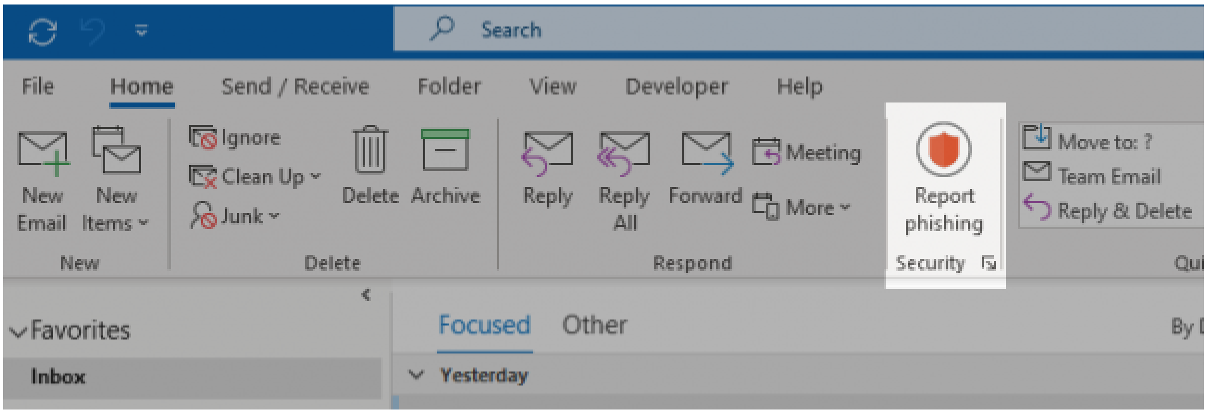
Screener MSI Plugin

The screener comes with the Report Plugin.
It supports Desktop Outlook application.

The MSI plugin is supposed to be used for desktop installations of the office mail clients listed below:

- Outlook 2010,
- Outlook 2013
- Outlook 2016
- Outlook 2019

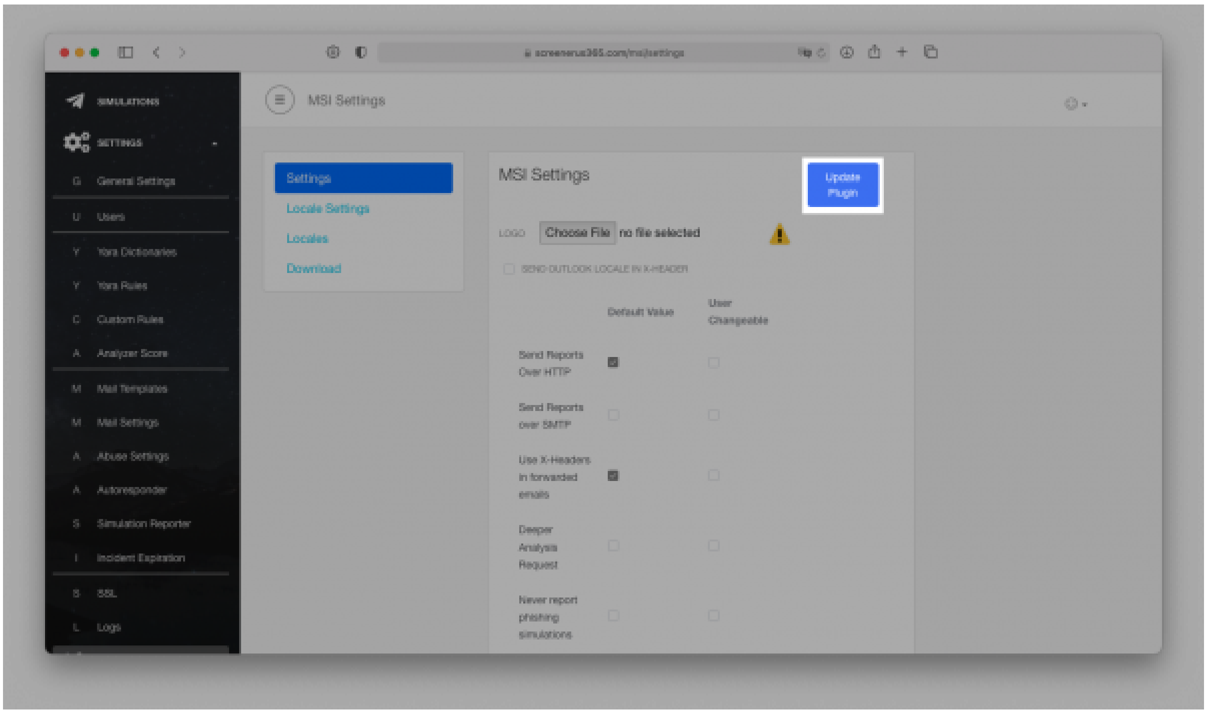
This add-in gives your users a safe way to forward suspected Emails with only one click and have them analyzed automatically by Screener. The tool empowers users to proactively participate in an organization’s security program and makes it easy for your employees to report any suspicious email they receive. It has two main features



a) Forward the mail (.msg or .eml) to a predefined mail address (e.g. your security team). Within the plugin, you have the ability to define a custom message that appears to the user after the mail gets reported. Once the message gets forwarded to your team, it will automatically be deleted from the user's inbox to prevent future exposure.
b) Report back to Screener: the plugin may forward suspected phishing emails as well Screener generated emails back to the Screener server via HTTPS or SMTP. If the mail was generated by LUCY, the reports will be automatically identified as phishing simulation. All other emails can be analyzed in Screener automatically at first, then by a Screener user.

Update

Go to the Plugins → MSI → Settings and press the "Update" button.



MSI Settings

LOGO Choose File no file selected

☐ SEND OUTLOOK LOCALE IN X-HEADER

	Default Value	User Changeable
Send Reports Over HTTP	☑	☐
Send Reports over SMTP	☐	☐
Use X-Headers in forwarded emails	☑	☐
Deeper Analysis Request	☐	☐
Never report phishing simulations	☐	☐

To download the latest version of MSI there should be a network connection between the Screener host and update.phishing-server.com.
The procedure will update the plugin inside of Screener. To update it on the users workstations it is necessary to re-download it from the Screener and re-deploy across the workstations.

Configuration

The configuration of the MSI plugin and phishing events is done within Plugin → MSI Menu.
There are 4 submenus, such as:

- Settings
- Locale Settings
- Locales
- Download

You can make multiple configurations and use them for different customers or organizational units. Please create a configuration, save it and download the corresponding plugin. You can repeat this step as often as you like for other organizations.

Settings

Setting Name	Description
Logo (ico)	Choose an icon for visual representation of plugin's button in the Outlook MSI interface. Once it has been picked up there is a preview and an option to delete icon.
Send Outlook Locale in X-Header	TBD
Send Reports Over HTTP	Enable this option if you want the Outlook Plugin to send a copy of the reported phishing mail to Screener (does not include emails from phishing simulations)

Setting Name	Description
Send Reports over SMTP	Enable this option if you want to forward the mail to the predefined mail address via SMTP. If enabled, the plugin will send the report to the email you provided on the same page. That is supposed to be your own email or the email of your security team. Please do not use this method at the same time with HTTP to send reports to Screener, if you do not want to have duplicated reports. Only pick one delivery method.
Send Reports over SMTP	Enable this option if you want to forward the mail to the predefined mail address via SMTP. If enabled, the plugin will send the report to the email you provided on the same page. That is supposed to be your own email or the email of your security team. Please do not use this method at the same time with HTTP to send reports to Screener, if you do not want to have duplicated reports. Only pick one delivery method.
Use X-Headers in forwarded emails	If true, the plugin will make the following changes in the email forwarded over SMTP: * Add a new header X-CI-Report: True * Add an HTML code <p>X-CI-Report: True</p> after the body tag within the email body.
Deeper Analysis Request	If true, the plugin will ask the user whether to request a deeper analysis of the reported phishing mail.
Never report phishing simulations	No reports will be sent over HTTP if a user reports a simulation email generated by Lucy. So the plugin will send only "real phishing" emails over HTTP.
Send phishing simulation over HTTP	If the option is enabled, the plugin will send reports regarding phishing simulations to Screener via HTTP.
Delete reported email	Set this action option and the plugin will delete the reported emails.
Inline Message Forwarding	If true, the plugin will clear the body of the forwarded email when sending the report via SMTP.
Send reported mail attachment in EML format	Reported email message will be sent as an *.eml attachment.
Disable Autoresponder For Reports	If true, Screener will not send an automatic email to a user as a reaction to report.
Enable Comment to Deeper Analysis Request	If Deeper Analysis Request is true, the plugin will offer to the user an additional text box where the user can type any comment to the deeper analysis request. Additionally, the user can configure a custom text that will appear instead of "Yes" or "NO" labels on the buttons
User External IP	Enable this feature if the Screener is used publically. In case if the domain name is set, it'll appear here. If disabled, the Screener will listen to a local interface. Use this if Screener is used in Intranet
Port for Report	By default, Screener Listen the 443 port to receive reports over HTTP
Report Email	External Email address that should receive reports to.
Move reported email to Junk E-mail of the current user	Set this action option and the plugin will move reported email to Junk E-mail of the current user.
Move reported email to non-system folder named	Set this option and the plugin will move reported emails to the custom-named folder. Type in the folder name in the field below.

Locale Settings

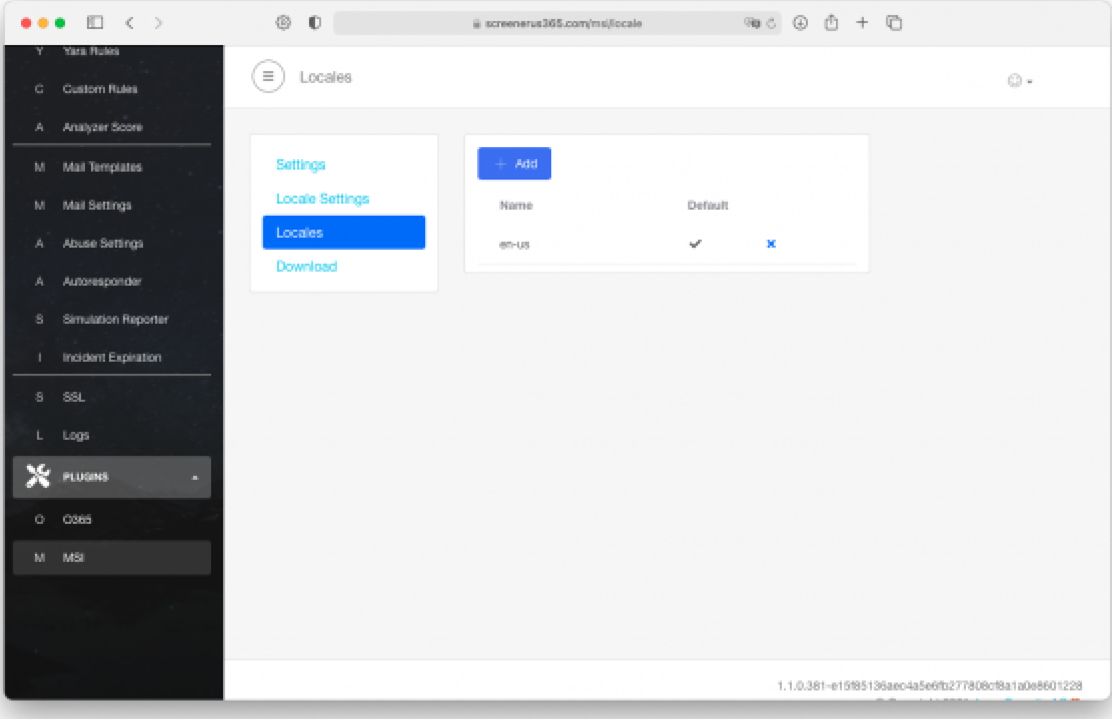
Setting Name	Description
Locale Settings	Pick the Locale that you would like to configure
Settings Title	TBD

Setting Name	**Description**
Ribbon Label	The name of the area in which the button is located.
Button Message	The name of the button in Outlook.
Button Super Tip	The help text displayed when the user hovers the mouse over the button.
Report Title	The title of the message that will be displayed after the user marks a suspected phishing email and clicks the plugin button.
Error Title	The title of the message that will be displayed when any error occurs.
User Request Message	The message that will be displayed after the user marks a suspected phishing email and clicks the plugin button.
Deeper Analysis Request Message	Deeper analysis request confirmation text. This message box is shown after user clicks on the report button.
No Selection Message	The title of the message that will be displayed after the user clicks phish button without any selected email.
Thank you message for Lucy mails	The message that will be displayed for all emails, that are created by Lucy within a simulated phishing campaign.
Thank you message	The message that will be displayed after the user marks a suspected phishing email and pushed the plugin button.
Eval Error Message	Text displayed when the error of getting the selected item occurs.
Send Error Message	The message that will be displayed when an issue with sending the report occurs.
Unsupported Message	Text displayed when user tries to report an unsupported item (calendar event, etc).
Subject	The subject of the forwarded email message when sending a report over SMTP. You may use %subject% variable to insert the subject of the phishing email. Example: Phish Alert %subject%.
Local Analyze Button	TBD
Remote Analyze Button	TBD
Reset Confirmation Title	TBD
Reset Confirmation Message	TBD
Error Super Tip	TBD
For "Yes" action	Set the Deeper Analysis Request Custom Button for "Yes" action.
For "No" action	Set the Deeper Analysis Request Custom Button for "No" action.

Locales

This menu allows adding custom locales. By default there is only en-us locale.
Below are some examples of additional locales:

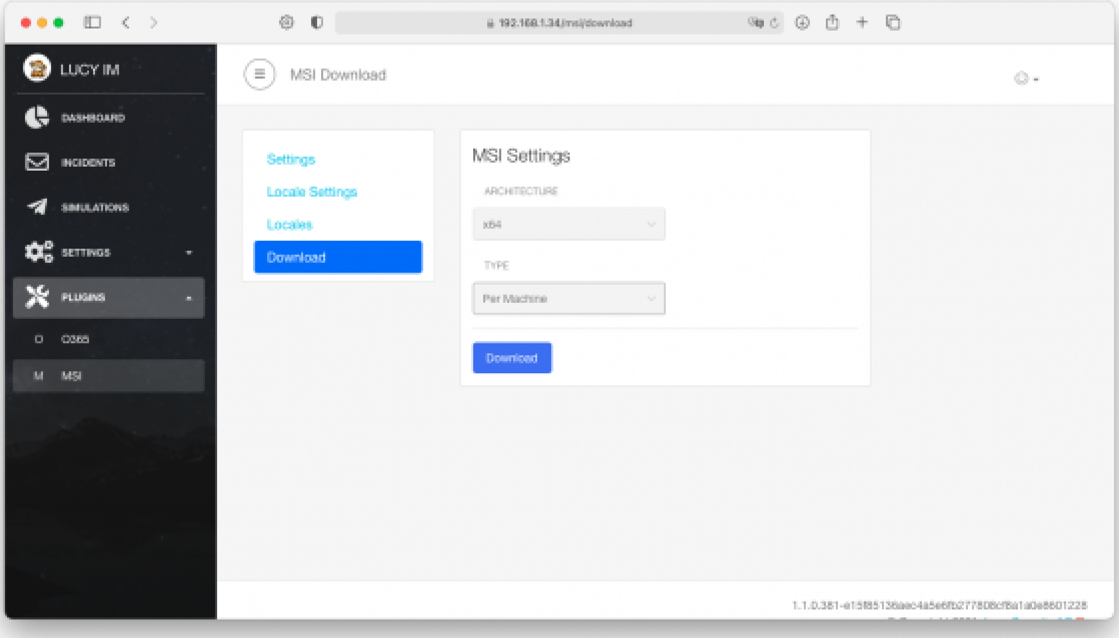
- de-de - German
- es-es - Spanish
- ar-ae - Arabic Emirates
- fr-fr - French



Name	Default	
en-us	✓	✗

Download

This page allows downloading the MSI plugin.
Select architecture (x86\x64) and the type(Per User/Per Machine), then press the download button.



ARCHITECTURE: x64

TYPE: Per Machine

Once you configured the plugin in the Screener UI and install it, you will notice that the settings can be viewed or changed locally. However in order to be able to change it, first turn on the settings in the Screener's plugin settings.

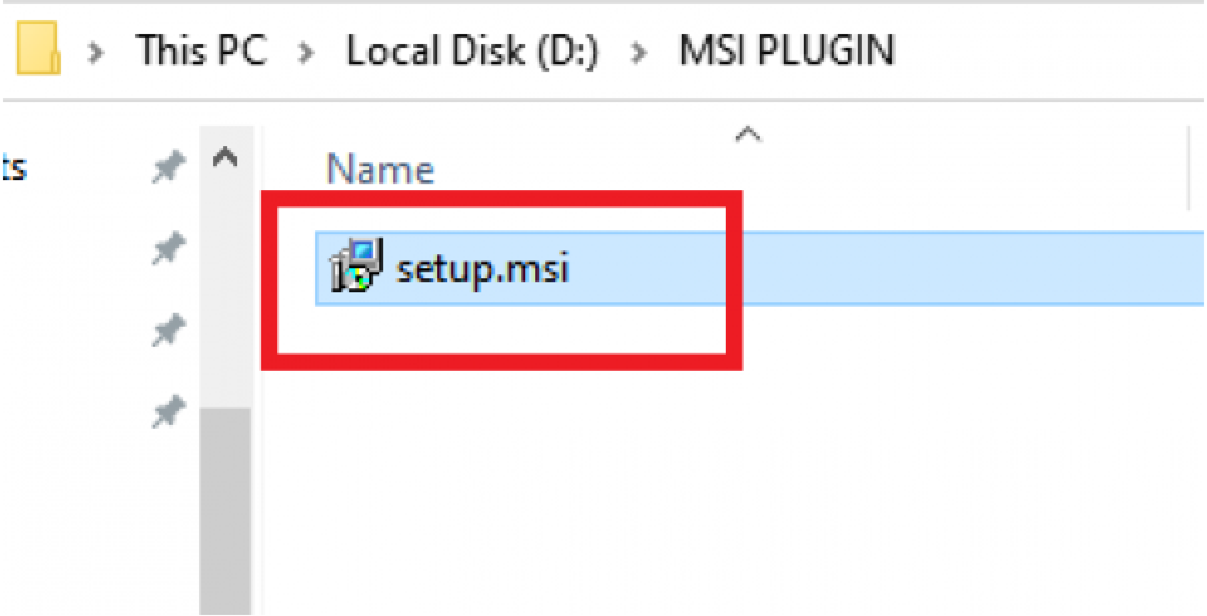
The screener always listens to port 25 (SMTP). It accepts every email message that comes in.

This can not be deactivated in the plugin settings. For this scheme to work, there should be an MX record pointing to the screener.

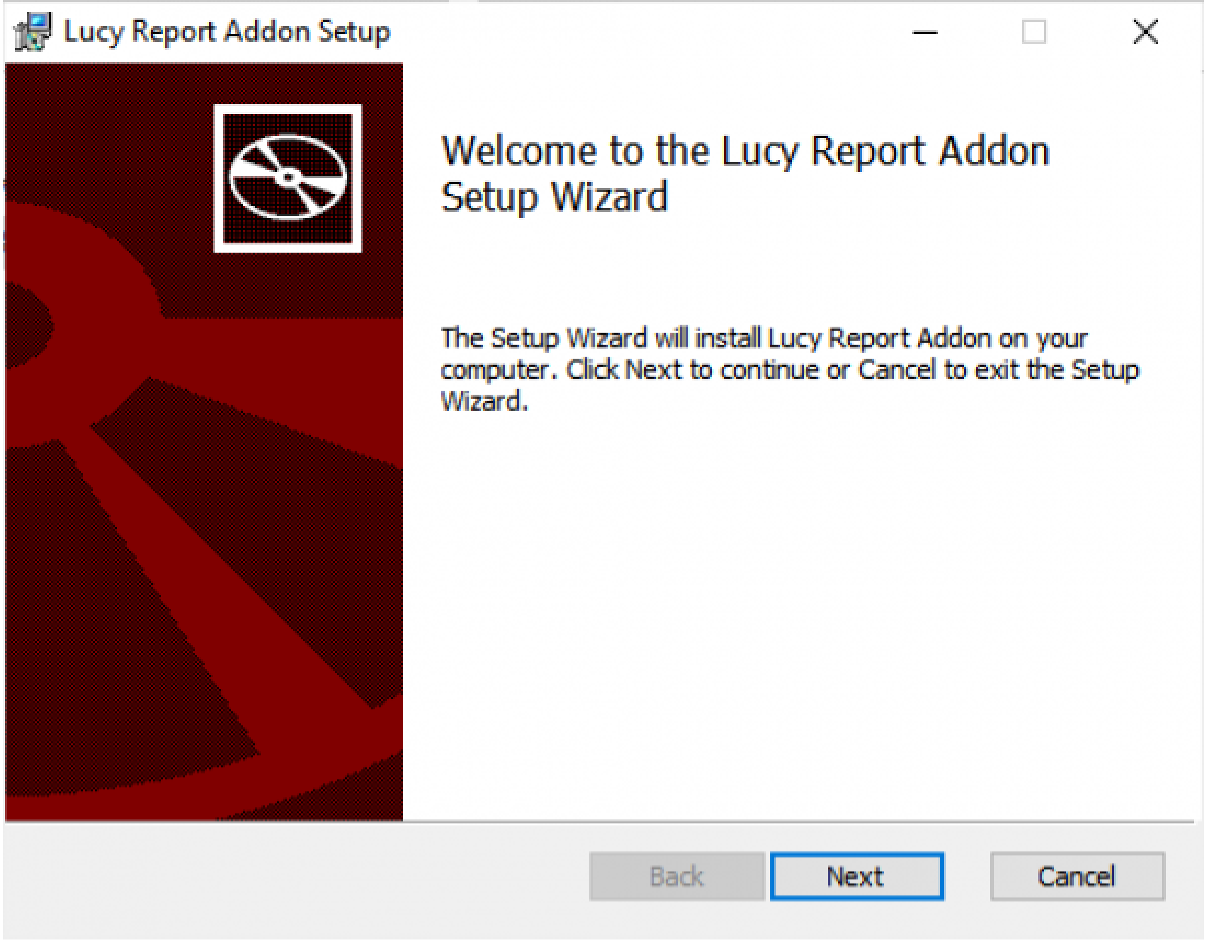
Deployment of the MSI Plugin

The plugin installer needs user to have read and write access at least to keys under HKCU (per user). User Wide plugin will affect only one user of a particular PC. Machine Wide plugin will be available for every user of a PC once it is installed.

Step 1
Download the plugin from the Download menu. Run it.



Step 2
See the welcome screen. Press "Next"

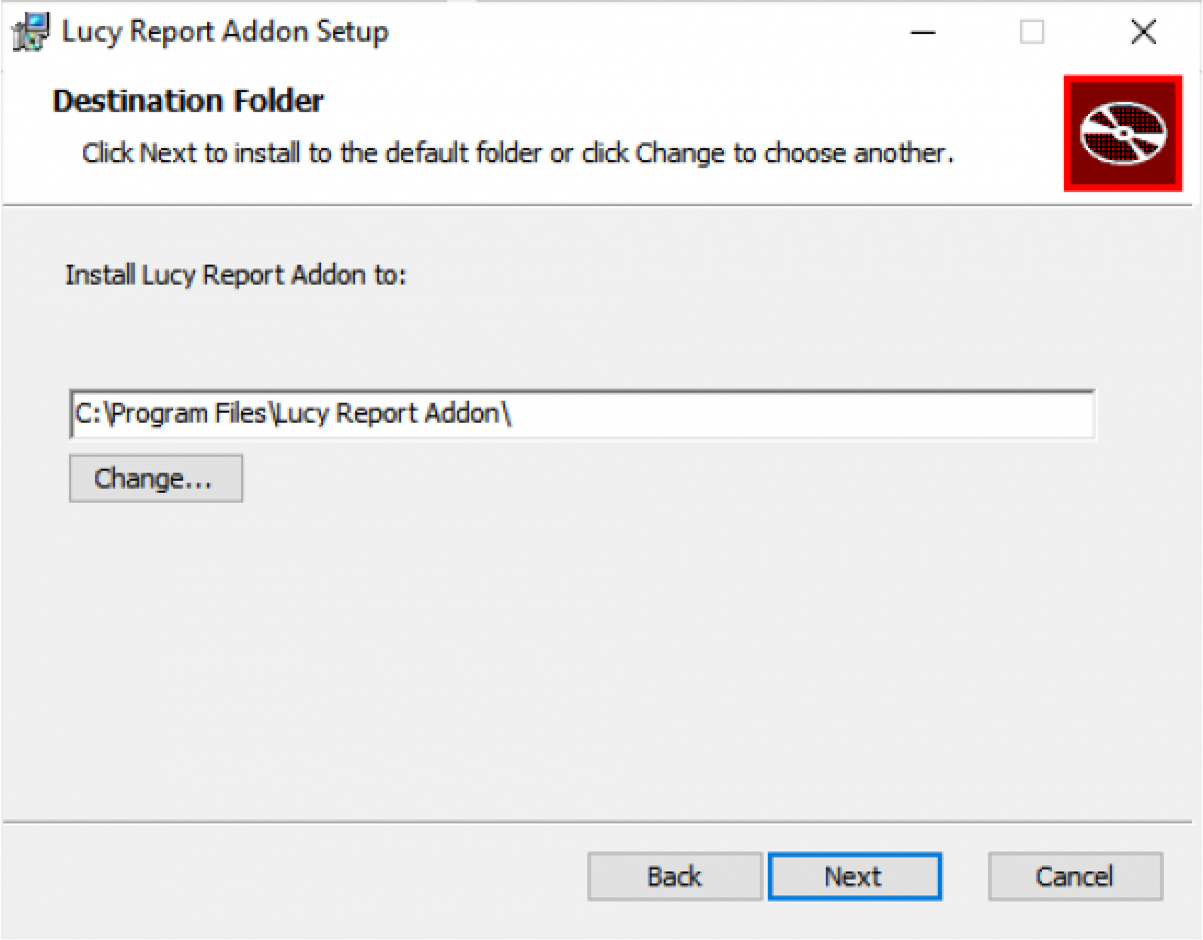


Welcome to the Lucy Report Addon Setup Wizard

The Setup Wizard will install Lucy Report Addon on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

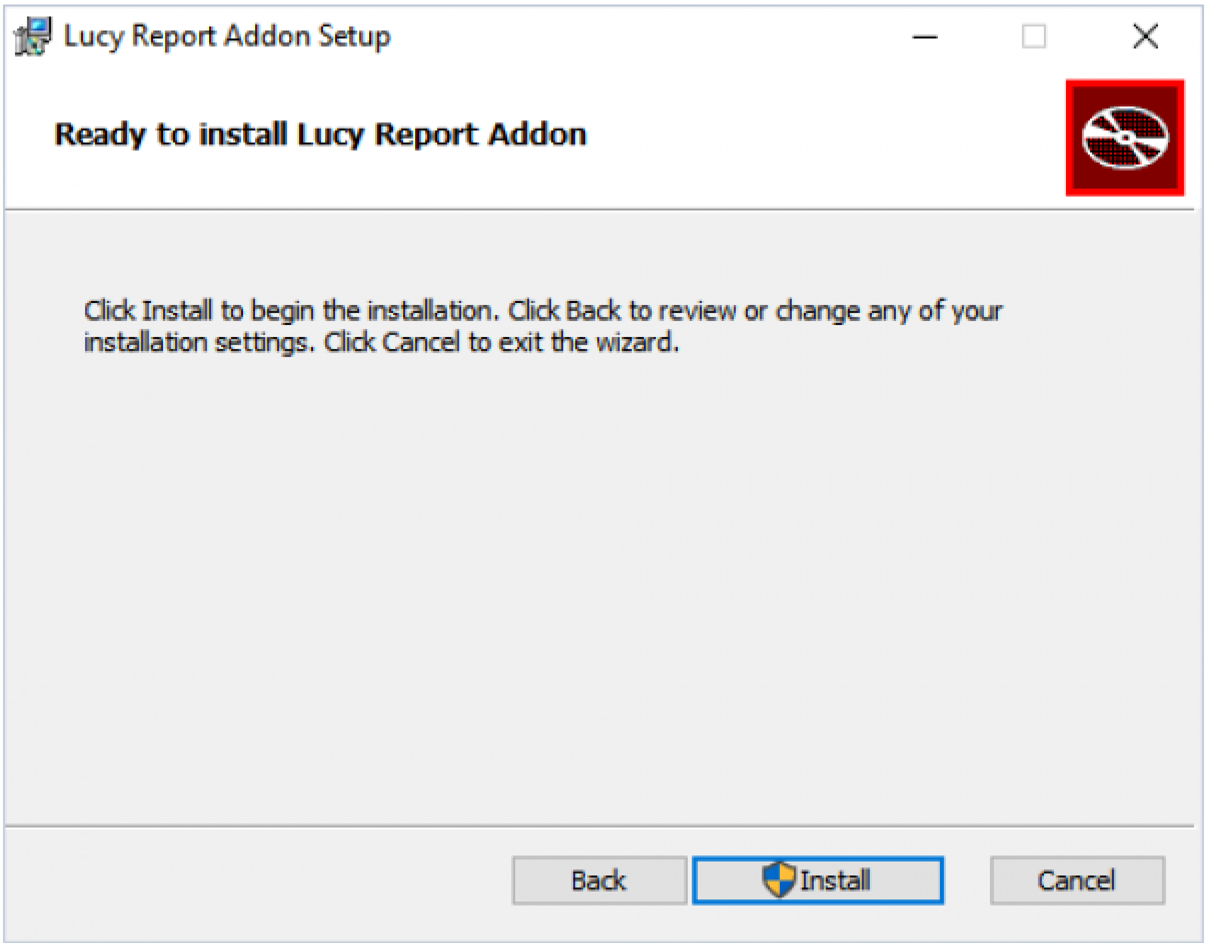
Step 3

Set the Installation Path. Press "Next".


Lucy Report Addon Setup
Destination Folder
Click Next to install to the default folder or click Change to choose another.
Install Lucy Report Addon to:
C:\Program Files\Lucy Report Addon\
Change...
Back
Next
Cancel

Step 4

Ready to install. Press "Install". Administrator rights might be required.

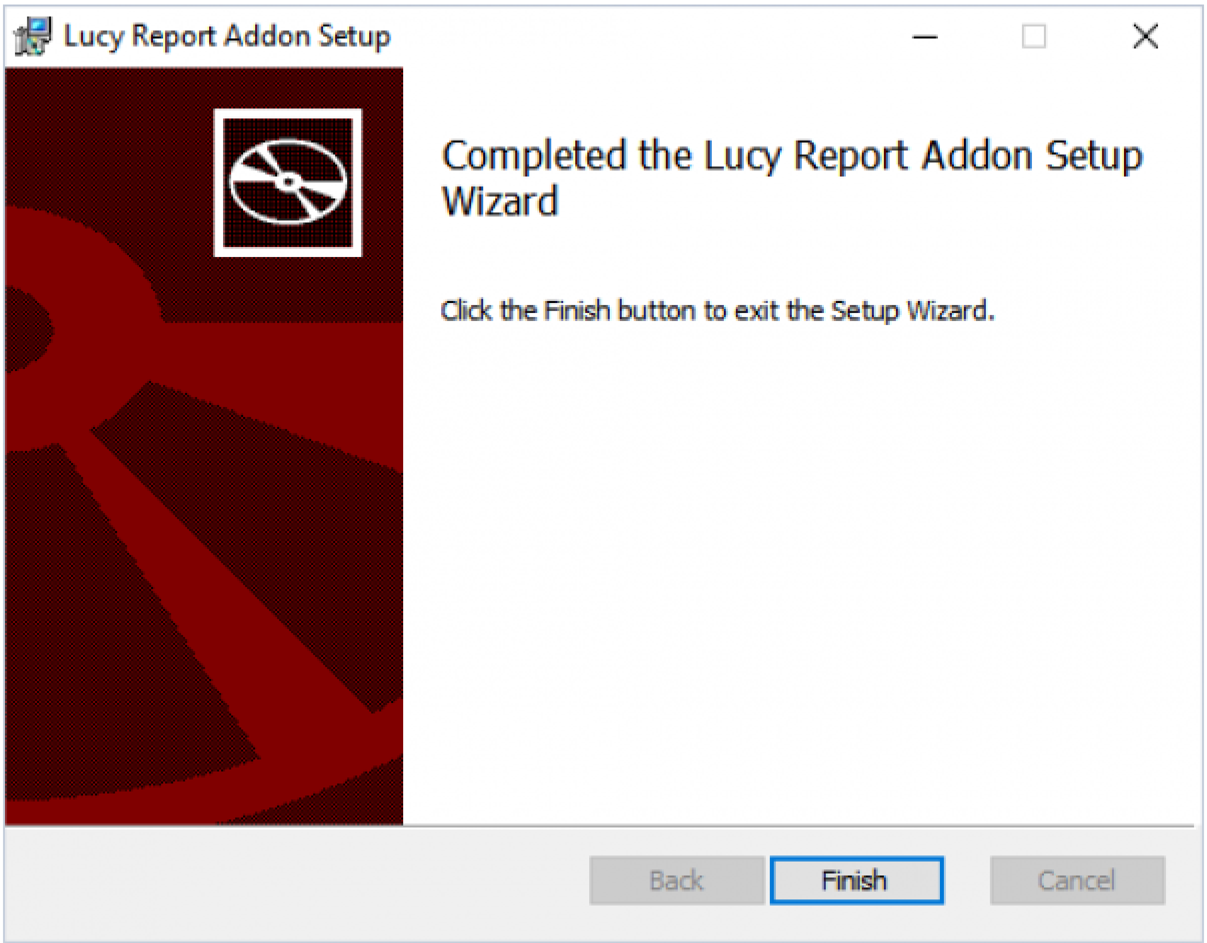


Ready to install Lucy Report Addon

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Step 5

Installation Complete. Press the "Finish" button.



Completed the Lucy Report Addon Setup Wizard

Click the Finish button to exit the Setup Wizard.

Upon installation, a temporary config.dat file is created. But all settings are written in the registry and can therefore be controlled via GPO. The plugin may be installed in the user context HKCU or in machine context (to HKLM).

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

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

Last update: **2021/04/27 18:58**