SMARTLOCKR

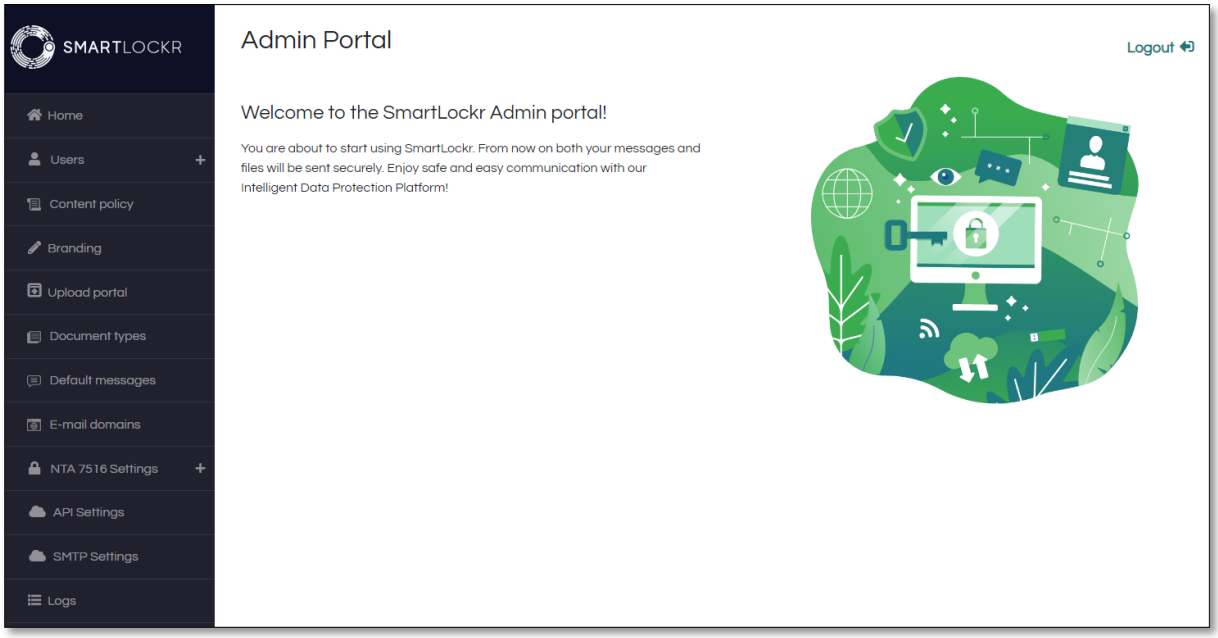
SmartLockr Admin Portal

Table of Contents

Introduction

The admin portal provides a clear overview of all SmartLockr activities and a central point to configure all settings. This way, you always maintain control over the secure exchange of sensitive information within the organization.

When logging into the admin portal, you see a welcoming screen as well as a menu bar on the left where all sections of the portal can be found. Here you can make changes and monitor how SmartLockr is used:

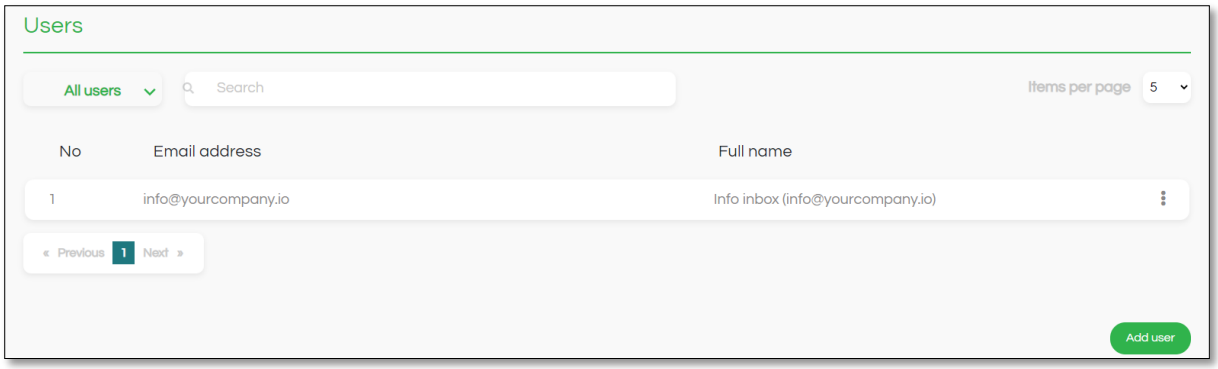


Each section will be briefly explained below. This clarifies what you can expect as an administrator and what options are available.

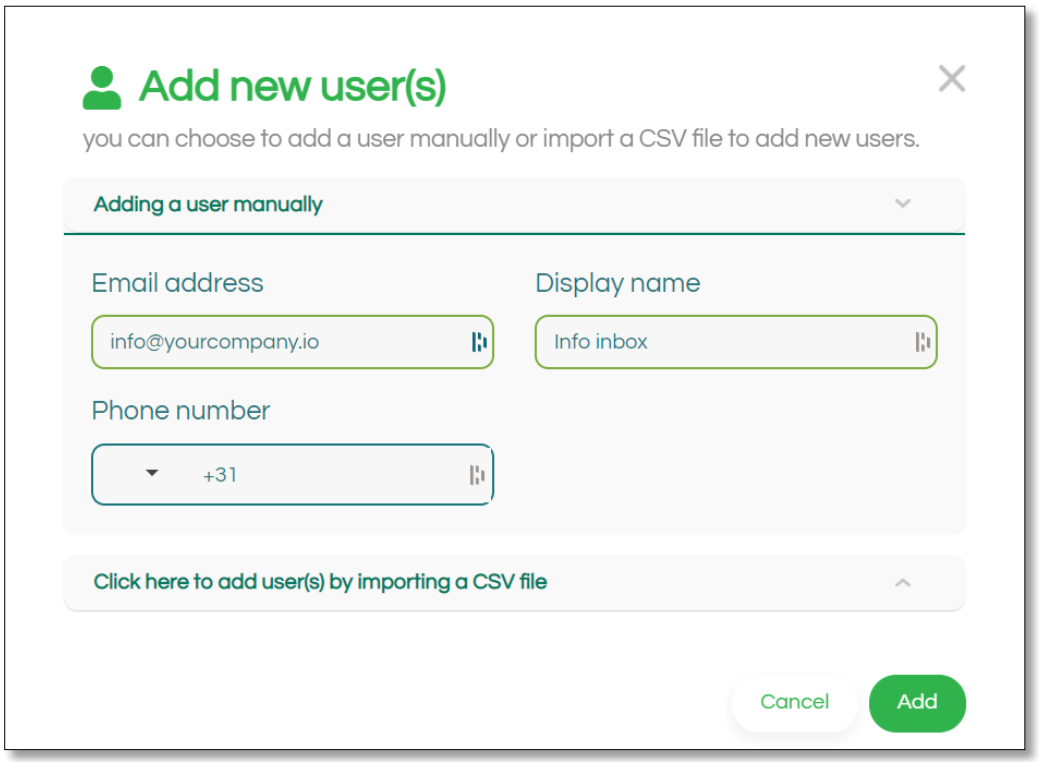
01. Users

Under “Users” you will find an overview of all SmartLockr users within your organization. You can configure settings for these users. By drawing up guidelines, you can better control the safe use of SmartLockr.

To get started, it is important to assign the purchased licenses to users. You can do this by adding the users within the organization to the admin portal:

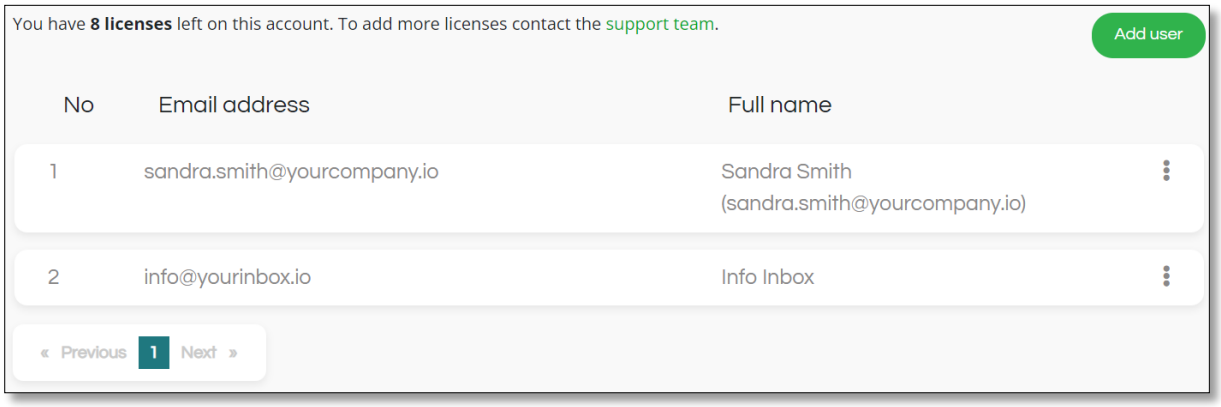


To add users, click on the green button “Add user” at the bottom right. A screen will open where you can add users:



You can add users to your list in two ways. You can add them manually as well as import them from a CSV file. When you upload one or more users through a CSV file, you can save time with SmartLockr, as we can simultaneously activate the account(s) for you and assign the license.

After you have added the users, they will be visible in the overview. If you want to find a user quickly, you can use the search bar at the top to locate them.



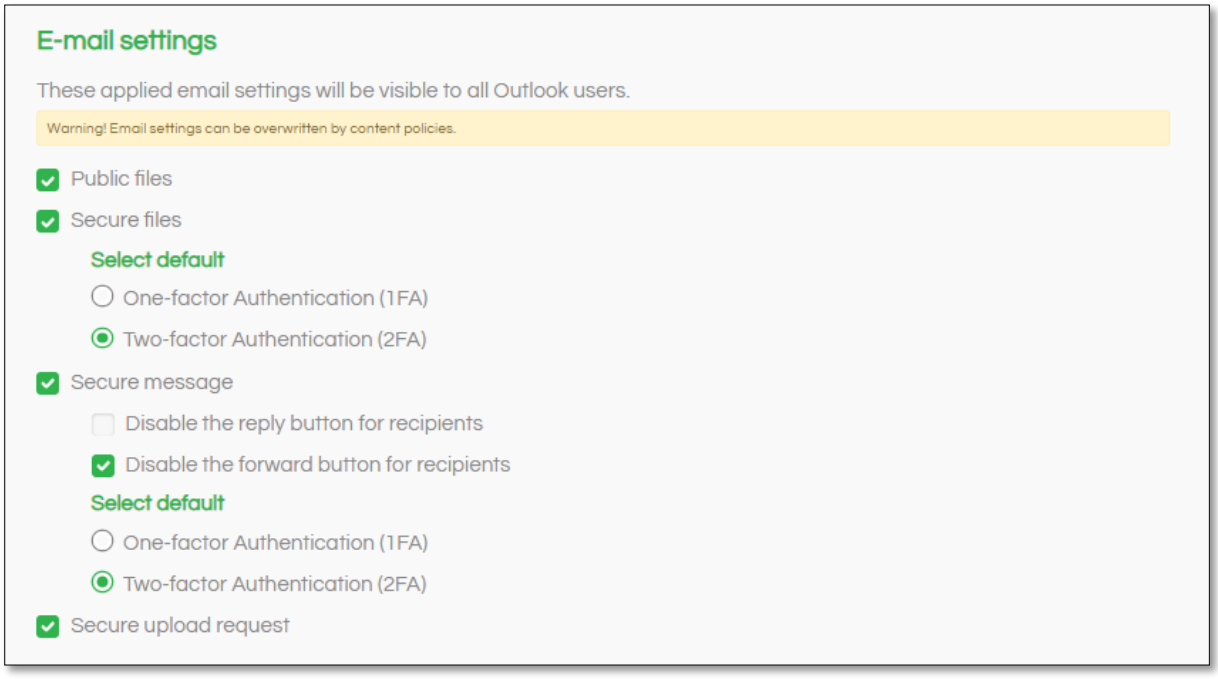
When users are added manually, they will receive an activation email to activate the account.

Please note: for customers linked to Single Sign-on (SSO), these users are added automatically. This takes place when they log in using the Outlook plug-in or any other authentication pages of SmartLockr.

1.1. Outlook settings

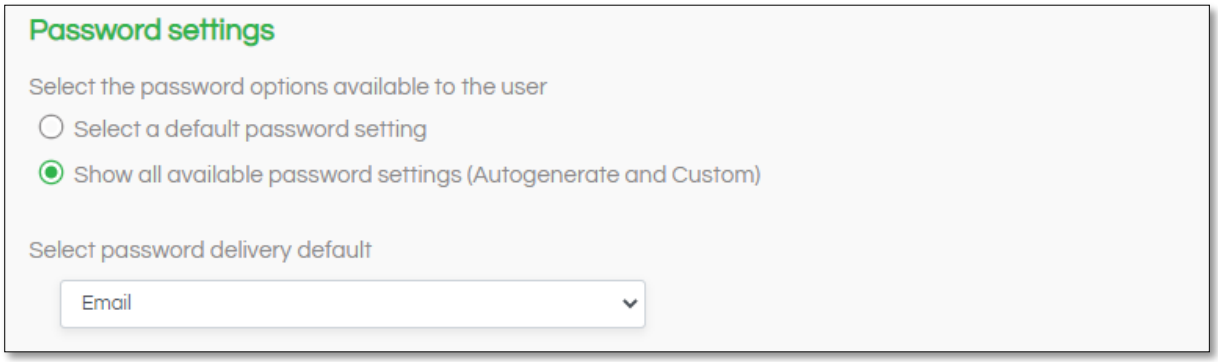
Email settings

The email settings allow you to configure how SmartLockr should be used. There are several options: public files, secure files, secure message, and secure upload request. Indicate whether to use one-factor or two-factor authentication:



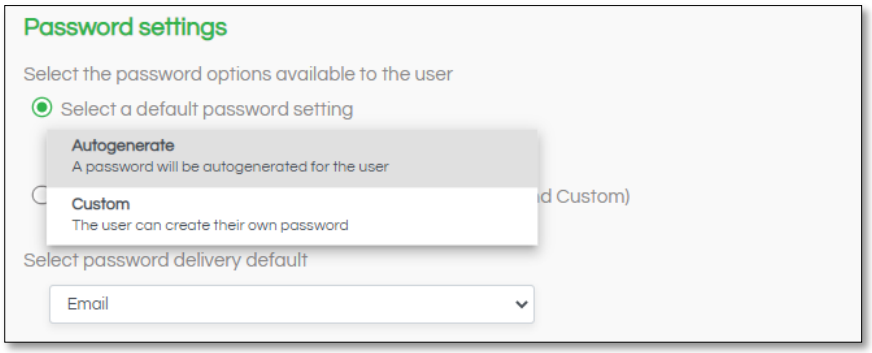
Password settings

When 1FA is applied, recipients can only access the message with a password. The password settings can be configured here:



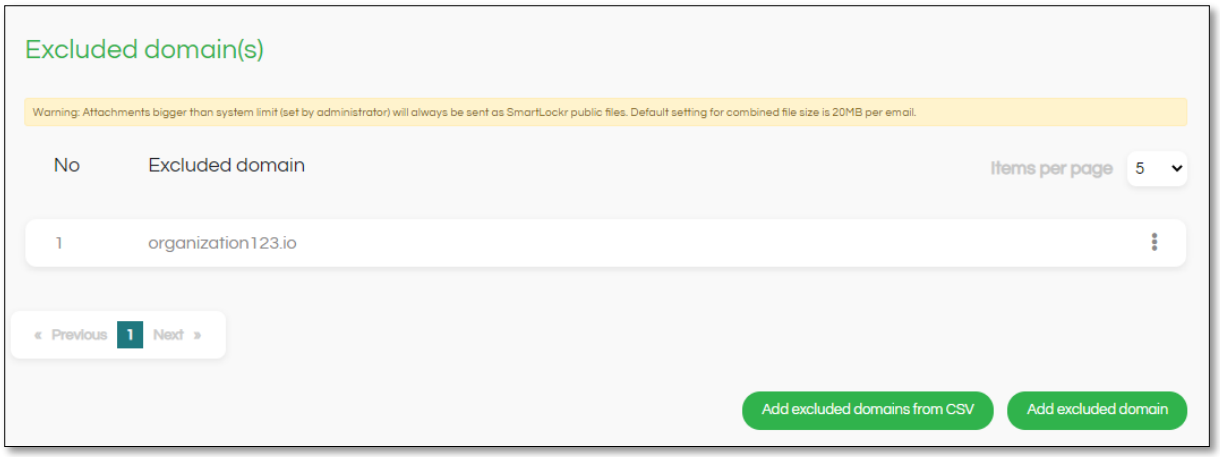
The users create a password for the recipients, which is sent through SmartLockr. There are two options: the password can be generated automatically or created by the user.

You can choose to keep both options open to the user or set one of the two options as default.



1.2. Recipient policy

There is an option to exclude domains so that emails are sent as normal emails. This may be desirable if, for example, you have a lot of contact with certain relations outside the organization, for which you do not need extra security from SmartLockr. Or when you communicate with organizations, for example, where employees are not allowed to click on links in emails:



As a system administrator, you can also upload multiple excluded domains at the same time with a CSV file.

1.3. Security settings

In addition to excluding domains, you can also disable ongoing sessions for users:

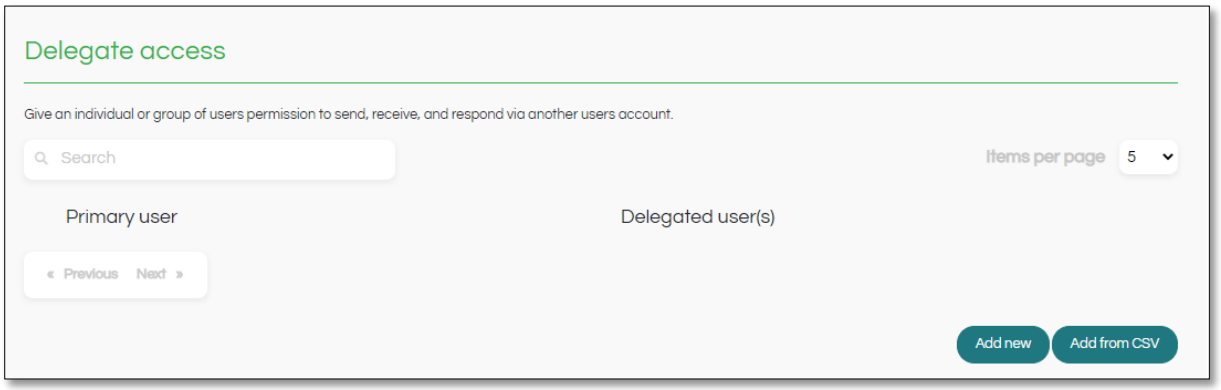
This prevents the existing logged-in sessions in the browser to run in the background, which would facilitate access to Smartlockr messages and/or files by third parties.

1.4. Authorized access

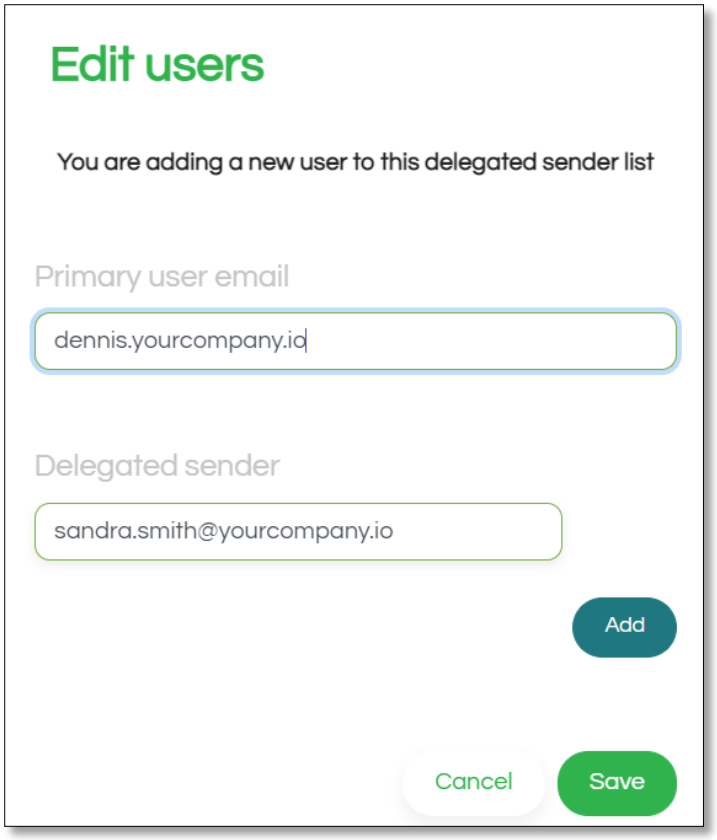
There is the option of granting a user or a group access to another user's inbox (individual inbox) or to a shared inbox. This allows users to send, receive and respond to incoming emails from the other inbox. This requires authorized access.

Authorizing user(s) for the Individual inbox

You can authorize others (Authorized User) to use someone else's inbox (Primary User). You do this by clicking the button “Add new”:



You will see the following screen, where you can add one or more Authorized Users:



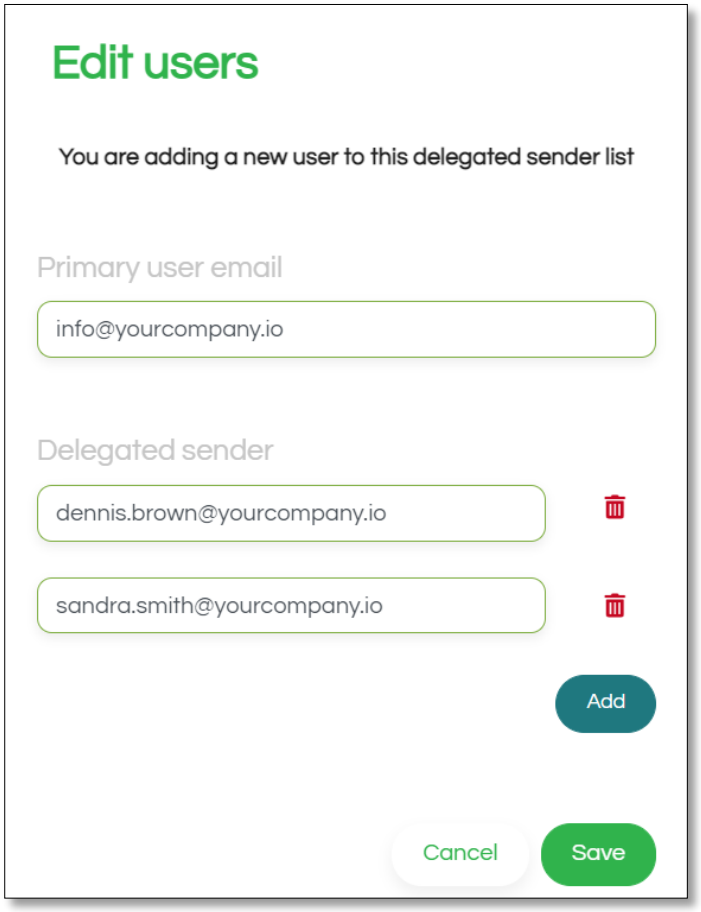
Please Note: In order to use the Primary User's email address, this email address must be known as a user within SmartLockr (see 2. Users).

If you click on the bottom button “Save”, the settings will be saved in SmartLockr:

Please note: To authorize a user, you also need to set the authorization settings within Office365. Once this is done, the inbox can be used by the Authorized User.

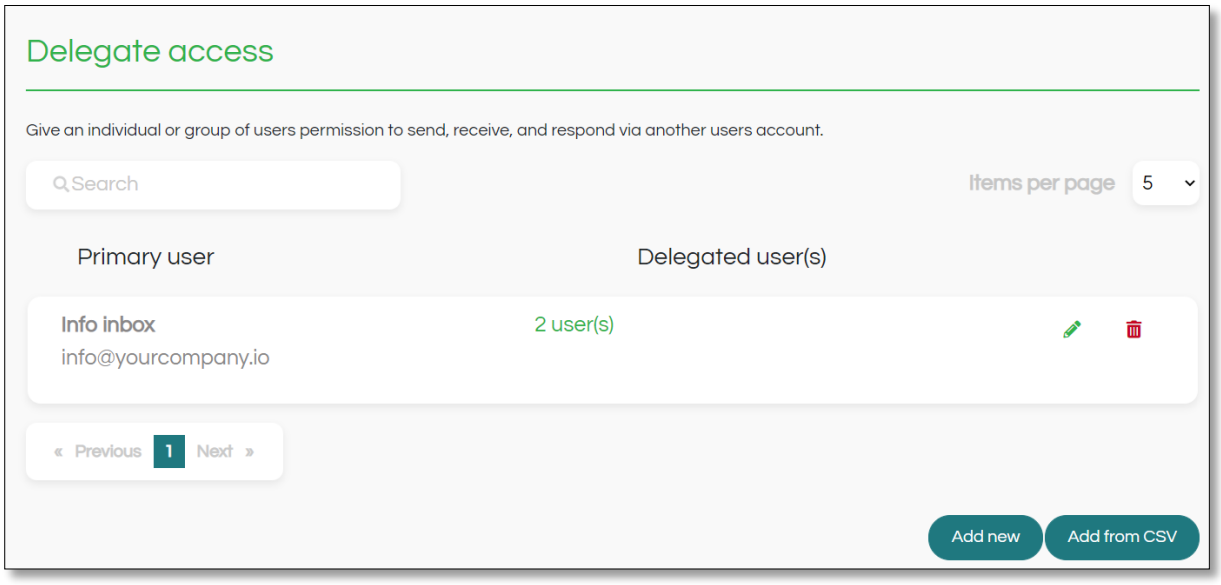
Authorizing user(s) for the Shared Inbox

It is also possible to use a shared inbox as a group, such as *info@yourcompany.io* and *administration@yourcompany*.io Authorizing users for the shared inbox works in the same way as authorizing users for the individual inbox:



Please note: In order to use a shared inbox, it is important to add this email address as a user (see 2. Users). A license is required for the shared inbox, which means that shared inboxes can only be used if these email addresses have been added as a user.

In the overview “Authorized access”, you can then see who has access to the inbox, who is authorized to work in a user’s inbox, and you can adjust and/or delete users where necessary:



02. Content Policy

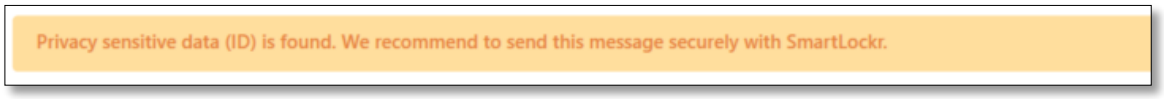
The content policy allows you to apply appropriate security for sensitive content that requires it. As an administrator, you can set content filters for this. These are filters based on:

- **Words** that are sensitive within your organization, such as "Citizen Service Number *(BSN)*", "Patient File" or "Passport"; or
- **Regular expressions (RegEx)** or patterns through which a system will understand a text and the context around it. Think of the 9-digit Citizen Service Number *(BSN)* "123456789" or "234-2234-234". The latter is an example of a pattern that could be specific within your organization (XXX- XXXX-XXX).

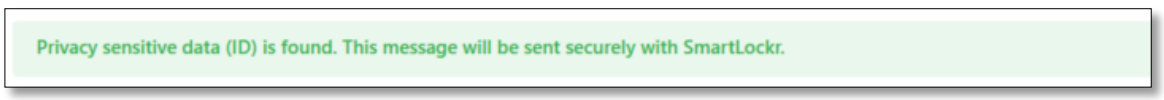
2.1. Policy types by trigger words

If users process content filters while composing a message, SmartLockr will be triggered. Three situations can arise, depending on the settings:

1. The user's attention is drawn to the fact that sensitive content has been included in the message. It is recommended to send the message securely with SmartLockr:

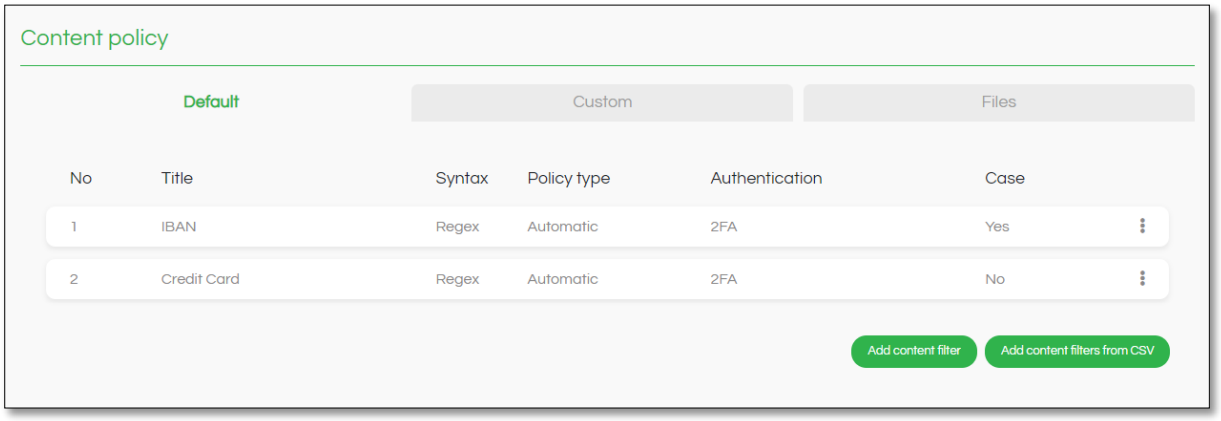


2. SmartLockr switches on automatically but can be turned off by the user.
3. SmartLockr switches on immediately and the message is forced to be sent with one or two-factor authentication. This setting cannot be changed by the user:

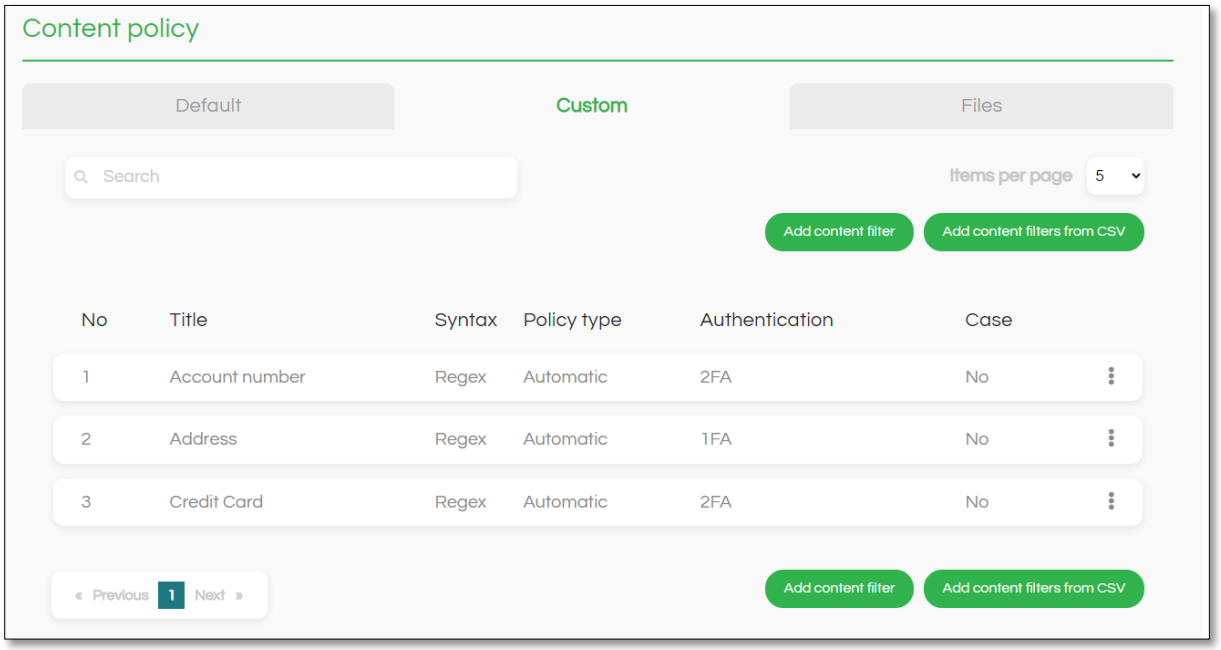


2.2. Trigger on words, regular expressions, and files

SmartLockr has a standard library of words that many organizations consider sensitive information:

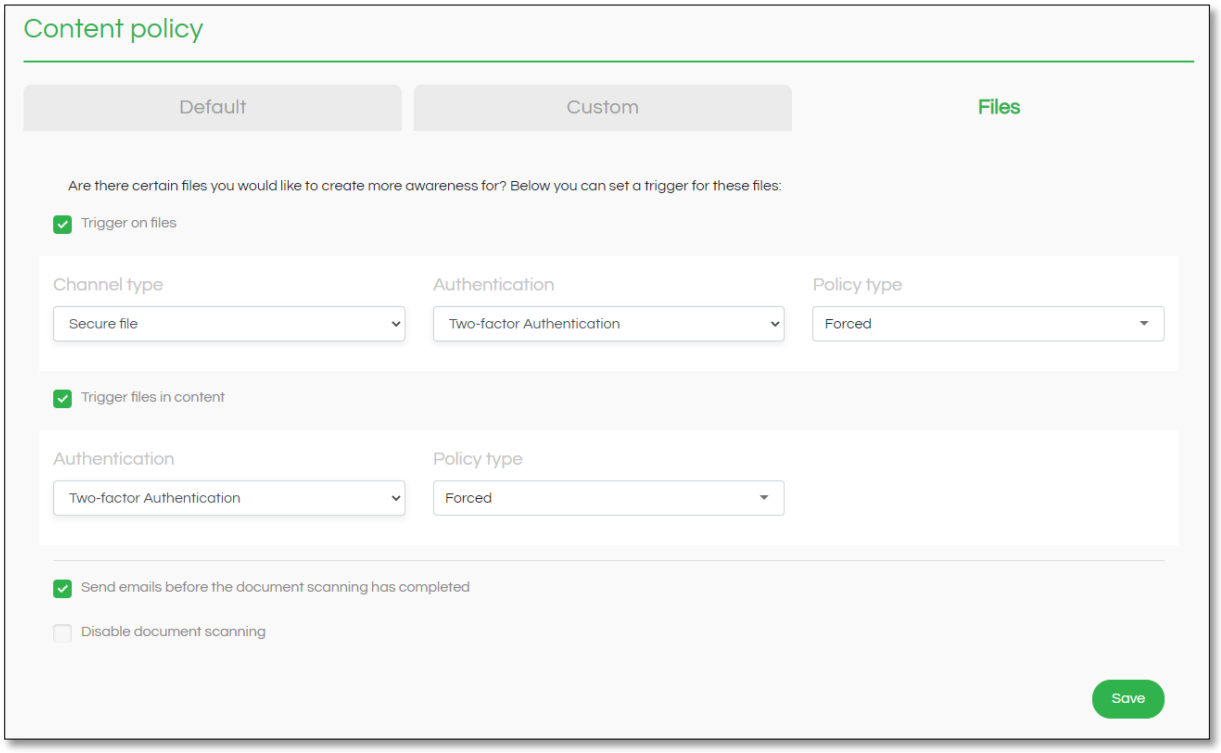


You can also add words to this library, such as "patient record" and "Citizen Service Number *(BSN)*", as in this example:



If you want to edit any words after you have entered them into the admin portal, you can easily find them by using the search bar at the top of the screen.

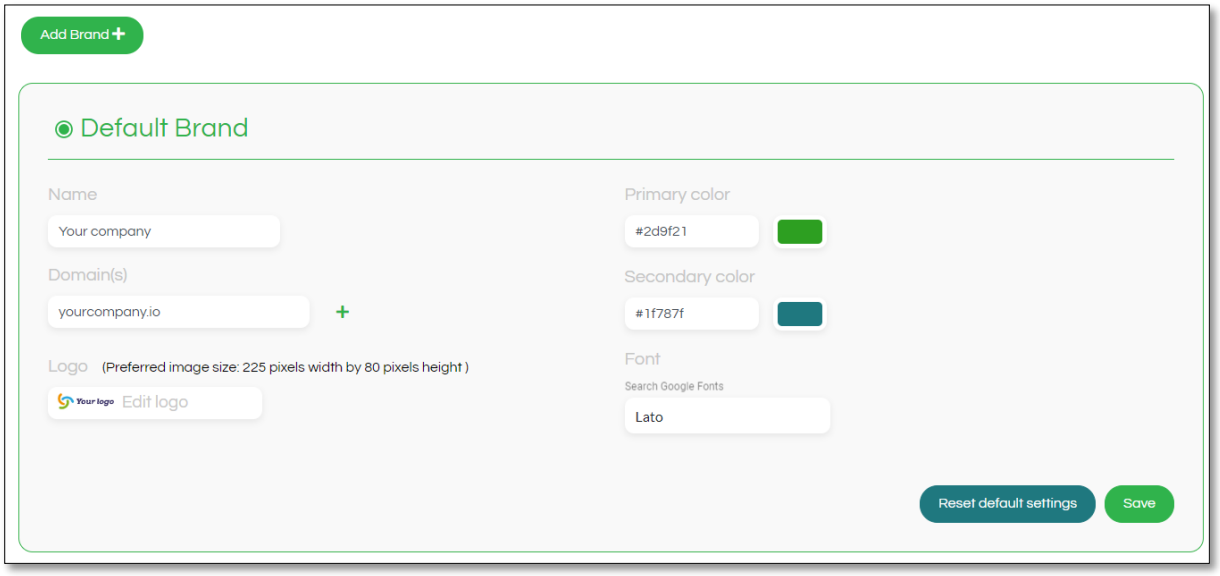
In addition to triggers on words, it is also possible to set triggers on files. As a SmartLockr administrator, you have the option to send an email with one or more supported documents only after the scan of this documentation has been completed:



If there are files for which you want to create more awareness, you have the option to do that with a trigger on files or content. If your organization wants to apply a content policy that differs in many ways from the standard SmartLockr content policy, system administrators can upload one or more CSV files with a content policy simultaneously.

03. Branding

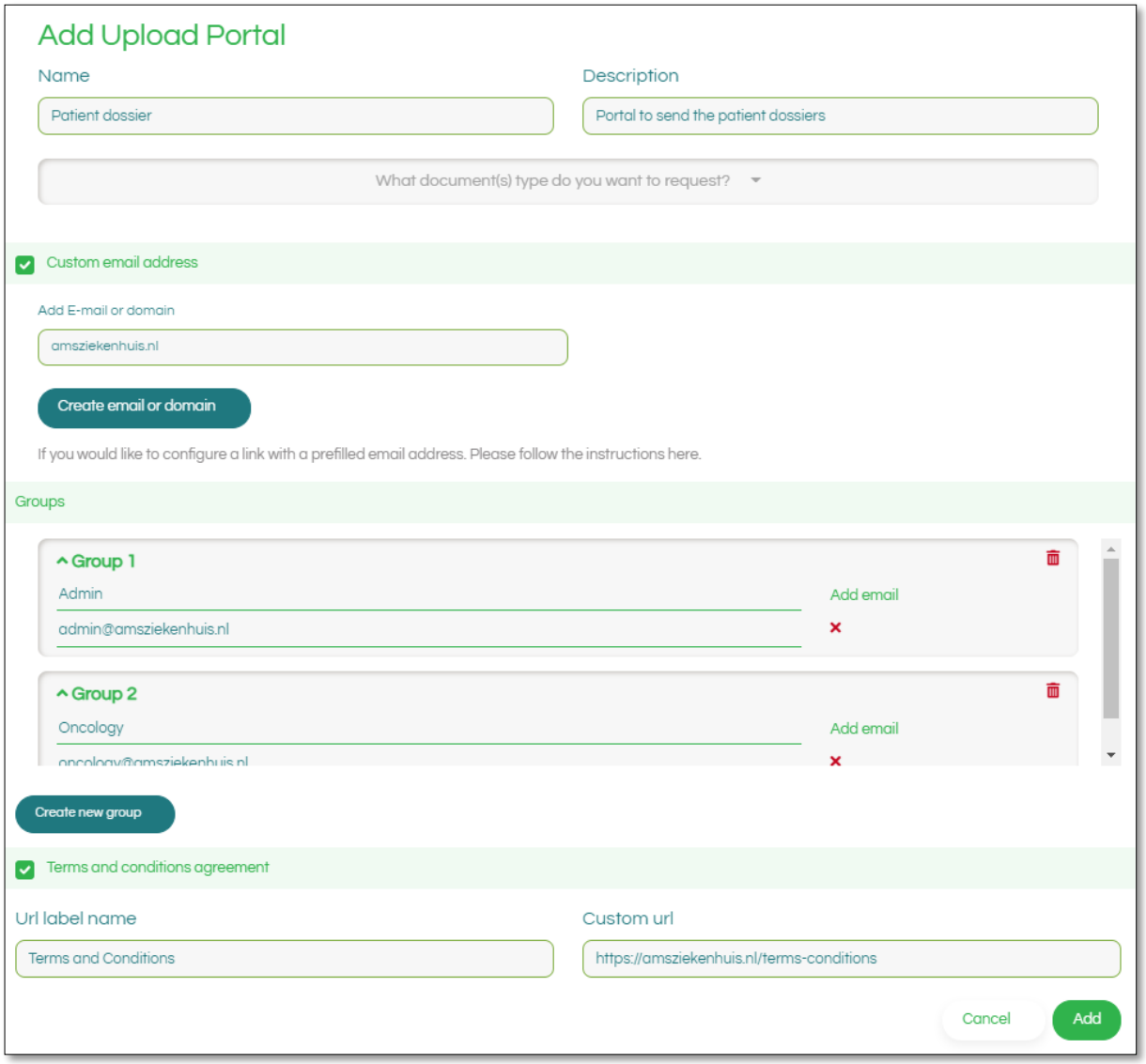
Your branding ensures recognizability of your organization. That is why you can implement your corporate identity, so that emails and portals have the recognizable image of your organization. If there are multiple corporate identities, you can add these:



04. Upload Portal

With upload portals, the organization will receive files easily and securely. It is therefore possible to create different portals for the different files your organization receives. You can also indicate which type of file you want to receive, who or which departments should be notified and who should receive the files.

When you click on “Add upload portal”, you will see the screen where you can set up the portal:



These are the available settings:

- **Name**

  This is the name of the portal, as recipients see it.

- **Description**

  A short description clarifies what this portal is for.

- **Request file types**

  You can preset which file types you wish to receive (see 6. Document types).

- **Custom email address**

  Set which departments and/or persons should receive the files. People who upload the files do not have to add recipients as you have already set this up in advance. This will also make it impossible to send the file to another email address or domain. If you leave this field empty, the sender can choose the recipient address themselves.

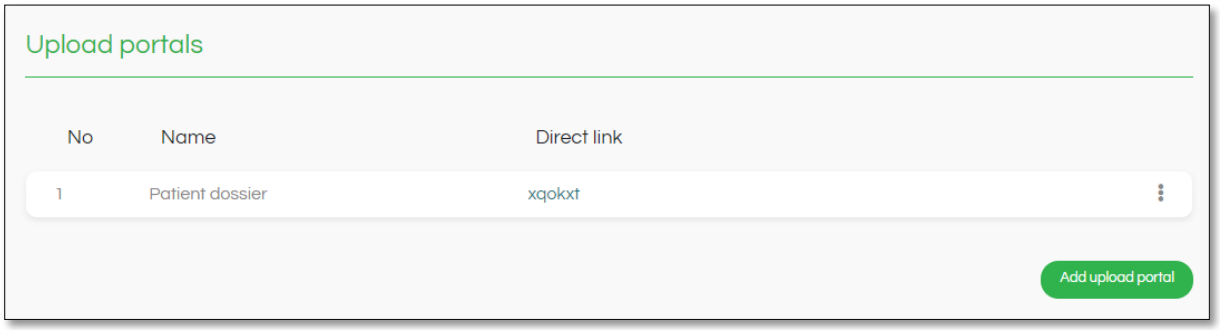
- **Groups**

  By creating groups and linking email addresses to them, you can let those who need to upload the files choose which department to send the files to.

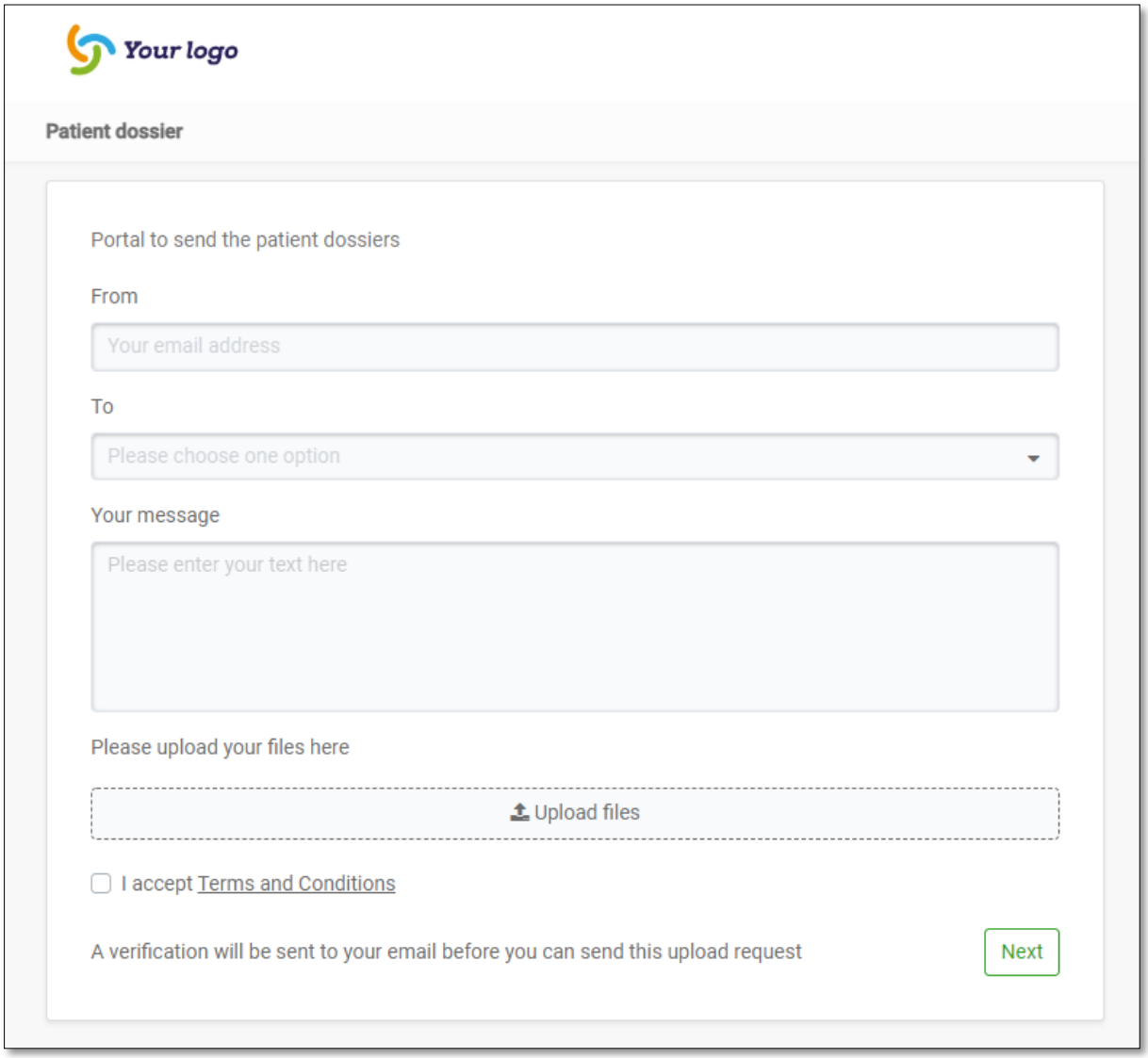
- **Terms**

  In some cases you want to add the terms and conditions of your organization. You can add these yourself with a link to the terms and conditions as they can be found on your website, for example.

Once the upload portal is created, it will be added to the list:

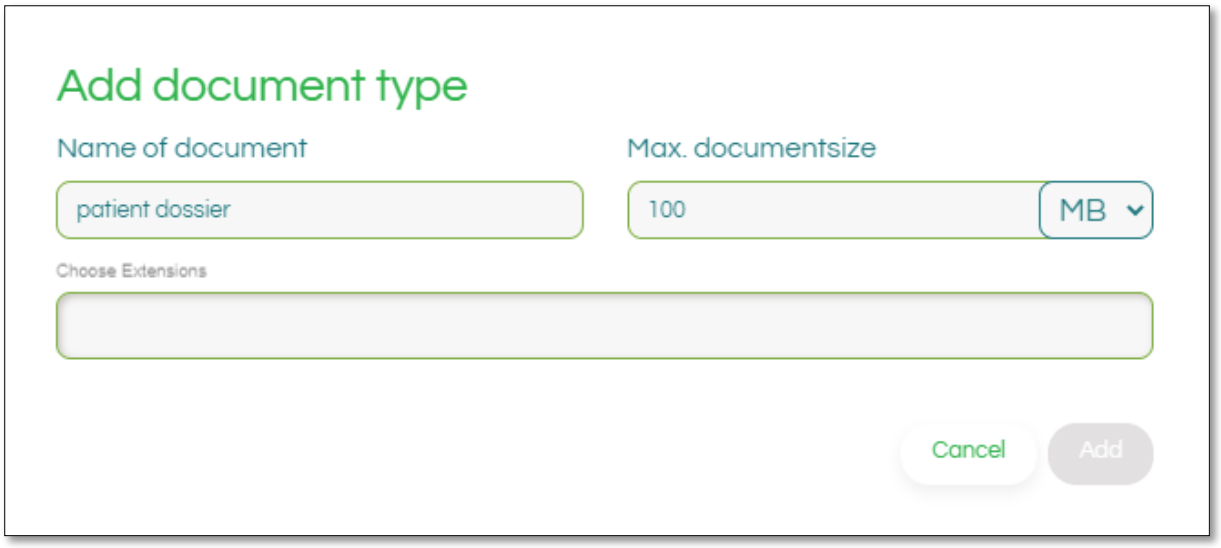


The direct link takes you to the portal page, where the settings you have made are immediately visible:

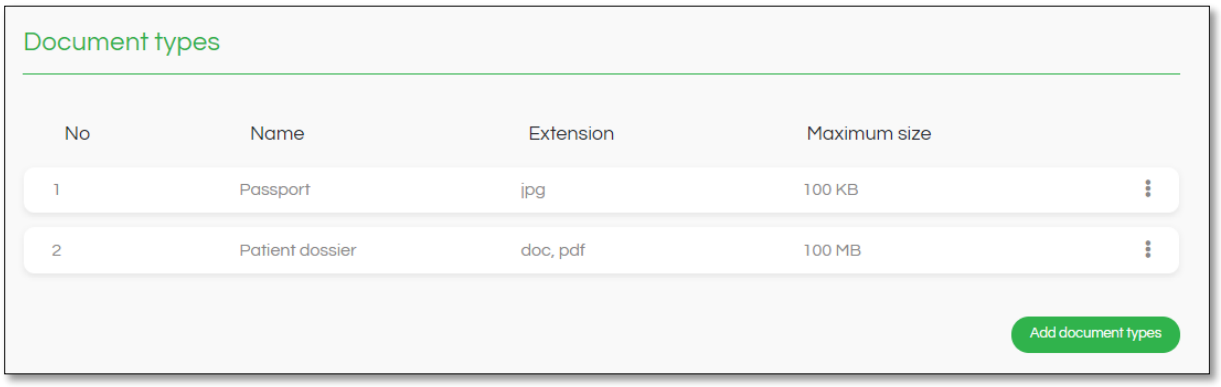


05. Document Types

Files are requested by email through upload requests and portals. To make it easy, you can indicate which type of file you wish to receive. Simply indicate which extension (.doc, .docx, .pdf etc.) and maximum size the file should have:



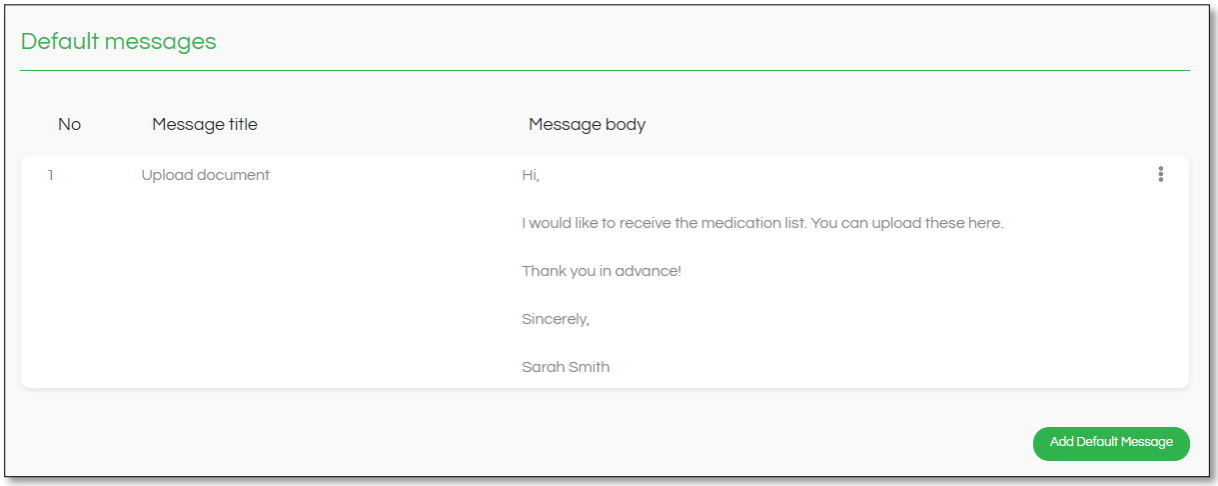
The overview will look like this:



By pre-setting which files you wish to receive, you prevent wrong or even malicious files from being uploaded.

06. Default messages

Are upload requests used to regularly request the same type of file? Then you can set default messages, so that the user can work more efficiently:



07. Email Domain

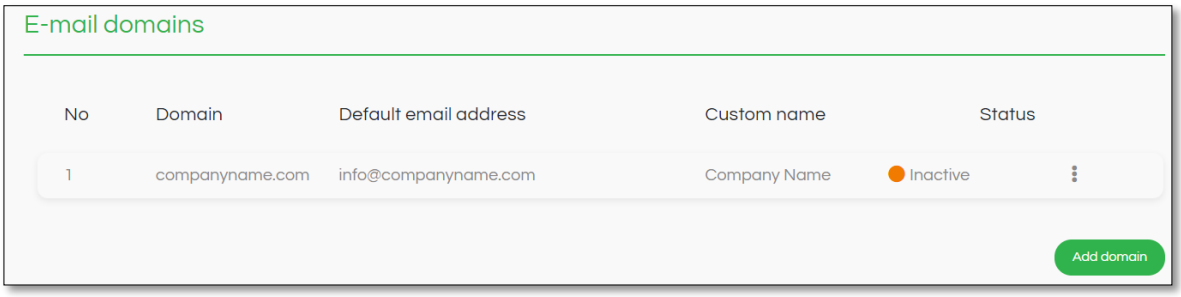
Notification emails are sent from SmartLockr, unless you configure it differently. You can customize it so that recipients receive emails from a domain that is recognizable to them.

Follow the below steps to set up the email domain you would like your recipients to see.

1. Click on 'Add domain' after choosing the option 'Email domains' in the admin portal menu. A pop-up window will now open.
2. In the field 'Default email address' you add the email address you would like to use. After this is done, the field 'Domain name' will be filled in automatically.
3. Now you can choose which name you would like your recipients to see when they receive emails from you. Enter this in the field 'Customer sender name'.
4. Click the 'add' button after making sure that everything has been filled correctly.

5. A few settings will now appear that need to be configured to your DNS server(s). If you cannot do this yourself, we recommend that you ask your IT department or IT partner to help.
6. You will now receive an email to the address that you chose. Please verify the address by clicking this email.
7. Click on the verify button when you have finished the DNS changes (in step 5) and email verification (in step 6). SmartLockr's servers will test the DNS changes to verify that if everything is correctly set up. If this is the case, the feature will turn itself on automatically.

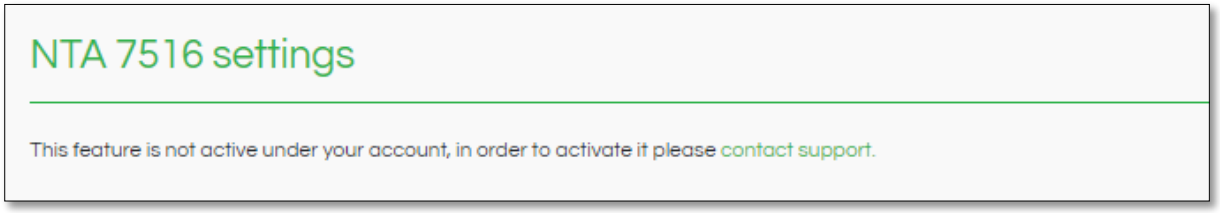
You are now ready to go! If you have more than one email domains, you can repeat the steps above to add them. Via the screen you see below, it is also possible to activate and deactivate your different domains.



08. NTA 7516 Settings

The NTA 7516 is a privacy standard in the Netherlands that ensures private health information is sent out securely. It is mainly used for the healthcare sector, municipalities, and the legal sector.

SmartLockr lets you communicate in NTA 7516 compliant way, but it is a feature that must be activated. If you see the below screen in your admin portal, it means that it is not active on your account. If you would like to start using this feature, you can contact Customer Support.

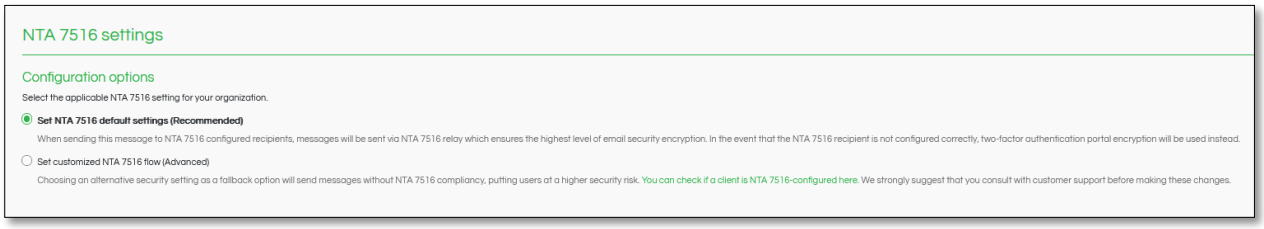


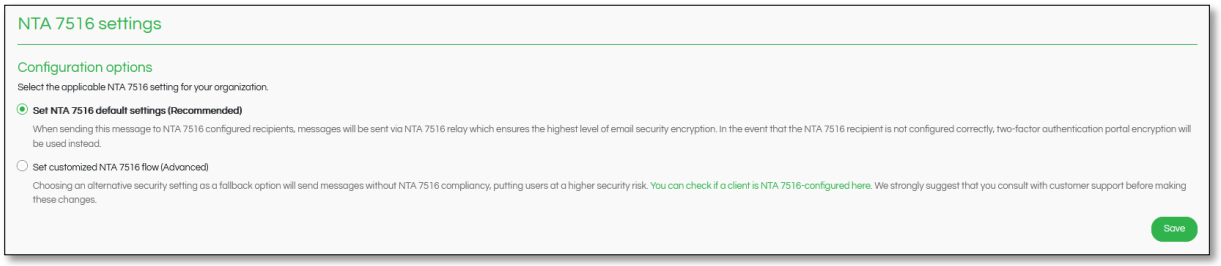
When the NTA 7516 feature has been activated on your account, you can partially customize how you would like to use it. Below we explain your two options and how they work.

8.1. Option 1: Set NTA 7516 default settings (Recommended)

Messages to NTA 7516 configured recipients will be sent via NTA 7516 relay. This is only done when two-factor authentication (2FA) is needed. If the recipient is not configured correctly according to NTA 7516, they will instead receive the email with SmartLockr's two-factor authentication (2FA) as a fall back option.

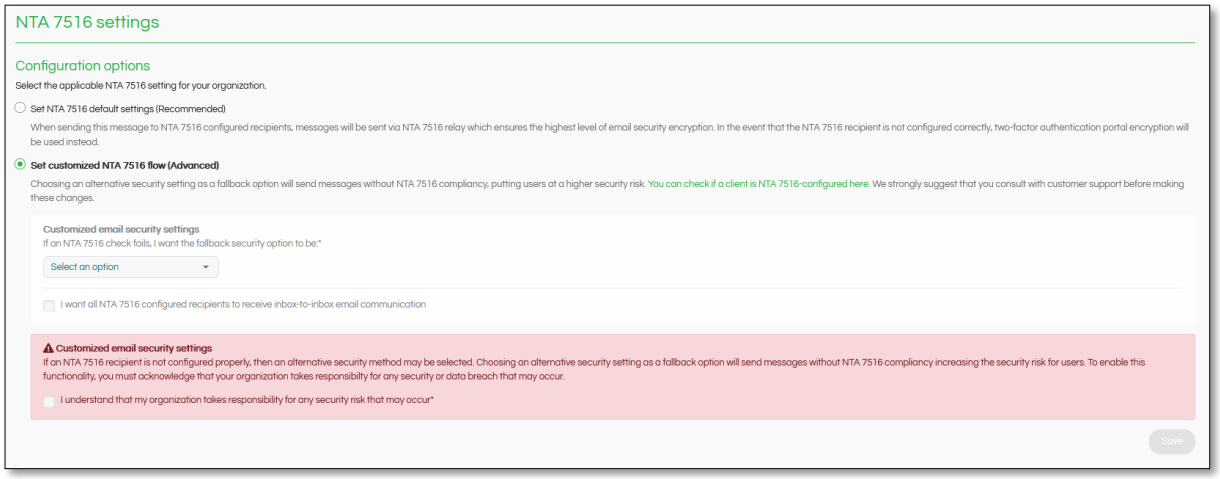
Sending an email with SmartLockr's two-factor authentication means that the recipient's phone number must be filled in by the sender. The recipient then receives a SMS code which gives them access to the email.





8.2. Option 2: Set Customized NTA 7516 flow (Advanced)

Messages to NTA 7516 configured recipients will be sent via NTA 7516 relay. If the recipient is not configured correctly according to NTA 7516, you can choose your fall back security option yourself.



The customized choice can be preferable when sending emails to an address without a clear recipient, like a shared inbox. In this case, the sender might not have access to a phone number for the recipient and therefore two-factor authentication with a SMS code won't work. In this scenario, a fall back option with one-factor authentication (1FA) could be a better choice.

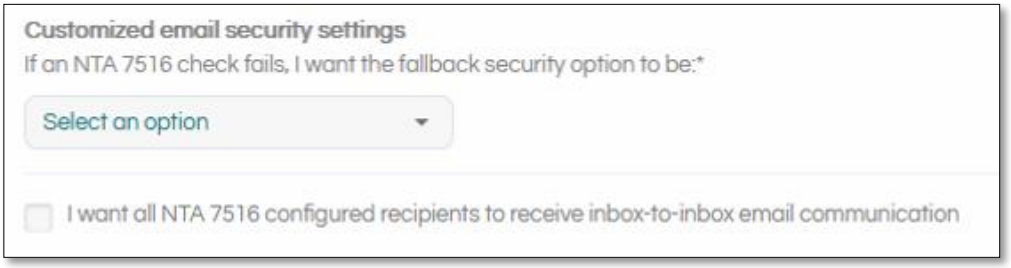
With the customized setting you can choose if your fall back option should be:

- Secure message (2FA)
- Secure message (1FA)
- Secure file (2FA)
- Secure file (1FA)
- Public file

Please note, however, that if you do choose a fall back option with one-factor authentication or public file, it will no longer be NTA 7516 compliant.

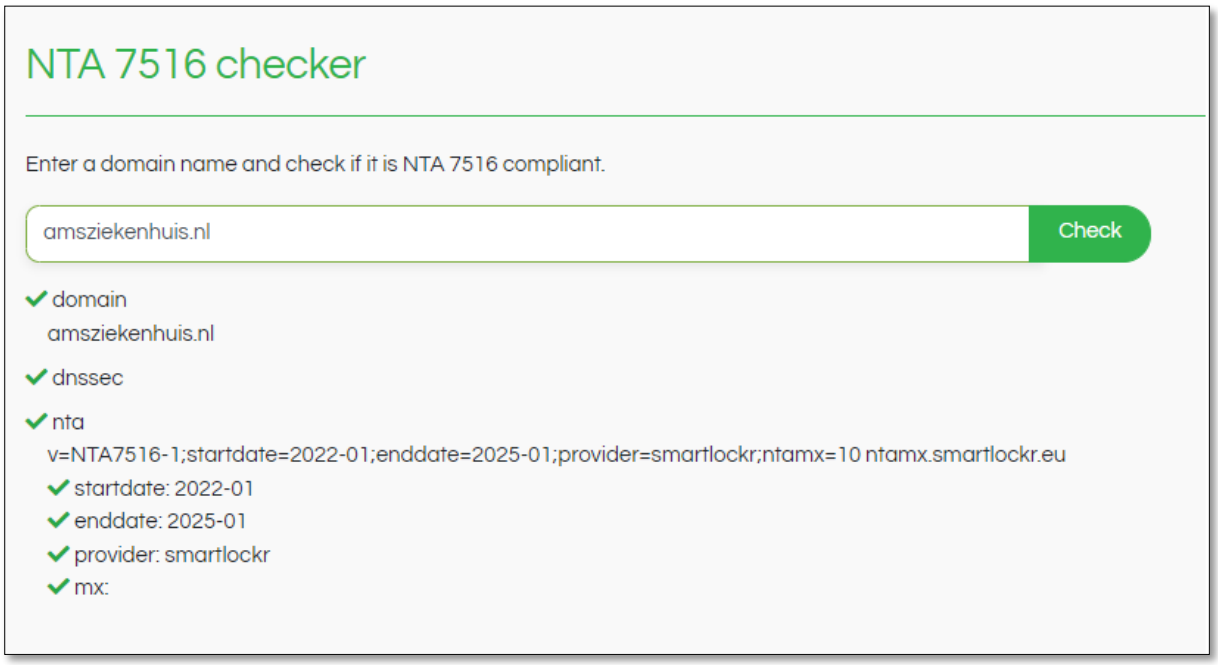
With the customized option, you can also choose that all NTA 7516 configured recipients will receive inbox-to-inbox communication. This means that your message will always be sent via the NTA 7516 relay, rather than only when 2FA is needed. If this is not possible, your fall back option will be used instead.

You choose this option by checking the box “I want all NTA 7516 configured recipients to receive inbox-to-inbox communication”.



8.3. NTA 7516 checker

With this function you can see if a domain is NTA 7516 compliant before sending an email. Simply put in the domain name and press check, like shown in the screen below.

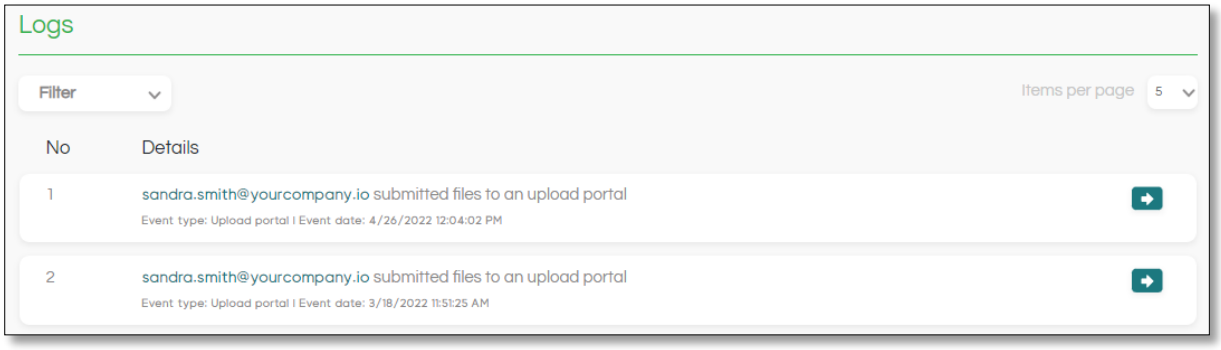


09. API & SMTP Relay Service

Should your organization use the SmartLockr API or SMTP Relay Service, you can also control these settings through the administrator portal. These settings are turned on by default and require several additional settings.

10. Logs

All activities sent with SmartLockr are stored in the logs. Here you can see what each user has sent/created, through which channel and when:



If information has been sent incorrectly by users, administrators have the rights to block the recipient(s), file(s) and the entire email for regular users.

However, regular users can also see their own logs and take the same actions as listed above, by visiting this page: https://admin.smartlockr.eu.

11. Learn more

Do you have any questions after reading this manual? You can always contact our Support Team directly at support@smartlockr.eu or +31 (0)20 - 244 0350 (option 1).