



## HOW TO SET UP TWO-FACTOR AUTHENTICATION

Multi-factor Authentication (MFA) is an authentication method that requires you to provide two or more verification factors to gain access to a resource such as an application or online account. It helps protect your account as well as the content within SmartRoom by requiring you to identify yourself by more than a username and password.

When logging into a SmartRoom with multi-factor authentication enabled, users will be prompted by the dialog box below to set up two-factor authentication.

- 1) Click the “SET UP TWO-FACTOR AUTHENTICATION” blue button to initiate the process




 Two-factor authentication is required to access this room.

You can setup two-factor authentication via your account settings by clicking the link below.

Once configured you will need to re-login to SmartRoom for the change to take effect.

If you need help please contact our [Customer Support](#)

 SET UP TWO-FACTOR AUTHENTICATION

 SELECT ANOTHER ROOM

 LOGOUT

- 2) On the “Two-Factor Authentication” tab click on the +Add TOTP button




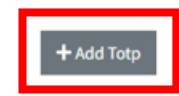
 SmartRoom  CreditorInfo  SmartExchange

 Profile

 Two Factor Authentication

 Change Password

 Your account does not have any two factor authentication provider configured.

 + Add Totp

### 3) Follow the instructions on the screen



#### Step 1: Get the App

Download and install the [Google Authenticator](#), [Duo Mobile](#), or [Windows Phone Authenticator](#) app for your phone or tablet.



#### Step 2: Scan this Barcode

Open the authentication app and:

- Tap the “+” icon in the top right of the app
- Scan this image to the left, using your phone’s camera



#### Step 3: Save changes!

Ensure you save your 2FA configuration. You’ll be required to enter a code created by the authentication app next time you sign into your SmartIdentity account.

Enter your current password.

Then enter a code created by the authentication app below and save your TOTP configuration.

Password

PIN Code

#### What is TOTP?

A **Time-based One-Time Password (TOTP)** application automatically generates an authentication code that changes after a certain period of time. We strongly recommend using a TOTP application to configure Two Factor Authentication (2FA). TOTP applications are more reliable than SMS, especially for locations outside the US.

**Tip:** To configure authentication via TOTP on multiple devices, during setup, scan the QR code using each device at the same time. If 2FA is already enabled and you want to add another device, you must re-configure 2FA from your user profile.

#### Step 1: Get the App

Download and install the Google Authenticator, Duo Mobile or Windows Phone Authenticator app for your phone or tablet.

#### Step 2: Scan the Barcode on the screen

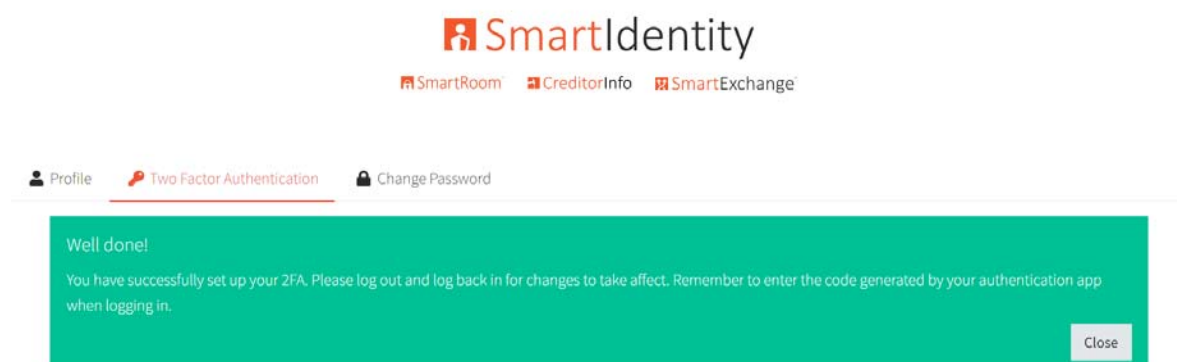
Open the authentication app and follow the app’s instructions. The app will ask you to scan the barcode on screen using your phone’s camera. For the Google Authenticator app, tap the “+” icon and then “Scan a QR code”.

#### Step 3: Save changes!

Ensure you save your two-factor configuration. You will be required to enter a code created by the authentication app next time you sign into your account.

**Step 4:** Enter the code (without spaces) created by the authentication app to the **Pin Code** field.

**Step 5:** Enter your SmartRoom password to the **Password** field, then click on **Continue**



**Step 6:** When you go back to the SmartRoom page, logout and then log back in using your credentials. This time you will be prompted to enter the code by your authenticator app.

Authenticator code

**ENTER THE CODE WITHOUT SPACES**

**LOG IN**

### Troubleshooting Tips for Google Authenticator:

If you are not able to pair Google Authenticator with SmartIdentity despite providing the correct code, please check your phone's time and make sure it's set to auto. Google authenticator will not work when the time is not correctly synced.

Below are the steps to set the correct time.

#### My Google Authenticator codes don't work

It may be because the time isn't correctly synced on your Google Authenticator app.

To set the correct time:

1. On your Android device, go to the main menu of the Google Authenticator app.
2. Tap More : > **Settings** > **Time correction for codes** > **Sync now**.

On the next screen, the app confirms the time has been synced. You should be able to sign in. The sync will only affect the internal time of your Google Authenticator app, and will not change your device's Date & Time settings.

#### FOR ASSISTANCE:

**EMAIL:** [SMARTROOMSUPPORT@SMARTROOM.COM](mailto:SMARTROOMSUPPORT@SMARTROOM.COM)

**CALL:** NORTH AMERICA +1.877.332.5739  
ASIA: +852.800.930.643

EUROPE: 00.800.3325.7666  
JAPAN: 0120.974.858

INDIA: 000.800.100.8914