

# Los IP Addresses/los dominios/las direcciones de correo electrónico exentos del ESA despiden la configuración

## Contenido

[Introducción](#)

[Los IP Addresses/los dominios/las direcciones de correo electrónico exentos del ESA despiden la configuración](#)

[Correo saliente](#)

[Correo entrante](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo configurar entrante y el correo saliente para eximir los IP Addresses, los dominios, o las direcciones de correo electrónico para Cisco envía por correo electrónico el dispositivo de seguridad (ESA).

## Los IP Addresses/los dominios/las direcciones de correo electrónico exentos del ESA despiden la configuración

Usted puede especificar los dominios receptores en los cuales inhabilitar la verificación de la despedida cuando el ESA entrega a esos dominios. Usted necesitará configurar el correo saliente y entrante.

## Correo saliente

1. Vaya a las directivas del correo > a los controles del destino.
2. Selecto "agregue el destino...".
3. Llame el nuevo destino "example.com".
4. En las configuraciones, fije la "verificación de la despedida" a no.
5. Someta y confíe los cambios.

Destination Controls	
Destination:	<input type="text" value="example.com"/>
IP Address Preference:	<input type="text" value="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:	<input type="text" value="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:	<input type="text" value="Default"/>  <i>Bounce Profile can be configured at Network &gt; Bounce Profiles.</i>

Nota: Para el correo saliente, usted puede referir solamente al dominio del destino y no a una dirección IP o a una dirección de correo electrónico.

## Correo entrante

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> <input type="checkbox"/> Verify Client Certificate
	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
	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: <input type="text" value="DEFAULT"/>
SPF/SIDF Verification:	<input type="radio"/> On <input checked="" type="radio"/> Off
	Conformance Level: <input type="text" value="SIDF Compatible"/>
	Downgrade PRA verification result if 'resent-sender:' 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: <input type="text" value="DEFAULT"/>
	DMARC Feedback Reports: <input type="checkbox"/> Send aggregate feedback reports <small>* DMARC reporting message must be DMARC compliant.            * Recommended: Enable TLS encryption for domains that will receive reports. Go to Mail Policies &gt; Destination Controls.</small>
Bounce Verification:	Consider Unlagged Bounces to be Valid: <input checked="" type="radio"/> Yes <input type="radio"/> No <small>(Applies only if bounce verification address tagging is in use. See Mail Policies &gt; Bounce Verification.)</small>

Notas: El error configurar su correo entrante puede hacer su ESA caer los mensajes de despedida válidos para los mensajes.

Notas: Para verificar que la verificación de la despedida esté inhabilitada para este dominio, usted puede habilitar "los registros del debug del dominio" y atar los registros para verificar.

## Información Relacionada

- [Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)