

¿Por qué la verificación SPF falla para las contestaciones a los mensajes encriptados o para los correos electrónicos enviados directamente dentro de los CRE?

Contenido

[Introducción](#)

[¿Por qué la verificación SPF falla para las contestaciones a los mensajes encriptados o para los correos electrónicos enviados directamente dentro de los CRE?](#)

Introducción

Este documento describe cómo configurar el expediente del Marco de políticas del remitente (SPF) para los mensajes del servicio del sobre registrado de Cisco (CRE).

¿Por qué la verificación SPF falla para las contestaciones a los mensajes encriptados o para los correos electrónicos enviados directamente dentro de los CRE?

Para los correos electrónicos enviados de los CRE (asegure la contestación o seguro componga los correos electrónicos), la verificación SPF falla en el extremo receptor. La razón es porque es seguro componga y asegure las contestaciones se generan y los servidores dominantes recibidos de los entregados. La dirección IP saliente no hará juego los IP Addresses mencionados en el extremo de los beneficiarios. Para solucionar este problema, agregue esta declaración al expediente SPF de su dominio:

```
include:res.cisco.com
```