ONDMARC by RED SIFT

Your free trial guide

A comprehensive breakdown of the key tasks you should complete during your OnDMARC trial.

Welcome to OnDMARC!

This guide will help you get started so you get the most out of your free, unrestricted trial. We know your great initiative got you here and it's our simple, easy-to-use tools that will guide you through implementing what's missing and **demonstrating success in clear reports by the end of your 14-day trial!**

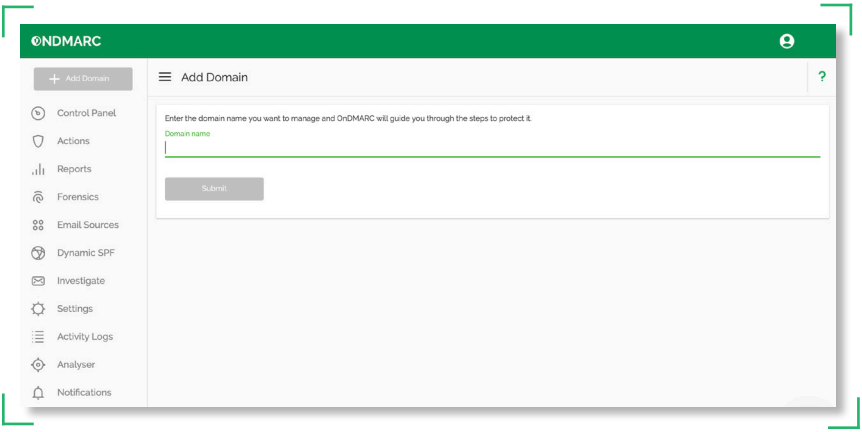
Here's what you'll need to get started

- ✓ At least one domain under your management that you want to secure
- ✓ Access to your domain's DNS
- ✓ A cup of tea to sit back with and look at the big picture of your email landscape
- ✓ An idea of the email services your organization use
- ✓ Another cup of tea to fuel you as you follow simple set-up instructions

1 Sign up and plug us in!

Add the domains you want to protect

Click '*+Add Domain*" in the left panel, then '*submit*' all the domains you manage one by one.



Update Your DNS

Once you have added all the domains you want to manage, you'll be given a unique DMARC record to enter into your DNS, this DMARC record will be the same for all the domains you add. You can see here that the policy is set to "*p=none*" meaning that you're in reporting only mode, for now you're simply plugging OnDMARC into your domain so we can start analyzing and interpreting your email activity.

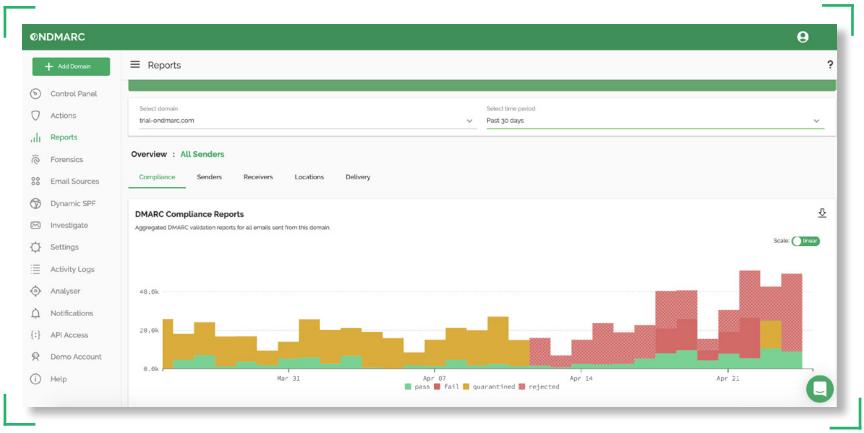
2 Get full visibility of your email landscape

See the big picture

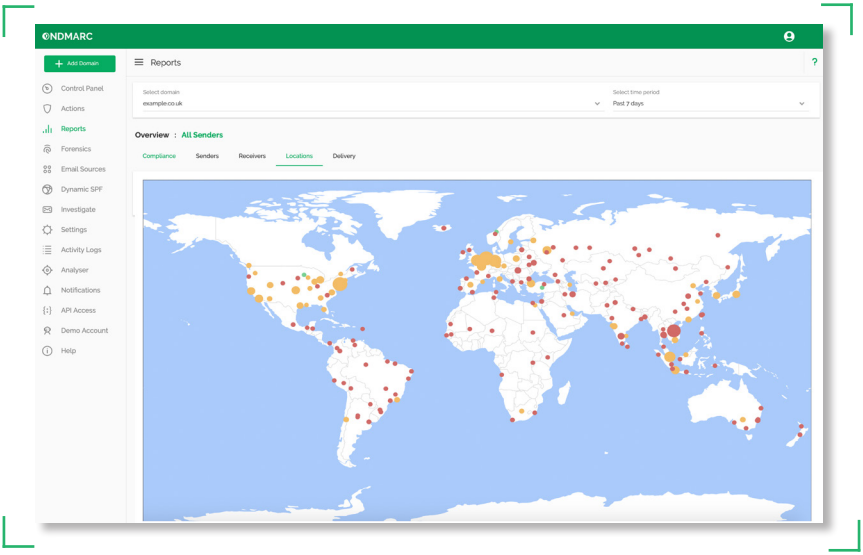
After 24 hours your first DMARC reports will be in.

In the left panel, select **Reports** to see what's going on across your domains. Being able to provide your organization with a clear view of exactly what's going on across their entire email landscape is already an early win on your part.

The first view you'll see is **Compliance** which highlights how the emails sent from your domain presently pass or fail the security protocols SPF and DKIM.



Another perspective you must see during the trial is **Locations** for an impressive (and hopefully not too worrying) global map of who is using your domain with or without authorization. See an example below:



Wait, there's more to see!

Here's a quick rundown of the other report types that make up our comprehensive visuals:

- **Senders** - All sources that have sent email using your domain and the percentages of emails that pass or fail authentication. Why not click one of interest and dive deeper into why the email failed for a full breakdown.
- **Receivers** - Check out the top 5 mail providers your recipients use or download the full list.
- **Delivery** - The overall delivery per day to help you understand email deliverability.

As a new user at the beginning of your DMARC journey, it's great to suddenly have full visibility of your email landscape, but sometimes it can feel overwhelming when the results show unauthorized activity happening! Don't fret, we'll guide you through each step you need to take to remediate these threats so you can confidently address block email impersonation based phishing attacks. So let's keep going...

3 Ready to see your expert sidekick in action?

Part 1. Take a look at your to-do list

As your expert DMARC guide, we'll tell you where to start, what there is to do and how to do it.

First, click on the **Actions** tab in the left panel to get a crystal clear list view of the work to be done. To produce this, OnDMARC reviewed the reports you've just checked out in Step 2 and identified missing security protocols for you! Additionally, we've provided all the necessary instructions to quickly and confidently configure them - You're welcome! ☺

Part 2. Mark the email providers you recognize

It's simple, just tell us whether or not you recognize each email source from the list we've generated. You do this by marking each one as a *Threat* or an *Asset*. Let's quickly define these:

Asset - This is an email source you recognize and trust, all that's left to do is make sure it's properly configured for DMARC.

Threat - This is an email source you do not recognize and want to mark as unauthorized.

Seen something you're unsure of? You can dive deeper into an individual source simply by clicking it and we'll give you further information to help inform your classification.

Part 3. Configure with confidence

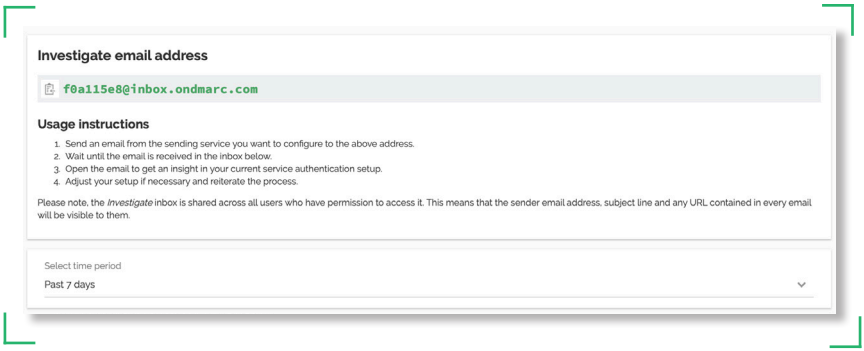
As promised, OnDMARC has carefully written helpful step-by-step instructions to quickly and confidently configure the security protocols for each email source. But first, you'll need to switch back to **Actions** and select **Senders** for a full list of outstanding **Email Sources** and their configuration instructions.

For well-known sources like G Suite, we'll actually auto-populate the SPF part and the DKIM selector. For lesser-known sources, instructions will appear in your **Actions** tab with set up instructions for each one.

Part 4. Take a quick checkup

Before OnDMARC making changes to your DNS would typically take up to 24 hours to surface in an updated report. Well, now you can see if the changes you made in the steps above had the desired effect in a matter of seconds.

Go to **Investigate** to find your unique inbox and send a 'test' email to display the results for all modern security protocols: DMARC, SPF, DKIM, FCrDNS, and TLS. Here's how it looks:



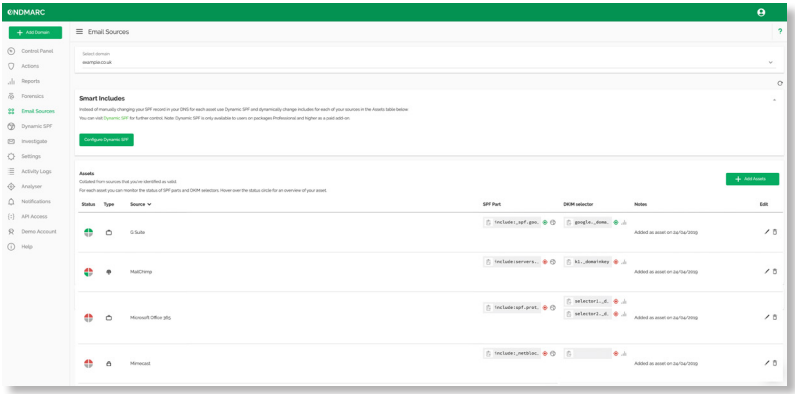
To learn more about FCrDNS and TLS simply look them up in the Help Centre by going to **Help** in the left navigation panel.

If you really want to show off and you're happy with what you've done so far, why not compare these results to a security protocol standard as a standardized target to aim for. Whilst in **Investigate** you can compare your email security against four different profiles: *UK Minimum Security Standards, US Binding Operational Directive 18:01, OnDMARC Default, or OnDMARC Deliverability.*

4 Now you're on a roll, here's how to stay on track

Part 1 - How compliant are your email Assets?

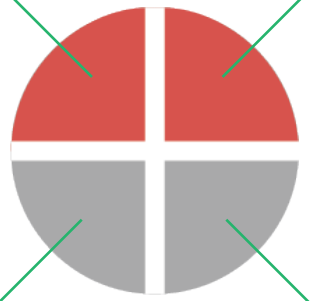
Here's how you can see the full effect of your actions when configuring the different security protocols for an email source. Go to **Email Sources** in the left panel to launch an overview of all sources you've marked as Assets in the previous steps. See an example below:



This offers you more insight into the status of each individual source with a clear 4 part wheel. This icon gives you an instant overview of whether a source is DMARC compliant or not. Here's what they represent:

If you have the correct SPF in your DNS.

If you have the correct DKIM in your DNS.



If we have seen traffic to confirm SPF is passing.

If we have seen traffic to confirm DKIM is passing.

Ideally, you want to see all green quadrants but here's a quick breakdown by color:

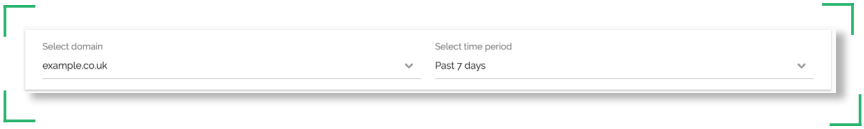
Grey - Nothing to worry about, we just haven't seen any traffic yet.
Red - This is a failure so you'll want to work on this until it's green.
Green - Nice work, this is a pass!

Once you have spent time going through the process of authorizing ALL your email sources so they have 4 green quadrants and you have gone 7 days with no failures for authorized traffic, then you are ready for full DMARC protection.

5 Let's see what you've accomplished so far

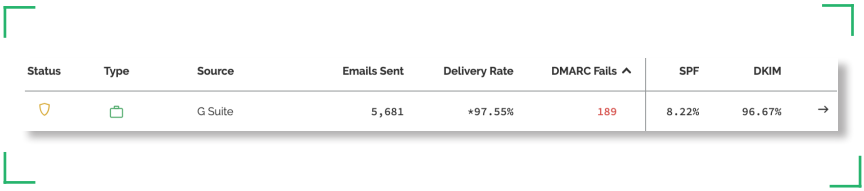
Part 1 - Grab the right reports

We hope you've made some good progress by now! Return to your **Reports** section and go to **Senders** using the links just above the graph. From here you can now select the domain you want to look at and then filter the time period using the top panel as shown below:



In '*Select time period*' go to '*Custom*' and choose the earliest time period that you started reporting and hit the download icon in the right-hand corner. Now you want to simply do the same again but for the most recent week - this should have some great stats to compare.

Part 2. Knowing what to look for



Status	Type	Source	Emails Sent	Delivery Rate	DMARC Fails	SPF	DKIM	
		G Suite	5,681	*97.55%	189	8.22%	96.67%	→

Don't worry, we weren't just going to leave you there to figure out what to look at. Here are some key points you can compare between the two reports:

Improved deliverability

The Delivery Rate percentage should have increased.

Reduced DMARC fails

The number of DMARC fails you had at the start of the trial should be lower.

Improving your own email authentication

This is shown by an increase in SPF and DKIM percentages for an Asset.

Location Map

Switch to the Location perspective for this one and if you're seeing fewer red dots and more amber or green dots then you can be confident that this demonstrates an increase in correctly configured email security protocols - Nice work!

Bonus Points!

You may also spot other senders pass with 100% DKIM even though they are unknown to you. This is because they are acting as forwarders i.e. forwarding legitimate traffic from your already fully configured Assets.

We suggest you try this out near the end of your 14-day trial so that you've had a chance to configure some of your security protocols and there's enough data to see how its taken effect. In other words, it's time to impress someone with the initiative you took - and we'll give you what you need to back it up without even being in p=quarantine yet!

We make a great team, let's stick together!

With your initiative and our simple tools, you've hopefully been able to test the waters and see how simple it is to navigate your email landscape and take the first steps to secure your domain from impersonation.

However, like all things security focused, further configurations are needed over time to get to evolve your security from this reporting mode (p=none) to full protection (p=reject) once we've fully configured all your email sources together and you're ready to hit the switch to actively blocking all unauthorized emails from reaching anyone's inboxes.

We hope this isn't goodbye and if you have any further questions about OnDMARC then get in touch with one of the team at **contact@ondmarc.com** - we'll be happy to help.

Stay secure,

Team OnDMARC