

為安全電子郵件網關配置DKIM大金鑰驗證

目錄

[簡介](#)

[必要條件](#)

[採用元件](#)

[概觀](#)

[設定](#)

[驗證](#)

[相關資訊](#)

簡介

本檔案說明已簽署電子郵件的擴充DKIM較大金鑰大小驗證功能。

必要條件

需要具備SEG設定和配置的一般知識。

採用元件

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1及更高版本
- DKIM驗證配置檔案
- 郵件流策略

"本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路處於活動狀態，請確保您瞭解所有命令的潛在影響。"

概觀

SEG可以執行DKIM簽名電子郵件的入站驗證。

過去，SEG驗證金鑰範圍為512-2048，而不是15.5 AsyncOS。

AsyncOS 15.5支援1024-4096位的金鑰範圍

雖然升級前包含512-768的設定檔仍然有效，但是512和768位元大小的金鑰15.5現在已停用。

設定

SEG設定非常小，以適應新的金鑰大小。

在WebUI中導覽至：

- 郵件策略
 - 網域金鑰
 - DKIM驗證配置檔案

Outbound DKIM Verification

Profile Name:

Smallest Key to be Accepted: Bits

Largest Key to be Accepted: Bits

Maximum Number of Signatures in the Message to Verify: Use Default (5)

Key Query Timeout Limit: Use Default (10 Seconds) Seconds

Limit to Tolerate Wall Clock Asynchronization Between Sender and Verifier: Use Default (60 Seconds) Seconds

Use a Body Length Parameter: Yes No

SMTP Action for Temporary Failure: Accept Reject

Change SMTP Response Settings

Response Code:

Description:

SMTP Action for Permanent Failure: Accept Reject

Change SMTP Response Settings

Response Code:

Description:

DKIM驗證配置檔案

DKIM Verification Profiles Items per page 20


Profile Name ▲	Smallest Key (Bits)	Largest Key (Bits)	Key Query Timeout (Seconds)	Use Body Length Parameter	SMTP Action For Temporary Failure	SMTP Action For Permanent Failure	Maximum Number of Signatures to Verify	All <input type="checkbox"/> Delete
DEFAULT	512	2048	10	Yes	Accept	Accept	5	<input type="checkbox"/>
DKIM_Large	1024	4096	10	Yes	Accept	Accept	5	<input type="checkbox"/>

DKIM驗證配置檔案概要頁

將新的DKIM驗證配置檔案應用於所需的傳入郵件流策略：

- 郵件策略
 - 郵件流策略
 - 根據您的組織首選項，選擇所需的郵件流策略以應用新的DKIM驗證配置檔案。
 - 向下滾動至「Security Features (安全功能)」部分，找到「DKIM Verification：」
 - 選取您選擇的適當設定檔。

DKIM Verification:	<input type="radio"/> Use Default (On: DEFAULT) <input checked="" type="radio"/> On <input type="radio"/> Off	DEFAULT
	Use DKIM Verification Profile: 	✓ DKIM_Large

 注意：在AsyncOS 15.5之前，DKIM驗證被限制為2048位，並且會傳遞一個較大的金鑰大小作為無符號。

驗證

SEG不會記錄郵件日誌或郵件跟蹤中金鑰大小的詳細資訊。

在AsyncOS 15.5之前，大型1024-4096 DKIM簽名會作為無簽名通過。

DKIM大金鑰大小的某些小指示符需要進行後處理檢查。

- b=值的標題擷取和檢閱。雖然此值不是直接計算值，但金鑰大小越大，該值就越大。
- DKIM DNS記錄顯示配對的公鑰，其大小從（估計）512位的180位元組增加到4096位的800位元組。
- 公開搜尋「DKIM金鑰大小檢查」可產生多個網站，其中包含擷取DKIM記錄的搜尋工具。使用選擇器和域，這些站點查詢DNS記錄並生成金鑰位大小，DNS查詢結果在輸出中。

相關資訊

- [Cisco Secure Email Gateway - 安裝指南](#)
- [用於支援指南的思科安全郵件網關啟動頁面](#)
- [Cisco Secure Email Gateway - 版本說明](#)

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）。