



SmartLockr

Beheerdersportaal

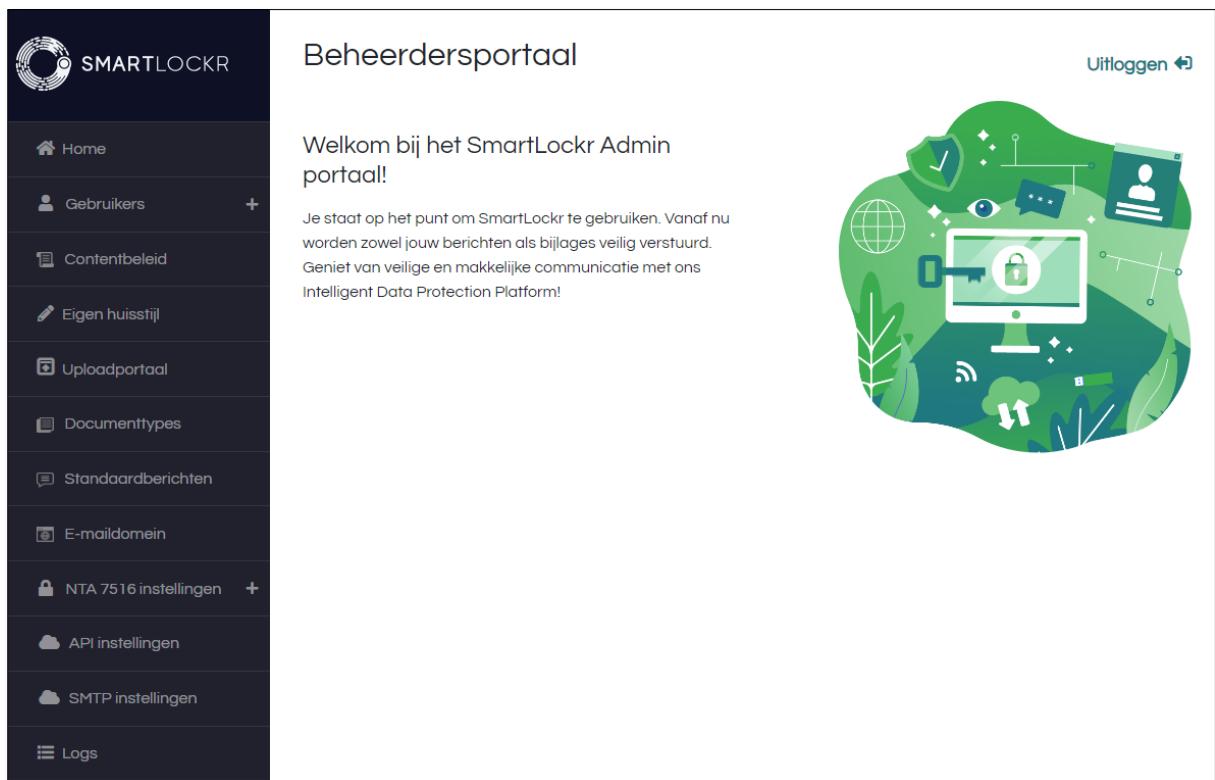
Inhoudsopgave

1. Gebruikers	4
1.1 Outlook instellingen	6
1.2 Ontvangersbeleid	7
1.3 Veiligheidsinstellingen	8
1.4 Toegang gemachtigden	8
2. Contentbeleid	12
2.1 Beleidstypes op triggerwoorden	12
2.2 Triggers op woorden, reguliere expressies en bestanden	13
3. Eigen huisstijl	15
4. Uploadportaal	16
5. Documenttypes	19
6. Standaardberichten	20
7. E-maildomein	21
8. NTA 7516 instellingen	22
8.1 Optie 1: Gebruik de standaardinstellingen van de NTA 7516	22
8.2 Optie 2: Stel aangepaste NTA 7516 flow in (geavanceerd)	23
8.3 NTA 7516 checker	24
9. API & Relay Service	25
10. Logs	26
11. Meer weten?	27

Inleiding

Met het beheerdersportaal heb je een duidelijk overzicht van alle SmartLockr activiteiten én heb je een centraal punt om alle instellingen te doen. Zo behoud je altijd de controle over de veilige uitwisseling van gevoelige informatie binnen de organisatie.

Als je inlogt in het beheerdersportaal, zie je een welkomstscherm en een menubalk aan de linkerkant waar je alle onderdelen van het portaal kan vinden. Hier kun je wijzigingen doorvoeren en monitoren hoe SmartLockr wordt gebruikt:

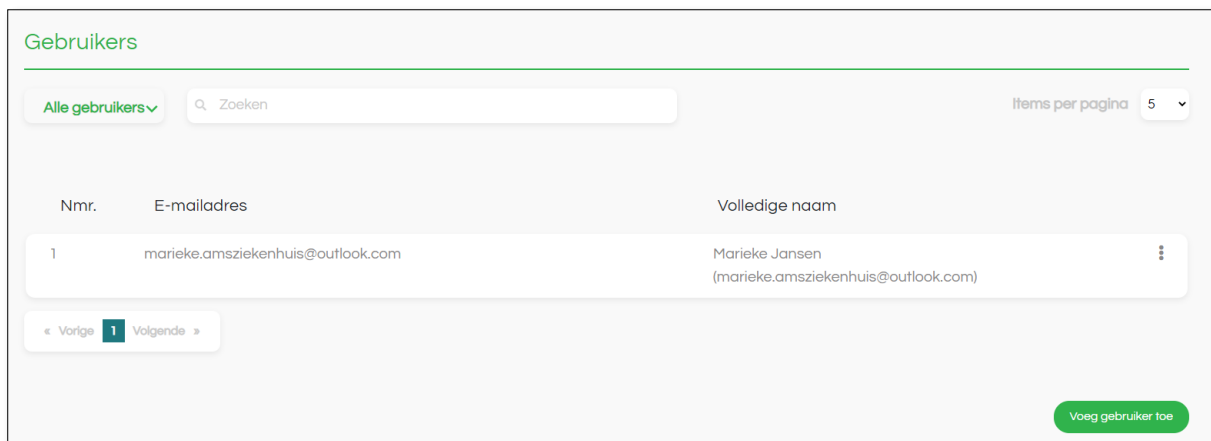


Hierna zal elk onderdeel kort worden toegelicht. Op deze manier is het duidelijk wat je als beheerder kunt verwachten en welke mogelijkheden er voor jou zijn.

01. Gebruikers

Onder “gebruikers” heb je een overzicht van alle SmartLockr gebruikers binnen de organisatie. Voor deze gebruikers kun je instellingen toepassen. Door richtlijnen op te stellen kun je het veilige gebruik van SmartLockr beter controleren.

Om te kunnen beginnen is het belangrijk om de aangeschafte licenties toe te wijzen aan gebruikers. Dit doe je door de gebruikers binnen de organisatie toe te voegen aan het beheerdersportaal:



Om gebruikers toe te voegen klik je op de groene knop “Voeg gebruiker toe” die je rechtsonder vindt. Vervolgens wordt er een scherm geopend waar je gebruikers kunt toevoegen.

Het toevoegen van gebruikers kan op twee manieren. Je kunt ze zowel handmatig toevoegen als importeren vanuit een CSV bestand. Wanneer je een of meerdere gebruikers upload via een CSV-bestand, kan je met SmartLockr tijd besparen, aangezien we gelijktijdig het(/de) account(s) voor je kunnen activeren en de licentie kunnen toewijzen.



Nieuwe gebruiker(s) toevoegen

Je kan ervoor kiezen om gebruikers handmatig toe te voegen of te importeren vanuit een CSV bestand.

Gebruiker handmatig toevoegen

E-mailadres

sarah.smith@amszorginstelling.nl

Naamweergave

Sarah Smith

Telefoonnummer

+31

Klik hier om nieuwe gebruikers te importeren vanuit een CSV bestand

Annuleren
Opslaan

Nadat je de gebruikers hebt toegevoegd, worden ze zichtbaar in het overzicht. Als je een gebruiker snel wilt vinden, kan je de zoekbalk bovenaan gebruiken om ze te vinden.

Gebruikers

Alle gebruikers
Zoeken
Items per pagina 5

Nmr.	E-mailadres	Volledige naam
1	sarah.smith@amszorginstelling.nl	Sarah Smit (sarah.smith@amszorginstelling.nl)
2	marieke.amsziekenhuis@outlook.com	Marieke Jansen (marieke.amsziekenhuis@outlook.com)

« Vorige 1 Volgende »

Voeg gebruiker toe

Wanneer gebruikers handmatig zijn toegevoegd, dan ontvangen zij een activatie e-mail om het account te activeren.

Let op: voor klanten die gekoppeld zijn aan Single Sign-on (SSO) worden deze gebruikers automatisch toegevoegd. Dit gebeurt wanneer zij inloggen middels de Outlook plug-in, of andere authenticatiepagina's van SmartLockr.

1.1. Outlook instellingen

E-mailinstellingen

Met de e-mailinstellingen kun je instellen hoe SmartLockr moet worden gebruikt. Er zijn namelijk verschillende opties: openbaar bestand, beveiligd bestand, beveiligd bericht en beveiligd uploadverzoek. Geef aan of er gebruik moet worden gemaakt van een-factor of twee-factor authenticatie:

E-mailinstellingen

Deze e-mail instellingen zullen zichtbaar zijn voor alle Outlook gebruikers.

Let op! Deze e-mailinstellingen kunnen worden overschreden door het contentbeleid.

- ☒ Openbare bestanden
- ☒ Beveiligd bestanden
 - Selecteer standaard beveiliging
 - ☐ Een-factor-authenticatie (1FA)
 - ☒ Twee-factor-authenticatie (2FA)
- ☒ Beveiligd bericht
 - ☐ Schakel reacties van ontvangers uit
 - ☒ Schakel doorsturen door ontvangers uit
 - Selecteer standaard beveiliging
 - ☐ Een-factor-authenticatie (1FA)
 - ☒ Twee-factor-authenticatie (2FA)
- ☒ Beveiligd uploadverzoek

Wachtwoordinstellingen

Wanneer 1FA wordt toegepast, krijgen ontvangers alleen toegang tot het bericht met een wachtwoord. De instellingen voor het wachtwoord kunnen hier worden ingesteld:

Wachtwoordinstellingen

Selecteer de wachtwoord opties die beschikbaar zijn voor de gebruiker

- ☐ Selecteer een standaard wachtwoordinstelling
- ☒ Laat alle beschikbare wachtwoorden zien (automatisch gegenereerd en custom)

Selecteer standaard wachtwoord ontvangst

e-mail

De gebruikers maken een wachtwoord aan voor de ontvangers, die via SmartLockr wordt verzonden. Daarbij zijn er twee opties: het wachtwoord kan automatisch worden

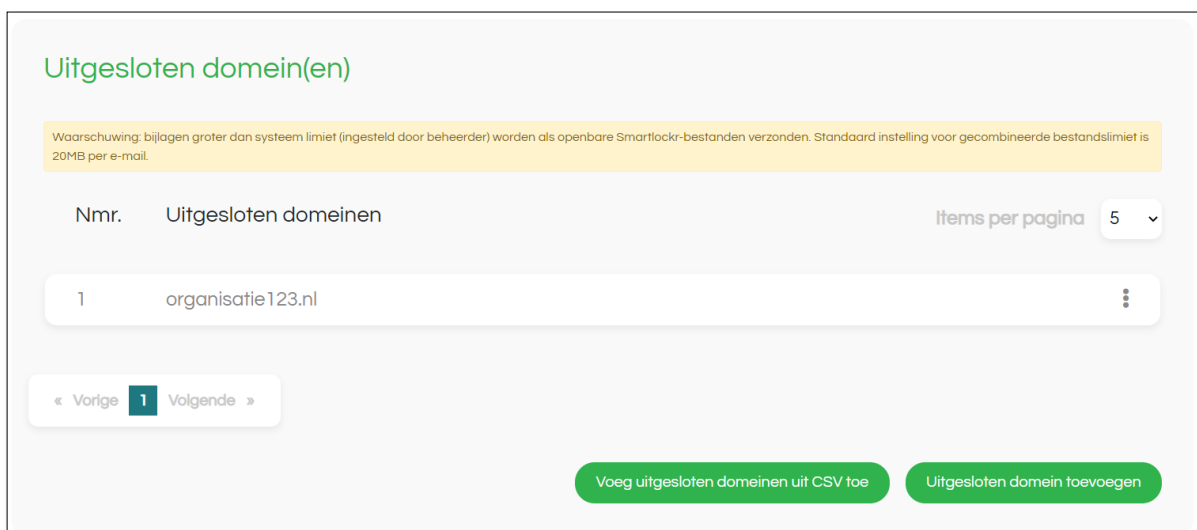
gegenereerd of de gebruiker maakt het wachtwoord zelf aan.

Je kan ervoor kiezen om beide opties open te houden voor de gebruiker of één van de twee opties als standaard in te stellen.



1.2. Ontvangersbeleid

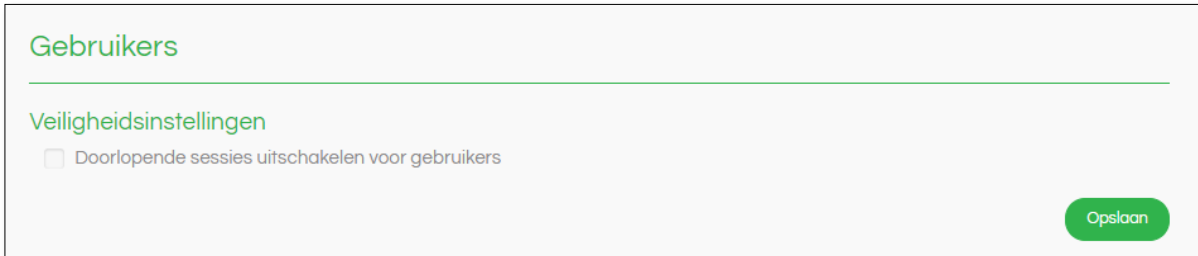
Er is de mogelijkheid om domeinen uit te sluiten, zodat e-mails als normale e-mails worden verzonden. Dit kan gewenst zijn als je bijvoorbeeld veel contact hebt met bepaalde relaties buiten de organisatie, waar je geen extra beveiliging van SmartLockr voor nodig hebt. Of wanneer je bijvoorbeeld communiceert met organisaties, waarbij de werknemers niet op links in e-mails mogen klikken:



Tevens kan je als systeembeheerder meerdere uitgesloten domeinen tegelijkertijd uploaden met een CSV-bestand.

1.3. Veiligheidsinstellingen

Naast het uitsluiten van domeinen, kun je ook doorlopende sessies voor gebruikers uitschakelen:



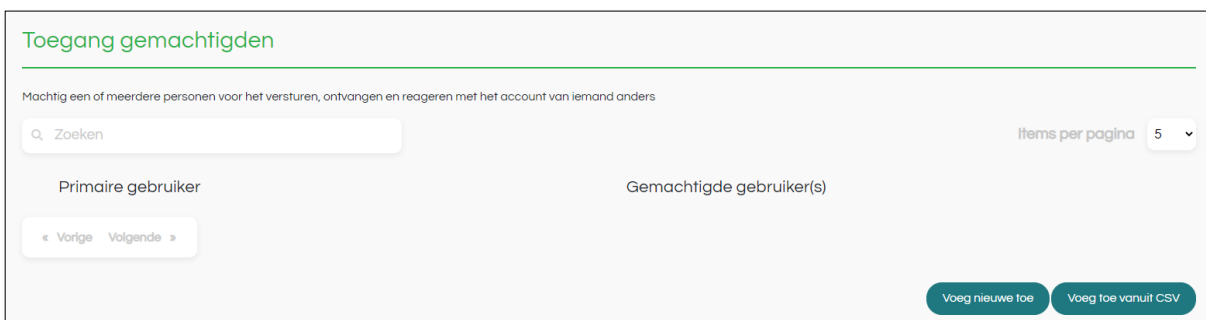
Hiermee voorkom je dat de bestaande ingelogde sessies in de browser op de achtergrond blijven doorlopen. Dit zorgt ervoor dat toegang tot de inbox door derden onmogelijk wordt gemaakt.

1.4. Toegang gemachtigden

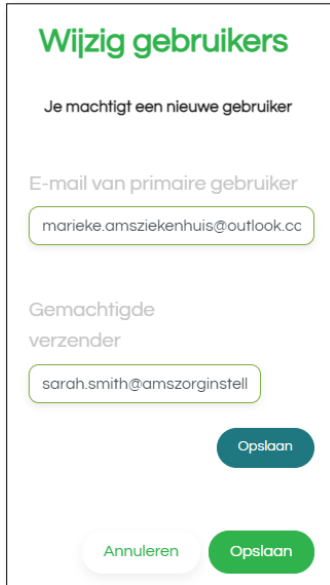
Er bestaat de mogelijkheid om een gebruiker of een groep gebruikers toegang te geven tot de inbox van een andere gebruiker (individuele inbox) of van een gedeelde inbox. Zo kan men e-mails versturen, ontvangen en reageren op binnenkomende e-mails vanuit de andere inbox. Hier is gemachtigde toegang voor nodig.

Machtigen van gebruiker(s) voor de Individuele inbox

Je kan anderen (Gemachtigde gebruiker) machtigen om de inbox van iemand anders (Primaire gebruiker) te gebruiken. Dat doe je door op de knop "Voeg nieuwe toe" te klikken:



Vervolgens zie je het volgende scherm, waar je één of meerdere Gemachtigde gebruikers kunt toevoegen:



Wijzig gebruikers

Je machtigt een nieuwe gebruiker

E-mail van primaire gebruiker

marieke.amsziekenhuis@outlook.cc

Gemachtigde verzender

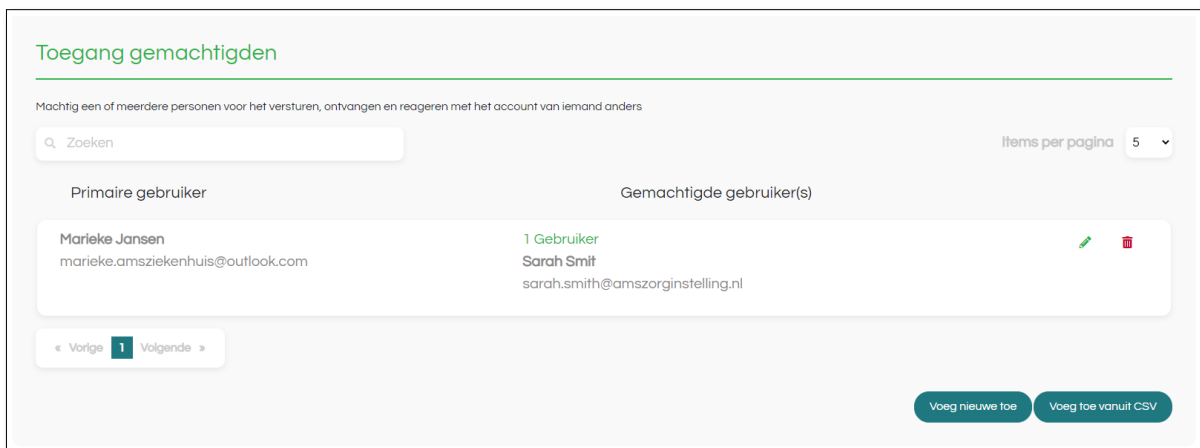
sarah.smith@amszorginstell

Opslaan

Annuleren Opslaan

Let op: om het e-mailadres van de Primaire gebruiker te kunnen gebruiken, moet dit e-mailadres binnen SmartLockr bekend staan als gebruiker (zie 2. Gebruikers).

Als je vervolgens op de onderste knop "Opslaan" klikt, dan staan de instellingen binnen SmartLockr goed:



Toegang gemachtigden

Machtig een of meerdere personen voor het versturen, ontvangen en reageren met het account van iemand anders

Zoeken

Items per pagina 5

Primaire gebruiker	Gemachtigde gebruiker(s)
Marieke Jansen marieke.amsziekenhuis@outlook.com	1 Gebruiker Sarah Smit sarah.smith@amszorginstelling.nl

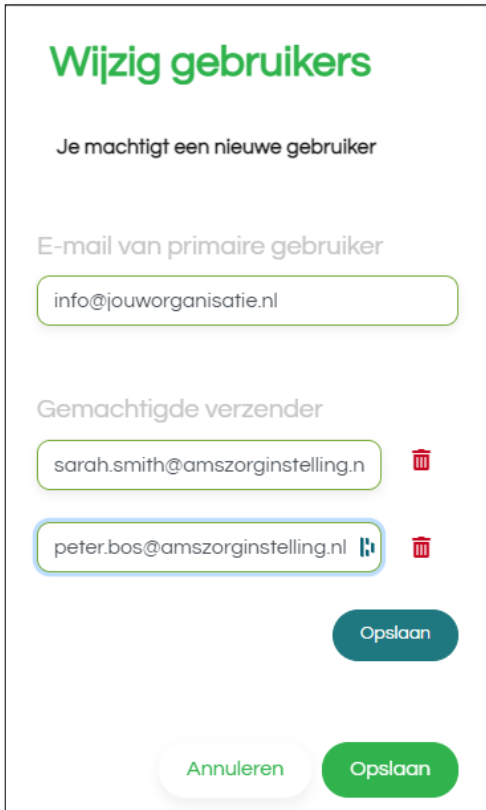
« Vorige 1 Volgende »

Voeg nieuwe toe Voeg toe vanuit CSV

Let op: om ook daadwerkelijk een gebruiker te machtigen, dien je ook de machtigingsinstellingen binnen Office365 te verrichten. Pas wanneer dat is gedaan, kan de inbox worden gebruikt door de Gemachtigde gebruiker.

Machtigen van gebruiker(s) voor de Gedeelde inbox

Het is ook mogelijk om als groep gebruik te maken van een gedeelde inbox, zoals *info@jouworganisatie.nl* en *administratie@jouworganisatie.nl*. Het machtigen van gebruikers voor de gedeelde inbox werkt hetzelfde als bij het machtigen van de individuele inbox:



Let op: om gebruik te kunnen maken van een gedeelde inbox is het belangrijk om dit e-mailadres als gebruiker toe te voegen (zie 2. Gebruikers). Er is voor de gedeelde inbox namelijk een licentie nodig, waardoor gedeelde inboxes alleen kunnen worden gebruikt als deze e-mailadressen zijn toegevoegd als gebruiker.

In het overzicht “Gemachtigde toegang” kun je vervolgens zien wie er toegang hebben tot de inbox, wie gemachtigd zijn om te werken in de inbox van een gebruiker en kun je, waar nodig, aanpassingen doen en/of gebruikers verwijderen:

Toegang gemachtigden

Machtig een of meerdere personen voor het versturen, ontvangen en reageren met het account van iemand anders

Items per pagina 5

Primaire gebruiker	Gemachtigde gebruiker(s)	
Info inbox info@jouworganisatie.nl	2 Gebruiker	 

« Vorige
1
Volgende »

Voeg nieuwe toe
Voeg toe vanuit CSV

02. Contentbeleid

Met het contentbeleid kun je gepaste beveiliging toepassen, voor gevoelige content waar dit voor nodig is. 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 een tekst en de context er omheen zal begrijpen. Denk hierbij aan de 9-cijferige reeks van een Burgerservicenummer “123456789” of “234-2234-234”. Deze laatste reeks is een voorbeeld van een patroon wat specifiek zou kunnen zijn binnen je organisatie (XXX- XXXX-XXX).

2.1. Beleidstypes op triggerwoorden

Als gebruikers contentfilters verwerken tijdens het opstellen van een bericht, wordt SmartLockr getriggerd. Daarbij kunnen zich drie situaties voordoen, afhankelijk van de instellingen:

1. 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:

Er zijn privacygevoelige gegevens (Burgerservicenummer) gevonden. Wij raden je aan dit bericht beveiligd te verzenden met SmartLockr.

2. SmartLockr springt automatisch aan, maar kan worden uitgeschakeld door de gebruiker.
3. SmartLockr springt direct aan en het bericht wordt geforceerd verzonden met een- of twee-factor authenticatie. Deze instelling kan niet worden veranderd door de gebruiker:

Er zijn privacygevoelige gegevens (Patiëntendossier) gevonden. Dit bericht wordt daarom beveiligd verzonden met SmartLockr.

2.2. Triggers op woorden, reguliere expressies en bestanden

SmartLockr heeft een standaardbibliotheek met woorden die voor veel organisaties als gevoelige informatie gelden:

Contentbeleid						
Standaard		Aangepast			Bestanden	
Nee	Titel	syntax	beleidstype	Authenticatie	Hoofdlettergevoelig	
1	BSN	Regex	Automatic	2FA	Nee	☒
2	IBAN	Word	Automatic	2FA	Nee	☒
3	Credit card	Regex	Automatic	2FA	Nee	☒

Aan deze bibliotheek kun je ook woorden toevoegen, zoals in dit voorbeeld “patiëntendossier” en “BSN”:

Contentbeleid

Standaard

Aangepast

Bestanden

Q Zoeken

Items per pagina

5

Contentfilter toevoegen

Voeg contentfilters toe vanuit CSV

Nmr.	Titel	syntax	beleidstype	Authenticatie	Hoofdlettergevoelig
1	Burgerservicenummer	Regex	Automatic	2FA	Nee
2	IBAN	Regex	Automatic	2FA	Ja
3	Credit Card	Regex	Automatic	2FA	Nee
4	BSN	Regex	Automatic	2FA	Nee

« Vorige

1

Volgende »

Contentfilter toevoegen

Voeg contentfilters toe vanuit CSV

Als je woorden wilt wijzigen nadat je ze hebt toegevoegd, kan je ze makkelijk terugvinden door de zoekbalk bovenaan het scherm te gebruiken.

Naast triggers op woorden is er ook de mogelijkheid om triggers op bestanden in te stellen. Als SmartLockr systeembeheerder heb je de optie om het versturen van een e-mail met een of meerdere ondersteunde documenten pas te versturen nadat de scan van deze

documentatie is voltooid:

Contentbeleid

Standaard

Aangepast

Bestanden

Zijn er bepaalde bestanden waar je meer bewustwording voor wil creëren? Hieronder kun je triggers instellen voor de bestanden:

☒ Trigger op bestanden

Type kanaal

Beveiligd bestand

Authenticatie

Twee-factor-authenticatie

beleidstype

verplicht

☒ Trigger bestanden in inhoud

Authenticatie

Twee-factor-authenticatie

beleidstype

automatisch

☒ Verstuur e-mail voordat document(en) volledig zijn gescand

☐ Document scannen uitzetten

Opslaan

Als er bestanden zijn waar je meer bewustwording voor wilt creëren, dan heb je de optie om dat te doen met een trigger op bestanden en een trigger op inhoud van bestanden. Wanneer je organisatie een contentbeleid wil toepassen dat op veel punten afwijkt van het standaard contentbeleid van SmartLockr, dan kan je als systeembeheerder een of meerdere CSV-bestanden met een contentbeleid gelijktijdig uploaden.

03. Eigen huisstijl

Een eigen huisstijl zorgt voor de herkenbaarheid van je organisatie. Daarom kun je jullie 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:

Merk toevoegen +

Standaard merk

Naam

AMS Ziekenhuis

Domein(en)

smartlockr.eu

Logo (Gewenste afbeelding: 225 pixels breedte 80 pixels hoogte)

AMS

Edit logo

Primaire kleur

#1e9e3d

Secundaire kleur

#1f787f

Lettertype

Zoek Google Fonts

Lato

Standaardinstellingen wissen

Opslaan

04. Uploadportaal

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 als 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.

Wanneer je op “Uploadportaal toevoegen” klikt, dan zie je het scherm waar je het portaal kunt inrichten:

Uploadportaal toevoegen

Naam

Patiëntendossier

Beschrijving

Portaal voor het versturen van patiëntendossiers

Welke bestandstypes wil je aanvragen?

☒ Aangepast e-mailadres

E-mail of domein toevoegen

ams.ziekenhuis.nl

E-mail of domein aanmaken

Het is ook mogelijk om een link door te sturen met een vooraf ingevuld e-mailadres. Als je dat wil, volg dan de volgende instructies.

Groups

^ Groep 1

Administratie

administratie@ams.ziekenhuis.nl

E-mail toevoegen

^ Groep 2

Afdeling Oncologie

oncologie@ams.ziekenhuis.nl

E-mail toevoegen

Nieuwe groep aanmaken

☒ Voorwaarden

URL label naam

Voorwaarden

Eigen url

https://amsziekenhuis.nl/algemene-voorwaarden

Annuleren

Opslaan

Dit zijn de instellingen die je kunt verrichten:

- **Naam**
Dit is de naam van het portaal, zoals ontvangers het zien.
- **Beschrijving**
Een korte beschrijving maakt duidelijk waar dit portaal voor dient.
- **Bestandstypes aanvragen**
Je kan vooraf instellen welke bestandstypes je wenst te ontvangen (zie 6. Documenttypes).
- **Aangepast e-maildomein**
Stel in welke afdelingen en/of personen de bestanden dienen te ontvangen.
Personen die de bestanden uploaden hoeven hierdoor geen ontvangers toe te voegen: dit heb je namelijk al van te voren ingesteld. Dit maakt het ook onmogelijk om het bestand naar een ander mailadres of domein te versturen. Als je het veld leeg laat, kan de zender het ontvangstadres zelf verzenden.
- **Groepen**
Door groepen te creëren en daar e-mailadressen aan te koppelen, kun je degenen die de bestanden moeten uploaden laten kiezen naar welke afdeling de bestanden moeten worden toegestuurd.
- **Voorwaarden**
In enkele gevallen wil je de algemene voorwaarden van je organisatie toevoegen. Deze kun je zelf toevoegen met een link naar de voorwaarden zoals ze bijvoorbeeld op je website staan.

Zodra het uploadportaal is aangemaakt, wordt deze toegevoegd aan de lijst:

Uploadportalen		
Nmr.	Naam	Directe link
1	Patiëntendossier	02who5

Uploadportaal toevoegen

Via de directe link kom je op de portaalpagina, waarbij de instellingen die je hebt verricht direct zichtbaar zijn:



Patiëntendossier

Portaal voor het versturen van patiëntendossiers

Van

Je e-mailadres

Naar

Kies een optie

Administratie

Afdeling Oncologie

Verzend naar een ontvanger

Upload je bestand(en)

Bestanden uploaden

☐ Ik ga akkoord met [Voorwaarden](#)

Je krijgt via e-mail een verificatie toegestuurd om dit uploadverzoek te voltooien

Volgende

05. Documenttypes

Middels uploadverzoeken en -portalen 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 hebben:

Documenttype toevoegen

Bestandsnaam

Patiëntendossier

Max. bestandsgrootte

100

MB

Bestandstype kiezen

doc

pdf

Annuleren

Opslaan

Vervolgens zie je het op deze manier terug in het overzicht:

Nummer	Naam	Bestandstype	Maximum grootte	
1	Paspoort	jpg	100 KB	
2	Patiëntendossier	doc, pdf	100 MB	

Documenttypes toevoegen

Door vooraf in te stellen welke bestanden je wenst te ontvangen, voorkom je dat er verkeerde of zelfs schadelijke bestanden worden geüpload.

06. Standaardberichten

Worden uploadverzoeken gebruikt om met regelmaat hetzelfde type bestand op te vragen? Dan kun je hier standaardberichten instellen, zodat de gebruiker efficiënter kan werken:

Standaardberichten

Nmr.	Onderwerp	Inhoud
1	Document uploaden	Beste, Graag ontvang ik de medicatielijst. Deze kun je hier uploaden. Alvast bedankt! Met vriendelijke groet, Sarah Smit

Standaardbericht toevoegen

07. E-maildomein

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

Het instellen kan in ons beheerdersportaal (<https://admin.smartlockr.eu>). Volg de stappen hieronder om het e-maildomein op te zetten waarvan je wilt dat het zichtbaar is voor de ontvangers:

1. Klik op "Email-domein" in het beheerportaal.
2. Klik "Domein toevoegen".
3. Je kiest als eerste het email adres dat je wilt gebruiken voor de ontvangers. (bv. noreply@uwdomein.nl).
4. Het domein wordt automatisch ingevuld, hier hoeft je niks aan te doen.
5. De volgende stap is de afzender naam invoeren. Dit kunt u zelf bepalen. (bv. Uw Domein Notificaties).
6. Nadat u op "toevoegen" heeft geklikt wordt er aangegeven wat er aangepast moet worden in de DNS instellingen om het eigen domein te laten werken. Doorgaans wordt dit gedaan door uw IT afdeling of IT partner.
7. Verwerk de notificatiemail die is binnengekomen op het ingevoerde mail adres.
8. Nadat de verificatie per email (Stap 7) en de DNS aanpassingen (Stap 6) gedaan zijn kan je op "verify" klikken en zal als de DNS waarden kloppen het email domein automatisch aangezet worden.

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

E-maildomein				
Nmr.	Domein	Standaard e-mailadres	Aangepaste naam	Staat
1	amsziekenhuis.nl	info@amsziekenhuis.nl	Ams Ziekenhuis	Inactief

Domein bewerken

Actieveer dit domein

Domein verwijderen

Domein toevoegen

Als er maar 1 email domein in gebruik is dan zijn we klaar, als er meerdere email domeinen in gebruik zijn dan kan je bovenstaande stappen voor alle domeinen herhalen en ze ook voor de gebruikers op die domeinen instellen.

08. NTA 7516 instellingen

De NTA 7516 is een privacynorm in Nederland die ervoor zorgt dat particuliere gezondheidsinformatie veilig wordt verzonden. Het wordt vooral gebruikt voor de zorgsector, gemeenten en de juridische sector.

SmartLockr zorgt ervoor dat je volgens de NTA 7516 norm kunt communiceren, maar deze functie moet eerst geactiveerd worden. Als je het onderstaande scherm ziet in je beheerdersportaal, betekent dit deze functie niet actief is op je account. Mocht je deze functie willen gebruiken, neem dan contact op met [support](#).

NTA 7516 instellingen

Deze functie is niet actief onder je account. Om deze te activeren neem contact op met de [support afdeling](#).

Wanneer de NTA 7516-functie op jouw account is geactiveerd, kun je gedeeltelijk zelf bepalen hoe je deze wilt gebruiken. Hieronder leggen we uit wat de twee opties zijn en hoe ze werken.

8.1. Optie 1: Gebruik de standaardinstellingen van de NTA 7516

Berichten aan ontvangers die zijn geconfigureerd voor NTA 7516 worden verzonden via NTA 7516 relay. Dit wordt alleen gedaan wanneer twee-factor authenticatie (2FA) nodig is. Als de ontvanger niet correct is geconfigureerd volgens NTA 7516, zullen zij in plaats daarvan een e-mail ontvangen met SmartLockr's twee-factor authenticatie (2FA) als een reserveoptie.

NTA 7516 instellingen

Configuratiemogelijkheden

Selecteer de NTA 7516 instelling die van toepassing is op jouw organisatie.

☒ NTA 7516 standaardinstellingen instellen (aanbevolen)

Bij het verzenden van dit bericht naar ontvangers die zijn geconfigureerd voor NTA 7516, worden berichten verzonden via NTA 7516 relay, wat het hoogste niveau van versleuteling van e-mailbeveiliging garandeert. In het geval dat de NTA 7516 ontvanger niet correct is geconfigureerd, zal in plaats daarvan twee-factor authenticatie portal-encryptie worden gebruikt.

☐ Aangepaste NTA 7516 flow instellen (geavanceerd)

Wanneer je een alternatieve beveiligingsinstelling als reserveoptie kiest, worden berichten zonder NTA 7516 compatibiliteit verzonden, waardoor gebruikers een hoger beveiligingsrisico lopen. Je kunt hier controleren of een client NTA 7516 geconfigureerd is. Wij raden je sterk aan om deze keuze met customer support te overleggen voordat je deze wijzigingen aanbrengt.

Opslaan

Het versturen van een e-mail met SmartLockr's twee-factor authenticatie betekent dat het telefoonnummer van de ontvanger moet worden ingevuld door de verzender. De ontvanger ontvangt vervolgens een sms-code die toegang geeft tot de e-mail.

8.2. Optie 2: Stel aangepaste NTA 7516 flow in (geavanceerd)

Berichten aan ontvangers die zijn geconfigureerd voor NTA 7516 worden verzonden via NTA 7516 relay. Dit wordt alleen gedaan als twee-factor authenticatie (2FA) nodig is. Als de ontvanger niet correct is geconfigureerd volgens NTA 7516, kun je zelf je reserveoptie kiezen.

NTA 7516 instellingen

Configuratiemogelijkheden

Selecteer de NTA 7516 instelling die van toepassing is op jouw organisatie.

☐ NTA 7516 standaardinstellingen instellen (aanbevolen)

Bij het verzenden van dit bericht naar ontvangers die zijn geconfigureerd voor NTA 7516, worden berichten verzonden via NTA 7516 relay, wat het hoogste niveau van versleuteling van e-mailbeveiliging garandeert. In het geval dat de NTA 7516 ontvanger niet correct is geconfigureerd, zal in plaats daarvan twee-factor authenticatie portal-encryptie worden gebruikt.

☒ Aangepaste NTA 7516 flow instellen (geavanceerd)

Wanneer je een alternatieve beveiligingsinstelling als reserveoptie kiest, worden berichten zonder NTA 7516 compatibiliteit verzonden, waardoor gebruikers een hoger beveiligingsrisico lopen. Je kunt hier controleren of een client NTA 7516 geconfigureerd is. Wij raden je sterk aan om deze keuze met customer support te overleggen voordat je deze wijzigingen aanbrengt.

Aangepaste e-mailbeveiligingsinstellingen

Als een NTA 7516 check mislukt, wil ik graag deze reserve beveiligingsoptie*

Kies een optie

☐ Ik wil dat alle NTA 7516 geconfigureerde ontvangers inbox-to-inbox email communicatie ontvangen.

⚠ Aangepaste e-mailbeveiligingsinstellingen

Indien een NTA 7516 ontvanger niet correct is geconfigureerd, kan een alternatieve beveiligingsmethode worden gekozen. Door een alternatieve beveiligingsinstelling als reserve optie te kiezen, worden berichten met NTA 7516 compatibiliteit verzonden, waardoor het beveiligingsrisico voor gebruikers toeneemt. Om deze functionaliteit in te schakelen, moet u erkennen dat uw organisatie de verantwoordelijkheid op zich neemt voor elk gegevenslek dat kan optreden.

☐ Ik begrijp dat mijn organisatie de verantwoordelijkheid draagt voor elk veiligheidsrisico dat zich kan voordoen.*

Opslaan

De aangepaste keuze kan je voorkeur hebben wanneer e-mails bijvoorbeeld verzonden worden naar een adres zonder duidelijke ontvanger, zoals een gedeelde inbox. Aan een gedeelde mailbox kun je namelijk geen telefoonnummer koppelen en werkt twee-factor authenticatie met telefoonnummer niet. In dit scenario kan een reserveoptie met één-factorauthenticatie (1FA) een betere keuze zijn.

Met de aangepaste instelling kunt je kiezen wat jouw reserveoptie moet zijn:

- Beveiligd bericht (2FA)
- Beveilig bericht (1FA)
- Beveiligd bestand (2FA)
- Beveiligd bestand (1FA)
- Openbaar bestand

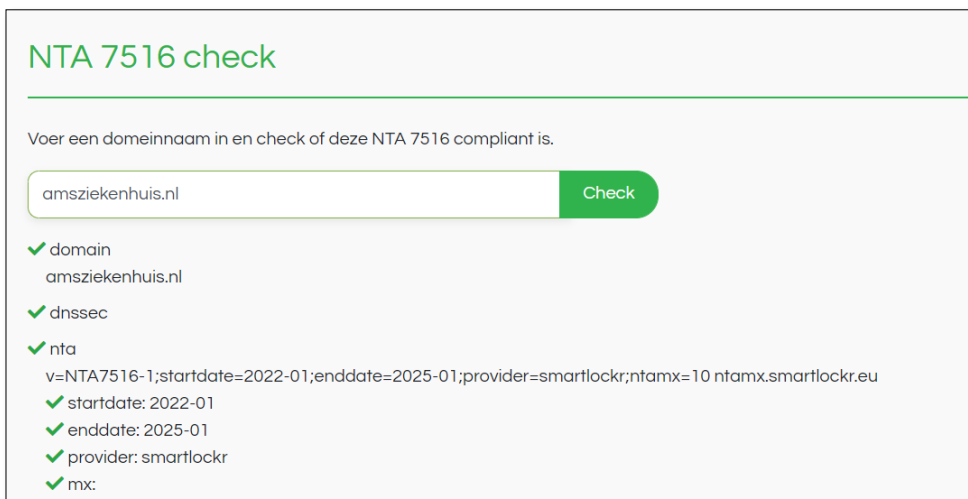
Let wel op dat als je kiest voor een reserveoptie met één-factorauthenticatie of een openbaar bestand, deze **niet** langer voldoet aan NTA 7516.

Met de aangepaste instellingen kun je er ook voor kiezen dat alle NTA 7516 geconfigureerde ontvangers inbox-to-inbox communicatie zullen ontvangen. Dit betekent dat je bericht altijd via de NTA 7516-relay zal worden verzonden, in plaats van alleen wanneer er 2FA nodig is. Als dit niet mogelijk is, zal in plaats daarvan jouw gekozen reserveoptie worden gebruikt.

Je kiest deze optie door het vakje "Ik wil dat alle NTA 7516 geconfigureerde ontvangers inbox-to-inbox email communicatie ontvangen" aan te vinken.

8.3. NTA 7516 checker

Met deze functie kun je zien of een domein voldoet aan de NTA 7516 voordat je een e-mail verstuurt. Voer gewoon de domeinnaam in en druk op check, zoals aangegeven in het onderstaande scherm.



The screenshot shows a web interface titled "NTA 7516 check". Below the title, there is a text prompt: "Voer een domeinnaam in en check of deze NTA 7516 compliant is." A text input field contains the domain "amsziekenhuis.nl", and a green "Check" button is to its right. Below the input field, a list of checks is displayed, each with a green checkmark icon:

- ✓ domain
amsziekenhuis.nl
- ✓ dnssec
- ✓ nta
v=NTA7516-1;startdate=2022-01;enddate=2025-01;provider=smartlockr;ntamx=10 ntamx.smartlockr.eu
- ✓ startdate: 2022-01
- ✓ enddate: 2025-01
- ✓ provider: smartlockr
- ✓ mx:

09. API & SMTP Relay Service

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

10. Logs

Alle activiteiten die met SmartLockr zijn verstuurd, worden opgeslagen in de logs. Hier kun je zien wat elke gebruiker heeft verstuurd/aangemaakt, via welk kanaal en wanneer:

Logs	
Filter 	Items per pagina 5 
Nmr.	Details
1	sarah.smith@amszorginstelling.nl heeft een beveiligd uploadverzoek verzonden  Type bericht: Beveiligd uploadverzoek Datum: 2-2-2022 14:39:25
2	sarah.smith@amszorginstelling.nl heeft een beveiligd uploadverzoek verzonden  Type bericht: Beveiligd uploadverzoek Datum: 2-2-2022 13:54:02

Mocht het zo zijn dat er informatie foutief is verstuurd door gebruikers, dan heb je als beheerder de rechten om de ontvanger(s), bestand(en) en de gehele e-mail te blokkeren.

Echter, regelmatige gebruikers kunnen ook hun eigen logs zien en dezelfde acties ondernemen als hierboven, door de deze pagina te bezoeken:

<https://admin.smartlockr.eu>.

11. Meer weten?

Heb je nog vragen naar aanleiding van deze handleiding? Dan kan er altijd direct contact worden opgenomen met onze Support-afdeling via support@smartlockr.eu of 020 – 244 0350 (optie 1).