SMARTLOCKR

SmartLockr beheerdersportaal

Alles wat je als beheerder nodig hebt. Overzichtelijk, in één portaal.

Over het beheerdersportaal

Met dit portaal heb je als beheerder een duidelijk overzicht van alle activiteiten. Dit is namelijk de omgeving waar je o.a. inzichten krijgt over het gebruik van SmartLockr. Daarnaast kun je hier ook verschillende instellingen doen, waardoor je altijd controle behoudt over de veilige uitwisseling van gevoelige informatie binnen de organisatie.

Het beheerdersportaal bestaat uit de volgende onderdelen:

- **Logs**
- **Gebruikersmanagement**
- **Contentbeleid**
- **Eigen huisstijl**
- **Uploadportaal**
- **Documenttypes**
- **Standaardberichten**
- **E-maildomein**
- **API instellingen**
- **SMTP Instellingen**

Hierna zal elk onderdeel kort worden toegelicht. Op deze manier is het duidelijk wat je als beheerder kunt verwachten en welke mogelijkheden er zijn.

Logs
Alle activiteiten die met SmartLockr zijn verstuurd, worden opgeslagen in de logs. Hier kun je vervolgens zien welke gebruiker iets heeft verstuurd, via welk kanaal en wanneer:

Mocht het zo zijn dat er informatie foutief is verzonden, dan heb je de mogelijkheid om zowel de ontvanger(s) te blokkeren als ook het hele bericht.

Gebruikersmanagement

Voor gebruikers binnen de organisatie kunnen er verschillende instellingen worden gedaan. Zo kun je:

- Gebruikers toevoegen, accounts activeren en deactiveren;
- De opties *Openbare bestanden*, *Beveiligde bestanden*, *Beveiligd bericht* en *Beveiligd uploadverzoek* activeren of deactiveren. Daarnaast kun je *een- of twee-factor authenticatie* forceren (slechts mogelijk voor *Beveiligde bestanden* & *Beveiligd bericht*);
- Domeinen uitsluiten, zodat informatie niet met ontvangers van deze domeinen kan worden gedeeld;
- Veiligheidsinstellingen verrichten, waarbij je doorlopende sessies voor gebruikers kunt uitschakelen.

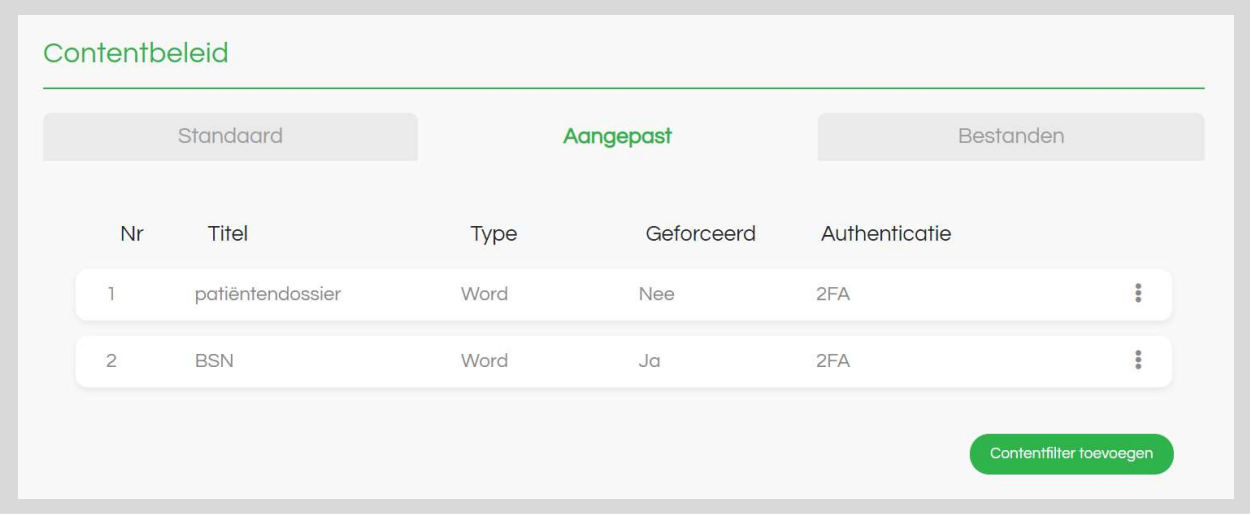
Contentbeleid

Met het contentbeleid kun je extra aandacht besteden aan gevoelige content. Als beheerder stel je hier contentfilters voor in. Dit zijn filters op basis van:

- **woorden** die binnen je organisatie gevoelig zijn zoals bijvoorbeeld “Burgerservicenummer”, “Patiëntendossier” of “Paspoort” of,
- **reguliere expressies (RegEx)** oftewel patronen waardoor een systeem tekst en de context er omheen zal begrijpen. Denk hierbij aan de 9-cijferige reeks van een Burgerservicenummer “123456789” of “234-2234-234” wat misschien specifiek is binnen de organisatie voor bijvoorbeeld patiëntendossiers.

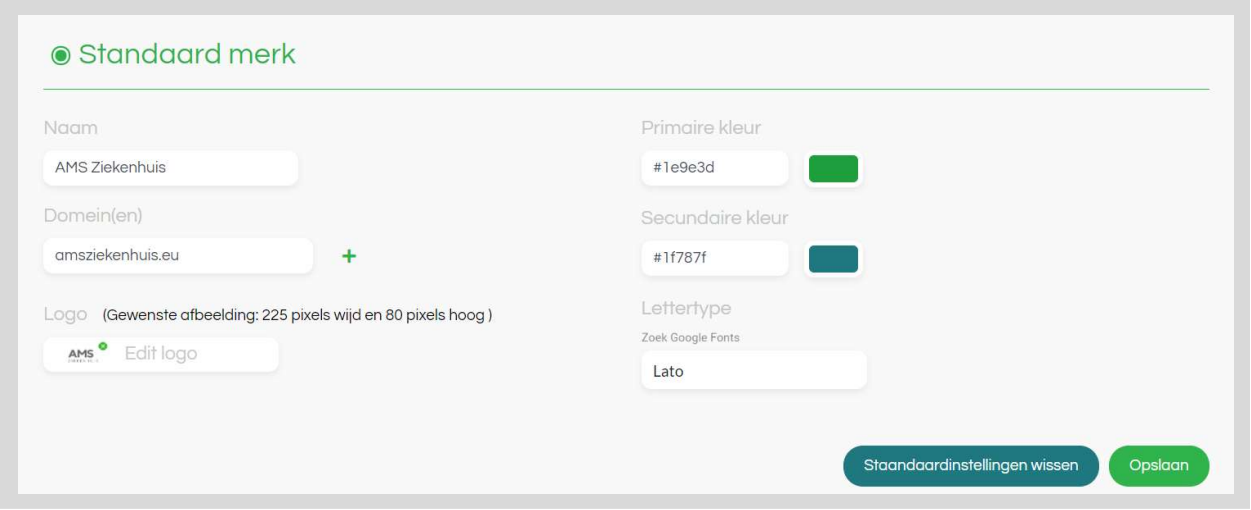
Als de gebruiker een van deze filters verwerkt tijdens het opstellen van een bericht, wordt SmartLockr getriggerd. Daarbij kunnen zich de volgende situaties voordoen, afhankelijk van de instellingen:

- De gebruiker wordt erop geattendeerd dat er gevoelige content in het bericht is verwerkt. Er wordt aangeraden om het bericht veilig te versturen met SmartLockr;
- SmartLockr springt direct aan en wordt geforceerd met twee-factor authenticatie verstuurd. Deze instelling is door de beheerder gedaan en kan niet worden aangepast door de gebruiker.



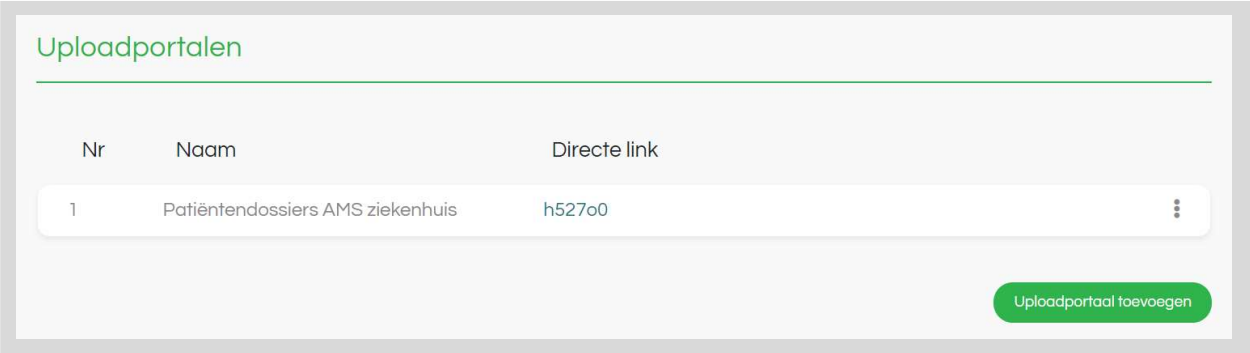
Eigen huisstijl

Een eigen huisstijl zorgt voor de herkenbaarheid van je organisatie. Daarom kun je jouw huisstijl doorvoeren, waardoor e-mails en portalen de herkenbare uitstraling van de organisatie krijgen. Mochten er meerdere huisstijlen zijn, dan kun je die ook toevoegen:



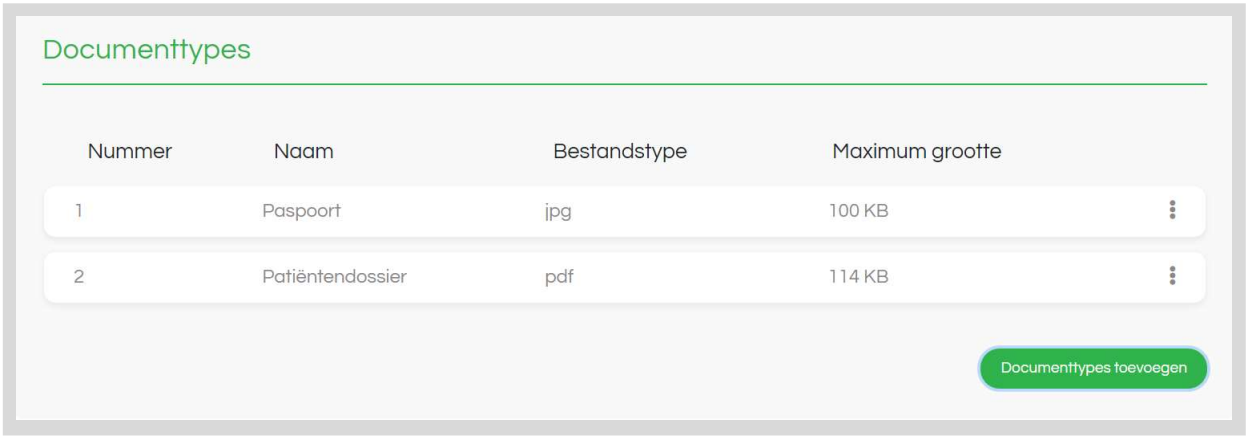
Uploadportalen

Met uploadportalen komen bestanden eenvoudig en veilig de organisatie binnen. Het is dan ook mogelijk om verschillende portalen aan te maken, voor de verschillende bestanden die je organisatie ontvangt. Daarbij kun je aangeven welk type bestand je wilt ontvangen, wie of welke afdelingen hiervan op de hoogte moeten worden gesteld en wie de bestanden dient te ontvangen:



Documenttypes

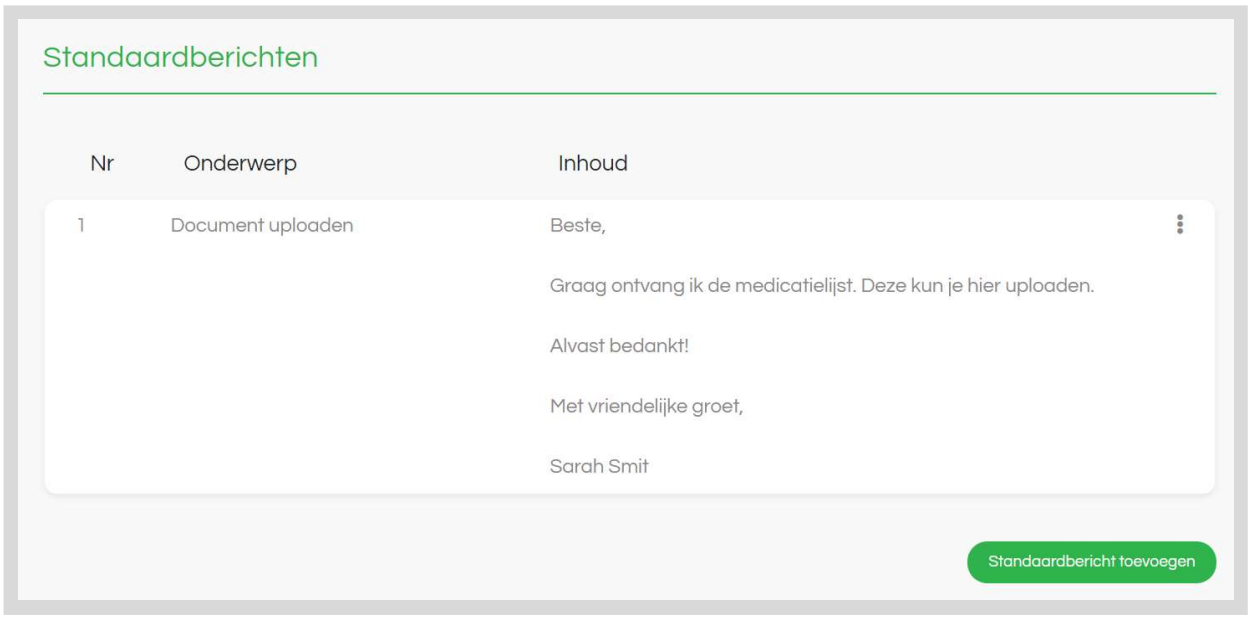
Met uploadverzoeken worden bestanden opgevraagd per e-mail. Om het makkelijk te maken, kun je daarbij aangeven welk type bestand je wenst te ontvangen. Je geeft eenvoudig aan welke extensie (doc, docx, pdf etc.) en maximum grootte het bestand dient te bevatten:



Zo voorkom je dat er verkeerde of zelfs schadelijke bestanden worden geüpload.

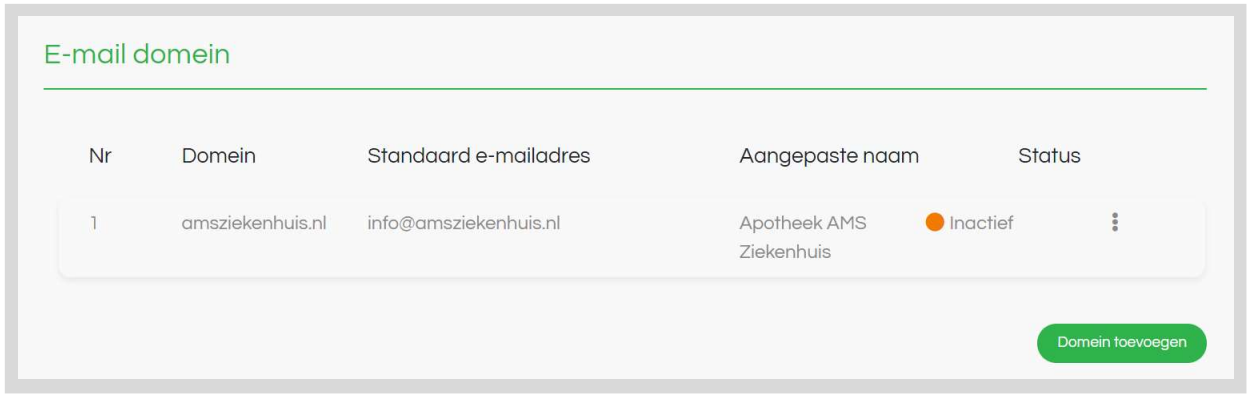
Standaardberichten

Worden uploadverzoeken gebruikt om met regelmaat hetzelfde type bestand op te vragen? Dan kun je hier standaardberichten instellen, zodat de gebruiker niet constant hetzelfde bericht hoeft op te stellen:



E-mail domein

Notificatie e-mails worden vanuit SmartLockr verstuurd, tenzij je dit anders instelt. Het is namelijk mogelijk om dit aan te passen naar je organisatie. Op deze manier krijgen ontvangers e-mails van een voor hen herkenbaar domein:



In dit scherm kunnen de verschillende domeinen worden geactiveerd en gedeactiveerd.

Mocht je als organisatie gebruik maken van de SmartLockr API of SMTP Relay Service, dan kun je deze instellingen ook via het beheerdersportaal regelen.

Bij vragen kan er altijd contact worden opgenomen met onze Support-afdeling via support@smartlockr.eu of 020 – 244 0350 (optie 1).