

S/MIME Certificate

Lucy emails (both attack and awareness) can be sent digitally signed using S/MIME method. Lucy can generate digital signature file or use the certificate issued by internal CA.

In order to enable S/MIME signature simply proceed to the Mail Settings within the scenario (Attack Settings or Awareness Settings). Check the **Use S/MIME Certificate** checkbox and upload the certificate file and key file. Click **Save**. Emails sent within this scenario will be delivered with digital signature.

Mail Settings Scenario Status: Running

Scenario Settings

- Mail Settings
- SSL Settings
- Bound Awareness Scenarios
- Landing Page Template
- Message Template
- Errors

Delivery Method Use System Settings

☒ Use S/MIME Certificate

[Generate Certificate](#)

SSL Certificate [Choose File](#) No file chosen
server.crt

SSL Key [Choose File](#) No file chosen
server.key

SSL Key Password

SSL Chain [Choose File](#) No file chosen

[Save](#)

Also, Lucy can create self-signed S/MIME certificates that can be also added to the emails. Simply press the **Generate Certificate** button and fill out the required fields according to the scenario. Click **Generate** and **Save**.

Generate S/MIME self-signed Certificate ×

Email *

Country * **State *** **City ***

Organization Name * **Organization Unit ***

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

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=s_mime_certificate

Last update: **2021/03/05 23:20**

