

Log files explained

The following article comprises an overview of Lucy's logging sequences. Lucy keeps an internal log of application events. Thus, besides analyzing service logs (apache2 web server, postfix mail server and etc), one can also monitor most of the application events and perform an investigation of occurring errors.

Lucy internal logs

Depending on the instance type (on-premise or our VPS) administrators can access Lucy log files from the web interface and/or from the backend. Directory **/opt/phishing/runtime** contains log files of the web application on the server. Same directory archive + webserver error log can be downloaded from Lucy web interface under **Support → Send Logs**. The only apparent distinction is that on the server, logs can be dynamically monitored in real-time.

Here is the list of the log files followed by a short overview:

1. **application.log** Application-related log that collects errors from database and webserver.
2. **resque_worker.log** The file that stores the journal of all Lucy events. Every job produces at least 2 notifications: job start and finish. Notification messages consist of the timestamp, id of the process, arguments (e.g. campaign data), and job status.
3. **awarenessrescheduler.log** File contains plain notifications of re-scheduled awareness sent to the recipients.
4. **console.log** Log file that collects events from various services and utilities used by background processes.
5. **mailcrawler.log** Events related to the [mail manager](#) job get logged in here. Mail manager work
6. **migration.log** Journal that is filled only in case Lucy instance is being migrated from version to version (for Lucy version < 4.2)
7. **proxystat.log** If Lucy is working behind the proxy, all the related events will appear in here.
8. **reminders.log** Log file for events related to reminders in campaigns.
9. **resque_emailparse.log** Contains log for email parse job
10. **resque_enduser.log** Log file for job updating victims statistics.
11. **resque_letsencrypt.log** This file keeps a log of events related to Let's Encrypt API.
12. **resque_scheduler.log** File contains the log of the scheduler events: schedule rule start and finish for each recipient.
13. **resque_ssl.log** All SSL-related events: certificate creation, renewal, import, and etc.
14. **resque_stats.log** Log of the campaign statistics job that regularly updates campaign results in the web interface.
15. **resque_system.log** Jobs that affect system performance, e.g. updates, reboots, shutdowns, process killjobs.
16. **resque_victim.log** Events related to binding recipient groups to campaigns.
17. **resque_visit.log** Log of recipients visits to scenario web pages (both attack and awareness). The recipient's personal data is represented only with the victim's id here. Thus, no sensitive data is exposed whilst visit data is attributed to the victim (IP address, user agent, OS and etc).
18. **scheduler.log** Scheduler log file.
19. **systemmonitoring.log** System status log file.

Status - Log of user actions


Lucy also provides an opportunity to monitor users' activity: login-logout, started campaigns, messages sent and etc. Log files can be found within the user interface under **Support → Status**.

The screenshot displays the 'Status' page in the Lucy application. The top navigation bar includes 'Your Software Name', 'Campaigns', 'Incidents', 'Settings', 'Support', 'Tools', and a user profile icon. The breadcrumb trail shows 'Home / Status'. The main heading is 'Status'. On the right, there are 'Export' and 'Clear' buttons. Below the heading is a table of logs with three columns: 'Time', 'Message', and 'User'. A red box highlights a log entry for '06.05.2021 17:06:15 - 06.05.2021 17:14:39' with the message '2 Campaigns Renamed' and user 'User (krek@user.com)'. To the right of the table is a 'Filter' panel with a 'Type' dropdown set to 'All', 'From' and 'To' date pickers both set to '11.05.2021', and an 'Update' button. Below the filter panel is a 'Current User' section with a table showing 'Name' and 'User'.

Time	Message	User
07.05.2021 21:19:15 - 11.05.2021 20:10:11	5 Users Logged in	User (krek@user.com)
06.05.2021 17:06:15 - 06.05.2021 17:14:39	2 Campaigns Renamed	User (krek@user.com)
05.05.2021 19:50:40 - 06.05.2021 16:23:33	3 Users Logged in	User (krek@user.com)
05.05.2021 15:54:37 - 05.05.2021 16:13:45	2 Campaigns Added	User1 (test1@user.com)
05.05.2021 15:53:10	1 Users Logged in	User1 (test1@user.com)
04.05.2021 23:21:57 - 05.05.2021 15:34:04	2 Users Logged in	User (krek@user.com)
04.05.2021 21:35:00 - 04.05.2021 21:35:00	6 Messages Sent	System
04.05.2021 20:56:44	1 Campaigns Added	User (krek@user.com)
04.05.2021 14:10:59 - 04.05.2021 20:51:57	3 Users Logged in	User (krek@user.com)
03.05.2021 23:39:04 - 03.05.2021 23:40:18	3 Messages Sent	System
03.05.2021 22:56:10 - 03.05.2021 23:38:19	2 Users Logged in	User (krek@user.com)

As of the screenshot:

1. Status logs are presented in the list: time of the event, type of the event, and username.
2. Logs can be filtered on the right pane. You can filter events by the type of action and specify the time period.
3. Logs can be exported in CSV or XML format by pressing the **Export** button.
4. Lucy's log journal can also be removed from the instance by pressing the **Clear** button.
5. By pressing on the date one can proceed to a more detailed view of the log. It contains events with short messages describing the event briefly. Also, on the right one can always find a pane with information about the current user: name, phone and etc.

Your Software Name Campaigns Incidents Settings ▾ Support ▾ Tools ▾ 

Home / Status /

Status Clear

Time	Message	User
06.05.2021 17:14:39	Test campaign 1: campaign renamed	User (krek@user.com)
06.05.2021 17:06:15	Track Responses: campaign renamed	User (krek@user.com)

« 1 » 50 ▾

Current User

Name	User
Email	krek@user.com
Phone	N/A
Role	Administrator

Your copyright goes here

Service Logs

Lucy also keeps journaling service logs - apache2 web server log and mail server log. These can be accessed under **Support → Service Logs**. You can choose the file and specify the time period within the accordant fields. There are three files (and their older versions):

1. mail.log - contains postfix mail server events.
2. access.log - apache2 web server log that contains all requests received.
3. error.log - apache2 web server errors.



From:

<https://wiki.lucysecurity.com/> - LUCY

Permanent link:

https://wiki.lucysecurity.com/doku.php?id=lucy_logging_concept

Last update: **2021/05/12 02:10**

