

Review DMARC Reports and Resolve Verification Problems with DMP

Contents

[Introduction](#)

[Q. How does SPF work?](#)

[Q. How does DKIM work?](#)

[Q. How does DMARC work?](#)

[Q. How can I set up Email Authentication with DMP?](#)

[Q. DMP hosts my SPF record, DKIM record, and DMARC policy. How can I detect errors or malicious activity?](#)

Introduction

This document describes how to verify the DMARC reports processed by DMP to understand SPF and DKIM verdicts and maintain a secure email ecosystem.

Q. How does SPF work?

A. Sender Policy Framework (SPF) allows domain owners to specify which senders can send messages on behalf of your domain.

Q. How does DKIM work?

A. Domain Keys Identified Mail (DKIM) uses a key pair. A private key for authorized senders to add a digital signature to messages and a public key for receivers to verify the authenticity of the digital signatures, ensuring the message was not modified in transit.




Q. How does DMARC work?

A. Domain-based Message Authentication, Reporting, and Conformance (DMARC) ensures that all available identities are aligned with From header. Domain owners specify a policy for receivers on how they must handle failing messages and where to send feedback reports, making it easy to identify errors or phishing campaigns.

Q. How can I set up Email Authentication with DMP?

A. Cisco Domain Protection (DMP) can manage and host your SPF, DKIM and DMARC records. It requires you to publish DNS TXT records in your domains to delegate the administration to DMP. Once DMP hosts your records, you can manage approved senders, DKIM signing keys, and your DMARC policy via DMP administration portal.

Click the **Configuration Completed** bar in the **DMP Dashboard** to verify your domain status.

DMARC Policy	SPF		DKIM	
	Record	Pass	Key	Pass
 H	 H	100%	 H	75%

H Hosted by Cisco

Q. DMP hosts my SPF record, DKIM record, and DMARC policy. How can I detect errors or malicious activity?

A. You can diagnose errors and malicious activity via the DMP administrator portal. Navigate to **Analyze > Email Traffic**. Click the **Modify Settings** button. Select **Single Domain** and choose a **domain** from the drop-down menu.

Modify Report Settings

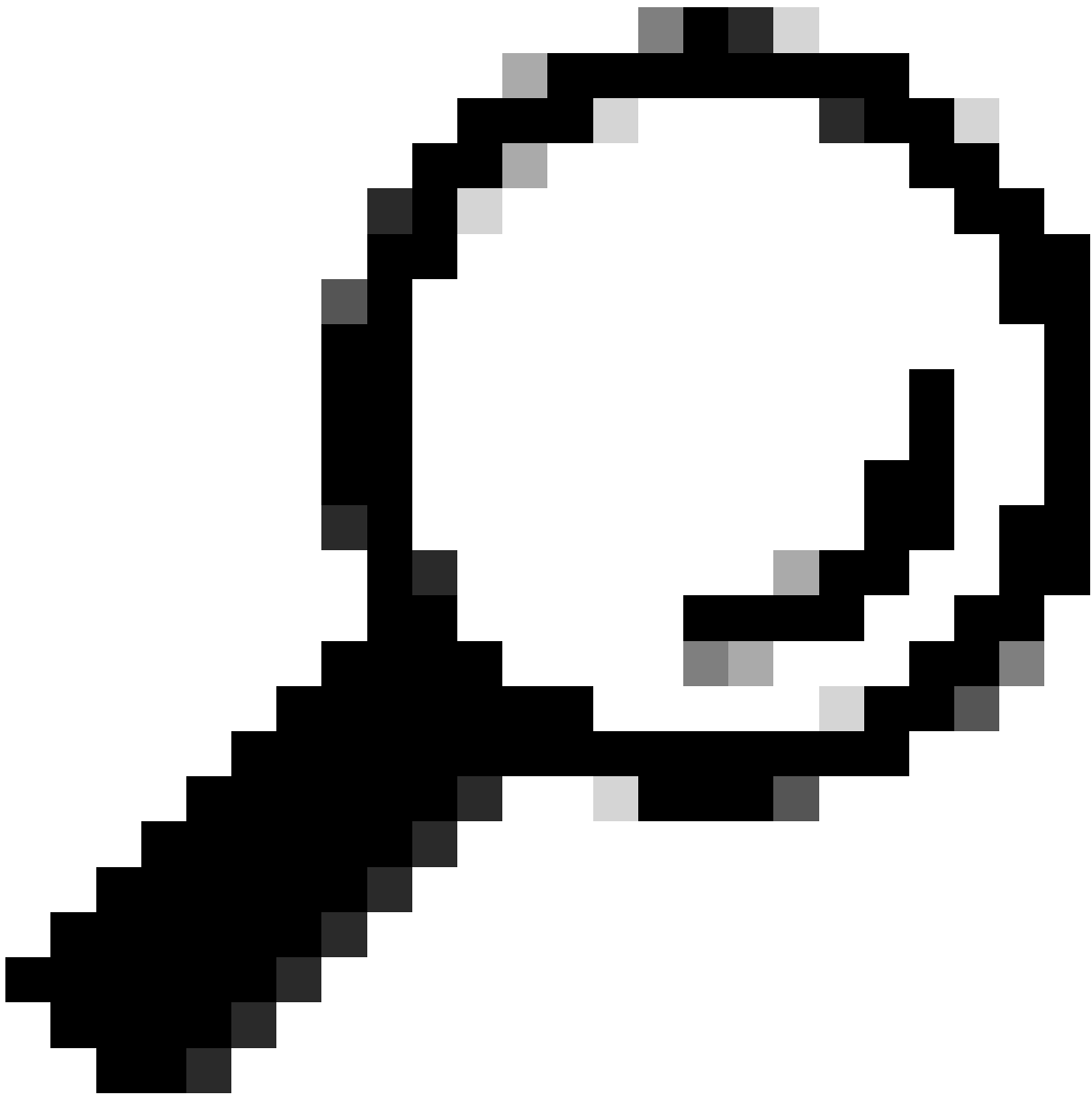
Select Domains

Domain Group: ☐ Active Domains

Single Domain: ☒

Under the **Things I Can Fix** section, select the **What are my SPF problems?** or **What are my DKIM problems?** report.

Hover over a chart section for an explanation of the corresponding problem or **click on a section** to drill down the details.



Tip: Select a longer **Data Range** in the **Modify Report Settings** to have an accurate status of your email ecosystem. You can find valid senders in your domain that you are not aware of or that are not signing messages yet.
