

# User Manual for Networked Electronic Lock Kit

**Version 1  
December 2019**



**CHATSWORTH  
PRODUCTS**

800-834-4969  
chatsworth.com  
techsupport@chatsworth.com

While every effort has been made to ensure the accuracy of all information, CPI does not accept liability for any errors or omissions and reserves the right to change information and descriptions of listed services and products.

©2019 Chatsworth Products, Inc. All rights reserved. Chatsworth Products, Clik-Nut, CPI, CPI Passive Cooling, eConnect, Evolution, GlobalFrame, MegaFrame, Motive, QuadraRack, RMR, Saf-T-Grip, Secure Array, SeismicFrame, SlimFrame, TeraFrame and Velocity are federally registered trademarks of Chatsworth Products. CUBE-IT, EuroFrame and Simply Efficient are trademarks of Chatsworth Products. All other trademarks belong to their respective companies. 11/19 MKT-60020-725

## TABLE OF CONTENTS

INTRODUCTION.....	3
PRODUCT FEATURES .....	4
PRODUCT LABELING AND CERTIFICATIONS .....	5
INSTALLATION CHECKLIST .....	6
INSTALLATION GUIDE .....	7
USING THE BUILT-IN WEB SERVER APPLICATION .....	8
Cabinet Access– Overview .....	13
Cabinet Access – Settings .....	13
Cabinet Access – Radius Card Settings .....	14
Logging – Overview .....	15
Logging – Export Logs .....	16
Logging – Settings .....	16
Notification - Thresholds .....	17
Environmental Thresholds .....	18
Notification - Routing.....	19
Settings –PDU.....	21
Settings - Environmental.....	22
Settings – Network.....	22
Settings – SNMP .....	23
Settings – Emails .....	24
Settings – Clone.....	25
Administration – User Management .....	26
Administration – Radius Authentication.....	27
Administration – LDAP Authentication .....	28
Administration – Advanced .....	28
Administration – Upgrade Firmware .....	30
USING THE APPLICATION PROGRAMING INTERFACE (API) .....	31
TROUBLESHOOTING GUIDE .....	31
APPENDIX .....	33

## INTRODUCTION

### User Manual for Networked Electronic Lock Kit

This document is the User Manual for CPI Networked Electronic Lock Kit (P/N 14667-001).

©2019 Chatsworth Products, Inc. All rights reserved.

UL Listed for use in US and Canada.

### Legal Information

The information contained in this guide is subject to change without notice. Chatsworth Products, Inc. (CPI) shall not be liable for technical or editorial errors or omissions contained herein; nor is it liable for any injury, loss, or incidental or consequential damages resulting from the furnishing, performance or use of this material and equipment.

### Warranty

CPI warrants all CPI-branded hardware products to be free from defects in material and/or workmanship (CPI's Standard Limited Warranty) for a period of three (3) years following the date of purchase (the Original Warranty Period).

The customer must contact CPI in writing or by oral communication confirmed in writing within the Original Warranty Period to report a product that the customer claims is defective. CPI reserves the sole and absolute right to determine whether or not the product or any part thereof is defective. In the event a product (or any part thereof) is determined by CPI to be defective (an Accepted Claim), CPI will provide a re-manufactured or replacement product or part (the Replacement Product) at no cost to the customer and issue a Return Material Authorization (RMA) number.

### Extended Limited Warranty

CPI Extended limited warranties on CPI-Branded Electronic and Non-Electronic hardware products are available for two additional years beyond the expiration of the Original Warranty Period (3 years). CPI's Extended Limited Warranty can be purchased concurrently with, or separately from, the initial purchase of the product until the expiration of the Original Warranty Period for that product.

For more information on CPI Warranties, [visit the website](#).



### Nomenclature

**device:** Power Distribution Unit product

**Socket/Receptacle/Outlet:** Electrical output port

**Secure Array™:** Connects up to 32 devices under one IP address. A second connection provides failover capability, allowing linked devices to stay connected when one loses functionality.

**Primary Role:** The role that is assigned to the device that is attached to the network and serves as the beginning of the Secure Array. This device should have a level of functionality that is equal to or higher than that of all the remaining devices within the array. In an array with several devices with the highest level of functionality, the device with the most outlets among this group should be assigned the Primary Role.

**Secondary Role:** The role assigned to a device that is 1) linked to the primary device, or 2) a standalone device.

**Alternate Role:** The role assigned to the device that is connected to the network to provide a

backup network connection if the Primary Role device loses power. This device must be equivalent to the Primary device in functionality and number of outlets.

## PRODUCT FEATURES

**Physical Dimensions: Controller Module is 1.4"H x 7"W x 4"D (34.9 mm x 177.8 mm x 101.6 mm)**

**Input Voltage:** 100 - 240V, 50/60Hz; IEC C14 connector w/detachable C13 to C14 power cord

### Mounting and Installation Instruction

1. Device comes with magnetic buttons. Select the preferred location and secure the device onto the cabinet.
2. An optional device external Bonding Strap (Part number: **024-717664-001**) is included with the device, and is an enhanced feature for RFI and EMI noise reduction when required. Follow Grounding and Bonding methods when connecting the Ground Wire to the Racks and/or Cabinets at customer discretion.

**USB port:** Quantity: 2

Function: CPI Firmware upgrades

### **Secure Array®/ Device Linking/Serial Port:**

Connector type: (2) RJ45 for (1) link-in/serial combo port and (1) link-out port for serial communication and device linking using a Cat 5/6 cable

### **Environmental ports:**

Connector type: (1) RJ11

Connection: (1) or (2) Environmental probes (order separately; order two probes with a splitter P/N 17761-003 to connect two probes).

For environmental sensing of temperature (°F or °C) and relative humidity (%)





### **Ethernet port:**

Connector type: (1) RJ45 Speed: 10/100/1000

Megabit/sec

Support: IPv6; IPv4; SNMP v1, v2, v3.

## PRODUCT LABELING AND CERTIFICATIONS

	<p>The presence of the CE Mark on equipment means that it has been designed, tested and certified as complying with all applicable European Union (CE) regulations and recommendations.</p>
	<p>This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.</p>
	<p>Samples of this product met UL's safety requirements for US and Canada.</p>
	<p>Do not dispose this product as unsorted municipal waste.</p>

### Safety Warnings and Cautions

- **DO NOT OPEN THE CONTROLLER MODULE.** There are no user serviceable parts within the device. Opening or removing covers, receptacle plates, or other access points may expose you to dangerous shock hazards or other risks. Refer all servicing to qualified service personnel.
- Do not spill any liquids on the controller.
- Do not insert objects of any kind into the controller via vent holes or any openings as they may contact dangerous voltage points, which can be fatal or cause harmful electric shock, fire or equipment failure.
- Do not place any heavy objects on the power cord. Damage to the cord may cause shock or fire.
- **RESTRICTED ACCESS LOCATION:** location for equipment where both of the following apply:
  - Access can only be gained by **SERVICE PERSONS** or by **USERS** who have been instructed about the reasons for the restrictions applied to the location and about any precautions that shall be taken
  - Access is using a **TOOL** or lock and key, or other means of security, and is controlled by the authority responsible for the location.
- **Hot surface warning label:** The equipment may be hot under full load.
- If using the 10/100/1000MB Ethernet port at a 1000MB (Gigabit) speed, please use shielded Ethernet cables only.



## INSTALLATION CHECKLIST

- Connect wires between latch and CAN bus module
- Connect wires between sensors and CAN bus module
- Connect wires between CAN bus and device. Aux 1 should be connected to the rear door's CAN module. Aux 2 should be connected to the front door's CAN module.
- Login to the web GUI using the default login information of "admin/admin", and navigate to the "Cabinet Access – Settings" page.
- Select the checkbox for the appropriate lock you wish to enable, and click "Save"
- The lock is powered when you see a continuous blue light on the lock. At this point you should be able to refresh the web page and see the status update appropriately.
- Program the Card Reader and Smart Card ID (Go to [Page 33](#) for detailed information).
- Use the web GUI to change cabinet access and logging settings (Cabinet Access and Logging tabs respectively)
- The light will flash magenta/blue when the latch opens

### Additional Software

The Networked Electronic Lock Kit can be configured, monitored and controlled using the built-in software as explained in this manual.

In addition to the software that is built-in to the Networked Electronic Lock Kit, there is an upgrade software program for firmware upgrade:



- Firmware Upgrader software allows you to upgrade firmware over the network for multiple standalone and linked devices that have firmware version 3.xx.xxx or later.
- Download from <http://www.chatsworth.com/support-and-downloads/downloads/software/>

## **INSTALLATION GUIDE**

### **External Connections:**

- Install the device into the cabinet and secure the device external ground wire to the cabinet ground stud.
- Optional: In/ Serial Port:
- For Secure Array when linking devices, use a standard Cat 5/6 cable.
- Optional: Ethernet Port: Connect to LAN. Use CAT5/6 cable.
- Optional: Environmental Sensor Port.
- Use Temperature and Humidity sensors (P/N 14665-001):
- Optional: Out Port: For Secure Array when linking devices. Use a standard Cat 5/6 cable.
- Optional: USB Port: For firmware upgrades use USB Flash Drive.

### **Energizing the Device:**

- Attach the input power cord to a matching power source.
- The device status light will blink Green for about 60 seconds as the device is booting up.

## USING THE BUILT-IN WEB SERVER APPLICATION

### Login

All eConnect devices, excluding Basic models, are shipped with:

A 1 GB Ethernet connection and built-in Web Server Application Default IP address:

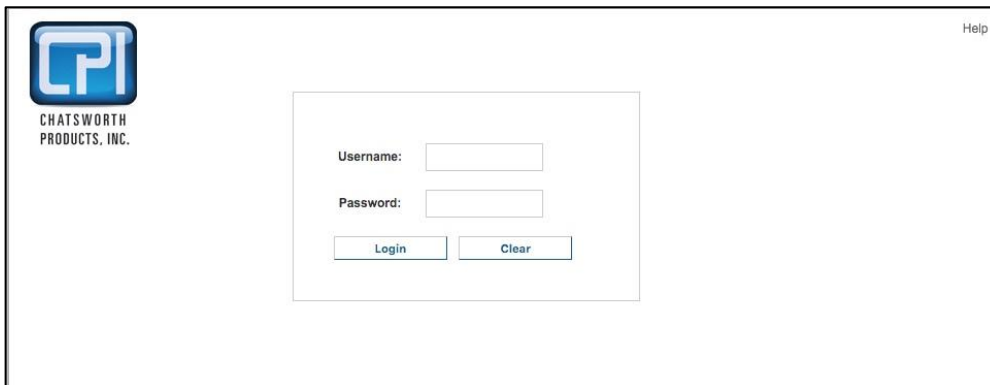
**192.168.123.123**

Default Username/Password: **admin/admin**

You can access the device using the default IP address, or you can use the LCD Local display to change the default IP address to the appropriate IP address.

- To access the device, connect the Ethernet port to a network switch
- From Web Browser on a computer that is network accessible to the device, type: <http://device.address>. For example, the default would be: <http://192.168.123.123>

The Login Screen will display:



Log in using default Username and password: **admin**, **admin** and **click on Login** button or username and password if it has been created.

### First Login – Set Date and Time

The device has data logging and alarm notification functions that benefit from a time and date stamp. However, the device does not have an internal clock. So, each time you power the device, you must manually set the time and date or assign a Time Server to do so automatically.

To assign a Time Server, click on the **Settings** tab, **Network** sub menu. Scroll down the page to the heading **Time Servers**.



StatusCabinet AccessLoggingNotificationsSettingsAdministration

PDUEnvironmentalNetworkSNMPEmailsCloneMy Profile

### Network Settings

Edit network related configuration properties.

#### TCP / IP Configuration

Enable Protocols: IPv4 and IPv6

☒ Manually Configure IPv4  
☒ Link Local IPv6 fe80::20e:d3ff:fe06:9eb8/64  
☐ Global IP ☒ Manually Configure IPv6

##### IPv4 Setup

IP Address 192.168.123.123

Subnet Mask 255.255.255.0

Default Gateway 192.168.123.1

##### IPv4 DNS Servers

Primary DNS Server 0.0.0.0

Secondary DNS Server 0.0.0.0

##### IPv6 Setup

IP Address

Prefix Length 0

Default Gateway

##### IPv6 DNS Servers

Primary DNS Server

Secondary DNS Server

#### Time Servers

RFC Time Server

NTP Time Server

SaveCancel

#### Web Access Settings

☒ Enable HTTP Port: 80  
☒ Enable HTTPS Port: 443  
☒ Manufacturer Certificate  
☐ Custom Certificate

SaveCancel

Enter the IP Address of the RFC or NTP Time Server.

The device must have network access to the time server. For detailed network setup, see **Settings – Network** on [page 22](#).

If you do not utilize a time server, or decide to set the time and date manually, click on the **Administration** tab, **Advanced** sub menu.

Status	Outlet	Cabinet Access	Logging	Notifications	Settings	Administration
User Management	Radius Authentication	LDAP Authentication	Advanced	Upgrade Firmware	My Profile	

---

**Advanced**

The PDU time can be configured by synchronizing the PDU with the web browser, if desired. Clicking "Soft Reboot" will perform a reboot of the entire system. Also, the PDU can be reverted back to factory defaults in certain categories. "Reset Network" will reset settings on the "Settings - Network" and "Settings - SNMP" tabs. "Reset Configuration" will reset all settings not related to the network or user configuration. "Reset Users" will reset all configuration on the "Administration - User Management" tab. "Reset All" functions as if all three choices were selected simultaneously.

**PDU Info**

Firmware: 4.10.678  
 Configuration ID: P6-4A163-C1D  
 Serial Number:  
 MAC Address: 00:0E:D3:00:FF:45

---

**Time and Date Settings**

Browser date and Time: Wed, 06 Nov 2019 20:46:08 UTC [Sync PDU Time](#)

PDU Time in UTC

Time: 20 Hrs 45 Mins 58 Secs  
 Date: 6 Nov 2019

[Save](#) [Cancel](#)

---

[SOFT REBOOT](#)

---

**Factory Defaults**

☐ Reset Network ☐ Reset Configuration  
☐ Reset Users ☐ Reset All

[APPLY DEFAULTS](#)

Click on **Sync device time** and then **Save** button to update the clock on the device using the browser date and time, or manually set the time with the drop boxes.

**Note that if you perform a firmware upgrade, the device will reboot and the time will need to be manually reset, unless you have assigned Time Server to the device.**

The remainder of the manual is ordered according to the tabs on the screen displayed above, so the next section is Status and the Status sub menus.

If an optional Environmental Probe is attached to the device, temperature and humidity will be displayed under Sensor Status. You can connect two probes to each device. The doors and the locks will be displayed under Front Door Status and Rear Door Status.

## Status – Overview

Click on the **Status** tab, **Overview** sub menu to view circuit, sensor, input and outlet status.

**Sensor Status**

	Temp	Humidity
Probe 1 Name		
Probe 2 Name		

**PDU Input Status**

	Current
Line1	0.00A

**Status****Cabinet Access**LoggingNotificationsSettingsAdministration

**Overview**AlarmsMy Profile

**Status Overview**

Overview of the Electronic Access Control environmental probe status and cabinet lock status.

**Sensor Status**

	Temp	Humidity
Probe1 Name		
Probe2 Name		

**Front Door Status**

State
Door: Not Configured
Lock: Not Configured

**Rear Door Status**

State
Door: Not Configured
Lock: Not Configured

Once alarm thresholds are set (see [page 18](#)), the Sensor Status table under the Status tab, Overview submenu will show the operating range as a green bar, warning range as a yellow bar, and alarm range as a red bar. The actual measured value will be shown as a black line overlaying the graph.

This allows a quick visual reference for available power within the acceptable operating range for each circuit. The total power consumed is also displayed at the bottom of the graph as a percentage of power available.

Scroll down.

If an optional Temperature and Humidity Sensor is attached to the device, temperature and humidity will be displayed under Sensor Status. You can connect two sensors to each device.

Door status:

- **Not Configured:** Lock is not enabled.
- **Closed:** Door is closed.
- **Opened:** Door is opened.
- **Tampered Open:** Door is opened, and lock is locked or tampered unlocked or force unlocked.

Lock status:

- **Not Configured:** Lock is not enabled.
- **Locked:** Lock is locked and handle is in the cradle
- **Force Unlocked:** Unlock using the GUI
- **Tamper Unlocked:** Unlock using the key and handle is not in the cradle.
- **Unlocked via Key Card:** A registered smart card was used to unlock.

Scroll down.

## Status – Alarms

Click on **Alarms** to view a summary of Alarm messages, if there are any present:

Warning thresholds are indicated by a **yellow-colored** rectangular alarm status symbol.  
Critical thresholds are indicated by a **red-colored** rectangular alarm status symbol.

The screenshot shows the 'Alarms Status' page. The top navigation bar includes 'Status', 'Cabinet Access', 'Logging', 'Notifications', 'Settings', and 'Administration'. Below this, a sub-navigation bar has 'Overview' and 'Alarms'. The main content area is titled 'Alarms Status' and includes a summary: 'Summary of all active alarms within the PDU. If the PDU is an active Primary in a SecureArray™, all active alarms within the SecureArray™ are shown as well.' Below the summary is a table with columns: '#', 'Status', 'PDU Name', and 'Alarm'. The table contains one row with a yellow status symbol, 'IPDU2', and the message 'Voltage dropped below Warning Low Threshold in Branch CB1'. On the left side, there is a 'SecureArray™' section with a 'Sort ASC' dropdown and a list of PDU names: 'IPDU2', 'SA1-3-33', and 'SA1-3-34'.

#	Status	PDU Name	Alarm
1	Yellow	IPDU2	Voltage dropped below Warning Low Threshold in Branch CB1

The screenshot shows the 'Alarms Status' page. The top navigation bar includes 'Status', 'Cabinet Access', 'Logging', 'Notifications', 'Settings', and 'Administration'. Below this, a sub-navigation bar has 'Overview' and 'Alarms'. The main content area is titled 'Alarms Status' and includes a summary: 'Summary of all active alarms within the PDU. If the PDU is an active Primary in a SecureArray™, all active alarms within the SecureArray™ are shown as well.' Below the summary is a table with columns: '#', 'Status', 'PDU Name', and 'Alarm'. The table contains one row with a red status symbol, 'IPDU2', and the message 'Voltage dropped below Critical Low Threshold in Branch CB1'. On the left side, there is a 'SecureArray™' section with a 'Sort ASC' dropdown and a list of PDU names: 'IPDU2', 'SA1-3-33', and 'SA1-3-34'.

#	Status	PDU Name	Alarm
1	Red	IPDU2	Voltage dropped below Critical Low Threshold in Branch CB1

Note: The CPI alerts and notification system can be broken down into a few components:

- Configured thresholds
- Active alarms based on the current metrics in relation to the configured thresholds
- Notifications of these alarms in the form of SNMP traps, log entries, and emails when configured.

## Cabinet Access– Overview

View the state of the two cabinet doors and the recent Openings/Closings.

The screenshot shows the 'Cabinet Access Overview' page. At the top is a navigation bar with tabs: Status, Cabinet Access (selected), Logging, Notifications, Settings, and Administration. Below this is a sub-navigation bar with 'Overview' (selected), 'Settings', and 'Radius Card Settings'. A 'My Profile' link is on the right. The main content area is titled 'Cabinet Access Overview' and includes a descriptive paragraph. It features two side-by-side status boxes for 'Front Door Status' and 'Rear Door Status'. Each box shows 'State', 'Door: Not Configured', 'Lock: Not Configured', and an 'UNLOCK' button. At the bottom, there is a table for 'Recent Openings/Closings' with columns: Door, Cabinet, PDU, Time Opened, and Time Closed.

Door	Cabinet	PDU	Time Opened	Time Closed
------	---------	-----	-------------	-------------

## Cabinet Access – Settings

The screenshot shows the 'Cabinet Access Settings' page. The navigation bar is the same as the overview page. The sub-navigation bar shows 'Settings' (selected) and 'Radius Card Settings'. The main content area is titled 'Cabinet Access Settings' and includes a descriptive paragraph. It features two input fields: 'Cabinet Lock Open Time' (set to 5 seconds) and 'Cabinet Door Open Alarm Time' (set to 10 minutes). Below these are two checkboxes: 'Enable Front Lock' and 'Enable Rear Lock'. At the bottom, there are 'Save' and 'Cancel' buttons. The 'Front Door Status' and 'Rear Door Status' boxes are also present, showing 'State', 'Door: Not Configured', and 'Lock: Not Configured'.

Enter the **Cabinet Lock Open Time**: 1 – 30 seconds. The default value is 5 seconds

Enter **Cabinet Door Open Alarm Time**: 1 – 240 mins. The default value is 10 minutes

Check box to enable Front or/and Rear Lock(s) where applicable  
Click on **Save** to save the configured data.

## Cabinet Access – Radius Card Settings

StatusCabinet AccessLoggingNotificationsSettingsAdministration

OverviewSettingsRadius Card SettingsMy Profile

Radius Card Access Control Authentication

Users authenticated via Radius will have "Viewer" permission. To grant a user additional permission, create a local account under User Management and edit the user to assign an appropriate Group: User, Cabinet or Admin. Users need Group: Cabinet or Admin permission for Cabinet Access with the Electronic Access Control system.

☐ Enable Radius Card Authentication

Use IPv6☐

Radius Server 1

Radius Server 2

Radius Server 3

Radius Secret

Connection Test

Test Card ID:

Port: 1812

Port: 1812

Port: 1812

Save

Cancel

Check the Enable Radius Card Authentication box to be able to enter the server information

Check the Use IPv6 box. If applicable click **Save**

## Logging – Overview

StatusCabinet AccessLoggingNotificationsSettingsAdministration

OverviewExport LogsSettingsMy Profile

### Logging Overview

The system creates an events log (syslog) of system changes. Logs are stored locally until exported. The bar below indicates the amount of local storage that is used. The table below is a summary of the last 10 (syslog) events. Use the Logging-Settings tab to configure the data log (metrics) interval, remote storage server location and remote events log (syslog) server location. Use the Logging-Export Logs tab to search for and manually export logs.

#### Log Module Usage

Metrics Data

0%

#### Syslog Quickview

Syslog Filter

Reload Entries

☒ Event☒ Audit☒ System

#### Syslog Entries

Time (UTC)	Entry
Nov 27 13:59:32	[Unit Cabinet]:[Unit Name]:[Audit] User admin logged in on the web GUI interface.
Nov 27 13:58:41	[Unit Cabinet]:[Unit Name]:[System] PDU cold booted. Outlet configuration will be applied.
Nov 27 13:58:41	[Unit Cabinet]:[Unit Name]:[System] PDU cold booted. Outlet configuration will be applied.
Nov 19 21:46:16	[Unit Cabinet]:[Unit Name]:[Audit] User admin logged in on the web GUI interface.
Jan 6 03:56:20	[Unit Cabinet]:[Unit Name]:[Audit] PDU reboot requested by admin.

Select Syslog Filter by checking the check box(es) and click on the **Reload Entries** button to obtain up-to-date information.

## Logging – Export Logs

Status	Cabinet Access	<b>Logging</b>	Notifications	Settings	Administration
Overview	<b>Export Logs</b>	Settings	My Profile		

---

### Export Logs

Select which type of data you wish to retrieve, then specify the time interval you wish to view data from. You can choose to "Quick View" your data, which will present the data in a spreadsheet, "Download" your data in a CSV format, or "Transfer" the CSV file to the server specified on the Settings page.

**Report Type**

☒ Event Log File

**Log file:** Jan 6 03:56:20 - Current ▾

---

**DOWNLOAD**   **TRANSFER TO SERVER**   **DELETE**

Select type of file and select the log file to be exported.

Click on **DOWNLOAD** to download selected file to the connecting computer.

Click on **TRANSFER TO SERVER** to save the file on the designated storage server.

Click on **DELETE** to remove the save file from the device

## Logging – Settings

Status	Cabinet Access	<b>Logging</b>	Notifications	<b>Settings</b>	Administration
Overview	Export Logs	<b>Settings</b>	My Profile		

---

### Log Settings

Enable the data logging to have outlet, branch, and environmental data logged to a .dat file at the specified logging interval. The .dat file can be downloaded on the "Export Logs" page. A separate application is used to convert the .dat file to .csv files. The Log Server can be enabled for manual or auto-transfer of the .dat and syslog files to another server available over the network. Auto-transfers will take place every 6 hours once enabled. Manual transfers are initiated via the "Export Logs" page. The Syslog server option can be enabled for real-time streaming of syslog data to a pre-configured syslog server available on the network.

**Data Logging Settings**

Enable Logging: ☐

Logging Interval: 0 minutes

Log Full Warning Level: 75 %

---

**Event Logging Settings**

Log Identity: CPI\_EAC

Log Facility: LOG\_LOCAL0 ▾

---

**Storage Server** ☐

SSH Server Address:  Port: 0

Destination Directory:

Connection options:

User Name:

Password:

Auto-Transfer Data Log: ☐

Auto-Transfer Event Log: ☐

**Save and Test Connection**



### Metric Data Logging:

Check Enable Logging check box to begin capturing data on the device internal memory. Input the desired interval and Log Full Warning Level percentage.

### Event Logging Settings:

Log Identity and Log Facilities are preset on the device memory system. Pick any Log Local to store data locally.

### Storage Server:

Input information for Data Log and Event Log to be stored remotely. Make sure to click on the **Save and Test Connection** button to validate the connection and authorization to save data on the remote server.

### Syslog Server:

Allows the use of the remote server as the Syslog instead of the device itself.

Click on **Save** to save all input data.

## Notification - Thresholds

StatusCabinet AccessLoggingNotificationsSettingsAdministration

ThresholdsRoutingMy Profile

### Notification Thresholds

Specify the data thresholds that will trigger an alarm event for this unit. There are both low and high, critical and warning thresholds. The outlet and branch threshold tables allow values to be copied from one row to all rows in the table.

#### Environmental Thresholds

Clear All

Sensor	Critical Low	Warning Low	Warning High	Critical High
Temperature 1	<input type="text"/> °F	<input type="text"/> °F	<input type="text"/> °F	<input type="text"/> °F
Temperature 2	<input type="text"/> °F	<input type="text"/> °F	<input type="text"/> °F	<input type="text"/> °F
Humidity 1	<input type="text"/> %	<input type="text"/> %	<input type="text"/> %	<input type="text"/> %
Humidity 2	<input type="text"/> %	<input type="text"/> %	<input type="text"/> %	<input type="text"/> %

SaveCancel

## Environmental Thresholds

StatusCabinet AccessLoggingNotificationsSettingsAdministration

ThresholdsRoutingMy Profile

### Notification Thresholds

Specify the data thresholds that will trigger an alarm event for this unit. There are both low and high, critical and warning thresholds. The outlet and branch threshold tables allow values to be copied from one row to all rows in the table.

#### Environmental Thresholds

Clear All

Sensor	Critical Low	Warning Low	Warning High	Critical High
Temperature 1	0 °F	0 °F	0 °F	0 °F
Temperature 2	0 °F	0 °F	0 °F	0 °F
Humidity 1	0 %	0 %	0 %	0 %
Humidity 2	0 %	0 %	0 %	0 %

SaveCancel

Input all desired limitations to be set as thresholds.  
Click on **Save**.

Scroll down to input other thresholds.

## Notification - Routing

Status	Cabinet Access	Logging	Notifications	Settings	Administration
Thresholds	Routing				My Profile

### Notification Routing

Specify how you would like to be notified of an alarm event for this unit. You can choose to have an entry in the syslog file, a trap sent via SNMP (if the appropriate SNMP settings are configured on the Settings - SNMP page), and have an email notification sent (if the email setup has been completed on the Notifications - Emails page).

#### Temperature Notifications

Event	Log	Trap	Email
Temperature Critical Low	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Temperature Warning Low	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Temperature Warning High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Temperature Critical High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### Humidity Notifications

Event	Log	Trap	Email
Humidity Critical Low	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Humidity Warning Low	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Humidity Warning High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Humidity Critical High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### Door and Lock Notifications

Event	Log	Trap	Email
Badge Scanned and Verified	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Badge Scanned and Not Verified	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Door Opens or Closes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lock Opens or Closes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Door Open Longer than Alarm Period	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### System Notifications

Event	Log	Trap	Email
System Firmware Update Applied	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System Configuration Change	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PDU Receptacle Change	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System System Reboot	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System Accessed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SecureArray™ State Change	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Select method(s) of notifications for Temperature, Humidity if applicable by checking the check box(es): Log, Trap, Email.

Select method(s) of notifications for Door, Lock and device if applicable by checking the check box(es): Log, Trap, Email.

Click on Save to save the input data.

With regards to emails, if a particular alarm becomes active, the device will send an email in response to this alarm becoming active, if configured to do so. This configuration includes the email settings to get emails to work at all, plus the configuration on the **Notifications – Routing** page, which determines which the alarms will provoke an email being sent.

These email messages will include which alarms have become active/cleared at the moment the email was sent. They do not, however, contain a message for every currently active alarm, only the alarms that have just “tripped” or “cleared”.

Scroll down for more notification settings.

## Settings –PDU

**System Settings**

Edit SecureArray™ and general system related configuration properties.

Cabinet ID:

System Name:\*

System Location:

Primary System: ☐

Out Of Service: ☐ No alarms will be sent

Sum Amps: ☐ Amperage will be summed across all branches

Use this tab to set the system for the Controller Module

**Service Out-of-Service-checkbox:** Check this box to deactivate the Electronic Lock Kit alarms if a device goes offline or becomes “unlinked.” Use this checkbox for planned service.

Enter desired **Device Name** and **Location**.

**Out of Service checkbox:** Check this box to deactivate alarms if a device goes offline or becomes “unlinked.” Use this checkbox for planned service.

**Primary system checkbox:** Devices can be linked together through a Secure Array to share a single IP address through a single network connection. The check box for Primary device should only be checked if this device is linked with other devices, and if this is the device that is attached to the network. If this device is not linked to other devices, do not check the Primary Device check box.

Fill in the desired choices and click on **Save**.

## Settings - Environmental

The screenshot shows the 'Settings' tab selected in a web interface. The top navigation bar includes 'Status', 'Cabinet Access', 'Logging', 'Notifications', 'Settings', and 'Administration'. Below this, a sub-navigation bar shows 'PDU', 'Environmental', 'Network', 'SNMP', 'Emails', and 'Clone'. The 'Environmental' sub-tab is active. The main content area is titled 'Environmental Settings' and contains the text 'Edit general environmental probe settings.' Below this, there are two radio buttons for 'Unit of Measure': '°F' (selected) and '°C'. There are two text input fields for 'Probe 1 Name' and 'Probe 2 Name'. At the bottom of the form are 'Save' and 'Cancel' buttons. A vertical scrollbar is visible on the right side of the page.

Select choice of temperature unit, enter name for the temperature and humidity sensors. Click on **Save**.

## Settings – Network

The screenshot shows the 'Settings' tab selected in a web interface. The top navigation bar includes 'Status', 'Cabinet Access', 'Logging', 'Notifications', 'Settings', and 'Administration'. Below this, a sub-navigation bar shows 'PDU', 'Environmental', 'Network', 'SNMP', 'Emails', and 'Clone'. The 'Network' sub-tab is active. The main content area is titled 'Network Settings' and contains the text 'Edit network related configuration properties.' Below this, there is a section for 'TCP / IP Configuration'. It includes a dropdown menu for 'Enable Protocols' set to 'IPv4 and IPv6'. There are checkboxes for 'Manually Configure IPv4' (checked), 'Link Local IPv6' (checked, with address 'fe80::20e:d3ff:fe06:9eb8/64'), and 'Global IP' (unchecked). There is also a checkbox for 'Manually Configure IPv6' (checked). Below this, there are two columns of settings. The left column is for 'IPv4 Setup' and includes fields for 'IP Address' (192.168.123.123), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (192.168.123.1), 'IPv4 DNS Servers' (Primary: 0.0.0.0, Secondary: 0.0.0.0). The right column is for 'IPv6 Setup' and includes fields for 'IP Address', 'Prefix Length' (0), 'Default Gateway', and 'IPv6 DNS Servers' (Primary, Secondary). Below these columns is a section for 'Time Servers' with fields for 'RFC Time Server' and 'NTP Time Server'. At the bottom of the form are 'Save' and 'Cancel' buttons. Below the form is a section for 'Web Access Settings'. A vertical scrollbar is visible on the right side of the page.

- **Network** - Using the Enable Protocols combo box, select the Network Protocol(s). Enter data for IPv4 and/or IPv6 Networking.
- **Time Servers** – Designate a time server as the source for time after each reboot (requires a network connection). As an alternative, you can manually set the time from the Administration tab, Advanced sub menu.
- **Web Access Settings** –Designate the port for accessing the device using a web browser and HTTP or HTTPS. Click on **Save**.

## Settings – SNMP

StatusCabinet AccessLoggingNotificationsSettingsAdministration

PDUEnvironmentalNetworkSNMPEmailsCloneMy Profile

### SNMP Settings

Edit SNMP and trap related configuration properties.

☒ Enable SNMP Access

Listen Port:

Trap Port:

Security Level:

#### SNMP V1 and V2c Settings

Read Community:  (Default: public)

Write Community:  (Default: private)

Limit Host Access ☐

Host 1 IP Address: IPv4:  IPv6:

Host 2 IP Address: IPv4:  IPv6:

Host 3 IP Address: IPv4:  IPv6:

#### SNMP V3 Settings

USM User:

Auth Algorithm:

Auth Password:

Priv Algorithm:

Priv Password:

Context Name:

#### Send Traps To

Host 1 IP Address: IPv4:  IPv6:

Host 2 IP Address: IPv4:  IPv6:

Host 3 IP Address: IPv4:  IPv6:

#### Additional Trap Settings:

Alarm Interval:  Minutes

Log Interval:  Minutes

Log Difference:  Amps

Save

Cancel

Enter data for SNMP v1, v2c or v3 settings.  
Enter the IP Addresses you want to send traps to.  
Click on **Save** to save all entered data.

## Settings – Emails

**Notification Setup**

Setup a connection with an SMTP server to use for sending emails when alarms are raised in the system. Be sure to specify which alarms you wish to receive emails for on the 'Notifications Routing' page.

☐ Enable Email Notification

**Save** **Cancel**

The device does not include a mail server. In order to provide email notifications for the device, you must first setup an email account for the device on an accessible mail server.

- **SMTP Mail Server** – the mail server where the account resides, ex: smtp.google.com.
- **Port Number** – the provider's port number, usually 465 or 25.
- Check **Use TLS** or **Start TLS** check box(es) to match your provider's encryption requirements.
- **Email address** – the email address assigned to the device
- If **Authentication** is required, select **Specify Credentials** from the drop-down list.
- Enter the **Username** and **Password** for the Email account.
- Select **Anonymous** if no Username and Password are required.
- Enter the email address(es) of the **Recipient(s)** (eg: your technician's email address.)
- Click on **Save** and **Send a Test Email** to make sure notification setup is correctly. The device must have network access to the mail server.



# Settings – Clone

StatusCabinet AccessLoggingNotificationsSettingsAdministration

PDUEnvironmentalNetworkSNMPEmailsCloneMy Profile

Clone and Transfer Settings

Select the settings you wish to clone from this Primary PDU to any number of PDUs on the daisy chain.

Settings to Clone:

Select All

☐ Branch Voltage Thresholds

☐ Branch Current Thresholds

☐ Outlet Reset Delays

☐ Outlet ON Delays

☐ Outlet Current Thresholds

☐ Temperature Thresholds

☐ Humidity Thresholds

☐ Temperature Unit

☐ Trap Interval

☐ Sum Amps Setting

☐ Out-of-Service Setting

☐ Notification Specifications

☐ Logging Settings

Select PDU's to Clone to:

CloneCancel

Click on the check box(es) for all information to be cloned.  
Click on the list the device(s) to be cloned to.  
Click the **Clone** button.

## Administration – User Management

StatusCabinet AccessLoggingNotificationsSettingsAdministration

User ManagementRadius AuthenticationLDAP AuthenticationAdvancedUpgrade FirmwareMy Profile

User Management

Create, edit, and delete users. Users can be a member of one of 4 groups: Admin, Cabinet, Viewer, User. A user's group will determine a user's level of web interface access. The 'Viewer' group has no configuration access. The 'User' group has limited configuration access. The 'Cabinet' group has the same level of configuration access as the 'User' group, but also has access to the 'Cabinet Access' tab in the web interface. The 'Admin' group has access to every tab in the web interface

Clone To: 

Clone

User Name	Group	Card ID	Action	
admin	Admin		Edit	Delete

Create User

Create User

Username:

Password:

Confirm Password:

Card ID:

Group:

Admin

Create

Cancel

Click on **Create User** to add a new user.

Create User

Create User

Username:

Password:

Confirm Password:

Card ID:

Group:

Admin

Create

Cancel

Input the username and password and click on **Create**.

To edit an existing user. Click on **Edit** for that username.

User Profile

User Name:

Password:

(Leave blank to keep current password)

Confirm Password:

Card ID:

Group:

Admin

Save

Cancel

Change the necessary information. Input the Smart Card ID for the Electronic Lock Kit. If you don't know your Smart Card ID, see Appendix on [Page 33](#). The same information should be input for both the Primary and Alternate device to assure the same logging authority will be carried through.

Click on **Save**.

## Administration – Radius Authentication

Status

Cabinet Access

Logging

Notifications

Settings

Administration

User Management

Radius Authentication

LDAP Authentication

Advanced

Upgrade Firmware

My Profile

Radius Authentication

Users authenticated via Radius will have "Viewer" permission. To grant a user additional permission, create a local account under User Management and edit the user to assign an appropriate Group: User, Cabinet or Admin. Users need Group: Cabinet or Admin permission for Cabinet Access with the Electronic Access Control system.

☐ Enable Radius Authentication

Use IPv6

☐

Radius Server 1

Port: 1812

Radius Server 2

Port: 1812

Radius Server 3

Port: 1812

Radius Secret

Connection Test

User Name:

Password:

Save

Cancel

For network/website authentication using **Radius Authentication**, enter the necessary information and **Save**. Note that users will need to be added under the **Local User List** to have **Control** or **Admin** capabilities.

## Administration – LDAP Authentication

The screenshot shows the 'Administration' tab selected in the top navigation bar. Below it, the 'LDAP Authentication' sub-tab is active. The page contains a section titled 'LDAP Authentication' with a descriptive paragraph: 'Users authenticated via LDAP will have "Viewer" permission. To grant a user additional permission, create a local account under User Management and edit the user to assign an appropriate Group: User, Cabinet or Admin. Users need Group: Cabinet or Admin permission for Cabinet Access with the Electronic Access Control system.' Below this text are several configuration fields: 'Enable LDAP Authentication' (a checkbox), 'LDAP Server URI' (a text input field), 'Base DN' (a text input field), 'Username' (a text input field), 'Connection' (a text input field), and 'Test Password' (a text input field). To the right of these fields, there is a text block showing LDAP URI examples: 'ldaps://<ipaddress>:[port]' and 'ldap://<ipaddress>:[port]', followed by a sample entry: 'For domain example.com cn=users,dc=example,dc=com'. At the bottom of the configuration section are 'Save' and 'Cancel' buttons.

For network/website authentication using LDAP Authentication, enter the necessary information and Save. Note that users will need to be added under the **Local User List** to have **Control** or **Admin** capabilities.

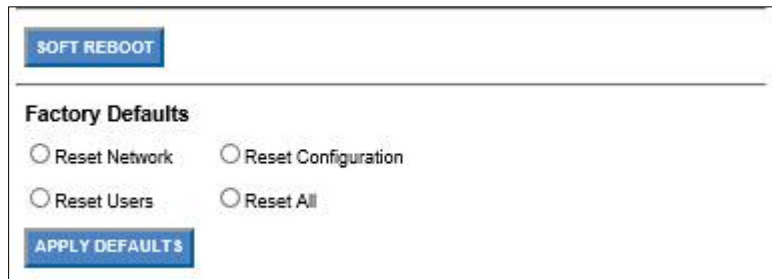
## Administration – Advanced

The screenshot shows the 'Administration' tab selected in the top navigation bar. Below it, the 'Advanced' sub-tab is active. The page contains several sections: 'Advanced' with a paragraph about system time configuration and reboot options; 'PDU Info' with fields for 'Firmware: 4.4.211 (Bootloader: unknown)', 'Serial Number: 116000003504e0003', and 'MAC Address: 00:0E:D3:06:9E:B8'; 'Time and Date Settings' with a 'Browser date and Time: Tue, 19 Nov 2019 22:02:27 UTC' and a 'Sync PDU Time' button; 'PDU Time in UTC' with dropdowns for 'Time: 22 Hrs 2 Mins 26 Secs' and 'Date: 19 Nov 2019'; a 'SOFT REBOOT' button; and 'Factory Defaults' with radio buttons for 'Reset Network', 'Reset Configuration', 'Reset Users', and 'Reset All', followed by an 'APPLY DEFAULTS' button.

PDU Info (Device info) includes serial number and MAC address. Model number and firmware version are also displayed in the gray summary box at the top of each screen.

Verify the **Time** and **Date Settings** to ensure date/time stamps on logs and alarms are correct.

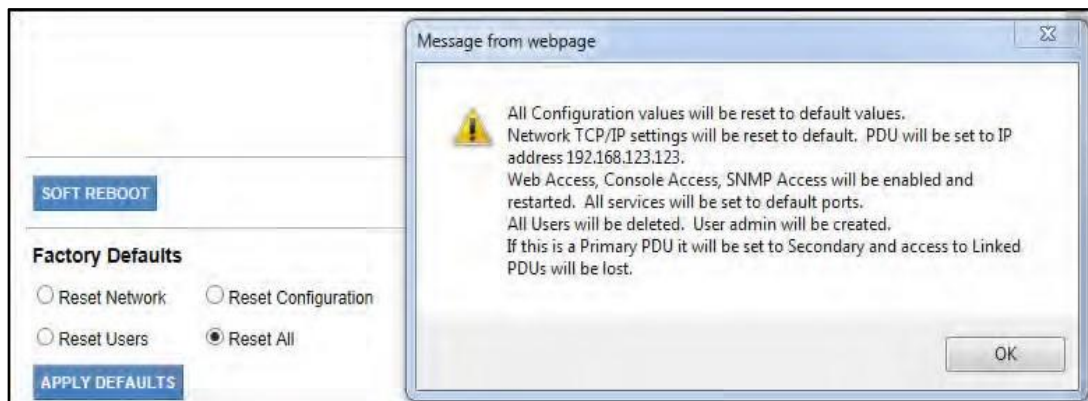
**Soft reboot** restarts the network connection, but does not power down outlets. Use this if you have connection problems.



The screenshot shows a web interface for configuring factory defaults. At the top is a blue button labeled "SOFT REBOOT". Below it is a section titled "Factory Defaults" containing four radio button options: "Reset Network", "Reset Configuration", "Reset Users", and "Reset All". At the bottom of this section is a blue button labeled "APPLY DEFAULTS".

**Factory Defaults** reset customer-entered values to the original factory defaults:

- **Reset Network** – Resets the device Network information to factory defaults including IP address (192.168.123.123). You may lose your network connection.
- **Reset Configuration** – Resets the device Configuration information to factory defaults including device name, alarms thresholds, etc. You will lose all configured fields.
- **Reset User** – Deletes all users except the single factory default admin user. Login will be reset to admin, admin and this user will have full admin capabilities.
- **Reset All** – Resets all fields to factory defaults.



To reset to factory defaults, select the appropriate radial button.

Review the warning message.

Click the **Apply Defaults** button to apply selected defaults. Resets are applied immediately.

## Administration – Upgrade Firmware

**Upgrade Firmware**

The version of firmware installed on this unit is listed in the gray box above.

You will need to specify your 'Upgrade Option' as shown below. 'Versions Less Than' refer to a version that is less than the version being used to upgrade the unit. 'Versions Not Equal' will only update if the unit's current version is not the same as the version being used to upgrade the unit, regardless of being newer or older. 'Force All Versions' will apply the version being used to upgrade the unit. The unit can be upgraded via HTTP, FTP, or TFTP. To initiate an upgrade, select the appropriate radio button, specify the appropriate fields, and click the 'Upgrade' button. The 'Test' button can be used to verify connectivity to the HTTP, FTP, or TFTP server.

Upgrade Option: ☒ Versions Less Than ☐ Versions Not Equal ☐ Force All Versions

☒ Upgrade this PDU via Network

☐ HTTP or FTP URL:  (eg: http://192.168.100.1/cpipack.bin)

☐ TFTP Server IP:  Filename:

☐ File  No file chosen

Post the downloaded firmware to an accessible HTTPS/FTP or TFTP directory or to a directory on a computer on the same network subnet as the device.

For HTTPS/FTP or TFTP upgrade, enter HTTPS/FTP or TFTP data.  
Click on **the Test** button to assure the remote site can be reached.  
Click on the **Upgrade** button to perform the upgrade.

For File upgrade, browse to the file and select the file (.bin).  
Click on **the Test** button to assure the computer can be reached.  
Click on the **Upgrade** button to perform the upgrade.

To upgrade the secondary device(s), select radial button Upgrade Linked devices and select the device to be upgraded.

Click on **the Test** button to assure the computer can be reached.  
Click on the **Upgrade** button to perform the upgrade.

*Note: This process runs in the background, can be unattended and the upgrading device(s) will still be fully functional while upgrading. However, this may take several hours depending on the number of devices in the Secure Array and amount of network traffic.*

After successful installation, the new firmware version will display in the device Info box at the top of the screen.

## USING THE APPLICATION PROGRAMING INTERFACE (API)

Refer to this link to get API instructions ([https://www.chatsworth.com/en-US/Documents/Software/Bulk\\_API\\_Excel\\_122108.zip](https://www.chatsworth.com/en-US/Documents/Software/Bulk_API_Excel_122108.zip))

Additional information about API Best Practices refer to <https://bocoup.com/blog/documenting-your-api>

## TROUBLESHOOTING GUIDE

### Local display is blank:

- Check the device status LED.
- Make sure the device is plugged into a live source.
- Timeout feature might be activated, press the middle button.

### Receptacle has no power:

- Check the circuit breaker for the branch. If necessary, switch it off then back on and recheck. (Note that all equipment connected to the branch will lose power.)
- Check power at the source.

### The device cannot establish Link to another device:

- Verify that proper cable is used to interface devices, use a standard Cat 5/6, 4-pair network cabinet with RJ45 connectors on both ends.
- Make sure the connectors are snapped in securely.
- Verify the integrity of the cable.

### Devices in the Secure Array are not displaying in the interface:

- Verify that the device models are compatible.
- Models with auxiliary ports will only connect to models that support Gigabit Ethernet.

### devices in the Secure Array are not displaying data that is appropriate to their level of functionality:

- Verify that the devices assigned to the PRIMARY and ALTERNATE roles are represented by the units with the highest level of functionality within the array.
- If the problem persists, verify that the units in the PRIMARY and ALTERNATE roles have the highest number of outlets within their functionality.

### No Ethernet Connection:

- Verify connection with a ping tool from any computer in the network.
- Check that the green LED in the device Ethernet port is lit.
- Check that the end connectors are snapped in place.

- Check the integrity of the cabling from the device's Ethernet port to the network switch/hub/router.
- Verify the port integrity of the network switch/hub/router.
- Verify via serial port that the network configurations for the device are set properly.

**For eConnect device with Electronic Lock Kit installed:**

**Lock issue**

**If lock status shows as “Not Configured” or “Lost Communication”**

- Check the cable that is connecting the lock to the CAN bus module for continuity.
- Check the cable that is connecting the CAN bus module to the device for continuity.

**If lock status shows as “Unlocked”**

- Check that the lock is locked using the appropriate mechanical key
- Check the cable that is connecting the lock to the CAN bus module for continuity.

**Door issue**

**If door status shows as “Not Configured” or “Lost Communication”**

- Check the cable that is connecting the door sensors with the CAN bus module for continuity.
- Check the cable that is connecting the CAN bus module to the device for continuity.

**If door status shows as “Open” while the door is closed:**

- Check that the door magnets are aligned properly.
- Check that the cable that is connecting the door magnets with the CAN bus module for continuity.

**Customer Support:**

US Tech Support: 1-800-834-4969 • [techsupport@chatsworth.com](mailto:techsupport@chatsworth.com)



## APPENDIX

### Regulatory Information:

CE

FCC Part 15, Class A

EN 55022

RoHS Compliant

UL &cUL Listed IEC

62368

Operating Temperature: 32 - 149°F (0 - 65°C) at Input Power Rating (kW) Operating non-condensing relative Humidity: 5 - 95%

Operating Elevation: 0-10000 ft (0-3000 m)

Storage Temperature: -13 - 149°F (-25 - 65°C)

Storage Relative Humidity: 5 - 95%

Storage Elevation: 0-50000ft (0-15000 m)

The Technical Construction File is held by CPI.

### Assigning a Smart Card ID

As discussed in the section **Administration – User Management** (page 50), each user may be assigned a unique smart card ID associated with their account that allows the device to unlock the Electronic Lock Kit mechanism (if installed) when a smart card is presented to the cabinet door lock. If the smart card ID is not known, there are two methods that can be used to interrogate the card electronically, in order to retrieve the smart card ID, and enter it into the eConnect system.

The first method utilizes the card reader and the event-logging system described in the **Logging – Overview** section of this manual to acquire the smart card ID.

Whenever a smart card is presented to Electronic Lock Kit, the key ID is read off the card, and then is compared to all key IDs known by the eConnect system. If the key ID is unknown, an entry is appended to the syslog to show that cabinet access has been attempted by an unknown user. The log entry includes the unknown smart card ID. The smart card ID can then be read from the syslog, and then entered into a user profile.

To easily copy the card ID from the syslog, double click the last set of characters on the pertinent log entry with the left mouse button to highlight it, then click the right mouse button and select **Copy** (or press **Ctrl-C** on the computer keyboard) to copy the characters to the windows clipboard.

## Syslog Entries

Time (UTC)	Entry
Feb 9 19:05:07	[PDU Cabinet]:[P6 lock tester]:[Audit] User admin logged in on the web GUI interface.
Feb 9 19:04:34	[PDU Cabinet]:[P6 lock tester]:[Audit] Front Door has encountered a failed access attempt. Card ID was <b>caa4b301f8ff12a4</b>

Next, find the user that will be associated with this card, or create a new user if necessary and add the username and password and click save. Change the Group association for this user to the cabinet, place the mouse cursor on the Card ID text box and left click once, then paste the smart card ID in with mouse right-click **Paste** (or via the keyboard by pressing **Ctrl-V**). Be sure to press the **Save** button to save the smart card ID.

From this point forward, the smart card ID will be known to the system and associated with the user. Note that once the card ID is into the system, it will no longer be displayed in the syslog entry for security purposes.

**Create User**


---

**User Profile**

User Name:

cardUser

Password:

 (Leave blank to keep current password)

Confirm Password:

Card ID:

caa4b301f8ff12a4

Group:

Cabinet ▼

Save

Cancel

The second method to interrogate an unknown smart card is to utilize the pcProx® Plus external card reader, CPI part number 36653-001, and a windows-based computer that is logged on to the eConnect web interface. The external card reader plugs into any available USB port on the computer and will generate “keystrokes” when a card is presented. Thus, the user places the mouse cursor on the Card ID text box, and when the card is presented to the external reader, the smart card ID characters are injected into the text box automatically, as if they were entered manually with a keyboard.

The external USB card reader does require software to be downloaded from the third-party vendor’s website, and configured to the type of smart card intended to be used on the system.

**NOTE:** At the time of writing of this manual, configurations have been tested for card types DesFire, HiD, iClass®, MIFARE and Prox cards. Other types of cards may be used with this reader, although some changes may need to be made to the external card reader settings so the key codes are correct. A comparison could be made between the syslog entry method described above to find the proper settings that provide a match for that family of cards. From that point forward, no changes to the external card reader’s configuration should be required to enroll more cards of the same type.

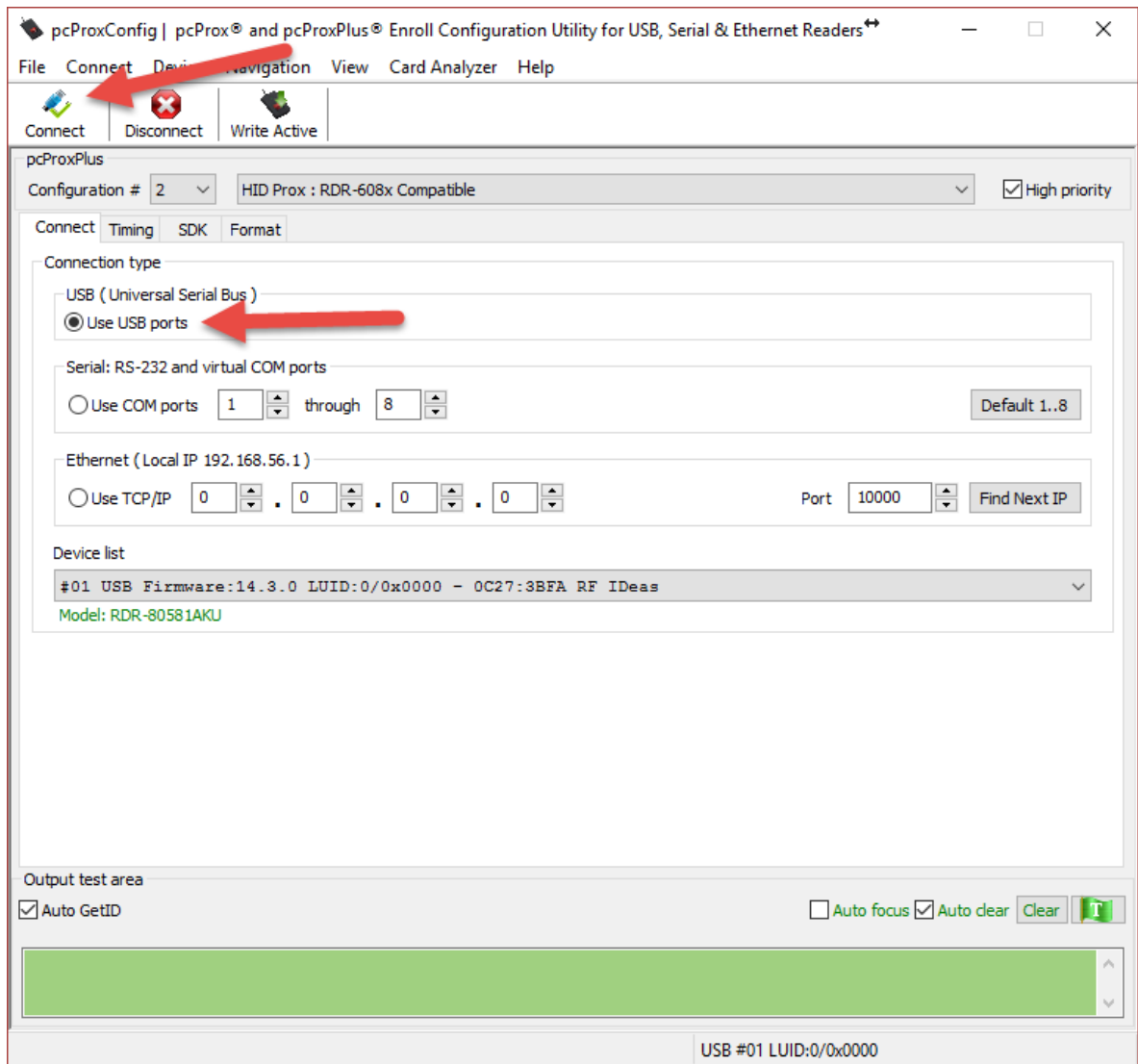
## Preparation

To configure the pcProx® Plus card reader, you must have the pcProx® Configuration Utility installed on your computer, which is available at

[www.rfideas.com/support/product-support/pcprox-plus](http://www.rfideas.com/support/product-support/pcprox-plus)

Click on the link above and save the resultant zip file to a directory on the computer. Unzip the contents of the zip file and click on the file pcProxConfig.exe (be sure the PC user has Administrator privileges to install programs). The pcProx® Configuration Utility will be installed with a start menu shortcut at **RF IDEas -> PCProx5 -> pcProxConfig.exe**

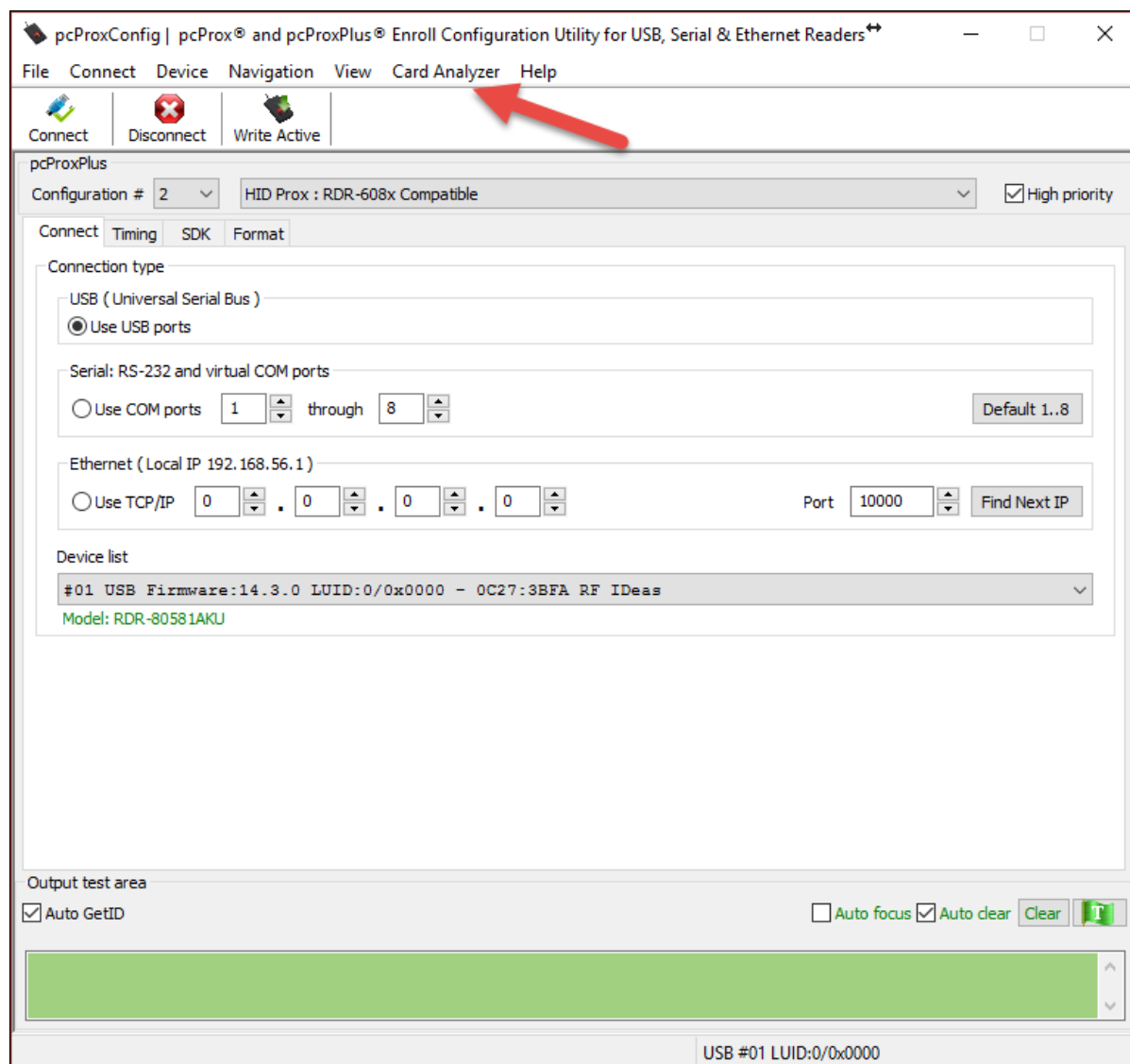
Plug in the pcProx® Plus card reader into an available USB port. Run the program PcProxConfig from the Windows start menu, click **Use USB ports**, and select the **Connect** button in the upper left of the screen to associate the program to the external reader.



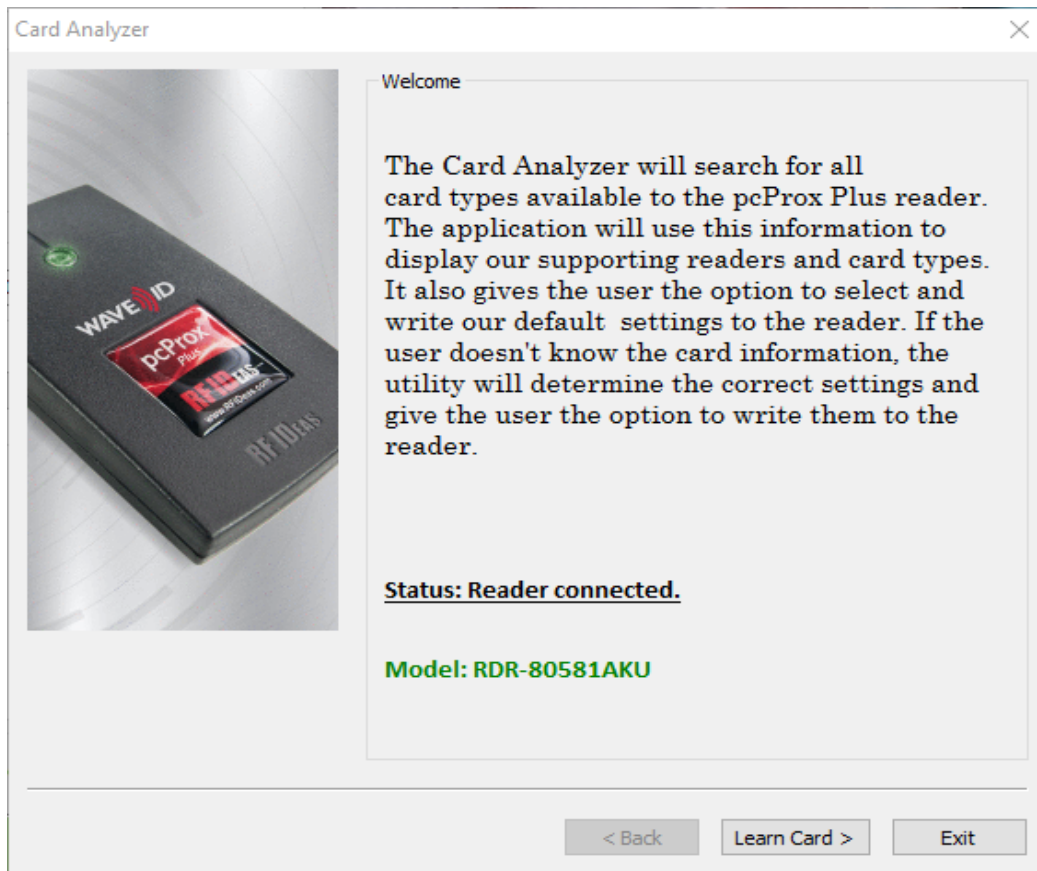
## Determining what Card Profile to use

The pcProx® Plus Card enrollment reader must be tailored to the **RFID Card Type** that will be used with the Electronic Lock Kit system. If the card type is one of the Desfire, HiD iClass, Mifare Classic or Prox, please proceed to **Programming the pcProx® Plus reader** on page 83.

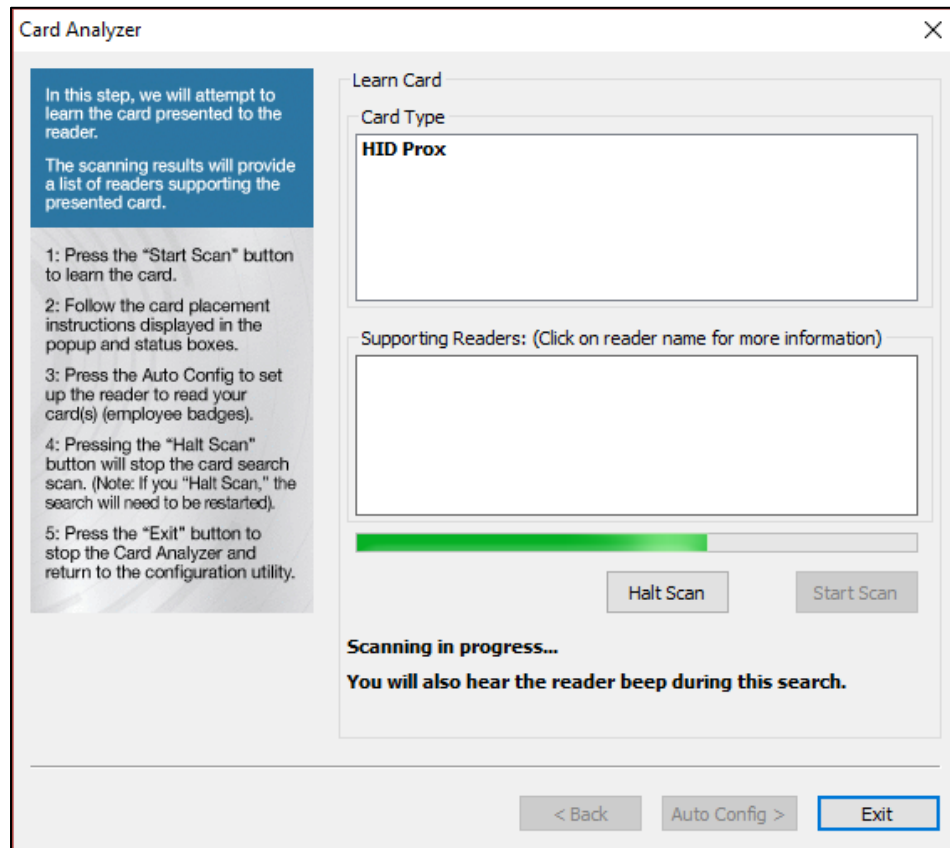
If the RFID card type is not known, the “**Card Analyzer**” Wizard, found under the “Card Analyzer” menu of the pcProxConfig program, can be used to scan for the Card Type:



After selecting Card Analyzer from the menu, place the ID card on the reader and press the Learn Card button:



The reader will then scan through several card types. When a compatible card type is found the **Card Type** box will show the type of card.



After determining the type, the user is ready to write the proper settings to the pcProx® Plus reader.

### Programming the pcProx® Plus reader

In order for the pcProx® Plus reader to be compatible with the Electronic Lock Kit, the card reader must be flashed with the proper reader settings, as shown in the following steps:

The **Card Type** must be set from the drop-down selector on the **Format – Data Format** tab page. Additionally, the other fields and checkboxes on that page should initially be configured as shown below. Three advanced settings shown within a red rectangle must be checked or unchecked, depending on the **Card Type**. After all the settings have been made press the **Write Active** button to write the settings to the pcProx® Plus reader.

pcProxConfig | pcProx® and pcProxPlus® Enroll Configuration Utility for USB, Serial & Ethernet Readers

File Connect Device Navigation View Card Analyzer Help

Connect Disconnect Write Active

pcProxPlus

Configuration # 2 HID Prox : RDR-608x Compatible High priority

Connect Timing SDK Format

☒ Data format / Delimiters ☐ Extended / Hashing

Data format Delimiters Extended Hashing

ABC 123 : 987654321XYZT GN

Wiegand to keystroke data format

Parity bits

Strip leading bit count 0

Strip trailing bit count 0

☐ Send FAC ☐ Send FAC as hexadecimal number

☐ Send ID ☒ Send ID as hexadecimal number

ID field bit count 16

☐ Fix length FAC / ID fields

FAC digits 3

ID digits 5

Advanced settings

☐ Only read cards with this bit count 26

☐ Display hexadecimal in lowercase (a-f)

☐ Use numeric keypad for 0-9 (European)

☐ AZERTY keyboard shift lock

☐ FAC extended precision math on

☒ ID extended precision math on

☐ Reverse Wiegand bytes

☐ Reverse Wiegand bits

☒ Invert Wiegand bits

☐ Emulate ProxPro - append serial checksum

Output test area

☒ Auto GetID ☐ Auto focus ☒ Auto clear Clear T

Ready USB #01 LUID:0/0x0000



## Common RFID Card Types and Reader Format Settings

### Desfire Card:

pcProxConfig | pcProx® and pcProxPlus® Enroll Configuration Utility for USB, Serial & Ethernet...

File Connect Device Navigation View Card Analyzer Help

Connect Disconnect Write Active

pcProxPlus

Configuration # 1 DESFire CSN (Oyster, NFC 4) High priority

Connect Timing SDK Format

☒ Data format / Delimiters ☐ Extended / Hashing

Data format Delimiters Extended Hashing

ABC 123 : 987654321XYZT GN

Wiegand to keystroke data format

Parity bits

Strip leading bit count 0

Strip trailing bit count 0

☐ Send FAC ☐ Send FAC as hexadecimal number

☐ Send ID ☒ Send ID as hexadecimal number

ID field bit count 64

☐ Fix length FAC / ID fields

FAC digits 3

ID digits 5

Advanced settings

☐ Only read cards with this bit count 64

☐ Display hexadecimal in lowercase (a-f)

☐ Use numeric keypad for 0-9 (European)

☐ AZERTY keyboard shift lock

☐ FAC extended precision math on

☒ ID extended precision math on

☐ Reverse Wiegand bytes

☐ Reverse Wiegand bits

☒ Invert Wiegand bits

☐ Emulate ProxPro - append serial checksum

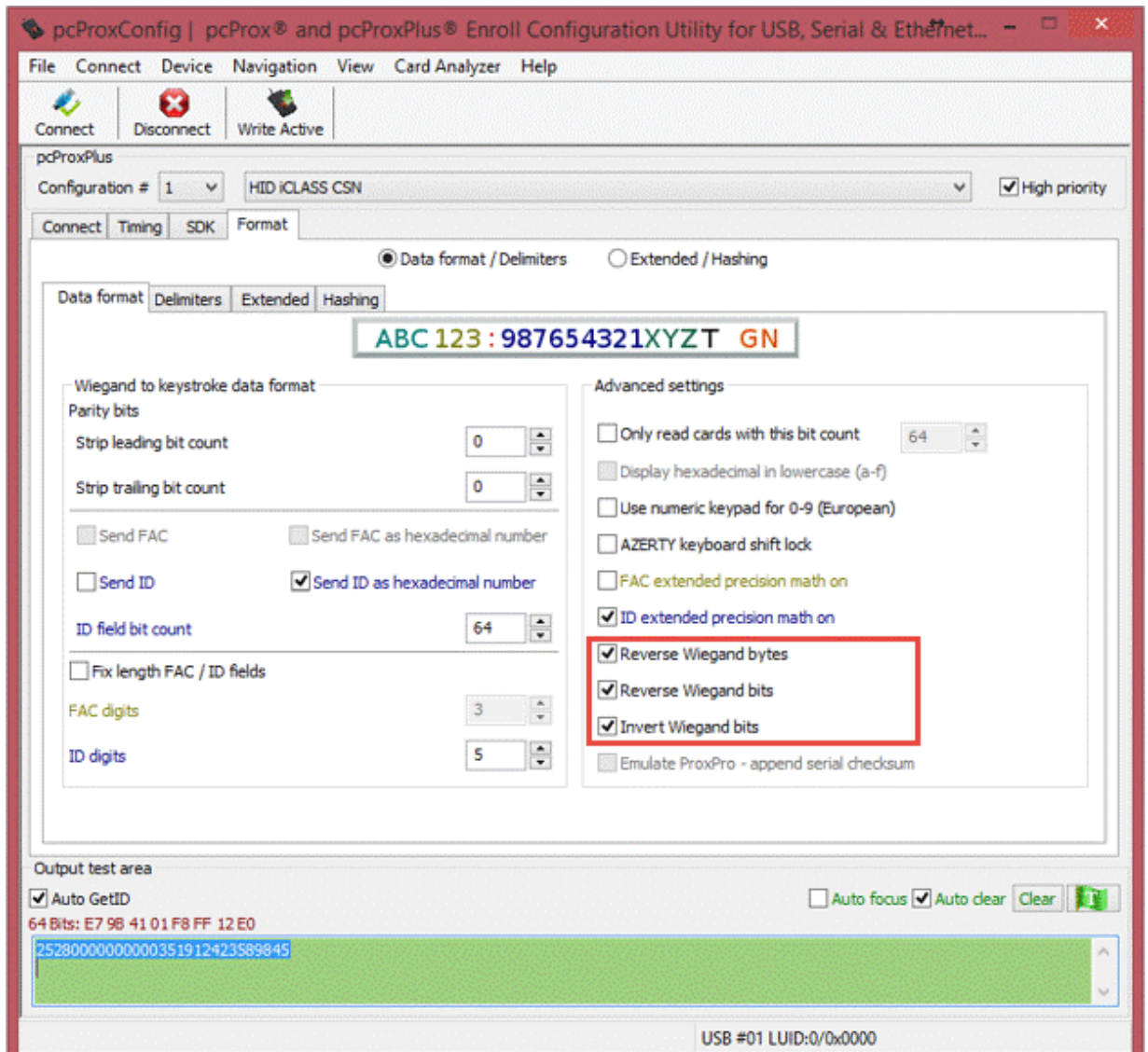
Output test area

☐ Auto GetID ☐ Auto focus ☒ Auto clear Clear T

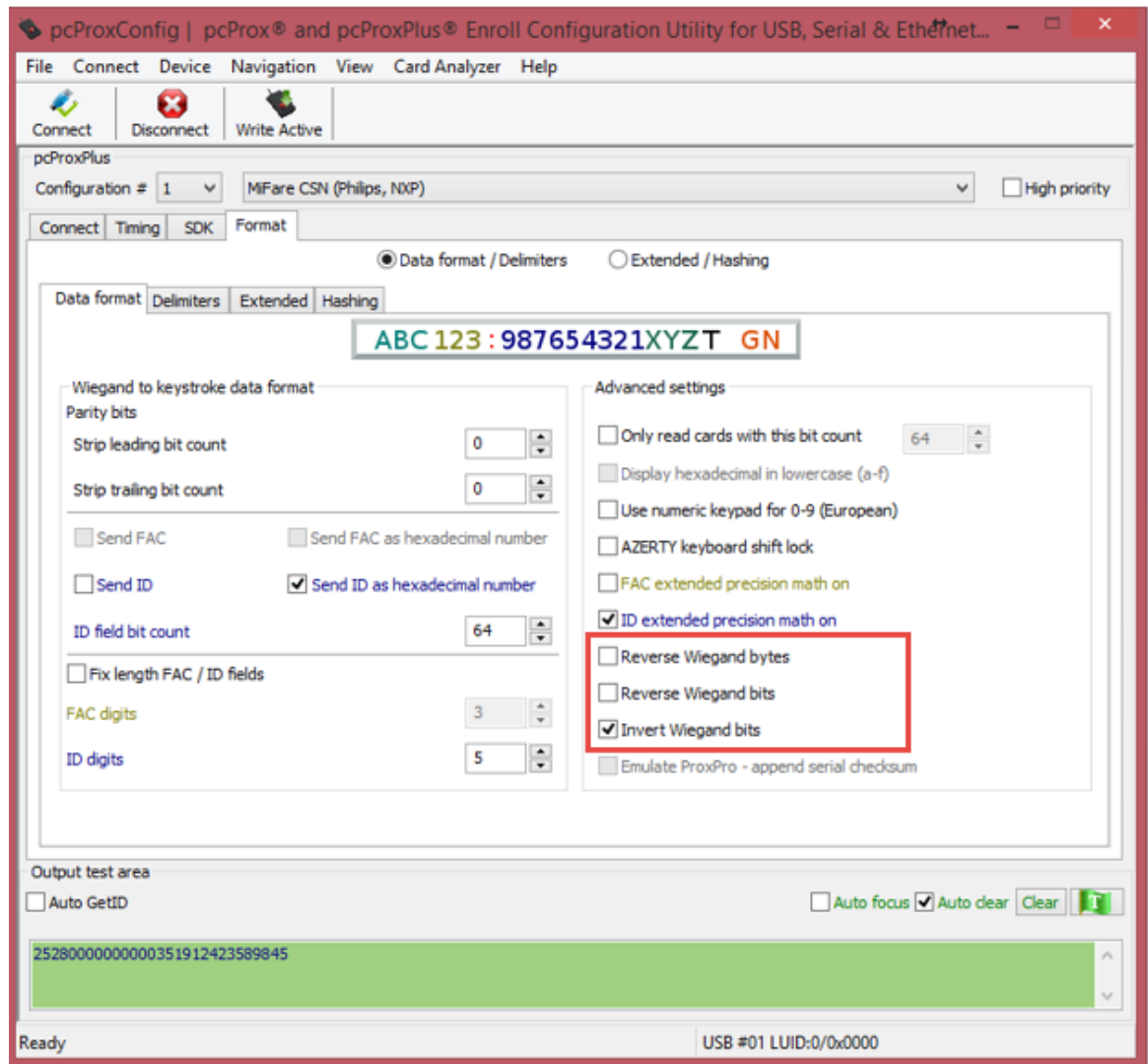
25280000000000351912423589845

Ready USB #01 LUID:0/0x0000

## HiD iClass Card:



## MiFare Classic Card:



## Prox Card:

Prox cards require an additional settings in the **Wiegand to keystroke data format** box, as shown below:

The screenshot shows the **pcProxConfig** application window. The title bar reads "pcProxConfig | pcProx® and pcProxPlus® Enroll Configuration Utility for USB, Serial & Ethernet...". The menu bar includes File, Connect, Device, Navigation, View, Card Analyzer, and Help. Below the menu bar are buttons for Connect, Disconnect, and Write Active. The main window is titled "pcProxPlus" and shows "Configuration # 1" and "HID Prox : RDR-608x Compatible". The "Format" tab is selected, showing "Data format / Delimiters" and "Extended / Hashing" options. The "Data format" sub-tab is active, displaying a preview of the data format: "ABC 123 : 987654321XYZT GN". The "Wiegand to keystroke data format" section is highlighted with a red box. It contains the following settings: "Strip leading bit count" set to 1, "Strip trailing bit count" set to 1, "Send FAC" (unchecked), "Send FAC as hexadecimal number" (unchecked), "Send ID" (checked), "Send ID as hexadecimal number" (checked), "ID field bit count" set to 16, "Fix length FAC / ID fields" (unchecked), "FAC digits" set to 3, and "ID digits" set to 5. The "Advanced settings" section is also highlighted with a red box. It contains the following settings: "Only read cards with this bit count" set to 26, "Display hexadecimal in lowercase (a-f)" (unchecked), "Use numeric keypad for 0-9 (European)" (unchecked), "AZERTY keyboard shift lock" (unchecked), "FAC extended precision math on" (unchecked), "ID extended precision math on" (unchecked), "Reverse Wiegand bytes" (unchecked), "Reverse Wiegand bits" (unchecked), "Invert Wiegand bits" (checked), and "Emulate ProxPro - append serial checksum" (unchecked). The "Output test area" at the bottom shows "Auto GetID" (unchecked), "Auto focus" (unchecked), "Auto clear" (checked), and a "Clear" button. The output area displays the text "2528000000000351912423589845". The status bar at the bottom right shows "USB #01 LUID:0/0x0000".