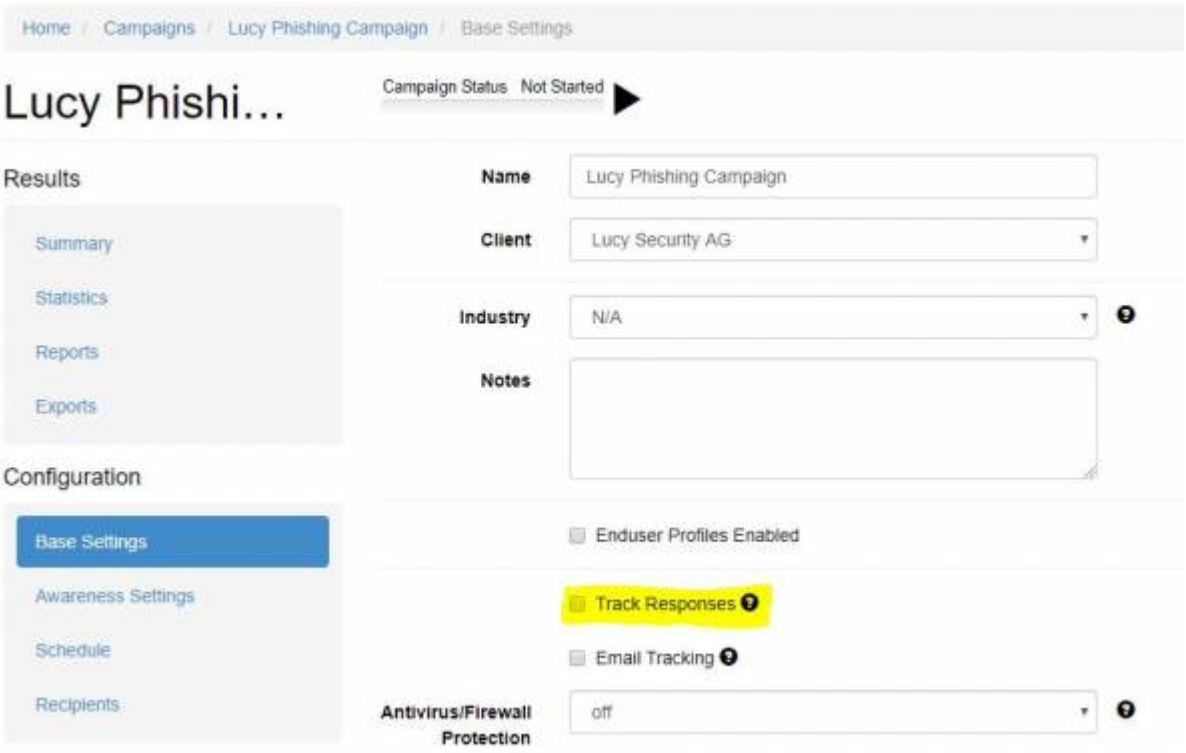
Response Detection

For accurate statistics, Lucy has the functionality to work with emails that came in response to a phishing email. Thus, you can determine which of the recipients did not actually receive the e-mail(for example email was not delivered and Lucy received a response from the mail server) or do not include the auto-responses in the statistics.

Please note that Automated Response Detection will not work if some conditions are not met:

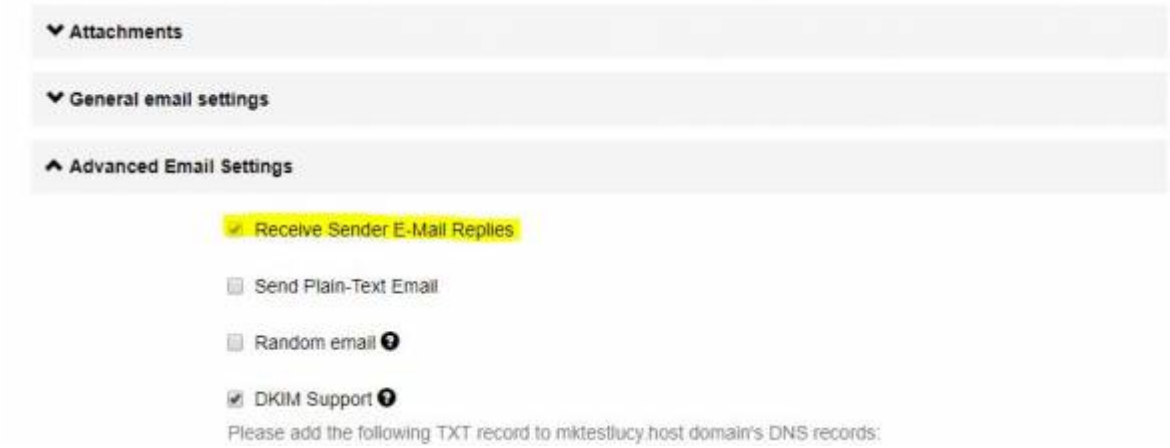
1. Sender's domain (used in the Scenario Settings > Message Template) must have MX records pointed to the Lucy server. If MX records configured correctly, responses to the sender email will be deliver to the Lucy server and Lucy will be able to process these responses. Otherwise, if MX record of the sender domain is not pointed to the Lucy server, responses do not deliver to the Lucy, and Automated Response Detection option will not work.

2. You need to enable Track Responses option in the campaign Base Settings:



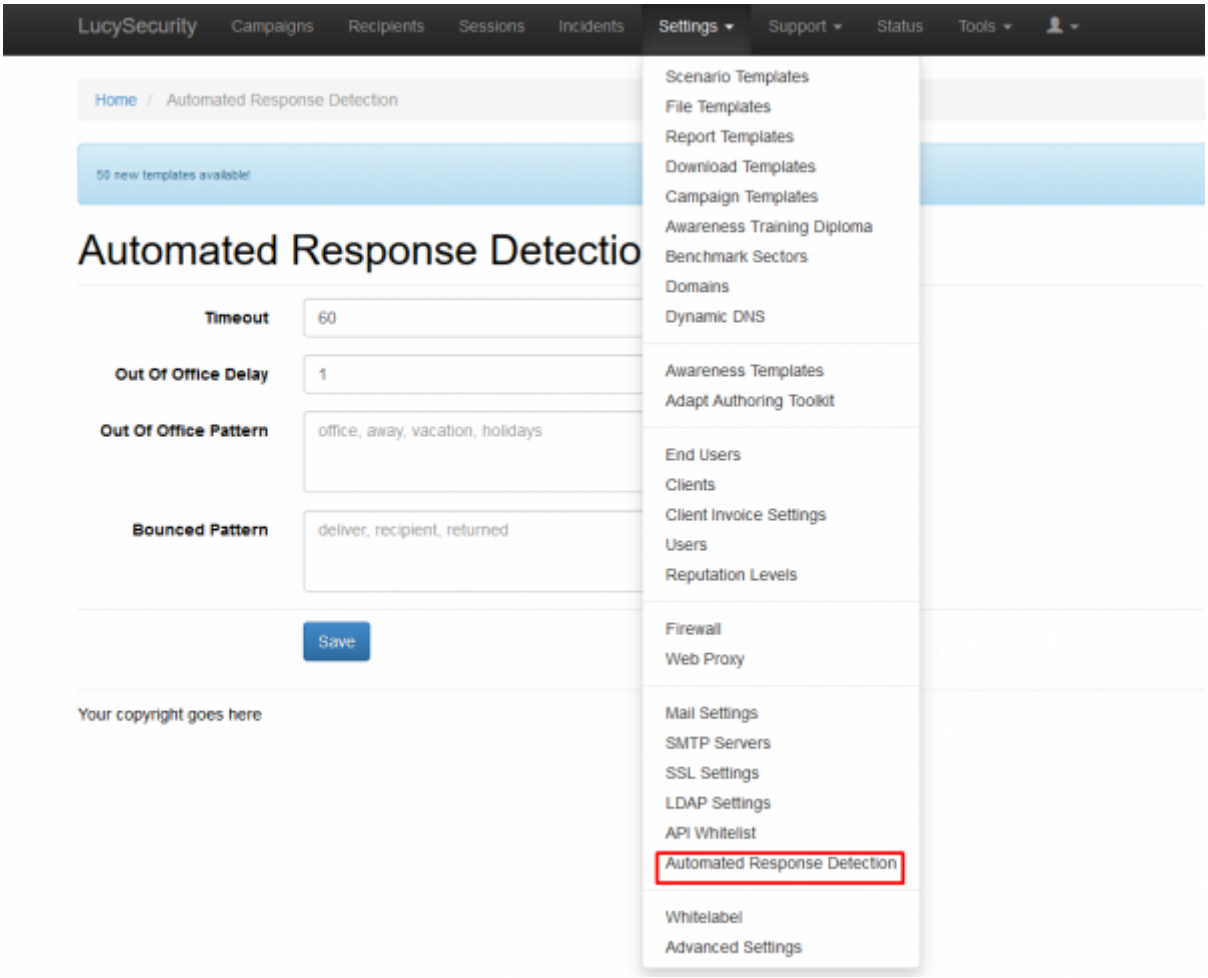
This option will enable Automated Response Detection in the **all** scenarios of this campaign.

3. If you need to enable this option for a separate scenario, open the Scenario Base Settings > Message Template page and enable Receive Sender E-Mail Replies option in the Advanced Email Settings section:

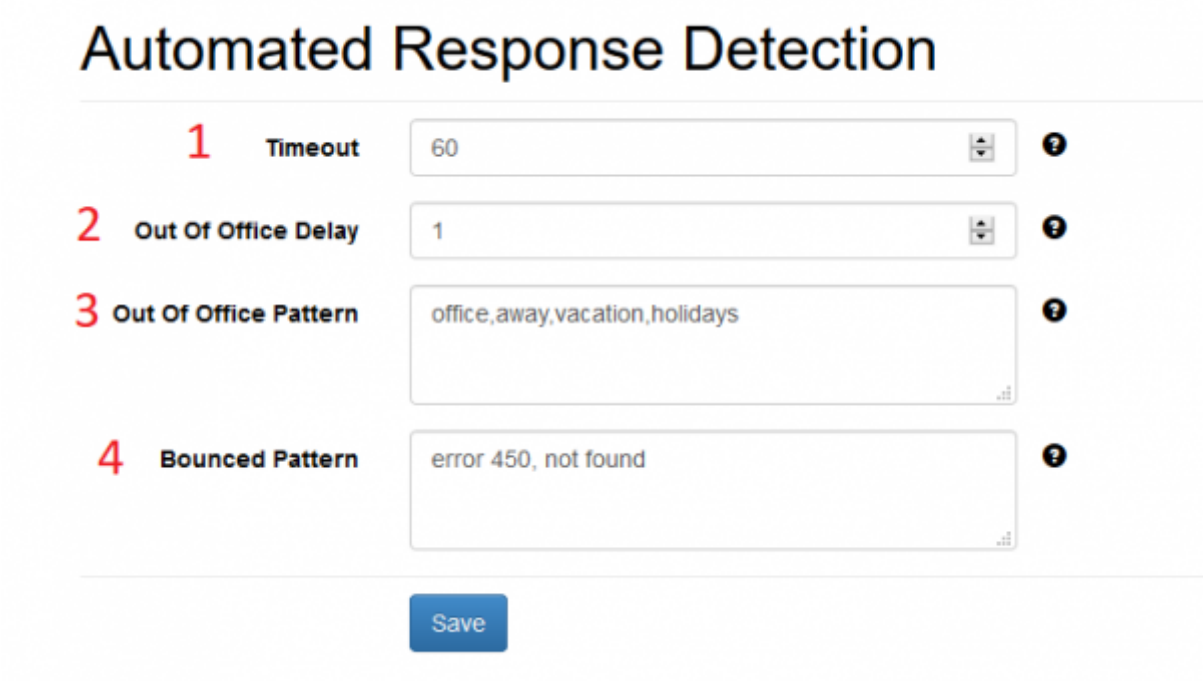


Automated Response Detection settings

You could change settings of Automated Response Detection here:



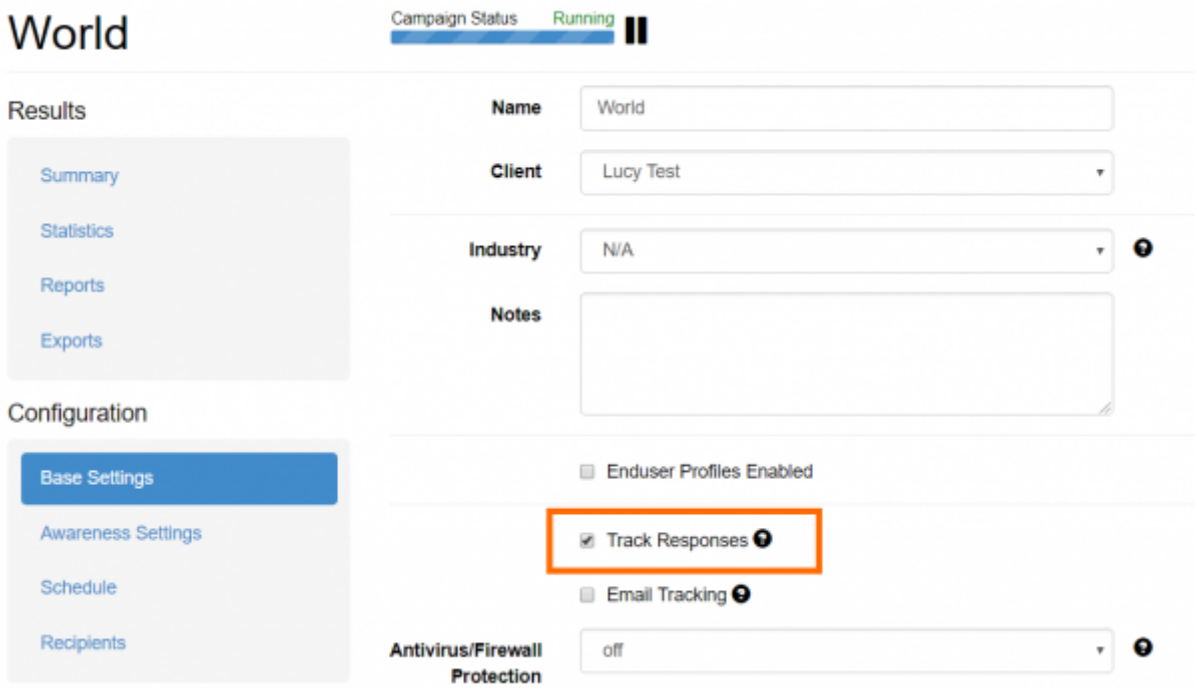
There are 4 main types of track responses settings:



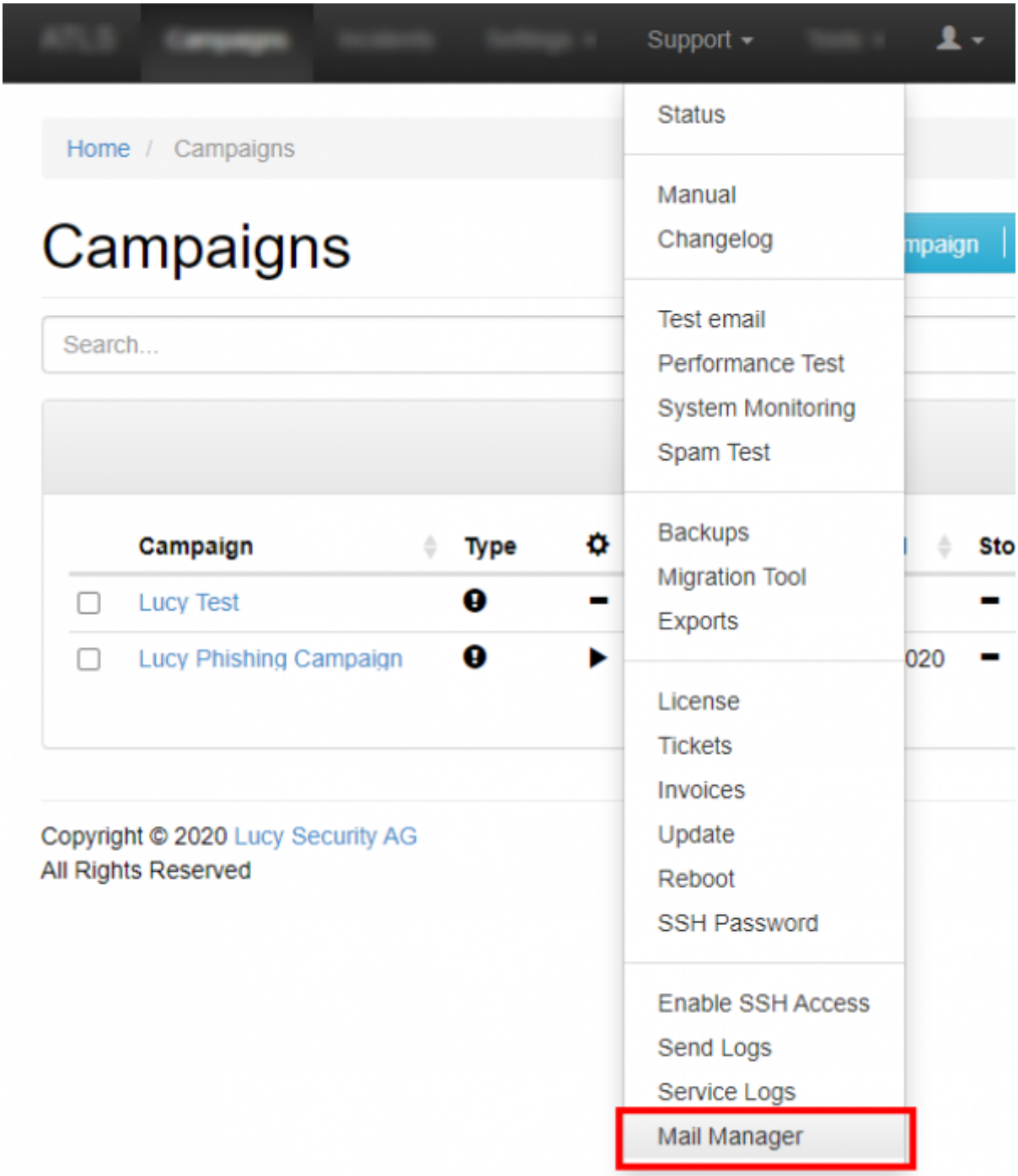
1. Emails returned immediately after sending a phishing emails are most likely an auto-reply. If an email will arrive within the given period (in seconds) after submitting an attack email, the incoming email will be treated as an automated response.
2. The best way to coverage all recipients in a campaign is to resend phishing email to victims who for some reason set up an automated response. Since most likely the victim is not in the workplace or he does not read the email, it is best to resend the message in a few days. In this field, specify number of days to wait until sending a reminder for the victim that is out of office.
3. Patterns to find in replies to mark them as 'out of office' responses. For example its can be patterns related with holidays or business trip. A repeated email will arrive in the number of days specified in "Out Of Office Delay"
4. Each mail server has its own template of bounced emails. In this field, you can specify pattern to find in replies to mark them as 'bounced' responses or some errors from mail server.

Mail Manager

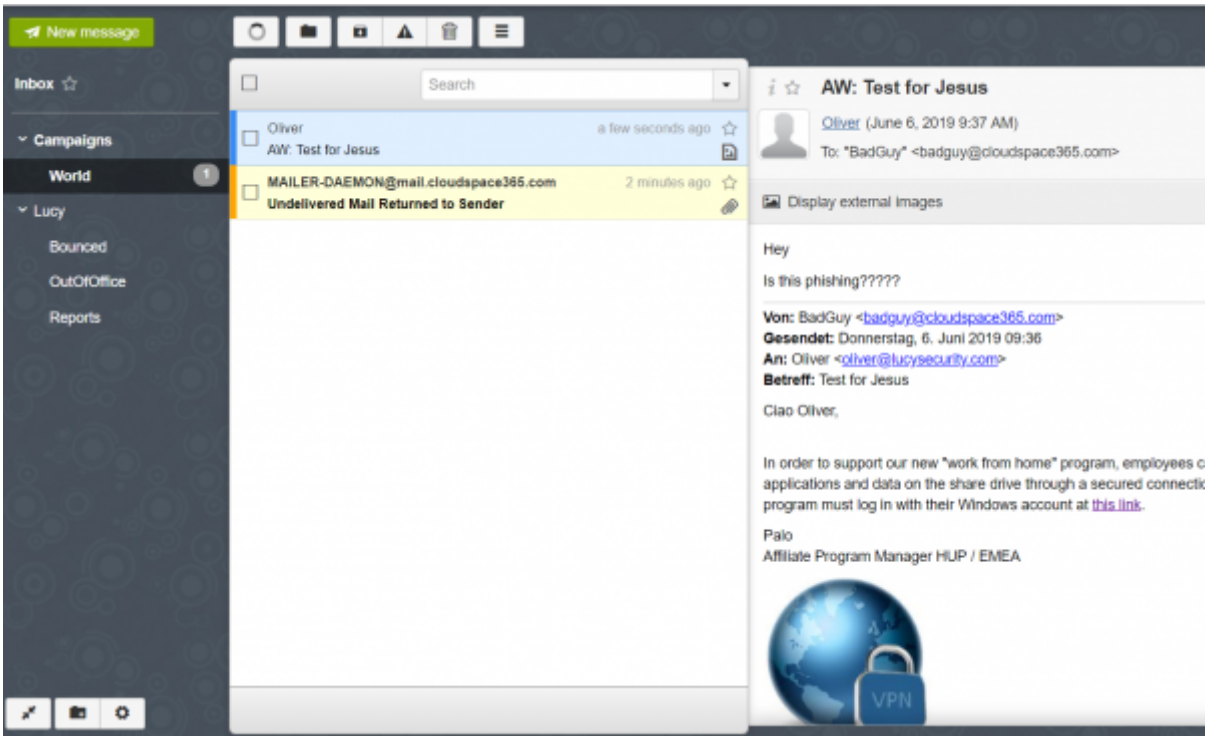
The mail manager allows interactive communication with the recipient. First of all, this type of communication must be activated in the campaign. Please make sure the MX record for the sender email points to LUCY. See response detection chapter.



You can the see email replies in the mail manager which is accessible here:



The multi-staged interactive communication can then continue within the mail manager:



From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=response_detection&rev=1564051800

Last update: **2019/07/25 12:50**