Step 1 - Configuring DMARC on Your Domain

https://campus.barracuda.com/doc/112164999/

Note that when you first configure DMARC, it is in Reporting Mode only – it reports issues but does not protect against them.
You must complete all three steps of this process to enable DMARC enforcement:

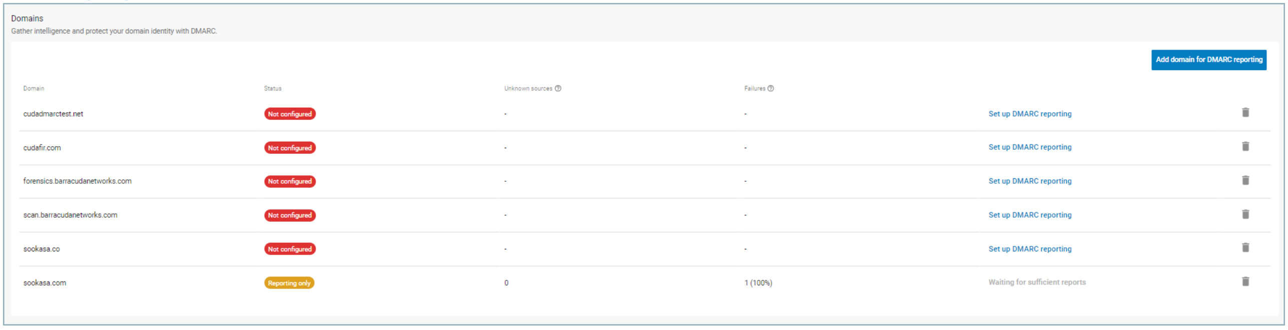
- Step 1 - Configuring DMARC on Your Domain (this step)
- Step 2 - Working with Email Sources
- Step 3 - Enabling DMARC Enforcement

If your Microsoft 365 account is connected to Barracuda Networks, start with Setting up Domain Fraud Protection with Microsoft 365 below. Your domains will already be visible on the Domain Fraud Protection page.
Otherwise, start at Setting up Domain Fraud Protection in Standalone. You will have to manually add and verify your domains.

Setting up Domain Fraud Protection with Microsoft 365

To configure DMARC on your domain, complete the following steps:

1. Log into Barracuda Domain Fraud Protection at https://login.barracudanetworks.com/signin.
2. On the left navigation menu select **Domain Fraud Protection**.
   Domains associated with your Microsoft 365 account are visible in the table, with the status of **Not Configured**. They are verified as your domains and need to be configured for DMARC. (For information on configuring domains not affiliated with your Microsoft 365 account, see Setting up Domain Fraud Protection in Standalone.)

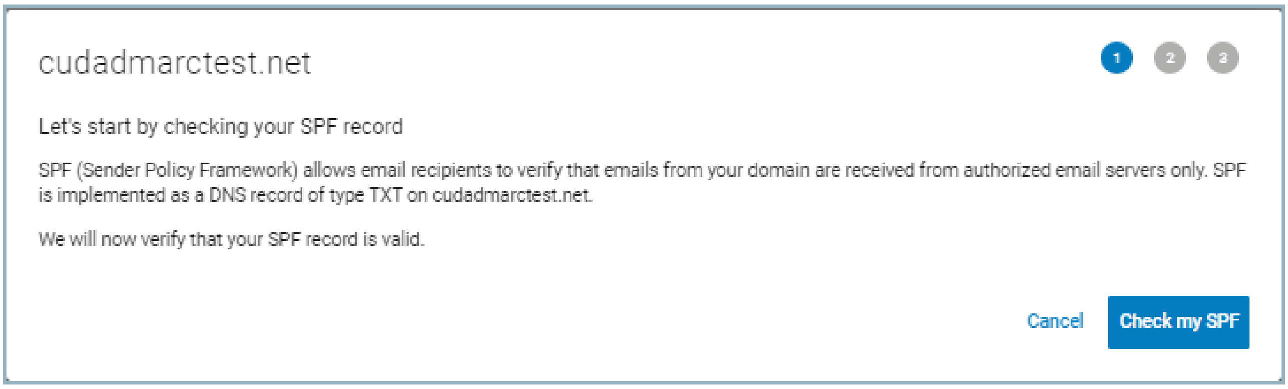


Domains

Gather intelligence and protect your domain identity with DMARC.

Domain	Status	Unknown sources	Failures		
cudadmarctest.net	Not configured	-	-	Set up DMARC reporting	🗑
cudafir.com	Not configured	-	-	Set up DMARC reporting	🗑
forensics.barracudanetworks.com	Not configured	-	-	Set up DMARC reporting	🗑
scan.barracudanetworks.com	Not configured	-	-	Set up DMARC reporting	🗑
sookasa.co	Not configured	-	-	Set up DMARC reporting	🗑
sookasa.com	Reporting only	0	1 (100%)	Waiting for sufficient reports	🗑

3. Locate a domain you want to configure and click **Set Up DMARC Reporting** and follow the instructions.
   Begin by checking that your SPF record is valid. Click **Check My SPF**.



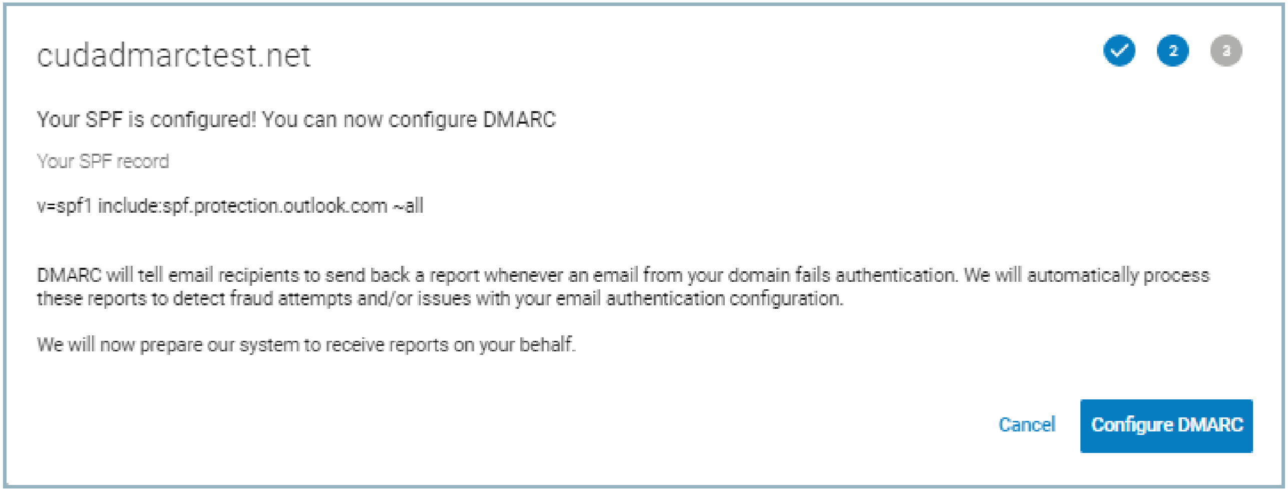
cudadmarctest.net

Let's start by checking your SPF record

SPF (Sender Policy Framework) allows email recipients to verify that emails from your domain are received from authorized email servers only. SPF is implemented as a DNS record of type TXT on cudadmarctest.net.

We will now verify that your SPF record is valid.

4. If your SPF record is valid, you can continue by clicking **Configure DMARC**.



cudadmarctest.net

Your SPF is configured! You can now configure DMARC

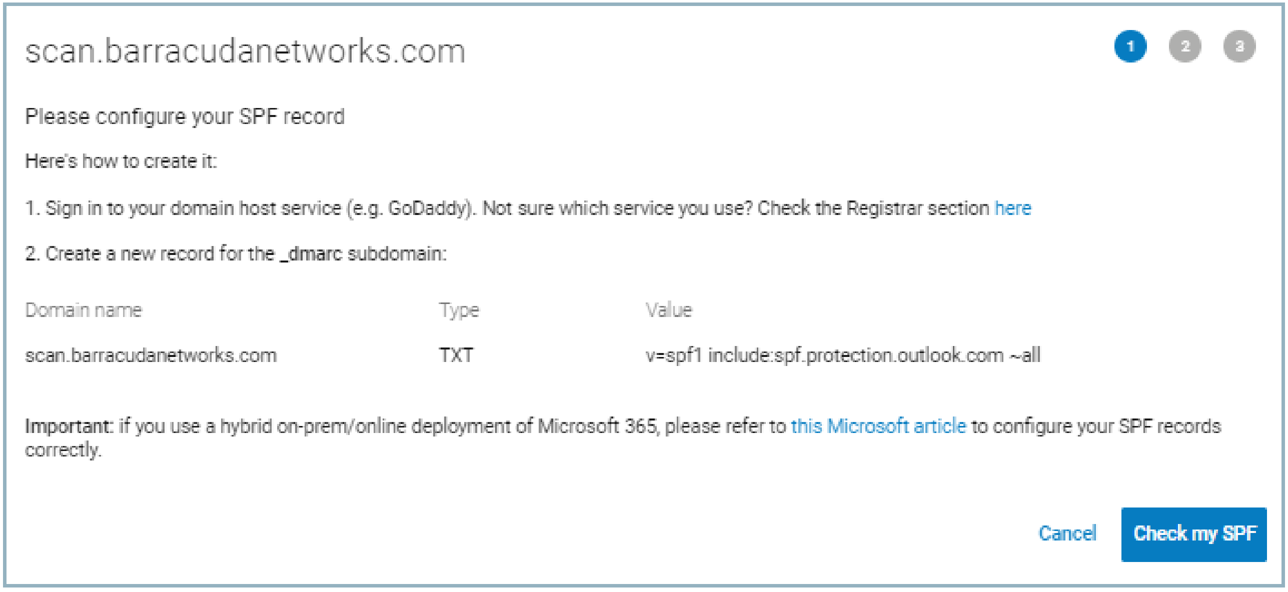
Your SPF record

v=spf1 include:spf.protection.outlook.com ~all

DMARC will tell email recipients to send back a report whenever an email from your domain fails authentication. We will automatically process these reports to detect fraud attempts and/or issues with your email authentication configuration.

We will now prepare our system to receive reports on your behalf.

If you need to configure your SPF record, follow the instructions, then click **Check My SPF**.



scan.barracudanetworks.com

Please configure your SPF record

Here's how to create it:

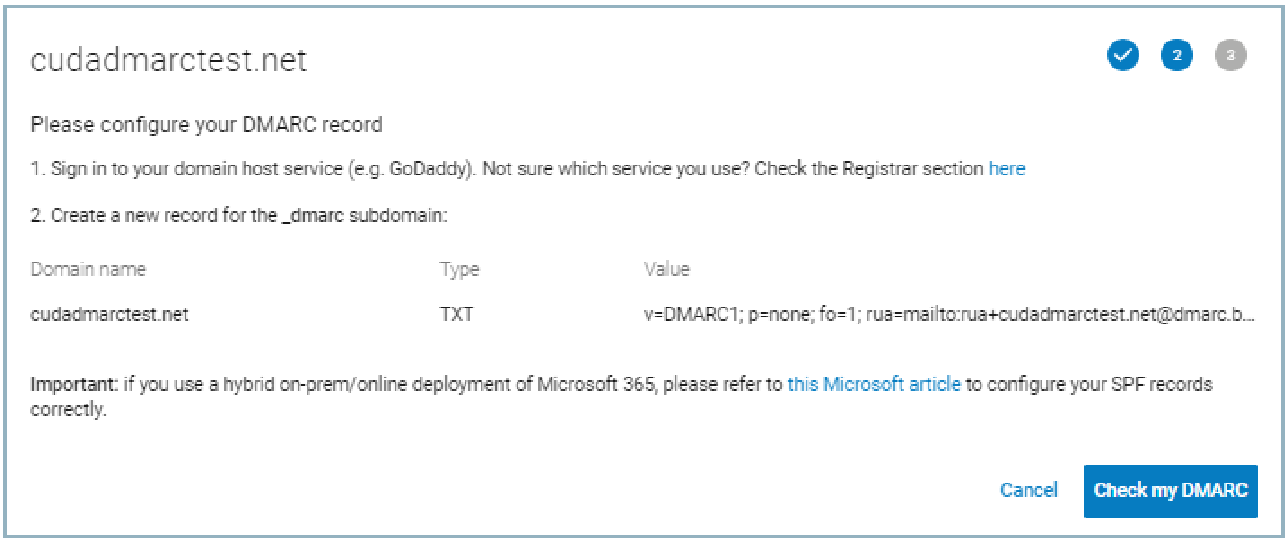
1. Sign in to your domain host service (e.g. GoDaddy). Not sure which service you use? Check the Registrar section here

2. Create a new record for the _dmarc subdomain:

Domain name	Type	Value
scan.barracudanetworks.com	TXT	v=spf1 include:spf.protection.outlook.com ~all

Important: if you use a hybrid on-prem/online deployment of Microsoft 365, please refer to this Microsoft article to configure your SPF records correctly.

5. Configure your DMARC record according to the instructions on the screen. After you update your DNS record, wait a few minutes and then click **Check My DMARC** to confirm the DNS update.
   Note that DMARC records are *not* case sensitive.



cudadmarctest.net

Please configure your DMARC record

1. Sign in to your domain host service (e.g. GoDaddy). Not sure which service you use? Check the Registrar section here

2. Create a new record for the _dmarc subdomain:

Domain name	Type	Value
cudadmarctest.net	TXT	v=DMARC1; p=none; fo=1; rua=mailto:rua+cudadmarctest.net@dmarc.b...

Important: if you use a hybrid on-prem/online deployment of Microsoft 365, please refer to this Microsoft article to configure your SPF records correctly.

Example of a DMARC record: *v=DMARC1; p=none; fo=1; rua=mailto:rua+cudadmarctest.net@dmarc.barracudanetworks.com; ruf=mailto:ruf+cudadmarctest.net@dmarc.barracudanetworks.com*

Clicking the DMARC value within the wizard will copy the entire string to your clipboard

The status of your domain is now **Reporting Only**. It will report, but not enforce DMARC.

1. Repeat this step for all the domains you want to protect with DMARC.

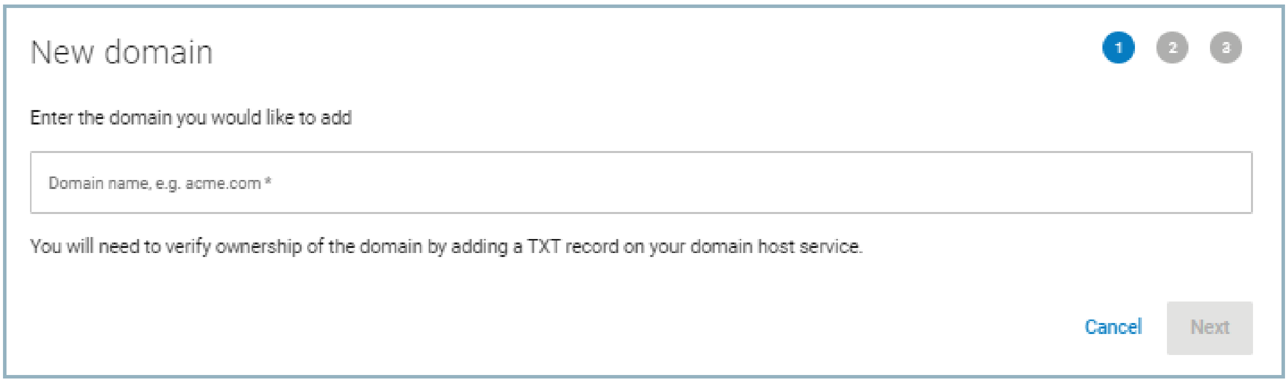
Continue with Step 2 - Working with Email Sources.

Setting up Domain Fraud Protection in Standalone

Domains that do not automatically appear in the Domains table must be set up manually. If you want to configure a domain for DMARC, you must verify ownership of the domain by adding a text record on the domain host service.

To add and configure a domain for DMARC protection:

1. At the top of the **Domains** page, click **Add Domain for DMARC Reporting**.
2. Provide the Domain Name, in the format `example.com`, then click **Next**.



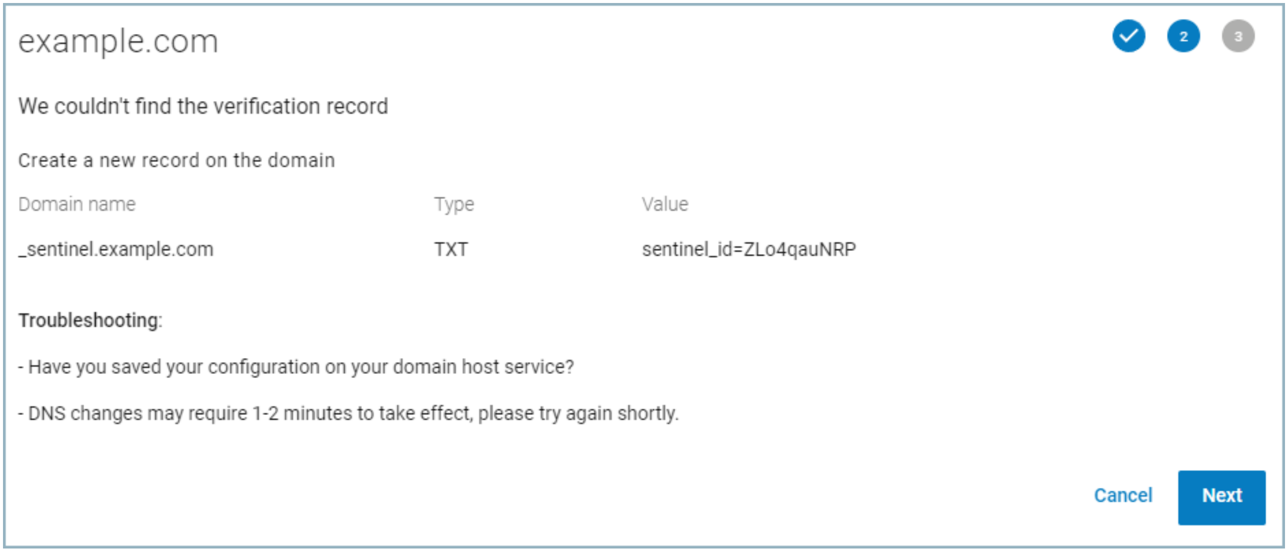
New domain

Enter the domain you would like to add

Domain name, e.g. acme.com *

You will need to verify ownership of the domain by adding a TXT record on your domain host service.

3. Verify that you own the domain by adding the text record specified in the instructions. Then click **Next**.
   As noted on the screen, this action verifies that you own the domain. It is *not* used for protecting your domain.



example.com

We couldn't find the verification record

Create a new record on the domain

Domain name	Type	Value
_sentinel.example.com	TXT	sentinel_id=ZLo4qauNRP

Troubleshooting:

- Have you saved your configuration on your domain host service?

- DNS changes may require 1-2 minutes to take effect, please try again shortly.

4. The system verifies your ownership of the domain. Click **Finish** to complete the process.
   Go to the top of the page and follow the instructions for configuring DMARC on this new domain.

Figures

1. domains-dmarc-reporting.png
2. check-spf.png
3. configure-dmarc.png
4. check-spf-2.png
5. check-my-dmarc.png
6. new-domain.png
7. verify-domain-ownership.png