

# 如何傳送示例消息以確保防病毒引擎在思科郵件安全裝置(ESA)上掃描

## 目錄

### [簡介](#)

[如何傳送示例消息以確保防病毒引擎在思科郵件安全裝置\(ESA\)上掃描](#)

[建立TXT檔案](#)

[傳送示例消息](#)

[UNIX CLI](#)

[Outlook](#)

[驗證](#)

[相關資訊](#)

---

## 簡介

本文檔介紹如何傳送示例消息以確保Sophos防病毒或McAfee防病毒引擎在思科郵件安全裝置(ESA)上掃描。

## 如何傳送示例消息以確保防病毒引擎在思科郵件安全裝置(ESA)上掃描

通過通過ESA傳送包含測試病毒負載的示例消息，我們可以觸發Sophos或McAfee防病毒引擎。在執行本文檔中列出的步驟之前，您需要設定傳入或傳出郵件策略，並將郵件策略配置為具有防病毒丟棄或隔離受病毒感染的郵件。本文使用從EICAR([www.eicar.org](http://www.eicar.org))提供的ASCII代碼，該代碼將模擬測試病毒作為附件：

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

**附註：**每個EICAR:此測試檔案已提供給EICAR，作為「EICAR標準防病毒測試檔案」分發，它滿足上面列出的所有標準。傳閱是安全的，因為它不是病毒，不包括任何病毒代碼片段。大多數產品對它的反應就像病毒一樣（儘管它們通常使用明顯的名稱，如「EICAR-AV-Test」）。

## 建立TXT檔案

使用上面的ASCII字串，建立.txt檔案，並將該字串作為檔案主體寫入。您將能夠將此檔案作為示例郵件中的附件傳送。

## 傳送示例消息

根據您的工作方式，您可以通過ESA以各種方式傳送示例消息。通過UNIX CLI使用mail或Outlook（或其他電子郵件應用程式）提供了兩種示例方法。

## UNIX CLI

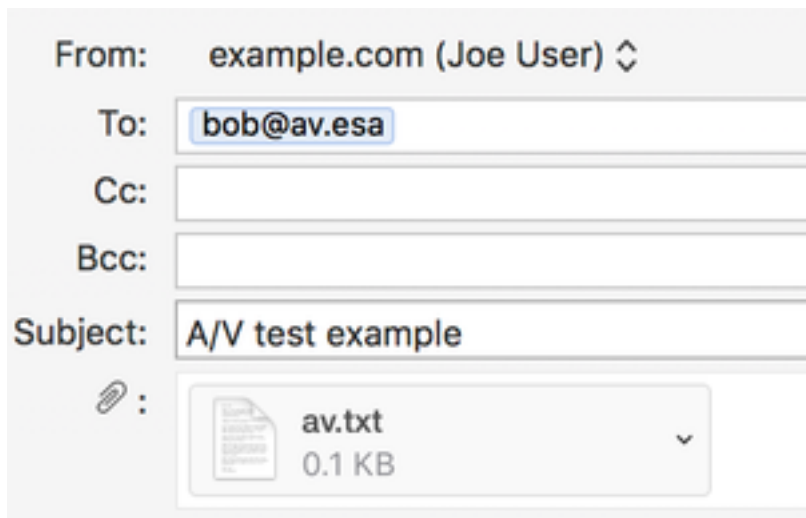
```
joe@unix.local:~$ echo "TEST MESSAGE w/ ATTACHMENT" | mail -s "A/V test example" -A av.txt bob@av.esa
```

需要正確設定UNIX環境，以便通過ESA傳送或中繼郵件。

## Outlook

使用Outlook ( 或其他電子郵件應用程式 )，您可以通過以下兩種方式傳送ASCII代碼：1)使用建立的.txt檔案，2)直接將ASCII字串貼上到郵件正文中。

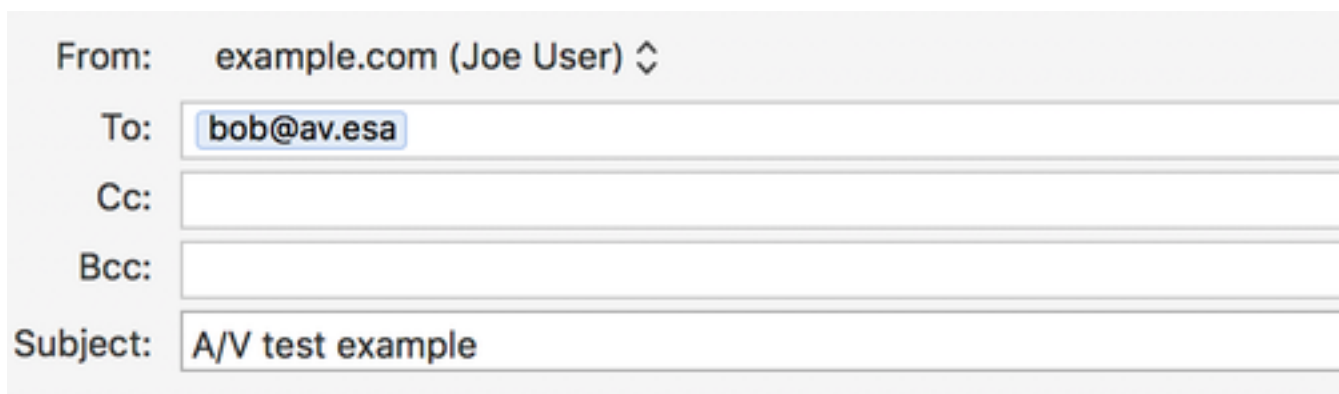
使用.txt檔案作為附件：



The screenshot shows an Outlook email composition window. The 'From' field is 'example.com (Joe User)'. The 'To' field is 'bob@av.esa'. The 'Subject' field is 'A/V test example'. There is an attachment named 'av.txt' with a size of '0.1 KB'.

## TEST MESSAGE w/ ATTACHMENT

使用郵件正文中的ASCII字串：



The screenshot shows an Outlook email composition window. The 'From' field is 'example.com (Joe User)'. The 'To' field is 'bob@av.esa'. The 'Subject' field is 'A/V test example'.

```
X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

需要正確設定Outlook ( 或其他電子郵件應用程式 ) 才能通過ESA傳送或中繼郵件。

## 驗證

在ESA CLI上，在傳送示例消息之前使用tail mail\_logs命令。 在檢視郵件日誌時，您會看到

## McAfee以「病毒」的身份掃描並捕獲郵件：

```
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
```

## 通過Sophos傳送和掃描的同一郵件：

```
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

在本實驗中，ESA將「受病毒感染的郵件」配置為隔離特定郵件策略上的「應用到郵件的操作」。ESA上的操作可能會有所不同，具體取決於郵件策略中防病毒處理的受病毒感染的郵件所採取的操作。

## 相關資訊

- [技術支援與文件 - Cisco Systems](#)