



Smartlockr

User manual

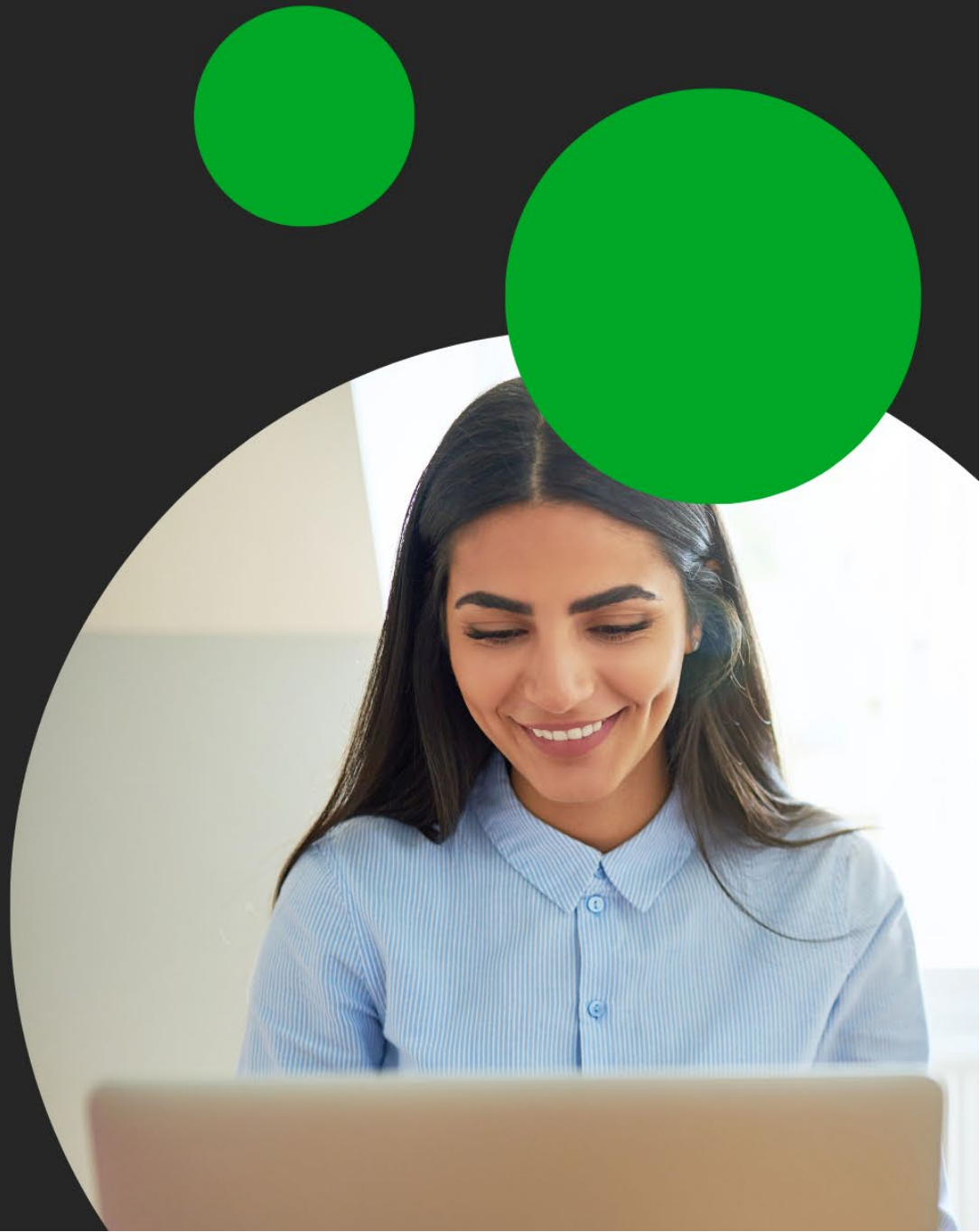


Table of contents

Introduction	4
1. Using the Smartlockr plug-in	5
1.1 Using Smartlockr the manual way.....	5
1.1.1 Choose your message type via the Smartlockr button.....	6
1.1.2 Using the Smartlockr slider button.....	6
1.2 Using Smartlockr the automatic way.....	8
1.3 Notifications.....	9
2. Sending files and messages securely	10
2.1 Public files.....	11
2.2 Secure files.....	13
2.3 Secure message.....	14
2.4 File settings.....	15
3. Multi-factor authentication	16
3.1 One-factor authentication	16
3.2 Two-factor authentication.....	20
4. Confirming attachments and recipients.....	23
5. Tracking and blocking.....	25
5.1 Tracking sent emails.....	25
5.2 Blocking emails.....	26
5.2.1 Blocking files.....	26
5.2.2 Blocking recipients.....	27
5.2.3 Blocking an entire email.....	28
6. Requesting files	29
6.1 Secure upload request.....	29

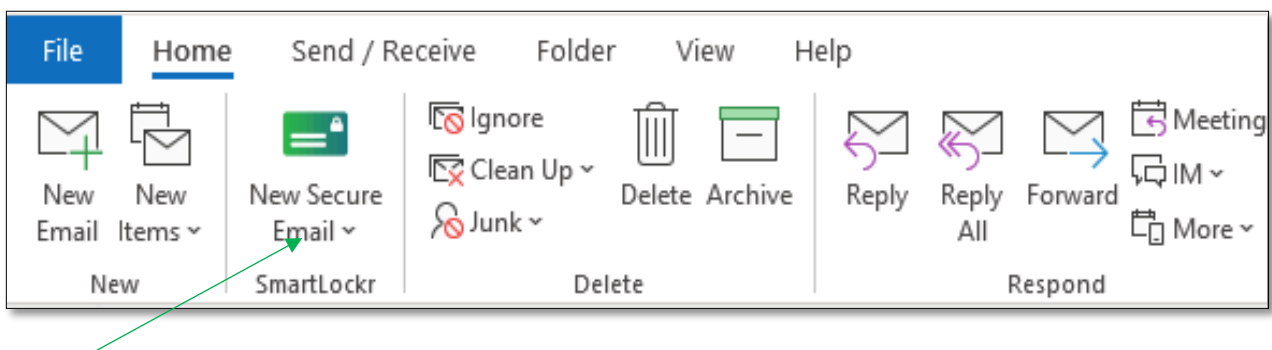
6.1.1 Secure upload request for the recipient.....	30
6.1.2 After your recipient has uploaded the file.....	32
6.2 Secure upload portals.....	33
6.2.1 To send a file via an upload portal.....	34
6.2.2 Secure upload portals for the recipient.....	35
7. What Smartlockr looks like for your recipient	36
7.1 Receiving a Public file through Smartlockr	36
7.2 Receiving Secure files and Secure messages through Smartlockr.....	37
8. You made it!.....	42

Introduction

Starting today, you and your data can count on the best possible security, because after reading this manual:

- you no longer have to worry about your data being compromised;
- you can safely send and receive files of any size;
- you will automatically comply with all rules and regulations concerning data and privacy.

All of this is possible through the *Smartlockr Intelligent Data Protection Platform*, which you can (or soon will) recognize by this new green button in your Outlook:



This user manual shows you how the Smartlockr plug-in for Outlook works. After reading this document, you will know how to use all the different functions, as well as what secure messages from Smartlockr looks like for the recipient.

Welcome to Smartlockr!

Our purpose is to create a carefree worklife for you and everyone around you. We do this by making safe emailing as easy as possible, so you can focus on your job!

We hope this manual shows you how easy it can be to protect your data. Should you have any questions though, you can always ask them to the system administrator within your organization, the IT-department or have them reach out to our [support team](#).

01. Using the Smartlockr Plug-in

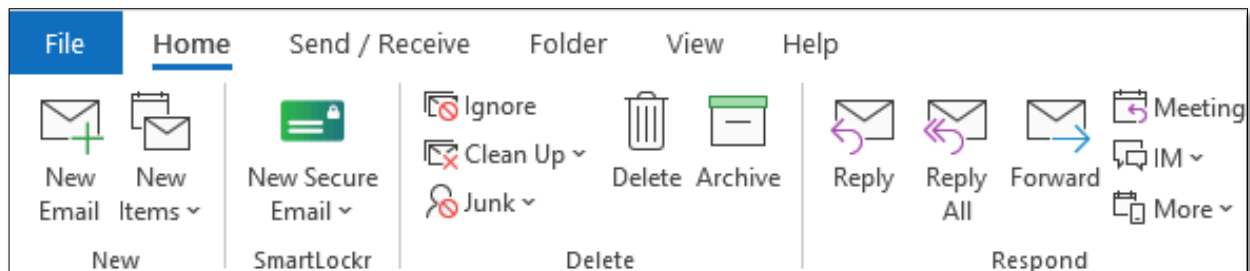
After installing the plug-in, you will notice the green Smartlockr button in the Outlook toolbar. There are two different ways of using Smartlockr: the manual or the automatic way.

1. Using Smartlockr manually means clicking the Smartlockr button and choosing which type of security you want to apply to your email.
2. Using Smartlockr automatically lets us take care of the security for you, with the help of a content filter and automatic notifications! Nice, right?

1.1 Using Smartlockr the manual way

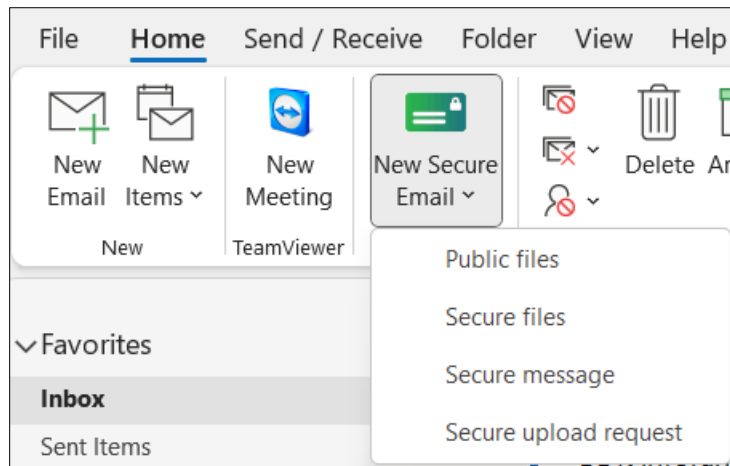
Using Smartlockr manually is easy. Simply click the green button in Outlook and choose the option that fits your needs. You can also turn Smartlockr on manually while writing an email. Below you can see what this looks like in Outlook.

Smartlockr button in the Outlook toolbar:



1.1.1 Choose your message type via the Smartlockr button

Step 1: Click on the Smartlockr button and select the message type you would like (please see 'Chapter 2: Sending messages and files securely' for an explanation of the different types).

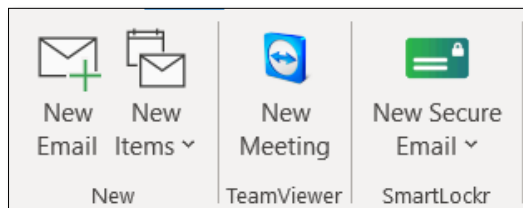


Step 2: Write your email and/or attach your file.

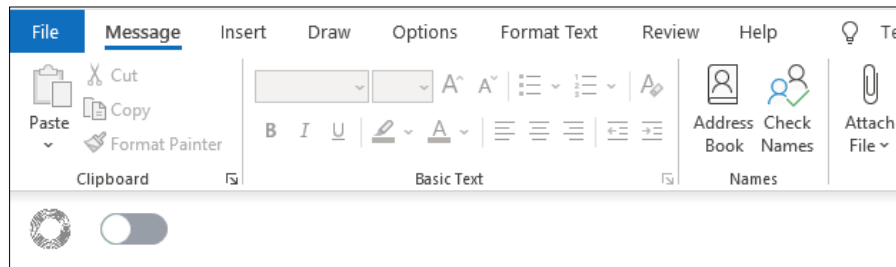
1.1.2 Using the Smartlockr slider button

You can also turn on Smartlockr at any time when writing an email, without preselecting your preferred option.

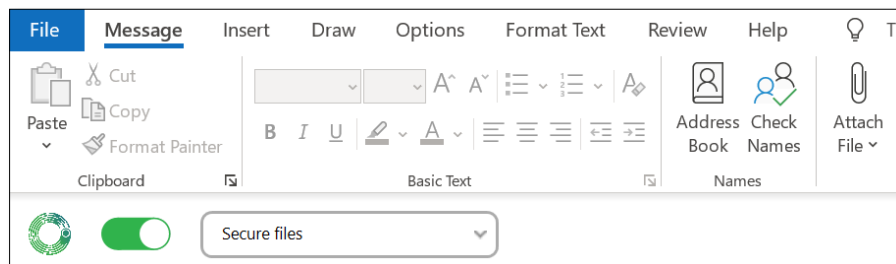
Step 1: Click on 'New email' in the Outlook toolbar.



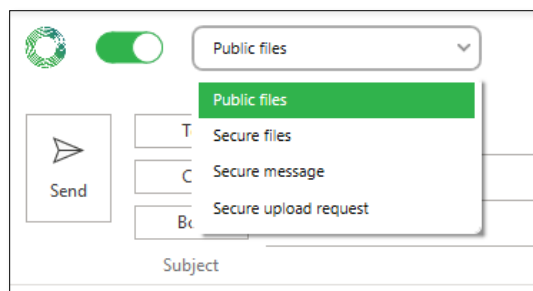
Step 2: In the top left corner you will see a Smartlockr logo with a slider button in grey. To activate Smartlockr simply slide the button to the right.



Step 3: When Smartlockr is activated, the color will change to green.



Step 4: You can also select the message type and security level before sending your email. Please see '*Chapter 2: Sending messages and files securely*' for an explanation of each option.



1.2 Using Smartlockr the automatic way

Using Smartlockr automatically helps you protect sensitive data and catch small mistakes that could easily be missed. When installing Smartlockr, your administrator can choose to apply a content filter. This content filter includes trigger words meant to scope out sensitive data like 'social security number' or 'address'. With a content filter, Smartlockr will recognize the trigger words in your emails or attachments and apply the right security automatically. Based on your organization's configurations, one of three things will happen:

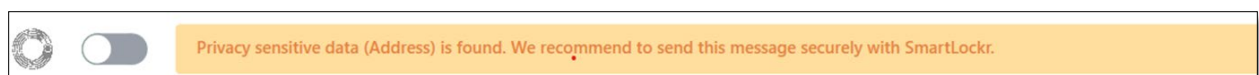
1. You will get a message, notifying you that sensitive information has been found and that it is recommended to send your email with Smartlockr. Smartlockr can also notify you if you have added a recipient that does not belong to your organization and recommend that you send the email securely.
2. Smartlockr will turn itself on, but you have the option to turn it off. The user can also change security level and change between one-factor authentication (1FA) and two-factor authentication (2FA).
3. Smartlockr will turn itself on and you will be required to send your message securely.

Below you can see examples of what this looks like in Outlook.

Privacy sensitive data found with forced or automatic security settings.



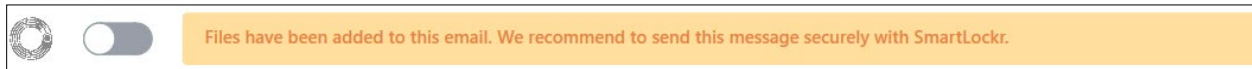
Privacy sensitive data found with notification settings on.



1.3 Notifications

Now for the amazing part: even when you do not turn Smartlockr on, or use one of the trigger words set up by your system administrator, you are still protected. Smartlockr is always working in the background and sends you notifications when you need to be extra careful. For example, when you are sending an email outside of your organization or attaching documents.

This way you are always aware of security threats and stay in control of your data!

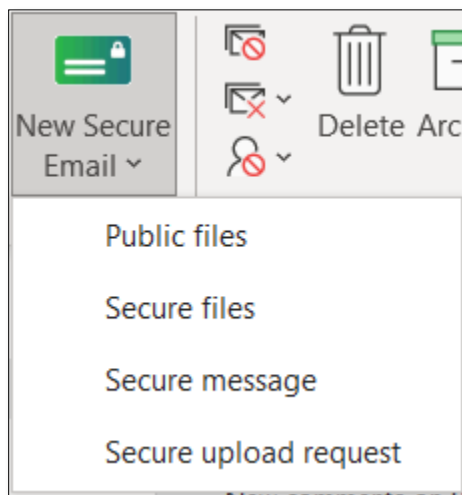


02. Sending files and messages securely

There are four different options for sending secure emails via Smartlockr. Below we will show you how to send files and messages with our plug-in, using three of these options. We will also give you a small explanation of what each option does.

For an explanation and step-by-step guide on how to use the secure upload request, please see '*Chapter 6: Requesting files*'.

First, choose which type of email you would like to send by clicking on the Smartlockr button and click on any of the alternatives in the drop-down menu, as shown below.



2.1 Public files

When choosing the option 'Public files', your files are sent with encryption, but there is no authentication. This means that anyone with access to the file link will be able to open it.

The message is also not encrypted when using the option 'Public files' and will therefore be displayed in the initial email to the recipient, rather than in the secure channel.

Step 1: Write your email and attach files as you usually would, after choosing 'Public files' in the drop-down menu.

Step 2: Click 'send'.

Step 3: This will take you to the 'Confirm Recipient and Files' window. Confirm your attachments and click next.

CONFIRM ATTACHMENTS



CONFIRM RECIPIENTS


To proceed in sending this e-mail, you must "Select all". If there are files you no longer want to send, close this window and remove the document from the attachments section.

<input checked="" type="checkbox"/>	SELECT ALL (1)	
<input checked="" type="checkbox"/>	Document 123-456.pdf	25.08 KB


Next

Step 4: Confirm your recipients and click send. Your message has now been sent!






SET A PASSWORD



CONFIRM ATTACHMENTS



CONFIRM RECIPIENTS

To proceed in sending this e-mail, you must "Select all". If there are recipients you no longer want to send, close this window and remove them from this e-mail.

☒

SELECT ALL (1)

☒

emma.nychospital@outlook.com

emma.nychospital@outlook.com

Previous

Send

2.2 Secure files

With this option, *only* your files will be encrypted. The message is not and will therefore be displayed in the initial email to the recipient, rather than in the secure channel.

This option requires authentication from the recipient.

Step 1: Write your email and attach files like you usually would, after choosing 'Secure files' in the drop-down menu.

Step 2: Click 'send'.

Step 3: This will take you to the 'Confirm Recipient and Files' window. Here you can select which authentication level you want. Smartlockr lets you choose between one-factor authentication (password) or two-factor authentication (text message) (please see '*Chapter 3: Multi-factor authentication*' for additional information). By clicking on the drop-down menu at the top of the confirmation screen you can choose the option that you want.

The screenshot shows the 'Confirm Recipient and Files' window. At the top left, there is a settings gear icon and a dropdown menu currently set to 'One-factor authentication'. The dropdown menu is open, showing two options: 'One-factor authentication' (selected) and 'Two-factor authentication'. The 'One-factor authentication' option has a subtext: 'A password will be sent to the recipient by e-mail address only'. The 'Two-factor authentication' option has a subtext: 'Both recipient's e-mail address and phone number will be verified'. Below the dropdown, a message states: 'To proceed in sending this e-mail, you must "Select all". If there are files you no longer want to send, close this window and remove the document from the attachments section.' At the bottom, there is a section for selecting attachments. It includes a checkbox labeled 'SELECT ALL (1)' and a list of attachments. The first attachment is 'Patient-dossier 234-456.pdf' with a size of '115.02 KB'. In the background, there are two circular icons: a green one with a document icon labeled 'CONFIRM ATTACHMENTS' and a grey one with a person icon labeled 'CONFIRM RECIPIENTS'.

Step 4: After choosing the level of authentication; you will be asked to confirm your files and recipients. The next steps differ depending on your choice of authentication. You will either be asked to generate a password (for one-factor authentication) or fill in the recipient's phone number (two-factor authentication). Please see '*Chapter 4: Confirm attachments and recipients*' for more information on how to proceed.

2.3 Secure message

The option 'Secure message' encrypts both your email body and attachments.

Step 1: Write your email and attach any files as you usually would, after choosing 'Secure message' in the drop-down menu.

Step 2: Click 'send'.

Step 3: This will take you to the 'Confirm Recipient and Files' window. Here you can select which authentication level you want. Smartlockr lets you choose between one-factor authentication (password) or two-factor authentication (text message) (please see '*Chapter 3: Multi-factor authentication*' for additional information). By clicking on the drop-down menu at the top of the confirmation screen you can choose the option that you want.

The screenshot shows a window titled "Confirm Recipient and Files" with a close button (X) in the top right corner. At the top left, there is a settings gear icon and a dropdown menu currently set to "One-factor authentication". Below the dropdown, two authentication options are listed: "One-factor authentication" (A password will be sent to the recipient by e-mail address only) and "Two-factor authentication" (Both recipient's e-mail address and phone number will be verified). A message states: "To proceed in sending this e-mail, you must 'Select all'. If there are files you no longer want to send, close this window and remove the document from the attachments section." Below this message is a "SELECT ALL (1)" button. Underneath, a list of attachments is shown, including "Patient-dossier 234-456.pdf" with a size of "115.02 KB". On the right side of the window, there are two icons: a green circle with a 'u' icon labeled "CONFIRM ATTACHMENTS" and a grey circle with a person icon labeled "CONFIRM RECIPIENTS".

Step 4: After choosing the level of authentication; you will be asked to confirm your files and recipients. The next steps differ depending on your choice of authentication. You will either be asked to generate a password (for one-factor authentication) or fill in the recipient's phone number (two-factor authentication). Please see '*Chapter 4: Confirm attachments and recipients*' for more information on how to proceed.

2.4 File settings

In all the options mentioned above, you can also adjust the settings for your attachments. Via the gear icon in the top-left corner of your screen, you can see how long any attached documents will be accessible for, as well as the maximum number of times they can be downloaded.

In the image below, the number of downloads is 0, but of course you can change this number as you see fit.

The screenshot shows a 'Message settings' dialog box with a sidebar on the left and a main content area on the right. The sidebar contains 'Message settings' and 'Documents accessible until:' with fields for 'Date' (7/9/2021) and 'Time' (11:15). Below this is 'Max amount of downloads' with a description 'Number of times the recipient can download the document and attachments' and a value of 0. The main content area has a progress bar with three steps: 'SET A PASSWORD', 'CONFIRM ATTACHMENTS', and 'CONFIRM RECIPIENTS'. Below the progress bar is a warning: 'To proceed in sending this e-mail, you must "Select all". If there are files you no longer want to send, close this window and remove the document from the attachments section.' At the bottom, there is a list of attachments with a checkbox for 'SELECT ALL (1)' and a specific attachment 'Patient-dossier 234-456.pdf' with a size of 115.02 KB.

Attachment	Size
Patient-dossier 234-456.pdf	115.02 KB

By default, the download link will expire after 14 days. However, this can be reduced to a shorter time limit if you like (14 days is the maximum, but a higher retention period can be added for an additional cost).

03. Multi-factor authentication

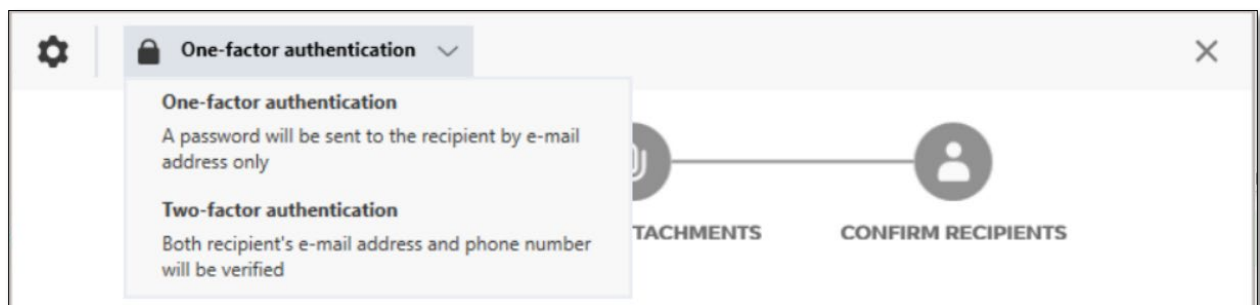
When you choose to send the email using 'Secure files' or 'Secure message' you can select the authentication level you prefer. Smartlockr lets you choose between one-factor or two-factor authentication. In this chapter we explain the difference between these two options and how to use them.

3.1 One-factor authentication

Choosing one-factor authentication means that the recipient will be sent a *password* before they can access their file(s). It offers an extra in-between step to ensure the right recipient has access to the file(s). If you want to be even more secure, please make sure to choose *two-factor authentication* (see *chapter 3.2!*).

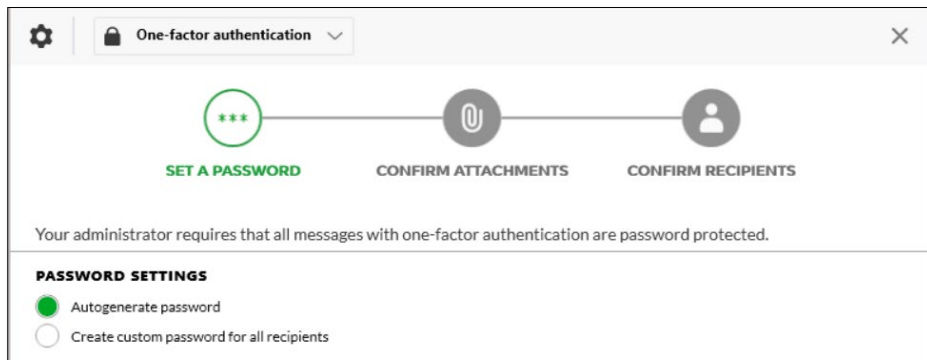
When selecting 'Secure message' or 'Secure file', you can choose which authentication level you want after writing your message and attaching your files. When you hit 'send', a confirmation wizard will open with a dropdown menu at the top of the screen. Here you can choose between one-factor authentication or two-factor authentication.

Step 1: Select 'one-factor authentication' in the dropdown menu.

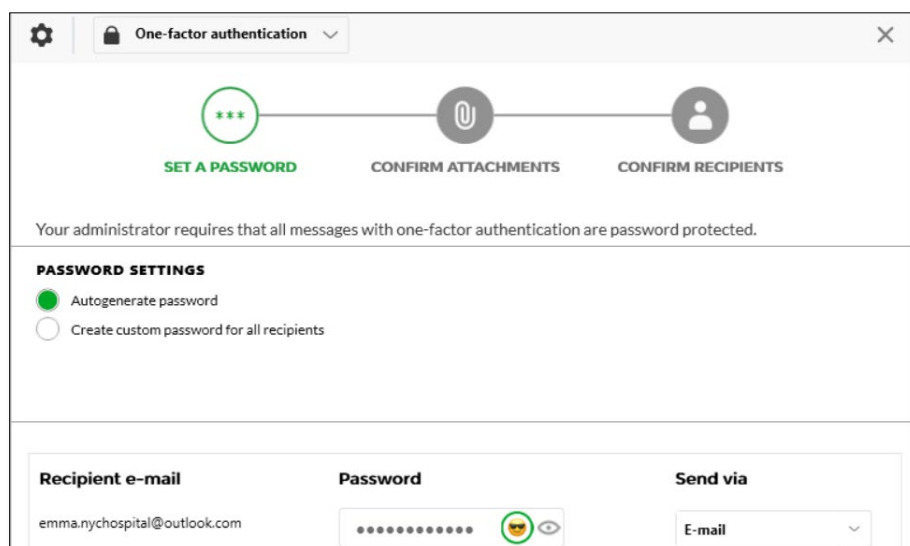


One-factor authentication enables you to set up a password which will be sent to the recipient's email. This password allows them to open the message and/or file(s).

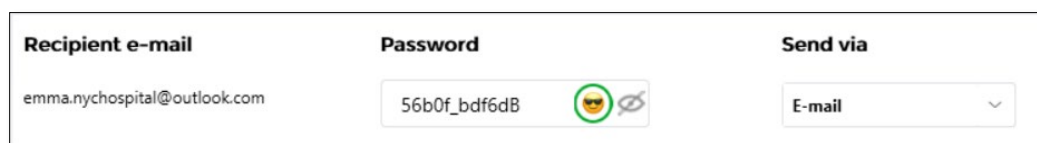
Step 2: You can either autogenerate a password or create your own for your recipient. Choose autogenerate or create a custom password. *Please note that a Smartlockr administrator have the possibility to hide one or both options. If you cannot find 1FA or either alternatives, this is why.*



Step 2.1: You have selected 'Autogenerate password'.



Smartlockr will then automatically create a safe password for you to use. By clicking the eye icon next to the password, it will become visible to you.



Step 2.2: You have selected 'Create custom password for all recipients'.


As soon as you fill out your password, Smartlockr will tell you whether this is a safe password to use. The emoji will be circled by a red or orange ring if it is not secure enough!



PASSWORD SETTINGS

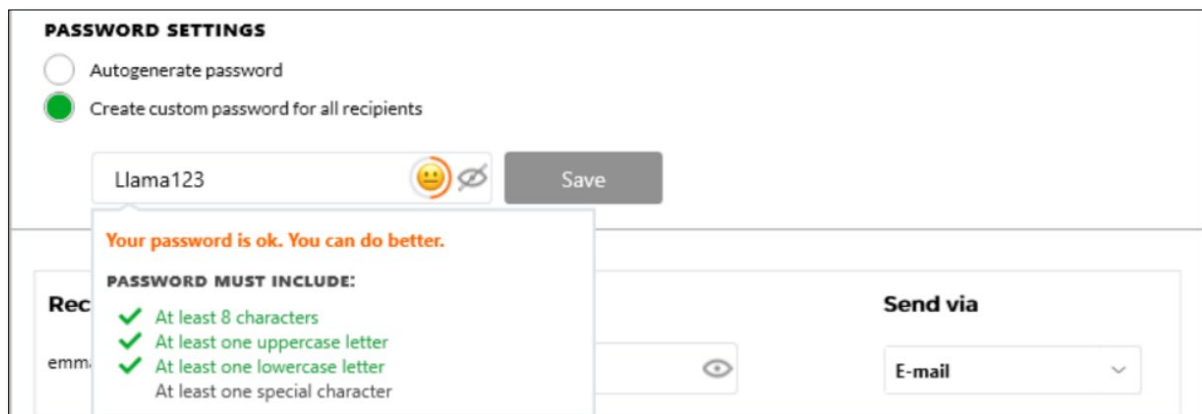
☐ Autogenerate password

☒ Create custom password for all recipients

Llama123  

Save



By hovering over the emoji, you can see what else your password needs before it's deemed safe. You will not be able to send your email without a safe password.



PASSWORD SETTINGS

☐ Autogenerate password

☒ Create custom password for all recipients

Llama123  

Save


Your password is ok. You can do better.

PASSWORD MUST INCLUDE:

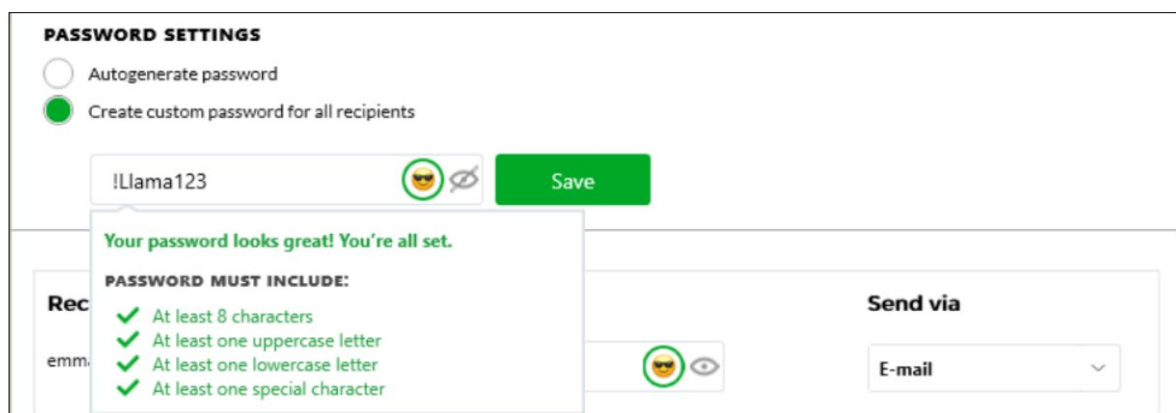
- ✓ At least 8 characters
- ✓ At least one uppercase letter
- ✓ At least one lowercase letter
- At least one special character

Rec emm

Send via

 E-mail



The emoji will have a green ring sporting a chic pair of sunglasses if it is safe to use. You will also be able to send your email as the 'next' button will now be green.



PASSWORD SETTINGS

☐ Autogenerate password

☒ Create custom password for all recipients

!Llama123  

Save



Your password looks great! You're all set.

PASSWORD MUST INCLUDE:

- ✓ At least 8 characters
- ✓ At least one uppercase letter
- ✓ At least one lowercase letter
- ✓ At least one special character

Rec emm

Send via

  E-mail

Step 3: Choose how you want to send your email via the dropdown menu under 'Send via'. The two options are 'Email' or 'Other'.

'Other' is used if you want to directly tell your recipient your password, by calling them for example, while 'Email' simply sends the password in an email.

Step 4: When you have generated a safe password and chosen how to send it, you can now send out your email. Click 'next'.

The screenshot shows a web interface for setting up one-factor authentication. At the top, there's a header with a gear icon, a dropdown menu labeled "One-factor authentication", and a close button. Below the header is a progress bar with three steps: "SET A PASSWORD" (highlighted in green), "CONFIRM ATTACHMENTS", and "CONFIRM RECIPIENTS". A message states: "Your administrator requires that all messages with one-factor authentication are password protected." Under the "PASSWORD SETTINGS" section, there are two radio buttons: "Autogenerate password" (unselected) and "Create custom password for all recipients" (selected). Below this is a text input field containing "iLlama123", a toggle icon, and a green "Save" button. The bottom section contains three fields: "Recipient e-mail" with the value "emma.nychospital@outlook.com", "Password" with a masked input field and a toggle icon, and "Send via" with a dropdown menu showing "E-mail". A green "Next" button is located at the bottom right.

3.2 Two-factor authentication

Choosing two-factor authentication means that your recipient will receive a passcode on their mobile phone number before they can access the file(s). This authenticates your recipient in two steps:

1. By their personal log-in details for their email address.
2. By their phone number, which is given by the sender.

When selecting 'Secure message' or 'Secure files', you can choose which authentication level you want after writing your message and attaching your files. When you hit 'send', a confirmation wizard will open with a dropdown menu at the top of the screen. Here you can choose **two-factor authentication**.

Step 1: Select 'two-factor authentication' in the dropdown menu.



Two-factor authentication allows the system to send out a SMS-code to your recipient. They need this code to open your message and/or files.


Step 2: Confirm your attachments and click 'next'.


The screenshot shows a window titled "Two-factor authentication" with a close button (X) in the top right corner. At the top, there is a progress bar with three steps: "SET A PASSWORD" (represented by a circle with three asterisks), "CONFIRM ATTACHMENTS" (represented by a circle with a paperclip icon and highlighted in green), and "CONFIRM RECIPIENTS" (represented by a circle with a person icon). Below the progress bar, a message states: "To proceed in sending this e-mail, you must 'Select all'. If there are files you no longer want to send, close this window and remove the document from the attachments section." Below this message is a list of attachments. The first item is "SELECT ALL (1)" with a checked checkbox. Below it is "Document 123-456.pdf" with a checked checkbox and a size of "25.08 KB". At the bottom right, there is a green button labeled "Next".


Step 3: In the third step, you will need to fill out a phone number for your recipient. This is the number the SMS-code will be sent to.


The screenshot shows a window titled "Tvåfaktorsautentisering" with a close button (X) in the top right corner. At the top, there is a progress bar with three steps: "STÄLL IN ETT LÖSENORD" (represented by a circle with three asterisks), "BEKRÄFTA BIFOGADE FILER" (represented by a circle with a paperclip icon), and "BEKRÄFTA MOTTAGARE" (represented by a circle with a person icon and highlighted in green). Below the progress bar, a message states: "För att fortsätta skicka detta e-postmeddelande måste du 'Markera alla'. Om det finns mottagare som du inte längre vill skicka till, stäng det här fönstret och ta bort dem från det här e-postmeddelandet." Below this message is a list of recipients. The first item is "VÄLJ ALLA (1)" with an unchecked checkbox. Below it is "Emma. nychospital@outlook. com" with an unchecked checkbox. To the right of the email address is a text field for a phone number, which currently contains "+46" and has a dropdown arrow. The text field is highlighted with a red border.

After filling out the phone number(s), Smartlockr will show you a green checkmark. After selecting your recipient (see also chapter 4 on '*confirming attachments and recipients*'), you will be able to send your email.




Two-factor authentication 






SET A PASSWORD



CONFIRM ATTACHMENTS




CONFIRM RECIPIENTS

To proceed in sending this e-mail, you must "Select all". If there are recipients you no longer want to send, close this window and remove them from this e-mail.


☐ SELECT ALL (1)

☐ **emma.nychospital@outlook.com**

emma.nychospital@outlook.com

 +1

2345678910



04. Confirming attachments and recipients

After selecting one-factor or two-factor authentication, Smartlockr will ask you to confirm both the attachment and the recipient(s) email address. This is a built-in trigger that will prevent errors in sending sensitive data to the wrong person or giving out the wrong file(s).

Step 1: Confirm the file(s). Please check whether this is the correct file to send to your recipient.

The screenshot shows a window titled "One-factor authentication" with a close button (X) in the top right corner. At the top, there is a progress bar with three steps: "SET A PASSWORD" (marked with a green circle and three asterisks), "CONFIRM ATTACHMENTS" (marked with a green circle and a paperclip icon), and "CONFIRM RECIPIENTS" (marked with a grey circle and a person icon). The "CONFIRM ATTACHMENTS" step is currently active. Below the progress bar, a message states: "To proceed in sending this e-mail, you must 'Select all'. If there are files you no longer want to send, close this window and remove the document from the attachments section." Below this message is a table with two rows. The first row is a header with a green checkmark icon and the text "SELECT ALL (1)". The second row contains a green checkmark icon, the text "Document 123-456.pdf", and the text "25.08 KB". At the bottom of the window, there are two green buttons: "Previous" on the left and "Next" on the right.

<input checked="" type="checkbox"/> SELECT ALL (1)		
<input checked="" type="checkbox"/>	Document 123-456.pdf	25.08 KB

Only when you have confirmed your attachment(s), will you be able to click 'Next' and proceed to the last step.

Step 2: Confirm your recipient(s) (and fill in their telephone numbers if you have chosen two-factor authentication. Please *'Chapter 3: Multi-factor authentication'* for more information).

The image shows a window titled "One-factor authentication" with a close button (X) in the top right corner. At the top, there is a progress bar with three steps: "SET A PASSWORD" (represented by a circle with three asterisks), "CONFIRM ATTACHMENTS" (represented by a circle with a paperclip icon), and "CONFIRM RECIPIENTS" (represented by a circle with a person icon). The "CONFIRM RECIPIENTS" step is currently active. Below the progress bar, a message states: "To proceed in sending this e-mail, you must 'Select all'. If there are recipients you no longer want to send, close this window and remove them from this e-mail." Below this message is a list of recipients. The first item is "SELECT ALL (1)" with a checked checkbox. Below it is a single recipient: "emma.nychospital@outlook.com" with a checked checkbox. At the bottom of the window, there are two green buttons: "Previous" on the left and "Send" on the right.

One-factor authentication

SET A PASSWORD CONFIRM ATTACHMENTS CONFIRM RECIPIENTS

To proceed in sending this e-mail, you must "Select all". If there are recipients you no longer want to send, close this window and remove them from this e-mail.

☒ SELECT ALL (1)

☒ emma.nychospital@outlook.com emma.nychospital@outlook.com

Previous Send

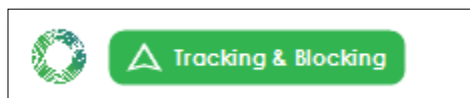
After confirming that this is the correct recipient, you can proceed to send your email.

05. Tracking and blocking

Smartlockr prevents data breaches also after an email has been sent. In this chapter we will explain how to track and block a sent email.

5.1 Tracking sent emails

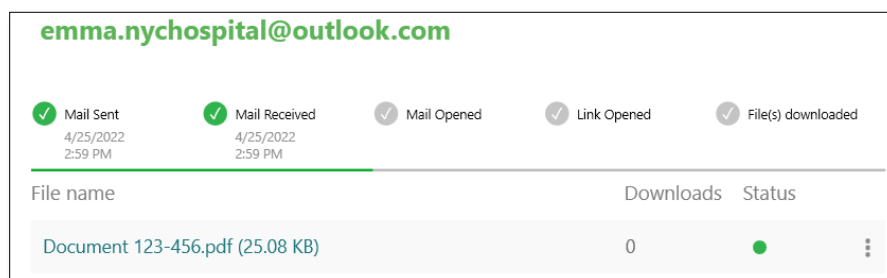
Emails sent with Smartlockr can be found in the 'Sent items' folder of your Outlook. Select an email sent with Smartlockr and you will see a green button labelled 'Tracking & Blocking'.



Step 1: Click the 'Tracking & Blocking' button. You will then see the following screen:



Step 2: Click on 'See tracking and file information'. Here you can see if your email has been received, whether it has been opened and if the file has already been downloaded. If you want to block a recipient or a file, please read on to '*Chapter 5.2: Blocking emails*'.

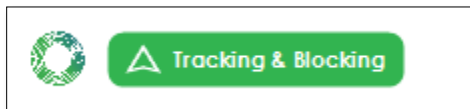


5.2 Blocking emails

If you accidentally sent out the wrong information or chose the wrong recipient, you have the option to block an email, files, or recipients. If you have sent a 'Secure message' you can block both the email and the files as everything is encrypted, while the options 'Public file' and 'Secure file' only lets you block your attachments.

5.2.1 Blocking files

Step 1: Return to your sent emails in Outlook and click on the email you have sent out. Click on the 'Tracking & blocking' button.

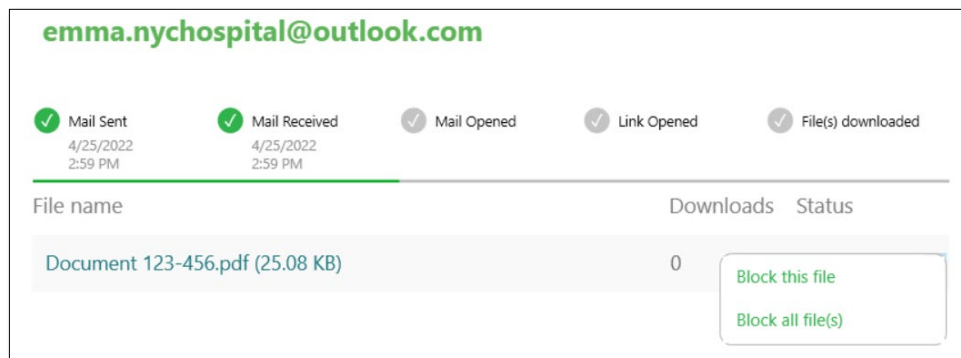


Step 2: Click 'See tracking and file information'.



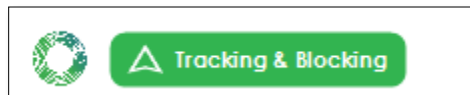
You will now see the status of your sent email. If the recipient has not yet downloaded the file or opened the link, it not too late to block your files and prevent them from being read.

Step 3: Click on the three dots next to the status. You can now block separate or all files.

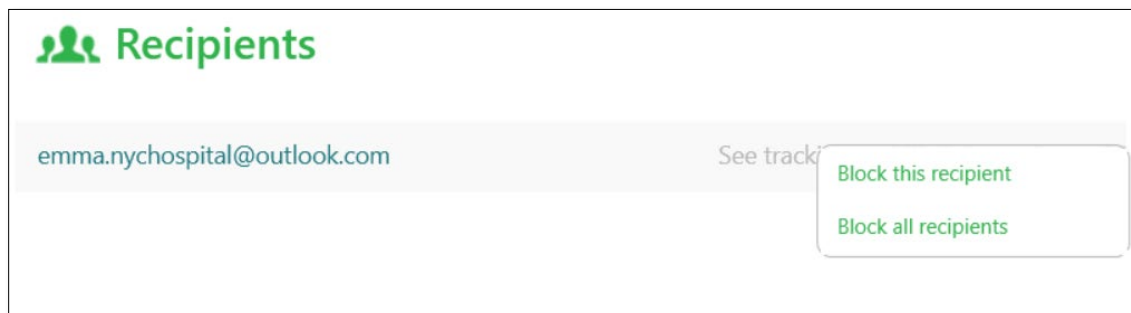


5.2.2 Blocking recipients

Step 1: Return to your sent emails in Outlook and click on the email you have sent out. Click on the 'Tracking & blocking' button.

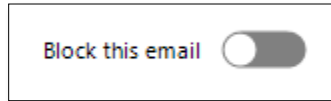


Step 2: Click on the three dots next to the recipient. You now have the option to block separate or all recipients.



5.2.3 Blocking an entire email

Blocking an entire email is possible by going to the 'sent' folder in Outlook. Once again you will see the 'Tracking & blocking' button and on the right side you will find a toggle that says 'Block this email'.



Clicking this button will turn it red and your entire email is now blocked. Keep in mind that this only works if your email has not already opened by the recipient.



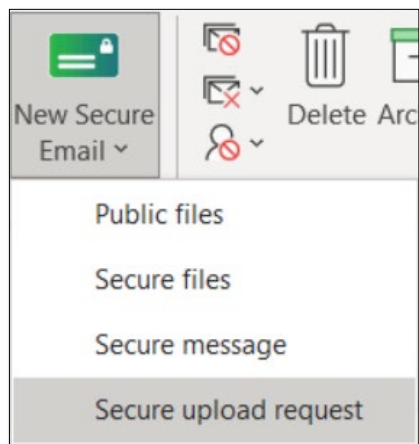
06. Requesting files

To ensure you always receive the correct attachments in a safe way, Smartlockr lets you request files. You can either do this by sending a secure upload request or asking to have files uploaded via an upload portal.

6.1 Secure upload request

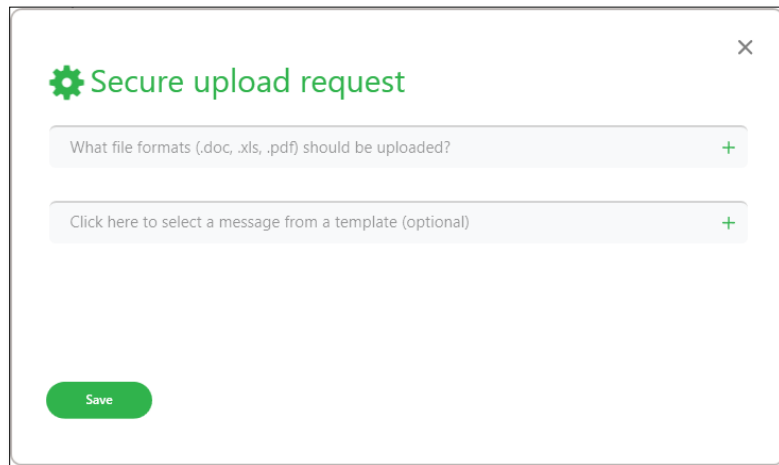
A secure upload request allows you to request files from anyone through a safe upload portal.

Step 1: Select your upload request by clicking the dropdown menu as you are creating a new email.



Step 2: You will now see a pop-up window as shown below. Here you can choose the file formats and/or select a template for explaining your request (if your administrator has added these templates). Click save when you are done.

If you want to fill out your own message, please continue by clicking save without making a choice in the dropdown menu. You will then be able to write your own message for the upload request and your recipient can decide on their file type.

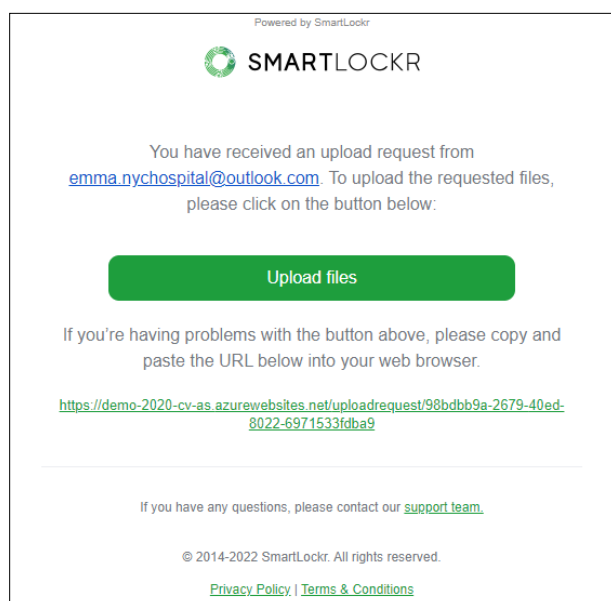


A dialog box titled "Secure upload request" with a green gear icon and a close button (X) in the top right corner. It contains two input fields, each with a green plus icon on the right: "What file formats (.doc, .xls, .pdf) should be uploaded?" and "Click here to select a message from a template (optional)". At the bottom left is a green "Save" button.

Step 3: Click 'Send' and confirm that you have added the correct recipients. Click 'Send' again. Read more about this in '*Chapter 4: Confirm attachments and recipients*'.

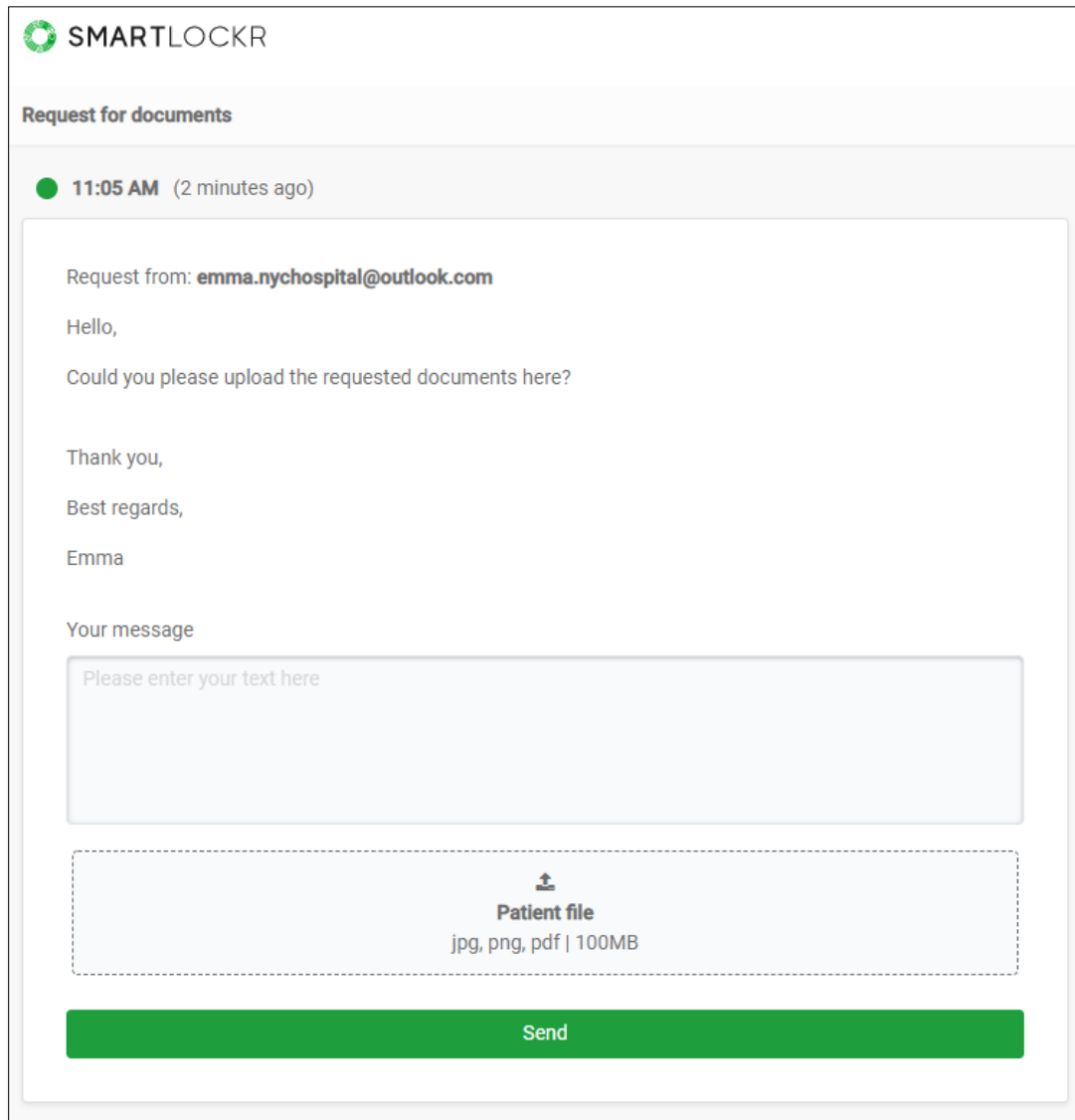
6.1.1 Secure upload request for the recipient

Step 1: Open the email. Your recipient will receive an email like the one shown below:



An email template from SmartLockr. At the top, it says "Powered by SmartLockr" and features the SmartLockr logo. The main text reads: "You have received an upload request from emma.nychospital@outlook.com. To upload the requested files, please click on the button below:". Below this is a large green button labeled "Upload files". Further down, it says: "If you're having problems with the button above, please copy and paste the URL below into your web browser." followed by a long URL: <https://demo-2020-cv-as.azurewebsites.net/uploadrequest/98bdbb9a-2679-40ed-8022-6971533fdb9>. At the bottom, it says: "If you have any questions, please contact our [support team](#)." and includes a footer with "© 2014-2022 SmartLockr. All rights reserved." and links to "Privacy Policy" and "Terms & Conditions".

Step 2: Click the 'Upload files' button. Your recipient will be forwarded to an upload page that includes your personal message (if you have written one):

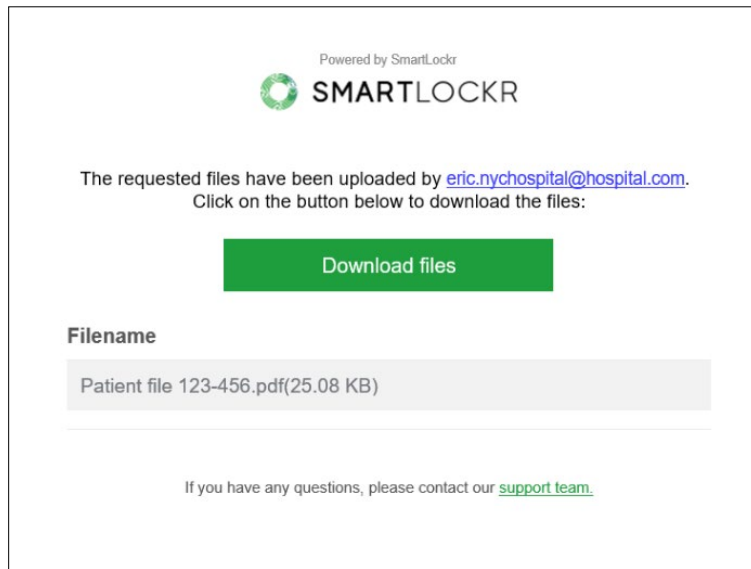


The screenshot shows the SMARTLOCKR interface for requesting documents. At the top, the SMARTLOCKR logo is displayed. Below it, the title 'Request for documents' is shown. A green dot icon and the time '11:05 AM (2 minutes ago)' are visible. The main content area contains a message from 'emma.nychospital@outlook.com' with the text: 'Hello, Could you please upload the requested documents here? Thank you, Best regards, Emma'. Below the message is a text input field with the placeholder 'Please enter your text here'. Underneath the input field is a dashed box containing an upload icon, the text 'Patient file', and the supported file types 'jpg, png, pdf | 100MB'. At the bottom of the interface is a green 'Send' button.

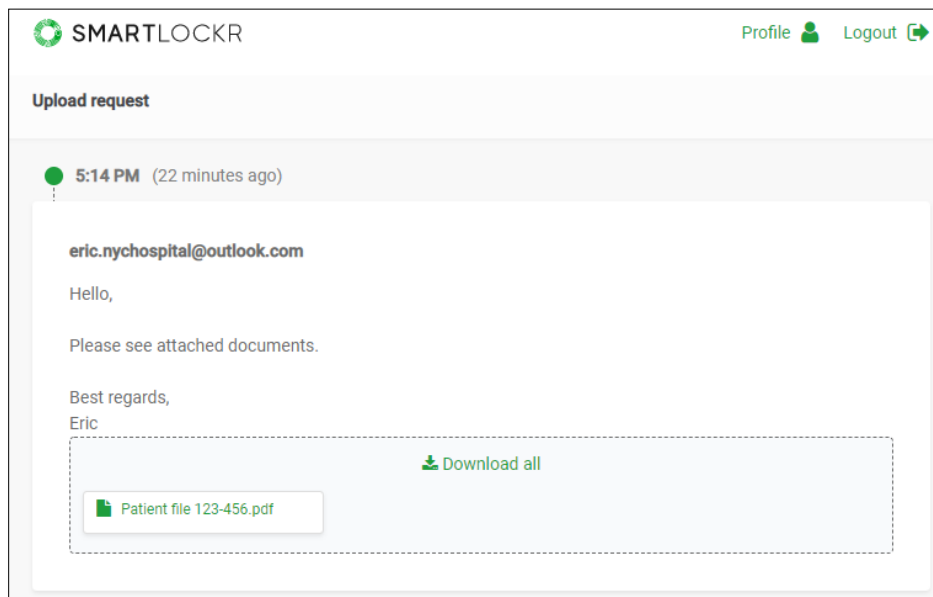
Step 3: Here your recipient can upload the files before hitting 'send'. Their file has now been sent.

6.1.2 After your recipient has uploaded the file

Step 1: Once your recipient has uploaded their files, you will receive a notification email as shown below:



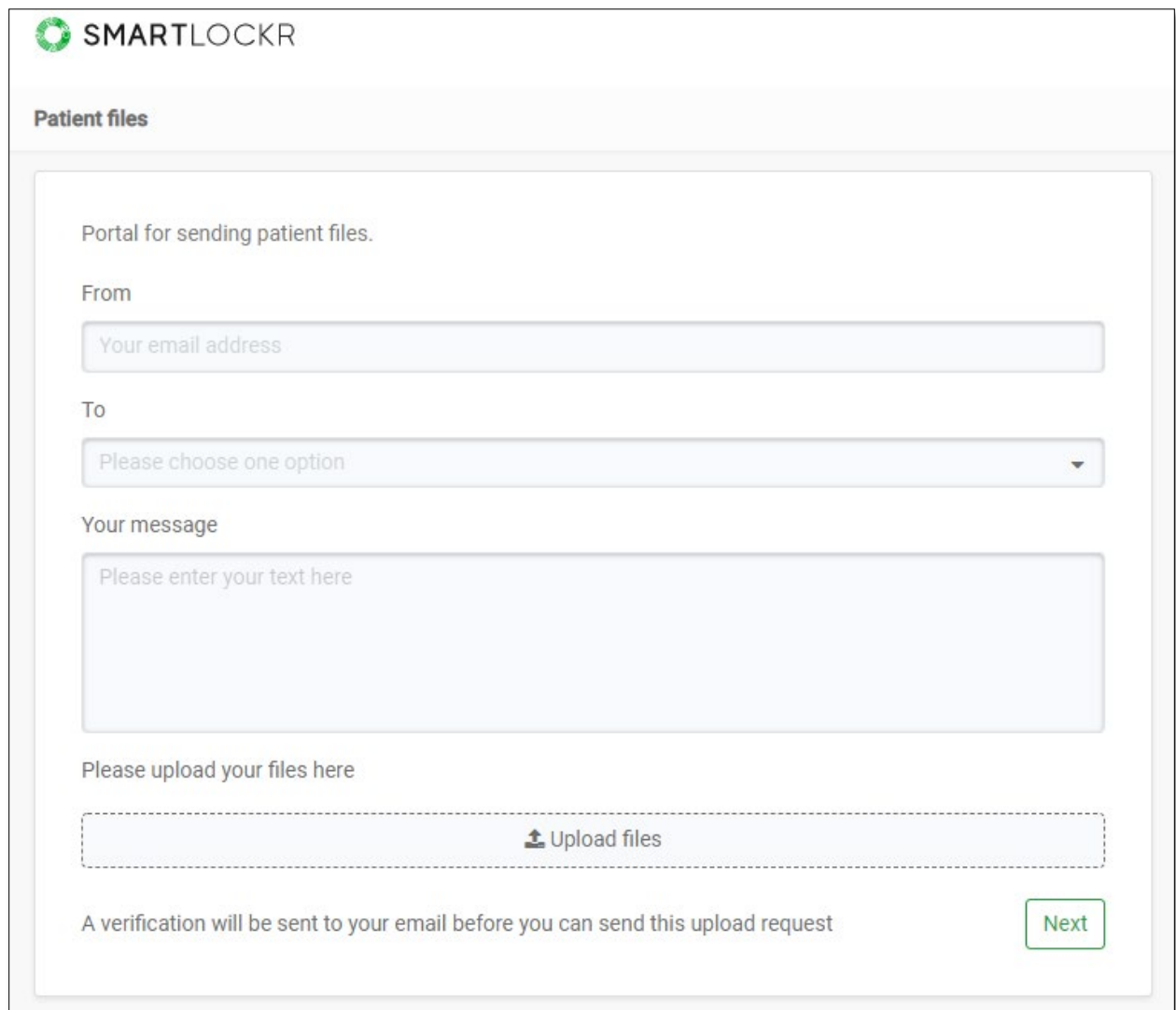
Step 2: Click on 'Download files' to access your file(s). If you click on 'Download all' in the next screen (as shown below), you will receive the documents as a ZIP file. You can also download them one by one, by clicking on the file names:



6.2 Secure upload portals

An Upload Portal is a portal where external relations can go online at any time to send their files securely and directly to your organization. These can be set up and created by your system administrator in the admin portal. Here they can also decide which kind of files and document types that can be sent via the upload portal.

Below you can see an image of what an upload portal could look like.



The image shows a web interface for SMARTLOCKR, specifically the 'Patient files' section. The interface is designed for sending patient files and includes the following elements:

- SMARTLOCKR logo:** Located at the top left of the interface.
- Patient files header:** A sub-header indicating the purpose of the portal.
- Portal description:** A text box stating 'Portal for sending patient files.'
- From field:** A text input field labeled 'From' with the placeholder text 'Your email address'.
- To field:** A dropdown menu labeled 'To' with the placeholder text 'Please choose one option' and a downward arrow.
- Your message field:** A large text area labeled 'Your message' with the placeholder text 'Please enter your text here'.
- Upload instruction:** A text label 'Please upload your files here' above a dashed rectangular box.
- Upload button:** A button with an upward arrow icon and the text 'Upload files' inside the dashed box.
- Verification notice:** A text line at the bottom stating 'A verification will be sent to your email before you can send this upload request'.
- Next button:** A green button labeled 'Next' located at the bottom right of the form.

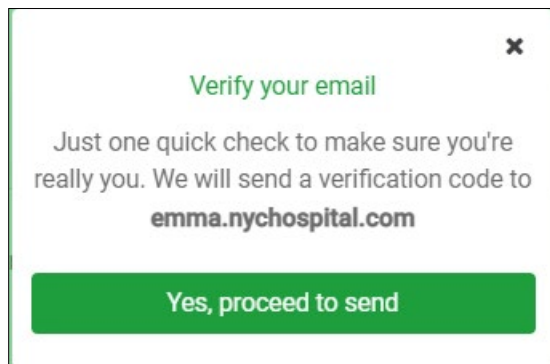
6.2.1 To send a file via an upload portal

Step 1: When adding a file to an upload portal, you start with writing your email address in the field marked 'From'.

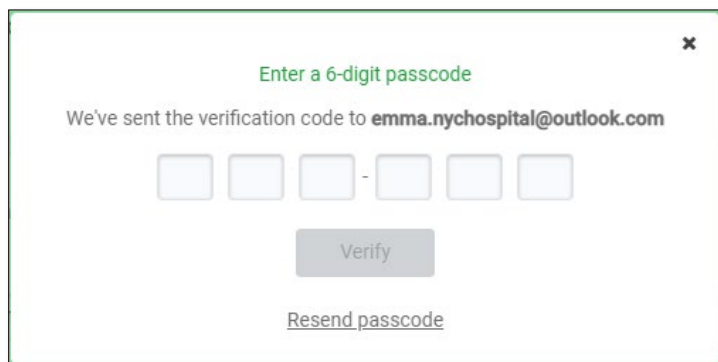
Step 2: Under 'To' you can either choose between pre-determined recipients that were added by the system administrator or enter an email address manually. *Please note that the Smartlockr administrator has the option to remove the 'To' field. In this case, the visitor can only use the upload portal to send attachments to a pre-decided email address.*

Step 3: If you wish, you can add a message before uploading the files. Then click 'Next'.

Step 4: A pop-up window will open asking you to verify your email. Check that you have entered the correct address and then click 'Yes, proceed to send'.



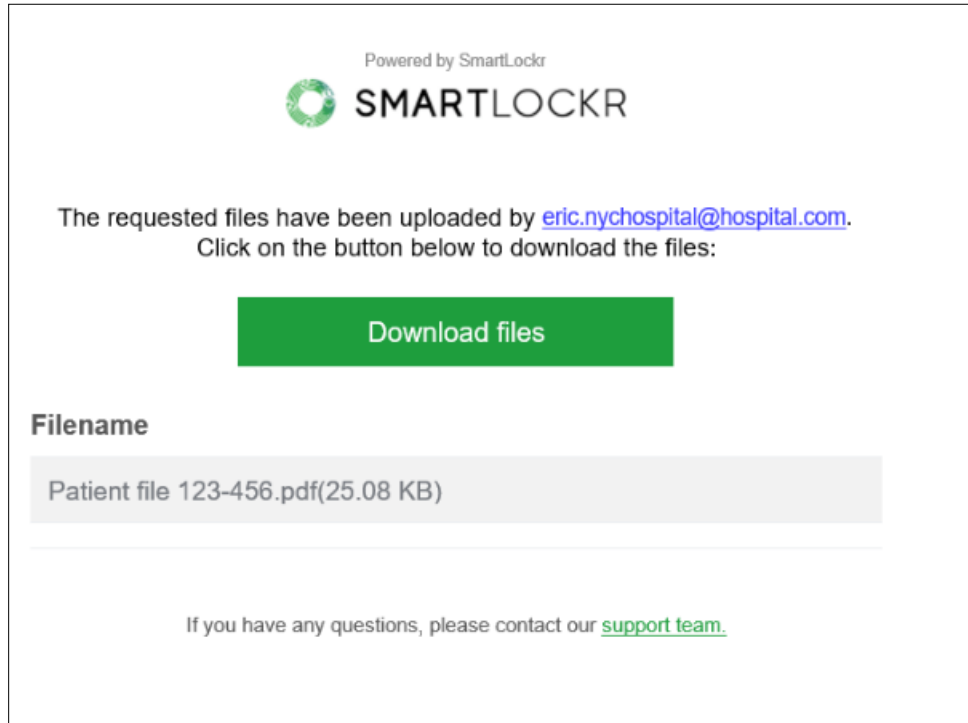
Step 5: A verification code will be sent to your email address to verify that you are who you say you are. A pop-up window will appear where you can enter the code that has been sent to you.



After this, your files will be sent to the recipient, and you will get a notification email that your files were successfully sent.

6.2.2 Secure upload portals for the recipient

When someone sends a file to you via an upload portal, a notification is sent to your email address, as shown in the image below.



To download the files, simply click the button that says, 'Download files'.

07. What Smartlockr looks like for your recipient

When you use Smartlockr to send a secure email, the recipient will also use Smartlockr to receive emails and attachments. That is why we included a chapter on what Smartlockr looks like for a recipient, so using Smartlockr will be as easy for them as it is for you!

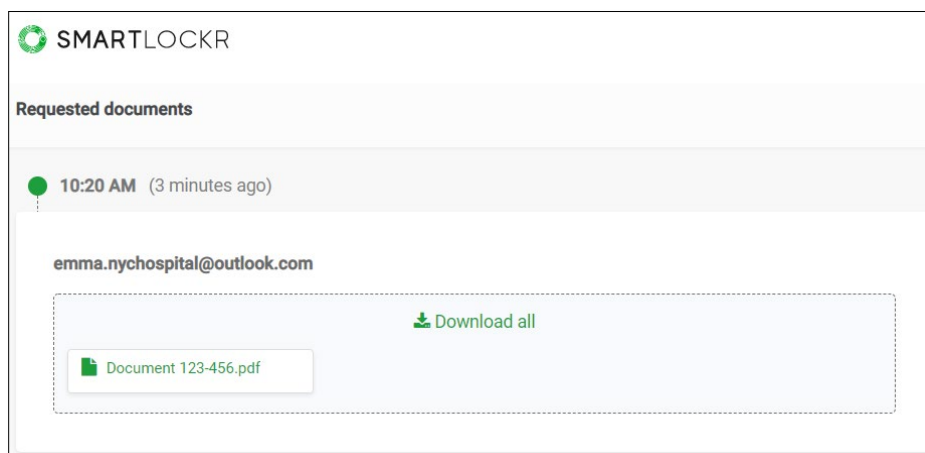
7.1 Receiving a Public file through Smartlockr

When you send a message and/or attachment using the 'public file' option, the recipient will receive an email that looks like this:



Step 1: To access the file, the recipient simply clicks on the green button.

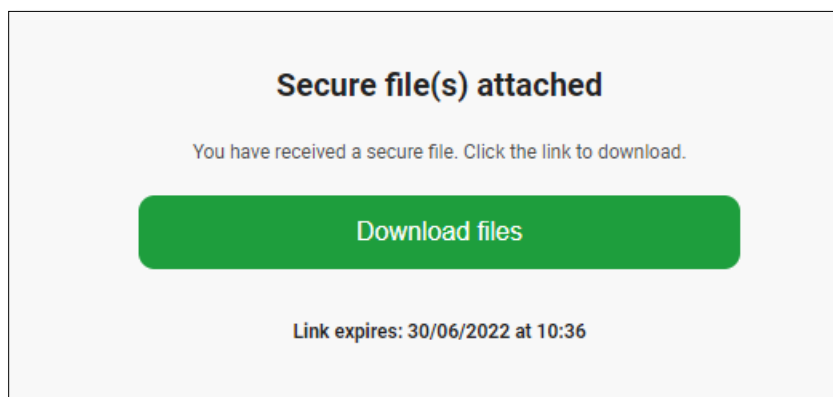
Step 2: This takes them to a channel where they can download their files by either clicking 'Download all', and receive the documents as a ZIP file, or download them one by one, by clicking on the file names:



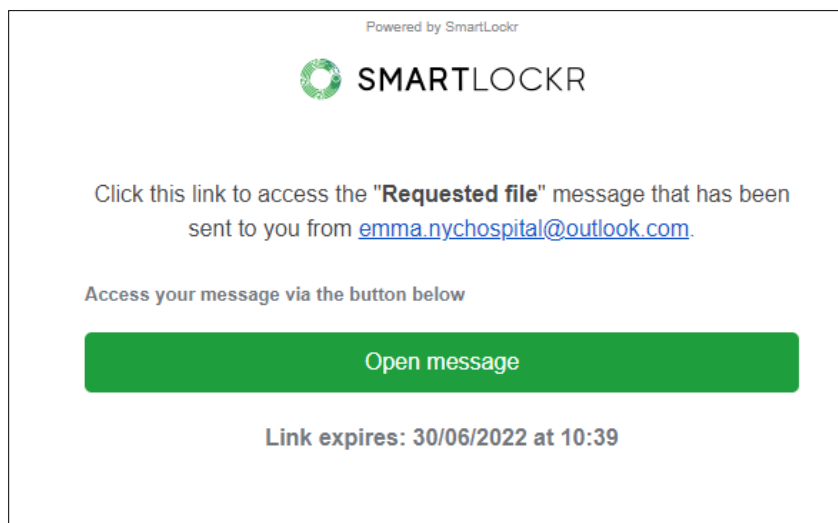
7.2 Receiving Secure files and Secure messages through Smartlockr

When you send a Secure file or a Secure message through Smartlockr, you can choose between using one-factor authentication and two-factor authentication.

Using one-factor authentication when sending a Secure file or Secure message through Smartlockr, the recipient will receive two emails. The first one grants access to the sent files/message. The notifications look slightly different but the procedure to gain access are the same. Please see screenshots below.

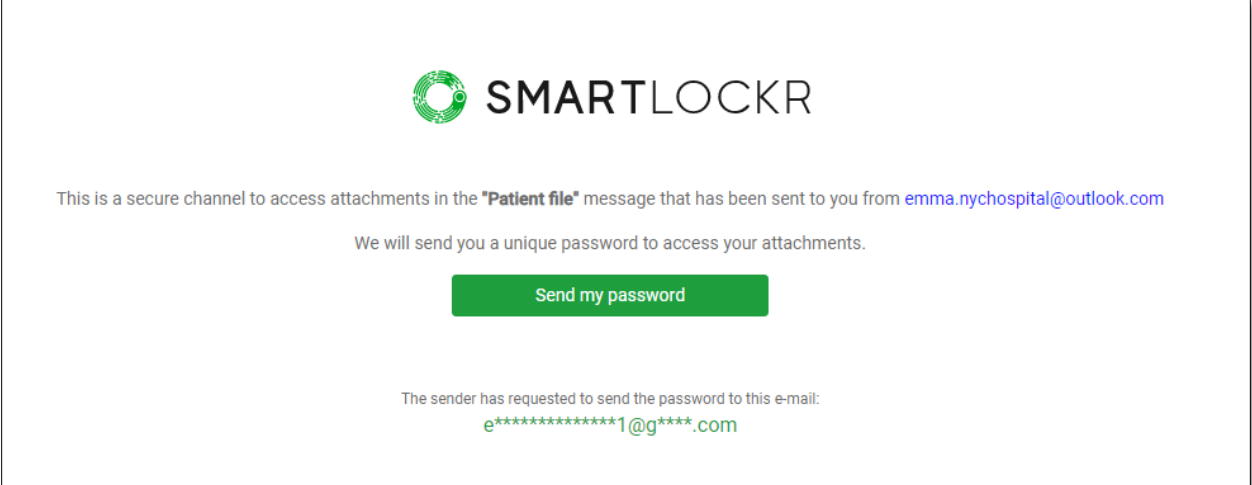


Notification for a secure file above.



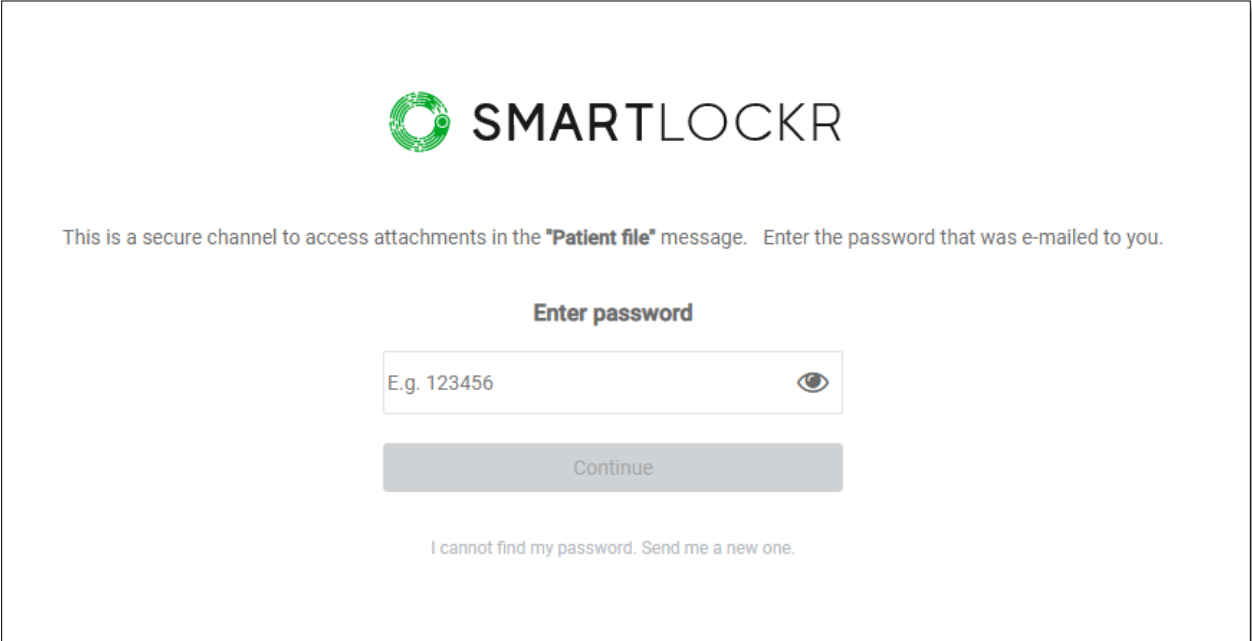
Notification for a secure message above.

Before getting access to the secure channel with the message/file(s), the recipients must fill in their password. When clicking 'Download files' and 'Open message' the channel opens and the recipient can receive their password by clicking 'Send my password'.



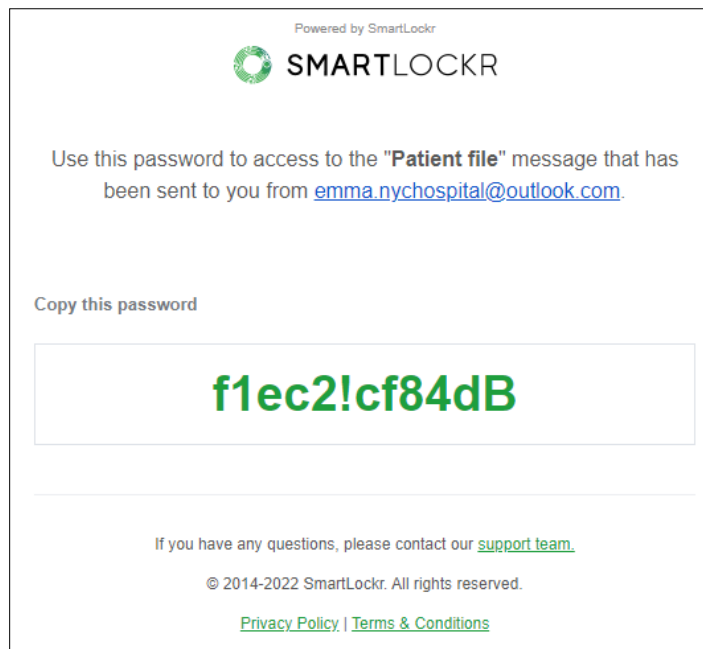
The image shows a web interface for SMARTLOCKR. At the top is the SMARTLOCKR logo, which consists of a green circular icon with a stylized 'S' and the word 'SMARTLOCKR' in a bold, sans-serif font. Below the logo, the text reads: 'This is a secure channel to access attachments in the "Patient file" message that has been sent to you from emma.nychospital@outlook.com'. This is followed by the sentence: 'We will send you a unique password to access your attachments.' In the center is a green rectangular button with the text 'Send my password'. Below the button, it says: 'The sender has requested to send the password to this e-mail: e*****1@g****.com'.

When this is done, a field where the password can be entered appears.

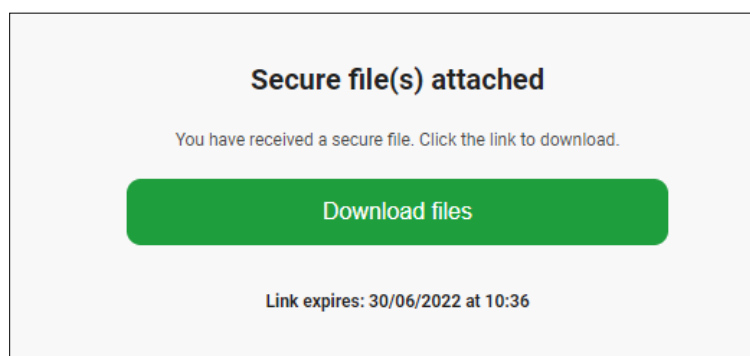


The image shows a web interface for SMARTLOCKR, similar to the previous one. It features the same SMARTLOCKR logo at the top. Below the logo, the text reads: 'This is a secure channel to access attachments in the "Patient file" message. Enter the password that was e-mailed to you.' In the center is the heading 'Enter password'. Below this is a text input field with the placeholder text 'E.g. 123456' and a small eye icon on the right side. Below the input field is a grey rectangular button with the text 'Continue'. At the bottom, there is a link that says: 'I cannot find my password. Send me a new one.'

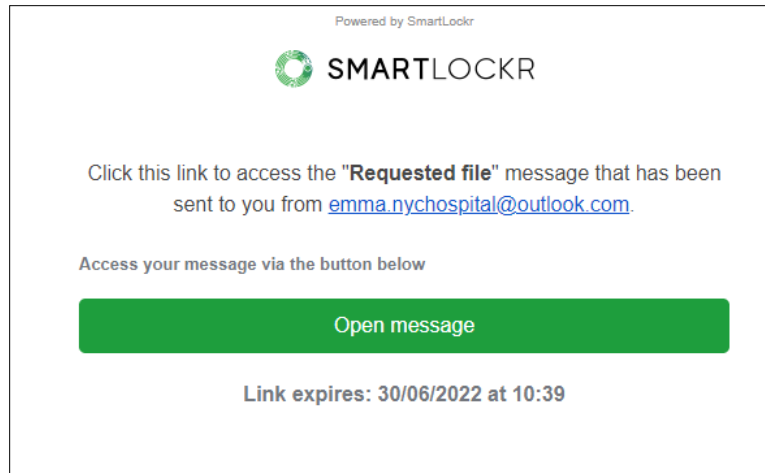
The recipient will also receive another email which contains the password. The recipient copies this password and enters it into the secure channel to get access to the message/files.



Using two-factor authentication when sending a Secure files or Secure message through Smartlockr, the recipient will receive one email and one text message on their phone. The first email looks the same as for one-factor authentication.

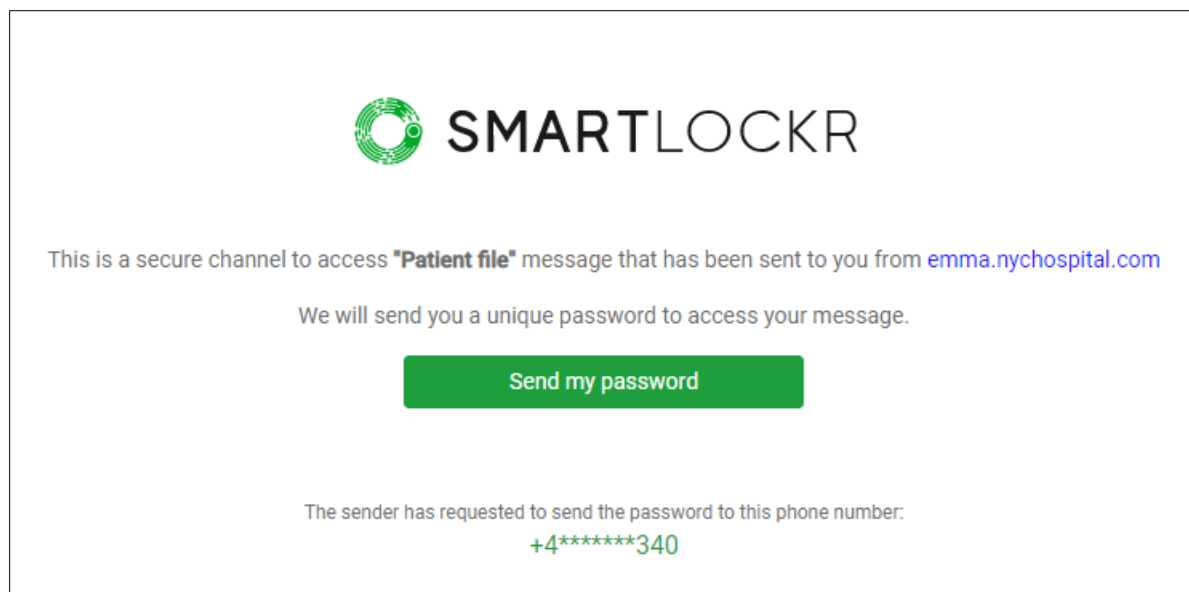


Notification for a secure file above.

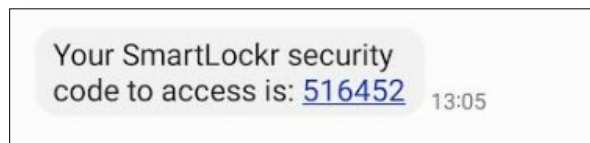


Notification for a secure message above.

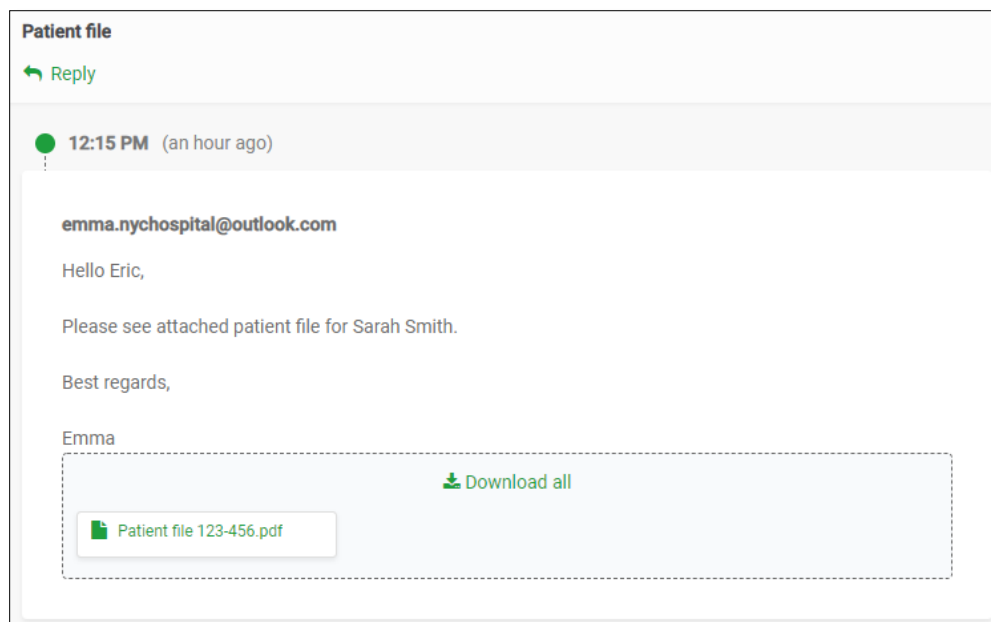
When clicking 'Download files' or 'Open message', the secure channel opens and the recipient can get their code by clicking 'Send my password'.



After this a code will be sent to the recipient's phone number and a field where it can be entered will appear on the secure channel.

The SmartLockr login interface. At the top is the SmartLockr logo, which consists of a green circular icon with a lock symbol and the text "SMARTLOCKR". Below the logo, a message states: "This is a secure channel to access 'Patient file' message. Enter the password that was sent to you." Underneath this is a heading "Enter password". A text input field contains the placeholder text "E.g. 123456" and has a toggle eye icon on its right. Below the input field is a gray "Continue" button. At the bottom, there is a link that says "I cannot find my password. Send me a new one."

After this has been done the recipient will have access to the message and/or file(s).



08. You made it!

Congratulations, you now know how to use the Smartlockr Intelligent Data Protection Platform to easily send and receive emails with the optimal security.

Because we strive for Smartlockr to closely fit the needs of your organization, we have granted your administrator the ability to customize the plug-in accordingly. As a result, your Smartlockr experience could differ slightly from the examples presented in this manual.

Should you have any questions about using Smartlockr, we would heartily recommend you contact the administrator of your organization or your IT department. If they happen to have any questions themselves, or need additional help, they are also more than welcome to reach out to Smartlockr's [support team](#).

We hope you will enjoy using Smartlockr and enjoy the peace of mind that comes with knowing your data is always protected!