防止資料丟失 — 解決分類錯誤和掃描故障

目錄

簡介

本文描述常見方法，用於排除與郵件安全裝置(ESA)上的資料丟失防護(DLP)相關的錯誤分類和掃描故障（或失誤）。

必要條件

- 運行AsyncOS 11.x或更高版本的ESA。
- DLP功能金鑰已安裝並正在使用。

重要資訊

必須注意的是，ESA上的DLP是即插即用的，您可以啟用它、建立策略，並開始掃描敏感資料；但是，您還應注意，只有調整DLP以滿足您的公司特定要求後，才能獲得最佳結果。這將包括DLP策略的型別、策略匹配詳細資訊、調整嚴重性規模、過濾和其他自定義等內容。

違規與無違規日誌示例

以下是您在郵件日誌和/或郵件跟蹤中可能看到的DLP違規的一些示例。日誌行將包括時間戳、日誌記錄級別、MID編號、違規或無違規、嚴重性和風險因素以及匹配的策略。

```
Thu Jul 11 16:05:28 2019 Info: MID 40 DLP violation. Severity: CRITICAL (Risk Factor: 96). DLP policy match: 'US HIPAA and HITECH'.

Thu Jul 11 16:41:50 2019 Info: MID 46 DLP violation. Severity: LOW (Risk Factor: 24). DLP policy match: 'US State Regulations (Indiana HB 1101)'.
```

如果未發現違規，則郵件日誌和/或郵件跟蹤將只記錄*DLP無違規*。

```
Mon Jan 20 12:59:01 2020 Info: MID 26245883 DLP no violation
```

故障排除核對表

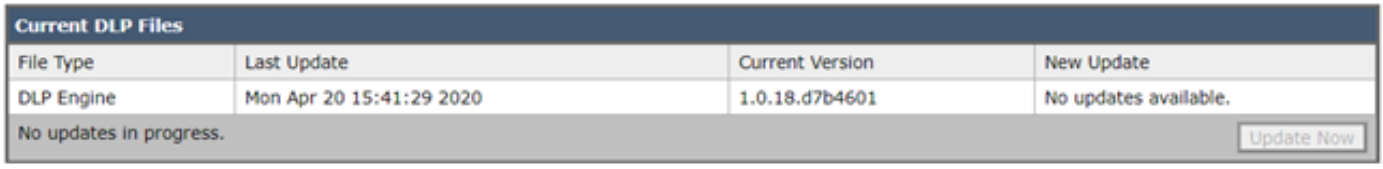
下面提供了一些常見專案，可在處理DLP錯誤分類或掃描失敗/錯誤時進行檢查。

附註：這不是一份詳盡的清單。如果您希望看到包含的內容，請聯絡Cisco TAC。

確認DLP引擎的版本

預設情況下，DLP引擎更新不會自動更新，因此確保運行包含任何最新增強功能或錯誤修復程式的最新版本至關重要。

您可以在GUI的*Security Services*下導航到*Data Loss Prevention*，以確認當前引擎版本並檢視是否有可用的更新。如果更新可用，則可以按一下*Update Now*執行更新。

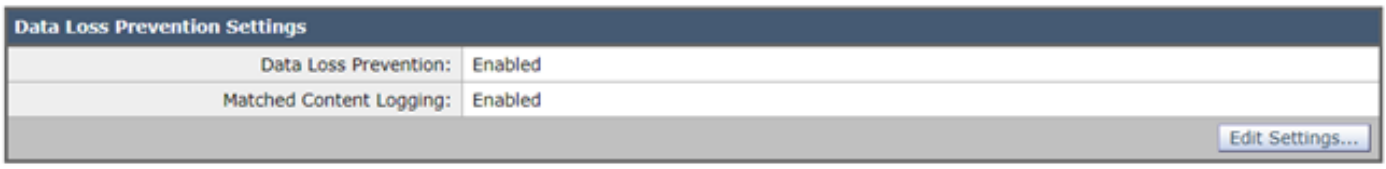


啟用匹配的內容記錄

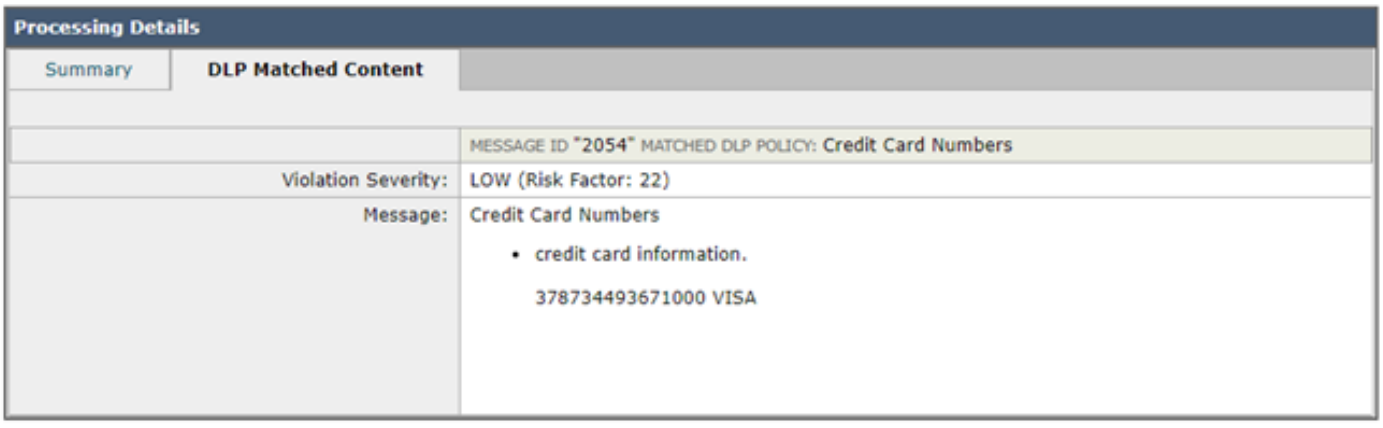
DLP提供了記錄違反DLP策略的內容以及周圍內容的選項。然後，可以在*郵件跟蹤*中檢視此資料，以幫助跟蹤郵件中的哪些內容可能會導致特定違規。

注意：瞭解如果啟用，此內容可能包括敏感資料（如信用卡號和社會保障號等）是很重要的。

您可以在GUI中的*Security Services*下導航到*Data Loss Prevention*，以檢視是否啟用了*Matched Content Logging*。



在郵件跟蹤中顯示的匹配內容日誌記錄示例

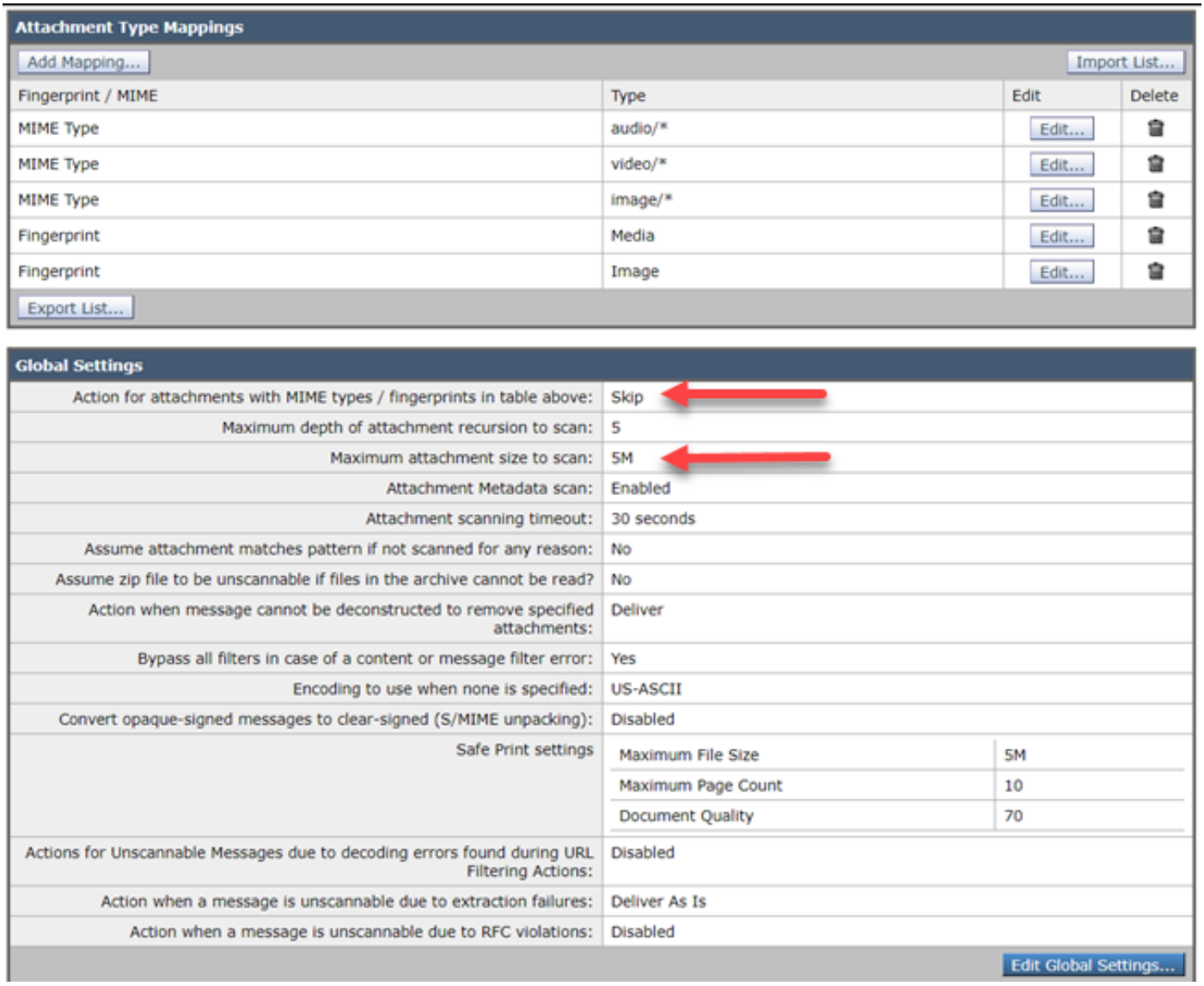


檢視掃描行為配置

ESA上的掃描行為配置也會影響DLP掃描後的功能。以下面的螢幕截圖為例，該截圖配置的最大附件掃描大小為**5M**，任何較大的內容都可能會導致DLP掃描丟失。此外，對**具有MIME型別設定**的附件執行的操作是另一個要審閱的常見項。應將其設定為**跳過**的預設值，這樣將跳過列出的MIME型別，並且掃描所有其他型別。如果設定為「掃描」，則只掃*描表中列出的*那些MIME型別。

同樣，此處列出的其他設定可能會影響DLP掃描，應根據附件/電子郵件內容予以考慮。

您可以在GUI中的*Security Services*下導航到*Scan Behavior*，也可以在CLI中運行*scanconfig*命令。



Attachment Type Mappings

Add Mapping... | Import List...

Fingerprint / MIME	Type	Edit	Delete
MIME Type	audio/*	Edit...	
MIME Type	video/*	Edit...	
MIME Type	image/*	Edit...	
Fingerprint	Media	Edit...	
Fingerprint	Image	Edit...	

Export List...

Global Settings

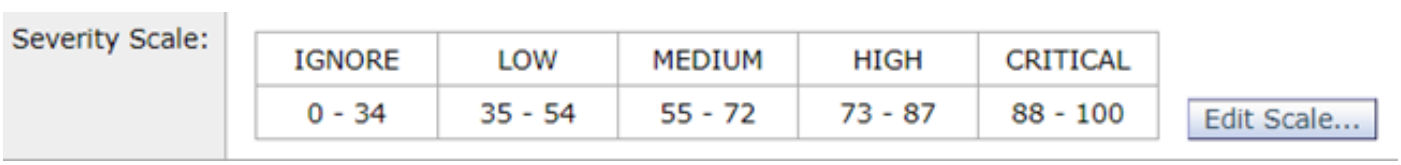
Action for attachments with MIME types / fingerprints in table above:	Skip
Maximum depth of attachment recursion to scan:	5
Maximum attachment size to scan:	5M
Attachment Metadata scan:	Enabled
Attachment scanning timeout:	30 seconds
Assume attachment matches pattern if not scanned for any reason:	No
Assume zip file to be unscannable if files in the archive cannot be read?	No
Action when message cannot be deconstructed to remove specified attachments:	Deliver
Bypass all filters in case of a content or message filter error:	Yes
Encoding to use when none is specified:	US-ASCII
Convert opaque-signed messages to clear-signed (S/MIME unpacking):	Disabled
Safe Print settings	Maximum File Size: 5M Maximum Page Count: 10 Document Quality: 70
Actions for Unscannable Messages due to decoding errors found during URL Filtering Actions:	Disabled
Action when a message is unscannable due to extraction failures:	Deliver As Is
Action when a message is unscannable due to RFC violations:	Disabled

Edit Global Settings...

檢視嚴重性刻度配置

對於大多數環境，預設嚴重性擴展閾值已足夠；但是，如果您需要修改它們來協助進行假陰性(FN)或假陽性(FP)匹配，則可以這樣做。您還可以通過建立新的虛擬策略並比較它們來確認DLP策略是否使用建議的預設閾值。

注意：不同的預定義策略（例如，美國HIPAA與PCI-DSS）將具有不同的擴展性。



Severity Scale:

IGNORE	LOW	MEDIUM	HIGH	CRITICAL
0 - 34	35 - 54	55 - 72	73 - 87	88 - 100

Edit Scale...

檢視新增到篩選器發件人和收件人欄位的電子郵件地址

檢查在這些欄位中輸入的條目是否與發件人和/或收件人電子郵件地址的正確大小寫匹配。Filter Sender and Recipients欄位區分大**小寫**。如果電子郵件地址在郵件客戶端中類似「TestEmail@mail.com」，並且以「testemail@mail.com」的形式輸入到這些欄位，則不會觸發DLP策略。

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 什麼是資料丟失保護？
- 觸發DLP違規以測試ESA上的HIPAA策略