Überprüfung von DMARC-Berichten und Behebung von Verifizierungsproblemen mit DMP

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die von DMP verarbeiteten DMARC-Berichte überprüft werden, um SPF- und DKIM-Urteile zu verstehen und ein sicheres E-Mail-System zu gewährleisten.

F. Wie wirkt die SPF?

A. Mit dem Sender Policy Framework (SPF) können Domäneninhaber festlegen, welche Absender Nachrichten für Ihre Domäne senden dürfen.

F. Wie wirkt DKIM?

A. DKIM (Domain Keys Identified Mail) verwendet ein Schlüsselpaar. Ein privater Schlüssel für autorisierte Absender, um Nachrichten eine digitale Signatur hinzuzufügen, und ein öffentlicher Schlüssel für Empfänger, um die Authentizität der digitalen Signaturen zu überprüfen und sicherzustellen, dass die Nachricht während der Übertragung nicht geändert wurde.

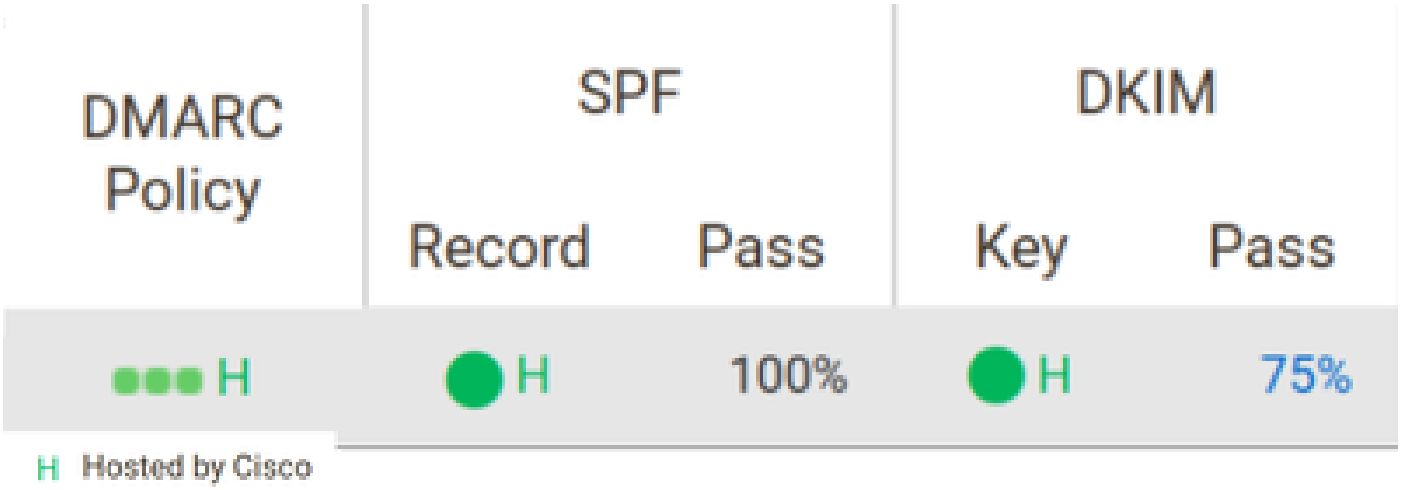
F. Wie wirkt DMARC?

A. Domain-based Message Authentication, Reporting and Conformance (DMARC) stellt sicher, dass alle verfügbaren Identitäten mit dem Von-Header ausgerichtet sind. Domäneninhaber legen eine Richtlinie für Empfänger fest, die regelt, wie sie mit fehlerhaften Nachrichten umgehen müssen und wohin Feedback-Berichte gesendet werden sollen. So können Fehler oder Phishing-Kampagnen leichter identifiziert werden.

Frage: Wie kann ich die E-Mail-Authentifizierung mit DMP einrichten?

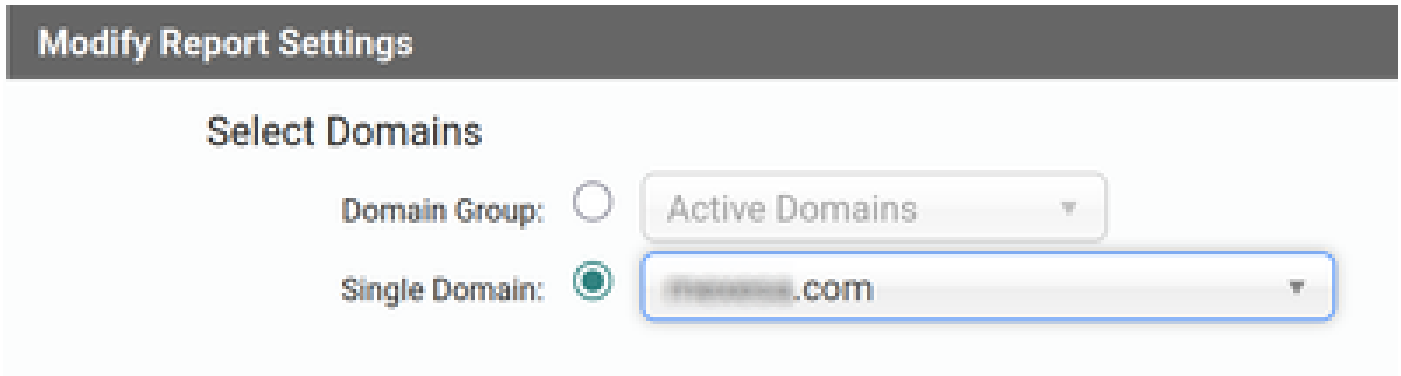
A.: Cisco Domain Protection (DMP) kann Ihre SPF-, DKIM- und DMARC-Datensätze verwalten und hosten. Sie müssen DNS TXT-Einträge in Ihren Domänen veröffentlichen, um die Administration an DMP zu delegieren. Sobald DMP Ihre Datensätze hostet, können Sie genehmigte Absender, DKIM-Signaturschlüssel und Ihre DMARC-Richtlinie über das DMP-Administrationsportal verwalten.

Klicken Sie auf die Leiste Konfiguration abgeschlossen im DMP Dashboard, um Ihren Domänenstatus zu überprüfen.



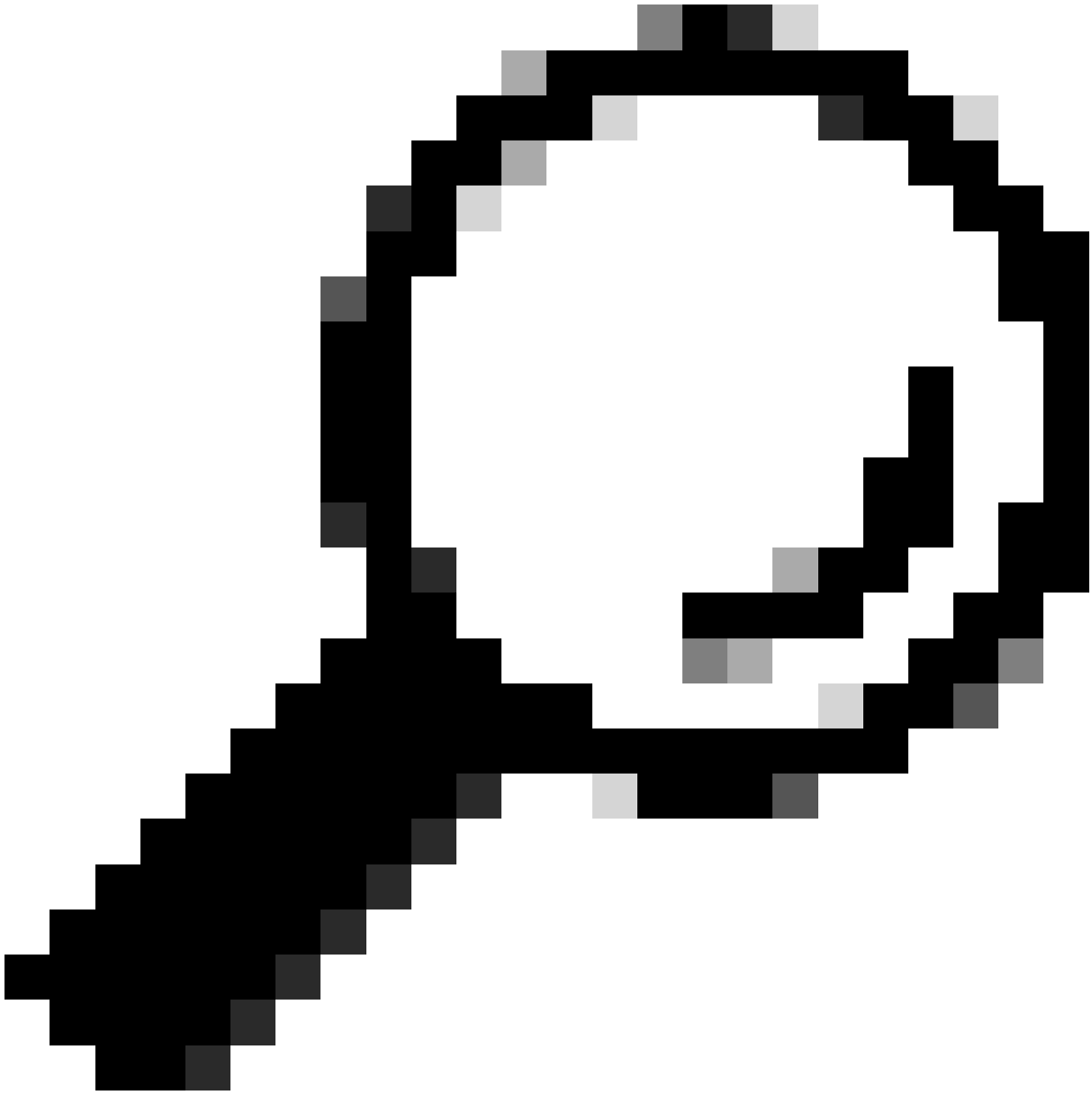
Frage: DMP hostet meinen SPF-Datensatz, DKIM-Datensatz und die DMARC-Richtlinie. Wie kann ich Fehler oder schädliche Aktivitäten erkennen?

A. Sie können Fehler und schädliche Aktivitäten über das DMP-Administratorportal diagnostizieren. Navigieren Sie zu Analysieren > E-Mail-Verkehr. Klicken Sie auf die Schaltfläche Einstellungen ändern. Wählen Sie Single Domain (Einzeldomäne) aus, und wählen Sie eine Domäne aus dem Dropdown-Menü aus.



Wählen Sie im Abschnitt "Dinge, die ich reparieren kann" den Bericht Was sind meine SPF-Probleme? oder Was sind meine DKIM-Probleme? aus.

Bewegen Sie den Mauszeiger über einen Diagrammabschnitt, um das entsprechende Problem zu erklären, oder klicken Sie auf einen Abschnitt, um die Details anzuzeigen.



Tipp: Wählen Sie einen längeren Datenbereich unter Berichtseinstellungen ändern aus, um einen genauen Status Ihres E-Mail-Systems zu erhalten. Sie können gültige Absender in Ihrer Domäne finden, die Ihnen noch nicht bekannt sind oder die noch keine Nachrichten signieren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.