# ESA — 更換現有DKIM金鑰，無停機時間

## 目錄



## 簡介

本文說明如何在不停機的情況下替換ESA上現有的DKIM簽名金鑰和DNS中的DKIM公鑰。

## 需求

1. 對郵件安全裝置(ESA)的訪問。
2. 訪問DNS以新增/刪除TXT記錄。
3. ESA必須已經使用DKIM配置檔案對郵件進行簽名。

## 建立新的DKIM簽名金鑰

您首先需要在ESA上建立新的DKIM簽名金鑰：

1. 轉到「郵件策略」>「簽名金鑰」，然後選擇「新增金鑰……」
2. 為DKIM金鑰命名，並生成新的私鑰或貼上到現有私鑰中。 **附註**：*在大多數情況下，建議您選擇2048位私鑰大小*。
3. 提交更改。
   **附註**：此更改不會影響DKIM簽名或郵件流。我們只是新增DKIM簽名金鑰，尚未將其應用於任何DKIM簽名配置檔案。

## 生成新的DKIM簽名配置檔案並將DNS記錄發佈到DNS

接下來，您需要建立新的DKIM簽名配置檔案，從該DKIM簽名配置檔案生成DKIM DNS記錄並將該記錄發佈到DNS:

1. 轉到「郵件策略」>「簽名配置檔案」，然後按一下「新增配置檔案……」 在「配置檔名稱」欄位中為配置檔案指定描述性名稱。在「域名」欄位中輸入您的域。在"Selector"欄位中輸入新的選擇器字串。
   **附註**： *選擇器是一個任意字串，用於允許給定域的多個DKIM DNS記錄。我們將使用選擇器為您的域在DNS中允許多個DKIM DNS記錄。必須使用不同於現有DKIM簽名配置檔案的新選擇器。*
   在「Signing Key」欄位中選擇在上一節中建立的DKIM簽名金鑰。在簽名配置檔案的最底部

，新增新的「使用者」。 此使用者應為未使用的佔位符電子郵件地址。 **注意**：*您必須將未使用的電子郵件地址新增為此簽名配置檔案的使用者。否則，此配置檔案可能會在發佈DKIM TXT記錄之前對出站郵件進行簽名，從而導致DKIM驗證失敗。將未使用的電子郵件地址新增為使用者可確保此簽名配置檔案不會對任何出站郵件進行簽名。*點選提交。

2. 在此處，針對您剛剛建立的簽名配置檔案，按一下「DNS文本記錄」列中的「生成」，然後複製生成的DNS記錄。其外觀應類似於以下內容：

```
selector2._domainkey.example.com. IN TXT "v=DKIM1;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwMaX6wMAk4iQoLNWiEkj0BrIRMDHXQ7743OQUOYZQqEXS
s+jMGomOknAZJpjR8TwmYHVPbD+30QRw0qEiRY3hYcmKOCWZ/hTo+NQ8qj1CSc1LTMdV0HWAi2AGsVOT8BdFHkyxg40
oyGWgktzc1q7zIgWM8usHfKVWFzYgnattNzyEqHsfI7lGilz5gdHBOvmF8LrDSfN"
"KtGrTtvIxJM8pWeJm6pg6TM/cy0FypS2azkrl9riJcWWDvu38JXFL/eeYjGnB1zQeR5Pnbc3sVJd3cGaWx1bWjepyN
QZ1PrS6Zwr7ZxSRa316Oxc36uCid5JAq0z+IcH4KkHqUueSGuGhwIDAQAB;"
```

3. 提交更改。
4. 將步驟2中的DKIM DNS TXT記錄提交到DNS。
5. 等待DKIM DNS TXT記錄完全傳播。

# 刪除舊簽名配置檔案並從新簽名配置檔案中刪除佔位符使用者

將DKIM TXT記錄提交到DNS並確保它已傳播後，下一步是刪除舊的簽名配置檔案並從新的簽名配置檔案中刪除佔位符使用者：

> **附註**： *強烈建議您在繼續執行以下步驟之前備份ESA配置檔案。這是因為如果刪除了舊的DKIM簽名配置檔案，並且需要恢復為以前的配置，則可以輕鬆載入已備份的配置檔案。*

1. 轉至Mail Policies > Signing Profiles，選擇舊的DKIM簽名配置檔案，然後按一下「Delete」。
2. 進入新的DKIM簽名配置檔案，選擇當前佔位符使用者，然後按一下「刪除」。
3. 按一下「提交」。
4. 在「Test Profile」列下，按一下新DKIM簽名配置檔案的「Test」。如果測試成功，請繼續執行下一步。如果不是，請確認DKIM DNS TXT記錄已完全傳播。
5. 提交所做的更改。

# 測試郵件流以確認DKIM通過

此時，您已完成進一步配置DKIM。但是，您應測試DKIM簽名，以確保它按預期對出站郵件進行簽名並通過DKIM驗證：

1. 通過ESA傳送消息，確保它獲得ESA簽名的DKIM以及另一台主機驗證的DKIM。
2. 在另一端收到消息後，檢查消息的報頭中是否存在報頭「Authentication-Results」。 查詢標頭的DKIM部分以確認它是否通過DKIM驗證。標題應類似於以下內容：
```
Authentication-Results: mx1.example.net; spf=SoftFail smtp.mailfrom=user1@example.net;
dkim=pass header.i=none; dmarc=fail (p=none dis=none) d=example.net
```
3. 查詢標頭「DKIM-Signature」，並確認使用了正確的選擇器和域：

```
DKIM-Signature: a=rsa-sha256; d=example.net; s=selector2;
  c=simple; q=dns/txt; i=@example.net;
  t=1117574938; x=1118006938;
  h=from:to:subject:date;
  bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
  b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
```

VoG4ZHRNiYzR

4. 一旦您確信DKIM正在按預期工作，請至少等待一個星期，然後再刪除舊的DKIM TXT記錄。這可確保已處理由舊DKIM金鑰簽名的所有郵件。