

Controleer of DKIM werkt

Inhoud

[Inleiding](#)

[Verificatie](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u kunt controleren of DKIM werkt.

Verificatie

Op de Cisco e-mail security applicatie (ESA), is de eenvoudigste manier om te controleren of DKIM werkt, het verzenden van een e-mail naar een externe account en het controleren van de headers. In het onderstaande voorbeeld werd een bericht naar een @gmail.com-account verzonden:

```
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
```

U dient dkim=pass te zien in de verificatie-Resultaten lijn.

Opmerking: Houd er rekening mee dat bepaalde klanten zoals Yahoo er veel kopregels op na houden. Controleer dit bij meerdere klanten om er zeker van te zijn dat het werkt.

U kunt ook naar een aantal van deze externe bronnen verwijzen om de configuratie van het apparaat te controleren:

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

dkim-test@testing.dkim.org

Er zijn ook verschillende andere Reflectors beschikbaar:

Momenteel met RFC4871:

Port 25: check-auth@verifier.port25.com

Momenteel controleren zij zowel RFC4871 (als RFC4870):
ALT-N: dkim-test@altn.com

Momenteel controleren zij zowel RFC4871 (als RFC4870):
Sendmail: sa-test@sendmail.net

Momenteel controleren zij zowel ontwerp allman-00 als allman-01:
Elandsys: autorespond+dkim@dk.elandsys.com

Momenteel controleren zij zowel RFC4871 (als RFC4870):
Blackops: dktest@blackops.org

Gerelateerde informatie

- [Cisco e-mail security applicatie - eindgebruikershandleidingen](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)