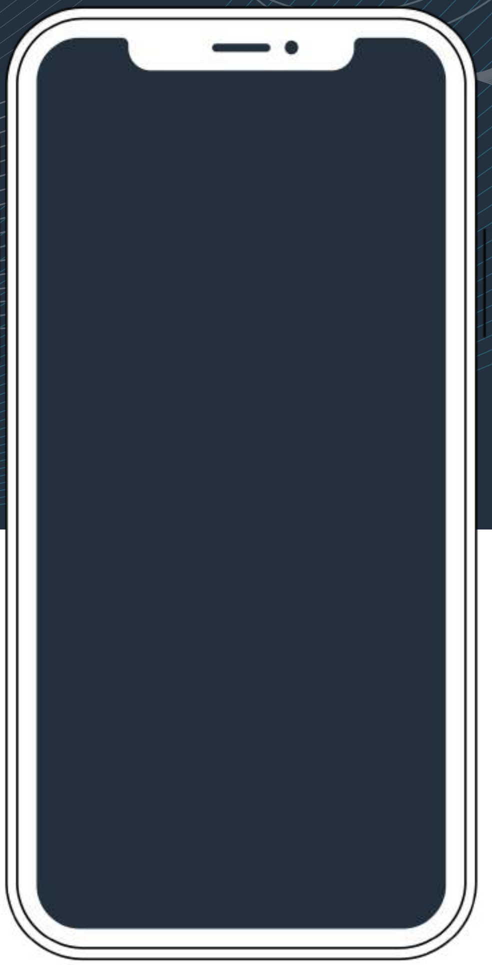
safetrust

Getting Started

Safetrust Quickstart



INSTALL GUIDE

safetrust.com

Last Updated November 08, 2021

About this guide

01

This document includes step-by-step instructions for registering identity systems, creating people, configuring readers, and assigning virtual credentials.

Note: This guide assumes that you meet the pre-requisites listed in **02** of this document prior to commencing the set-up process.

This document is specifically for administrators and is not suitable for end-users. If you require assistance at any point during the set-up process, please contact your local 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

☑ You have acknowledged and accepted the terms and conditions of use for this system

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

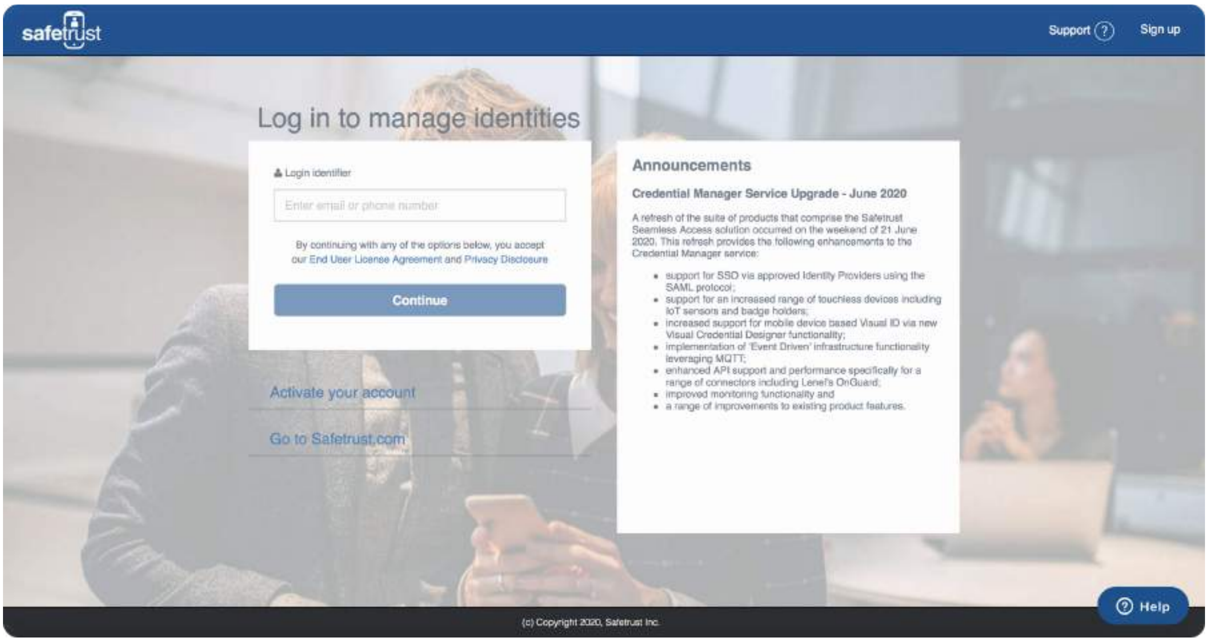
03

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.



Log in to manage identities

Login identifier

Enter email or phone number

By continuing with any of the options below, you accept our End User License Agreement and Privacy Disclosure

Announcements

Credential Manager Service Upgrade - June 2020

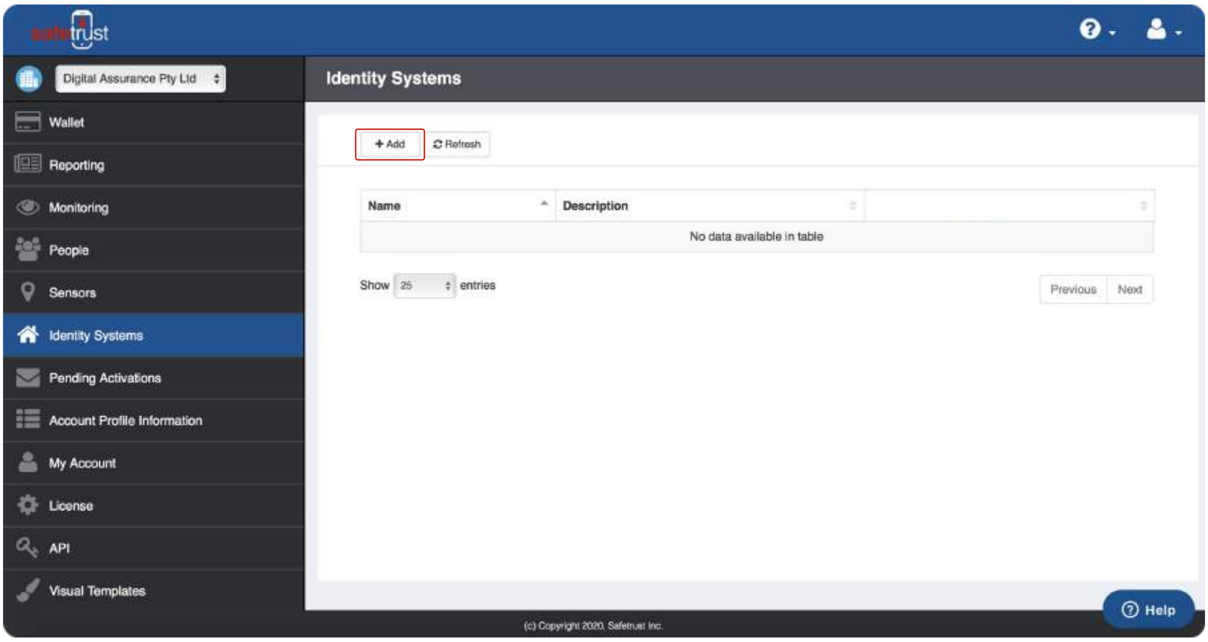
A refresh of the suite of products that comprise the Safetrust Seamless Access solution occurred on the weekend of 21 June 2020. This refresh provides the following enhancements to the Credential Manager service:

- support for SSO via approved Identity Providers using the SAML protocol;
- support for an increased range of touchless devices including IoT sensors and badge holders;
- increased support for mobile device based Visual ID via new Visual Credential Designer functionality;
- implementation of 'Event Driven' infrastructure functionality leveraging MQTT;
- enhanced API support and performance specifically for a range of connectors including Lenel's OnGuard;
- improved monitoring functionality and
- a range of improvements to existing product features.

(c) Copyright 2020, Safetrust Inc.

Step 2:

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



Identity Systems

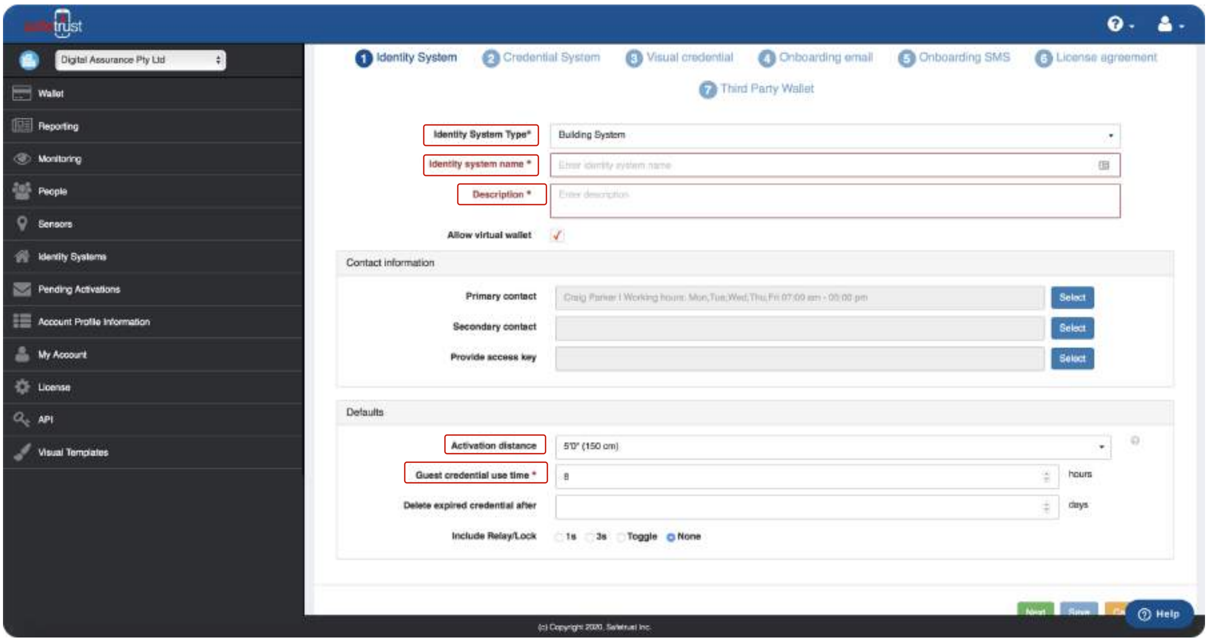
Name	Description	
No data available in table		

Show 25 entries

(c) Copyright 2020, Safetrust Inc.

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.



Identity System Type*: Building System

Identity system name *: Enter identity system name

Description *: Enter description

Allow virtual wallet ✓

Contact information

Primary contact: Craig Parker I Working hours: Mon,Tue,Wed,Thu,Fri 07:00 am - 00:00 pm

Secondary contact:

Provide access key:

Defaults

Activation distance: 5'0" (150 cm)

Guest credential use time *: 8 hours

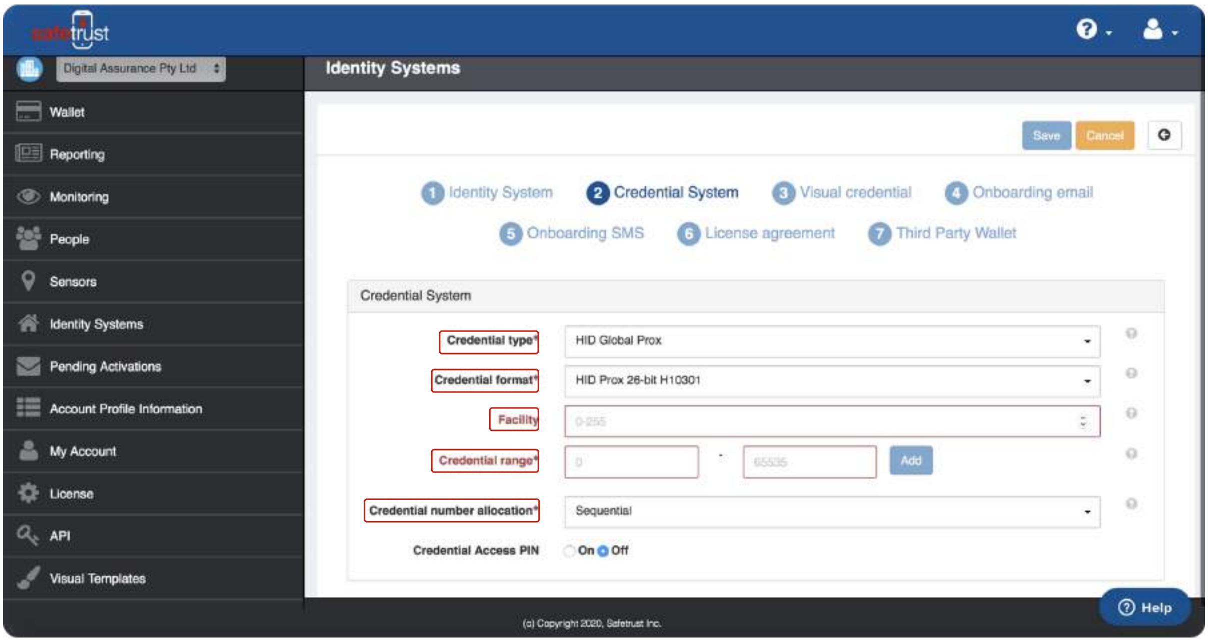
Delete expired credential after: days

Include Relay/Lock ○ 1s ○ 3s ○ Toggle ● None

(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.



Credential System

Credential type*: HID Global Prox

Credential format*: HID Prox 26-bit H10301

Facility: 0-255

Credential range*: 0 - 65535

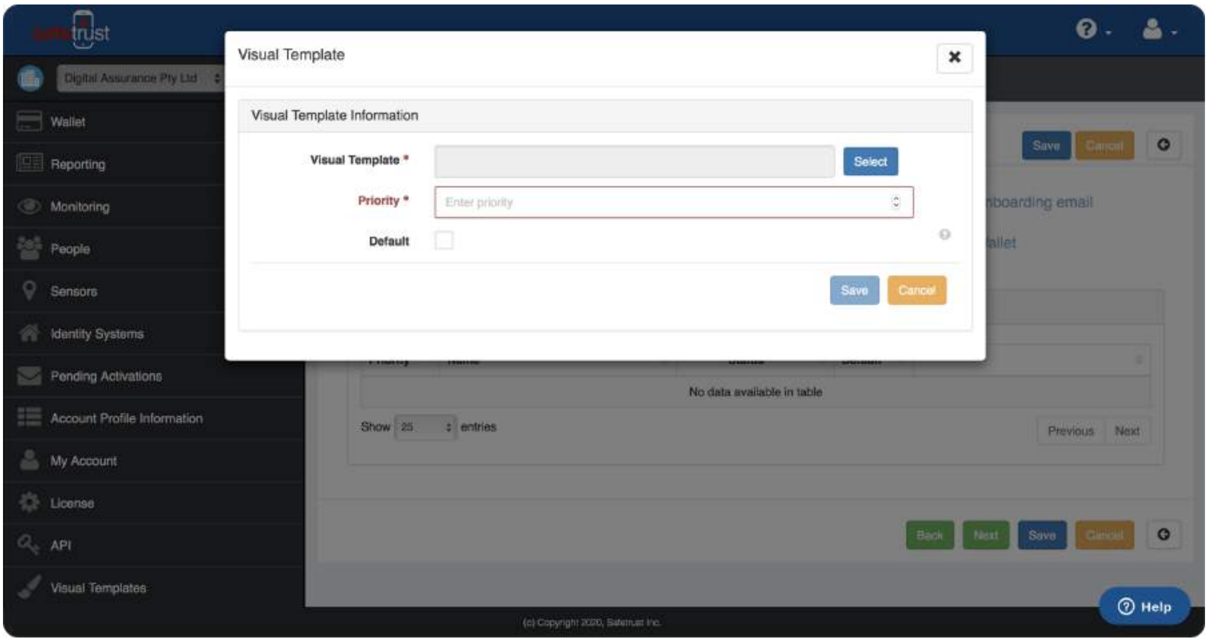
Credential number allocation*: Sequential

Credential Access PIN ○ On ● Off

(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.



Visual Template

Visual Template Information

Visual Template *

Priority * Enter priority

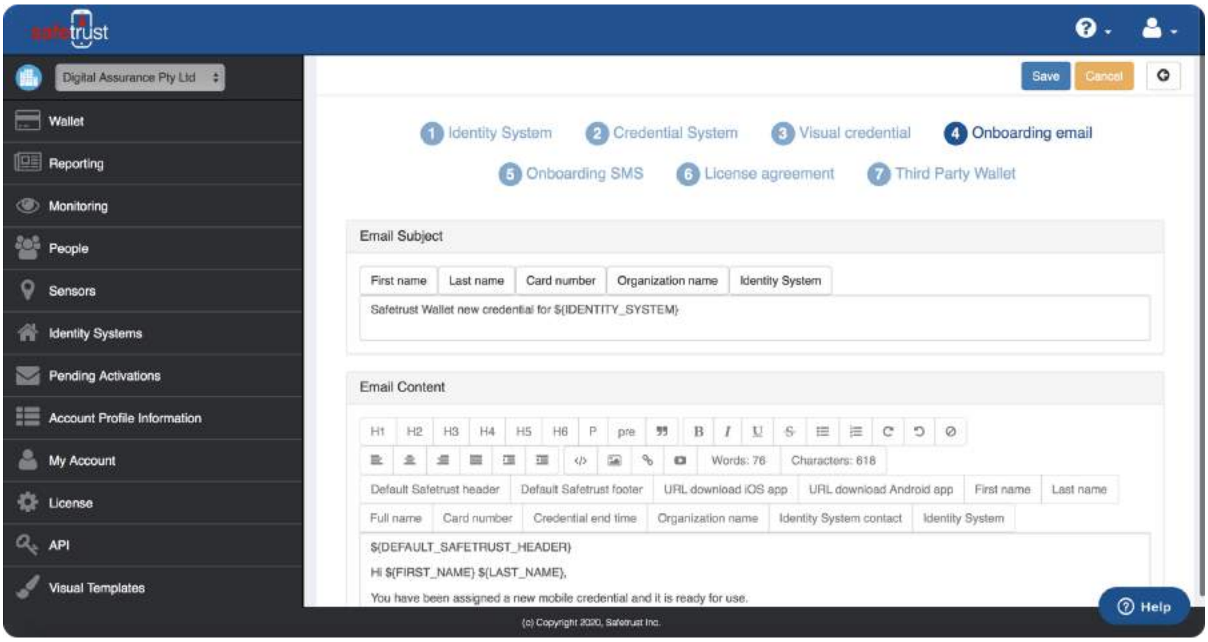
Default □

No data available in table

Show 25 entries

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.



1 Identity System 2 Credential System 3 Visual credential 4 Onboarding email
5 Onboarding SMS 6 License agreement 7 Third Party Wallet

Email Subject

Safetrust Wallet new credential for ${IDENTITY_SYSTEM}

Email Content

Words: 76 Characters: 618

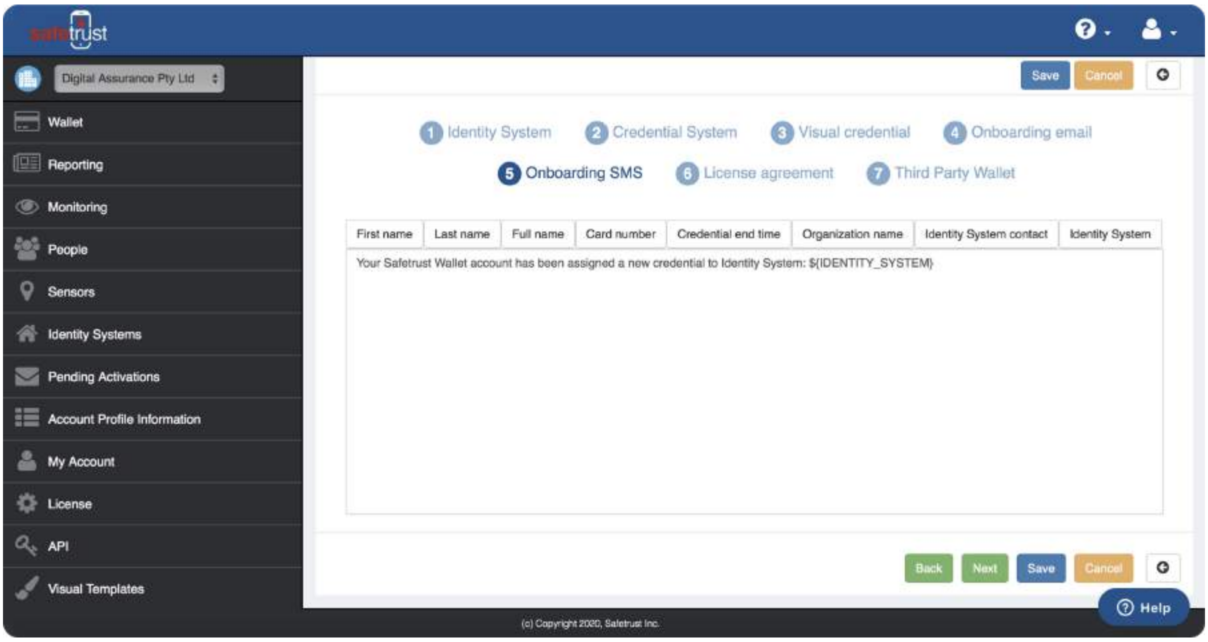
${DEFAULT_SAFETRUST_HEADER}

Hi ${FIRST_NAME} ${LAST_NAME},

You have been assigned a new mobile credential and it is ready for use.

Step 7: Optional

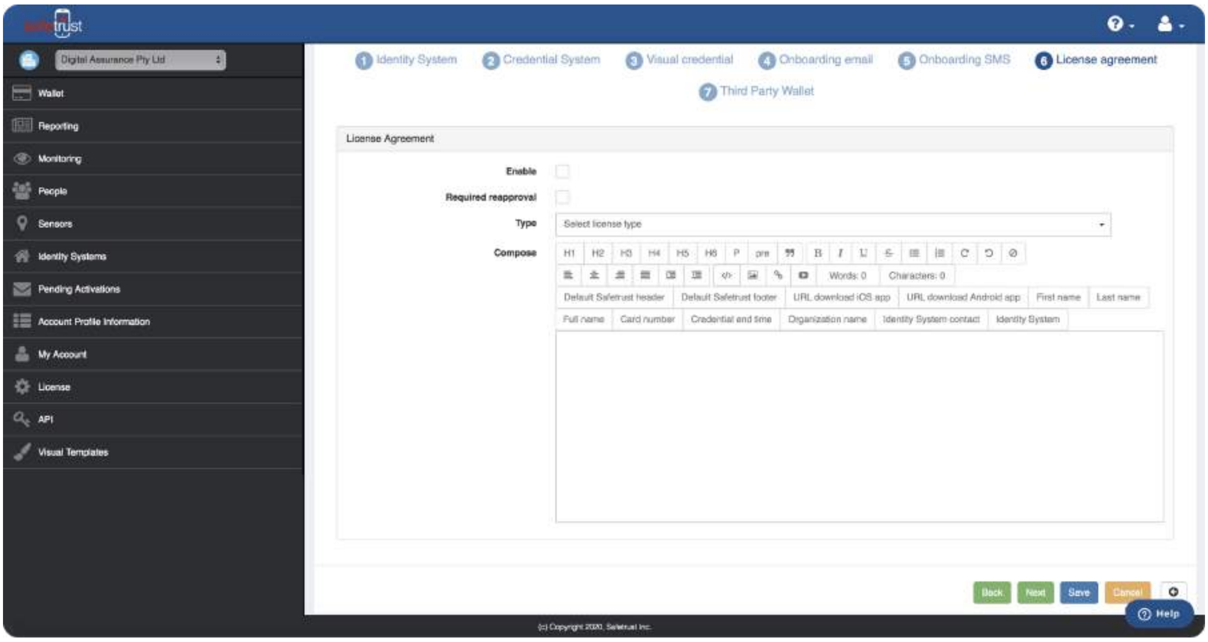
Customize your welcome SMS for new people in your organization and click **Next** to continue.



Your Safetrust Wallet account has been assigned a new credential to Identity System: ${IDENTITY_SYSTEM}

Step 8: Optional

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



License Agreement

Enable □

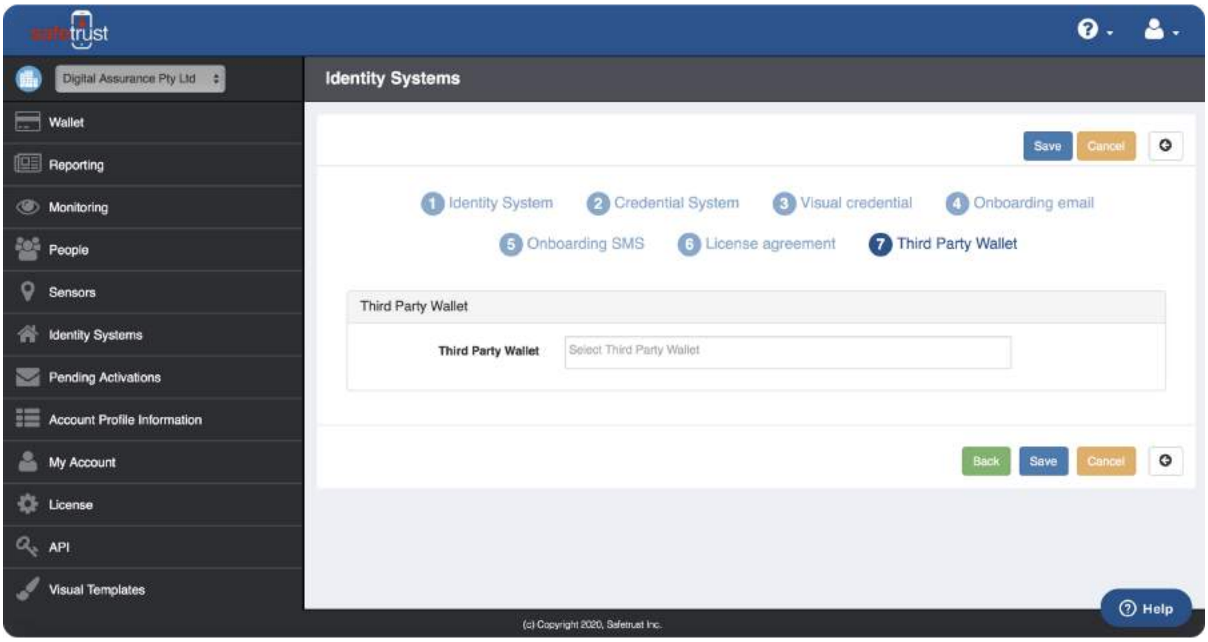
Required reapproval □

Type: Select license type

Compose

Step 9: Optional

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



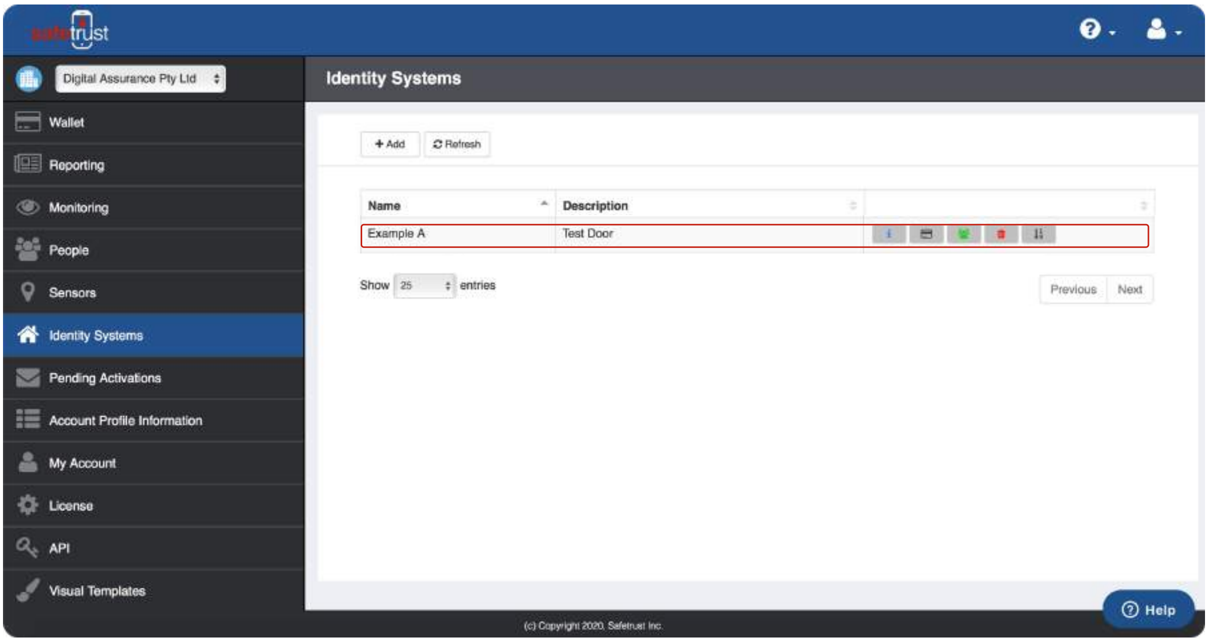
Identity Systems

Third Party Wallet

Third Party Wallet: Select Third Party Wallet

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.



Identity Systems

Name	Description	
Example A	Test Door	

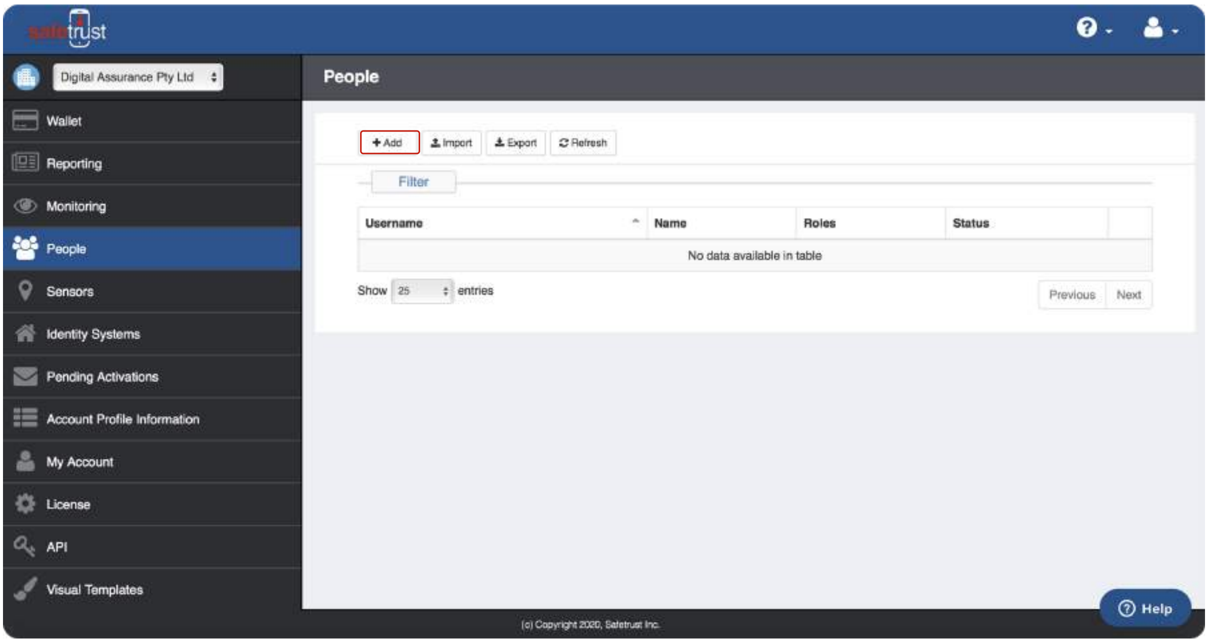
Show 25 entries

04

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.

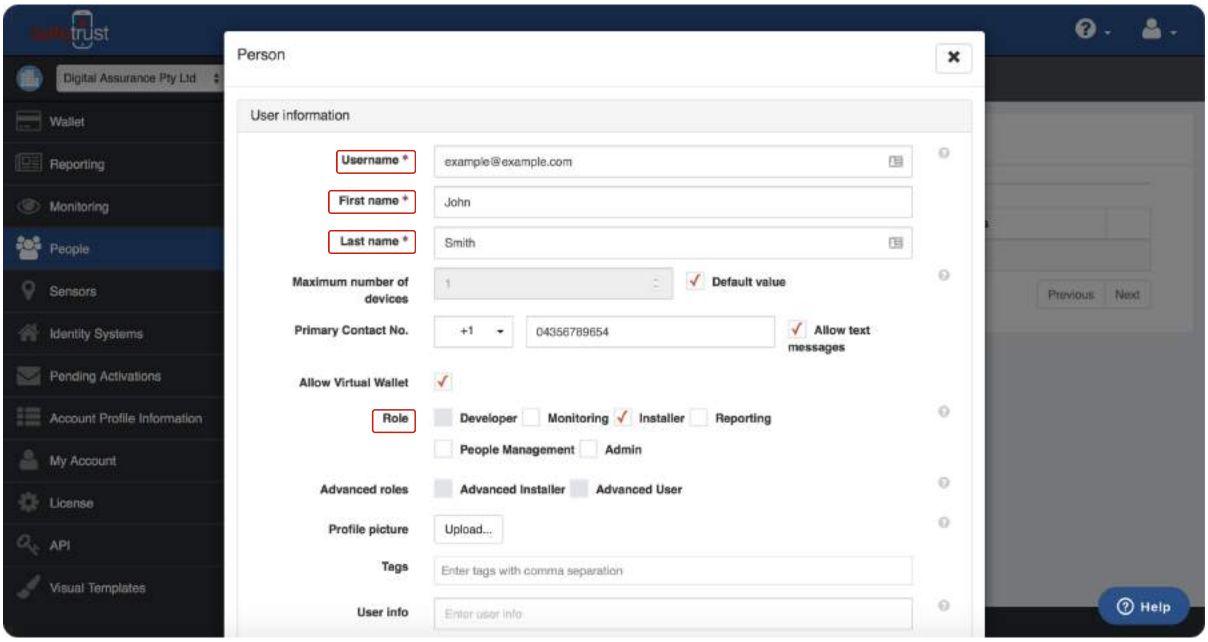


Username	Name	Roles	Status
No data available in table			

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.



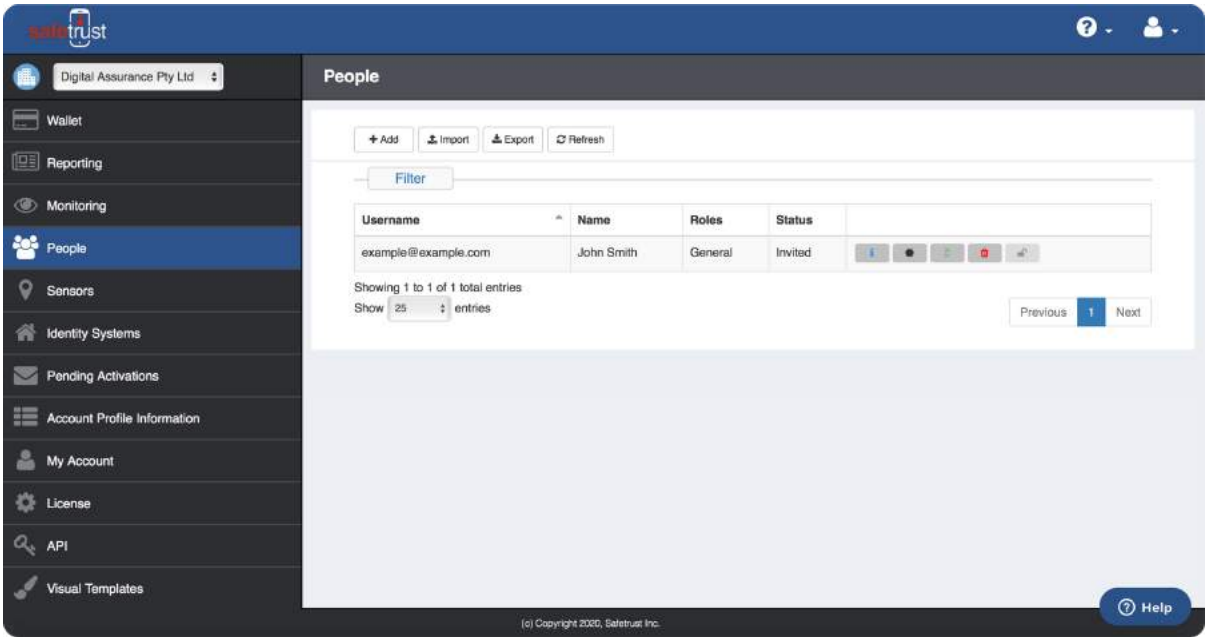
Person

User information

Username *	example@example.com
First name *	John
Last name *	Smith
Maximum number of devices	1 ☑ Default value
Primary Contact No.	+1 04356789654 ☑ Allow text messages
Allow Virtual Wallet	☑
Role	□ Developer □ Monitoring ☑ Installer □ Reporting □ People Management □ Admin
Advanced roles	□ Advanced Installer □ Advanced User
Profile picture	Upload...
Tags	Enter tags with comma separation
User info	Enter user info

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 ● n.

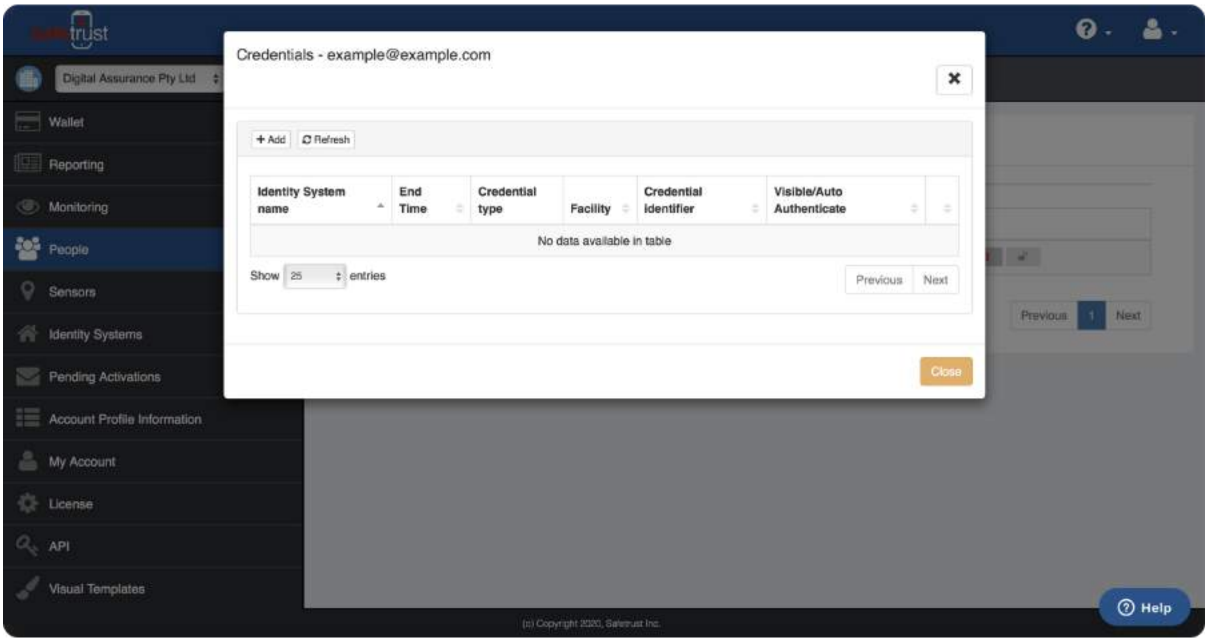


Username	Name	Roles	Status	
example@example.com	John Smith	General	Invited	●

Showing 1 to 1 of 1 total entries

Step 4:

Click the **Add** button.

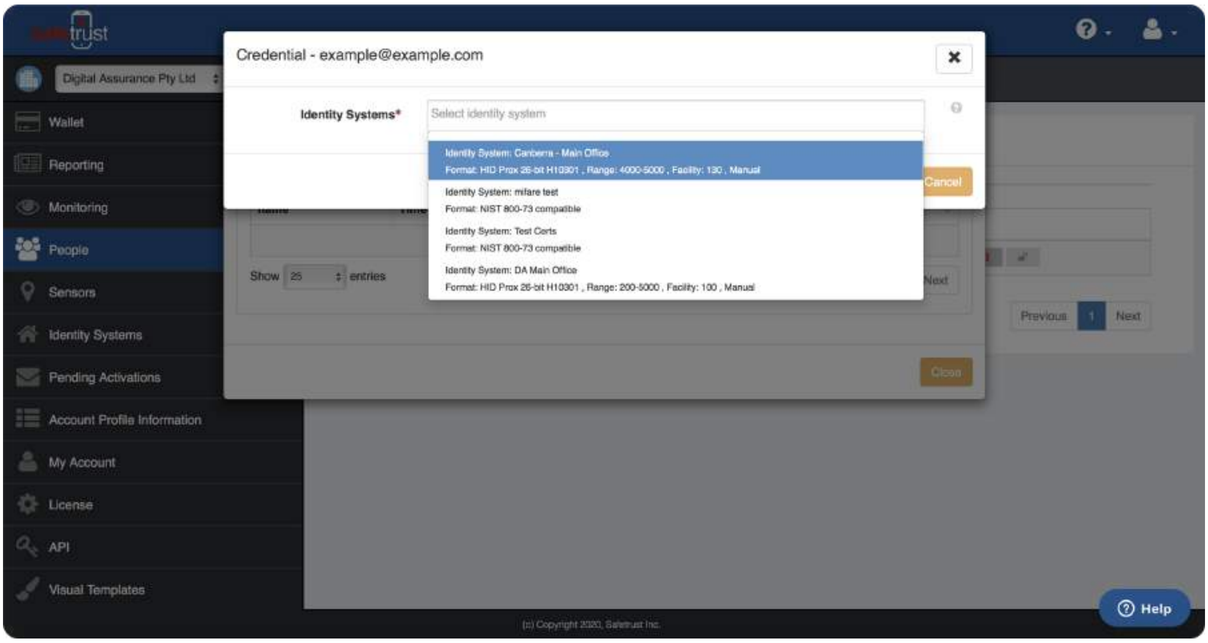


Credentials - example@example.com

Identity System name	End Time	Credential type	Facility	Credential identifier	Visible/Auto Authenticate	
No data available in table						

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.



Credential - example@example.com

Identity Systems* Select identity system

Identity System: Canberra - Main Office
Format: HID Prox 26-bit H10301 , Range: 4000-5000 , Facility: 130 , Manual

Identity System: mifare test
Format: NIST 800-73 compatible

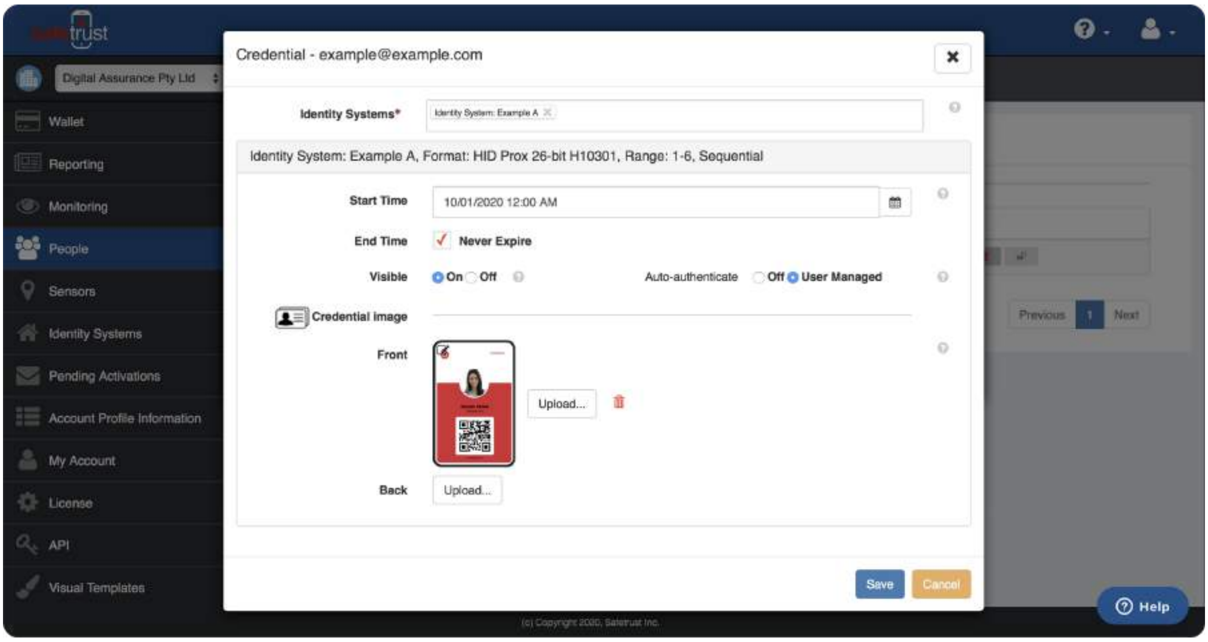
Identity System: Test Certs
Format: NIST 800-73 compatible

Identity System: DA Main Office
Format: HID Prox 26-bit H10301 , Range: 200-5000 , Facility: 100 , Manual

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.



Credential - example@example.com

Identity Systems* Identity System: Example A

Identity System: Example A, Format: HID Prox 26-bit H10301, Range: 1-6, Sequential

Start Time 10/01/2020 12:00 AM

End Time ☑ Never Expire

Visible ● On ○ Off

Auto-authenticate ○ Off ● User Managed

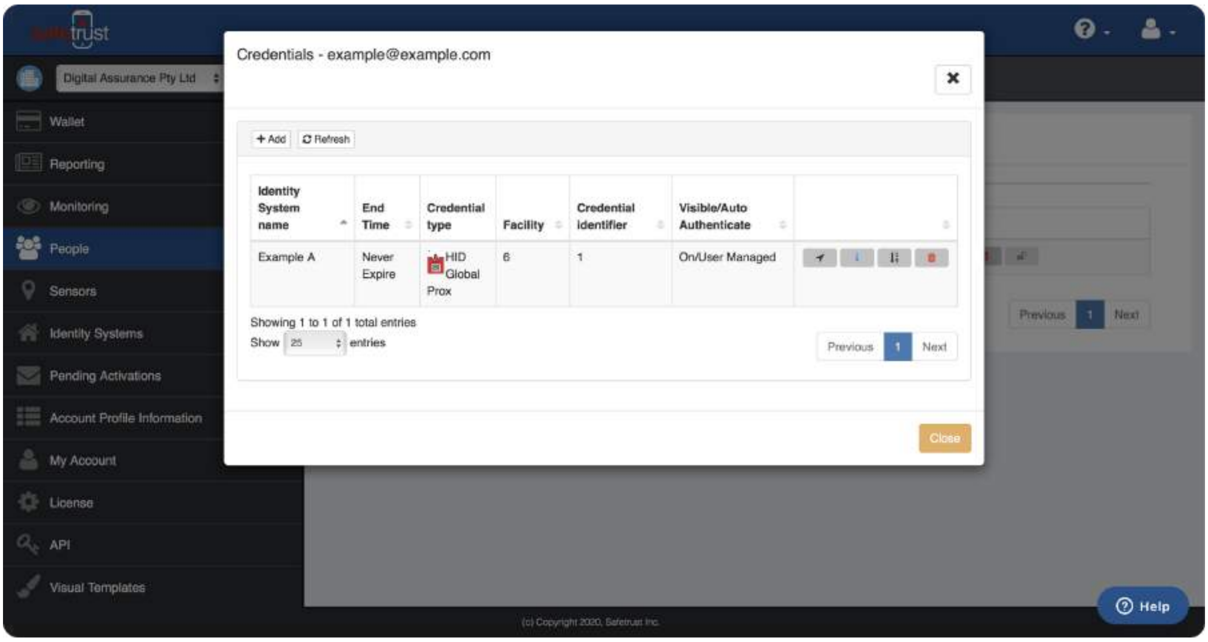
Credential image

Front

Back

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.



Credentials - example@example.com

Identity System name	End Time	Credential type	Facility	Credential identifier	Visible/Auto Authenticate	
Example A	Never Expire	HID Global Prox	6	1	On/User Managed	

Showing 1 to 1 of 1 total entries

Show 25 entries

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.

05

Configuring a New Sensor

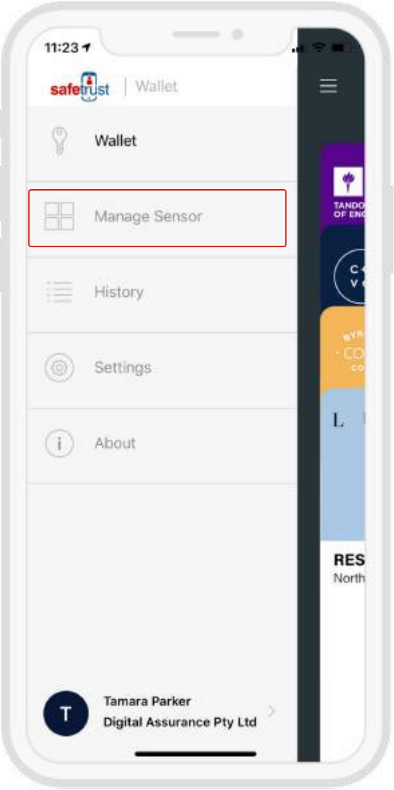
Step 1: Open the Safetrust Wallet

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.

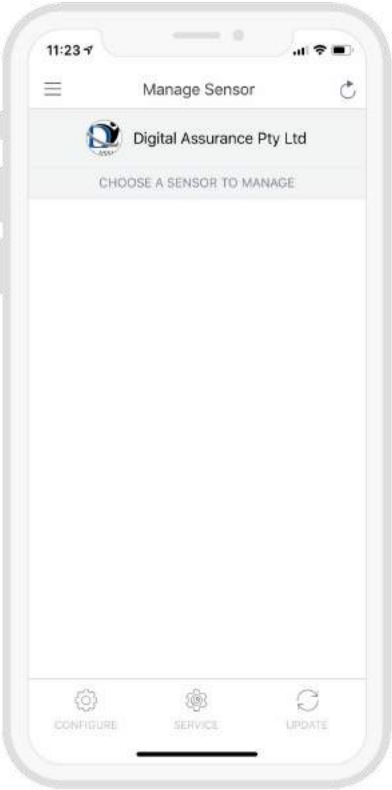


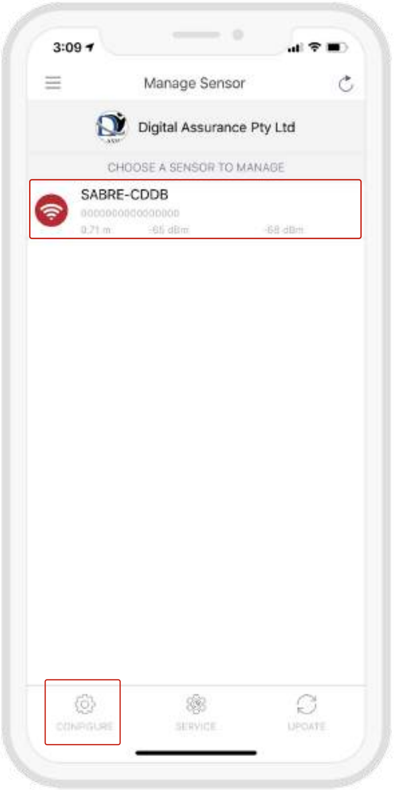
Step 2: Choose a sensor to manage

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.



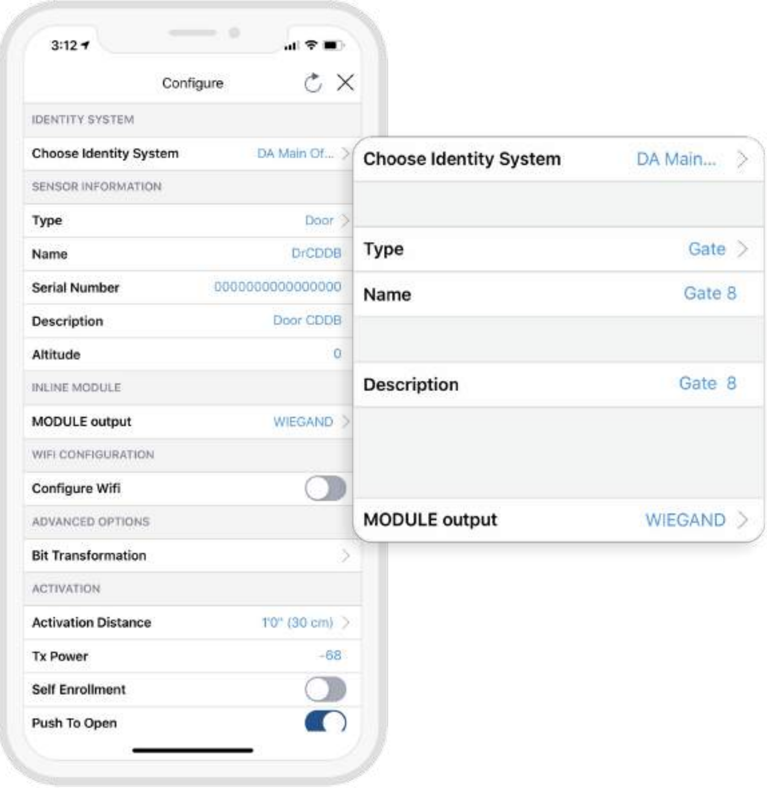


Step 3: Input sensor information

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).



3:12

Configure

IDENTITY SYSTEM

Choose Identity System: DA Main Of...

SENSOR INFORMATION

Type: Door

Name: DrCDDB

Serial Number: 0000000000000000

Description: Door CDDB

Altitude: 0

INLINE MODULE

MODULE output: WIEGAND

WIFI CONFIGURATION

Configure Wifi ○

ADVANCED OPTIONS

Bit Transformation

ACTIVATION

Activation Distance: 1'0" (30 cm)

Tx Power: -68

Self Enrollment ○

Push To Open ●

Choose Identity System: DA Main...

Type: Gate

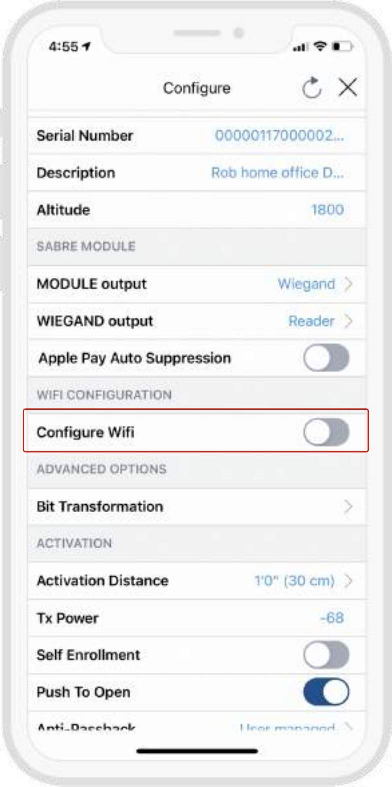
Name: Gate 8

Description: Gate 8

MODULE output: WIEGAND

Configuring WiFi:

1. To connect the sensor to a WiFi network, click the 'Configure Wifi' toggle button. Switching the toggle will reveal additional settings below.



4:55

Configure

Serial Number: 00000117000002...

Description: Rob home office D...

Altitude: 1800

SABRE MODULE

MODULE output: Wiegand

WIEGAND output: Reader

Apple Pay Auto Suppression ○

WIFI CONFIGURATION

Configure Wifi ○

ADVANCED OPTIONS

Bit Transformation

ACTIVATION

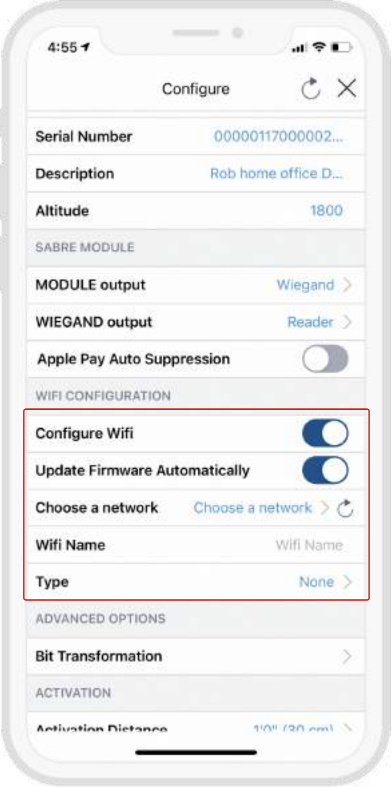
Activation Distance: 1'0" (30 cm)

Tx Power: -68

Self Enrollment ○

Push To Open ●

Anti-Passback: User managed



4:55

Configure

Serial Number: 00000117000002...

Description: Rob home office D...

Altitude: 1800

SABRE MODULE

MODULE output: Wiegand

WIEGAND output: Reader

Apple Pay Auto Suppression ○

WIFI CONFIGURATION

Configure Wifi ●

Update Firmware Automatically ●

Choose a network: Choose a network

Wifi Name: Wifi Name

Type: None

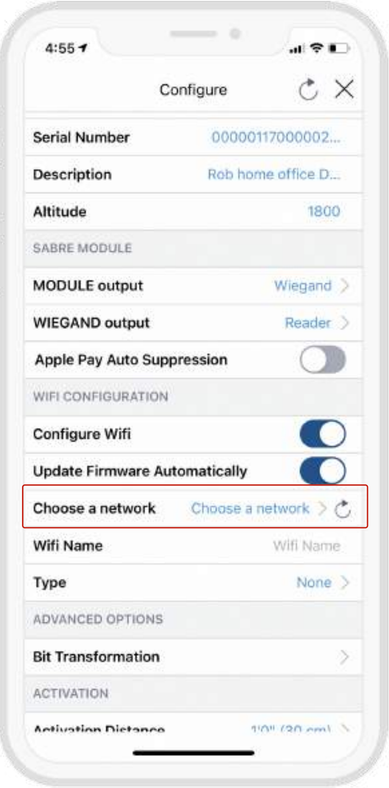
ADVANCED OPTIONS

Bit Transformation

ACTIVATION

Activation Distance: 1'0" (30 cm)

2. Click the 'Choose a network' setting or type in the Wifi Name in the 'Wifi Name' field. If your network is not listed, try clicking the refresh icon next to 'Choose a network'.



4:55

Configure

Serial Number 00000117000002...

Description Rob home office D...

Altitude 1800

SABRE MODULE

MODULE output Wiegand

WIEGAND output Reader

Apple Pay Auto Suppression ○

WIFI CONFIGURATION

Configure Wifi ●

Update Firmware Automatically ●

Choose a network Choose a network

Wifi Name Wifi Name

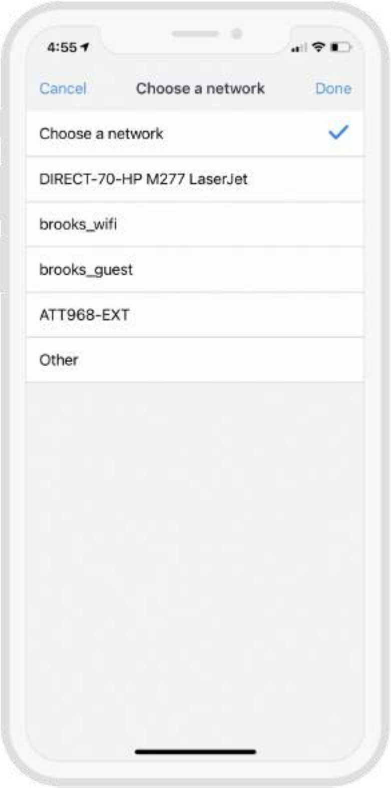
Type None

ADVANCED OPTIONS

Bit Transformation

ACTIVATION

Activation Distance 1'0" (30 cm)



4:55

Cancel Choose a network Done

Choose a network ✓

DIRECT-70-HP M277 LaserJet

brooks_wifi

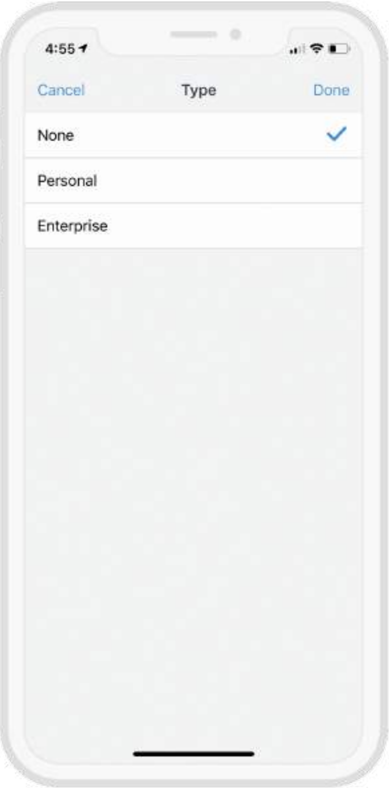
brooks_guest

ATT968-EXT

Other

3. Choose the network type - Personal or Enterprise.

4. For Enterprise 802.1X networks, click the 'Root certificate' and 'Client p12' buttons to upload your certificates. Type the P12 password in the 'P12 password' field.



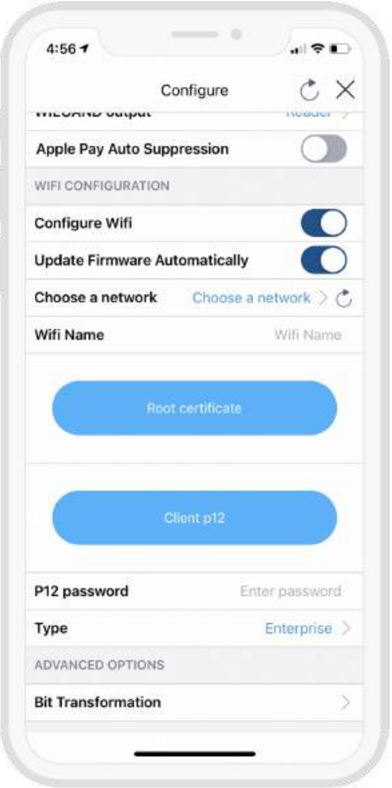
4:55

Cancel Type Done

None ✓

Personal

Enterprise



4:56

Configure

WIEGAND output Reader

Apple Pay Auto Suppression ○

WIFI CONFIGURATION

Configure Wifi ●

Update Firmware Automatically ●

Choose a network Choose a network

Wifi Name Wifi Name

Root certificate

Client p12

P12 password Enter password

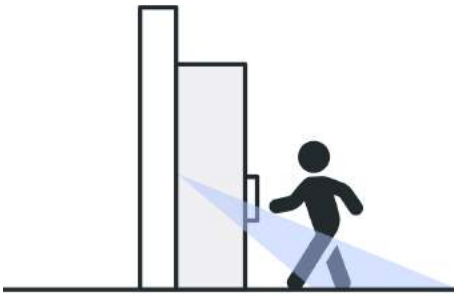
Type Enterprise

ADVANCED OPTIONS

Bit Transformation

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

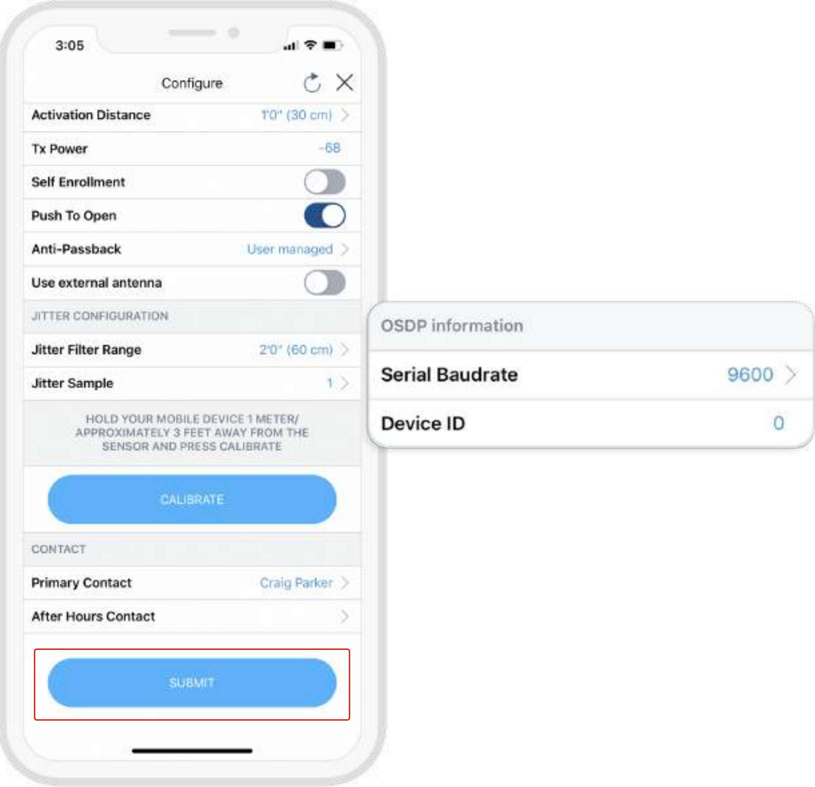
The Anti-Passback setting defines the number of seconds between each attempt to resend a mobile credential.

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.

OSDP Output:

If the **Output** is set to OSDP, select the **Serial Baudrate** and set the **Device ID** to match the settings of the access control panel.

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



Configure

Activation Distance	1'0" (30 cm)
Tx Power	-68
Self Enrollment	○
Push To Open	●
Anti-Passback	User managed
Use external antenna	○
JITTER CONFIGURATION	
Jitter Filter Range	2'0" (60 cm)
Jitter Sample	1

HOLD YOUR MOBILE DEVICE 1 METER/ APPROXIMATELY 3 FEET AWAY FROM THE SENSOR AND PRESS CALIBRATE

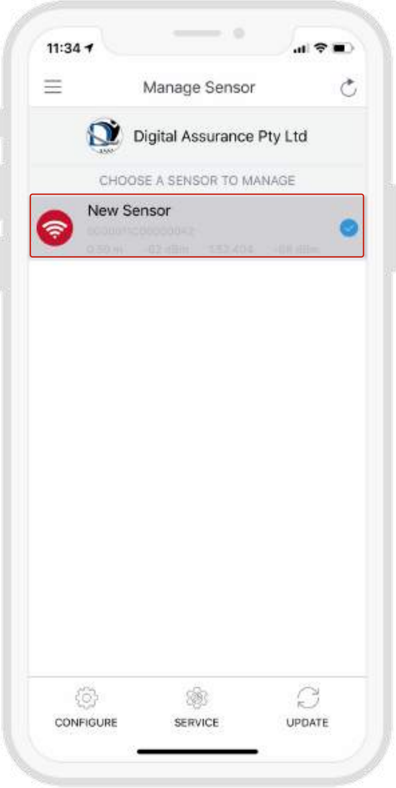
CONTACT	
Primary Contact	Craig Parker
After Hours Contact	

OSDP information

Serial Baudrate	9600
Device ID	0

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.



06

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.

EVENT
Launch Networking Drinks

WHERE
The Commons QV

TICKET
Sunday Ticket

WHEN
9 Sep 2020 at 6:00 pm

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 sales@safetrust.com