Server Technology's Monitoring Solution Featuring Bluetooth® Wireless Technology and the ST Eye Mobile App (for Android) – Part Numbers KIT-STEYE-01 and KIT-STEYE-10

Purpose

This technical note provides functional information about Server Technology's innovative solution featuring secure Bluetooth® wireless technology for mobile monitoring using an Android device. This unique data center solution is the first time Bluetooth wireless technology has been paired with the Cabinet Distribution Unit (CDU) for mobile access that provides fast viewing of device operational data.

Using Server Technology's ST Eye mobile app, you can remotely monitor critical information about a CDU – with easy access to power and environmental data – displayed directly on your Android device in the ST Eye user interface.

The following areas of the Bluetooth® wireless technology solution are covered in this document:

- Hardware connection between the Bluetooth module and the CDU.
- Security issues for the data center when using this solution.
- Methods for discovering a Bluetooth module or scanning a QR Code label.
- User interface of the ST Eye mobile app for the Android device.
- Configuration of the Sentry firmware parameters used in the Bluetooth solution.

Why Use This Solution?

Server Technology's mobile monitoring solution offers the following significant benefits for the data center:

- Easy connection with Bluetooth® technology for quick and easy mobile monitoring of critical CDU information at the cabinet.
- Server Technology's **free** ST Eye mobile app and user interface for mobile monitoring. No other app or purchased license key are required to get started with this solution.
- Use your own Android mobile device in the data center anytime for instant access to the CDU. Locked cabinets and hot aisle device access are no longer obstacles for obtaining immediate device data.
- A physical connection is not required at the cabinet between a computer and the CDU (via the network or serial port) to obtain CDU data.
- If your Android device is connected to the wireless network in the data center, ST Eye will also allow mobile access for login to the CDU via the secure web interface of the Sentry firmware.

System Overview

The following system illustration identifies the key hardware and software components:

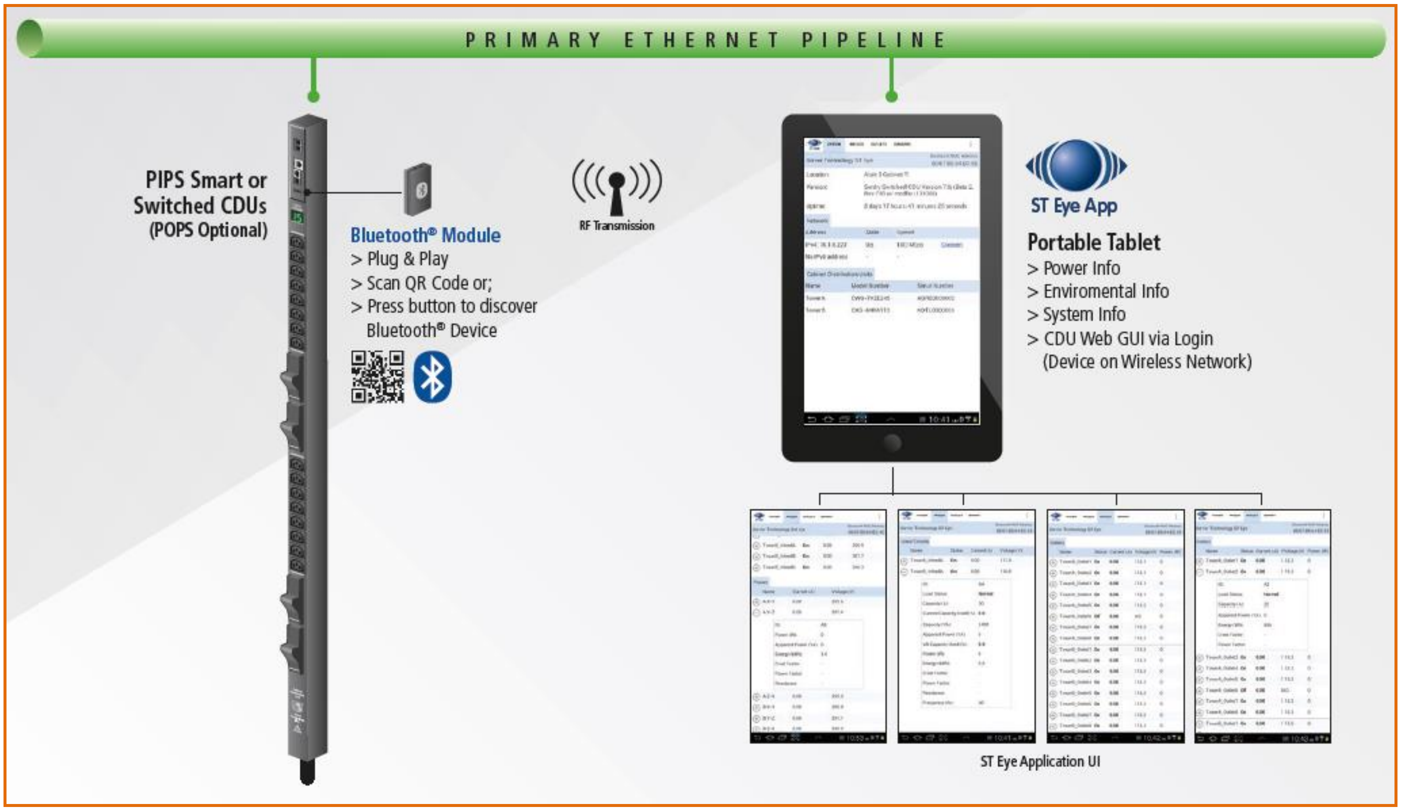

PRIMARY ETHERNET PIPELINE
PIPS Smart or Switched CDUs (POPS Optional)
Bluetooth® Module
> Plug & Play
> Scan QR Code or;
> Press button to discover Bluetooth® Device
RF Transmission
ST Eye App
Portable Tablet
> Power Info
> Enviromental Info
> System Info
> CDU Web GUI via Login (Device on Wireless Network)
ST Eye Application UI

Figure 1. System Overview of Mobile Monitoring Using Bluetooth® Wireless Technology

System Components

As shown in Figure 1 (left to right), several items are part of Server Technology's mobile solution:

Server Technology CDU

Server Technology's intelligent PIPS-enabled Switched or PIPS-enabled Smart CDU that has been made ready for a connection to the Bluetooth® module.

The Bluetooth® Module

The separate, external Bluetooth wireless device connected to the CDU via a locking cable. The module establishes a secure connection for the overall solution.

QR Code Label

The Quick Response (QR) dimensional barcode labels provided by Server Technology for scanning with the Android mobile device.

ST Eye

Server Technology's **free** mobile application for download to the Android mobile device. The app makes system, infeed, outlet, and sensor data available from the CDU for mobile viewing and monitoring.

Data Center Security

Server Technology has addressed the key areas of security in the Bluetooth® technology solution:

Secure Bluetooth® Communications

The Server Technology solution provides a secure and wireless way to obtain power data. Server Technology's mobile application, ST Eye, uses the improved technical methods from the Bluetooth® core specification, version 2.1, known as "secure simple pairing," which eliminates security vulnerabilities found in older Bluetooth systems.

The Server Technology Bluetooth connection in this solution is encrypted with the EO stream cipher to prevent passive eavesdropping. The encryption key is established using the Elliptic-Curve-Diffie-Hellman (ECDH) key exchange. To prevent differential cryptanalysis attacks against the cipher, the encryption key is rotated every packet. New keys will be established before they are reused.

Based on recommendations from the National Institute of Standards and Technology (NIST), several options have been programmed into the solution to limit the discoverability of Cabinet Distribution Units (CDUs):

- Users can lower the range of the Bluetooth module to prevent connections from colocation neighbors.
- Sensitive data is not transmitted over the connection, such as user credentials.
- The pin code used for hardware authentication is hashed to prevent recovery.
- No commands are available via the ST Eye mobile app to modify the state of the CDU.
- Limited Discoverability Feature – The ST Eye app is shipped with limited discoverability so the Bluetooth module does not broadcast until the user explicitly instructs the module to do so by pressing a button or by making a configuration change.

The user can also rely on ST Eye's unique QR code discovery method to connect out-of-band to a CDU used in this solution. The QR code method prevents eavesdroppers from discovering Bluetooth modules in a colocation environment.

In conclusion, the Server Technology solution uses the security improvements mentioned above to prevent published attacks against the Bluetooth technology connection. The solution successfully balances security and ease-of-use.

Note: This encryption does not prevent unwanted Bluetooth communications if a user somehow gains access to the address of the Bluetooth module.

Security of the Bluetooth® Module

Within the existing security of the Bluetooth® module, the ST Eye mobile app security also relies on the physical security of the module itself, as well as the short distances under which the Bluetooth module can communicate.

In addition, Server Technology added a check in the Sentry firmware not to allow any modifications to any part of the firmware system through a Bluetooth connection. This means firmware system data cannot be changed through the Bluetooth AUX port, even if there was physical access to a remote Bluetooth port, or even if the mobile phone app was hacked in the attempt to write system data.

Security Measures

To access the Bluetooth® information using the ST Eye mobile app, the following items must be in place:

- Users must be physically present in the data center.
- Users must have a mobile device with them on which the ST Eye app was installed.
- Users must have access to the QR Code label or be able to physically press the pushbutton on the Bluetooth module to initiate communication.
- Once connected to the Bluetooth module using the ST Eye mobile app, all that users can do is **view** CDU operational information – no control actions can be performed.
- The only way to move from the ST Eye mobile app to the Sentry firmware user interface for the CDU is to place the Android mobile device on the data center's wireless network. Sentry firmware username and password are then required for login and access to the CDU.

Overall Security

Security of the solution using the Bluetooth® wireless technology is ensured with the combination of:

- Inherent Bluetooth security
- Required physical access to both the data center and the Bluetooth module

In addition, considering the fact that the user can only **view** CDU information when using the ST Eye mobile app, all these noted safeguards make a hacking attempt pointless.

Before You Begin

You will need the following items to start using the solution, but note that you do not need to purchase a software license key.

Server Technology Cabinet Distribution Units (CDUs)

Server Technology's intelligent CDUs (Smart or Switched products) with Power Infeed Power Sensing (PIPS) technology. In addition, the CDU must be equipped with an auxiliary port specifically used for connection to the separate Bluetooth® module.

Sentry Firmware

Sentry firmware, version 7.0j or later, is required to allow configuration of several parameters used in the solution.

Mobile Device

An Android mobile device, version 2.3.3 or later, to use for camera-scanning of QR Code labels and for display of collected CDU data.

ST Eye Mobile Application

Server Technology's mobile app, ST Eye, downloaded on the Android device. No other apps are required.

The Bluetooth® Technology Hardware Kits

Initial deployment of the Bluetooth® solution is provided by Server Technology as a bundle that will be shipped with two major components:

- PIPS-enabled Switched or Smart CDU equipped with the AUX port, and
- Hardware kit (part number KIT-STEYE-10) with a 10' locking cable.

Later deployment of CDUs for the Bluetooth® solution will offer another hardware kit (part number KIT-STEYE-01) with a 1' locking cable, if a shorter cable length is preferred.

Note: KIT-STEYE-01 (with the 1' locking cable) or KIT-STEYE-10 (with the 10' locking cable) can be purchased separately as an optional accessory without a CDU.

Both hardware kits (KIT-STEYE-10 and KIT-STEYE-01) contain the following items:

- Locking Cable
- Bluetooth® Module
- QR Code Labels

Locking Cable

The locking cable establishes a physical connection between the Bluetooth® module and the CDU. One end of the cable connects to the module and the other end connects to the AUX port of the CDU.

- Part number KIT-STEYE-10 – contains a 10' cable (bundled with the CDU for initial shipments of the Bluetooth solution).
- Part number KIT-STEYE-01 – contains a 1' cable (available for future purchase as a separate and optional accessory).

Bluetooth® Module

The Bluetooth® module is the small wireless device that is physically connected by the locking cable to the CDU. A factory-placed QR Code label on the module contains specific NIC information that ties the label to the Bluetooth module.

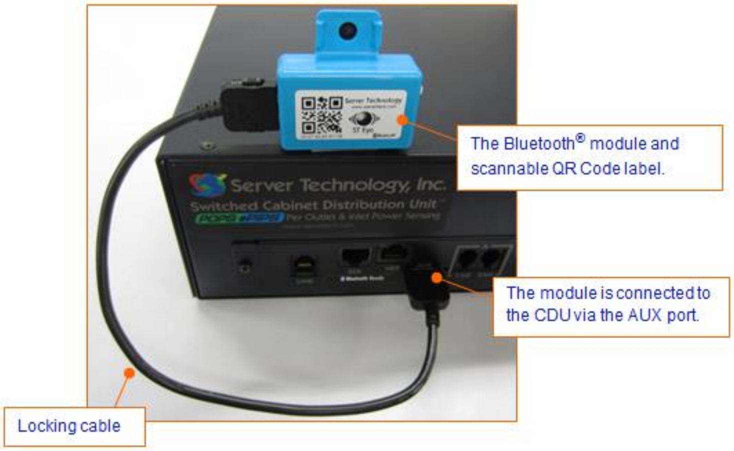

The Bluetooth® module and scannable QR Code label.
The module is connected to the CDU via the AUX port.
Locking cable
Server Technology, Inc.
Switched Cabinet Distribution Unit

Figure 2. Bluetooth Module (showing connection to the CDU)

QR Code Labels

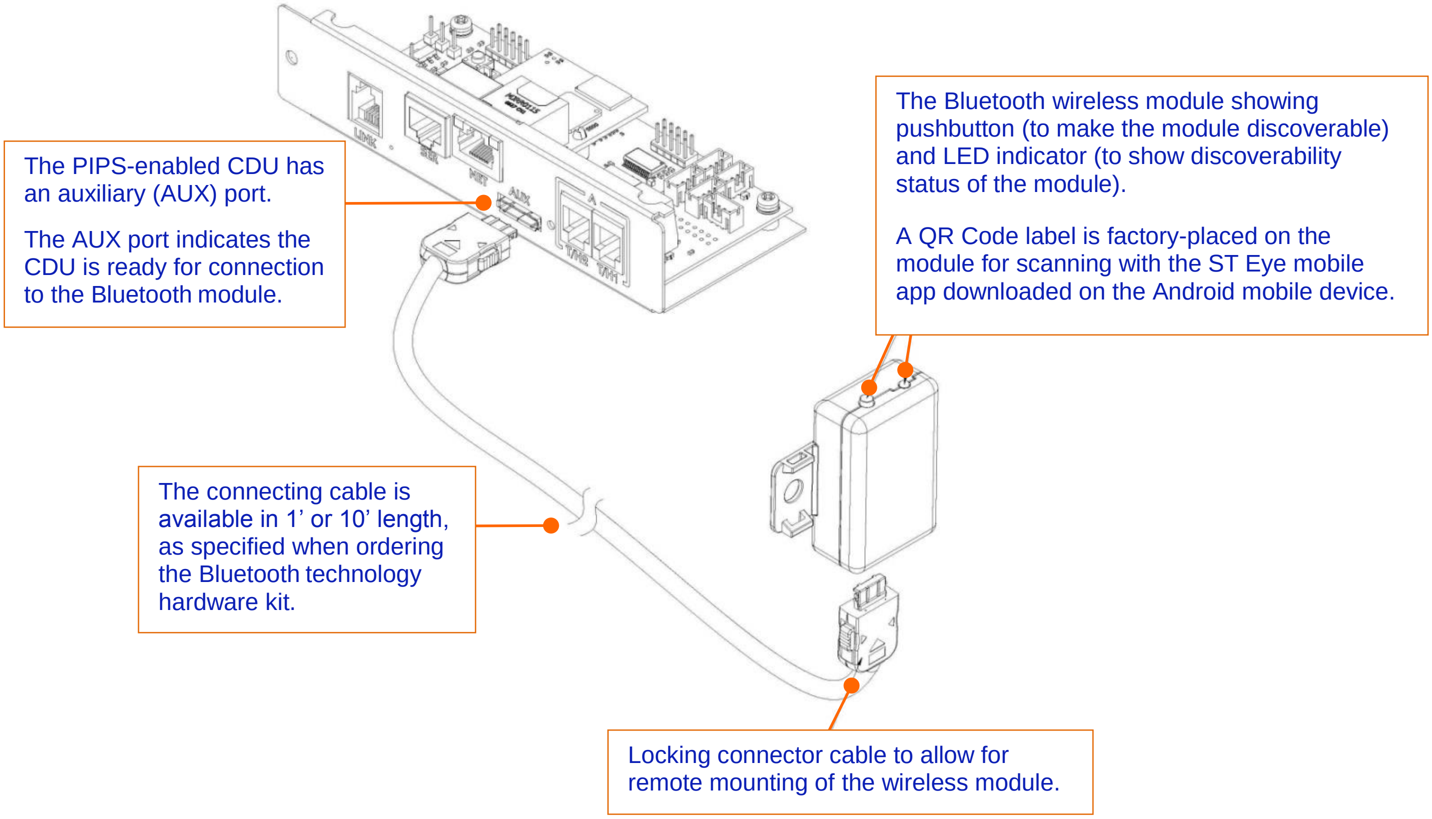
Two QR Code labels for connecting Bluetooth® modules are included in your kit:

- The smaller label (below left) is factory-placed on the module.
- The larger, separate label (below right) is **optional** for placement anywhere on the CDU or cabinet for easy scanning, based on your equipment layout.

Note: Both QR Code labels are active and function the same way when scanned with the Android device.

Making the Bluetooth® Wireless Connection

This drawing shows the overall hardware connection of the PIPS CDU to the separate Bluetooth® module:



The PIPS-enabled CDU has an auxiliary (AUX) port.

The AUX port indicates the CDU is ready for connection to the Bluetooth module.

The Bluetooth wireless module showing pushbutton (to make the module discoverable) and LED indicator (to show discoverability status of the module).

A QR Code label is factory-placed on the module for scanning with the ST Eye mobile app downloaded on the Android mobile device.

The connecting cable is available in 1’ or 10’ length, as specified when ordering the Bluetooth technology hardware kit.

Locking connector cable to allow for remote mounting of the wireless module.

Figure 3. Hardware Connection Using Bluetooth Wireless Technology

Bluetooth® Ready Sticker

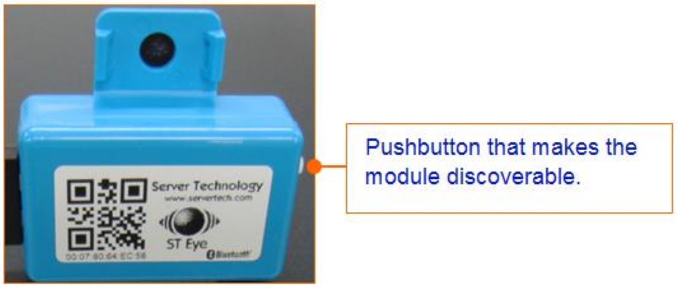
A separate “Bluetooth Ready” sticker (not a QR Code label for scanning) is factory-placed on the CDU to identify the device as ready to be used in the mobile solution.

Note: Even if the ready sticker is missing, you can still tell if a CDU in your equipment layout is ready for the mobile monitoring solution by the AUX port installed specifically to connect to the Bluetooth module.

Discoverability of the Bluetooth® Module

The Bluetooth® module communicates with the CDU to establish a secure Bluetooth connection that makes CDU operational data available for viewing.

The module has a pushbutton on one side that you press to make the module discoverable. To be discovered, first the module must be in proper discoverability mode, based on Sentry firmware settings, described below.



Pushbutton that makes the module discoverable.

Figure 4. Close-up of the Bluetooth Module (showing QR code label and pushbutton)

LED Indicator Discoverability Status:

A blue LED indicator (located next to the pushbutton on the module) shows discoverability status of the module.

- Light flashing = module is discoverable; flashing occurs when pushbutton on the module is pressed.
- Light off = module is not discoverable.
- Light on = module is connected.

Firmware Discoverability Settings

Sentry firmware, version 7.0j or later, uses the following user-configured settings to set the discoverability status of the module:

Firmware Discoverability Settings	
Setting	Description
Always	Bluetooth® module is discoverable – even without pressing the pushbutton.
Limited	(Default) Pushbutton on the Bluetooth® module must be pressed to make the module discoverable for 60-seconds.
Never	Bluetooth® module is **never** in discoverable mode.

The above discoverability settings, along with other Bluetooth® parameters, are available for configuration by the Sentry firmware administrative-user account.

For more information, see Configuring Bluetooth Parameters Using Sentry Firmware.

Working with the ST Eye Mobile App

Server Technology's ST Eye app works over a secure connection with Bluetooth® wireless technology to locate special CDUs in the data center that have been made ready for the mobile monitoring solution. ST Eye collects key operational data from the CDUs and display the information for viewing on the Android mobile device.

Pre-Download Checklist

Before using the ST Eye app, make sure the following steps have been done:

☑ Ordered and received the Bluetooth technology hardware kit from Server Technology.

☑ Connected the Bluetooth module (with its factory-placed QR Code label) to a PIPS CDU with the AUX port.

☑ (Optional) Placed the separate QR Code label (received in the hardware kit) anywhere on the CDU or cabinet.

☑ (Optional) Configured the Bluetooth module discoverability state (Always, Limited, Never) via Sentry firmware.

Note: The Bluetooth module and the Sentry firmware, version 7.0j or later, ship with the default "Limited" discoverability setting (requires pushbutton to be pressed when discovering the module.) For more information about these settings, see the table on the previous page.

The next step is to download and install the ST Eye app.

Downloading ST Eye

The **free** ST Eye mobile app can be downloaded from either Google Play or the Server Technology website.

From Google Play:

Note: Make sure you have an Android device that works with Google Play.

Step 1. Click https://play.google.com/store/apps/details?id=com.servertech.bluetooth.android and search for "Server Technology Eye" in the Google Play Store app on your Android device.

Step 2. Click the ST Eye icon as shown in Google Play, and download/install the app as instructed.

From the Server Technology website:

Step 1. Click http://www.servertech.com/products/accessories/st-eye to display the ST Eye product page.

Step 2. Click the **Application File** link near the bottom of the page to start downloading.

Step 3. Transfer the file to your mobile device.

Step 4. You may need to enable 3rd party applications on your Android device. Go to **Settings > Security > Enable Unknown Sources**, or refer to Android resources for your device.

Step 5. Open the file (typically "ServerTechBluetooth.apk") and confirm the installation.

Get Started Fast

When downloaded on the Android device, ST Eye provides two connection methods for mobile access of CDU information:

- **Discovering a Bluetooth® Module:** A module is discovered based on its discoverability status, as determined in the settings of the Sentry firmware. The module must be in a discoverable state (firmware setting must be “Always” or “Limited”; the setting cannot be “Never”). The pushbutton on the module must be pressed to discover the module.

- **Connecting with a QR Code Label:** A scan of a QR Code label using the camera on your Android mobile device to connect for mobile access. This connection method is done without the need to discover the Bluetooth module by pressing the pushbutton on the module. This connection is also made regardless of the discoverability status of the module.

Choose a method that works better for your data center equipment layout, the placement of the Bluetooth modules in or around cabinets, and the firmware settings you may have configured to control the discoverability status of the module.

Discovering a Bluetooth® Module

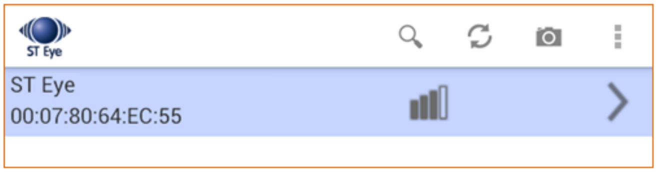
Step 1. Press the pushbutton on the Bluetooth® module you want to discover.

Step 2. Open the mobile app by selecting the ST Eye icon from the applications list on your Android touchscreen. The app opens in the Main View (startup screen).

Note: If Bluetooth is turned off on the Android device, you will get a request to turn on Bluetooth.

A discovery of nearby Bluetooth modules automatically starts. The ST Eye app attempts to locate any nearby discoverable modules (within about 100’).

A discovered module populates a list in ST Eye’s Main View (startup screen) as follows:



ST Eye
00:07:80:64:EC:55

The list includes the following information:

- Bluetooth® Module Name: Either the default name (“ST Eye”, as shown in the above screenshot), or the name as configured by the administrator using the Sentry firmware.

  For more information about these settings, see Configuring Bluetooth Parameters Using Sentry Firmware.

- MAC address of the module; for example, 00:07:80:64:EC:55 as the example shows.

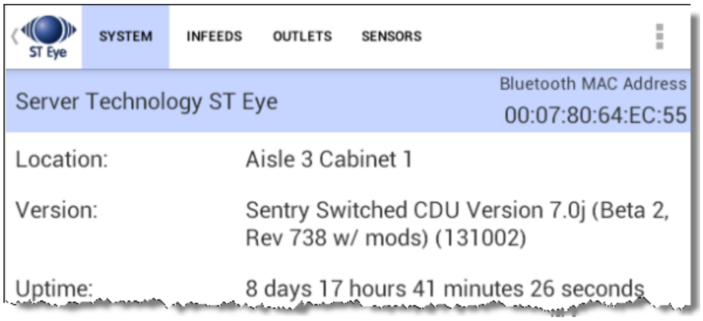
- Signal strength expressed in 0-4 bars. Multiple Bluetooth modules appear in the list sorted by signal strength.

Step 3. Select a module in the list.

A connection to the Bluetooth module is attempted, which may take a few seconds. Only one connection to a module is allowed at a time.

If connection fails, an error displays, and ST Eye goes back to the Main View (startup screen). If connection succeeds, then ST Eye starts receiving and displaying CDU data, refreshing the screen data every 10-seconds.

ST Eye's Device View opens with the default System tab to display CDU information:



Server Technology ST Eye

Bluetooth MAC Address 00:07:80:64:EC:55

Location: Aisle 3 Cabinet 1

Version: Sentry Switched CDU Version 7.0j (Beta 2, Rev 738 w/ mods) (131002)

Uptime: 8 days 17 hours 41 minutes 26 seconds

Step 4. You can now navigate the System, Infeeds, Outlets, and Sensors tabs to view additional device details.

Note: CDU information is available for view-only; no control actions on the CDU can be performed.

Connecting with a QR Code Label

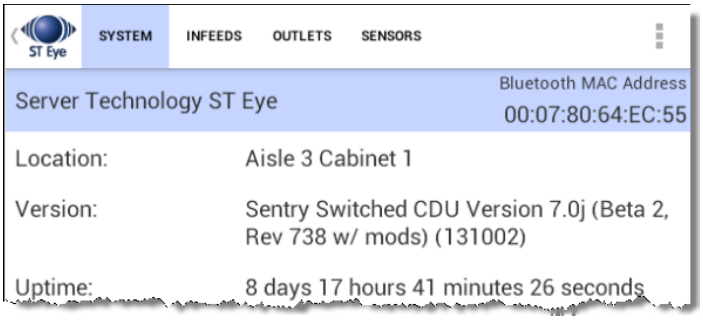
Step 1. Open the mobile app by selecting the ST Eye icon from the applications list on your Android touchscreen. The app opens in the Main View (startup screen).

Note: If the Bluetooth® technology is turned off on the Android device, you will get a request to turn it on.

Step 2. Select the **Camera** button on the mobile device.

Step 3. In the Camera view, position the device to scan a QR Code label, as shown:

When a valid QR Code label is located, ST Eye connects to the Bluetooth modules, displays CDU information in the default System tab, and refreshes displayed data every 10-seconds.



Server Technology ST Eye

Bluetooth MAC Address
00:07:80:64:EC:55

Location: Aisle 3 Cabinet 1

Version: Sentry Switched CDU Version 7.0j (Beta 2, Rev 738 w/ mods) (131002)

Uptime: 8 days 17 hours 41 minutes 26 seconds

Step 4. You can now navigate the System, Infeeds, Outlets, and Sensors tabs to view additional device details.

Note: CDU information is available for view-only; no control actions on the CDU can be performed.

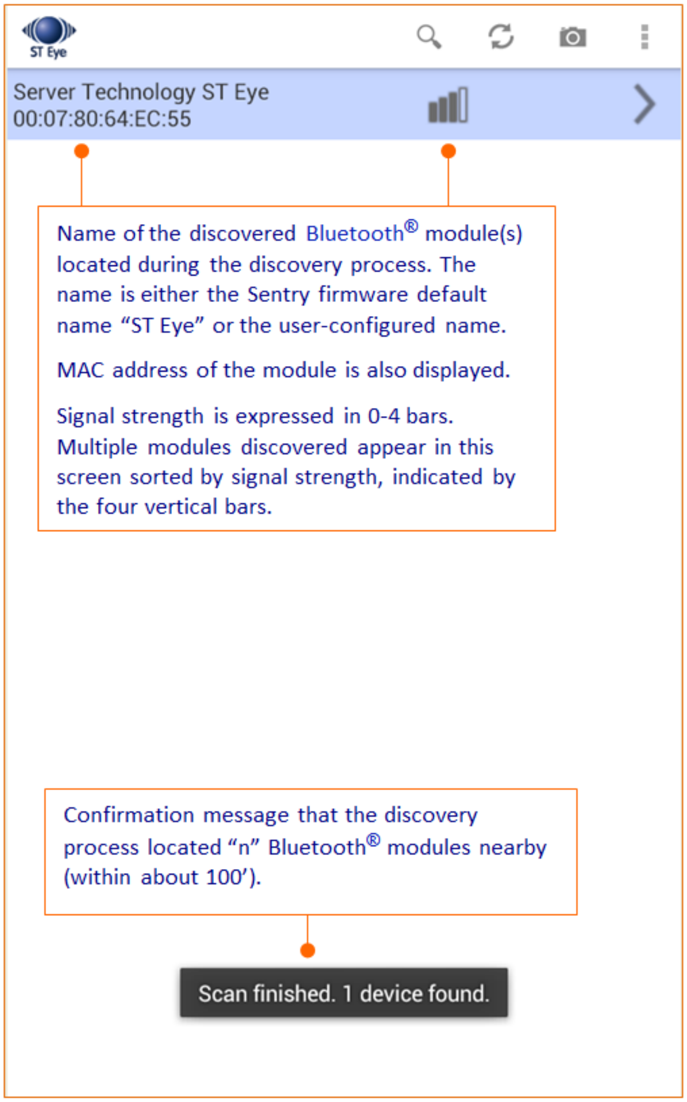
The ST Eye User Interface

The screens in the ST Eye app are organized into three main views:

- Main View – The ST Eye startup screen
- Camera View – Camera on the Android device for scanning QR Code labels
- Device View – System, Infeed, Outlet, and Sensor tabs displaying detailed CDU information.

Main View – Startup Screen

The Main View shows one or more discovered Bluetooth® modules.



Name of the discovered Bluetooth® module(s) located during the discovery process. The name is either the Sentry firmware default name "ST Eye" or the user-configured name.

MAC address of the module is also displayed.

Signal strength is expressed in 0-4 bars. Multiple modules discovered appear in this screen sorted by signal strength, indicated by the four vertical bars.

Confirmation message that the discovery process located "n" Bluetooth® modules nearby (within about 100').

Scan finished. 1 device found.

Search. Opens a search box to allow searching a device list; filters the list as you type.

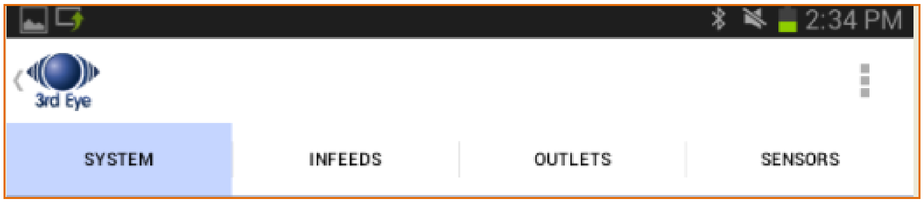
Refresh. Starts another discovery for a Bluetooth® module. To discover the module, you will need to press the pushbutton on the module – this allows the module to be discovered. Note that when a discovery is in process, the Refresh button is disabled.

QR Scan. Opens the Camera view for scanning QR Code labels. Position the Android device to scan the QR Code label on the Bluetooth® module, or the optional label placed on the CDU or cabinet.

Options overflow section. Select to display additional overflow options: About (shows STI Eye About page) and Quit (exits from the ST Eye app).

Device View – Information Tabs

Operational data collected from a CDU displays as soon as the CDU is connected. The data appears in a ribbon of four separate information tabs on the Android screen, opening in the default System tab:



System: Default display tab; shows general, non-power information about a CDU, such as network and tower data. Also provides a Connect link to the Sentry firmware for a CDU.

Infeeds: Shows the operational details for single-phase and 3-phase infeeds.

Outlets: Provides a list of outlets, and outlet status, in each tower of the CDU.

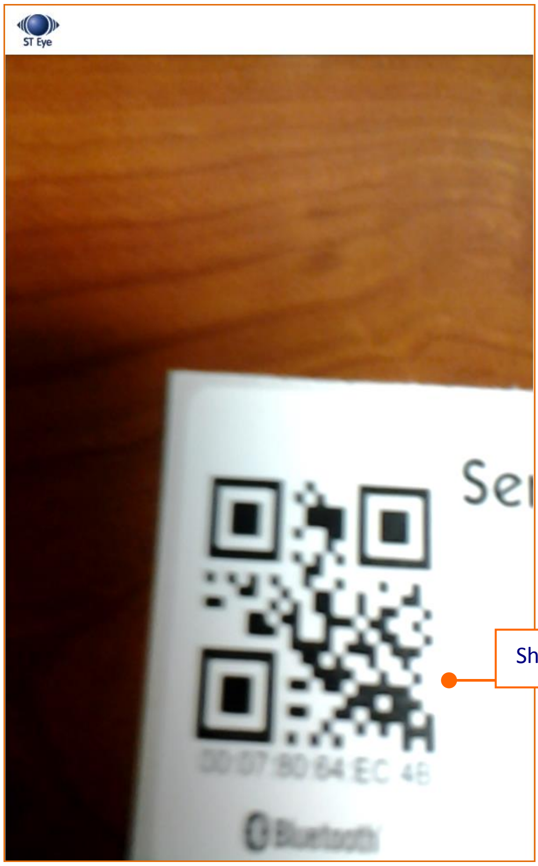
Sensors: Displays the current status of an environmental sensor with readings for temperature and humidity.

Note: Depending on the Android mobile device and the details ST Eye is currently displaying, viewing data in portrait orientation on the device screens may result in character wrapping. If you find that data is hard to read, it is recommended that you adjust font size (and any other related display settings) for your specific mobile device to improve readability on the screen.

Camera View

Displays the current view of the camera on the mobile device.

Select 📷 and position the Android device to scan a QR Code label.

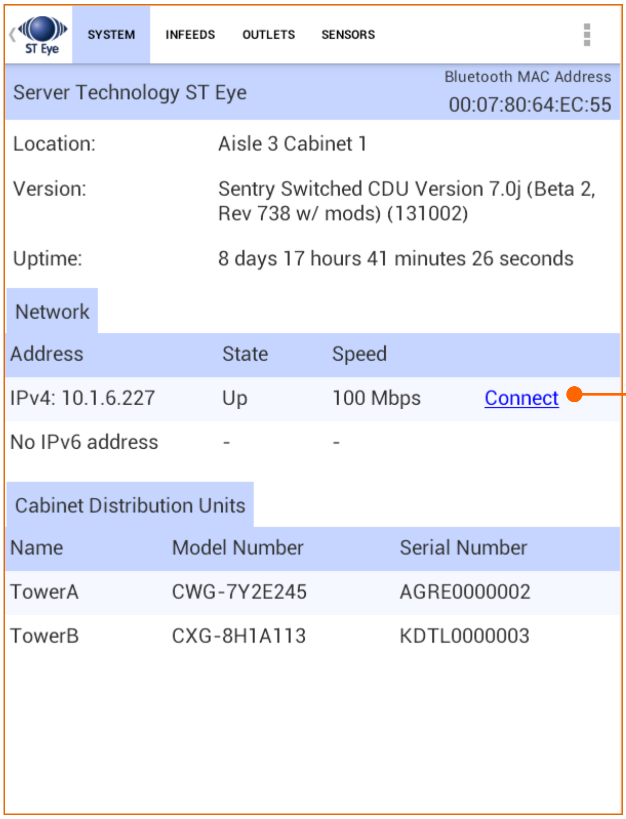


Shows a scan of the QR Code label.

You may have a device that shows ST Eye’s lightning bolt ⚡ icon to turn on the LED torch mode, which is useful when scanning a label in a room with dim lighting.

Device View – System Tab

Default information screen; displays general, non-power information about a CDU, such as network and tower data.



Server Technology ST Eye

Bluetooth MAC Address
00:07:80:64:EC:55

Location:	Aisle 3 Cabinet 1
Version:	Sentry Switched CDU Version 7.0j (Beta 2, Rev 738 w/ mods) (131002)
Uptime:	8 days 17 hours 41 minutes 26 seconds

Network

Address	State	Speed	
IPv4: 10.1.6.227	Up	100 Mbps	Connect
No IPv6 address	-	-	

Cabinet Distribution Units

Name	Model Number	Serial Number
TowerA	CWG-7Y2E245	AGRE0000002
TowerB	CXG-8H1A113	KDTL0000003

The Connect link to the right of a network address in the list allows access to the Sentry firmware Web interface. Login to the firmware is required.

The link uses http/https (with Wi-Fi) and the port, as configured on the firmware. If both http and https are enabled, https will be used.

Your Android device must be connected to the wireless network in the data center to allow access to the firmware.

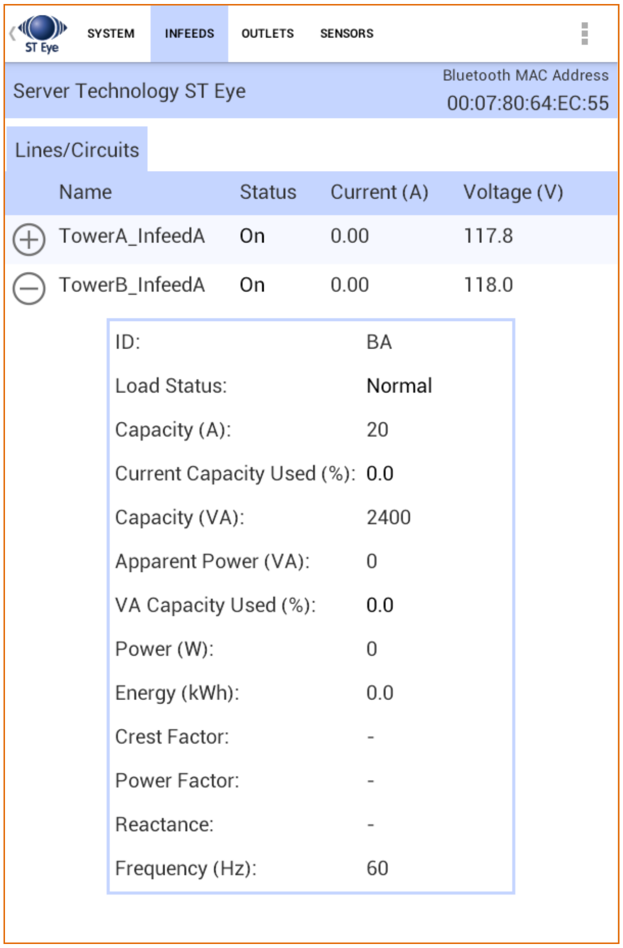
Both IPv4 and IPv6 IP addresses can be displayed in the device list.

Device View – Infeeds Tab

Provides the operational details for single-phase and 3-phase infeeds.

Single Phase – with expanded details

Shows device details for lines/circuits.



Server Technology ST Eye

Bluetooth MAC Address
00:07:80:64:EC:55

	Name	Status	Current (A)	Voltage (V)
⊕	TowerA_InfeedA	On	0.00	117.8
⊖	TowerB_InfeedA	On	0.00	118.0

ID:	BA
Load Status:	Normal
Capacity (A):	20
Current Capacity Used (%):	0.0
Capacity (VA):	2400
Apparent Power (VA):	0
VA Capacity Used (%):	0.0
Power (W):	0
Energy (kWh):	0.0
Crest Factor:	-
Power Factor:	-
Reactance:	-
Frequency (Hz):	60

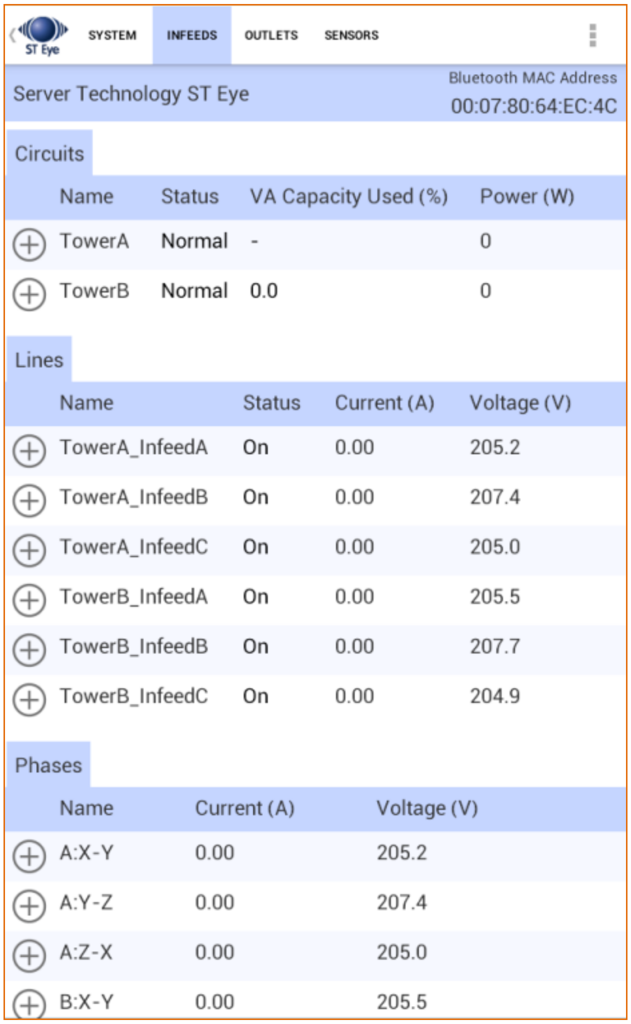
The VA Capacity Used field for line (single-phase) will display in **red** if the value is greater than 80%.

Device View – Infeeds Tab *(continued…)*

3-Phase

Shows data for all three areas of the 3-phase device:

- Circuits
- Lines
- Phases



Server Technology ST Eye

Bluetooth MAC Address
00:07:80:64:EC:4C

Circuits

Name	Status	VA Capacity Used (%)	Power (W)
TowerA	Normal	-	0
TowerB	Normal	0.0	0

Lines

Name	Status	Current (A)	Voltage (V)
TowerA_InfeedA	On	0.00	205.2
TowerA_InfeedB	On	0.00	207.4
TowerA_InfeedC	On	0.00	205.0
TowerB_InfeedA	On	0.00	205.5
TowerB_InfeedB	On	0.00	207.7
TowerB_InfeedC	On	0.00	204.9

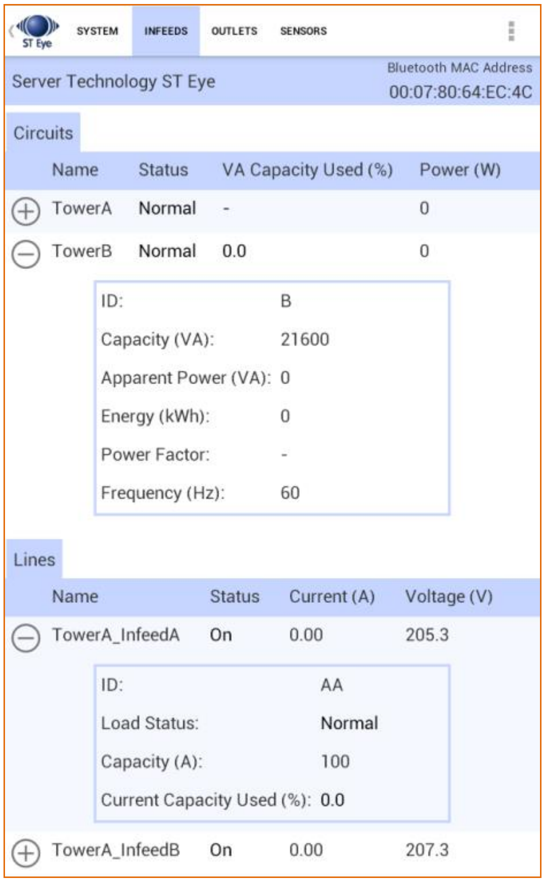
Phases

Name	Current (A)	Voltage (V)
A:X-Y	0.00	205.2
A:Y-Z	0.00	207.4
A:Z-X	0.00	205.0
B:X-Y	0.00	205.5

Device View – Infeeds Tab *(continued…)*

3-Phase – with expanded circuit/line details

Shows details expanded for a circuit and a line:



Server Technology ST Eye

Bluetooth MAC Address
00:07:80:64:EC:4C

Circuits

	Name	Status	VA Capacity Used (%)	Power (W)
⊕	TowerA	Normal	-	0
⊖	TowerB	Normal	0.0	0

ID:	B
Capacity (VA):	21600
Apparent Power (VA):	0
Energy (kWh):	0
Power Factor:	-
Frequency (Hz):	60

Lines

	Name	Status	Current (A)	Voltage (V)
⊖	TowerA_InfeedA	On	0.00	205.3

ID:	AA
Load Status:	Normal
Capacity (A):	100
Current Capacity Used (%):	0.0

	Name	Status	Current (A)	Voltage (V)
⊕	TowerA_InfeedB	On	0.00	207.3

For the Circuits:

- The Capacity (VA) field for a circuit will display in red if the value is greater than 80%.
- Circuit (3 phase) status is No Comm, Fan Fail, Over Temp.
- Circuit (3 phase) VA Capacity Used is greater than 80%.

For the Lines:

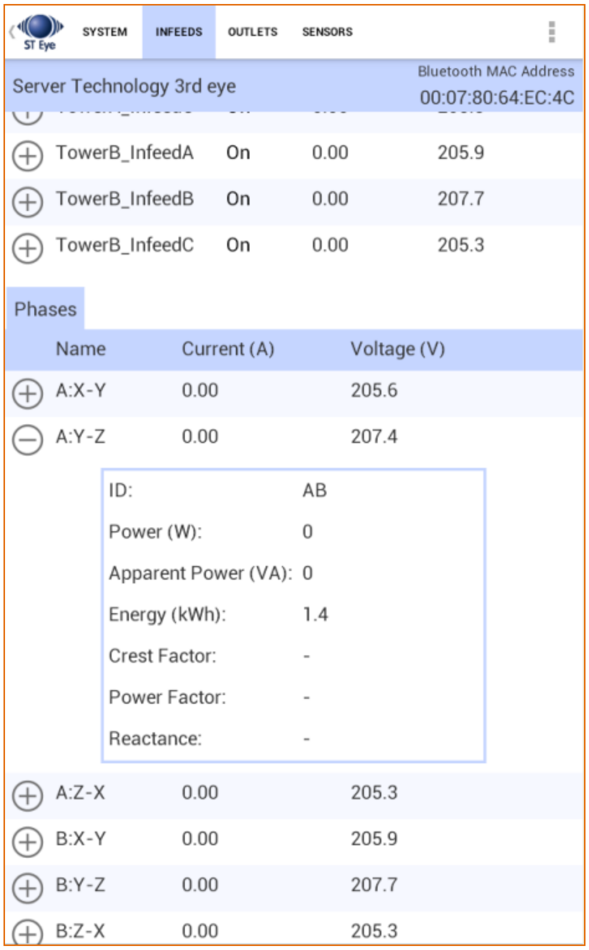
The following Line values will display in red if:

- Line Load Status is Overload, Read Error, No Comm.
- Line Status is Off/Error, On/Error, No Comm, Off/Fuse, On/Fuse.
- Line Current Capacity Used is greater than 80%.

Device View – Infeeds Tab *(continued…)*

3-Phase – with expanded phase details

Shows details expanded for one of the phases:



Server Technology 3rd eye

Bluetooth MAC Address
00:07:80:64:EC:4C

⊕	TowerB_InfeedA	On	0.00	205.9
⊕	TowerB_InfeedB	On	0.00	207.7
⊕	TowerB_InfeedC	On	0.00	205.3

Phases

	Name	Current (A)	Voltage (V)
⊕	A:X-Y	0.00	205.6
⊖	A:Y-Z	0.00	207.4

ID:	AB
Power (W):	0
Apparent Power (VA):	0
Energy (kWh):	1.4
Crest Factor:	-
Power Factor:	-
Reactance:	-

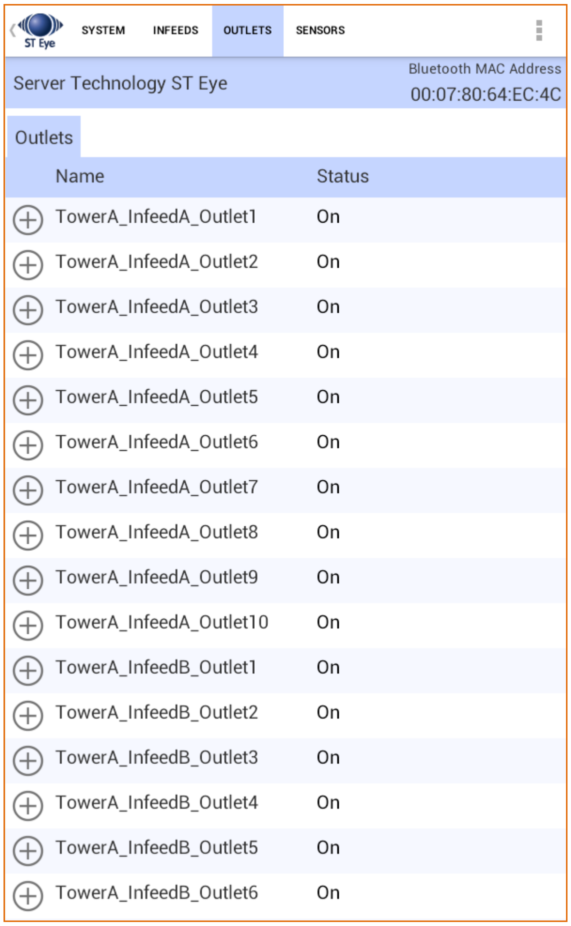
⊕	A:Z-X	0.00	205.3
⊕	B:X-Y	0.00	205.9
⊕	B:Y-Z	0.00	207.7
⊕	B:Z-X	0.00	205.3

Device View – Outlets Tab

Provides a list of outlets in the CDU. All outlets in each tower are displayed.

List of Non-POPS Outlets

Shows the outlets in a Non-POPS CDU:



Server Technology ST Eye

Bluetooth MAC Address 00:07:80:64:EC:4C

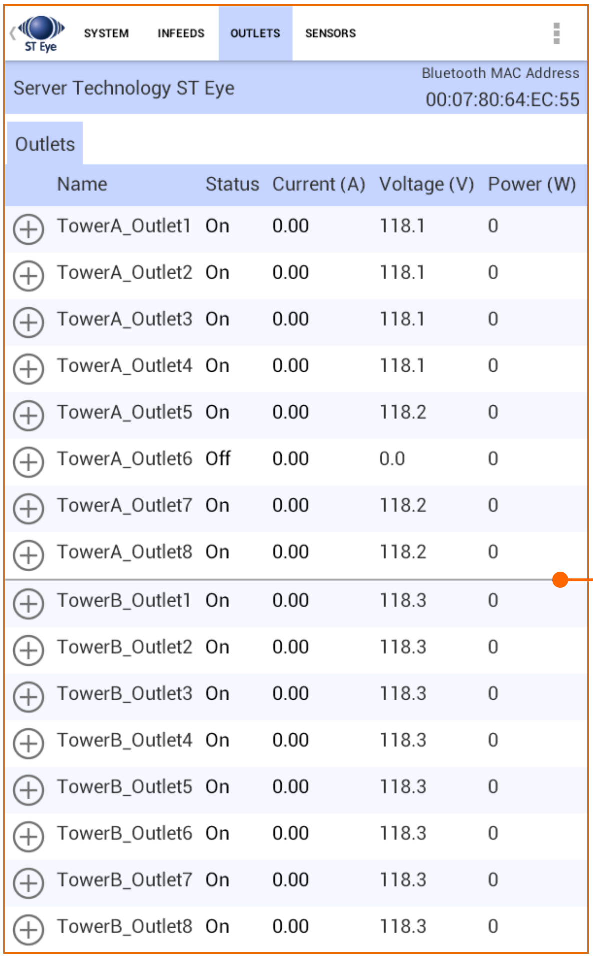
Outlets

Name	Status
TowerA_InfeedA_Outlet1	On
TowerA_InfeedA_Outlet2	On
TowerA_InfeedA_Outlet3	On
TowerA_InfeedA_Outlet4	On
TowerA_InfeedA_Outlet5	On
TowerA_InfeedA_Outlet6	On
TowerA_InfeedA_Outlet7	On
TowerA_InfeedA_Outlet8	On
TowerA_InfeedA_Outlet9	On
TowerA_InfeedA_Outlet10	On
TowerA_InfeedB_Outlet1	On
TowerA_InfeedB_Outlet2	On
TowerA_InfeedB_Outlet3	On
TowerA_InfeedB_Outlet4	On
TowerA_InfeedB_Outlet5	On
TowerA_InfeedB_Outlet6	On

Device View – Outlets Tab *(continued…)*

List of POPS Outlets

Shows the outlets in a POPS CDU:



Server Technology ST Eye

Bluetooth MAC Address
00:07:80:64:EC:55

Outlets

Name	Status	Current (A)	Voltage (V)	Power (W)
TowerA_Outlet1	On	0.00	118.1	0
TowerA_Outlet2	On	0.00	118.1	0
TowerA_Outlet3	On	0.00	118.1	0
TowerA_Outlet4	On	0.00	118.1	0
TowerA_Outlet5	On	0.00	118.2	0
TowerA_Outlet6	Off	0.00	0.0	0
TowerA_Outlet7	On	0.00	118.2	0
TowerA_Outlet8	On	0.00	118.2	0
TowerB_Outlet1	On	0.00	118.3	0
TowerB_Outlet2	On	0.00	118.3	0
TowerB_Outlet3	On	0.00	118.3	0
TowerB_Outlet4	On	0.00	118.3	0
TowerB_Outlet5	On	0.00	118.3	0
TowerB_Outlet6	On	0.00	118.3	0
TowerB_Outlet7	On	0.00	118.3	0
TowerB_Outlet8	On	0.00	118.3	0

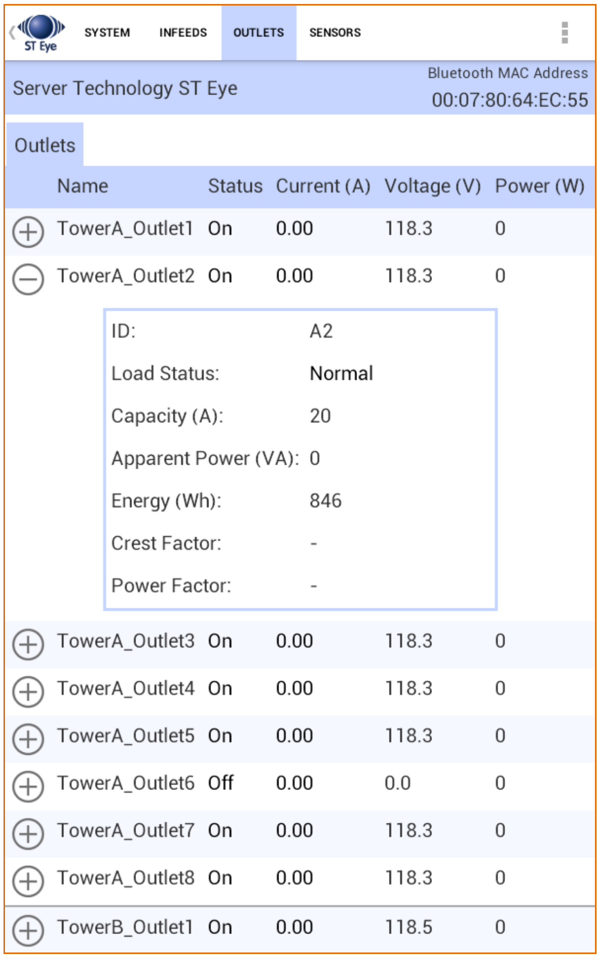
The outlets in the list are displayed within their tower.

A horizontal line separates outlets in different towers, like TowerA outlets are separated from TowerB outlets in this example.

Device View – Outlets Tab *(continued…)*

List of POPS Outlets – with expanded outlet details

Shows the expanded details for an outlet in a POPS CDU:



Server Technology ST Eye

Bluetooth MAC Address
00:07:80:64:EC:55

Outlets

Name	Status	Current (A)	Voltage (V)	Power (W)
⊕ TowerA_Outlet1	On	0.00	118.3	0
⊖ TowerA_Outlet2	On	0.00	118.3	0

ID:	A2
Load Status:	Normal
Capacity (A):	20
Apparent Power (VA):	0
Energy (Wh):	846
Crest Factor:	-
Power Factor:	-

Name	Status	Current (A)	Voltage (V)	Power (W)
⊕ TowerA_Outlet3	On	0.00	118.3	0
⊕ TowerA_Outlet4	On	0.00	118.3	0
⊕ TowerA_Outlet5	On	0.00	118.3	0
⊕ TowerA_Outlet6	Off	0.00	0.0	0
⊕ TowerA_Outlet7	On	0.00	118.3	0
⊕ TowerA_Outlet8	On	0.00	118.3	0
⊕ TowerB_Outlet1	On	0.00	118.5	0

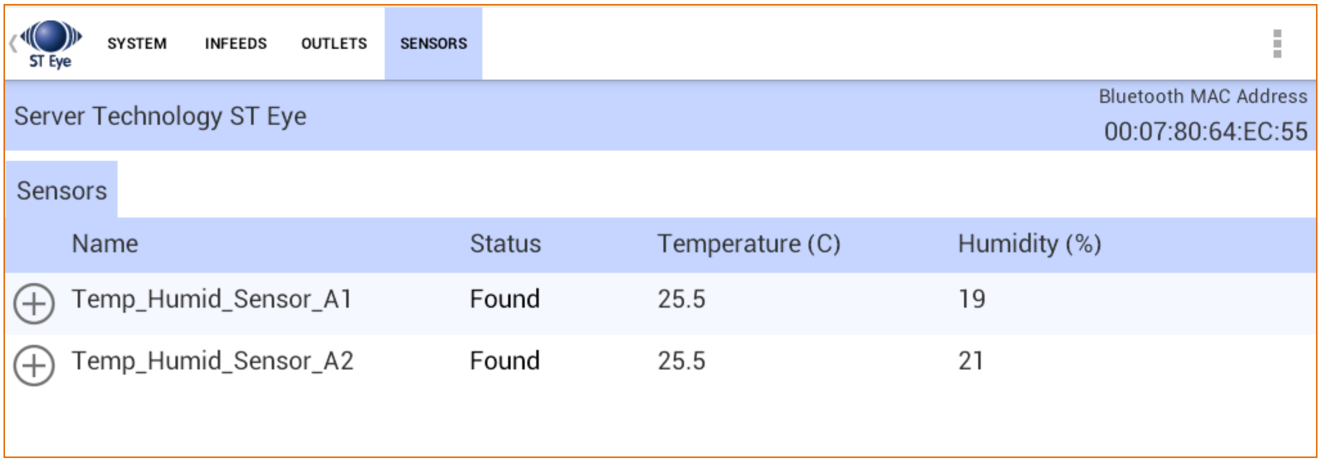
Details reported from the CDU show outlet ID and the POPS data fields.

The following values will display in red if:

- Outlet Load Status is Overload, Read Error, No Comm.
- Outlet Status is Off/Error, On/Error, No Comm, Off/Fuse, or On/Fuse.
- Outlet Load is greater than 80% of the capacity.

Device View – Sensors Tab

Shows the current status of an environmental sensor. Descriptive sensor name is displayed along with sensor readings for temperature and humidity.



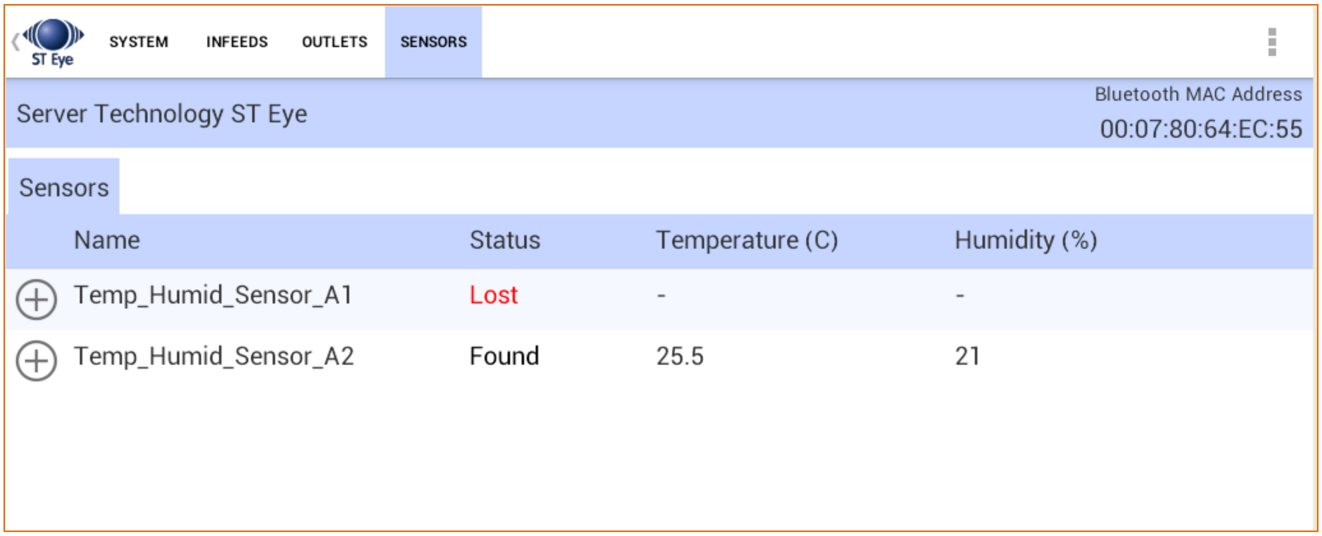
Server Technology ST Eye

Bluetooth MAC Address
00:07:80:64:EC:55

Sensors

Name	Status	Temperature (C)	Humidity (%)
Temp_Humid_Sensor_A1	Found	25.5	19
Temp_Humid_Sensor_A2	Found	25.5	21

Each sensor is displayed in Celsius or Fahrenheit, as Celsius is shown in the example above for temperature value. If no sensors are found, the Sensors screen will be blank.



Server Technology ST Eye

Bluetooth MAC Address
00:07:80:64:EC:55

Sensors

Name	Status	Temperature (C)	Humidity (%)
Temp_Humid_Sensor_A1	Lost	-	-
Temp_Humid_Sensor_A2	Found	25.5	21

If sensor status is Lost or No Comm, the status field is displayed in red, as shown above.

Configuring Bluetooth® Parameters Using Sentry Firmware

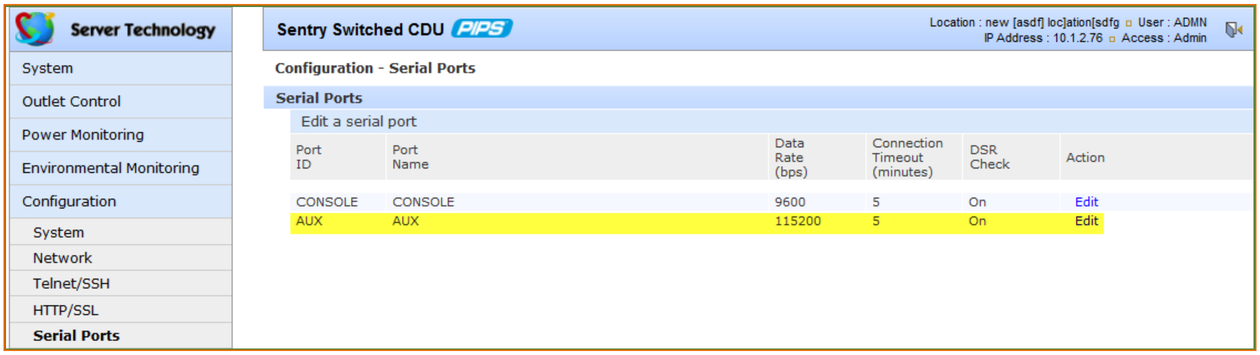
If a CDU has been equipped for the mobile monitoring solution using Bluetooth ® technology, the AUX serial port will be installed on the CDU, and the following parameters will be available in the Sentry firmware, version 7.0j or later, for configuration by the administrative-user account.

Firmware Bluetooth Parameters	
Parameter	**Description and Valid Values/Range**
The Bluetooth Module Name	Descriptive name of the Bluetooth module that displays in the list of discovered modules on the Android device. The default module name is "ST Eye". The name cannot be blank; maximum length is 31 characters.
Discoverability Status	Settings that determine the current status of the pushbutton on the Bluetooth module. • Always – The Bluetooth module is discoverable, even without pressing the pushbutton. • Limited – (Default). The pushbutton on the Bluetooth module must be pressed to make the module discoverable for 60-seconds. • Never – The Bluetooth module is never in discoverable mode.
Pin Code	The pin code is available for legacy Bluetooth modules that require a pin to pair the module. Although not used in current Bluetooth modules, the pin code is supported if needed. Default is 9611; must be 4-digits; range is 0000 to 9999.
Transmission Power	Designated transmission power (dbm) for the Bluetooth module. Note that lowering the transmission power reduces the effective range of the module. Range is -6 to 4 dbm; default is 0.

The Bluetooth parameters can be configured using either the Web Interface or Command Line Interface (CLI) of the Sentry firmware as described below.

From the Web Interface

Step 1. Go to **Configuration > Serial Ports:**



Location : new [asdf] loc]ation[sdfg User : ADMN
IP Address : 10.1.2.76 Access : Admin

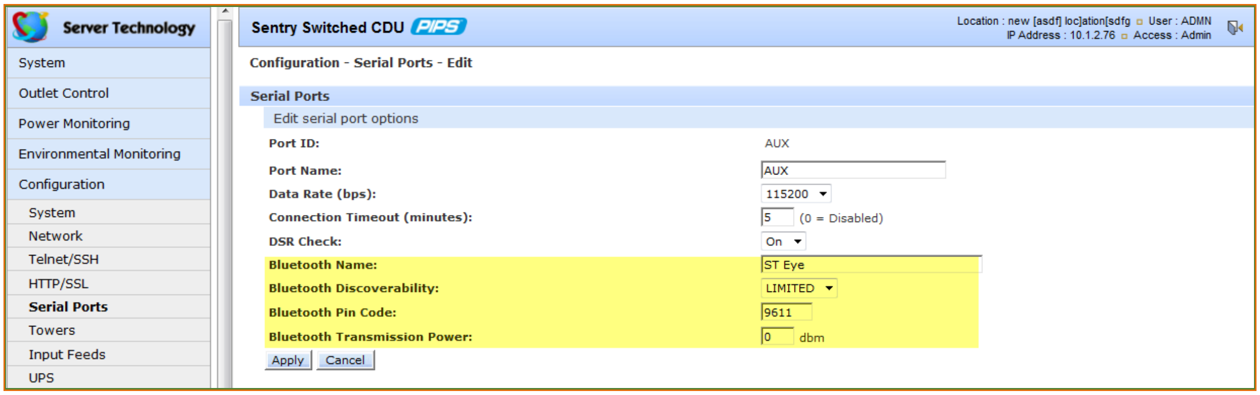
Configuration - Serial Ports

Serial Ports

Edit a serial port

Port ID	Port Name	Data Rate (bps)	Connection Timeout (minutes)	DSR Check	Action
CONSOLE	CONSOLE	9600	5	On	Edit
AUX	AUX	115200	5	On	Edit

Step 2. For the AUX port, click the **Edit** link.



Configuration - Serial Ports - Edit

Serial Ports

Edit serial port options

Port ID:	AUX
Port Name:	AUX
Data Rate (bps):	115200
Connection Timeout (minutes):	5 (0 = Disabled)
DSR Check:	On
Bluetooth Name:	ST Eye
Bluetooth Discoverability:	LIMITED
Bluetooth Pin Code:	9611
Bluetooth Transmission Power:	0 dbm

Step 3. On the Edit page for the AUX port, configure the Bluetooth® parameter fields for name, discoverability, pin code, and transmission power using the values and ranges as noted in the previous table.

From the CLI

Step 1. At the Switched CDU: (or Smart CDU:) prompt (using the values and ranges noted in the previous table), issue one or more of the following commands, as needed:

`set bluetooth name` – Provide a custom descriptive name for the Bluetooth® module.

`set bluetooth discover` – Enter “always”, “limited”, or “never” for the discoverability status of the module.

`set bluetooth pincode` – Configure a 4–digit numeric value for the pincode of a legacy module.

`set bluetooth transpwr` – Designate transmission power (dbm) for the module.

Regulatory Compliance

Federal Communications Commission (FCC)

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Contact Technical Support

Experience Server Technology's FREE Technical Support

Server Technology understands that there are often questions when installing and/or using a new product. Free Technical Support is provided from 8 a.m. to 5 p.m. PST, Monday through Friday. After-hours service is provided to ensure your requests are handled quickly no matter what time zone or country you are located in.

Server Technology, Inc.

1040 Sandhill Drive	Tel:	1-800-835-1515	Web:	www.servertech.com
Reno, Nevada 89521 USA	Fax:	775-284-2065	Email:	support@servertech.com

Server Technology, the Globe logo, Sentry, Switched CDU, CDU, PRO2, PIPS, POPS, PDU Power Pivot, and StartUp Stick are trademarks of Server Technology, Inc., registered in the US. EZip is a trademark of Server Technology.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Server Technology, Inc. disclaims any proprietary interest in trademarks and trade names other than its own.