Install LUCY using the Linux install script (install.sh)

How much time is required?

The installation is very simple and straight forwarded. After downloading and executing the installer script everything will run automatically in the background. Depending on your internet connection speed an installation can take 30-60 minutes.

Which OS is required for the default docker installation of LUCY?

LUCY supports docker and therefore runs on all known Linux systems (https://www.docker.com/). Docker Engine is supported on Linux, Cloud, Windows, and OS X. Installation instructions are available for the following:

On Linux:

- Arch Linux
- CentOS
- CRUX Linux
- Debian
- Fedora
- FrugalWare
- Gentoo
- Oracle Linux
- Red Hat Enterprise Linux
- openSUSE and SUSE Linux Enterprise
- Ubuntu

The shell script will check if your system has already docker installed. If not, it will guide you through the installation process and install all necessary components automatically.

Can LUCY be installed on older Linux Kernel Version (< 3.10)?

The older versions of the linux setup script (< 2.8) have been tested on Debian 7 (Wheezy), Debian 8 (Jessie), Ubuntu 12.04 and Ubuntu 14.04. As an additional requirement, you need to have openssl installed. A 3.10 Linux kernel is the minimum requirement for Docker. Kernels older than 3.10 lack some of the features required to run Docker containers. In case you use an older Linux Kernel you will need to install LUCY on Debian 7 or Ubuntu 12.

General Preparation

- **Make sure you have openssl installed**: You can do this by typing "apt-get install openssl" in the terminal.
- **Make sure you use an updated list of repositories**: Get the latest list by typing "apt-get update" (apt-get update downloads the package lists from the repositories and "updates" them to get information on the newest versions of packages).
- **Make sure you have the latest PEM files**: Run "apt-get install ca-certificates". This package includes PEM files of CA certificates to allow SSL-based applications to check for the authenticity of SSL connection.
- **Make sure you have enough disk space in your temp drive**: Free some space by using "umount /tmp" in case there is not enough space. In general the LUCY installation requires at least 30 GB HD. Other hardware requirements are described here.

Can I run other applications on the same server?

It's highly recommended to install LUCY on a separate virtual or physical host (VPS or dedicated server) as LUCY's shell installer is pretty intrusive and may disrupt other custom software packages installed on the host. Make sure no other applications are running on that host which use same ports as LUCY (like a mail server running on 25 or a web server running on port 80).

What minimal packages are needed for the installer to work?

Make sure you have an updated repository list and the following packages installed:

- openssl
- ca-certificates

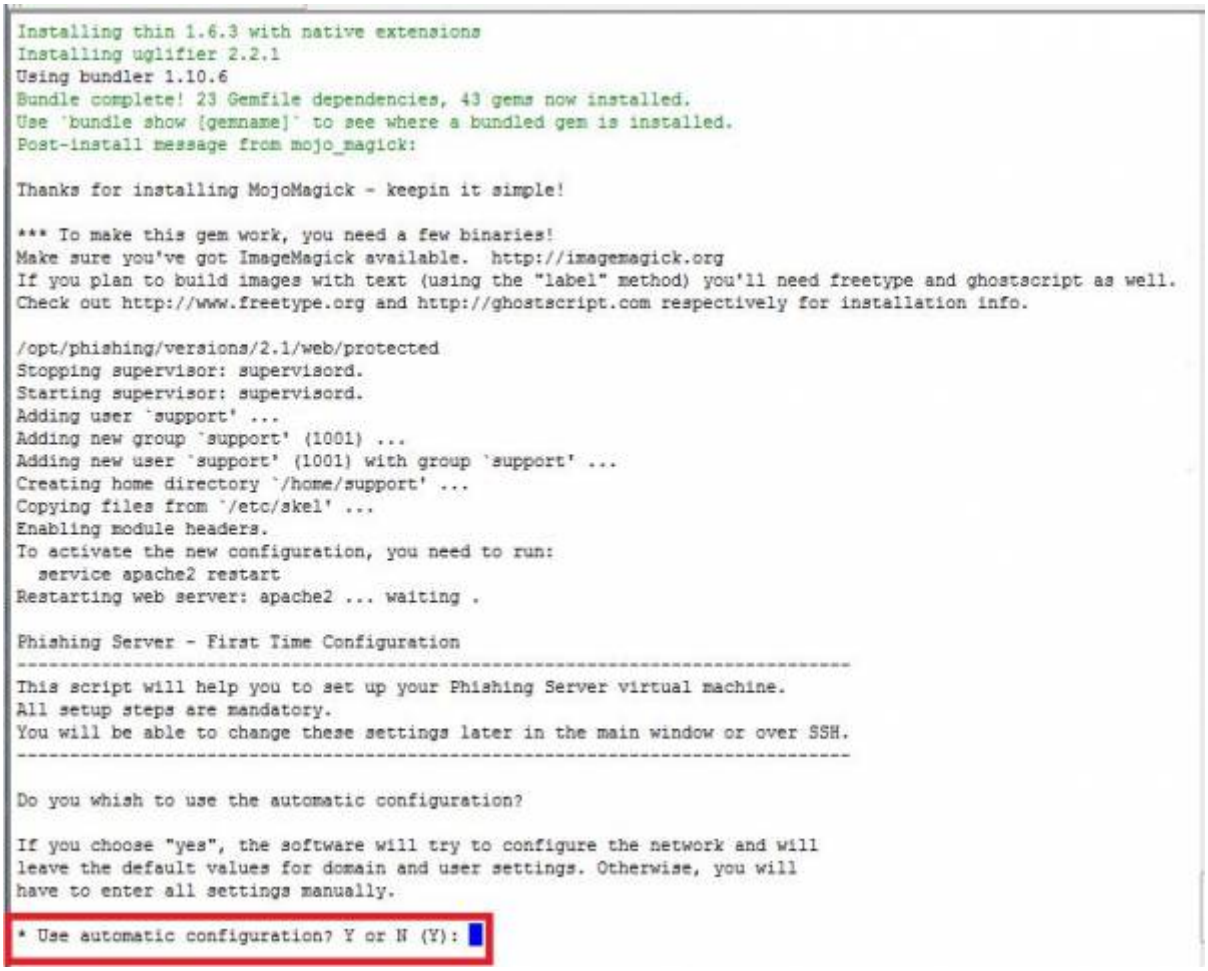
What are the hardware/Disk requirements?

- TMP: You will need at least 1 GB Space in the tmp directory. Please unmounts your tmp in case you need to free some space there (example: "umount /tmp")
- Other hardware requirements can be found here

Installation tutorial

1) First of all, download the file that you are going to execute e.g. "install.sh" from our download location (usually under http://phishing-server.com) and save it in your directory. If your using a terminal you first need to enumerate the current download link by pressing F12 in your browser when visiting our download section and then use **wget** to download the file (example: "wget http://download.phishing-server.com/dl/lucy-latest/install.sh"

2) Secondly, open the Terminal from Menu "Accessories \ Terminal".
3) Now type cd to the directory where you downloaded the file.
4) Then type chmod +x name_of_file.sh to make your file executable (example "**chmod +x install.sh**").
5) Now type ./name_of_file.sh to execute the file (Example "**./install.sh**"). If you are able to install LUCY without docker (this is the preferred method), please use the **"./install.sh legacy"** command.
6) You will be asked if you want to install LUCY (Install LUCY (y/n)?) Please type "**y**" and press enter. During the installation LUCY will connect to our centralized custom repository to download the necessary packages.
7) As soon as the installation is finished, the automatic setup script should start.



8) Login to LUCY with the Webbrowser. Continue the setup in the browser using the credentials provided in the setup script. If you want to install a commercial version, please provide us with the workstation ID.

9) Define your default mail delivery method in LUCY. In case you use the build in mail server: set the hostname for the mail server.

10) Setup a domain in LUCY. This domain can be used for phishing simulations (landing pages) or the elearning portal.

11) Create a trusted certificate for the administration of LUCY.

12) Create all the required administrators users in LUCY.

13) Download all the latest templates

14) Update LUCY to the latest version

15) Consider implementing additional security layers

16) Give LUCY a custom branding

17) Once you are all set you can try to setup your first campaign. If you experience issues with mail delivery (e.g. SPAM filtering), check out this chapter. If your test emails do not arrive at all, please consult this article.

Start the installation script manually after a successful installation

Execute the command
python /opt/phishing/current/tools/setup/setup.py

or in LUCY > 2.8:
docker exec -it lucy /bin/bash
python /opt/phishing/current/tools/setup/setup.py

Installation problem? Contact our support

In case you are planning to purchase LUCY or you are already a commercial client you can contact support@lucysecurity.com to open a ticket. We will get in touch with you within 24 hours.

Uninstall LUCY

In 3.2 we will provide an uninstaller. For now if you want to remove LUCY you first need to get a list of all packages installed using $awk '/^Selecting/ {gsub(/\./,""); print $5}' /var/log/apt/term.log (which displays installed packages in historical order, and then purges the last packages). That list will enable you to remove the according packages.

Frequently asked questions (FAQ)

Which components are installed with the installer script? What modifications are made to Linux OS by the installer?

When Lucy is installed as a docker image, it gets downloaded from https://hub.docker.com (you can search for Lucysecurity there) to internal docker storage that is managed by docker itself – as any

other usual docker image. Usually it's **/var/lib/docker/**. After that the installer launches the image with specific parameters, extracts a management script (that launches Lucy's console setup tool) to **/tmp/files**, moves it to **/usr/bin/lucy-setup.sh** and removes the **/tmp/files** folder. These are all changes that the docker-based installer does, all other software and files are within the container.

When installing Lucy in a "legacy" way (which is possible only for Debians, as the installer requires some Debian-specific packages and software versions), the installer adds around 500 new packages, does very deep system changes, including configuring the login shell, changing other services (postfix, apache, etc).

The installer checks if docker is installed and installs it from the official docker website. Are there any downsides of having docker engine pre-installed?

No, pre-installed docker engine is just fine and will work completely the same. Just make sure it will be updated on time.

Who patches the Docker Runtime and host Linux system when security vulnerabilities become known?

When using a Docker-based installation, the Docker engine and all packages on the host are managed by the host package management system – be it RHEL package management or Debian/Ubuntu APT. Lucy's docker container has no access to outer system and therefore cannot install any updates there. When using a "legacy" installation, all software packages are updated along with Lucy updates using Lucy's Debian mirrors.

How does Lucy update when it's running in Docker?

After installing a Docker container with Lucy, Docker's container system is not involved anymore - all updates are performed within the container using container's APT system with our custom package mirror.

Is the container included in the installer payload or is the container loaded via docker pull?

Lucy's container is downloaded from https://hub.docker.com (official Docker Hub) during installation.

When configuring proxy in Lucy, what software is affected?

In case of Docker installation, only software inside the container is affected. There are no

consequences for the software on the host system. When using a legacy installer, the proxy configured will be used as a default proxy for the whole Linux system.

How do you back up Lucy?

Speaking of Docker container installation, the backup is seamless and is a peace of cake. First of all you "commit" the container, making a static image of it with all files, changes, etc: **docker commit lucy lucy-backup** After that you:

- either save it as a tar file: **docker save -o /path/to/lucy-backup.tar lucy-backup**
- or export it to your private docker registry: **docker push lucy-backup**

The backup image can be recovered easily from file by **docker load -I /path/to/lucy-backup.tar** (in case of local file) or **docker pull lucy-backup** (in case of private docker registry)

After that you can start your container as a regular docker container with this command: **docker run –privileged -v /proc/sysrq-trigger:/sysrq -d -p 80:80 -p 443:443 -p 25:25 -p 5001:5001 –name lucy –restart=always lucy-backup /bin/bash /etc/run-services.sh**

Things get a bit more difficult in case of "legacy" installation - you should back up multiple directories, where configurations and files are stored:

- /opt/phishing
- /etc/
- /var/lib

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

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=installing_lucy_on_linux&rev=1539130643

Last update: **2019/07/25 12:51**