Configuring Avast Business Antivirus Policies: Enabling and Customizing File Shield

https://campus.barracuda.com/doc/91129732/

File Shield is available for both Workstations and Servers.

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

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

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

- To exclude all HTML files, type **.htm** into the text box.
- 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 .

1. Click one of the following tabs:
    - **Workstation Settings**
    - **Server Settings**
2. Click the **Active Protection** tab.
3. In the **Shields** section, move the slider to enable **File Shield**.
4. Click **Apply Changes**.

To Configure When File Shield Scans Files

1. Click **Configuration** > **Policies** > **Avast Antivirus**.
2. Click the name of a policy.
3. Click one of the following tabs:
    - **Workstation Settings**
    - **Server Settings**
4. Click the **Active Protection** tab.
5. Click the **Scan behavior** tab.
6. Click the **Customize** link in the **File Shield** section.
7. In the **Scan When Executing** section, click any of the following:
    - **Scan programs when executing**
    - **Scan scripts when executing**

- **Scan libraries when executing**

8. In the **Scan When Opening** section, click 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 documents 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. To scan all files that have a specific file extensions, click the **Scan files with custom extension** check box. Type the extension in the box, then click **Add**. Repeat until you have added all your extensions.
    You can use wildcard characters. and click **Add**.
12. Click **Apply Changes**.

Configuring Avast Business Antivirus Policies: Excluding Files, File Types, and Locations from File Shield

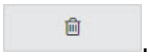
You can modify the list of locations that will not be scanned. Exclusions are files and locations that will not be scanned. Enable the check boxes to define when the file is not scanned, when the file is read, written to, or executed. You can use wildcards in file names, paths, and extensions, such as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

Exclusions that you specify on this screen only apply to File Shield and do not affect any other scans or Shields. To exclude a location from all Avast Business Antivirus scans, see Configuring Avast Business Antivirus Policies: Excluding Files, Folders, or URLs from Scans and Shields.

1. Click **Configuration** > **Policies** > **Avast Antivirus**.
2. Click the name of a policy.
3. Click one of the following tabs:
   - **Workstation Settings**
   - **Server Settings**
4. Click the **Active Protection** tab.
5. Click the **Customize** link in the **File Shield** section.
6. Click the **Exclusions** tab.
7. Click any of the following check boxes:
   - **R**—Read
   - **W**—Write
   - **E**—Execute

8. Type a file name, path, or extension.
9. Click **Add**.
10. Repeat steps 8-9 until all your chosen file names, paths, and extensions are excluded.
11. Click **Apply Changes**.

To Remove a File Shield Exclusion

1. Click **Configuration** > **Policies** > **Avast Antivirus**.
2. Click the name of a policy.
3. Click one of the following tabs:
   - **Workstation Settings**
   - **Server Settings**
4. Click the **Active Protection** tab.
5. Click the **Customize** link in the **File Shield** section.
6. Click the **Exclusions** tab.
7. Next to the exclusion you want to remove, click  .
8. Click **Apply Changes**.

Configuring Avast Business Antivirus Policies: Customizing 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 programs, or suspicious file is detected.

1. Click **Configuration** > **Policies** > **Avast Antivirus**.
2. Click the name of a policy.
3. Click one of the following tabs:
   - **Workstation Settings**
   - **Server Settings**
4. Click the **Active Protection** tab.
5. Click the **Customize** link in the **File Shield** section.
6. Click the **Actions** tab.
7. Click one of the following tabs:
   - **Virus**
   - **PUP**
   - **Suspicious**
8. Select an option in the **Choose what action Avast will perform after finding a virus** box.
9. Select an option in the **if the action fails, use** box.
10. In the **Options** section, click any of the following check boxes:
    - **Show notifications for actions**
    - **Perform the selected action when the system restarts**
11. In the **Processing Infected Archives** section, click one of the following check boxes:
    - **Try to remove only the packed file from the archive; if it fails, do nothing**
    - **Try to remove only the packed file; if it fails, remove the whole containing archive**
    - **Always remove the whole archive**

12. Click **Apply Changes**.

Configuring Avast Business Antivirus Policies: Customizing Which Archive Files Avast Attempts 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. Click **Configuration** > **Policies** > **Avast Antivirus**.
2. Click the name of a policy.
3. Click one of the following tabs:
    - **Workstation Settings**
    - **Server Settings**
4. Click the **Active Protection** tab.
5. Click the **Customize** link in the **File Shield** section.
6. Click the **Packers** tab.
7. Do one of the following:
    - Click **All packers**.
    - Click the check boxes of individual packers.
8. Click **Apply Changes**.

Configuring Avast Business Antivirus Policies: Customizing Avast Antivirus File Shield Sensitivity

You can define the following settings for **File Shield**:

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. **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.

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. Click **Configuration** > **Policies** > **Avast Antivirus**.
2. Click the name of a policy.
3. Click one of the following tabs:
   - **Workstation Settings**
   - **Server Settings**
4. Click the **Active Protection** tab.
5. Click the **Customize** link in the **File Shield** section.
6. Click the **Sensitivity** tab.
7. Select an option in the **Heuristics Sensitivity** box.
8. Click any of the following check boxes:
   - **Use code emulation**
   - **Test whole files**
   - **Scan for potentially unwanted programs (PUPs)**
9. Click **Apply Changes**.

Configuring Avast Business Antivirus Policies: Generating and Customizing 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. Click **Configuration** > **Policies** > **Avast Antivirus**.
2. Click the name of a policy.
3. Click one of the following tabs:
   - **Workstation Settings**
   - **Server Settings**
4. Click the **Active Protection** tab.
5. Click the **Customize** link in the **File Shield** section.
6. Click the **Report File** tab.
7. Click the **Generate Report File** check box.
8. Type a name in the **File Name** box.
9. Select the **File Type**.
10. Select an option in the **If File Exists** box.
11. Click any of the **Reported Items** you want to include in the report:
    1. **Infected items**
    2. **Hard errors**

3. **Soft errors**
4. **OK items**
5. **Skipped items**

12. Click **Apply Changes**.

Configuring Avast Business Antivirus Policies: Customizing File Shield Advanced Settings

You can configure advanced and performance-related settings of antivirus scans.

1. Click **Configuration** > **Policies** > **Avast Antivirus**.
2. Click the name of a policy.
3. Click one of the following tabs:
   - **Workstation Settings**
   - **Server Settings**
4. Click the **Active Protection** tab.
5. Click the **Customize** link in the **File Shield** section.
6. Click the **Advanced Settings** tab.
7. Click any of the following check boxes:
   - **Do not Scan Verified System DLLs**—Excludes verified **system library files** (.dll) from scanning.
   - **Use Transient Caching**—Files which have been previously scanned and temporarily verified as clean are not scanned again until the next system restart or virus definitions update.
   - **Use Persistent Caching**—Trusted files that are verified as safe are not scanned again, even after a system restart or virus definitions update.
8. Click **Apply Changes**.

Figures