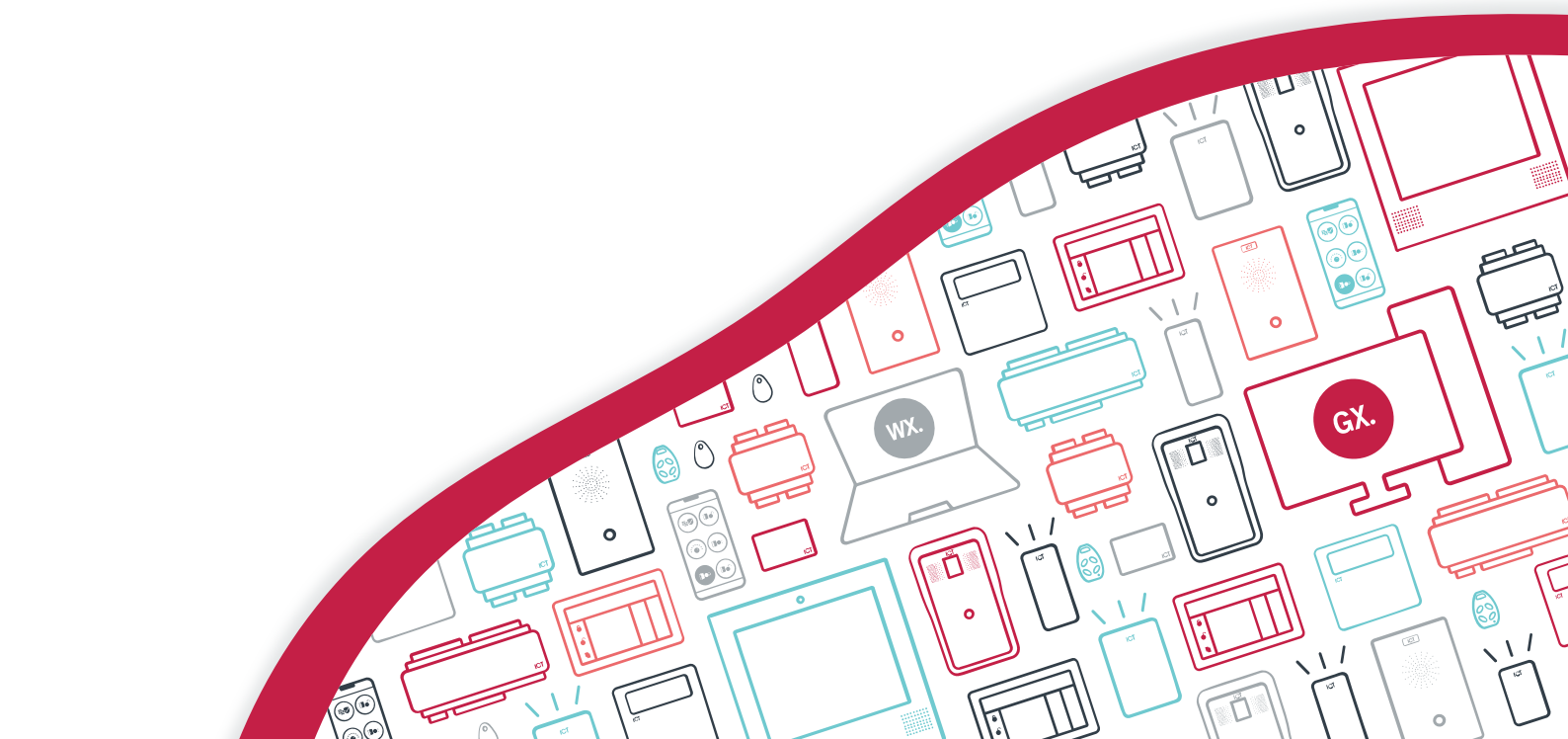
Protege Tenancy Portal

User Guide



Last Published: 01-May-24 11:08 AM

Contents

Introduction

The Protege Tenancy Portal is a convenient cloud service for managing contacts in the Protege Vandal Resistant Touchscreen Entry Station.

With Protege GX integration, user records programmed in Protege GX are synchronized to a phonebook in the tenancy portal. The portal automatically creates a SIP account and Protege Mobile App account for each user's email address, then downloads the phonebook to one or more entry stations. This allows visitors to video call a tenant on their Protege Mobile App, or voice call to a mobile phone or landline. The tenant can then unlock the front door from the call screen, creating a seamless entry experience.

Prerequisites

Tenancy Portal

To access the tenancy portal you must have a tenancy portal account. To obtain a tenancy portal account, contact ICT Customer Services. You can also be invited to the tenancy portal by a portal company operator.

Entry Station

For details on configuring the entry station's web, video and SIP settings, see the Programming the Entry Station section in the Protege Vandal Resistant Touchscreen Entry Station Installation Manual.

- The entry station must have internet access. For video calls, the entry station's JPEG video feed must be configured for access over the internet.
- Each entry station requires a SIP account provided by ICT, which must be configured in the entry station's web interface. For assistance obtaining and setting up your SIP account, contact ICT Support.
- Entry station firmware version 1.12.201 or higher.
- To unlock a door from the entry station, you must set up Protege GX entry station integration. Instructions are included in this guide (see page 22).

Mobile App

To receive video calls, users must have Protege Mobile App version 1.0.3.77 or higher.

Protege GX User Integration

To integrate the tenancy portal with Protege GX, the following prerequisites are required:

Software	Version	Notes
Protege GX	4.3.326.6 or higher	
Protege GX SOAP Service	1.6.0.6 or higher	Ensure that you know the endpoint address for the SOAP service. To achieve secure communications it is recommended to connect to the HTTPS endpoint. For installation and connection instructions, see the Protege GX SOAP Service Installation Manual.
Protege GX Tenancy Portal Synchronization Service	1.1.1.4 or higher	Instructions for installing the service are included in this guide (see page 14).
Microsoft .NET	4.8 or higher	

Licensing

The Protege Tenancy Portal is an annual subscription service.

License	Order Code	Notes
Protege Tenancy Portal VoIP Line Subscription	VOIP-TP-1L	1 per entry station.
Protege Tenancy Portal Apartment Subscription	VOIP-TP-50	1 per tenancy portal tenancy.
	VOIP-TP-125	
	VOIP-TP-250	

The Tenancy Portal

Tenancy Portal Terminology

The following terms, roles and records are used within the Protege Tenancy Portal.

Term	Description
Company	The business or organization which is administering records in the portal.
Company Operator	Assigned to a company. Has full access to maintain the records associated with the company they are assigned to, including adding and removing company operators.
Place	Corresponds to a physical site, such as an apartment building, which is assigned to and administered under the company.
Concierge	Assigned to a place. Has full access to maintain the records associated with the place they are assigned to, including adding and removing concierges.
Phonebook	The contact list and details for tenants in a place. Phonebooks can be exported or synchronized to the entry station directory.
Tenancy	Individual apartments or dwellings within the building. Tenancies can contain multiple tenants. Any number of tenancies can be included in a place.
Tenant	The individual contacts or people who live in the tenancies. All tenants assigned to tenancies within a place are included in its phonebook (unless opted out).

Logging in to the Tenancy Portal

When you are added as a Company Operator or Concierge you will receive an email detailing how to complete your tenancy portal account setup.

Once you complete the account setup you can then log in and start managing your Places and Tenancies.

1. You can access the Protege Tenancy Portal at https://wirelesscredentials.com/Tenancies.
2. On the Login screen, enter the email address associated with your portal account and your account password, then click **Login**.

If you forget your account password you can click **Forgot Password?** then on the next screen enter your email address and click **Send Reset Link** to send a password reset link to your email address.

Do not click the Create an Account option on the login screen. This is for used portal administration and will not provide the owner of the email address with access to the tenancy portal.

Changing Your Password

1. Log in to the Protege Tenancy Portal.
2. Open **Your Account** from the navigation pane.
3. Enter and confirm your New Password (minimum 6 characters).
4. Click **Change Password**.

When changing your account password, remember to update any configurations which also use this account for access, such as the Protege GX User Integration (see page 11).

Tenancy Portal Accounts & Roles

To access the tenancy portal you must have a tenancy portal account, which allows you to log in to the portal.

Once you are logged in to the portal the role or roles you are assigned to determine which records you are able to access. You need to be assigned to a role in a company or place in order to access records associated with that company or place. There are two roles which determine the levels of tenancy portal access.

- A **Company Operator** is assigned to a company, and can access and maintain the company, its places, tenancies and tenants.
- A **Concierge** is assigned to a place, and can access and maintain the place, its tenancies and tenants.

You can be assigned to unlimited concierge and company operator roles, however if using the Protege GX User Integration you should have company operator access to one company only (see page 11).

The table below outlines the access that these roles have within the portal.

- Full access to view, add, edit and delete records.
- Access to view and edit records only.
- No access to records.

Record	Company Operator	Concierge
Company	✓	✗
Company Operators	✓	✗
Places	✓	✓
Concierges	✓	✓
Phonebooks	✓	✓
Phonebook Contacts	✓	✓
Tenancies	✓	✓
Tenants	✓	✓

Using the Tenancy Portal

The primary function of the tenancy portal is to provide an integration with Protege GX to automatically generate phonebooks from user records. Adding and updating of places, phonebooks, tenancies and tenants is maintained through Protege GX, and records should not be altered directly in the portal as undesired results will occur.

However, if not using the Protege GX integration, tenants and related records can be added and maintained directly in the portal, enabling you to manually generate a phonebook for use in the entry station directory.

1. Log in to the Protege Tenancy Portal.
2. To assign a **Company Operator** to administer your company records:
   - Open the **Companies** window from the navigation pane.
   - In the **Company Operators** section, enter a valid **Email** address and click **Add Company Operator**.
     - The portal will process your request, then display Success. Company Operator Added.
     - The person will receive an email inviting them to log in to the portal.
   - To remove a company operator, click **Remove Company Operator** beside the record, then click **OK**.

   Only a current company operator of the selected company can add or remove company operator records.
3. To create a new place:
   - Open the **Places** window from the navigation pane.
   - Click **Create Place**.
   - Select your **Company**.
   - Add a **Name** and, optionally, a **Description** for the place.
   - Click **Create Place**.
4. To add a concierge to administer a place:
   - Open the **Places** window from the navigation pane and select your **Place**.
   - Enter the **Email** address for the concierge and click **Add Concierge**.
     - The portal will process your request, then display Success. Concierge Added.
     - The person will receive an email inviting them to log in to the portal.
   - To remove a concierge, click **Remove Concierge** beside the record, then click **OK**.
5. To add a phonebook for the place:
   - Open the **Phonebooks** window from the navigation pane.
   - Click **Create Phonebook**.
   - Select the **Place** created above and assign a **Name** for the phonebook.
   - Click **Add Phonebook**. The phonebook will automatically be populated with all of the tenants associated with the place. Any new tenants added to the place will also be automatically added to the phonebook.
6. To add tenancies to the place:
   - Open the **Tenancies** window from the navigation pane.
   - Click **Add Tenancy**.
   - Select the **Place** created above, then add a **Name** (e.g. Apartment 501) and a **Description** (optional).
   - Click **Add Tenancy**.
7. When the tenancy has been saved, you can add tenants.
   - In the **Tenants** section, enter a **First Name** and **Last Name** to identify the tenant.
   - You must enter an **Email** address and/or valid **Phone Number** for the tenant.

     The Phone Number field is only available when the Include in Phonebook option is selected.

     - When an email address is entered a mobile app account and SIP account are automatically created and the tenant can receive video calls from the entry station directory to their mobile app account.

If the user already has a mobile app account, enter the email address associated with that account.

  - When a phone number is entered and no email is present no mobile app account or SIP account is created. The tenant's phone number is exported to the entry station directory and they can receive voice calls from the entry station directory to their mobile device or land line.
  - If both are entered the email takes priority. The phone number is merely a record in the phonebook.
- To include the tenant in the export to the entry station directory, ensure that **Include in Phonebook** is enabled and the phonebook for the place is selected.

  This can be disabled for any tenants who do not wish to appear in the entry station directory.
- Click **Add Tenant**.

Each tenant added with an email address automatically has a SIP account created on the ICT hosted PBX server and assigned to them. They will also receive an email notifying them that they have been assigned to a tenancy, and inviting them to download the Protege mobile app if they have not already done so.

Protege GX User Integration

Protege Tenancy Portal integration with Protege GX allows selected Protege GX users to be synchronized to the tenancy portal as tenants in tenancies, automatically populating the phonebook for the associated place.

The following records and settings are exported from Protege GX to the tenancy portal:

Protege GX Records	Tenancy Portal Records
Site	Place Phonebook
Tenancy name (assigned to a user)	Tenancy
User	Tenant
Email address	SIP account Mobile app account
Phone number	Phone number
PIN code	PIN code

Setup Summary

1. Obtain a tenancy portal account from ICT (see below).
2. Create a synchronization operator in Protege GX (see next page).
3. Enable synchronization in Protege GX (see next page).
4. Enter user contact details and tenancy names (see next page).
5. Install and configure the synchronization service (see page 14).

Important Notes

- User email addresses must be unique for each Protege GX site.
- Because the synchronization process overwrites tenants with Protege GX user data, all changes to tenants must be made in the Protege GX user records. Changes in the tenancy portal will be overwritten by the synchronization process, and unexpected results may occur if changes are made directly in the portal while the sync service is not connected.
- The synchronization process appends Protege GX site data to places, adding and updating but not deleting.

Limitations

- Only one phonebook is created per Protege GX site. To create additional phonebooks you must program a new site for each one. However, be aware that sites in Protege GX are not able to share resources such as users, access levels or schedules, so should only be used for completely separate properties.
- The integration cannot use or merge with an existing phonebook in the tenancy portal.

Synchronization Account

To synchronize the tenancy portal with Protege GX you need a tenancy portal account, and this account must be assigned as a **Company Operator** for the company you want to synchronize to. This is necessary to provide the synchronization service with the access required to synchronize records to the company.

This account must be used as the synchronization account for the integration (see next page).

To obtain a tenancy portal account, contact ICT Customer Services. A company operator account can also be added to the company by an existing company operator (see page 8).

Synchronization Operator

A Protege GX operator is required to provide access for the synchronization service. It is strongly recommended that an operator be created solely for use with this integration. This will ensure that the service has sufficient permissions to synchronize the data, and makes it simple to identify and audit changes made by the service.

1. In Protege GX, navigate to **Global | Operators**.
2. Click **Add** and create a new operator with a descriptive **Name** (e.g. Tenancy Portal Synchronization Service).
3. Enter a **Username** and **Password** for the operator. Make a note of these. They will be used when configuring the synchronization service.

   The operator must have a logon password. It is **not** possible to Use Windows Authentication for this operator.
4. Set the **Role** to Administrator. This level of access is necessary for the synchronization.
5. Click **Save**.

Enabling Tenancy Portal Synchronization

Enabling tenancy portal synchronization causes user PIN codes to be revealed in plain text via the SOAP service and web client. This occurs even when PIN security measures are enabled (see next page).

Tenancy portal synchronization needs to be enabled for each Protege GX site that you want to synchronize.

- Each site is synchronized to the tenancy portal as a place with a phonebook.
- Each place is assigned to the company that the tenancy portal account has company operator access to.

Each tenancy portal account should have company operator access to one company only. If access to multiple companies is required, separate tenancy portal accounts and logins should be used. If the same login is used to integrate multiple sites they will all be assigned to the first company (alphabetically) that the login has access to.

1. Navigate to **Global | Sites** and select or create the site that will be synchronized to the portal.
2. In the **Portal** tab, check the **Enable portal synchronization** option.
3. Enter the **Username** and **Password** used for logging in to the tenancy portal with the synchronization account.

   This login must have **company operator** access to the company that the site will be synchronized to.
4. Click **Save**.

Protege GX User Synchronization

For a Protege GX user to be synchronized to the tenancy portal they require:

1. An email address or phone number entered
2. A tenancy name defined

If both these requirements are met the user will be synchronized to the portal.

Email Address vs Phone Number

- Users synchronized with an **email address** will have a mobile app account and SIP account automatically generated. This will allow visitors to video call the user on their mobile app account from the entry station.

If the email address is changed a new mobile app account and SIP account are automatically generated and associated with the new email.

- Users synchronized with a **phone number only** do not have a mobile app account or SIP account created. In the absence of email and the associated accounts the user's phone number is exported to the entry station directory. Visitors can voice call the user on their mobile device or land line from the entry station.

  If an email is later added a mobile app account and SIP account will then be automatically generated. This will replace the phone number in the entry station directory.

- For users synchronized with an email address and phone number the email takes priority. A mobile app account and SIP account will be generated and visitors can video call the user on their mobile app account. The user's phone number is not exported to the entry station directory.

  If the email is later removed the phone number will instead be exported to the entry station directory to allow voice calls, but the mobile app account and SIP account are not deleted or disabled.

Synchronizing Users

1. Navigate to **Users | Users** and select or add a user to synchronize.
2. To synchronize a user with a Protege mobile app account and SIP account for video calls, enter the user's email address in the **Email** field. This must be a unique address (see below).
3. Navigate to the **Portal** tab.

   The Portal tab is only available when synchronization is enabled for the site.

4. To synchronize a user with a phone contact for voice calls, enter the user's **Phone number**. Duplicate phone numbers are allowed so that multiple users from a tenancy can use the same directory contact number.

   The phone number will only be used in the entry station directory if no email address is present.

5. Enter the **Tenancy name** for the user as you want it to appear in the tenancy portal and phonebook.

   Remember to maintain consistent naming conventions and ensure that users from the same tenancy have exactly the same tenancy name entered (e.g. Room1 or Room 01).

6. Click **Save**.

When a user is synchronized, if the email address is already associated with a mobile app account, the existing account is used. If a mobile app account **does not** exist for the address, a mobile app account and SIP account will automatically be generated for the user. The user will then receive an email with a link to install the mobile app.

If more than one user in a **site** is synchronized with the same email address unexpected results may occur.

A user can be synchronized with the same email address from multiple Protege GX sites or databases. When this occurs the user is synchronized as a unique tenant record in the places and phonebooks associated with the different sites, but they will use the same mobile app and SIP accounts which already exist for that email address.

User PIN Synchronization

The entry station can be programmed to activate controllable devices such as doors, elevator floors, lighting and climate control. Users simply enter their PIN, either into the numeric keypad of the touchscreen or into their phone during a call with the entry station, to activate the programmed functions.

For more information, see Enabling Entry Station Integration with Protege GX (page 22).

PIN Security Warning

PINs cannot be encrypted in the tenancy portal. They must exist in plain text in the phonebook so that they can be read and imported into the entry station directory. Therefore, when tenancy portal synchronization is enabled the SOAP service returns PINs in plain text to all requests. This means that all web client operators who can view users, and all other applications that use the SOAP service, will display unmasked PINs, regardless of the configuration of the following security settings.

- **Global | Global Settings | Encrypt user PINs**
- **Global | Operators | Show PIN numbers for users**
- **Global | Sites | Site defaults | Require dual credential for keypad access**

When using the Protege GX integration, careful consideration should be given to providing company operator or concierge access to portal records, as these users will be able to view user PINs in the phonebook.

Protege GX Synchronization Service

Integration with Protege GX is managed by the **Protege GX Tenancy Portal Synchronization Service**. The service periodically checks and syncs the selected Protege GX sites and users to the tenancy portal.

The synchronization treats places differently to tenants. Places are added and updated by the integration, but not deleted. Tenants and tenancies are updated with current Protege GX user data.

- The service will read from the portal upon connection, and then every hour thereafter. It will sync to the portal directly after the first read, and then according to the sync interval setting.
- The synchronization service performs an append function to places, where it updates but does not delete.
- New synced sites will be added as a new place, and changes to the site will be updated in the portal.
- If a synced site is deleted in Protege GX, the associated place, phonebook, tenancy and tenant data will remain in the tenancy portal. Nothing is removed.
- Places that are manually added in the tenancy portal will not be updated or deleted by the synchronization.
- The synchronization performs an update function for tenants and tenancies. The sync service reads and caches the current data for the place, then updates this with the current associated Protege GX user data.
- If a user exists in Protege GX but not in the tenancy portal place, they are added.
- If a user has been modified in Protege GX, they are updated in the portal.
- If a user exists in the portal but does not exist in Protege GX, they are deleted from the portal.
- Any tenants that are added directly in the tenancy portal will be deleted by the synchronization.
- Any changes to synced tenants that are made directly in the tenancy portal will be overwritten by updates in the synchronization.
- If a synced user is deleted in Protege GX, the associated phonebook entry and tenant record will be deleted from the tenancy portal, but the associated mobile app account and SIP account will not be deleted.

Synchronization Service Installation

The synchronization service is installed using the **ProtegeGXTenancyPortalSynchronization** installation executable.

1. Run the installation executable to launch the installation wizard.
2. Click **Next** to continue.
3. Click **Next** to begin the installation.
4. Click **Next** to install the service in the default directory, or **Change...** to select a different directory.
5. When the installation is complete, click **Finish**.

   Enabling the **Launch on click "Finish"** option will launch the synchronization manager on completion.

The Protege GX Tenancy Portal Synchronization Service is now installed and by default is set for automatic startup. It will now need to be configured for the integration (see below).

Synchronization Manager

The synchronization service is configured using the **Protege GX Tenancy Portal Synchronization Manager**. You can access this from the Windows Start menu, or by opening the TenancyPortalSyncManager.exe from the installation directory (The default location is: C:\Program Files (x86)\Integrated Control Technology\Protege GX Tenancy Portal Synchronization Service) .

The service can also be stopped and started via the Windows Services panel.

To enable the service to perform the synchronization the SOAP address and operator logon need to be configured to establish connection to the SOAP service. The sync interval also needs to be defined.

1. Open the synchronization manager via the Start menu or installation directory.
2. Before making any configuration changes, click the **Stop** button to stop the service.

   Updates are committed when clicking Start, so this helps to ensure that changes are saved.
3. Set the **Sync interval** to the frequency of Minutes or Seconds for the service to sync Protege GX records.
4. Ensure that the **SOAP service address** is correct for connection to the SOAP service.

   To achieve secure communications it is recommended to connect to the HTTPS endpoint of the SOAP service.
5. Set the **Operator username** to the Username of the synchronization operator (see page 11).
6. Set the **Operator password** to the Password of the synchronization operator.
7. The **Portal server address** defines server access for tenancy portal updates. This should be left at the default setting of https://www.protege-mobile.com/ unless instructed by ICT Technical Support.
8. The **Auth server address** defines server access for mobile app accounts. This should be left at the default setting of https://auth.protegex.cloud/ unless instructed by ICT Technical Support.
9. Click the **Start** button to commit the configuration changes and start the service.

Synchronization Manager SOAP Errors

If the sync service is unable to connect to the SOAP service, one of the following error messages will be displayed at the bottom of the synchronization manager user interface.

Error	Description
Failed to locate installed Windows Service \"Protege GX Tenancy Portal Synchronization Service"	TenancyPortalSynchronizationService.exe is not found
Failed to Load Application Settings	The settings.xml cannot be loaded
Protege GX SOAP Service Address is invalid	Incorrect SOAP service address
Operator logon to Protege GX failed. Error: Exception: An error occurred while making the HTTP request to https://localhost:8030/ProtegeGXSOAPService/service.svc. This could be due to the fact that the server certificate is not configured properly with HTTP.SYS in the HTTPS case. This could also be caused by a mismatch of the security binding between the client and the server. responseCode: 0	Incorrect SOAP service address port
Operator logon to Protege GX failed. Error: Unable to connect to endpoint" \"https://localhost:8040/ProtegeGXSOAPService1/service.svc\". Ensure the Protege GX Data Service is running and that SOAP is able to accept requests at this time. responseCode: 0	Incorrect SOAP service name
Operator logon to Protege GX failed. Error: Logon Failed responseCode: 5	Incorrect SOAP service operator Username and/or Password

If the Portal/Auth server address is incorrect, the service manager will not display any error messages. Error events will be displayed in the sync service console window and logged in the log file (see next page).

Synchronization Events

Once the service is started it will begin attempting to synchronize, generating events of its activity.

The service will read from the portal upon connection, and then every hour thereafter. It will sync to the portal directly after the first read, and then according to the sync frequency setting.

To view live sync events in the sync service console window, go to the installation directory (The default location is: C:\Program Files (x86)\Integrated Control Technology\Protege GX Tenancy Portal Synchronization Service) and open the **TenancyPortalSynchronizationService.exe**. A log file is also generated in the **logs** folder in the installation directory.

Synchronization Event Examples

Below are examples of typical synchronization events.

Note: The date/time component has been omitted from these examples for brevity.

Initializing Synchronization

```
[INFO ] - Starting Synchronization with
ProtegeGXTenancyPortalSynchronizationService
[INFO ] - Start reading from portal
[INFO ] - Login to portal: https://www.protege-mobile.com/) for user
testuser@yourcompany.co successfully
```

Reading from the Tenancy Portal

```
[INFO ] - Site 5 read from portal successfully
[INFO ] - Phonebooks of site 5 read from portal successfully
[INFO ] - PhonebooksEntries of PhoneBook TestSite1 is read from portal
successfully
[INFO ] - User with email testuser1@yourcompany.co is read from portal
successfully
[INFO ] - User with email testuser2@yourcompany.co is read from portal
successfully
[INFO ] - User with email testuser3@yourcompany.co is read from portal
successfully
[INFO ] - Finish reading from portal successfully
[INFO ] - Next read from portal will begin at 17/03/2022 7:03:37 PM
```

Synchronizing to the Tenancy Portal - No Change

```
[INFO ] - Start syncing to portal
[INFO ] - Start syncing sites to portal
[INFO ] - No sites changes need to sync to portal
[INFO ] - No users changes for site 5 to sync to portal
[INFO ] - Data synced to portal successfully
[INFO ] - Next retry will begin at 17/03/2022 6:04:35 PM
```

Synchronizing to the Tenancy Portal - Protege GX Site Added

```
[INFO ] - Start syncing to portal
[INFO ] - Start syncing sites to portal
[INFO ] - Companies of testuser@yourcompany.co is read from portal
successfully
[INFO ] - Site TestSite2 successfully added to portal
[ERROR] - There isn't any Phonebooks for site 6
[INFO ] - Phonebook TestSite2 successfully added to portal
[INFO ] - Finish syncing sites to portal
[INFO ] - No users changes for site 5 to sync to portal
[INFO ] - Tenancies of TestSite2 is read from portal successfully
[INFO ] - Tenancy TestSite2 Apartment1 added to portal successfully
[INFO ] - App account created for user 223 successfully
[INFO ] - User 223 added to tenancy TestSite2 Apartment1 successfully
[INFO ] - User 223 added to phonebookentry successfully
[INFO ] - User 223 added to phonebook TestSite2 successfully
[INFO ] - Users of site 6 added to portal successfully
[INFO ] - Data synced to portal successfully
[INFO ] - Next retry will begin at 17/03/2022 6:05:55 PM
```

Synchronizing to the Tenancy Portal - Protege GX Site Deleted

```
[INFO ] - Start syncing to portal
[INFO ] - Start syncing sites to portal
[INFO ] - No sites changes need to sync to portal
[INFO ] - Site 6 deleted from Protege GX but still exist in portal
[INFO ] - Finish syncing sites to portal
[INFO ] - No users changes for site 5 to sync to portal
[INFO ] - Data synced to portal successfully
[INFO ] - Next retry will begin at 17/03/2022 6:07:15 PM
```

Synchronizing to the Tenancy Portal - Protege GX User Added

```
[INFO ] - Start syncing to portal
[INFO ] - Start syncing sites to portal
[INFO ] - No sites changes need to sync to portal
[INFO ] - Finish syncing sites to portal
[INFO ] - Tenancies of TestSite1 is read from portal successfully
[INFO ] - App account created for user 224 successfully
[INFO ] - User 224 added to tenancy TestSite1 Apartment2 successfully
[INFO ] - User 224 added to phonebookentry successfully
[INFO ] - User 224 added to phonebook TestSite1 successfully
[INFO ] - Users of site 5 update in portal successfully
[INFO ] - Data synced to portal successfully
[INFO ] - Next retry will begin at 17/03/2022 6:08:35 PM
```

Synchronizing to the Tenancy Portal - Protege GX User Updated

```
[INFO ] - Start syncing to portal
[INFO ] - Start syncing sites to portal
[INFO ] - No sites changes need to sync to portal
[INFO ] - Finish syncing sites to portal
[INFO ] - Tenancies of TestSite1 is read from portal successfully
[INFO ] - User 223 successfully updated in ApartmentsUsers in portal
[INFO ] - User 223 successfully updated in PhoneBookEntries in portal
[INFO ] - Users of site 5 update in portal successfully
[INFO ] - Data synced to portal successfully
[INFO ] - Next retry will begin at 17/03/2022 6:08:35 PM
```

Synchronizing to the Tenancy Portal - Protege GX User Deleted

```
[INFO ] - Start syncing to portal
[INFO ] - Start syncing sites to portal
[INFO ] - No sites changes need to sync to portal
[INFO ] - Finish syncing sites to portal
[INFO ] - User with email testuser3@yourcompany.co deleted from tenancy
TestSite2 Apartment3 successfully
[INFO ] - User with email testuser3@yourcompany.co deleted from phonebook
successfully
[INFO ] - User with email testuser3@yourcompany.co deleted from portal
successfully
[INFO ] - Data synced to portal successfully
[INFO ] - Next retry will begin at 17/03/2022 6:09:55 PM
```

Synchronization Error Events

Below are examples of synchronization errors.

Note: The date/time component has been omitted from these examples for brevity.

Portal Login Errors

Incorrect **Portal server address** (sync manager) or incorrect portal login **Credentials** (**Global | Sites | Portal**).

```
[ERROR] - Failed to retrieve authentication token to portal:
https://www.protege-mobile.com/) for user Tenancy Portal Synchronization
Service, The remote name could not be resolved: 'protege-mobile.com'
[ERROR] - Failed to add site 6 to portal
```

Site portal login **Credentials** (**Global | Sites | Portal**) not assigned to company as company operator, or not using the required sync service version (see page 4).

```
[ERROR] - Failed to retrieve companies for Site {site.SiteId} from portal
```

Sync Service Starting

The following individual errors may be generated by the sync service not starting correctly.

```
[ERROR] - WriteError($"Failed to load saved settings, please use the
synchronization manager to clear all errors, then try again.")
[ERROR] - WriteError($"Resolve the error message(s) above then restart the
service to try again.")
[ERROR] - WriteError($"Sync failure. Exception type {ex.GetType().FullName}.
Exception message: {ex.Message}")
[ERROR] - WriteError($"Data synced to portal failed")
[ERROR] - WriteError($"Sync failure.Exception type {ex.GetType().FullName}.
Exception message: {ex.Message}")
```

Sync Service Connecting to SOAP Service

The following individual errors may be generated by the sync service failing to connect to the SOAP service.

```
[ERROR] - MessageLogger.WriteError($"Failed to list existing Sites from
{OEMSettings.ApplicationName}")
[ERROR] - MessageLogger.WriteError($"Failed to get existing Site (Id
{site.SiteId}) from {OEMSettings.ApplicationName}")
[ERROR] - MessageLogger.WriteError($"Sync failure (GetSitesFromGX).
Exception: {ex.Message}")
[ERROR] - MessageLogger.WriteError($"Failed to get existing User (User Id
{user.UserId}) from {OEMSettings.ApplicationName}")
[ERROR] - MessageLogger.WriteError($"Sync failure (GetUsersFromGX).
Exception: {ex.Message}")
[ERROR] - MessageLogger.WriteError($"Failed to list existing users in site
(Id {siteId}) from {OEMSettings.ApplicationName}")
```

Advanced Synchronization Service Settings

Some optional settings are available to optimize the performance of the synchronization service. These must be edited in the settings file for the service.

Advanced Settings

- **MaxDegreeOfParallelism**: This setting determines the maximum number of parallel threads that the computer will use when synchronizing user records with the tenancy portal. Increasing the number of threads can improve performance when synchronizing a large number of users.

- The default setting is 2.
- 3-5 threads typically gives good performance, but this must be tested to find the optimal value for your setup.
- -1 instructs the service to use all available threads.

Editing the Settings File

1. Navigate to the installation directory for the service. By default, this is C:\Program Files (x86)\Integrated Control Technology\Protege GX Tenancy Portal Synchronization Service
2. Run the Tenancy Portal Synchronization Manager.
3. Click **Stop** to stop the service.
4. Open **settings.xml** using a text editor.

   Files in this directory require administrator permissions to edit. You may need to open the file as an administrator using an application like Notepad++, or make a copy in a different directory to edit and replace the original.

5. Locate the following section of the XML code:

```
<SynchronizationSettings>
  <AppSettingsVersion>1</AppSettingsVersion>
  <Interval>1</Interval>
  <IntervalUnit>1</IntervalUnit>
</SynchronizationSettings>
```

6. Before the closing **</SynchronizationSettings>** tag, insert the advanced setting you wish to program. For example:

```
<SynchronizationSettings>
  <AppSettingsVersion>1</AppSettingsVersion>
  <Interval>1</Interval>
  <IntervalUnit>1</IntervalUnit>
  <MaxDegreeOfParallelism>4</MaxDegreeOfParallelism>
</SynchronizationSettings>
```

7. Save the file.
8. Use the synchronization manager to start the service.

Entry Station Integration

The directory of the Protege entry station can be populated with a tenancy portal phonebook, either via manual import of a phonebook CSV file or by automated synchronization with the tenancy portal.

It is also possible for users to unlock the door from their mobile app or phone call so that their guests can enter the building. This requires the entry station to be integrated with Protege GX as a keypad.

Configuration is performed in the entry station's web interface. The default IP address is 192.168.1.34.

For additional integration options, see the Protege Vandal Resistant Touchscreen Entry Station Installation Manual.

Synchronizing a Phonebook

Tenancy portal directory integration synchronizes a Protege Tenancy Portal phonebook with the entry station's directory. The entry station will automatically sync the designated phonebook with its directory every 60 minutes, replacing the existing directory with the new phonebook sync, so no manual deleting, importing or maintenance of the entry station directory is required.

When synchronizing the directory with a tenancy portal phonebook it is not possible to manually add or maintain contacts. All directory information is deleted and replaced by the synchronized phonebook.

1. To synchronize the entry station directory with a tenancy portal phonebook, you will need the phonebook ID.
   - Log in to the Protege Tenancy Portal at https://wirelesscredentials.com/Tenancies.
   - Browse to the phonebook you wish to sync.
   - The phonebook ID is displayed in a read-only field. Click **Copy to Clipboard**.
2. Log in to the entry station's web interface and navigate to **Device Settings | Directory Sync**.
3. Paste the copied ID into the **Phonebook ID** field, then **Save** the new settings.

   When a Phonebook ID is saved in the directory configuration the existing directory is immediately deleted.
4. Within 30 seconds the phonebook details with be synced to the entry station directory. The entry station will re-sync the phonebook every 60 minutes.

Manually Importing a Phonebook

A Protege Tenancy Portal phonebook can be manually imported into the entry station's directory.

1. To import a tenancy portal phonebook, you will need to export the phonebook to a CSV file.
   - Log in to the Protege Tenancy Portal at https://wirelesscredentials.com/Tenancies.
   - Browse to the phonebook you wish to export and click **Export Contacts to CSV**.

     The browser will download a CSV file that includes all the tenants' names, email addresses, tenancies and SIP extensions to your **Downloads** folder.
2. Log in to the entry station's web interface and navigate to the **Directory** main menu.
3. Click **Import** in the toolbar, then **Choose File**.
4. Browse to the CSV file that you just downloaded from the tenancy portal. Click **OK** to import the tenants.

Note: When you import contacts from a CSV, they are added to the current contact list instead of overwriting it. This means that duplicate contacts may be created. To prevent this, delete existing contacts before import. You can multiselect the contacts with **Shift + Click** or **Control + Click**, then press **Delete**.

Enabling Entry Station Integration with Protege GX

In order for users to unlock the door from their mobile app or phone call, the entry station must be integrated with Protege GX.

Configuring the Entry Station in Protege GX

The following instructions describe how to add the entry station to Protege GX as a keypad. This enables door control using keypad programming.

Configure the Entry Station Settings

1. Open the entry station's web interface by entering the IP address into your web browser address bar.
2. Log in using your operator login details.
3. Navigate to **Device Settings | General**.
4. In the **Controller** section, set the **Con IP Address** to the IP address of the controller you want to connect the entry station to.
5. Set the **Mod TX Port** to 9450 (the controller's module TCP port).
6. Set the **Address** to a currently unassigned keypad physical address number.
7. Click **Save**.

Configure the Controller

Controller module TCP communications are disabled by default and must be enabled by a command.

1. In Protege GX, navigate to **Sites | Controllers**.
2. Expand the **Commands** section and enter the following command:
   `EnableModuleTCP = true`
3. Click **Save**.

Confirm Connection

1. In Protege GX, navigate to **Sites | Controllers**.
2. Right click on the controller you are linking the entry station to and click **Module addressing**.
3. The entry station should display within the module addressing window as a keypad.

   If you have multiple keypads connected, use the entry station's serial number to locate the correct record.

Add Keypad

1. If the entry station is displayed in the module addressing window, navigate to **Expanders | Keypads** and click **Add**.
2. Enter a **Name** for the entry station.
3. For the **Physical address**, select the keypad address configured in the entry station's web interface.
4. Click **Save**.
5. In the **Configure Module** popup window:
   - Set the **Inputs** to 0
   - Set the **Outputs** to 1
   - Disable the **Add trouble inputs** option.
6. Click **Add now** to complete the process.

Linking a Door to the Entry Station

Once the entry station has been configured as a keypad in Protege GX, it can be configured for door control. The following instructions outline how to link a Protege GX controlled door to the entry station.

Create a Keypad Group

1. Navigate to **Groups | Keypad groups**.
2. Click **Add** and enter a **Name** for the keypad group.
3. In the **Keypads** section, click **Add**.
4. Select the entry station's **Keypad** record and click **OK**.
5. Click **Save**.

Create a Menu Group

1. Navigate to **Groups | Menu groups** and click **Add**.
2. Enter a **Name** for the menu group.
3. In the **Settings** section, ensure that the **User (2)** option is enabled.
4. In the **Keypad groups** section, add the keypad group containing the entry station's keypad record.
5. Click **Save**.

Configure the Keypad Door Control

1. Navigate to **Expanders | Keypads** and select the entry station's keypad record.
2. Select the **Configuration** tab.
3. In the **Door connected to keypad** field, select the door you want to control with the entry station.
4. In the **Options 1** tab, enable the **Function key unlocks door when logged in (REX)** option.

   This configures the keypad to grant access with entry of a valid PIN, using either onscreen login or phone.
5. Click **Save**.

PIN-free Access

The entry station can be configured to unlock the door via phone call without the need for a PIN. To activate this feature, go to the **Options 1** tab and enable the **Function key unlocks door when logged out (REX)** option. The door can then be unlocked by simply entering * into a phone keypad during a call with the entry station.

PIN-free access is via phone call only. Doors cannot be unlocked via the onscreen login without a valid PIN.

Configure the Access Level

1. Navigate to **Users | Access levels** and create or select an existing access level.
2. In the **Doors** tab, ensure that the door linked to the entry station is added.
3. In the **Menu groups** tab, click **Add**.
4. Select the menu group created for the entry station and click **OK**.
5. Click **Save**.

Making and Receiving Calls

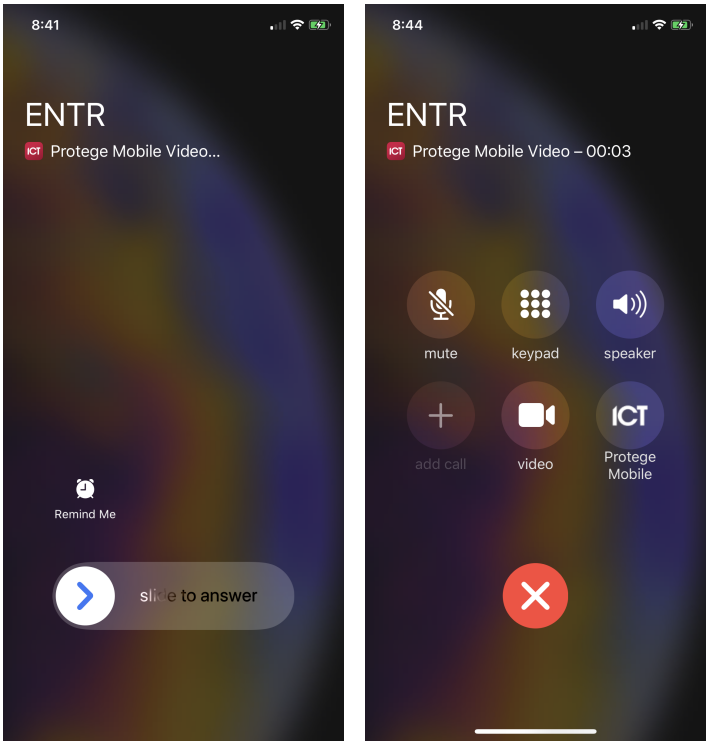
Once the contacts are loaded into the entry station, visitors can simply select the tenant's name and press call to initiate a video call. The tenant will receive the call directly to their phone, provided that they have the Protege mobile app installed and access to the internet.

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.

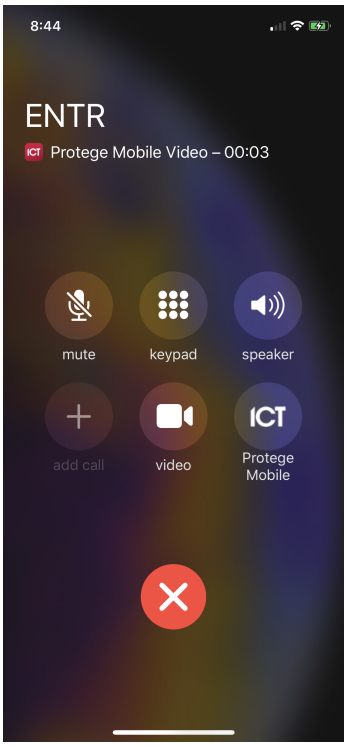
Call Handling - Lock Screen

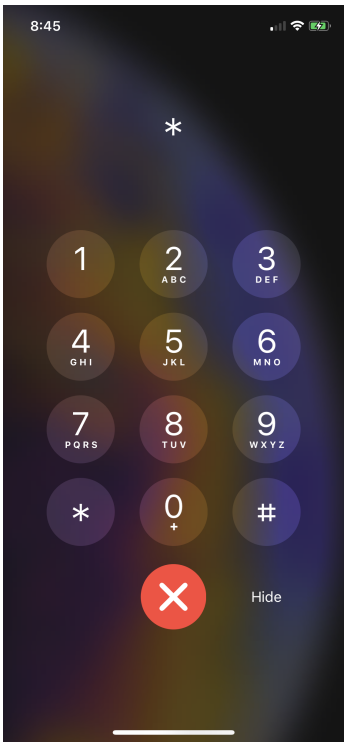
When an incoming call is received while the device is **locked**, the standard call interface is displayed. The user must **slide to answer** the incoming call.



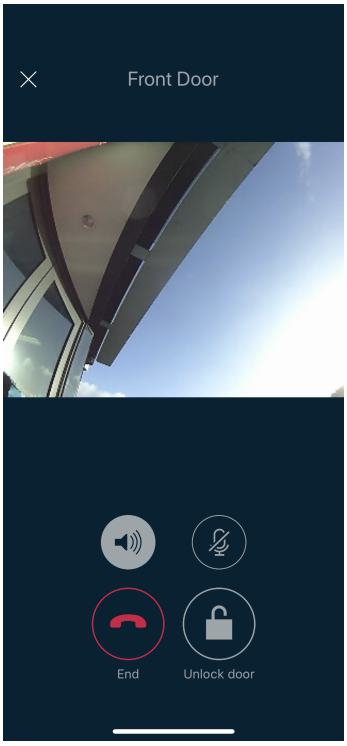
When the call is answered from the lock screen, the **answered call screen** is displayed and call audio is available.

To **unlock the door** from the answered call screen, press the **keypad** key, then press the ***** key.





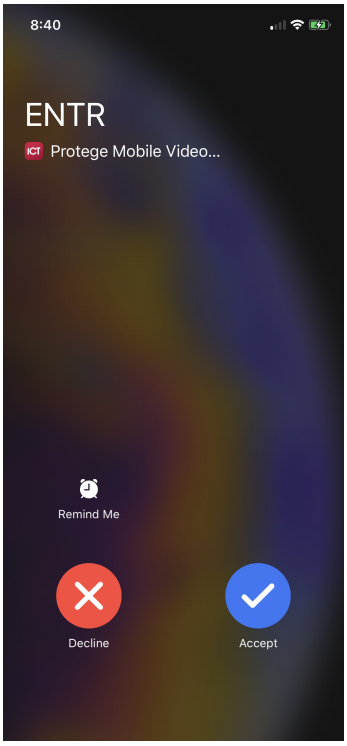
To view the video feed, press either the **video** or **Protege Mobile** button, then unlock the mobile device. This will launch the app and the **in app call screen** will be displayed.



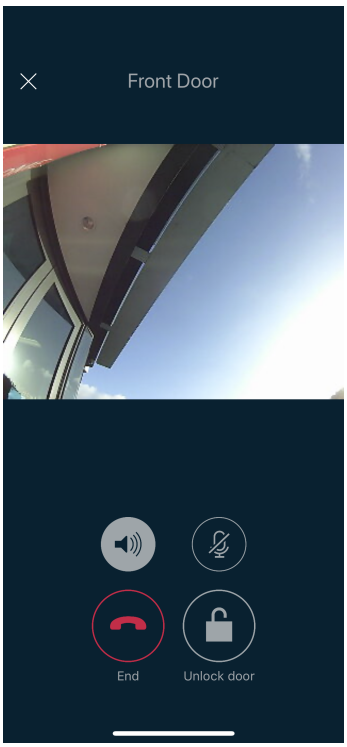
To unlock the door from the **in app call screen**, press the **Unlock door** key.

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.

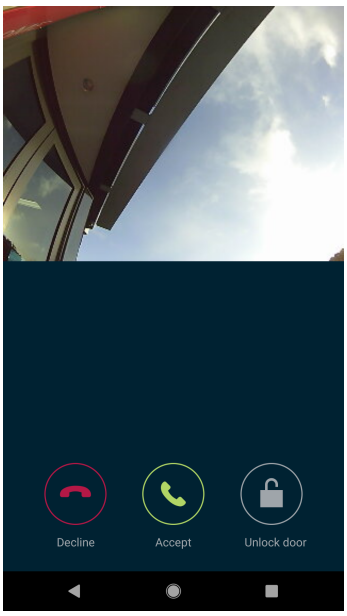
Android SIP Operation

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

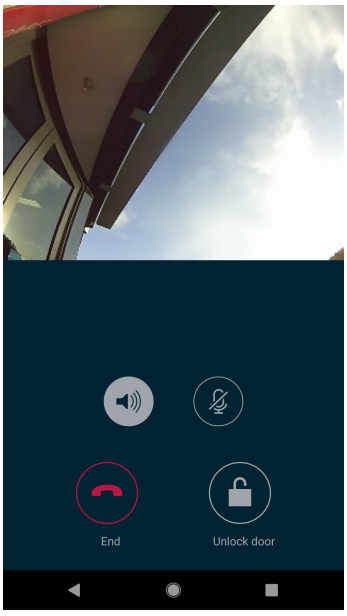
In order to start the app when it is closed and receive video, push notifications must be enabled for the app. When you install and run the app for the first time you will be prompted to enable push notifications. Alternatively, you can enable notifications from the Android settings on the device at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



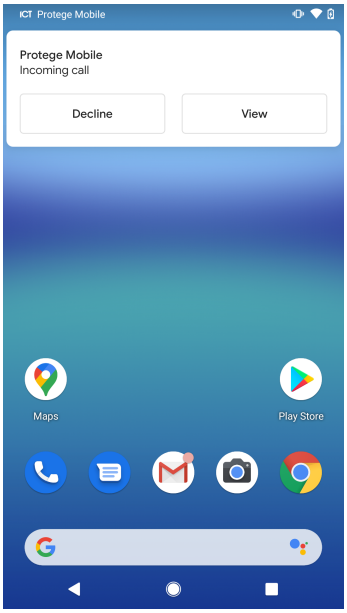
This screen displays the video feed. You can **Accept** or **Decline** the call, or unlock the door by pressing the **Unlock door** key.



Accepting the call will display the **answered call screen**, which provides additional options to mute the call or enable the loudspeaker.

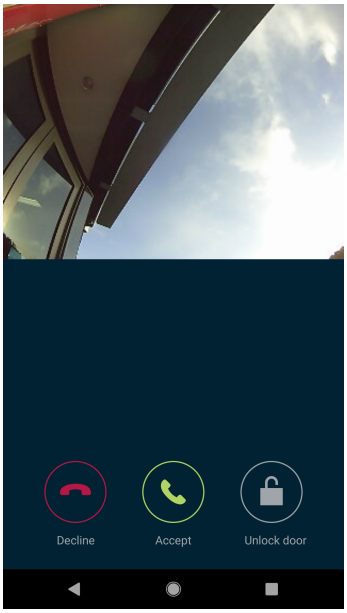
Call Handling - Home Screen or In App

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.

Troubleshooting

- **Problem**: Calls placed from the entry station are not coming through to the mobile app, or are audio only.
  This may occur when the tenant's mobile app does not have the correct notification settings to receive the video call. Ensure that notifications are turned on for the Protege mobile app.
- **Problem**: The app can receive calls, but the caller cannot hear the recipient.
  Ensure that the Protege mobile app has permission to access the phone's microphone (i.e. access to record sound).

Release History

This section contains the release history for the Protege GX Tenancy Portal Synchronization Service since its initial release (1.0.0.3).

Version 1.1.1.1

- Changed the name of the sync service from Wireless Credentials Synchronization Service to Tenancy Portal Synchronization Service, to better describe the purpose of the integration.
- Resolved an issue where sync service failed to retrieve companies from the portal, causing the sync to fail.
- Resolved an issue where the company operator account used for the synchronization needed to have a mobile credential. This is no longer required.

Version 1.1.1.4

- Resolved an issue where large numbers of duplicate records could be created in the tenancy portal.
- Improved the performance of the synchronization service when synchronizing large phonebooks. The number of threads used by the service is now configurable (see page 19).

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.

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