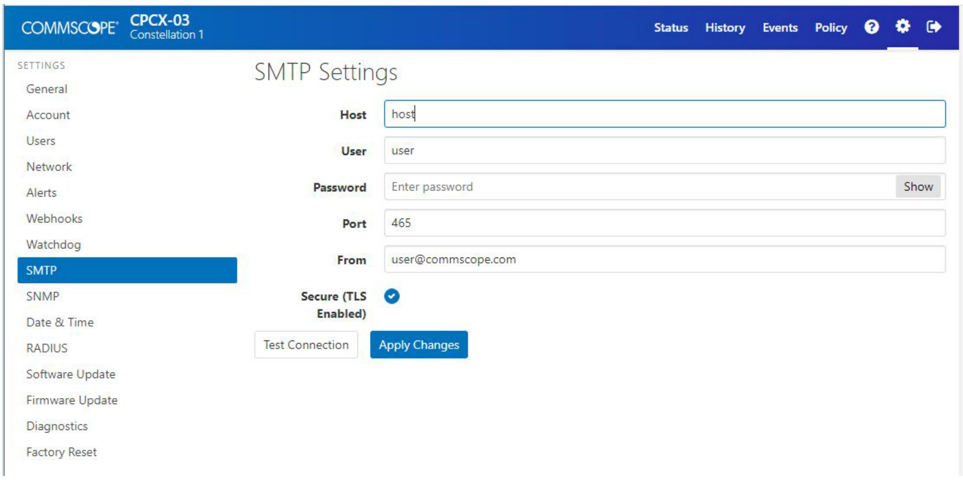
COMMSCOPE®

TC-96349-IP
Rev A, December 2022
commscope.com

User Manual

Constellation™ Management Software for Transmitters (CMX-MGT)



SMTP Settings

Host: host

User: user

Password: Enter password

Port: 465

From: user@commscope.com

Secure (TLS Enabled): ✓

SNMP Management Window

Content **Page**

(continued)

Content Page

ABOUT THIS DOCUMENT

REVISION HISTORY

This is the original version of this document.

TRADEMARKS

CommScope (logo), CommScope, and Constellation are trademarks of CommScope, Inc.

LIST OF ALL CONSTELLATION PRODUCTS

Table 1 lists all currently available Constellation products with catalog numbers and Material IDs (MIDs).

Table 1. Constellation Products

PRODUCT	CATALOG #	MID
Power Transmitter	CPCX-12	760254285
Management Module	CTX-MGT	760254286
Power Supply	CPM-3K	760254287
Transmitter Card	CTX-6	760254288
Multi-Chassis Synch Card	CMX-6	760254289
SAF D to L620P Cord	CABLE-PWR SAFD-L620P	760254290
C19 to L620P Cord	CABLE-PWR C19-L620P	760254291
C19 to 5-15P Cord	CABLE-PWR C19-515P	760254292
Power Transition Panel	CPT-PP-48C	760254293
Power Patch Cable	CTX-CBL-10	760254294
Powered Backplane	CPCB-1	760252855
Edge Enclosure	CPCE-1	760252854
TBD	HFPC	TBD
Power Supply Bay Cover	PM500-COVER	760254642

List of All Constellation Publications

Table 2 lists technical publications available for the Constellation system. These manuals can be accessed online using the QR code on the product packaging or by contacting the CommScope Support Center at https://www.commscope.com/SupportCenter

Table 2. Constellation Technical Publications

Publication Title	Publication #
Constellation Power Transition Panel (CPT-PP-48C) User Manual	TC-96343-IP
Constellation Transmitter Card (CTX-6) Data Sheet	TC-96344-IP
Constellation Power Supply (3PM-3K) Data Sheet	TC-96345-IP
Constellation Multi-Chassis Synch Card (CMX-6) Quick Start Guide	TC-96346-IP
Constellation Power Supply Bay Cover (PM500-COVER) Data Sheet	TC-96347-IP
Constellation Management Software for Transmitters User Manual	TC-96349-IP
Constellation Edge Enclosure (CPCE-1) With Powered Backplane (CPCB1) User Manual	TC-96350-IP
Constellation Best Practices Guide	TC-96351-IP
Constellation Power Transmitter (CPX-12) Quick Start Guide	TC-96354-IP

Contact Information

- To find out more about CommScope® products, visit us on the web at www.commscope.com
- For technical assistance, customer service, or to report any missing/damaged parts, visit us at http://www.commscope.com/SupportCenter

1 SOFTWARE OVERVIEW

This section lists the software and networking features of the management software for CommScope's Constellation Power Transmitter (CPCX-12) and related products including:

- Power Supply (CPM-3K)
- Transmitter Card (CTX-6)
- Multi-Chassis Synch Card (CMX-6)
- Power Transition Panel (CPT-PP-48C)
- Powered Backplane (CPCB-1), and
- Edge Enclosure (CPCE-1).

1.1 Revision History

The first software release for this software is version 1.0.0.

The latest software release is version 1.X.X (October 2022.) For software upgrade questions, contact http:///www.commscope.com/SupportCenter

1.2 Basic Network Capabilities

- 10/100 Bps Ethernet interface
- IPv4 static and DHCP addressing
- IPv6 link-local and Global addressing

1.3 Network Application Protocols

- HTTP
- HTTPS with self-signed certificate (since v1.4)
- mDNS
- SNMP v1 and v2c
- DNS
- NTP
- SMTP+TLS
- RADIUS

1.4 Software Features

- Control, management, and administration via web UI
- Local user authentication with user access roles
- Scheduled and hardware-triggered policy rules
- Local logging of power, fault, and events
- REST/JSON API
- 6 months of data retention
- CSV history export
- Remote software & firmware updates
- Push notification via HTTP/S webhooks
- Email notifications via SMTP+TLS
- SNMP v1 and v2c GET, SET, & traps
- RADIUS user authentication + RBAC

1.5 Basic Network Requirements

The Constellation Management Software for Transmitters requires the following network elements to be present at the installation site in order for the software to operate correctly:

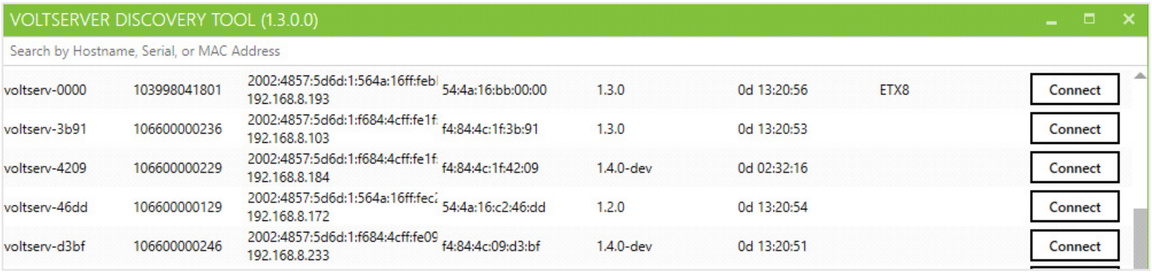
- IPv4 via DHCP (default) or static IPv4 address, or IPv6 via Ethernet,
- Access to some DNS server (set by DHCP option 6 in IPv4 DHCP mode),
- Access to some NTP server for accurate event time stamping and TLS certificate validation. The device uses a set of public NTP servers by default.

2 DEVICE NETWORK DISCOVERY

2.1 mDNS and AutoIP

In order to access the software, the device's network address must be known. Out of the box, the device uses DHCP to make it "plug-and-play" with most IP-based networks. There are several ways to discover the assigned IP address of a device, which are described here.

Network Discovery can be done via the Constellation Discovery Tool or "tool-less" via mDNS. The recommended approach is using the Constellation Discovery Tool, shown in Figure 1, for quick acquisition of all devices on the network, as shown below.



VOLTSERVER DISCOVERY TOOL (1.3.0.0)

Search by Hostname, Serial, or MAC Address

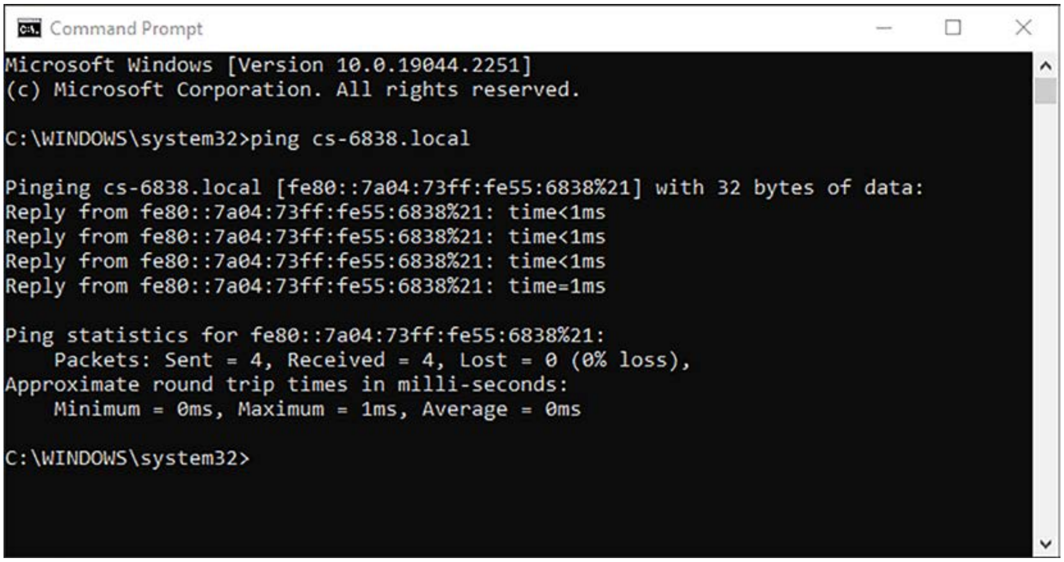
voltserv-0000	103998041801	2002:4857:5d6d:1:564a:16ff:feb 192.168.8.193	54:4a:16:bb:00:00	1.3.0	0d 13:20:56	ETX8	Connect
voltserv-3b91	106600000236	2002:4857:5d6d:1:f684:4cff:fe1f 192.168.8.103	f4:84:4c:1f:3b:91	1.3.0	0d 13:20:53		Connect
voltserv-4209	106600000229	2002:4857:5d6d:1:f684:4cff:fe1f 192.168.8.184	f4:84:4c:1f:42:09	1.4.0-dev	0d 02:32:16		Connect
voltserv-46dd	106600000129	2002:4857:5d6d:1:564a:16ff:fec 192.168.8.172	54:4a:16:c2:46:dd	1.2.0	0d 13:20:54		Connect
voltserv-d3bf	106600000246	2002:4857:5d6d:1:f684:4cff:fe09 192.168.8.233	f4:84:4c:09:d3:bf	1.4.0-dev	0d 13:20:51		Connect

Figure 1. Discovery Tool for Windows

2.2 IP Discovery via mDNS

If a device's hostname is already known, its IP address can be discovered via mDNS. The default hostname and MAC address are printed on the label on the side of each device.

A routable IP for the device can be discovered by running "`ping [hostname].local`" as shown in Figure 2.



Command Prompt

```
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping cs-6838.local

Pinging cs-6838.local [fe80::7a04:73ff:fe55:6838%21] with 32 bytes of data:
Reply from fe80::7a04:73ff:fe55:6838%21: time<1ms
Reply from fe80::7a04:73ff:fe55:6838%21: time<1ms
Reply from fe80::7a04:73ff:fe55:6838%21: time<1ms
Reply from fe80::7a04:73ff:fe55:6838%21: time=1ms

Ping statistics for fe80::7a04:73ff:fe55:6838%21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\WINDOWS\system32>
```

Figure 2. Ping Test

Note: By default, the device hostname is **`cs-`XXXX** where **XXXX** are the last 4 characters of the device's MAC address. For example, if the device's MAC ends with **`68:38`**, the default hostname will be **`cs-6838`**

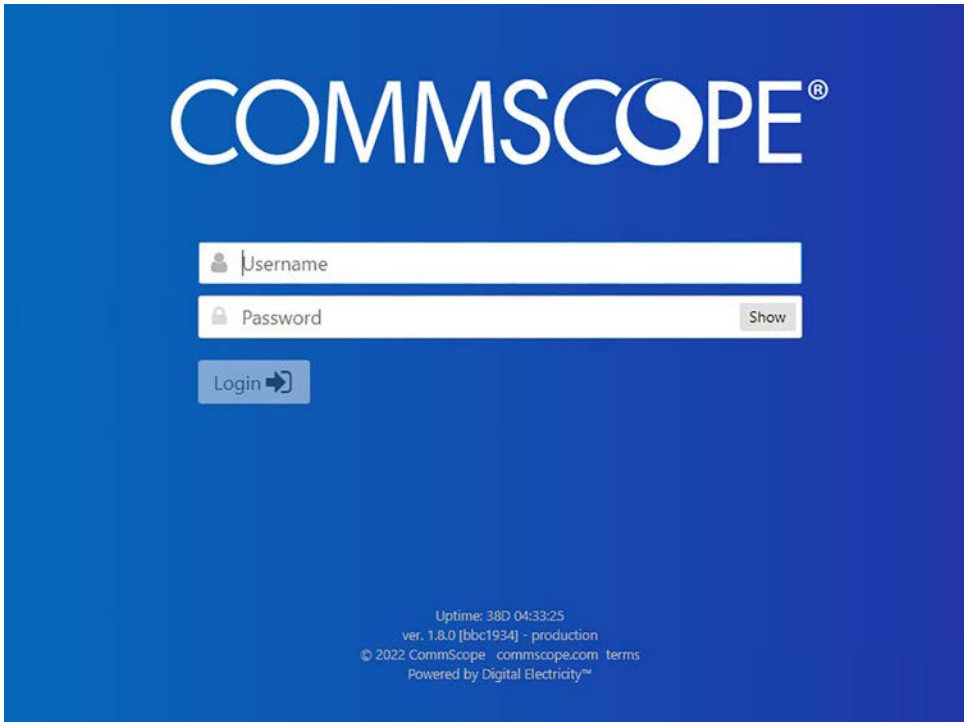
Test network connectivity to the device by opening a command prompt and running **`ping [hostname].local`**

If the device is connected directly from a laptop/PC to its Ethernet port (for example. “crossover cable”), the “**`ping [hostname].local`**” command will discover the device’s AutoIP (**`169.254.x.x`**) address.

3 ACCESS

3.1 Web UI Login

Most user interaction with the software will occur via the web interface hosted on the device. To access, open “**`http://constellation-XXXX.local`**” or “**`http://[ip address of the device]`**” in a supported browser. The login page, shown in Figure 3, will appear:



Uptime: 38D 04:33:25
ver. 1.8.0 [bbc1934] - production
© 2022 CommScope commscope.com terms
Powered by Digital Electricity™

Figure 3. Device Login Page

The factory-programmed password can be found on the unit label on the rear or side of the device. The default username is **`admin`**.

3.2 HTTPS Web Access

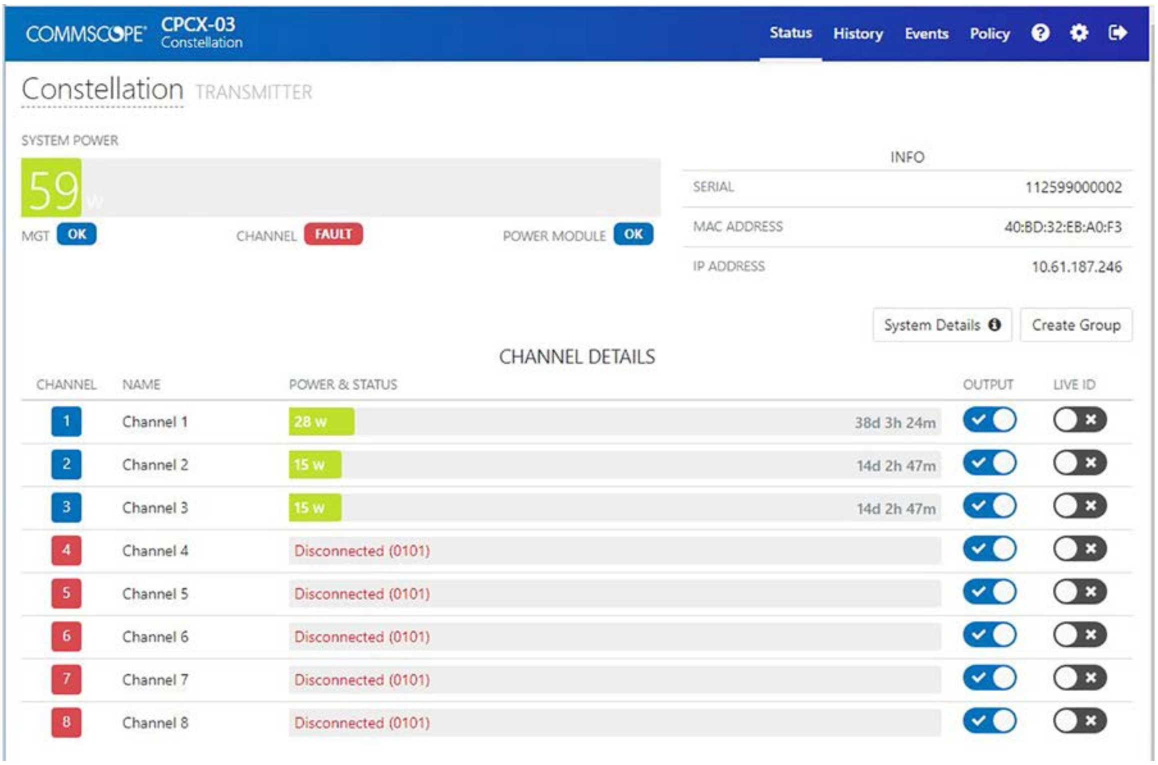
The device also provides access via HTTPS, using a self-signed certificate. Because it is not possible for browsers to trust a self-signed certificate, a warning will appear the first time the HTTPS page is opened.

4 STATUS

4.1 Status Page

All “real-time” device telemetry is displayed on the Status page, shown in Figure 4, including:

- Device name (editable)
- Total system power
- System faults
- Device serial, MAC, and IP addresses
- Channel number and editable channel name
- Channel power, status, faults
- Channel analog set point (lighting only)
- Channel uptime



Constellation TRANSMITTER

SYSTEM POWER

59 W

MGT OK CHANNEL FAULT POWER MODULE OK

INFO

SERIAL	112599000002
MAC ADDRESS	40:BD:32:EB:A0:F3
IP ADDRESS	10.61.187.246

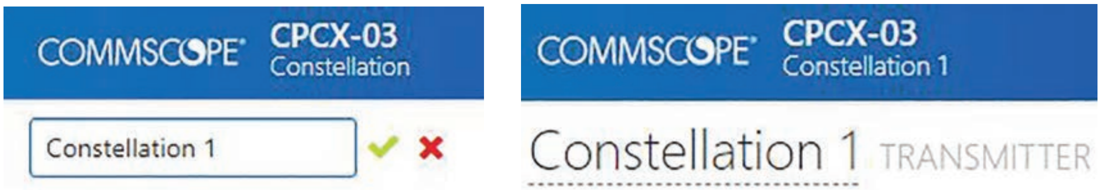
CHANNEL DETAILS

CHANNEL	NAME	POWER & STATUS		OUTPUT	LIVE ID
1	Channel 1	28 w	38d 3h 24m	✓	✗
2	Channel 2	15 w	14d 2h 47m	✓	✗
3	Channel 3	15 w	14d 2h 47m	✓	✗
4	Channel 4	Disconnected (0101)		✓	✗
5	Channel 5	Disconnected (0101)		✓	✗
6	Channel 6	Disconnected (0101)		✓	✗
7	Channel 7	Disconnected (0101)		✓	✗
8	Channel 8	Disconnected (0101)		✓	✗

Figure 4. Status Page

4.1.1 Device Name

The device name may be changed by clicking on it, as shown in Figure 5.



Constellation 1 ✓ ✗

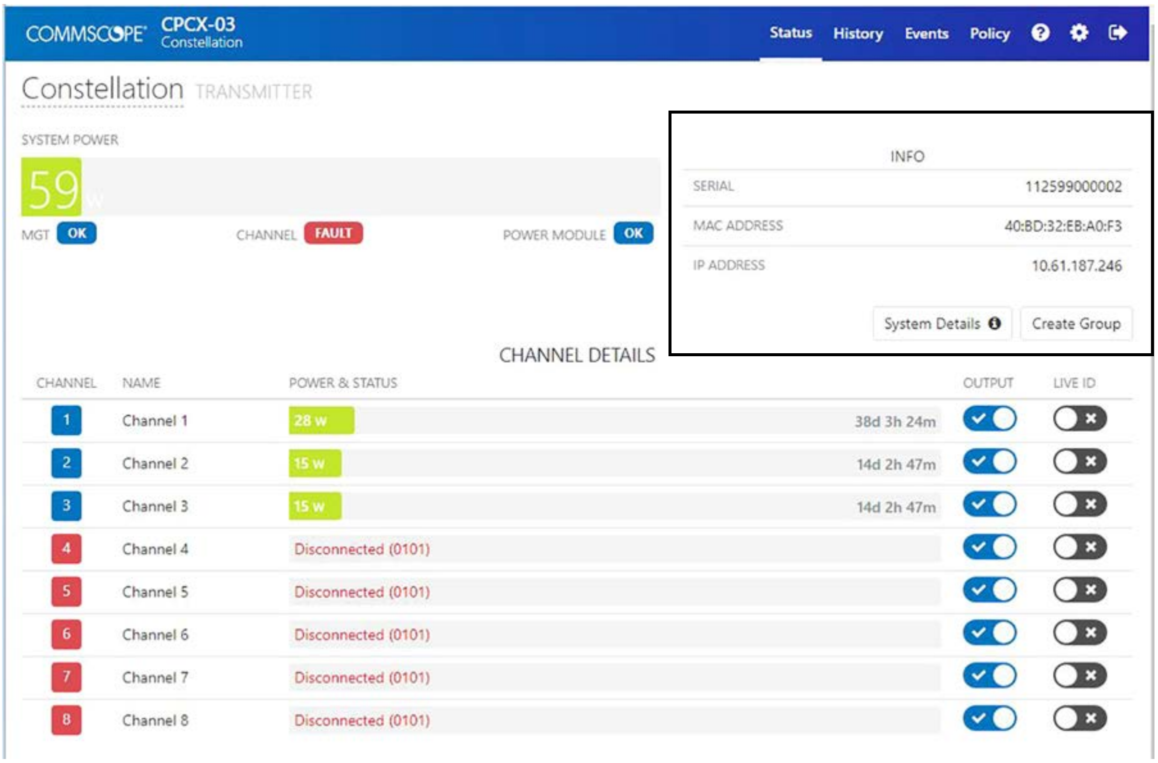
Constellation 1

28014-A

Figure 5. Changing the Device Name

4.1.2 Device Details

Network and device details are visible in the top right quadrant of the Status page, as shown in Figure 6.



SYSTEM POWER 59 W

MGT OK | CHANNEL FAULT | POWER MODULE OK

INFO

SERIAL	112599000002
MAC ADDRESS	40:BD:32:EB:A0:F3
IP ADDRESS	10.61.187.246

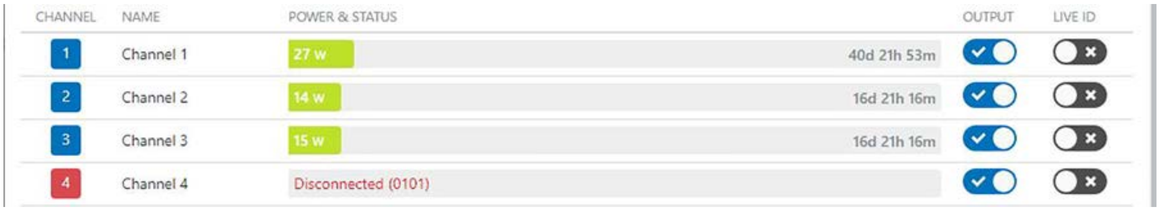
CHANNEL DETAILS

CHANNEL	NAME	POWER & STATUS		OUTPUT	LIVE ID
1	Channel 1	28 W	38d 3h 24m	✓	✗
2	Channel 2	15 W	14d 2h 47m	✓	✗
3	Channel 3	15 W	14d 2h 47m	✓	✗
4	Channel 4	Disconnected (0101)		✓	✗
5	Channel 5	Disconnected (0101)		✓	✗
6	Channel 6	Disconnected (0101)		✓	✗
7	Channel 7	Disconnected (0101)		✓	✗
8	Channel 8	Disconnected (0101)		✓	✗

Figure 6. Device Serial Number, MAC Address, and IP Address

4.1.3 Channel Status

Name, power, uptime, and output/live ID status can be seen for each channel, as shown in Figure 7. If this is a lighting product, output “level” control is also present.

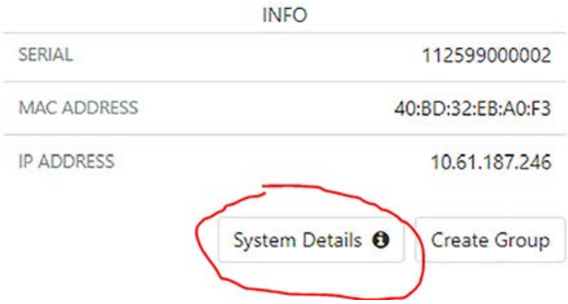


CHANNEL	NAME	POWER & STATUS		OUTPUT	LIVE ID
1	Channel 1	27 w	40d 21h 53m	✓	✗
2	Channel 2	14 w	16d 21h 16m	✓	✗
3	Channel 3	15 w	16d 21h 16m	✓	✗
4	Channel 4	Disconnected (0101)		✓	✗

Figure 7. Channel Status

4.1.4 System Details

Detailed status can be found by clicking the “System Details” button located on the Status page within the INFO box, as shown in Figure 8.

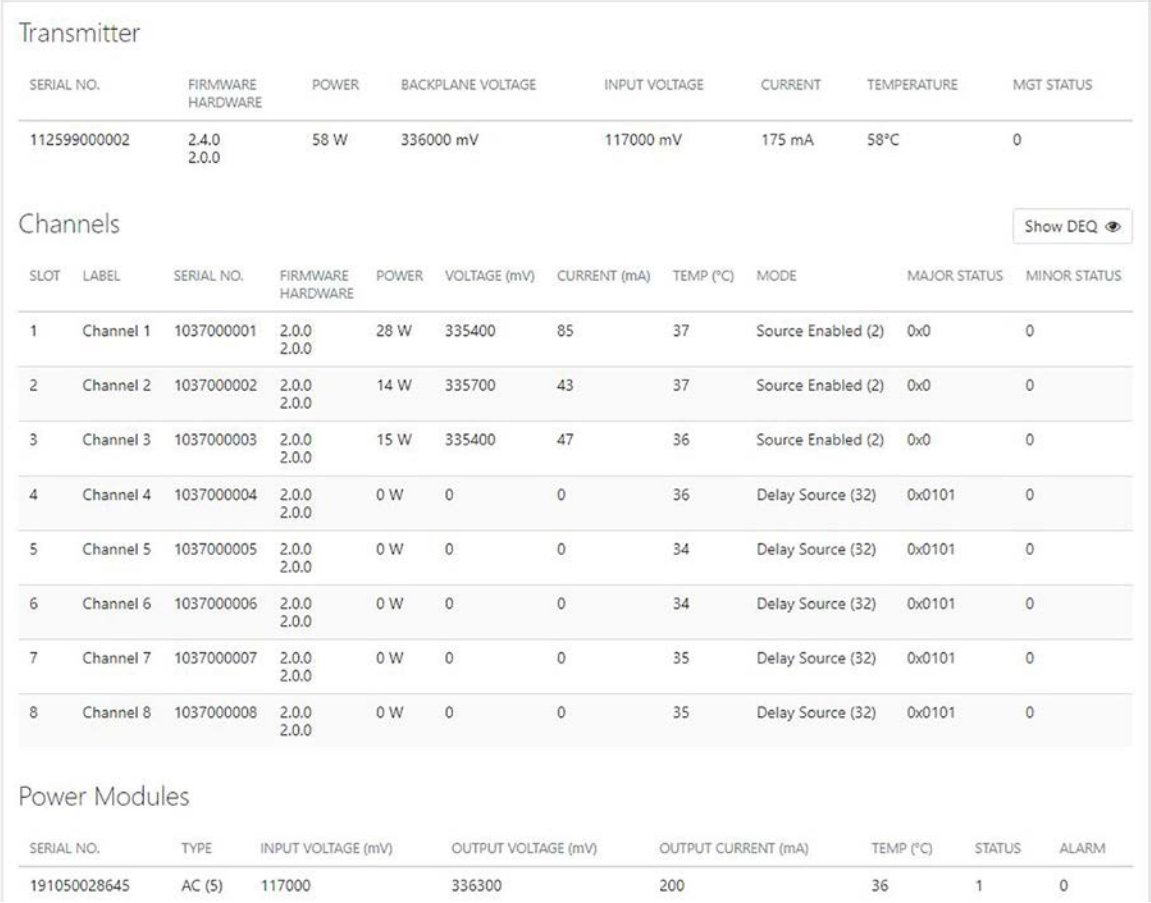


INFO

SERIAL	112599000002
MAC ADDRESS	40:BD:32:EB:A0:F3
IP ADDRESS	10.61.187.246

Figure 8. System Details Button

The system details display in a window such as shown in Figure 9.



Transmitter

SERIAL NO.	FIRMWARE HARDWARE	POWER	BACKPLANE VOLTAGE	INPUT VOLTAGE	CURRENT	TEMPERATURE	MGT STATUS
112599000002	2.4.0 2.0.0	58 W	336000 mV	117000 mV	175 mA	58°C	0

Channels

SLOT	LABEL	SERIAL NO.	FIRMWARE HARDWARE	POWER	VOLTAGE (mV)	CURRENT (mA)	TEMP (°C)	MODE	MAJOR STATUS	MINOR STATUS
1	Channel 1	1037000001	2.0.0 2.0.0	28 W	335400	85	37	Source Enabled (2)	0x0	0
2	Channel 2	1037000002	2.0.0 2.0.0	14 W	335700	43	37	Source Enabled (2)	0x0	0
3	Channel 3	1037000003	2.0.0 2.0.0	15 W	335400	47	36	Source Enabled (2)	0x0	0
4	Channel 4	1037000004	2.0.0 2.0.0	0 W	0	0	36	Delay Source (32)	0x0101	0
5	Channel 5	1037000005	2.0.0 2.0.0	0 W	0	0	34	Delay Source (32)	0x0101	0
6	Channel 6	1037000006	2.0.0 2.0.0	0 W	0	0	34	Delay Source (32)	0x0101	0
7	Channel 7	1037000007	2.0.0 2.0.0	0 W	0	0	35	Delay Source (32)	0x0101	0
8	Channel 8	1037000008	2.0.0 2.0.0	0 W	0	0	35	Delay Source (32)	0x0101	0

Power Modules

SERIAL NO.	TYPE	INPUT VOLTAGE (mV)	OUTPUT VOLTAGE (mV)	OUTPUT CURRENT (mA)	TEMP (°C)	STATUS	ALARM
191050028645	AC (5)	117000	336300	200	36	1	0

Figure 9. System Details Window

This information may be useful for troubleshooting. At the top of the System Details table, there are three buttons:

4.1.4.1 Upload Button

Information about this device will be upload to CommScope and notify a CommScope Support technician.

4.1.4.2 Copy Button

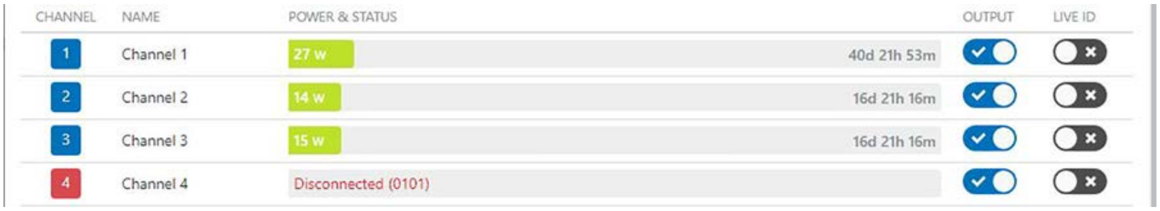
System information is copied to the clipboard, or a dialog is opened to be manually copied and pasted.

4.1.4.3 Email Button

The user’s default mail handler will open to compose a new email message to CommScope Support with system information automatically copied in the body of the email.

4.1.5 Faults

System status including MGT, channel, and power module faults are displayed within the Power & Status bar as shown for the "Disconected (010)" message in Figure 10.

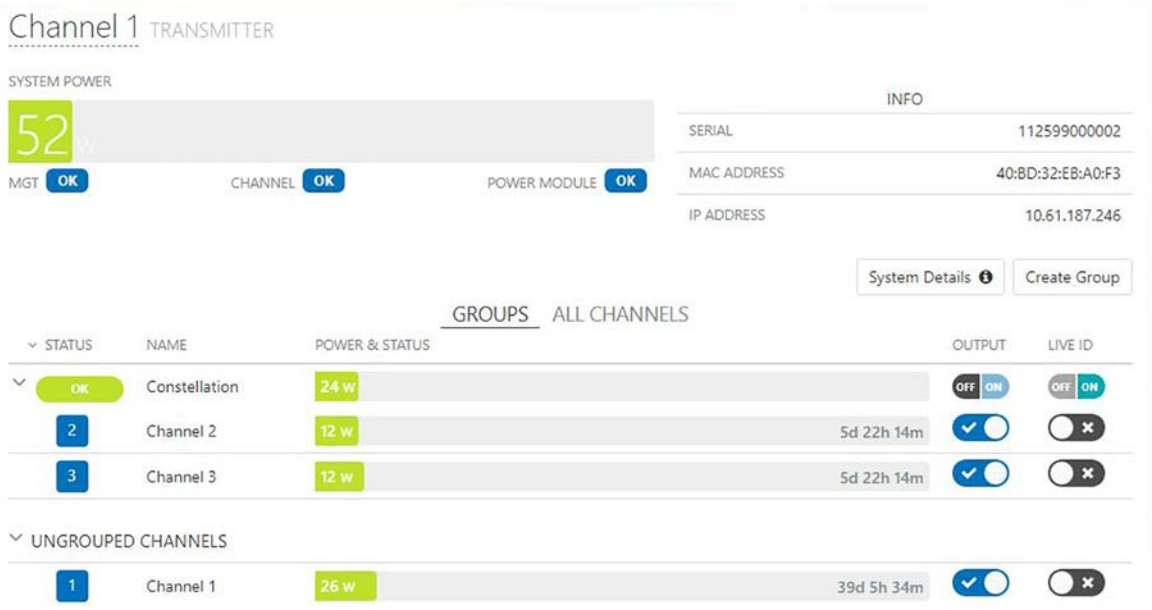


CHANNEL	NAME	POWER & STATUS		OUTPUT	LIVE ID
1	Channel 1	27 w	40d 21h 53m	✓	✗
2	Channel 2	14 w	16d 21h 16m	✓	✗
3	Channel 3	15 w	16d 21h 16m	✓	✗
4	Channel 4	Disconnected (0101)		✓	✗

Figure 10. Fault Displayed in Power Status Column

4.2 Channel Grouping

Channel grouping is used when more than one channel is connected to the same receiver. Figure 11 shows a channel group composed of Channel 2 and Channel 3.



Channel 1 TRANSMITTER

SYSTEM POWER

52 W

MGT OK CHANNEL OK POWER MODULE OK

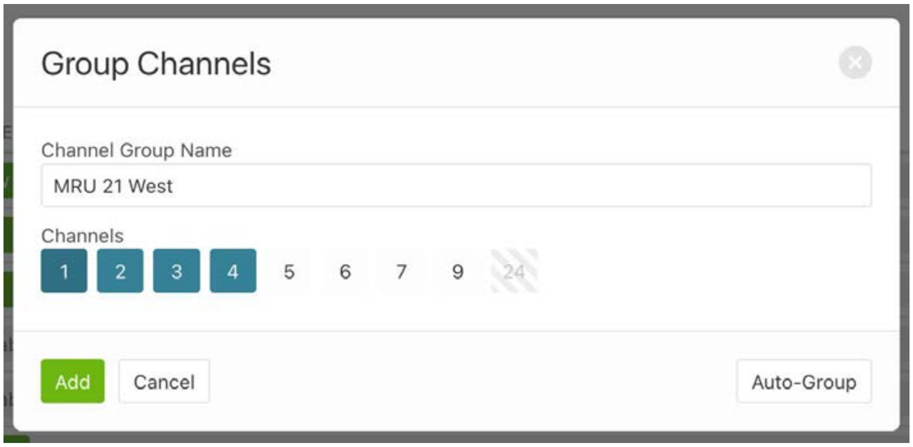
INFO	
SERIAL	112599000002
MAC ADDRESS	40:BD:32:EB:A0:F3
IP ADDRESS	10.61.187.246

STATUS	NAME	POWER & STATUS		OUTPUT	LIVE ID
OK	Constellation	24 w		OFF ON	OFF ON
2	Channel 2	12 w	5d 22h 14m	✓	✗
3	Channel 3	12 w	5d 22h 14m	✓	✗
UNGROUPED CHANNELS					
1	Channel 1	26 w	39d 5h 34m	✓	✗

Figure 11. Channel Group

4.2.1 Creating a Channel Group

Channel groups can be manually created from the status page. Click the "Create Group" button in the upper right of the window. A dialog will appear (Figure 12).



Group Channels

Channel Group Name: MRU 21 West

Channels: 1 2 3 4 (selected) 5 6 7 9 24

Figure 12. Channel Group Dialog

Give the group a name (usually name of the load or location), and select which channels are in the group. Only group channels that are connected to the same DE receiver.

4.2.2 Possible Channel Group Statuses

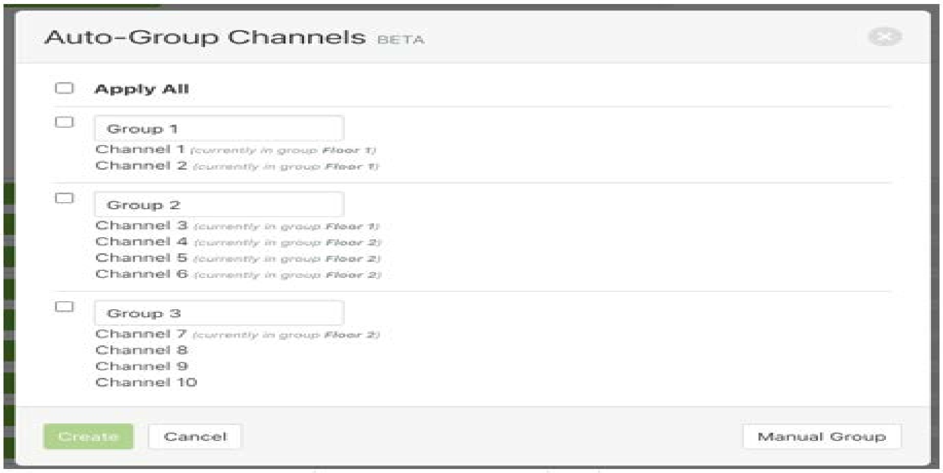
Table 3 shows the possible statuses for a channel group.

Table 3. Constellation Channel Group Statuses

STATUS	DESCRIPTION
OK	All channels in the group are delivering power to the load
Degraded	At least one channel in the group is disconnected or faulted, but other channels continue to deliver power
Outage	No channels in the group are delivering power
Mixed	One or more channels in the group are turned off but all other channels are delivering power

4.2.3 Automatic Grouping

Automatic grouping (Auto-Grouping) can attempt to infer channel groups based on channel slot and load information as shown in the example in Figure 13. Note auto-grouping only works for enabled (connected, not faulted) channels. The auto group feature provides a list of suggested groupings. The user may choose which groups to create from the auto-group suggestion



Auto-Group Channels BETA

□ **Apply All**

□ Group 1
Channel 1 *(currently in group Floor 1)*
Channel 2 *(currently in group Floor 1)*

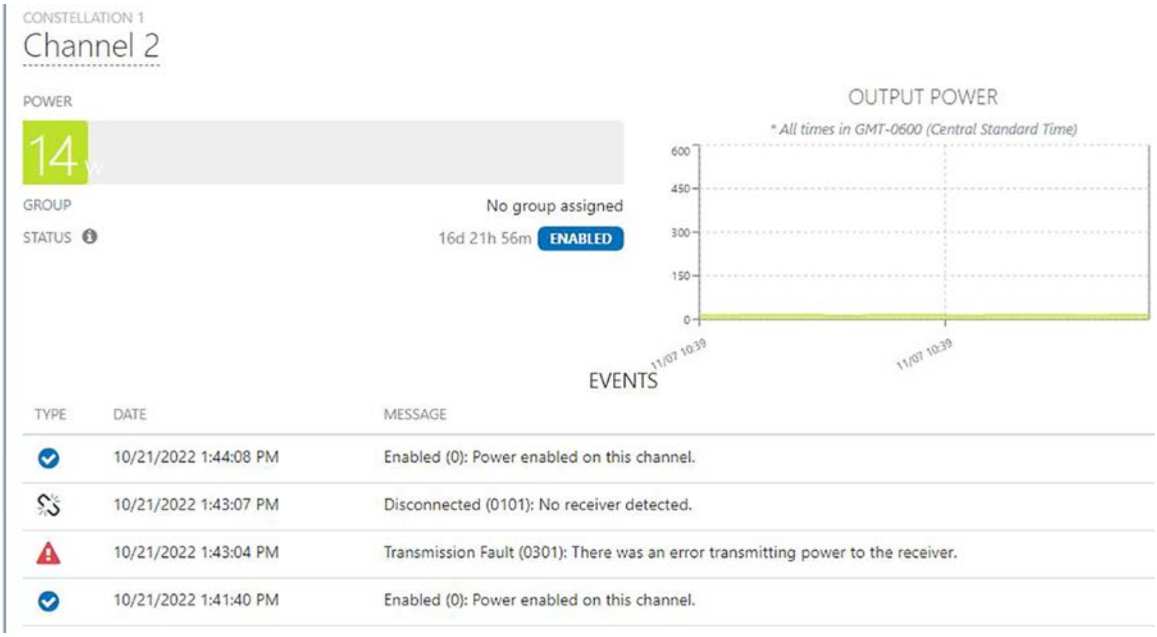
□ Group 2
Channel 3 *(currently in group Floor 1)*
Channel 4 *(currently in group Floor 2)*
Channel 5 *(currently in group Floor 2)*
Channel 6 *(currently in group Floor 2)*

□ Group 3
Channel 7 *(currently in group Floor 2)*
Channel 8
Channel 9
Channel 10

Figure 13. Auto Grouping

4.2.4 Obtaining Channel Details

Clicking on any channel name or number from the Status page will show the channel detail page shown in Figure 14. Recent events, power data, and present channel status can be viewed on this page. The channel name may be edited by clicking on the name in the upper left, in the same manner as editing the transmitter name on the main page.



CONSTELLATION 1
Channel 2

POWER
14 W

GROUP: No group assigned
STATUS: 16d 21h 56m ENABLED

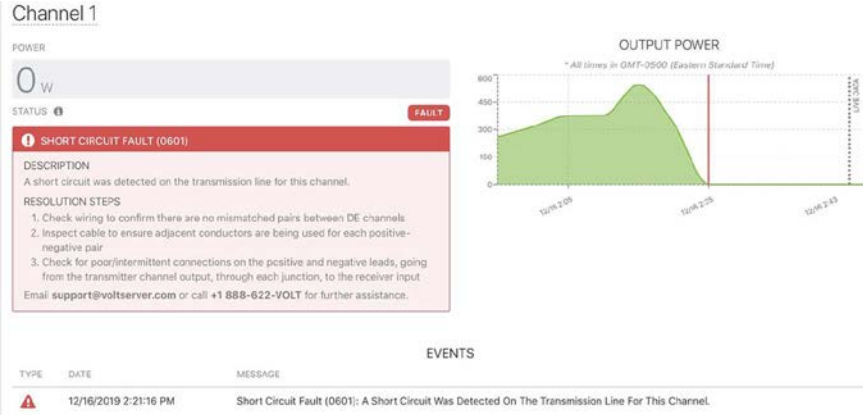
EVENTS

TYPE	DATE	MESSAGE
✓	10/21/2022 1:44:08 PM	Enabled (0): Power enabled on this channel.
	10/21/2022 1:43:07 PM	Disconnected (0101): No receiver detected.
⚠	10/21/2022 1:43:04 PM	Transmission Fault (0301): There was an error transmitting power to the receiver.
✓	10/21/2022 1:41:40 PM	Enabled (0): Power enabled on this channel.

Figure 14. Channel Details Page

4.2.5 Channel Fault Details

If the Channel Details page is open and the channel is faulted, fault information and troubleshooting steps will be displayed as shown in Figure 15:



Channel 1

POWER

0 W

STATUS

FAULT

SHORT CIRCUIT FAULT (0601)

DESCRIPTION

A short circuit was detected on the transmission line for this channel.

RESOLUTION STEPS

1. Check wiring to confirm there are no mismatched pairs between DE channels
2. Inspect cable to ensure adjacent conductors are being used for each positive-negative pair
3. Check for poor/intermittent connections on the positive and negative leads, going from the transmitter channel output, through each junction, to the receiver input

Email **support@voltserver.com** or call **+1 888-622-VOLT** for further assistance.

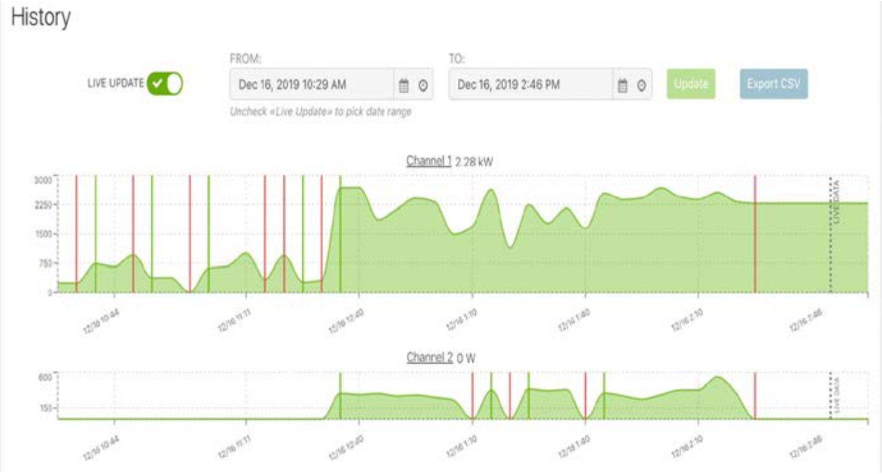
EVENTS

TYPE	DATE	MESSAGE
⚠	12/16/2019 2:21:16 PM	Short Circuit Fault (0601): A Short Circuit Was Detected On The Transmission Line For This Channel.

Figure 15. Channel Fault Details

5 HISTORY

All device history is stored for a maximum of 6 months on local persistent storage. History is retained through reboots, power loss, software updates, and so on. Events older than the retention period are periodically purged to preserve storage space The history page displays power over time charts for the unit and each channel. See the example in Figure 16.



History

LIVE UPDATE ☑

FROM: Dec 16, 2019 10:29 AM

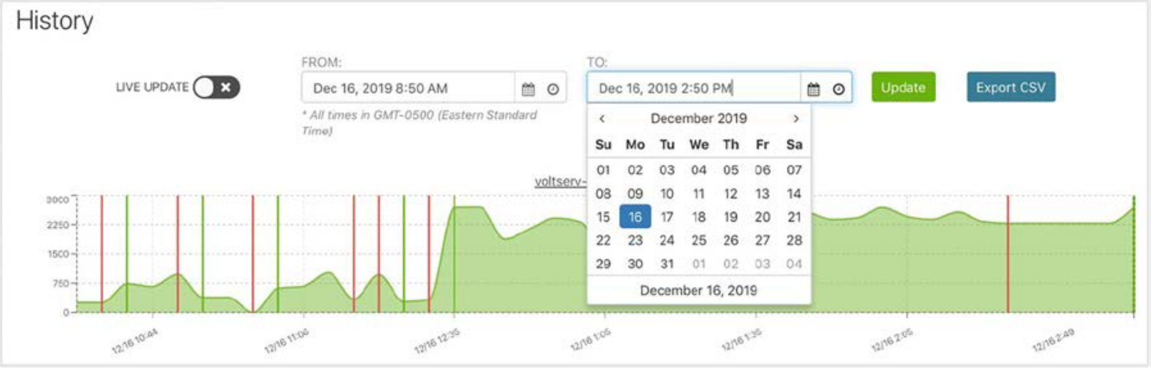
TO: Dec 16, 2019 2:46 PM

Uncheck «Live Update» to pick date range

Figure 16. History Page

5.1 Choosing a History Date Range

When viewing the History and Events pages, by default, the most recent data is displayed and will live-update. To view older history, uncheck “LIVE UPDATE,” then choose the desired “FROM” and “TO” date range, then click “Update.”



History

LIVE UPDATE ☒

FROM: Dec 16, 2019 8:50 AM

* All times in GMT-0500 (Eastern Standard Time)

TO: Dec 16, 2019 2:50 PM

December 2019

Su	Mo	Tu	We	Th	Fr	Sa
01	02	03	04	05	06	07
08	09	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	01	02	03	04

December 16, 2019

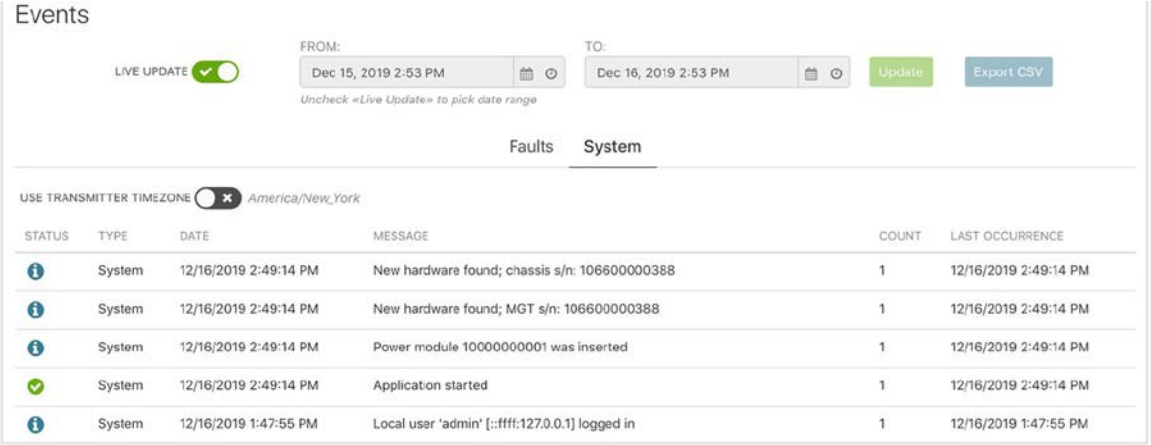
Figure 17. History Date Range

5.2 FCSV Export

After selecting a date range, you may click the “Export CSV” button to download data in a format that can be manipulated in Excel. Note that exports are limited to 500 rows for each data type.

6 EVENTS

The Events page displays a list of channel faults and system events.



Events

LIVE UPDATE ☑

FROM: Dec 15, 2019 2:53 PM

TO: Dec 16, 2019 2:53 PM

Uncheck «Live Update» to pick date range

USE TRANSMITTER TIMEZONE ☒ America/New_York

STATUS	TYPE	DATE	MESSAGE	COUNT	LAST OCCURRENCE
ℹ	System	12/16/2019 2:49:14 PM	New hardware found; chassis s/n: 106600000388	1	12/16/2019 2:49:14 PM
ℹ	System	12/16/2019 2:49:14 PM	New hardware found; MGT s/n: 106600000388	1	12/16/2019 2:49:14 PM
ℹ	System	12/16/2019 2:49:14 PM	Power module 10000000001 was inserted	1	12/16/2019 2:49:14 PM
✓	System	12/16/2019 2:49:14 PM	Application started	1	12/16/2019 2:49:14 PM
ℹ	System	12/16/2019 1:47:55 PM	Local user 'admin' [::ffff:127.0.0.1] logged in	1	12/16/2019 1:47:55 PM

Figure 18. Events Page

The application records the following events:

- Channel faults and output toggle events
- Channel group faults and output toggle events (non-lighting products only)
- System faults
- Network events (IP address assigned/ changed)
- SNMP traps sent
- Software reboot
- Factory reset
- Power module inserted or changed
- Software update started, completed, and failed
- Firmware update started, completed, and failed
- User log-in/ log-out

7 POLICY

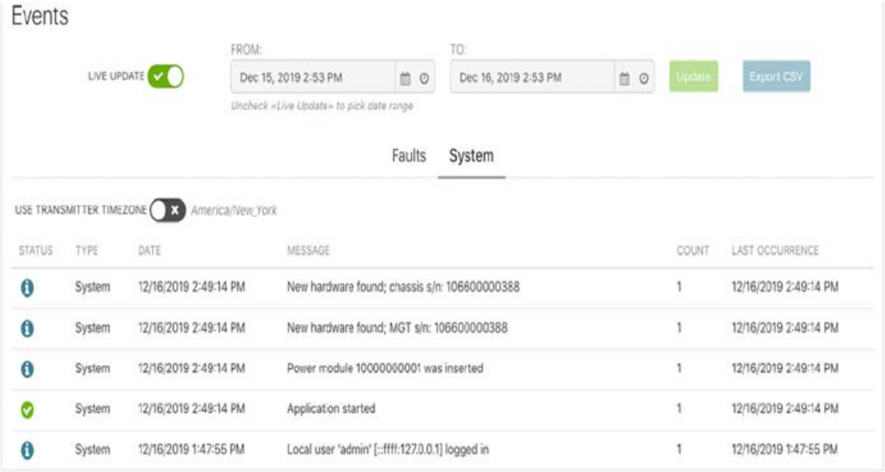
Policies may be created to instruct the device to perform actions based on input events or a time schedule.

7.1 Available Policy Actions

- Fade channel output (lighting only)
- Set channel group output (non-lighting only)
- Log system event message
- Send email
- Delay (pause between actions)

7.2 Policy Examples

Figure 19, Figure 20, and Figure 21 show examples of policies.



Events

LIVE UPDATE ✓ | FROM: Dec 15, 2019 2:53 PM | TO: Dec 16, 2019 2:53 PM | Update | Export CSV

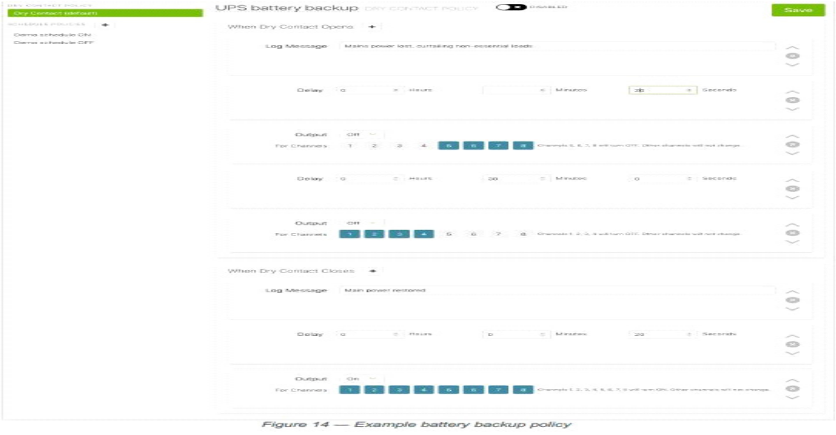
Uncheck «Live Update» to pick date range

Faults | System

USE TRANSMITTER TIMEZONE ✗ America/New_York

STATUS	TYPE	DATE	MESSAGE	COUNT	LAST OCCURRENCE
ℹ	System	12/16/2019 2:49:14 PM	New hardware found; chassis s/n: 106600000388	1	12/16/2019 2:49:14 PM
ℹ	System	12/16/2019 2:49:14 PM	New hardware found; MGT s/n: 106600000388	1	12/16/2019 2:49:14 PM
ℹ	System	12/16/2019 2:49:14 PM	Power module 10000000001 was inserted	1	12/16/2019 2:49:14 PM
✓	System	12/16/2019 2:49:14 PM	Application started	1	12/16/2019 2:49:14 PM
ℹ	System	12/16/2019 1:47:55 PM	Local user 'admin' [::ffff:127.0.0.1] logged in	1	12/16/2019 1:47:55 PM

Figure 19. Scheduled Policy With Fading (Lighting Only)



UPS battery backup DRY CONTACT POLICY

When Dry Contact Opens +

Log Message: Mains power lost, curtailing non-essential loads

Delay: 0 Hours, Minutes, 20 Seconds

Output: Off
For Channels: 1 2 3 4 **5 6 7 8** Channels 5, 6, 7, 8 will turn OFF. Other channels will not change.

Delay: 0 Hours, 30 Minutes, 0 Seconds

Output: Off
For Channels: **1 2 3 4** 5 6 7 8 Channels 1, 2, 3, 4 will turn OFF. Other channels will not change.

When Dry Contact Closes +

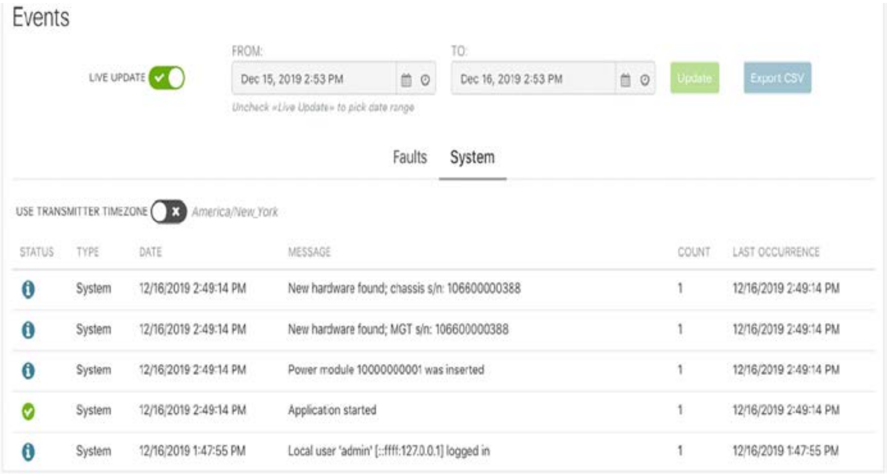
Log Message: Main power restored

Delay: 0 Hours, 0 Minutes, 20 Seconds

Output: On
For Channels: **1 2 3 4 5 6 7 8** Channels 1, 2, 3, 4, 5, 6, 7, 8 will turn ON. Other channels will not change.

Figure 14 — Example battery backup policy

Figure 20. Scheduled Action



FROM: Dec 15, 2019 2:53 PM

TO: Dec 16, 2019 2:53 PM

Uncheck «Live Update» to pick date range

USE TRANSMITTER TIMEZONE *America/New_York*

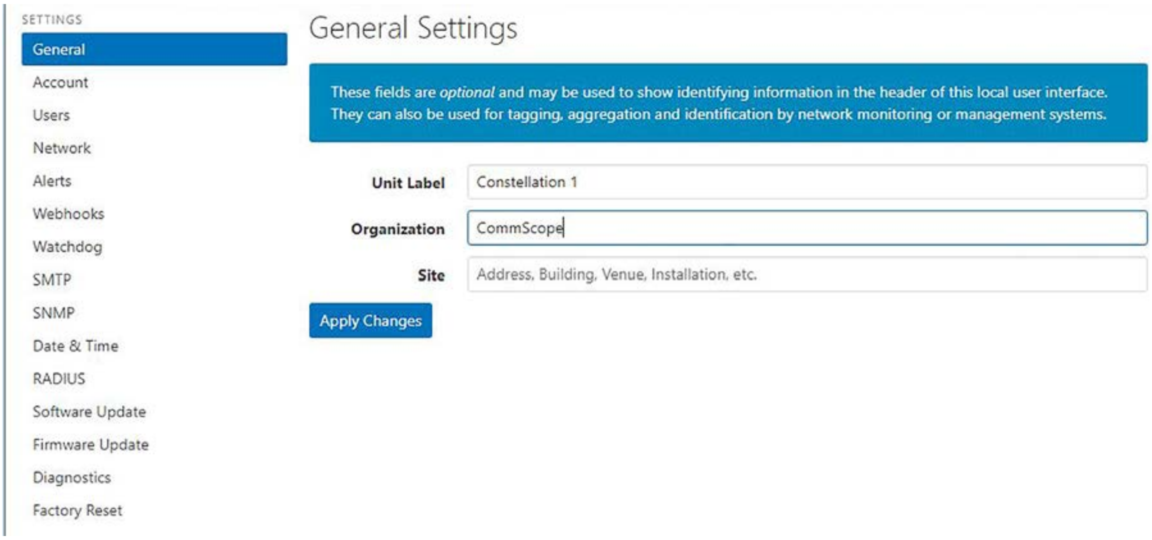
STATUS	TYPE	DATE	MESSAGE	COUNT	LAST OCCURRENCE
ⓘ	System	12/16/2019 2:49:14 PM	New hardware found; chassis s/n: 106600000388	1	12/16/2019 2:49:14 PM
ⓘ	System	12/16/2019 2:49:14 PM	New hardware found; MGT s/n: 106600000388	1	12/16/2019 2:49:14 PM
ⓘ	System	12/16/2019 2:49:14 PM	Power module 1000000001 was inserted	1	12/16/2019 2:49:14 PM
✓	System	12/16/2019 2:49:14 PM	Application started	1	12/16/2019 2:49:14 PM
ⓘ	System	12/16/2019 1:47:55 PM	Local user 'admin' [::ffff:127.0.0.1] logged in	1	12/16/2019 1:47:55 PM

Figure 21. UPS Battery Backup Policy

8 SETTINGS

8.1 General

The device can be configured to display a non-default name for labeling purposes, as shown in the example in Figure 22. There are three configurable fields: **label**, **organization**, and **site**. Each field can be used as grouping or other logical identifiers and will be displayed in the web page's navigation bar.



These fields are *optional* and may be used to show identifying information in the header of this local user interface. They can also be used for tagging, aggregation and identification by network monitoring or management systems.

Unit Label Constellation 1

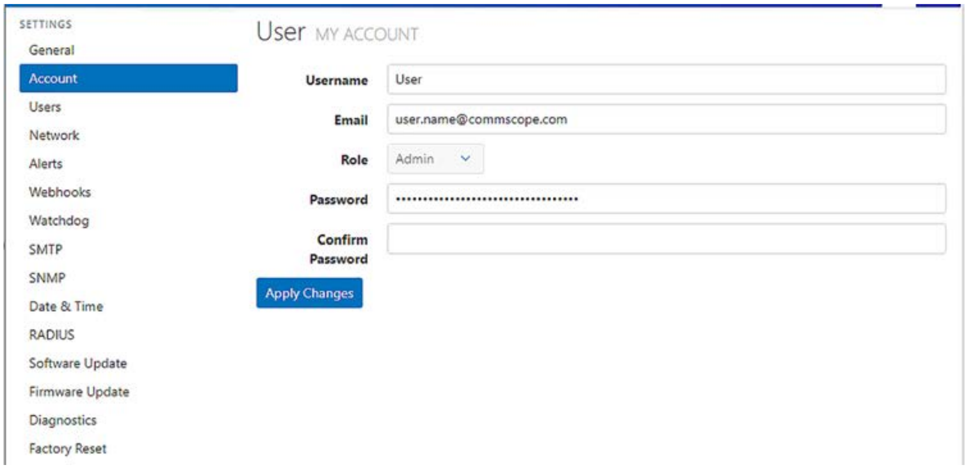
Organization CommScope

Site Address, Building, Venue, Installation, etc.

Figure 22. General Settings

8.2 Account

The Accounts page, shown in Figure 22, is used to add or edit a User and assign a User role. This page is available to the system administrator for every user and is available to a non-administrative user for the associated account only.



User MY ACCOUNT

Username: User

Email: user.name@commscope.com

Role: Admin

Password: ••••••••••••••••••••••••••••••••••

Confirm Password:

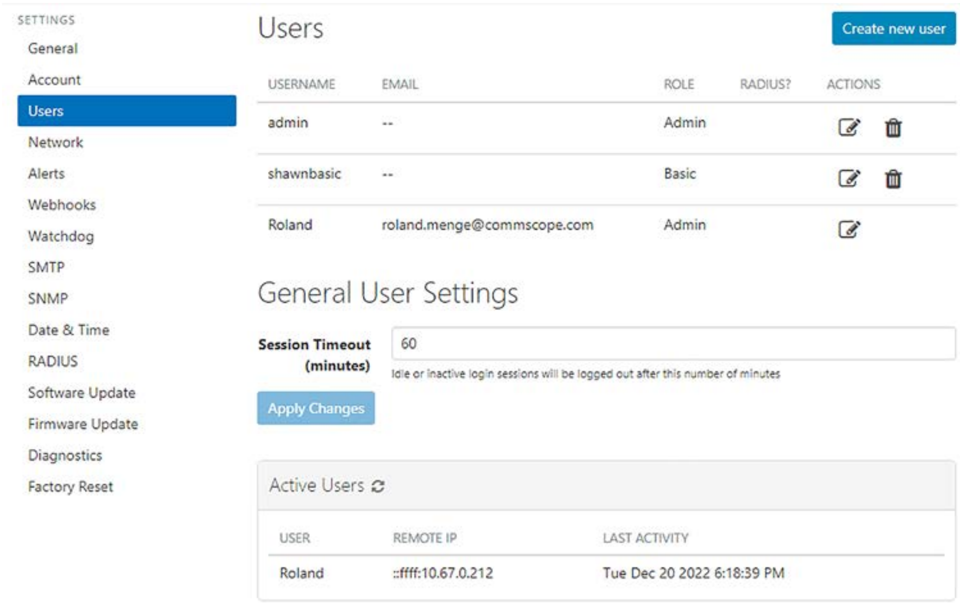
Figure 23. Account Page

8.3 Users

An administrator may create, view, edit, or delete local user accounts. Multiple accounts may be used either for auditing purposes or to provide multiple access levels to the device.

The “session timeout” may also be configured. This controls how long an idle session remains logged in. The default value is 60 minutes. The minimum session timeout is 5 minutes.

The Users Settings page, shown in Figure 24, also displays active user sessions including remote IP address and last activity.



Users

USERNAME	EMAIL	ROLE	RADIUS?	ACTIONS
admin	--	Admin		
shawnbasic	--	Basic		
Roland	roland.menge@commscope.com	Admin		

General User Settings

Session Timeout (minutes): 60

Idle or inactive login sessions will be logged out after this number of minutes

Active Users

USER	REMOTE IP	LAST ACTIVITY
Roland	::ffff:10.67.0.212	Tue Dec 20 2022 6:18:39 PM

Figure 24. Users Settings Page Showing Three Local Users and a RADIUS User

8.3.1 User Access Control

Multiple users may be created with one of the following access roles: **admin**, **operator** and **basic**. The following matrix outlines what software capabilities are allowed for each role:.

Table 4. User Access Control

FEATURE	ADMIN	OPERATOR	BASIC
View status page (real time inventory)	x	x	x
View channel status	x	x	x
View device history	x	x	x
View fault events	x	x	x
View system events	x	x	
Change device name	x	x	
Change channel name	x	x	
Change channel outputs	x	x	
Toggle channel live ID	x	x	
View policies	x	x	x
Create, edit policies	x	x	
Enable or disable policies			
Change own password	x	x	x
Change own email	x	x	x

Table 4. User Access Control

FEATURE	ADMIN	OPERATOR	BASIC
View users / sessions	x	x	
Create user	x		
Edit user	x		
Create / edit alerts	x	x	
Change / view webhook settings	x		
Create / view hostname	x		
Change / view network settings	x		
Change / view NTP settings	x		
Change / view SMTP settings	x		
Change / view SNMP settings	x		
Change / view RADIUS settings	x		
Change / view SSH settings	x		
Change / view fault handling settings	x		
Change / view lighting settings	x		
Change diagnostic reporting	x		
Perform factory data reset			
View software version			
Perform software update			
View firmware version			
Perform firmware update			
Create / edit / delete a channel group			
View channel group status			
Toggle channel group outputs			
Toggle channel group live ID			
Change external watchdog settings			
Pet external watchdog			

8.3.2 External Authentication and Access Control (RADIUS)

An administrator may configure the device to delegate AAC to a local RADIUS server, using the “PAP” or “CHAP” authentication. When RADIUS is enabled, all user logins that do not match a local account will be sent to the RADIUS server. If the server gives an “Access-Accept” response, the requesting user will be logged in.

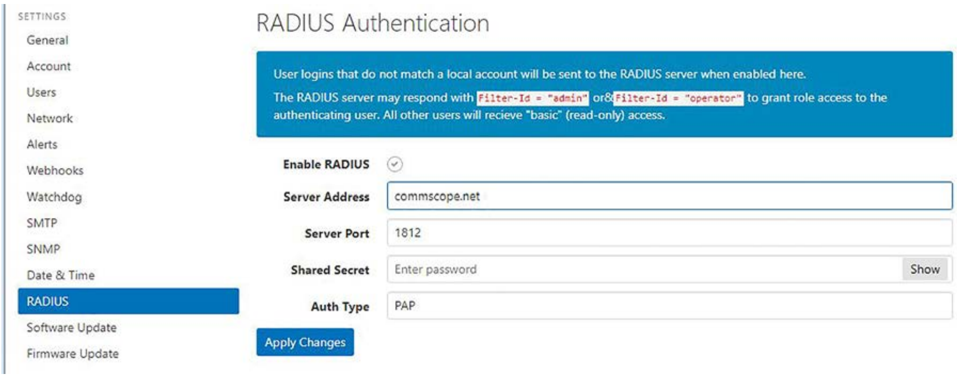
If the RADIUS server provides a “Session-Timeout” attribute in the “Access-Accept” response, the device will automatically re-authenticate the user’s credentials after that many seconds. If no

“Session-Timeout” attribute is given, the device will re-authenticate with the RADIUS server every 5 minutes while the user is active.

To grant the Operator or Admin role to a RADIUS user, add the “Filter-Id” attribute with a value of “`admin`” or “`operator`”. If no Filter-Id is attribute is sent, the user is granted “Basic” access.

Prior to v1.8.0, devices used the “Cisco-AVPair” VSA to designate role access. This method should be considered deprecated in favor of the standard Filter-Id attribute starting in v1.8.0.

CHAP authentication was added in v1.8.0.



RADIUS Authentication

User logins that do not match a local account will be sent to the RADIUS server when enabled here.

The RADIUS server may respond with `Filter-Id = "admin"` or&`Filter-Id = "operator"` to grant role access to the authenticating user. All other users will recieve "basic" (read-only) access.

Enable RADIUS ✓

Server Address: commscope.net

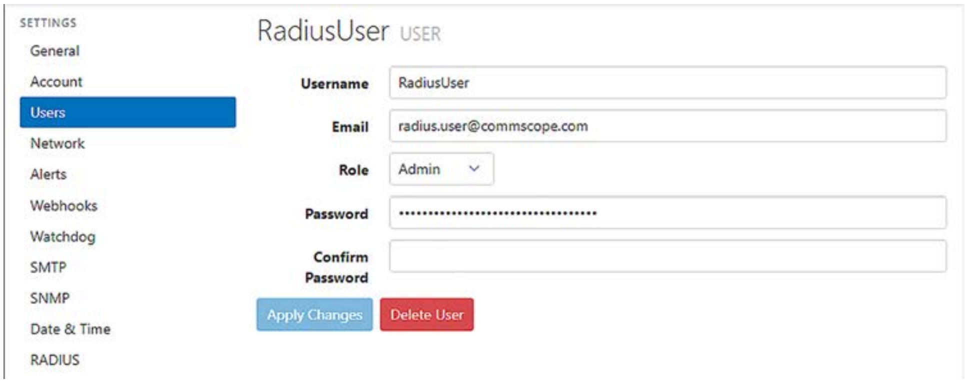
Server Port: 1812

Shared Secret: Enter password

Auth Type: PAP

Figure 25. RADIUS Authentication Settings

Note: RADIUS user settings (name, email, role, password) cannot be modified from the “Users” settings page



RadiusUser USER

Username: RadiusUser

Email: radius.user@commscope.com

Role: Admin

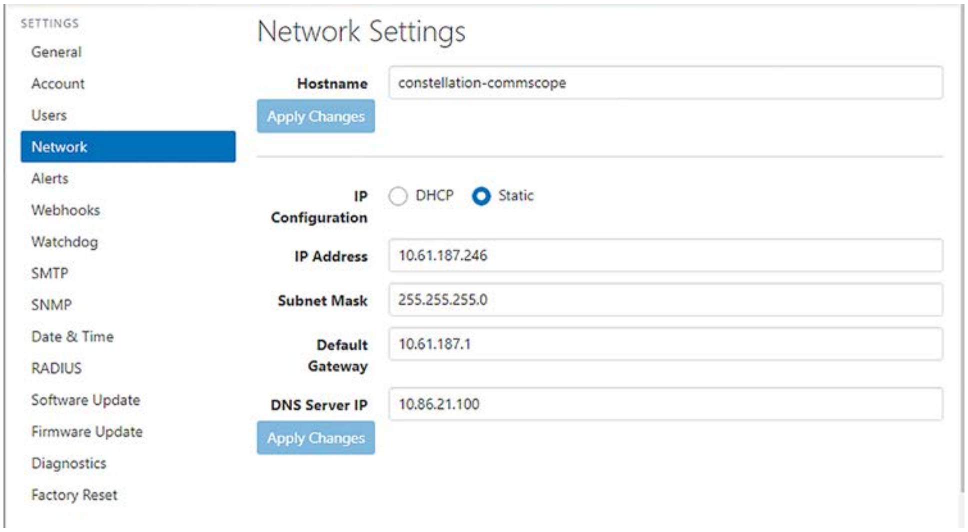
Password: ••••••••••••••••••••••••••••••••

Confirm Password:

Figure 26. RADIUS Managed View

8.4 Network

Hostname and static IPv4 address may be changed if desired.using the Network Settings page shown in Figure 27,



Network Settings

Hostname: constellation-commscope

IP Configuration: ○ DHCP ● Static

IP Address: 10.61.187.246

Subnet Mask: 255.255.255.0

Default Gateway: 10.61.187.1

DNS Server IP: 10.86.21.100

Figure 27. Network Settings Page

If settings are changed, the browser will redirect to the new IP address or hostname after settings are applied. You will likely be required to login to the web UI again after an IP address or hostname change.

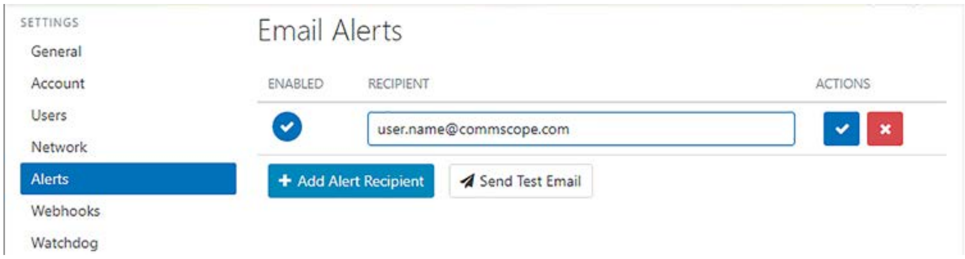
IPv6 addressing is not configurable via the user interface: by default, a link local address is assigned, and the device will also negotiate a global address if a prefix is advertised via IPv6 RA.

DNS

DNS access from the device is strongly recommended as it may be used for various other network facilities such as SMTP and NTP server name resolution. When configured for DHCP, the device expects to receive a list of DNS servers via DHCP option 6.

8.5 Alerts

The Email Alerts page may be used to identify configured to send email alerts to SMTP server as is shown in Figure 31. The device supports TLS encryption for SMTP connections.

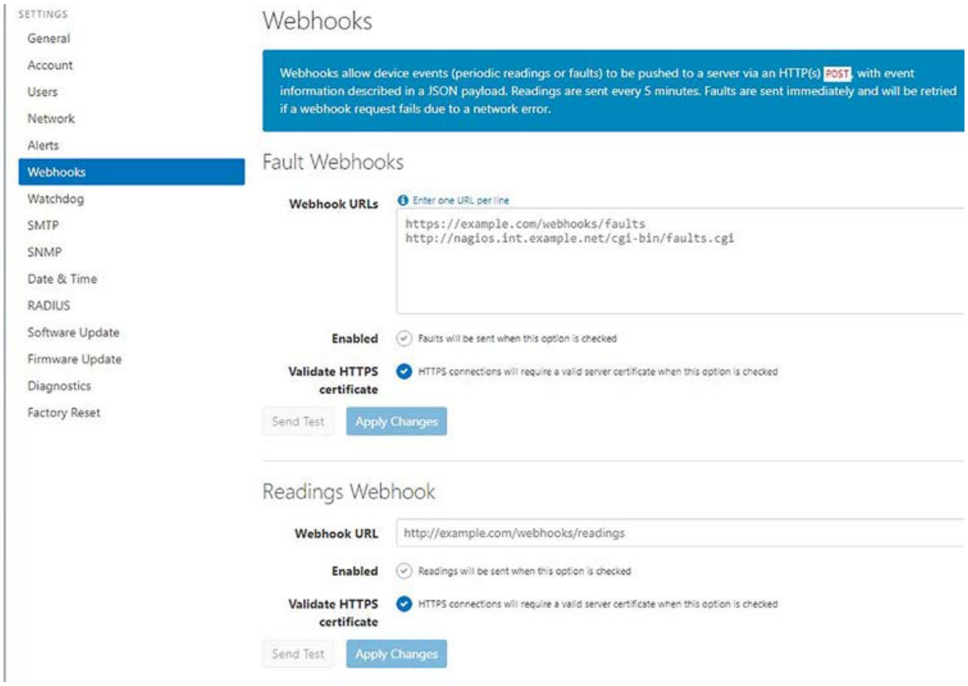


ENABLED ✓ RECIPIENT user.name@commscope.com

Figure 28. SMTP Settings With TLS

8.6 Webhooks

Devices can send fault events and periodic telemetry readings to automated event handling and system monitoring services using HTTP/S webhooks. When enabled, the device will send an HTTP POST with a JSON payload describing the event and identifying information of the device. Figure 29 shows the Webhooks page.



Webhooks allow device events (periodic readings or faults) to be pushed to a server via an HTTP(s) POST, with event information described in a JSON payload. Readings are sent every 5 minutes. Faults are sent immediately and will be retried if a webhook request fails due to a network error.

Webhook URLs Enter one URL per line

```
https://example.com/webhooks/faults
http://nagios.int.example.net/cgi-bin/faults.cgi
```

Enabled ○ Faults will be sent when this option is checked

Validate HTTPS certificate ● HTTPS connections will require a valid server certificate when this option is checked

Webhook URL http://example.com/webhooks/readings

Enabled ○ Readings will be sent when this option is checked

Validate HTTPS certificate ● HTTPS connections will require a valid server certificate when this option is checked

Figure 29. Webhooks Page

Use the “Send test” button to send a test payload for validation. A local system event will be logged if Webhooks fail to be sent (e.g. due to network failure.)

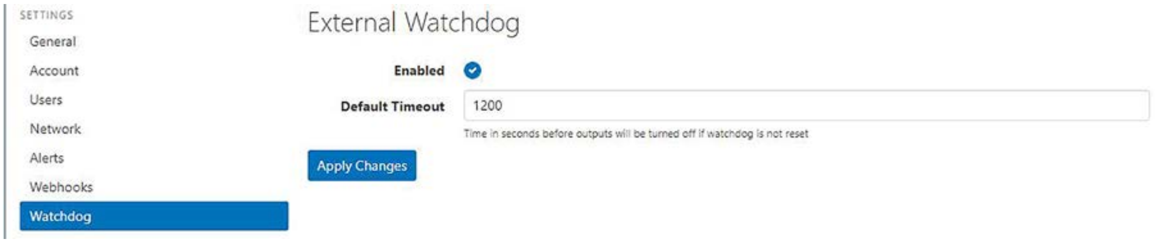
Faults webhooks are sent, at most, once every 5 seconds, with a maximum of 50 faults in a single request. If a webhook request fails, the failed webhook will be retried with exponential back off to a maximum of 10 minutes between retries. Multiple fault webhooks may be configured, one per line to a maximum of 20 destinations.

Readings are pushed every 5 minutes to a single destination. Reading webhooks are not retried if a request fails.

8.7 Watchdog

The external watchdog is a failsafe feature that, when enabled, turns off the outputs of all channels if an external application (typically the VoltServer hosted app) loses connectivity to the unit for an extended period of time. This feature is disabled by default and should not be enabled except in applications approved by VoltServer Support team.

The External Watchdog setting is disabled by default.



External Watchdog

Enabled ✓

Default Timeout 1200

Time in seconds before outputs will be turned off if watchdog is not reset

Figure 30. External Watchdog

8.8 SMTP

The device may be configured to send email alerts to SMTP server as is shown in Figure 31. The device supports TLS encryption for SMTP connections.

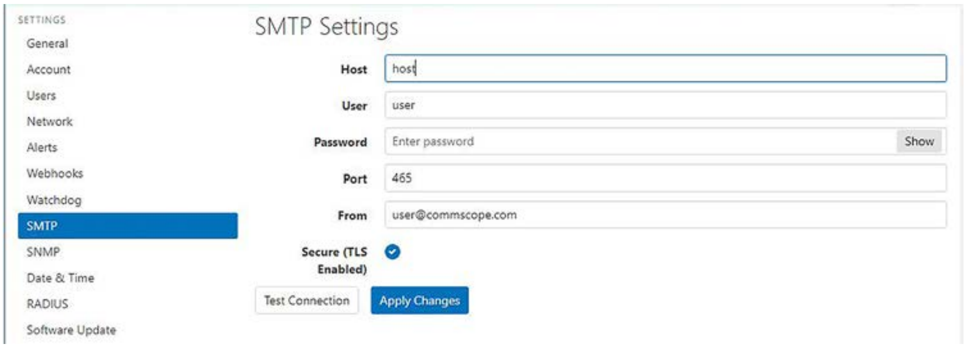
Use the “Test Connection” button to validate credentials and network reachability before applying settings.

Once an SMTP server is configured, alert recipients may be added, and a test email can be sent:

Note: Alerts are sent for Channel Faults and System Faults only.

A local system event will be logged if the device fails to send an SMTP alert (for example, due to network issues.)

Alerts are sent at most once every 30 seconds, with a maximum of 20 events (most recent.) One alert email is sent with all enabled recipients in the “To” field of the email. The subject line of the alert message will read “Constellation alert for device <hostname>”. If the device fails to send the request to the SMTP server (configured below) the alerts will remain enqueued and retry with a 5 second delay until the server is reached.



SMTP Settings

Host: host

User: user

Password: Enter password

Port: 465

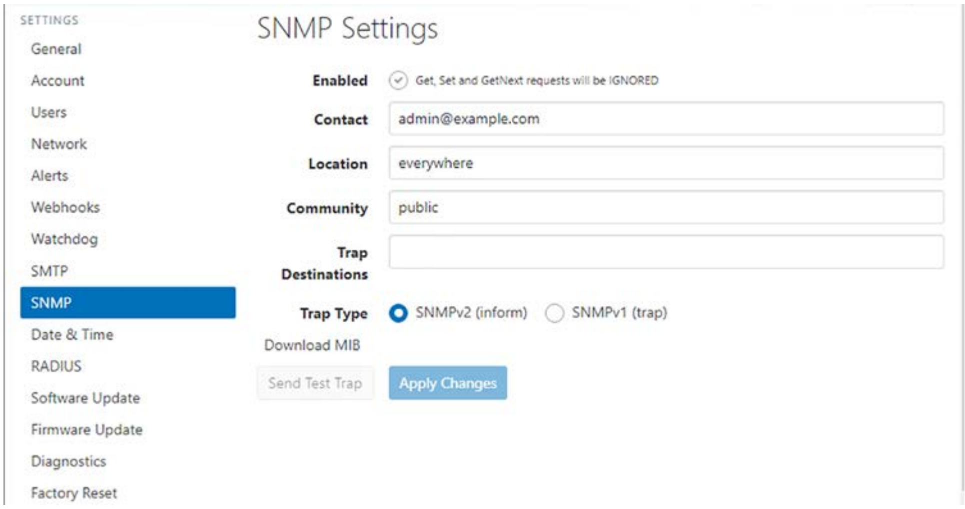
From: user@commscope.com

Secure (TLS Enabled): ✓

Figure 31. SMTP Settings With TLS

8.9 SNMP

The software supports SNMPv2c and SNMPv1 for GET, SET, and Inform operations, according to the COMMSCOPE-CONTROLLER MIB. Traps are sent for channel and system faults. See supplementary SNMP integration package for MIB details and packet capture samples. SNMPv2c is selected by default. Figure 32 shows the SNMP Settings page.



SNMP Settings

Enabled: ○ Get, Set and GetNext requests will be IGNORED

Contact: admin@example.com

Location: everywhere

Community: public

Trap Destinations:

Trap Type: ● SNMPv2 (inform) ○ SNMPv1 (trap)

Figure 32. SNMP Settings

Send Test Trap

Use the “Send Test Trap” button to validate trap destinations. This will send up to four separate alarms (v2 inform or v1 trap, depending on the chosen setting) to each trap destination specified. The alarms are:

- mgtFaultAlarm
- txCardFaultAlarm

- txGroupStatusAlarm (for group supported devices)
- powerModuelStatusAlarm

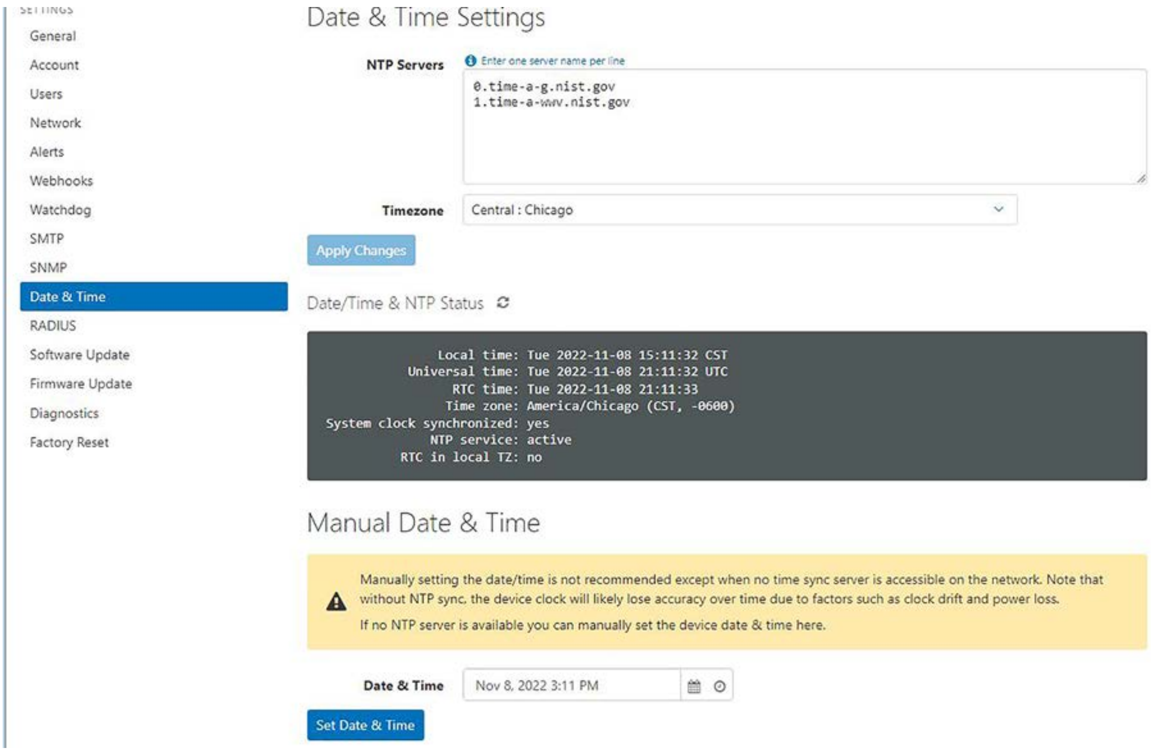
This may be used to test both network reachability to the trap destinations as well as parsing by the trap recipient.

8.10 Date & Time

By default, the device is configured to sync to public, load-balanced NTP servers from ntp.org. If using DHCP, the device will also sync to an NTP server specified by DHCP option 042. Network access to an NTP server is strongly advised in order to ensure accurate timestamps of readings, faults, and system events.

If no NTP servers are reachable, device date/time can be set manually.

The device date and time can be viewed, as well as present timezone and NTP sync status.



Date & Time Settings

NTP Servers — Enter one server name per line

```
0.time-a-g.nist.gov
1.time-a-wwv.nist.gov
```

Timezone: Central : Chicago

Date/Time & NTP Status

```
             Local time: Tue 2022-11-08 15:11:32 CST
         Universal time: Tue 2022-11-08 21:11:32 UTC
               RTC time: Tue 2022-11-08 21:11:33
              Time zone: America/Chicago (CST, -0600)
System clock synchronized: yes
            NTP service: active
        RTC in local TZ: no
```

Manual Date & Time

Manually setting the date/time is not recommended except when no time sync server is accessible on the network. Note that without NTP sync, the device clock will likely lose accuracy over time due to factors such as clock drift and power loss.

If no NTP server is available you can manually set the device date & time here.

Date & Time: Nov 8, 2022 3:11 PM

Figure 33. Date & Time Settings Page

8.11 RADIUS

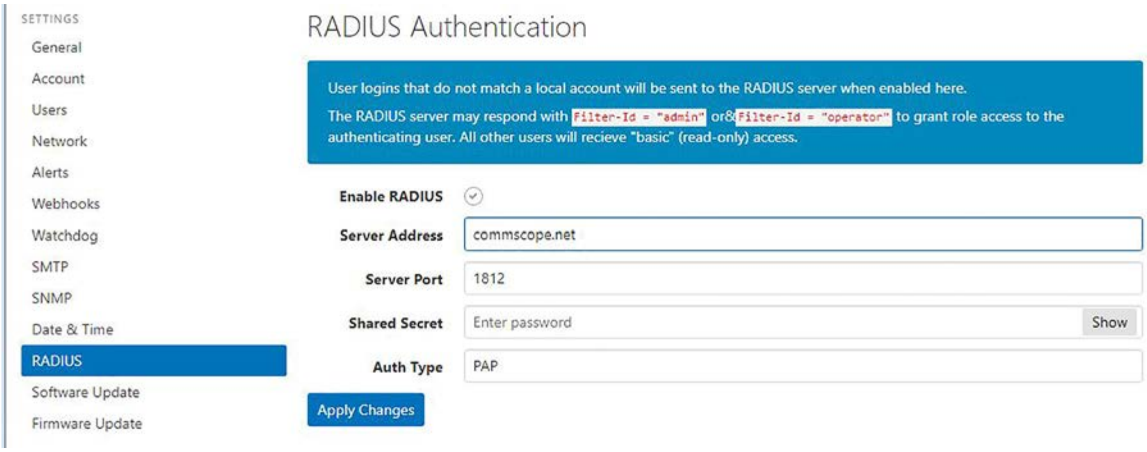
An administrator may configure the device to delegate AAC to a local RADIUS server, using the "PAP" or "CHAP" authentication. When RADIUS is enabled, all user logins that do not match a local account will be sent to the RADIUS server. If the server gives an “Access-Accept” response, the requesting user will be logged in.

If the RADIUS server provides a “Session-Timeout” attribute in the “Access-Accept” response, the device will automatically re-authenticate the user’s credentials after that many seconds. If no “Session-Timeout” attribute is given, the device will re-authenticate with the RADIUS server every 5 minutes while the user is active.

To grant the Operator or Admin role to a RADIUS user, add the “Filter-Id” attribute with a value of “`admin`” or “`operator`”. If no Filter-Id is attribute is sent, the user is granted “Basic” access.

Prior to v1.8.0, devices used the “Cisco-AVPair” VSA to designate role access. This method should be considered deprecated in favor of the standard Filter-Id attribute starting in v1.8.0.

CHAP authentication was added in v1.8.0.



RADIUS Authentication

User logins that do not match a local account will be sent to the RADIUS server when enabled here.

The RADIUS server may respond with `Filter-Id = "admin"` or&`Filter-Id = "operator"` to grant role access to the authenticating user. All other users will recieve "basic" (read-only) access.

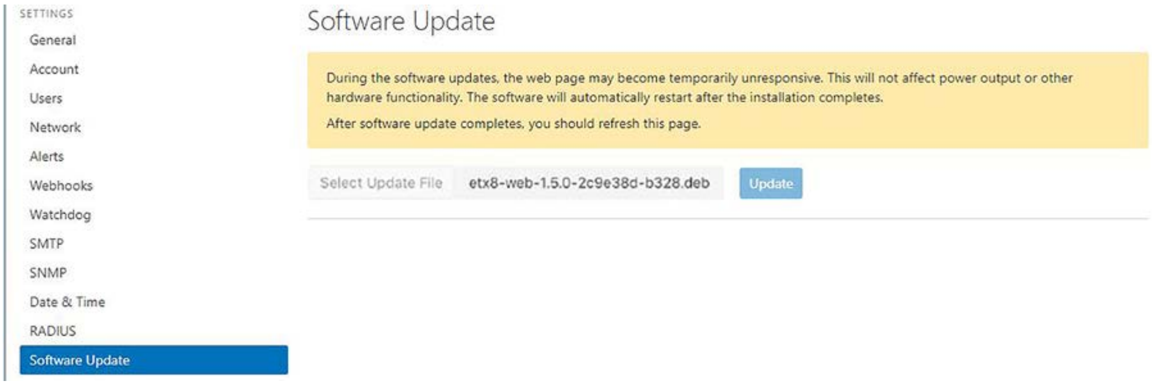
Enable RADIUS	✓
Server Address	commscope.net
Server Port	1812
Shared Secret	Enter password
Auth Type	PAP

Figure 34. RADIUS Authentication Settings

Note: RADIUS user settings (name, email, role, password) cannot be modified from the “Users” settings page

8.12 Software Update

Software updates can be performed without interrupting Digital Electricity power. Select an update file provided by CommScope support, then click “Update:”



Software Update

During the software updates, the web page may become temporarily unresponsive. This will not affect power output or other hardware functionality. The software will automatically restart after the installation completes.

After software update completes, you should refresh this page.

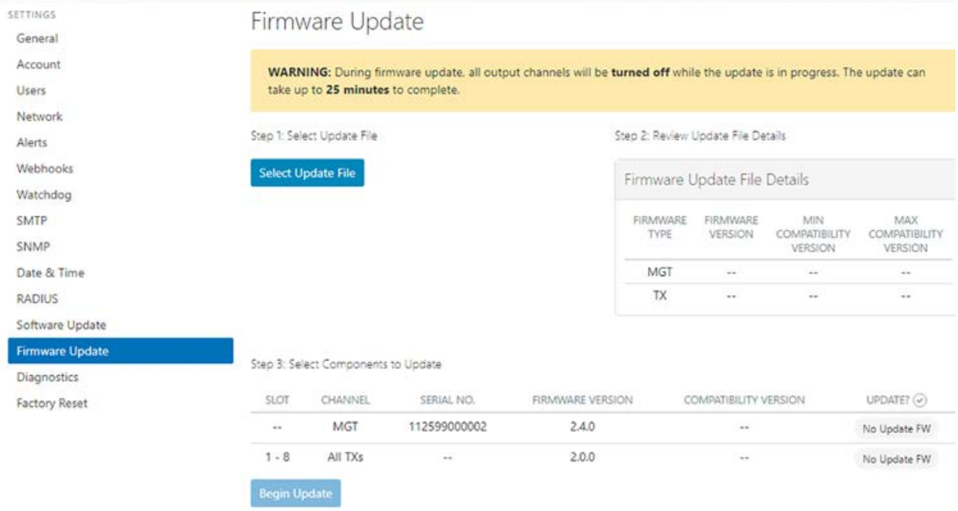
Select Update File: etx8-web-1.5.0-2c9e38d-b328.deb

Figure 35. Software Update

Note: While performing software updates,certain software functions such as policy, event logging, alerting, and programmatic (API) access may be temporarily unavailable. The software will automatically restart when the update completes. The user will be prompted to re-login.

8.13 Firmware Update

Device firmware may be updated via the web interface. Select an update file provided by VoltServer support. The application will indicate which components may be upgraded with the given firmware package depending on hardware compatibility. Select the components to be updated, and then click “Begin Update”.



Firmware Update

WARNING: During firmware update, all output channels will be **turned off** while the update is in progress. The update can take up to **25 minutes** to complete.

Step 1: Select Update File

Step 2: Review Update File Details

Firmware Update File Details

FIRMWARE TYPE	FIRMWARE VERSION	MIN COMPATIBILITY VERSION	MAX COMPATIBILITY VERSION
MGT	--	--	--
TX	--	--	--

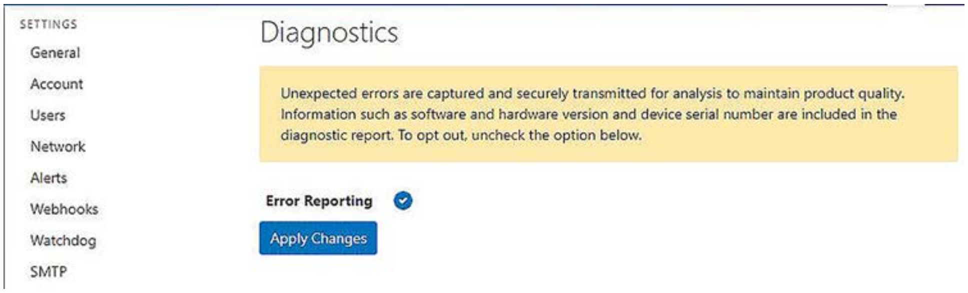
Step 3: Select Components to Update

SLOT	CHANNEL	SERIAL NO.	FIRMWARE VERSION	COMPATIBILITY VERSION	UPDATE?
--	MGT	112599000002	2.4.0	--	No Update FW
1 - 8	All TXs	--	2.0.0	--	No Update FW

Figure 36. Firmware Update

8.14 Diagnostics

Error reporting is disabled by default. When enabled, if the device encounters an unexpected error, it will attempt to securely send an error report to CommScope, for support and quality improvement purposes. All error reports are transmitted over HTTPS/TLS and do not contain any sensitive information. To enable this behavior, check the “Error reporting” box on the Diagnostics page, then click “Apply Changes.”



Unexpected errors are captured and securely transmitted for analysis to maintain product quality. Information such as software and hardware version and device serial number are included in the diagnostic report. To opt out, uncheck the option below.

Error Reporting ☑

Figure 37. Diagnostic Settings

8.15 Factory Reset

The device can be factory reset to its “out of the box” state using the “Factory Data Reset” button. All settings will be restored to their defaults. All user data including policies, channel groups, names, users, events and reading history will be deleted. The user will be required to re-login using the factory default username and password after performing a factory reset.

9 LIGHTING

ETX8-SA-277 lighting units have additional settings to configure the current limits used on the device. These settings can be set via the “Lighting” settings page. Note these settings should not be changed from VoltServer recommended values based on your lighting system design. Improperly setting these values could result in damage to light fixtures.

9.1 Nominal and Max Current Limits

These settings must be correctly set based on the type and configuration of lighting fixture used. Consult VoltServer support before setting or changing these values.

9.2 Default Output State (Lighting Only)

The default output state option allows changing the default DE output behavior on power up

Table 5. Constellation Technical Publications

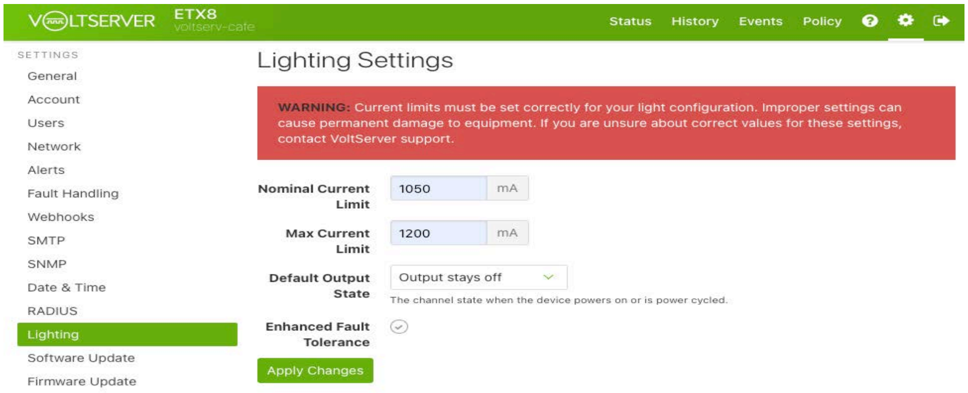
ACTION	RESULT
Output Stays Off	All DE outputs will be off until turned on via user control or API
Turn on	All DE outputs will turn on to the last nonzero set point
Restore last set point	All DE outputs will turn on to the last set point before power loss (including off, if a channel was off before power loss.)

The factory default option is “Output stays off.”

This feature was added in v1.7.0.

9.3 Enhanced Fault Tolerance (Lighting Only)

When enabled, enhanced fault tolerance works to minimize flickering and faults that may occur at certain intensity levels. Note that this feature trades off intensity range for fault avoidance and should not be enabled except on units with channels that are prone to transmission faults.



Lighting Settings

WARNING: Current limits must be set correctly for your light configuration. Improper settings can cause permanent damage to equipment. If you are unsure about correct values for these settings, contact VoltServer support.

Nominal Current Limit: 1050 mA

Max Current Limit: 1200 mA

Default Output State: Output stays off

The channel state when the device powers on or is power cycled.

Enhanced Fault Tolerance: ✓

Figure 38.

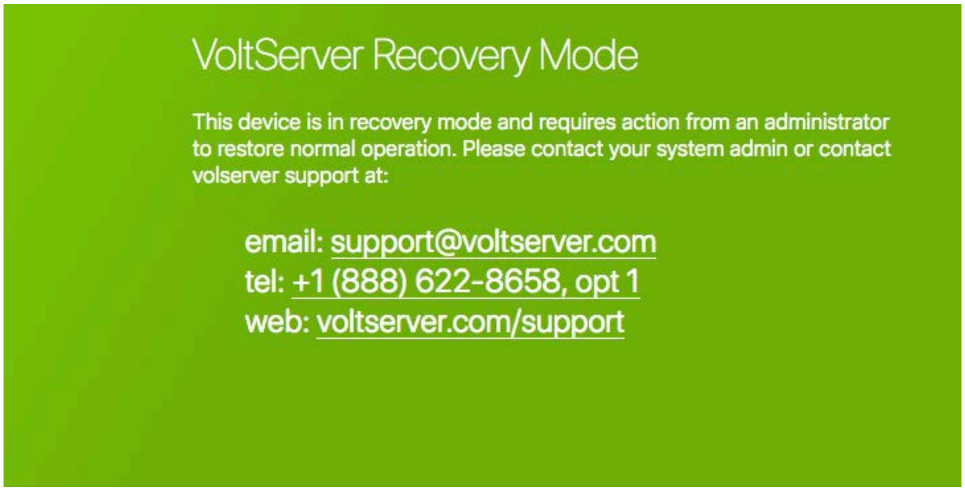
10 TROUBLESHOOTING AND RECOVERY PROCEDURES

10.1 Software API

All software capabilities outlined in this document are exposed via REST API. API authentication uses the same account credentials as GUI user logins. See the supplementary API documentation for full details.

10.2 Software Recovery Mode

In the exceptional event that the software becomes corrupted or the module otherwise fails to boot normally, the device may enter recovery mode. This is visually indicated by a “Blue heartbeat” on the “SW” LED of the Constellation Management Module (CTX-MGT)(See MGT500E Software LED<XREF>). In this state, the device will revert to its default hostname that is printed on the product label and use IPv4 DHCP addressing and mDNS (e.g. should be accessible at `http://voltserv-XXXX.local` where XXXX is the last two bytes of its MAC, in hex.) The following web page will be visible while the device is in recovery mod



VoltServer Recovery Mode

This device is in recovery mode and requires action from an administrator to restore normal operation. Please contact your system admin or contact volserver support at:

email: support@voltserver.com
tel: +1 (888) 622-8658, opt 1
web: voltserver.com/support

Figure 39. Software Recovery Mode

While Recovery Mode is active, the device will open SSH port 4222, username `root`, password `d1g1talP0wer` to facilitate performing a system upgrade. This should not be performed except when a full system wipe is required.

Recovery Mode may also be entered during power up: Immediately after power-on or software reboot, hold the “Factory” button for 5 seconds. On MGT500E, recovery mode is indicated by a blue “heartbeat” blink pattern on the “SW” LED.

To leave recovery mode, simply reboot the device without holding the “Factory” button.

If a device continues to enter recovery mode without pressing the “Factory” button during boot, please contact CommScope support.

10.3 Constellation Management Module (MGT500E) Software LED

The Constellation Management Module (MGT500E) has a “SW” LED that indicates the present status of the software.

LED PATTERN	LED PATTERN	NOTE
BLU ● 🟦 🟦	5 s after power-on.reboot	Software module power-on and pre-boot. Pushing “Factory” button during this time causes device to boot in Recovery Mode
GRN ● 🟩🟩⬜🟩🟩⬜	30 s (approximately)	Software is booting (green “heartbeat” blink pattern)
GRN ● ▬▬▬▬▬▬	Until reboot	Software is running
BLU ● 🟦⬜⬜🟦⬜⬜🟦	20 s (approximately)	Factory reset is in progress
BLU ● 🟦🟦⬜🟦🟦⬜	Until reboot	Software is in recovery mode (blue “heartbeat”)

11 HARDWARE BUTTONS

The Constellation Power Transmitter (CPCX-12) has two physical buttons recessed behind the front panel. Buttons may be pressed using a thin implement such as a paperclip or multimeter probe.

11.1 Factory

The “Factory” button performs a factory reset and restores all settings to factory defaults, including network settings, user accounts, and deletes all history data from the device. To perform a factory reset, press and **hold the “Factory” button for at least 3 seconds**. Reset will begin when the button is released. Starting with software version 1.6.0, the “SW” button on the MGT500E will display a “fast blue” blink while the reset is in progress. At the end of the factory reset procedure, the software will reboot.

11.2 Reboot

The “Reboot” button causes the software to reboot. This is a software-only reboot and does not reset any hardware conditions.