DMARC RUF Reporting - Forensic Reports (ruf)

The "ruf" tag in DMARC policy selection allows you to receive forensic reports via email to a specified email address.

DMARC ruf Address - ("**ruf=mailto:something@yourdomain.com**")
The "ruf" tag specifies the email address to which forensic reports should be sent. Forensic reports provide valuable valuable information about individual email messages that failed DMARC authentication, including message email headers and body.

Here is how the "ruf" tag works:

1. **Set up the ruf tag:** In your DMARC record, you specify the "ruf" tag followed by an email address where you want to receive forensic reports. This email address typically belongs to you or your organization's email administrator, or can be provided to you by a Managed DMARC Service Provider, like GlowHost.
2. **Receiving forensic reports:** When a receiving mail server encounters an email with your domain in the From address, along with a DMARC policy published for your domain, and if the email fails DMARC authentication, it may generate a forensic report based on how the email complies with your DMARC policy. These reports are then sent to the email address specified in the "ruf" tag.
3. **Contents of forensic reports:** Forensic reports provide a detailed snapshot of the email that failed DMARC authentication. They include the full message headers, body, and sometimes even the attachments, allowing you to thoroughly analyze the email and identify potential issues, such as unauthorized use of your domain, phishing attempts, or other misconfigurations.
4. **Frequency of forensic reports:** Unlike aggregate reports, which are sent periodically and in batches, forensic reports are typically sent immediately after the detection of an email that fails DMARC authentication. This ensures that you receive timely information about potentially malicious or suspicious emails.
5. **Analyzing forensic reports:** Once you start to receive forensic reports, you can analyze them to understand why a particular email failed DMARC authentication, identify any anomalies or suspicious patterns, and take appropriate actions to address the underlying issues, such as updating SPF or DKIM records, investigating potential phishing attempts, or improving email authentication practices.

An example DMARC selector containing the "ruf" tag might look something like this: "**ruf=mailto:forensic-reports@yourdomain.com**" - you would use your own email address of choice to receive these reports.

By specifying the "ruf" tag in your DMARC record, you enable the generation and delivery of forensic reports, which are crucial for investigating and mitigating potential threats to the security and integrity of your domain's email communications.

Related Topics:

- What is DMARC?
- DMARC Policy Selectors & Tags Quick Reference
- DMARC None or Ignore Policy
- DMARC Quarantine Policy
- DMARC Reject Policy
- DMARC Policy Percentages
- DMARC RUA Reporting - Aggregate Reports (rua)
- DMARC Subdomain Policy (sp)
- DMARC DKIM Alignment (adkim)
- DMARC SPF Alignment (aspf)
- What is BIMI?
- What is a VMC?
- DMARC, DKIM, SPF and BIMI Info
