eConnect Firmware Release Notes 5.3.792 02/05/2021

Applicability

This firmware revision is an incremental release, adding additional error handling within the power management functionality for individual eConnect PDU's with an MCM4 controller. **Do not use this firmware version if any of the PDU's within the Secure Array have an MCM1 controller.** Below is a guide to identify whether your eConnect PDU has an MCM4 or MCM1 controller:

MCM4 controller:

The unit is marked as "eConnect Controller 4"
The unit has two Auxiliary Ports labeled as "AUX1" and "AUX2".
The unit has two USB connectors.

MCM1 controller:

The unit does not have "AUX1" and "AUX2" ports.
The unit has one USB connector.

New Features:

- Added support for rebooting child PDU's in the SecureArray
- Added support for additional child functions in the SecureArray
  - Added child Outlet functions
    - o Outlet Config
    - o Outlet Alerts
  - Added child Sensor Alert functions
  - Added child EAS Config functions

Bug Fixes:

- Addressed small discrepancy in help menu - reboot PDU command.
- Some CLI commands are now case insensitive
- Addressed lack of temperature continuity within CLI commands
- Update and refine of the SecureArray SNMP tables.
- Final fixes for the TableView method on the iReasoning MIB browser.
- Addressed issue with PDU list on User Management page.
- WebUI Copyright Year to 2021
- Increased Time and Date Settings to support through year 2025
- Removed 'Shared Role' functions
- Addressed issue with Monitored Pro units not changing LED's to blue at runtime.

United States
Agoura Hills, CA
800-834-4969
Canada
Toronto, Ontario, Canada
+905-850-7770
www.chatsworth.com

Europe
Buckinghamshire, UK
+441628524834

Middle East & Africa
Dubai, UAE
+971-4-2602125

Doha, Qatar
+974-4-267422

Latin America
Mexico City
+52-55-5203-7525
Toll Free within Mexico
800-201-7592
chatsworth.com.co

Asia Pacific
Shanghai
+86 21 6880-0266
chatsworth.com.cn

CHATSWORTH PRODUCTS

Known Limitations:

- Emails and Traps for secondary alarms may contain metrics data that is up to a minute out-of-date.
- The Console 2 Port (Micro-USB) is currently not supported. Support will be added in a future release.

Upgrade Procedure:

There are few different ways to upgrade the PDU. For HTTP/FTP/TFTP options, please consult the PDU instruction manual. The PDU can also be upgraded via USB, or, if running Firmware that is 5.0.678 or later, via file upload. To obtain the latest available firmware .zip file, download from http://www.chatsworth.com/support-and-downloads/downloads/software/

Via USB:

- Unzip the contents of the file pn-cpi-924-30543-001-20210129-svn21029.zip to a USB flash drive. There is one file which must be transferred to the root directory: cpipack3-20210129-svn21029.bin.
- Plug the USB flash Drive into the USB port on the PDU and use the LCD menu to perform the firmware upgrade.
- Confirm the new firmware version after the PDU reboots is 5.3.792

Via WebUI File Upload:

- Unzip the contents of the file pn-cpi-924-30543-001-20210129-svn21029.zip to directory of choice.
- Login to the WebUI of the PDU and navigate to the “Administration – Upgrade Firmware” web page
- Select the “Upgrade this PDU via Network” radio button, followed by the “File” radio button of the sub-menu
- Click the “Choose File” button and navigate to the location of the extracted .zip file
- Select the cpipack3-20210129-svn21029.bin file and then click “Upgrade” in the WebUI
- Confirm the new firmware version after the PDU reboots is 5.3.792

Radius Card Authentication

The eConnect PDU now supports the ability to centralize card authentication information on a Radius server. You must first configure your RADIUS server to support the card authentication by the eConnect PDU.

There are 2 ways to utilize the Radius Card Authentication system:

1. The radius server can serve as the sole central repository for user information. In this scenario, a reply from the radius server includes the Filter-Id attribute to indicate the associated group for the card/user. If the Filter-Id attribute is not provided and method 2 below is not used, then the system will not unlock the cabinet.
2. The radius server serves solely as a central authentication authority. Users are created on the individual PDUs and assigned to groups. In this case, the Username attribute must be returned to the PDU by the radius server. If the Username does not exist in the local PDU data store, then the system will not unlock the cabinet.

A sample configuration is provided below. This configuration was performed using FreeRADIUS.

Below is a sample Users file entry to work with the eConnect using card Authentication. "xxxxxxxxxx" below is the code from the card being used.

```
# eConnect LOCK USER
xxxxxxxxxx Password = "cpixxxxxxxxxx"
    User-Name="user", (this can be anything that the user desires)
    Filter-Id="Cabinet"
```

Once the RADIUS server has been configured, you can enable RADIUS Card authentication on the eConnect PDU.

1. Log into the eConnect PDU and navigate to "Cabinet Access" -> "RADIUS Card Settings"
2. Click the "Enable Radius Card Authentication" check box.
3. If using IPv6 addresses to the Radius Server, then click the "Use IPv6" check box.
4. Enter at least one Radius server address and port.
5. Enter the shared secret between the PDU and the Radius server.
6. Provide a test card ID to use for testing the connection.
7. Click the Save button. The system will send the Radius request to the server to validate the connection.

If using method 2 from above, you may add users through the "Administration" -> "User Management" page.

Technical RADIUS Detail

The eConnect PDU will send along the following information in the initial Radius Auth request.

Field Identified	Source	Description
Service-Type	From PDU	This Attribute indicates the type of service that has requested, or the type of service to be provided. The Service Type attribute is always set to Login for card authentications.
NAS-IP-Address	From PDU	This Attribute indicates the identifying IP Address of the NAS which is requesting authentication of the user, and SHOULD be unique to the NAS within the scope of the RADIUS server. NAS-IP-Address is only used in Access-Request packets. Either NAS IP-Address or NAS-Identifier MUST be present in an Access-Request packet. This is the IP address of the PDU.
NAS-Port	From PDU	For card authentications, the NAS-Port attribute will be 129.
NAS-Port-ID	From PDU	The attribute will include the name of the PDU with "#eas" appended to the end.
NAS-Port-Type	From PDU	This value is set to 15.
User-Name	From Radius To PDU	The user name associated with the card ID.
Filter-Id	From Radius	The PDU group the user should be associated with. This should be on of: • Admin • Cabinet • User • Viewer If this value is not sent with the response, then the User-Name returned will need to be a user configured locally on the PDU, otherwise access will not be granted to the user.

Radius User Authentication

The eConnect PDU has improved Radius server support. Radius may now be used as the primary central user authentication/authorization system. You must first configure your RADIUS server to support the user authentication by the eConnect PDU.

There are 2 ways to utilize the Radius User Authentication system:

1. The radius server can serve as the sole central repository for user information. In this scenario, a reply from the radius server includes the Filter-Id attribute to indicate the associated group for the card/user. If the Filter-Id attribute is not provided and method 2 below is not used, then the system will not unlock the cabinet.
2. The radius server serves solely as a central authentication authority. Users are created on the individual PDUs and assigned to groups. In this case, the User-name attribute must be returned to the PDU by the radius server. If the Username does not exist in the local PDU data store, then the system will not unlock the cabinet.

A sample configuration is provided below. This configuration was performed using FreeRADIUS.

Below is a sample Users file entry to work with the eConnect using card Authentication. "xxxxxxxxxx" below is the code from the card being used.

```
# eConnect LOCK USER
xxxxxxxxxx Password = "cpixxxxxxxxxx"
    User-Name="user", (this can be anything that the user desires)
    Filter-Id="Cabinet"
```

Once the RADIUS server has been configured, you can enable RADIUS Card authentication on the eConnect PDU.

1. Log into the eConnect PDU and navigate to “Cabinet Access” -> “RADIUS Card Settings”
2. Click the “Enable Radius Card Authentication” check box.
3. If using IPv6 addresses to the Radius Server, then click the “Use IPv6” check box.
4. Enter at least one Radius server address and port.
5. Enter the shared secret between the PDU and the Radius server.
6. Provide a test card ID to use for testing the connection.
7. Click the save button. The system will send the Radius request to the server to validate the connection.

If using method 2 from above, you may add users through the “Administration” -> “User Management” page.

Technical RADIUS Detail

The eConnect PDU will send along the following information in the initial Radius Auth request.

Field Identified	Source	Description
Service-Type	From PDU	This Attribute indicates the type of service that has requested, or the type of service to be provided. The Service-Type attribute is always set to Login for card authentications.
NAS-IP-Address	From PDU	This Attribute indicates the identifying IP Address of the NAS which is requesting authentication of the user, and SHOULD be unique to the NAS within the scope of the RADIUS server. NAS-IP-Address is only used in Access-Request packets. Either NAS IP-Address or NAS-Identifier MUST be present in an Access-Request packet. This is the IP address of the PDU.
NAS-Port	From PDU	For user authentications, the NAS-Port attribute will be 1.
NAS-Port-ID	From PDU	The attribute will include the name of the PDU with “#http_ssh” appended to the end.
NAS-Port-Type	From PDU	This value is set to 15.
Framed-IP-Address	From PDU	This Attribute will be the IP address of the user’s remote computer.
Calling-Station-Id	From PDU	This attribute will be the IP address of the user’s remote computer.
User-Name	From Radius To PDU	The user name associated with the card ID.
Filter-Id	From Radius	The PDU group the user should be associated with. This should be on of: • Admin • Cabinet • User • Viewer If this value is not sent with the response, then the User-Name returned will need to be a user configured locally on the PDU, otherwise access will not be granted to the user.