

Getting Started

Safetrust Quickstart

- 01 — About this guide
- 02 — Pre set-up checklist
- 03 — Creating an Identity System
- 04 — Creating People & Assigning Credentials
- 05 — Configuring a New Sensor
- 06 — Getting Access

About this guide

01

This guide is designed to assist with the configuration of your ELATEC TWN4 Series Readers (any reader with BLE, especially MultiTech 2, Front reader and Slim) for use with Safetrust virtual credentials.

These instructions will step you through the setup of an Identity System within the Safetrust Credential Manager platform, as well as the creation of people and credentials, which are required prior to configuring your ELATEC reader.

If you require assistance at any point during the setup process, please contact your local ELATEC sales representative.

Pre set-up checklist

02

- You have an account for the Safetrust Credential Manager Platform
- You have the appropriate role-based access for completing operational tasks
- Your account has a valid license

Login to Credential Manager to verify your account, access role, and license info.

If you require assistance in setting up your initial customer account, please don't hesitate to contact your local sales representative.

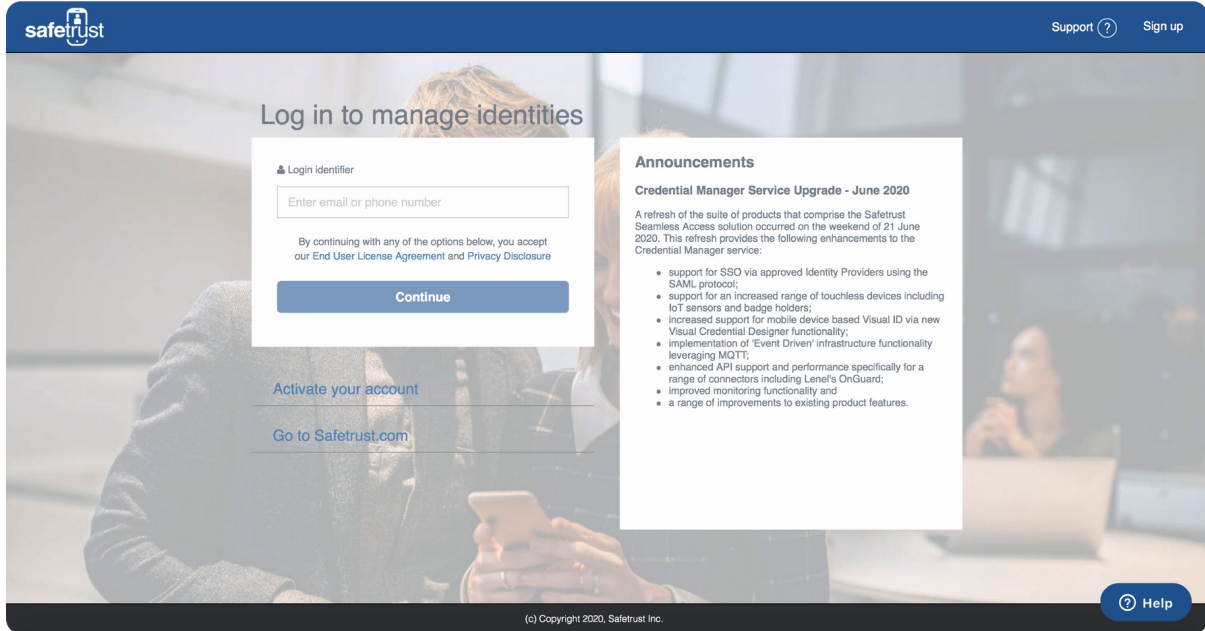


Creating an Identity System

Step 1:

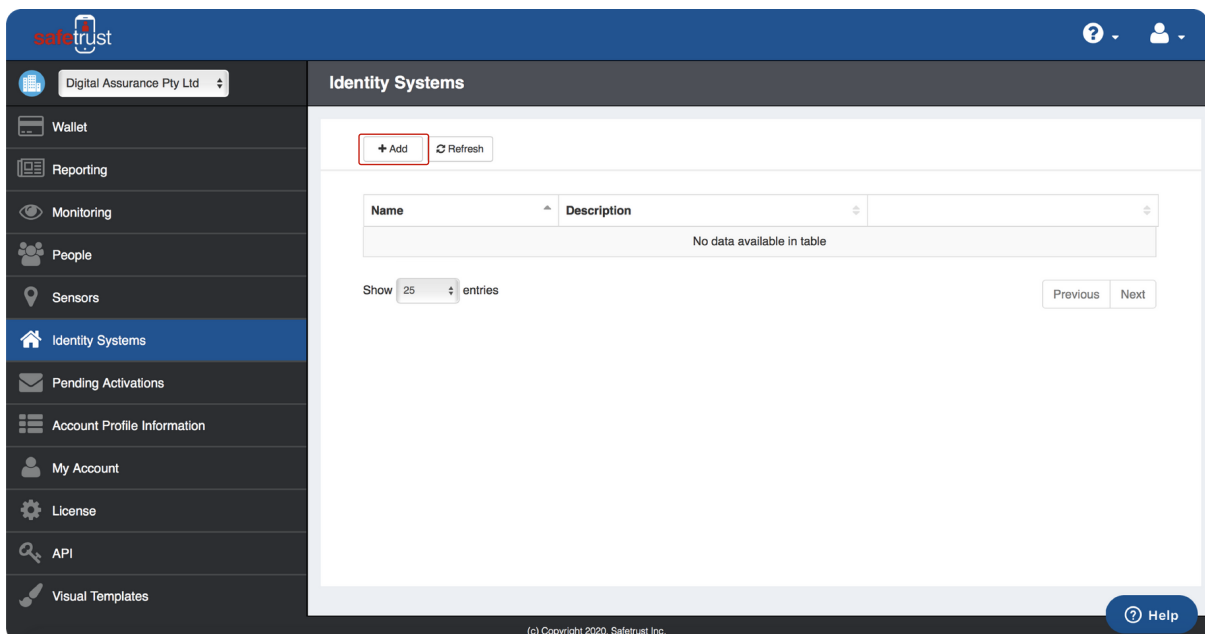
Access the Safetrust Credential Manager platform via <http://www.safetrust.com> by clicking **Log In** from the right hand side of the navigation.

When the portal is open, use the email or phone number you created your account with to logon.



Step 2:

From the navigation panel on the left, select **Identity Systems** and click **Add** to create a new system.



Step 3:

You must complete the fields for **Identity System Type**, **Identity system name**, **Description**, **Activation Distance** and **Guest credential use time** before proceeding. When complete, click the green **Next** button to continue.

The screenshot shows the 'Third Party Wallet' configuration page in the Safetrust interface. The progress bar at the top indicates that steps 1 through 6 are completed, and step 7, 'Third Party Wallet', is the current step. The form contains the following fields and options:

- Identity System Type***: Building System
- Identity system name***: Enter identity system name
- Description***: Enter description
- Allow virtual wallet**:
- Contact information**:
 - Primary contact**: Craig Parker | Working hours: Mon,Tue,Wed,Thu,Fri 07:00 am - 05:00 pm (with a 'Select' button)
 - Secondary contact**: (with a 'Select' button)
 - Provide access key**: (with a 'Select' button)
- Defaults**:
 - Activation distance**: 5'0" (150 cm)
 - Guest credential use time***: 8 hours
 - Delete expired credential after**: (with a 'days' dropdown)
 - Include Relay/Lock**: 1s 3s Toggle None

At the bottom right, there are buttons for 'Next' (green), 'Save' (orange), 'Cancel' (grey), and 'Help' (blue with a question mark icon). The footer text reads '(c) Copyright 2020, Safetrust Inc.'

Step 4:

Under the **Credential type** dropdown, select your preferred credential type. You are also required to specify the **Credential format**, a **Facility** code, and a **Credential range** for future credentials you assign. You can also choose a **Credential number allocation** from either Sequential, Random or Manual depending on your requirements.

The screenshot shows the 'Credential System' configuration page in the Safetrust interface. The progress bar at the top indicates that all steps from 1 to 7 are completed. The form contains the following fields and options:

- Credential type***: HID Global Prox
- Credential format***: HID Prox 26-bit H10301
- Facility**: 0-255
- Credential range***: 0 to 65535 (with an 'Add' button)
- Credential number allocation***: Sequential
- Credential Access PIN**: On Off

At the top right, there are buttons for 'Save' (blue), 'Cancel' (orange), and a refresh icon (grey). At the bottom right, there is a 'Help' button (blue with a question mark icon). The footer text reads '(c) Copyright 2020, Safetrust Inc.'

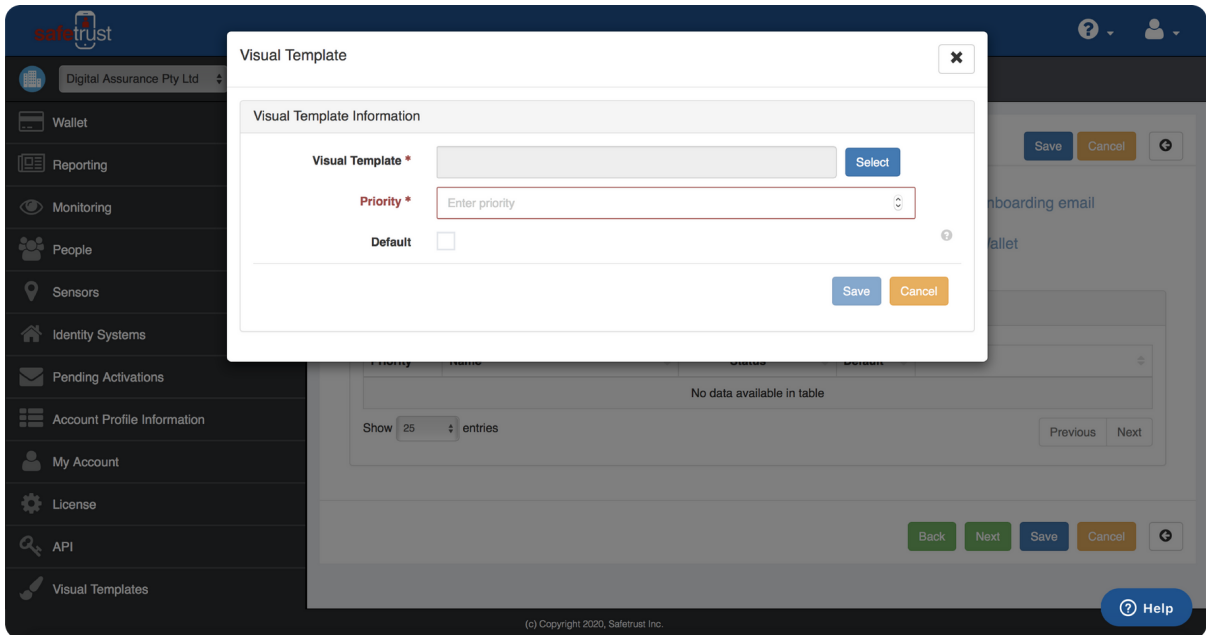


Step 5: Optional

Visual Template: Select a visual template for your credential images from the drop down.

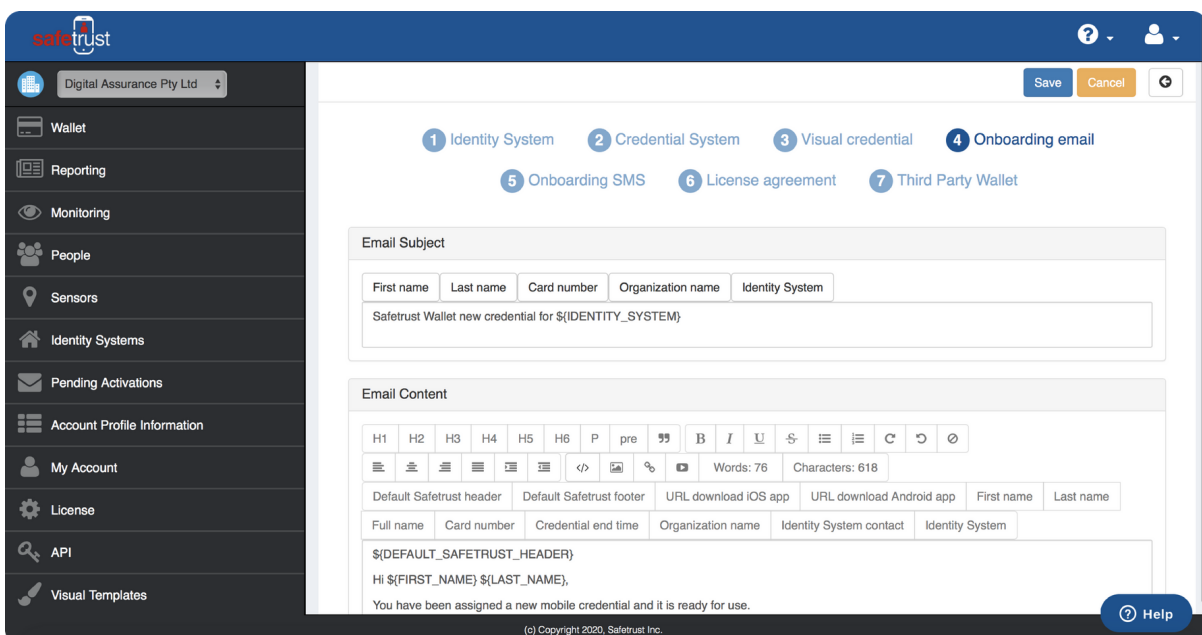
Priority: Numerical value of sequence (enter **1** if you want this template to be first).

Default: Check this box if you want this template to be chosen upon creation of a credential.



Step 6:

Customize your welcome email for new people in your organization and click **Next** to continue. If you do not wish to onboard people via SMS, you do not have additional License agreements for your users, and you are not using a Third Party Wallet, you can click **Save** to skip steps 7-9 and finalise your new Identity System.



Step 7: Optional

Customize your welcome SMS for new people in your organization and click **Next** to continue.

The screenshot shows the Safetrust web interface for configuring the Onboarding SMS. The left sidebar contains navigation options: Wallet, Reporting, Monitoring, People, Sensors, Identity Systems, Pending Activations, Account Profile Information, My Account, License, API, and Visual Templates. The main content area has a progress bar with seven steps: 1 Identity System, 2 Credential System, 3 Visual credential, 4 Onboarding email, 5 Onboarding SMS (highlighted), 6 License agreement, and 7 Third Party Wallet. Below the progress bar is a text editor for the SMS message. The message content is: "Your Safetrust Wallet account has been assigned a new credential to Identity System: \${IDENTITY_SYSTEM}". The text editor includes a toolbar with various formatting options and a table with columns: First name, Last name, Full name, Card number, Credential end time, Organization name, Identity System contact, and Identity System. At the bottom of the editor are buttons for Back, Next, Save, Cancel, and a Help icon. The footer of the interface reads "(c) Copyright 2020, Safetrust Inc."

Step 8: Optional

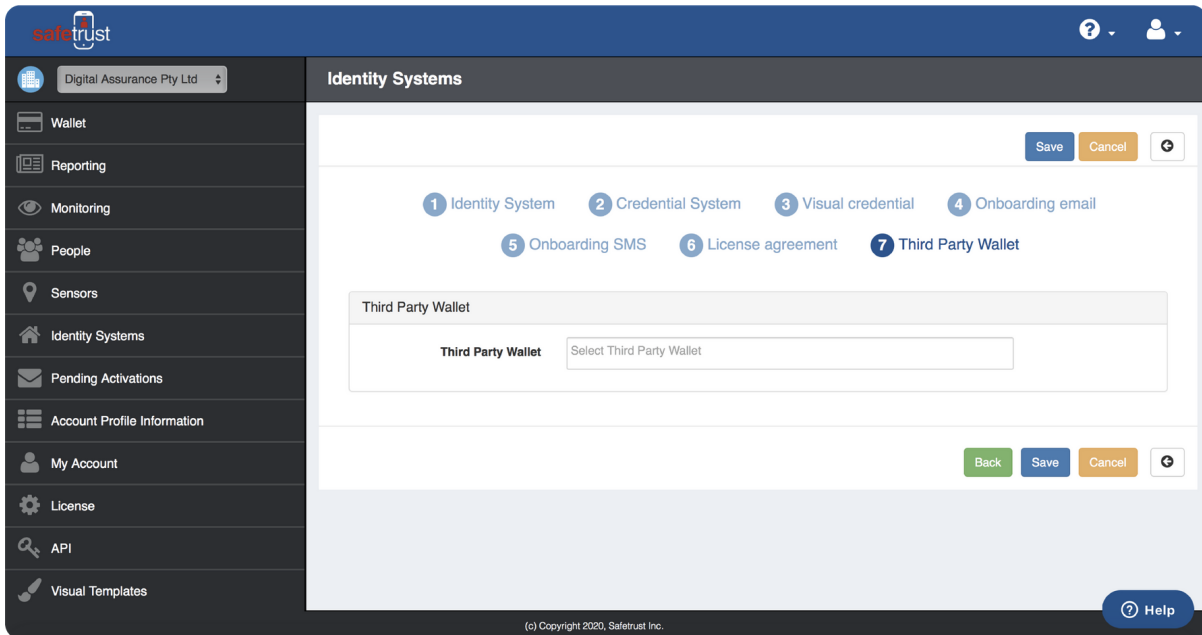
If you have an additional licencing agreement you wish for your users to agree to, please add it in this step.

The screenshot shows the Safetrust web interface for configuring the License Agreement. The left sidebar is the same as in Step 7. The main content area has a progress bar with seven steps: 1 Identity System, 2 Credential System, 3 Visual credential, 4 Onboarding email, 5 Onboarding SMS, 6 License agreement (highlighted), and 7 Third Party Wallet. Below the progress bar is the "License Agreement" configuration form. It includes an "Enable" checkbox, a "Required reapproval" checkbox, and a "Type" dropdown menu labeled "Select license type". Below these is a rich text editor with a toolbar and a table with columns: Full name, Card number, Credential end time, Organization name, Identity System contact, and Identity System. At the bottom of the editor are buttons for Back, Next, Save, Cancel, and a Help icon. The footer of the interface reads "(c) Copyright 2020, Safetrust Inc."



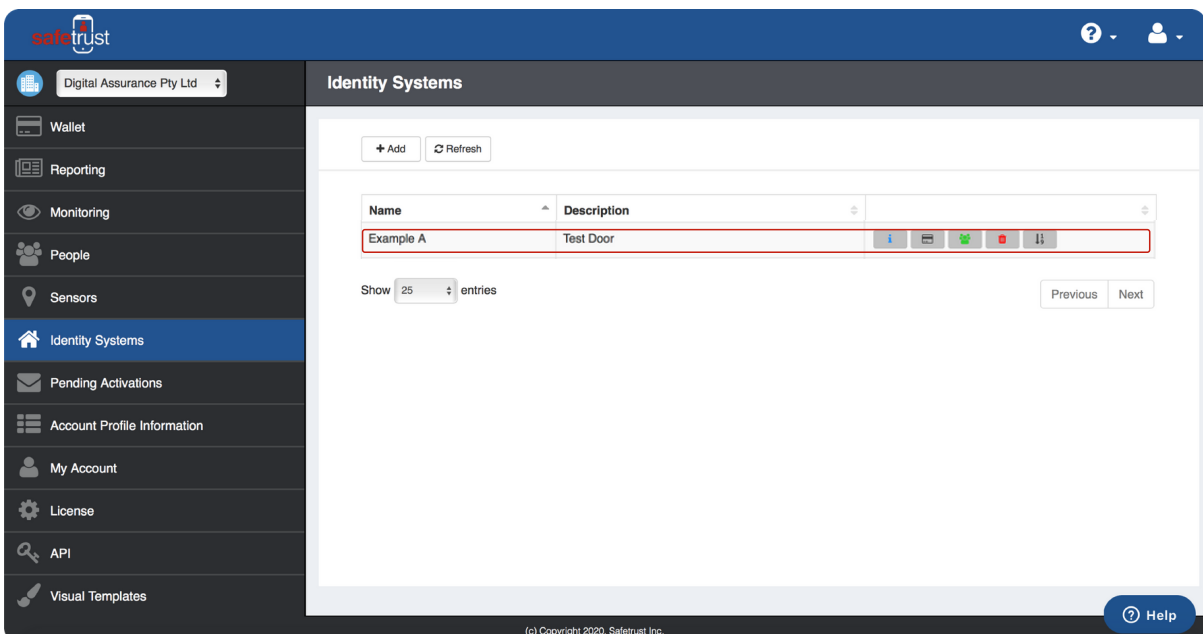
Step 9: Optional

If you are using a Third-Party Wallet with the Safetrust SDK, please specify here.



Complete!

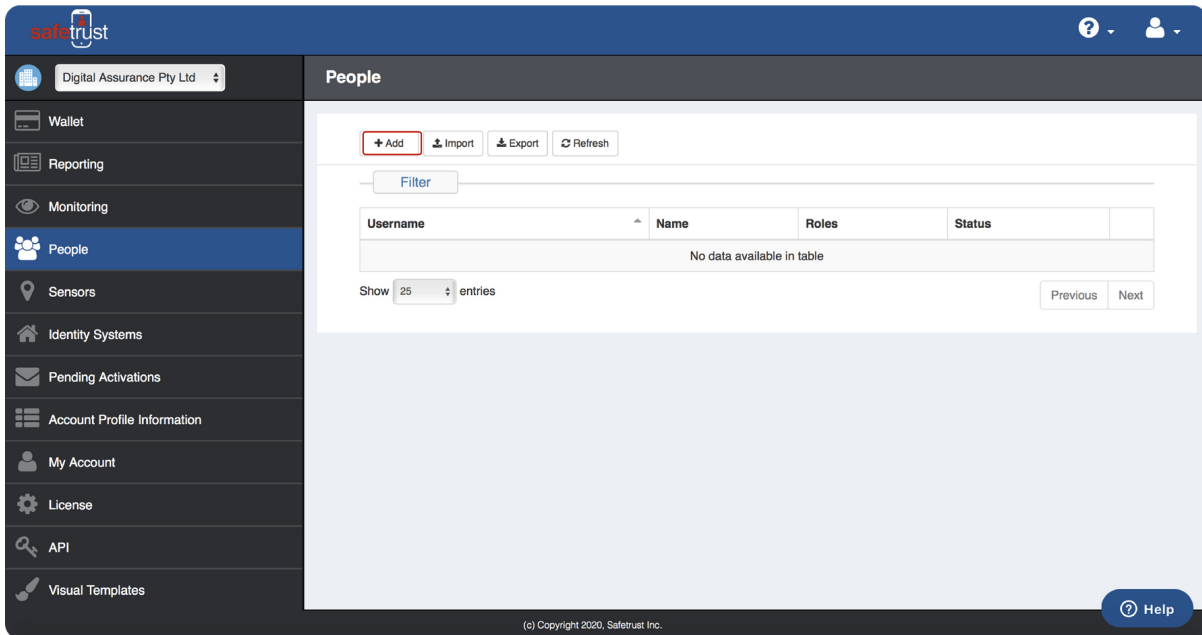
Once you click **Save**, you should see your new Identity System listed in the main tab. You are now ready to create people and assign credentials for this Identity System.



Creating People & Assigning Credentials

Step 1:

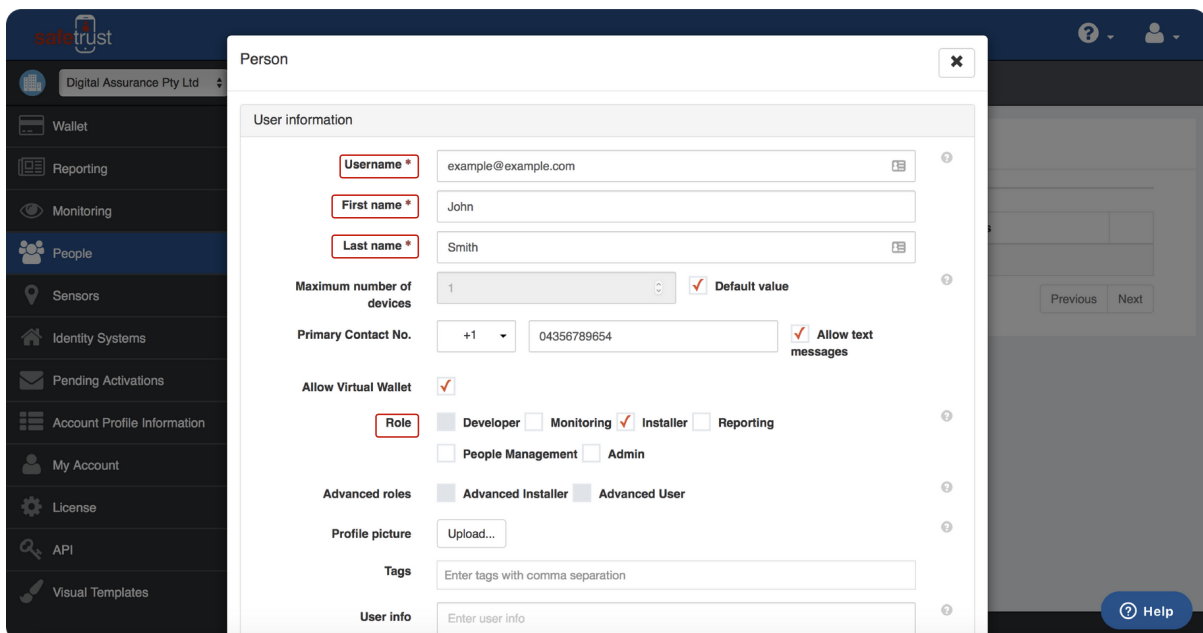
Return to the left navigation panel and select the 'People' tab. Click **Add** to create one person at a time or click **Import** to register bulk users via the CSV file format specified.



Step 2:

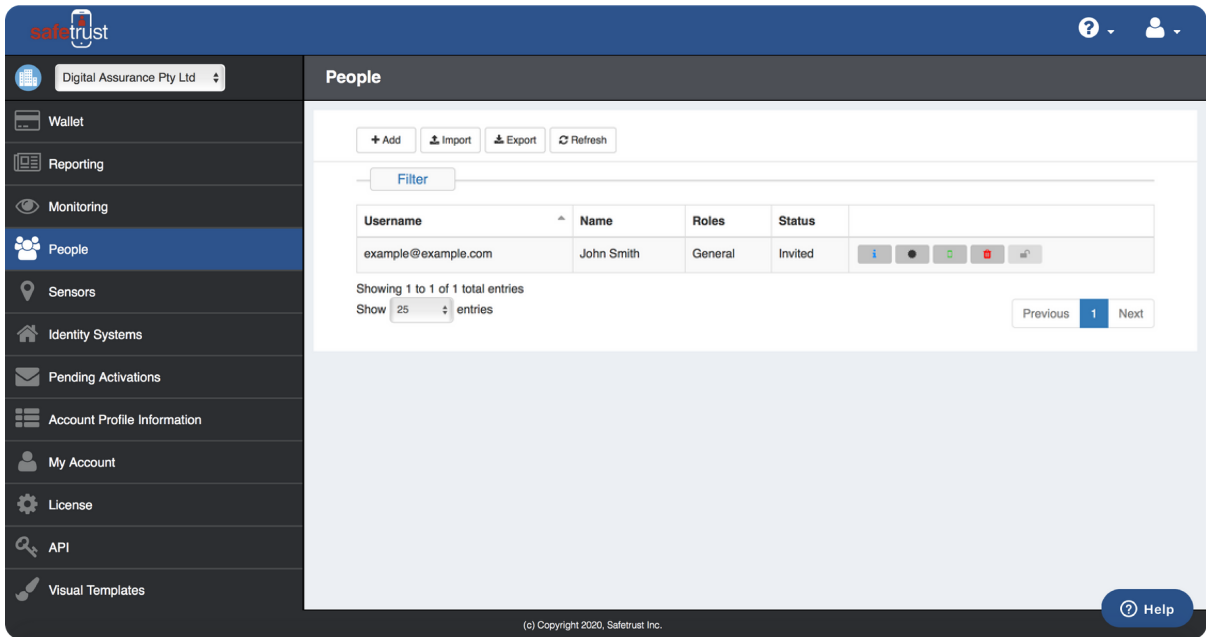
Enter a **Username** (email or mobile number), **First name**, and **Last name** for the person and click **Save** to complete.

Note: While it is not a mandatory field, you can also assign a **Role** from the options available. A person will require an **Installer** role or higher in order to configure readers.



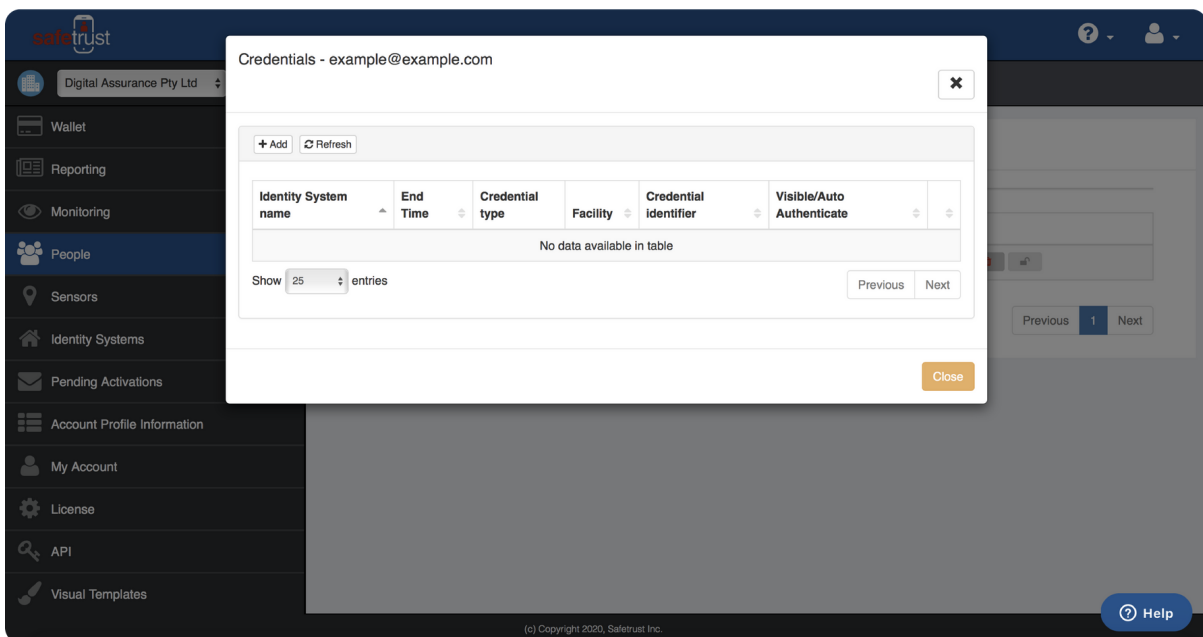
Step 3:

When a new person is created they will show as an entry on the main tab. To see a person's active credentials, or to add a new credential, click the  icon.



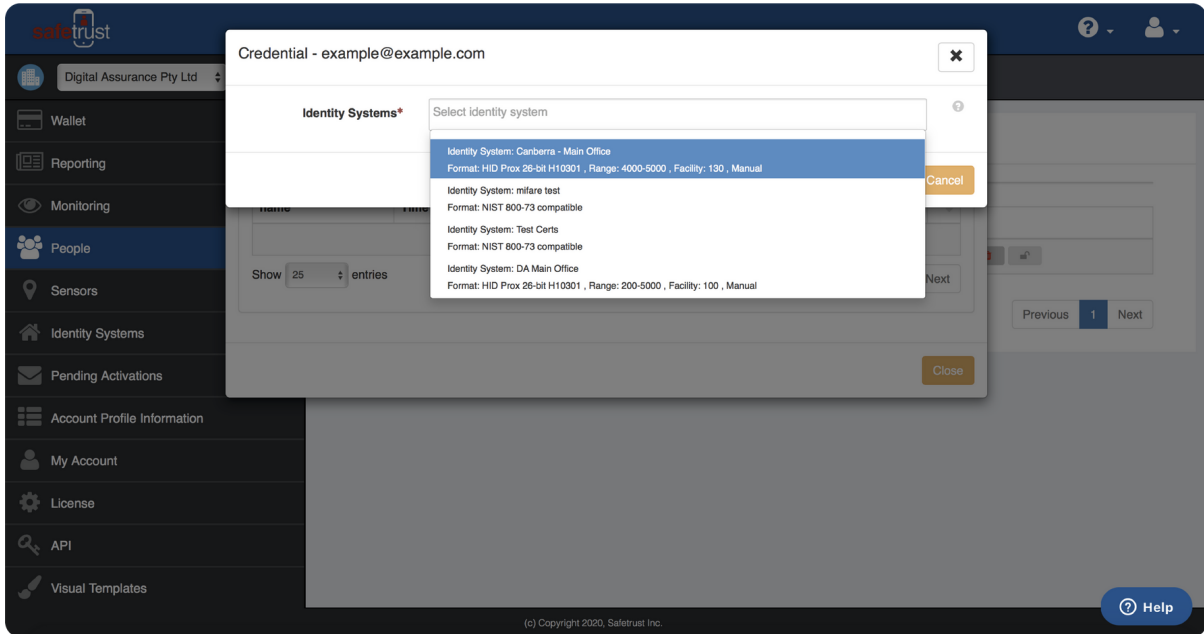
Step 4:

Click the **Add** button.



Step 5:

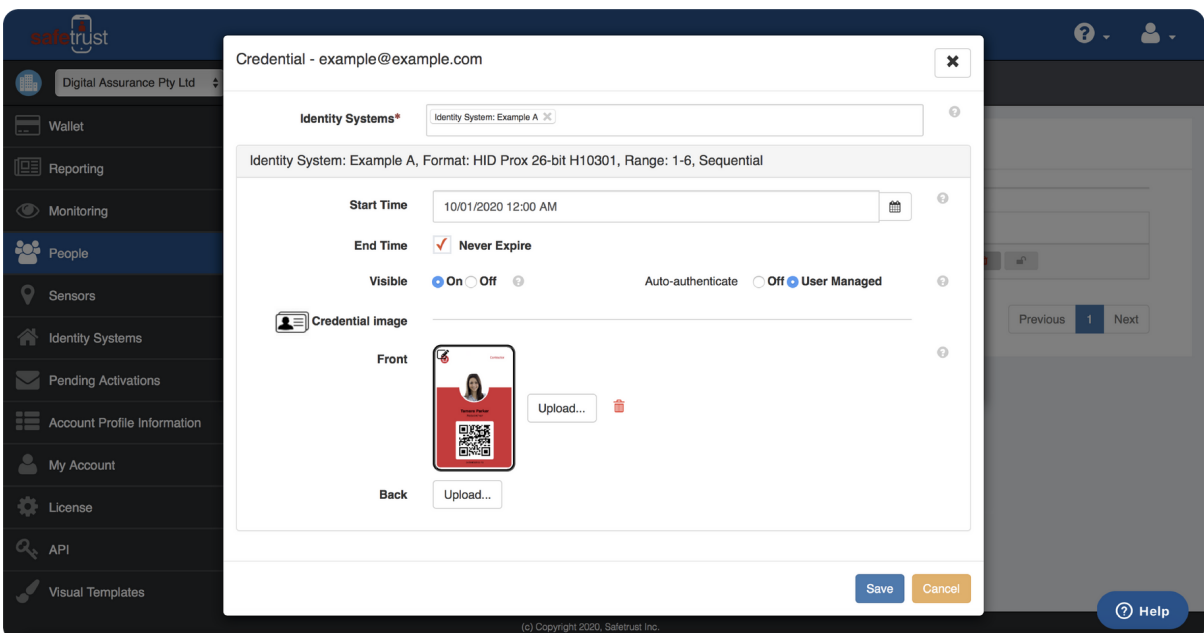
Select the Identity System you just created from the dropdown. If you have multiple identity systems created (like shown on this screen) you may need to scroll.



Step 6:

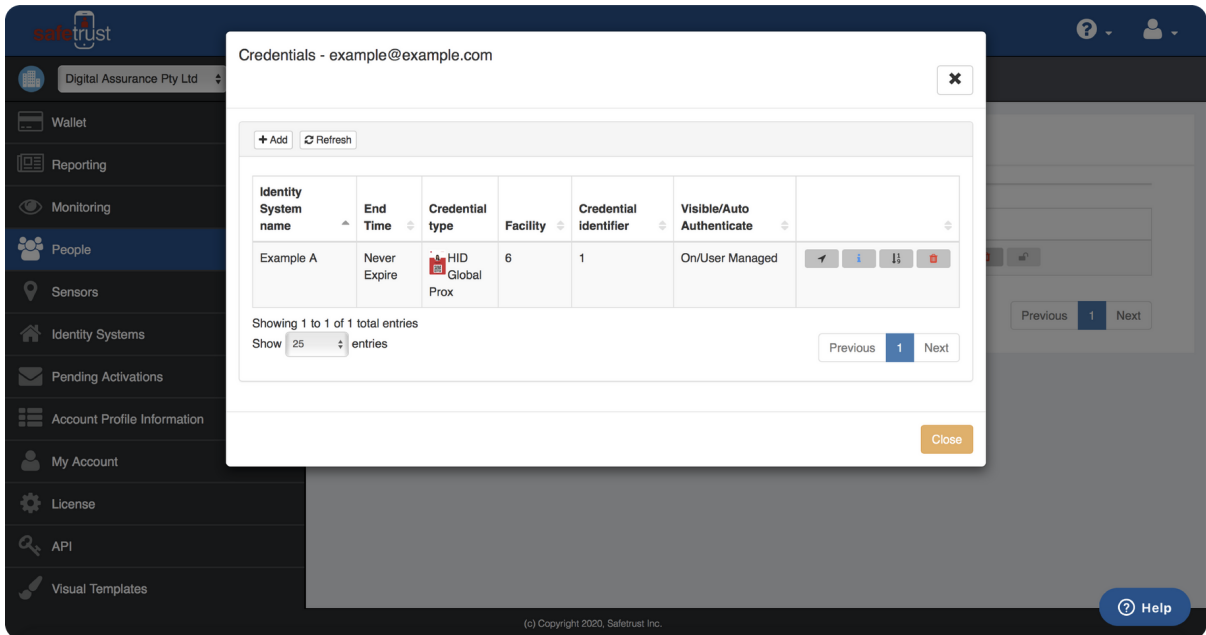
Set a **Start Time** and **End Time** for the credential. You can also upload personalized credential images for each person using the **Upload** buttons which will appear if you have not already assigned a Visual Template to the Identity System. Click **Save** to finish.

Note: The credential will automatically be set to **Never Expire**. You will need to un-check this box to specify an end time.



Step 7:

Your new credential will be sent to this person and will show under their account like the screen below. Check that all the information is entered correctly and click the **Close** button to exit the dialogue box.



Complete!

Once the identity system, users and credentials have been setup, the next step is to download the Safetrust Wallet App via the App Store (for iOS devices) or Google Play (for Android devices).

After downloading, follow the prompts on your onboarding email or SMS to activate your Wallet account.




Configuring a New Sensor

Step 1: Open the Safetrust Wallet

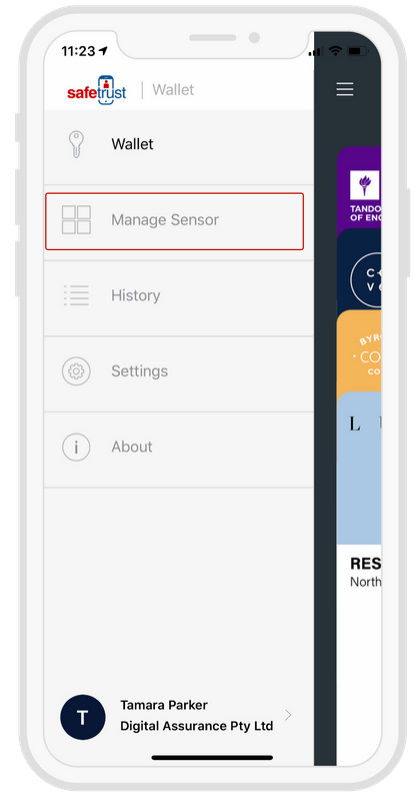
The Safetrust Wallet App communicates with the sensor via Bluetooth and configures the sensor for an Identity System.

Setup:

- Open your Safetrust Wallet App or download it from the App Store or Google Play if you haven't already.
- Login with Google Sign-In or with the username and password that you set your Safetrust account up with.

Select the  **Manage Sensor** tab from the navigation on the left hand side.

Note: You can also configure a sensor using the Credential Manager platform if you are not able to be in range of the sensor.

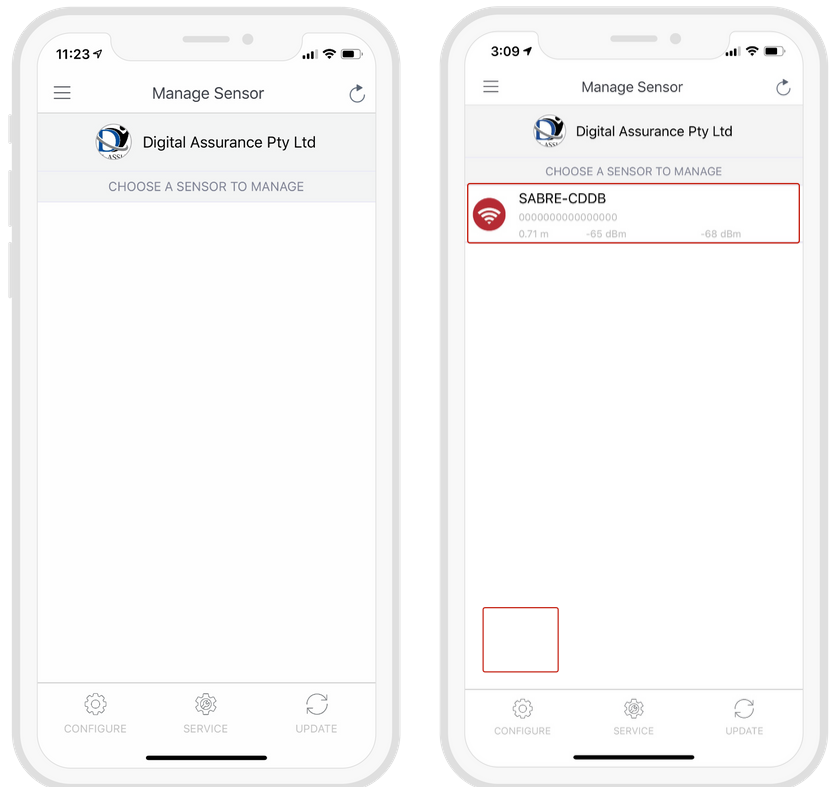


Step 2: Choose a sensor to manage

With the **Manage Sensor** tab open, bring the phone in range of the SABRE and once visible from the App, click on the sensor.

Note: You may need to click the refresh button in the top right hand corner.

Once the sensor is highlighted, click  **CONFIGURE** from the bottom options.



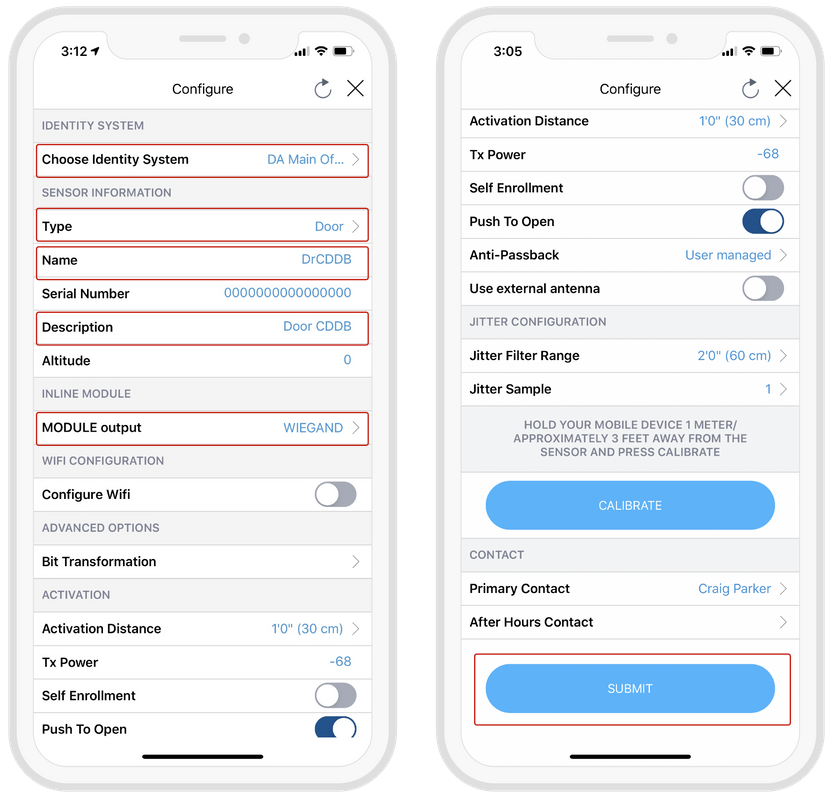
Step 3: Input sensor information

The settings show a range of configuration options for the sensor, however the following fields are the main settings that require action at this time.

Setup:

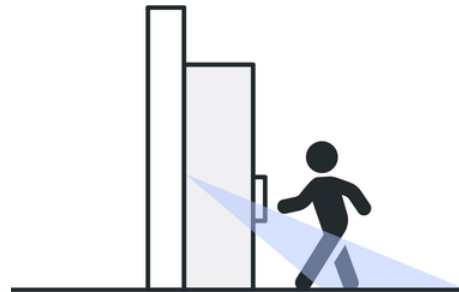
- Choose an **Identity System**.
- Specify the **Type** of access from the dropdown (eg. Door, Gate etc.)
- Assign a short **Name** and **Description** using alphanumeric characters.
- Choose an **Output** for the sensor (the default is set to Wiegand).

Once you have adjusted all the configuration settings, scroll to the bottom of the page and click **SUBMIT** to successfully complete the sensor configuration.



Activation Distance

Set the Activation Distance for your sensor between touch and 50 ft (15m). The distance will automatically be set to 30cm, meaning a user needs to be within 30cm in order to "Auto Authenticate" to the reader.



Anti-passback

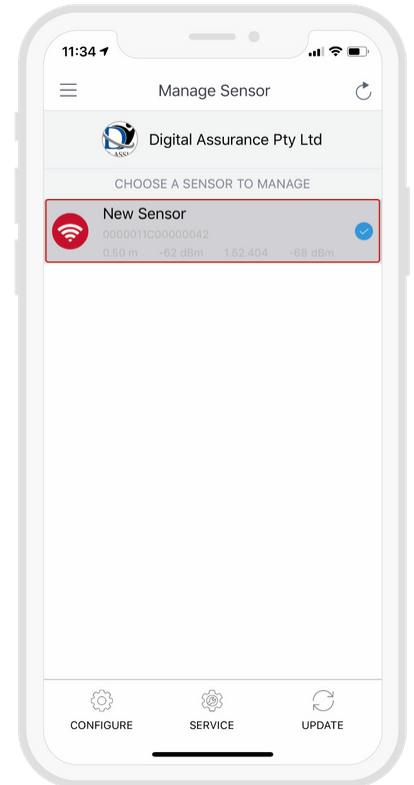
The Anti-Passback setting defines the number of seconds between each attempt to resend a mobile credential.

Anti-Passback can be used to prevent users from passing their credential back for another user to borrow and to stop users entering an area by simply following or tailgating another user.



Step 4: Configuration complete!

When the SABRE information is saved successfully to Credential Manager and assigned to the Identity System, the new description will appear in the **Manage Sensor** tab with a unique serial number assigned.



Getting Access







Using your mobile wallet

Getting Access:

- ✓ To authenticate for a door, boomgate, elevator, or whatever your Identity System is set up for, simply present your mobile device running the Safetrust Wallet application to the reader.
- ✓ When the phone is within the configured activation range, the LED on the assigned credential for this sensor will turn yellow.
- ✓ If Auto Authenticate is enabled for the mobile credential, the credential will be sent to the SABRE whenever the mobile device is within the activation zone.



	Touchless Access	Enjoy hands-free, seamless access without needing to take your phone out of your pocket.
	Tap or wave in	Present your phone within the activation range of the reader just like a traditional card of fob.
	Biometric	Increase your security by adding 2FA to your credentials.
	Cards	Maintain support for your existing keycards and fobs. Use both mobile credentials and plastic credentials at the door.



Safetrust delivers a touchless access experience that makes the new workplace secure, healthier and convenient. Using virtual credentials stored in your mobile phone or wearable, Safetrust enables employees to move seamlessly through secured doors, elevators, turnstiles and more. Safetrust eliminates the need to replace your existing readers by leveraging your existing infrastructure, providing a fast, cost-effective, and convenient upgrade path to touchless virtual credentials. Safetrust is headquartered in Fremont, California.

Want to Learn More?

[Contact support-rfid@elatec.com](mailto:support-rfid@elatec.com)

