Configuring Avast Business Antivirus Policies: Enabling and Customizing Mail Shield

https://campus.barracuda.com/doc/90442253/

Mail Shield is available for both Workstations and Servers.

Mail Shield checks incoming and outgoing email messages for viruses and links to malicious websites. This only applies to messages handled by mail management software installed on your computer, such as MS Outlook. If you access your web based email account via an Internet Internet browser, your devices are protected by other 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. In the **Shields** section, move the slider to enable **Mail Shield**.
6. Click **Apply Changes**.

To Identify Which Messages Mail Shield Protects

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 **Mail Shield** section.
6. Click the **Main Settings** tab.
7. Click any of the following check boxes:
   - **Scan inbound mail (POP3, IMAP4)**
   - **Scan outbound mail (SMTP)**
   - **Scan newsgroup messages (NNTP)**
8. Click **Apply Changes**.

Configuring Avast Business Antivirus Policies: Configuring Notes and Warnings for Emails Scanned by Mail Shield

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

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

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

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

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

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 **Mail Shield** section.
6. Click the **Behavior** tab.
7. Click 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**
    - **Add a warning to the subject line of infected e-mails** and type the warning to add.
8. In the **MS Outlook only** section, click any of the following check boxes
    - **Show splash screen**
    - **Scan files when attaching to e-mail**
    - **Scan archived messages when opening**
    - **Unread messages only**
9. Click **Apply Changes**.

Configuring Avast Business Antivirus Policies: Scanning SSL connections with Mail Shield

Mail Shield is available for both Workstations and Servers.

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

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 **Mail Shield** section.
6. Click the **SSL Scanning** tab.
7. Click the **Scan SSL connections** check box.
8. Click **Apply Changes**.

Configuring Avast Business Antivirus Policies: Choosing the Action to Take When Mail Shield Finds a Virus, Potentially Unwanted Program, or Suspicious File

Mail Shield is available for both Workstations and Servers.

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

Configuring Avast Business Antivirus Policies: Customizing Which Archive Files Mail Shield Attempts to Unpack

Mail Shield is available for both Workstations and Servers.

You can choose which archive (packer) files Avast Business Antivirus should attempt to unpack during the **Mail Shield** process. **Mail Shield** is better able to analyze files for malware when files are unpacked. To unpack a file is the same as to extract a file from an archive. Original archives, including the files contained within, remain intact when being processed by **Mail 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 **Mail Shield** section.
6. Click the **Packers** tab.
7. Do one of the following:
    - Click **All packers**.
    - Clear the **All packers** check box, then click the check boxes of individual packers.
8. Click **Apply Changes**.

Configuring Avast Business Antivirus Policies: Customizing Mail Shield Scanning Sensitivity

Mail Shield is available for both Workstations and Servers.

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 **Mail 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 **Mail 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 a Mail Shield Report

Mail Shield is available for both Workstations and Servers.

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

To Generate and Customize Mail Shield Reports

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 **Mail 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:
    - **Infected items**
    - **Hard errors**
    - **Soft errors**
    - **OK items**
    - **Skipped items**
12. Click **Apply Changes**.