eConnect Firmware Release Notes 4.13.883

Applicability

This firmware revision is intended for individual eConnect PDU's with an MCM2 or MCM3 controller or eConnect PDU's within a Secure Array, all of which have an MCM2 or MCM3 controller. Do not use this firmware version if any of the PDU's within the Secure Array has an MCM1 controller. Below is a guide to identify eConnect PDU 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.

MCM3 controller:
The unit has two Auxiliary Ports labeled as "AUX1" and "AUX2".
The unit has the Ethernet Port labeled as "10/100/1000 MB".
The unit has two USB connectors.

MCM2 controller:
The unit does not have "AUX1" and "AUX2" ports.
The unit has the Ethernet Port labelled as "10/100/1000 MB".
The unit has one USB connector.

MCM1 controller:
The unit does not have "AUX1" and "AUX2" ports.
The unit has the Ethernet Port is labelled as 10/100 MB only.
The unit has one USB connector.

Security Updates:

- Resolved an issue preventing a SecureArray Primary from enabling Radius Card Authentication on a Secondary PDU.
- Fixed messaging reported with Radius User & Card Authentication checks.
- Fixed a bug that blocked Radius User Test via CLI/SSH.
- Fixed a bug where a User's 'Group' affiliations was lost during Radius Authentication Checks.

New Features:

- SecureArray Primary now identifies a Secondary's Radius settings, if they exist, and will use them for Authentication when a user connects to the Secondary via the Primary's WebUI.
- Input Lines are shown on individual LCD screens.
- Improved functionality for editing User's via the CLI

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

Issues Addressed:

- Fixed an SNMP issue, not reflecting correct PDU IP address for primary unit at SNMP secureArraySystem "saPduTable"
- Fixed a SecureArray SNMP issue where Secondary Temp and Humidity values were switched.
- Resolved an issue with the SecureArray WebUI that would reset the Secondary PDU URL when the "logout" link is clicked.
- Fixed an issue, only found in SNMP, that caused a name change of Sensor Probe 2 to be applied to Sensor Probe 1.
- Addressed an SNMP issue where saInputTop, saCelsiusTemp and saSumAmps could be set to values other than '0' or '1'.
- Addressed bounds checking issues for user password modifications and creations via CLI
- Addressed bounds checking issues for username creation
- Improved bounds checking for PDU Store User Attributes
- addressed supported minimum values for Alarm Interval and Datalog Interval configuration items
- Addressed inconsistencies with audit entries for CLI based interactions.
- addressed presentation inconsistency for Alarm Interval and Datalog Interval configuration values.
- Electronic Access Control configurations on 36650-001 were missing a key entry. The system would not boot correctly without this entry. The system was updated to provide a default value for the missing entry.
- The "PDU Receptacle Change" setting in Notification Routing was incorrectly tied to the "PDU Configuration Change" setting.
- Improved functionality for editing Users via the CLI
- Addressed an issue where SNMP Sets to the OID tree .1.3.6.1.4.1.30932.1.10.1.1.8.1 were using the value for the Alarm Interval instead of the value requested in the SNMP Set operation.

Known Limitations:

- Emails and Traps for secondary alarms may contain metrics data that is up to a minute out-of-date.
- MCM2 and MCM3 units will report outlet level power factor, but this power factor is not acquired at an outlet level due to hardware limitations. The reading is acquired at the branch level and then copied to outlets associated with that branch.
- Any configuration changes made while running 4.1x.xxx, followed by returning to 4.4.253 are NOT preserved when 4.13.883 imports the data. Other than Outlet Groups, configuration changes made while running 4.4.253 ARE preserved

Upgrade Procedure:

- Obtain the firmware .zip file from http://www.chatsworth.com/support-and-downloads/downloads/software/
- Unzip the contents of the file pn-cpi-924-30531-001-20220221-svn22052.zip to a USB flash drive. There is one file which must be transferred to the root directory: cpipack3-20220221-svn22052.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 4.13.883

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.