have different settings templates, the deployment is added to each settings template, and each device is updated according to the schedule of the settings template applied to it.

The patches displayed for on the Patches page are the patches that have been found to be missing on any device that has been scanned. For example, if you select a patch to deploy, but you select a device that doesn't need that patch (Maybe because it doesn't have the required software), that patch is not deployed to that device.

IMPORTANT Ad hoc deployment does not add any patches to scheduled deployments on an ongoing basis. Patches that are excluded from settings templates will remain excluded. If you want to add patches on an ongoing, recurring basis, follow the To configure automatic patch deployment procedure.

TO MANUALLY DEPLOY PATCHES

1. Click **Patches**  .
2. In the left-hand pane, select the check boxes of the patches you would like to install.
3. In the right-hand pane, select the check boxes of the devices you would like to install the patches on.
4. Click **Action**, then click **Deploy on schedule**. The patch will be deployed on the selected devices according to the patch deployment schedule in their settings template(s).

TO IGNORE MISSING PATCHES

1. Click **Patches**  .
2. In the left-hand pane, select the check boxes of the patches you would like to ignore and remove from the list until the next scheduled scan for patches.
3. Click **Actions**, then click **Ignore**.

TO ROLL BACK APPLIED PATCHES

You may want to remove patches that have already been deployed if they cause unforeseen problems in your network. This option is only available for patches supporting uninstall functionality.

1. Click **Patches**  .
2. In the left-hand pane, select the check boxes of the deployed patches you would like to remove.
3. Click **Action**, then click **Roll back patch**.

NOTE You may search for patches by Bulletin ID/KB, vendor, release date, and patch status/severity.

Once you have successfully scanned and deployed patches on your devices, you can view the results of patch scans and deployment on your Dashboard.

CHAPTER NINE:

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 Workstation, Windows Server, and Mac OS X—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 custom template. However, the default template cannot be customized or deleted, though it can be renamed. 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

For more information please see the General Settings section.

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 single settings template contains settings for Windows Workstations, Windows Servers, and Mac OS X. You do not need to create separate policies for each operating system.

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		
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	X	
Wi-Fi Inspector	X		
Rescue Disk	X	X	
Passwords	X		

Creating and editing settings templates

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**
   - **Windows Server**
   - **Mac OS X**
3. Click the **Active Protection** tab, then perform any of the following:

   For both Windows Workstations and Windows Servers:

   - File Shield
   - Mail Shield
   - Web Shield
   - Anti-spam
   - Data Shredder
   - Sandbox

- Rescue Disk

For Windows Workstations only:

- Real Site
- Firewall
- Behavior Shield
- Webcam Shield
- Security Browser Extension
- Browser Cleanup
- Passwords
- SecureLine VPN
- Wi-Fi Inspector

For Windows Servers only:

- Exchange Server Protection
- SharePoint Server Protection

For Mac OS X:

- File Shield for Mac OS X
- Mail Shield for Mac OS X
- Web Shield for Mac OS X

4 Click the **General** Settings tab, then perform either of the following:

- General Settings for Windows Workstations and Windows Servers
- General Settings for Mac OS X

5 Click the **Antivirus settings** tab, then follow the Antivirus Settings for Windows Workstations and Windows Servers procedure.
6 Click the **Troubleshooting** tab, then follow the Troubleshooting Settings for Windows Workstations and Windows Servers procedure.
7 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

NOTE Any devices using the settings template need to be removed from it before the template can be deleted.

1. Click **Device settings**  .
2. Click the **More** button at the right of a template.
3. Click **Delete**.

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

You cannot 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.

TO CHANGE THE SETTINGS TEMPLATE FOR A GROUP OR DEVICE VIA THE ASSIGNED GROUPS AND DEVICES SCREEN

1. Click **Device settings**  .
2. Click the **Settings used** column in the settings template.
3. Select the check box or boxes beside the group(s) or device(s) you would like to change the settings template for.
4. Click **Change settings**.

ACTIVE PROTECTION

NOTE Most Active Protection features are installed with the Avast Business Antivirus, but these components can be uninstalled and reinstalled as needed via the settings template. Mac OS X protection components cannot be installed or uninstalled but can be turned off.

TO INSTALL OR UNINSTALL AN ACTIVE PROTECTION COMPONENT

1. Click **Device Settings**  , then click the name of a settings template.
2. Click either of the following tabs:
   - **Windows Workstation**
   - **Windows Server**
3. Click the **Active Protection** tab.
4. Do one of the following:
   - If the component is not installed, click the **Install this component link** next to the component you want to install. Then click **I understand, install component**.
   - If the component is already installed, click the next to the component you wish to uninstall, then click **Uninstall this component**. Click **I understand, uninstall component**.
5. Click **Apply Changes**.

Enabling and Disabling Components

Nearly all the shields and tools available in Avast Business Antivirus can be enabled or disabled in the settings templates. This is especially useful if you are trying to install only a few of the components on a server, or just keeping your number of tools to a minimum. Some tools, however, can only be installed or uninstalled entirely, such as Sandbox and Rescue Disk.

To enable or disable components

1. Click **Device settings**  .
2. Click the name of a settings template.
3. Click one of the following tabs:
   - **Windows Workstation**
   - **Windows Server**
   - **Mac OS X**
4. Click the **Active Protection** tab.
5. Move the slider to  to enable the component. Move the slider to  to disable the component.
6. Click **Apply Changes**.

File Shield for Windows Workstations and Windows Servers

For Mac OS X settings, see 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 always keep this shield turned on and only make configuration changes if you have an advanced understanding of malware protection principles.

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.
- **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 files with custom extensions**, then type the custom extensions to scan.
- **Scan all files**
- **Do not scan files on remote shares**
- **Do not scan files on removable media**

11 Click **Apply Changes**.

NOTE You can use wildcard characters. For information on using wildcard characters, see About file paths in Settings Templates.

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

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 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.

1 In the Customization menu for **File Shield**, click the **Exclusions** tab.
2 Select any of the following check boxes:

- **R**—Read
- **W**—Write
- **X**—Execute

3 Type a file name, path, or extension, then click **Add**.
4 Repeat step 3 until all your chosen file names, paths, and extensions are excluded.
5 Click **Apply Changes**.

TO REMOVE A FILE SHIELD EXCLUSION

1 In the Customization menu for **File Shield**, click the **Exclusions** tab.
2 Next to the exclusion you want to remove, click  .
3 Click **Apply Changes**.

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

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

1. In the Customization menu for **File Shield**, click the **Actions** tab.
2. Click one of the following tabs:
   - **Virus**
   - **PUP**
   - **Suspicious**
3. Select an option in the **Choose what action Avast will perform after finding a virus/PUP/suspicious file** box.
4. If applicable, select an option in the **if the action fails, use** box.
5. In the **Options** section, select any of the following check boxes:
   - **Show notifications for actions**
   - **Perform the selected action when the system restarts**
6. In the **Processing of 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**
7. Click **Apply Changes**.

TO CONFIGURE WHICH ARCHIVE FILES AVAST TRIES TO UNPACK DURING A FILE SHIELD SCAN

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.

1. In the Customization menu for **File Shield**, click the **Packers** tab.
2. Do one of the following:
   - Select **All packers**.
   - Clear the **All** packers check box, then select the check boxes of individual packers.
3. Click **Apply Changes**.

TO CONFIGURE FILE SHIELD SENSITIVITY

You can adjust the sensitivity of the Avast Antivirus File Shield scan.

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.

1. In the Customization menu for **File Shield**, click the **Sensitivity** tab.
2. Select an option in the **Heuristics Sensitivity** box.
3. Select any of the following check boxes:
   - **Use code emulation**
   - **Test whole files**
   - **Scan for potentially unwanted programs (PUPs)**
4. Click **Apply Changes**.

TO GENERATE AND CONFIGURE FILE SHIELD REPORTS

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

1. In the Customization menu for **File Shield**, click the **Report File** tab.
2. Select the **Generate Report File** check box.
3. Type a name in the **File Name** box.
4. Select the **File Type**.
5. Select an option in the **If File Exists** box.
6. Select any of the **Reported Items** you want to include in the report:
   - **Infected items**
   - **Hard errors**
   - **Soft errors**
   - **OK items**
   - **Skipped items**
7. Click **Apply Changes**.

File Shield for Mac OS X

For Windows Workstations and Windows Servers settings, see 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 always keep this shield turned on and only make configuration changes if you have an advanced understanding of malware protection principles.

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**.

To exclude 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.

IMPORTANT For information on how to use file paths, see About File Paths in Settings Templates.

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

To remove a File Shield Exclusion for Mac OS X

1. In the **Active Protection** tab for Mac OS X, click the **Customize** link in the **File Shield** section.
2. Next to the exclusion you want to remove, click  .
3. Click **Apply Changes**.

Mail Shield for Windows Workstations and Windows Servers

IMPORTANT We do not recommend you install this component on a server OS that is also running Microsoft Exchange. The Exchange and Anti-spam components handle Exchange-level filtering and will conflict with this component.

For Mac OS X settings, see Mail Shield for Mac OS X.

Mail Shield checks incoming and outgoing e-mail 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 e-mail account via an Internet browser, your devices are protected by other Shields.

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**.

To configure notes and warnings for e-mails scanned by Mail Shield

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

The following settings attach notes to the bottom of incoming or outgoing e-mails:

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

The following settings attach notes to the subject line of e-mails:

Add a warning to the subject line of infected e-mails—Tags e-mails with the subject line **VIRUS** if the e-mail contains malware. You can also specify your own tag in the text box.

1. In the Customization menu for **Mail Shield**, click the **Behavior** tab.
2. 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.

3. 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**
4. Click **Apply Changes**.

TO SCAN SSL CONNECTIONS WITH MAIL SHIELD

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

1. In the Customization menu for **Mail Shield**, click the **SSL Scanning** tab.
2. Select the **Scan SSL connections** check box.
3. Click **Apply Changes**.

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

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

1. In the Customization menu for **Mail Shield**, click the **Actions** tab.
2. Click one of the following tabs:
   - **Virus**
   - **PUP**
   - **Suspicious**
3. Select an option in the **Choose what action Avast will perform after finding a virus/PUP/suspicious file** box.
4. If applicable, select an option in the **if the action fails, use** box.
5. 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.
6. 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**
7. Click **Apply Changes**.

TO CONFIGURE WHICH ARCHIVE FILES AVAST TRIES TO UNPACK

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.

1. In the Customization menu for **Mail Shield**, click the **Packers** tab.
2. Do one of the following:
   - Click **All packers**.
   - Clear the **All packers** check box, then select the check boxes of individual packers.
3. Click **Apply Changes**.

TO CONFIGURE MAIL SHIELD SENSITIVITY

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.

1. In the Customization menu for **Mail Shield**, click the **Sensitivity** tab.
2. Select an option in the **Heuristics Sensitivity** box.
3. Select any of the following check boxes:
   - **Use code emulation**
   - **Test whole files**
   - **Scan for potentially unwanted programs (PUPs)**
4. Click **Apply Changes**.

TO GENERATE AND CONFIGURE MAIL SHIELD REPORTS

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

1. In the Customization menu for **Mail Shield**, click the **Report File** tab.
2. Select the **Generate Report File** check box.
3. Type a name in the **File Name** box.
4. Select the **File Type**.

5 Select an option in the **If File Exists** box.
6 Select any of the **Reported Items** you want to include in the report:

- **Infected items**
- **Hard errors**
- **Soft errors**
- **OK items**
- **Skipped items**

7 Click **Apply Changes**.

Mail Shield for Mac OS X

IMPORTANT We do not recommend you install this component on a server OS that is also running Microsoft Exchange. The Exchange and Anti-spam components handle Exchange-level filtering and will conflict with this component.

For Windows Workstations and Windows Servers settings, see Mail Shield for Windows Workstations and Windows Servers.

Mail Shield checks incoming and outgoing e-mail 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 e-mail account through an Internet browser, your devices are protected by other Shields.

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 for Mac OS X

1 In the **Active Protection** tab for **Mac OS X**, click the **Customize** link in the **Mail Shield** section.
2 In the **Exclusion** list, do the following

- Select a mail service.
- Type a host name.
- Click **Add**.

3 Repeat step 2 until the list of exclusions is complete.
4 Click **Apply Changes**.

To remove a Mail Shield exclusion for Mac OS X

1. In the **Active Protection** tab for **Mac OS X**, click the **Customize** link in the **Mail Shield** section.
2. Next to the exclusion you want to remove, click  .
3. Click **Apply Changes**.

Web Shield for Windows Workstations and Windows Servers

IMPORTANT We do not recommend you install this component on a server OS that is also running Microsoft Exchange. The Exchange and Anti-spam components handle Exchange-level filtering and will conflict with this component.

For Mac OS X settings, see 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 configure 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 **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 lesser-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 lesser-known web applications is authorized and is not scanned for malware by the Shield.
8. In the **HTTPS scanning** section, select **Enable**, then select any of the following check boxes:
   - Use intelligent stream scanning
   - Do not scan trusted sites
   - Block malware URLs
   - Script scanning
9. Click **Apply Changes**.

To configure the file types Web Shield scans

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.

1. In the Customization menu for **Web Shield**, click the **Web Scanning** tab.
2. To scan every file when downloaded, select the **Scan all files** check box.
3. 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**.
4. Repeat step 3 until all extensions are added.
5. To not unpack archives even if they have trusted digital signatures, select the **Do not unpack archives with valid digital signatures** check box.
6. Click **Apply Changes**.

To remove a file type or MIME-type from Web Shield scans

1. In the Customization menu for **Web Shield**, click the **Web Scanning** tab.
2. Next to the file type or MIME-type you want to remove, click .
3. Click **Apply Changes**.

To exclude URLs, MIME-types, and processes from Web Shield

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 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. In the Customization menu for **Web Shield**, click the **Exclusions** tab.
2. 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 MIME-type and click **Add**.
   - To exclude a process, in the **Use Processes to Exclude** section, select the **Enable** check box, then type the path to the process and click **Add**.
3. Repeat step 2 until all your chosen URLs, MIME-types, and processes are excluded.
4. Click **Apply Changes**.

To remove an exclusion from a file, file type, or location in Web Shield

1. In the Customization menu for **Web Shield**, click the **Exclusions** tab.
2. Next to the exclusion you want to remove, click .

3 Click **Apply Changes**.

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

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

1 In the Customization menu for **Web Shield**, click the **Actions** tab.
2 Click one of the following tabs:

- **Virus**
- **PUP**
- **Suspicious**

3 Select an option in the **Choose what action Avast will perform after finding a virus/PUP/suspicious file** box.
4 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.
5 Click **Apply Changes**.

TO CONFIGURE WHICH ARCHIVE FILES AVAST TRIES TO UNPACK

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.

1 In the Customization menu for **Web Shield**, click the **Packers** tab.
2 Do one of the following:

- Select **All packers**.
- Clear the **All packers** check box, then select the check boxes of individual packers.

3 Click **Apply Changes**.

TO CONFIGURE WEB SHIELD SENSITIVITY

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

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.

1. In the Customization menu for **Web Shield**, click the **Sensitivity** tab.
2. Select an option in the **Heuristics Sensitivity** box.
3. Select any of the following check boxes:
   - **Use code emulation**
   - **Test whole files**
   - **Scan for potentially unwanted programs (PUPs)**
4. Click **Apply Changes**.

To block URLs with Web Shield

Site blocking lets you create a custom list of URLs that users cannot 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.

1. In the Customization menu for **Web Shield**, click the **Site Blocking** tab.
2. Select the **Enable site blocking** check box.
3. Type a **URL** and click **Add**.
4. Repeat step 3 until you have added all the URLs you want to block.
5. Click **Apply Changes**.

To remove a site block in Web Shield

1. In the Customization menu for **Web Shield**, click the **Site Blocking** tab.
2. Next to the block you want to remove, click .
3. Click **Apply Changes**.

To exclude URLs from Web Shield script scanning

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 Excluding Files, Folders, or URLs from Scans and Shields for Windows Workstations and Windows Servers.

1. In the Customization menu for **Web Shield**, click the **Script Exclusions** tab.
2. Select the **Enable** check box.
3. Type a URL and click **Add**.

4 Repeat step 3 until you have added all the URLs you want to exclude.
5 Click **Apply Changes**.

TO REMOVE A URL EXCLUSION FROM WEB SHIELD SCRIPT SCANNING

1 In the Customization menu for **Web Shield**, click the **Script Exclusion** tab.
2 Next to the exclusion you want to remove, click  .
3 Click **Apply Changes**.

TO GENERATE AND CONFIGURE WEB SHIELD REPORTS

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

1 In the Customization menu for **Web Shield**, click the **Report File** tab.
2 Select the **Generate Report File** check box.
3 Type a name in the **File Name** box.
4 Select the **File Type**.
5 Select an option in the **If File Exists** box.
6 Select any of the **Reported Items** you want to include in the report:

- **Infected items**
- **Hard errors**
- **Soft errors**
- **OK items**
- **Skipped items**

7 Click **Apply Changes**.

WEB SHIELD FOR MAC OS X

IMPORTANT We do not recommend you install this component on a server OS that is also running Microsoft Exchange. The Exchange and Anti-spam components handle Exchange-level filtering and will conflict with this component.

For Windows Workstations and Windows Servers settings, see 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 CONFIGURE 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 Click the **Customize** link in the **Web Shield** section.
6 Click the **Main Settings** tab.
7 Do any of the following:

- Select the check box in the **Enable IPv6** section to enable scanning on devices using Internet Protocol version 6.
- Select the check box in the **Scan secured connections** section to enable scanning of sites that are accessed over secured connections. To only scan secured connections from browsers, and not other applications, select the **Scan secured connections from browsers only** check box.
- Select the check box in the PUP section to list background programs such as spyware, that could potentially be downloaded.

8 Click **Apply Changes**.

To exclude safe URLs from the Web Shield scan for Mac OS X

1 In the **Active Protection** tab for **Mac OS X**, click the **Customize** link in the **Web Shield** section.
2 In the **Exclusion** list, do the following:

- Select **http** or **https**.
- Type a host name.
- Click **Add**.

3 Repeat step 2 until the list of exclusions is complete.
4 Click **Apply Changes**.

To remove a Web Shield exclusion for Mac OS X

1 In the **Active Protection** tab for **Mac OS X**, click the **Customize** link in the **Web Shield** section.
2 Next to the exclusion you want to remove, click  .
3 Click **Apply Changes**.

Real Site for Windows Workstations

Real Site protects against DNS (Domain Name System) hijacking to ensure you get to the actual website you want to visit. Real Site does not have any configurable options but is available to users in Avast Business Antivirus.

Anti-spam for Windows Workstations and Windows Servers

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

You can configure the active Anti-spam settings 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 e-mails
- when to retrieve new rules
- enabling LiveFeed

- Microsoft Outlook features

TO CONFIGURE ACTIVE ANTI-SPAM

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 e-mails, select the **Mark** check box, then type a message.
9. To include a message of the Subject line of phishing e-mails, select the **Mark** check box, then type a message.
10. To whitelist recipients of outbound e-mails automatically, select one of the following check boxes:
    - **Add recipients of outbound e-mails 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 e-mails 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**.

TO ADD E-MAIL ADDRESSES TO THE ANTI-SPAM WHITE LIST

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

1. In the Customization menu for **Anti-**spam, click the **White List** tab.
2. Type an e-mail address in the **White List** box and click **Add**.

NOTE Type the full e-mail address. Wildcard characters are not permitted.

3. Repeat step 2 until all e-mail addresses are added.
4. Click **Apply Changes**.

TO REMOVE AN E-MAIL ADDRESS FROM THE ANTI-SPAM WHITE LIST

1. In the Customization menu for **Anti-**spam, click the **White List** tab.
2. Next to the exclusion you want to remove, click  .

3 Click **Apply Changes**.

NOTE In Avast Business Antivirus versions 19.5 and newer, you can also overwrite local whitelist settings by clicking the check box next to **Advanced settings**.

TO ADD E-MAIL ADDRESSES TO THE ANTI-SPAM BLACK LIST

The Black List is a list of senders whose e-mails are always treated as spam.

1 In the Customization menu for **Anti-**spam, click the **Black List** tab.
2 Type an e-mail address in the **Black List** box and click **Add.**

NOTE Type the full e-mail address. Wildcard characters are not permitted.

3 Repeat step 2 until all e-mail addresses are added.
4 Click **Apply Changes**.

TO REMOVE AN E-MAIL ADDRESS FROM THE ANTI-SPAM BLACK LIST

1 In the Customization menu for **Anti-**spam, click the **Black List** tab.
2 Next to the exclusion you want to remove, click  .
3 Click **Apply Changes**.

NOTE In Avast Business Antivirus versions 19.5 and newer, you can also overwrite local blacklist settings by clicking the check box next to **Advanced settings**.

FIREWALL FOR WINDOWS WORKSTATIONS

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

TO ASSIGN A PROFILE TO A DEFINED NETWORK AND DEFINE NETWORKS

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 for **Firewall** in the **Antivirus Protection** 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**, end users can set their own profile for the network.

8 If applicable, select the **Overwrite 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 If you would like to define networks, do the following:

- In the **Network name** box, type a name for the network.
- In the **MAC address of network router** box, type the network box's MAC address.
- In the **Profile** box, select a profile.
- Click **Add**.

10 Repeat step 9 for all networks you want to add.
11 Click **Apply Changes**.

TO UPDATE OR EDIT A DEFINED NETWORK

1 In the Customization menu for **Firewall**, click the **Networks** tab.
2 In the **Defined networks** box, click on the network you would like to make changes to.
3 Make your changes.
4 Click **Update**.

From the **Networks** tab you can also select check boxes to enable or disable the following:

- **Internet Connection Sharing mode**—allows a trusted user to connect to the internet through your PC, or to troubleshoot problems with devices, such as your printer, connected to the internet via your PC. Ticking this option opens certain ports which are usually closed, decreasing the level of security.
- **Allow all connections with Friends when in Private mode**—allows all networks listed as Friends when you are connected to a Private mode network.
- **Disable controlling network profiles by the console**—lets the local user control network profile selection entirely. A restart is required to propagate change of the settings on the clients' computers. The rest of the firewall settings remain controlled by the console.

TO OVERRIDE USER-DEFINED FIREWALL RULES

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

1 In the Customization menu for **Firewall**, click the **Rules** tab.
2 Select the **Control all rules via the web console** check box.
3 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 In the Customization menu for **Firewall**, click the **Rules** tab.
2 Click the **System Rules** tab.
3 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.

4 Click **Apply Changes**.

TO DEFINE A DEFAULT FIREWALL RULE FOR APPLICATIONS

You can define a default rule for applications that do not have a specific rule defined. The default rule is applied to any application that does not appear in the list on this page.

1 In the Customization menu for **Firewall**, click the **Rules** tab.
2 Click the **Application Rules** tab.
3 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.

4 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. In the Customization menu for **Firewall**, click the **Rules** tab.
2. Click the **Application Rules** tab.
3. Click **Add application rule**.
4. In **Application name** box, type a name for the rule.
5. 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**.

6. 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.
7. Click **Add 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 **Set custom packet rules**.
5. To add a new rule, click **Add new rule** and 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 action.
   - 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.

6 Click **Update**.
7 Click **Add application rule**.
8 Click **Apply Changes**.

NOTES

- To edit an application rule, next to the rule click  , make your changes, then click **Save application rule**.
- To delete a rule, next to the rule click  , then click **Yes**.

TO DEFINE FIREWALL ADVANCED PACKET RULES

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

1 In the Customization menu for **Firewall**, click the **Rules** tab.
2 Click the **Advanced packet rules** tab.

TO ADD A NEW PACKET RULE

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 To edit any of the existing rules, click a rule, make your changes, then click **Update**.
5 To disable a rule, click a rule. In the **Enabled** column, clear the check box, then click **Update**.
6 Click **Apply Changes**.

TO EDIT A PACKET RULE

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

1 On the **Advanced packet rules** tab, click any custom rule you have created.
2 Make your changes, then click **Update**.
3 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, then click **Update**.
3. 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 **Yes**.
3. Click **Apply Changes**.

BEHAVIOR SHIELD 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 DEFINE WHAT BEHAVIOR SHIELD DOES WITH SUSPICIOUS PROGRAMS

You can configure how Behavior Shield deals with suspicious files that it encounters.

1. In the **Active Protection** tab for **Behavior Shield**, click the **Customize** link.
2. In the **Main Settings** section, select a check box from the following options to define how to deal with suspicious programs:
   - **Always ask**
   - **Automatically move detected threats to the Chest**
   - **Automatically move known threats to the Chest**
3. Click **Apply Changes**.

TO EXCLUDE LOCATIONS FROM BEHAVIOR SHIELD SCANS

You can set up file locations that are excluded from Behavior Shield.

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 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. In the **Active Protection** tab for **Behavior Shield**, click the **Customize** link.
2. In the **Exclusions** section, type a file location to exclude and click **Add**.
3. Repeat step 2 until all locations are added.
4. Click **Apply Changes**.

To remove an exclusion from Behavior Shield

1. In the **Active Protection** tab for **Behavior Shield**, click the **Customize** link.
2. Next to the exclusion you want to remove, click  .
3. Click **Apply Changes**.

Webcam Shield 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 set the Webcam Shield mode

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 settings template 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 settings template, 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.

1. In the **Active Protection** tab for **Webcam Shield**, click the **Customize** link.
2. 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 the setting template's application permission lists are disabled. No applications are allowed to use the webcam.

3. To disable end users' lists and only use the one configured in your settings template, select the **Overwrite the application list which was already set by the user** check box.
4. Click **Apply Changes**.

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

TO CREATE A WEBCAM ACCESS LIST

1. In the Active Protection tab for Webcam Shield, click the Customize link.
2. 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**.

3. Repeat step 2 until you have added all the applications you want to block and/or allow.

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

4. 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.

5. Click **Apply Changes**.

SECURITY BROWSER EXTENSION FOR WINDOWS WORKSTATIONS

Security Browser Extension is a web browser extension designed to improve online security and overall experience when browsing the Internet. Security Browser Extension does not have any configurable options but is available to users in Avast Business Antivirus.

EXCHANGE SERVER PROTECTION FOR WINDOWS SERVERS

Exchange Server protection is available for Windows Servers and protects your Exchange Server from threats.

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**.

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

1 In the **Customization** menu for **Exchange Server protection**, click the **Actions** tab.
2 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**

3 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**

4 Click **Apply Changes**.

TO BLOCK E-MAIL ATTACHMENTS ON EXCHANGE SERVERS

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

1 In the **Customization** menu for **Exchange Server protection**, click the **Blocking** tab.
2 Select the **Enable attachment blocking by name** check box.
3 Type a filename mask and click **Add**.
4 Repeat step 3 until you have added all the attachment filenames you want to block.
5 To configure the file that replaces the attachment, type in the following boxes:

- **Filename replacement**
- **Replace with**

6 Click **Apply Changes**.

SHAREPOINT SERVER PROTECTION FOR WINDOWS SERVERS

SharePoint server protection is available for Windows servers and protects your SharePoint Server from threats. SharePoint server protection does not have any configurable options but is available to users in Avast Business Antivirus.

Browser Cleanup for Windows Workstations

Browser Cleanup is available for Windows Workstations and removes unwanted browser add-ons and toolbars. Browser Cleanup does not have any configurable options but is available to users in Avast Business Antivirus.

Data Shredder for Windows Workstations and 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 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 or increase/decrease the number using the plus and minus signs in the box.
8. Click **Apply Changes**.

Sandbox for Windows Workstations and 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 one of the following tabs:
   - **Windows Workstation**
   - **Windows Server**

4 Click the **Active Protection** tab.
5 Click the **Customize** link in the **Sandbox** section.
6 Click the **Sandbox Storage** tab.
7 Choose 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**.

TO CONFIGURE SANDBOX WEB BROWSER OPTIONS

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.

1 In the **Customization** menu for **Sandbox**, click the **Web Browsers** tab.
2 To save trusted downloaded files outside the Sandbox location, select the **Save trusted downloaded files outside the sandbox** check box.
3 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.

4 To save virtualized web browser files, select the **Cache web browser files (sandbox will not be automatically deleted)** check box.
5 To clean up Sandbox storage on a recurring basis, 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.

6 Click **Apply Changes**.

TO SET WHICH APPLICATIONS ARE VIRTUALIZED IN SANDBOX

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 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 following procedure.

IMPORTANT For information on how to use file paths, see About File Paths in Settings Templates.

1 In the **Customization** menu for **Sandbox**, click the **Virtualized Processes** tab.
2 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**.

3 Repeat step 2 until all applications and folders are added.
4 Click **Apply Changes**.

TO STOP VIRTUALIZING A PROCESS IN SANDBOX

1 In the **Customization** menu for **Sandbox**, click the **Virtualized Processes** tab.
2 Next to the process you want to stop virtualizing, click  .
3 Click **Apply Changes**.

TO SPECIFY LOCATIONS THAT CANNOT BE ACCESSED BY VIRTUALIZED APPLICATIONS

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.

1 In the **Customization** menu for **Sandbox**, click the **Privacy** tab.
2 In the **Private Pre-set Locations** select one of the following for each location:

- **Blocked**
- **Allowed**

3. For user-defined locations, type a file path, click select either **Blocked** or **Allowed**, then click **Add**.
4. Repeat step 3 until all locations are defined.
5. Click **Apply Changes**.

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

1. In the **Customization** menu for **Sandbox**, click the **Privacy** tab.
2. Next to the process you want to stop virtualizing, click .
3. Click **Apply Changes**.

TO SPECIFY LOCATIONS THAT WILL NOT BE VIRTUALIZED

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.

1. In the **Customization** menu for **Sandbox**, click the **Exclusions** tab.
2. Type a file path and click **Add**.
3. Repeat step 2 until you have added all the paths you want to exclude.
4. Click **Apply Changes**.

TO REMOVE AN EXCLUSION FROM A VIRTUALIZED LOCATION

1. In the **Customization** menu for **Sandbox**, click the **Exclusions** tab.
2. Next to the exclusion you want to remove, click .
3. Click **Apply Changes**.

TO GIVE PERMISSION FOR A VIRTUALIZED APPLICATION TO ACCESS THE INTERNET

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

1. In the **Customization** menu for **Sandbox**, click the **Internet access** tab.
2. 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**
3. 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 have identified all the applications you want to access the Internet.
4. Repeat step 3 until you have added all the paths you want to exclude.

5 Click **Apply Changes**.

TO REMOVE PERMISSION FOR A VIRTUALIZED APPLICATION TO ACCESS THE INTERNET

1 In the **Customization** menu for **Sandbox**, click the **Internet Access** tab.
2 Next to the application you want to prevent from accessing the Internet, click .
3 Click **Apply Changes**.

SECURELINE VPN FOR WINDOWS WORKSTATIONS AND WINDOWS SERVERS

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 does not have any configurable options but is available to users in Avast Business Antivirus.

NOTE While SecureLine VPN is available for both Windows Workstations and Servers, the component only appears in the Windows Workstations tab of the Settings Template.

WI-FI INSPECTOR FOR WINDOWS WORKSTATIONS

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 does not have any configurable options but is available to users in Avast Business Antivirus.

RESCUE DISK FOR WINDOWS WORKSTATIONS AND 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 does not have any configurable options but is available to users in Avast Business Antivirus.

PASSWORDS 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 does not have any configurable options but is available to users in Avast Business Antivirus.

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.

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.
   - **Reputation Services**—allows Avast to query their file reputation database to help make security decisions
   - **Debug logging**—Records operations, processes, and errors that occur. Enabling this will create very large log files on the target devices.
   - **Avast tray icon**—Displays an icon in the tray.
6. In the When to update section, choose automatic or manual updates for the following:
   - **Virus definitions updates**
   - **Program updates**
7. If you are using devices with Antivirus version 18.4 and older, click the dropdown and choose an option for **Virus definitions updates and Program updates**:
   - Via available **Local Update Servers**
   - Directly from Avast Update Servers
8. 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.
   - Select **SOCKS v4 proxy**, then select an address and port.
9. Click **Apply Changes**.

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 definitions 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 you are using devices with Antivirus version 18.4 and older, click the dropdown and choose an option for **Virus definitions updates and Program updates**:
   - Via available **Local Update Servers**
   - Directly from Avast Update Servers
8. Click **Apply Changes**.

Setting up Master Agents and Local Update Servers

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 or Local Update Server in any Settings Template.

Ideally, the devices you choose to be Master Agents should always be accessible to other devices on the network and available when other workstations need to update. If you set up multiple Master Agents, your devices can update from another even if one is unavailable.

You will have to add a device via the Devices tab before you can set it up as a Master Agent. Please see the How to Add Devices section for more details.

NOTE Devices and the Management console still communicate directly for licensing, usage date, and threat notifications.

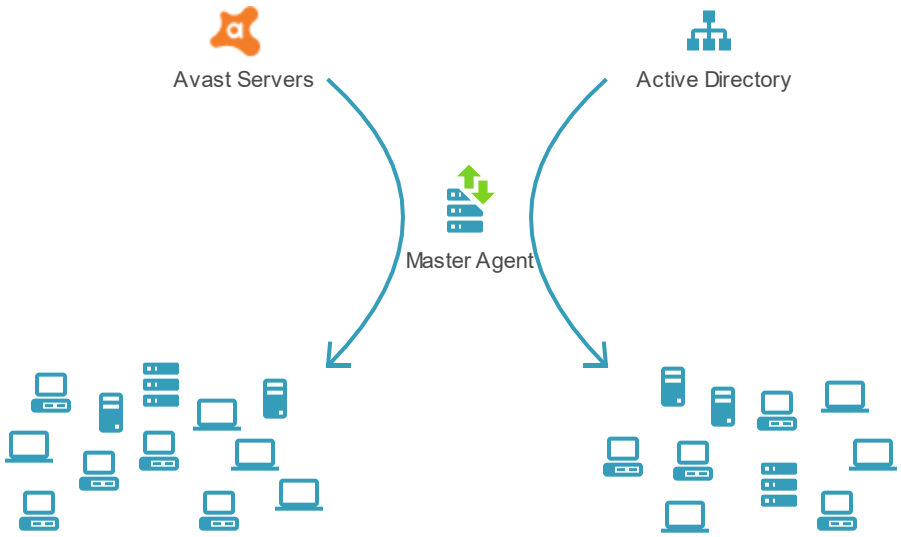
Master Agent requirements

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. Select an operating system in the **Filter devices** list and/or 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 AS A LOCAL UPDATE SERVER

Master Agents can be used by devices 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 settings template.
3 Click one of the following tabs matching the device type this template will be applied to:

- **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.

NOTE When it is used to provide updates to other devices, a Master Agent is referred to as a Local Update Server or an Update Mirror.

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. Click the **Master Agents** tab.
3. Move the slider 

next to the Master Agent to **On**.
4. Select the IP address of your Master Agent device in the **Select mirror IP address** list.
5. Click **Turn ON**.

To turn a Master Agent off

1. Click **General Settings** .
2. Click the **Master Agents** tab.
3. Move the slider 

next to the Master Agent to **Off**.
4. 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. Click the **Master Agents** tab.
3. Move the slider 

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

Antivirus Settings

Antivirus settings for Windows Workstations and Windows Servers

The Antivirus settings of settings templates include:

- **DeepScreen**—Enable to run suspicious programs that are not 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

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 one of the following:
   - **Always block suspicious files**
   - **Allow me to run suspicious files**
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**.

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

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 In the **Antivirus Settings** tab, click the **Exclusions** tab.
2 In the **Exclusions** section, click one of the following tabs:

- **File Paths**
- **URL Addresses**
- **DeepScreen**
- **Hardened Mode**

3 Next to the exclusion you want to remove, click  .
4 Click **Apply Changes**.

TROUBLESHOOTING SETTINGS

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.
- **Limit program access for Guest account**—Prevents a Guest user logged into one of your devices from accessing or altering Avast Business Antivirus files.
- **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**
- **Limit program access for Guest account**
- **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**.

PATCH MANAGEMENT VIA SETTINGS TEMPLATES

Starting a trial or purchasing a license for patch management includes patching for applications from 150 different software vendors. Only missing patches, discovered by patch scans, are installed. Because only patches that are found to be missing are deployed, it's a good idea to schedule automatic deployment of patches after the scan for missing patches is complete. For example, if you schedule the scan and deployment at 22:00 daily and a scan discovers a missing patch at 22:01 on Tuesday, that patch will not be deployed until 22:00 on Wednesday. The amount of time a scan for missing patches takes depends on the number of patches being searched for and the number of devices being scanned.

If you want to have different devices or groups of devices to have different patching schedules or to exclude different application patches, you can set up multiple settings templates. Because devices can only have one settings template applied to them at a time, you may need to create multiple settings templates with the same Antivirus options, but different patch deployment schedules.

If you don't want to install patches for certain applications, or patches from specific vendors, you can customize patch exclusions in the settings template. Patches that you exclude from a settings template can still be installed using an ad hoc patch deployment on the Patches page.

IMPORTANT When you enable patch deployment on a device, Windows Defender is disabled on that device.

ENABLING OR DISABLING PATCH MANAGEMENT

When a license or trial of Patch Management is purchased and applied to a device, patch scanning is automatically enabled for that device. You can disable this feature according to your network needs and preferences. For example, if you want the patches for a specific group of devices to not be scanned or managed by the Cloud Management Console, you can disable patch scanning by ensuring a Patch Management subscription is not applied to the device(s) or removing the subscription, if there is one.

If Patch Management is enabled for your devices and you want them to scan and/or deploy patches automatically, you need to configure this in the settings templates. Apply the template to the devices

and groups you want to automatically perform patch scanning and deployment by following the To apply a template to a device or device group procedure.

Configuring Patch Management

In settings templates, you can alter the settings for scheduled patch scans, how and when missing patches are deployed, customize patch exclusions, and decide whether to automatically restart endpoint devices after patch deployment.

To configure patch scanning

1. Click **Device settings**  .
2. Click the name of a settings template.
3. Click the **Patch Management** tab.
4. In the **Step 1. Scan for missing patches** section, select one of the following scan frequencies:
   - **Daily**—In the **At** box, select the hour and minute when the scans should occur.
   - **Weekly**—In the **Every** box, select the day of the week when the scans occur, then select the hour and minute.
   - **Monthly**—In the **Every** box, select the day of the month when the scans occur, then select the hour and minute.

IMPORTANT If you are performing monthly scans, please ensure the day of the month you've chosen occurs every month. For example, do not choose the 31st day of the month unless you specifically want to skip scanning on months without 31 days.

5. Click **Apply Changes**.

To configure automatic patch deployment

1. Click **Device settings**  .
2. Click the name of a settings template.
3. Click the **Patch Management** tab.
4. In the **Step 2. Deploy patches** section, select one of the following options for what occurs after patch scans:
   - **Do not deploy patches**. Patches will need to be deployed manually.
   - **Deploy patches immediately once found missing**.
   - **Deploy patches later**. If you choose this option, you will need to then select the deployment frequency (Daily, Weekly, or Monthly). This option is useful if you would like to schedule patch deployment for non-work hours.
5. Click **Apply Changes**.

To add patch exclusions

1. Click **Device settings**  .
2. Click the name of a settings template.
3. Click the **Patch Management** tab.
4. In the **Patch exclusions** section, click **Add exclusion**.

5 From the list of vendors and products, mark the box beside the patches you wish to exclude from scanning and deployment. For vendors with multiple products, you can either exclude the entire vendor or choose which of their products to exclude.
6 From the **Choose which patch severities you want to exclude** menu, select patch severities to exclude for the selected vendor and/or product(s). You may select multiple severities. If you do not want to exclude any patch severities, select None.

NOTE The None option includes vendors that don't assign severities to their patches.

7 Click **Add exclusion**.
8 Repeat steps 4-7 until you have added all the patches you want to exclude from deployment.
9 Click **Apply Changes**.

TO REMOVE PATCH EXCLUSIONS

1 Click **Device settings**  .
2 Click the name of a settings template.
3 Click the **Patch Management** tab.
4 In the **Patch exclusions** section, do one of the following:

- To delete one or more exclusions, click the **Delete**  button beside each exclusion.
- To delete all exclusions, click the **Reset to defaults** link.

5 Click **Apply Changes**.

TO CONFIGURE ENDPOINT DEVICE RESTART

Often, patches require devices to be restarted after installation. When you install patches using settings templates, you can tell devices to restart and control when that restart begins. If patches are installed but those patches don't require a restart, the devices won't be restarted.

1 Click **Device settings**  .
2 Click the name of a settings template.
3 Click the **Patch Management** tab.
4 In the **Step 3. Restart endpoint devices** section, select one of the following options for endpoint device restart:

- **Do not restart**—You will have to restart manually either from the console or on the physical endpoint device.
- **Restart when user logs off**—Display a message that restart is needed to the endpoint user. If no one is logged in, the device will restart automatically.
- **Force restart automatically**—The device will be restarted automatically without any options for the endpoint user. A warning message will be displayed on the user's machine ten minutes prior to device restart.
- **Force restart automatically but with options for user (Recommended)**—The device will be set to be restarted automatically, and a warning message will be displayed on the user's machine an hour prior to device restart. However, the user will be able to either postpone the restart up to 3 times or cancel the restart altogether, depending on which box you select.

IMPORTANT For patches that require a restart, Patch Management will not display the Deployed status until the device has been restarted successfully.

About file paths in Settings templates

In certain elements of Settings templates, wildcard characters can help you when you do not know the exact file path or file name of files you want to include or exclude, or if you want to indicate multiple files in one path.

Character	Meaning
?	Replaces a single character For example, `ab?.html` matches the files `abc.html`, `abd.html`, and `abe.html`. It will not match the file `abc.htm`.
*	Replaces zero or more characters For example `*.mtl` matches the files `abc.html` and `d.txt`. The pattern `*txt` matches the files `abc.txt`, `x.txt`, and `xyztxt`.

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 TEN:

REPORTS

The Reports page displays a visual representation of data for:

- **Devices**
- **Tasks**
- **Patches**
- **Threats**

IMPORTANT Avast Business Cloud Management Console does not currently support any methods of exporting report data or graphics.

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

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

TO CHANGE THE REPORTING PERIOD

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

TO CHANGE REGIONAL SETTINGS ON THE REPORTS PAGE

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**.

REGIONAL SETTINGS

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 Sunday, all weekly reports begin on Sundays. 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**.

DEVICES REPORT

This area displays information on devices. The number of devices removed and 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.

DEVICES 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 will not be included in the count for devices removed or devices added.

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 were not 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.

PATCHES REPORT

This area displays information on the results of patch scanning and deployment across all managed devices. You can view the patch report for this week, last week, this month, last month, the last three months, and this year.

PATCHES OVERVIEW

The overview shows the results of all found patches in all possible states on devices in a selected timeframe. The four sections on the table show patches that are Missing, Scheduled, Failed, and Deployed. Additionally, each section details how many devices are involved. It is possible for the number of patches in a section to not match the number of devices.

TOP 10 DEVICES WITH PATCHES SUCCESSFULLY DEPLOYED

Displays the 10 devices with patches Deployed.

TOP 10 DEVICES WITH PATCHES FAILED TO DEPLOY

Displays the 10 devices with patches that most frequently Failed to deploy.

TOP 10 DEVICES WITH PATCHES MISSING

Displays the top 10 most frequent Missing patches on devices.

TOP 10 PATCHED APPLICATIONS

Displays the 10 most frequent applications patched on devices.

TOP 10 PATCHED VENDORS

Displays the 10 most frequent vendors patched on devices.

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.

CHAPTER ELEVEN:

SUBSCRIPTIONS

The Subscriptions page displays valuable information about your Avast Business Antivirus and Patch Management subscriptions 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

TO VIEW INFORMATION ABOUT PROTECTION AND SUBSCRIPTIONS

1. Click **Subscriptions**  .
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**.

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 and Patch Management 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 cannot 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 **Subscriptions**  .
2. Under an Antivirus tier that you have a license for, click the **Manage Subscription** link.

TO EXTEND THE EXPIRY DATE OF YOUR LICENSE

1. Click **Subscriptions**.
2. Under an Antivirus tier that you have a license for, click the **Manage Subscription link**.

TO START A LICENSE TRIAL FOR ANTIVIRUS OR PATCH MANAGEMENT

To use Patch Management, you must also have a license for Avast Business Antivirus; however, you can enroll in a 30-day trial of Patch Deployment if you also enroll in a 30-day trial of Avast Business Antivirus at the same time.

1. Click **Subscriptions**  .
2. Do one of the following:

   - Under an Antivirus tier that you do not have a license for, click **Try**.
   - If you already have a license for an Antivirus tier, click **Try** next to Patch Management.

TO BUY LICENSES FOR ANTIVIRUS OR PATCH MANAGEMENT

To use Patch Management, you must also have a license for Avast Business Antivirus. If you don't have a license for Avast Business Antivirus, you can purchase both at the same time.

1. Click **Subscriptions**  .
2. Do one of the following:

   - To buy licenses for additional devices for an Antivirus tier that you already have a license for, click **Subscribe more devices**.
   - To buy or renew a license for an Antivirus tier that you do not have a license for, beside your desired tier click **Buy** if you have not started a trial of the tier or **Buy now** if you have a trial version of that tier.
   - If you have a license for an Antivirus tier, next to Patch management click **Buy** if you have not started a trial or **Buy now** if you have a trial.
   - If you don't have a license, beside your desired tier click **Buy Now**, then click **Antivirus + Patch**.

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 **Subscriptions**  .
2. Click the **Refresh** button at the top right of the page.

TO UPLOAD YOUR LICENSE

1. Click **Subscriptions**  .
2. Click the **Got activation code?** link.
3. Type your license code.
4. Click **Activate**.

TO COMPARE THE PROTECTION LEVEL OF ANTIVIRUS PRODUCTS

1. Click **Subscriptions**  .
2. Click the **Compare all business products** link at the top of the page.

IMPORTANT If you need to change the license for a singular device, this can be done only on the Devices tab. Reasons you might change the license are if you purchased a different Avast Business Antivirus product and want to activate the change on your device(s), such as moving from Antivirus Pro to Antivirus Pro Plus.

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**.
3. Click **Apply** for the license you want to change to.

CHAPTER TWELVE:

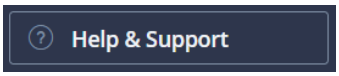
HELP & SUPPORT

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 section of this manual
- Looking for the answer to your technical questions on the Avast forum and in the Knowledge Base

The Help & Support button located at the bottom left hand corner of your Navigation Bar provides you with different help and support sections.

Click the 

button to reach the Help & Support menu, where you will find the following support sections:

SUPPORT DOCUMENTS

- **User manuals**
  - Link to our Cloud Console User Manual
- **Knowledge Base articles**
  - Link to our Avast Knowledge Base for additional how to articles
- **Product development**
  - Link to our Product Development Roadmap so you can learn more about up and coming features and enhancements
- **Legal documents**
  - Link to avast.com/legal site for more legal information
- **Learn more about this console**
  - Link to our Avast Business Cloud Management Console product page on avast.com
  - Link to our Avast Business Blog site
  - Link to our Avast Business Forum

CONTACT OUR SUPPORT

- **Chat with our support staff**
  - Instantly chat with one of our Technical Support agents
- **Submit a technical support ticket**
  - Submit an e-mail to our Technical Support group for e-mail support
- **Call our support staff**
  - View the list of phone numbers for contacting our Technical Support team

TO SUBMIT A TICKET TO AVAST TECHNICAL SUPPORT

NOTE All fields are mandatory.

1. Click **Create New Ticket**.
2. Type the following:
   - **Company**
   - **Contact Name**
   - **E-mail**
   - **Phone**
   - **Subject**
   - **Description**
3. Click **Send**.

HELP US BECOME BETTER

- **Vote for and submit new ideas**
  - Link to our Avast Business Idea page, submit new features and enhancements that you would like to see in our Avast Business Cloud Management Console and Client
- **Tell us about your user experience**
  - Link to our User Experience Survey that will help us know what you think of our Avast Business Cloud Management Console

AVAST LABS

Avast customers can opt in to add experimental functionalities to their Cloud Console. These functions are not complete and may produce bugs or errors in the Console.

ENABLING LABS

1. Click **General Settings**  .
2. On the **General** tab, click the slider beside *Enable labs features*.
3. Click **Save**.

When you enable Labs, a new tab labeled Labs will appear below Subscriptions. You can use that page to view the available experimental options and choose which ones you would like to test with your company.

TROUBLESHOOTING

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

WHERE CAN I FIND LOGS?

The Avast Business Cloud Management Console does not create logs that are stored on your computer.

CAN I TURN ON DEBUG LOGGING?

You can turn on debug logging, but it is not recommended, since it creates many logs. Debug logging can be enabled in the General Settings tab of the Settings Template.

MY DEVICE IS INSTALLED BUT DOES NOT APPEAR IN THE CONSOLE.

This may be because the device does not support IPv6 hostnames.

Why are Master Agents not working?

If a Master Agent is not 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 does support devices using a proxy server. Proxy servers can be configured in the General Settings tab of the Settings Template.

Can I use Avast Business Cloud Management Console on an offline network?

Avast Business Cloud Management Console requires access to the internet.

Can I move a device being managed from my Cloud Management Console to the On-Premise Management Console, or vice-versa?

No, you cannot transfer a device between the Cloud Management Console and the On-Premise Management Console, and vice versa, at this time. If you are changing consoles, you will have to reinstall the devices on the new console.

Can I export settings such as exclusions from one Console and import them into another?

This is not a feature at the current time but may be implemented in the future.

How does the Console know whether my device is a server or a workstation?

The Console looks at the device's OS name to determine whether it is a workstation or a server.

How do I fix Error Code #550 "No SMTP server defined. Use real server address instead of 127.0.0.1 in your account"?

This error occurs when Web Shield and Mail Shield are installed on a server operating system that is also running Microsoft Exchange. To resolve, ensure both Shields are completely turned off and removed from the device.

INDEX