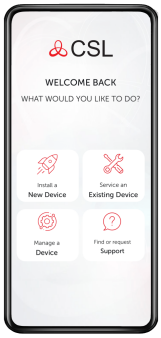
PRODUKTSUPPORT

My Base App 2.0

Uppdaterad den 18 mars 2025



Our handy Installer App allows you to configure and test your connected devices. Remotely access, configure and test your connected devices wherever you are via your smartphone or your browser.

To download the My Base App today, please visit:

Download on the App Store GET IT ON Google Play

(https://play.google.com/store/apps/details?id=com.cslgroup.mybase&hl=en_GB&gl=US)

Senaste informationen
https://csl-group.cloud/se/stod/my-base/

Quick Guide

The App Store (https://apps.apple.com/gb/app/csl-my-base/id1479184708#?platform=iphone)

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

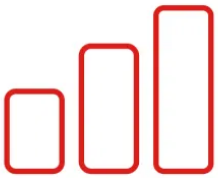
Registrera dig nu (https://csl-group.cloud/se/resurser/my-base-app-2-0/#contact)

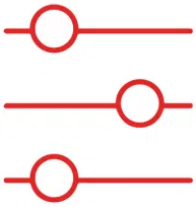
One-Time Access Portal (https://mybase.csl-group.cloud/new-install)

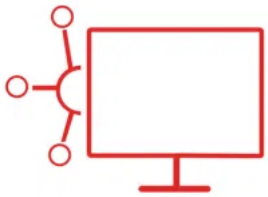
Introduction

My Base provides Installers with the ability to manage and configure DualCom Pro devices on a handy App/Web portal.

Simply download **CSL My Base** from your appropriate App store and obtain log-in information from CSL (or the CSL web administrator within your company) to access these great features:

View path status	Check signal strength	View panel connection status	Configure static IP information
			

Amend panel connection 	Change pin configuration 	Check ATS path availability 	Remotely upgrade device firmware 
View Alarms (you must still check with your ARC that alarms are being received by them) 	Test Alarm 	Invert fault relay 	Configure outputs 

Amend Smart Reporting	Add estate name
	

User Management for My Base 2.0 & the CSL Live Shop

User Management

The User Management area within CSL Live allows you to create/manage Shop and My Base logins for your employees – feature only available for accounts with 'Admin' Permissions. User Management is not available via the My Base App, you must use the CSL Live portal via a web browser. CSL Live is split into two sections the Shop and My Base. 'Admin' permissions are given for these sections separately. You will only be able to create/manage users under the area you have been allocated 'Admin' permissions.

For Example

- Accounts with 'Admin' permissions for the Shop – can create/manage users for the Shop.
- Accounts with 'Admin' permissions for My Base – can create/manage users for My Base.
- Accounts with 'Admin' permissions for both – can create/manage users for both.

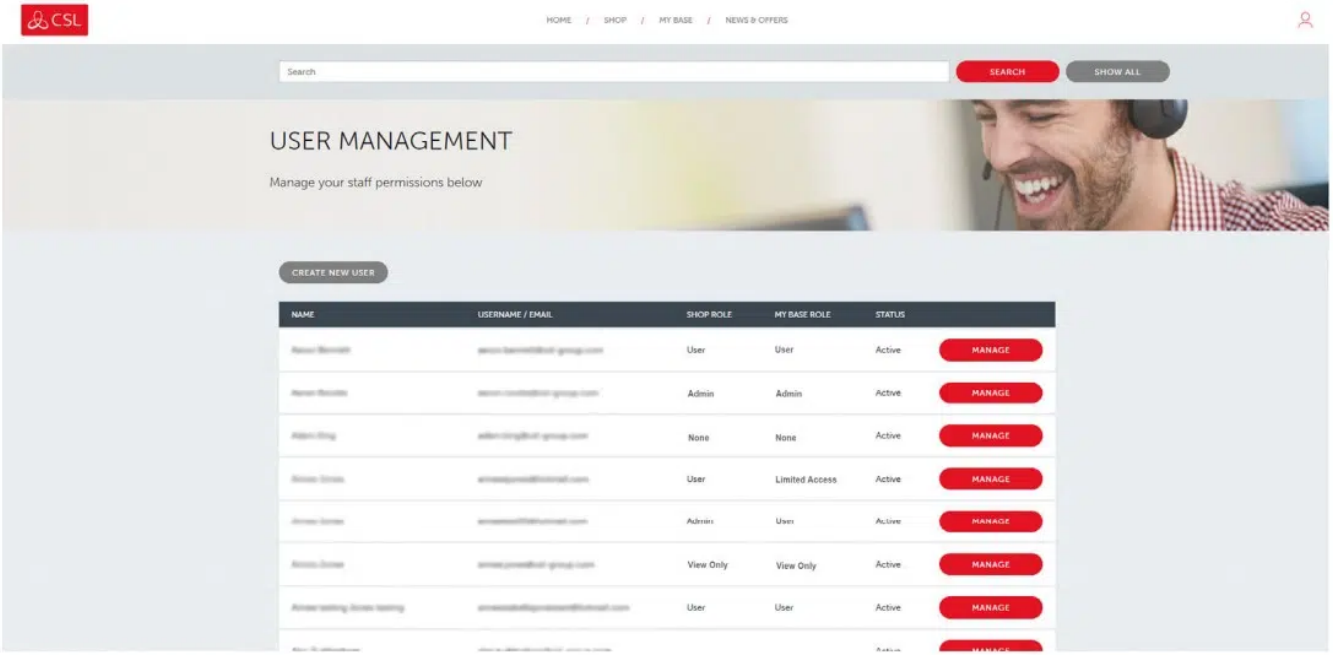
Accessing the User Management area from CSL Live Shop or My Base

Admin users will be able to access this feature via the 'Person' icon in the top right of the screen, under 'User Management'.



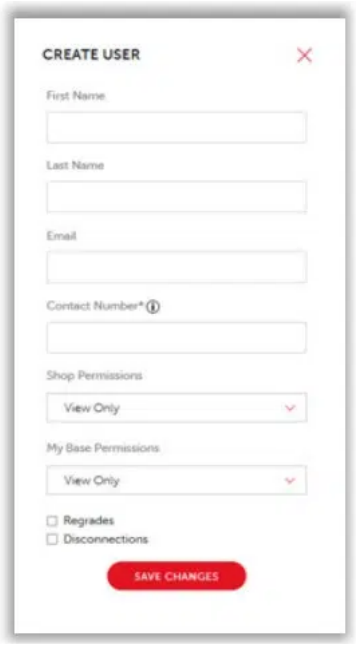
User Management Home Page

The User Management home page is where you can view and search all logins under your account. You will be able to create new logins and amend an existing account's credentials. There is also the ability to deactivate any account should this be required.



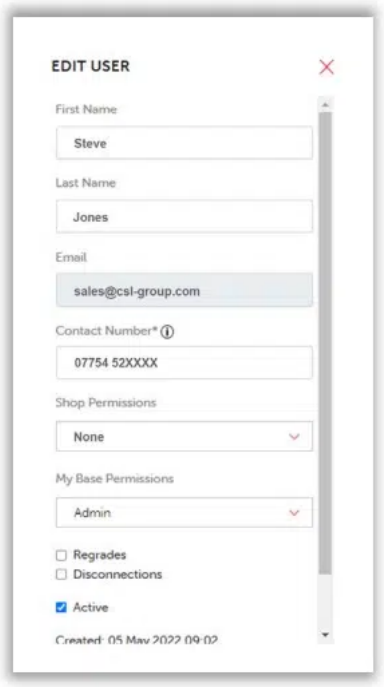
Create New User

Click ‘Create User’, just above the table. A pop-up box will be displayed where you can add a new user’s details to create a new login. You will only be able to view and select the available roles under ‘Shop Permissions’ and ‘My Base Permissions’ if your account has ‘Admin’ permissions for these areas.



Manage Existing Users

Select 'Manage' on the user you wish to amend. A pop-up box will be displayed where you can amend the user's details. You can amend their: first name, last name, Shop/My Base credentials and deactivate an account. You can also view when the user was created and when they last logged into this section.



More information:

- 'Regrades and Disconnections' tick box (ARCs only) – this enables ARC Admin users to initiate a regrade or disconnection request via My Base (web portal only) on behalf of the Installer.
- UDL/Remote Manager Access. Should any My Base users also require Remote Manager access, please contact us. (https://csl-group.cloud/se/kontakta-oss/)
- Permission roles explained: for an overview of the roles, please click here or for a more detailed explanation, see page 3 of this document.

Permissions Explained

CSL Live				
	View only	User	Admin	None

View recent orders	Y	Y	Y	N
Track orders	Y	Y	Y	N
View products	N	Y	Y	N
Order products	N	Y	Y	N
Access service requests	N	N	Y	N
Approve/reject service requests	N	N	Y	N
Receive service request notification emails	N	N	Y	N
Create additional users	N	N	Y	N
Suspend current users	N	N	Y	N
Manage email notifications	N	N	Y	N

My Base

	View only	User	Admin	Limited site access	One Time Access
View Sites	Y	Y	Y	Only searched site	N
Search Sites	Y	Y	Y	Only searched site	N
Site Search Boxes	Y	Y	Y	N	N
Filter Search	Y	Y	Y	N	N
Live Chat	Y	Y	Y	Y	Y

Enter site	Y	Y	Y	Y	Only new/pending
Edit address	N	Y	Y	Y	Only new/pending
Edit Smart Reporting	N	Y	Y	Y	Only new/pending
Firmware upgrade	N	Y	Y	Y	Only new/pending
Reboot	N	Y	Y	Y	Only new/pending
Edit panel	N	Y	Y	Y	Only new/pending
Edit pins	N	Y	Y	Y	Only new/pending
View Path Status	Y	Y	Y	Y	Only new/pending
Edit Path Config	N	Y	Y	Y	Only new/pending
Send Test Alarms	N	Y	Y	Y	Only new/pending
View Availability Chart	Y	Y	Y	Y	Only new/pending
View Alarms	Y	Y	Y	Y	Only new/pending
Filter Alarms	Y	Y	Y	Y	Only new/pending
Export Alarms	Y	Y	Y	Y	Only new/pending
Invert Relay Output	N	Y	Y	Y	Only new/pending
Initiate Change Grade Request	N	Y	Y	N	N

Initiate Disconnection Request	N	Y	Y	N	N

Multi-Factor Authentication

How To Set It Up:

1. Enter your username and password on CSL Live or the My Base App as usual.
2. Open your Authenticator App, and select 'send code via email' or 'send code via SMS'.
3. Receive a code from your Authenticator App, program, email or SMS.
4. Enter the code in CSL Live or the My Base App.
5. You are now securely logged in.

What Is Multi-Factor Authentication (MFA)?

MFA is an authentication process that requires two methods to verify the identity of a user, strengthening the access security of a system. This form of authentication protects against phishing, social engineering and password brute-force attacks. Moreover, it has the capability to secure logins from attackers exploiting weak or stolen credentials.

Why Is MFA Important?

MFA is a vital part of a zero-trust security model. To protect sensitive data, users requesting access to data must confirm they are who they say they are. MFA ensures protection against many security threats that target user passwords and accounts, such as those mentioned above. If a remote attacker can tap into a computer via a user's internet connection, they could gain access to the user's password, along with a second form of authentication, if both are delivered over the same channel. Remote attackers can't attempt to steal a user's identity (in order to gain unauthorised access to information stored in applications) without that individual's physical device. By integrating MFA, attackers will be unable to access private accounts without possessing a user's physical device needed to complete the second factor.

What Type Of MFA Does CSL Use?

CSL uses time-factor authentication, sometimes referred to as Time-Based, One Time Password (TOTP). The TOTP MFA method generates a code in time-based intervals that the user must enter in order to gain access. The passcode generated by the authenticators, or SMS/email, expires after a certain period and a new one will be generated the next time a user logs into their account. TOTP is part of the Open Authentication (OAUTH) security architecture.

CSL has implemented time-factor authentication with OTP, email and SMS. Here is a list of commonly used authenticators approved by CSL:

- Free OTP
- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- 2FA Authenticator (2FAS)
- Aegis Authenticator
- Authy
- Due Mobile IBM Security Verify How does it work?



1. Enter your username and password on CSL Live as usual
2. Receive a code from your Authenticator App, programme, email or SMS
3. Enter the code in CSL Live
4. You are now securely logged in

Which Industries Use MFA?

End-point security is rapidly becoming an important concern for many industries. Regardless of which applications users are accessing, protecting credentials is paramount to ensuring the security of the wider business.

Retail		Now the nation's largest employing industry, remote attacks have become dominant in the sector and difficult to prevent. Additionally, security solutions are becoming increasingly important for retail as information technology adjusts to a perimeter-less environment. MFA provides peace of mind for companies within retail – allowing them to authenticate the identities of users accessing their networks through remote desktops and personal mobile devices.
Banking		Banks use MFA to protect against the many hacking attempts made on both their own internal and their customer's systems. MFA has helped many large banks improve their resiliency against such attacks. It has become paramount for all banks to know which users and devices are accessing their systems at any given time. MFA allows the Banking industry to secure remote devices and authenticate every login attempt
Social Media		Social media platforms and agencies use MFA to protect the personal data of billions of users worldwide. Companies, such as Facebook, use authentication to shield their developers from hacking attempts when working on the company's internal networks. MFA also makes security easier for social media companies by simplifying the access process for developers. Cloud-based MFA solution protects developers, and users in turn, by eliminating the need for hardware and software installation.

Government		Current IT developments are challenging government agencies to implement rapid changes to their infrastructure, as they look to accommodate the shift to cloud and mobile. MFA technology assists government agencies as they put forward zero-trust policies for the millions of users who need access.

MFA FAQs

What if a user has lost or replaced their mobile device?

MFA relies on users to have a device with which to authenticate. If that smartphone or laptop is lost, stolen or replaced, users can self-enrol a new device by resetting their password via CSL Live. This feature can also be used if the user purchases a new phone or laptop to register MFA on their new device. Wherever a user is in the world and whatever technology they are using, their information will be secure.

Can I set up MFA on multiple devices?

Yes, you can set up MFA on multiple devices – MFA lets you link multiple devices to your account.

My chosen authenticator isn't on the list, is it OK to use?

CSL has tested and approved those listed in this document. We recommend that you use these authenticators in order to ensure the reliability and accessibility of your CSL Live account.

I can't use an authenticator App, what are my other options?

We've developed backup options for SMS and email in case you cannot use an authenticator app for whatever reason. Simply select the SMS or email option when the system prompts you for a one-time code. All SMS/emails have an expiry time of 60 seconds.

How can I find out more?

For more information on MFA standard practices and guidelines please follow the links below.

National Cyber Security Centre (https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services)

National Institute of Standards and Technology (https://www.nist.gov/back-basics-multi-factor-authentication)

FAQs

What is the My Base App?

The My Base App is a self-service management platform for all DualCom Pro devices. The App allows you to check your signal strength, request regrades, send test alarms, view availability graphs, edit panel profiles, upgrade firmware and view alarm logs.

How do I gain access to the My Base App?

Once you've installed the My Base App from your applicable App Store, please visit the CSL Website to register for a My Base account. Please click here. (https://csl-group.cloud/se/resurser/my-base-app-2-0/#contact)

For security, we'll contact you in order to authorise your request and set the appropriate permission levels for your My Base account. Once approved, we'll send you your login credentials.

Need Support? Call CSL Technical Support on +44 (0) 1895 474 444.

Can I manage permissions and access of the users within my company?

Yes, this feature is now available via the CSL Live web portal. Click here (https://csl-group.cloud/se/support/my-base/) to access our User Management guide.

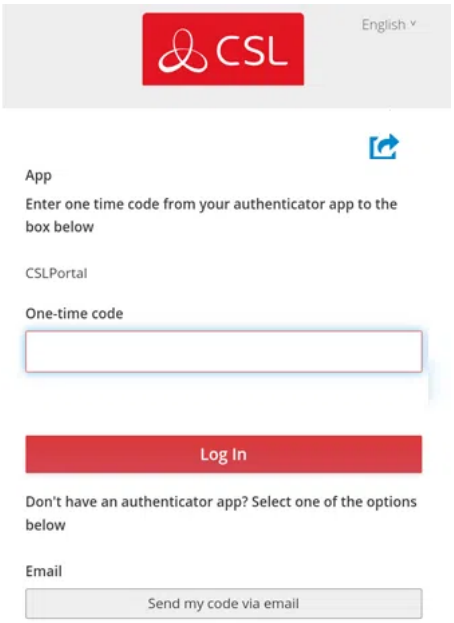
How do I set up Multi-Factor Authentication on the My Base App?

For security, multi-factor authentication (MFA) is now required to use the My Base App. MFA increases security on our platform and requires users to authenticate themselves via their username/password and with a time-limited code (each code expires after 60 seconds). This code is obtained via an Authenticator App, email or SMS. New authentication is required **once every 30 days**; if the user **logs out** or if we **update CSL Live.**

How it works:

1. Log in to My Base as normal with your username and password.
2. Receive a code via an Authenticator App, email or SMS.
3. Enter the code within My Base.

4. You are now securely logged in.



If you have any issues with the steps above, resetting your password will restart the authentication process. If the issue persists and you require support, call CSL Technical Support on +44 (0) 1895 474 444.

Which Authenticator Apps work with My Base?

Here is a list of commonly used authenticators approved by CSL:

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

My login credentials aren't working for the My Base App, what shall I do?

Resetting your password will restart the multi-factor authentication process and resolve most issues with logging on. If you're not receiving an email or text with your one-time access code you'll need to call CSL Technical Support to update your contact details. Please call us via +44 (0) 1895 474 444.

Can I check a device's signal strength via My Base?

Yes – once a device is commissioned, you will be able to check whether the device is connected and what signal strength it has (only relevant for Radio paths, LAN paths simply show if LAN is connected or not).

Signal strength is shown on a scale from 0 – 10, with 10 being the highest strength. You should aim for a minimum of 4/10 or more to send & receive signals reliably. Devices meeting this strength level will show a GREEN TICK next to the path. Devices with 3/10 or less will show a RED CROSS next to the path. This is not a suitable level of connectivity; you may experience issues sending and receiving signals.

Can I send a test call/alarm via My Base?

Yes – first enter any live site. Under Signalling Paths, press the symbol in the top right, where there are 3 lines. You should see an option to send a test call/alarm. All calls, including tests, are logged at the bottom of the site you are on. Simply scroll to the bottom to see these.

Can I see any drops in connectivity via the My Base App?

Yes – first enter any live site. Under Availability Graphs, you will see the availability of all paths. A displayed values of 1 means no issues with availability on a given day. Values of 0 mean a loss in availability. Graphs show up to 30 days of data, but graphs can be adjusted to just show from 1 – 30 days; use the slider to adjust this.

Can I upgrade the firmware of a device via the My Base App?

Yes – find the device in need of the upgrade. Once selected, scroll to the Hardware section and click the button that says UPGRADE. A dialogue box will appear to confirm the upgrade, click yes and the firmware upgrade will commence. This dialogue box will disappear and the button that said UPGRADE will now say VIEW STATUS. This can now be pressed to view the status of your request.

There are two phases to the upgrade, initialising the request and completion of the request. You will see text that says Firmware Update Complete once everything has been successfully upgraded.

Can I change a device's panel profile via the My Base App?

Yes – select the device you wish to change the panel profile for. Under the Hardware section, press the icon in the top right, where there are 3 lines. Click the option that says Edit Panel. You can select up to two panel profiles. Once you are happy with your selection/s click Save Changes to confirm. This will automatically initiate a reboot after which the panel profile/s will have changed.

When you now look at the panel profile for the device, in the Hardware section, it will display the name of the new profile/s you selected.

Permissions

Permissions Guide

The My Base App enables Installer companies to work in the most efficient way possible. However, not everyone needs access to everything! This is why we have created different permission levels depending on the employee's role and responsibilities. The table below outlines the permission levels available. Contact us today via sales@csl-group.cloud to set your team up! Are you an Admin User? Simply log in via CSL Live on a web browser to start managing your team's permissions!

Permission level	Suitable for	My Base login details are required	View current installation	View installed sites	Configure & test	Manage user access & notifications
View Only	**Office Staff**	Yes	Yes	Yes		
One Time Access*	**Contractor/ 3rd Party**	Yes Serial number & connection ID of device required for access	Yes 24 hours only		Yes 24 hours only	
Limited Site Access**	**Engineers**	Yes	Yes Scan the QR code on the device	Yes Scan the QR code on the device	Yes Scan the QR code on the device	
User	**Senior Engineers**	Yes	Yes	Yes	Yes	
Admin***	**Management**	Yes	Yes	Yes	Yes	Yes

IMPORTANT

*** One-Time Access** – access to the device is only available via a web browser – mybase.csl-group.cloud/new-install (https://cslgroup.enginecms.co.uk/formgen/editform/chapters_uk/mybase.csl-group.cloud/new-install)

**** Limited Site Access** – scan the device's QR code on-site to provide access via the My Base App

***** Admin** – User Management is only available on CSL Live via a web browser, not via the My Base App