

檢視DMARC報告並使用DMP解決驗證問題

目錄

[簡介](#)

[SPF是如何工作的？](#)

[DKIM是如何工作的？](#)

[DMARC如何工作？](#)

[問：如何使用DMP設定電子郵件身份驗證？](#)

[Q. DMP託管我的SPF記錄、DKIM記錄和DMARC策略。如何檢測錯誤或惡意活動？](#)

簡介

本文檔介紹如何驗證DMP處理的DMARC報告，以瞭解SPF和DKIM判定並維護安全的電子郵件生態系統。

SPF是如何工作的？

答：發件者策略框架(SPF)允許域所有者指定哪些發件人可以代表您的域傳送郵件。

DKIM是如何工作的？

A.域金鑰識別郵件(DKIM)使用金鑰對。授權發件人向消息新增數位簽章的私鑰和接收者驗證數位簽章真實性的公鑰，確保消息在傳送過程中未被修改。

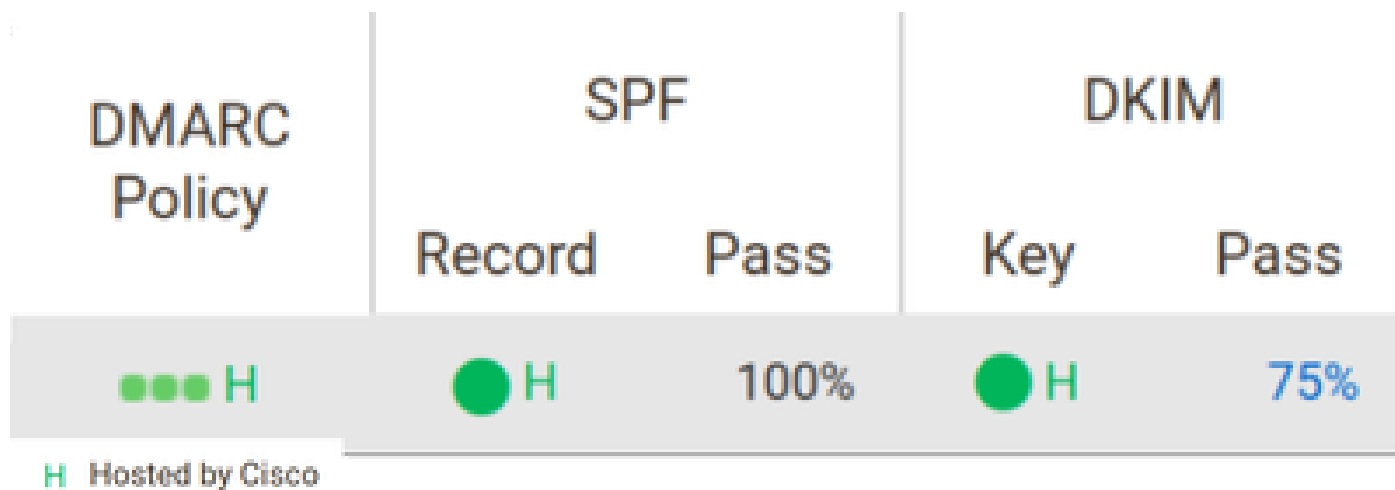
DMARC如何工作？

A.基於域的報文身份驗證、報告和一致性(DMARC)確保所有可用標識與From報頭保持一致。域所有者為接收者指定一個策略，告知接收者必須如何處理失敗郵件以及要將反饋報告傳送到何處，以便輕鬆識別錯誤或網路釣魚活動。

問：如何使用DMP設定電子郵件身份驗證？

答：Cisco Domain Protection(DMP)可以管理和託管您的SPF、DKIM和DMARC記錄。它要求您在域中發佈DNS TXT記錄，以將管理委託給DMP。在DMP託管您的記錄後，您可以通過DMP管理門戶管理批准的發件人、DKIM簽名金鑰和DMARC策略。

按一下DMP Dashboard中的Configuration Completed欄以驗證域狀態。



Q. DMP託管我的SPF記錄、DKIM記錄和DMARC策略。如何檢測錯誤或惡意活動？

A.您可以通過DMP管理員門戶診斷錯誤和惡意活動。導航到分析>電子郵件流量。按一下修改設定按鈕。選擇Single Domain，然後從下拉選單中選擇域。

Modify Report Settings

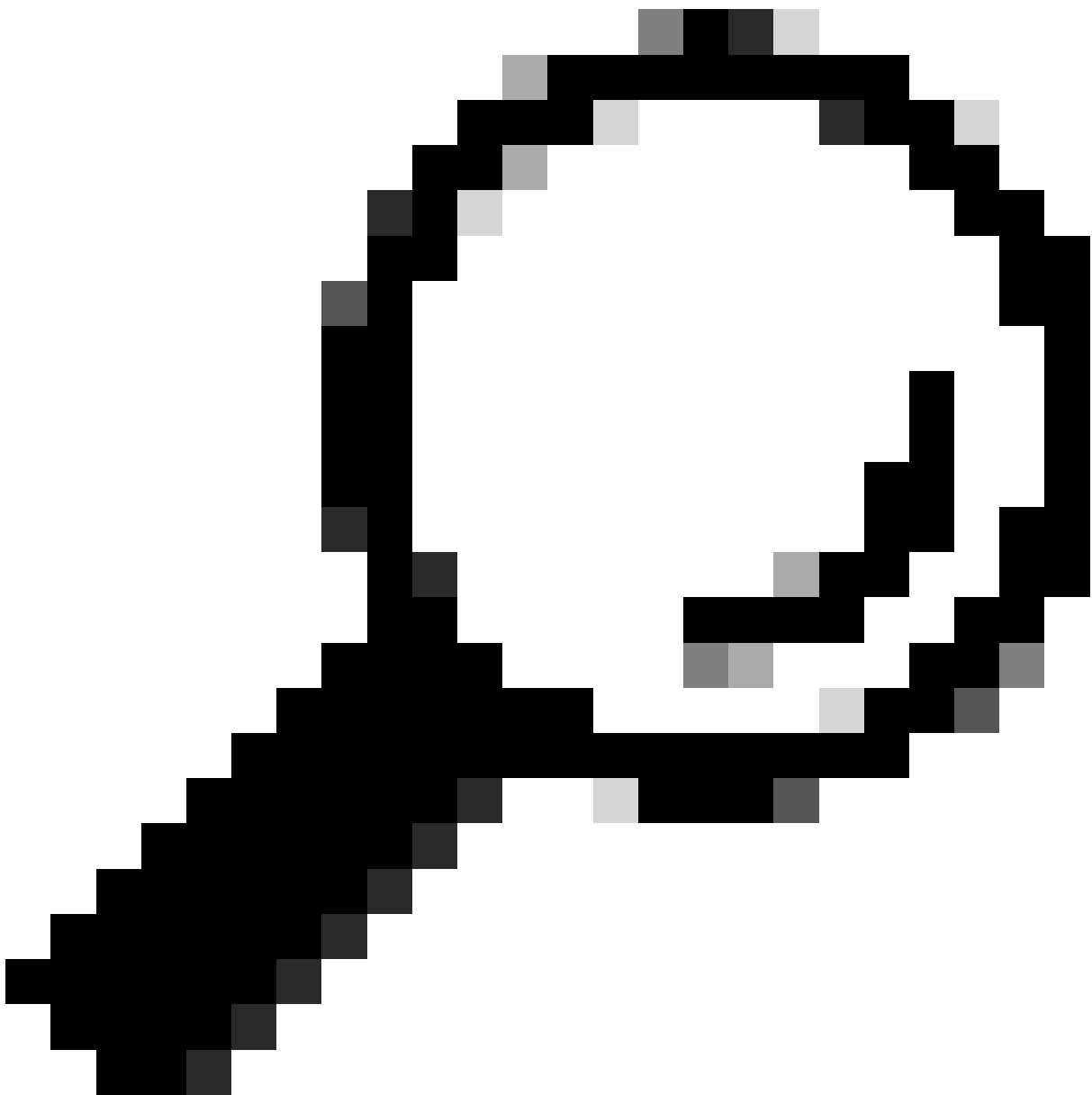
Select Domains

Domain Group: ☐ Active Domains

Single Domain: ☒

在「Things I Can Fix」部分下，選擇「What are my SPF problems?」或「What are my DKIM problems?」報告。

將滑鼠懸停在圖表節上可檢視相應問題的說明，或單擊某個節可細化詳細資訊。



提示：在修改報告設定中選擇更長的資料範圍，以準確瞭解您的電子郵件生態系統狀態。
您可以在您的域中找到您不知道或尚未對郵件進行簽名的有效發件人。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。