

# CMS User Login with Two-factor Authentication

## Overview

Two-factor authentication (2FA) is mandatory for CMS logins. Every CMS user is required to enter their password and verify the login through a PIN (passcode) from an authenticator app on their personal device. This two step procedure provides an extra security layer to check that the person logging into the CMS *is* the owner of the account.

## For CMS Users

You will be required to set up 2FA when you next attempt to login to CMS.

For two-factor authentication, you must have the following ready:

- **an *authenticating device***: this is usually a personal device you have access to during the login process, e.g., your smartphone,
- **an *authenticator app*** installed on your authenticating device.

There are a number of free third party Authenticator apps that you can easily download to your personal devices. Some popular ones are Google Authenticator, Authy and Microsoft Authenticator.

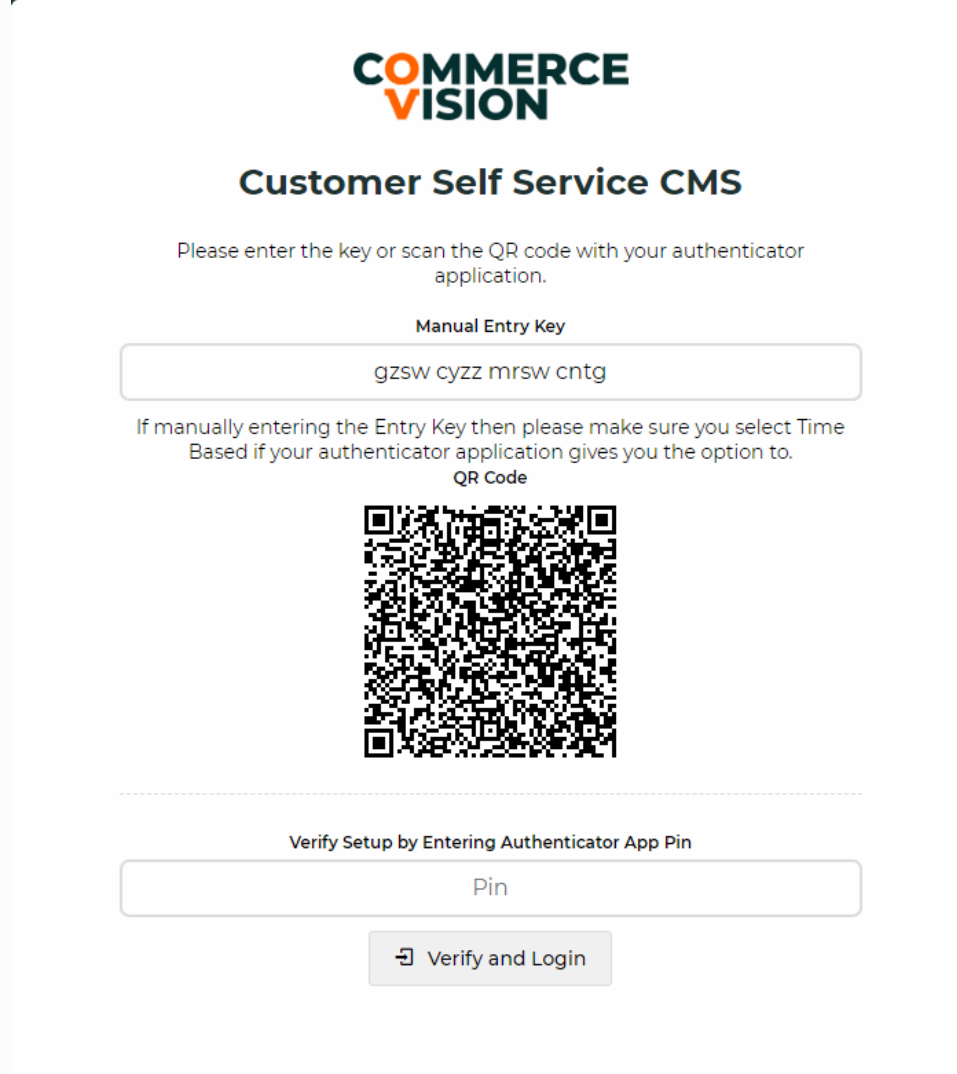
**NOTE** - The authenticating procedure may vary slightly for different apps but they all involve scanning a QR Code or manually entering an entry key, and then obtaining the authentication PIN for login.

### On this page:

- [Overview](#)
- [For CMS Users](#)
  - [Initial Authentication Setup Procedure:](#)
  - [Subsequent Logins](#)
- [Failed Logins](#)
  - [Reset 2FA by User](#)
  - [Unlock Another CMS User](#)
- [Password Changes](#)
  - [Resetting your 2FA](#)
- [For Administrators](#)
  - [Reset 2FA by Admin](#)
- [Force two-factor authentication on a User](#)
- [Related help](#)

## Initial Authentication Setup Procedure:

1. At the CMS login screen, enter your Username and Password, then click **Login**.
2. Instead of being logged in, the Authentication popup displays.



The screenshot shows a web browser window with the Commerce Vision logo at the top. Below the logo is the title "Customer Self Service CMS". A message reads: "Please enter the key or scan the QR code with your authenticator application." There are two options: "Manual Entry Key" and "QR Code". Under "Manual Entry Key", there is a text input field containing "gzsw cyzz mrswn cntg". Under "QR Code", there is a QR code. Below these options is a section titled "Verify Setup by Entering Authenticator App Pin" with a text input field containing "Pin". At the bottom of this section is a button labeled "Verify and Login".

3. Open the authenticator app on your authenticating device.
4. Either scan the QR Code or type in the Manual Entry Key. **NOTE** - if the 'Manual Entry Key' option is used, ensure 'Time-Based' is selected if you are asked to select a 'Type of Key' option.
5. The authenticator app generates a PIN that expires in a set amount of time. Enter this PIN in the Authentication popup.
6. Click **Verify and Login**. If the PIN is valid, access to CMS will be granted.

## Subsequent Logins

- Once you have successfully set up 2FA, the authenticator app saves the account for CMS login. At the next login, simply open the authenticator app in your device to get a valid PIN. This PIN is entered after the Username/Password step.



## Customer Self Service CMS

Two-Factor Application Pin

P|n

Confirm

If you need to reset your two-factor authentication for this account please contact the Commerce Vision Support Team using the below phone number Monday - Friday (8:30am - 5pm AEST) exc. public holidays & weekends

+61 7 3369 3733

### Failed Logins

- You have three attempts at logging in. After the third failed attempt, you will be locked out for an hour. Or you can ask another CMS user from your company or your Administrator to unlock you.

Under certain circumstances, you receive an error message that the PIN is invalid.

There are several reasons that could have caused it:

- You have not set up the 2FA correctly
- You entered an incorrect PIN.
- If not one of the above, the next most likely cause that the PIN you entered has expired. When a PIN is generated, it is current for a 30 second block based on UTC time. The UTC time is based on the time on your device. The PIN you entered must be generated between 5 minutes before current time and 5 minutes after current time. This means your phone time must be quite close to the time on the server, if not exactly the same. If let's say you set your phone time 10 minutes ahead of actual time, the PIN you entered may not be accepted.

### Reset 2FA by User

- An authenticated User can reset and set up a new authentication when logged in CMS. To reset authentication, they just follow the steps for [User Reset for 2FA](#). Once the procedure is completed, the new authentication will automatically replace the old one.

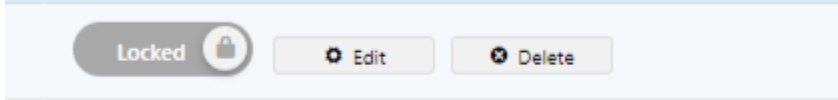
### Unlock Another CMS User

A CMS user in your company can unlock a user whose account is locked due to too many failed attempts. **NOTE** - If there are no other CMS users in your company, your account can be unlocked by Commerce Vision.

To unlock a CMS user:

- In CMS, go to **Users CMS Users**.
- In **User Search**, find the user.

3. A locked user will have the **Locked** button next to them. Click on it to unlock the user.




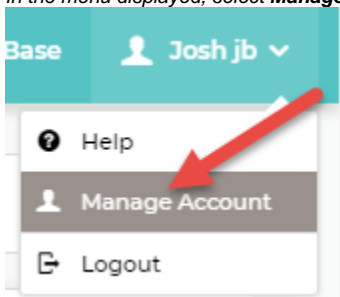
**NOTE** - The Locked button is also displayed in the Edit User's page.

## Password Changes

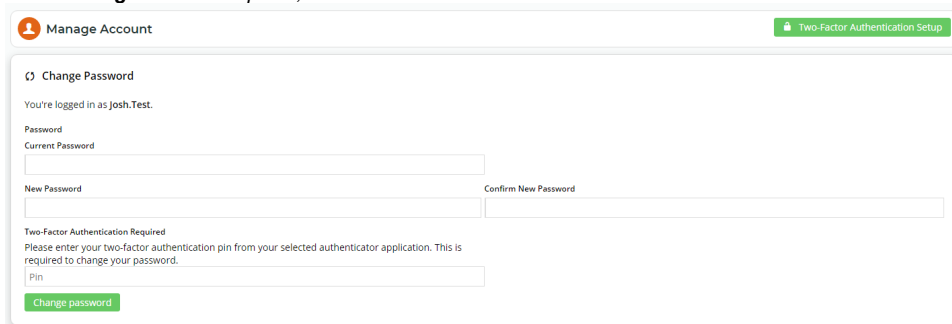
- When two-factor authentication is active for the User, a Password change by the User must be authorised by entering a valid PIN.

*To change the CMS password,*

1. While logged into CMS, hover over the  icon on the top right corner of the screen.
2. In the menu displayed, select **Manage Account**.



3. In the '**Change Password**' panel, enter the Current/New Password details.



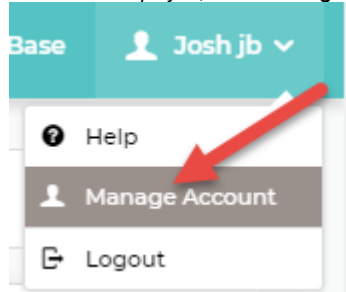
4. In **Two-Factor Authentication Required**, enter a valid PIN obtained from the authenticator app.
5. Click **Change Password**.

## Resetting your 2FA

- A User can reset 2FA for their CMS login. They must be logged into the CMS at the time.

1. In the CMS, hover over the  icon on the top right corner of the screen.

2. In the menu displayed, select **Manage Account**.



3. In the **Manage Account** screen, click the **Two-Factor Authentication Setup** button.

A screenshot of the 'Manage Account' screen. At the top, there's a header with a user icon and the text 'Manage Account'. To the right of this header is a green button labeled 'Two-Factor Authentication Setup', which is highlighted by a red arrow. Below the header, there's a section titled 'Change Password' with a sub-header 'You're logged in as Josh.Test.'. It contains fields for 'Current Password', 'New Password', and 'Confirm New Password'. Below these fields is a section titled 'Two-Factor Authentication Required' with a sub-header 'Please enter your two-factor authentication pin from your selected authenticator application. This is required to change your password.' and a 'Pin' field. At the bottom of this section is a green button labeled 'Change password'.

4. In the **Setup Two-Factor Authentication** screen, you will see a generated 'Manual Entry Key' and a 'QR Code'.

A screenshot of the 'Setup Two-Factor Authentication' screen. It has a header with a user icon and the text 'Setup Two-Factor Authentication'. Below the header, there's a section titled 'Please enter the key or scan the QR code with your authenticator application.' It contains a 'Manual Entry Key' field with a red arrow pointing to it, showing the text 'mqdt omru mqzt qqlf'. Below this is a section titled 'If manually entering the Entry Key then please make sure you select Time Based if your authenticator application gives you the option to.' followed by a 'QR Code' field with a red arrow pointing to it, showing a QR code. At the bottom, there's a section titled 'Verify Setup by Entering Authenticator App Pin' with a 'Pin' field and a 'Verify and Save' button.

5. In your authenticating device, open the authenticator app and either scan the QR Code or type in the Manual Entry Key. **NOTE** - if the 'Manual Entry Key' option is used, ensure 'Time-Based' is selected if you are asked to select a 'Type of Key' option.
6. The Authenticator app will generate a PIN. Enter this PIN in **Verify Setup by Entering Authenticator App PIN**.
7. Click **Verify and Save**. If the PIN is valid, setup is successful and you will be logged into CMS. **NOTE** - A popup error message will display if the PIN is invalid.

## For Administrators

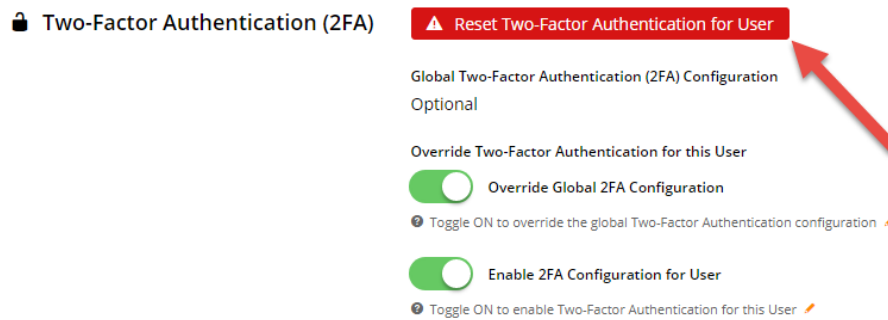
### Reset 2FA by Admin

CMS Administrators and Commerce Vision can clear the current authentication set up by a User by resetting the User's authentication. This step is required if forced two-factor authentication is to be disabled for a User or the User has lost access to their current authentication.

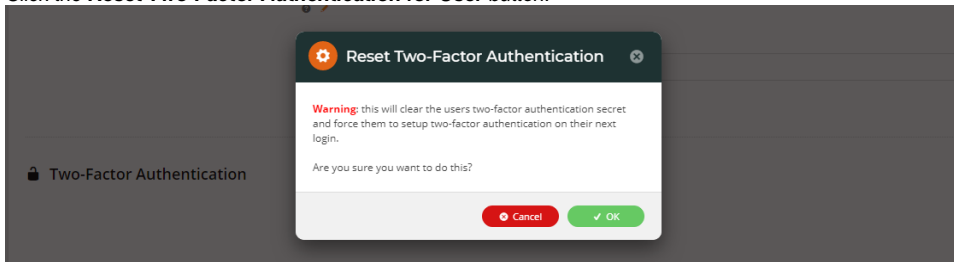
To reset a User's authentication,

1. Navigate to **Users CMS Users**.

2. Use the **User Search** tool to find the specific User and click **Edit**.
3. Scroll down to the **Two-Factor Authentication (2FA)** section.
4. When a User has a current authentication set up, the **Reset Two-Factor Authentication for User** button will appear.



5. Click the **Reset Two-Factor Authentication for User** button.



6. In the **Reset Two-Factor Authentication** popup, click **OK** to confirm you want to delete the current authentication.

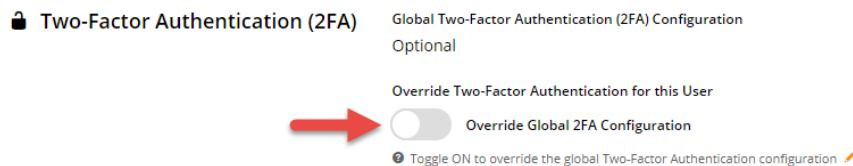
## Force two-factor authentication on a User

**NOTE - This section only applies if 2FA is not globally active.**

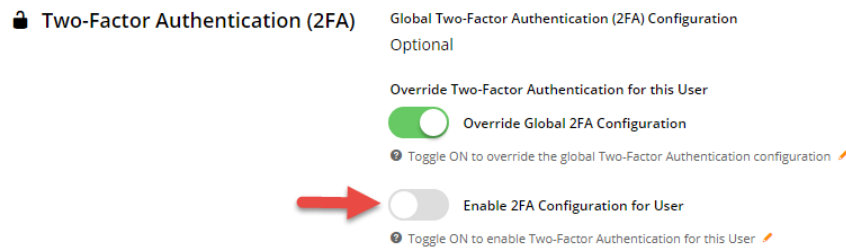
CMS Administrators can make two-factor authentication mandatory (forced) for Users. Forced authentication must be enabled for each User individually as the global setting is OFF.

To enable two-factor authentication for a User,

1. Navigate to **Users CMS Users**.
2. Use the **User Search** tool to find the User and click **Edit**.
3. Scroll down to the **Two-Factor Authentication (2FA)** section.
4. Toggle ON **Override Global 2FA Configuration**.

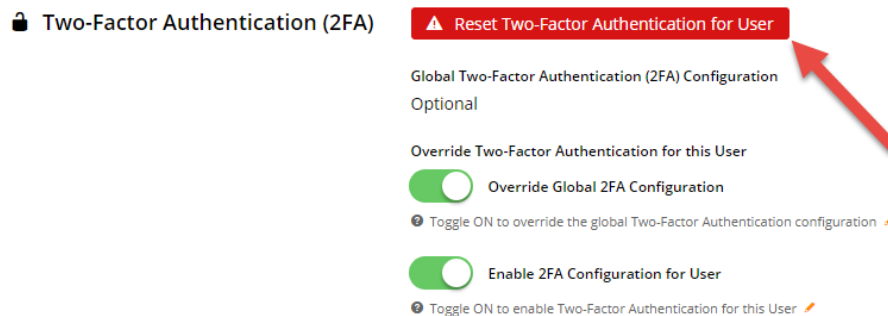


5. Once **Override Global 2FA Configuration** is on, the **Enable 2FA Configuration for User** toggle will display. Toggle this ON.



6. To save the setting, click **Save & Exit**.

7. When a user has set up their authentication, Administrators will see a red **Reset two factor Authentication for User** button in the **Two-Factor Authentication (2FA)** section.



#### Disabling forced authentication

Administrators can disable forced authentication for a User by toggling OFF **Override Global 2FA Configuration** and **Enable 2FA Configuration for User** and saving the change. However, if the User has set up a current authentication, the system will not permit disabling until the authentication has been cleared ([reset](#)).

## Related help

- [Create CMS Users](#)
- [Custom CMS User Role Permissions](#)
- [How to delete a CMS user](#)