On-premise installation vs. installation in the cloud

Lucy can be installed on-premise or in the internet on any cloud server.

Reasons for installing on an external server in the internet are:

- **Public IP address outside your network range**: Prevents your infrastructure from being blacklisted.
- **Direct access**: The server will not be blocked by any security products already in place within your own infrastructure.
- **Less possible conflicts with integration**: A LUCY server placed directly in the internet will be setup very fast as it does not require a complex integration process with your mail, DNS and firewall infrastructure
- **Smaller attack surface**: As the LUCY server requires a web based access for end users from the internet (e.g. accessing their mails from mobile devices), you might need to punch a hole in your firewall and allow inbound access to a LUCY server. If you place LUCY in the intranet (see this chapter), your might violate your zone concept.

Reasons for installing LUCY on premises are:

- **Legal**: Some laws might not allow you to store sensitive data on an external server outside your network or outside your country. Especially with the new data protection law in Europe (GDPR) you need to make sure any personalized or sensitive data is secured.
- **Integration with certain features**: LUCY comes with different API's such as the LDAP API, the REST API etc. which are common for backend applications that are usually not exposed to the internet.
- **Security**: LUCY might store sensitive data like windows login, user names, emails etc. within the database. Integrating the LUCY server in the internal protection layers (IDS, FW etc.) will minimize the risks of successful attacks.

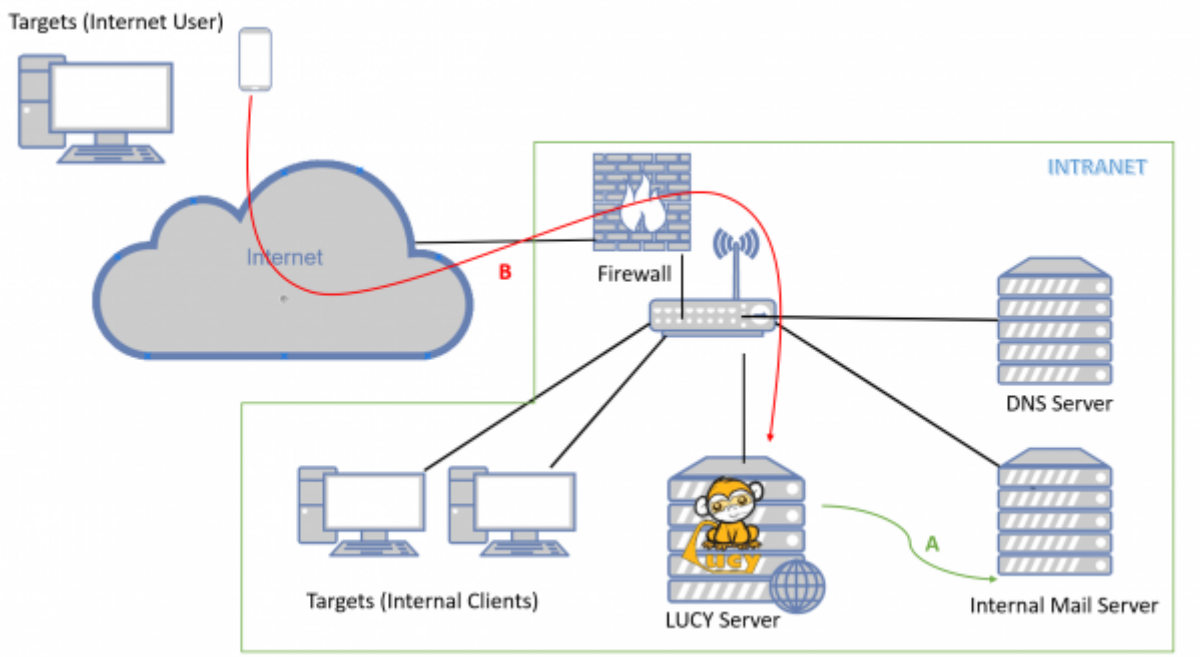
Where to place LUCY in an on-premise installation?

You can place LUCY in the intranet or within a secured zone (DMZ). If you want to allow external users (e.g. mobile users with smartphones) to access LUCY's websites (attack simulations or e-learning), an installation in the intranet is not recommended for security reasons. The web server would be directly accessible from the Internet. In case of a vulnerability in the system or application, an attacker would have direct access to the intranet via the LUCY server. In such a case you should install LUCY in a separate zone. In that case you could consider using one LUCY instance only as a reverse proxy in that zone, and install the main application within the intranet as a "master instance". This configuration is described here.

On premise installation technical checklist

- **Mail integration**: LUCY has different mail delivery methods. See this chapter. The main two mail delivery methods are using the build-in mail server or your own mail relay. The mail relay could be our internal mail server. Please keep in mind that in LUCY you can send two types of email: firstly, mails for the attack simulations. On the other hand mails for the awareness

training. Especially with mails for phishing simulations, the use of your own mail server can be viewed critically. When sending emails through your own mail server, the technically experienced recipient would see in the mail header that the email comes from the trustworthy internal server and can probably not be real phishing. Some organizations also classify the external emails with a special tag (e.g. "external email"). If this tag is missing because an internal mail server is used, the employees trust these emails and it is difficult to train them not to trust these emails. Therefore, when using the internal mail server, you should make sure that the emails look the same to the recipient as they do from the outside. But also using the build-in mail server comes with challenges: LUCY would need to be able to resolve the MX record (this is usually an external public IP which is not reachable form an internal network) for your own organisation and then deliver the mails to that server. Depending where LUCY is installed, you probably need to open the SMTP port or make sure, that LUCY knows (correct DNS record), where to send the emails.



- **DNS integration**. You can quickly setup new domains in LUCY. Details are described here. Those domains could be used for the landing pages (Phishing or E-learning) or the mail sender (awareness and attack simulation). The internal clients will need to resolve those domains. Therefore, you need to create the according DNS entries also on your internal DNS server and point the records to LUCY. If the landing pages need to be accessed from users in the internet directly (without VPN), you need to make sure that the DNS records are also created on an externally accessible DNS server.
- **Creating DNS records**. You will need two domain types in LUCY: Attack simulation domains and domains for your awareness training. The **attack simulation domain** could be used for your phishing website in your attack simulation. We recommend reserving first a generic domain like "cloud-services625.com". If you create a wildcard A-record for that domain, you can then use a matching subdomain. Let’s say you prepare a phishing simulation with some web-based email service. Using the subdomain "webmail" would give you the domain "webmail.cloud-services625.com" for the landing page. If you ask the user to download a file, you could use "download.cloud-services625.com" etc. If you want to do more sophisticated attacks you can reserve a typo squatted version of your own domain name. Typo squatting is a

technique of registering domain names which look similar to some legitimate domain name. For instance, given google.com, one example of typo squatting domain might be g00gle.com. You can use https://spoofing.lucysecurity.com to verify what variations of a domain name are available. You can use the domain from your landing page also for the email sender (like sender@cloud-services625.com). But as the sender email domain is a free text field that can be used with any domain name, it is not required to reserve a domain for just sending emails. There are some rules though when it comes to sending on behalf of other domain names: You can only use domain names that really exist. You can only use domain names that are not SPF protected (unless you white list them on your mail server). You can only use domains that also have an MX record. That means, you cannot use "@apple.com" as there is an SPF entry for this domain. You also cannot use "@this-does-not-exist.com". But you could use "@example.com" - a domain that exists, but is not protected. The website MX Toolbox helps you verifying if a MX or SPF record exists. **Awareness Website Domain**: Try to avoid using the same domain for attack simulations as for the awareness training. If possible, point a trusted domain record to LUCY like "training.your-domain.com" and send awareness emails using your own mail server as a relay in LUCY.

- **HTTP/HTTPS access for recipients**: The landing pages and the E-learning needs to be accessible via http or https (see this chapter for SSL configuration). If users from the internet have to access those pages, you need to make sure that you have set up an according port forwarding rule on your firewall together with a NAT entry, that points to LUCY.
- **HTTP/HTTPS access for LUCY:** LUCY needs to be able to connect to our update server "193.25.100.129 (update.phishing-server.com)". If you use a forwarding web proxy in your organisation, please make sure LUCY is configured to use that proxy (https://wiki.lucysecurity.com/doku.php?id=we_use_a_proxy_to_connect_to_the_internet).
- **Security products and whitelisting**: You need to ensure that the LUCY IP is whitelisted on all your security products (mainly the SPAM filters). Otherwise, you might end up blocking legitimate infrastructure elements within your own infrastructure.
- **Securing the access**: Once you finished the setup, you might want to prevent users from accessing the web based administration. In this chapter we discuss a few tips on how to secure LUCY.

On premise installation technical procedure

Hardware Please make sure you have the hardware ready with sufficient disk space (>200 GB) and memory (>4 GB). More details here: https://wiki.lucysecurity.com/doku.php?id=hardware

Download If you have decided to do an on premise installation you will first need to download LUCY from our webpage. Please choose one of our installers or images:

- **Virtual Box**: http://download.phishing-server.com/dl/lucy-latest/virtualbox.zip
- **Linux Installer**: http://download.phishing-server.com/dl/lucy-latest/install.sh
- **ESX/ESXi**: http://download.phishing-server.com/dl/lucy-latest/esxi.ova
- **Vmware Image**: http://download.phishing-server.com/dl/lucy-latest/vmware.zip
- **Amazon**: http://www.lucysecurity.com/PS/doc/dokuwiki/doku.php?id=installing_lucy_in_amazon

If you require a different format (e.g. ovf), search for the according converter (e.g. search for "convert ova to ovf"). All downloads are automatically treated as a community edition.

Installation Once downloaded, please install LUCY according to the download type:

- Installing LUCY on LINUX
- Installing LUCY in Virtualbox
- Installing LUCY in Vmware
- Installing LUCY in Amazon
- Installing LUCY on Windows
- Converting LUCY from VMware ESX to Hyper-V

Login Login to LUCY with the Webbrowser using the IP address of your server. Continue the setup in the browser using the credentials provided in the setup script. If you want to use a domain for your administration UI, Connect to your LUCY instance with the root or phishing account. If you connect as root, please execute the command python /opt/phishing/current/tools/setup/setup.py (if you have a docker based installation, execute: docker exec -it lucy /bin/bash and then press enter and execute python /opt/phishing/current/tools/setup/setup.py). Within the setup script menu please choose menu item "domain configuration" and set the domain for your admin UI here.

License: Please send us the workstation ID (http://www.lucysecurity.com/PS/doc/dokuwiki/doku.php?id=how_to_activate_lucy&s[]=#where_to_find_the_workstation_id).

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

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

SSL Setup Create a trusted certificate for the administration of LUCY.

User management Create all the required administrators users in LUCY.

Updating Download all of the latest templates. Update LUCY to the latest version

Hardening Consider implementing additional security layers

White Label Give LUCY a custom branding

Test campaign Once you are all set you can try to setup your first campaign

LUCY Vmware technical components

When you download and boot the VMware Image, all software components are integrated in that image. There is no need to install any additional software. All components (DB, mail server, web server etc,) are bundles within the VMware images and controlled by the internal LUCY software, which runs transparently in the background. The updating of those components is also done within the LUCY software through internal processes, which are not visible to the end user.