Networked Electronic Access Control User Manual

Version 1.0
October 2017

techsupport@chatsworth.com
www.chatsworth.com

Table of Contents

INTRODUCTION – User Manual for Networked Electronic Access Control

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

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

FC ICES-003 Class A "I.T.E." Tested to Comply With FCC Standards	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.
c UL us LISTED	Samples of this product met UL's safety requirements for US and Canada.
	Do not dispose this product as unsorted municipal waste.

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:

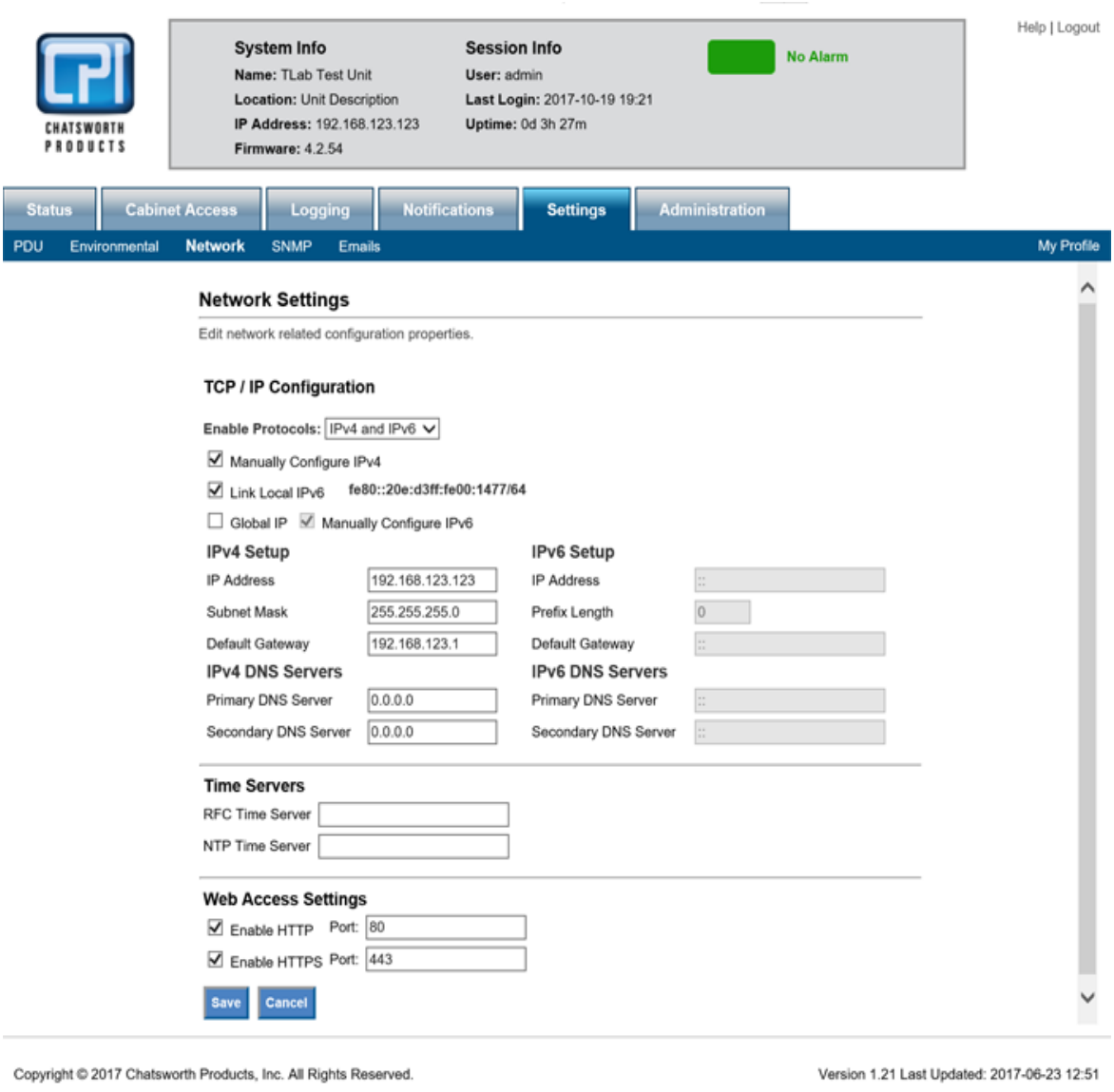
Log in using default User name and password: **admin**, **admin** and **click on Login** button or user name and password if it has been created.

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.**

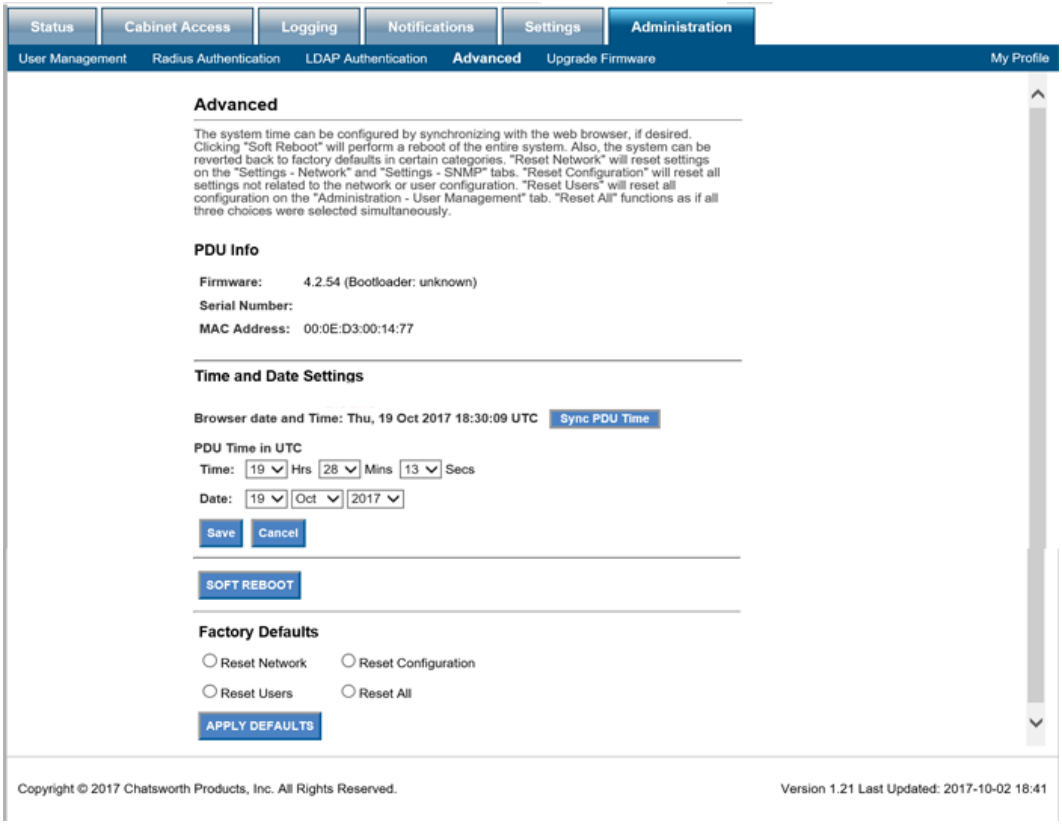
Network Settings



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.

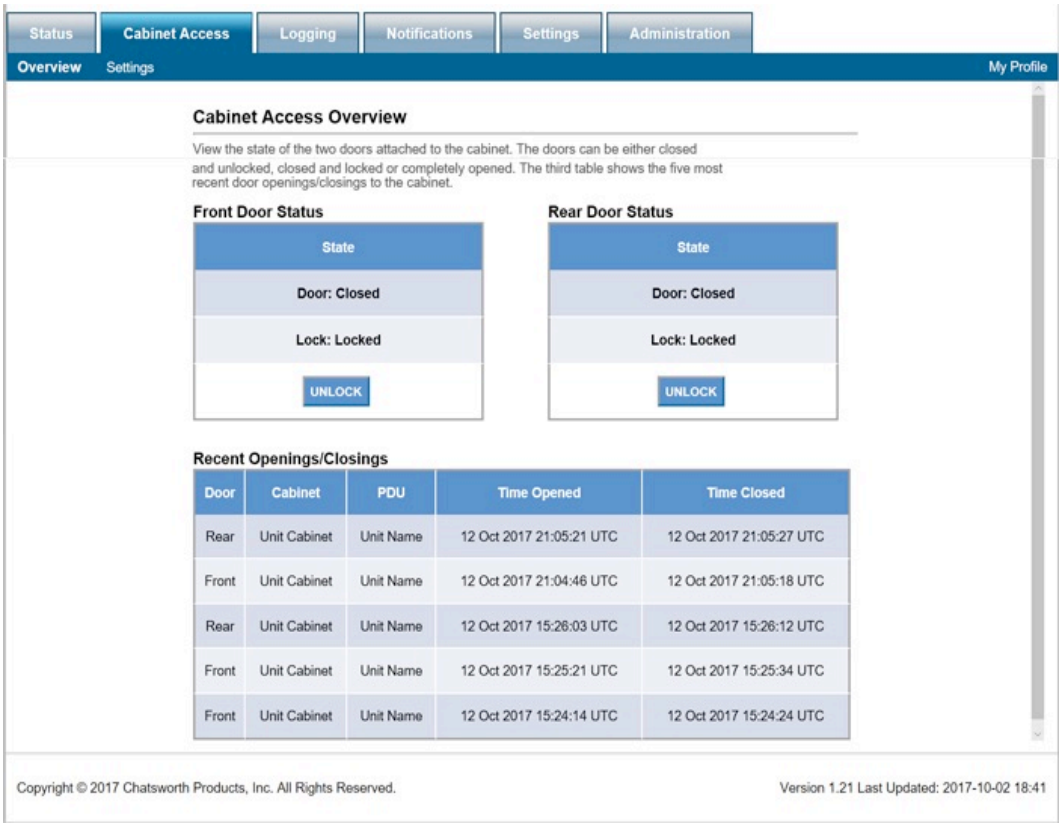
Status – Alarms

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

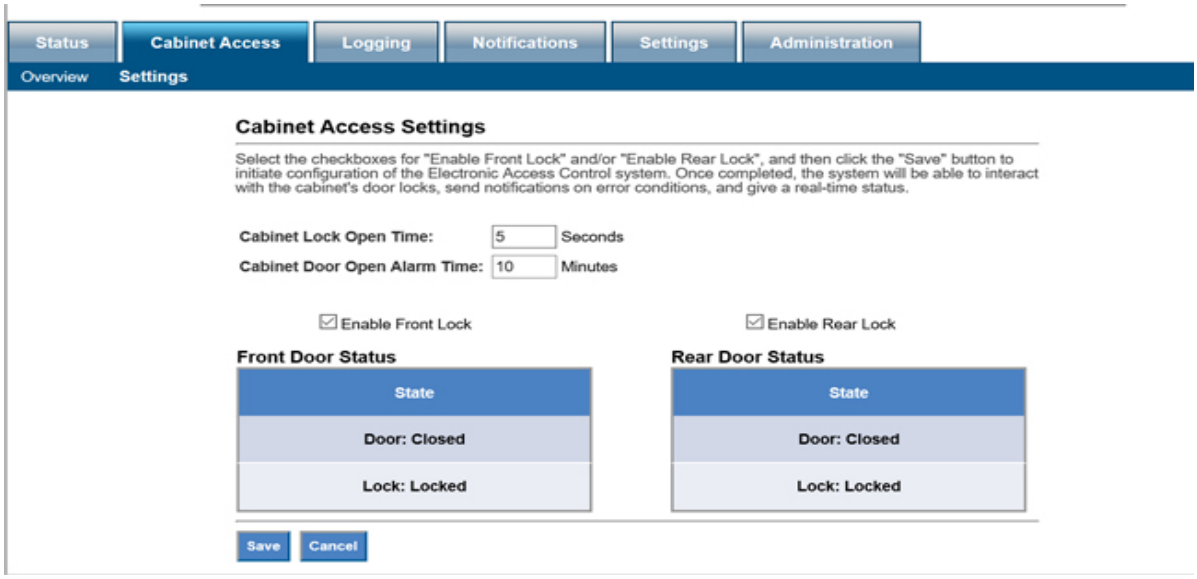
Warning thresholds are indicated by a yellow-colored rectangular alarm status symbol. Critical thresholds are indicated by a red-colored rectangular alarm status symbol.

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



Cabinet Access – Settings

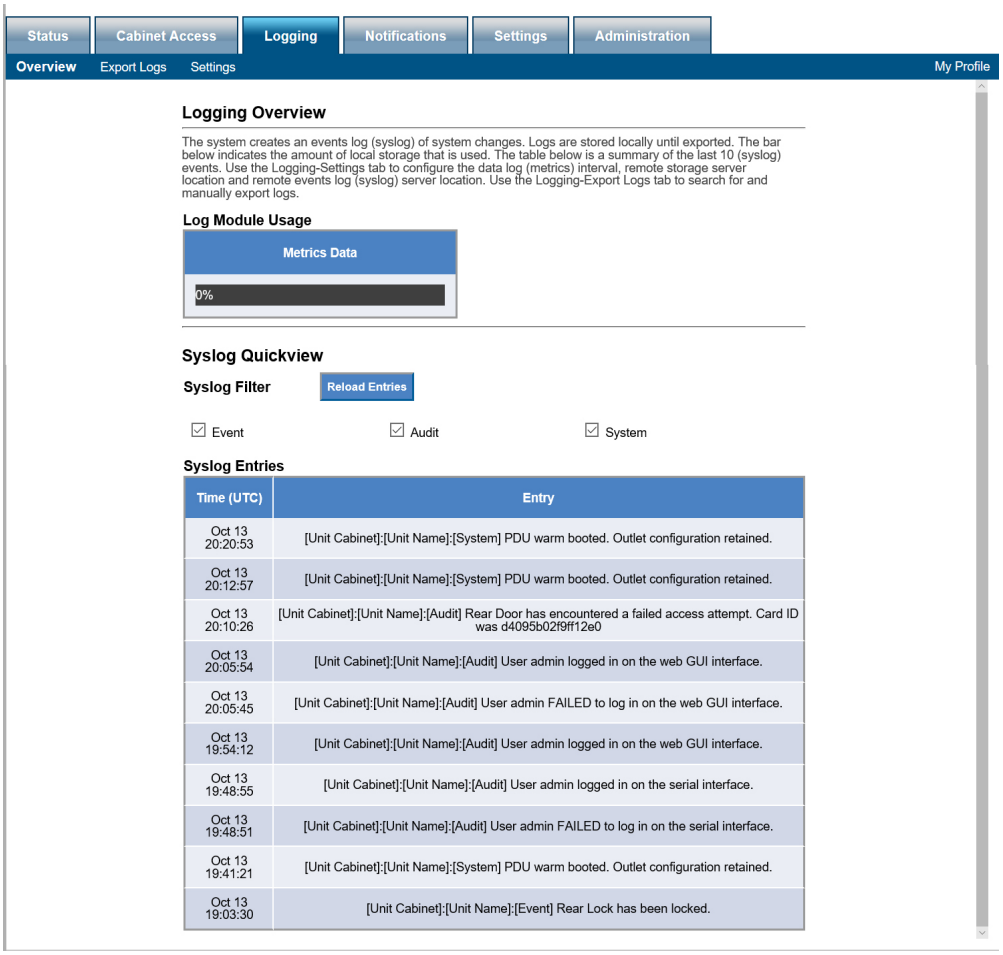


Enter the **Cabinet Lock Open Time**: 1 – 30 seconds. The default value is 5 seconds

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

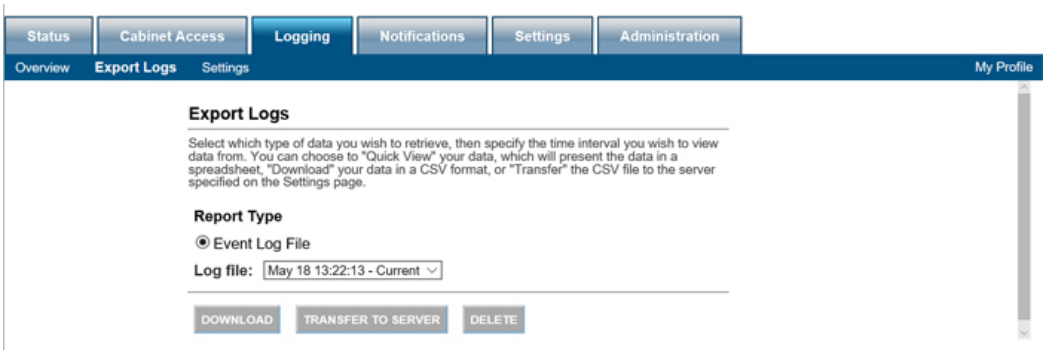
Check box to enable Front or/and Rear Lock(s) where applicable.
Click on **Save** to save the configured data.

Logging - Overview



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

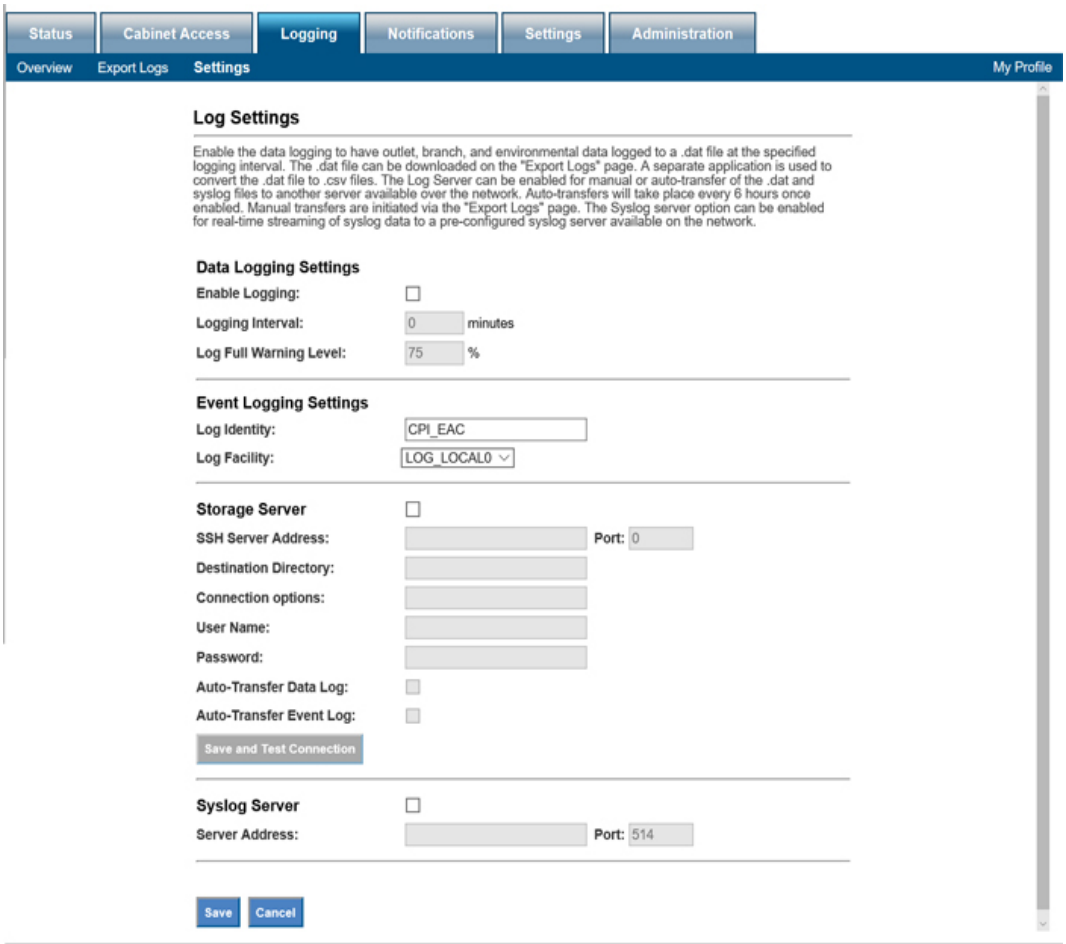
Logging – Export Logs



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



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.

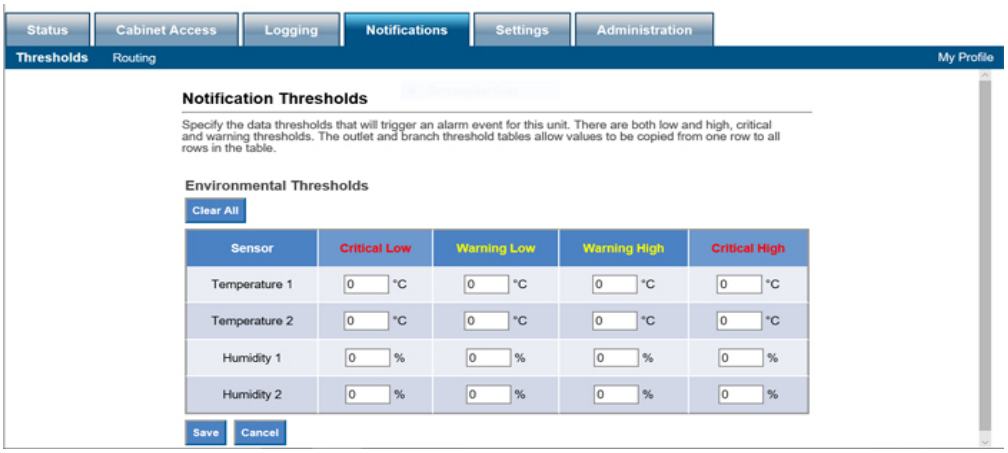
Event Logging Settings:
Log Identity and Log Facilities are preset on the device's memory system. Pick any Log Local to store data locally.

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



Environmental Thresholds

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

Notification - Routing

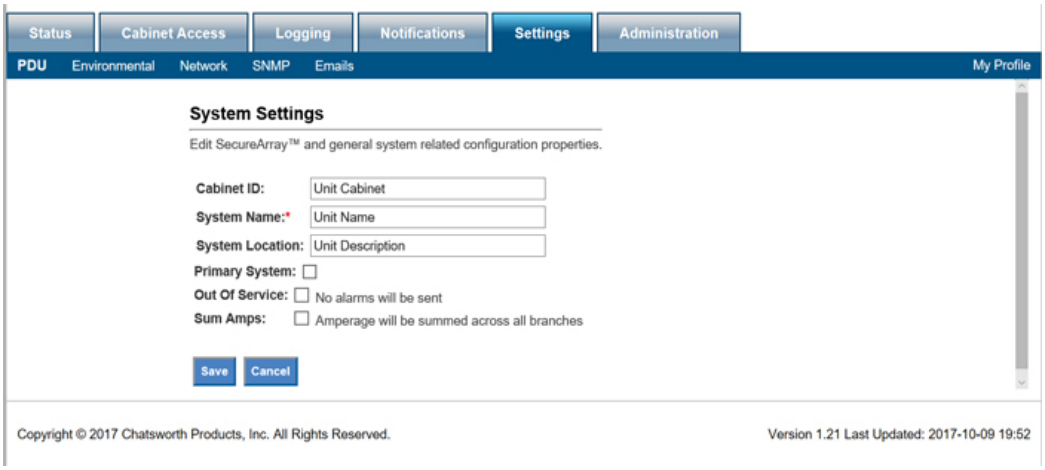
Select method(s) of notifications for Temperature, Humidity if applicable by checking the check box(es): Log, Trap, Email.

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



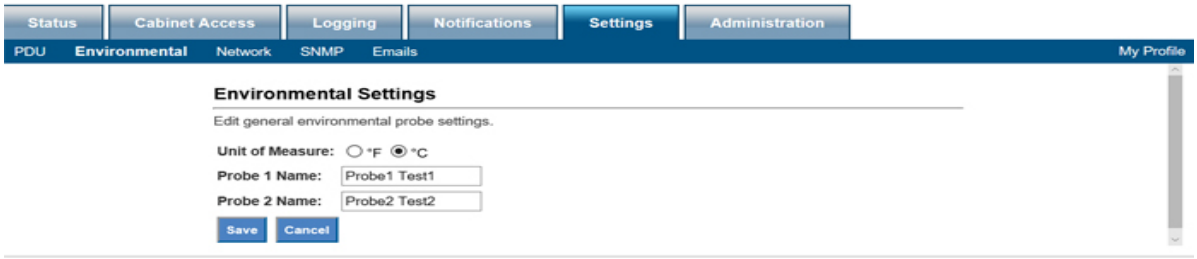
Enter desired **Device Name** and **Location**.

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.

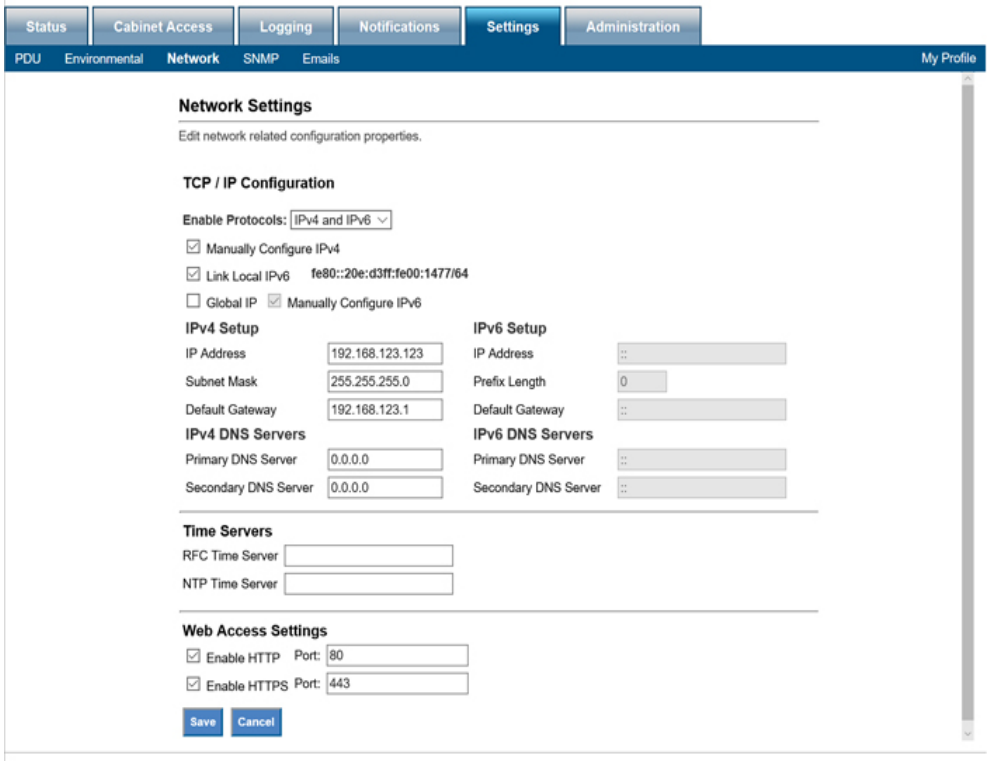
Fill in the desired choices and click on **Save**.

Settings - Environmental



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

Settings – Network



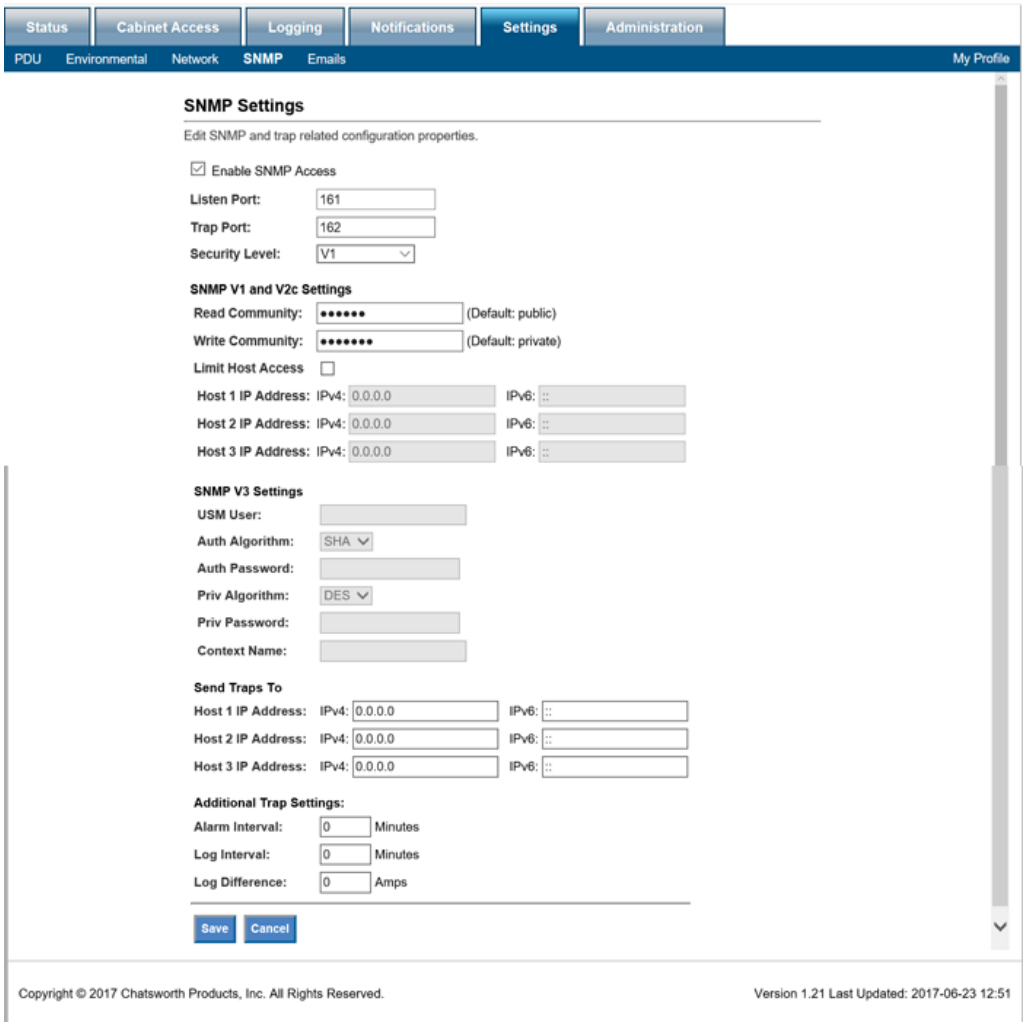
• **Network** - Using the Enable Protocols combo box, select the Network Protocol(s). Enter data for IPv4 and/or IPv6 Networking.

• **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**.

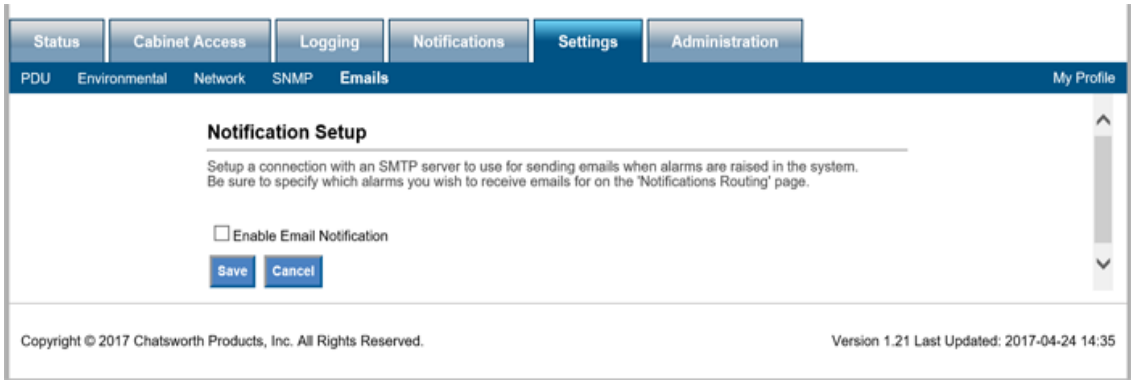
Settings – SNMP



Enter data for SNMP v1, v2c or v3 settings.
Enter the IP Addresses you want to send traps to.

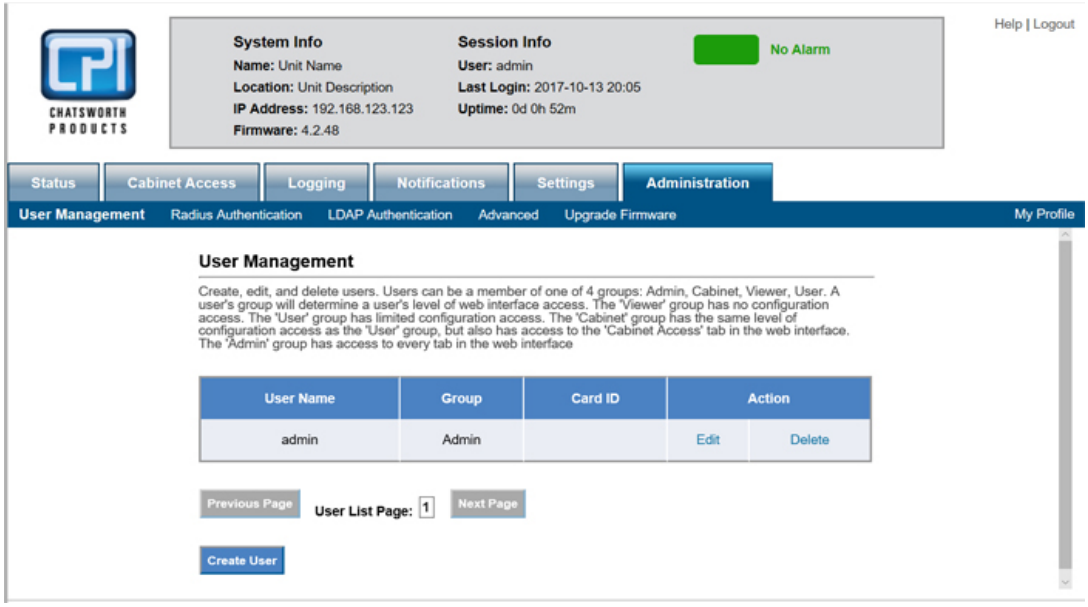
Click on **Save** to save all entered data.

Settings – Emails

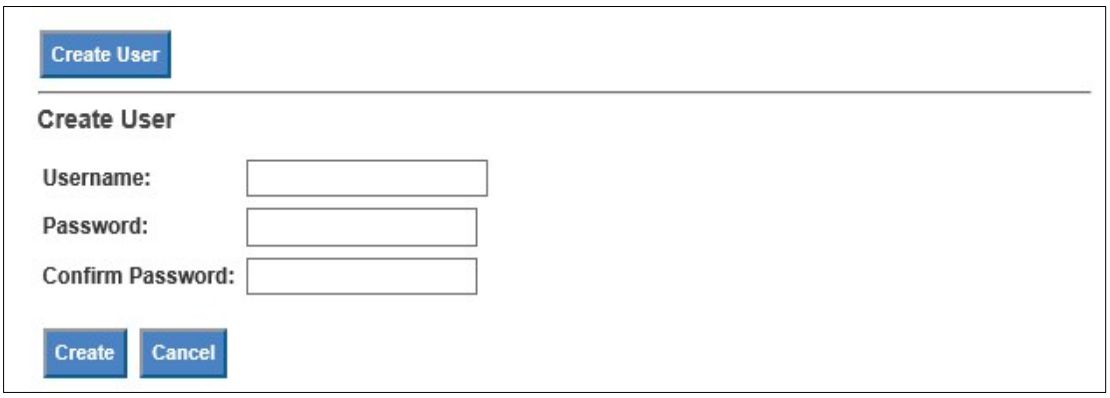


The device does not include a mail server. In order to provide email notifications for the device, you must first setup an email account for the device on an accessible mail server.

Administration – User Management



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.

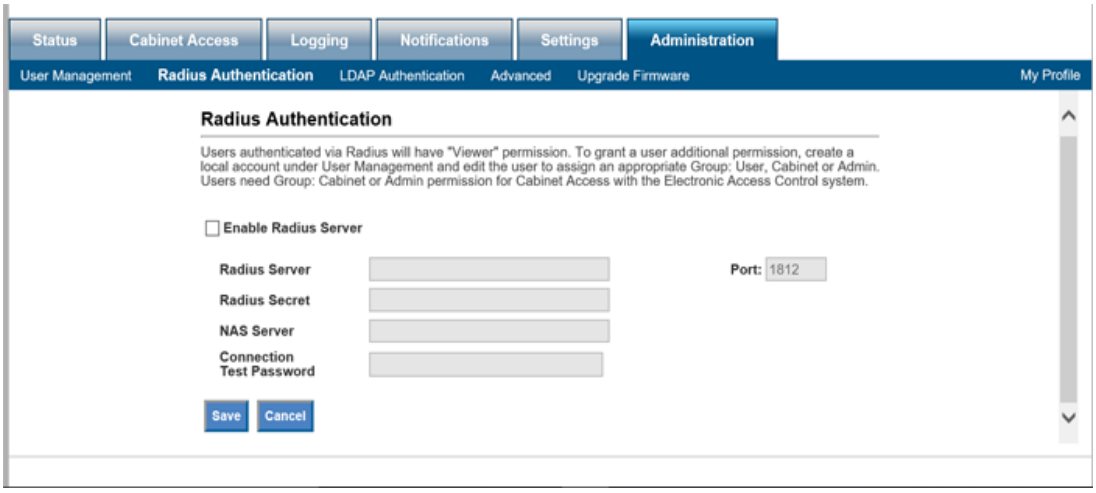
Change the necessary information. Input the Key Card ID for the Electronic Access Control. If you don't know your Key Card ID, see Appendix.

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.

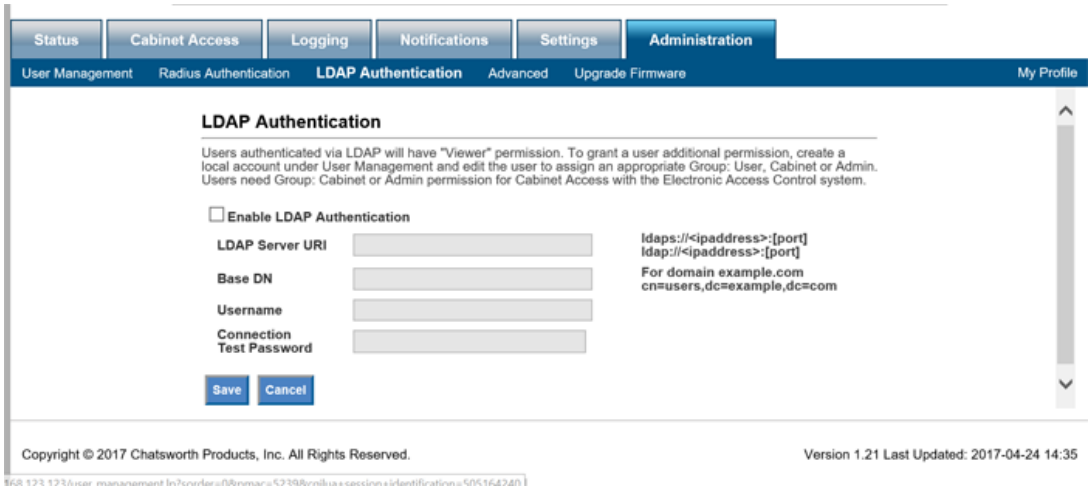
Click on **Save**.

Administration – Radius Authentication



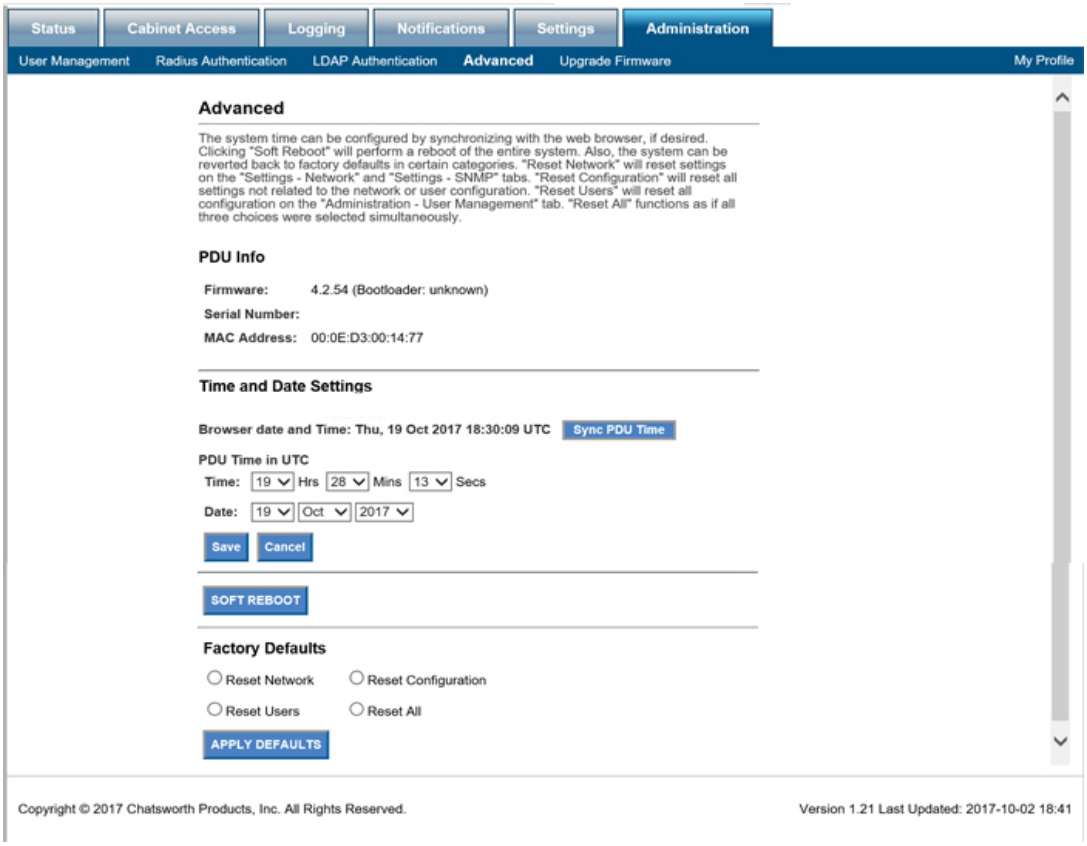
For network/website authentication using **Radius Authentication**, enter the necessary information and **Save**. Note that users will need to be added under the **Local User List** to have **Control** or **Admin** capabilities.

Administration – LDAP Authentication



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.

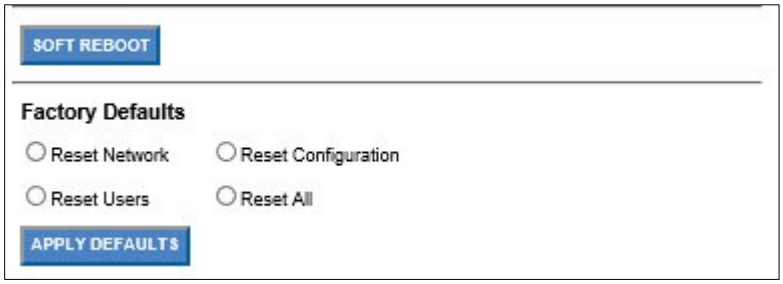
Administration – Advanced



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.

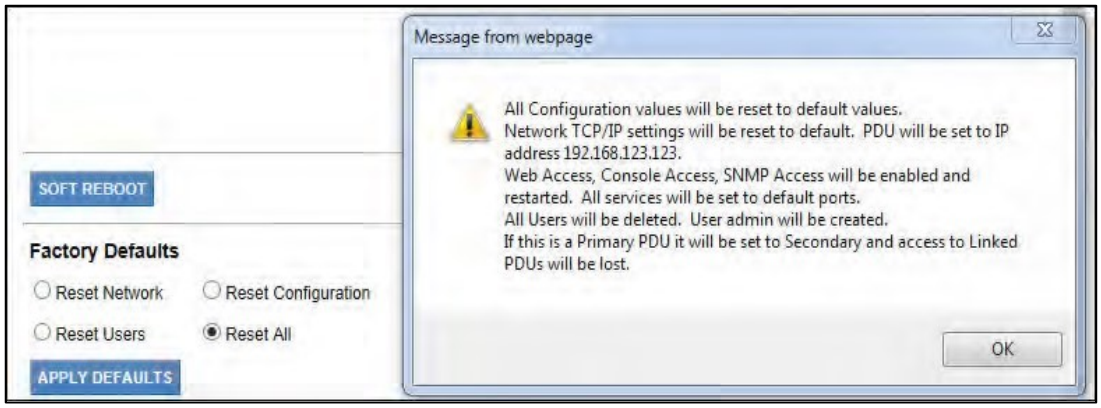
Verify the **Time** and **Date Settings** to ensure date/time stamps on logs and alarms are correct.

Soft reboot restarts the network connection
Use this if you have connection problems.



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.

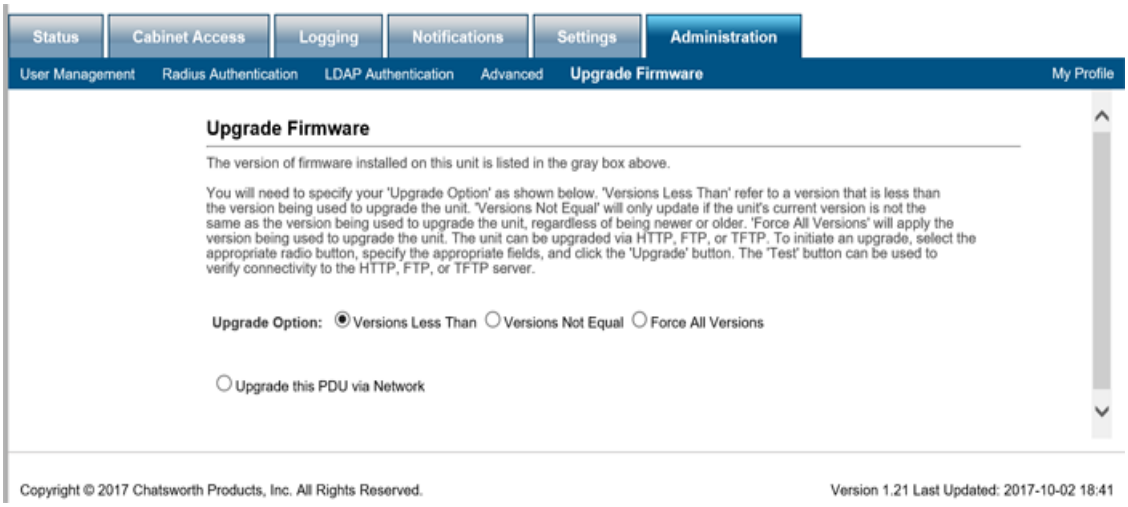


To reset to factory defaults, select the appropriate radial button. Review the warning message.

Click the **Apply Defaults** button to apply selected defaults.

Resets are applied immediately.

Administration – Firmware Upgrade



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.

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.

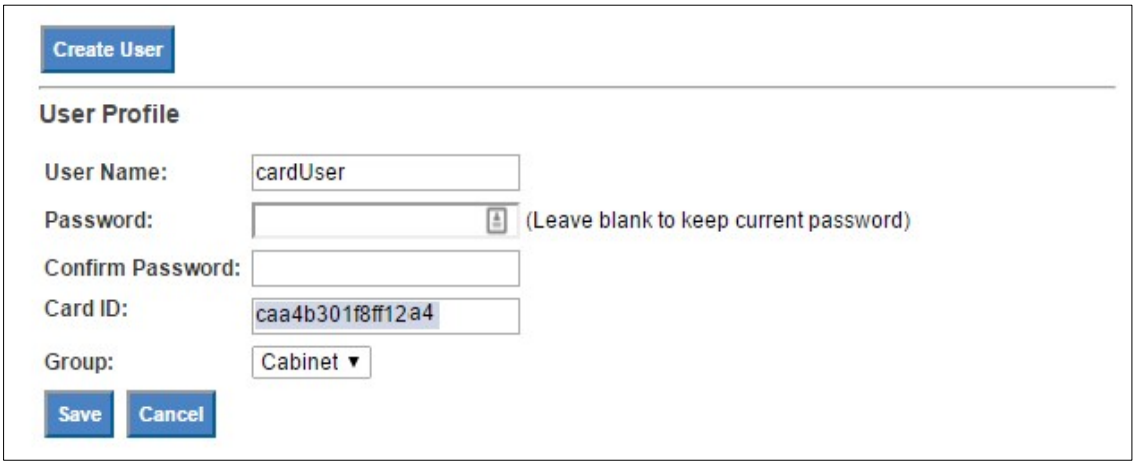
To easily copy the card ID from the syslog, double click the last set of characters on the pertinent log entry with the left mouse button to highlight it, then click the right mouse button and select **Copy** (or press **Ctrl-C** on the computer keyboard) to copy the characters to the windows clipboard.

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 caa4b301f8ff12a4

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 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.

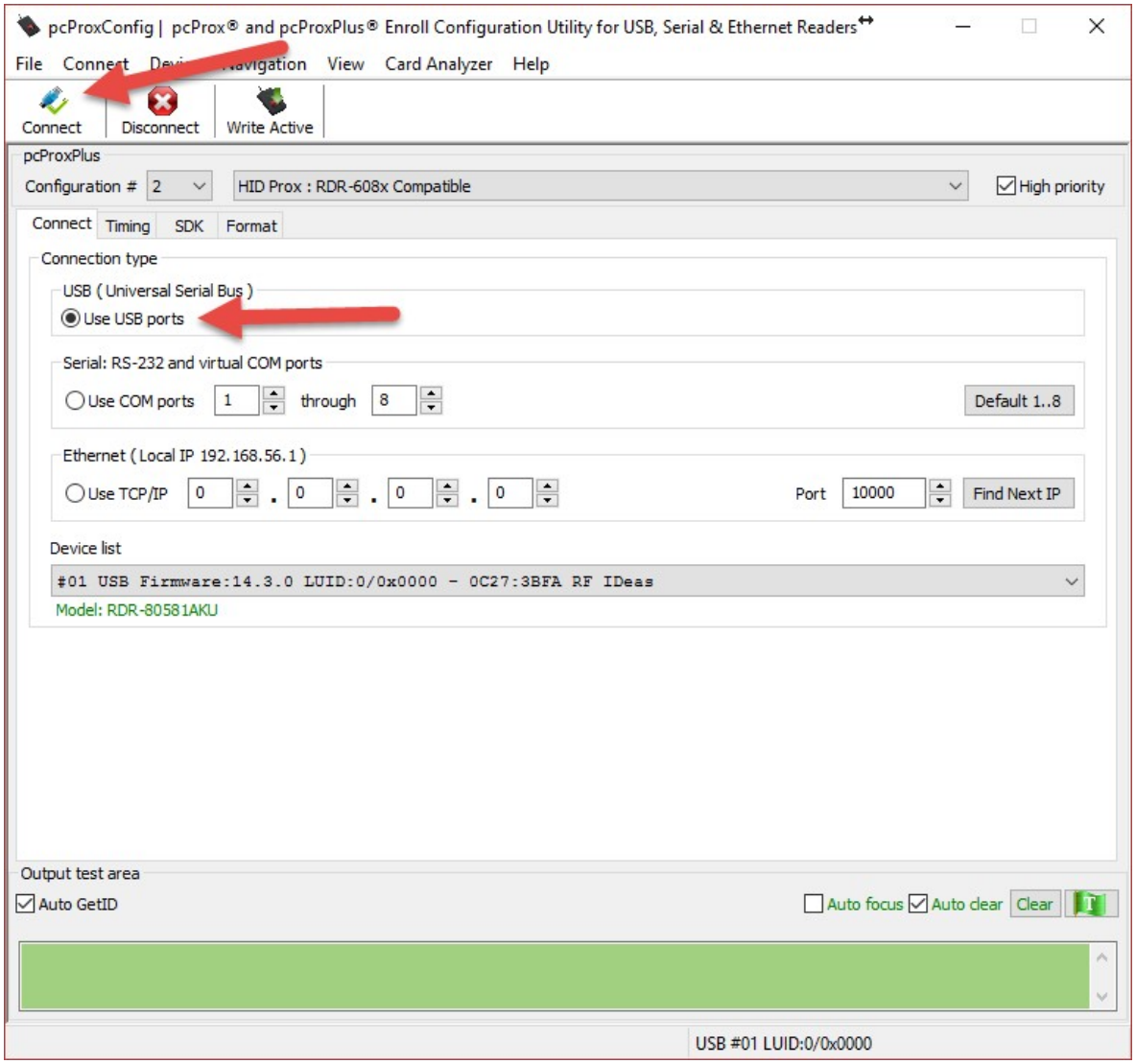
Configuring the pcPROX Plus Reader

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

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**

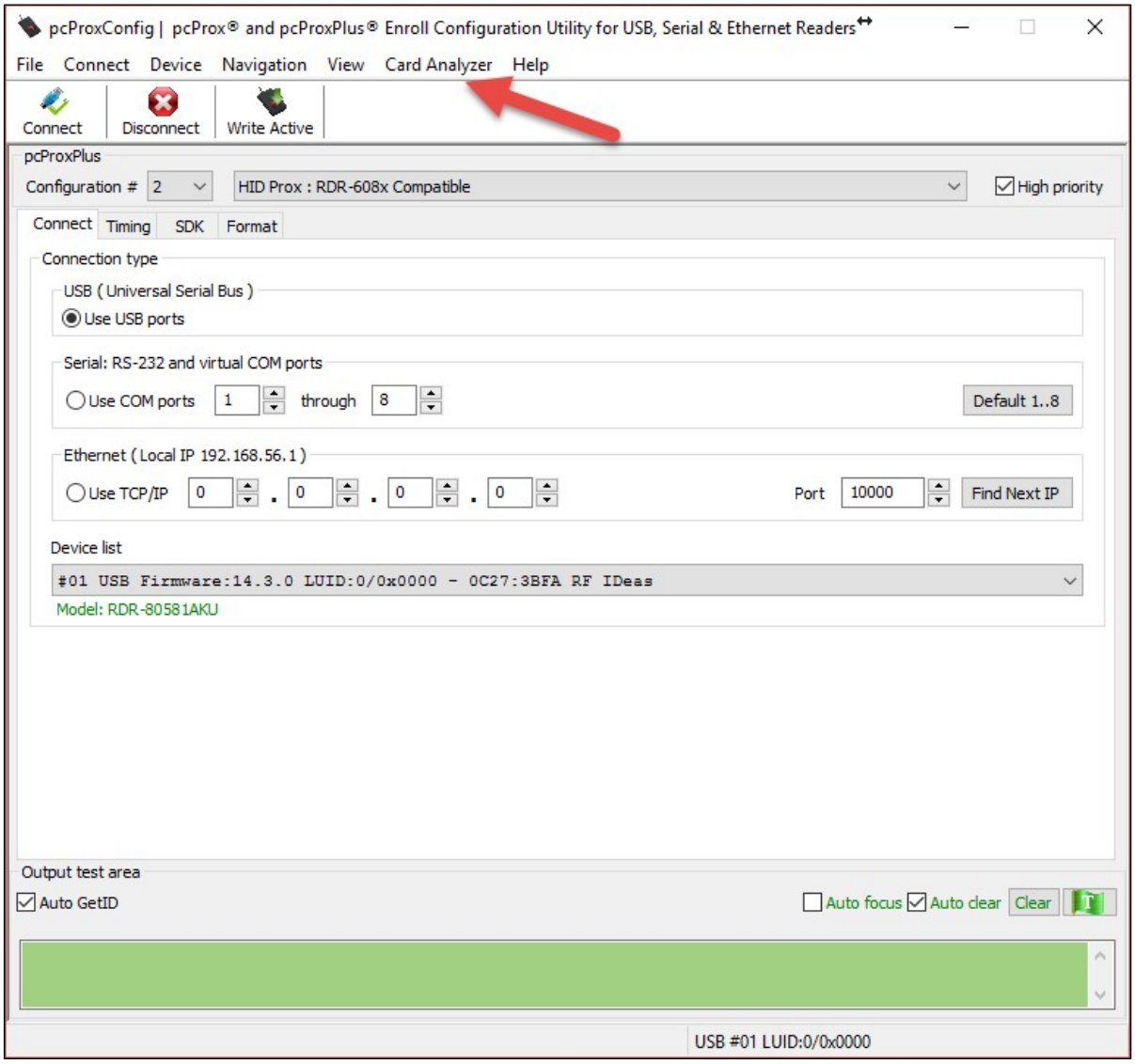
Plug in the pcProx® Plus card reader into an available USB port**.** Run the program PcProxConfig from the Windows start menu, click **Use USB ports,** and select the **Connect** button in the upper left of the screen to associate the program to the external reader.



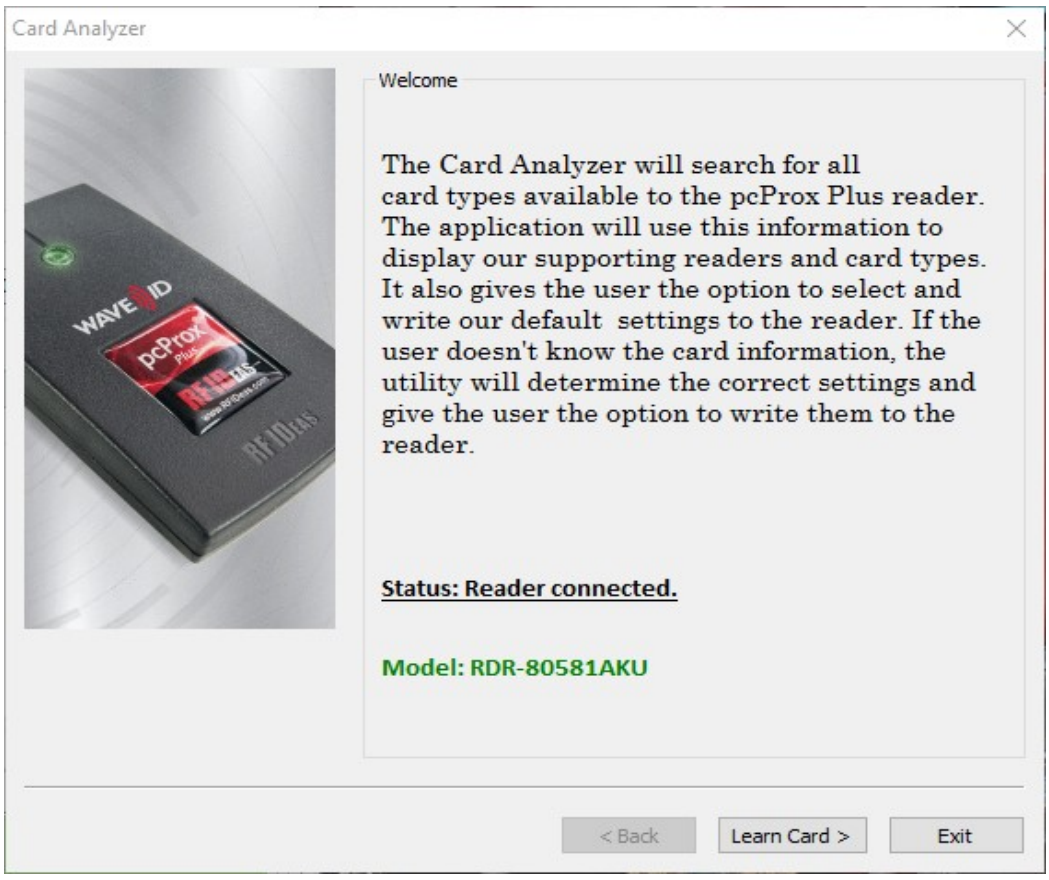
Determining what Card Profile to use

The pcProx® Plus Card enrollment reader must 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.

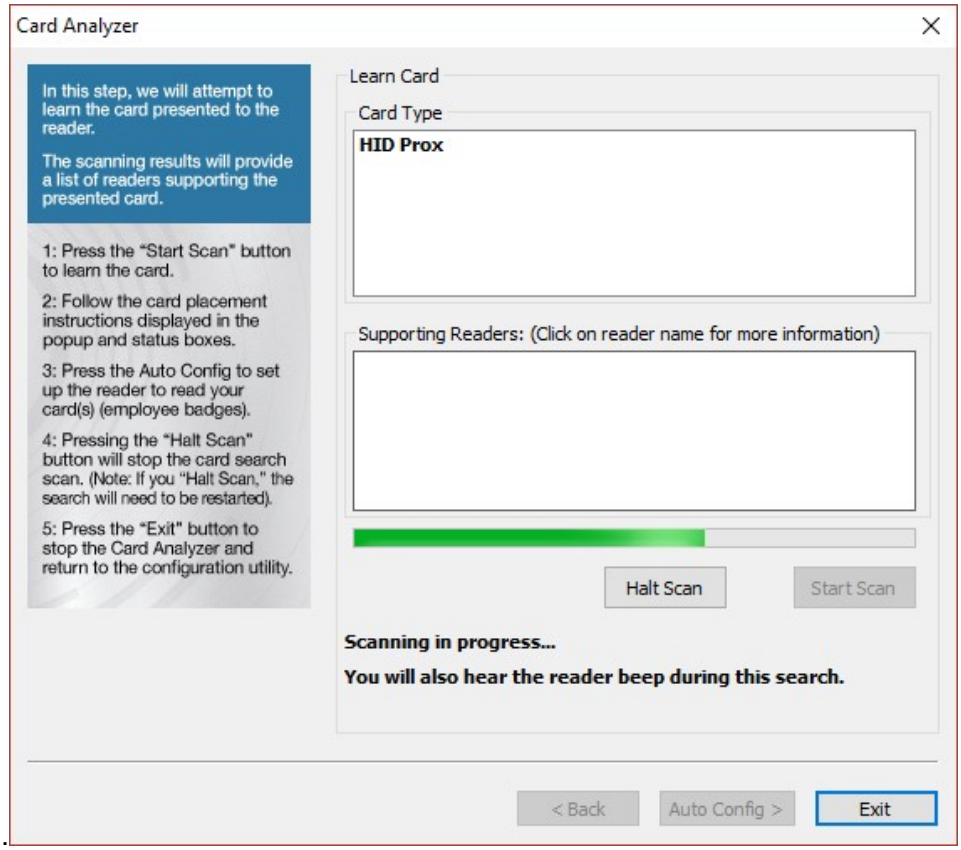
If the RFID card type is not known, the "**Card Analyzer**" Wizard, found under the "Card Analyzer" menu of the pcProxConfig program, can be used to scan for the Card Type:



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.



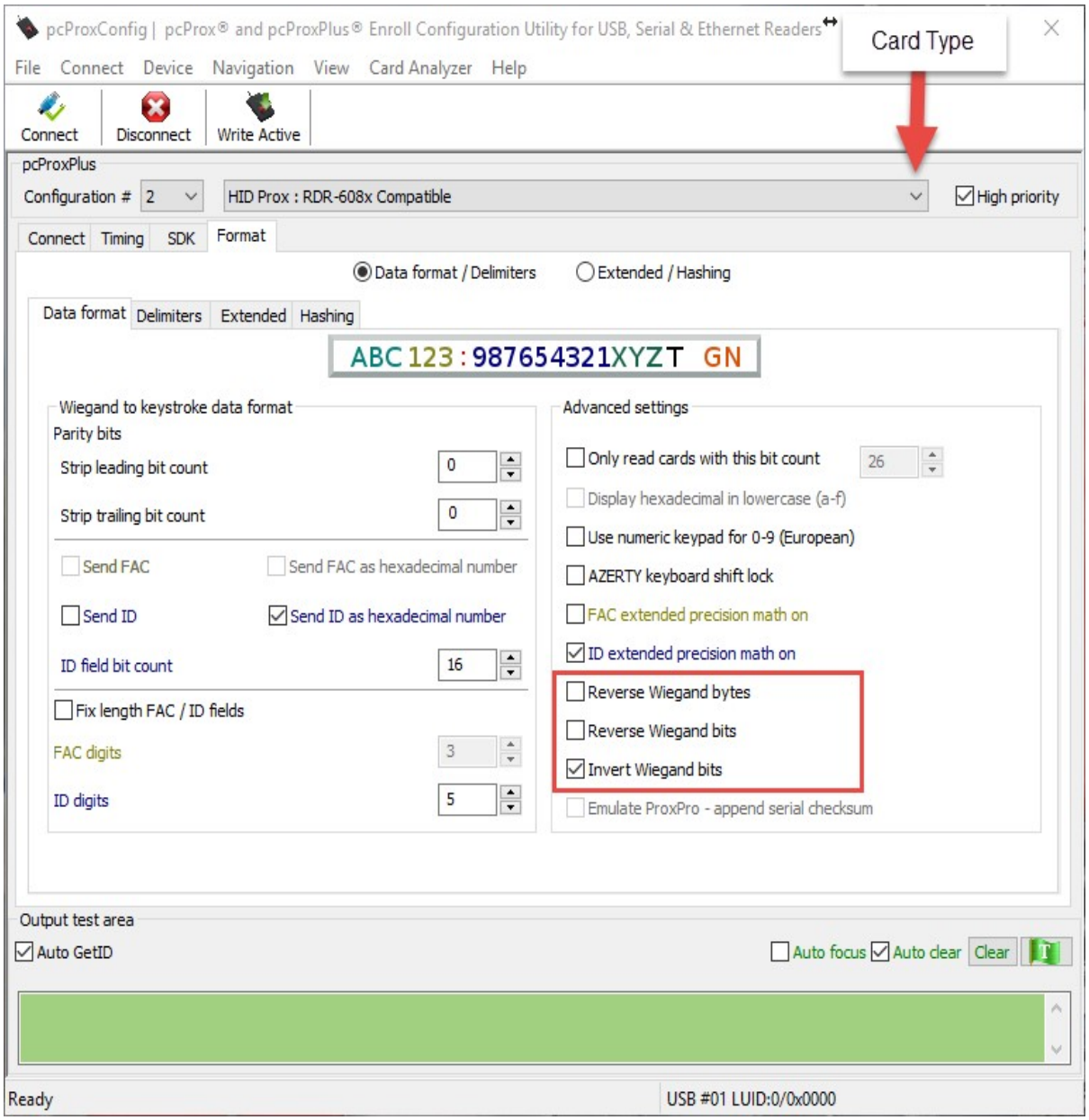
After determining the type, the user is ready to write the proper settings to the pcProx® Plus reader.

Programming the pcProx® Plus reader

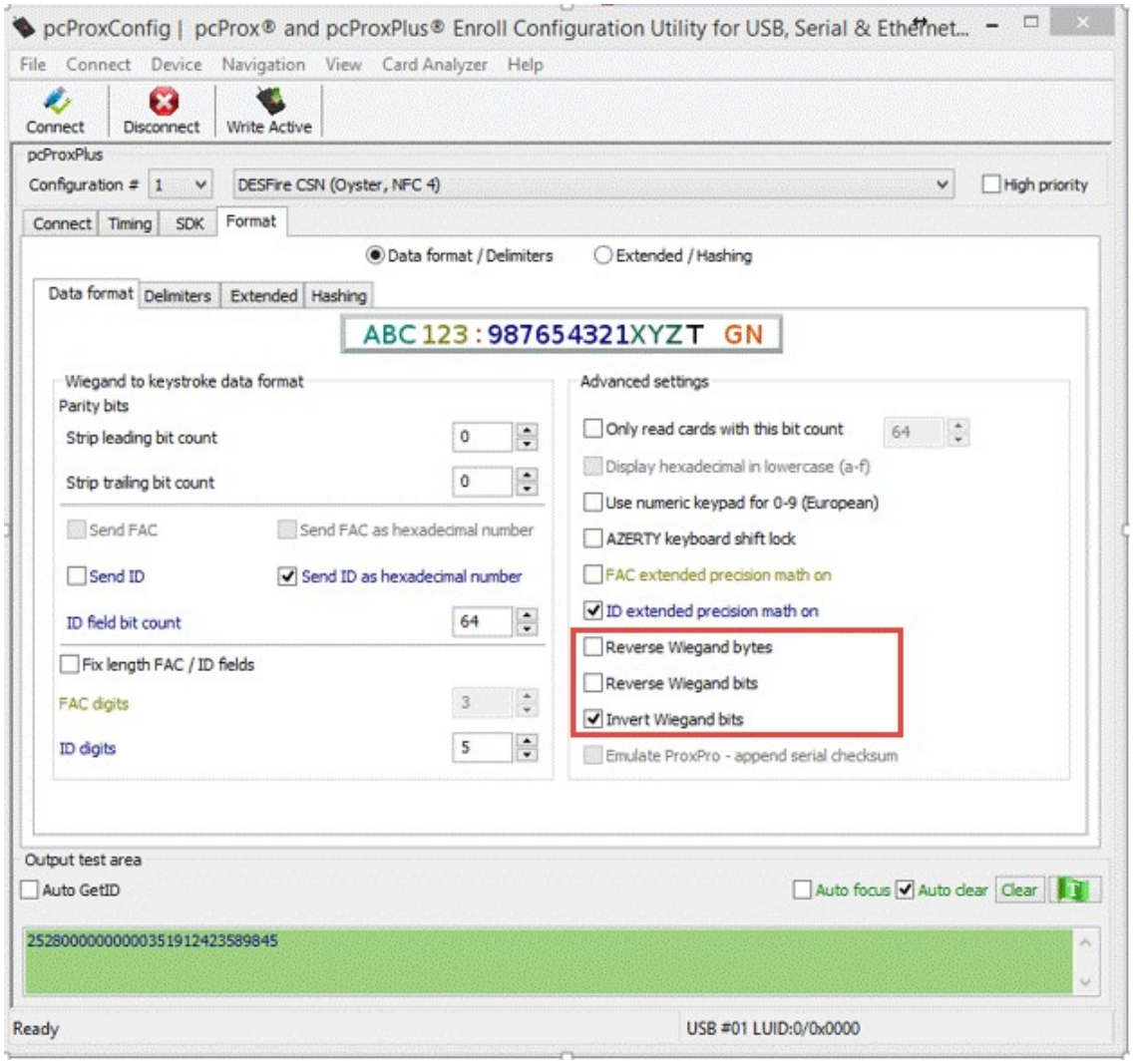
In order for the pcProx® Plus reader to be compatible with the Networked EAC, the card reader must be flashed with the proper reader settings, as shown in the following steps:

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.

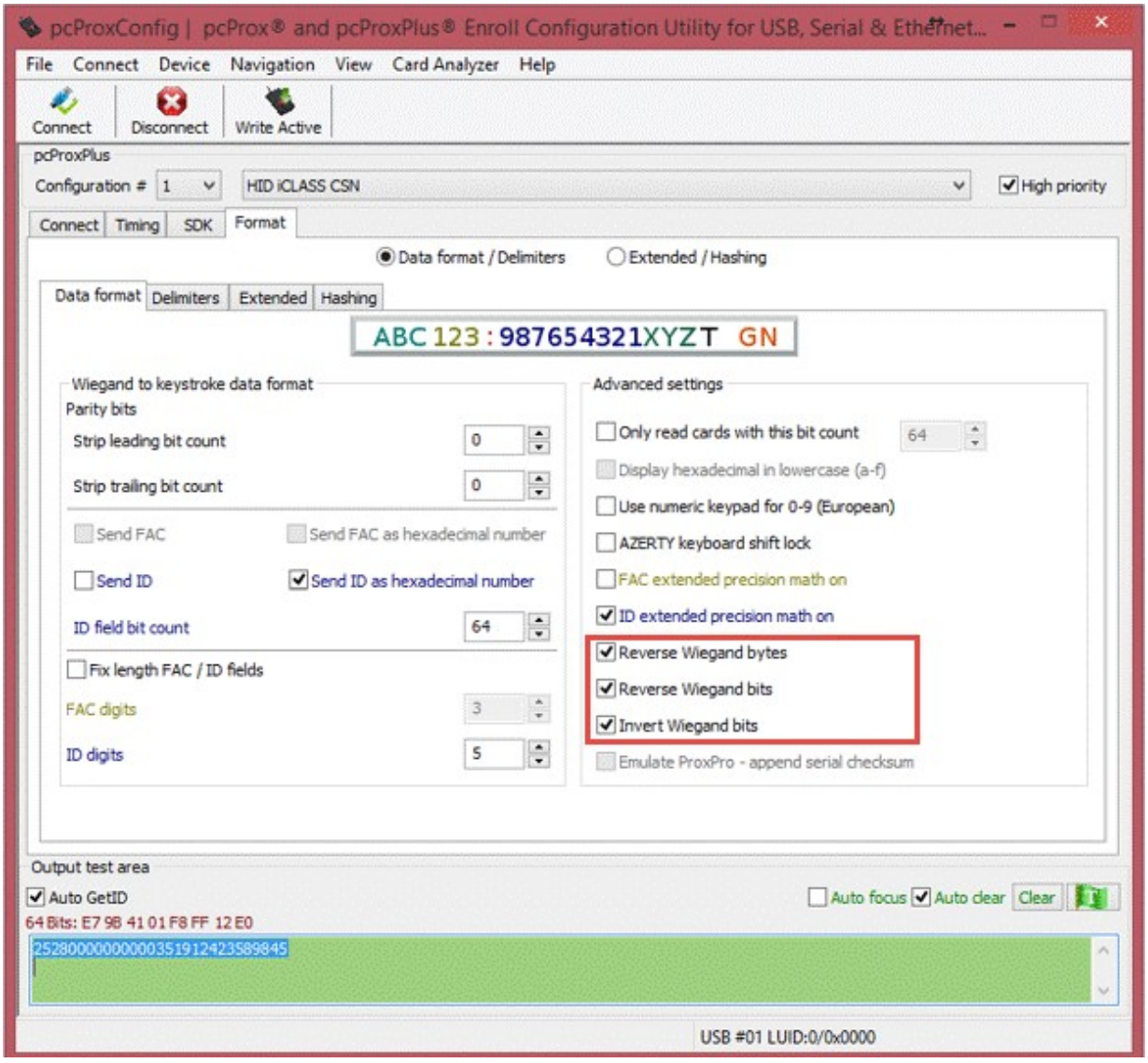
Programming the pcProx® Plus reader



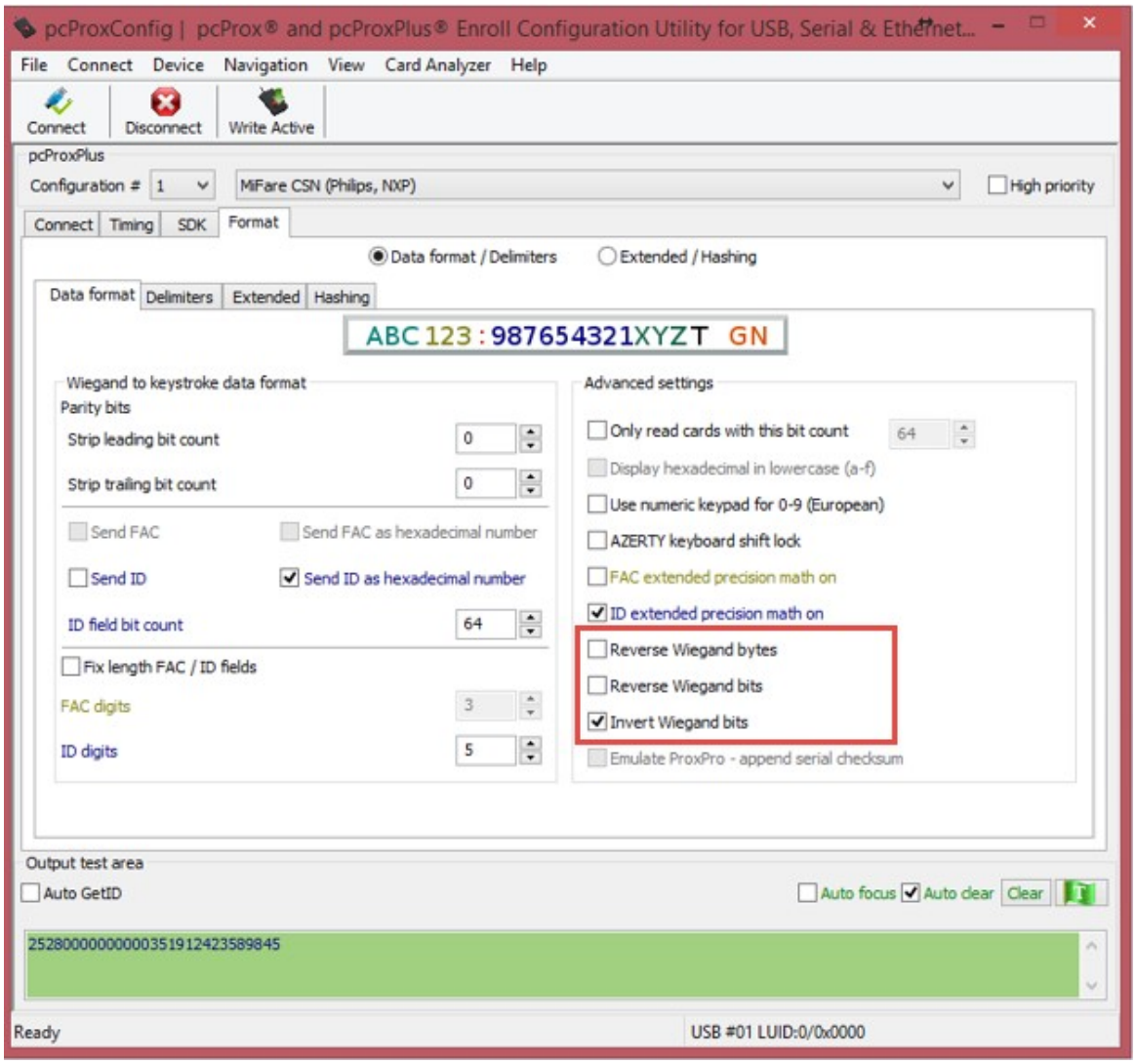
Common RFID Card Types and Reader Format Settings Desfire Card:



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: