LUCY offers you to create a certificate for:

- Campaigns
- the Admin Interface

Trusted ADMIN Certificate Generation with LUCY > 3.1

First set the correct FQDN within the setup script (domain configuration). Example: if you configured the domain "phishig-server.com" within LUCY you could create the FQDN access.phishing-server.com within the setup script. If you want to generate a trusted certificate for the admin access please go to "settings/ssl settings" and choose "lets encrypt" as the method. LUCY will automatically use the domain configured in the system to generate the certificate. The certificate generation might take up to 5 minutes. Please be patient and wait until the message "certificate created" appears. If you get a "request failed" error it means that you ran into performance issues. In that case please retry to initialize the setup again. Here is a summary again:

- **Step 1:** create a DNS entry, that points to LUCY and which is reachable from the internet (LetsEncrypt needs to verify the domain in order to save the settings). E.g. create a DNS entry like admin.yourdomain.com that points to LUCY.
- **Step 2:** Start the setup script and go to the domain configuration. In the domain configuration please save your FQDN (e.g. admin.yourdomain.com).
- Step 3: Restart LUCY
- **Step 4:** Go to the settings/SSL settings menu, choose "letsencrypt" and let LUCY generate the trusted certificate. If the page is not refreshing automatically: please refresh the page after max 5 minutes.

Lucy Campaigns I	Recipients Sessions	Settings 👻	Support 🗸	Status	Account	Logout
Home / SSL Settings		Scenario Te Awareness	Templates			
SSL Settin	gs	File Templa Not Found	Template			
	Vse Custom SSL Ce	Download T	emplates			
SSL Provider	Generate Or Upload	Benchmark	Sectors			- 6
	Please select Generate Or Upload Let's Encrypt	opdate				
SSL Certificate	Durchsuchen K	Reboot SSH Passw	ord			
SSL Key	Durchsuchen K	Domains				
SSL Key Password		Dynamic DN	IS			6
SSL Chain	Durchsuchen K	Clients Users				6
	Save	Mail Setting				
Copyright © 2016 Lucy Phi	shing GmbH	SSL Setting				
All Rights Reserved		Advanced 9	offings			

Using SSL for attack simulations or awareness training

• **SSL for attack simulations:** You have the option to generate a certificate or upload one. If you want the certificate to be trusted to avoid an SSL error message please pick "lets encrypt". Please go to the scenario settings within the base settings of your campaign and then click on "SSL settings" (1). In case of LetsEncrypt (2) it will automatically use the domain (3) configured within the scenario settings. You can enter a valid email address (4) in the last field. Please note, that "Let's Encrypt" needs a publicly available domain name to generate a certificate. Please make sure your domain is accessible and points to Lucy.

	Login & Ma… ≦	enario Status: Not Started	•	
	Summary Scenario Settings		Use Custom SSL Certificate If this is not checked, visiting the scenario landing page will clear th out.	e authentication cookie and you will be logged
1	Mail Settings SSL Settings	SSL Provider	Lef's Encrypt	• 2
	Landing Page Template Message Template	Domain	office365 cloudspace365 solutions Let's Encrypt needs a publicity available domain name to generate	✓ 3
	Errors		a certificate. Please make sure your domain is accessible and points to Lucy.	
		E-mail		4
			Save	

• **SSL for E-Learning:** Please gp to "awareness settings" within your campaign and then within the according scenario settings of your awareness template select the SSL options:

SL Settings	Campaign Status: Not	Started
Base Settings Website	SSL Provider	✓ Use Custom SSL Certificate ● Let's Encrypt •
SSL Settings Certificate Message	Domain	 Enable Domain Checking Ims.cloudspace365.solutions Let's Encrypt needs a publicly available domain name to generate a certificate. Please make sure your domain is accessible and points to Lucy.

• Link generation within the message template:: If you enable SSL in your campaign scenario, LUCY will populate the %link% variable with "https://domain-in-scenario-settings" instead of "http://domain-in-scenario-settings"

Delete/renew certificates

Deleting certificates requires you to uncheck the certificate checkbox and save the changes:

Home / SSL Settings	
SSL Setting	gs
	Use Custom SSL Certificate
	Save

Create a Certificate within a Campaign LUCY < 3.1

If you decide to use SSL for the campaign and you want to generate a custom certificate you can do this by clicking Generate CSR or Certificate.

	C Generate CSR or Certificate	
SSL Certificate		Browse
SSL Key	Γ	Browse
SSL Key Password		
Password		

===== Create a CSR (Certificate Signing Request) ====="

If you want to create a new official certificate, you first need to create a CSR. You can use an online service like:

- https://tools.ssl.com/
- https://www.thesslstore.com/ssltools/csr-generator.php
- https://www.gogetssl.com/online-csr-generator/

After the verification, (most providers will either do a verification by sending an email to the email address within the WHOIS record or to the email specified within the CSR) you will have to upload the certificate to LUCY.

As an alternative: LUCY enables you to create a CSR by clicking "Generate CSR or Certificate".

Import Certificate

You can also import an official trusted certificate. Simply upload the files to LUCY. If the private key is protected with a password, you need to enter that password as well.

Note that the server only accepts files with the following extension:

- SSL Certificate: crt
- SSL Key: key
- SSL Chain: crt, ca, ca-bundle

SSL Certificate		Browse
SSL Key	ſ	Browse
SSL Key Password		•
SSL Chain	P	Browse

Note: If you want to get an official certificate for free, you can always use trial certificates which are valid for 90 days (example :

https://www.comodo.com/e-commerce/ssl-certificates/free-ssl-certificate.php)

Known Issues

In LUCY < 4.5 the certificate autorenew might not work for several reasons.

a. If you are using <u>Lucy 4.2 or older</u> version and using the "**Let's Encrypt**" provider SSL certificate generation fails, you need to delete the old certificate before re-creating the certificate again. You can do that using the following command:

```
cd /tmp
sudo -u postgres psql phishing -c "UPDATE domains_ssl SET is_deleted=TRUE
WHERE NOT is_deleted"
```

(!) Please take into account that the command above will delete **all** existing SSL certificates!

b. For Lucy <u>4.3 and newer version</u> this could have happened after the migration from the version 4.2 via the Migration Tool. In that case please contact our support team (support@lucysecurity.com) to fix the issue.

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

Permanent link: https://wiki.lucysecurity.com/doku.php?id=ssl_configuration&rev=1544596546

Last update: 2019/07/25 12:50

