

# How to send a sample message to ensure Anti-Virus engine is scanning on a Cisco Email Security Appliance (ESA)

## Contents

[Introduction](#)

[How to send a sample message to ensure Anti-Virus engine is scanning on a Cisco Email Security Appliance \(ESA\)](#)

[Create a TXT File](#)

[Sending Sample Message](#)

[UNIX CLI](#)

[Outlook](#)

[Verification](#)

[Related Information](#)

---

## Introduction

This document describes how to send a sample message to ensure either the Sophos anti-virus or McAfee anti-virus engine is scanning on a Cisco Email Security Appliance (ESA).

## How to send a sample message to ensure Anti-Virus engine is scanning on a Cisco Email Security Appliance (ESA)

By sending a sample message with a test viral payload through the ESA, we can trigger the Sophos or McAfee anti-virus engine. Prior to performing the steps listed in this document, you will need to set up your Incoming or Outgoing Mail Policy and configure the mail policy to have anti-virus drop or quarantine virus infected messages. This document uses ASCII code provided from EICAR ([www.eicar.org](http://www.eicar.org)) that will simulate a [test virus](#) as an attachment:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

**Note:** Per EICAR: *This test file has been provided to EICAR for distribution as the "EICAR Standard Anti-Virus Test File", and it satisfies all the criteria listed above. It is safe to pass around, because it is not a virus, and does not include any fragments of viral code. Most products react to it as if it were a virus (though they typically report it with an obvious name, such as "EICAR-AV-Test").*

## Create a TXT File

Using the ASCII string above, create a .txt file and place the string as written as the body of the file. You will be able to send this file as an attachment in your sample message.

## Sending Sample Message

Depending on how you work, you can send the sample message through the ESA various ways. Two example methods are via UNIX CLI using the **mail** or from Outlook (or other email application).

### UNIX CLI

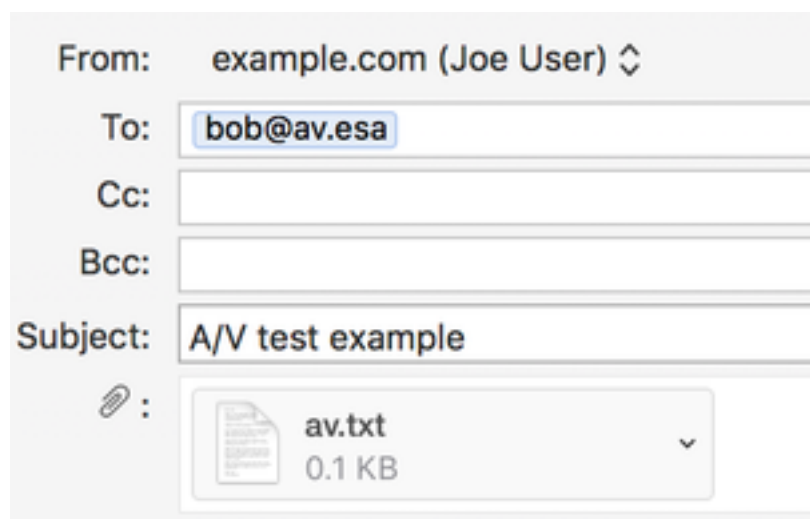
```
joe@unix.local:~$ echo "TEST MESSAGE w/ ATTACHMENT" | mail -s "A/V test example" -A av.txt bob@av.esa
```

Your UNIX environment will need to be properly setup to send or relay mail through your ESA.

### Outlook

Using Outlook (or another email application), you have two choices in sending the ASCII code through: 1) using the created .txt file, 2) direct paste of the ASCII string in the body of the mail message.

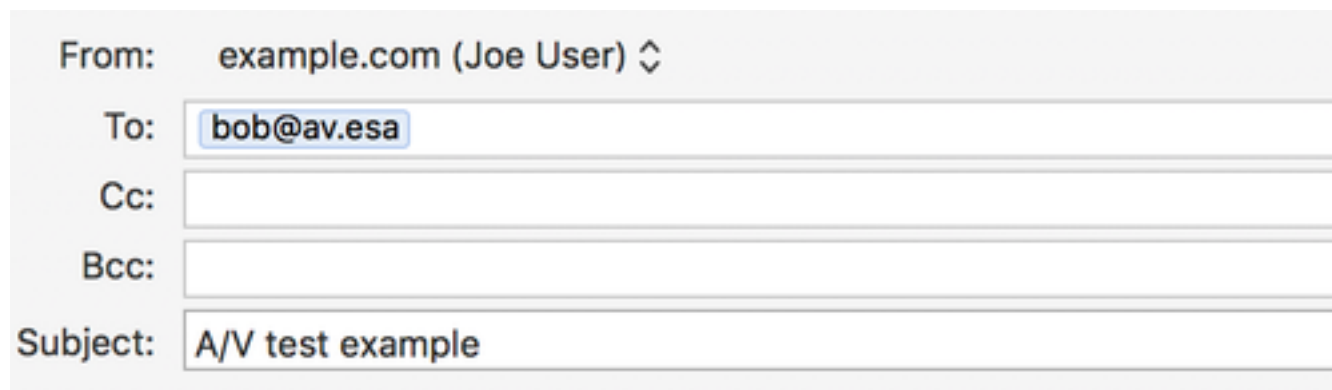
Using the .txt file as an attachment:



The screenshot shows an Outlook email composition window. The 'From' field is 'example.com (Joe User)' with a dropdown arrow. The 'To' field contains 'bob@av.esa'. The 'Cc' and 'Bcc' fields are empty. The 'Subject' field contains 'A/V test example'. Below the subject field, there is a paperclip icon followed by a file attachment box. The box contains a document icon, the filename 'av.txt', and the size '0.1 KB'. A small downward arrow is on the right side of the attachment box.

### TEST MESSAGE w/ ATTACHMENT

Using the ASCII string in the body of the mail message:



The screenshot shows an Outlook email composition window, similar to the one above but without the attachment. The 'From' field is 'example.com (Joe User)' with a dropdown arrow. The 'To' field contains 'bob@av.esa'. The 'Cc' and 'Bcc' fields are empty. The 'Subject' field contains 'A/V test example'.

X5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H\*

Your Outlook (or other email application) will need to be properly setup to send or relay mail through your ESA.

## Verification

On the ESA CLI, use the command **tail mail\_logs** prior to sending the sample message. While watching the mail log you will see the message is scanned and caught by McAfee as "VIRAL":

```
Wed Sep 13 11:42:38 2017 Info: New SMTP ICID 306 interface Management (10.1.2.84) address
10.1.2.85 reverse dns host zane.local verified yes
Wed Sep 13 11:42:38 2017 Info: ICID 306 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country
Australia
Wed Sep 13 11:42:38 2017 Info: Start MID 405 ICID 306
Wed Sep 13 11:42:38 2017 Info: MID 405 ICID 306 From: <joe@example.com>
Wed Sep 13 11:42:38 2017 Info: MID 405 ICID 306 RID 0 To: <bob@av.esa>
Wed Sep 13 11:42:38 2017 Info: MID 405 Message-ID '<20170913153801.0EDA1A0121@example.com>'
Wed Sep 13 11:42:38 2017 Info: MID 405 Subject 'A/V test attachment'
Wed Sep 13 11:42:38 2017 Info: MID 405 ready 1057 bytes from <joe@example.com>
Wed Sep 13 11:42:38 2017 Info: MID 405 attachment 'av.txt'
Wed Sep 13 11:42:38 2017 Info: ICID 306 close
Wed Sep 13 11:42:38 2017 Info: MID 405 matched all recipients for per-recipient policy my_av in
the inbound table
Wed Sep 13 11:42:38 2017 Info: MID 405 interim AV verdict using McAfee VIRAL
Wed Sep 13 11:42:38 2017 Info: MID 405 antivirus positive 'EICAR test file'
Wed Sep 13 11:42:38 2017 Info: MID 405 enqueued for transfer to centralized quarantine "Virus"
(a/v verdict VIRAL)
Wed Sep 13 11:42:38 2017 Info: MID 405 queued for delivery
Wed Sep 13 11:42:38 2017 Info: New SMTP DCID 239 interface 10.1.2.84 address 10.1.2.87 port 7025
Wed Sep 13 11:42:38 2017 Info: DCID 239 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-GCM-
SHA384 the.cpq.host
Wed Sep 13 11:42:38 2017 Info: Delivery start DCID 239 MID 405 to RID [0] to Centralized Policy
Quarantine
Wed Sep 13 11:42:38 2017 Info: Message done DCID 239 MID 405 to RID [0] (centralized policy
quarantine)
Wed Sep 13 11:42:38 2017 Info: MID 405 RID [0] Response 'ok: Message 49 accepted'
Wed Sep 13 11:42:38 2017 Info: Message finished MID 405 done
Wed Sep 13 11:42:43 2017 Info: DCID 239 close
```

The same message sent through and scanned by Sophos:

```
Wed Sep 13 11:44:24 2017 Info: New SMTP ICID 307 interface Management (10.1.2.84) address
10.1.2.85 reverse dns host zane.local verified yes
Wed Sep 13 11:44:24 2017 Info: ICID 307 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country
Australia
Wed Sep 13 11:44:24 2017 Info: Start MID 406 ICID 307
Wed Sep 13 11:44:24 2017 Info: MID 406 ICID 307 From: <joe@example.com>
Wed Sep 13 11:44:24 2017 Info: MID 406 ICID 307 RID 0 To: <bob@av.esa>
Wed Sep 13 11:44:24 2017 Info: MID 406 Message-ID '<20170913153946.E20C7A0121@example.com>'
Wed Sep 13 11:44:24 2017 Info: MID 406 Subject 'A/V test attachment'
Wed Sep 13 11:44:24 2017 Info: MID 406 ready 1057 bytes from <joe@example.com>
Wed Sep 13 11:44:24 2017 Info: MID 406 attachment 'av.txt'
Wed Sep 13 11:44:24 2017 Info: ICID 307 close
Wed Sep 13 11:44:24 2017 Info: MID 406 matched all recipients for per-recipient policy my_av in
the inbound table
Wed Sep 13 11:44:24 2017 Info: MID 406 interim AV verdict using Sophos VIRAL
Wed Sep 13 11:44:24 2017 Info: MID 406 antivirus positive 'EICAR-AV-Test'
Wed Sep 13 11:44:24 2017 Info: MID 406 enqueued for transfer to centralized quarantine "Virus"
(a/v verdict VIRAL)
Wed Sep 13 11:44:24 2017 Info: MID 406 queued for delivery
Wed Sep 13 11:44:24 2017 Info: New SMTP DCID 240 interface 10.1.2.84 address 10.1.2.87 port 7025
Wed Sep 13 11:44:24 2017 Info: DCID 240 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-GCM-
SHA384 the.cpq.host
```

Wed Sep 13 11:44:24 2017 Info: Delivery start DCID 240 MID 406 to RID [0] to Centralized Policy Quarantine

Wed Sep 13 11:44:24 2017 Info: Message done DCID 240 MID 406 to RID [0] (centralized policy quarantine)

Wed Sep 13 11:44:24 2017 Info: MID 406 RID [0] Response 'ok: Message 50 accepted'

Wed Sep 13 11:44:24 2017 Info: Message finished MID 406 done

Wed Sep 13 11:44:29 2017 Info: DCID 240 close

On this lab ESA, 'Virus Infected Messages' are configured to Quarantine for "Action Applied to Message" on the particular mail policy. The action on your ESA may vary, based on the action taken for virus infected messages handled by anti-virus on your mail policy.

## Related Information

- [Technical Support & Documentation - Cisco Systems](#)