eConnect Firmware Release Notes 4.4.211

Applicability

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

MCM3 controller:
The unit has two Auxiliary Ports labeled as "AUX1" and "AUX2".
The unit has the Ethernet Port labelled 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.

New Features:

- Radius – Radius functionality has been updated and improved.
  - o Radius User Authentication – Allows the system to validate access to the system through the Radius server. The Radius Server may reply to an authentication request with the Access Group using the "Filter-Id" element. Additionally, the system has added support for multiple Radius servers.
  - o Radius Card Authentication – Allows the system to validate Electronic Access Control cards against a Radius Server. The PDU will send the card ID as the user name and prepend "cpi" to the card ID as the password. The Radius Server must reply with the user name and the "Filter-Id" to allow access.
- Bulk Restful API – The PDU system now supports a Restful API. The Restful API enables Bulk configuration capability through the eConnect Web UI. It also enables applications such as Power IQ to perform bulk configuration changes and firmware upgrades (Note: Utilization of these capabilities will require release of Power IQ ver 6.3)
- Individual Cabinet Access Controls – The Electronic access control system now supports individual access to cabinets. Users can be also be cloned across cabinets.
- Custom HTTPS Certificates – Users can specify their own custom HTTPS certificates. The certificate file uploaded to the PDU should be a PEM file for SSL support (Should contain both the private key and the certificate).
- New Firmware File Upload – Users can select a firmware bin file located on the local PC rather than specifying a TFTP or HTTP location.
- New SecureArray Firmware Update Progress – The system will now report transfer/upgrade progress to the secondary PDUs on a SecureArray.
- Electronic Lock Error/Failure Feedback – Electronic Locks now will flash red when there is an bad read or when a user is denied access to the PDU.

US & Canada
+1-800-834-4969
Toronto, Ontario, Canada
+905-850-7770
chatsworth.com
techsupport@chatsworth.com

Latin America
+52-55-5203-7525
Toll Free within Mexico
01-800-01-7592
chatsworth.com.co

Europe
+44-1628-524-834
chatsworth.com

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

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

CHATSWORTH PRODUCTS

Bug Fixes:

- Addressed a bug where users could not change their password through the “My Profile” page.
- Addressed a bug in the SNMP system that prevented a walk through all the available OIDs.
- Addressed a bug on the status overview page that was not displaying the “Current usage & thresholds” meter properly.
- Addressed a bug with the outlet status showing “off” in the outlet setup table, even though it was “on”.
- Addressed a bug with Chrome preventing users from logging into the PDU.
- Addressed a bug with the user name being blank on the “My Profile” page for secondaries.
- Addressed a bug with the incorrect user name being displayed on the “My Profile” page for primaries.
- Addressed a bug with the “Clear” button on the login page not clearing the user name field.
- Updated the Unity MIB to include possible error codes and explanations for the trapInforErrorCode field.
- Addressed a bug with the outlets using the incorrect “Outlet Reset Delay” value. Outlets were using the next highest value.
- Addressed a bug with allowing special characters when editing a user name.
- Changed the “Select All” radio selection to a button.
- Addressed a bug with email subject lines coming from secondary PDUs on a SecureArray. The subject line should include the secondary cabinet or PDU.
- Addressed a bug with email sending email from an invalid email address rather than the one configured on the email page.
- Addressed a bug with email showing an invalid list of recipients.
- Addressed a bug with disabling email settings still sending email out to users.
- Addressed a bug with emails not containing any information in the body.

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-924-30531-001-20181127-svn18331.zip to a USB flash drive. There is one file which must be transferred to the root directory; cpipack3-20181127-svn18331.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 PDU new firmware version after the PDU reboots is the following:
  - Firmware version: 4.4.211

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 server 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, the system will not un-lock the cabinet.
2. The radius server servers 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 User-Name does not exist in the local PDU data store, then the system will not un-lock 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 server 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, the system will not un-lock the cabinet.
2. The radius server servers 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 User-Name does not exist in the local PDU data store, then the system will not un-lock 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.
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.