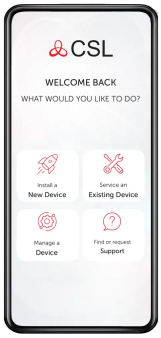
PRODUCTONDERSTEUNING

My Base App 2.0

Bijgewerkt op 18 maart 2025



Met onze handige Installateurs App kunt u uw aangesloten apparaten configureren en testen. U kunt uw aangesloten apparaten op afstand benaderen, configureren en testen, waar u zich ook bevindt, gemakkelijk via uw smartphone of browser.

Om de My Base App te downloaden, gaat u naar:

Download on the App Store (https://apps.apple.com/gb/app/csl-my-base/id1479184708#?platform=iphone) GET IT ON Google Play (https://play.google.com/store/apps/details?id=com.cslgroup.mybase&hl=en_GB&gl=US)

Meest recente informatie
https://csl-group.cloud/nl/ondersteuning/my-base/

Handleiding

Download in de App Store (https://apps.apple.com/nl/app/csl-my-base/id1479184708#?platform=iphone)

Download via Google Play (https://play.google.com/store/apps/details?id=com.cslgroup.mybase&hl=nl_nl&gl=US&pli=1)

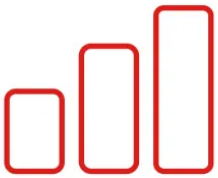
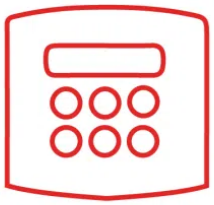
Registreer vandaag nog (https://csl-group.cloud/nl/hulpmiddelen/my-base-app-2-0/#contact)

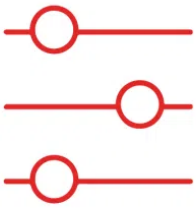
Eenmalig Toegang tot Portaal (https://mybase.csl-group.cloud/new-install)

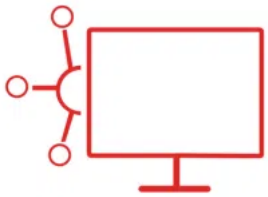
Introductie

My Base biedt installateurs de mogelijkheid om DualCom Pro-apparaten te beheren en configureren via een handige app/webportal.

Download eenvoudig **CSL My Base** uit de juiste App Store en verkrijg inloggegevens van CSL (of de CSL-admin binnen uw bedrijf) om toegang te krijgen tot deze geweldige functies:

Bekijk pad-status	Controleer signaalsterkte	Bekijk status paneel-connectie	Configureer statische IP informatie
			

Paneelverbinding wijzigen 	Pinconfiguratie aanpassen 	ATS-padbeschikbaarheid controleren 	Apparaatfirmware op afstand upgraden 
Alarmen bekijken (U moet nog steeds bij uw PAC controleren of de alarmen bij hen binnenkomen) 	Alarm Testen 	Storingsrelais omkeren 	Uitgangen configureren 

Smart Reporting wijzigen	Referenties toevoegen
	

Gebruikersbeheer voor My Base 2.0 & de CSL Live Shop

Gebruikersbeheer

Het gedeelte Gebruikersbeheer binnen CSL Live stelt u in staat om Shop- en My Base-logins voor uw medewerkers aan te maken en te beheren. Deze functie is alleen beschikbaar voor gebruikers met 'Admin'-rechten. Gebruikersbeheer is niet beschikbaar via de My Base App; u moet hiervoor het CSL Live-portaal via een webbrowser gebruiken.

CSL Live is onderverdeeld in twee secties: de Shop en My Base. 'Admin'-rechten worden afzonderlijk toegekend voor deze secties. U kunt alleen gebruikers aanmaken en beheren binnen het gedeelte waarvoor u 'Admin'-rechten heeft gekregen.

Bijvoorbeeld

- Gebruikers met 'Admin'-rechten voor de Shop kunnen gebruikers voor de Shop aanmaken en beheren.
- Gebruikers met 'Admin'-rechten voor My Base kunnen gebruikers voor My Base aanmaken en beheren.
- Gebruikers met 'Admin'-rechten voor beide kunnen gebruikers voor zowel de Shop als My Base aanmaken en beheren.

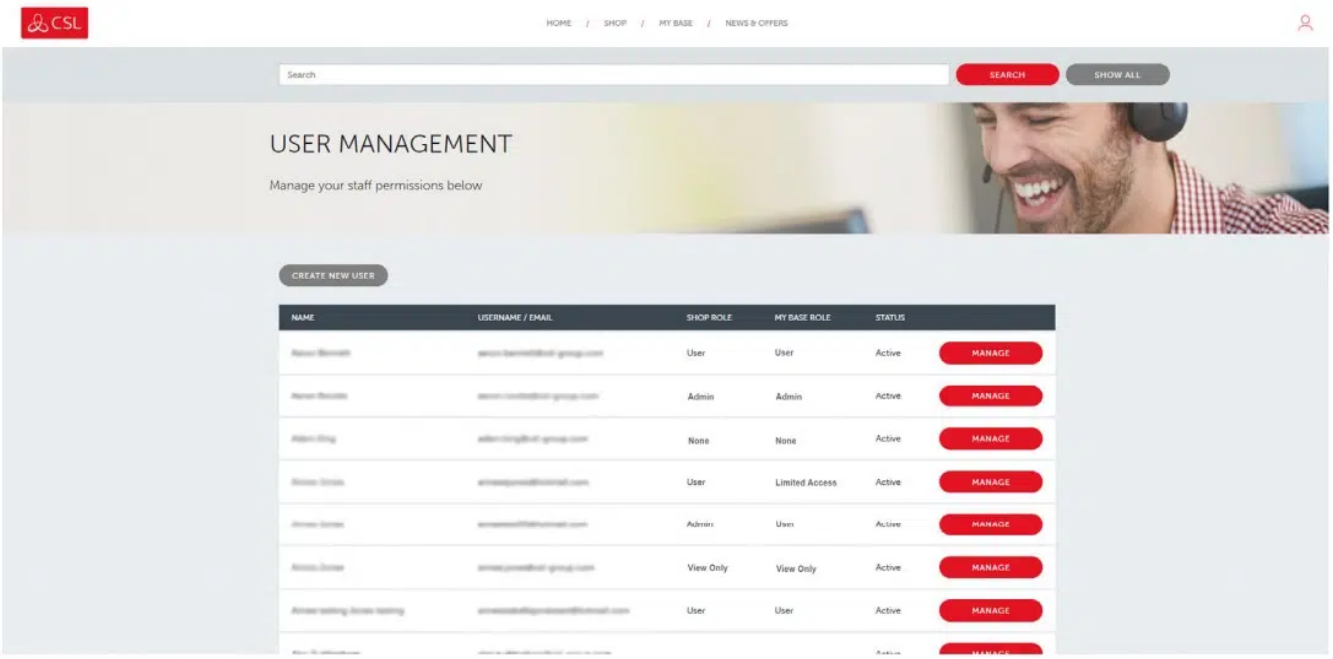
Toegang tot het gedeelte Gebruikersbeheer vanuit CSL Live Shop of My Base

Beheerders kunnen deze functie benaderen via het 'Personen'-icoon in de rechterbovenhoek van het scherm, onder 'Gebruikersbeheer'.



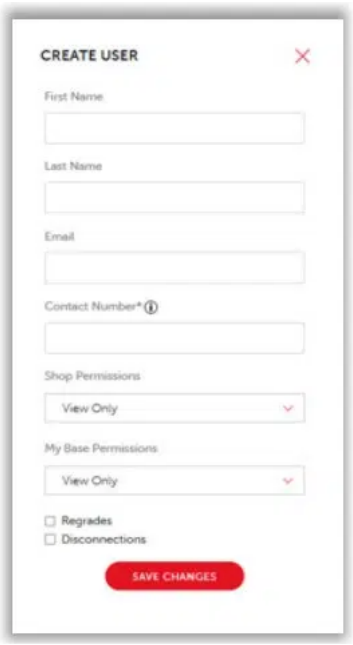
Startpagina Gebruikersbeheer

De startpagina van Gebruikersbeheer is waar u alle inloggegevens onder uw account kunt bekijken en doorzoeken. U kunt nieuwe inloggegevens aanmaken en de inloggegevens van een bestaand account wijzigen. Er is ook de mogelijkheid om een account te deactiveren indien nodig.



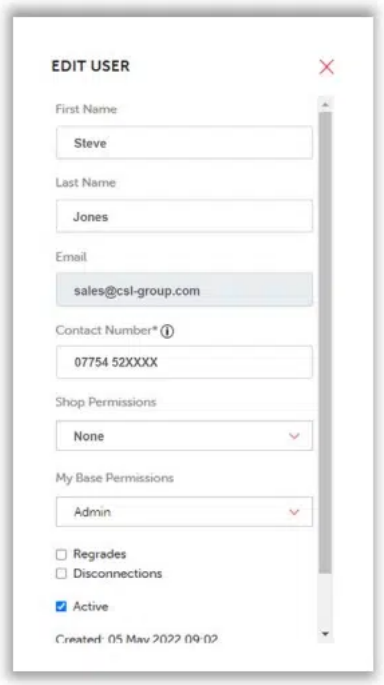
Nieuw gebruiker aanmaken

Klik op ‘Nieuw gebruiker aanmaken’, net boven de tabel. Een pop-upvenster wordt weergegeven waarin u de gegevens van een nieuwe gebruiker kunt toevoegen om een nieuw inlogaccount te creëren. U kunt de beschikbare rollen onder ‘Shop-rechten’ en ‘My Base-rechten’ alleen bekijken en selecteren als uw account ‘Admin’-rechten heeft voor deze gebieden.



Bestaande gebruikers beheren

Selecteer 'Beheren' bij de gebruiker die u wilt aanpassen. Een pop-upvenster wordt weergegeven waarin u de gegevens van de gebruiker kunt wijzigen. U kunt de volgende gegevens aanpassen: voornaam, achternaam, Shop/My Base-inloggegevens en het deactiveren van een account. U kunt ook zien wanneer de gebruiker is aangemaakt en wanneer zij voor het laatst in deze sectie zijn ingelogd.



Meer informatie:

- 'Regrades en ontkoppelingen' vinkje (alleen voor ARC's) – hiermee kunnen ARC Admin-gebruikers een regrade- of ontkoppelingsverzoek via My Base (alleen webportal) namens de installateur initiëren.
- UDL/Remote Manager Toegang. Als My Base-gebruikers ook toegang tot Remote Manager nodig hebben, neem dan contact (https://csl-group.cloud/nl/contact/) met ons op.
- Permissies uitgelegd: voor een overzicht van de permissies kunt u pagina 3 van dit document raadplegen.

Permissies uitgelegd

CSL Live				
	Bekijken	Gebruiker	Admin	Geen

Bestellingen bekijken	J	J	J	N
Bestellingen traceren	J	J	J	N
Producten bekijken	N	J	J	N
Producten bestellen	N	J	J	N
Toegang tot serviceverzoeken	N	N	J	N
Goedkeuren/afwijzen van serviceverzoeken	N	N	J	N
Ontvangen van e-mailmeldingen over serviceverzoeken	N	N	J	N
Aanmaken van extra gebruikers	N	N	J	N
Deactiveren van huidige gebruikers	N	N	J	N
Beheren van e-mailmeldingen	N	N	J	N

My Base

	Bekijken	Gebruiker	Admin	Beperkte toegang tot aansluiting	Eenmalige toegang
Aansluitingen bekijken	J	J	J	Alleen specifieke aansluiting	N
Aansluitingen opzoeken	J	J	J	Alleen specifieke aansluiting	N
Aansluitingen zoekvakjes	J	J	J	N	N

Filters	J	J	J	N	N
Live Chat	J	J	J	J	J
Aansluiting toevoegen	J	J	J	J	Alleen nieuw/in behandeling
Adres wijzigen	N	J	J	J	Alleen nieuw/in behandeling
Smart Reporting wijzigen	N	J	J	J	Alleen nieuw/in behandeling
Firmware upgrade	N	J	J	J	Alleen nieuw/in behandeling
Opnieuw opstarten	N	J	J	Y	Alleen nieuw/in behandeling
Paneel wijzigen	N	J	J	J	Alleen nieuw/in behandeling
Ingangen wijzigen	N	J	J	J	Alleen nieuw/in behandeling
Pad status bekijken	J	J	J	J	Alleen nieuw/in behandeling
Pad Config wijzigen	N	J	J	J	Alleen nieuw/in behandeling
Test Alarmen versturen	N	J	J	J	Alleen nieuw/in behandeling
Bekijk beschikbaarheids grafiek	J	J	J	J	Alleen nieuw/in behandeling
Alarmen bekijken	J	J	J	J	Alleen nieuw/in behandeling
Alarmen filteren	J	J	J	J	Alleen nieuw/in behandeling
Alarmen exporteren	J	J	J	J	Alleen nieuw/in behandeling

Relaisuitgang omkeren	N	J	J	J	Alleen nieuw/in behandeling
Regrade-aanvraag initiëren	N	J	J	N	N
Ontkoppelingsaanvraag initiëren	N	J	J	N	N

Multi-Factor Authenticatie

Hoe in te stellen:

1. Voer zoals gewoonlijk uw gebruikersnaam en wachtwoord in op CSL Live of de My Base App.
2. Open uw Authenticator App en selecteer ‘verstuur code via e-mail’ of ‘verstuur code via SMS’.
3. Ontvang een code van uw Authenticator App, programma, e-mail of sms.
4. Voer de code in CSL Live of de My Base App in.
5. U bent nu veilig ingelogd.

Wat Is Multi-Factor Authenticatie (MFA)?

MFA is een verificatieproces dat twee methoden vereist om de identiteit van een gebruiker te verifiëren, waardoor de toegangsbeveiliging van een systeem wordt versterkt. Deze vorm van authenticatie beschermt tegen phishing, social engineering en wachtwoord aanvallen. Bovendien kan het aanmeldingen beveiligen tegen hackers die zwakke of gestolen inloggegevens gebruiken.

Waarom is MFA belangrijk?

MFA is een essentieel onderdeel van een ‘zero-trust’ beveiligingsmodel. Om gevoelige gegevens te beschermen, dienen gebruikers die toegang tot gegevens vragen te bevestigen dat ze zijn wie ze zeggen dat ze zijn. MFA biedt bescherming tegen veel beveiligingsrisico’s die gericht zijn op wachtwoorden en accounts van gebruikers, zoals de hierboven genoemde. Als een aanvaller op afstand toegang kan krijgen tot een computer via de internetverbinding van een gebruiker, kan hij toegang krijgen tot het wachtwoord van de gebruiker, samen met een tweede vorm van authenticatie, als beide via hetzelfde kanaal worden geleverd. Aanvallers op afstand kunnen niet proberen de identiteit van een gebruiker te stelen (om ongeautoriseerde toegang te krijgen tot informatie die is opgeslagen in applicaties) zonder het fysieke apparaat van die persoon. Door MFA te integreren, kunnen aanvallers geen toegang krijgen tot privéaccounts zonder het fysieke apparaat van de gebruiker te bezitten dat dient om de tweede factor te voltooien.

Welk type MFA gebruikt CSL?

CSL gebruikt verificatie op basis van tijdfactor, ook wel Time-Based, One Time Password (TOTP) genoemd. De TOTP MFA-methode genereert met tijdsintervallen een code die de gebruiker dient in te voeren om toegang te krijgen. De wachtwoordcode die wordt gegenereerd door de authenticators, of SMS/e-mail, verloopt na een bepaalde periode en een nieuwe wordt gegenereerd de volgende keer dat een gebruiker inlogt op zijn account. TOTP maakt deel uit van de Open Authenticatie (OAUTH) beveiligingsarchitectuur.
CSL heeft tijdfactorauthenticatie geïmplementeerd met OTP, e-mail en SMS. Hier is een lijst met veelgebruikte authenticators die zijn goedgekeurd door CSL:

- Free OTP
- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- 2FA Authenticator (2FAS)
- Aegis Authenticator
- Authy
- Due Mobile IBM Security



1. Voer zoals gewoonlijk uw gebruikersnaam en wachtwoord in op CSL Live
2. Ontvang een code van uw Authenticator App, programma, e-mail of SMS
3. Voer de code in CSL Live in
4. U bent nu veilig ingelogd

Welke sectoren gebruiken MFA?

Beveiliging van eindpunten wordt snel een belangrijk aandachtspunt voor veel industrieën. Ongeacht tot welke applicaties gebruikers toegang hebben, het beschermen van referenties is van het grootste belang om de veiligheid van het bedrijf in het algemeen te garanderen.

Detailhandel		De grootste werkgelegenheidssector van het land, aanvallen op afstand zijn dominant geworden in de sector en moeilijk te voorkomen. Daarnaast worden beveiligingsoplossingen steeds belangrijker voor de detailhandel nu informatietechnologie zich aanpast aan een omgeving zonder perimeter.MFA biedt gemoedsrust voor bedrijven in de detailhandel – het stelt hen in staat om de identiteit te verifiëren van gebruikers die toegang hebben tot hun netwerken via externe desktops en persoonlijke mobiele apparaten.
Banken		Banken gebruiken MFA om zich te beschermen tegen de vele hackpogingen op zowel hun eigen interne systemen als die van hun klanten. MFA heeft veel grote banken geholpen hun weerbaarheid tegen dergelijke aanvallen te verbeteren. Het is voor alle banken van het grootste belang om te weten welke gebruikers en apparaten op welk moment toegang hebben tot hun systemen. MFA stelt de banksector in staat om apparaten op afstand te beveiligen en elke inlogpoging te verifiëren.
Sociale Media		Sociale mediaplatforms en -agentschappen gebruiken MFA om de persoonlijke gegevens van miljarden gebruikers wereldwijd te beschermen. Bedrijven zoals Facebook gebruiken authenticatie om hun ontwikkelaars te beschermen tegen hackpogingen wanneer ze op de interne netwerken van het bedrijf werken. MFA maakt beveiliging ook eenvoudiger voor sociale mediabedrijven door het toegangsproces voor ontwikkelaars te vereenvoudigen. Cloud-gebaseerde MFA-oplossing beschermt ontwikkelaars en gebruikers op hun beurt door hardware- en software-installatie overbodig te maken.

Overheid		De huidige IT-ontwikkelingen dagen overheidsinstanties uit om snelle veranderingen in hun infrastructuur door te voeren, terwijl ze de verschuiving naar cloud en mobiel proberen op te vangen. MFA-technologie helpt overheidsinstellingen bij het opstellen van een zero-trust beleid voor de miljoenen gebruikers die toegang dienen te krijgen.

MFA Veelgestelde vragen

Wat als een gebruiker zijn mobiele apparaat kwijt is of vervangt?

MFA vertrouwt erop dat gebruikers een apparaat hebben waarmee ze zich kunnen verifiëren.Als die smartphone of laptop verloren, gestolen of vervangen is, kunnen gebruikers zelf een nieuw apparaat registreren door hun wachtwoord opnieuw in te stellen via CSL Live. Deze functie kan ook worden gebruikt als de gebruiker een nieuwe telefoon of laptop koopt om MFA te registreren op hun nieuwe apparaat. Waar ter wereld een gebruiker zich ook bevindt en welke technologie hij ook gebruikt, zijn informatie zal veilig zijn.

Kan ik MFA instellen op meerdere apparaten?

Ja, u kunt MFA op meerdere apparaten instellen – met MFA kunt u meerdere apparaten aan uw account koppelen.

Mijn gekozen authenticator staat niet op de lijst, is het OK om te gebruiken?

CSL heeft de authenticators in dit document getest en goedgekeurd. We raden u aan deze authenticators te gebruiken om de betrouwbaarheid en toegankelijkheid van uw CSL Live account te garanderen.

Ik kan geen authenticator App gebruiken, wat zijn mijn andere opties?

We hebben back-up opties voor SMS en e-mail ontwikkeld voor het geval u om welke reden dan ook geen authenticator app kunt gebruiken.Selecteer gewoon de optie SMS of e-mail wanneer het systeem u om een eenmalige code vraagt. Alle SMS/e-mails hebben een vervaltijd van 60 seconden.

Hoe kan ik meer te weten komen?
Volg de onderstaande links voor meer informatie over MFA standaardpraktijken en richtlijnen.

Digitial Trust Center (https://www.digitaltrustcenter.nl/tweefactorauthenticatie)

Veelgestelde vragen

Wat is de My Base App

De My Base App is een platform voor het beheer van alle DualCom Pro apparaten. Met de app kunt u uw signaalsterkte controleren, upgrades aanvragen, testalarmen versturen, beschikbaarheidsgrafieken bekijken, paneelprofielen bewerken, firmware upgraden en alarmlogs bekijken.

Hoe krijg ik toegang tot de app My Base?

Zodra u de My Base app uit uw App Store hebt geïnstalleerd, gaat u naar de CSL website om u te registreren voor een My Base account, klik hier. (https://csl-group.cloud/nl/hulpmiddelen/my-base-app-2-0/#contact)

Voor de veiligheid nemen wij contact met u op om uw aanvraag te autoriseren en de juiste machtigingsniveaus in te stellen voor uw My Base account. Na goedkeuring sturen wij u uw inloggegevens.

Heeft u hulp nodig? Bel CSL Technische Ondersteuning op +31 (0) 88 474 7777

Kan ik machtigingen en toegang van gebruikers binnen mijn bedrijf beheren?

Ja, deze functie is nu beschikbaar via het CSL Live webportaal. Klik hier (https://csl-group.cloud/nl/hulpmiddelen/my-base-app-2-0/#contact) om naar onze handleiding voor gebruikersbeheer te gaan.

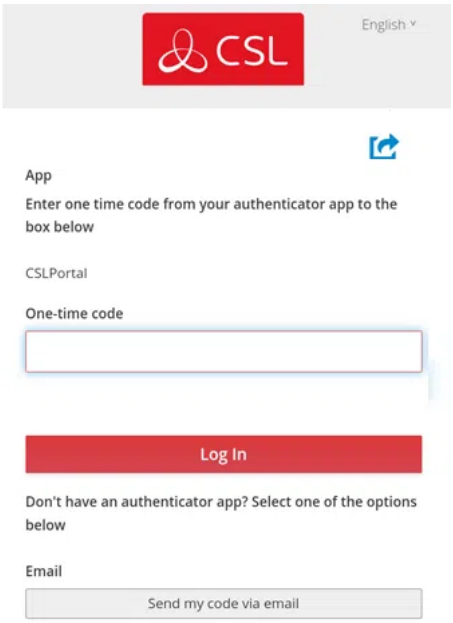
Hoe stel ik Multi-Factor Authenticatie in op de My Base app?

Voor de veiligheid is multifactorauthenticatie (MFA) nu vereist om de My Base App te gebruiken. MFA verhoogt de veiligheid op ons platform en vereist dat gebruikers zich authenticeren via hun gebruikersnaam/wachtwoord en met een tijdsgebonden code (elke code verloopt na 60 seconden). Deze code wordt verkregen via een Authenticator App, e-mail of sms. Een nieuwe authenticatie is **elke 30 dagen** nodig; als de gebruiker **uitlogt** of als we **CSL Live updaten.**

Hoe werkt het?

1. Log in op My Base zoals normaal met uw gebruikersnaam en wachtwoord.
2. Ontvang een code via een Authenticator App, e-mail of sms.
3. Voer de code in My Base in.

4. U bent nu veilig ingelogd.



Als u problemen ondervindt met de bovenstaande stappen, kunt u het verificatieproces opnieuw starten door uw wachtwoord te resetten.Als het probleem zich blijft voordoen en u ondersteuning nodig hebt, bel dan CSL Technical Support op +44 (0) 1895 474 444.Als het probleem zich blijft voordoen en u ondersteuning nodig hebt, bel dan CSL Technische Ondersteuning op +31 (0) 88 474 7777

Welke Authenticator apps werken met My Base?

Hier is een lijst met veelgebruikte authenticators die zijn erkend door CSL:

- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- 2FA Authenticator (2FAS)
- Aegis Authenticator
- Authy
- Due Mobile
- IBM Security Verify
- Free OTP

Mijn inloggegevens werken niet voor de My Base App, wat moet ik doen?

Als u uw wachtwoord opnieuw instelt, wordt het multifactorauthenticatieproces opnieuw gestart en zijn de meeste problemen met inloggen opgelost. Als u geen e-mail of sms met uw eenmalige toegangscode ontvangt, dient u CSL Technische Ondersteuning te bellen om uw contactgegevens bij te werken. Bel ons via +31 (0) 88 474 7777.

Kan ik de signaalsterkte van een apparaat controleren via My Base?

Ja – zodra een apparaat in gebruik is genomen, kunt u controleren of het apparaat verbonden is en welke signaalsterkte het heeft (alleen relevant voor radiopaden, LAN-paden laten gewoon zien of LAN verbonden is of niet).
De signaalsterkte wordt weergegeven op een schaal van 0 – 10, waarbij 10 de hoogste sterkte is. U dient te streven naar een minimum van 4/10 of meer om betrouwbaar signalen te verzenden en te ontvangen. Apparaten die aan deze sterkte voldoen, zullen een GROENE TIK naast het pad weergeven. Apparaten met 3/10 of minder tonen een ROOD KRUISJE naast het pad. Dit is geen geschikt connectiviteitsniveau; u kunt problemen ondervinden met het verzenden en ontvangen van signalen.

Kan ik een testoproep/alarm versturen via My Base?

Ja – ga eerst naar een live site. Druk onder Transmissiepaden op het symbool rechtsboven, waar 3 regels staan. U dient een optie te zien om een testoproep/alarm te verzenden. Alle oproepen, inclusief tests, worden gelogd onderaan de site waarop u zich bevindt. Scroll gewoon naar beneden om deze te zien.

Kan ik eventuele verbindingsdalingen zien via de My Base App?

Ja – ga eerst naar een live site. Onder beschikbaarheidsgrafieken ziet u de beschikbaarheid van alle paden. Een weergegeven waarde van 1 betekent dat er geen problemen zijn met de beschikbaarheid op een bepaalde dag. Een waarde van 0 betekent een verlies in beschikbaarheid. Grafieken tonen tot 30 dagen aan gegevens, maar grafieken kunnen aangepast worden om slechts 1 – 30 dagen te tonen; gebruik de schuifknop om dit aan te passen.

Kan ik de firmware van een apparaat upgraden via de My Base App?

Ja – zoek het apparaat dat een upgrade dient te krijgen. Eenmaal geselecteerd, scroll je naar de Hardware-sectie en klik je op de knop met de tekst UPGRADE. Er verschijnt een dialoogvenster om de upgrade te bevestigen, klik op ja en de firmware-upgrade wordt uitgevoerd. Dit dialoogvenster verdwijnt en op de knop met de tekst UPGRADE staat nu VIEW STATUS. U kunt nu op deze knop drukken om de status van uw verzoek te bekijken.

De upgrade bestaat uit twee fasen: het initialiseren van de aanvraag en het voltooien van de aanvraag. U ziet de tekst Firmware-update voltooid zodra alles met succes is geüpgraded.

Kan ik het paneelprofiel van een apparaat wijzigen via de My Base App?

Ja – selecteer het apparaat waarvoor u het paneelprofiel wilt wijzigen. Druk in het gedeelte Hardware op het pictogram rechtsboven, waar 3 regels staan. Klik op de optie Paneel bewerken. U kunt maximaal twee paneelprofielen selecteren. Als u tevreden bent met uw selectie(s) klikt u op Wijzigingen opslaan om te bevestigen. Dit start automatisch een herstart waarna de paneelprofielen zijn gewijzigd.
Wanneer u nu het paneelprofiel voor het apparaat bekijkt, wordt in het gedeelte Hardware de naam van het/de nieuwe geselecteerde profiel(en) weergegeven.

Permissies

Permissies Handleiding

Met de My Base App kunnen installateurs zo efficiënt mogelijk werken. Maar niet iedereen dient overal toegang toe te hebben! Daarom hebben we verschillende toestemmingsniveaus gecreëerd, afhankelijk van de rol en verantwoordelijkheden van de medewerker. De tabel hieronder geeft een overzicht van de beschikbare toestemmingsniveaus. Neem vandaag nog contact met ons op via sales-eu@csl-group.cloud om uw team in te stellen! Bent u een Admin Gebruiker? Log dan in via CSL Live op een webbrowser om de rechten van uw team te beheren!

Permissie niveau	Geschikt voor	My Base login details zijn vereist	Huidige installatie bekijken	Geïnstalleerde sites bekijken	Configureren & testen	Gebruikerstoegang en meldingen beheren
Bekijken	**Kantoorpersoneel**	Ja	Ja	Ja		
Eenmalige Toegang*	**Aannemer/ 3e partij**	Ja Serienummer & Connectie-ID van apparaat vereist voor toegang	Ja 24 uur		Ja 24 uur	
Beperkte toegang**	**Monteurs**	Ja	Ja Scan de QR-code op het apparaat	Ja Scan de QR-code op het apparaat	Ja Scan the QR code on the device	
Gebruiker	**Senior Ingenieurs**	Ja	Ja	Ja	Ja	
Admin***	**Management**	Ja	Ja	Ja	Ja	Ja

BELANGRIJK

* **Eenmalige toegang** – toegang tot het apparaat is alleen beschikbaar via een webbrowser – mybase.csl-group.cloud/new-install (https://cslgroup.enginecms.co.uk/formgen/editform/chapters_uk/mybase.csl-group.cloud/new-install)

** **Beperkte site-toegang** – scan de QR-code van het apparaat ter plaatse om toegang te krijgen via de My Base App.

*** **Admin** – Gebruikersbeheer is alleen beschikbaar op CSL Live via een webbrowser, niet via de My Base App.