eConnect Firmware Release Notes 5.3.825 (07/30/2021)

Applicability

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 your 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:

- The remote NTP server does not respond to mode 6 queries. https://scan.shadowserver.org/ntpversion/
- CVE-2016-7434: The remote NTP server is affected by a denial-of-service vulnerability
- Fixed an issue that allowed the 'Private RSA Key' to be exposed when 'WebUI: Settings - Network "View Certificate"' is chosen.

New Features:

- Using the WebUI, under the 'Settings' Tab – PDU, the 'SecureArray® Role' is now a Radio Button
    - o This feature allows for a single Role selection 'Primary', 'Alternate' or 'Secondary'.
- Support for SSH to log into the CLI has been added.
- The CLI now can create, update, and delete Outlet groups.

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 issue where 'Warn Min Humid' alerts were being sent as 'Warn Max Humid' alerts.
- Fixed an issue within SecureArray® where a 'Secondary' may drop off the array and never reconnect.
- Fixed an issue where WebUI Outlet Groups could be badly formatted when outlets are missing.
- Fixed an issue where SNMP: WALK operation times out after the "celsiusTemp" OID.
- Fixed an issue where the WebUI would show "Power Factor", a metric value not used by MCM2 & MCM3 eConnect Systems.
- Fixed an issue that resulted in a reboot if the IP address was changed via the LCD.
- Fixed an issue where a PDU, missing from a SecureArray, could impact the PDU list when doing an Upgrade to linked PDUs.
- Fixed an issue where errant network config changes would report a false positive.
- Fixed an error where changes to IPv6 Radius Card Enable/Disable errantly reported "Radius NAS Port".
- Fixed issues with Enable/Disable of EAC Locks.
- Fixed an issue where a SecureArray is randomly logged out of the WebUI.
- Fixed an issue within SecureArray where SNMP traps would have out of date data.
- Fixed an issue within SecureArray where outlet toggle commands were delayed.
- Fixed an issue with SNMP Trap #35's bit field (iso.org.dod.internet.private.enterprises.cpi.products.cpiPDU.metrics.alarms.recep1To32AlarmsMaxMap.0) was reporting an incorrect value.
- Fixed an issue within SecureArray where secondary units were not sending SNMP trap #35.
- Fixed a few CLI related issues:
    - o Changes to clarify errors associated with the handling of Outlet Groups.
    - o Re-Login accepted errant credentials without notifying the user that the login failed or, in some cases, might incorrectly report "Insufficient Rights".
    - o EAS Authorization was not working.
    - o Clean-up of an extraneous error message on login. The error seemed to indicate that there was an error when there wasn't.
    - o Clean-up of the "ldap-user test" command output. The command would provide a false failure message.
- Fixed a couple of issues within Bulk API:
    - o Outlet related calls might return errant data.
    - o Radius setting changes not applied.
    - o No error feedback for attempting to SET configuration items that do not exist.
    - o Changes to the LDAP settings were not taking effect until the system was rebooted.
    - o Metrics endpoints returning error Stack trace.
- Fixed several issues with Notifications.
    - o CLI Login success/failure or User 'Adding'/'Removal' or 'Modification' notifications.
    - o Duplicate notifications when changes are made to a user account.
    - o E-mail notifications not being sent for User Modifications.
    - o Secondary EAC Successful Card Scan notifications
    - o Entries in the log that were incorrectly ordered.
    - o Temperature Alert Emails would place a '0' after the decimal point.
    - o Cabinet Access – Disable Locks notifications were missing.

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:

- Obtain the firmware .zip file from http://www.chatsworth.com/support-and-downloads/downloads/software/
- Unzip the contents of the file pn-cpi-924-30543-001-20210722-svn21203.zip to a USB flash drive. There is one file which must be transferred to the root directory: pn-cpi-924-30543-001-20210722-svn21203.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 5.3.825

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.