

# 從ESA退回配置中免除IP地址/域/電子郵件地址

## 目錄

### [簡介](#)

[從ESA退回配置中免除IP地址/域/電子郵件地址](#)

[出站郵件](#)

[入站郵件](#)

[相關資訊](#)

## 簡介

本文說明如何配置入站和出站郵件，以免除思科郵件安全裝置(ESA)的IP地址、域或電子郵件地址。

## 從ESA退回配置中免除IP地址/域/電子郵件地址

ESA證。您需要配置出站和入站郵件。

## 出站郵件

1. 轉至Mail Policies > Destination Controls。
2. 選擇「新增目標.....」。
3. 呼叫新目標「example.com」。
4. 在設定中，將「退回驗證」設定為「否」。
5. 提交和提交更改。

Destination Controls	
Destination:	<input type="text" value="example.com"/>
IP Address Preference:	Default (IPv6 Preferred)
Limits:	Concurrent Connections: <input type="radio"/> Use Default (500) <input checked="" type="radio"/> Maximum of <input type="text" value="500"/> (between 1 and 1,000)
	Maximum Messages Per Connection: <input type="radio"/> Use Default (50) <input checked="" type="radio"/> Maximum of <input type="text" value="50"/> (between 1 and 1,000)
	Recipients: <input checked="" type="radio"/> Use Default (No Limit) <input type="radio"/> Maximum of <input type="text" value="0"/> per <input type="text" value="60"/> minutes <i>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</i>
	Apply limits: Per Destination: <input checked="" type="radio"/> Entire Domain <input type="radio"/> Each Mail Exchanger (MX Record) IP address  Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway <i>(recommended if Virtual Gateways are in use)</i>
TLS Support:	Default (None)  <i>A security certificate/key has not yet been configured. Enabling TLS will automatically enable the "Demo" certificate/key. (To configure a different certificate/key, start the CLI and use the certconfig command.)</i>
Bounce Verification:	Perform address tagging: <input type="radio"/> Default (No) <input checked="" type="radio"/> No <input type="radio"/> Yes  <i>Applies only if bounce verification address tagging is in use. See Mail Policies &gt; Bounce Verification.</i>
Bounce Profile:	Default  <i>Bounce Profile can be configured at Network &gt; Bounce Profiles.</i>

注意：對於出站郵件，您只能引用目標域，而不能引用IP地址或電子郵件地址。

## 入站郵件

Security Features	
Spam Detection:	<input checked="" type="radio"/> On <input type="radio"/> Off
Virus Protection:	<input checked="" type="radio"/> On <input type="radio"/> Off
Encryption and Authentication:	TLS: <input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required <i>A security certificate/key has not been configured and assigned to a listener. (See Network &gt; Certificates.) Enabling TLS will automatically use the "Demo" certificate/key for listeners.</i>
	SMTP Authentication: <input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
	If Both TLS and SMTP Authentication are enabled: <input type="checkbox"/> Require TLS To Offer SMTP Authentication
	<input type="checkbox"/> Verify Client Certificate
Domain Key/DMARC Signing:	<input type="radio"/> On <input checked="" type="radio"/> Off
DKIM Verification:	<input type="radio"/> On <input checked="" type="radio"/> Off
	Use DKIM Verification Profile: DEFAULT
SPI/SIDF Verification:	<input type="radio"/> On <input checked="" type="radio"/> Off
	Conformance Level: SIDP Compatible
	Downgrade PRA verification result if 'Resent-From:' or 'Resent-From:' were used: <input type="radio"/> No <input type="radio"/> Yes
	HELO Test: <input type="radio"/> Off <input checked="" type="radio"/> On
DMARC Verification:	<input type="radio"/> On <input checked="" type="radio"/> Off
	Use DMARC Verification Profile: DEFAULT
	DMARC Feedback Reports: <input type="checkbox"/> <i>* DMARC reporting message must be DMARC compliant.            * Recommended: Enable TLS encryption for domains that will receive reports. Go to Mail Policies &gt; Destination Controls.</i>
	<input type="checkbox"/> Send aggregate feedback reports
Bounce Verification:	Consider Untagged Bounces to be Valid: <input checked="" type="radio"/> Yes <input type="radio"/> No <i>(Applies only if bounce verification address tagging is in use. See Mail Policies &gt; Bounce Verification.)</i>

附註：無法配置入站郵件可能導致ESA丟棄郵件的有效退回郵件。

注意：要驗證是否已為此域禁用退回驗證，您可以啟用「域調試日誌」並跟蹤日誌以進行驗證。

## 相關資訊

- [Cisco Email Security Appliance — 最終使用手冊](#)
- [技術支援與文件 - Cisco Systems](#)