PRT-MOB-IF

Protege Config App

User Guide

Last Published: 12-Jan-23 12:00 PM

Contents

Introduction

The Protege Config App is specifically designed to provide a secure, convenient and flexible way to program a **Bluetooth**® enabled ICT card reader.

Use the Config App to easily configure credential formats, set the reader address or baud rate, program the LED mode, put the reader into 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 few taps on your 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 7).

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 22), 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 (e.g. 'TSEC') 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.

Account Binding

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

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 Config App

To begin using the Protege Config App you will first need to download and install it on your mobile device. The 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**.

Updating the Config App

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

Updating for Android Devices

1. On your Android device, navigate to the **Google Play Store**.
2. At the top right, tap the profile icon.
3. Tap **Manage apps & device**. Apps with an update available are labeled 'Update available'.
4. Beside the Protege Config App, tap **Update**.

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

Updating for iPhone / iPad

1. On your iOS device, navigate to the **App Store**.
2. Tap your profile icon at the top of the screen.
3. Scroll to see pending updates and release notes.
4. Beside the Protege Config App, tap **Update**.

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

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.

On startup, a warning will advise you to close the Mobile App before configuring any readers. While the Config App and Mobile App can operate at the same time, transmissions from the Mobile App may interfere with Bluetooth® connections from the Config App and cause reader programming to fail.

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 select 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 **Account 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.
- **Account Settings**: Set and change your PIN and PIN request frequency. View and delete your account data.
- **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.

Account Settings

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

Changing the Security Level

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

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

Changing your PIN

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

Deleting your PIN

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

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

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

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

Deleting your Account

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

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

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

Mobile Credential Settings

Each device that has the Protege Config App installed is assigned a set of mobile credentials that you can use to unlock Protege controlled doors using Bluetooth®. These mobile credentials can be used with compatible card readers to allow convenient testing of reader programming without needing to switch to the Mobile App.

1. Open the main menu.
2. Tap **Mobile Credential Settings**.
3. The **Mobile Credentials** include the site code and card number (Credential) assigned to your device.
4. Use the **Bluetooth proximity** slider to set the Bluetooth® field range of your device. Setting the field towards Near means that your device won't communicate with the reader until it is presented very close to it. By setting the field towards Far you can use your device to unlock a door from a greater distance.
5. **Scan to unlock**: Unlocks the nearest door when in range. The range is determined by the Bluetooth® Proximity slider setting described above. This option requires **Bluetooth®** enabled on your phone.

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 Management

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

Config programming examples are provided later in this document (see page 24).

1. To create a new config, tap the **+** at the top right of the screen.
2. Enter a **Config name** to describe the profile you are configuring.
3. Tap **Add TLV** and select the required TLV setting from the list, then configure any associated settings.
4. Once all **TLV** settings are configured, **Save** the new config.

All saved configs associated with your account are displayed on the **Reader Configuration** page. Edit or delete configs by swiping left on the config, then tapping the **Edit** or **Delete** icon.

TLV Settings

The following TLV settings are available in the Protege Config App.

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.

Update Key (NFC & Bluetooth)

This TLV can be used to conveniently update the custom mobile encryption key and associated card linkages programmed on the reader with the mobile credential encryption key associated with the **credential profile**.

This only applies to sites which have a custom mobile credential with a registered encryption key.

For more information, see Config Example: Custom Mobile Credential (page 31).

- **Keyslot**: Specifies the mobile credential slot where the mobile credential encryption key will be stored.

Mobile Credential Keyslot

This setting is used to load custom mobile credential encryption keys onto the reader so that it can read a custom mobile access credential. It must be used in conjunction with the **Card Linkages** TLV (see page 16) to enable the NFC and Bluetooth® functionality to read the custom credential from the assigned keyslot.

This only applies to sites which have a custom mobile credential with a registered encryption key.

For more information, see Config Example: Custom Mobile Credential (page 31).

- **Keyslot** Specifies the mobile credential slot where the mobile credential encryption key will be stored.

Keyslots 0 and 1 are reserved for the card settings lock login and OSDP session key respectively.

Keyslot Availability

Keyslot	Description
0	Card Settings Lock Login
1	OSDP Session Key
2	Available
3	Available
4	Available

While slots 0 and 1 can be used if not required for the card settings lock login or OSDP session key, it is recommended to avoid using these keyslots to prevent potential future issues if the configuration changes.

LED Mode

Set the reader to use either normally blue, normally green or dual LED mode.

The default setting is single LED mode, normally blue.

- **LED Mode**:
  - Dual: Allows the signaling of both LEDs independently using the LED control lines
  - Blue: Blue LED is on by default
  - Green: Green LED is on by default

Dual LED mode requires the reader to be wired with both the orange and brown LED control lines connected.

Backlight Level

Set the brightness of the keypad backlight (for readers with keypads).

- **Backlight Level**:
  - Disabled
  - Very Low
  - Low (default setting)
  - Medium
  - High
  - Very High

Device Mode

The Device Mode TLV is used to factory default the reader or put it into an update mode.

The device mode must be the first TLV in the config, so when you add this TLV it will be automatically placed above any other TLVs programmed previously.

- **Device Mode**:
  - Firmware Update Mode: Put the reader into boot mode so that new firmware can be loaded.
  - Factory Default EEPROM: Default the reader back to its shipped factory default configuration.

    This **cannot be undone**. Once the reader is defaulted you will need to reapply all configuration programming.
  - OSDP Install Mode: Put the reader into OSDP installation mode so that it is ready to accept initiation of a secure channel session from the connected controller or module.

Wiegand Style

Define the bit length style the reader will output, and specify transmission enforcement options.

- **Style**: Specify the bit length for the Wiegand output.
  - 26 Bit Output
  - 27 Bit Output
  - 32 Bit Output
  - 34 Bit Output
  - Legacy Undefined Output: This is a legacy option that has no effect.
  - Legacy Undefined Output: This is a legacy option that has no effect.
  - 66 Bit Output
  - 37 Bit Output
  - 64 Bit Output
  - 37 Bit (No Site Code)
  - Kantech KSF Format
  - Legacy Undefined Output: This is a legacy option that has no effect.
  - Auto / Card Defined
  - 36 Bit Output

  > The reader's default setting is Auto / Card Defined, where it will not attempt to modify the formatting on the card. For all other settings the reader will read the card and re-format the card data before sending it.

- **Enforce Options**: Optionally specify a transmission enforcement option.
  - Enforce on CSN: Enforce the configured Wiegand style on CSN transmission.

    If this option is **not** enabled:
    - CSN will be sent as the complete CSN in **auto** mode.
    - CSN will be sent as a valid HID card in **26 or 34 bit** Wiegand style (parity bit, CSN bytes, parity bit).
    - CSN will be padded or truncated in **any other** Wiegand style.
  - Enforce on OSDP: Enforce the configured Wiegand style on OSDP interpreted card transmission.

    If this option is not enabled, OSDP transmissions will not be formatted to the configured Wiegand style.

125kHz Formats

The 125kHz Formats TLV is used to enable/disable specific 125kHz card types.

- **125kHz Formats**:
  - 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

Set the reader output mode to configure its operating protocol.

- **Output Mode**:
  - Wiegand
  - ICT Smart Reader (RS485)
  - Custom Serial (RS485)
  - Smart Serial: This mode is valid for reader firmware up to and including version **1.04.260**
  - OSDP: This mode is valid for reader firmware **1.04.261** and above

  > The reader output mode automatically switches to ICT Smart Reader (RS485) when connected with RS-485 wiring configuration.

Tamper

The Tamper TLV is used to enable/disable intelligent reader tamper mode for detecting readers which have been disconnected. When enabled, the reader will check in to the device it is connected to every 30 seconds.

Custom RS485 Format

Specify the format to use when the reader **Output Mode** has been set to Custom Serial (RS485) (see above).

- **Custom Format**: Enter the string to 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.

Access Credentials

Customize the reader configuration to enable reading of different types of credentials.

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

This TLV only configures the credential structure. Before this can be utilized by the reader you will need to:

- add the encryption key to a **Keyslot** (see page 21)
- add your custom format string to a **Custom Card Format Slot** (see page 17)
- create a **Card Linkage** (see page 16) to link all the elements together

A programming example is provided to help illustrate this process (see page 29).

- **Slot**: Specifies the credential slot where the access credential configuration will be stored.

  The default slot assignments are displayed in the table below.

  The default credential types in slots 0-4 should **not** be removed under normal operation. Slots 5-8 are empty.

Slot	Credential
0	MIFARE Classic
1	MIFARE Secured
2	MIFARE DESFire
3	ISO7816 (NFC)
4	Bluetooth®
5	Available
6	Available
7	Available
8	Available

- **Credential Type**:
  - Disabled: Disables the selected credential slot
  - Mifare Classic
  - Mifare DESFire
  - ISO7618 (NFC)
  - Bluetooth

  Additional options are specific to the credential type selected

  MIFARE Classic:

  - **Block**: The MIFARE block number
  - **Key Type**: Set the key type to type A or type B
  - **Keyslot**: The keyslot to use as the MIFARE Classic sector key
  - **Flags**: Select the Diversify Key option to enable key diversification
  - **Diversification Keyslot**: The keyslot to use for diversification (if enabled)

  MIFARE DESFire:

  - **App ID** The DESFire application ID to access
  - **AES Keyslot**: The keyslot to use for AES authentication
  - **File Number**: The file number to access in the DESFire application
  - **Key Number**: The DESFire keynumber to use for read access
  - **Diversification**: The diversification method to use
    - No diversification
    - ICT diversification
    - AV2 diversification

  ISO7816 (NFC):

  - **App ID** The DESFire application ID to access
  - **AES Keyslot**: The keyslot to use for AES authentication
  - **File Number**: The file number to access in the DESFire application

Bluetooth:

- **Keyslot**: The keyslot to use for creating the encrypted session
- **Key Number**: The key number being sent in the challenge packet to the mobile device

Card Linkages

The Card Linkages TLV is used for linking credential types to custom card formats and encryption keys.

When the reader finds a credential that it can read, the linkage configuration specifies where to find the custom card formats and encryption keys to interpret that credential type, and how the card data is encrypted.

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

- **Linkage Slot**: The card linkage slot where the linkage configuration will be stored
- **Flags**: The decryption method to use:
  - AES 256 Decryption: If enabled, the reader expects data on the card to be encrypted with AES 256 in addition to the security on the card itself (e.g. MIFARE crypto1/DESFire key).
  - AES 256 Decryption CBC: If enabled, the reader expects data on the card to be encrypted with AES 256 with Cipher Block Chaining in addition to the security on the card itself.
  - AES IV In First Block: If enabled, the reader expects the IV (Initialization Vector) to be in the first block received from the card. Otherwise, it initializes the IV with all zeros.
  - Serial Diversified: If enabled, the reader expects the key for the encryption above to be diversified against the card serial number.
- **Keyslot**: The keyslot to link the custom encryption keys that will be used to authenticate the access credential
- **Access Credential Slot**: The slot to link the **Access Credential** configuration
- **Format Slot**: The **Custom Card Format Slot** to link the custom format string which describes how to interpret data from the card being read

CSN Reading Mode

The CSN Reading Mode TLV is used to enable/disable CSN (Card Serial Number) reading for MIFARE, DESFire and other NFC cards.

- **CSN Reading Mode**:
  - Mifare CSN (ISO14443a3)
  - Mifare CSN Reversed (ISO14443a3)
  - ISO 14443-4 CSN (DESFire)
  - ISO 14443-4 CSN Reversed (DESFire)
  - ISO15693 CSN: This is a legacy option. ISO15693 CSN capable cards are no longer supported
  - ISO15693 CSN Reversed: This is a legacy option. ISO15693 CSN capable cards are no longer supported

> The reader will first attempt to read the card using the encoded access credential before reading CSN. 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 PSK formatted Kantech, Tecom or Motorola cards for PSK capable readers.

PSK card formats require specific hardware to operate.

- **PSK Decryption**:
  - Raw Decoding: Reads raw data. Does not attempt to decrypt.
  - Kantech
  - Tecom
  - Motorola T1

Keypad Output Format

Define the data format the reader will use to send keypad input data.

This configuration applies when sending PIN data over Wiegand only.

- **Keypad Output Format**:
  - ARK501 (Default)
  - 26 Bit
  - 4 Bit
  - 4 Bit Parity
  - 4 Bit Buffered
  - 4 Bit Parity Buffered
  - 36 Bit Output

Low Frequency Flags

The Low Frequency Flag TLV is used to enable reading of legacy HID low frequency formats, which may be required for backward compatibility on older sites.

When enabled, the reader will interpret 125kHz HID cards using a legacy version of the HID format. When disabled, the reader will read 125kHz HID cards using the standard HID format. This is the default.

There is currently no selection option to disable this programming once enabled. To disable low frequency flags, apply a **Hex** TLV with hex code **160100**.

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.

- **Slot**: The custom card format slot where the custom format configuration will be stored.
- **Format**: Enter the required custom card format string.

  The string must be in ASCII format, up to a maximum of 64 ASCII characters.

  For example, %64r sets the format to 64 bit raw, so the reader will read the first 64 bits of data off the card.

Custom Card Format ASCII Codes

The custom card format is defined using ASCII codes. The following ASCII format codes are supported.

- **%Xs**: The next **X bits** on the card will be interpreted as the **site code**.
- **%Xc**: The next **X bits** on the card will be interpreted as the **card number**.
- **%Xu**: The next **X bits** on the card will be **unused/ignored**.
- **%Xr**: The next **X bits** on the card will be interpreted as **raw data**. That is, the data may be site code or card number. Exactly how the raw data is interpreted will depend on the configuration of your system.
- **%Xk**: the following card data must match the key stored in **keyslot X** on the reader.

  The length of card data which must match is determined by the length of the key stored on the reader.
- %**XmY**: the next **X bits** on the card must match the following **Y bits** of the ASCII format string.

  e.g. %32mcccc means the next 32 bits on the card must match the ASCII pattern of cccc.
- **%XnY**: the next **X bits** on the card must **not** match the following **Y bits** of the ASCII format string.

  e.g. %32ncccc means the next 32 bits on the card must be other than the ASCII pattern of cccc.
- **%Xl**: the next X bits on the card will be interpreted as a **length**. This length will be stored and can subsequently be accessed by substituting '**l**' for the number of bits to be interpreted as some formatting character.

  e.g. %8l%ls means the next 8 bits represent the length value l. Once this length value has been read from the card the subsequent 'l' bits on the card will be interpreted as the site code.

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. Other slots in the palette are used for other designated functions (such as to indicate area state, function codes, or two factor authentication required).

The LED Color TLV allows custom programming of the default reader LED colors by replacing the color assigned in the slots with a different color.

Changing the color assigned to a slot changes all functions associated with the original color.

A programming example is provided to help illustrate LED color configuration (see page 26).

- **Color**: Select a color by tapping or dragging on the color picker. Alternatively, you can type a color code into the field below the color picker. Tap the **arrow** icons 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.
- **Index**: Defines the color slot to be updated. Each index corresponds to a particular function of the card reader.

Color Slot Index

The color slot index and the default color assigned to each slot are outlined in the table below.

This table applies to raw TLVs programmed directly on the card reader only. Configurations programmed in Protege GX are adjusted by 1 for the controller's 'off' index (0), such that Red=1 through to Crimson=16.

Color Slot Index	Default Color
0	Red
1	Amber
2	Orange
3	Yellow
4	Lime
5	Green
6	Mint
7	Turquoise
8	Cyan
9	Sky Blue
10	Cobalt
11	Blue
12	Violet
13	Purple
14	Magenta
15	Crimson

Color slot 5 is the default color for access granted. Color slot 11 is the default reader idle color. Changing the default colors will mean the reader LEDs no longer display as expected for events and functions, which may complicate support requests. It is recommended to keep a register of any LED color changes.

Wiegand Site Code

The Wiegand Site Code TLV is used to configure the site code sent with keypad input data in 26 bit and 36 bit Wiegand keypad output formats (see page 13). Both of those keypad formats have a site code which is sent along with the PIN. This TLV allows you to define that site code.

- **Wiegand Site Code**: The site code may be entered in decimal or hexadecimal format.

This configuration applies when sending PIN data over 26 bit and 36 bit Wiegand only.

Reread Mode

Configure the reader to continuously reread a card that is kept within range.

This option can be used with the tSec Extra Card Holder Cover (Ordering code: PRX-TSEC-XCDH) .

The reader will send a card read to the controller every 3 seconds while a card is present in front of the reader, regardless of whether the card has been read before. The reader can also be set to silently reread the card, where it disables the beeps generated when the card is read.

- **Reread Mode**:
  - Enable Reread
  - Silent Reread

There is currently no selection option to disable this programming once enabled. To disable reread mode, apply a **Hex** TLV with hex code **200100**.

Reader Address

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

The Reader Address TLV allows you to program the reader's address configuration.

This may be required to set a specific address when connecting to third-party systems.

This TLV can also be used to configure an RS-485 reader as an entry reader (address 0) or exit reader (address 1).

This does not apply for tSec readers with the green and orange wires joined. When these wires are joined the reader is always an exit reader and the address cannot be configured.

- **Reader Address**: Enter the address to program the reader with. The maximum supported address is 127.

Uart Configuration

Define the baud rate of the RS-485 interface for compatibility with third-party systems.

- **Baud**:
  - 4800
  - 9600
  - 14400
  - 19200
  - 38400
  - 57600
  - 115200

Hex

An open field for entering a hex code to program a custom TLV.

- **Hex**: Enter the custom TLV hex code to achieve the desired programming.

Custom TLVs

Custom TLVs can be used to send configuration commands to a reader. A TLV consists of a type definition, data length measured in bytes (which does not include the type or length), and the data value itself. The type and length are fixed in size, and the value field is of variable size.

- **Type**: Specifies the setting or configuration type that the value applies to.
- **Length**: The size of the value field in bytes.
- **Value**: The variable-sized series of bytes containing the data that will be applied to the configuration.

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.

Keyslot

There is currently no preconfigured config app TLV for loading custom encryption keys for non-mobile credentials onto the reader. This is achieved by applying a custom Hex TLV (see above).

The following TLV structure is used to create a hex code which will load custom encryption keys onto the reader.

Type	Length	Value
0x03	≤ 33	[up to 32 byte key] [keyslot]

The type (03) is followed by the length (in bytes) and the value, made up of the encryption key (up to 32 bytes) and the keyslot where the encryption key will be stored (1 byte). Each key is assigned to a specific slot.

TLV Example

```
03 11 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA 02
```

This TLV sets keyslot 2 to use the 128 bit key AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.

Keyslot Availability

Keyslots 0 and 1 are reserved for the card settings lock login and OSDP session key respectively.

Keyslot	Hex	Description
0	0x00	Card Settings Lock Login
1	0x01	OSDP Session Key
2	0x02	Available
3	0x03	Available
4	0x04	Available

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 **Output Mode** option.
5. Tap the dropdown and select **OSDP**.
6. 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: OSDP Install Mode

The following programming example demonstrates how to create a config that puts the reader into OSDP installation mode so that it is ready to accept initiation of a secure channel session.

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 OSDP Install 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 **OSDP Install 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 OSDP Install Mode 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 tSec readers the address can only be programmed when the green and orange wires are **not** connected together. When the reader's green and orange wires are joined it is hardwired to **always** use 1 as its address.

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: 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 the reader programming.

Dual LED mode requires the reader to be wired with both the orange and brown LED control lines connected.

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 or dragging on the color picker. Alternatively, you can type a color code into the field below the color picker. Tap the **arrow** icons 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: 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: 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.

Config Example: Custom Credential

This programming example will demonstrate the process for one of the more complex config scenarios: programming a reader to read a custom credential.

In this scenario we will create a config to program the reader to read a DESFire card, using the following steps:

1. Add the **encryption key** for our DESFire card into a **keyslot**.
2. Configure the DESFire **access credential** settings.
3. Configure a format string that matches the **data format** of the card.
4. Create a **card linkage** which links these components together so that the reader can decrypt the card data and find the custom card format and encryption key to interpret the DESFire credential type.

This is a hypothetical scenario. Before programming a custom credential TLV you would need to know the specific credential configuration requirements, such as App ID, key number, data format, etc.

Add the Encryption Key

We will first add the encryption key for our DESFire card into a keyslot, using a Keyslot Hex TLV (see page 21).

For this example, we want to add encryption key FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF to keyslot 2.

1. Tap **Add TLV** and select the **Hex** option.
2. Enter the hex code 03 11 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF 02 (omit the spaces).

Configure the DESFire Credential

Credential settings are configured using the Access Credentials TLV (see page 14).

1. Tap **Add TLV** and select **Access Credentials**.
2. Apply the following access credential configuration:
   - **Slot**: 7
   - **Credential Type**: Mifare DESFire
   - **App ID**: A1B2C3
   - **AES Keyslot**: 3
   - **File Number**: 0
   - **Key Number**: 1
   - **Diversification**: AV2 Diversification

Configure the Format String

Our format string needs to be added using the Custom Card Format Slots TLV (see page 17).

The format string needs to match the data format of our DESFire card. In this example we will use 64 bit raw, so the reader will read the first 64 bits of data off the card, and we will add it to slot 6.

1. Tap **Add TLV** and select **Custom Card Format Slots**.
2. Set the **Slot Number** to 6.
3. Tap **Format** and enter the format string 25363472.

Custom card formats must be entered using ASCII code. 25363472 is the ASCII code for %64r (64 bit raw).

Create a Card Linkage

Finally, we can create our card linkage to tie everything together, using the Card Linkages TLV (see page 16).

For our scenario, we need to define the card linkage parameters as follows:

1. Tap **Add TLV** and select **Card Linkages**.
2. Set the following card linkage configuration:
   - **Linkage Slot**: 6
   - **Flags**: AES 256 Decryption
   - **Keyslot**: 2 (this is the keyslot where we stored our encryption key)
   - **Access Credential Slot**: 7 (this is the slot where we stored our DESFire credential configuration)
   - **Format Slot**: 6 (this is the slot where we stored our card format string)

Save and Apply

With all the components completed you can now **Save** the config. The new credential programming can be applied to the reader within 2 minutes of startup.

Config Example: Custom Mobile Credential

The following programming example demonstrates how to create a config that will enable the reader to read a custom mobile credential.

This programming only applies to sites which have a custom mobile credential with a registered encryption key.

While ICT readers are automatically enabled to read mobile credentials, registered custom mobile credentials have an encryption key assigned to the mobile credential profile and readers need to be programmed to decrypt the associated credentials. There are two methods available for configuring custom mobile credential programming in the config app. You can use either the Mobile Credential Keyslot TLV along with the associated Card Linkages TLV, or use the Update Key (NFC & Bluetooth) TLV which automatically configures the card linkages in the background.

Mobile Credential Keyslot

1. Define the **mobile credential keyslot** where the mobile credential encryption key will be stored.
2. Create a **card linkage** to configure NFC functionality to read the custom credential.
3. Create a **card linkage** to configure Bluetooth® functionality to read the custom credential.

Define the Mobile Credential Keyslot

You first need to define the slot where the profile's mobile credential encryption key will be stored.

Slots 0 and 1 are generally reserved, so only slots 2, 3 and 4 are available (see page 11).

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.

   This **must** be the profile with the mobile credential encryption key assigned.
3. **Add** a new **Reader Configuration** named appropriately (e.g. Custom Mobile Credential).
4. Tap the **Add TLV** dropdown and select the **Mobile Credential Keyslot** option.
5. Set the **Keyslot** to a suitable slot number.

Configure the NFC Card Linkage

1. Tap **Add TLV** and select **Card Linkages**.
2. Apply the following card linkage configuration:
   - **Linkage Slot**: 3
   - **Flags**: Enable both AES 256 Decrypt CBC and AES IV in first block.
   - **Keyslot**: Set to the **Mobile Credential Keyslot** number defined above.
   - **Access Credential Slot**: 3
   - **Format Slot**: 3

Configure the Bluetooth® Card Linkage

1. Tap **Add TLV** and select **Card Linkages**.
2. Apply the following card linkage configuration:
   - **Linkage Slot**: 4
   - **Flags**: Enable both AES 256 Decrypt CBC and AES IV in first block.
   - **Keyslot**: Set to the **Mobile Credential Keyslot** number defined above.
   - **Access Credential Slot**: 4
   - **Format Slot**: 4

Save and Apply

With all the components completed you can now **Save** the config. The custom mobile credential programming can be applied to the reader within 2 minutes of startup.

Update Key (NFC & Bluetooth)

The above process can also be simplified using the Update Key (NFC & Bluetooth) TLV, where only the keyslot needs to be configured. The NFC and Bluetooth® card linkages are automatically configured in the background.

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.

   This **must** be the profile with the mobile credential encryption key assigned.

3. **Add** a new **Reader Configuration** named appropriately (e.g. Custom Mobile Credential).
4. Tap the **Add TLV** dropdown and select the **Update Key (NFC & Bluetooth)** option.
5. Set the **Keyslot** to a suitable slot number.

   Slots 0 and 1 are generally reserved, so only slots 2, 3 and 4 are available (see page 11).

6. You can now **Save** the config and apply to the required reader(s) within two minutes of startup.

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.

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.