Mochadocs

Globaal overview

Technische beveiligingsmaatregelen

Mochadocs

Globaal overview

Technische beveiligingsmaatregelen

Disclaimer

The information provided in our multimedia materials including eBooks, Case Studies, Podcasts, Explainers, Courses, Animations, Transcripts, Commercials and other material is for general informational purposes only. All information on the Site and our mobile application is provided in good faith, however we make no representation or warranty of any kind, express or implied, regarding the accuracy, adequacy, validity, reliability, availability, or completeness of any information on the Site or our mobile application The use of the Mochadocs multimedia materials does not create an customer-client or any other professional-client relationship between you and Mochadocs.

UNDER NO CIRCUMSTANCE SHALL WE HAVE ANY LIABILITY TO YOU FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF THE SITE OR OUR MOBILE APPLICATION OR RELIANCE ON ANY INFORMATION PROVIDED ON THE SITE AND OUR MOBILE APPLICATION. YOUR USE OF THE SITE AND OUR MOBILE APPLICATION AND YOUR RELIANCE ON ANY INFORMATION ON THE SITE AND OUR MOBILE APPLICATION IS SOLELY AT YOUR OWN RISK.

This disclaimer is subject to change without notice, and you should review it regularly for any updates.

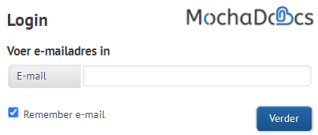
By using Mochadocs multimedia materials, you agree to the terms of this disclaimer.

Mochadocs

Index

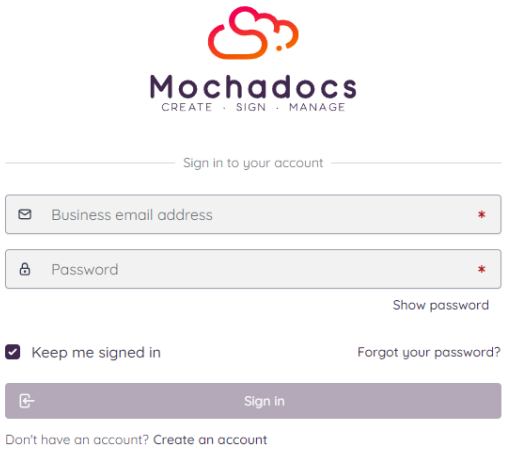
Authenticatie

CM1 (Contract Management):



- Basis authenticatie gebeurt via een combinatie van gebruikersnaam en wachtwoord.
- Tweefactorauthenticatie (2FA): Beschikbaar via authenticator-apps, wat een extra beveiligingslaag toevoegt door een eenmalig gegenereerde code naast de standaard inloggegevens te vereisen.
- Single Sign-On (SSO): Aanwezig, waardoor gebruikers met één set inloggegevens toegang kunnen krijgen tot meerdere systemen zonder opnieuw te hoeven inloggen.

CLM (Contract Lifecycle Management):



- Momenteel wordt standaard 2FA toegepast via e-mailauthenticatie, waarbij een eenmalige code naar het geregistreerde e-mailadres van de gebruiker wordt gestuurd. Authenticator-apps staan op de roadmap voor nabije toekomstige implementatie.
- Single Sign-On (SSO): Nog niet beschikbaar in CLM, staat eveneens gepland op de roadmap voor nabije toekomstige ontwikkeling.

Beveiliging en integriteit

Gescheiden Architectuur

De web-frontend is strikt gescheiden van de backend-architectuur. De backend is alleen toegankelijk via beveiligde kanalen, zoals VPN, en alleen door geautoriseerd DevOps-personeel. Dit minimaliseert de kans op onbevoegde toegang en verhoogt de beveiliging van gevoelige gegevens.

Versleutelde Communicatie

Alle communicatie tussen servers en datatransfers wordt beveiligd met relevante encryptie door middel van certificaten. Dit zorgt ervoor dat onderschepping van gegevens tijdens de overdracht niet mogelijk is, waardoor de vertrouwelijkheid en integriteit van de gegevens behouden blijft.

Gecompartimenteerde Databases

We hanteren gecompartimenteerde databases per klant, ook wel tenant-based genoemd. Dit betekent dat alle data per klant strikt gescheiden is, waardoor gegevens van verschillende klanten nooit gemengd raken en de privacy en beveiliging van iedere klant gegarandeerd zijn.

Bescherming tegen DDoS-aanvallen

We maken gebruik van tools zoals CloudFlare om bescherming te bieden tegen Distributed Denial-of-Service (DDoS) aanvallen, waarbij de server overspoeld wordt met verzoeken. Deze tools helpen bij het filteren en afhandelen van kwaadwillende verzoeken om de beschikbaarheid van de service te waarborgen.

Load Balancing

Om de servers te ontlasten tijdens momenten van veel verkeer, maken we gebruik van load-balancing tools. Deze tools verdelen de inkomende verzoeken gelijkmatig over meerdere servers, waardoor de servers altijd bereikbaar blijven en goede responstijden behouden.

ISO-gecertificeerde Ontwikkelprocessen

Onze softwareontwikkeling volgt ISO-gecertificeerde processen en standaarden. De code wordt gecontroleerd door Quality Assurance (QA) medewerkers en geautomatiseerde tools die de code valideren en kwetsbaarheden in gebruikte libraries signaleren. Dit zorgt ervoor dat geen ongeautoriseerde code live komt te staan en dat kwetsbaarheden snel worden opgespoord en verholpen.

Health-Checks en Automatische Failover

We hebben health-checks ingebouwd in onze architectuur om downtime onmiddellijk te signaleren. Load-balancers vangen dit automatisch op door alternatieve servers beschikbaar te stellen, zodat de dienstverlening ononderbroken blijft en de beschikbaarheid gewaarborgd is.

Microservices-architectuur

Onze applicaties zijn ontwikkeld volgens een microservices-architectuur, waarbij functionaliteiten strikt gescheiden zijn. Deze services communiceren alleen via geautoriseerde interfaces, wat de beveiliging en onderhoudbaarheid van de applicatie verbetert.

Versleutelde Back-ups

Back-ups van data worden versleuteld opgeslagen. Dit zorgt ervoor dat de gegevens onleesbaar zijn voor onbevoegden, zelfs als de back-ups in verkeerde handen zouden vallen.

ISO 27001-certificering en Audits

We zijn ISO 27001-gecertificeerd, wat betekent dat we voldoen aan strenge internationale normen voor informatiebeveiliging. Jaarlijkse audits bevestigen dat we voortdurend aan deze normen blijven voldoen en onze beveiligingspraktijken up-to-date houden. Download hier het ISO 27001 certificaat (onderaan de pagina bij Fundamental Files - Technical)

Gedetailleerdere Procesbeschrijvingen en Beveiligingsmaatregelen

Authenticatie en Toegangsbeheer

Bij CM1 wordt de basis authenticatie afgehandeld via een combinatie van gebruikersnaam en wachtwoord, aangevuld met tweefactorauthenticatie (2FA) via authenticator-apps zoals Google Authenticator of Microsoft Authenticator. Dit voegt een cruciale beveiligingslaag toe door een dynamische, tijdgebaseerde eenmalige code te vereisen naast de standaard inloggegevens.

Single Sign-On (SSO)

CM1 ondersteunt SSO, wat gebruikers in staat stelt om met één set inloggegevens toegang te krijgen tot meerdere systemen en applicaties zonder opnieuw te hoeven inloggen. Dit verhoogt zowel het gebruiksgemak als de beveiliging door de noodzaak voor meerdere wachtwoorden te elimineren.

Bij CLM is momenteel 2FA beschikbaar via e-mailauthenticatie, waarbij een eenmalige code naar het geregistreerde e-mailadres van de gebruiker wordt gestuurd. De ondersteuning voor authenticator-apps staat op de roadmap voor nabije toekomstige ontwikkeling, wat de beveiliging en gebruikservaring verder zal verbeteren.

Single Sign-On (SSO)

Hoewel momenteel niet beschikbaar voor CLM, staat SSO op de roadmap voor toekomstige ontwikkeling, wat de beveiliging en gebruikservaring verder zal verbeteren.

Beveiliging van de Infrastructuur

Scheiding van Web-Frontend en Backend

Onze infrastructuur is zo ontworpen dat de web-frontend strikt gescheiden is van de backend. De backend is alleen toegankelijk via beveiligde kanalen zoals VPN en alleen door geautoriseerd DevOps-personeel. Dit vermindert het risico op onbevoegde toegang aanzienlijk.

Versleuteling van Dataverkeer

Alle communicatie tussen servers en datatransfers wordt beveiligd met relevante encryptie via certificaten (bijvoorbeeld TLS). Dit garandeert dat gegevens tijdens de overdracht niet onderschept of gemanipuleerd kunnen worden.

Gecompartimenteerde Databases

We gebruiken een tenant-based model voor onze databases, wat betekent dat de gegevens van elke klant strikt gescheiden zijn. Dit voorkomt dat gegevens van verschillende klanten vermengd raken en beschermt de privacy en beveiliging van klantgegevens.

Bescherming tegen Cyberaanvallen:

DDoS-bescherming

We gebruiken tools zoals CloudFlare om bescherming te bieden tegen Distributed Denial-of-Service (DDoS) aanvallen. Deze tools filteren kwaadwillende verzoeken uit, waardoor onze servers beschermd blijven tegen overbelasting en de diensten beschikbaar blijven voor legitieme gebruikers.

Load Balancing

Om te zorgen voor een gelijkmatige verdeling van het verkeer en om te voorkomen dat servers overbelast raken tijdens piekmomenten, maken we gebruik van load-balancing tools. Deze tools helpen om de responstijden kort te houden en de beschikbaarheid van de diensten te waarborgen.

Softwareontwikkeling en Kwetsbaarhedenbeheer

ISO-gecertificeerde Ontwikkelprocessen

Onze softwareontwikkeling volgt strikte ISO-gecertificeerde processen en standaarden. Dit omvat zowel handmatige codebeoordelingen door Quality Assurance (QA) medewerkers als geautomatiseerde scans die de code controleren op kwetsbaarheden in gebruikte libraries. Hierdoor kunnen we snel eventuele beveiligingslekken identificeren en verhelpen.

Health-Checks en Automatische Failover

Onze infrastructuur bevat ingebouwde health-checks die de status van servers en diensten continu monitoren. Bij detectie van downtime schakelen load-balancers automatisch over naar alternatieve servers, zodat de diensten ononderbroken beschikbaar blijven.

Geavanceerde Architectuur en Gegevensbescherming

Microservices-architectuur

We gebruiken een microservices-architectuur voor de ontwikkeling van onze applicaties. Dit betekent dat verschillende functionaliteiten van de applicatie als afzonderlijke services worden ontwikkeld en beheerd, die alleen via geautoriseerde interfaces met elkaar communiceren. Dit verhoogt de beveiliging en maakt het eenvoudiger om individuele componenten te onderhouden en te updaten.

Versleutelde Back-ups

Onze back-ups worden versleuteld opgeslagen, wat betekent dat de gegevens onleesbaar zijn voor onbevoegden, zelfs als de back-ups zouden worden buitgemaakt. Dit biedt een extra beveiligingslaag voor de gegevens van onze klanten.

ISO 27001-certificering en Audits

We zijn ISO 27001-gecertificeerd, een internationaal erkende norm voor informatiebeveiliging. We ondergaan jaarlijkse audits om ervoor te zorgen dat we aan deze norm blijven voldoen en om onze beveiligingsmaatregelen continu te verbeteren. Deze certificering bevestigt onze inzet voor de hoogste niveaus van beveiliging en gegevensbescherming.

Belangrijk naslagwerk

Security Statement

Privacy Policy

Product & Service Catalog

Mochadocs Enterprise BV

Netherlands, United Kingdom, Luxembourg & Belgium

Roomweg 167-F

Prismare Building

2nd & 3rd floor

7523 BM Enschede

Nederland

Telefoon: +31 85 400 4800

Chamber of Commerce: 81453825