

Configuring Avast Business Antivirus Policies: Enabling and Configuring Webcam Shield

<https://campus.barracuda.com/doc/90442231/>

Webcam Shield is available for Workstations only, not Servers.

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.

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.

1. Click **Configuration > Policies > Avast Antivirus**.
2. Click the name of a policy.
3. Click the **Workstation Settings** tab.
4. Click the **Active Protection** tab.
5. In the **Shields** section, move the slider to enable **Webcam Shield**.
6. Click **Apply Changes**.

To Configure Webcam Shield

The settings for **Webcam Shield** consist of two parts:

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

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

When you create your AV policy, the mode you choose overrides the mode the user chooses. You also have the option to replace the user's application permission list with your own, which means that the user's application permission list is ignored.

However, in **No mercy** mode, no applications are allowed, not even the applications on the application permission list.

To choose the Webcam Shield Mode

1. Click **Configuration > Policies > Avast Antivirus**.

2. Click the name of a policy.
3. Click the **Workstation Settings** tab.
4. Click the **Active Protection** tab.
5. Click the **Customize** link in the **Webcam Shield** section.
6. Select one of the following modes:
 - **Smart** automatically allows trusted applications to access the webcam. If an untrusted application attempts to access the webcam, a notification appears, asking the user to block or allow the application. After selecting an option, the application appears on the **Webcam Shield Settings** screen, where the user can view its status and select additional actions.
 - **Strict** notifies the user each time any application attempts to access the webcam and allows the user to decide if the application is blocked or allowed. After blocking or allowing an application, the application appears on the **Webcam Shield Settings** screen where the user can view its status and select additional actions.
 - **No mercy** blocks all applications from accessing the webcam. If you choose **No mercy**, both the user's and **AV policy application permission** lists are disabled. No applications are allowed to use the webcam.
7. Click **Apply Changes**.

To disable users' webcam access list

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

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

1. Click **Configuration > Policies > Avast Antivirus**.
2. Click the name of a policy.
3. Click the **Workstation Settings** tab.
4. Click the **Active Protection** tab.
5. Click the **Customize** link in the **Webcam Shield** section.
6. Select **Overwrite the application list which was already set by the user**.
7. Click **Apply Changes**.

To create a webcam access list

Webcam access lists are valid in **Smart** and **Strict** modes.

1. Click **Configuration > Policies > Avast Antivirus**.
2. Click the name of a policy.
3. Click the **Workstation Settings** tab.
4. Click the **Active Protection** tab.
5. Click the **Customize** link in the **Webcam Shield** section.

6. Do either of the following in the **Applications** section:
 - To block webcam access for a specific application, type the path to the application in the box, click the **Blocked** check box, then click **Add**.
 - To allow webcam access for a specific application, type the path to the application in the box, click the **Allowed** check box, then click **Add**.
7. Repeat step 6 until you have added all the applications you want to block and allow.

When you type the path to your application, include the application name and its file extension.
8. To remove the setting for a blocked or allowed application, click the **Delete** icon next to the application. Once the permission is removed, the application is subject to the mode you chose in the main settings.

To help you enter the application path, you can use the environment variables in the **Application** section.
9. Click **Apply Changes**.

© Barracuda Networks Inc., 2021 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.