ICT

PRT-MOB-IF

Protege Mobile App

User Guide

Last Published: 11-Jul-23 08:34 AM

Contents

Introduction

The Protege Mobile App allows you to monitor and control your business while on the go, all from a touch of your mobile device. With the swipe of a finger you can connect to any of your configured places and check statuses, arm or disarm, control lights, locks, signage, heating - even cameras - from anywhere, at any time.

The app provides instant access to system events and status and enables you to arm/disarm with a simple tap. No more second guessing whether you set the alarm before you left the office.

A couple of taps on your way to work and you have the heating and lights turned on, transforming a cold, dark office into a warm and inviting environment. And fumbling for your access card becomes a thing of the past as you can use the app to unlock the door.

When paired with Bluetooth® and NFC enabled readers, the mobile app makes access easier than ever. Mobile credentials provide the flexibility and added convenience of card-free access from your device. No more issues with lost or forgotten cards and tags - simply present your mobile device within range of the reader to gain entry. Customize the read range, and you don't even need to take your phone out of your pocket.

Prerequisites

The Protege Mobile App can be used with the associated mobile credential to gain access at card readers, instead of a traditional access card.

The app can also connect to your Protege X, Protege WX and Protege GX places, allowing you to view and control the status of resources on the site.

Each app usage has different requirements, as outlined further below. The following prerequisites are required for all mobile app operation:

- **Protege Mobile App**: Can be installed from the Google Play Store or the App Store (see page 8).

  You can log in to your mobile app account on multiple mobile devices, such as smartphones or tablets. For more information, see Device Limits (page 13).

- **Protege Mobile Credential**: One credential is required for each mobile app account, even if it is not used for door access. Mobile credentials can be purchased from ICT using the product code PRX-MCR.
- **Internet connection**: Your mobile credential is issued from ICT's secure cloud server. Each time you open the app you will need an internet connection to log in and access your credential.

  Once you have logged in the credential will remain valid on your device for as long as the app is running, even if you no longer have internet access. You can also still use the credential while the app is minimized.

  Your device may automatically terminate the app if it has been running for longer than allowed (this varies between devices). When this occurs you will need to log in again.

Using Mobile Credentials for Access

To use the Protege Mobile App to gain access at a card reader you require the following:

- **NFC / Bluetooth® capable Android or iOS device**
- **NFC / Bluetooth® capable card readers**: This feature requires firmware version 1.04.178 or higher.

Connecting to a Protege X Place

To connect to a Protege X place using the mobile app you need to sign in with your authenticated Protege X operator account credentials, including two-factor authentication.

Connecting to a Protege WX Place

To connect to a Protege WX place using the mobile app you need an operational Protege WX controller which is accessible over the internet or local network.

It is strongly recommended that an HTTPS certificate from a trusted certificate authority is installed on your Protege WX place controller. For more information, see Application Note 210: Securing the Protege Mobile App.

Connecting to a Protege GX Place

To connect to a Protege GX place using the mobile app the following components are required:

Component	Version	Notes
Protege GX	4.2.181.10 or higher	
Protege GX SOAP Service	1.5.0.15 or higher	
Protege GX Web Client	1.44.0.17 or higher	Must be accessible over the internet or local network.

It is strongly recommended that an HTTPS certificate from a trusted certificate authority is installed on your Protege GX web client. For more information, see Application Note 210: Securing the Protege Mobile App.

Account Binding

Protege Mobile App data is linked to your account and not to the device the app is installed on. This enables you to log in to the app on multiple devices and retain your settings.

Language Setting

On startup the mobile app will detect the language set in the device and automatically use that language. If you change the device's language setting you will need to restart the app before it will detect the new language.

Not all languages are supported. If the device language is not available the app will default to English.

Supported Languages

The mobile app currently supports the following languages:

- Czech
- Dutch
- English
- Estonian
- Finnish
- French
- German
- Greek
- Hungarian
- Italian
- Norwegian
- Polish
- Russian
- Serbian
- Spanish
- Swedish

There are some missing translations within all supported language packs. These will be improved over time.

Initial Setup

Installing the App

To begin using the mobile app you will first need to download and install it on your phone or mobile device. The Protege Mobile App is available from the Google Play Store and from the App Store.

Downloading for Android Devices

1. On your Android device, navigate to the **Google Play Store**.

2. Enter **Protege Mobile** into the Search Bar.

3. Select the **Protege Mobile** App.

4. Tap **Install**.

Downloading for iOS Devices

1. On your iOS device, navigate to the **App Store**.

2. From the search bar, enter **Protege Mobile**.

3. Select the **Protege Mobile** App.

4. Tap **GET**.

Logging In

If you do not have an existing mobile app account it is easy to create a new one, either by entering a new email address and password or by signing in with a social media account.

Mobile app data is linked to your account and not to the device the app is installed on. This enables you to log in to the app on multiple devices and retain your settings.

Once you select a login method ensure that it is the only method you use to access the app. Each method creates a unique account which will not be able to access the mobile credential or configurations linked to other accounts.

Logging In for the First Time

1. Open the Protege Mobile App.

2. You will be presented with a **Login** screen. When you log in for the first time you can select your preferred authentication method:
   - Sign in using an existing Protege Mobile App account
   - Sign in with Facebook
   - Sign in with Google
   - Sign in with Twitter
   - Create new account

   Signing in with social media accounts is only available for Android devices.

3. If creating a new account you will be prompted to create new credentials (username and password) for use with this account and accept the terms and privacy policy. If signing in with social media you may be asked to enter your credentials, or you may proceed automatically if you are logged in on your device.

4. Next you will be prompted to create a PIN code for use with this account. Enter a unique four-digit PIN, then re-enter the same PIN to verify it.

5. From the **Require PIN** drop-down, select how frequently you would like to be prompted to enter this PIN while using the mobile app.

    You can edit these settings and your PIN in the future from the **Account Settings** page.

6. When finished, tap **DONE**.

7. Information about the available menus is displayed. Tap **GOT IT** to close the list.

Updating the Mobile App

Depending on your device configuration, the Protege Mobile App may update automatically on your device when new updates are available, or you may need to update the app manually.

Updating for Android Devices

1. On your Android device navigate to the **Google Play Store**.

2. At the top right, tap the profile icon.

3. Tap **Manage apps & device**. Apps with an update available are labeled 'Update available'.

4. Beside the Protege Mobile App, tap **Update**.

You can also configure the app to update automatically. In **Manage apps & device**, tap **Manage** and select the Protege Mobile App. Tap **More** [**⋮**] and turn on **Enable auto-update**.

Updating for iPhone / iPad

1. On your iOS device, navigate to the **App Store**.

2. Tap your profile icon at the top of the screen.

3. Scroll to see pending updates and release notes.

4. Beside the Protege Mobile App, tap **Update**.

You can configure your device to update apps automatically. In **Settings** tap **App Store** and turn on **App Updates**.

Basic Navigation

Main Menu

From the main menu you can view and access the setup and configuration options, along with all the functional monitoring and control pages.

Navigating the Menus

Navigating your way through the Protege Mobile App is simple and intuitive.

- You can access the menu pages via the main menu, or by using the shortcuts at the bottom of the screen.
- To access the main menu tap the menu icon at the top left, and from there tap the menu you want to access.
- You can swipe left/right to move between pages.

Searching

1. To easily search for records using keywords tap the search icon at the top of the screen.
2. Type the name of the record. Matching records are displayed automatically and will be filtered as you type.
3. When complete, tap **X** to clear the search.

If the search icon is not visible, tap the down arrow (▼) at the top of the page to display the Advanced Menu.

Account Settings

The Account Settings menu provides access to settings that allow you to select your PIN security level, change or remove your PIN, and view and delete your account details.

Changing the Security Level

Changing the security level will allow you to define how often the app prompts you to enter your PIN.

1. From the main menu, select **Account Settings**.
2. When prompted, enter your PIN to access your account settings.
3. Tap the drop-down for the **Require PIN** menu.
4. Select how often you want the app to prompt you to enter your PIN.
5. Tap **Save**.

Changing your PIN

1. From the main menu, select **Account Settings** and enter your PIN when prompted.
2. Tap **CHANGE PIN**.
3. Enter your old PIN.
4. Enter your new PIN, then re-enter your new PIN to confirm. Your PIN is updated.

Deleting your PIN

From any screen that prompts for PIN entry, the app allows you to delete your PIN. This is helpful if you have forgotten your PIN, allowing you to delete it and then create a new one after logging in securely to the app.

1. When prompted for your PIN, tap the trash can icon.
2. On the **PIN Deletion** warning tap **OK** to proceed and delete your PIN.

Your PIN will be deleted and you will be logged out of the app.

When you next log in you will be prompted to **Enter new PIN**. You will also be prompted to select the security level for your new PIN. Select your preferred **Require PIN** level, then tap **DONE**.

Deleting your Account

Deleting your account allows you to **permanently** delete your mobile account and remove your personal information, places and settings, mobile credentials, SIP configurations and reader configurations from the app .

1. From the main menu, select **Account Settings** and enter your PIN when prompted.
2. Tap **ACCOUNT DETAILS**. Your account Email and UserID are displayed.
3. Tap **DELETE ACCOUNT**.
4. On the **Delete Account** warning tap **OK** to proceed and delete your account.

> This action cannot be undone and your account and settings cannot be recovered. If you delete your account you will need to establish a new account in order to use the app in the future.

Mobile Credential Settings

Each device that has the Protege Mobile App installed is assigned a set of mobile credentials that you can use to unlock Protege controlled doors using Bluetooth® and NFC. These mobile credentials can be used with compatible card readers.

1. Open the main menu.

2. Tap **Mobile Credential Settings**.

3. The **Mobile Credentials** include the site code and card number (Credential) assigned to your device.

4. The **Settings** section allows you to enable or disable the following access features:

   - **Proximity unlock**: Unlocks the nearest door when in range. The range is determined by the Bluetooth Proximity slider setting described below. This option requires **Bluetooth**® enabled on your phone.

   - **Shake to unlock**: Unlocks the nearest door when you shake your phone when in range. The range is determined by the general Bluetooth® range of your phone, including external factors, not by the Bluetooth Proximity slider setting. This option requires **Bluetooth**® enabled on your phone.

   - **NFC unlock**: Unlocks the door when you present your phone close to the reader, like a regular card credential. This option requires **NFC** enabled on your phone.

   These features may require additional phone hardware or configuration requirements.

5. Use the **Bluetooth Proximity** slider to set the Bluetooth® field range of your device. Setting the field towards Near means that your device won't communicate with the reader until it is presented very close to it. By setting the field towards Far you can use your device to unlock a door from a greater distance.

Assigning Credentials

When a mobile credential has been assigned to the app it must still be assigned to the user record in the Protege system before the app user will be granted access.

Assigning the Credentials in Protege X

1. Sign in to the Protege X place.

2. Navigate to **Users** and select the user to assign the credential to.

3. In the **Access Cards** section, click **Edit**.

4. Click **Add** and in the **Facility Number** and **Card Number** fields enter the Credential details as they are displayed on the mobile device.

5. Click **Save**.

Assigning the Credentials in Protege WX

1. Launch and log in to the Protege WX web interface.

2. Navigate to **Users | Users | General** and select the user to assign the credential to.

3. In the **Access Cards** section, enter the Credential details as they are displayed on the mobile device.

4. Click **Save**.

Assigning the Credentials in Protege GX

1. Launch and log in to the Protege GX client.

2. Navigate to **Users | Users | General** and select the user to assign the credential to.

3. In the **Card Numbers** section, enter the Credential details as they are displayed on the mobile device.

4. Click **Save**.

After the credential has been configured in the software it may take a few minutes for it to download to the controller. After that you can switch Bluetooth® on and begin using your device for access.

Device Limits

By default, each Protege mobile credential can be installed on an unlimited number of devices. However, in some situations your system administrator may have limited the number of devices each credential can be installed on.

If you reach the device limit for a credential you can still log in to the app on additional devices, but you will not be able to use that credential. A warning is displayed for the affected credential in the **Mobile Credential Settings**.

If you exceed the device limit ask your building manager or system administrator to remove an old device from the list, allowing you to access your credential on the new device. Your administrator can also revoke permissions for a device which has been lost or stolen, preventing unauthorized parties using the device to gain access.

My Places

The My Places page is where you add, edit and select the places you want to monitor and control. From the main menu, navigate to **My Places**. All of your configured places will be listed.

Tap to select the place you want to access. The home page for the site will then be displayed. The home page displays the controls and alerts that you have selected for the place and can be configured using the features in the advanced menu.

All settings, access and control are specific to the configuration of the selected place. To view or control another place, make a new selection.

To **Edit** the details of your place, tap the edit icon to the right of the list. From here you can also **Delete** your place from the app if required.

Creating a Place

You can create as many places as you need to access. They will all be attributed to your same mobile account login, no matter which device you are using, and you will be assigned the access privileges of your system operator. If your operator has different access privileges at different places this will automatically come through to the mobile app, and you will have access to each place according to your relevant operator access.

When creating a place there is no check to prevent you adding the same place multiple times, resulting in duplicate listings. If this occurs you can simply delete any additional listings.

Protege X

If you are an operator of a Protege X place you can sign in to the app with your authenticated Protege X operator account credentials to control your Protege X place.

For information on signing in requirements and activating your operator account, see the Protege X online help.

1. From the main menu, select **My Places** and tap the plus (**+**) icon to add a place.
2. Set the **Type** to Protege X.
3. To enable **Push Notifications**, drag the slider across.

    For more information, see Push Notifications (page 21).

4. Tap **SAVE**.
5. If you enabled push notifications, the **Disclaimer** page will load. Read the disclaimer and tap **ACCEPT** to continue.
6. The Protege X sign in page will load. You need to sign in with your operator account for the place you want to add. Enter your Protege X account **Email Address** and **Password**, then tap **Sign In**.
7. The authentication page will prompt you to Enter the verification code from your authenticator app.
8. Open your authenticator app. The code for your authenticated account will be displayed. Copy and paste or manually enter your code on the Protege X authentication page, then tap **Verify**.

    New random codes are generated every 30-60 seconds, depending on the app. If you take too long to enter the code it will refresh and no longer be valid.

9. Once signed in, if you have access to multiple Protege X places you will see the prompt **Select Place**.

    Your permissions in the mobile app correspond to your operator role for the selected Protege X place. You will only be able to perform functions on the app that your operator has access to in Protege X.

10. If you enabled push notifications, the **Select Controller** page will load. Select the controller to receive push notifications from, then tap **OK**.

    A service called PUSH - DO NOT TOUCH will automatically be created in Protege X for the selected controller. This service will send push notifications to any app accounts that connect to that controller.

    If this service already exists for the selected controller, the app will connect to the existing service instead.

    - Each Protege X place currently supports receiving push notifications from one controller only.

      This functionality will be expanded in future releases.

    - A controller's push service can only be connected to each user's app account once. This includes adding the controller in a Protege X place and adding the same controller in a Protege WX place.

      If you attempt to configure push notifications for a controller that is already connected in your mobile app places you will see **Error**: Same place is already registered on this account.

    - If you disable push notifications for the place, or delete the place from your mobile app, the service will **not** be disabled or deleted from Protege X as it may be in use by other accounts.

Once your Protege X place is configured it will appear in your My Places list and can be accessed any time you log in to the Mobile App. When you have Protege X places in your list, any time you log in to the Mobile App you will also need to sign in to Protege X with two-factor authentication as part of the cloud security requirements.

Protege WX and Protege GX

If you are a manager or system administrator you can add a place in the app to control your Protege site, using your Protege WX or Protege GX operator login.

1. From the main menu, select **My Places** and tap the plus (**+**) icon to add a place.

2. Set the **Type** to Protege GX/Protege WX.

3. Enter a **Name** for your place. This would typically be the site name.

4. Enter the **External Address** of the Protege system that you are connecting the app to.

   This is the URL that you use to access your system from outside the site's WiFi coverage. It is strongly recommended that you use the HTTPS address to achieve a secure connection.

   - Protege WX: The URL used to access Protege WX.
   - Protege GX: The URL used to access the Protege GX Web Client from outside of your building's network.

5. Enter the **Internal Address** of the Protege system that you are connecting the app to.

   This is the URL that you use to access your system on site, usually through WiFi. It is strongly recommended that you use the HTTPS address to achieve a secure connection.

6. Enter your operator login **Username** and **Password** that you use when accessing your Protege system.

   Your permissions in the mobile app correspond to your operator role and security levels for the Protege site. You will only be able to perform functions on the app that your operator has access to on the system.

7. To enable **Push Notifications**, drag the slider across.

   For more information, see Push Notifications (page 21).

8. Tap **Save**.

9. One or more additional popups are displayed:
   - **Disclaimer**: If push notifications have been enabled, tap **Accept** to acknowledge that you have read and understood the terms of use.
   - **Site Name**: If you are connecting to Protege GX, select the place (site) that the mobile app will connect to.
   - **Push Notification Services**: If push notifications have been enabled, select one or more Report IP services that will send push notifications. This is only required for Protege GX (see page 21).

Once your place is configured it will appear in your My Places list and can be accessed any time you log in to the Mobile App.

Using the Advanced Menu

On each of the control pages you can toggle the **Advanced** menu by tapping the down arrow (▼) located in the top right corner. The Advanced menu enables you to:

- Switch between grid and list view
- Remove and add items from the home page of the place
- Re-order the records that display on the home page
- Use the search function

Switching Between List and Grid View

To toggle to the list view tap the list icon. To toggle back to the grid view tap the grid icon.

Removing and Adding Records on the Home Page

When you tap the home icon it will appear green, indicating that items can be added or removed.

Items that are already included on the home page will have a red icon displayed beside them, indicating that they can be removed. Items with a green icon are not currently displayed on the home page and can be added.

You can select multiple items to add or remove at the same time. When your selections are complete, tap the home icon to save your changes.

Re-ordering Home Page Records

To change the order that records appear in on the home page tap the exchange icon. The list re-order icon will be displayed beside the items to indicate that records can be re-ordered.

Press and drag the required records to the desired positions to re-position items within the list as required. When complete, tap the exchange icon again to save your changes.

Using the Search Function

To use the search function tap the search icon. Enter a keyword or phrase to narrow down the list. All records that match the search will be displayed. When complete, tap **X** to clear the search.

Operation

The Protege Mobile App offers the convenience of being able to control your system remotely and monitor events as they happen. This section outlines how to change the state of resources through manual commands and how to view and filter events.

Second Language Display

The mobile app supports the 'Second Language' name for Protege X and Protege GX records which have that option. When the device language is **not set to English** the app will check and use the **Name (second language)** field when displaying the record. If the second language field is blank it will default to the primary **Name** field.

Doors

1. From the **Doors** page you can change the state of a door (e.g. locked/unlocked) by tapping the record. This enables you to toggle the available door states, depending on the door's configuration.
2. To latch unlock the door, press and hold the record to trigger the state change.

Manual Commands

Tap the ellipsis [**...**] icon to open the manual commands menu for a door and apply manual commands.

- **Door Control**:
  - Lock
  - Unlock (temporarily activate the lock)
  - Unlock Latched (activate the lock and keep the door unlocked)
- **Door Lockdown**:
  - Allow Entry
  - Allow Exit
  - Allow Entry + Exit
  - Deny Entry + Exit
  - Clear (remove the lockdown from the door)

Areas

1. From the **Areas** page, tap an area to arm / disarm.
2. Once you've tapped the area, it goes into exit / entry delay.
3. Once the delay time has elapsed, the area arms / disarms.
4. If the programming allows, you can force arm the area by pressing and holding the record.

Manual Commands

Tap the ellipsis [**...**] icon to open the manual commands menu for an area and apply manual commands.

- **Disarm**:
  - Disarm (disarm the main portion of the area)
  - Disarm 24 (disarm the 24HR portion of the area)
- **Arm**:
  - Arm (arm both the main and 24HR portions of the area)
  - Force Arm (force arm the main portion of the area)
  - Arm Stay (stay arm the main portion of the area)

- Arm Instant (instantly arm the main portion of the area and disable the entry delay)
- Force Arm Instant (instantly force arm the main portion of the area and disable the entry delay)
- Arm 24 (arm the 24HR portion of the area)
- Walk Test Enable (arm the area for a walk test)
- Walk Test Disable (disarm the area to end the walk test)
- Silence Alarm (silence the alarm and disarm the area)

Sensors

1. The **Sensors** page allows you to view the status and bypass or remove the bypass from an input.
2. If the programming allows, press and hold a record to latch bypass the input.

Manual Commands

Tap the ellipsis [**...**] icon to open the manual commands menu for an input and apply manual commands.

- **Bypass**:
    - Remove (remove any bypass from the input)
    - Until Next Disarm (bypass the input until an area assigned to the input is disarmed)
    - Permanently (bypass the input permanently so it is always ignored by area arming)

Controls

1. From the **Controls** page, tap the outputs to turn them on / off.
2. To activate the outputs for a defined period, press and hold the record.
3. Select the activation time by scrolling the **hours/mins/secs** counters, then tap **ACTIVATE TIMED** to apply.

Manual Commands

Tap the ellipsis [**...**] icon to open the manual commands menu for an output and apply manual commands.

- **Control**:
    - Deactivate
    - Activate
    - Activate For Time (activate the output for the time entered in the window). Select the activation time by scrolling the **hours/mins/secs** counters, then tap **ACTIVATE TIMED** to apply.

Events

1. To view live events, open the main menu and tap **Events**.
2. From the Events view you can scroll through the displayed events.
3. To easily search the events using keywords, tap the filter icon in the top right corner.
4. The events are displayed automatically and filtered as you type.
5. When finished, tap **Done** to clear the filter.

Cameras

The Protege Mobile App supports the monitoring of IP cameras that allow direct URL access to either a static JPG image feed or a streaming MJPG video feed.

Adding a Camera

1. Open the main menu and tap **Cameras**.

2. Enter a **Name** to identify the camera.

3. Set the **Display Options** for the camera. Choose between **Display RTSP Stream** for a video feed and **Refresh Static JPG** for images.

4. Enter the **External Address** of the camera stream.

   This is the URL that you use to access your system from outside the site's WiFi coverage.

5. Enter the **Internal Address** of the camera stream.

   This is the URL that you use to access your system on site, usually through WiFi.

6. If the Refresh Static JPG Display option is selected, set the **Image Refresh Rate**. This defines how often the image is refreshed in the app.

7. If the camera requires authentication, enable the **Use Authentication** option, then enter the **Username** and **Password** that you use to access the camera.

8. Tap **Save**.

To edit camera settings, go to the cameras list and tap the edit icon to the right of the list. From here you can also delete the camera if required.

Viewing Cameras

1. Navigate to the **Home** page or the **Cameras** menu and locate the camera.

2. Tap the camera to view the feed.

3. The live feed is displayed. When finished, tap **Close** to return to the home page.

Push Notifications

The Protege Mobile App enables you to subscribe to push notifications that send alerts for system and sensor activity. These notifications are displayed locally on your device and allow you to know when the system is disarmed at the start of the day, armed when everyone goes home, and when any alarms are triggered.

Push notifications for the mobile app are generated by a specially configured reporting service.

- **Protege X**: The reporting service is created automatically when the option is enabled in the app.

  The service is limited to reporting from one controller in each place. If your place has multiple controllers you will only receive notifications for objects and activity associated with the selected controller. This is a known current limitation of the push notifications reporting service.

- **Protege WX**: The reporting service is created automatically when the option is enabled in the app and associated with all areas in your system. You cannot choose which areas to report on.
- **Protege GX**: Refer to Application Note 201: Protege GX Push Notification Setup, available on the ICT Website.

Push notifications can be enabled on the app when creating or editing your place.

Push Notification Language

For the following languages, push notifications are sent in the language that is set in the mobile device's language settings:

- French (fr)
- Spanish (es)

All other languages will currently be sent in English. This will be expanded in future releases.

There is currently a known issue where push notifications are sent in French when the device language is set to Estonian (et), Greek (el), Italian (it), Polish (pl) or Russian (ru). This will be addressed in a coming release.

SIP

The Protege Mobile App allows you to configure your smartphone or mobile device for communication with any SIP enabled device.

- The registration status is displayed.
  - If the registration is successful, **Online** will be displayed.
  - If registration is unsuccessful, **Offline** will be displayed.
- **SIP IP**: Enter the SIP server's IP address.
- **Account**: Enter the account name of the SIP extension that has been allocated by the SIP system.
- **Password**: Enter the password for the SIP extension that has been allocated by the SIP system.
- **Realm**: Enter the security domain where this account is valid.
- **Port**: The proxy server port. This is usually 5060.

Entry Station Operation

The Protege Mobile App is able to receive SIP calls from a Protege Vandal Resistant Touchscreen Entry Station. A user who is listed in the entry station's directory can accept video calls from the entry station and open a linked door, all conveniently from their mobile device.

Both the mobile app (see previous page) and the entry station must have a SIP account configured. Contact your installer to determine the configuration of your entry station.

iOS SIP Operation

iOS call handling allows the mobile app to present the system call screen when an incoming call arrives to the device. However the user must answer the call before they can use the video or door unlock functions.

Call Handling - Lock Screen

When an incoming call is received while the device is **locked**, the standard call interface is displayed. The user must **slide to answer** the incoming call.
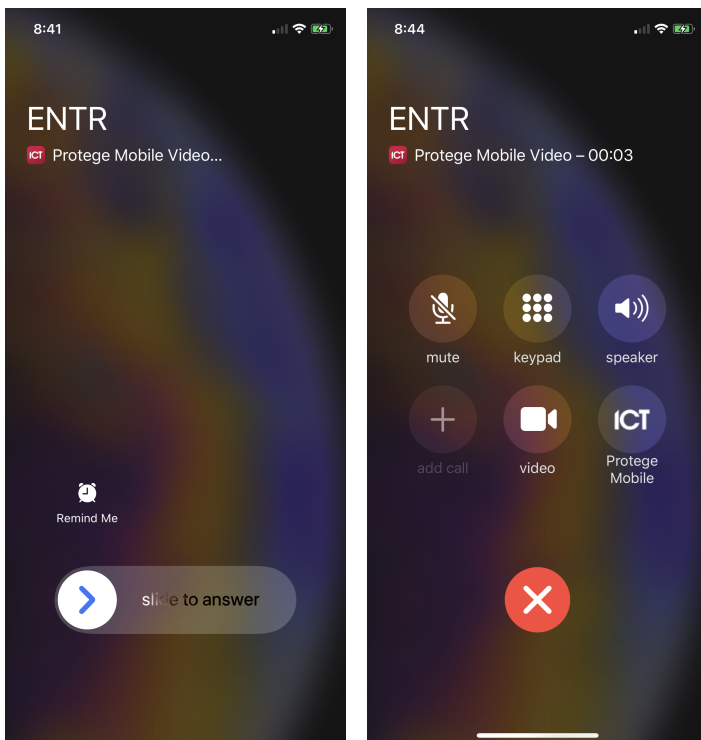
When the call is answered from the lock screen, the **answered call screen** is displayed and call audio is available.

To **unlock the door** from the answered call screen, press the **keypad** key, then press the ***** key.
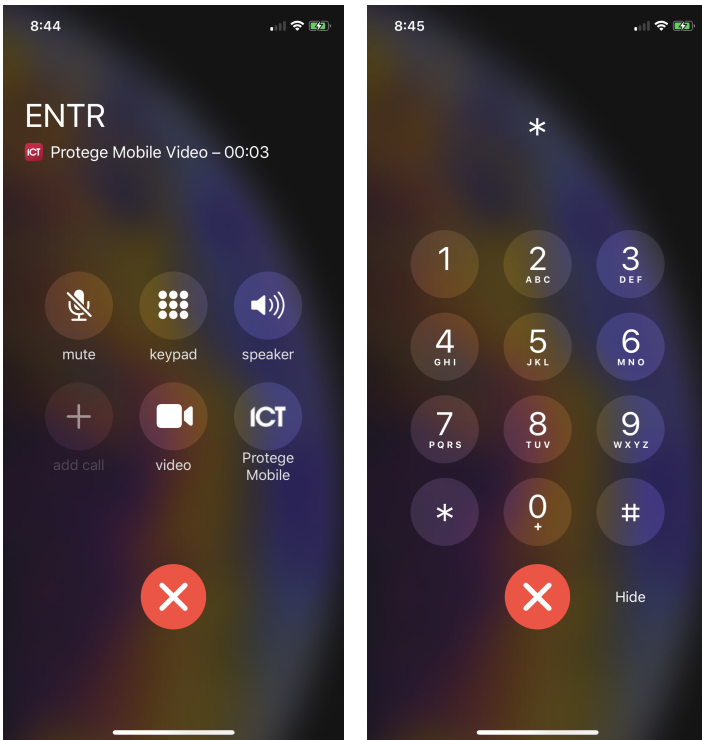
To view the video feed, press either the **video** or **Protege Mobile** button, then unlock the mobile device. This will launch the app and the **in app call screen** will be displayed.
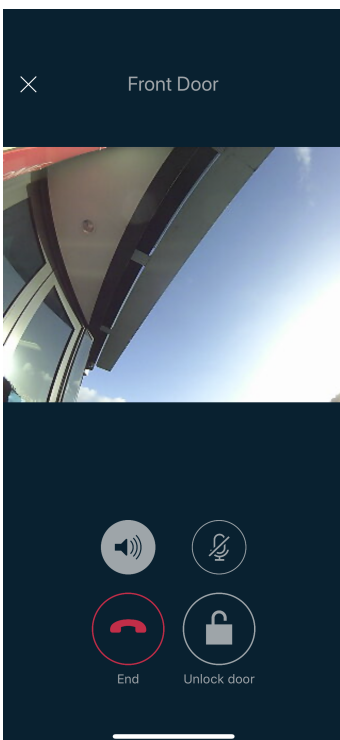
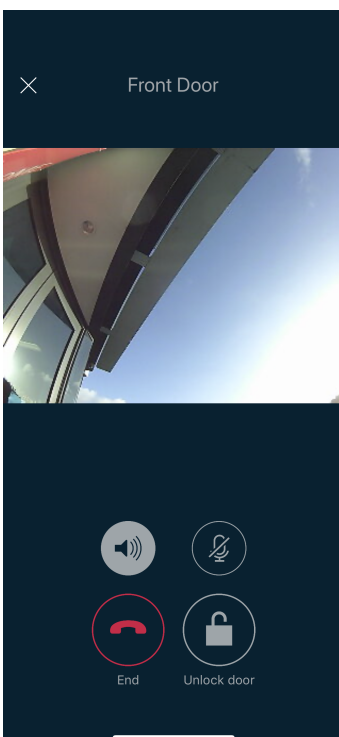To unlock the door from the **in app call screen**, press the **Unlock door** key.

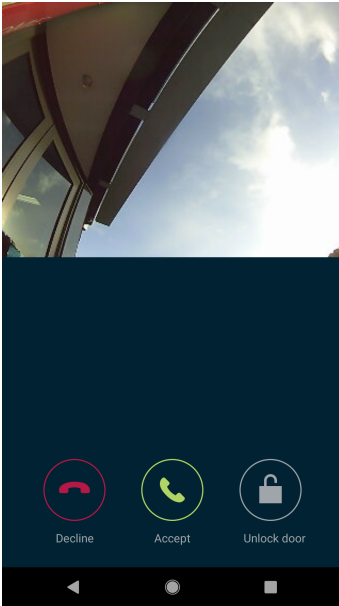## Call Handling - Home Screen or In App

When an incoming call is received while the device is **unlocked** the incoming call screen is displayed, and the user can **Accept** or **Decline** the incoming call.
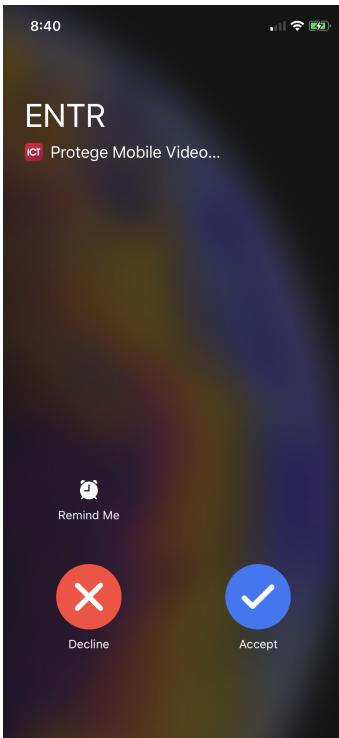
When the call is answered from the **home screen**, the app will launch and display the **in app call screen**, showing the video feed immediately.

To unlock the door from the **in app call screen**, press the **Unlock door** key.

Android SIP Operation

Android uses a custom call screen and notifications to manage incoming calls.

In order to start the app when it is closed and receive video, push notifications must be enabled for the app. When you install and run the app for the first time you will be prompted to enable push notifications. Alternatively, you can enable notifications from the Android settings on the device at any time after.

Call Handling - Lock Screen

When an incoming call is received while the device is **locked** or the Protege Mobile App **is open and in the foreground**, the **in app call screen** will be displayed.

This screen displays the video feed. You can **Accept** or **Decline** the call, or unlock the door by pressing the **Unlock door** key.
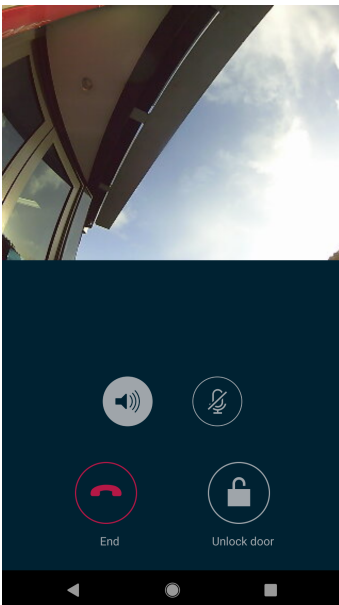
Accepting the call will display the **answered call screen**, which provides additional options to mute the call or enable the loudspeaker.

Call Handling - Home Screen or In App

When an incoming call is received while the device is **unlocked** and the Protege Mobile App **is not in the foreground**, a notification will be displayed alerting the user to the incoming call.
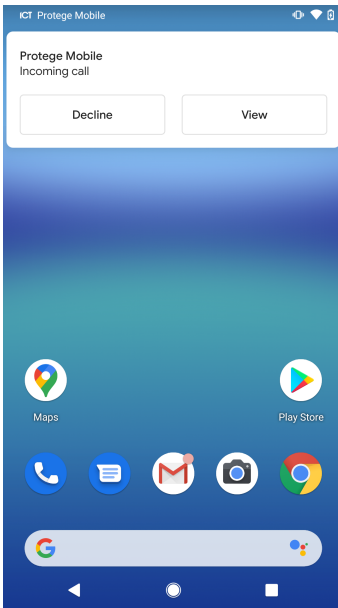
The user can **Decline** or **View** the incoming call.

Choosing to **View** the call will launch the app and display the **in app call screen**, including the live video feed, where the user can **Accept** or **Decline** the call.
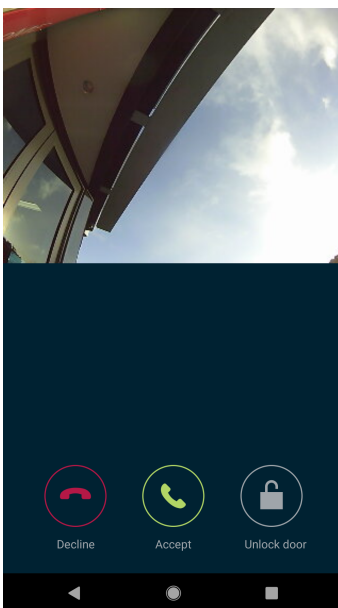
To unlock the door from the **in app call screen**, press the **Unlock door** key.

Disclaimer and Warranty

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.

For warranty information, see our Standard Product Warranty.