Avast Business

Quick Start: Business Hub

For more help or troubleshooting, please visit our online documentation:

https://businesshelp.avast.com/

Table of Contents

Introduction to the Business Hub

The Business Hub allows you to manage multiple sites or customers from a single console. This cloud-based platform helps reduce the burdens of maintaining, configuring, and optimizing endpoint security. The Hub is ideal for:

- Medium- to large-sized companies with multiple office locations or sites
- IT Service Providers managing multiple customers
- Existing users of the Avast Business Cloud Console using the account switching functionality (for more information, see Managing Companies)

The Business Hub 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 the Business Hub, 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.

Console Setup

Setting Up the Hub

Verify Console System Requirements

Business Hub

Browsers (latest versions recommended):

- Google Chrome
- Firefox
- Safari
- Microsoft Edge

Avast Business Antivirus Endpoints

Windows:

- 11 – x64, x86
- 10 – all versions except Mobile and IoT Core Edition – x64, x86
- 8/8.1 – all versions except RT and Starter Edition – x64, x86
- 7 SP1 – requires KB3033929requiresKB3033929 – x64, x86
- Server 2022, 2019, 2016, 2012 – any edition with latest service pack excluding Server Core – x64
- Server 2008 R2 – requires KB3033929requiresKB3033929 – x64
- Small Business Server 2011 – x64

Supported applications:

- Exchange Server 2022, 2019, 2016, 2013, 2010
- SharePoint Server 2019, 2016, 2012, 2010
- SharePoint Services 3.0 and higher

Mac:

We support ARM-based chips on MacOS devices.

- MacOS 10.11 (El Capitan or later with at least 500MB free disk space), prefer 11.x Big Sur or later

Linux:

- CentOS 7 and above
- Debian 8 and above
- Red Hat Enterprise Linux 7.4 and above
- Ubuntu LTS 16.04 and above

Android:

- Android 6.0 (Marshmallow) or higher

iPhone/iPod touch:

- iOS 13.0 or higher

iPad:

- iPadOS 13.0 or higher

Verify Console Firewall Requirements

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

Geoblocking

Avast web services are hosted in many countries around the world. Therefore, we do not recommend geoblocking in your firewall settings.

If geoblocking is necessary, we recommend you set URL Allow rules to supercede geo-blocking, so Avast traffic can still be allowed.

Ports (TCP & UDP)

- 53 – Secure DNS services (only if using Real Site component)
- 80 – Internet vulnerability checks and feature updates
- 443 – Encrypted communication
- 8080, 8090 – Communication between console and clients within local network (only for On-Premise Console)
- 4158 – Mirror, for local updates within local network
- 7074 – Remote Deployment within local network

URLs

- *.avast.com
- *.avcdn.net
- islonline.net (Hub only, for Remote Control)
- *.managedoffsitebackup.net (Hub only, for Cloud Backup)
- *.sosonlinebackup.com (Hub only, for Cloud Backup)

Setting Up the Console

Registration

Even if you are a current customer, you will need to create a new account for the Hub using a unique email address.

Existing Partners:

1. Navigate to the Avast Partner Portal
2. Go to the Avast Business Management Console section and click **Register**
3. Follow the steps to create a Hub

Existing or New Customers:

1. Navigate to https://new-business.avast.com/
2. Click **Create an account**
3. Enter the administrator email address and desired password
4. Enter the company details, and choose between Small or medium business, Large business, Managed Service Provider (MSP), and Security Vendor (Reseller-/VAR/Distributor)
    - **If you select MSP or Security Vendor, you will be asked to use the Partner Portal if you are a registered Avast partner**
5. Select **Multi-company console**, then click **Finish and Create Your Console**

Console Configuration

1. Click **Create Site** or **+ Site** from the left-hand drop-down menu
    - **The normal Hub allows users to create Sites, but if a Partner registers for the Hub via the Partner Portal, their Console will use "Customers" instead**

of "Sites". These terms will be used more or less interchangeably in the documentation.

2. Enter the *Site Name* and *Region*
3. Select whether or not to begin trials for Avast Business Antivirus and Patch Management for the site
4. Click **Create Site**

The top-level Dashboard will be populated with the created site(s).

Users

You can add a Global Admin (for access to all customers) or Site User (for access to individual sites).

1. Click the *Users* tab
2. Click **+ User** in the top right
3. Enter the user email address
4. Select either **Global Admin** or **Site User**
    - **Site Users can be customized to have varying levels of access across Sites, and will access multiple sites via Account Switching within the Console**

When you have multiple Sites, you can switch between them using the left-hand drop-down menu.

Activating Licenses in the Hub

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

1. With no site selected in the left-hand drop-down menu, click **Dashboard**
2. Beneath the Site you are going to activate, click **Activate Subscription**
3. Click **Enter activation code**
4. Enter the activation code and confirm it is correct

Assigning Licenses to Devices

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

Without a customer selected, Partners can see an overview of all customers or sites. However, you can also select a customer/site from the drop-down menu to view their devices. This will display device names, status and alerts, operating system, assigned group, assigned policy, Antivirus version, Patch Management subscription, Premium Remote Control subscription, and the time the device was last connected to the Cloud Console.

You can alter the assigned subscription for a device, for instance if you purchase seats for a different Antivirus version or a subscription for Patch Management.

1. In the Hub, select the site you would like to manage in the left-hand navigation pane
2. Click the *Devices* tab
3. Do one of the following:
    - Select the check boxes beside multiple devices and click **More** at the top right
    - Click the three dots within the device list
4. Select **Change ▸ Change Service Subscription**
5. Use the drop-downs to select which subscription(s) you would like to use for Antivirus and Patch Management
6. Click **Apply**

This procedure will require the affected device(s) to restart.

Adding Devices

Adding Devices via the Installer File or Shareable Link

You can add devices to a Site directly from the Dashboard without drilling down to the site. When creating installers, the previously selected settings will be retained so you will not have to select them again.

Downloading Installer

1. Select which type of installer you need:
    - Windows .exe (for workstations and servers)
    - Windows .msi (for deployment using GPO)
    - MacOS X .dmg
2. Select the installer size (Light vs Full)
    - **If you select Light, the other services will be downloaded upon installation of the Antivirus agent. This option is not recommended if you are installing Antivirus on multiple devices at the same, as each machine will individually contact Avast servers to download the other services.**
3. Select the subscriptions for Avast Business Antivirus, Patch Management, and whether or not to activate Remote Control
4. Choose the Group and Policy the device will use
    - **If desired, you can activate your devices and select the subscriptions to use after installation by checking the box with that option.**

5. Choose whether to automatically remove competitive antivirus products on the device
6. Ensure you have defined the correct Proxy Server, if any, in the policy you are applying to the device
7. Click **Download installer** and specify where to save the installation package–such as on a flash drive or network drive

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

Installing on the Local Client

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

1. Copy the installer file to a location accessible by the end device
2. Double-click on the installer file to run it
3. If asked to allow the application to make changes to your device, click **Yes**
4. Wait while Avast Business Antivirus is installed on the device
5. When prompted, restart the device
6. The device should now be visible in your Console

Global Policies

Partners and customers using the Hub can create and manage policies across their entire network, and for specific sites or customers.

Main Benefits

- Configure policies on a single page
- Apply policies to all devices regardless of operating system
- Create and manage exclusions in one place
- Create site- or customer-specific exclusions when opening a Global Policy from the site's Policies tab
- Utilize predefined settings for Workstations and Servers

What to Expect

- Existing policies will have the following alterations to enable this shift:
- Policies with settings for multiple operating systems will be separated into multiple policies based on the operating system
    - **Example: If you have one policy with different settings for Windows Workstations, Windows Servers, and MacOS X, you will see three different policies. These policies will include the operating system type at the end for your reference.**
- Policy names will remain the same
- All devices will be automatically assigned policies based on their operating system
    - **Example: Windows Workstations that were using a policy with settings for Workstations, Servers, and MacOS X will be assigned to the policy for**

Creating a New Global Policy

1. Open the Hub
2. Click the **Policies** tab
3. Click **+ Policy**
4. Enter the name you would like to use for the policy
5. If desired, enter a description for the policy
6. Choose whether to base the new policy from a predetermined Avastpolicy or an existing policy, then make a selection in the drop-down menu
7. Click **Create**

Configuring Your Policy

Once you have created a policy, you can edit the settings by clicking its name in the table. A drawer will open with five tabs, and a few buttons at the top. You can use these buttons to revert the policy to its original settings, or to duplicate it. If you want to delete your policy, you can do so by clicking the **three dots** and selecting **Delete Policy**.

Overview

This tab provides some brief details about the policy. You can edit the description by clicking the pencil icon. You can also see when the policy was created and last updated.

General Settings

General Settings: using the toggles, enable or disable Password Protection, Silent Mode, Reputation Services, Debug Logging, Avast Tray Icon, and Scan of External Drives. You can also choose which version of Avast Business Antivirus the assigned devices will use by typing either a version number, "latest", or "stable" in the Version Switch section.

Updates: select either Automatic or Manual updates for your Virus definitions and Program (see Configuring Virus Definition and Antivirus Updates). If needed, you can configure the settings for a proxy to be used during updates (see Configuring Proxy Settings for Devices).

Troubleshooting: using the toggles, enable or disable Anti-rootkit Monitor, Avast Self-defense Module, Limited Program Access for Guest Accounts, and Hardware-assisted Virtualization. You can also enter the details for your mail ports.

Restart Options: select when to restart endpoint devices between only when needed by the Antivirus or Patch Management service, automatically, when user logs off, or not at all. For more information on these options, see Configuring Restarts and Cache Clearance.

Service Settings

Antivirus

General Settings: enable or disable CyberCapture and Hardened mode

Antivirus Scans: set the frequency and schedule for Quick and Full System Antivirus Scans. For more information, see Device Scanning Tasks.

Antivirus Protection: enable, disable, and configure settings for the main protection components

Data Protection: enable, disable, and configure settings for this category of components

Identity Protection: enable, disable, and configure settings for this category of components

For more information on these components, see Component Overview. You can access the settings for configurable components by clicking the drop-down arrow beside its name.

Patch Management

Patch Scans and Deployments: set the frequency of scans for missing patches, and whether or not to deploy missing patches immediately, on a specific schedule, or manually

Other Settings: select when to clear the local patch files on the end device

For more information on Patch Management's various settings, see Patch Management.

Firewall

Firewall settings ▸ Networks: select the firewall profiles for undefined network connections, and define networks

Firewall rules: set the various System, Application, and Advanced Packet rules

For more information, see the articles in the *Firewall* section of Configuring Settings and Policies.

Exclusions

Antivirus Exclusions: enter exclusion paths to be excluded from either All scans and shields, or specific Shields. For more information, see Configuring Standard Antivirus Exclusions and Configuring Component-Specific Exclusions.

Patch Management: enter exclusions for selected patch vendors and severities. For more information, see Patch Exclusions.

Creating Site-specific Exclusions

1. Select the site from the drop-down menu in the top-left
2. Click the **Policies** tab
3. Select the name of the Global Policy from the list
    - **Ensure the site can access the Global Policy by assigning it (see below).**
4. Navigate to **Exclusions ▸ Antivirus Exclusions**
5. Enter the site-specific exclusion(s) in the desired tab
6. Click **Save**

Assignments

Click **+ Assign to sites** to enable specific sites to use the Global Policy. You can also remove sites from the assignment list using the check boxes and clicking **Unassign policy**.

Once you have made changes to the policy, click Save at the bottom-right of the drawer.

Glossary

A

Anti-spam

Antivirus component designed to scan outgoing and incoming emails for threats.

Antivirus

A service which keeps devices safe from viruses and other threats. Requires regular virus definition updates to be effective.

av

A service which keeps devices safe from viruses and other threats. Requires regular virus definition updates to be effective.

Avast Business Antivirus

A service which keeps devices safe from viruses and other threats. Requires regular virus definition updates to be effective.

AVG Business Antivirus

A service which keeps devices safe from viruses and other threats. Requires regular virus definition updates to be effective.

D

Device

Personal computers, laptops, or server devices you would like to add to your network.

E

Exception

Individual or uncategorized websites, files, etc allowed or blocked by Antivirus.

Exclusion

Individual or uncategorized websites, files, etc allowed or blocked by Antivirus.

F

Firewall

Antivirus component which scans all outgoing and incoming traffic to a device for threats.

G

Group

Organizational structure used for managing numbers of devices on a network. Your Console comes with a default group which can be renamed, but cannot not be deleted.

L

License

The type of subscription you have for a specific, paid Avast or AVG product.

Local Update Server

Device(s) in your network designated by your Console to download, deploy to, or scan other networked machines.

M

Master Agent

Device(s) in your network designated by your Console to download, deploy to, or scan other networked machines.

P

Policy

A set of settings applied to device(s) from your Console to automate client-side Antivirus processes.

Potentially Unwanted Program

Programs which sometimes act similarly to malware or spyware, usually installed as part of another installation.

PUP

Programs which sometimes act similarly to malware or spyware, usually installed as part of another installation.

Q

Quarantine

Component of Antivirus which quarantines potentially infected files until it has been determined that it is safe to permanently delete them, either manually or according to a schedule.

R

Remote Deployment

Method of installing Antivirus from your Console to all chosen devices on the local network, only available when a device on the network already has Antivirus

installed through a different method.

S

Subscription

The type of subscription you have for a specific, paid Avast or AVG product.

V

Virus Chest

Component of Antivirus which quarantines potentially infected files until it has been determined that it is safe to permanently delete them, either manually or according to a schedule.