



Bulk Configuration Tool

User Manual

Release 2

Issue 1

Copyright © 2019 Panduit Corp. All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from Panduit. No patent liability is assumed with respect to the use of the information contained herein.

Although every precaution has been taken in the preparation of this book, Panduit assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Table of Contents

Table of Contents	3
Introduction	4
Install	5
Uninstall	6
Using the BCT	7
Select SKU type	8
Create a New Conf.ini File	9
Select SKU Number	9
User Account Settings	9
PDU Settings	15
Device Configuration Settings	29
Power Settings	32
Save As	36
Updating the PDU	37
PDU Accessory Setup	39
Help	44

Introduction

BCT tool can be used to create, deploy, and update the configuration file of SmartZone G5 PDUs. It makes the task of commissioning or updating your installed base of units fast and simple. BCT can also be used as a quick and convenient tool for updating the firmware in the units.

This is Version 2 Release 1 of the Bulk Configuration Tool User Manual.

Install

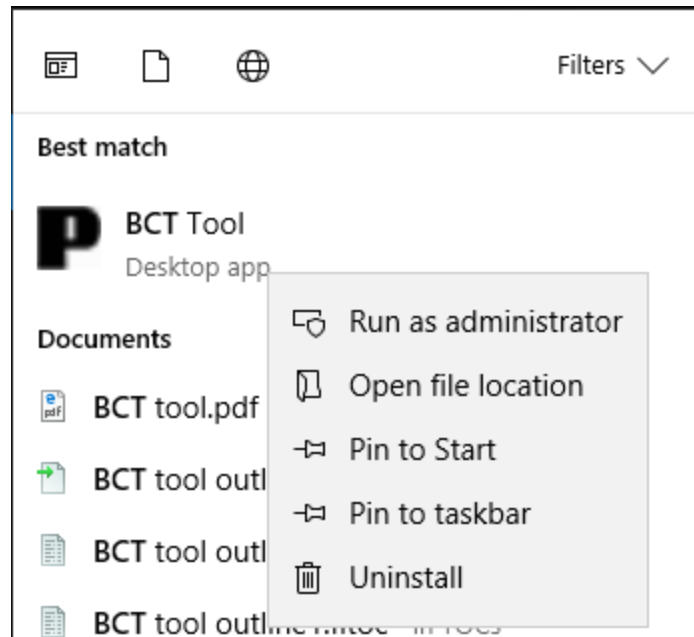
To install the BCT Tool onto a Windows 10 environment.

1. Select **setup.exe** from the options.
2. Follow the installation process and click **Finish**.

Uninstall

To uninstall the BCT Tool from a Windows 10 environment.

1. Select the **Start** button from the Home ribbon and find the BCT tool.
2. Right-click the app to bring up the drop-down menu.



3. Select **Uninstall**.
4. The BCT tool should be removed from your PC.

Using the BCT

The main purposes of the Bulk Configuration Tool are to create a new configuration and bulk replicate that configuration across your install base or to bulk update the firmware across your install base.

Create a Configuration File

1. Press **Select SKU Type**.
2. Press **OK**.
3. Press the **Create a New Conf.ini file** button.
4. Select a PDU from the SKU List.
5. Press **New**.
6. Go to **Settings** to update all.
 - This displays the power settings.
7. Go to **Settings** to update the configuration.
8. Select **File** and select **Save As** to save the Conf.ini file.

Create a List of iPDUs by Scanning the Network

1. Go to **Tool** tab and select **Firmware Upload**.
2. Choose **IP Scan** from IP Settings.
3. Enter the **Start IP** and the **Stop IP** and the **Community** string.
4. Enter the **User** name and the **Password**.
5. Hit **Scan**.

Note: The usernames and passwords need to be the same for this to work.

To upgrade the configuration, they all must be the same SKU type.

Manually Add a Single IP into the PDU List

1. Select **IP** from IP settings.
2. Enter the IP Address.
3. Enter the User Name and Password.

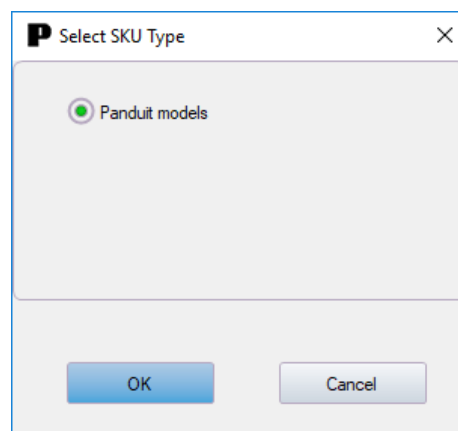
4. Hit **Insert**.
5. Select **Ping** to ensure the address exists.

Updating the iPDUs

1. Select the radio button next to the type of update. Either Firmware Upgrade, Boot Code Upgrade, or Configuration Update.
2. Select the corresponding box (Firmware, Boot, or Conf) to choose a file.
 - This displays the computer desktop.
3. Select the file to push to the PDU.
4. Select **Flash**. This will send the file to the selected PDU (the IP address or addresses highlighted).

Select SKU type

1. Select the document icon from the top-left screen to display the Select SKU Type. Press **OK**.

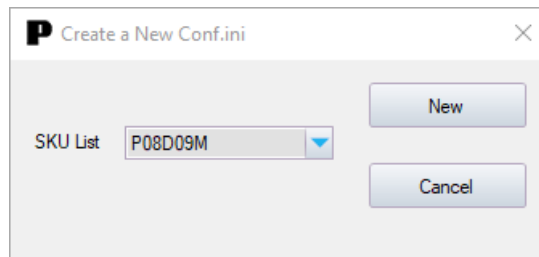


Create a New Conf.ini File

This option allows a user to create a new conf.ini file for distribution.

Select SKU Number

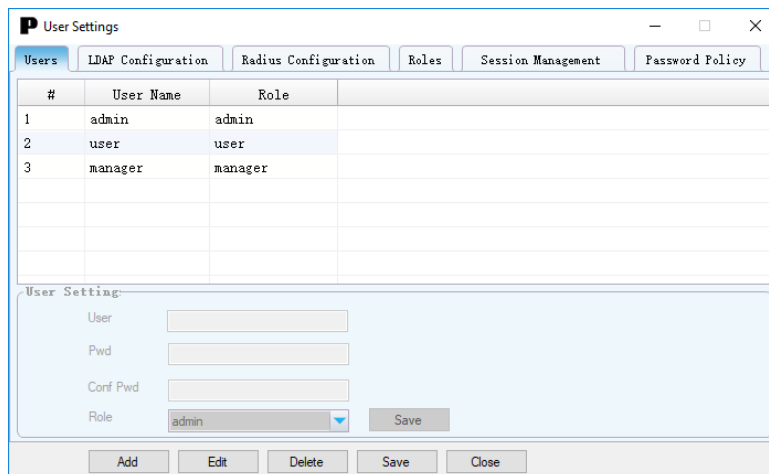
1. Select the blue plus from the top-left screen to display the Create a New Conf.ini.
2. Select desired SKU type from the drop-down menu and press **New**.



User Account Settings

Users

1. Select **Settings** from the top ribbon and choose **User Accounts**.
2. The Users tab displays in User Settings.



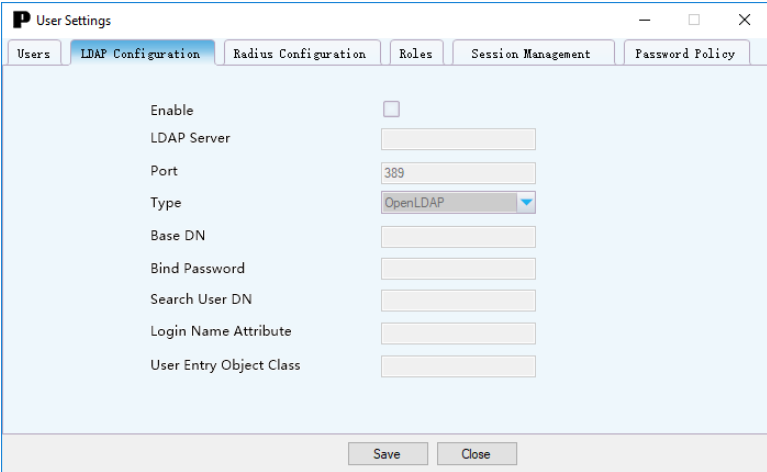
LDAP Configuration

The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

1. Go to User Accounts and select **LDAP Configuration**.
2. Select the **Enable** checkbox.
3. Use the drop-down menu to choose the **Type of LDAP Server**. Either **Open LDAP** or **Microsoft Active Directory**.
4. Enter a **Port**.

Note: For Microsoft, this is typically 389.

5. Enter the **Base DN** field, i.e. DC=subdomain, DC=mydomain, DC=com
6. Enter the **Bind Password**.
7. Enter **sAMAccountName** (typically) into the **Login Name Attribute** field.
8. Enter person in the **User Entry Object Class** field.
9. Press **Save**.



The screenshot shows the 'User Settings' dialog box with the 'LDAP Configuration' tab selected. The dialog has a title bar with a 'P' icon and standard window controls. Below the title bar are several tabs: 'Users', 'LDAP Configuration', 'Radius Configuration', 'Roles', 'Session Management', and 'Password Policy'. The 'LDAP Configuration' tab is active and contains the following fields:

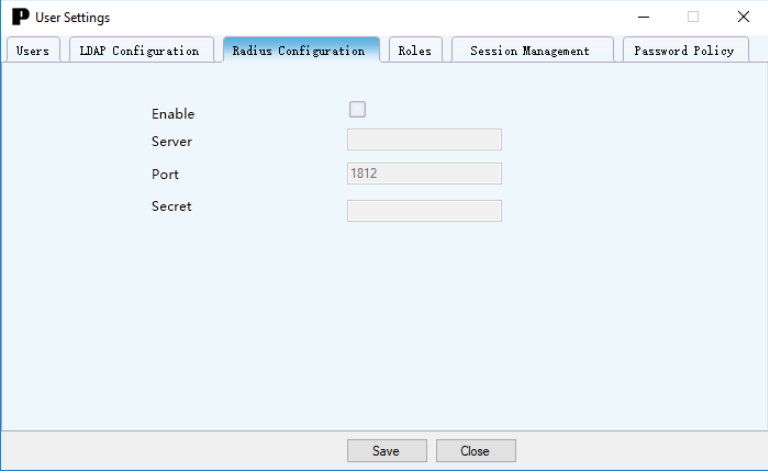
Enable	<input type="checkbox"/>
LDAP Server	<input type="text"/>
Port	<input type="text" value="389"/>
Type	<input type="text" value="OpenLDAP"/>
Base DN	<input type="text"/>
Bind Password	<input type="text"/>
Search User DN	<input type="text"/>
Login Name Attribute	<input type="text"/>
User Entry Object Class	<input type="text"/>

At the bottom of the dialog are two buttons: 'Save' and 'Close'.

Radius Configuration

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol, operating on port 1812 that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.

1. Go to **User Accounts** and select **Radius Configuration**.
2. Select the **Enable** checkbox.
3. Enter the **Server**.
4. Enter the **Secret**.



The screenshot shows a window titled "User Settings" with a tabbed interface. The "Radius Configuration" tab is selected. The window contains the following fields:

Field	Value
Enable	<input type="checkbox"/>
Server	<input type="text"/>
Port	1812
Secret	<input type="text"/>

At the bottom of the window, there are "Save" and "Close" buttons.

Roles

The Role tab defines a user's full operating permissions. All users must be added by the Admin user.

Admin: Full permissions that cannot be modified or deleted.

User: Limited permissions that can be modified or deleted. By default, these permissions are:

- Change Input Phase Setting
- Change Circuit Breaker Setting
- Switch Outlet
- Change Outlet Setting

- Change Own Password
- Change Event Settings

Manager: Permissions for user customized roles can be set as needed.

To add a User:

1. Go to **User Accounts** and select **Roles**.
2. Select **Add** from the bottom tab to begin filling out the necessary fields.
3. Enter the **Role Name** (admin, user, manager, etc.).

Note: Role name must be between 4 to 32 characters and cannot be repeated.

4. Enter the **Description**.

Note: Description must be between 4 to 32 characters and cannot be repeated.

5. Select the desired **Privileges**.
6. Press **Save**.

To Edit a User Role:

1. Go to **User Accounts** and select **Roles**.
2. Select **Edit**. Make the desired changes to the role name and privileges.
3. Press **Save**.

To Delete a User

1. Go to **User Accounts** and select **Roles**.
2. Select the role.

Note: To select multiple users, Shift Click to highlight multiple profiles.

3. Select **Delete**.
4. Press **Yes** to confirm the deletion or **No** to cancel.

#	Role	Role Description
1	admin	admin operation
2	user	user operation
3	manager	Redfish Manager

User Setting:

Role Name

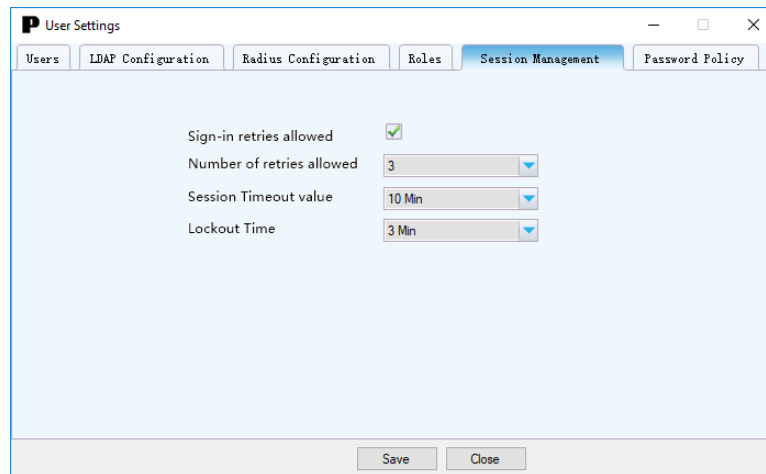
Description

Privileges Admin Privilege

Session Management

Session Management allows users to designate several sign-ins to the Web UI, a lockout time, and a timeout value.

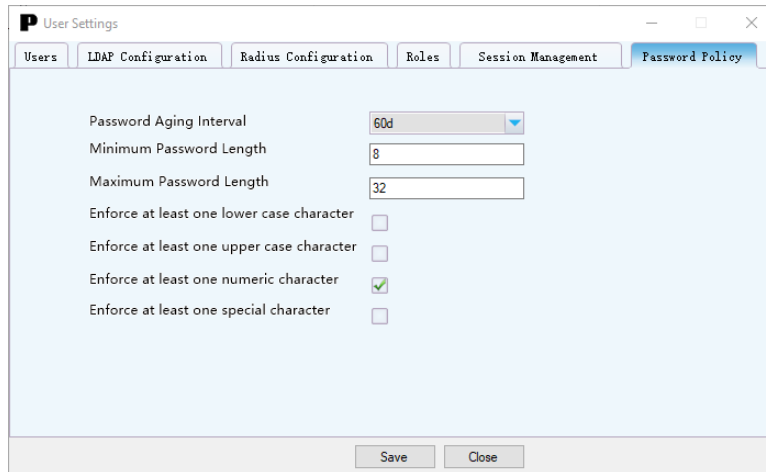
1. Go to User Accounts and select **Session Management**.
2. Select or deselect the **Sign-in Retries Allowed** box based on the needs of the Web UI.
3. Choose from the drop-down menu how many retries are allowed upon sign-in. (1-10 retries are allowed.)
4. Choose the **Session Timeout Value** from the drop-down menu. (1-minute to 24-hour increments)
5. Choose a Lockout Time from the drop-down menu. (1 minute to Infinite increment)
6. Press **Save**.



Password Policy

Password Policy provides users the ability to change and enforce different strengths to their passwords.

1. Choose a Password Aging Interval from the drop-down menu. (7 days to 365 days)
2. Enter a Minimum Password Length.
3. Enter a Maximum Password Length.
 - To enforce at least one lower case character, check the box.
 - To enforce at least one upper case character, check the box.
 - To enforce at least one numeric character, check the box.
 - To enforce at least one special character, check the box.
4. Press **Save**.



PDU Settings

PDU Settings configures Network Settings, System Management, SNMP Manager Receiver, Email Setup, and Event Notifications.

Network Settings

IP Configuration

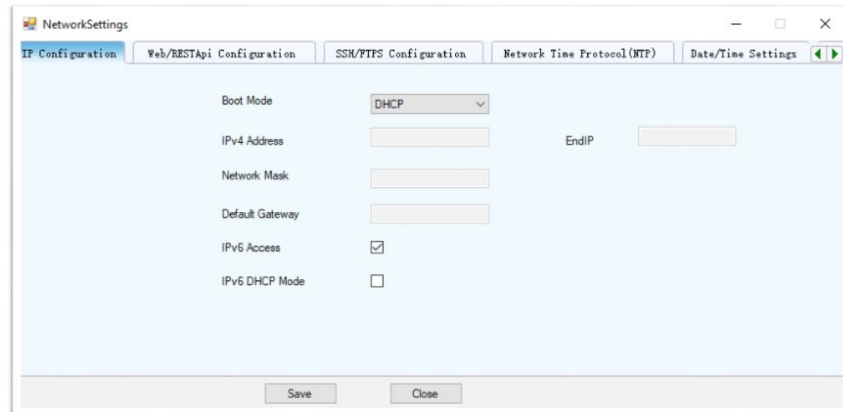
IP Configuration gives the option to between Static IP and DHCP (Dynamic H).

1. Go to Network Settings and choose **IP Configuration**.
2. Select the Boot Mode drop-down menu to choose **Static** or **DHCP** (Dynamic Hot Configuration Protocol).
3. If connecting to a Static IP, enter the **IPv4 Address**, **Network Mask**, **Default Gateway**, and **EndIP**.

Note: If DHCP is chosen, the fields will not be available.

Note: If you are creating an image for a USB drive to bring up multiple PDUs, the IPv4 Address will be the IP address of the first PDU. The configuration will automatically increment the IP on the next PDUs until the last EndIP is reached.

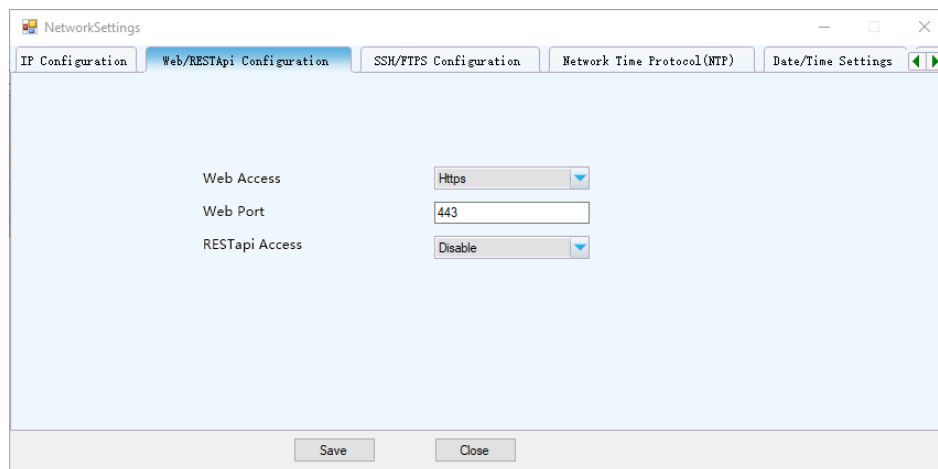
4. Check the IPv6 Access box if desired.
5. Check the IPv6 DHCP Mode box if desired.



Web/RESTApi Configuration

The Web/RESTApi Configuration tab gives the user the ability to enable or disable the Web UI or RESTapi.

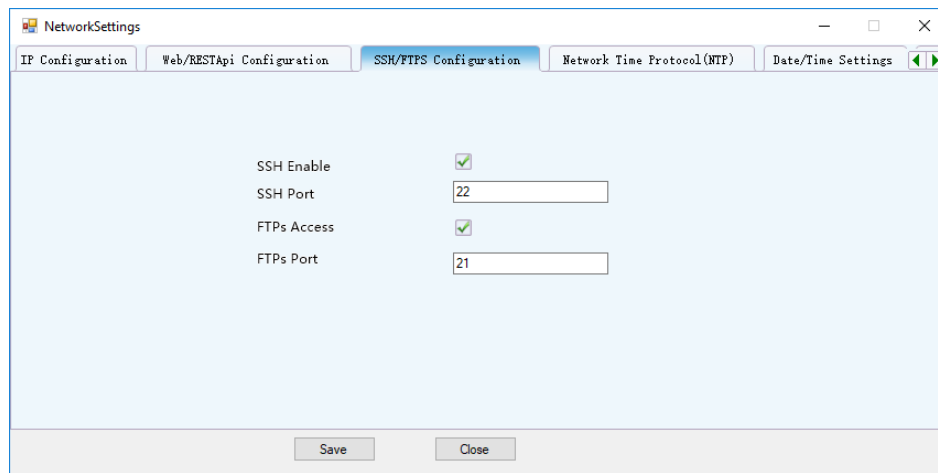
1. Go to Network Settings and select an option from the Web Access Drop-down menu.
2. Enter the appropriate number into the Web Port field.
3. In the RESTapi Access dropdown menu, select **Enable** or **Disable**.
4. Press **Save**.



SSH/FTPS Configuration

The SSH/FTPS Configuration enables the access to the command line interface of the Web UI.

1. Go to Network Settings and Select **SSH/FTPS Configuration**.
2. Check whether SSH or FTPs configuration is enabled (or both).
3. Enter the Port fields.
4. Press **Save**.



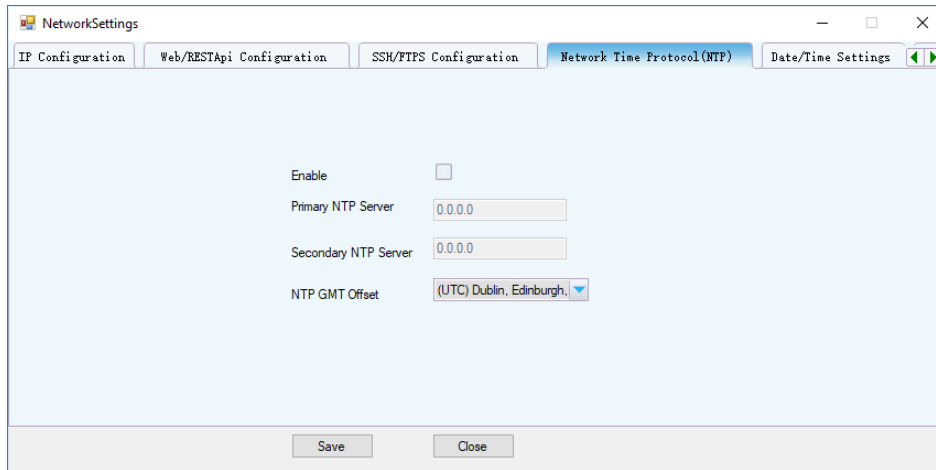
The screenshot shows a window titled "NetworkSettings" with several tabs: "IP Configuration", "Web/RESTApi Configuration", "SSH/FTPS Configuration" (which is selected), "Network Time Protocol(NTP)", and "Date/Time Settings". The "SSH/FTPS Configuration" tab contains the following settings:

SSH Enable	<input checked="" type="checkbox"/>
SSH Port	<input type="text" value="22"/>
FTPs Access	<input checked="" type="checkbox"/>
FTPs Port	<input type="text" value="21"/>

At the bottom of the window, there are two buttons: "Save" and "Close".

Network Time Protocol (NTP)

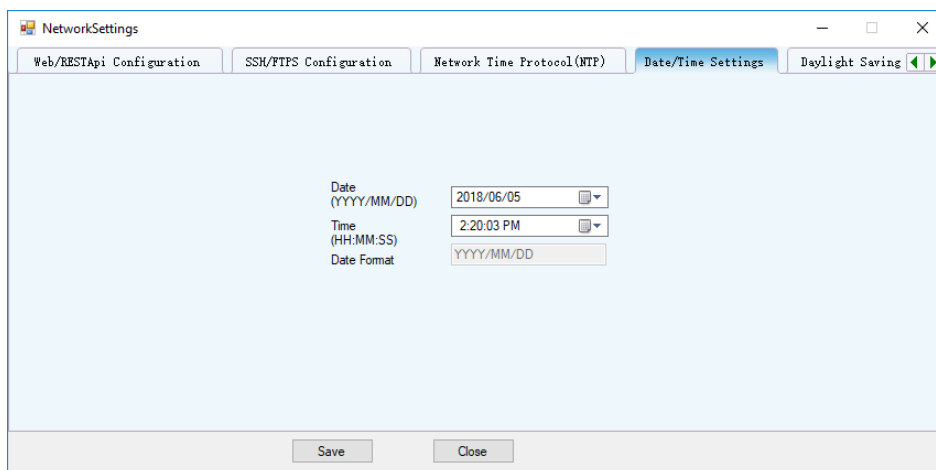
The Network Time Protocol allows a user to synchronize their clock with specific date and times.



Date/Time Settings

The Date/Time Settings are internal clocks that can be set manually (or synchronized to the NTP).

1. Go to Network Settings and select the Date/Time Settings tab.
2. Enter a Date or select a Date from the drop-down menu.
 - Use the YYYY/MM/DD format when entering the date into the field.
3. Enter a Time or select a Time from the drop-down menu.
 - Use the HH:MM:SS format when entering the time into the field.
4. Press **Save**.



Daylight Savings Time (DST)

The Daylight Saving Time setting provides the Start Month, Time and End Month, Time of Daylight Saving Time along with a Time Offset option.

The screenshot shows a window titled "NetworkSettings" with several tabs: "SSH/FTPS Configuration", "Network Time Protocol (NTP)", "Date/Time Settings", and "Daylight Saving Time (DST)". The "Daylight Saving Time (DST)" tab is active. The configuration area includes an "Enable" checkbox, which is currently unchecked. Below it are several dropdown menus: "Start Month" (with three sub-dropdowns), "Start Time(HH:MM:SS)" (with three sub-dropdowns), "End Month" (with three sub-dropdowns), "End Time(HH:MM:SS)" (with three sub-dropdowns), and "Time Offset" (with one dropdown). At the bottom of the window are "Save" and "Close" buttons.

System Management

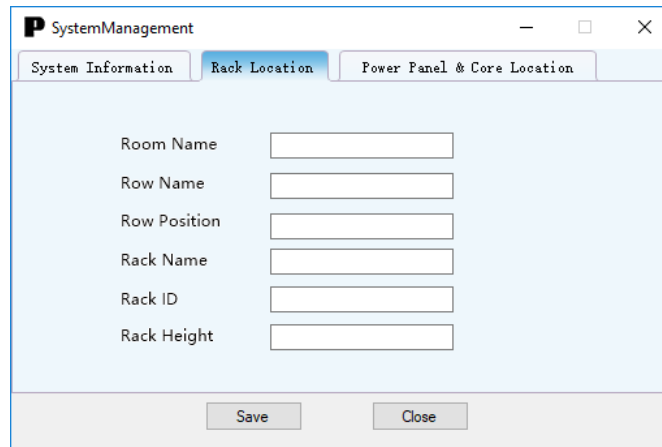
System Information

The System Information tab requires System, Contact, Rack, and Power information.

The screenshot shows a window titled "SystemManagement" with three tabs: "System Information", "Rack Location", and "Power Panel & Core Location". The "System Information" tab is active. The configuration area includes five text input fields: "System Name", "Contact Name", "Contact Email", "Contact Phone", and "Contact Location". At the bottom of the window are "Save" and "Close" buttons.

Rack Location

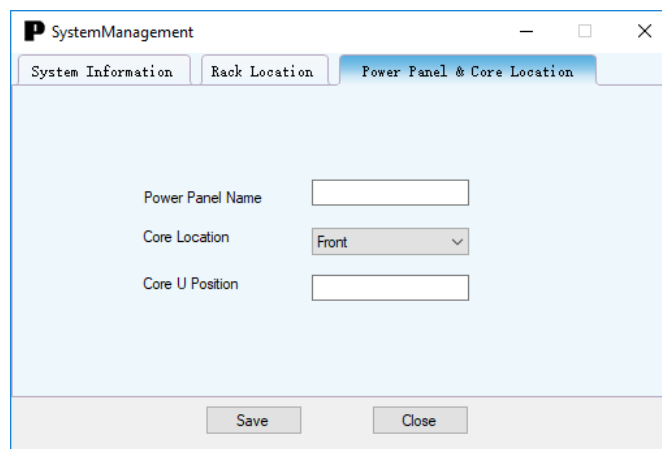
The Rack Location requires the Room Name, Row Name, Row Position, Rack Name, Rack ID, and Rack Height to be entered.



The screenshot shows a window titled "SystemManagement" with three tabs: "System Information", "Rack Location", and "Power Panel & Core Location". The "Rack Location" tab is active. It contains six text input fields labeled "Room Name", "Row Name", "Row Position", "Rack Name", "Rack ID", and "Rack Height". At the bottom of the window are two buttons: "Save" and "Close".

Power Panel & Core Location

The Power Panel & Core Location setting is required to locate the panel in the Front or Back of the PDU.



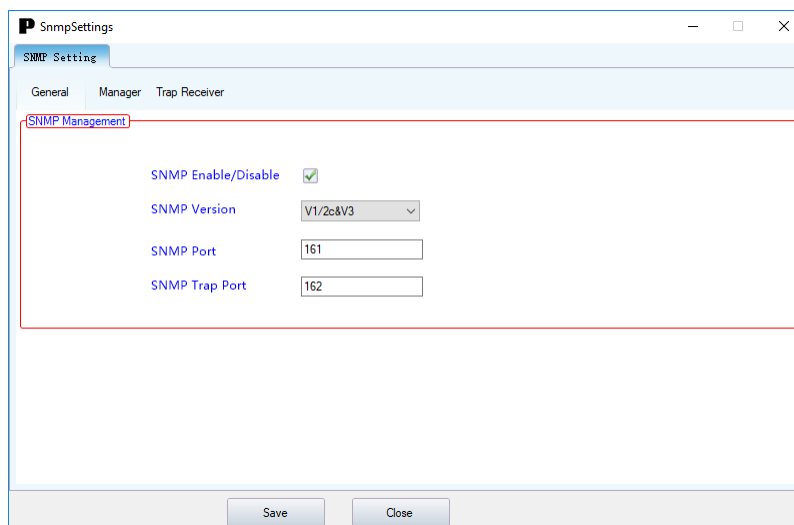
The screenshot shows the same "SystemManagement" window, but with the "Power Panel & Core Location" tab active. It contains three input fields: "Power Panel Name" (text input), "Core Location" (dropdown menu with "Front" selected), and "Core U Position" (text input). At the bottom are "Save" and "Close" buttons.

SNMP Manager/Trap Receiver

SNMP Setting (Simple Network Management Protocol) can be used to manage the G5 PDUs remotely.

General

1. Go to SNMP Manager/Trap Receiver and select **SNMP Setting**. In the General tab, select the **SNMP Enable/Disable** box to allow communication between an SNMP manager.
2. Choose from the SNMP Version drop-down menu to choose a version and enter the **SNMP Port** and **SNMP Trap Port**.
3. Press **Save**.



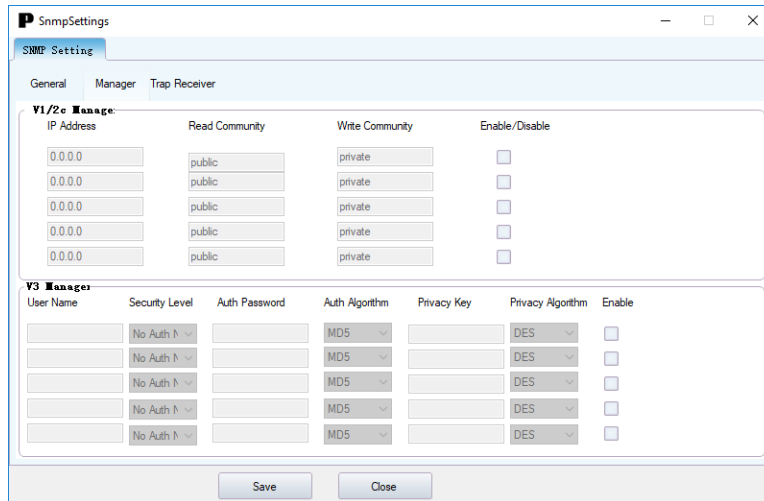
The screenshot shows a window titled "SnmpSettings" with a tab labeled "SNMP Setting". The window has three tabs: "General", "Manager", and "Trap Receiver". The "General" tab is active. A red box highlights the "SNMP Management" section, which contains the following settings:

SNMP Enable/Disable	<input checked="" type="checkbox"/>
SNMP Version	V1/2c&V3
SNMP Port	161
SNMP Trap Port	162

At the bottom of the window, there are two buttons: "Save" and "Close".

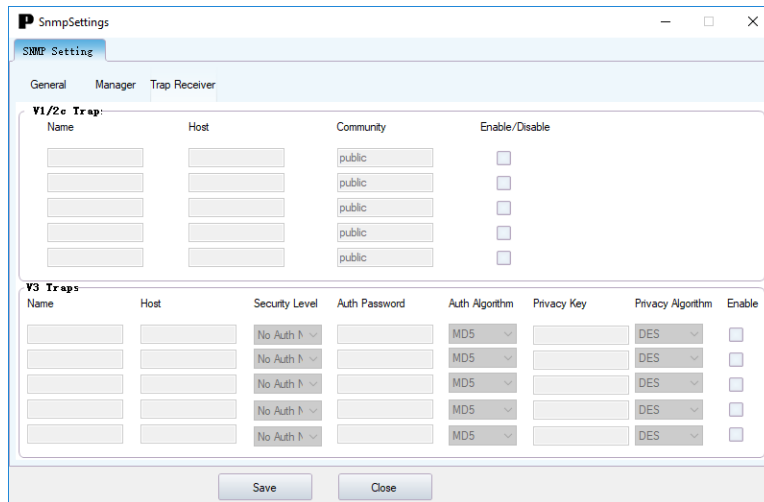
Manager

1. Select the **Enable** check box based on which strings you wish to enable.
2. Go to SNMP Manager/Trap Receiver and select **SNMP Setting**. In the Manager tab, complete the Read and Write Community String. (Typically, these strings are public.)
3. Select the **Enable** check box based on which user names you wish to enable.
4. Enter the User Names, Authorized Password, Privacy Key, along with required algorithms.
5. Press **Save**.



Trap Receiver

Events are sent to the Trap Receiver to keep an internal log of events.



Email Setup - SMTP Account Settings

An SMTP message (Simple Mail Transfer Protocol) or email is set up in the SMTP Account Settings. The G5 PDU can be configured to send alerts or event messages via email using SMTP settings. this requires the SMTP settings to be configured with an IP address for the SMTP server and a valid email address.

1. Go to PDU Settings and select **Email Setup**.
2. Enter the IP address (or name) of the mail server in the Email Server Address.
3. Enter an email address to send the reports in the Sender Address.
4. Enter the port number for the SMTP in the Port Field. The default is 25.
5. Enter a Username (if the server requires one).
6. Enter a Password (if the server requires one).
7. Enter the number of Sending Retries. The default is 3 retries.
8. Enter the Time Interval between Sending Retries (in minutes). The default is 6 minutes.
9. Select the **Server Requires Authentication** box if the SMTP server requires a password authentication.
10. Press **Save**.

The screenshot shows a dialog box titled "Email Settings" with a close button (X) in the top right corner. It has two tabs: "SMTP Account Settings" (active) and "Email Recipients". The "SMTP Account Settings" tab contains the following fields and controls:

- Email Server Address: Input field with a red error message "Not a valid Email Address" to its right.
- Sender Address: Input field.
- Port: Input field with the value "25".
- Username: Input field.
- Password: Input field.
- Number of Sending Retries: Input field with the value "3".
- Time Interval Btw Sending Retries(in Minutes): Input field with the value "6".
- Server Requires authentication: A checkbox that is currently unchecked, with the label "Enable" next to it.

At the bottom of the dialog are two buttons: "Save" and "Close".

Email Recipients

The Email Recipients enables specific email addresses to receive alerts from the G5 PDU.

1. Go to **PDU Settings** and select **Email Setup**.
2. Select the **Email Recipients** tab and begin entering desired email addresses.
3. Select the **Enable** checkbox on the email addresses that should receive alerts.

Note: A group alias is recommended when more than five emails are used.

#	Email Address	Enable
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>

Event Notifications

When the PDU meets a certain condition, (i.e., a temperature sensor exceeds the warning limit) a notification will alert.

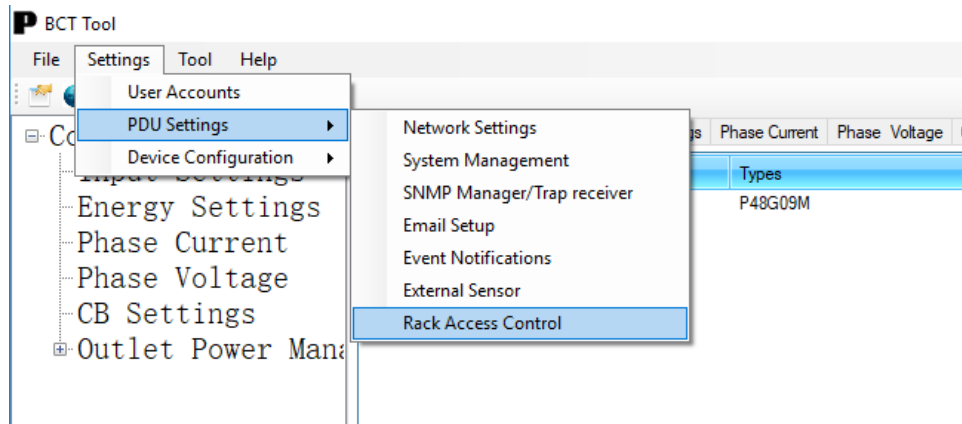
1. Go to **PDU Settings** and select **Event Notifications**.
2. Check the Email, SNMP Trap, and/or Syslog you wish to enable based on the Event.
3. Press **Save**.

Events	<input type="checkbox"/> Email	<input type="checkbox"/> SNMP Trap	<input type="checkbox"/> Syslog
Circuit Breaker Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User Activity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Smart Rack Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Outlet Power Control Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Critical Alarm	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Warning Alarm	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Password/Settings Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network Card Reset/Start	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
External Sensor Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PDU Configuration File Imported/Exported	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User Role Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Firmware Update	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Communication Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Daisy Chain Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enter Bootloader Mode	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LDAP/Radius Error	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

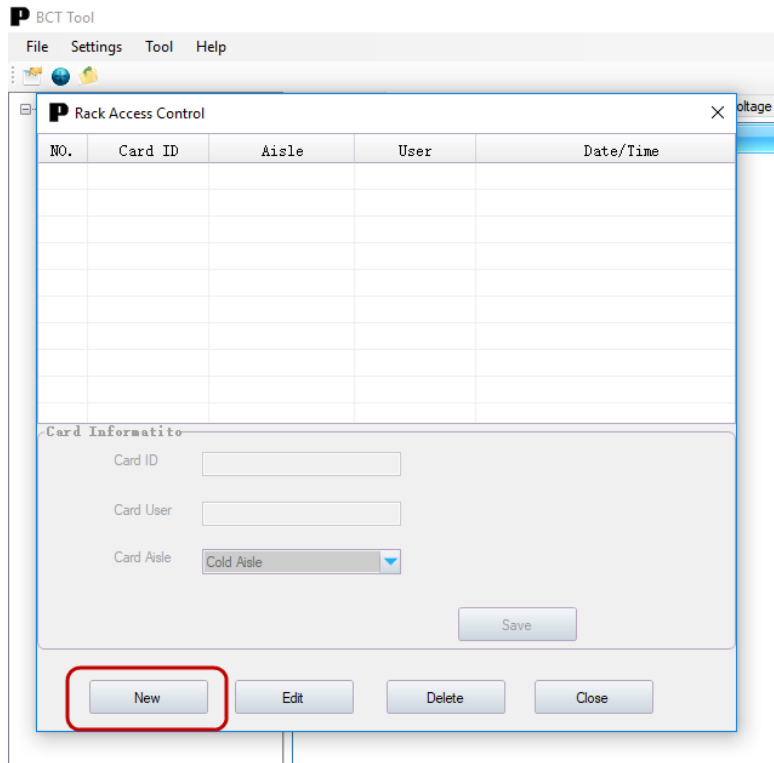
Rack Access Control

How to install the Rack Access Control in the Bulk Configuration Tool.

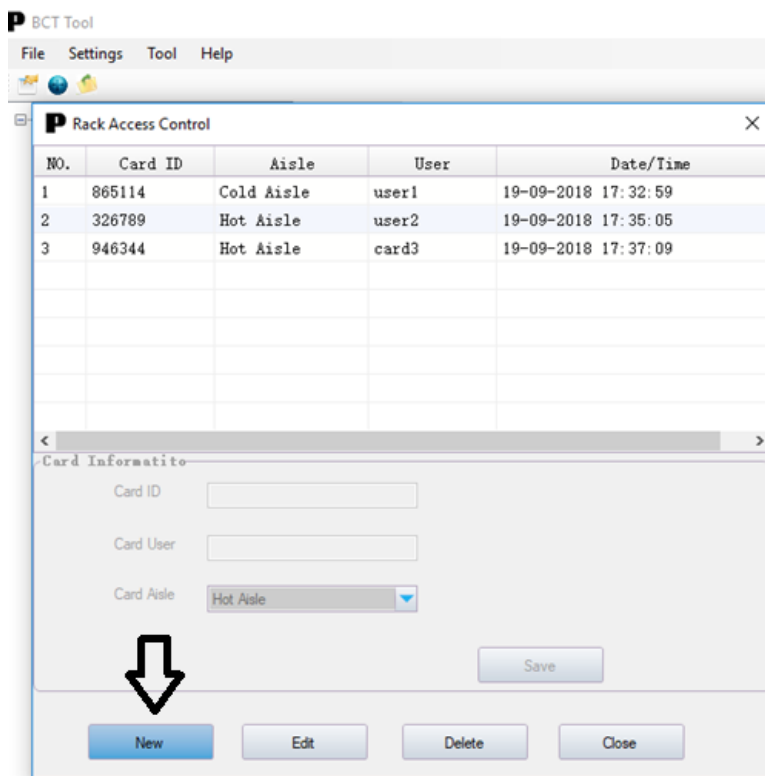
1. Select **Settings** from the top drop-down ribbon and hover over **PDU Settings** and select **Rack Access Control**.



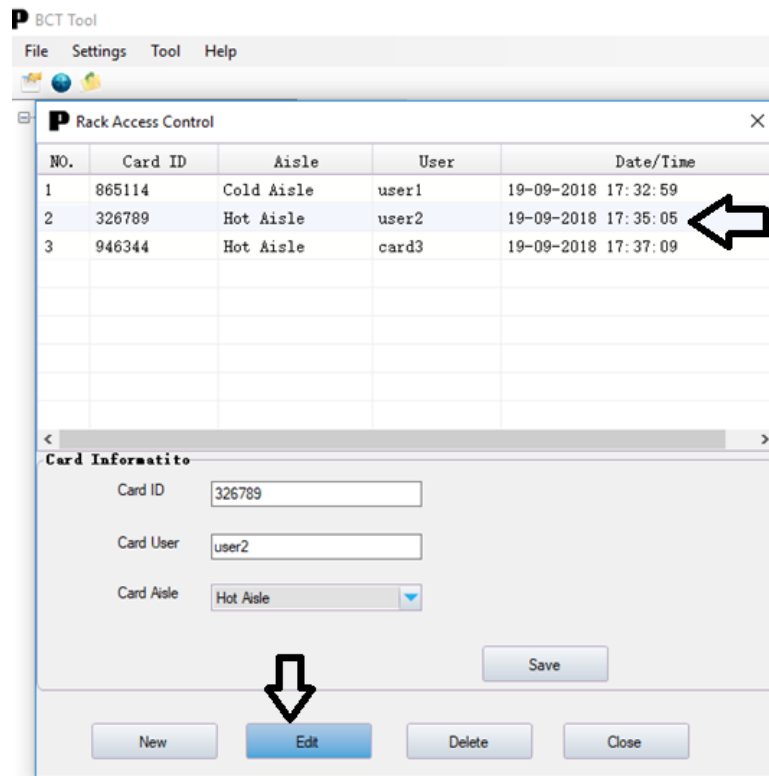
2. The Rack Access Control window will appear. Select **New** to add new card information.



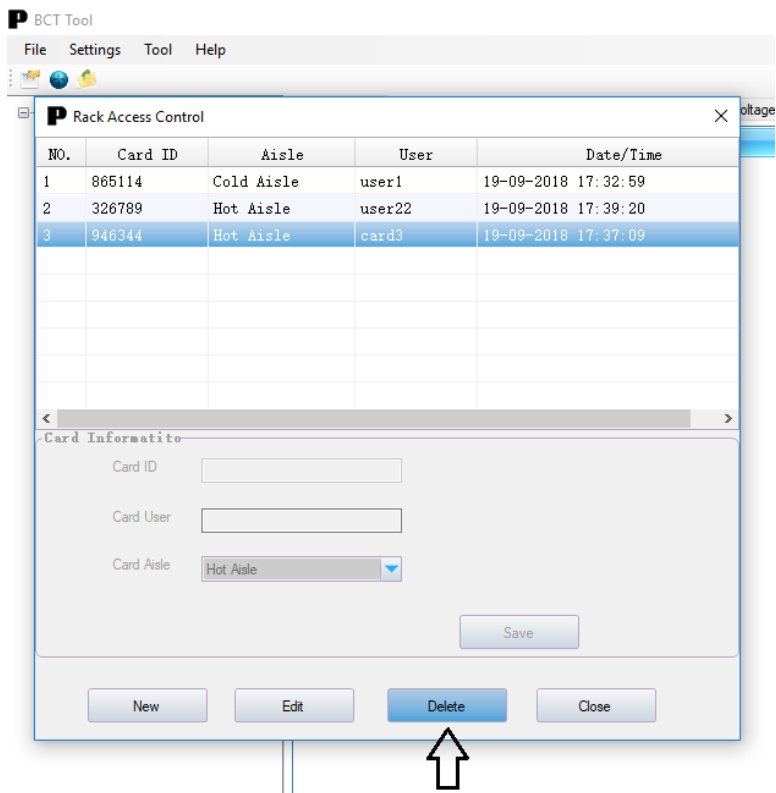
3. Enter the Card ID, Name, and select the aisle.
4. Click **Save**. The new card details will appear in the table.



5. To edit, select the card details to update and click **Edit** to begin making changes.



6. To delete card details, select the card information and click **Delete**.



7. Close the window once the card information is entered.
8. Save the conf.ini file and upload this file to the PDU connected with HID to update the card information.

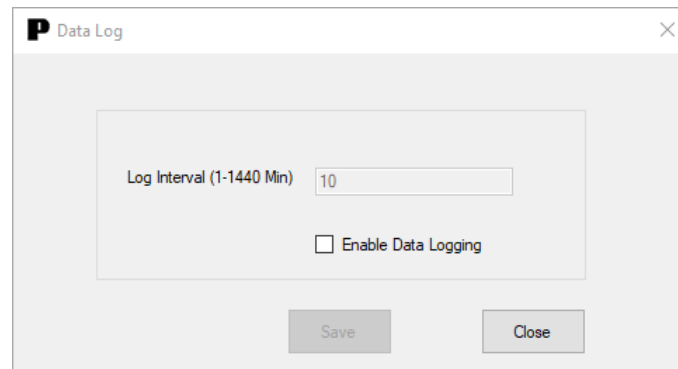
Device Configuration Settings

Data Log

The G5 PDU maintains a data log of up to 2000 records.

The period of time visible in the data log at any one time depends on the time between data log entries. You can configure the time range of each record from 1 to 1440 minutes. Once the data log reaches the maximum 2000 records, the oldest entries are overwritten by newer entries.

1. Go to **Device Configuration** and select **Data Log**.
2. Enter an interval number in the Log Interval field. Valid range is from 1 to 1440 minutes. The default time is 10 minutes.
3. Press **Save** to save the changes.



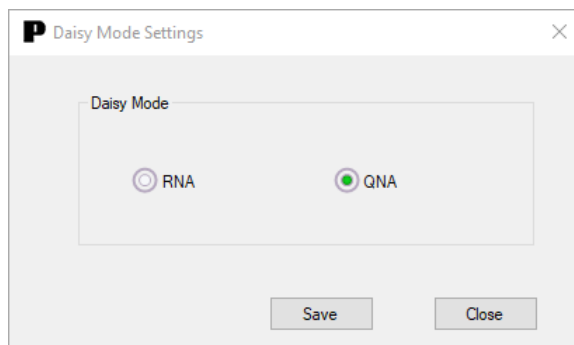
The screenshot shows a dialog box titled "Data Log" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Log Interval (1-1440 Min)" containing the number "10". Below the input field is a checkbox labeled "Enable Data Logging" which is currently unchecked. At the bottom of the dialog, there are two buttons: "Save" and "Close".

Daisy Chain Mode

The daisy chain functionality reduces the number of IP addresses and physical network connections by connecting up to 4 PDUs together.

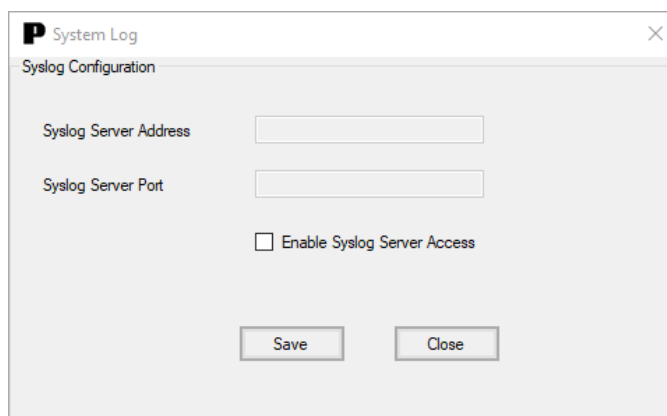
In daisy chain mode (also known as QNA: Quad Network Access), up to four (4) PDUs can be connected via one (1) IP address. This allows users to gather information and data of all daisy-chained PDUs from the main PDU.

1. Go to **Device Configuration** and select **Daisy Chain Mode**.
2. *By default, it is set to QNA (Daisy Chain) Mode.*
3. Press **Save**



System Log Configuration

1. Go to **Device Configuration** and select **System Log Configuration**.
2. Enable the Syslog Server Access to access fields.
3. Enter the Syslog Server Address.
4. Enter the Syslog Server Port.
5. Press **Save**.

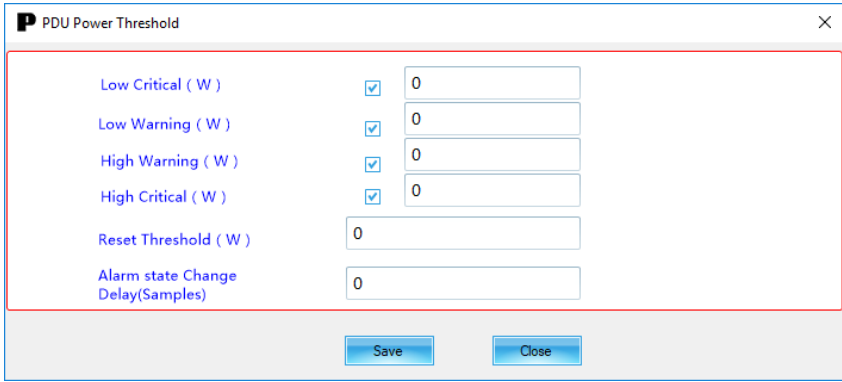


Power Settings

Input Settings

The Input Settings change the PDU warning thresholds.

1. Select **Input Settings** tab and select the **PDU Power Threshold Settings**.
2. Enter the Low Critical (W) field.
3. Enter the Low Warning (W) field.
4. Enter the High Warning (W) field.
5. Enter the High Critical (W) field.
6. Enter the Reset Threshold (W) field.
7. Enter the Alarm State Change Delay (Samples) field.
8. Press **Save**.



The screenshot shows a window titled "PDU Power Threshold" with a close button (X) in the top right corner. The window contains the following settings:

Low Critical (W)	<input checked="" type="checkbox"/>	0
Low Warning (W)	<input checked="" type="checkbox"/>	0
High Warning (W)	<input checked="" type="checkbox"/>	0
High Critical (W)	<input checked="" type="checkbox"/>	0
Reset Threshold (W)		0
Alarm state Change Delay(Samples)		0

At the bottom of the window, there are two buttons: "Save" and "Close".

Energy Settings

1. Select the **Energy Settings** tab and select **PDU1Setting**.
2. Enter the High Critical field.
3. Enter the High Warning field.
4. Enter the Reset Threshold field.
5. Enter the Alarm state Change Delay.
6. Press **Save**.

The screenshot shows a configuration window titled "PDU Energy Threshold". It contains the following fields and controls:

- High Critical:** A checked checkbox and a text input field containing "2147483".
- High Warning:** A checked checkbox and a text input field containing "2147483".
- Reset Threshold:** A text input field containing "0".
- Alarm state Change Delay(Samples):** A text input field containing "0".

At the bottom of the window are two buttons: "Save" and "Close".

Phase Current

1. Select the **Phase Current** tab and select **Phase1Setting** to update phase 1.
2. Enter the Low Critical (A) field.
3. Enter the Low Warning (A) field.
4. Enter the High Warning (A) field.
5. Enter the High Critical (A) field.
6. Enter the Rest Threshold (A) field.
7. Enter the Alarm state Change Delay (Samples) field.
8. Press **Save**.
9. Repeat Steps 2-8 for all phases.

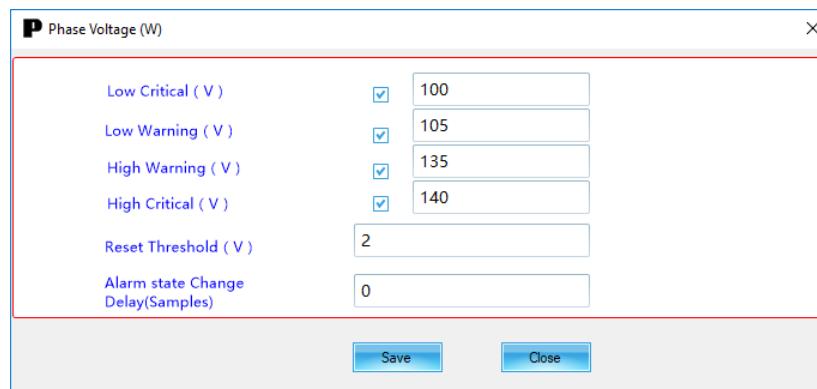
The screenshot shows a configuration window titled "Phase Current". It contains the following fields and controls:

- Low Critical (A):** A checked checkbox and a text input field containing "0".
- Low Warning (A):** A checked checkbox and a text input field containing "0".
- High Warning (A):** A checked checkbox and a text input field containing "14".
- High Critical (A):** A checked checkbox and a text input field containing "16".
- Reset Threshold (A):** A text input field containing "1".
- Alarm state Change Delay(Samples):** A text input field containing "0".

At the bottom of the window are two buttons: "Save" and "Close".

Phase Voltage

1. Select the **Phase Voltage** tab and select **Phase1Setting**.
2. Enter the Low Critical (V) field.
3. Enter the Low Warning (V) field.
4. Enter the High Warning (V) field.
5. Enter the High Critical (V) field.
6. Enter the Reset Threshold (V) field.
7. Enter the Alarm state Change Delay (Samples) field.
8. Press **Save**.



Setting	Checkbox	Value
Low Critical (V)	<input checked="" type="checkbox"/>	100
Low Warning (V)	<input checked="" type="checkbox"/>	105
High Warning (V)	<input checked="" type="checkbox"/>	135
High Critical (V)	<input checked="" type="checkbox"/>	140
Reset Threshold (V)		2
Alarm state Change Delay(Samples)		0

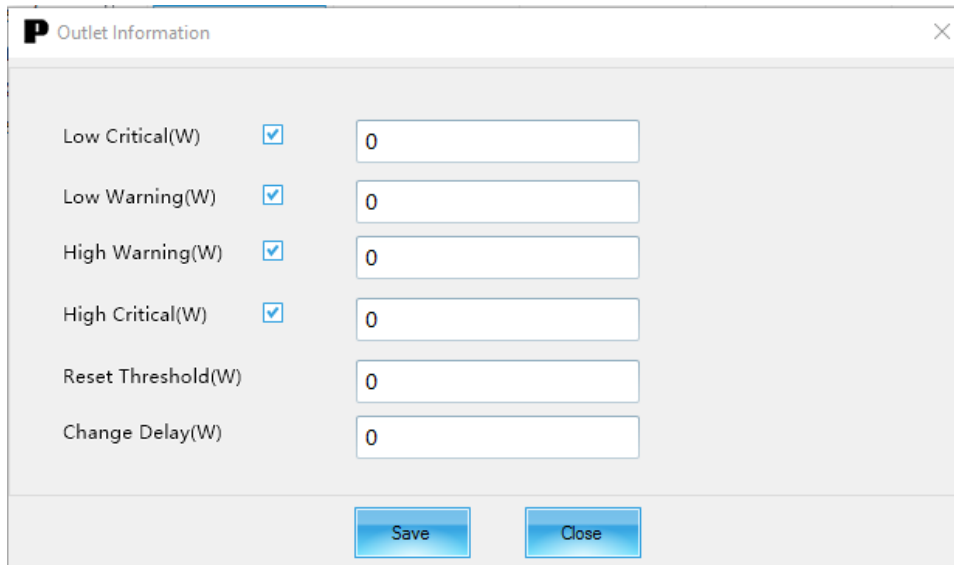
Circuit Breaker Settings

1. Select the **CBSettings** tab if the PDU has circuit breakers. Then hit the **B1Setting** to update the setting for breaker 1.
2. Enter the Low Critical (A) field.
3. Enter the Low Warning (A) field.
4. Enter the High Warning (A) field.
5. Enter the High Critical (A) field.
6. Enter the Reset Threshold (A) field.
7. Enter the Alarm state Change Delay (Samples) field.
8. Press **Save**.
9. Repeat Steps 2-8 for all breakers.

Setting	Checkbox	Value
Low Critical (A)	<input checked="" type="checkbox"/>	0
Low Warning (A)	<input checked="" type="checkbox"/>	0
High Warning (A)	<input checked="" type="checkbox"/>	11
High Critical (A)	<input checked="" type="checkbox"/>	14
Reset Threshold (A)	<input type="checkbox"/>	1
Alarm state Change Delay(Samples)	<input type="checkbox"/>	0

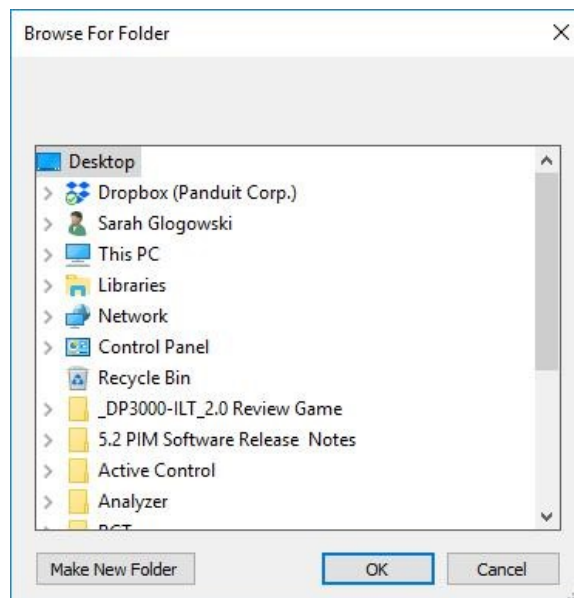
Outlet Power Management

1. Select the **Outlet Power Management** tab if the PDU has Per Outlet Monitoring. Then hit **Outlet1Setting** to update the setting for outlet 1.
2. Enter the Low Critical (W) field.
3. Enter the Low Warning (W) field.
4. Enter the High Warning (W) field.
5. Enter the High Critical (W) field.
6. Enter the Reset Threshold (W) field.
7. Enter the Alarm state Change Delay (Samples) field.
8. Press **Save**.
9. Repeat Steps 2-8 for all outlets.



Save As

1. Select **File** and choose **Save As**. The Browse for Folder screen will appear.
2. Select a folder to store your conf.ini file.



Updating the PDU

Adding Individual PDUs

1. Go to the **Tool** tab and select **IP**.
2. Enter the IP address.
3. Enter user name and password.
4. Select **Insert**.
5. Repeat steps 4-5 for each individual PDU in need of updates.
6. Select **Ping**.

Adding Multiple PDUs

1. Go to **Tool** tab.
2. Select **IP scan** tab.
3. Enter the starting IP address.
4. Enter the ending IP address.
5. Enter the SNMP read community string.
6. Enter the user name and password to access the PDU.
7. Select **Scan** to scan the network.

The screenshot displays the FirmwareUpload application window. It is divided into several sections:

- File Settings:** Contains three radio buttons for selecting the file type: **Firmware** (selected), **Boot**, and **Conf**. Each radio button is accompanied by a text input field and a corresponding button.
- IP Settings:** Contains two tabs: **IP** and **IP Scan**. Under the **IP** tab, there are three text input fields for **IP Address**, **User Name**, and **Password**, each with a corresponding button: **Insert**, **Ping**, and **Flash**.
- Upload Details:** Contains a table with two columns: **IP Address** and **User Name**. Below the table are three buttons: **Delete**, **Delete All**, and **Close**.

Upgrading Firmware

1. Select the **Firmware** button to select the Panduit.FW.
2. Select the **Radio** button next to firmware.
3. Select **Flash** to update the PDUs.

Upgrade the Boot Loader

1. Select the **Boot** button to select the Panduit bin.
2. Select **Radio** button next to Boot.
3. Select **Flash** to update the PDUs.

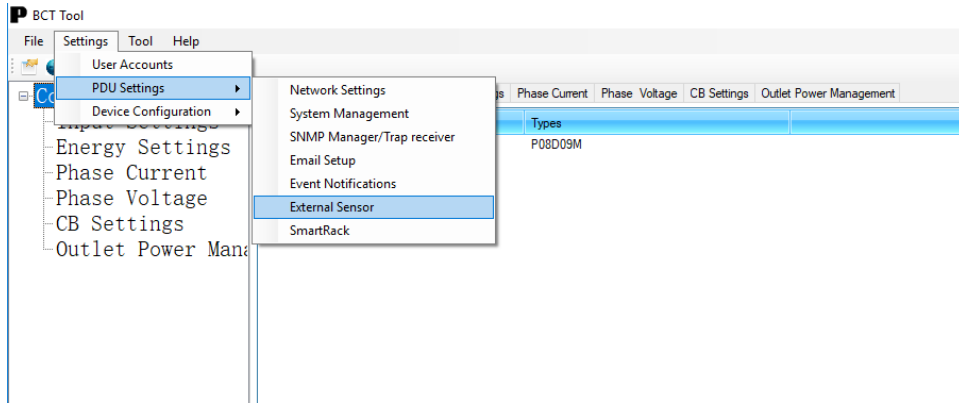
Configuration Update

1. Select **Conf** button to select the conf.ini.
2. Select **Radio** button next to Conf.
3. Select **Flash** to update the PDUs.

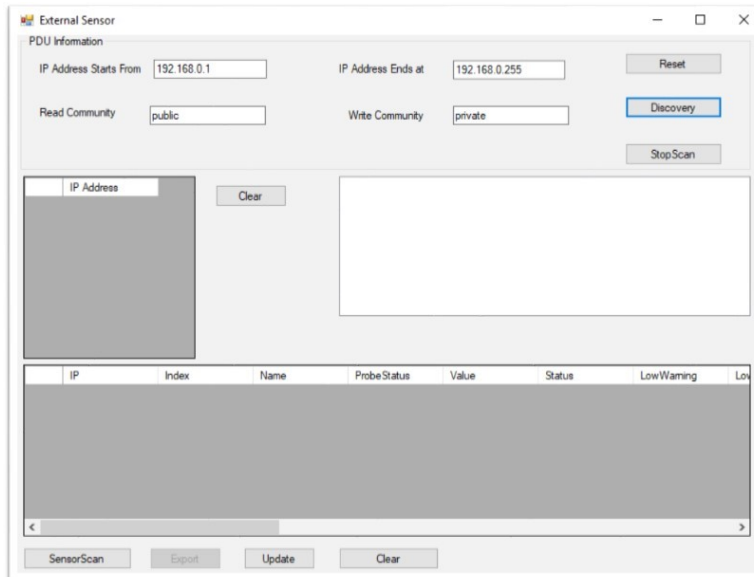
PDU Accessory Setup

How to install multiple iPDUs and accessories onto your Network using the BCT bulk configuration tool.

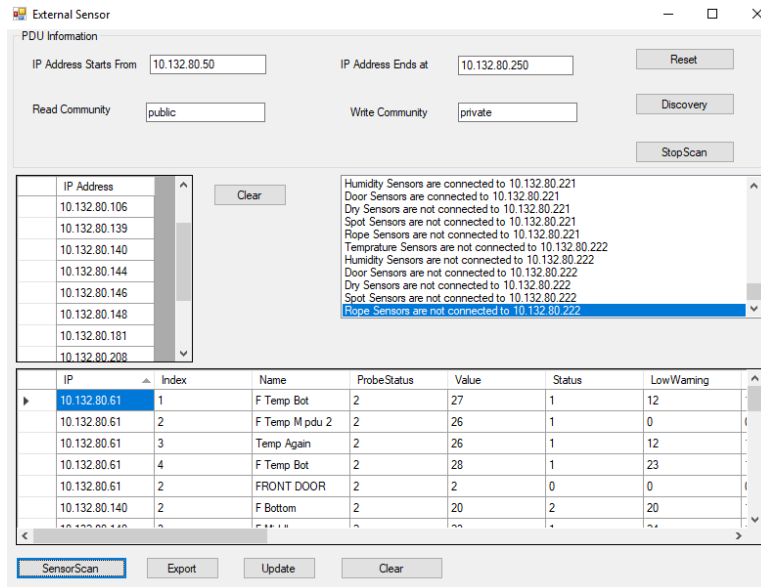
1. Select **Tool** from the top drop-down ribbon and then choose **External Sensors**.



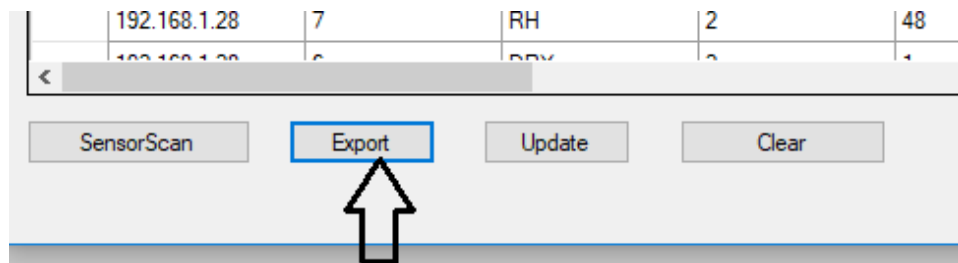
2. The below dialog box opens displaying the External Sensor window.



3. Enter the IP address range (start with IP and end IP) to discover all the Panduit PDUs that are in the network.
4. Enter the SNMP read and write the community string then click the **Discovery** button.
5. Once the Discovery is complete, the scanned Panduit IPs will appear on the left IP address table.
6. Select **Sensor Scan** to connect all the sensors to the PDU.



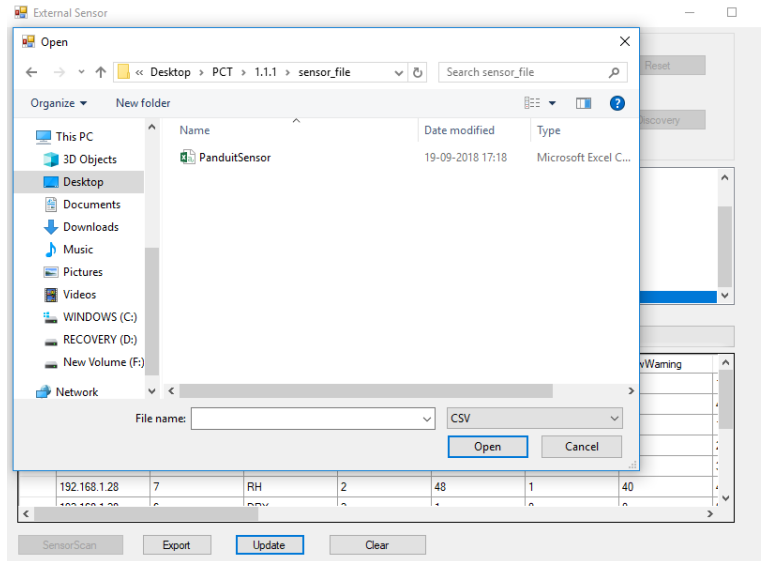
7. Export the file (.csv file) to desktop and edit the sensor name and threshold values.



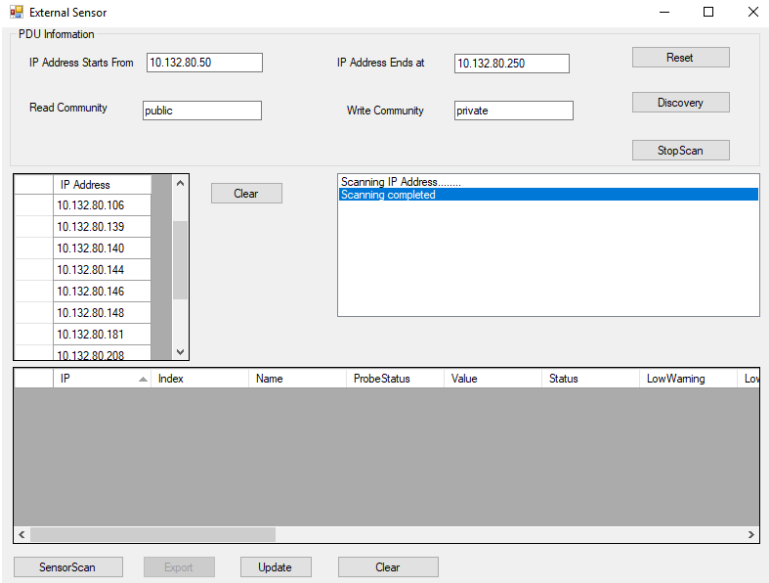
8. Open the PanduitSensor.csv file and edit the sensor name and threshold values.

For **Temperature Sensors**, the user can edit the following column fields:

11. Save and close the file after updating the values in PanduitSensor.csv file.
12. To update the sensor values, click **Update** and select the edited sensor file.



13. Once the update is complete, clear the **Sensor Scan** window and re-scan for the sensors by clicking the **Sensor Scan**.
14. Verify if the updated values appear for each sensor.



Help

Selecting the Help button gives the option to choose a Language and to read the Version number of the BCT Tool.

Language

1. Select **Help** and choose the **Language** drop-down menu and choose your desired language.
 - The language options are English, German, and Chinese.

About BCT

1. Select **Help** and choose **About BCT...**
2. The version number of the BCT Tool will display. Press the **X** at the top right when complete.

