

Step 1 - Configuring DMARC on Your Domain

<https://campus.barracuda.com/doc/73719857/>

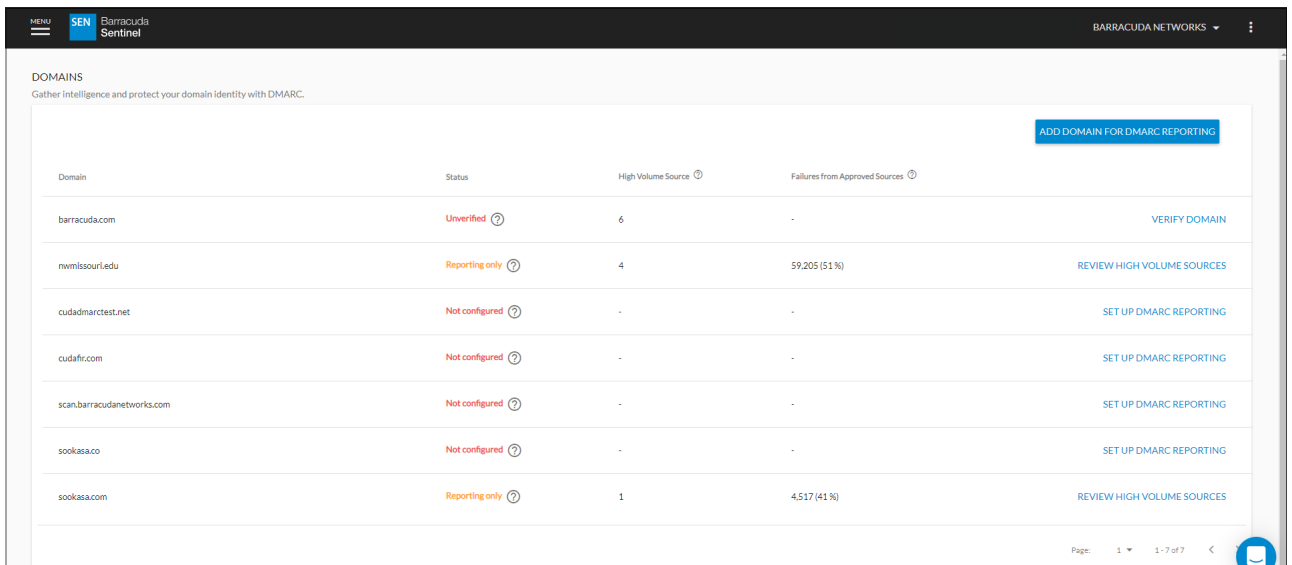
Note that when you first configure DMARC, it is in Reporting Mode only – it reports issues but does not protect against them.

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](#)

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

1. Log into the Barracuda Sentinel dashboard at <https://sentinel.barracudanetworks.com/signin>.
2. Click the menu button at the top left of the dashboard and select **Domain Fraud**. Domains associated with your Office 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 Office 365 account, see information at the end of this article.



The screenshot shows the 'DOMAINS' section of the Barracuda Sentinel dashboard. The table lists domains with their status, high volume sources, and failures from approved sources. A blue button 'ADD DOMAIN FOR DMARC REPORTING' is visible in the top right corner of the table area.

Domain	Status	High Volume Source	Failures from Approved Sources	Action
barracuda.com	Unverified	6	-	VERIFY DOMAIN
mwmisour.edu	Reporting only	4	59,205 (51 %)	REVIEW HIGH VOLUME SOURCES
cuadmarctest.net	Not configured	-	-	SET UP DMARC REPORTING
cuadfir.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	1	4,517 (41 %)	REVIEW HIGH VOLUME SOURCES

3. Select 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**.

scan.barracudanetworks.com 1 2 3

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 scan.barracudanetworks.com.

We will now verify that your SPF record is valid.

CANCEL CHECK MY SPF

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

scan.barracudanetworks.com 1 2 3

Your SPF is configured! You can now configure DMARC

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.

CANCEL CONFIGURE DMARC

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

scan.barracudanetworks.com 1 2 3

Please configure your SPF record

We were unable to find an SPF record on your domain. To set one up:

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 with this value:

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 Office 365, please refer to [this Microsoft article](#) to configure your SPF records correctly.

CANCEL CHECK MY SPF

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.

scan.barracudanetworks.com 1 2 3

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:

Name	Type	Value
<u>_dmarc.cudadmarctest.net</u>	TXT	"v=DMARC1; p=none; fo=1; rua=mailto:rua+cudadmarctest.net@dmarc.barracudanetwc

Please note: adding this record will not change your email deliverability or affect your emails in any way. It will only signal email recipients to send feedback when emails from your domain fail to authenticate.

[CANCEL](#) [CHECK MY DMARC](#)

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

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

Continue with [Step 2 - Working with Email Sources](#).

Domains Not Associated with your Office 365 Account

Domains that are not a part of your Office 365 account do not automatically appear in the Domains table. 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 1 2 3

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.

[CANCEL](#) [NEXT](#)

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 1 2 3

Please verify you own the domain

Create a new record on the domain

Domain name	Type	Value
._sentinel.example.com	TXT	sentinel_id=G5i64Sj2NS

Please note: adding this entry will only verify that you own this domain. It is not a DMARC record for it.

[DISMISS](#) [NEXT](#)

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.png
2. DMARC1.png
3. DMARC2.png
4. NeedConfigureSPF.png
5. DMARC3.png
6. newDomain.png
7. verifyOwnership.png

© Barracuda Networks Inc., 2021 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.