# Verifique que DKIM trabalha

## Índice



## Introdução

Este documento descreve como verificar que DKIM trabalha.

## Verificação

Na ferramenta de segurança do email de Cisco (ESA), a maneira a mais fácil de verificar que DKIM está trabalhando é enviar um email a uma conta da parte externa e verificar os encabeçamentos.  No exemplo abaixo, uma mensagem foi enviada a uma conta @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
```

Você deve ver os dkim=pass na linha dos Autenticação-resultados.

> **Note**: Esteja por favor ciente que alguns clientes tais como Yahoo tendem a descascar muitos encabeçamentos.  Verifique por favor isto em clientes múltiplos para ter certeza que está trabalhando.

Você pode igualmente referir alguns destes origens externa para verificar sua configuração:

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

dkim-test@testing.dkim.org

Há vários refletores disponíveis também:

Atualmente verificando com RFC4871:
Porta 25: check-auth@verifier.port25.com

Atualmente verificando ambo o RFC4871 (e RFC4870):
Alternativo: dkim-test@altn.com

Atualmente verificando ambo o RFC4871 (e RFC4870):
Sendmail: sa-test@sendmail.net

Atualmente verificando o esboço allman-00 e o allman-01:
Elandsys: autorespond+dkim@dk.elandsys.com

Atualmente verificando ambo o RFC4871 (e RFC4870):
Blackops: dktest@blackops.org

## Informações Relacionadas

- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final
- Suporte Técnico e Documentação - Cisco Systems