MAX by LOGICnow | Mail

# 1. Attachment blocking update - **October 2016**

## 1.1 Overview

Granular Attachment Handling policies allow administrators for a domain or organisation to control the security risk posed by email attachments. In addition to all email attachments being scanned by multiple antivirus engines including zero-day prevention, administrators can now control how attachments of certain file types are handled, before they reach the customer's mail server.

The majority of harmful files are transmitted as attachments. Because of this risk, it is important to control which types are permitted inside your network perimeter. The LOGICnow Mail Security platform offers administrators the ability to control how a number of different groups of attachment types are handled. The options for handling are:

- **Treat the message as normal** - by examining the message with standard spam and virus filters
- **Treat the message as if it is spam** - by allowing the message to appear in quarantine and in digests and be released later if necessary
- **Treat the message as a virus** - by blocking the message from delivery and, by default, hiding the message from the quarantine.

## 1.2 How does the attachment scanning work?

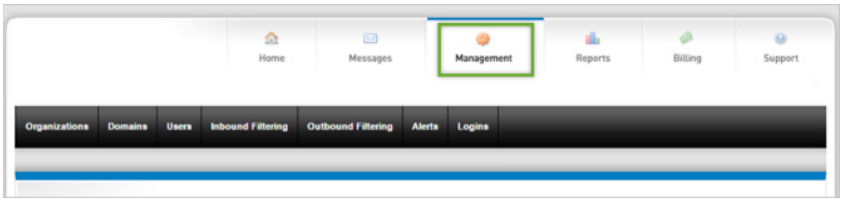
Whether or not attachment blocking is enabled, all messages and their attachments are automatically scanned for viruses by four anti-virus engines with multiple, complimentary technologies including zero-hour virus detection.

In addition to this standard filtering, when the attachment blocking is enabled, all emails with attachments are scanned against the additional rules for attachment blocking when the messages are received by the filters. The attachments are scanned for their detected file type as well as the filename extension.

**Note** - Attachments can beblocked based on the detected file type (e.g. an executable or a media file), and/or by their file extension (e.g. exe, avi).

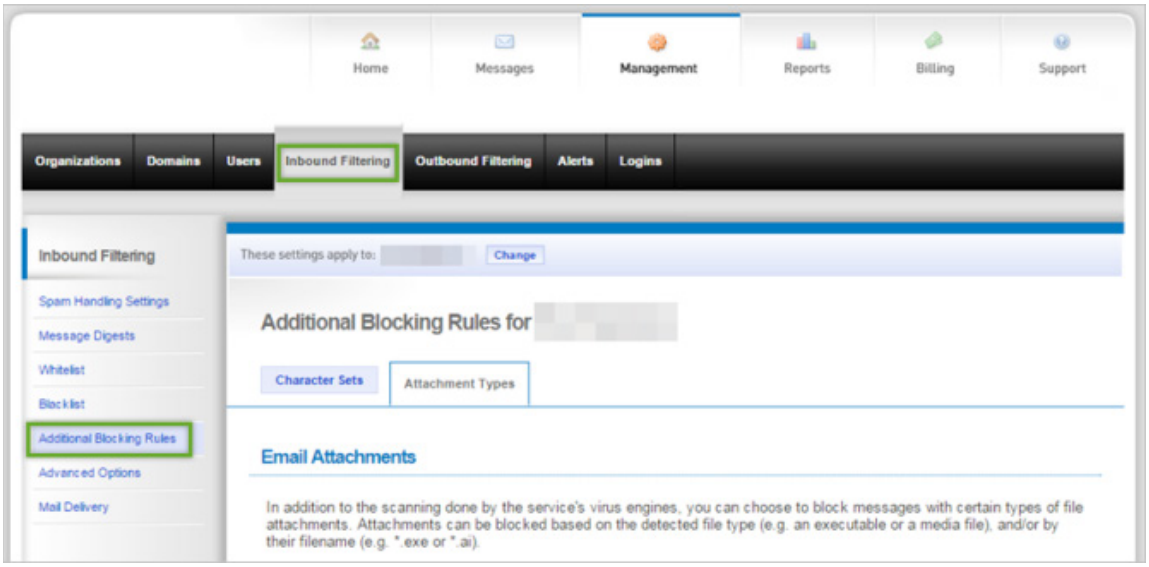
# 1.3 How do I configure attachment type blocking?

1. Open the **Control Panel** and click on the **Management** tab.

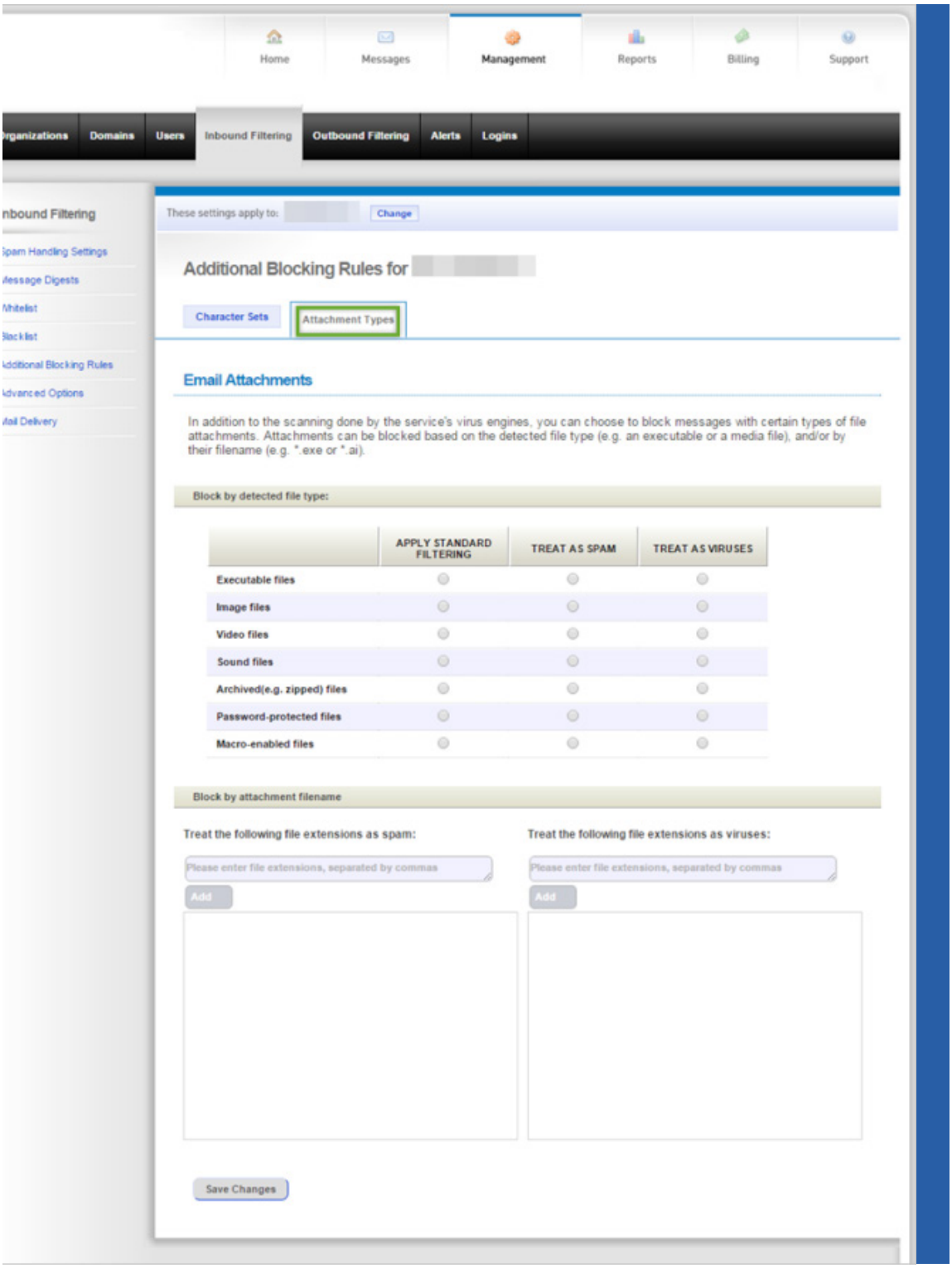



2. Click to display the **Domains** sub-tab and select the domain you want to modify.

3. Next, click on the **Inbound Filtering** sub-tab and then select **Additional Blocking Rules**.



4. Click to display the **Attachment Types** tab:



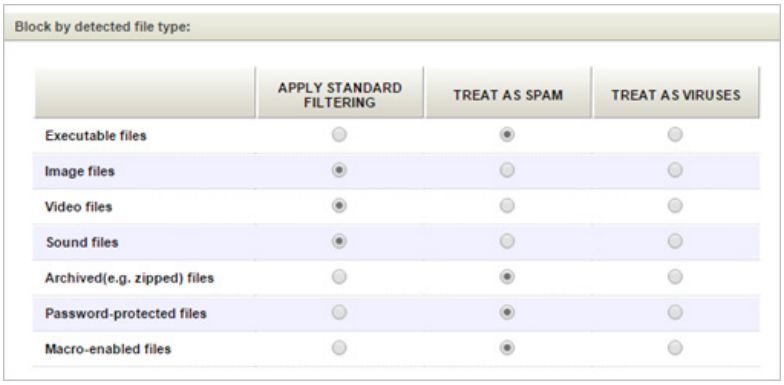

5. In the section **Block by detected filetype**, choose how you would like the listed file types to be handled.

The service will attempt to determine the file type based on the signature of the attachment rather than the filename of the attachment. (The signature is derived from the initial bytes from the file which indicate the type of file.) The options available for handling messages with detected attachment types are:

- **Apply standard filtering** - No special handling will occur if that file type is detected; the message will be subjected to the standard spam and virus filters

- **Treat as Spam** - Messages containing an attachment of the detected file type will be treated as spam and quarantined/handled as the settings for the user/domain dictate

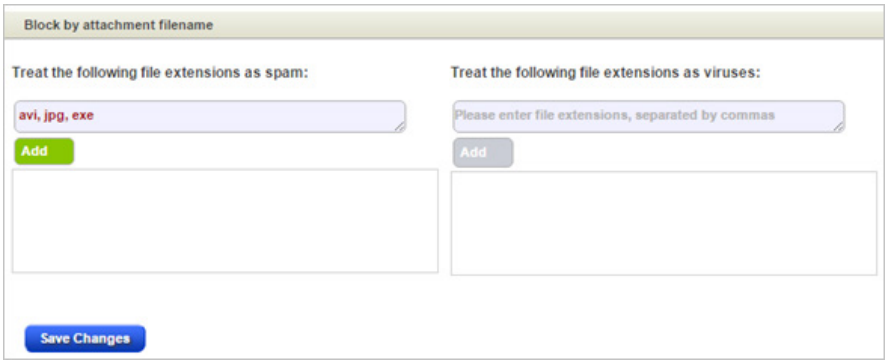
- **Treat as Virus** - Messages with the detected file type will be treated as viruses. This means that they will not be delivered and will not be visible within the quarantine, to guard against inadvertent release of malware,




Additionally, you can configure the blocking of attachments based on filenames. This allows for more granular control; for example, you may wish to block zip files but not rar files.

6. To specify individual filename-based attachment blocking, enter one or more extensions into the appropriate box in the **Block by attachment filename** section and click on **Add**. If entering multiple filetypes, separate them with commas e.g. avi, jpg, exe.

7. Click **Save changes** to activate your settings - the blocking should be effective immediately.




## Remove blocking by filetype

To remove the blocking of a given file type, simply click on the X next to that file type, then save your changes.

---

**Note** - It is possible that an administrator has enabled attachment based filename blocking at a higher level within the service; in this case the inherited attachment types are shown but are not removable except by that administrator.

**Note** - As with the detected file types, when specifying the individual filenames, you have the choice of having those file types treated as spam or viruses. (In the event that a specific filename is specified for handling as both spam and virus, the service will treat that file extension as a virus.)

**Note** - You may use attachment blocking based on the detected file type, and/or based on the specified filename(s), depending on your needs.

## Connect with us!

Please get in touch if you have any questions about any of our services.


UK: +44 0 1313 414899
US: +1 855 801 5461
APAC: +61 8 7123 4068

info@LOGICnow.com

@LOGICnow




LOGICnow
CHOOSE INTELLIGENCE