Domain Authorization

https://campus.barracuda.com/doc/79463989/

Domain Authorization functionality replaces the former @Restricted Domains functionality.

If you see a warning message about unauthorized domains, click the warning message to manage the domains.

Before you can begin your campaign, you must authorize each of your domains. You do this by adding an innocuous text record to your domain in order to prove to the Barracuda PhishLine system that you own the domain. This is a security measure to ensure that you, in fact, have the authority to send emails to the domains you specify. The domain list is generated automatically based on the domains associated with each of the users you uploaded to your Address Books. You can also add the domains manually to authorize them in advance.

To authorize your domains:

1. Navigate to **Campaigns > Domain Authorization**.
2. Click **New**.
3. Enter the Domain Name you want to authorize.
4. Click **Save**.
5. When the page refreshes, locate and copy the TXT Record Content for the domain.
6. Add this TXT record to your domain through your DNS (Domain Name Server) provider. You can obtain instructions on how to add a TXT record to your domain from your DNS provider. See important information about timing below.

Organizational email address books often contain emails from associated entities, like consultants, contractors, and partners. These entities should not be receiving campaign emails, unless you are authorized to do so.

Note

You can choose to ignore one or more domains if you do not intend to use them in your campaigns. On the **Domain Authorization** page, select the **Ignore Domain** check box.

Timing of Domain Authorization

It is best to perform the complete domain authorization process described above at one time, adding the TXT record to your domain soon after you add the domain to Barracuda PhishLine. The sooner you add the TXT record to your domain, the sooner Barracuda PhishLine will authorize your domain.

Barracuda PhishLine checks new domains for TXT records on scheduled intervals, as shown in this table:

Time Since Domain Added	How Often Domain is Checked
< 24 hours ago	every 15 minutes
24-48 hours ago	every 30 minutes
40-96 hours ago	every 60 minutes
>96 hours ago	every 4 hours

Campaign Schedules and Test Emails

You cannot schedule unauthorized email addresses in any campaigns. If a user attempts to send a test email to an unauthorized domain, the email will not be sent until you authorize the domain.

Identifying Unauthorized Domains

Unauthorized domains are listed under **Campaign > Domain Authorization**. You can filter by **Validated** to list only the unauthorized domains. In addition, Barracuda Phishline warns you in the following locations:

- **Dashboard**: If there are any unauthorized email addresses in any of your Address Books.
- **Address Book**: If there are any unauthorized email addresses.
- **Campaign**: If there are any unauthorized email addresses in the Address Books associated with the campaign.

If you see a warning message about unauthorized domains, click the warning message to manage the domains.