التحقق من عمل DKIM

المحتويات

المقدمة

يوضح هذا المستند كيفية التحقق من عمل DKIM.

التحقق

على جهاز أمان البريد الإلكتروني (ESA) من Cisco، تعتبر أسهل طريقة للتحقق من عمل DKIM هي إرسال بريد إلكتروني إلى حساب خارجي والتحقق من الرؤوس. في المثال التالي، تم إرسال رسالة إلى حساب @gmail.com:

```
Delivered-To: user@gmail.com
<Return-Path: <bob@example.com
Received-SPF: pass (google.com: domain of bob@example.com
(designates <IP Address> as permitted sender
;<client-ip=<IP Address
Authentication-Results: mx.google.com; spf=pass
google.com: domain of bob@example.com designates)
;IP Address> as permitted sender) smtp.mail=bob@example.com>
dkim=pass (test mode) header.i=bob@example.com
```

يجب أن ترى dkim=pass في سطر Authentication-Results.

ملاحظة: يرجى الانتباه إلى أن بعض العملاء مثل Yahoo يميلون إلى تجريد العديد من الرؤوس. الرجاء التحقق من هذا على عدة عملاء للتأكد من أنه يعمل.

يمكنك أيضا الرجوع إلى بعض هذه المصادر الخارجية للتحقق من التكوين الخاص بك:

http://www.kitterman.com/spf/validate.html

dkim-test@testing.dkim.org

هناك العديد من العاكسات الأخرى متاحة أيضا:

التحقق حاليا مع RFC4871:
المنفذ 25: check-auth@verifier.port25.com

يتم حاليا التحقق من كل من RFC4871 (و RFC4870):
Alt-N: dkim-test@altn.com

يتم حاليا التحقق من كل من RFC4871 (و RFC4870):
Sendmail: sa-test@sendmail.net

يتم حاليا التحقق من كل من draft all-00 و all-01:
Elandsys: autorespond+dkim@dk.elandsys.com

يتم حاليا التحقق من كل من RFC4871 (و RFC4870) :
البلاك أوبس: dktest@blackops.org

معلومات ذات صلة

- جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).