



# SmartLockr Administratörsportal

# Innehållsförteckning

1. Användare	4
1.1 Outlook-inställningar	6
1.2 Mottagarpolicy	8
1.3 Säkerhetsinställningar	9
1.4 Auktoriserad åtkomst	9
2. Innehållspolicy	13
2.1 Policytyper efter triggerord	13
2.2 Trigger på ord, vanliga uttryck och filter	14
3. Grafisk profil	16
4. Uppladdningsportal	17
5. Dokumenttyper	20
6. Standardmeddelanden	21
7. E-postdomäner	22
8. API & SMTP Relay Service	24
9. Loggar	25
10. Har du fler frågor?	26



## Introduktion

Administratörsportalen ger en tydlig översikt över alla SmartLockr-aktiviteter och är en central punkt för att konfigurera alla inställningar. På så sätt har du alltid kontroll över det säkra utbytet av känslig information inom organisationen.

När du loggar in på administratörsportalen ser du en välkomstskärm med en meny till vänster. Här kan du hitta alla olika funktioner i portalen. Du kan även göra ändringar och övervaka hur SmartLockr används.



Varje avsnitt kommer att förklaras kort nedan. Detta förtydligar vad du kan förvänta dig som administratör och vilka alternativ som finns.



## 01. Användare

Under "Användare" hittar du en översikt över alla SmartLockr-användare inom din organisation. Du kan konfigurera inställningar för dessa användare. Genom att utarbeta riktlinjer kan du bättre kontrollera hur SmartLockr används.

För att komma i gång är det viktigt att tilldela de köpta licenserna till användare. Du kan göra detta genom att lägga till användarna inom organisationen till administratörsportalen:

Användare		
Alia användare~		Objekt per sida 5 🗸
Du har <b>9 licenser</b> kvar på detta konto. Vill du lägga till fler licenser? Vänligen kontakta vårt support-team.		Lägg till användare
Nummer E-postadress	Fullständigt namn	
1 johan@organisation.se	Johan Karlsson (johan@organisation.se)	:
« Föregående 1 Nästa »		
Du har <b>9 licenser</b> kvar på detta konto. Vill du lägga till fler licenser? Vänligen kontakta vårt support-team.		Lägg till användare

För att lägga till användare klickar du på den gröna knappen "Lägg till användare" längst ner till höger. Ett fönster kommer då att öppnas.

Du kan lägga till användare till din lista på två sätt. Antingen gör du det manuellt eller så importerar du dem från en CSV-fil. När du laddar upp en eller flera användare via en CSV-fil sparar du tid, eftersom vi samtidigt kan aktivera kontona och tilldela licenserna åt dig.

Lägg till nya användare Du kan välja att lägga till en användare manuellt eller användare.	r importera en CSV-fil för att lägga till nya	×
Lägg till en användare manuellt		~
E-postadress	Visningsnamn Johan Eriksson	lt)
Telefonnummer		
Klicka här om du vill lägga till användare genom att import	rera en CSV-fil	^
	Avbryt	Lägg till

Efter att du har lagt till användarna kommer de att synas i översikten. Om du vill hitta en användare snabbt, kan du använda sökfältet högst upp på sidan.

Användare	3		
Alla användar	<b>Q</b> , Sök		Objekt per sida 5 🗸
Du har <b>7 licenser</b> k	var på detta konto. Vill du lägga till fler licenser? Vänligen kontakta vårt support-team.		Lägg till användare
Nummer	E-postadress	Fullständigt namn	
1	anton@organisation.se	Anton Lind (anton@organisation.se)	:
2	johan@organisation.se	Johan Eriksson (johan@organisation.se)	
3	emma@organisation.se	Emma Sten (emma@organisation.se)	:
« Föregående	1 Nāsta »		
Du har <b>7 licenser</b> k	var på detta konto. Vill du lägga till fler licenser? Vänligen kontakta vårt support-team.		Lägg till användare

När användare läggs till manuellt kommer de att få ett aktiveringsmejl för att aktivera kontot.

Obs: för kunder kopplade till Single Sign-on (SSO) läggs dessa användare till automatiskt. Detta sker när de loggar in med SmartLockrs plugin för Outlook, eller någon annan av våra autentiseringssidor.

## 1.1 Outlook-inställningar

#### E-postinställningar

Under e-postinställningar kan du konfigurera hur SmartLockr ska användas. Det finns flera alternativ: offentliga filer, säkra filer, säkert meddelande och säker uppladdningsförfrågan. Du kan även ange om ni vill använda enfaktors- eller tvåfaktorsautentisering:

Outlook-inställningar
E-postinställningar
De tillämpade e-postinställningarna kommer att visas för alla Outlook-användare
Varningt E-postinställningarna kan skrivas över av innehållspalicyer
Offentliga filer
Säkra filer
Vālj standard
O Enfaktorsautentisering (1FA)
Tvåfaktorsautentisering (2FA)
Säkert meddelande
Avaktivera svarsknappen för mottagare
Avaktivera möjlighet till vidarebefordring för mottagare
Vālj standard
O Enfaktorsautentisering (1FA)
Tvåfaktorsautentisering (2FA)
Z Säker uppladdningsförfrågan

## Lösenordsinställningar

När enfaktorsautentisering tillämpas kan mottagarna endast komma åt meddelandet med ett lösenord. Lösenordsinställningarna kan konfigureras här:





Användarna skapar ett lösenord för mottagarna, som skickas via SmartLockr. Det finns två alternativ när det kommer till hur lösenordet skapas. Antingen genereras det automatiskt eller så skapas det av användaren.

Du kan välja mellan att hålla båda alternativen öppna för användaren, eller ställa in ett av de två alternativen som standard.

Lö	senordsinställningar	
Välj O	de lösenordsinställningar som är tillgär Välj standardinställning för lösenord	ngliga för användaren
С	<b>Skapa automatiskt</b> Ett lösenord skapas automatiskt åt användaren	gar (automatiskt och egeninställt)
Vä.	<b>Eget lösenord</b> Användaren kan skapa sitt eget lösenord	
	E-post ~	



#### **1.2** Mottagarpolicy

Det är möjligt att utesluta domäner så att all e-post till mottagare av denna domän alltid skickas som vanliga e-postmeddelanden. Detta kan vara önskvärt om du till exempel har mycket kontakt med vissa personer utanför din organisation, och du vet att du inte behöver SmartLockrs extra säkerhet när du kommunicerar med dem. Eller när du kommunicerar med organisationer vars anställda inte får klicka på länkar i epostmeddelanden:

Exkluder	ade domäner		
Varning: Bilagor som	är större än systemgränsen (inställd av administratören) kommer alltid att skickas som SmartLockrs offentliga filer. Standardinställningen för kombinerad filstorlek är 20 MB per e-p	ost.	
Nummer	Exkluderad domän Objekt per sida	5	•
1	organisation123.se	:	

Som systemadministratör kan du också ladda upp flera exkluderade domäner samtidigt med en CSV-fil.

## 1.3 Säkerhetsinställningar

Förutom att utesluta domäner kan du även avaktivera pågående sessioner för användare:



Detta förhindrar att befintliga inloggade sessioner i webbläsaren körs i bakgrunden, vilket skulle underlätta åtkomst till inkorgen för tredje part.

## 1.4 Auktoriserad åtkomst

Det är möjligt att ge en användare eller en grupp åtkomst till en annan användares inkorg (enskild inkorg) eller till en delad inkorg. Detta gör att användare kan skicka, ta emot och svara på inkommande e-postmeddelanden från den andra inkorgen. Detta kräver auktoriserad åtkomst.

#### Auktorisera användare för den enskilda inkorgen

Du kan tillåta andra (Anförtrodda användare) att använda någon annans inkorg (Primär användare). Du gör detta genom att klicka på knappen "Lägg till ny":

Ge tillgång			
Ge en individ eller grupp tillstånd att skicka, ta er	not och svara via en annans användares konto.		
Q,Sök		Objekt per sida	5 -
Primär användare	Anförtrodda användare		
« Föregående Nästa »			
		Lägg till ny Lägg till frår	ncsv



Du kommer att se följande skärm, där du kan lägga till en eller flera anförtrodda användare:

Redigera användare
Du lägger till en ny användare till denna anförtrodda avsändarlista
Primār e-postadress
anton@organisation.se
Anförtrodd avsändare
johan@organisation.se
Lāgg till
Avbryt Spara

Obs: För att kunna använda en primär användares e-postadress, måste denna e-postadress vara känd som en användare inom SmartLockr (se 2. Användare).

Om du klickar på den nedre knappen "Spara" kommer inställningarna att sparas i SmartLockr:

Ge tillgång		
e en individ eller grupp tillstånd att skicka, ta emot oc Q. Sök	h svara via en annans användares konto.	Objekt per sida 5 🗸
Primär användare	Anförtrodda användare	
<b>Johan Eriksson</b> johan@foretag.se	1 Användare eva@foretag.se	/ 1
« Föregående 1 Nästa »		
		Lägg till ny Lägg till från CSV

Obs: För att auktorisera en användare måste du även ställa in behörighetsinställningarna i Office365. När detta är gjort kan inkorgen användas av den anförtrodda användaren.



#### Auktorisera användare för delad inkorg

Det är också möjligt att använda en delad inkorg som en grupp, till exempel *info@organisation.se* och *administration@organisation.se*. Att auktorisera användare för den delade inkorgen fungerar på samma sätt som att auktorisera användare för den enskilda inkorgen:

Redigera användare	
Du lägger till en ny användare till denna anförtrodda avs	ändarlista
Primär e-postadress	
info@organisation.se	
Anförtrodd avsändare	
anton@organisation.se	ā
johan@organisation.se	Ē
	Lägg till
Avbryt	Spara

Obs: För att kunna använda en delad inkorg är det viktigt att lägga till denna e-postadress som användare (se 2. Användare). En licens krävs för den delade inkorgen, vilket innebär att delade inkorgar endast kan användas om dessa e-postadresser har lagts till som användare.



I översikten "Ge tillgång" kan du sedan se vem som har tillgång till inkorgen och vem som har behörighet att arbeta i en användares inkorg. Du kan dessutom justera och/eller ta bort användare vid behov:

Ge tillgång		
Ge en individ eller grupp tillstånd att skicka, ta em	ot och svara via en annans användares konto.	
Q.Sök	Objekt per sida	5 ~
Primär användare	Anförtrodda användare	
Information info@organisation.se	2 Användare	ā
« Föregående 1 Nästa »		
	Lägg till ny Lägg till fr	ån CSV



## **02.** Innehållspolicy

Innehållspolicyn tillåter dig att tillämpa lämplig säkerhet för känsligt innehåll. Som administratör kan du ställa in innehållsfilter för detta. Dessa är filter baserade på:

- Ord som är känsliga inom din organisation, som till exempel "Personnummer", "Patientfil" eller "Pass".
- Vanliga uttryck (RegEx) eller mönster genom vilka ett system kommer att förstå en text och sammanhanget runt den. Ett exempel är det tiosiffriga personnumret"8508221234" eller "850822-1234". Det senare är ett exempel på ett mönster som kan vara specifikt inom din organisation (XXXXXX-XXXX).

## 2.1 Policytyper efter triggerord

Om dessa ord eller uttryck används medan en användare skriver ett meddelande, kommer SmartLockr att känna av det. Tre situationer kan uppstå, beroende på era inställningar:

 Användarna uppmärksammas på att känsligt innehåll har inkluderats i meddelandet. De rekommenderas då att skicka meddelandet säkert med SmartLockr:



- 2. SmartLockr slås på automatiskt men kan stängas av användaren.
- 3. SmartLockr slås på direkt och meddelandet måste skickas med en- eller tvåfaktorsautentisering. Denna inställning kan inte ändras av användaren:



## 2.2 Trigger på ord, vanliga uttryck och filter

SmartLockr har ett standardbibliotek med ord som många organisationer anser vara känslig information.

Inne	Innehållspolicy						
	Standard		Anpassad		Filer		
	Nummer	Rubrik	Syntax	Policytyp	Autentisering	Skiftläge	
	1	Personnummer	Regex	Automatic	2FA	Nej	
	2	Kontonummer	Regex	Automatic	2FA	Ja 💽	
	3	Kreditkort	Regex	Automatic	2FA	Nej	

Du kan också lägga till ord i det här biblioteket, som "kontonummer" och

	Standard		Anpassad		Filer	
Q Sök					Objekt per sida	5
				Lägg till innehållsfilter	Lägg till innehållsfilter f	rån CSV
Numn	ner Rubrik	Syntax	Policytyp	Autentisering	Skiftläge	
1	Kontonummer	Word	Forced	2FA	Nej	:
2	adress	Word	Notification	1FA	Nej	:
3	Personnummer	Word	Automatic	2FA	Nej	:

"personnummer", som i det här exemplet:

Om du vill redigera inställningarna för några av dessa triggers efter att du har lagt till dem, kan du enkelt söka efter dem med hjälp av sökfältet.



Förutom triggers på ord går det även att sätta triggers på filer. Som SmartLockradministratör har du möjlighet att bestämma om ett e-postmeddelande med ett eller flera dokument kan skickas först efter att skanningen av filerna har slutförts:

Standard		Anpassad			Filer
Finns det vissa filer som du vill utmär	ka mer? Nedan I	kan du stâlla in en trigger för dessa filer.			
Kanaltyp		Autentisering		Policytyp	
Säker fil	~	Tvåfaktorsautentisering	~	Notifikation	-
<ul> <li>Triggade filer i innehållet</li> <li>Autentisering</li> </ul>		Policytyp			
Tvåfaktorsautentisering	~	Automatisk	-		
<ul> <li>Skicka e-post innan dokumentskan</li> <li>Inaktivera dokumentskanning</li> </ul>	nningen har avsl	utats			

Om det finns filer som du vill skapa mer medvetenhet kring, har du möjlighet att göra det med en trigger på filer eller innehåll. Skiljer sig din innehållspolicy på många sätt från den vanliga SmartLockr-innehållspolicyn, kan din systemadministratör ladda upp denna via CSV-filer.



## **03.** Grafisk profil

Din grafiska profil säkerställer att mottagarna av din e-post känner igen dina meddelanden. Därför kan du implementera denna i SmartLockr, så att e-post och portaler använder era logotyper och färger. Om ni har flera grafiska profiler kan du lägga till dessa:

Lägg till grafisk profil 🕇	
Standardiserad grafisk profil	
Namn	Primär färg
SmartLockr	#1e9e3d
Domän(er)	Sekundär färg
smartlockr.eu +	#1f787f
Logotyp	Typsnitt
(Önskad bildstorlek: 225 pixelbredd efter 80 pixelhöjd )	Sök i Google Fonts
SMARTLOCKR Edit logo	Lato
	Spara

## 04. Uppladdningsportal

Med uppladdningsportaler kommer din organisation att ta emot filer enkelt och säkert. Du kan skapa olika portaler för de olika filer som din organisation tar emot. Du kan också ange vilken typ av fil du vill ta emot, vem eller vilka avdelningar som ska meddelas och vem som ska ta emot filerna.

För att ställa in portalen klickar du på "Lägg till uppladdningsportal":

Lägg till uppladdningsportal		
Namn	Beskrivning	
Patientfiler	Portal för att skicka patientfiler	
Vilken typ av dokum	ent vill du begära? 👻	
Patientfiler ×		
Anpassad e-postadress		
Lägg till e-post eller domän		
	J	
Följ instruktionerna nedan om du vill konfigurera en länk med en förifylld e-postadre	255.	
Groups		
^ Gruppera 1		â
Gruppnamn		Lägg till e-post
E-mail 1		×
Skapa ny grupp		
Allmänna vilikor		
URL-beteckning	Anpassad URL	
Villkor	https://www.sjukhus.se/villkor	
		Avbryt Lögg till



Det här är de tillgängliga inställningarna:

• Namn

Detta är namnet på portalen, som mottagarna ser det.

#### Beskrivning

En kort beskrivning klargör vad denna portal är till för.

#### • Begär filtyper

Du kan ställa in vilka filtyper du vill ta emot i förväg (se 6. Dokumenttyper).

#### • Anpassad e-postadress

Ställ in vilka avdelningar och/eller personer som ska ta emot filerna. Personer som laddar upp filerna behöver inte lägga till mottagare: du har redan ställt in detta i förväg. Detta gör det också omöjligt att skicka en fil till en annan epostadress eller domän. Om du lämnar detta fält tomt kan avsändaren välja mottagare själv.

#### • Grupper

Genom att skapa grupper och länka e-postadresser till dem, kan du låta de som behöver ladda upp filerna välja vilken avdelning de ska skicka filerna till.

#### • Villkor

I vissa fall kanske du vill lägga till villkoren för din organisation. Du gör detta med en länk till villkoren som finns på till exempel din hemsida.

När uppladdningsportalen har skapats läggs den till i listan:

Uppladdningsportaler		
Nummer Namn	Direktlänk	
1 Patientfiler	vvycwk	:
		Lögg till uppladdningssportal



Direktlänken tar dig till portalsidan och inställningarna du har gjort syns omedelbart:

SMARTLOCKR			
itientfiler			
Vänligen ladda upp patientfilerna här			
Från			
Din e-postadress			
Till			
Ange mottagarens e-postadress			
Ditt meddelande			
Skriv in din text här			
Ladda upp dina filer här			
Patientfiler doc, pdf   1MB			
	)		
En verifiering kommer skickas till din e-post innan du kan skicka denna uppladdningsförfrågan.	Nästa		



## **05.** Dokumenttyper

Du begär filer via e-post genom uppladdningsförfrågningar och -portaler. För att göra det enkelt kan du ange vilken typ av fil du vill ta emot. Ange helt enkelt vilket filtillägg (.doc, .docx, .pdf etc.) och maximal storlek filen ska ha:

(MB ~)

Översikten kommer att se ut så här:

Dokumenttyper				
Nummer	Namn	Förlängning	Maximal storlek	
1	Patientfil	pdf	100 MB	1
2	Pass	jpg, png, pdf	100 MB	
				Lägg till dokumenttyper

Genom att ställa in vilka filer du vill ta emot i förväg förhindrar du att felaktiga, eller till och med skadliga, filer laddas upp.

## 06. Standardmeddelanden

Används uppladdningsförfrågningar för att regelbundet begära samma typ av fil? Du kan ställa in standardmeddelanden här, så att användaren kan arbeta mer effektivt:

Standardm	eddelanden		
Nummer	Ămne	Meddelandetext	
1	Ladda upp dokument	Hej	1
		Kan du vänligen ladda upp medicinlistan här?	
		Tack på förhand!	
		Vänlig hälsning. Johan	
		Lögg fill store	lardmeddelande



## 07. E-postdomäner

E-postmeddelanden med notifikationer skickas från SmartLockr, om du inte har konfigurerat det till att göra något annat. Du kan justera detta om du vill att mottagarna ska få dessa meddelanden från en domän som de känner igen.

Följ stegen nedan för att ställa in den e-postdomän du vill att dina mottagare ska se.

- 1. Klicka på 'Lägg till domän' efter att du har valt 'E-postdomäner' i administratörsfältets meny. Ett popupfönster kommer nu att öppnas.
- 2. I fältet 'Standard e-postadress' lägger du till den e-postadress som du vill använda. Efter att du har gjort detta kommer fältet 'Domän' att fyllas i automatiskt.
- 3. Nu kan du välja vilket namn du vill att dina mottagare ser när de tar emot e-post från dig. Lägg till detta i fältet 'Anpassat avsändarnamn'.
- 4. Klicka på 'Lägg till' efter att du har kontrollerat att allting har fyllts i korrekt.

Doman
organisation.se

- 5. Några inställningar kommer nu att visas. Dessa behöver konfigureras till dina DNS-servrar. Om du inte kan göra detta själv rekommenderar vi att du ber din ITavdelning eller IT-partner om hjälp.
- 6. Du kommer nu att få ett e-postmeddelande till den adress du valde. Vänligen verifiera adressen genom att klicka på detta e-postmeddelande.
- 7. Klicka på verifiera-knappen när du har färdigställt DNS-ändringarna (i steg 5) och e-postverifieringen (i steg 6). SmartLockrs servrar kommer att testa DNSändringarna för att säkerställa att allt har ställts in korrekt. Om detta är fallet kommer denna funktion att slås på automatiskt.



Du är redo! Om du har mer än en e-postdomän som du vill använda kan du repetera stegen ovan för att lägga till dem. Via fönstret du ser nedan kan du aktivera och inaktivera olika domäner.

E-mail domains						
	No	Domain	Default email address	Custom name	Status	
	1	companyname.com	info@companyname.com	Company Name	Inactive	
_						Add domain



## **08.** API & SMTP Relay Service

Om din organisation använder SmartLockrs API eller SMTP Relay Service, kan du justera även dessa inställningar via administratörsprotalen. Dessa inställningar är som standard avstängda och kräver flera ytterligare inställningar för att fungera.

## 09. Loggar

Alla aktiviteter som skickas med SmartLockr lagras i loggarna. Här kan du se vad varje användare har skickat/skapat, genom vilken kanal och när:

Loggar		
Filter	×	Objekt per sida 5 🗸
Nummer	Detaljer	
1	johan®organisation.se skickade ett säkert meddelande Händelsetyp: Säkert meddelande I Händelsedatum: 2022-08-12 13:56:04	
2	johan@organisation.se skickade en säker fil Händelsetyp: Säker fil I Händelsedatum: 2022-08-12 13:55:37	

Om information har skickats felaktigt av användare, har administratörer rätt att blockera mottagare, filer och hela e-postmeddelanden.

Vanliga användare kan dock se sina egna loggar och genomföra samma handlingar som vi listade ovan genom att besöka denna sida: <u>https://admin.smartlockr.eu</u>.



# **10.** Har du fler frågor?

Har du vidare frågor som vi inte har täckt i denna manual? Då kan du alltid kontakta vårt support-team via <u>support@smartlockr.eu</u> eller +31 (0)20 – 244 0350 (val 1).