

¿Por qué falla la verificación SPF para las respuestas a los mensajes cifrados o para los correos electrónicos enviados directamente desde CRES WebSafe?

Contenido

[Introducción](#)

[¿Por qué falla la verificación SPF para las respuestas a los mensajes cifrados o para los correos electrónicos enviados directamente desde CRES WebSafe?](#)

Introducción

Este documento describe cómo configurar el registro de la estructura de políticas de remitente (SPF) para los mensajes del servicio Cisco Registered Envelope Service (CRES).

¿Por qué falla la verificación SPF para las respuestas a los mensajes cifrados o para los correos electrónicos enviados directamente desde CRES WebSafe?

En el caso de los correos electrónicos enviados desde CRES (respuesta segura o mensajes de correo electrónico de redacción seguros), la verificación SPF falla en el extremo del destinatario. El motivo es que se generan y envían respuestas seguras y de composición desde los servidores de claves alojados. La dirección IP saliente no coincidirá con las direcciones IP enumeradas en el extremo de los destinatarios. Para resolver este problema, agregue esta instrucción al registro SPF de su dominio:

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