PRT-MOB-IF

Protege Config App

User Guide

Last Published: 15-Jun-22 2:12 PM

Contents

Introduction

The Protege Config App is specifically designed to provide a secure, convenient and flexible method for programming a **Bluetooth®** Wireless Technology enabled card reader.

Use the Protege Config App to easily configure LED colors, define the Bluetooth® read range, set the reader to firmware update mode or factory default the reader. A configurable hex setting also provides the flexibility of programming custom TLVs for advanced programming. All of this can be achieved with a couple of taps on your smartphone or mobile device.

Prerequisites

Config App

To use the Config App you will need:

- An app account
- A mobile credential

If you already have a Protege Mobile App account and mobile credential (product code: PRX-MCR), these same login credentials can be used to access the Config App.

If you do not have a Protege mobile credential, contact ICT Customer Services to be issued one for use with the Config App. You can make a new app account after installing the app (see page 6).

Card Reader

To use the Config App to program a card reader, the reader must meet the following requirements:

- Firmware version 1.04.254 or higher
- Bluetooth® capability
- RGB LEDs (if configuring LED colors)

Firmware version: It is not possible to specifically identify the firmware version on a reader. The version the reader was shipped with can be checked by contacting ICT Technical Support and providing the reader's serial number. Alternatively, upgrade the firmware to a known compatible version.

Bluetooth® capability: The sticker on the back of the reader identifies the hardware configuration. The Model code must contain **BT** to signify that the reader is Bluetooth® enabled.

Confirming Compatibility

Reader compatibility can be easily checked using the Config App. When programming the reader (see page 11), tap **Select Reader** to display a list of nearby readers that can be contacted over Bluetooth®. If the reader's serial number is displayed as a **Broadcast Address** (preceded by _R), the reader is compatible with the Config App.

If only the reader model is displayed, but not its serial number, then it cannot currently be configured using the app. The reader most likely requires a firmware upgrade before it can be configured using the app.

Programming Summary

To program a card reader using the Config App:

1. Log in to the app using your app account.
2. Select your **Credential Profile**.

   Your credential profile is automatically assigned to your app account with your mobile credential, and is based on the credential issuer and the site the credential was allocated to.

3. Create a **Reader Configuration** (config) comprising the required TLV settings.
4. Activate Bluetooth® on your device (if not already activated).
5. Power cycle the reader you want to program.
6. Select the **config** to program the reader with.
7. Apply the configuration to the reader, within two minutes of startup. Hold your mobile device close to the reader and tap **Scan Closest** to apply the configuration.

When programming is successful the reader will beep 4 times quickly, then restart.

Installing the App

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

Downloading for Android Devices

1. On your Android device, navigate to the **Google Play Store**.
2. Enter **Protege Config** into the search bar.
3. Select the **Protege Config** App.
4. Tap **Install**.

Downloading for iPhone / iPad

1. On your iOS device, navigate to the **App Store**.
2. From the search bar, enter **Protege Config**.
3. Select the **Protege Config** App.
4. Tap **GET**.

Logging In

The Protege Config App uses the same account credentials as your Protege Mobile App. If you already have an account on the Mobile App, you can simply use the same account to log in to the Config App.

While the Config App and Mobile App can operate at the same time, the Mobile App can interfere with Bluetooth® connections from the Config App and cause programming to fail, so it is strongly recommended to close the Mobile App before logging in to the Config App.

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

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

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

Logging In for the First Time

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

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

3. If creating a new account, you will be prompted to create new credentials (username and password) for use with this account. If signing in with social media, you may be asked to enter your credentials, or you may proceed automatically if you are logged in on your device.
4. When your login method is accepted, you will be presented with the End-User License Agreement. To continue, read through the agreement and tap **Accept**.

   This screen is only displayed after your first login.

5. Next you will be prompted to create a PIN for use with this account. Enter a unique four-digit PIN code, then re-enter the same PIN to verify it.
6. From the drop-down, select how frequently you would like to be prompted to enter this PIN while using the Config App.

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

Config App Navigation and Settings

You can navigate the Config App via the menu in the top left of the app. The following pages are available.

- **Reader Configuration**: All configuration and reader programming is performed through this page.
- **Security Settings**: Set and change your PIN and the frequency of PIN requests.
- **Mobile Credential Settings**:
  - View the details of your **Mobile Credentials**.
  - Set the **Bluetooth Proximity** (read distance for this device).
  - **Scan to Unlock** a reader. This feature transmits your credential to allow convenient testing when programming reader functions, without needing to switch to the Protege Mobile App.
- **Logout**: Logs you out of the Config App.

Reader Configuration

When you first access the reader configuration page you will be prompted to select your Credential Profile. Your profile is automatically assigned to your app account with your mobile credential, based on the issuer of the credential, and typically corresponds to the site or group your credential was allocated to.

If you do not have a credential profile, contact ICT Customer Services.

Config Options

A config is a configuration profile consisting of any number of TLV (Type Length Value) settings that provide configuration programming for ICT card readers.

- To create a new config, tap the **+** at the top right. Enter a **Config name** and add one or more **TLV** settings. Then **Save** the new config.

  Config programming examples are provided later in this document (see page 13).

- All existing configs are displayed on the **Reader Configuration** page.
- Edit or delete configs by swiping left on the config list, then tapping the **Edit** or **Delete** icon.

Important: Many of the available TLV settings contain advanced configuration options that may render a reader unusable if applied incorrectly. Please ensure that you understand these settings and their impact before implementation, or call ICT Technical Support for assistance.

TLV Settings

- **Update Key (NFC & Bluetooth)**: Update the programmed credentials in the reader to match those of the Protege mobile profile.
- **Keyslot**: This setting is used to load custom encryption keys onto the reader. Must be used in conjunction with **Credential Type** and **Credential Format Link** settings.

  For use of this feature, see Application Note 269: Configuring a Custom Mobile Credential.

- **LED Mode**: Choose between normally green, normally blue or dual LED mode.
- **Backlight Level**: Set the brightness of the keypad backlight (if fitted).
- **Device Mode**: Factory default the reader or put it into firmware update mode.

  Note: This must be the first TLV in the config.

- **Wiegand Style**: Select the Bit Length Style the reader will output and define Enforce options.
- **125kHz Formats**: Enable/Disable specific 125kHz card types.

  - Postech
  - HID
  - ICT
  - Guardtek
  - Em41xx
  - PSK

    PSK card formats require specific hardware to operate.
  - Guardall G-ProxII

    Guardall G-ProxII card formats require specific hardware to operate.

- **Output Mode**: Select Wiegand, ICT smart reader (RS-485) or custom serial (RS-485) output.

  The output mode automatically switches to ICT RS-485 when plugged in. Instructions for programming OSDP output mode are provided below (see page 13), or see Application Note 321: Configuring ICT Readers for OSDP Communication.
- **Tamper**: Enable intelligent tamper for detecting readers that have been disconnected.
- **Clone Card Options**: This is a legacy option that has no effect.
- **Custom RS485 Format**: Configure the output format of data when in custom RS-485 output mode.
  - %s = Site Decimal
  - %S = Site Hex
  - %c = Card Decimal
  - %C = Card Hex
  - %e = CSN Decimal
  - %E = CSN Hex
  - %p = Padded CSN Decimal
  - %P = Padded CSN Hex

  For example: "%s:%c" will output 233:4555 for a card with a Site Code of 233 and Card Number of 4555.
- **Card Settings Lock**: Locks access to the card settings.

  Before enabling the card settings lock, ensure that there is a key in slot 0. Once the card settings lock has been enabled any further configuration of the reader requires logging in with the correct key matching slot 0. If there is no key in slot 0 when the lock is applied, the reader will no longer be configurable.
- **Card Settings Lock Login**: Reader login which allows access and modification of settings on locked readers.

  This requires entry of the key matching slot 0 as noted above.
- **Access Credentials**: Customize the configuration for reading of different types of credentials.

  Changing this setting has the potential to render the reader unusable.
- **Card Linkages**: Link credential types, custom card formats and encryption keys.

  Changing this setting has the potential to render the reader unusable.
- **CSN Reading Mode**: Enable/Disable reading of CSN for MIFARE, DESFire, and other NFC cards.
  - Enable CSN reading for all ISO14443a3 capable cards (e.g. MIFARE)
  - Enable CSN reading for all ISO14443a4 capable cards (e.g. DESFire)
  - Optionally reverse either of the CSN readings
  - ISO15693 capable cards are no longer supported

  CSN will only be sent from the reader if the card cannot be read using any of the configured credentials.
- **PSK Decryption**: Enable the reader to read Kantech, Tecom or Motorola cards for PSK capable readers.

PSK card formats require specific hardware to operate.

- **Keypad Output Format**: Choose the format that the keypad input will use.
- **Low Frequency Flags**: Enable/Disable reading of legacy HID low frequency formats.
- **Custom Card Format Slots**: Allows the entry of a custom format string which describes how to interpret data from the card being read.

Changing this setting has the potential to render the reader unusable.

- **ISO14443 Modulation and Gain**: Customize modulation and gain settings as required.

Changing this setting has the potential to stop the reader from reading all cards, including programming cards.

- **LED Color Settings**: The reader has an internal palette of 16 configurable colors. The Index in the color settings refers to a slot number in the palette. For example, the reader normally uses slots 5 and 11 to show Unlocked (green) and Locked (blue) respectively. The other slots in the palette are used for other functions (for example, to indicate area state, function codes, two factor authentication required).

See below for a programming example using LED color configuration (see page 14).

- **BLE TX Power**: This is a legacy option that has no effect.
- **Wiegand Site Code**: Configure the site code sent with keypad input when in 26 bit and 36 bit keypad output formats.
- **Bluetooth Reader Range**: Configure the distance for the mobile app to attempt to unlock the door.

This setting is a percentage (100% by default) so setting at 200 will cause the app to open the door from approximately double the range.

- **Reread Mode**: Allow the reader to continuously reread a card that is kept within range. The reader can also be set to silently reread the card. This option can be used with the PRX-TSEC-XCDH card holder cover.
- **Reader Address**: Set the address configuration for ICT RS485, OSDP or Smart Serial connections.
- **Uart Configuration**: Set the baud rate and other settings of the RS-485 for compatibility with third-party systems.
- **Hex**: An open field for entering a hex code to program a custom TLV.

This setting requires high level understanding of TLV programming and should not be used unless directed by documentation or the ICT Technical Support team. This setting has the potential to render a reader unusable.

Programming a Card Reader

Once the required reader config is available in the Config App, it can be applied to individual readers via Bluetooth® communication.

ICT card readers can only be programmed within 2 minutes of startup. In order to program the reader you will need to disconnect power and complete programming within 2 minutes of powering up.

To program a Card Reader using the Protege Config App

1. Activate Bluetooth® on your device.
2. In the Config App, navigate to the **Reader Configuration** page and select the appropriate **Credential Profile**.
3. Tap the required config to apply to the reader. The selected config will be marked as ACTIVE.
4. Power cycle the reader that requires programming. The following steps must be completed in the next 2 minutes.
5. To apply the selected config to the nearest reader, place the device with the app close to the reader and tap **Scan Closest**.
   - The app should display Connecting to reader _R<SERIALNUMBER>. If there is no response, the device may need to be closer to the reader.
   - When programming is successful, the app will display the message Configuration of _R<SERIALNUMBER> successful and the reader will beep several times quickly and then restart.
   - If a power cycle is required, the app will display the message Failed to configure _R<SERIALNUMBER>. Configuration timeout. Please restart the reader.
6. To view and select from a list of nearby readers, tap **Select Reader**.
   - If the reader is compatible, its **Broadcast Address** (_R<SERIALNUMBER>) will be displayed in the list.
   - If only the reader model is displayed, this reader cannot be configured using the app.
   - The number to the right identifies the decibel response. The smaller the value (i.e. the closer to zero), the nearer the reader is to the device.

     The **Bluetooth Proximity** setting in **Mobile Credential Settings** can be adjusted to exclude readers that are further away.
7. Identify the appropriate reader and tap **Apply**.
   - The app should display Connecting to reader _R<SERIALNUMBER>.
   - When programming is successful, the app will display the message Configuration of _R<SERIALNUMBER> successful and the reader will beep several times quickly and then restart.
   - If a power cycle is required, the app will display the message Failed to configure _R<SERIALNUMBER>. Configuration timeout. Please restart the reader.
   - If the reader is not compatible, the app will display the message Failed to configure <READER>. Reader disconnected.

Failed Programming

Sometimes reader programming can fail. This may occur because of Bluetooth® connection interference, such as from the Mobile App, invalid config programming, or incorrect reader firmware.

If programming is unsuccessful, the reader will respond with **3 long beeps** (as opposed to the 4 short beeps when programming is completed successfully), and then restart.

If reader programming fails you should attempt to apply the config to the reader again, as the failure may have been caused by temporary interference.

If the reader continues to reject the programming, attempt to apply a previously applied config. Depending on the outcome, the new config may need to be checked or firmware may need to be updated. Previous programming may also need to be reapplied if there is a chance that earlier programming was unsuccessful.

Config Programming Examples

The following examples illustrate programming some common card reader configuration requirements, using the Config App.

Config Example: Enable OSDP

The following programming example demonstrates how to create a config that enables the card reader to use the OSDP communication protocol.

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.
3. **Add** a new **Reader Configuration** called OSDP Output Mode.
4. Tap the **Add TLV** dropdown and select the **Hex** option.
5. In the **Hex** field, enter the OSDP output mode hex code **`0B0104`**, then tap **Save**.

You can now apply the configuration to the required reader(s). Power cycle the reader and select and apply your new OSDP Output Mode config within two minutes of startup.

Config Example: OSDP Baud Rate

For a card reader operating in OSDP mode to communicate with an OSDP server, the reader must have the same baud rate setting as the reader port it is connected to. The default reader baud rate is 38400.

ICT card readers support the following baud rates:

Supported Baud Rates
4800 baud
9600 baud
19200 baud
38400 baud (default)
57600 baud
115200 baud

The following programming example demonstrates how to create a config that sets the reader baud rate to 9600.

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.
3. **Add** a new **Reader Configuration** called Baud Rate 9600.
4. Tap the **Add TLV** dropdown and select the **Uart Configuration** option.
5. Set the **Baud** to 9600, then tap **Save**.

You can now apply the configuration to the required reader(s). Power cycle the reader and select and apply your new Baud Rate 9600 config within two minutes of startup.

For more information on configuring readers to communicate using OSDP protocol , see Application Note 321: Configuring ICT Readers for OSDP Communication.

Config Example: Set Wiegand Output Mode

To configure the reader to output Wiegand data:

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.
3. **Add** a new **Reader Configuration** called Wiegand Output Mode.
4. Tap the **Add TLV** dropdown and select the **Output Mode** option.
5. Set the **Output Mode** to Wiegand Output, then tap **Save**.

You can now apply the configuration to the required reader(s). Power cycle the reader and select and apply your new Wiegand Output Mode config within two minutes of startup.

Config Example: Enable Dual LED Mode

By default ICT card readers operate in single LED mode (when wired in Wiegand configuration). To enable dual LED mode, you need to change its configuration.

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.
3. **Add** a new **Reader Configuration** called Dual LED Mode.
4. Tap the **Add TLV** dropdown and select the **LED Mode** option.
5. Set the **LED Mode** to Dual, then tap **Save**.

You can now apply the configuration to the required reader(s). Power cycle the reader and select and apply your new Dual LED Mode config within two minutes of startup.

Config Example: LED Colors

The following programming example demonstrates how to create a config that changes the LED colors displayed by card reader to indicate when a door is locked or unlocked.

1. In the Config App, navigate to the **Reader Configuration** page and select the appropriate **Credential Profile**.
2. Tap the **+** icon (top right) to create a new config. Give the config a **Name**.
3. Tap **Add TLV** to open the dropdown.
4. Select **LED Color Setting** and tap **OK**.
5. Tap on the **Color** field to display color details. Select a color by tapping (not dragging) on the color picker. Alternatively, you can type a color code into the field below the color picker. Tap the **Arrow** icon to switch between Hex, RGB and HSL color codes.

   Note that the color displayed by the reader LEDs will not perfectly match the screen of your device.
6. Tap on the **Index** field to enter an index number. Each index corresponds to a particular function of the card reader. In this case, select 5, which represents the Door Unlocked function.
7. Tap **Save**.
8. **Add** another TLV with the **LED Color Setting** option. Select another color as required.
9. Set the **Index** to 11, corresponding to the Door Locked function. Tap **Save**.
10. Tap **Save** again to save the config.

You can now apply the configuration to the required reader(s). Power cycle the reader and select and apply your new LED configurations within two minutes of startup.

Config Example: ISO14443 Gain for EV2 Tags

The ISO 14443 Modulation and Gain TLV is used to customize reader modulation and gain settings to allow the reader to read specific frequency formats. This setting configures the MFRC522 NFC chip, which controls the 13.56MHz antenna. MIFARE , DESFire and mobile NFC are all affected by this setting.

This setting has the potential to prevent the reader from reading 13.56MHz cards, including programming cards.

To read DESFire EV2 tags, the ISO14443 gain should be set to 6. Some card reader firmware versions do not contain the required ISO14443 gain configuration by default, so it is necessary to program the configuration.

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.
3. **Add** a new **Reader Configuration** called ISO14443 Gain for EV2 Tags.
4. Tap the **Add TLV** dropdown and select the **Hex** option.
5. In the **Hex** field, enter the ISO14443 Gain 6 Hex code **`180106`**, then tap **Save**.

You can now apply the configuration to the required reader(s). Power cycle the reader and select and apply your new ISO14443 Gain for EV2 Tags config within two minutes of startup.

Config Example: Reader Address

For protocols which support reader addressing, the address of a reader can be programmed via TLV configuration.

This TLV is only valid for protocols which support addressing (ICT RS485, OSDP or Smart Serial).

- This can be used to configure an RS-485 reader as an entry (0) or exit (1) reader.
- For a card reader operating in OSDP mode to be recognized on a third-party system, the reader address may need to be configured to meet the third-party system's addressing requirements.

For the tSec range of readers the address can only be programmed when the reader's green and orange wires are **not** connected together.

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.
3. **Add** a new **Reader Configuration** named appropriately (e.g. Reader Address 01 - Exit Reader).
4. Tap the **Add TLV** dropdown and select the **Reader Address** option.
5. Set the **Reader Address** to the required address, then tap **Save**.

You can now apply the configuration to the required reader(s). Power cycle the reader and select and apply your new reader address config within two minutes of startup.

Config Example: Firmware Update Mode

Before firmware can be updated on ICT card readers, the reader must be put into firmware update mode, also know as boot mode.

This must be the **first** TLV in the config.

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.
3. **Add** a new **Reader Configuration** called Firmware Update Mode.
4. Tap the **Add TLV** dropdown and select the **Device Mode** option.

   As it needs to be the first TLV in the config, the Device Mode TLV will be added above any existing TLVs.
5. Tap the dropdown and select **Firmware Update Mode**.
6. Tap **Save**.

You can now apply the configuration to the required reader(s). Power cycle the reader and select and apply your new Firmware Update Mode config within two minutes of startup.

When the config is applied the LEDs on the reader will flash to indicate it is starting in boot mode. The flashes will then slow to indicate the reader is in boot mode and ready for the firmware update. You will have approximately 30 seconds from the time you power the reader to load the firmware.

Config Example: Factory Default

The following programming example demonstrates how to create a config that will default the reader back to its shipped factory default configuration.

This must be the **first** TLV in the config.

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.
3. **Add** a new **Reader Configuration** called Factory Default.
4. Tap the **Add TLV** dropdown and select the **Device Mode** option.

   As it needs to be the first TLV in the config, the Device Mode TLV will be added above any existing TLVs.
5. Tap the dropdown and select **Factory Default EEProm**.
6. Tap **Save**.

You can now apply the configuration to the required reader(s). Power cycle the reader and select and apply your new Factory Default config within two minutes of startup.

This **cannot be undone**. Once the reader is defaulted you will need to reapply all configuration programming.

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.