Revisión de informes de DMARC y resolución de problemas de verificación con DMP

Contenido

Introducción

Este documento describe cómo verificar los informes de DMARC procesados por DMP para comprender los veredictos de SPF y DKIM y mantener un ecosistema de correo electrónico seguro.

P. ¿Cómo funciona SPF?

R. Sender Policy Framework (SPF) permite a los propietarios de dominios especificar qué remitentes pueden enviar mensajes en nombre de su dominio.

P. ¿Cómo funciona DKIM?

R. El correo identificado por claves de dominio (DKIM) utiliza un par de claves. Una clave privada para que los remitentes autorizados agreguen una firma digital a los mensajes y una clave pública para que los receptores comprueben la autenticidad de las firmas digitales, asegurándose de que el mensaje no se modificó durante el tránsito.

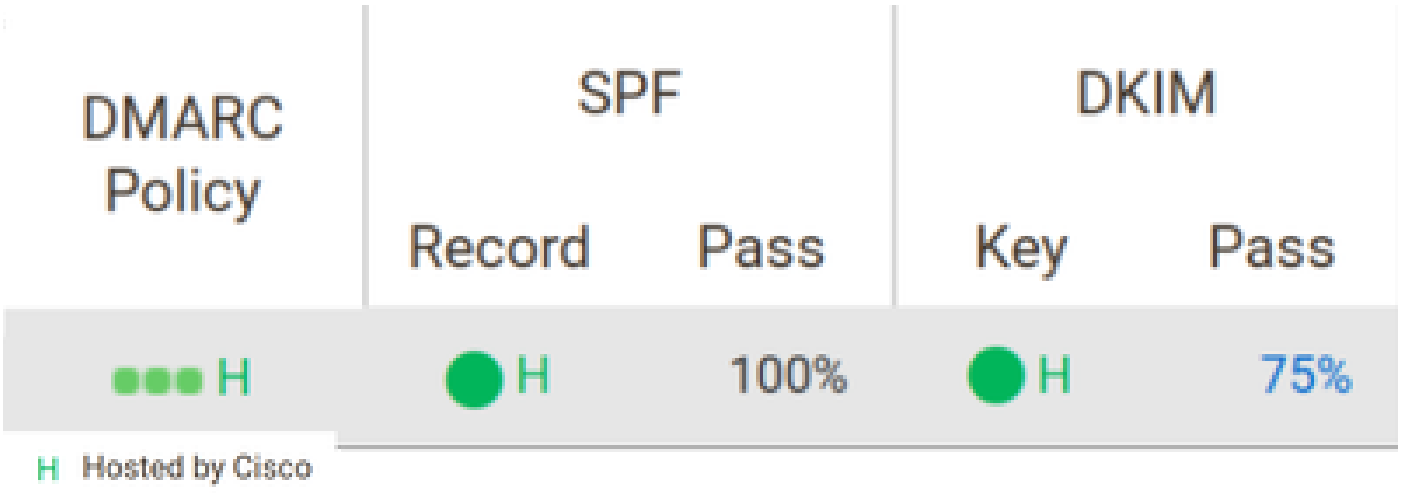
P. ¿Cómo funciona DMARC?

R. La autenticación de mensajes, informes y conformidad (DMARC) basada en dominio garantiza que todas las identidades disponibles estén alineadas con el encabezado De. Los propietarios de dominios especifican una política para los receptores sobre cómo deben gestionar los mensajes erróneos y dónde enviar los informes de comentarios, lo que facilita la identificación de errores o campañas de suplantación de identidad.

P. ¿Cómo puedo configurar la autenticación de correo electrónico con DMP?

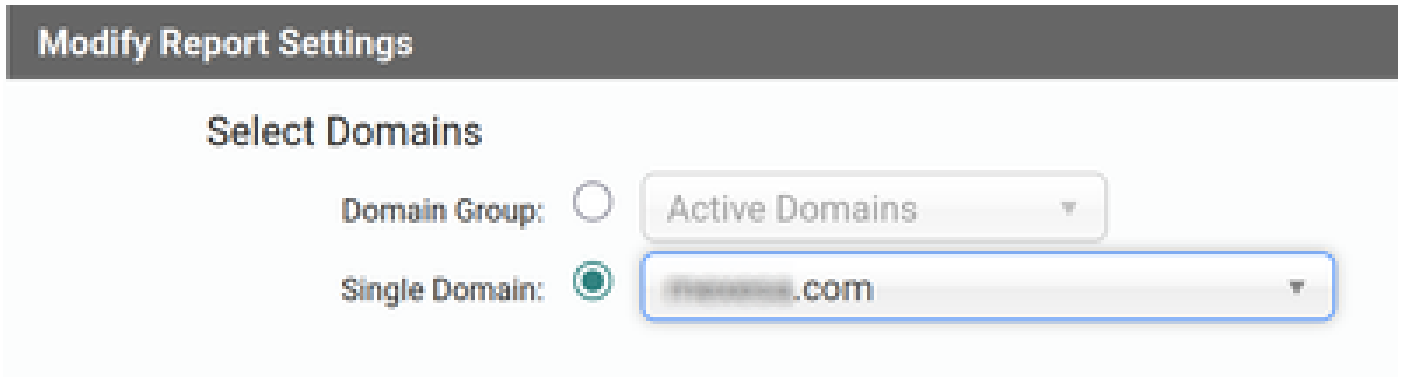
R. Cisco Domain Protection (DMP) puede gestionar y alojar sus registros SPF, DKIM y DMARC. Requiere que publique registros DNS TXT en sus dominios para delegar la administración en DMP. Una vez que DMP aloje sus registros, podrá gestionar remitentes aprobados, claves de firma DKIM y su política de DMARC a través del portal de administración de DMP.

Haga clic en la barra Configuration Completed en el Panel de DMP para verificar el estado de su dominio.



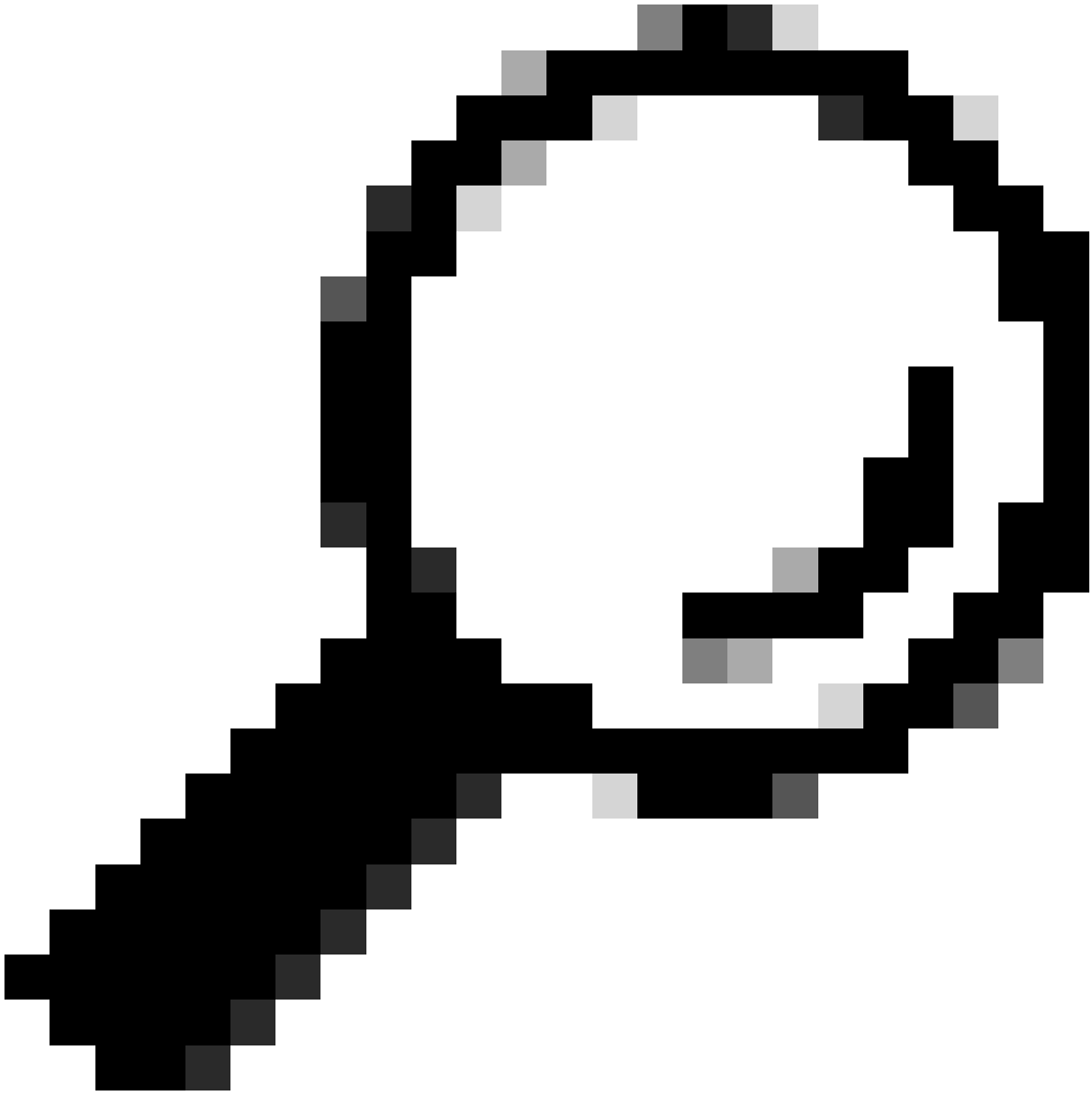
P. DMP aloja mi registro SPF, registro DKIM y política DMARC. ¿Cómo puedo detectar errores o actividad maliciosa?

R. Puede diagnosticar errores y actividades malintencionadas a través del portal del administrador de DMP. Navegue hasta Analizar > Tráfico de correo electrónico. Haga clic en el botón Modificar configuración. Seleccione Single Domain y elija un dominio en el menú desplegable.



En la sección Cosas que puedo solucionar, seleccione el informe ¿Cuáles son mis problemas de SPF? o ¿Cuáles son mis problemas de DKIM? .

Pase el ratón sobre una sección del gráfico para obtener una explicación del problema correspondiente o haga clic en una sección para obtener detalles.



Consejo: Seleccione un rango de datos más largo en Modificar configuración del informe para tener un estado preciso de su ecosistema de correo electrónico. Puede encontrar remitentes válidos en su dominio que no conoce o que aún no firman mensajes.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).