

Why is my virus type report showing a lower number of virus instances than my mail summary report?



Document ID: 118458

Contributed by Cisco TAC Engineers.

Oct 13, 2014

Contents

Question

Answer

Question

Why is my virus type report showing a lower number of virus instances than my mail summary report?

Answer

The Virus Type report on the Cisco Email Security Appliance (ESA) or Cisco Security Management Appliance (SMA) shows a lower number of virus instances than the mail summary report.

Example: The report on Virus Types lists a total of three viruses, while the Mail Summary Report shows 103 virus instances.

The difference in reporting is caused by the Virus Type Report lists (as the name says) reporting the actual names of viruses found by the antivirus engine, while the Mail Summary Report also counts the following events as 'virus':

- AV repaired message
- AV encrypted message that is dropped/quarantined
- AV unscannable message that is dropped/quarantined

So the Mail Summary Report also lists messages that do not contain a real virus (so that it would qualify for the virus type report), as they were not flagged as clean messages by the antivirus engine.