Step 1 - Configuring DMARC on Your Domain

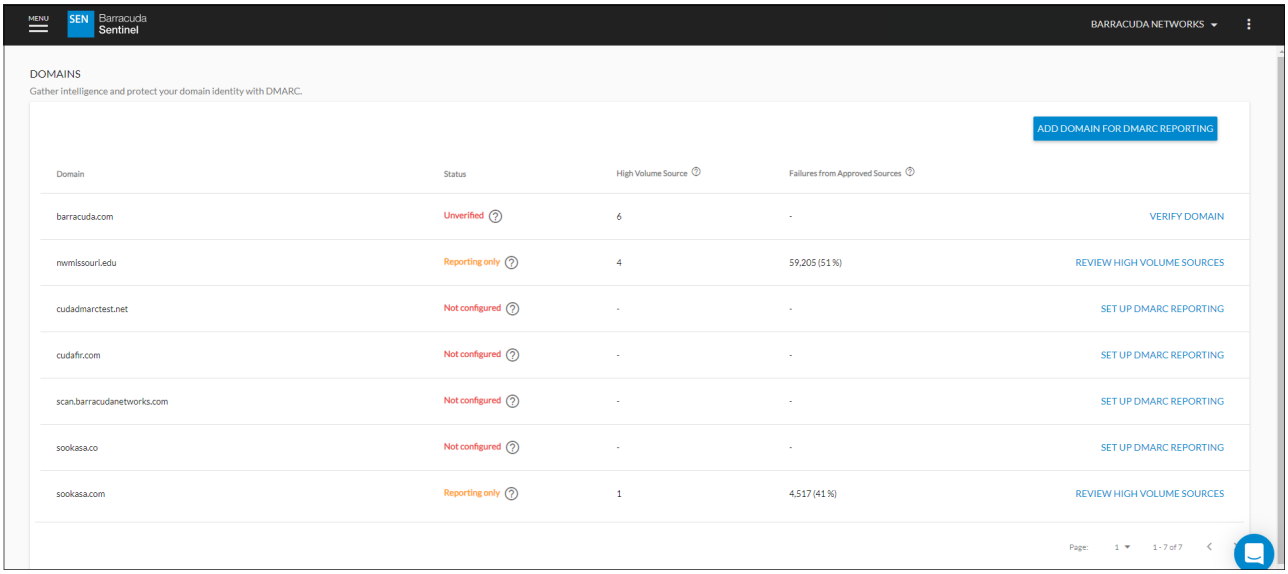
https://campus.barracuda.com/doc/73719857/

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:

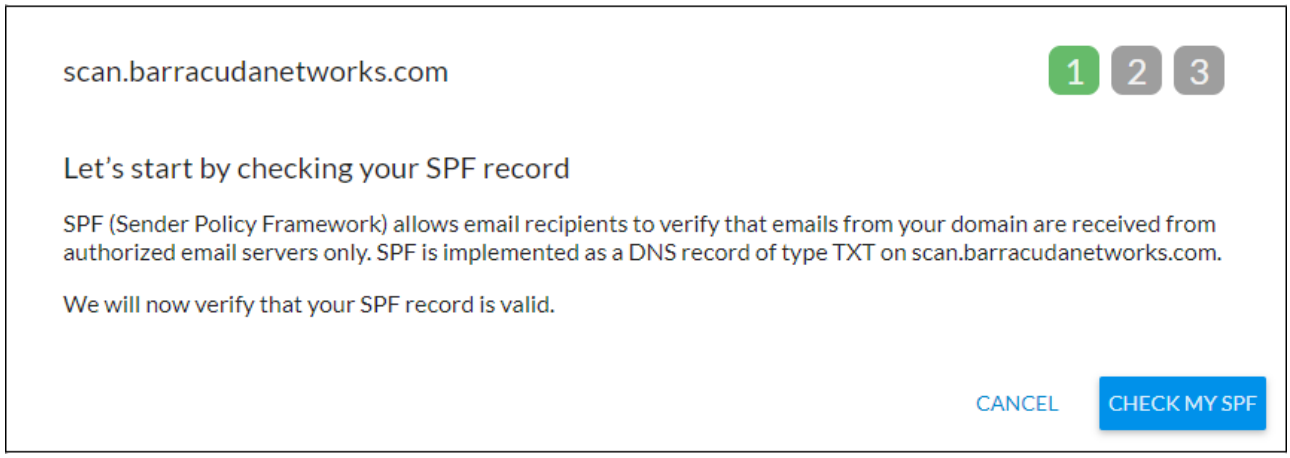
- Step 1 - Configuring DMARC on Your Domain (this step)
- Step 2 - Working with Email Sources
- Step 3 - Enabling DMARC Enforcement

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

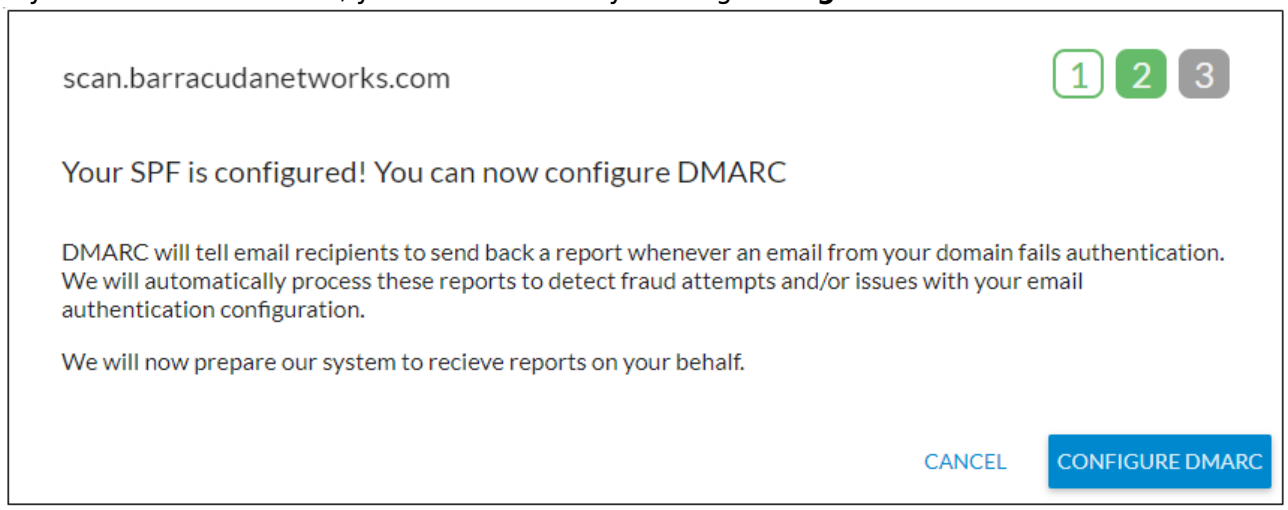
1. Log into the Barracuda Sentinel dashboard at https://sentinel.barracudanetworks.com/signin.
2. Click the menu button at the top left of the dashboard and select **Domain Fraud**.
   Domains associated with your Office 365 account are visible in the table, with the status of **Not Configured**. They 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.



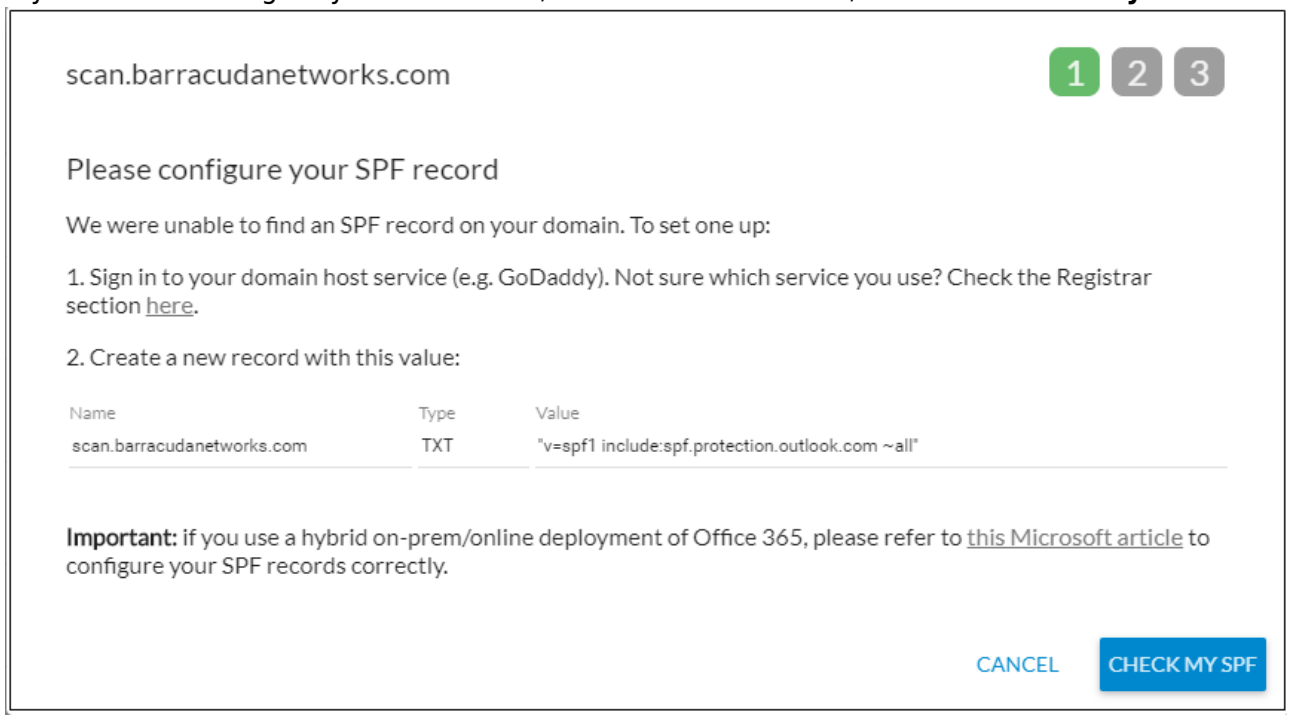
3. Select a domain you want to configure and click **Set Up DMARC Reporting** and follow the instructions.
   Begin by checking that your SPF record is valid. Click **Check My SPF**.



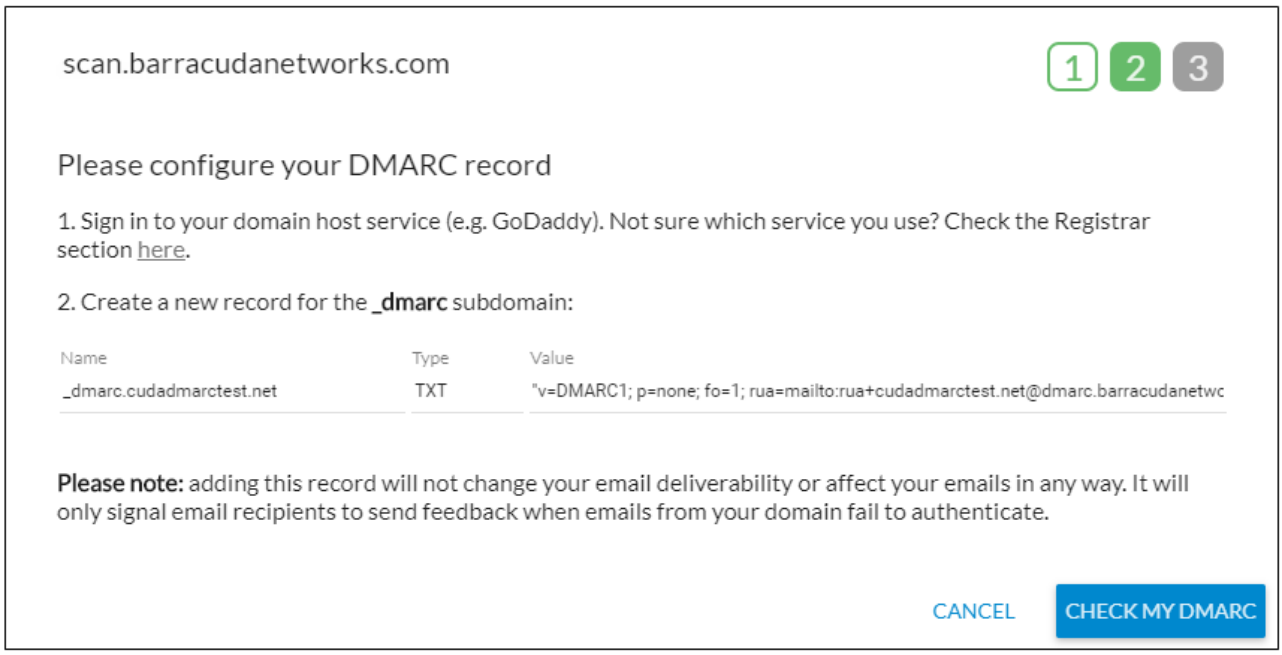
4. If your SPF record is valid, you can continue by clicking **Configure DMARC**.



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



   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.

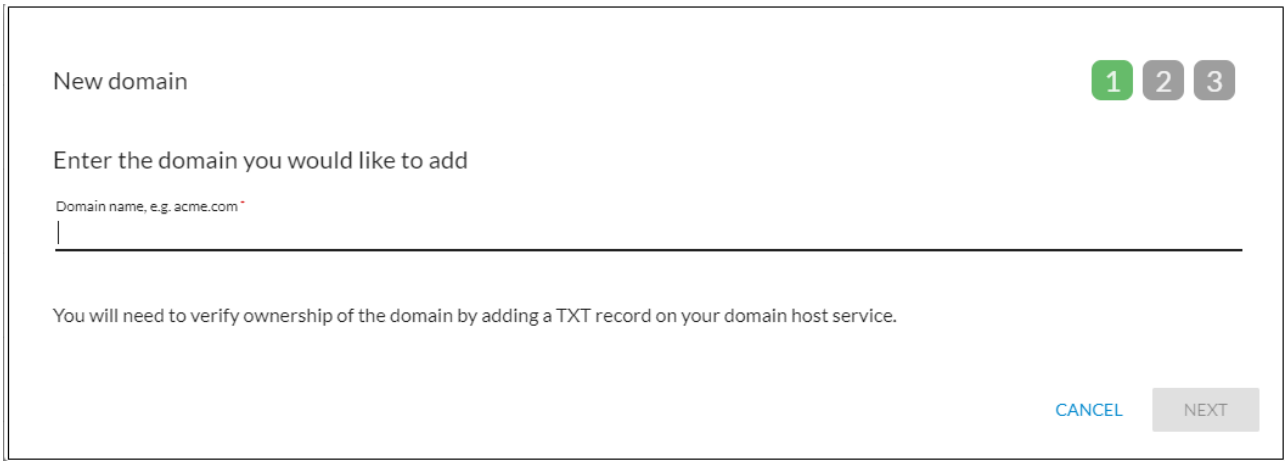
Continue with Step 2 - Working with Email Sources.

Domains Not Associated with your Office 365 Account

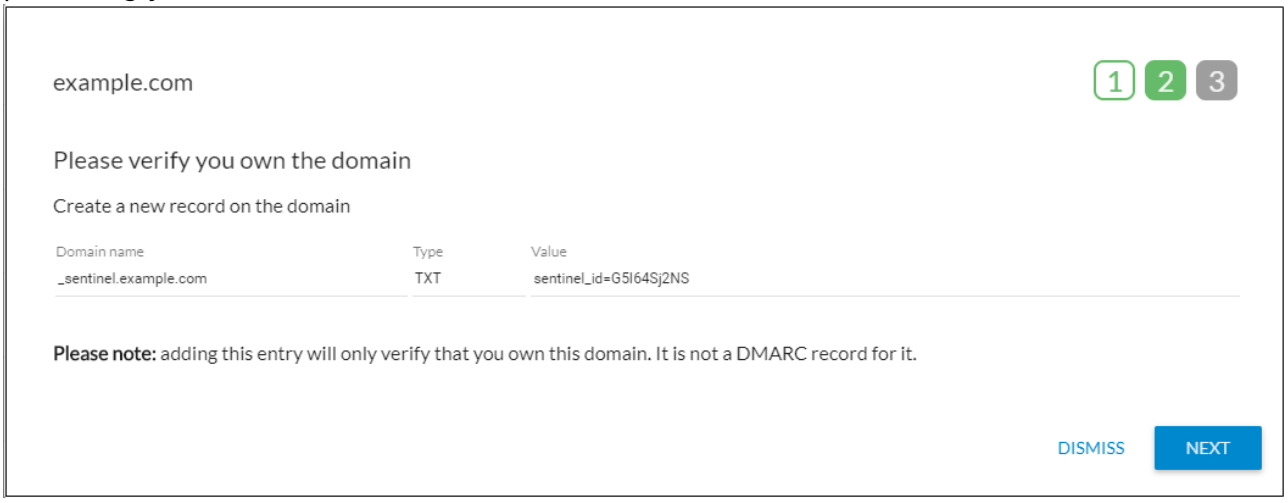
Domains that are not a part of your Office 365 account do not automatically appear in the Domains table. If you want to configure a domain for DMARC, you must verify ownership of the domain by adding a text record on the domain host service.

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**.



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.



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