PRT-IPIC-POE

Protege Vandal Resistant VoIP Intercom

Installation Manual

Last Published: 29-Jun-23 09:11 AM

Contents

Introduction

The Protege Vandal Resistant VoIP Intercom is a SIP compliant intercom unit providing audio communications.

Tough, durable and extremely robust, the intercom is designed to meet the harshest of environments. SIP capability allows the intercom to communicate with any VoIP enabled device, including smartphones, providing the ability to grant entry from virtually anywhere.

The current features of the intercom include:

- Vandal resistant design
- HD audio quality
- Fully VoIP compliant to allow communication with other intercoms or SIP devices including external phones
- Optional offline operation
- Call button can be programmed to dial a phone number or call another VoIP device
- Programmable auto-answer
- Interact with the controller to allow control of devices such as lights and doors
- Allows local door control
- 2 onboard inputs
- 2 onboard Form C relay outputs
- 12V DC power supply input or PoE

Installation Requirements

This equipment is to be installed in accordance with:

- The product installation instructions
- The Local Authority Having Jurisdiction (AHJ)

Safety Guidelines

Before installing the intercom, note the following:

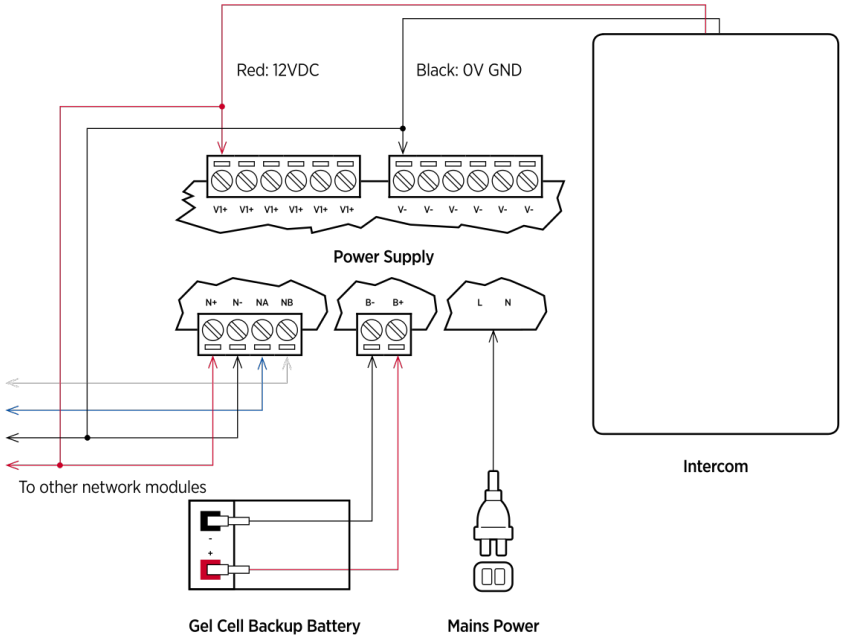
- The intercom should only be installed and configured by qualified installers.
- All installations are required to meet local wiring regulations and standards.

There are no user serviceable parts. If the intercom requires servicing or repair, return the unit to ICT.

Power Requirements

12V DC Power Supply

Power is supplied to the intercom by a 12V DC power supply connected to the V+ and V- terminals.



Power over Ethernet

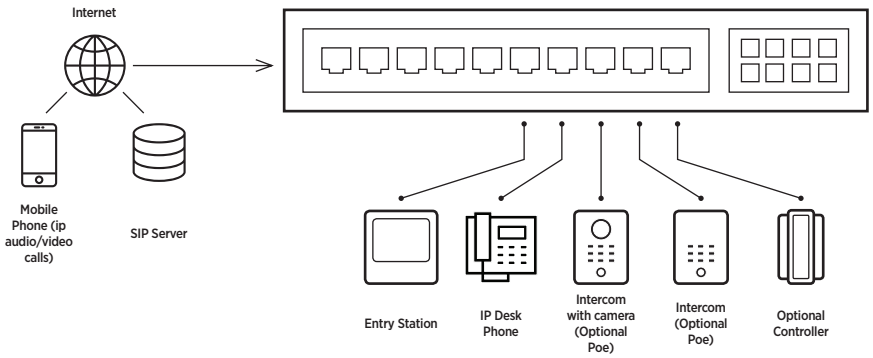
The intercom can alternatively be powered via an 802.3af Class 3 compatible PoE switch or router.

When PoE is used, the 12VDC + and - terminals must not be wired to any other power source.

10/100 Ethernet Connection

Ethernet connection allows for installations that use either a dedicated Protege network (recommended for multiple intercom installations) or simply connect the intercom and the controller to the building's existing network.

When installing an ethernet connection, the intercom should be interfaced using a standard Cat 5/6 segment (<100m in length) and should be connected to a suitable ethernet switch. Ethernet should be connected to the WAN port on the intercom PCB board. For more information, see Connections (page 9).



Supported Protocols

The intercom supports the following protocols:

- SIP
- DHCP Client: Dynamically assigns IP addresses, with the option to use static addressing
- RTP/SRTP
- Audio Encodings:
  - G.711U (PCMU)
  - G.711A (PCMA)
  - G.722
  - G.723.1
  - G.726-32
  - G.729AB

SIP Servers

The intercom supports SIP servers that comply with SIP protocol standards including Asterisk and 3CX.

Connections

Onboard Inputs

There are two onboard inputs on the intercom. This enables you to monitor the state of devices such as magnetic door contacts, motion detectors or REX buttons.

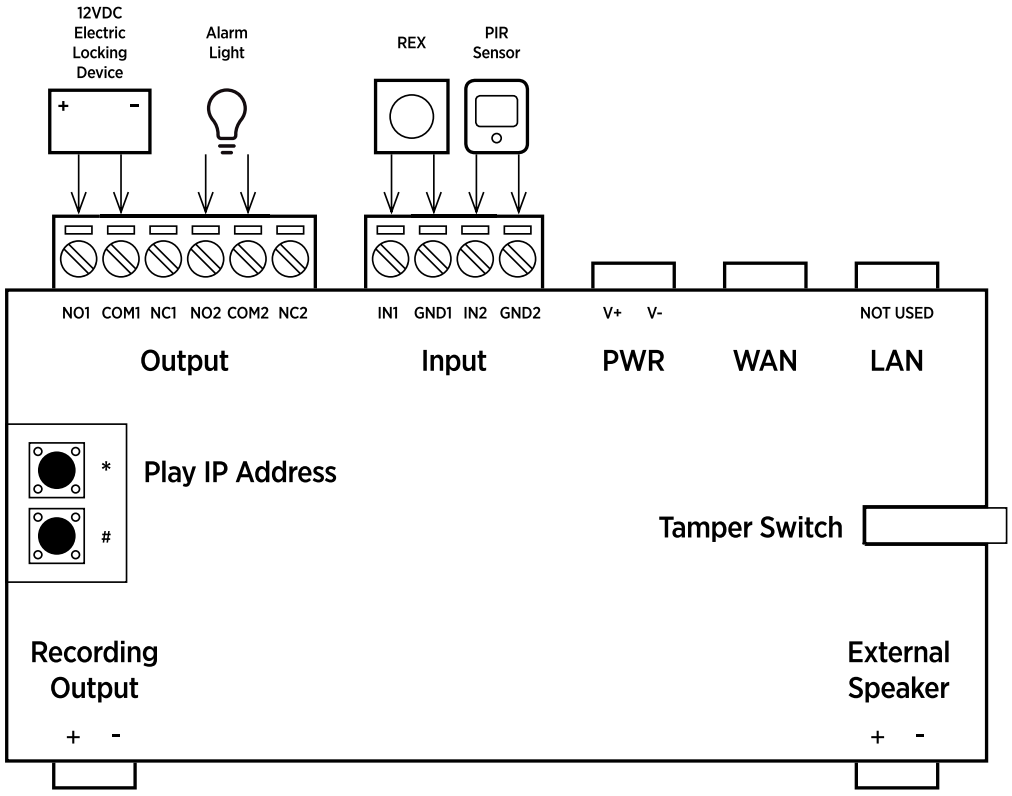
The onboard inputs can also be configured as a Protege input to enable Protege inputs to be triggered through the intercom. Refer to Configuring the Onboard Input for configuration details (see page 35).

Onboard Outputs

There are two onboard Form C relay outputs. These standalone outputs can be used to control devices such as door locks or lights directly from the intercom, independent of Protege system configuration (see page 33)

The relay outputs can switch to a maximum capacity of 24V DC 1A. Exceeding this will damage the output.

Ports



WAN Port

An **RJ45** network port for ethernet (including **PoE** - Power Over Ethernet connection).

Mounting and Installation

Wall Mounting Installation

The intercom is designed to be mounted on a wall. The following steps outline this procedure.

Tools

The following tools will be required to complete the installation:

- L-shaped hex tool (supplied)
- Phillips screwdriver (Ph2 or Ph3)
- Electric impact drill with 6mm drill bit
- Hammer
- RJ45 crimper

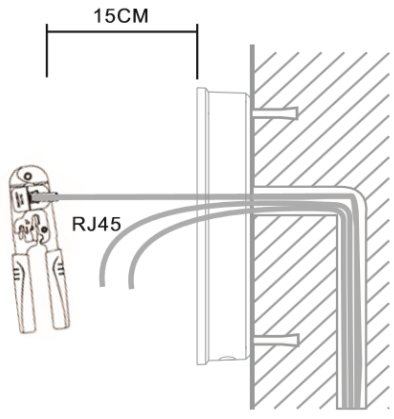
Preparation

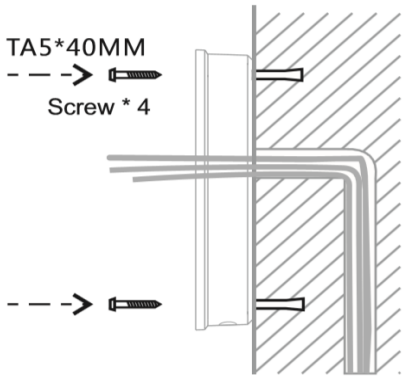
Prepare the installation area:

1. Place the **wall mounting template** sheet on the wall where the **intercom** will be located.
2. Drill 4 holes over the marks provided on the template. A drill hole depth of 50mm is recommended.
3. Remove the template and insert the screw anchors into the holes.

Mounting

1. Pull the cable through the cable hole in the **back panel**, leaving 15-20cm excess cable length.





2. With the L-shaped hex tool provided, remove the four security screws and lift the front plate out of the enclosure.
3. Using the 4 TA5 40mm screws, mount the **back panel** to the wall.

Note: the intercom is equipped with a secondary cable hole at the bottom of the back panel.

Connect and Test

1. Connect to the intercom board connectors:
   - RJ45
   - Power
   - Electric-Lock
2. Refer to the Connections page (see page 9).
3. To test, press the **#** key on the **circuit board** for 3 seconds to obtain the IP address of the intercom unit.

Do Not proceed until the electric checks are confirmed.

Completion

Attach the **front panel** carefully into the **back panel** and replace the 4 screws, ensuring the screws have been tightened correctly and the panels are secure to ensure waterproofing.

Hardware Configuration

Power on Sequence

The intercom takes approximately 25 seconds to boot after power has been supplied.

Once booted, open a web browser and enter the intercom's IP (default is 192.168.1.128) in the address bar.

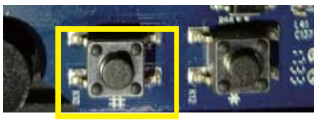
Log in when prompted: **User**: admin, **Password**: admin

Finding the Intercom on the Network

Select the IP Address # Key

If the currently configured IP address is unknown:

1. Ensure the intercom is powered on.
2. Remove the screws using the hex key provided and remove the **front panel**.
3. Lift the **main body** of the intercom out of the enclosure.
4. Locate and press the **#** labeled button on the **circuit board** for 3 seconds to activate an audio message through the built-in speaker which will announce the intercom's IP address.



5. Connect to the web interface by entering the IP address into the address bar of your web browser.
6. Log in when prompted: **User**: admin, **Password**: admin

Defaulting the Intercom

The intercom can be restored to its factory default settings using the following options:

Remotely Via the Intercom Web Interface

1. Open a web browser and enter the intercom's IP address in the address bar.
2. Log in when prompted: **User**: admin, **Password**: admin
3. Navigate to **System | Configurations**. Under **Reset to factory defaults** click **Reset**.
4. Click **OK** to confirm the restore and continue. The web interface will display Reboot Finish! when complete.

Defaulting the intercom will reset all settings and set the IP address to the default (192.168.1.128)

Using the Telnet Client

If the IP address or login details are unknown, the intercom can be restored to its factory default settings using the following procedure.

This method is only available on firmware version 2.6.0.6680 or higher.

1. Connect the intercom to the same switch/network as the PC.
2. Set the PC to a static IP address in the **192.168.10.xxx** range (xxx can be from 2-254).
3. Remove the power to the intercom.
4. Put the intercom into Update Mode by holding down the ***** and **#** buttons, then connecting power. After 5 seconds, release the buttons.

   Update Mode on the intercom can be verified by using the command prompt to ping 192.168.10.1

5. The intercom can be defaulted using any Telnet client. The instructions below describe defaulting the intercom using the PuTTY Telnet client tool.
   - Download the PuTTY installer package from putty.org and install.
   - Open the PuTTY Configuration tool.
   - Under **Connection Type** select **Telnet**.
   - Click **Open** to launch the PuTTY session.
   - On the **VoIP Phone System** screen, press **3** and **Enter** on the keyboard to **Clear Configuration**.
   - Then press **4** and **Enter** to **Exit and Reboot**. The intercom will take 30-60 seconds to reboot.
6. Remember to revert the PC back to its original IP address if changed at Step 2.

Defaulting the intercom will reset all settings and set the IP address to the default (192.168.1.128)

Programming the Intercom

This section describes the available settings, functions and features of the intercom and how to configure them through the web interface.

When you finish programming the intercom it is recommended to save the device configuration so that you can easily restore your programming if it ever becomes necessary (see page 17).

Intercom Web Interface

The web interface enables configuration and deployment of the intercom from a web environment, either for integration with a Protege system or to be set up for standalone operation.

Note: The web interface contains a number of intercom features and configuration settings that are not supported by ICT or the integration, and as such those options are not documented here.

Accessing the Web Interface

1. Open a web browser and enter the default IP address of the intercom: 192.168.1.128
2. When prompted to **Login** enter the default operator: **User**: admin, **Password**: admin.
   For security reasons, this password should be changed before deployment.
3. Click **Login**.

Once logged in, the main page is displayed. Select the menu options available on the main page to configure the intercom to your requirements. The menu options include:

- System
- Network
- Line
- Intercom Settings
- LED
- Security Settings
- Function Key

Initial Setup of the Intercom

In order to prepare the intercom for standard operation some basic settings will need to be configured via the intercom web interface.

Add the SIP Account

If the intercom is required to communicate with a SIP server, you need to add a SIP account.

If using direct IP dialing the SIP account does not need to be configured.

1. Navigate to **Line | SIP**.
2. In the **Basic Settings** section enter the SIP account parameters.
   - **Phone Number**: SIP account Login ID.
   - **Authentication Name**: The authentication ID of the account.
   - **Authentication Password**: SIP registration password.
   - Select **Activate**. This option must be selected to activate the line.
   - **SIP Proxy Server Address**: Proxy server IP or URL (usually the same as the SIP Registrar Server).
   - **SIP Proxy Server Port**: Proxy server port. Usually 5060.
3. Click **Apply**.
4. Ensure that the intercom has external internet access via the SIP port to allow it to connect to the SIP server.

   Contact your network administrator for help with allowing the intercom through the firewall.

If the SIP account is correctly configured the **Line Status** should display Registered. Otherwise, refer to Line | SIP for error details and SIP programming options.

Set up the Call Button

The call button will need to be configured to enable basic intercom use. This applies to both SIP and direct dialing operation.

1. Navigate to the **Function Key** menu.
2. From the **Type** dropdown list select **Hot Key**.
3. In the **Number 1** field enter the first number for the intercom to call when the call button is pressed.
4. Select the SIP **Line** for connection.
5. Set the **Subtype** to **Speed Dial**.
6. Click **Apply**.

For additional call button configurations, refer to the Function Key section (see page 31).

System

The System menu displays settings and status information and enables general configuration and management of your intercom device.

System | Information

Displays important details about your intercom including:

System Information

- **Model**: The device model.
- **Hardware**: The hardware version of the device.
- **Software**: The software version operating on the device.
- **Uptime**: The time duration that the device has been online or 'Up'.
- **Last Uptime**: The amount of time the device was online or 'Up' before the last reboot.
- **MEMInfo**: The ROM and RAM details of the device.
- **System Time**: The current time on the device.

Network

Displays the configuration information for the WAN Port including:

- **Network Mode**: The WAN port connection mode (**Static IP**, **DHCP**, **PPPoE**).
- **MAC**: The MAC address of the device.
- **IP**: The IP address of the WAN port.
- **Subnet Mask**: The network Subnet Mask.
- **Default Gateway**: The current Gateway IP address.

SIP Accounts

Displays the phone numbers and registration status for the SIP Lines, if configured.

System | Account

Enables management of users including adding and removing users and changing passwords and privileges.

There are two levels of user access. Administrators have access to all settings. Users have access to all configuration except user management and SIP server addressing. There are two default users:

- Default User: **User**: guest, **Password**: guest
- Default Administrator: **User**: admin, **Password**: admin

Add New User

Enables adding a new user to provide secure access to the web interface.

1. **Username**: Enter the login name for the new user.
2. **Web Authentication Password**: Enter the password for the new user to log in.
3. **Confirm Password**: Repeat the password for the new user to log in.
4. **Privilege**: Select the access level for the new user. Administrators have access to all settings. Users have access to all configuration except user management and SIP server addressing.
5. Click **Add** to complete adding the new user.

Important: Web authentication passwords must be no more than 30 characters. Only letters and numerals from the English alphabet can be used. This includes A-Z (upper or lower case) and 0-9. Use of any symbols or non-English characters has the potential to create an error and prevent logging in.

User Accounts

Displays the list of existing users and their assigned privilege level.

User Management

Users with administration privileges can manage existing users, including changing passwords and privilege levels, and deleting. You must first select the user from the drop-down list, and then choose your action.

1. To remove a selected user, click **Delete**. The user will be removed. **There is no warning before deleting**.

   To prevent potential system shut-out, the default admin user cannot be deleted.

2. To change a user's password and/or privilege level, select the user then click **Modify**. This accesses the Change Web Authentication Password page.

Change Web Authentication Password

Enables changing the login password and privilege level for the selected user.

Passwords must be no more than 30 characters. Saving a longer password will prevent logging in.

1. **Username**: The selected user that will be updated.
2. **Old Password**: Enter the existing password of the selected user.
3. **New Password**: Enter the **new** password to assign for the user to log in.
4. **Confirm Password**: Repeat the **new** password.
5. **Privilege**: Set the privilege level for the selected user.
6. Click **Apply** to apply the new settings.

If changing the privilege level without changing the password, you must also enter the old password into the New Password and Confirm Password fields, otherwise the user will be updated with a blank password.

System | Configurations

Enables management of device configuration by saving and importing configuration files. This is particularly helpful for ensuring consistent configuration settings are quickly and accurately applied to a number of devices.

Export Configurations

Enables exporting of current device configuration settings to a **.txt** or **.xml** file. Right click the appropriate link and select **'Save target as'** to export the configuration file to the desired file path and name.

Import Configurations

Enables importing of saved configuration settings from a **.txt** or **.xml** file to be uploaded to the device.

Importing configuration files is not supported in Firefox.

- **Configuration file**: Click **Select** to browse and select the required configuration file.
- Click **Import** to upload the configuration settings to the device. This will take some time as the new configuration is uploaded. The device will then perform a **Reboot** before prompting you to log in.

Reset to Factory Defaults

Click **Reset** to restore the device to the factory default settings. Then click **OK** to confirm.

All data including accounts and settings will be erased.

System | Upgrade

Enables the device to be upgraded to a new software version.

System upgrade is not supported in Firefox.

Software Upgrade

Displays the existing software version and enables updating to a newer (or compatible older) version.

- **Current Software Version**: The version of software currently loaded onto the device.
- **System Image File**: Click **Select** to browse and select the required configuration file.
- Click **Upgrade** to upload the new configuration settings to the device. This will take some time as the new configuration settings are uploaded. The web interface will display progress and a 'successfully completed' message at the end. The device will then perform a **Reboot** before prompting you to log in.

Upgrading Earlier Versions

It is not possible to upgrade PRT-IPIC-POE from version **2.4.2041.578** or earlier directly to version **2.6.0.6680** or later. This requires a specialized middle firmware and upgrade procedure. Attempting to upgrade an older version directly to a newer version may render the intercom inoperable.

Version 2.6.0.6680 represents a significant change in the firmware file format and upgrade process. In order to transition from the older format to the newer .bin file firmwares a middle firmware upgrade is required.

Once the intercom is upgraded to the newer format it is not possible to downgrade again.

1. Upgrade the intercom to the middle firmware. This version enables .bin file based updates.
   - Log in to the intercom's web interface and navigate to **Maintenance | Update**.
   - Select the 2c42MIMGV2_4_2071_589T20210623104807.z middle firmware file supplied by ICT.
   - Click **Upgrade** to upload the new firmware to the device.

   When complete the device will perform a reboot before prompting you to log in.
2. Upgrade the intercom to the new firmware.
   - Log in to the intercom's web interface and navigate to **Maintenance | Update**.
   - Select the firmware file supplied by ICT.
   - Click **Upgrade** to upload the new firmware to the device.

   When complete the device will perform a reboot before prompting you to log in.
3. Check the device's **Current Software Version** to confirm that it has successfully updated to the new version.

For assistance upgrading intercoms with older firmware versions please contact ICT Technical Support.

System | Auto Provision

This feature is not supported.

System | FDMS

This feature is not supported.

System | Tools

Additional tools and settings for managing the behavior of the device.

Syslog

This feature is not supported.

Network Packets Capture

This feature is not supported.

Reboot

Some configuration modifications require a system reboot to take effect. Click the **Reboot** button to perform an immediate reboot on the device.

Save the configuration before rebooting. For more information, see System | Configurations (page 17).

Network

The intercom has a built-in TCP/IP ethernet device which must be programmed with a valid TCP/IP address to allow the software to connect. The default IP address is set to 192.168.1.128.

Programming the IP address, subnet mask, and default gateway requires knowledge of the network and subnet that the system is connected to. You should always consult the network or system administrator before programming these values.

Network | Basic

Network Status

Displays the network configuration information for the device, including:

- **IP**: The intercom's IP address.
- **Subnet Mask**: The current Subnet Mask.
- **Default Gateway**: The current Gateway IP address.
- **MAC**: The MAC address of the intercom.
- **MAC Timestamp**: The aging time for dynamic MAC address entries.

Settings

Network settings need to be configured according to connection requirements. The intercom supports three network modes:

- **Static IP**: Network parameters are provided by the network administrator.
- **DHCP**: Network parameters are provided automatically by a DHCP server.
- **PPPoE**: This feature is not supported.

Note: Any changes made on this page require a Reboot to become active (see previous page).

Static IP

- **IP**: The Static IP address for the WAN port.
- **Subnet Mask**: The subnet mask.
- **Default Gateway**: The Gateway IP address.
- **Primary DNS Server**: The primary DNS server and address.
- **Secondary DNS Server**: The secondary DNS server address.

DHCP

When enabled, the intercom will use DHCP to dynamically acquire network parameters. To use this there must be a DHCP server on the network you are attempting to connect to.

DNS Server Configured by:

- Set to **DHCP** for automatic configuration.
- Set to **Manually configure** for manual configuration of Primary DNS Server and Secondary DNS Server settings.

Service Port Settings

Service port settings can be customized to enhance security. These should typically be left at the default settings, unless required by your network administrator.

- **Web Server Type**: HTTP or HTTPS.
- **HTTP Port**: Port for web browser access. Default setting is 80. Setting to 0 will disable HTTP access.
- **HTTPS Port**: Port for HTTPS access. Default setting is 443. Setting to 0 will disable HTTPS access.

  An HTTPS authentication certificate must be downloaded to the intercom before using HTTPS.

HTTPS Certification File

- Click **Select** to browse and select the required certification file.
- Click **Upload** to load the file to the device.
- Click **Delete** to remove the currently loaded HTTPS certification file.

Network | Advanced

This feature is not supported.

Network | VPN

This feature is not supported.

Network | Web Filter

This feature is not supported.

Line

Line | SIP

The SIP **Line** settings enable SIP account configuration. Select the SIP line to be configured.

Note: the settings on this page always apply to the specific SIP line selected. A number of the intercom's features can also be configured in Intercom Settings (see page 26), and are applied across all lines.

Line Status: Displays the current status of the selected line. If the SIP account is successfully registered, active and able to send and receive calls, the word Registered will be displayed.

If the line is not currently active one of the below errors will be displayed.

Error Code/Message	Description
Inactive	The line is not yet activated. The **Activate** option must be selected
401	Unauthorized (authentication failed). Check the authentication name and password
403 Forbidden	SIP server rejected registration. Check the authentication name and password
Timeout	No response from SIP server. Check network and SIP settings. May be caused by incorrect IP address or blocked internet access

Basic Settings

- **Phone Number**: SIP account login ID.
- **Display Name**: The name suggested to the SIP server for caller ID.
- **Authentication Name**: The authentication ID of the account.
- **Authentication Password**: SIP registration password.
- **Activate**: This option must be selected to activate the line.

- **SIP Proxy Server Address**: Proxy server IP or URL (usually the same as the SIP Registrar Server).
- **SIP Proxy Server Port**: Proxy server port. Usually 5060.
- **Backup Proxy Server Address**: This server will be used if the primary server is unavailable.
- **Backup Proxy Server Port**: The backup SIP Server port.
- **Outbound Proxy Address**: The outbound proxy server address provided by the service provider.
- **Outbound Proxy Port**: Usually 5060.
- **Realm**: SIP domain if different to the SIP Proxy Server Address.

Codecs Settings

Codecs can be **Enabled** and **Disabled** by selecting and moving them to the appropriate list, and priority can be set by altering the list order.

Advanced Settings

Note: the settings on this page always apply to the specific SIP line selected. Some intercom features such as DND can also be configured in **Intercom Settings** (see page 26) to be applied across all lines.

- **Enable DND**: Enable Do Not Disturb to block incoming calls to the selected line.
- **Blocking Anonymous Call**: Blocks any incoming call without a recognized caller ID.
- **Use 182 Response for Call waiting**: Set the 182 response for call waiting.

- **Anonymous Call Standard**: Selectable settings for SIP privacy protocol standards.
  - None
  - RFC3323
  - RFC3325
- **Dial Without Deregistered**: Set call out by proxy without registration.
- **Click To Talk**: Enable the click to talk feature.
- **User Agent**: Set the user agent if required.
- **Response Single Codec**: Enable single codec response to an incoming call request.

- **Ring Type**: Select the ring tone type for the selected line.
- **Conference Type**: Set to **Local** to set up a conference call on the intercom (supports a maximum of two remote parties) or set to **Server** to connect to a conference room on the server.
- **Server Conference Number**: The Conference Room number when Conference Type is set to Server.
- **Transfer Timeout**: The timeout setting (in seconds) for the call transfer process.
- **Enable Long Contact**: Allow additional characters in the contact field where required to include user agent capabilities as per RFC3840.
- **Use Quote in Display Name**: Include quotes in the Display Name.
- **TLS Version**: Select the TLS version. Supported protocols are TLS 1.0, TLS 1.1 or TLS 1.2.

- **Specific Server Type**: Specify a server type for the line to communicate with.
- **Registration Expiration**: The SIP expiration frequency.
- **Use VPN**: Set the line to use a restricted VPN.
- **Use STUN**: Set the line to use STUN for NAT traversal.
- **Convert URI**: Convert non-alphanumeric characters to hex code.
- **DTMF Type**: Set the DTMF type to be used for the line.
  - In-band
  - RFC2833
  - SIP_INFO
  - AUTO
- **DTMF SIP INFO Mode**: Set the mode as required.
  - Send 10/11
  - Send */#
- **Transportation Protocol**: Set the line to use **UDP**, **TCP** or **TLS** for SIP transmission.
- **Local Port**: Set the local port.
- **SIP Version**: Select the SIP version, **RFC2543** or **RFC3261**.
  - FROM
  - PAI-FROM
  - RPID-FROM
  - PAI-RPID-FROM
  - RPID-PAI-FROM
- **Caller ID Header**: Select as required.
- **Enable Strict Proxy**: Enables the use of strict routing. When the intercom receives packets from the server it will use the source IP address, not the address in the via field.
- **Enable user=phone**: Sets user=phone in SIP messages.

- **Enable DNS SRV**: Set the line to use DNS SRV which will resolve the FQDN in proxy server into a service list.
- **Keep Alive Type**: Set the line to use a dummy **UDP** or **SIP Option** packet to keep the NAT pinhole open.
- **Keep Alive Interval**: Set the transmitting interval.

- **Sync Clock Time**: Synchronize the device time with the server.
- **Enable Session Timer**: Set the line to enable call ending by session timer. The session will be ended after the timeout period if no new session timer event update is received.
- **Session Timeout**: Set the session timer timeout period.
- **Enable Rport**: Set the line to add rport in SIP headers.
- **Enable PRACK**: Set the line to support PRACK SIP messages.
- **Auto Change Port**: Enable/disable auto change port.
- **Keep Authentication**: Maintain authentication parameters from the previous authentication.
- **Auto TCP**: Use TCP protocol to guarantee usability of transport for SIP messages above 1500 bytes.
- **Enable SCA**: Enables/disables Shared Call Appearance of the line across multiple devices.
- **Enable GRUU**: Support Globally Routable User-Agent URI for call routing.

- **RTP Encryption**: Enable RTP encryption such that RTP transmission will be encrypted.
- **Enable MAC Header**: When enabled, all SIP messages strip MAC fields.
- **Enable Failback**: When enabled, if the intercom loses connection to the primary SIP server it will attempt connection to the secondary server. If it cannot connect or loses connection to the secondary SIP server it will attempt connection to the primary server again.
- **Enable Register MAC Header**: When enabled, register the message ribbon MAC field.

Line | Basic Settings

SIP Settings

- **Local SIP Port**: The port the intercom uses to connect to the SIP server.

  The default Local Port is 5060. This may be adjusted if required by the network administrator.

- **Registration Failure Retry Interval**: The retry interval when SIP registration fails. Default is 32 seconds.
- **Transaction Timer T1**: The round trip time (RTT) estimate.
- **Transaction Timer T2**: The maximum retransmit interval for non-INVITE requests and INVITE responses.
- **Transaction Timer T4**: The maximum duration that a message can remain in the network.
- **Enable Strict UA Match**: Enable/disable strict User Agent (UA) matching.
- **Strict Branch**: Enable/disable exact branch matching.

STUN Settings

A STUN (Simple Traversal of UDP through NAT) server allows a phone in a private network to know its public IP and port as well as the type of NAT being used. The intercom can then use this information to register itself to a SIP server so that it can make and receive calls while in a private network.

- **STUN NAT Traversal**: Displays whether STUN NAT Traversal is successful (TRUE or FALSE).
- **Server Address**: STUN Server IP address.
- **Server Port**: STUN Server Port. The default is 3478.
- **Binding Period**: STUN packets are sent at this interval to keep the NAT mapping active.
- **SIP Waiting Time**: The waiting time for SIP. This will vary depending on the network.

Line | SIP Hotspot

This feature is not supported.

Line | Blacklist

This feature is not supported.

Line | Action Plan

This feature is not supported.

Intercom Settings

Intercom Settings | Features

- **Limit Talk Duration**: When enabled, calls will automatically end after the maximum time.
- **Talk Duration**: The maximum time (in seconds) for intercom calls.
- **DND Mode**: Prevent incoming calls for the **phone** (all lines) or the **line**.
- **Ban Outgoing**: When enabled no outgoing calls can be made.
- **Enable Call Waiting**: When enabled allows users to answer a second incoming call.
- **Enable Call Waiting Tone**: When enabled plays an intercom ring tone alerting to a waiting call.
- **Enable Intercom**: When selected the device will accept the SIP header call information.
- **Enable Intercom Barge**: When enabled automatically answer calls in intercom mode during a call if the current call is intercom mode.
- **Enable Intercom Mute**: When enabled mutes incoming calls during an intercom call.
- **Enable Auto Dial Out**: Enables auto dial out on timeout.
- **Auto Dial Out Time**: Set the wait time before auto dial out.
- **Enable Auto Answer**: Enable the auto answer function and select the required line configuration.
- **Auto Answer Timeout**: Set the auto answer timeout.
- **Dial Fixed Length to Send**: When enabled requires a fixed length number to be entered when dialing.
- **Send Length**: The number of digits required when Dial Fixed Length to Send is enabled.
- **Voice Read IP**: Enable an IP voice broadcast.
- **System Language**: Set the voice prompt language.
- **Description**: The broadcast identification of the intercom.
- **Enable DND (Do Not Disturb)**: Prevents incoming calls according to the DND Mode. Outgoing calls will not be affected.
- **HangUp Delay**: The duration (in seconds) that the intercom plays the hang up tone when a call is ended.
- **Call Timeout**: The duration (in seconds) that the intercom will attempt a call before canceling.
- **Dial Number Voice Play**: When enabled, the intercom will announce each number pressed on the keypad.
- **Ring Timeout**: The duration (in seconds) before the intercom will cancel an unanswered incoming call.

Intercom Settings | Audio

Configure audio parameters such as voice codec, speaker volume, MIC volume and ringer volume.

Audio Settings

- **Codecs**: Up to six codecs can be configured, in priority order.

  Available audio codecs are: G.711A/U, G.722, G.723.1, G.726-32, G.729AB.

- **DTMF Payload Type**: The RTP Payload type that indicates DTMF. Default is 101.
- **Default Ring Type**: Select from 9 standard ring types.
- **G.729AB Payload Length**: G.729AB payload length. Adjust from 10 – 60ms.
- **Tone Standard**: Select which country's tone set should be used to indicate busy/ringing/hang up.
- **G.722 Timestamps**: Select 160/20ms or 320/20ms.
- **G.723.1 Bit Rate**: Select 5.3kb/s or 6.3kb/s.

Volume Settings

- **Speakerphone Volume**: The volume level for broadcast audio.
- **MIC Input Volume**: Configure the microphone volume level for audio when the intercom calls a phone.
- **Broadcast Output Volume**: The volume level for audio received in phone calls.

- **Signal Tone Volume**: The ring volume level for tones when the intercom is called.
- **Enable VAD**: Voice Activity Detection (VAD).

  If VAD is enabled, the G729 Payload length cannot be greater than 20 milliseconds.

- **Disable AEC**: Selecting this option will disable Acoustic Echo Cancellation processing. AEC stops audio from the loudspeaker mixing in to the microphone.

AEC Settings

This feature is not supported.

Sound Update

This feature is not supported.

Sound Select

This feature is not supported.

Sound Delete

This feature is not supported.

Alert Info Ring Settings

This feature is not supported.

Intercom Settings | Video

This feature is not supported.

Intercom Settings | MCAST

This feature is not supported.

Intercom Settings | Action URL

This feature is not supported.

Intercom Settings | Time/Date

There are two methods for setting the time and date on the intercom.

- Simple Network Time Protocol (SNTP)
- Manual Time

Network Time Server Settings (SNTP)

- **Time Synchronized via SNTP**: Select to enable time-sync via SNTP protocol.
- **Time Synchronized via DHCP**: This feature is not supported.
- **Primary Time Server**: Set the address of the primary time server.
- **Secondary Time Server**: Set the address of the secondary time server.
- Select the appropriate **Time Zone**.
- Set the **Resync Period** (in seconds) for the device to resynchronize time with the server.

  60 seconds is the recommended setting.

Daylight Saving Time Settings

Select the **Location** and **DST Set Type** for Daylight Savings behavior.

Manual Time Settings

Before setting the time manually the SNTP and DHCP options need to be disabled.

To manually set the time, select the Year, Month, Date, Hour and Minutes, then click **Apply**.

Intercom Settings | Time Plan

This feature is not supported.

Intercom Settings | Trusted Certificates

This feature is not supported.

Intercom Settings | Device Certificates

This feature is not supported.

LED

This feature is not supported.

Security Settings

Input Settings

The Input settings define the input configuration that will trigger a security alert.

- **Input Detect**: Select to enable input detection.
- **Key**: Select the DSS key or call which will trigger the alert.
- **Trigger Mode**:
  - When set to **Low Level** the input will trigger when the connection is opened or disconnected.
  - When set to **High Level** the input will trigger when the connection is closed or connected.
- **Detection Duration**: The duration (in seconds) that the input must be activated before the alert will be triggered.

  If no duration is set the alert will not be triggered.
- **Alert message send to server**: When selected the intercom will send a **SIP** alert message to the server.
- **Reset Alert message send to server**: When selected the intercom will send reset messages to the server.

Output Settings

- **Output Response**: Select to enable the onboard output.
- **Output Level**:
  - When set to **High Level** output levels operate as specified in **Connection Terminals**.
  - When set to **Low Level** all contact output levels are inverted.
- **Output Duration**: The time (in seconds) that the output remains activated when a trigger occurs.

Alert Trigger Settings

Output

The Output settings allow you to configure the alert triggers that will activate the onboard output.

- **Input Trigger**: Whenever the input configuration meets the trigger condition the output will be triggered.
  - **Reset Mode**: The triggered output can be reset when the Input state changes or the Duration expires.
- **Remote DTMF Trigger**: Enables triggering the output by Dual Tone Multi Frequency.
  - **Trigger Code**: The DTMF code entered into a phone keypad to activate the output.
  - **Reset Code**: The DTMF code to reset the output.
  - **Reset Mode**: The triggered output can be reset when then DTMF State changes or the Duration expires.
- **Active URI Trigger**: Enables triggering by Uniform Resource Identifier. The output is activated/deactivated when an http get is called for **http://{intercom ip}/cgi-bin/ConfigManApp.com?egs&output{output number}={Trigger Message or Reset Message}**.
  - **Trigger Message**: The message to activate the output.
  - **Reset Message**: The message to reset the output.
- **Remote SMS Trigger**: Enables triggering by SMS message.
  - **Trigger Message**: The SMS message to activate the output.
  - **Reset Message**: The SMS message to reset the output.
- **Call State Trigger**: The output will be triggered when the call state of the intercom matches the selected state. The following options can be selected by moving the required state(s) to the **Enabled State** list.
  - Talking
  - Ringing
  - Calling
  - Calling and Talking

- Calling and Talking (Calling)
- Calling and Ringing
- Talking and Ringing
- Ringing and Talking (Called)
- Calling, Talking and Ringing

Ring

The Ring settings allow you to configure the tone to be played by the intercom.

- **Alarm Ring Duration**: Specifies the time (in seconds) the tone rings when triggered.
- The following triggers can activate the tone:
  - Input Trigger
  - Remote DTMF Trigger
  - Active URI Trigger
  - Remote SMS Trigger
- When set to Default the tone is activated by the trigger for the defined ring duration.
- When Disabled the tone will not be activated by the trigger.

Tamper Alarm Settings

- **Tamper Alarm**: Select to enable the tamper alarm.
- **Alarm Command**: Message sent as a SIP message when a tamper alarm is triggered.
- **Reset Command**: Message which should be received from the server to reset the tamper alarm.
- **Reset Alerting Status**: Stop the alarm immediately.
- **Ring Type**: When set to Default the alarm is activated for the defined ring duration when the tamper alarm is triggered. When Disabled the alarm will not be activated by the tamper alarm.

Server Settings

- **Server Address**: The IP or Domain of the server to send SIP messages to when the input or tamper alarm is triggered.
- **Message**: The message to be sent when the input or tamper alarm is triggered.

Function Key

The Function Key menu enables configuration of the call button function settings.

Function Key Settings

- **Type**: The Key Type can be set to Hot Key or None.
  - When set to **None** the call button is Disabled. The intercom will only be able to receive calls.
  - When set to **Hot Key** the call button will dial the configured phone number or IP address.
  - **Key Event**: This feature is not supported.
  - **Multicast**: This feature is not supported.
  - **PTT**: This feature is not supported.
- **Number 1**: The primary number or IP address to be called.
- **Number 2**: The secondary number or IP address to be called.

  This can be utilized for main/secondary calling or day/night operation.
- Select the SIP **Line** where required for Hot Key functionality.
- **Subtype**: The key subtype defines the action.
  - When set to **Speed Dial** pressing the key calls the configured number.
  - When set to **Intercom** pressing the key makes an IP call to the configured IP phone address.

Advanced Settings

- **Use Function Key to Answer**: When enabled the call button can be used to answer a call.
- **Enable Speed Dial Hangup**: When enabled the call button can be used to end a call.
- **Hot Key Dial Mode Select**:
  - When set to **Main-Secondary** Number 2 will be called when the first number is not answered.
    - The **Call Switched Time** defines the delay (in seconds) before switching to the secondary number.
  - When set to **Day-Night** Number 2 will be called when the call button is pressed during night hours.
    - Night hours are defined by the period outside the **Day Start Time** to **Day End Time**.
- **Speed Dial Time**: This feature is not supported.

Main/Secondary Operation

The intercom can be programmed to call a secondary number if the main number is not answered.

Function Key Settings

1. From the **Type** list select **Hot Key**.
2. In the **Number 1** field, enter the first number or IP address to call when the call button is pressed.
3. In the **Number 2** field, enter the number or IP address to call when the first number is not answered.
4. Select the corresponding **Line** (Line 1 or Line 2) for the SIP account.
5. From the **Subtype** list select **Speed Dial**.

Advanced Settings

1. **Hot Key Dial Mode Select**: set to **Main-Secondary**.
2. Click **Apply**.

Day/Night Operation

The intercom can be programmed to call a day number or night number, according to the call time settings.

Function Key Settings

1. From the **Type** list select **Hot Key**.
2. In the **Number 1** field, enter the number to call when the call button is pressed during day hours.
3. In the **Number 2** field, enter the number to call when the call button is pressed during night hours.
4. Select the corresponding **Line** (Line 1 or Line 2) for the SIP account.
5. From the **Subtype** list select **Speed Dial**.

Advanced Settings

1. **Hot Key Dial Mode Select**: set to **Day-Night** and click **Apply**.
2. Configure the **Day Start Time** and **Day End Time**.

   Number 1 will be called inside these hours and Number 2 will be called outside these hours.

3. Click **Apply**.

Standalone Functionality

The following section applies to standalone operation where the intercom does not integrate with Protege systems.

Unlock a Door with Your Phone

The intercom's onboard output is configured from the web interface for operating in standalone mode.

The following steps outline how to set up a code which can be entered during a VoIP call from an IP phone to the intercom, enabling the user to remotely open a door.

1. From the intercom web interface, navigate to the **Security Settings** menu.
2. In the **Output Settings** section, check the **Output Response** option.
3. Set the required **Output Level** setting for your door:
   - When set to High Level (NC:closed) the normally open contact will be open when deactivated and closed when activated.
   - When set to Low Level (NO:open) the normally open contact will be closed when deactivated and open when activated.
4. In the **Alert Trigger Setting | Output** section, check **Remote DTMF Trigger**.
5. Set the **Trigger Code** to the code that will be entered to unlock the door during a call.

   Valid characters for trigger code entry are: 0-9, * and #
6. If desired, set the **Reset Code** to the code that will be entered to re-lock the door.
7. To re-lock the door after a specified period, set the **Reset Mode** to By Duration.
   - Define the reset period (in seconds) in the **Output Duration**.
8. To re-lock the door when the call ends, set the **Reset Mode** to By State.
9. To play a tone when the door is unlocked by a code, in the **Alert Trigger Setting | Ring** section, set the **Remote DTMF Trigger** to Default.
   - Set the **Alarm Ring Duration** to the desired duration.
10. Click **Apply**.

Unlock a Door with REX

The intercom's onboard input can be connected to a REX device to request exit through a door.

Ensure the REX button is wired correctly into the input block of the intercom.

1. From the intercom's web interface, navigate to the **Security Settings** menu.
2. In the **Input Settings** section, check **Input Detect**.
3. Set the **Trigger Mode** according to your REX device:
   - If your REX device closes the circuit when pressed, set Trigger Mode to Low Level Trigger (Close Trigger).
   - If your REX device opens the circuit when pressed, set Trigger Mode to High Level Trigger (Disconnect Trigger).
4. In the **Output Settings** section, check the **Output Response** option.
5. Set the required **Output Level** setting for your door:
   - When set to High Level (NC:closed) the normally open contact will be open when deactivated and closed when activated.
   - When set to Low Level (NO:open) the normally open contact will be closed when deactivated and open when activated.
6. Set the **Output Duration** to the duration (in seconds) the door should unlock for.
7. In the **Alert Trigger Setting** section, check the **Input Trigger** option.
8. Set the **Reset Mode** to By Duration.
9. To play a tone when the door is unlocked, in the **Alert Trigger Setting | Ring** section, set the **Input Trigger** to Default.
   - Set the **Alarm Ring Duration** to the desired duration.
10. Click **Apply**.

Configuring the Tamper Alarm

The intercom can be set up to sound an alarm if there is an attempt to dismantle or tamper with the intercom.

1. From the intercom web interface, navigate to the **Security Settings** menu.
2. In the **Tamper Alarm Settings** section, check **Tamper Alarm**.
3. Set the **Ring Type** to Default to play a tone when a tamper is triggered.
4. Click **Apply**.

The alarm can be stopped via the web interface by clicking **Reset Alerting Status**.

Protege Integration

The following section describes how to integrate the intercom with a Protege system.

The intercom is added as a keypad with an input. This allows the intercom's input to be added to a floor plan or status page, set to trigger output follows input control, or used in advanced automation control programming.

Prerequisites

Before attempting this integration, ensure that the following requirements have been met:

Component	Firmware Version
Protege GX Controller	2.08.869 or higher
Protege WX Controller	4.00.409 or higher

The controller and intercom must also be able to communicate with each other. To achieve this they must either be on the same network, or you must configure the routers and firewalls on each network to allow them to connect.

Configuring the Intercom to Communicate with the Protege Controller

1. Enter the IP address of the intercom in your web browser.
2. Log in when prompted: default **User**: admin, **Password**: admin.
3. Navigate to the **Security Settings** menu.
4. In the **Server Settings** section, set the **Server Address** to the IP address of the Protege controller.
5. Click **Apply** to update.

Configuring the Onboard Input as a Protege Input

The intercom's onboard input can be configured as a Protege input to extend the power and functionality of your Protege system to the intercom.

To enable this functionality the intercom needs to be configured to communicate with the Protege controller.

1. From the intercom web interface, navigate to the **Security Settings** menu.
2. In the **Input Settings** section, check **Input Detect**.
3. Set the **Trigger Mode** as required:
   - If your input device closes the circuit when activated, set the Trigger Mode to Low Level Trigger (Close Trigger).
   - If your input device opens the circuit when activated, set the Trigger Mode to High Level Trigger (Disconnect Trigger).
4. Check **Alert message send to server**.
5. Click **Apply**.

Adding the Intercom Setup in Protege GX

1. Log in to your Protege GX system.
2. Navigate to **Expanders | Keypads** and select the controller the intercom will connect to.
3. Click **Add** and enter a **Name** that describes the intercom.
4. Assign the intercom an available **Physical Address**.
5. In the **Commands** section add the command: `IPICV2_IP=192.168.1.128`

   If the default IP of the intercom has changed, update the IP address in the above command accordingly.
6. Click **Save**. The **Configure Module** pop-up window will be displayed.
7. Set the **Inputs** to 1, **Outputs** to 0 and check **Add Trouble Inputs**, then click **Add Now**.
8. Navigate to **Programming | Inputs** and assign **Areas And Input Types** to the keypad's input record as required, then click **Save**.
9. Navigate to **Sites | Controllers** and select the controller the intercom is connected to. In the **Commands** section add the following command: `IPICV2=1`
10. When the controller download is complete, right click the controller and select **Module Addressing**.
11. In the pop-up window, locate the new Keypad record, identified by the **Address** assigned above.
12. Check that the Registered and Online columns display **True**. If so the intercom is successfully connected.

Adding the Intercom Setup in Protege WX

1. Log in to your Protege WX system.
2. Navigate to **Expanders | Keypads**.
3. Click **Add** and enter a **Name** that describes the intercom.
4. Assign the intercom an available **Physical Address**.
5. In the **Commands** section add the command: `IPICV2_IP=192.168.1.128`

   If the default IP of the intercom has changed, update the IP address in the above command accordingly.
6. Click **Save**.
7. Navigate to **Programming | Inputs** and create a record for the intercom's input.
8. Set the **Module Address** to the keypad address assigned above.
9. Assign **Areas And Input Types** as required, then click **Save**.
10. Navigate to **System | Settings**.
11. In the **Commands** section add the following command: `IPICV2=1`
12. Click **Save**.

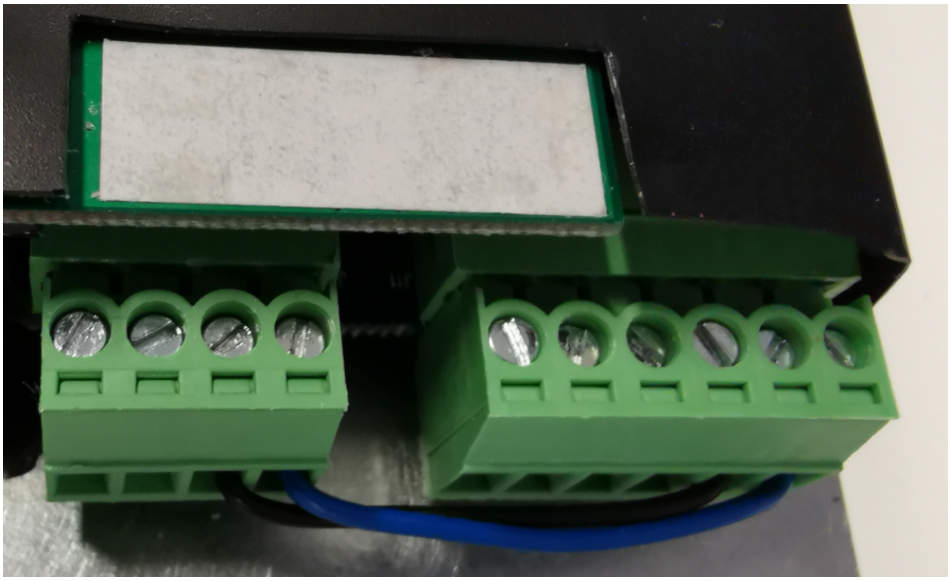
Intercom keypad records can also be added via the **Expanders Wizard**, however it will not Auto Detect the intercoms so they will need to be added manually as Additional Modules.

Trigger a Protege Input with Your Phone

The following steps outline how to set up a code which can be entered during a VoIP call from an IP phone to the intercom, enabling the user to remotely trigger a Protege input.

To enable this functionality the intercom unit's connection terminals need to be wired as below, with the input port contacts connected to the output port contacts:

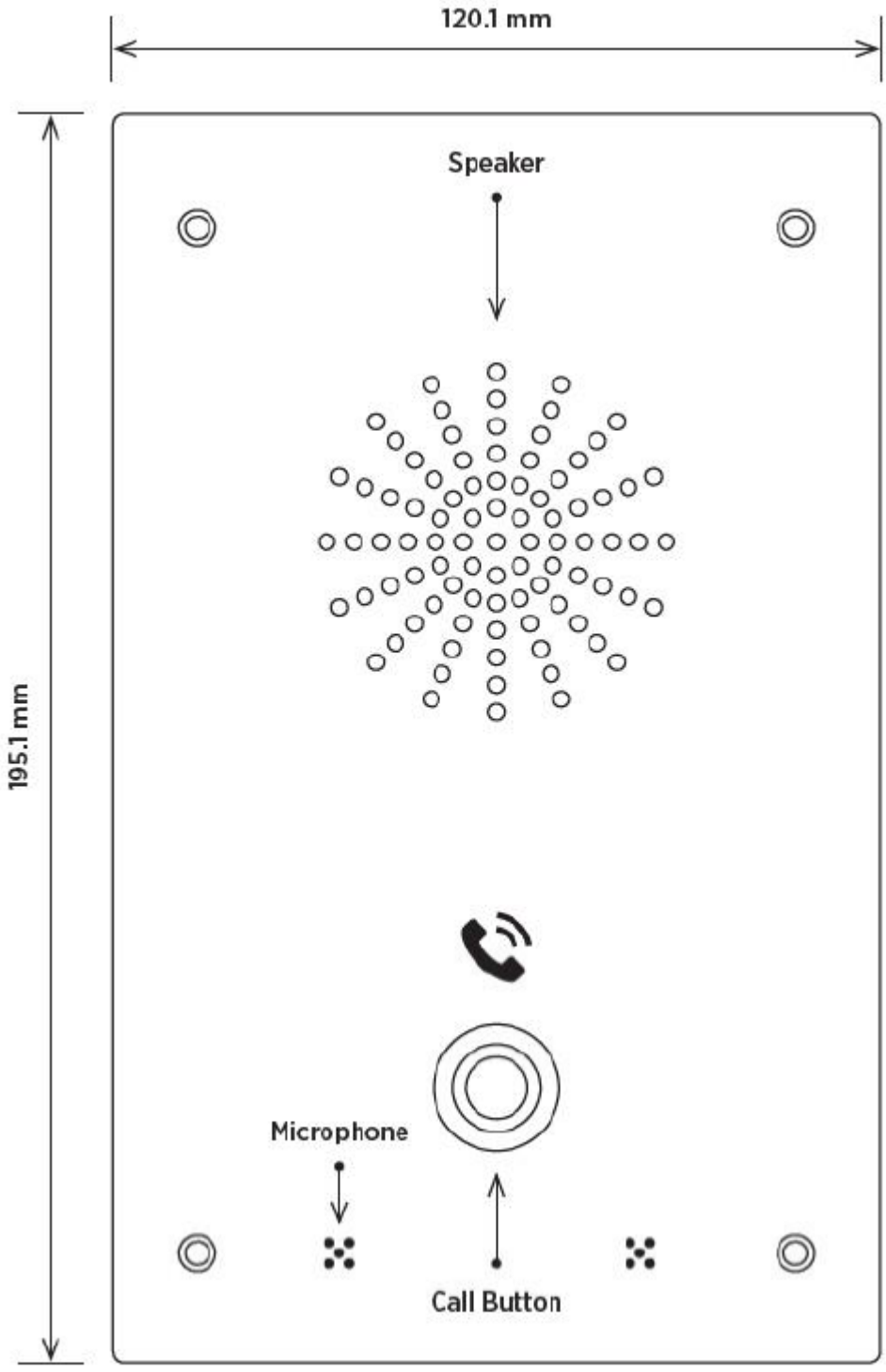
- The GND1 terminal connected to the COM1 (Common contact) terminal.
- The IN1 (Input 1) terminal connected to the NO1: (Normally open contact) terminal.



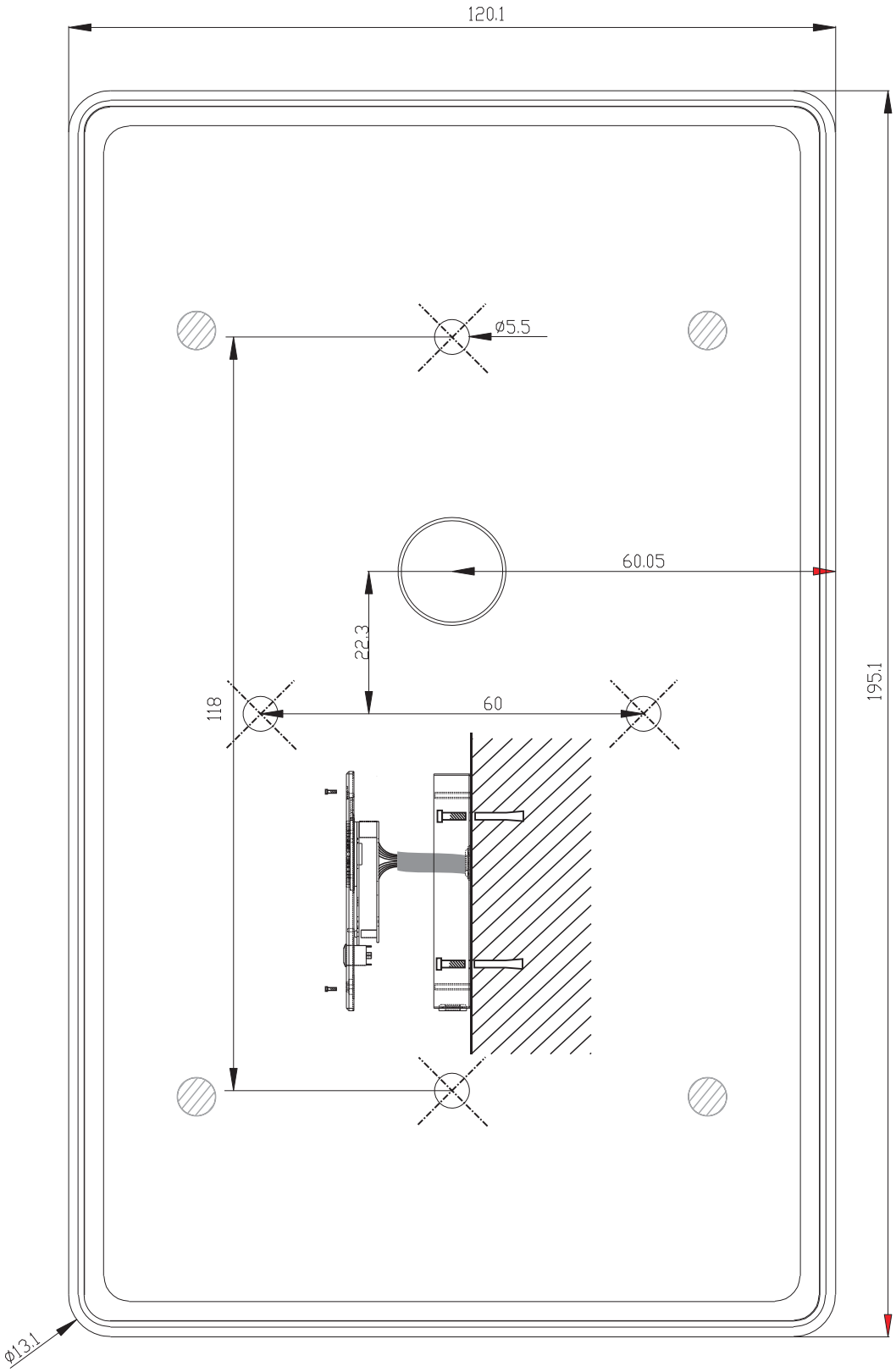
The intercom then needs to be configured to respond to the Remote DTMF Trigger.

1. Ensure that the intercom is online with the controller and has the onboard input enabled as described above (see page 35).
2. In **Security Settings | Input Settings**, set the **Trigger Mode** to High Level Trigger (Disconnect Trigger).
3. In the **Output Settings** section, check **Output Response**.
   - Set the **Output Level** to High Level (NC:closed).
   - Set the **Output Duration** to 1 second.
4. In the **Alert Trigger Setting | Output** section, check **Remote DTMF Trigger**.
   - Disable the **Input Trigger**.
5. Set the **Trigger Code** to the code that will be entered to trigger the input.
   (valid characters for trigger code entry are: 0-9, * and #)
6. Set the **Reset Mode** to By Duration.
7. To play a tone when the input is triggered, in the **Alert Trigger Setting | Ring** section, set **Remote DTMF Trigger** to Default.
   - Set the **Alarm Ring Duration** to the desired duration.
8. Click **Apply**.

Mechanical Diagram



Wall Mounting Template



Technical Specifications

The following specifications are important and vital to the correct operation of this product. Failure to adhere to the specifications will result in any warranty or guarantee that was provided becoming null and void.

Ordering Information		
PRT-IPIC-POE		Protege Vandal Resistant VoIP Intercom
Power Supply		
Operating Voltage		12VDC (9 -16VDC)
Operating Current		1A
Power over Ethernet		IEEE 802.3af Class 3
Communication		
Communication protocol		SIP 2.0(RFC-3261)
Speech flow	Protocols	RTP/SRTP
	Decoding	G.729 G.723 G.711 G.722 G.726 Codecs
	Audio Amplifier	2.5W
	Volume Control	Adjustable
	Full duplex speakerphone	Support (AEC)
Port	Recording output	One (3.5mm terminal block)
	Short circuit input	Two (3.5mm terminal block)
	Short circuit output	Two Form C relays (3.5mm terminal block) 24V DC 1A
	WAN port	10/100BASE-TX s Auto-MDIX, RJ-45
	Cables	CAT5 or better
Audio		
Microphone		Omnidirectional
Speaker		TY 4 ohm 3W
Dimensions		
Overall dimensions		195 x 120 x 39mm (7.67 x 4.72 x 1.53")
Net Weight		960g (33.9oz)
Gross Weight		1200g (42.3oz)
Environment		
Environmental IP Rating		IP65
Working Temperature		-40° to 70° Celsius (-40° to 158° Fahrenheit)
Storage Temperature		-40° to 70° Celsius (-40° to 158° Fahrenheit)
Working Humidity		10% to 95%

Integrated Control Technology continually strives to increase the performance of its products. As a result these specifications may change without notice. We recommend consulting our website (www.ict.co) for the latest documentation and product information.

New Zealand and Australia

General Product Statement

The RCM compliance label indicates that the supplier of the device asserts that it complies with all applicable standards.

European Standards

CE Statement CE

Conforms where applicable to European Union (EU) Low Voltage Directive (LVD) 2014/35/EU, Electromagnetic Compatibility (EMC) Directive 2014/30/EU, Radio Equipment Directive (RED)2014/53/EU and RoHS Recast (RoHS2) Directive: 2011/65/EU + Amendment Directive (EU) 2015/863.

This equipment complies with the rules, of the Official Journal of the European Union, for governing the Self Declaration of the CE Marking for the European Union as specified in the above directive(s).

WEEE 

Information on Disposal for Users of Waste Electrical & Electronic Equipment

This symbol on the product(s) and / or accompanying documents means that used electrical and electronic products should not be mixed with general household waste. For proper treatment, recovery and recycling, please take this product(s) to designated collection points where it will be accepted free of charge.

Alternatively, in some countries you may be able to return your products to your local retailer upon purchase of an equivalent new product.

Disposing of this product correctly will help save valuable resources and prevent any potential negative effects on human health and the environment, which could otherwise arise from inappropriate waste handling.

Please contact your local authority for further details of your nearest designated collection point.

Penalties may be applicable for incorrect disposal of this waste, in accordance with your national legislation.

For business users in the European Union

If you wish to discard electrical and electronic equipment, please contact your dealer or supplier for further information.

Information on Disposal in other Countries outside the European Union

This symbol is only valid in the European Union. If you wish to discard this product please contact your local authorities or dealer and ask for the correct method of disposal.

EN50131 Standards

This component meets the requirements and conditions for full compliance with EN50131 series of standards for equipment classification.

EN 50131-1:2006+A2:2017, EN 50131-3:2009, EN 50131-6:2008+A1:2014, EN 50131-10:2014, EN 50136-1:2012, EN 50136-2:2013, EN 60839-11-1:2013

Security Grade 4
Environmental Class II
Equipment Class: Fixed
Readers Environmental Class: IVA, IK07
SP1 (PSTN – voice protocol)
SP2 (PSTN – digital protocol)
SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + PSTN)
SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + USB-4G modem)

Tests EMC (operational) according to EN 55032:2015
Radiated disturbance EN 55032:2015
Power frequency magnetic field immunity tests (EN 61000-4-8)

EN50131

In order to comply with EN 50131-1 the following points should be noted:

- Ensure for Grade 3 or 4 compliant systems, the minimum PIN length is set for 6 digits.
- To comply with EN 50131-1 Engineer access must first be authorized by a user, therefore Installer codes will only be accepted when the system is unset. If additional restriction is required then Engineer access may be time limited to the first 30 seconds after the system is unset.
- Reporting delay –Violation off the entry path during the entry delay countdown will trigger a warning alarm. The warning alarm should not cause a main alarm signal and is not reported at this time. It can be signaled locally, visually and or by internal siren type. If the area is not disarmed within 30 seconds, the entry delay has expired or another instant input is violated, the main alarm will be triggered and reported.
- To comply with EN 50131-1 neither Internals Only on Part Set Input Alarm nor Internals Only on Part Set Tamper Alarm should be selected.
- To comply with EN 50131-1 Single Button Setting should not be selected.
- To comply with EN 50131-1 only one battery can be connected and monitored per system. If more capacity is required a single larger battery must be used.
- For Security Grade 4 installations, two forms of reporting are required. This can be satisfied using the onboard 2400bps modem included with the modem controller model, or through the incorporation of the PRT-4G-USB cellular modem module into the installation with the non-modem controller model.

Anti Masking

To comply with EN 50131-1 Grade 3 or 4 for Anti Masking, detectors with a separate or independent mask signal should be used and the mask output should be connected to another input.

I.e. Use 2 inputs per detector. One input for alarm/tamper and one input for masking.

To comply with EN 50131-1:

- Do not fit more than 10 unpowered detectors per input,
- Do not fit more than one non-latching powered detector per input,
- Do not mix unpowered detectors and non-latching powered detectors on an input.

To comply with EN 50131-1 the Entry Timer should not be programmed to more than 45 seconds.

To comply with EN 50131-1 the Bell Cut-Off Time should be programmed between 02 and 15 minutes.

EN 50131-1 requires that detector activation LEDs shall only be enabled during Walk Test. This is most conveniently achieved by using detectors with a Remote LED Disable input.

UK Conformity Assessment Mark

General Product Statement

The UKCA Compliance Label indicates that the supplier of the device asserts that it complies with all applicable standards.

FCC Compliance Statements

FCC Rules and Regulations CFR 47, Part 15, Subpart B

This equipment complies with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

Industry Canada Statement

ICES-003

This class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CAN ICES-3 (A)/NMB-3(A)

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.