

# Multi Factor Authentication

[See previous W5 version guide](#)

## **PURPOSE**

This document shows the steps on how to activate and deactivate multi factor authentication for the CS Lucas system.

## **WHY IS THIS IMPORTANT?**

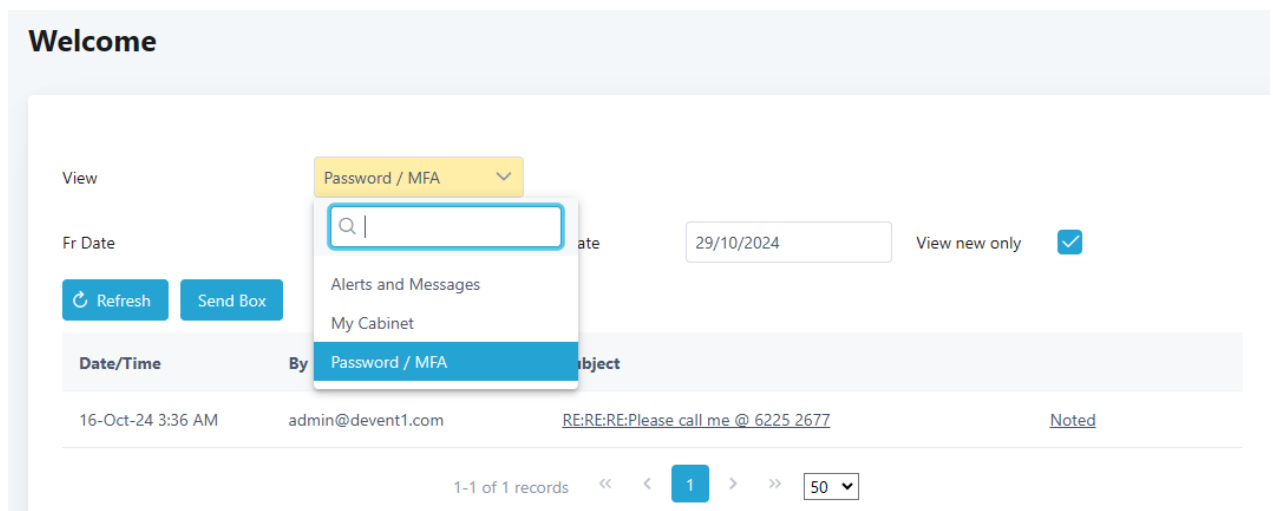
This is important as MFA is a security tool to verify the user's identity and ensures only those authorized are the only ones to access the system.

## **PROCEDURE**

### I. Activate MFA for Android devices

Pre-requisite: You'll require permission rights "10354 Activate MFA" to activate multi factor authentication. If you do not have permission, please contact your administrator.

1. From the Welcome menu, click on the dropdown in View field. Choose Password / MFA.



2. The Welcome – Password / MFA screen will be displayed.

## Welcome

View

Password / MFA



User ID

admin@devent1.com

Password expires in (days)

65

MFA Active

No

Change

Manage MFA

New Password

Rekey new password

Current Password

3. Click Manage MFA.

4. The Manage MFA screen is displayed. Please download and install Google Authenticator on your mobile device. For more details on setting up the app, [click here](#).

## Manage MFA

admin@devent1.com

✕ Cancel

⚙️ Configure

You need to install a Multi-Factor Authentication (MFA) app on your mobile device before continuing.

Launch the app, click on the Configure button above.

5. Click Configure.
6. The screen with instructions on activating MFA will display.


## Manage MFA

admin@devent1.com

✕ Cancel

⚙️ Activate

Step 1: Scan the QR image with your device.



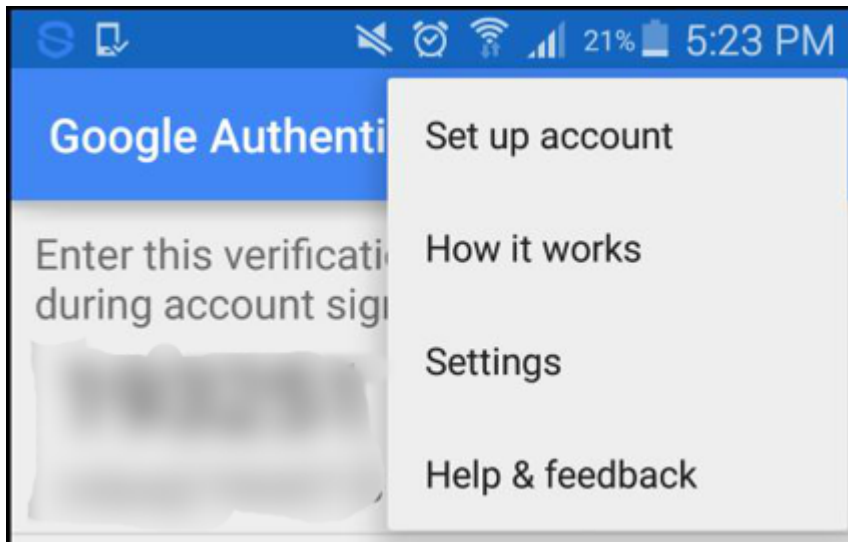
Alternatively, type the configuration key in you MFA app.

Y7FWKK5QMFJGOXKE

Step 2: Enter the next two consecutive code from the MFA device.

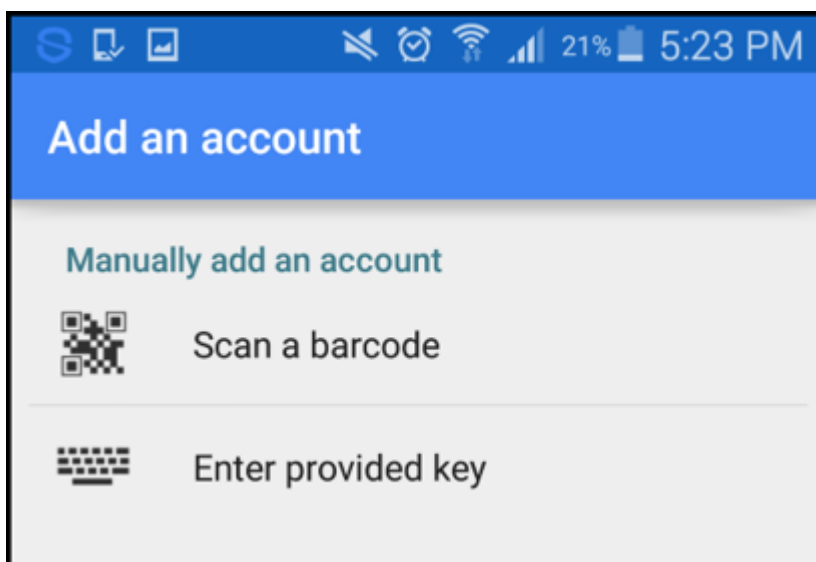
Step 3: Click Activate button above.

7. On your mobile device, open the Google Authentication application.
8. To add a new account, choose Set Up Account from the app's menu.



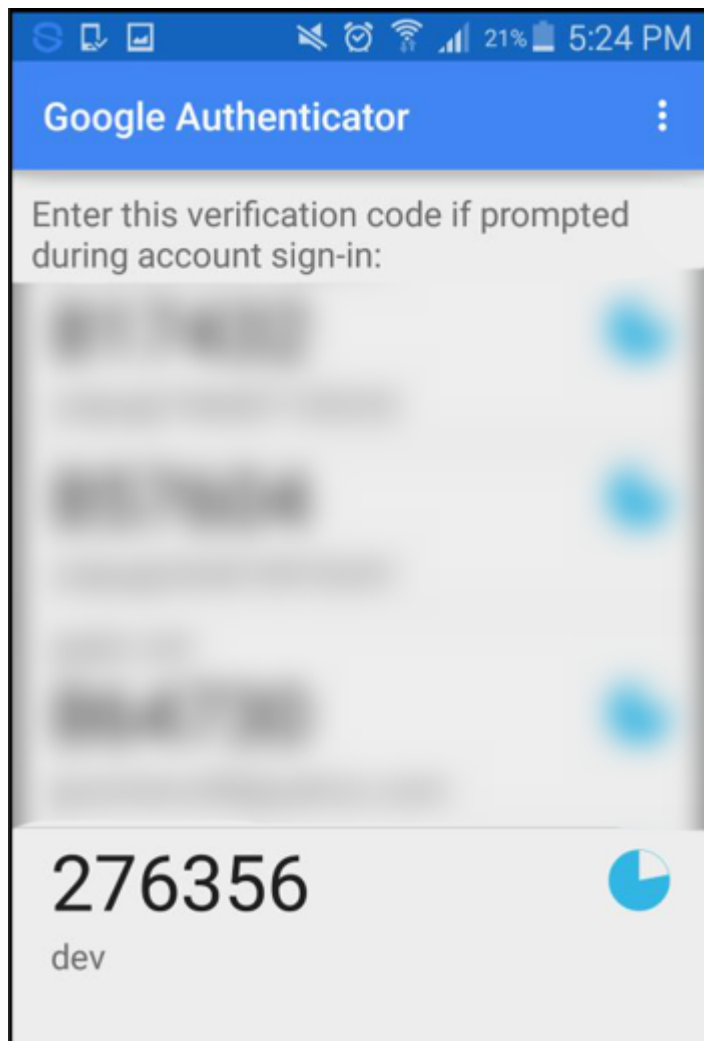
9. To link your mobile device to your CS Lucas account:

- Using QR code: Select Scan a barcode and then point your camera at the QR code on your computer.
- Manual Entry: Select Enter provided key and then enter the user id of your CS Lucas account in the “Enter account name” field. Next, enter the configuration key on your computer screen in the “Enter your key” field. Make sure to make the key Time Based and select Add.

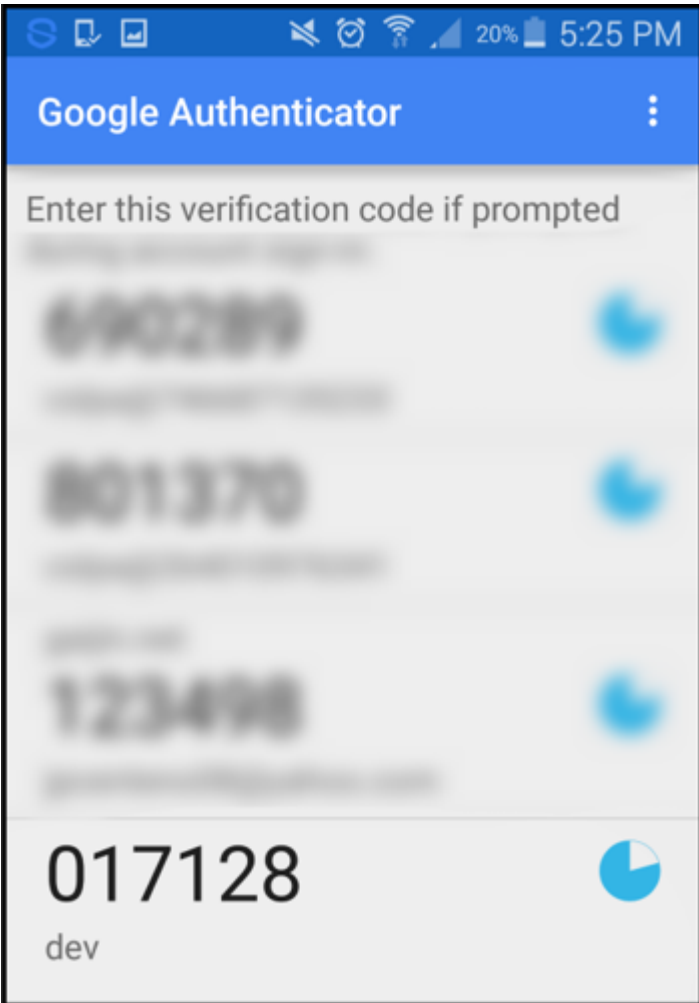


10. Next, enter the 6 digits code generated from the device on your computer screen. Enter the code in the first box. Wait for the authenticator to refresh with a new code, enter the code in the second box. Note that 2 codes must be entered consecutively. See screenshots below.

1st code:



2nd code:



## Manage MFA

admin@devent1.com

✕ Cancel

⚙️ Activate

Step 1: Scan the QR image with your device.



Alternatively, type the configuration key in you MFA app.

Y7FWKK5QMFJGOXKE

Step 2: Enter the next two consecutive code from the MFA device.

276356

017128

Step 3: Click Activate button above.

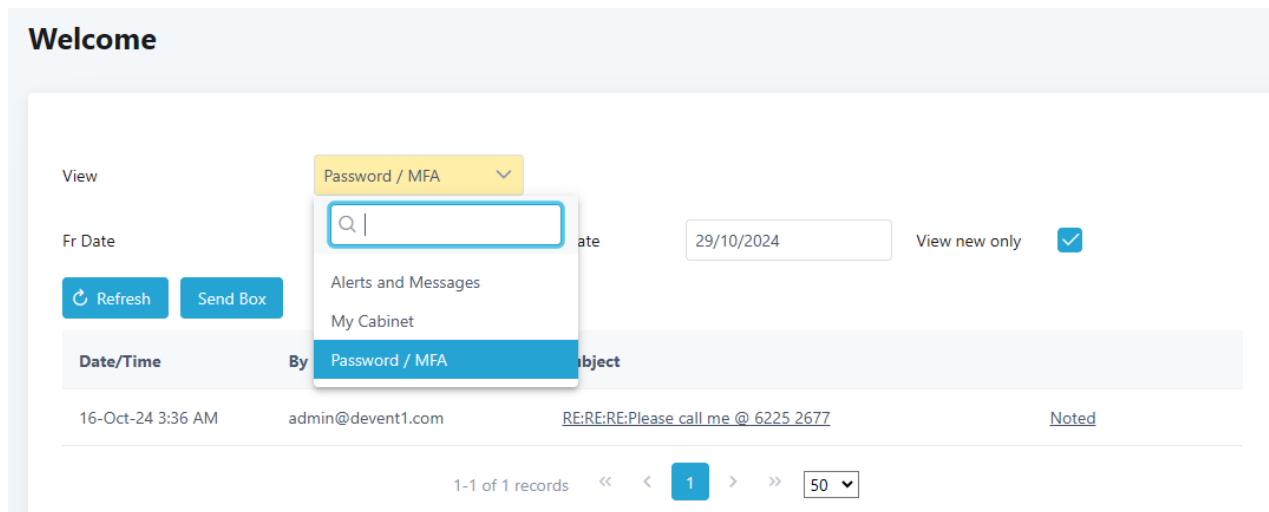
11. Click Activate. If your code is correct, you will see activation successful message. If your code is incorrect, please try generating new verification codes from your mobile devices.

12. Approve the user once MFA is successfully activated.

## II. Activate MFA for iPhone

Pre-requisite: You'll require permission rights "10354 Activate MFA" to activate multi factor authentication. If you do not have permission, please contact your administrator.

1. From the Welcome menu, click on the dropdown in View field. Choose Password / MFA.



2. The Welcome – Password / MFA screen will be displayed.

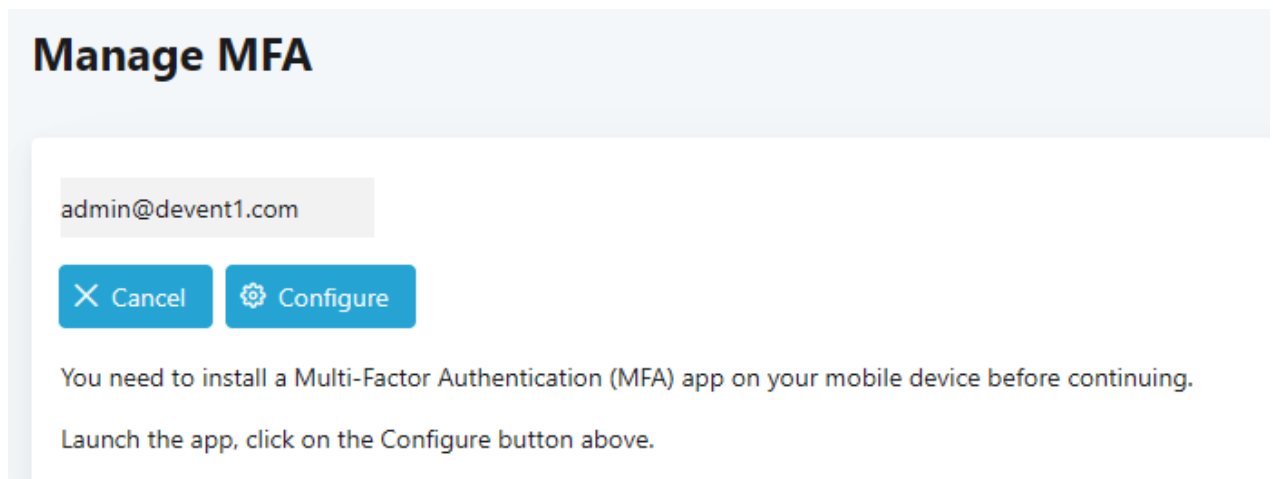
The screenshot shows the 'Welcome' screen with a 'Manage MFA' section. It includes a 'View' dropdown set to 'Password / MFA'. Below this, the 'User ID' is 'admin@devent1.com'. The 'Password expires in (days)' is '65'. The 'MFA Active' status is 'No'. There are two buttons: 'Change' and 'Manage MFA'. Below these are three input fields: 'New Password', 'Rekey new password', and 'Current Password'.

3. Click Manage MFA.

4. The Manage MFA screen is displayed. Please download and install Google



Authenticator on your mobile device. For more details on setting up the app, [click here](#).



5. Click Configure.

6. The screen with instructions on activating MFA will display.

## Manage MFA

admin@devent1.com

✕ Cancel

⚙️ Activate

Step 1: Scan the QR image with your device.



Alternatively, type the configuration key in you MFA app.

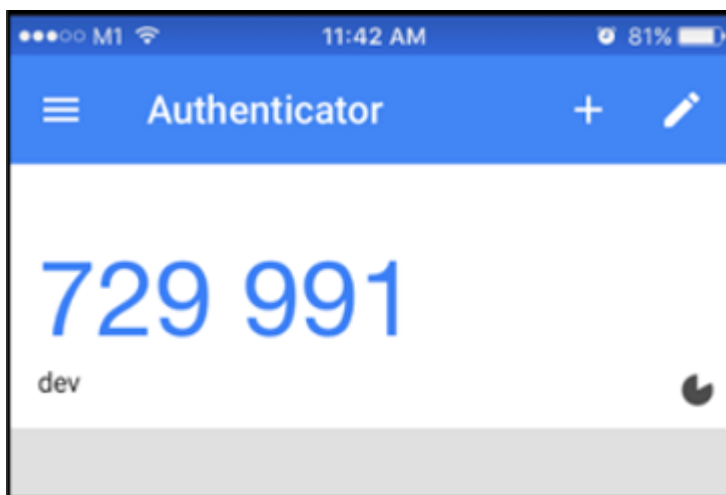
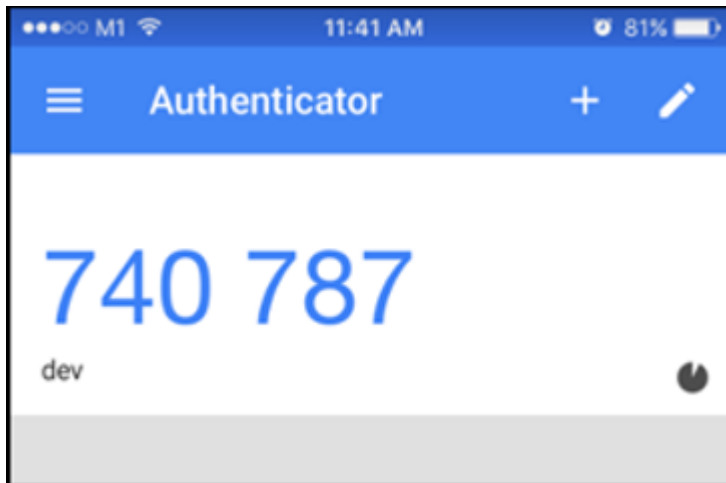
NBQUIP5RDTXAWDS4

Step 2: Enter the next two consecutive code from the MFA device.

Step 3: Click Activate button above.

7. On your mobile device, open the Google Authentication application.
8. If this is the first time you use Google Authenticator, tap on Begin Setup. To add a new account, tap on the plus icon.
9. To link your mobile device to your CS Lucas:
  - Using QR code: Select Scan barcode and then point your camera at the QR code on your computer.
  - Manual Entry: Select Manual entry and then enter the user id of your CS Lucas account in the “Account” field. Next, enter the configuration key on your computer screen in the “Key” field. Make sure to make the key is switched to Time Based and tap Done.

10. Next, enter the 6 digits code generated from the device on your computer screen. Enter the first code in the first box. Wait for the authenticator to refresh with a new code, enter the second code in the second box. Note that the 2 codes must be entered consecutively. See screenshots below.



## Manage MFA

admin@devent1.com

✕ Cancel

⚙️ Activate

Step 1: Scan the QR image with your device.



Alternatively, type the configuration key in you MFA app.

NBQUIP5RDTXAWDS4

Step 2: Enter the next two consecutive code from the MFA device.

740787

729991

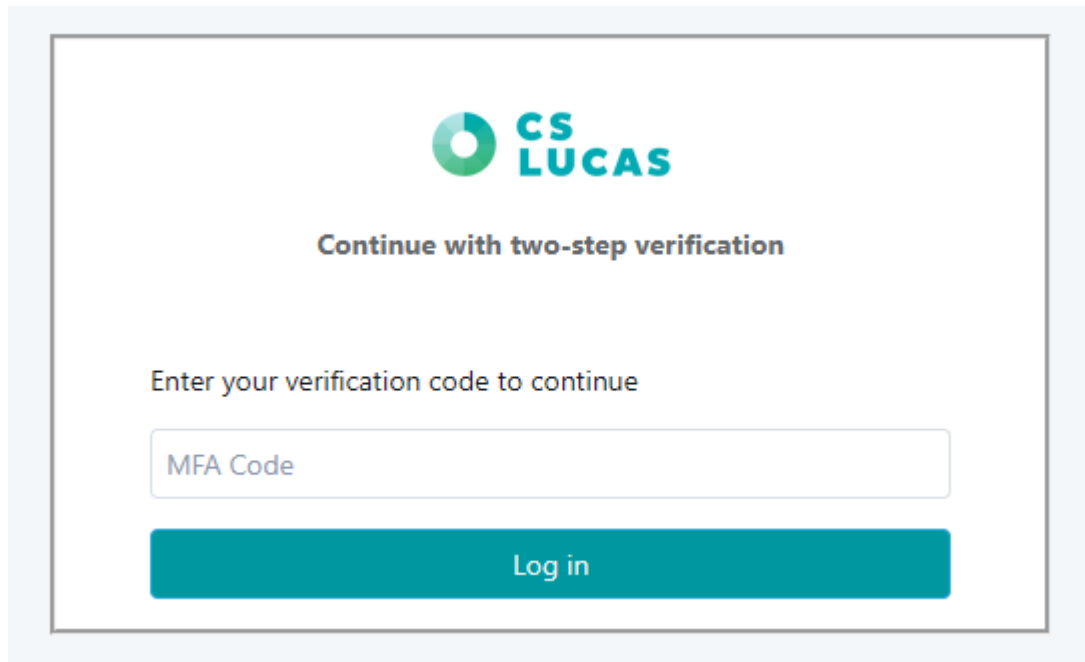
Step 3: Click Activate button above.

11. Click Activate. If your code is correct, you will see activation successful message. If your code is incorrect, please try generating new verification codes from your mobile devices.

12. Approve the user once MFA is successfully activated.

### III. Login with MFA

1. On the login page, sign in with user ID and password. Click Sign In.
2. The system asks for the MFA code.



**CS LUCAS**

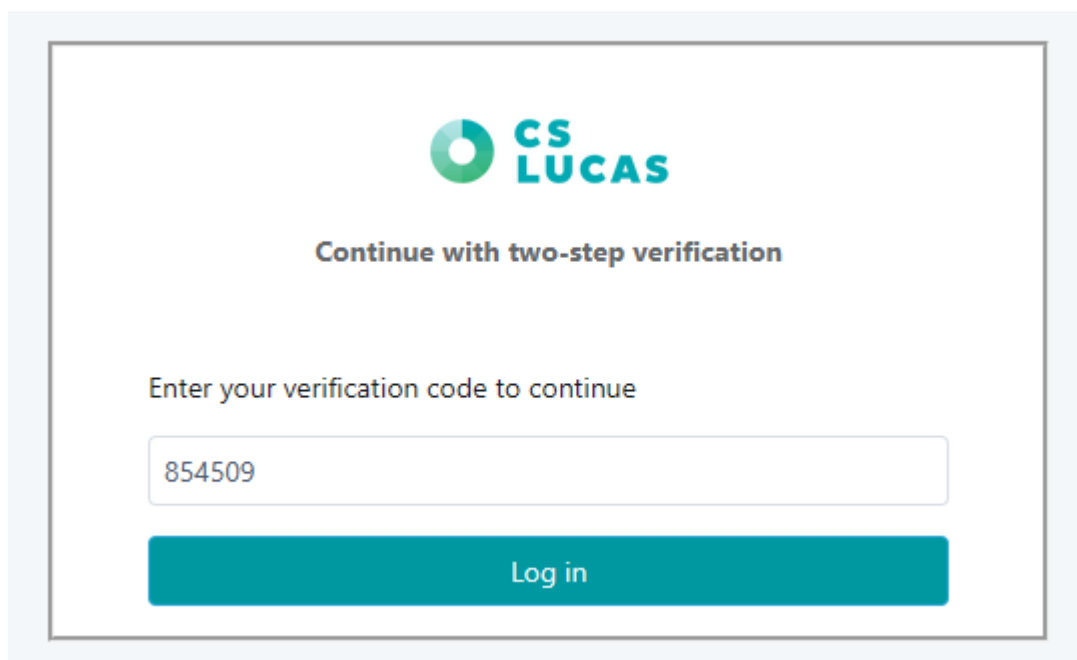
**Continue with two-step verification**

Enter your verification code to continue

MFA Code

Log in

3. Get the code generated by Google Authenticator and enter in the system.



**CS LUCAS**

**Continue with two-step verification**

Enter your verification code to continue

854509

Log in

4. Click Submit.

5. If the code is correct, you will be successfully login to the system. If the code is incorrect, please try generating a new code from your device again.

#### IV. Deactivate MFA

Pre-requisite: You'll require permission rights "10355 Deactivate MFA" to deactivate multi factor authentication. If you do not have permission, please contact your administrator.

1. To deactivate MFA, select Set Up > User and Rights.
2. Click on the User ID to deactivate MFA.
3. The Amend User screen displays.

**Amend User**

✕ Cancel

💾 Save

📄 Duplicate

🔑 Reset Password

👤 Assign Group

⚙️ Preference

⚙️ Deactivate MFA

≡ History

📁 File/Note

User ID\*

admin@devent1.com

Language

English (Default) ▾

Valid To\*

31/12/2099

Activation

Y

Full Name

admin

Email\*

admin@devent1.com

Department

- ▾

No IP Restriction

☒

+ Upload Profile Photo

Your password\*

4. Click Deactivate MFA. A pop-up window will appear to confirm that you want to deactivate MFA. Click Yes.

## Amend User

Cancel
Save
Duplicate
Reset Password
Assign Group
Preference
Deactivate MFA
History
File/Note

User ID\*  
admin@devent1.com

Language  
English (Default)

Valid To\*  
31/12/2099

Activation  
Y

Full Name  
admin

Email\*  
admin@devent1.com

Department  
-

No IP Restriction ☒

+ Upload Profile Photo

Your password\*

### Confirmation

⚠ Are you sure you want to deactivate MFA for this user?

✓ Yes
✗ No

5. This will deactivate the MFA and the next login will no longer require MFA.

Note: Deactivate MFA rights should be assigned to user administrator only so that he/she can deactivate for all users.

Deactivating a user’s MFA does not require approval after the deactivation.

## FREQUENTLY ASKED QUESTIONS

## RELATED INFORMATION

[Security Recommendations for CS Lucas](#)

## CHANGE HISTORY

Date	By	Changes
31-Aug-2016	Clarissa	Created.
27-Nov-2019	Lyra	Updated screenshots.
29-Oct-2024	T5	Updated to W6 instructions and screenshots.