如何在郵件安全裝置和雲郵件安全上存檔電子郵件？

目錄

簡介

本文檔介紹在電子郵件安全裝置(ESA)和Cloud Email Security(CES)上存檔電子郵件以進行檢索和審閱要遵循的步驟。

背景資訊

當您在ESA和CES上存檔電子郵件時，它可用於滿足法規要求，或提供其他資料手段用於進一步的郵件診斷和審查。存檔電子郵件充當電子郵件的輔助儲存，這些電子郵件以mbox日誌格式儲存在管理員的原始源中，以便進行檢索和驗證。

- 如果您決定啟用電子郵件存檔，建議將這些設定保留為預設值。預設值為10MB/日誌和10個最大保留日誌。將根據日誌檔案自身的大小繼續新增和滾動日誌。存檔郵箱日誌檔案根據通過裝置的電子郵件流量速率進行填充。隨著建立更多的日誌，舊的歸檔郵箱日誌會被刪除，以釋放空間用於建立新日誌。
- 在增加歸檔檔案大小和保留的最大日誌檔案之前，請確保裝置具有足夠的磁碟空間。
- 為了停止生成存檔郵箱日誌，您必須按策略禁用存檔功能。

附註：ESA和CES存檔郵箱日誌無法由安全管理裝置(SMA)檢索，並且在啟用此功能的情況下，按每個ESA和CES本地儲存。

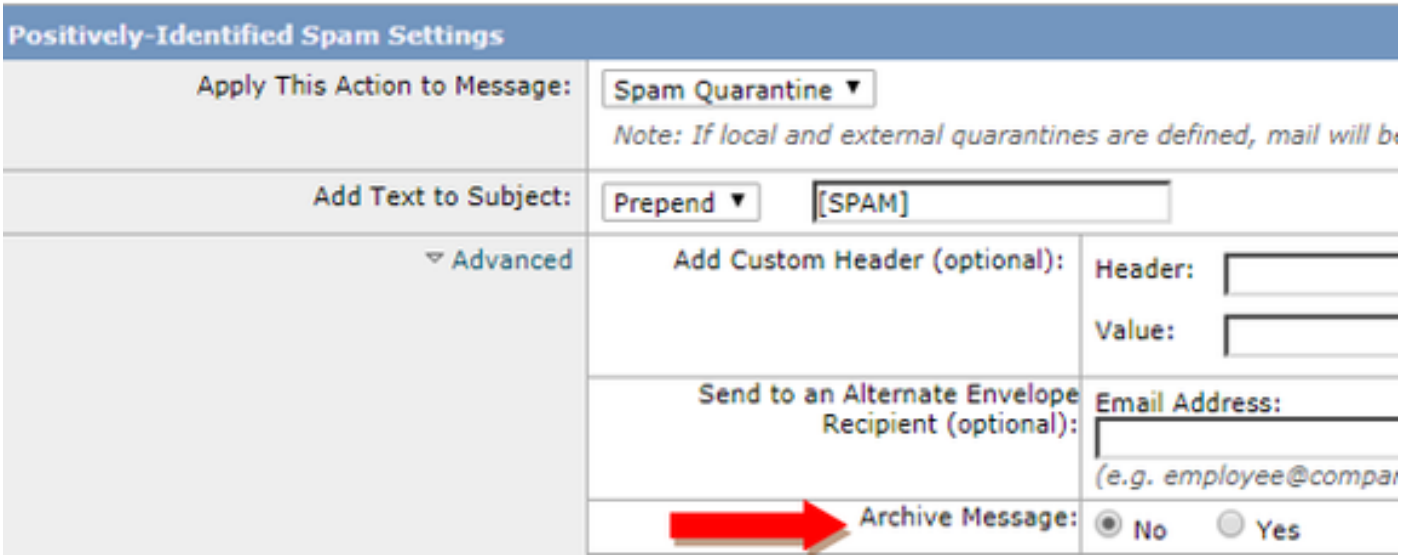
如何存檔ESA和CES上的電子郵件？

電子郵件存檔可用反垃圾郵件、防病毒、高級惡意軟體防護、灰色郵件和郵件篩選器。可以通過圖形使用者介面(GUI)或命令列介面(CLI)為反垃圾郵件、防病毒、高級惡意軟體防護和灰色郵件配置存檔操作。

對於郵件過濾器，可以使用CLI單獨配置存檔操作。

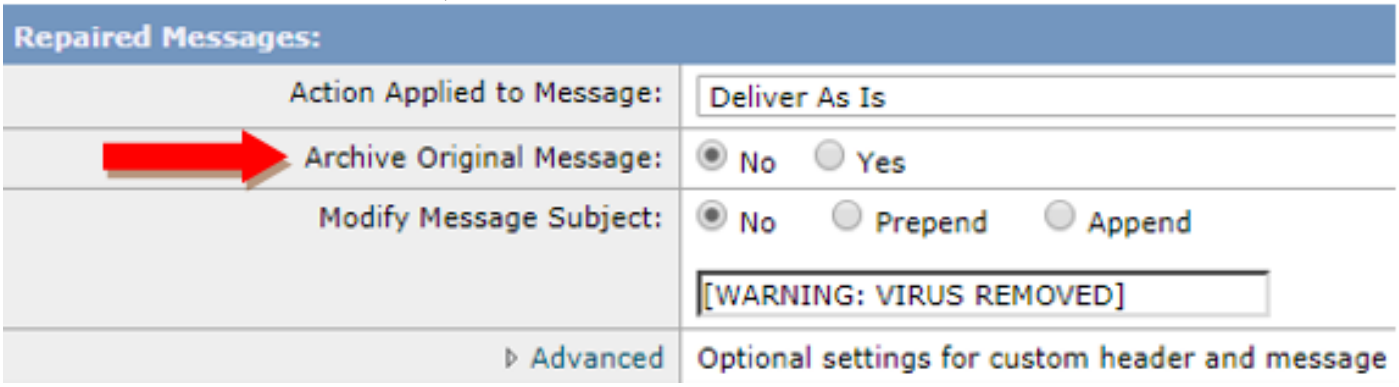
配置反垃圾郵件存檔

1. 導航到**GUI > Mail Policies > Incoming/Outgoing Mail Policies**。
2. 按一下相應策略的「反垃圾郵件」設定以配置電子郵件存檔。
3. 在「已正確識別的垃圾郵件設定」和/或「可疑垃圾郵件」設定的可用設定上按一下**高級**。
4. 按「Yes（是）」旁邊的單選按鈕以存檔具有相應反垃圾郵件判定結果的電子郵件。
5. 提交配置並提交這些更改，如下圖所示。



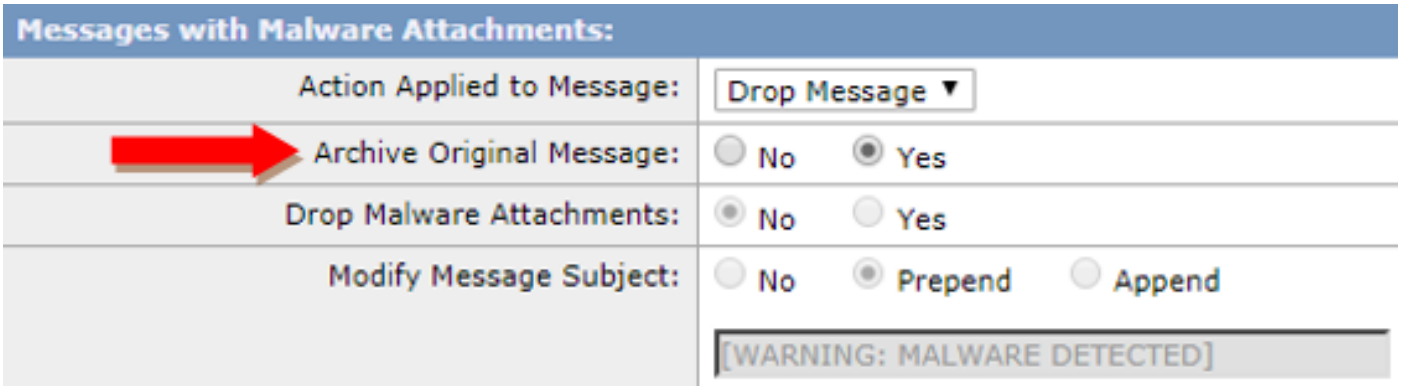
配置防病毒存檔

1. 導航到**GUI > Mail Policies > Incoming/Outgoing Mail Policies**。
2. 按一下相應策略上的防病毒設定以配置電子郵件歸檔。
3. 在要存檔原始郵件的每個掃描判定上，按「Yes（是）」旁邊的單選按鈕進行存檔。
4. 提交配置並提交這些更改，如下圖所示。



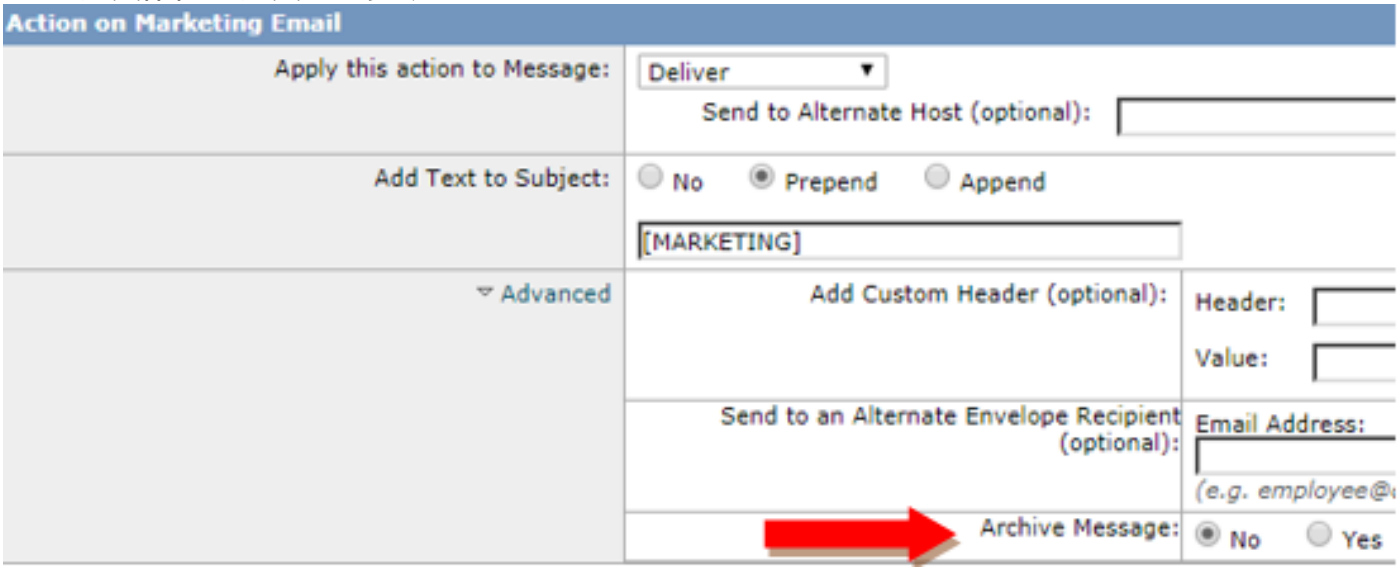
配置高級惡意軟體防護存檔

1. 導航到**GUI > Mail Policies > Incoming/Outgoing Mail Policies**。
2. 按一下相應策略上的Advanced Malware Protectionsettings（高級惡意軟體保護設定），以配置電子郵件存檔。
3. 在要存檔原始郵件的每個掃描判定上，按「Yes（是）」旁邊的單選按鈕進行存檔。
4. 提交配置並提交這些更改，如下圖所示。



配置灰色郵件存檔

1. 導航到**GUI > Mail Policies > Incoming/Outgoing Mail Policies**。
2. 按一下相應策略上的Graymail設定以配置電子郵件存檔。
3. 按一下Advanced（高級）開啟Marketing、Social、Bulk的可用設定。
4. 按「Yes（是）」旁邊的單選按鈕，以存檔帶有相應灰色郵件判定結果的電子郵件。
5. 提交配置並提交這些更改。



配置郵件過濾器存檔

> **注意**：必須使用包含歸檔操作的郵件過濾器才能檢視歸檔日誌。只能在CLI中建立郵件過濾器。

示例篩選器：

```
Test_Archive:
if (mail-from == "test1@cisco.com")
{
archive("Test");
}
```

1. 在CLI上登入裝置。
2. 如所提供的示例過濾器中所示，建立郵件過濾器。
3. 提交此篩選器並提交更改。

驗證存檔Mbox日誌可用性

當為各個服務提交歸檔配置時，歸檔的電子郵件將儲存在mbox格式的日誌檔案中。要驗證歸檔日誌是否可用於檢索，請導航到**GUI > System Administration > Log Subscriptions**。

安全服務歸檔檔案使用歸檔日誌型別建立單獨的日誌，如下圖所示：

Configured Log Subscriptions

Add Log Subscription...

Log Settings	Type ▲	Log Files	Rollover Interval
amp	AMP Engine Logs	amp/	None
amparchive	AMP Archive	amparchive/	None
antispam	Anti-Spam Logs	antispam/	None
antivirus	Anti-Virus Logs	antivirus/	None
asarchive	Anti-Spam Archive	asarchive/	None
authentication	Authentication Logs	authentication/	None
avarchive	Anti-Virus Archive	avarchive/	None

對於郵件過濾器，歸檔檔案配置僅從**CLI檢視**:

- **filters > logconfig**

```
demigod.cisco.com> filters

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> logconfig

Currently configured logs:
    Log Name          Log Type                  Retrieval          Interval
 ------------------------------------------------------------------------------
 1. Test              Filter Archive Logs       Manual Download    None
```

檢索Mbox日誌

對於獨立裝置，這些mbox日誌可以直接從GUI檢索。導航到**GUI > System Administration > Log Subscriptionand**按一下要檢索的相應歸檔日誌的**Log Files**。

對於集群裝置，可以使用FTP/安全複製(SCP)檢索mbox日誌，如本文所述。(https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00..。.)

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 什麼是 UNIX mbox（信箱）格式？
- 思科郵件安全裝置(ESA)中日誌儲存的位置，以及如何訪問這些日誌
- 如何從存檔mbox日誌提取電子郵件
- 技術支援與文件 - Cisco Systems