Contents

Securing you CleverLive account with Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a mechanism to allow an even stronger level of protection for users of the CleverLive (CL) digital signage portal.

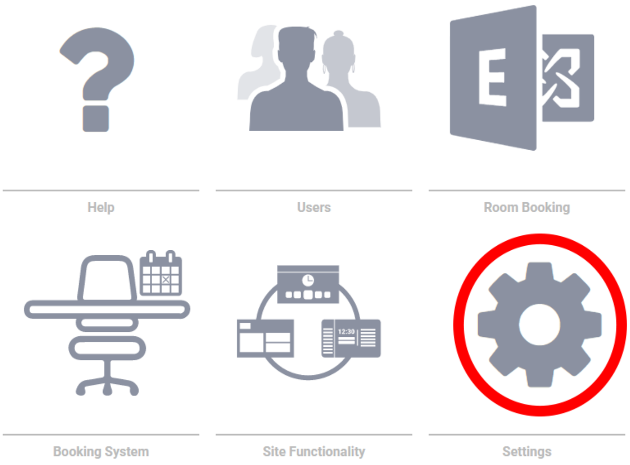
- Level 1 security – User name and password
- Level 2 security - User name and password + IP address locking
- Level 3 security - User name and password + MFA
- Level 4 security - User name and password + MFA + IP address locking

For admin and security purposes the CL platform has 3 level of users

1. Account Owner (AO)
2. Admin
3. General User (GU)

IP address locking

AO and Admin users can enter IP addresses into the IP whitelist which can be found under the setting menu on the AO and Admin home pages.



Once one or more IP addresses are entered, only users whose external internet IP addresses match these IP address can login to the CL platform.

This allows AO & Admins to limit users to only those logging in from within their own physical premise

Multi-Factor Authentication introduction

Multi-Factor Authentication (MFA), represented on the CL portal with the icon 🔒, is a world-wide standard for providing online applications with an extra level of security.

To use MFA you need to install an Authenticator application on your mobile phone. The CL portal supports all the major Authenticator apps (that use the TOTP algorithm) including Google Authenticator, Microsoft Authenticator, Authy Authenticator, DUO Authenticator and FreeOTP.

All applications work in the same way.

1. Install your application
2. Find the setting, in your app, to add a new account using a QR code
3. Scan the QR code presented to you by the CL platform with your Authenticator App
4. You Authenticator app makes a connection with the CL platform
5. Your Authenticator app will now create 6 digits password which are unique to CL and only valid for 30 seconds

Now every time you login to CL you

1. Enter your user name and password
2. You will next be prompted for a 6 digit code
3. Open your Authenticator app and it will provide the 6 digit code, valid for 30 seconds
4. Enter that code into CL
5. Login to CL is now complete

Account Owner (AO) MFA

The Account Owner (AO) is the login credentials used to initially set up the account on the CL portal.

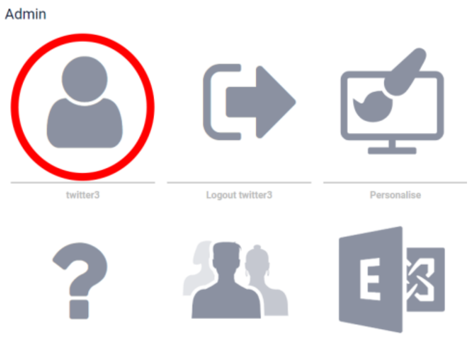
This account can be considered a super admin because

- it cannot be deleted, without deleting all other admin and general user accounts.
- Logging in with these credentials will always provide full admin privileges

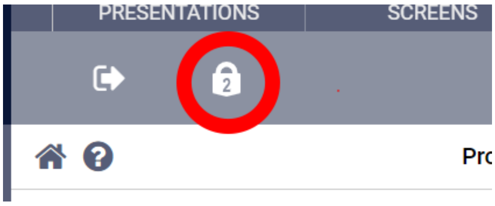
It is recommended that this account NOT be created using a staff members email address, in case they leave the business, but instead an email under the full control of the customers' IT department.

Applying MFA to the Account Owner (AO)

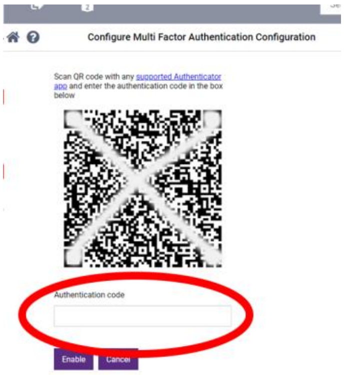
1. Login to CTL as Account Owner
2. On the home page go to the profile page



3. In the top toolbar click the MFA icon



4. Open your Chosen Authenticator app, scan the QR code shown and enter the 6 digit code it provides in the box shown and click enable



Configure Multi Factor Authentication Configuration

Scan QR code with any supported Authenticator app and enter the authentication code in the box below

Authentication code

MFA is now enabled

5. Recovery codes.
   If you enable MFA but lose your mobile phone, delete you Authenticator app, or for any other reason lose access to the ability to create the 6 digit MFA codes, you will be locked out of your account. As this is the AO account there are only two ways to regain access to your account.

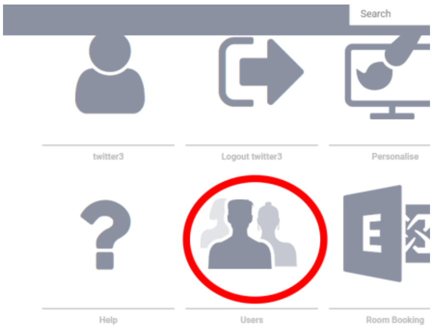
   a. When you first enable MFA you will see a page containing 10 off, single use, recovery codes. Store these in a **very** secure location and you can use them to regain access to your account later (up to 10 times). Once you close the page showing these codes you will not be able to access these codes again. Storing these codes is itself insecure, as they offer a backdoor into your account. It is the user's responsibility to decide if they need this facility and to so to store these codes securely.
   b. Contact Sahara Boxlight support. You will be asked for proof of identity, and this may incur a charge.

Disabling MFA from the AO account.

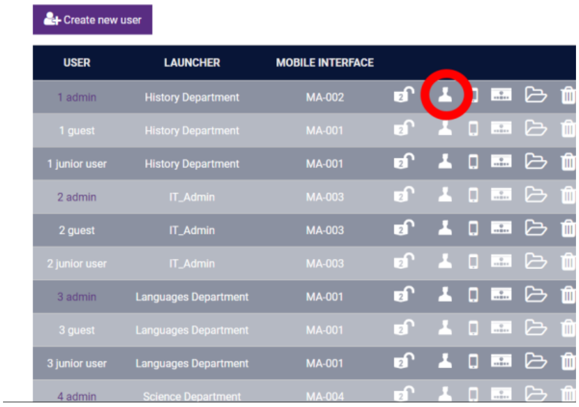
Repeat steps 1 to 3 (immediately above) and enter a code from your Authenticator app to remove the MFA requirement.

Creating Admin accounts

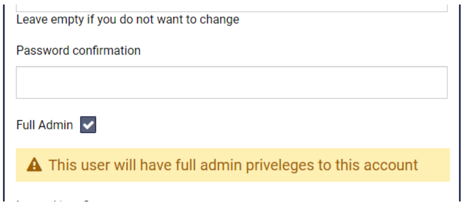
CL allows the AO to create general and admin users, who can be assigned privileges, using the 'Users' selection on the home admin page.



After a new user has been created, clicking on that user’s profile icon in the list of users allows the AO to add the permission that this user will be a full Admin



USER	LAUNCHER	MOBILE INTERFACE
1 admin	History Department	MA-002
1 guest	History Department	MA-001
1 junior user	History Department	MA-001
2 admin	IT_Admin	MA-003
2 guest	IT_Admin	MA-003
2 junior user	IT_Admin	MA-003
3 admin	Languages Department	MA-001
3 guest	Languages Department	MA-001
3 junior user	Languages Department	MA-001
4 admin	Science Department	MA-004



Leave empty if you do not want to change

Password confirmation

Full Admin ☑

This user will have full admin priveleges to this account

Once a user is made into an Admin user their username will be highlighted in purple.

Applying MFA to Admin accounts

Admin accounts can have MFA applied to in two ways

1) Following the same procedure as “Applying MFA to the Account Owner” described above
2) Using the procedure to “Apply MFA to general users” shown below.

Removing MFA from Admin accounts

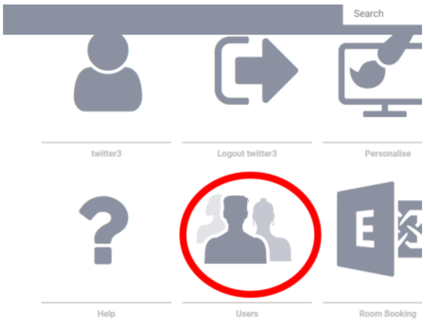
The Admin accounts can turn off MFA on their own account in two ways

1) Following the same procedure as “Disabling MFA from the AO account” described above
2) Using the procedure to “Removing MFA for general users” shown below

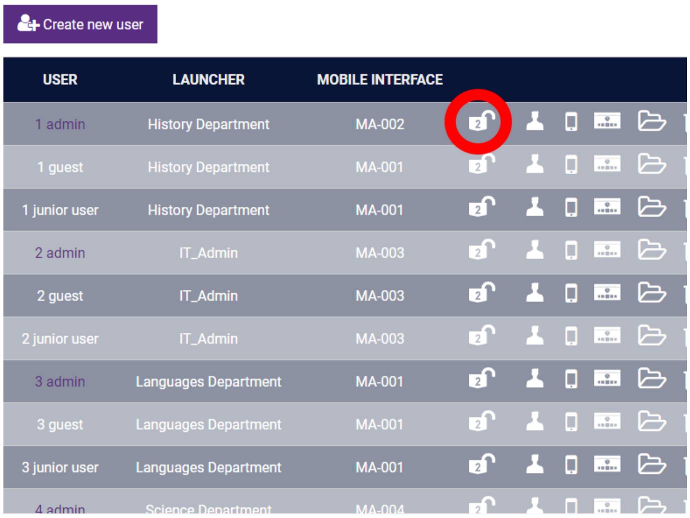
Apply MFA to general users

Account owners and Admin accounts can add General Users to an account and assign various permissions to these users. For example, a General User may be able to edit some text on a signage presentation or trigger an emergency alarm.

Guest Users are created and edited using the Users selection on the home admin page.



Once created, MFA policies can be set for General User (and Admin Users) by hovering over the MFA icon for a user.

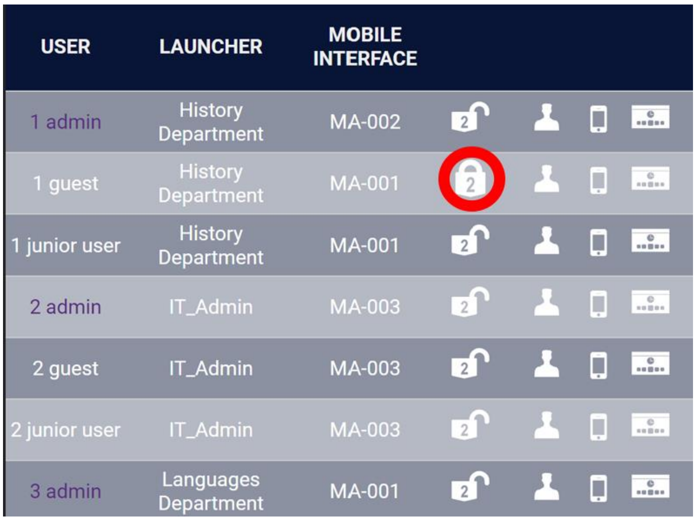


Create new user

USER	LAUNCHER	MOBILE INTERFACE
1 admin	History Department	MA-002
1 guest	History Department	MA-001
1 junior user	History Department	MA-001
2 admin	IT_Admin	MA-003
2 guest	IT_Admin	MA-003
2 junior user	IT_Admin	MA-003
3 admin	Languages Department	MA-001
3 guest	Languages Department	MA-001
3 junior user	Languages Department	MA-001
4 admin	Science Department	MA-004

When hovering over the MFA icon a selection appears. If the user does not have MFA applied to the account, the selection will say “Require MFA”.

If you click on “Require MFA” notification will appear that MFA is now required for this user to login and the icon changes from an unlocked padlock to a locked padlock



USER	LAUNCHER	MOBILE INTERFACE
1 admin	History Department	MA-002
1 guest	History Department	MA-001
1 junior user	History Department	MA-001
2 admin	IT_Admin	MA-003
2 guest	IT_Admin	MA-003
2 junior user	IT_Admin	MA-003
3 admin	Languages Department	MA-001

When the General User next tries to login to CL (or immediately if they are already logged in) they will be required to link their account to an Authenticator App, see "General User instructions for using MFA and Authenticator Apps" (below).

Removing and Resetting MFA for general and Admin Users

Once a requirement to use MFA has been set for a user it can be either removed or reset by hovering over a locked MFA padlock icon in the user list. It will offer either a single choice

1. Remove MFA requirement

Or offer three choices

1. Remove MFA requirement
2. Reset MFA
3. Turn MFA off and remove requirement

The single choice means that you set an MFA requirement, but the user has never linked their account to an Authenticator application. You can choose to remove the MFA requirement and the user will be unaffected.

The three choices occur if you set an MFA requirement and the user has connected their account to an Authenticator App. In this case there are three options.

1. Remove MFA requirement

Choose this is you no longer want to enforce an MFA requirement but are happy to let users carry on with MFA, if they are using it

2. Reset MFA

Choose this option if the User has lost access to their mobile phone or Authenticator application and needs to link it again

3. Turn MFA off and remove requirement

Choose this option if you want to actively stop user for using MFA.

General User instructions for using MFA and Authenticator Apps

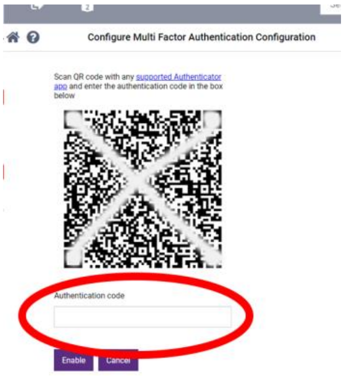
These instructions may be provided to CL guest users where the AO or Admin User has enforced an MFA requirement for the user.

To improve security, your CleverLive account administrator has implemented Multi Factor Authentication (MFA) on your CleverLive account login.

This means that once you have logged into your CL account, using your username and password, you will also have to enter a 6 digit security passcode generated be a third party Authenticator Application on your mobile phone. Your administrator will inform you if your company has a preferred Authenticator Application.

All industry standard Authentic Apps are supported including Google Authenticator, Microsoft Authenticator, Authy Authenticator, DUO Authenticator and FreeOTP.

1. Login to CleverLive using your username and password
2. Open your Chosen Authenticator app, scan the QR code shown and enter the 6 digit code it provides in the box shown and click enable



Configure Multi Factor Authentication Configuration

Scan QR code with any supported Authenticator app and enter the authentication code in the box below

MFA is now enabled

If you enable MFA but lose your mobile phone, delete you Authenticator app, or for any other reason lose access to the ability to create the 6 digit MFA codes, you will be locked out of your account. If you are locked out

a. When you first use MFA you will see a page containing 10 off, single use, recovery codes. Store these in a **very** secure location and you can use them to regain access to your account later (up to 10 times). Once you close the page showing these codes you will not be able to access these codes again. Storing these codes is itself insecure, as they offer a backdoor into your account. It is the user’s responsibility to decide if they need this facility and to so to store these codes securely.
b. If you chose not to store these codes ask your CL administrator to reset your MFA

Once MFA in enabled you will need to enter a 6 digit code, from your Authenticator app, in addition to your username and password every time you login to CL.