Protege Access+

Setup Guide

Last Published: 19-Mar-26 2:58 PM

Contents

Introduction

Protege Access+ empowers end users to access, monitor and control their buildings from their smartphones. With this convenient mobile app, you can:

- Unlock doors using a unique mobile credential via **Bluetooth® wireless technology** or NFC (Near Field Communication). Organizations can add branding to their mobile credentials, providing an opportunity to connect with employees, customers and residents.
- Connect to your Protege GX organization, allowing you to monitor and control your doors, areas, sensors and devices on the go.
- View live events and active alarms, and run reports on historical events.
- Receive push notifications when something happens on site.
- Receive video/audio calls from entry stations and intercoms.

Protege Access+ is available to install from the Apple App Store or Google Play Store.

This guide describes how to issue and assign mobile credentials, connect the mobile app to an organization and enable SIP calling. It is intended for installers and system administrators, providing you with the information you need to set end users up with the app.

Supported Mobile Devices

The Access+ app is supported on the following mobile device operating systems:

Operating System	Minimum Version	Notes
Android	11	
Apple iOS	17	Not supported on iPad. Apple devices do not support sending credentials over NFC.

Permissions

The following device permissions are required to operate the Protege Access+ app.

Some permissions have different names depending on the operating system version.

Android

Permission	Relevant Feature	Reason for Permission
Full Screen Intent	SIP Calling	Allows incoming calls to display on the full screen. Only required for some versions of Android.
Nearby Devices or Location	Mobile Credentials	Allows the app to find nearby card readers and transmit your Bluetooth® credential. On older Android versions, apps must request location permissions to use Bluetooth® functionality. ICT does not store your location.
Notifications	Push Notifications SIP Calling	Allows the app to display push notifications and incoming calls.
Microphone or Record Audio	SIP Calling	Allows the app to use your microphone for calls. ICT does not store audio recordings.

Apple iOS

Permission	Relevant Feature	Reason for Permission
Find Bluetooth Devices	Mobile Credentials	Allows the app to find nearby card readers and transmit your Bluetooth® credential. ICT does not store your location.
Notifications	Push Notifications SIP Calling	Allows the app to display push notifications and incoming calls.
Microphone	SIP Calling	Allows the app to use your microphone for calls. ICT does not store audio recordings.

Privacy and Data Management

Protege Access+ is subject to the ICT Privacy Policy: www.ict.co/privacy-policy

If you wish to delete your app account and all associated data, navigate to **Profile**, then **Account details**. Select **Delete account**.

When you delete your account, all of your mobile credentials are permanently disabled. If you want to use Protege Access+ again in future, you will need to request a new mobile credential from your building administrator.

Accessibility

Protege Access+ is designed to be compliant with WCAG 2.2 AA standards.

In addition, Protege Access+ supports the following screen readers for visually-impaired users:

- iPhone VoiceOver (see the iPhone documentation for more information and instructions)
- Android TalkBack (see the Android documentation for more information and instructions)

Limitations

Protege Access+ offers significant performance improvements over the previous Protege Mobile App and a slick new user interface. However, the app is still in development and not all features of the previous app are currently available.

- Protege Access+ does not support connecting to Protege WX or Protege X organizations for monitoring and control. However, you can still use mobile credentials in these systems.
- Currently you cannot limit the number of devices that a credential can be installed on. However, only one device can be logged in to an account at the same time, limiting the risk of credential sharing.
- The Protege Mobile App provided limited support for IP cameras. This is not available in Protege Access+, but improved video capabilities will be included in future.

ICT is actively developing Protege Access+. Get in touch with your ICT representative to share feedback and learn about upcoming features and improvements.

Known Issues

ICT would like to make you aware of the following known issues in the current version of the mobile app:

- On a site with more than one controller sending push notifications, it is currently not possible to select which controller you will receive the notifications from.

- Currently, users may be logged out of the app when they travel outside the region where they originally made their account (e.g. traveling from Australia to Canada). To work around this, create a new account using the same email address in the new region. You will have access to the same badges and you will be able to connect to your Protege GX server again.

  You may need to update your network configuration to accept connections from the new region. For more information, see Networking Requirements (page 13).

Transitioning from the Previous App

If your sites are using the previous Protege Mobile App, we recommend transitioning users to Protege Access+. This lets them take advantage of performance improvements and new features in the latest app.

This section covers what you need to know to help users transition from the Protege Mobile App to Protege Access+.

Creating an Account

In most cases it is simple for existing Protege Mobile App users to transition to Protege Access+. Simply download Protege Access+ from the Apple App Store or Google Play Store, then open the app and create a new account.

There are minor differences in the process depending on how the user originally made their account in Protege Mobile:

- **Signed up with Email**: The user can create a new account with the same email address. Their existing mobile credentials will be available in Protege Access+.
- **Signed up with Google**: Login with Google is no longer available, but the user can create a new account using the same email address (e.g. yourname@gmail.com). Their existing mobile credentials will be available in Protege Access+.
- **Signed up with Facebook**: Login with Facebook is no longer available and it is not possible to transition existing mobile credentials to the new account. Contact ICT Customer Services, who will issue a new mobile credential free of charge.

Once Protege Access+ is set up, the user can uninstall the Protege Mobile App from their device.

Protege GX Connection

To connect Protege Access+ to a Protege GX site, **the Protege GX SOAP service must be accessible over the internet**.

This is different from the previous mobile app, which connected to the Protege GX web client. It is no longer possible to connect over the local network.

For more information, see Networking Requirements (page 13).

SIP Settings

If the user had an existing SIP account created by the Protege Tenancy Portal, the details will be filled in automatically. If the user had a third-party SIP account, they must enter the settings to connect to it (see page 20).

Mobile Credentials

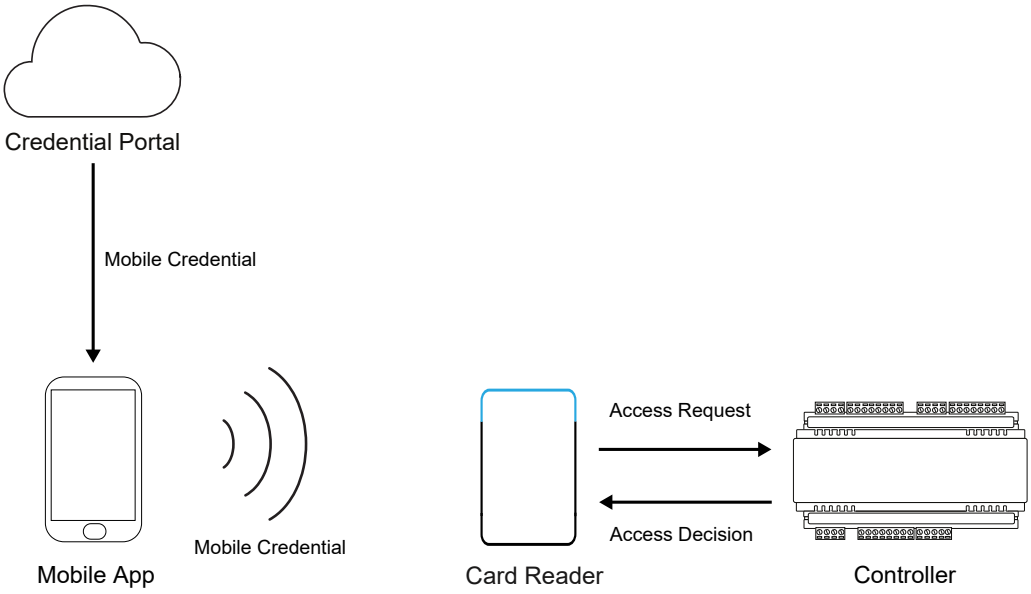
ICT mobile credentials provide door access at ICT card readers and wireless locks, replacing traditional access cards.

How It Works

The installer or administrator purchases mobile credentials from ICT. Administrators issue credentials to employees, residents or customers using their email addresses. They also enter the credential details on the user record in the Protege system.

The user receives an email inviting them to install Protege Access+ and create an account. When the user logs in, the app retrieves the credential from the credential portal and saves it to their device.

The user can now badge their mobile device at a card reader or tap the **Unlock Door** button. The Protege controller evaluates the user's access permissions and grants or denies access.



Prerequisites

One mobile credential is needed for each app account that will be used for access (see Issuing Mobile Credentials). The order code is: PRX-MCR.

ICT mobile credentials can be used in any Protege GX, Protege WX or Protege X system.

All ICT card readers with Bluetooth® Wireless Technology support mobile credentials. This includes:

- All TSL readers.
- All Protege wireless locks
- All tSec readers with **-BT** in the product code (e.g. PRX-TSEC-STD-BT-B).

ICT mobile credentials cannot be used with third-party card readers.

Issuing Mobile Credentials

Mobile credentials can be issued to users by company operators in the Protege Mobile Credential Management Portal.

When someone assigns you credentials you can issue, you will receive an email inviting you to create an account on the portal. Once you have an account, you can issue credentials to users as follows:

1. Web browse to https://wirelesscredentials.com
2. Log in with your email address and password.
3. On the **Mobile Credentials** page you can view the mobile credentials assigned to you. Select a credential with the correct **Credential Profile** (usually the company or building name).
4. Click **Issue Credential**.
5. Enter the user's email address.
6. Click **Enter**.
7. Make a note of the **Credential** details for assignment in the Protege system.

The user will now receive an email inviting them to install Protege Access+ and create an account.

For more information about assigning and issuing credentials, see the Protege Mobile Credential Management Portal User Guide.

Branded Mobile Credentials

Optionally, you can apply company branding to the mobile credential profile. This lets you display your company name, logo and other branding on the Badges page.

To set up company branding:

1. Web browse to https://wirelesscredentials.com
2. Log in with your email address and password.
3. Navigate to the **Credential Profiles** section.
4. Select the **Credential Profile** you wish to add branding to.
5. Configure the following settings to design the branded badge:
   - **Logo image**: Upload a PNG image (maximum size 1024 × 1024px, 200kb). For best results, use a square image with a transparent background.
   - Select either a **Background image** or a **Background color**.

     To use a background image, upload a JPG or PNG image (maximum size 1024 × 768px, 500kb). For best results, use a 4:3 aspect ratio.
   - **Overlay text**: This text is displayed in the title bar for the badge in white.

     This is typically the company's name or address. If no text is written here, the badge will display the name of the credential profile.
6. Click **Update Credential Branding**.

Assigning Mobile Credentials in Protege

You must also assign the mobile credential to a user in the Protege system to allow them to use it for access.

You will need the facility number and card number for the mobile credential, which you can find in the mobile credential management portal or the **Badges** page in Protege Access+ (**Settings** menu).

The credential details are displayed in the format FacilityNumber:CardNumber (e.g. 100:20494).

Assigning Credentials in Protege GX

1. Launch and log in to the Protege GX client.
2. Navigate to **Users | Users** and select the user to assign the credential to.
3. In the **Card numbers** section, enter **Facility number** and **Card number**.
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.

Assigning Credentials in Protege WX

1. Launch and log in to the Protege WX web interface.
2. Navigate to **Users | Users** and select the user to assign the credential to.
3. In the **Access Cards** section, enter the **Facility Number** and **Card Number**.
4. Click **Save**.

Assigning 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 enter the **Facility Number** and **Card Number**.
5. Click **Save**.

Using Mobile Credentials

When the credential is issued, you will receive an email inviting you to install Protege Access+. Download the app from the Google Play Store or Apple App Store and create a new account using the **email address** where you received the invitation.

You will need an internet connection the first time you log in to the mobile app to download your credential. After you have logged in, the mobile credential will remain valid on your device for up to a month even when you are not connected to the internet.

The credential is displayed on the **Badges** page. If you have more than one badge, you can swipe left and right to switch between them.

The credential is linked to the account's email address, not the device the app is installed on. If you change your phone, simply install the app and log in on the new phone.

Only one device can be logged in to the account at a time.

Unlocking Doors

There are three ways to unlock doors with Protege Access+:

- **Unlock nearest door**: Tap the button to unlock the nearest door using Bluetooth® Wireless Technology.
- **Proximity unlock**: Hold your phone near a card reader to unlock the door using Bluetooth® Wireless Technology. This enables you to unlock doors quickly without unlocking your phone, but uses more battery life as the phone is constantly scanning for nearby readers.

  You can enable or disable this feature in the **Settings**.

  Adjust the **Distance to unlock** until you find a distance that works for you. This can vary depending on the reader configuration, location and other factors.
- **NFC unlock**: Unlock doors using NFC (Near Field Communication) by holding the phone close to a card reader. NFC has a range of a few centimeters/inches.

  Only available on Android devices.

You can use the credential whenever the app is running, even when your phone is locked or the app is minimized.

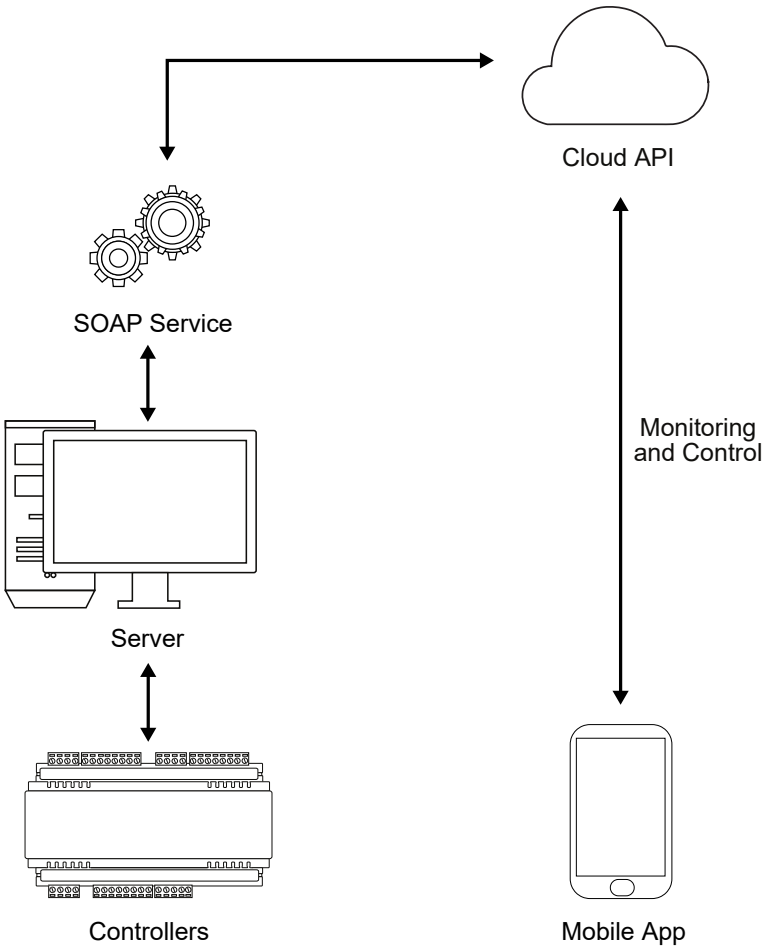
Connecting to Protege GX

Protege Access+ can connect to Protege GX organizations, enabling users to:

- View and search events and alarms.
- Monitor device status.
- Receive push notifications about area alarms and activity.
- Lock, unlock and lock down doors.
- Arm and disarm areas.
- Control outputs and bypass sensors.

How It Works

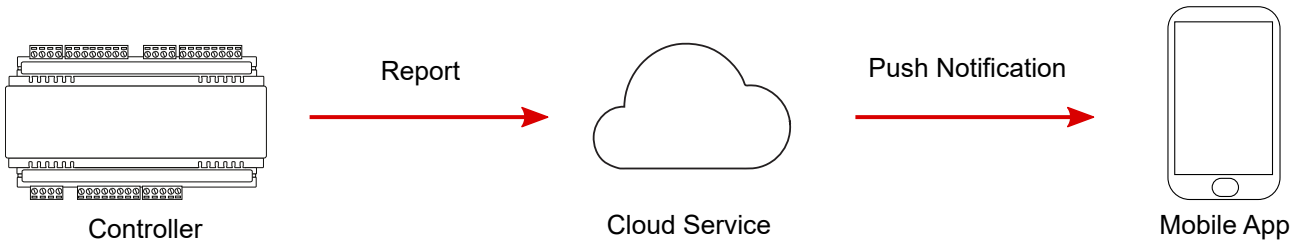
When you set up an organization in Protege Access+, the app connects to the Protege API (Application Programming Interface), which sits in the cloud. The Protege API in turn connects to the Protege GX system via the Protege GX SOAP Service, using your Protege GX operator credentials.



When you connect to the organization, you also have the option to enable push notifications.

Push notifications use a special Report IP service that is hosted on the controller. The reporting service monitors one or more areas. When a reportable event such as an alarm occurs, the controller sends the report to the ICT cloud service, which then sends out notifications to Protege Access+ accounts.

For push notifications to function, the controller must have access to the internet to report out to the push notification service.



Prerequisites

Component	Version
Protege GX	4.3.352 or higher
Protege GX SOAP Service	1.6.0.11 or higher

You can connect to an organization even if you do not have a mobile credential.

Networking Requirements

The mobile device must have internet access at all times to use the monitoring and control functions.

Protege GX SOAP Service

The Protege cloud API connects to the Protege GX SOAP service using HTTPS. The SOAP HTTPS endpoint (port 8040 by default) must be accessible over the internet via a fixed hostname or IP address.

Specifically, the network must allow inbound traffic from the cloud API to the SOAP service. You must permit traffic from the following endpoints:

- 20.153.190.26
- 20.157.220.85

There are a few ways to make SOAP accessible over the internet:

- The recommended method is to use a VPN service to create a secure tunnel to your SOAP endpoint. For example, Cloudflare Zero Trust enables you to create a tunnel. When setting up a Cloudflare tunnel, use the following settings:
  - **Service Type**: HTTPS
  - **URL**: IP address and HTTPS port used by the SOAP service (e.g. 192.168.1.2:8040)
  - **No TLS Verify**: Enabled
- Alternatively, use port forwarding to expose the HTTPS port of the SOAP service. Ensure that you have a domain name or static IP address available for the computer that SOAP is installed on.

You can check that the SOAP service is accessible by entering the following into a web browser:

https://your.domain.name:8040/ProtegeGXSOAPService/service.svc

End users must have the **domain name or IP address** when they are setting up their organization.

Push Notifications

Push notifications are generated by the controllers using a Report IP service. To send push notifications, the controllers must be able to report out over port **10105**. To ensure that the controller can report out:

1. Log in to the controller's web interface.
2. Navigate to **Settings | Adaptor - Onboard Ethernet**.
3. Set the **Subnet Mask** and **Default Gateway** as required for the network switch.

Typically you do not need to configure the firewall unless it is blocking outbound connections on this port.

Setting up Push Notifications

Some additional configuration is required in Protege GX before any app user can enable push notifications.

Creating the Report IP Service

Push notifications use a specially configured Report IP service:

1. Navigate to **Programming | Services**.
2. Select the **Controller** that will host this service in the toolbar.
3. Click **Add**.
4. For the service **Name** enter **PUSH - DO NOT TOUCH**.

   The service name must be entered **exactly** as above.
5. Set the **Service type** to Report IP.
6. Set the **Service mode** to 1 - Start with controller OS.
7. Select the **General** tab.
8. Set the **Client code** to the last six characters of the controller that the service is hosted by. For example, if the controller's serial number is C29E2FDA, the client code is 9E2FDA.
9. Set the **Reporting protocol** to Armor IP (TCP) encrypted.
10. Set the **Encryption level** to AES 256 bit.
11. Generate the 32-character encryption key at https://www.ict.co/Key-Generator. On the Key Generator page, click **Generate key**, then copy the resulting code and paste it into the **Encryption key** field.
12. Set the **IP address / Host name** to **40.86.94.33**.
13. Set the **IP port number** to **10105**.
14. Select the **Options** tab and enable the types of events you want to report:
    - Report open
    - Report close
    - Report alarms
    - Report tampers
    - Report restore
    - Report bypass
15. Click **Save**.
16. Right click on the service and select **Start service**.

Configuring the Areas

The reporting service must be assigned to all the areas that you wish to receive push notifications for, similar to a normal IP reporting service.

1. Navigate to **Programming | Areas** and select the area to enable push notifications for.
2. Select the **Configuration** tab and scroll down to the **Reporting services** section.
3. Click **Add** and select the **PUSH - DO NOT TOUCH** service, then click **OK**.
4. Click **Save**.

Operator Permissions

Protege Access+ uses Protege GX operator permissions to determine what the user is allowed to see and do in the app.

The operator will need some or all of the permissions outlined in the table below. You can program these using only a role, or using a security level as well for more granularity.

Feature	Role Table	Security Level Tables	Permission Required
Device Status	Controller programming windows	Areas Doors Inputs Outputs	Grant read only access
Control Devices	Manual commands	Area control commands Door control commands Output control commands Input control	Grant full access
Push Notifications	Controller programming windows	Controllers Services	Grant read only access

You can also use record groups to restrict which devices the user can see in the app.

For more information about using roles, security levels and record groups, see Application Note 191: Programming Operator Roles in Protege GX.

Creating a Role

As an example, we will create a basic role based on the end user preset, with additional access rights to allow them to monitor the site in Protege Access+.

1. In Protege GX, navigate to **Global | Roles**.
2. Add a new role with a descriptive name (e.g. Protege Access+ Operator).
3. Set the **Preset** to End User. This gives access to view and edit users, access levels, event reports and some additional functionality.
4. In the **Tables** tab, enable the following permissions:
   - **Controller programming windows**: Grant read only access
   - **Manual commands**: Grant full access
5. Click **Save**.
6. In **Global | Operators**, select an operator or add a new one. Assign the **Role**.

This operator will have access to view the status of areas, doors, inputs and outputs in the app, and send them manual commands. They will also be able to view events and receive push notifications.

Restricting Door Manual Commands

In some situations you may need to grant a user access to unlock doors, but not to perform advanced latch unlock and lockdown commands. For example, residents and visitors may be permitted to unlock a carpark gate, but they should not leave it open indefinitely.

To restrict manual commands:

1. In **Global | Roles**, select the role.
2. At the end of the **Name**, add the following text:
   `_RestrictMC`
3. Click **Save**.

All roles that end with this text will restrict the user's access in Protege Access+ so that they can only temporarily unlock or lock doors.

This feature does not restrict the user's access in the Protege GX client or web client.

Connecting to the Organization

To connect the app to Protege GX:

1. In the app, navigate to **Organizations**.
2. Tap the **+** button in the top right.
3. Enter the following details:
   - **Protocol**: https
   - **Domain or IP**: Enter the domain name or IP address used to connect to your SOAP server over the internet. Ask your system administrator if you do not know this.
   - **Port**: The IP port used to connect to the SOAP service. This is typically 8040.
   - **Path to Service.svc**: The path to the service.svc file on your SOAP server. You can usually leave this as the default setting.
   - **Username**: Your Protege GX operator username.
   - **Password**: Your Protege GX operator password.
4. Tap **Next**.
5. Tap **Select Organization** and select the Protege GX site you wish to connect to.

   If no organizations are available, confirm that your SOAP endpoint, username and password were typed correctly.
6. You can optionally link your organization to a badge, allowing you to take quick actions from the **Badges** screen. Tap **Show on badge** and select the badge you will link this organization to.
7. Tap **Next**.
8. Enable or disable **Push Notifications**.
9. Tap **Add Organization**.

Viewing and Controlling Your Organization

Once you have connected to your organization, tap on it to access the reporting, monitoring and control features.

Issues Requiring Attention

This section displays issues that are currently affecting the Protege GX system.

- **Controllers offline**: Displays whether there are any controllers currently offline with Protege GX. Offline controllers will continue to operate access, security and automation functions as normal. However, they will not send events, respond to controls or receive programming changes.

  Tap the tile to see which controllers are offline.
- **Health Status**: Displays the number of health status issues currently affecting the system. Common issues include offline modules, configuration errors and disabled functions.

  It is not possible to view the health status messages in the app. To view them, log in to the Protege GX client and navigate to **Sites | Controllers**. Right click on each controller record and select **Get health status**.
- **Alarms**: Displays the number of areas currently in alarm. Alarms may be caused by intruders, panic buttons, doors left open, system troubles and other incidents. Tap the tile to see which areas are in alarm.

Events

The **Events** page displays the **most recent 200 events** recorded by Protege GX. Use the search bar to search for specific people, doors, areas or other records within the last 200 events.

Reports

On the **Reports** page you can run event reports that have been set up in Protege GX. This is useful for investigating past events, including specific incidents such as alarms.

You can create event reports in the Protege GX software, under **Reports | Setup | Event**.

Controls

The **Controls** page displays the current status of areas, doors, sensors (inputs) and controls (outputs).

To control devices, tap on the device and select the control command you wish to send. For example, you can arm and disarm areas or lock and unlock doors.

Be aware that some commands may fail to complete successfully. For example, an area might fail to arm if there is still someone inside. Check the **Events** page to see the progress of your control.

Tap the ★ button to add devices to your favorites for quick access.

Organization Settings

To edit the settings for your organization:

1. Navigate to the **Organizations** tab and select the organization.
2. Swipe from the bottom up so that the page expands to the full screen.
3. Tap the **Settings** icon ⚙ at the top left.

The available settings are:

- **Show on badge**: Select a badge to associate with this organization. This adds shortcuts for the organization to the **Badges** screen.
- **Push notifications**: Enable or disable push notifications for this organization.
- **Delete organization**: Delete this organization and all associated data from your device.

Troubleshooting

Cannot connect to Protege GX organization

The app is not able to reach the Protege GX server. There are several possible causes for this, including:

- **Connection details contain errors**
  First, check your connection details for typos. Correct any errors and try again.
- **Username or password is incorrect**
  Check that you can log in to the Protege GX client or web client with these credentials.
  If you have forgotten your password, ask a Protege GX administrator to set a new temporary password, then log in to Protege GX and set your permanent password. You can use the new password to set up your site in Protege Access+.
- **Password needs to be reset**
  Log in to Protege GX with your current password. When prompted, enter a new password. You can then use the new password to set up your site in Protege Access+.
- **Operator does not have access to this site**
  Log in to Protege GX and confirm that you have access. Ask an administrator to check that your operator record has the correct **Role** (see page 15).

- **SOAP domain name, IP address or port is incorrect**

  Check these details by entering the full URL into a web browser (e.g. https://your.domain.name:8040/ProtegeGXSOAPService/service.svc). If the URL is correct, you will see a page titled **Service1 Service**.

- **SOAP Service is not accessible over the internet**

  Repeat the previous test using a web browser that is on a different network from the Protege GX server. If this does not work, check the settings in your VPN tunnel or router (see page 13).

The organization was previously connected but now will not load controls or events. It displays the message "Internal Server Error".

If something in the system changes, you may lose access to a site that you were connected to. This has a number of possible causes, including:

- Your Protege GX username or password has changed.
- Your Protege GX password needs to be reset. Log in to Protege GX to change your password.
- The SOAP service endpoint has changed.
- The SOAP service endpoint is currently not accessible over the internet. Check that you have an internet connection and that the VPN tunnel or other network routing is active.

If you need to reset your credentials or SOAP service endpoint, you must delete the organization and add it again:

1. In the **Organizations** tab, open your organization.
2. Swipe from the bottom up to fullscreen the organization.
3. Tap the **Settings** icon ⚙ at the top left.
4. Select **Delete organization**.
5. Add the organization again (see page 17).

Receiving SIP Calls

Protege Access+ can receive audio and video calls from the Protege entry station. Users can unlock doors during the call using the **Unlock** button, enabling them to let visitors into the building.

Each user must have a SIP account to receive intercom calls. You can purchase and set up SIP accounts manually, or integrate with the Protege Tenancy Portal to automatically create a SIP account for each user. See the Protege Tenancy Portal User Guide for more information and instructions.

For integrating with a Protege entry station without the tenancy portal, see the Protege Vandal Resistant Touchscreen Entry Station Installation Manual.

Setting Up a SIP Account

If you are using the Protege Tenancy Portal, each user's SIP account will be populated automatically along with their mobile credential.

For other SIP accounts, the user must enter the details manually:

1. In the app, navigate to the **Profile** tab.
2. Select **Intercom**.
3. Enter the details for the SIP account:
   - **SIP server**: Enter the SIP server's hostname or 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.
4. Click **Save**.

Unlocking Doors from a Call

When a SIP call is sent from an entry station, the user will receive a call notification on their phone. The app will automatically start if it was not running when the call was placed.

After accepting the call, the user can press the **Unlock** button to unlock the door connected to the entry station.

You must have an internet connection to receive SIP calls.

Troubleshooting SIP Calls

Calls are not coming through to Protege Access+, or are audio only.

This may occur when Protege Access+ is not allowed to push notifications when a call is received. Ensure that notifications are turned on for Protege Access+ in the device's settings.

The app can receive calls, but the caller cannot hear the recipient.

Ensure that Protege Access+ has permission to access the phone's microphone (i.e. access to record audio).

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.