Revisar relatórios de DMARC e resolver problemas de verificação com DMP

Contents

Introdução

Este documento descreve como verificar os relatórios DMARC processados pelo DMP para entender os vereditos de SPF e DKIM e manter um ecossistema de e-mail seguro.

P. Como o SPF funciona?

R. A Sender Policy Framework (SPF) permite que os proprietários do domínio especifiquem quais remetentes podem enviar mensagens em nome do seu domínio.

P. Como funciona o DKIM?

R. O DKIM (Domain Keys Identified Mail) usa um par de chaves. Uma chave privada para que os remetentes autorizados adicionem uma assinatura digital às mensagens e uma chave pública para que os receptores verifiquem a autenticidade das assinaturas digitais, garantindo que a mensagem não seja modificada em trânsito.

P. Como o DMARC funciona?

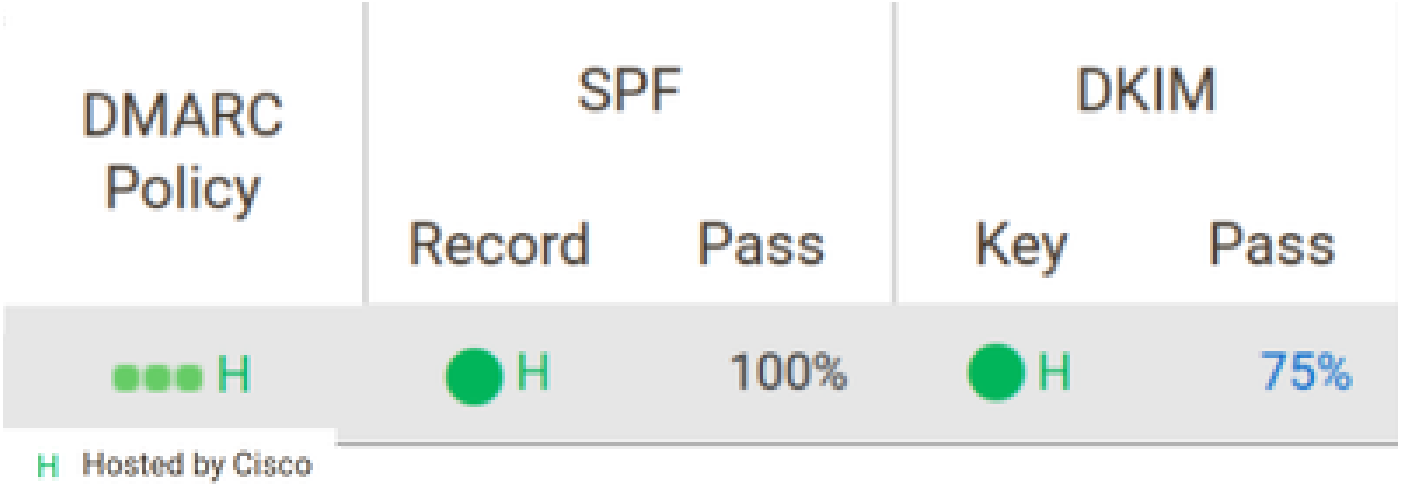
R. O DMARC (Domain-based Message Authentication, Reporting, and Conformance) garante que todas as identidades disponíveis sejam alinhadas com o cabeçalho De. Os proprietários de domínio especificam uma política para os receptores sobre como eles devem lidar com as mensagens com falha e para onde enviar os relatórios de feedback, facilitando a identificação de erros ou campanhas de phishing.

P. Como posso configurar a autenticação de e-mail com o DMP?

R. O Cisco Domain Protection (DMP) pode gerenciar e hospedar seus registros SPF, DKIM e DMARC. Ele exige que você publique registros TXT DNS em seus domínios para delegar a

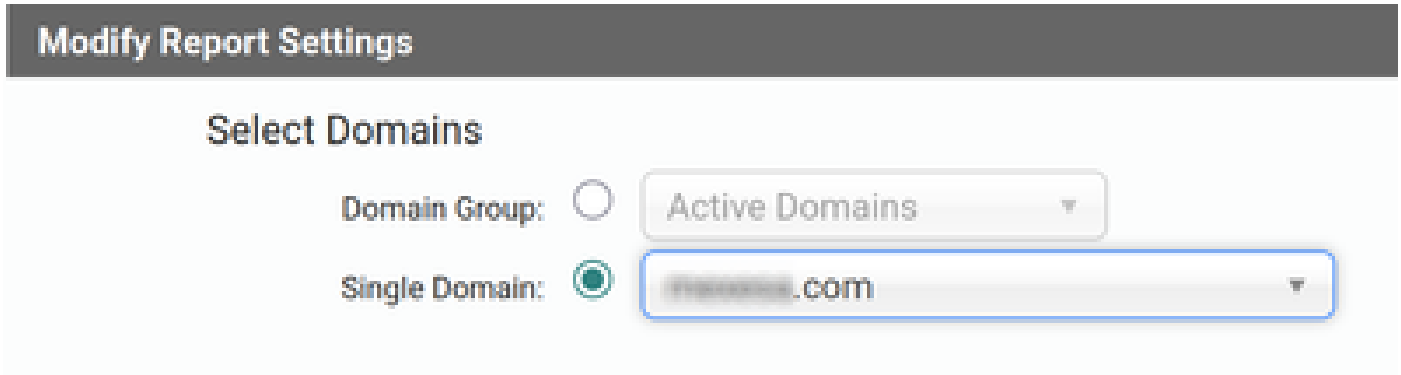
administração ao DMP. Depois que o DMP hospedar seus registros, você poderá gerenciar os remetentes aprovados, as chaves de assinatura DKIM e sua política DMARC por meio do portal de administração do DMP.

Clique na barra Configuração concluída no Painel do DMP para verificar o status do seu domínio.



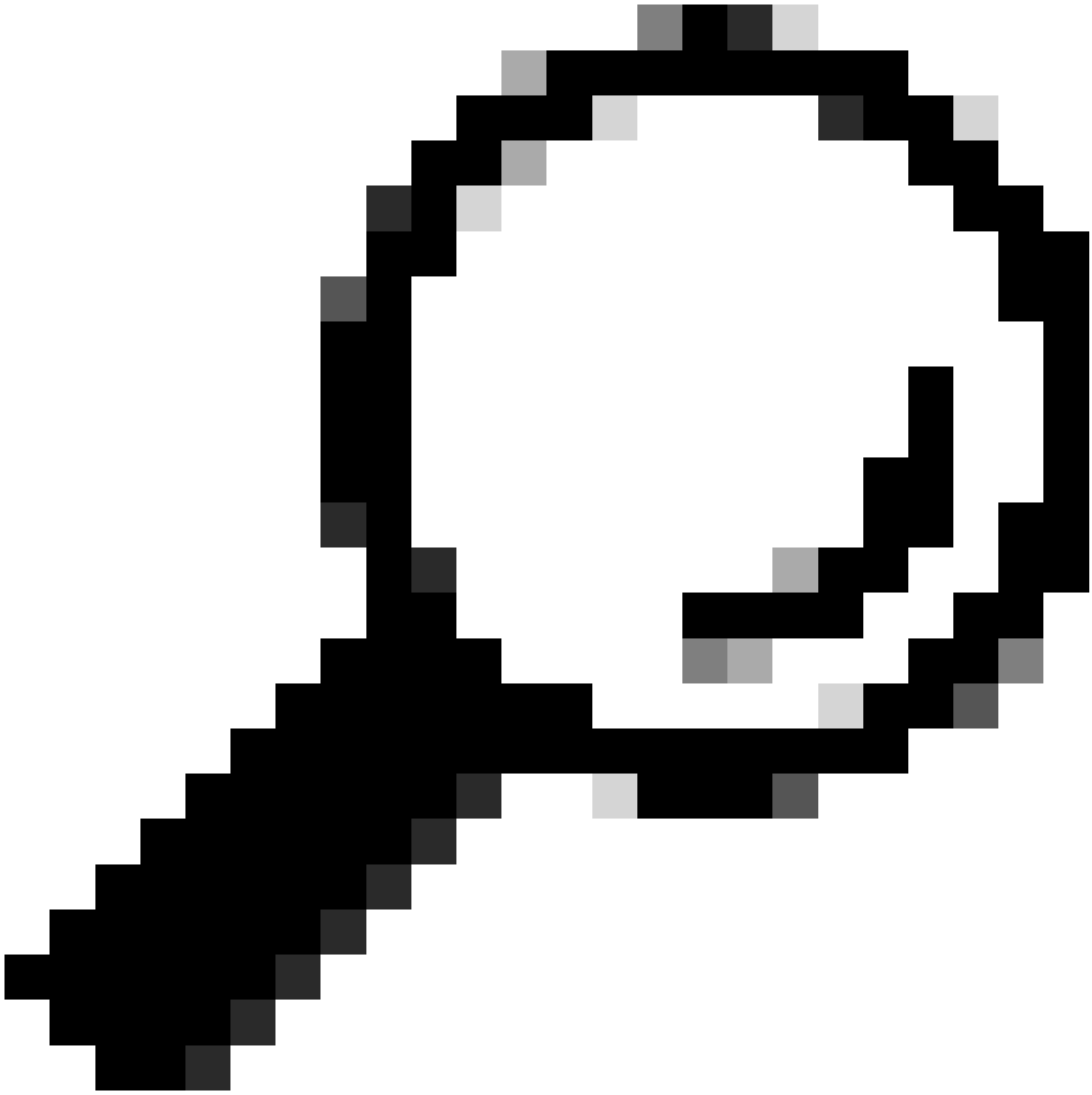
P. O DMP hospeda meu registro SPF, registro DKIM e política DMARC. Como posso detectar erros ou atividades mal-intencionadas?

R. Você pode diagnosticar erros e atividades mal-intencionadas por meio do portal do administrador do DMP. Navegue para Analisar > Tráfego de e-mail. Clique no botão Modificar configurações. Selecione Domínio único e escolha um domínio no menu suspenso.



Na seção Coisas que posso corrigir, selecione o relatório Quais são meus problemas de SPF? ou Quais são meus problemas de DKIM? .

Passe o mouse sobre uma seção de gráfico para obter uma explicação do problema correspondente ou clique em em uma seção para fazer o drill-down dos detalhes.



Tip: Selecione um Intervalo de dados maior em Modificar configurações do relatório para ter um status preciso do seu ecossistema de email. Você pode encontrar remetentes válidos em seu domínio dos quais não está ciente ou que ainda não estão assinando mensagens.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.