

---

# Networked Electronic Access Control User Manual

**Version 1.0**  
**October 2017**



**CHATSWORTH  
PRODUCTS**

[techsupport@chatsworth.com](mailto:techsupport@chatsworth.com)  
[www.chatsworth.com](http://www.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.

©2017 Chatsworth Products, Inc. All rights reserved. Chatsworth Products, CliK-Nut, CPI, CPI Passive Cooling, CUBE-IT PLUS, eConnect, Evolution, GlobalFrame, MegaFrame, OnTrac, QuadraRack, RMR, Saf-T-Grip, Seismic Frame, SlimFrame, TeraFrame and Velocity are federally registered trademarks of Chatsworth Products. EuroFrame, Motive, Secure Array and Simply Efficient are trademarks of Chatsworth Products. All other trademarks belong to their respective companies. 11/17 MKT-60020-696

## Table of Contents

Introduction .....	3
Legal Information .....	3
Warranty .....	3
Product Features .....	4
Product Labeling and Certifications .....	5
Installation Checklist .....	6
Installation Guide .....	7
Using Built-In Web Server Application .....	8
Network Settings .....	9
Status Alarms (screen) .....	11
Networked EAC – Overview (screen) .....	12
Logging – Overview .....	13
Logging – Export Logs .....	14
Logging – Settings .....	14
Notifications – Thresholds .....	15
Notifications – Routing .....	16
Settings – PDU .....	17
Settings – Environmental .....	18
Settings – SNMP .....	19
Settings – Emails .....	20
Administration- User Management .....	20
Administration – Radius Authentication .....	22
Administration – LDAP Authentication .....	22
Administration – Advanced .....	23
Administration – Firmware Upgrade .....	25
Troubleshooting Guide .....	26
Appendix .....	28
Configure the pcPROX Plus Reader .....	30
Programming the pcPROX Plus Reader .....	35
Common RFID Card Types .....	36
HiD iClass Card .....	37
MiFare Classic Card .....	38
Prox Card .....	39

# INTRODUCTION – User Manual for Networked Electronic Access Control

This document is the User Manual for Networked Electronic Access Control (EAC).

©2017 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 remanufactured 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

**PDU:** 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

**Input Voltage:** 110 - 220 Volts at 15 Amps, 50/60Hz power

**Power Input Cable:**

Length: Standard: 10 ft (3 m)

Plug type: ICC 14

### 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>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>

# INSTALLATION CHECKLIST

## Safety Warnings and Cautions

- DO NOT OPEN THE CHASSIS of the device. 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 chassis.
- Do not insert objects of any kind into the chassis 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.

## Checklist for Networked EAC:

- 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 Key Card ID (Go to Page xx 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 EAC 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 EAC, 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 Probe Port.
- Use environmental probes with splitter (P/N 117761-003):
- 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 devices are shipped with:

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

**192.168.123.123**

Default User name/Password: **admin/admin**

If the IP address of the device has been altered, then the user needs to reset the IP back to the Default address provided above.

You can access the device using the default IP address 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 IP address>. For example, the default would be: <http://192.168.123.123>

The Login Screen will display:



Log in using default User name and password: **admin, admin** and **click on Login** button or user name 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**.

## Network Settings

**System Info**  
Name: TLab Test Unit  
Location: Unit Description  
IP Address: 192.168.123.123  
Firmware: 4.2.54

**Session Info**  
User: admin  
Last Login: 2017-10-19 19:21  
Uptime: 0d 3h 27m

**No Alarm**

Help | Logout

Status Cabinet Access Logging Notifications **Settings** Administration

PDU Environmental **Network** SNMP Emails My 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:fe00:1477/64

Global IP  Manually Configure IPv6

<b>IPv4 Setup</b>	<b>IPv6 Setup</b>
IP Address: 192.168.123.123	IP Address: ..
Subnet Mask: 255.255.255.0	Prefix Length: 0
Default Gateway: 192.168.123.1	Default Gateway: ..

<b>IPv4 DNS Servers</b>	<b>IPv6 DNS Servers</b>
Primary DNS Server: 0.0.0.0	Primary DNS Server: ..
Secondary DNS Server: 0.0.0.0	Secondary DNS Server: ..

#### Time Servers

RFC Time Server:

NTP Time Server:

#### Web Access Settings

Enable HTTP Port: 80

Enable HTTPS Port: 443

Save Cancel

Copyright © 2017 Chatsworth Products, Inc. All Rights Reserved.

Version 1.21 Last Updated: 2017-06-23 12:51

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** (page 19).

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.

**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.

### Sensor Status

	Temp	Humidity
Probe1 Test1	71.38 °F	53.78 %
Probe2 Test2	73.07 °F	55.16 %

### Front Door Status

State
Door: Closed
Lock: Locked

### Rear Door Status

State
Door: Closed
Lock: Locked

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 key 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 ACK buttons can be used to acknowledge that an alarm is present.

By acknowledging an alarm, the yellow or red status indicator next to the device's display will stop blinking and notification for this particular alarm will no longer be sent out through SNMP. The alarm remains present in the Alarms Status page while the alarm is active. The ACK feature is recommended when the customer is aware of the alarm and in the process of resolving it, and does not want to be notified by the device any longer.

# Networked Electronic Access Control – Overview

My Profile
Overview Settings

Status
Cabinet Access
Logging
Notifications
Settings
Administration

### Cabinet Access Overview

View the state of the two doors attached to the cabinet. The doors can be either closed and unlocked, closed and locked or completely opened. The third table shows the five most recent door openings/closings to the cabinet.

#### Front Door Status

State
Door: Closed
Lock: Locked
<a href="#" style="color: #2c5e8c; text-decoration: none; padding: 2px 10px;">UNLOCK</a>

#### Rear Door Status

State
Door: Closed
Lock: Locked
<a href="#" style="color: #2c5e8c; text-decoration: none; padding: 2px 10px;">UNLOCK</a>

#### Recent Openings/Closings

Door	Cabinet	PDU	Time Opened	Time Closed
Rear	Unit Cabinet	Unit Name	12 Oct 2017 21:05:21 UTC	12 Oct 2017 21:05:27 UTC
Front	Unit Cabinet	Unit Name	12 Oct 2017 21:04:46 UTC	12 Oct 2017 21:05:18 UTC
Rear	Unit Cabinet	Unit Name	12 Oct 2017 15:26:03 UTC	12 Oct 2017 15:26:12 UTC
Front	Unit Cabinet	Unit Name	12 Oct 2017 15:25:21 UTC	12 Oct 2017 15:25:34 UTC
Front	Unit Cabinet	Unit Name	12 Oct 2017 15:24:14 UTC	12 Oct 2017 15:24:24 UTC

Copyright © 2017 Chatsworth Products, Inc. All Rights Reserved.
Version 1.21 Last Updated: 2017-10-02 18:41

# Cabinet Access – Settings

Overview Settings

Status
Cabinet Access
Logging
Notifications
Settings
Administration

### Cabinet Access Settings

Select the checkboxes for "Enable Front Lock" and/or "Enable Rear Lock", and then click the "Save" button to initiate configuration of the Electronic Access Control system. Once completed, the system will be able to interact with the cabinet's door locks, send notifications on error conditions, and give a real-time status.

Cabinet Lock Open Time:  Seconds

Cabinet Door Open Alarm Time:  Minutes

Enable Front Lock
 Enable Rear Lock

#### Front Door Status

State
Door: Closed
Lock: Locked

#### Rear Door Status

State
Door: Closed
Lock: Locked

Save
Cancel

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.

## Logging - Overview

**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
Oct 13 20:20:53	[Unit Cabinet];[Unit Name];[System] PDU warm booted. Outlet configuration retained.
Oct 13 20:12:57	[Unit Cabinet];[Unit Name];[System] PDU warm booted. Outlet configuration retained.
Oct 13 20:10:26	[Unit Cabinet];[Unit Name];[Audit] Rear Door has encountered a failed access attempt. Card ID was d4095b02f9ff12e0
Oct 13 20:05:54	[Unit Cabinet];[Unit Name];[Audit] User admin logged in on the web GUI interface.
Oct 13 20:05:45	[Unit Cabinet];[Unit Name];[Audit] User admin FAILED to log in on the web GUI interface.
Oct 13 19:54:12	[Unit Cabinet];[Unit Name];[Audit] User admin logged in on the web GUI interface.
Oct 13 19:48:55	[Unit Cabinet];[Unit Name];[Audit] User admin logged in on the serial interface.
Oct 13 19:48:51	[Unit Cabinet];[Unit Name];[Audit] User admin FAILED to log in on the serial interface.
Oct 13 19:41:21	[Unit Cabinet];[Unit Name];[System] PDU warm booted. Outlet configuration retained.
Oct 13 19:03:30	[Unit Cabinet];[Unit Name];[Event] Rear Lock has been locked.

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

**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: May 18 13:22:13 - 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

**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

**Syslog Server**

Server Address: \_\_\_\_\_ Port: 514

Save Cancel

### Metric Data Logging:

Check Enable Logging check box to begin capturing data on the device's 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's 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

The screenshot shows a web interface for configuring notification thresholds. At the top, there are navigation tabs: Status, Cabinet Access, Logging, Notifications (selected), Settings, and Administration. Below the tabs, there are sub-tabs: Thresholds (selected) and Routing. A 'My Profile' link is visible in the top right corner. The main content area is titled 'Notification Thresholds' and includes a descriptive paragraph: '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.' Below this is a section for 'Environmental Thresholds' with a 'Clear All' button. A table with 5 columns (Sensor, Critical Low, Warning Low, Warning High, Critical High) and 4 rows (Temperature 1, Temperature 2, Humidity 1, Humidity 2) is shown. Each cell in the table contains a text input field with a unit (°C or %). At the bottom of the table are 'Save' and 'Cancel' buttons.

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

## Environmental Thresholds

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

# 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 All
  Select All
  Select All

Save
Cancel

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 PDU if applicable by checking the check box(es): Log, Trap, Email.

Click on Save to save the input data.

## Settings – PDU

Use this tab to set the system for the Controller Module

The screenshot shows a web interface for configuring a PDU. At the top, there are navigation tabs: Status, Cabinet Access, Logging, Notifications, Settings (selected), and Administration. Below these are sub-tabs: PDU, Environmental, Network, SNMP, and Emails. A 'My Profile' link is visible in the top right. The main content area is titled 'System Settings' and includes the instruction: 'Edit SecureArray™ and general system related configuration properties.' The form contains the following fields and options:

- 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

At the bottom of the form are 'Save' and 'Cancel' buttons. The footer contains the text: 'Copyright © 2017 Chatsworth Products, Inc. All Rights Reserved.' and 'Version 1.21 Last Updated: 2017-10-09 19:52'.

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 'Environmental Settings' page. At the top, there is a navigation bar with tabs for 'Status', 'Cabinet Access', 'Logging', 'Notifications', 'Settings', and 'Administration'. Below this, there is a sub-navigation bar with 'PDU', 'Environmental', 'Network', 'SNMP', and 'Emails'. The 'Environmental Settings' section 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' and '\*C'. There are two text input fields for 'Probe 1 Name' (containing 'Probe1 Test1') and 'Probe 2 Name' (containing 'Probe2 Test2'). At the bottom of the form are 'Save' and 'Cancel' buttons.

Select choice of temperature unit, enter name for the probes. Click on **Save**.

## Settings – Network

The screenshot shows the 'Network Settings' page. At the top, there is a navigation bar with tabs for 'Status', 'Cabinet Access', 'Logging', 'Notifications', 'Settings', and 'Administration'. Below this, there is a sub-navigation bar with 'PDU', 'Environmental', 'Network', 'SNMP', and 'Emails'. The 'Network Settings' section is titled 'Network Settings' and contains the text 'Edit network related configuration properties.' Below this, there is a 'TCP / IP Configuration' section with a dropdown menu for 'Enable Protocols' (set to 'IPv4 and IPv6'). There are checkboxes for 'Manually Configure IPv4', 'Link Local IPv6' (with address 'fe80::20e:d3ff:fe00:1477/64'), 'Global IP', and 'Manually Configure IPv6'. Below this are two columns of settings: 'IPv4 Setup' and 'IPv6 Setup'. The 'IPv4 Setup' column has fields for 'IP Address' (192.168.123.123), 'Subnet Mask' (255.255.255.0), and 'Default Gateway' (192.168.123.1). The 'IPv6 Setup' column has fields for 'IP Address' (empty), 'Prefix Length' (0), and 'Default Gateway' (empty). Below these are 'IPv4 DNS Servers' and 'IPv6 DNS Servers' sections, each with 'Primary DNS Server' and 'Secondary DNS Server' fields. The 'IPv4 DNS Servers' fields contain '0.0.0.0'. Below these are 'Time Servers' with 'RFC Time Server' and 'NTP Time Server' fields. At the bottom are 'Web Access Settings' with checkboxes for 'Enable HTTP' (Port: 80) and 'Enable HTTPS' (Port: 443). At the bottom of the form are 'Save' and 'Cancel' buttons.

- **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 PDU using a web browser and HTTP or HTTPS.

Click on **Save**.

## Settings – SNMP

The screenshot shows the 'SNMP Settings' configuration page. At the top, there is a navigation bar with tabs for 'Status', 'Cabinet Access', 'Logging', 'Notifications', 'Settings' (which is active), and 'Administration'. Below this is a sub-navigation bar with 'PDU', 'Environmental', 'Network', 'SNMP' (which is active), and 'Emails'. The main content area is titled 'SNMP Settings' and includes the following sections:

- SNMP Settings**: A sub-header with the instruction 'Edit SNMP and trap related configuration properties.' Below it is a checked checkbox for 'Enable SNMP Access'. Fields for 'Listen Port' (161), 'Trap Port' (162), and 'Security Level' (V1) are present.
- SNMP V1 and V2c Settings**: Fields for 'Read Community' (default: public) and 'Write Community' (default: private). A 'Limit Host Access' checkbox is present. Three rows of 'Host IP Address' fields are shown, each with IPv4 and IPv6 input boxes.
- SNMP V3 Settings**: Fields for 'USM User', 'Auth Algorithm' (SHA), 'Auth Password', 'Priv Algorithm' (DES), 'Priv Password', and 'Context Name'.
- Send Traps To**: Three rows of 'Host IP Address' fields, each with IPv4 and IPv6 input boxes.
- Additional Trap Settings**: Fields for 'Alarm Interval' (0 Minutes), 'Log Interval' (0 Minutes), and 'Log Difference' (0 Amps).

At the bottom of the form are 'Save' and 'Cancel' buttons. The footer contains the copyright notice 'Copyright © 2017 Chatsworth Products, Inc. All Rights Reserved.' and the version information 'Version 1.21 Last Updated: 2017-06-23 12:51'.

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](#)

Copyright © 2017 Chatsworth Products, Inc. All Rights Reserved. Version 1.21 Last Updated: 2017-04-24 14:35

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.

## Administration – User Management

**System Info**  
Name: Unit Name  
Location: Unit Description  
IP Address: 192.168.123.123  
Firmware: 4.2.48

**Session Info**  
User: admin  
Last Login: 2017-10-13 20:05  
Uptime: 0d 0h 52m

[Help](#) | [Logout](#)

**User Management**

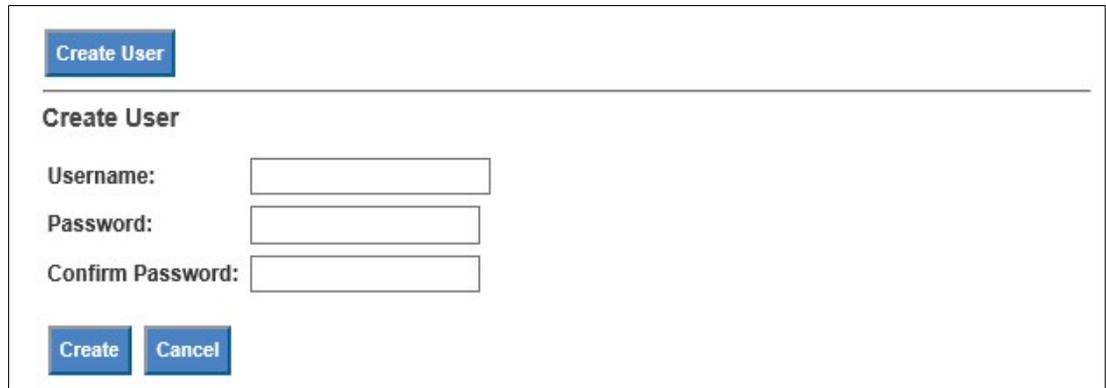
Create, edit, and delete users. Users can be a member of one of 4 groups: Admin, Cabinet, Viewer, User. A user's group will determine a user's level of web interface access. The 'Viewer' group has no configuration access. The 'User' group has limited configuration access. The 'Cabinet' group has the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

User Name	Group	Card ID	Action
admin	Admin		<a href="#">Edit</a> <a href="#">Delete</a>

[Previous Page](#) **User List Page: 1** [Next Page](#)

[Create User](#)

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



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

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



Change the necessary information. Input the Key Card ID for the Electronic Access Control. If you don't know your Key Card ID, see Appendix. The User Name must be in the Cabinet Group, for the user to see the cabinet tab.

**IMPORTANT:** 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

The screenshot shows the 'Administration' tab selected in the top navigation bar. Below it, the 'Radius Authentication' sub-tab is active. The page title is 'Radius Authentication'. A descriptive paragraph states: '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.'

There is a checkbox labeled 'Enable Radius Server' which is currently unchecked. Below this are several input fields: 'Radius Server', 'Radius Secret', 'NAS Server', 'Connection', and 'Test Password'. To the right of these fields is a 'Port' field with the value '1812'. At the bottom left of the form are 'Save' and 'Cancel' buttons.

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 title is 'LDAP Authentication'. A descriptive paragraph states: '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.'

There is a checkbox labeled 'Enable LDAP Authentication' which is currently unchecked. Below this are several input fields: 'LDAP Server URI', 'Base DN', 'Username', 'Connection', and 'Test Password'. To the right of these fields are two lines of text: 'ldaps://<ipaddress>:[port]' and 'ldap://<ipaddress>:[port]', followed by an example: 'For domain example.com cn=users,dc=example,dc=com'. At the bottom left of the form are 'Save' and 'Cancel' buttons.

Copyright © 2017 Chatsworth Products, Inc. All Rights Reserved. Version 1.21 Last Updated: 2017-04-24 14:35

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

**Advanced**

The system time can be configured by synchronizing with the web browser, if desired. Clicking "Soft Reboot" will perform a reboot of the entire system. Also, the system 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: 4.2.54 (Bootloader: unknown)  
Serial Number:  
MAC Address: 00:0E:D3:00:14:77

**Time and Date Settings**

Browser date and Time: Thu, 19 Oct 2017 18:30:09 UTC [Sync PDU Time](#)

PDU Time in UTC  
Time: 19 Hrs 28 Mins 13 Secs  
Date: 19 Oct 2017

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

[SOFT REBOOT](#)

**Factory Defaults**

Reset Network  Reset Configuration  
 Reset Users  Reset All

[APPLY DEFAULTS](#)

Copyright © 2017 Chatsworth Products, Inc. All Rights Reserved. Version 1.21 Last Updated: 2017-10-02 18:41

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  
Use this if you have connection problems.

[SOFT REBOOT](#)

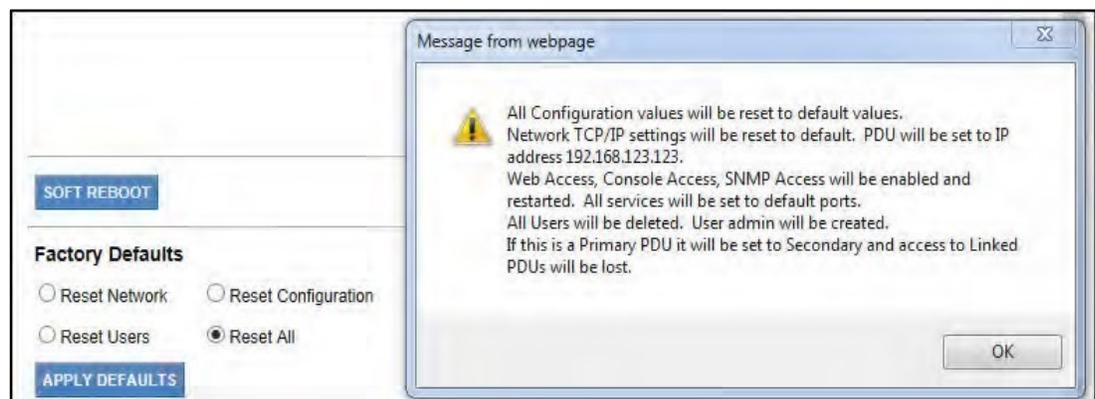
**Factory Defaults**

Reset Network  Reset Configuration  
 Reset Users  Reset All

[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 – Firmware Upgrade

**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

Copyright © 2017 Chatsworth Products, Inc. All Rights Reserved. Version 1.21 Last Updated: 2017-10-02 18:41

Post the downloaded firmware to an accessible HTTP/FTP or TFTP directory.

Enter HTTP/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.

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

### Additional Software

**Note:** Linked devices with firmware version **4.XX.XXX** or later can be upgraded from the network (remotely) using the Firmware Upgrader, a separate software program available from [www.chatsworth.com/Supportand-Downloads/Downloads/Software](http://www.chatsworth.com/Supportand-Downloads/Downloads/Software).

## TROUBLESHOOTING GUIDE

### **Controller cannot establish Link to another Controller:**

- 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.
- If problem persists after a power cycle, the device unit must be replaced.

### **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.
- If the Ethernet communication problem persists after power cycling it, replace the controller unit.

### **Lock issue**

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

- Check the cable that is connecting the swinghandle to the CAN bus module for continuity.
- Check the cable that is connecting the CAN bus module to the controller for continuity.

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

- Check that the swinghandle is locked using the appropriate mechanical key
- Check the cable that is connecting the swinghandle 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 controller 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**

# APPENDIX

## Regulatory Information:

FCC Part 15, Class A  
EN 55022  
RoHS  
UL & cUL 60950-1 Listed  
IEC 60950

## Assigning a Key Card ID

As discussed in the section **Administration – User Management** (page 71), each user may be assigned a unique key card ID associated with their account that allows the device to unlock EAC mechanism (if installed) when a key card is presented to the cabinet door lock. If the key card ID is not known, there are two methods that can be used to interrogate the card electronically, in order to retrieve the key card ID, and enter it into the 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 key card ID.

Whenever a key card is presented to the Networked EAC, the key ID is read off the card, and then is compared to all key IDs known by the 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 key card ID. The key card ID can then be read from the syslog, and then entered into a user profile.

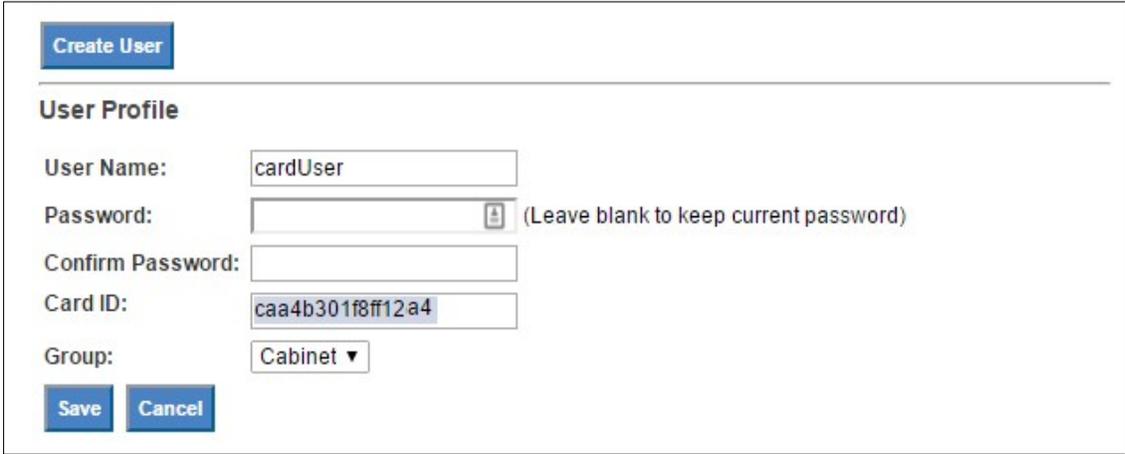
To easily copy the card ID from the syslog, double click the last set of characters on the pertinent log entry with the left mouse button to highlight it, then click the right mouse button and select **Copy** (or press **Ctrl-C** on the computer keyboard) to copy the characters to the windows clipboard.

### 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 user name 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 key 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 key card ID.

From this point forward, the key 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.



The screenshot shows a web interface for creating a user. At the top left is a blue button labeled "Create User". Below it is a section titled "User Profile". The form contains the following fields:

- User Name:** A text box containing "cardUser".
- Password:** A text box with a small icon on the right. To its right is the text "(Leave blank to keep current password)".
- Confirm Password:** An empty text box.
- Card ID:** A text box containing "caa4b301f8ff12a4".
- Group:** A dropdown menu currently showing "Cabinet".

At the bottom of the form are two blue buttons: "Save" and "Cancel".

The second method to interrogate an unknown key 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 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 key 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 key 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 Classic, 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.

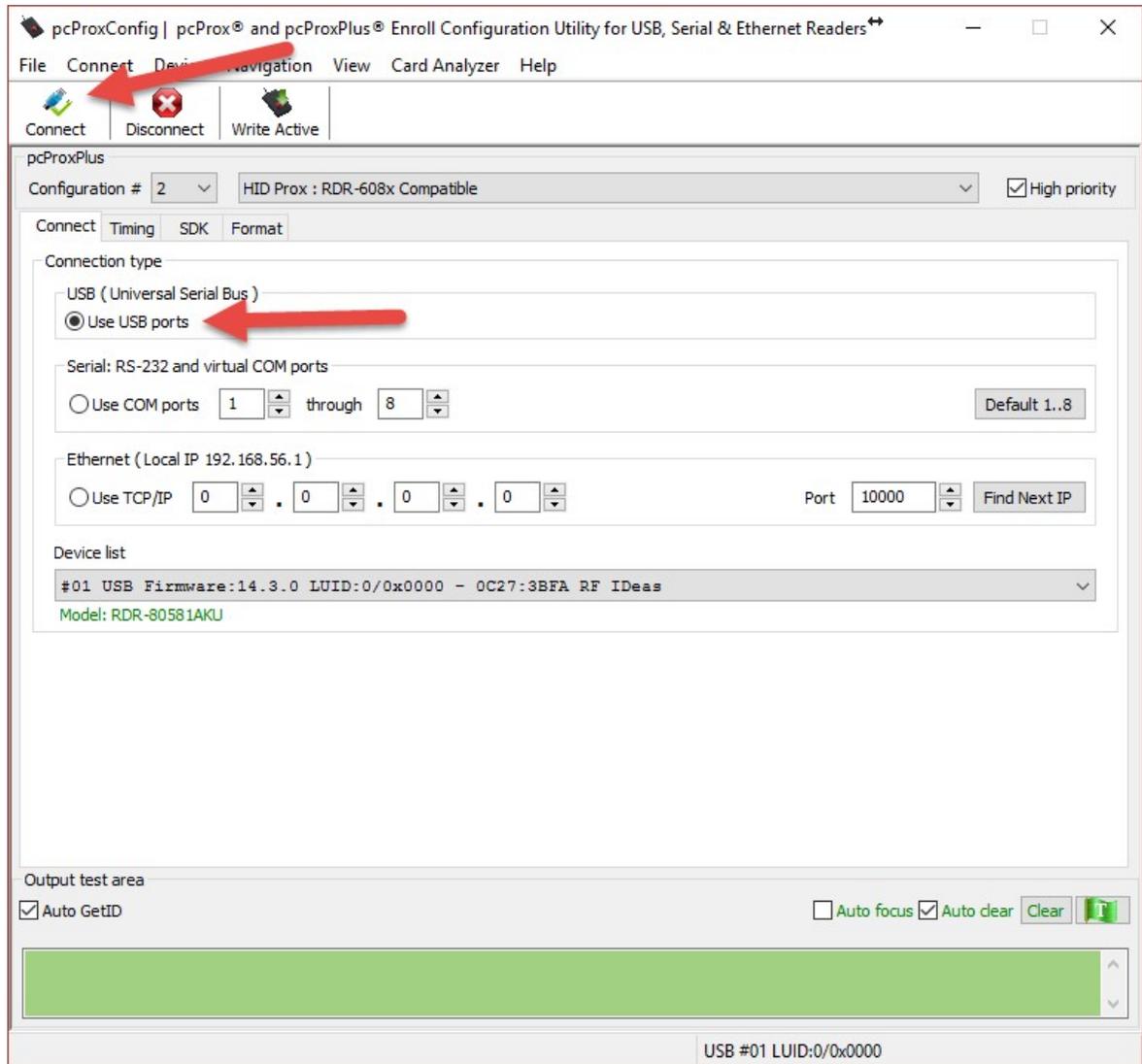
## Configuring the pcPROX Plus Reader

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**

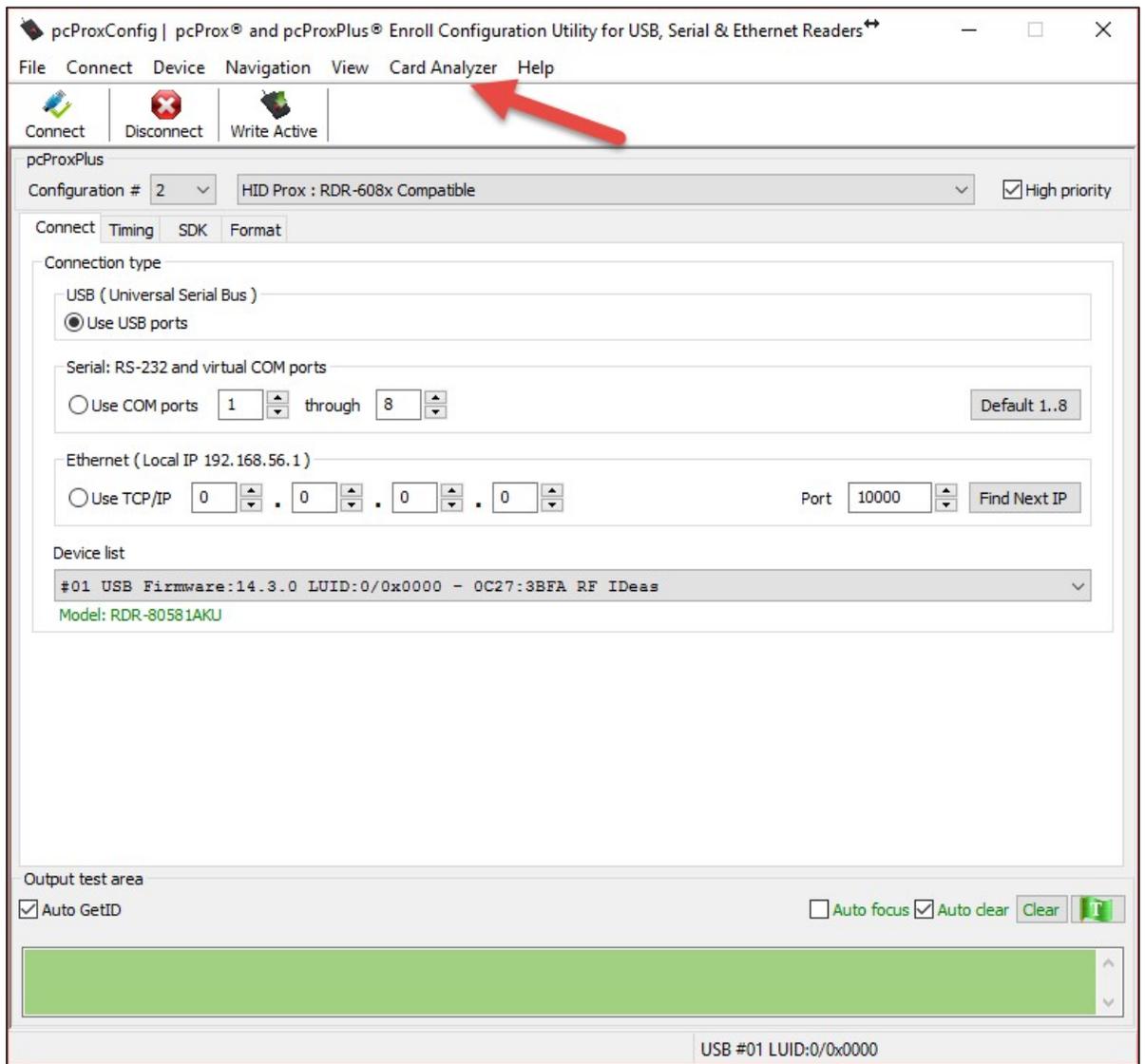
Plug in the pcProx® Plus card reader into an available USB port. Run the program PcProxConfig from the Windows start menu, click **Use USB ports**, and select the **Connect** button in the upper left of the screen to associate the program to the external reader.



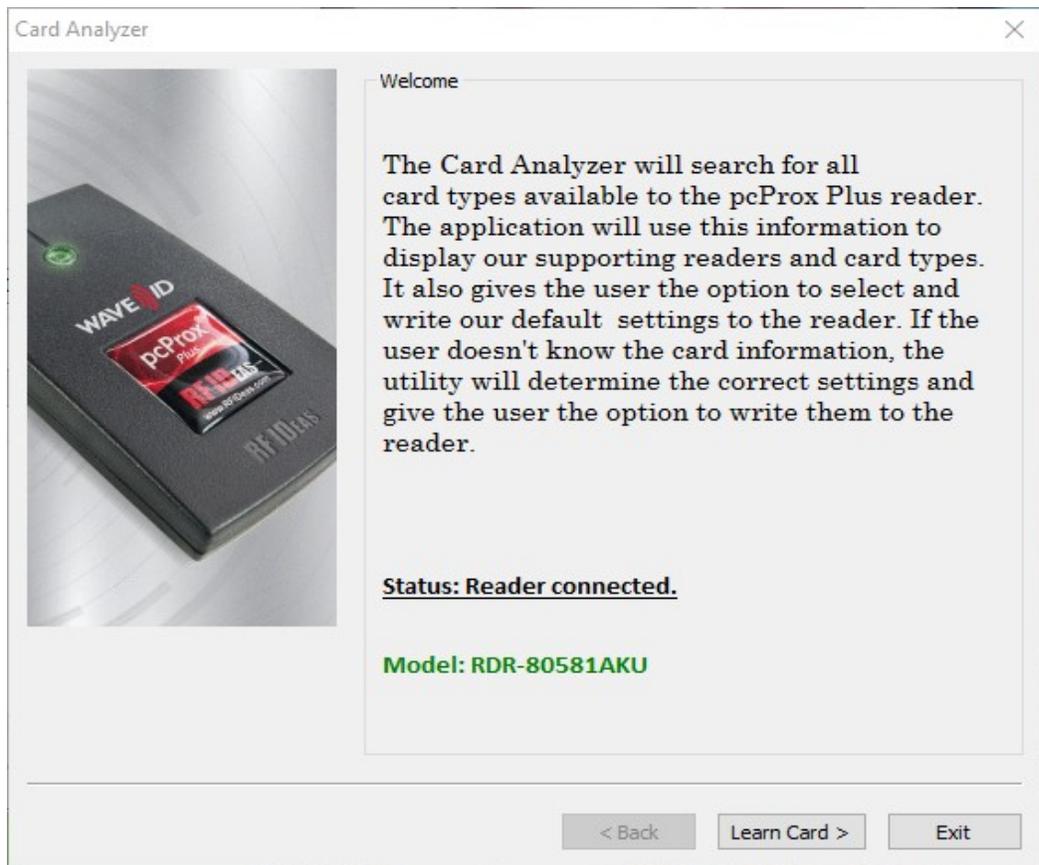
## Determining what Card Profile to use

The pcProx® Plus Card enrollment reader must be tailored to the **RFID Card Type** that will be used with the eConnect EAC 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.

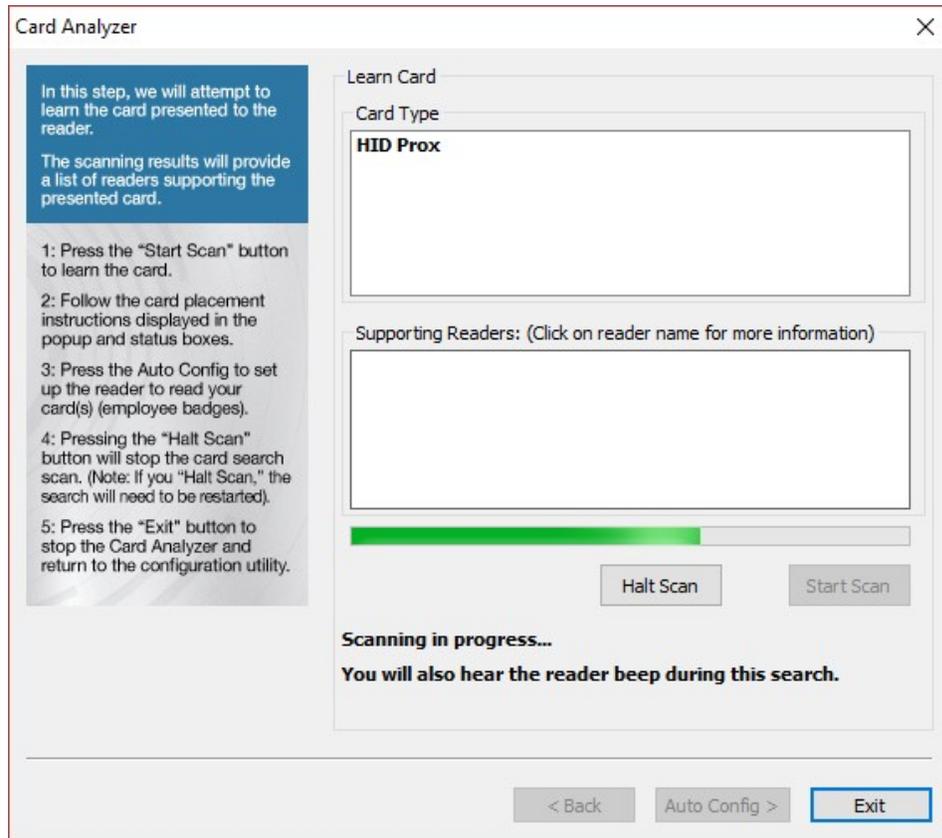
If the RFID card type is not known, the “**Card Analyzer**” Wizard, found under the “Card Analyzer” menu of the pcProxConfig program, can be used to scan for the Card Type:



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

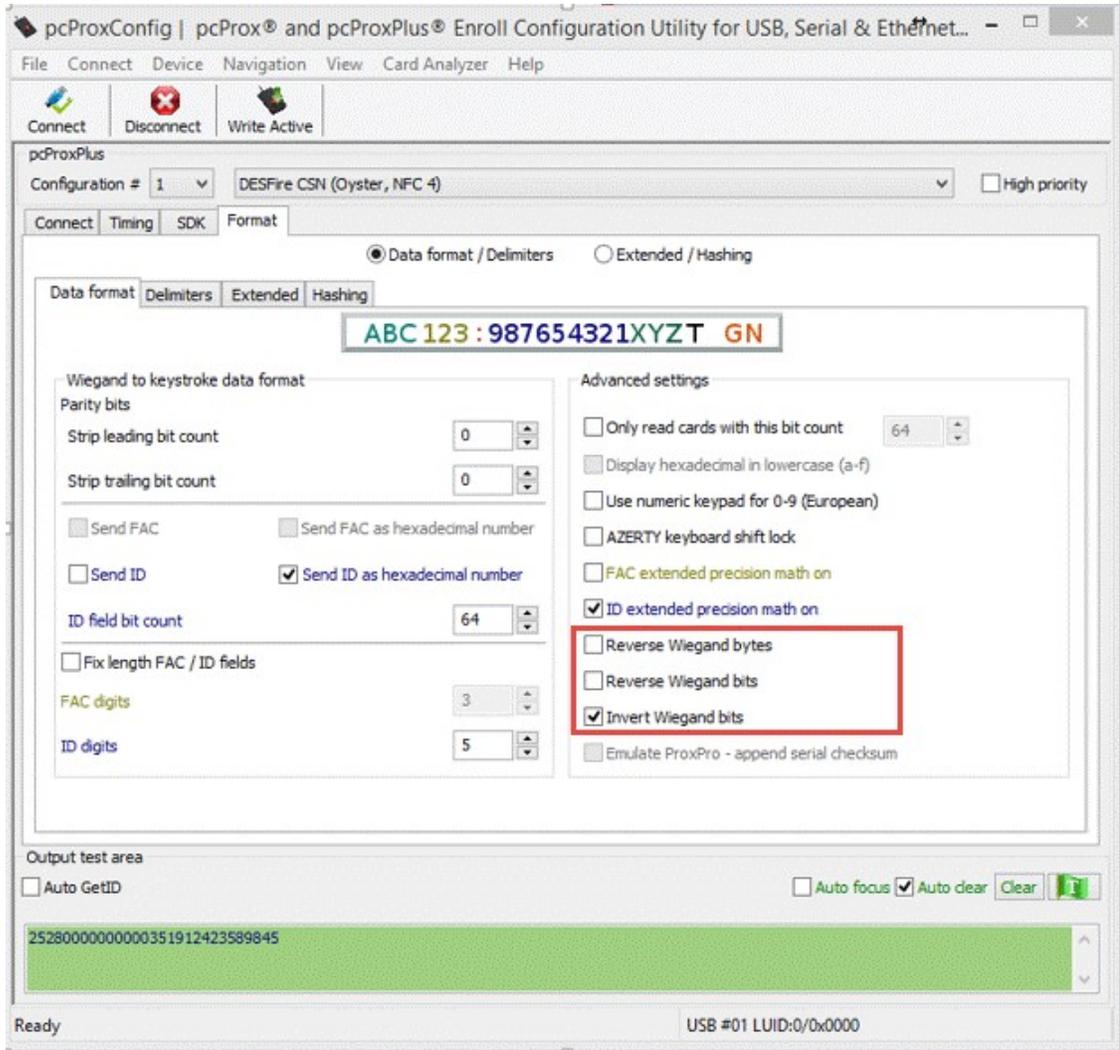
In order for the pcProx® Plus reader to be compatible with the Networked EAC, the card reader must be flashed with the proper reader settings, as shown in the following steps:

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.

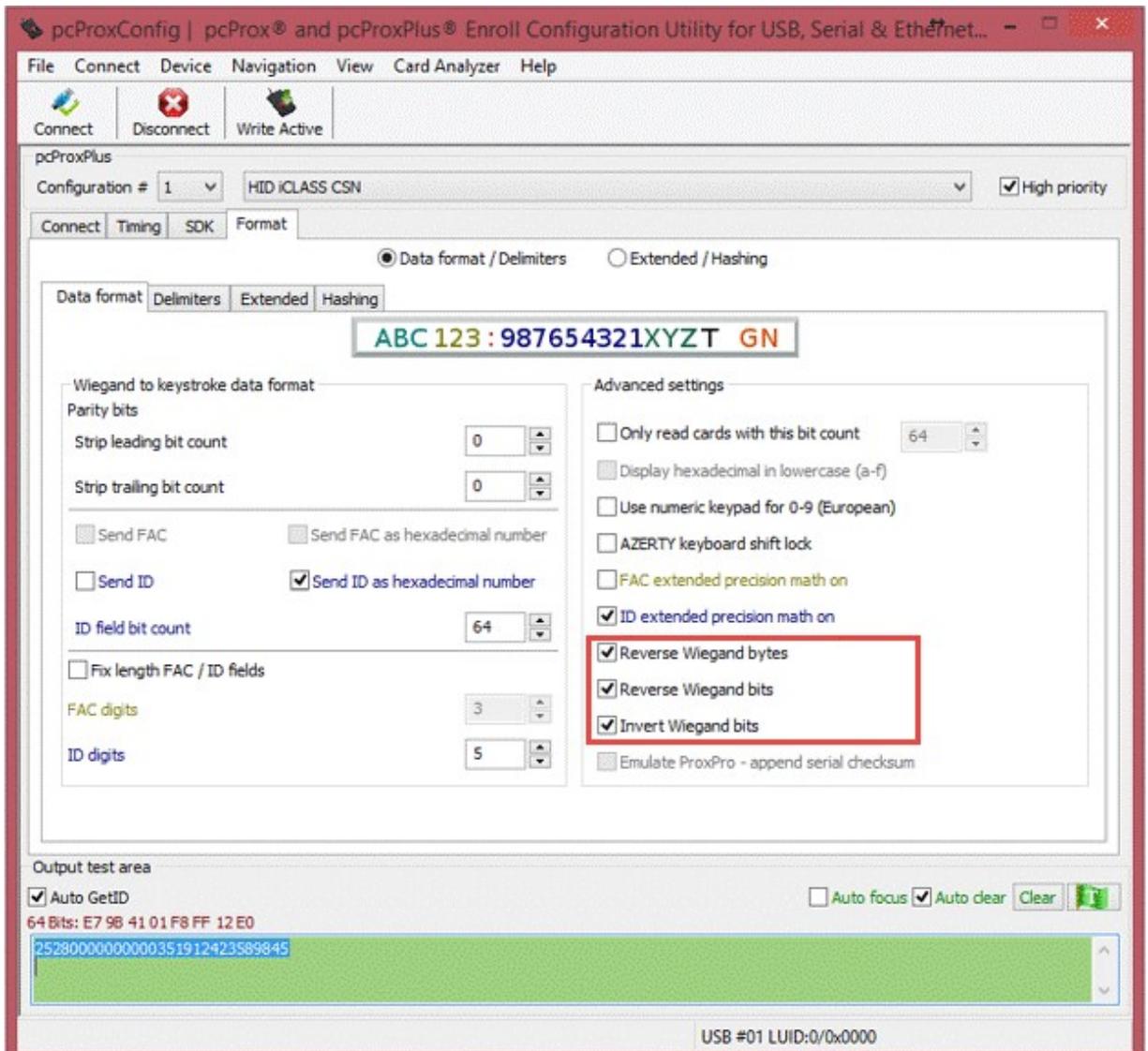
## Programming the pcProx® Plus reader

The screenshot shows the pcProxConfig application window. The title bar reads "pcProxConfig | pcProx® and pcProxPlus® Enroll Configuration Utility for USB, Serial & Ethernet Readers". The menu bar includes "File", "Connect", "Device", "Navigation", "View", "Card Analyzer", and "Help". The toolbar contains "Connect", "Disconnect", and "Write Active" buttons. The main window is titled "pcProxPlus" and shows "Configuration # 2" and "HID Prox : RDR-608x Compatible" selected in a dropdown. A "High priority" checkbox is checked. The "Format" tab is active, with "Data format / Delimiters" selected. The "Data format" section shows "ABC 123 : 987654321XYZT GN" in a preview box. The "Wiegand to keystroke data format" section includes "Parity bits" (Strip leading/trailing bit count: 0), "Send FAC" (unchecked), "Send ID" (unchecked), "ID field bit count" (16), "Fix length FAC / ID fields" (unchecked), "FAC digits" (3), and "ID digits" (5). The "Advanced settings" section includes "Only read cards with this bit count" (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" (checked), "Reverse Wiegand bytes" (unchecked), "Reverse Wiegand bits" (unchecked), "Invert Wiegand bits" (checked), and "Emulate ProxPro - append serial checksum" (unchecked). The "Output test area" has "Auto GetID" checked, "Auto focus" unchecked, "Auto clear" checked, and a "Clear" button. The status bar shows "Ready" and "USB #01 LUID:0/0x0000".

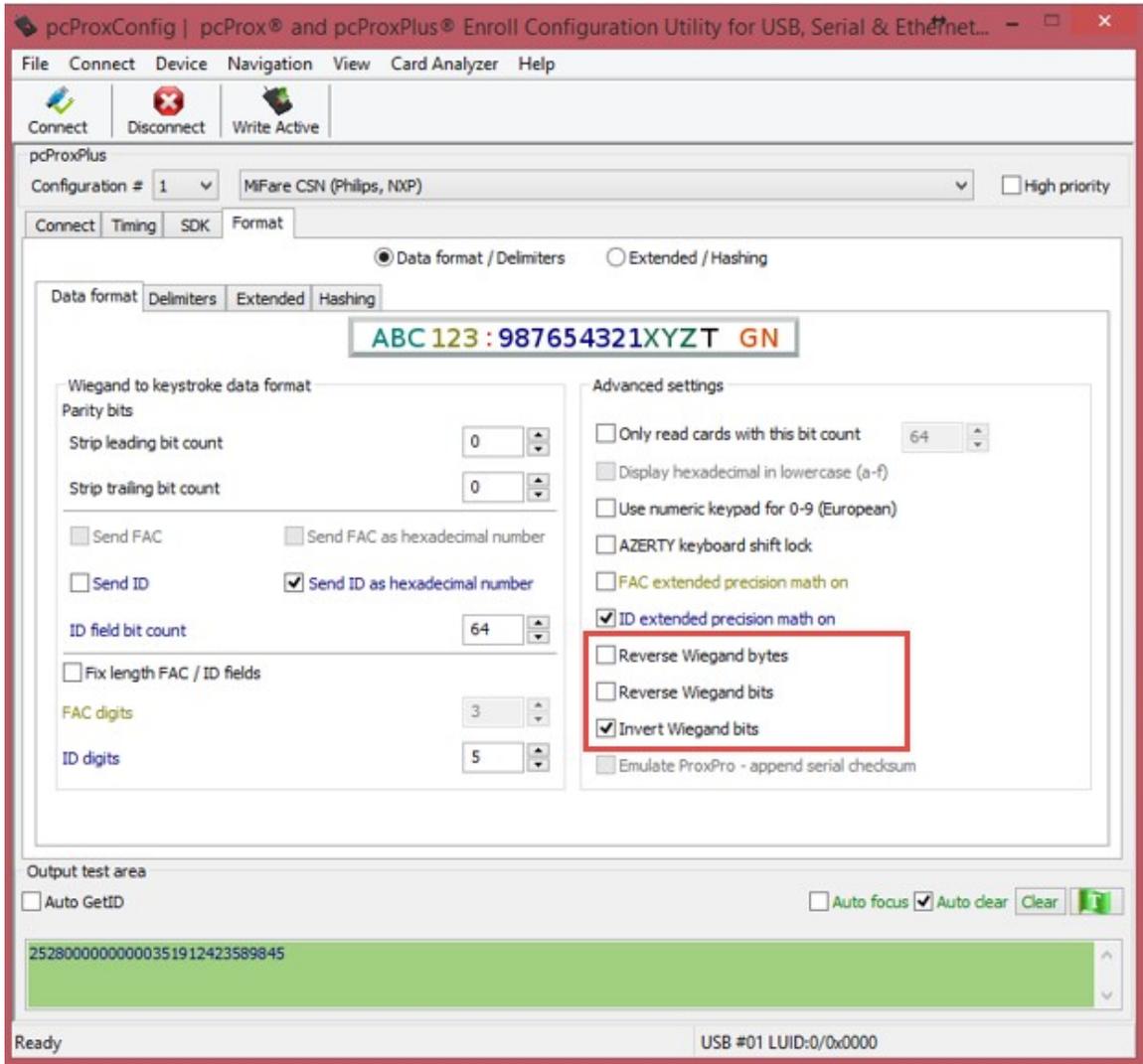
## Common RFID Card Types and Reader Format Settings Desfire Card:



## 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:

