interweb

Generated on 25/10/2026 11:42

KNOWLEDGE BASE · PUBLIC DOCUMENT

Creating your DMARC record, and reading what it sends back

E-mail

CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-748	v2026.10.21	Mozambique · English

Interweb Mozambique
RLX Holdings, S.A. · Group RLX Holdings
Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

https://www.meu.interweb.co.mz/knowledgebase/748

Creating your DMARC record, and reading what it sends back

E-mail Created on **September 27, 2026** Updated on **October 21, 2026** 5 min read



DMARC does two things at once, and it is the second one almost nobody uses. First: it tells receivers what to do with a message that fails SPF and DKIM. Second: it **asks for reports**, and starts showing you who is sending e-mail in your domain's name, including whoever should not be.

The why is written elsewhere: **SPF, DKIM and DMARC**. This is about creating the record and understanding what comes back.

> **Do not start here.**
> A strict DMARC policy before SPF and DKIM are right rejects **your own** mail: the invoices, the site contact form, the campaigns. Check the other two first with the cPanel tool: **creating your SPF record, step by step**.

The deliverability tool does not handle DMARC

Worth knowing before you go looking for it there. The **Email Deliverability** page checks and repairs **DKIM** and **SPF**, and states in writing that it **does not repair DMARC records**. DMARC is created in the zone editor, which is the next section.

Creating the record in the zone editor

The good news is that you do not have to write the line by hand. The zone editor carries **DMARC as a record type of its own**, with a form that assembles the text for you.

1. Open cPanel from My Interweb, go to **Zone Editor** and click **Manage** next to the domain.
2. **Add Record**, and in the list of types choose **DMARC**.

3. The name is filled in for you as `_dmarc` on your domain. Leave it alone: the name has to be exactly that.

4. Fill in the form using the table below. Always start with the gentlest policy.

5. Save with **Save Record**. The panel stores the line as a TXT record, which is what DMARC is underneath.

The form also has a **Raw** tab showing the whole line as text. Use it to check what the fields produced, or to paste in a line somebody handed you already written.

The fields, and what to start them at

Field	What it does, and where to start
Policy	What to do with a message that fails. **None** watches and changes nothing, **Quarantine** sends it to spam, **Reject** refuses it. **Start at None.**
Subdomain Policy	The same, for subdomains. Useful once the main domain is tightened and a subdomain is not yet.
Percentage	How much of your mail the policy applies to. It is there so you can tighten gradually instead of all at once.
DKIM Mode / SPF Mode	**Alignment**: *Relaxed* accepts a verified domain from the same family as the sender, *Strict* demands exactly the same one. Start at *Relaxed*.
Send Aggregate Mail Reports To	**The field that makes DMARC worth having.** One or more `mailto:` addresses, comma-separated, where the reports go.
Send Failure Reports To	Where notices about individual failed messages go. Not every receiver sends them.
Generate Failure Reports When	Whether a notice goes out when *any* check fails, or only when *all* of them do.
Report Format	The format of the reports. Leave it as it comes.
Report Interval	How often you want them, in seconds. Leave it as it comes, which is once a day.

With no address in *Send Aggregate Mail Reports To*, DMARC is blind.
A `none` policy with no reporting does nothing and tells you nothing: it is there, and it might as well not be.

Send the reports to a separate mailbox
, not the address you live in. They are machine mail, they come from many places, and they come every day.

Reading what comes back

Reports arrive as e-mail with a compressed attachment, one from each large receiver that handled your mail. Inside is an XML file, and it always answers the same questions:

What the report tells you	What you do about it
Which IP addresses sent mail carrying your domain	Go down the list. You should recognise all of them. The first report usually turns up one or two services you had forgotten.
How many messages came from each	That gives you the scale. An unknown IP with one message is noise; with thousands, it is a problem.
Whether they passed SPF and DKIM	A service of yours failing SPF is missing from your list: add it. See **creating your SPF record**.
Whether the verified domain aligns with the sender	This is the part that catches everyone: passing SPF is not enough if the domain that was verified is not the one in the From address. That is what the *Mode* fields control.

Read by eye, the XML becomes unreadable as soon as the volume grows. With a few reports a day you can open them and read them. With many, the normal route is a service that receives them and turns them into tables.

From watching to refusing, without breaking anything

1. **Policy None, with reporting on.** It changes nothing for anybody, and it starts showing you reality.
2. **Let it collect.** Wait until the reports have covered a full cycle of your business: the monthly invoicing, the campaign, the contact form.
3. **Fix what fails.** Every legitimate service showing up as failing either goes into your SPF, or gets a DKIM key of its own from that service.

4 **Move to Quarantine**, and use *Percentage* if you want to start with part of the mail. Keep reading the reports.

5 **Only at the end, Reject.** From then on, anyone sending in your name is refused. And so is any service of yours you left out.

! **Refused mail does not come back with a useful warning.**
On your side the message looks sent. On the other side it never existed. That is why you climb this one step at a time instead of jumping.

NEED A HAND?

Want to start on DMARC without risk? We will tell you the line to publish and help you read the first report.

Open a support ticket →

SEE ALSO

- **Professional e-mail** →
- **Frequently asked questions** →
- **Support Policy** →

interweb

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-MZ-KB-748 · v2026.10.21 · Generated on 25/10/2026 11:42