DMARC RUA Reporting - Aggregate Reports (rua)

The "rua" tag in DMARC policy selection allows you to receive aggregated email reports to a specified email address.

DMARC RUA Address - ("**rua=mailto:something@yourdomain.com**")
The "rua" tag specifies the email address to which aggregate reports should be sent. Aggregated reports provide valuable information about how your domain is being used and authenticated across remote recipient email servers and contain data about email traffic, authentication results, and sending sources.

Here is how the "rua" tag works:

1. **Set up the rua tag:** In your DMARC record, you specify the "rua" tag followed by an email address where you want to receive aggregate 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 aggregated 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, it may generate an aggregate report based on how the email complies with your DMARC policy. These reports are then sent to the email address specified in the "rua" tag.
3. **Contents of aggregated reports:** Aggregate reports contain information about the volume of email sent from your domain, the percentage of messages that passed or failed DMARC authentication, sources of email traffic (including IP addresses and domains), and details about the authentication methods used (SPF, DKIM).
4. **Frequency of aggregated reports:** Aggregate reports are typically sent on a regular basis, usually daily or at a frequency specified by the sender of the report. However, the actual frequency of reports may vary depending on the receiving mail server's configuration and the volume of email traffic from your domain.
5. **Analyzing aggregated reports:** Once you start to receive aggregated reports, you can analyze them to gain insights into your domain's email authentication status, identify sources of email traffic, detect potential abuse or spoofing attempts, and troubleshoot any authentication issues.

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

By specifying the "rua" tag in your DMARC record, you enable the generation and delivery of aggregate reports, which are essential for monitoring and improving 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 RUF Reporting - Forensic Reports (ruf)
- 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

Don't have the time or energy to learn, setup, monitor and maintain DMARC? What if you had a team of DMARC experts to do this for you?

Let us do DMARC for you. Check out Managed DMARC Services by GlowHost.