Antivirus Signature Bypass

In this page, you can manage problematic Antivirus Signatures that cause too many false positives.

Determining a problematic signature is as simple as looking at a blocked email's headers which would yield the actual signature that was used to block the email. For example:

```
Return-Path: <jlandaverderodas@fencedeckdirect.com>
Delivered-To: virus-quarantine
X-Envelope-To: <bill@domain.tld>
X-Envelope-To-Blocked: <bill@domain.tld>
X-Quarantine-ID: <CLjhQdETZxXS>
X-Amavis-Alert: INFECTED, message contains virus: Heuristics.Encrypted.PDF
X-Spam-Flag: NO
X-Spam-Score: 0
X-Spam-Level:
X-Spam-Status: No, score=x tag=-999 tag2=3.6 kill=12 tests=[]
```

Assuming, this was a legitimate email and you wished to bypass the signature that caused this email to be blocked, you would simply bypass the **Heuristics.Encrypted.PDF** signature.

Alternatively, looking at the System Logs and searching for the keyword **INFECTED** will also yield the actual signature. For example:

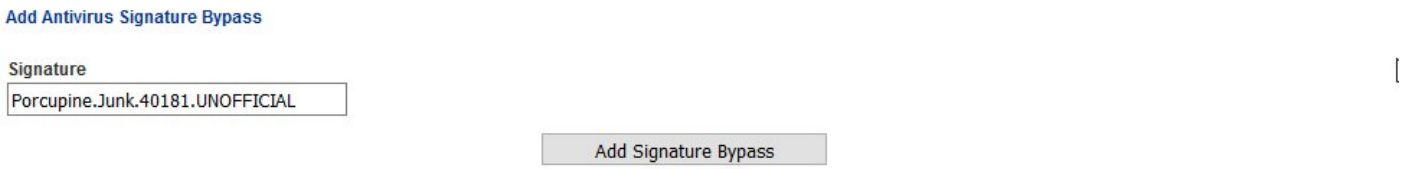
```
(04239-07) Blocked INFECTED (Porcupine.Junk.40181.UNOFFICIAL) {NoBounceInbound,Quarantined},
[66.23.206.148]:47676 [66.23.206.148] <costco-wholesale-dcomfort=fmhc.net@wholesalekostco.com> ->
<dcomfort@fmhc.net>, quarantine: virus/5/5i10CvwECO5J, Queue-ID: EF090403BB, Message-ID:
<0.0.0.18.1D3017FAF7702E0.172DE7@mail.wholesalekostco.com>, mail_id: 5i10CvwECO5J, Hits: -, size: 6800,
dkim_sd=dkim:wholesalekostco.com, 272 ms</dcomfort@fmhc.net></costco-wholesale-
dcomfort=fmhc.net@wholesalekostco.com>
```

Assuming, this was a legitimate email and you wished to bypass the signature that caused this email to be blocked, you would simply bypass the **Porcupine.Junk.40181.UNOFFICIAL** signature.

Add Antivirus Signature Bypass

1. In the **Add Antivirus Signature Bypass** section, below the **Signature** field enter the signature you wish to bypass and click the **Add Signature Bypass** button (**Figure 1**).

Figure 1



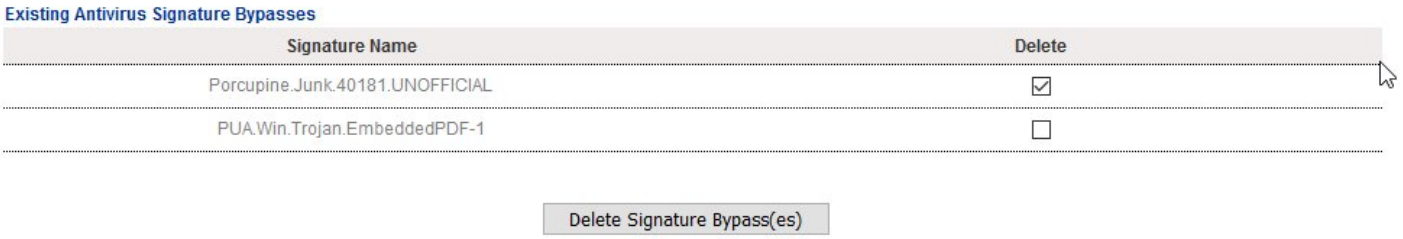
2. As you add signatures, they will show up under the **Existing Antivirus Signature Bypasses** section (**Figure 2**).

Figure 2

Delete Antivirus Signature Bypass

1. Under **Existing Antivirus Signature Bypasses** section, place a checkmark in the checkbox under the **Delete** column of the signatures you wish to delete.
2. Click the **Delete Signature bypass(es)** button below (**Figure 3**).

Figure 3



Revision #1
Created 2 January 2021 14:33:52 by Dino Edwards
Updated 20 May 2023 22:22:35 by Dino Edwards