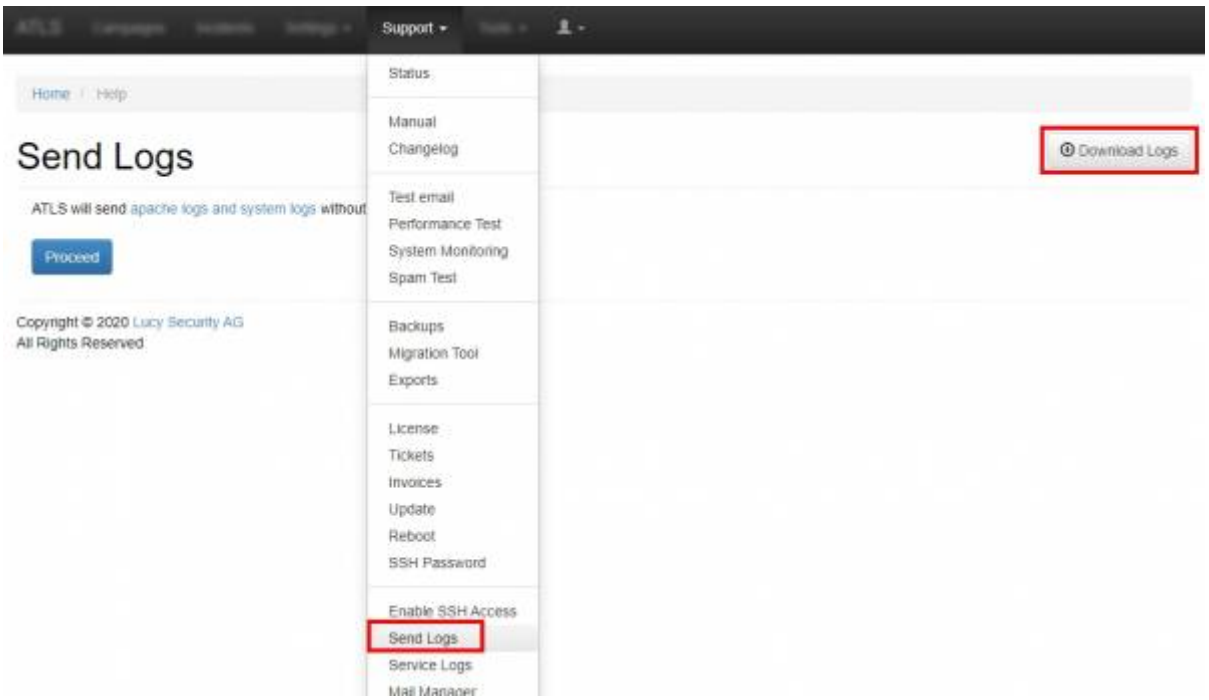
OUTBOUND COMMUNICATION REQUIRED: SORTED BY TYPE OF ACTION

LUCY might initiate certain communication channels to servers on the internet:

- **First Time Use - Obtaining Workstation ID**: When you install LUCY for the first time, LUCY will connect via HTTP to a server to get the current workstation key & ID. LUCY can also operate without that ID & key. This ID can be used later to upgrade LUCY from a community edition to a commercial license. No information about your environment, besides the current built version, is transmitted to our server.
- **Updates**: When performing updates LUCY may connect to our update server (fixed IP) and occasionally to a Debian repository (in older versions < 2.5).
- **SSH**: If you enable SSH in the Help Menu, LUCY will initiate a SSH connection to our SSH Jump Host (outbound). By default this is disabled. It is the clients responsibility to enable/disable the SSH port on LUCY itself.
- **Checks**: When you perform campaign checks (test your campaign settings), LUCY will connect to a few fixed servers. Since we also test within those checks, if the server is reachable from the internet (via HTTP or HTTPS) we initiate a HTTP/HTTPS connection inbound to your installation. No data is transmitted - only the connectivity is tested.
- **Running a Campaign**: LUCY might need to communicate via Port 25 or 465 (SMTP) outbound if you send mails to users over the internet
- **Vulnerability Checks**: If you need the client vulnerability detection feature enabled, you should also allow port 80 connection to static.nvd.nist.gov (129.6.13.177). That host is used to download NIST CVE database with vulnerabilities.
- **Logs**: In the Settings (found under Settings/Settings) Menu, you are able to send LUCY logs to us. Those logs contain only technical data about your installation (mainly Apache logs) - but all customized sensitive data is deleted (we don't collect any information about your campaign or the environment).



OUTBOUND COMMUNICATION: SORTED BY PORT & IP

IP	Function	Port	Protocol
176.9.154.150 (update.phishing-server.com)	Lucy Update/License Server/HTTP proxy	80/443 (HTTP/HTTPS)	TCP
176.9.154.150 (gta-update.does-it.net)	Linux repository	80 (HTTP)	TCP
8.8.8.8 (or any other DNS Server)	Your DNS Server	53 (DNS)	UPD
nvd.nist.gov	NIST CVE database (Optional)	443 (HTTPS)	TCP
0.0.0.0 (Any)	Mail Communication (Optional)	25 (SMTP)	TCP
193.25.101.87 (news.gtta.net)	Fetch LUCY Update News (Optional)	80 (HTTP)	TCP

INBOUND COMMUNICATION

In order to reach LUCY from the internet port 80 and 443 (if you use SSL in a campaign) needs to be open. No other ports are required. If LUCY should forward mails from users that respond to a phishing simulation port 25 (SMTP) needs to be opened as well.

Source IP	Destination	Port	Prot	Comment
ANY	Your LUCY Server IP	80/443 (HTTP/HTTPS)	TCP	Needed for accessing the landing pages & for certificate verification (http)
ANY	Your LUCY Server IP	25 (SMTP)	TCP	Only needed, if you want to catch email replies

MALWARE SIMULATION COMMUNICATION

Upon execution, the malware simulation tool will open the built in Internet Explorer or other default browser (in hidden mode) and send out the collected data to LUCY via HTTP or HTTPS (it will automatically choose HTTPS if you run your campaign via SSL). This tool will also work in environments where the Internet is accessed with Proxy servers - only allowing access for authorized Windows users.

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

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=network_communication_-_lucy_--_internet&rev=1564051795

Last update: **2019/07/25 12:49**