PRO2

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 PRO2 for mobile access that provides fast viewing of device operational data.

Using Server Technology's ST Eye mobile app, version 2.0, you can remotely monitor critical information about a PRO2 unit – 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 PRO2.

- 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 PRO2 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 PRO2. 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 PRO2 (via the network or serial port) to obtain PRO2 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 PRO2 via the secure web interface of the Sentry firmware.

System Overview

The following system illustration identifies the key hardware and software components:
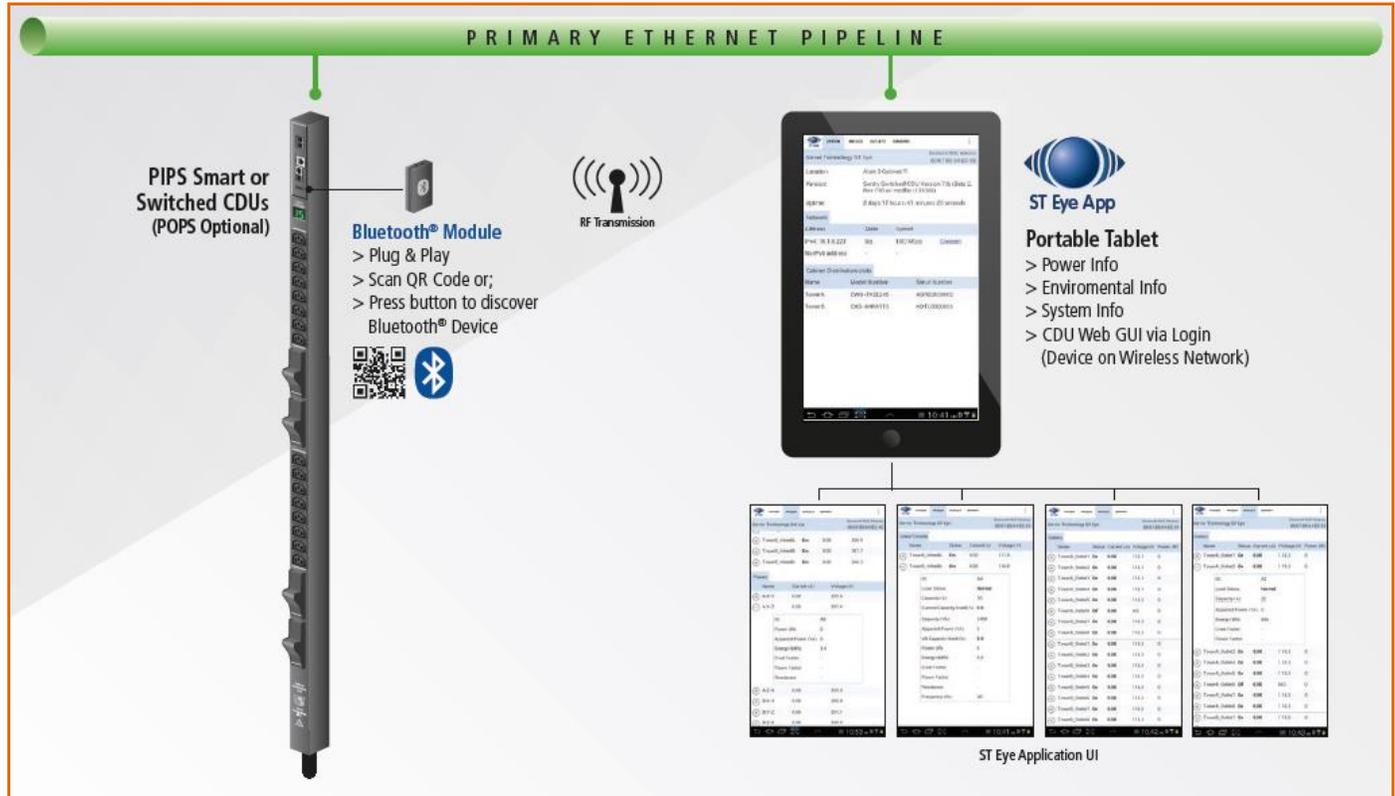
Figure 1. System Overview of Mobile Monitoring Using Bluetooth® Wireless Technology

System Components

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

Server Technology PRO2

Server Technology's intelligent Switched or Smart PRO2 (standard PIPS-enabled) and ready-made for connection to the Bluetooth® module.

The Bluetooth® Module

The separate, external Bluetooth wireless device connected to the PRO2 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 PRO2 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 PRO2.

- 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 PRO2 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 port on the PRO2 unit, 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** PRO2 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 PRO2 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 PRO2.

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** PRO2 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 PRO2 Units

Server Technology's intelligent PRO2 units (Smart or Switched products) with standard Power Infeed Power Sensing (PIPS) technology.

Note: Power Infeed Power Sensing (PIPS) is standard and enabled on all shipped PRO2 units. PIPS technology provides power monitoring per infeed/inlet to the PRO2 to monitor current, voltage, power (W), apparent power, crest factor, reactance, power factor, and accumulated energy (kWh).

Sentry Firmware

Sentry firmware, version 8.0 or later, is required to allow configuration of several parameters used in the solution. The PRO2 products will only operate with firmware 8.0.

Mobile Device

An Android mobile device, version 2.3.3 or later, to use for camera-scanning of QR Code labels and for displaying PRO2 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:

- Switched or Smart PRO2 (standard PIPS-enabled), and

- Hardware kit (part number KIT-STEYE-10) with a 10-foot locking cable.

Note: KIT-STEYE-01 (with a 1-foot locking cable) or KIT-STEYE-10 (with a 10-foot locking cable) can be purchased separately as an optional accessory without a PRO2.

Both hardware kits (KIT-STEYE-01 and KIT-STEYE-10) 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 PRO2. One end of the cable connects to the module and the other end connects to the Bluetooth port on the PRO2.

- Part number KIT-STEYE-10 – contains a 10' cable (bundled with the PRO2 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 PRO2. A factory-placed QR Code label on the module contains specific NIC information that ties the label to the Bluetooth module.

Figure 2. Bluetooth Module (showing connection to the PRO2)

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 standard PIPS-enabled PRO2 to the separate Bluetooth® module:


The PIPS-enabled PRO2 Bluetooth 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 PRO2 to identify the device as ready to be used in the mobile solution.

Discoverability of the Bluetooth® Module

The Bluetooth® module communicates with the PRO2 to establish a secure Bluetooth connection that makes operational data from the PRO2 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.
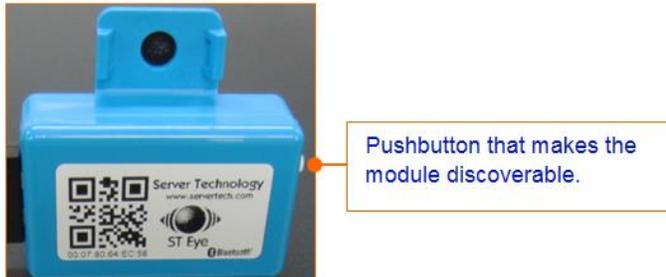
Figure 4. Close-up of the Bluetooth Module (showing QR code label and pushbutton)

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 8.0 or later, uses the following user-configured settings to set the discoverability status of the module:

Firmware Discoverability Settings	
Setting	**Description**
Enabled	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.
Disabled	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.

Discovering a Bluetooth® Module:

For a Bluetooth module to be discovered, the ST Eye app must be installed on the iPad/iPhone, and the module must be in a discoverable state – this means a flashing light on the module. The firmware setting that determines the status of the module must be Enabled or Limited (default). The setting cannot be Disabled.

Working with the ST Eye Mobile App

Server Technology's ST Eye app works over a secure connection with Bluetooth® wireless technology to locate PRO2 units in your data center for the mobile monitoring solution. ST Eye collects key operational data from the units 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 the Bluetooth port of a PRO2 unit (already PIPS-enabled).

☑ (Optional) Placed the separate QR Code label (received in the hardware kit) anywhere on the PRO2 or cabinet.

☑ (Optional) Configured the Bluetooth module discoverability state (Enabled, Limited, Disabled) using Sentry firmware.

Note: The Bluetooth module and the Sentry firmware, version 8.0 or later, ship with the default "Limited" discoverability setting (requires pushbutton to be pressed when discovering the module.) For a description of the settings, see the Firmware Discoverability Settings 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 "Enabled" or "Limited"; the setting cannot be "Disabled"). 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:

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 PRO2 data, refreshing the screen data every 10-seconds.

ST Eye's Device View opens with the default System tab to display PRO2 general system information:
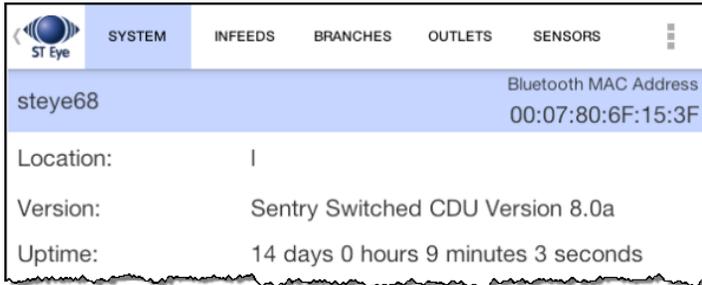
Step 4. You can now navigate the System, Infeeds, Branches, Outlets, and Sensors tabs to view additional device details.

**Note:** PRO2 information is available for view-only; no control actions on the PRO2 can be performed.

Connecting with a QR Code Label

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

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 PRO2 information in the default System tab, and refreshes displayed data every 10-seconds.
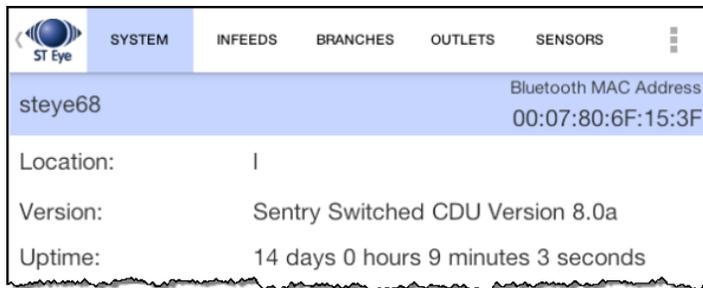
Step 4. You can now navigate the System, Infeeds, Branches, Outlets, and Sensors tabs to view additional device details about the PRO2 unit.

Note: PRO2 information is available for view-only; no control actions on the PRO2 unit 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 (discovery) screen

- Camera View – Camera on the Android device for scanning QR Code labels

- Device View – System, Infeed, Branches, Outlet, and Sensor tabs displaying detailed PRO2 information.

Main View – Discovery Screen

The Main View shows one or more discovered Bluetooth® modules.
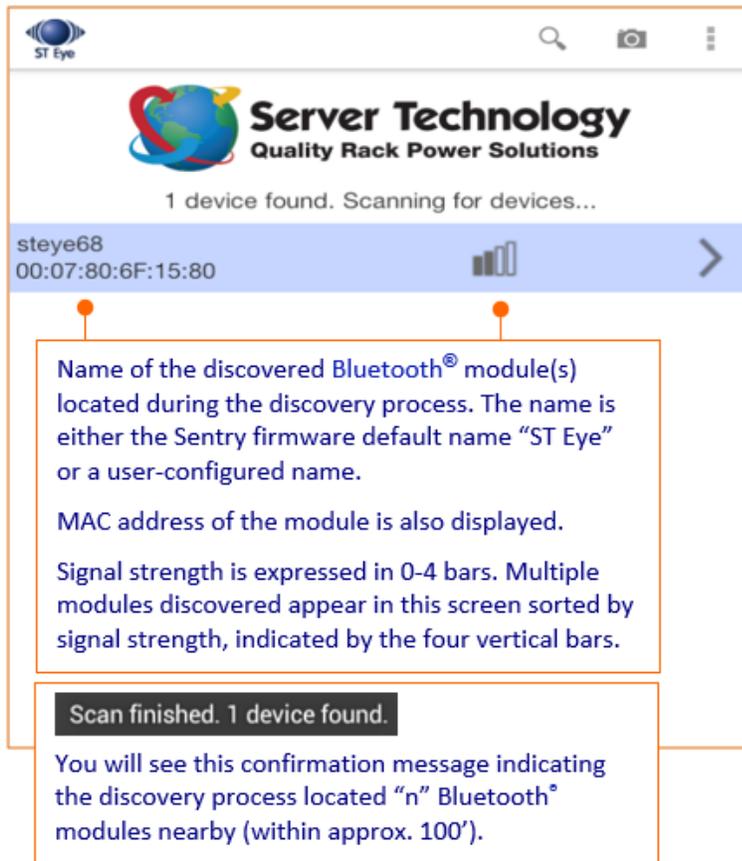
Search. Opens a search box to allow searching a device list; filters the list as you type.

Refresh. Starts another discovery for a Bluetooth® module. To discover the module, you will need to press the pushbutton on the module to allow the module to be discovered. Note that when a discovery is in procress, the Refresh button will be 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 PRO2 unit 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).

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

Scan finished. 1 device found.

You will see this confirmation message indicating the discovery process located "n" Bluetooth® modules nearby (within approx. 100').

Device View – Information Tabs

Operational data collected from a PRO2 displays as soon as the unit is connected. The data appears in a ribbon of five separate information tabs on the Android screen, opening at the (default) System tab:

System: Default display tab; shows general, non-power information about a PRO2 (location, version, uptime), and provides separate sections for network and unit information. Each unit in the list provides a link for direct connection to the Web interface login for Sentry firmware.

Infeeds: The operational details for the PRO2's cords, lines, and phases (for single-phase and 3-phase system) are separated into sections and displayed on the Infeeds screen.

Branches: The PRO2 measures every breaker and lists branches and over-current protectors (OCPs) together on this screen with a separate section for branches and OCPs, showing capacity, status, and current. If the PRO2 has no OCPs, then the OCP section will be blank.

Outlets: Provides a list of outlets in each PRO2 unit, showing status, current(A), and power(W). Each outlet can be expanded for additional operational data, such as voltage(V), capacity(A), energy(Wh), and more.

Sensors: Temperature and humidity sensors are listed with current status and temperature(C° or F°) and humidity (RH%) readings.

Device View – Expand/Collapse Data Items

To expand and view operational details for an item listed on the screen, click ⊕

To collapse the details, click ⊖

Collapsed view of a branch in the list

Expanded view with branch operational details

Device View – Exceeded Thresholds and Errors

A value will display red on the mobile device if the default (or user-configured) threshold value on the CDU is exceeded, or if a CDU error condition occurs.

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.

Scanning a QR Code label.

You may have a device that shows ST Eye's lightning bolt ⚡ icon. The icon turns on the LED torch mode, which is helpful when scanning a label in a room with dim lighting.

Device View – System Tab (default)

Shows general, non-power information about a PRO2 (location, version, uptime), along with information about the network and the unit.

The device list supports and displays IP addresses for both IPv4 and IPv6.

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.

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

Device View – Infeeds Tab

Arranges PRO2 operational details (for 1-phase and 3-phase systems) under Cords, Lines, and Phases subsections.

Infeeds Tab separates and lists Cords, Lines, and Phases

Device View – Infeeds Tab *(continued…)*

Expanded Infeeds > Cords View

	SYSTEM	INFEEDS	BRANCHES	OUTLETS	SENSORS	

steye68	Bluetooth MAC Address 00:07:80:6F:15:3F

Cords

	Name	Status	VA Capacity Used (%)	Power (W)
⊕	SEV-6503K_Cord_A	Normal	0.00	0
⊕	_Cord_A	Normal	2.09	480

ID:	BA
State:	On
Capacity (VA):	23040
Apparent Power (VA):	481
Energy (kWh):	189.1
Power Factor:	1.00
Frequency (Hz):	60
Balance (%):	20.0

Lines

	Name	State	Current (A)
⊕	AA:L1	On	0.00
⊕	AA:L2	On	0.00
⊕	AA:L3	On	0.00

Device View – Infeeds Tab *(continued…)*

Expanded Infeeds > Lines View

Device View – Infeeds Tab *(continued…)*

Expanded Infeeds > Phases View

	SYSTEM	INFEEDS	BRANCHES	OUTLETS	SENSORS	
ST Eye						

steye68			Bluetooth MAC Address
			00:07:80:6F:15:3F

⊕	BA:N	On	1.90	

Phases

	Name	Status	Current (A)	Voltage (V)
⊕	AA:L1-N	Normal	0.00	234.7
⊕	AA:L2-N	Normal	0.00	235.3
⊕	AA:L3-N	Normal	0.00	233.7
⊕	BA:L1-N	Normal	0.00	235.1
⊖	BA:L2-N	Normal	2.04	235.6

ID:	BA2
State:	On
Power (W):	480
Apparent Power (VA):	480
Energy (kWh):	81.9
Crest Factor:	1.5
Power Factor:	1.00
Reactance:	Resistive
Voltage Deviation (%):	-1.9

⊕	BA:L3-N	Normal	0.00	234.1

Device View – Branches Tab

Provides a separate list of over-current protectors (OCPs) and branches.

Subsections for Over-Current Protectors (OCPs) and Branches

| ST Eye | SYSTEM | INFEEDS | BRANCHES | OUTLETS | SENSORS | ⋮ |

| steye68 | Bluetooth MAC Address 00:07:80:6F:15:3F |

Over-Current Protectors

	Name	Status	Current (A)
⊕	AA:Branch_1	Normal	0.00
⊕	AA:Branch_2	Normal	0.00
⊕	AA:Branch_3	Normal	0.00
⊕	AA:Branch_4	Normal	0.00
⊕	AA:Branch_5	Normal	0.00
⊕	AA:Branch_6	Normal	0.00
⊕	BA:Branch_1	Normal	0.00
⊕	BA:Branch_2	Normal	0.00
⊕	BA:Branch_3	Normal	0.00
⊕	BA:Branch_4	Normal	1.97
⊕	BA:Branch_5	Normal	0.00
⊕	BA:Branch_6	Normal	0.00

Branches

	Name	Capacity (A)	Status
⊕	AA:Breaker_1	30	Normal
⊕	AA:Breaker_2	30	Normal

Server Technology, Inc.   Technical Note

Device View – Branches Tab *(continued…)*

Expanded Over-Current Protector (OCP) View

	SYSTEM	INFEEDS	BRANCHES	OUTLETS	SENSORS	

steye68 — Bluetooth MAC Address 00:07:80:6F:15:3F

Over-Current Protectors

Name	Status	Current (A)
⊕ AA:Branch_1	Normal	0.00
⊕ AA:Branch_2	Normal	0.00
⊕ AA:Branch_3	Normal	0.00
⊕ AA:Branch_4	Normal	0.00
⊕ AA:Branch_5	Normal	0.00
⊕ AA:Branch_6	Normal	0.00
⊕ BA:Branch_1	Normal	0.00
⊕ BA:Branch_2	Normal	0.00
⊕ BA:Branch_3	Normal	0.00
⊖ BA:Branch_4	Normal	1.97

ID:	BA4
State:	On
Current Capacity Used (%):	6.5

⊕ BA:Branch_5	Normal	0.00
⊕ BA:Branch_6	Normal	0.00

Branches

Device View – Branches Tab *(continued…)*

Expanded Branches View

SYSTEM	INFEEDS	BRANCHES	OUTLETS	SENSORS

steye68　　　　　　　　　　　Bluetooth MAC Address
　　　　　　　　　　　　　　　00:07:80:6F:15:3F

	BA:Branch_5	Normal	0.00
⊕	BA:Branch_6	Normal	0.00

Branches

	Name	Capacity (A)	Status
⊕	AA:Breaker_1	30	Normal
⊕	AA:Breaker_2	30	Normal
⊕	AA:Breaker_3	30	Normal
⊕	AA:Breaker_4	30	Normal
⊕	AA:Breaker_5	30	Normal
⊕	AA:Breaker_6	30	Normal
⊕	BA:Breaker_1	30	Normal
⊖	BA:Breaker_2	30	Normal

ID:　　BA2
State:　On

⊕	BA:Breaker_3	30	Normal
⊕	BA:Breaker_4	30	Normal
⊕	BA:Breaker_5	30	Normal
⊕	BA:Breaker_6	30	Normal

Device View – Outlets Tab

Shows a list of all outlets in the PRO2 unit.

Outlets List

	Name	State	Status	Current (A)	Power (W)
⊕	SEV-6503K_Outlet_A1	Idle On	Normal	0.00	0
⊕	SEV-6503K_Outlet_A2	Idle On	Normal	0.00	0
⊕	SEV-6503K_Outlet_A3	Idle On	Normal	0.00	0
⊕	SEV-6503K_Outlet_A4	Idle On	Normal	0.00	0
⊕	SEV-6503K_Outlet_A5	Idle On	Normal	0.00	0
⊕	SEV-6503K_Outlet_A6	Idle On	Normal	0.00	0
⊕	SEV-6503K_Outlet_A7	Idle On	Normal	0.00	0
⊕	SEV-6503K_Outlet_A8	Idle On	Normal	0.00	0
⊕	SEV-6503K_Outlet_A9	Idle On	Normal	0.00	0
⊕	SEV-6503K_Outlet_A10	Idle On	Normal	0.00	0
⊕	SEV-6503K_Outlet_A11	Idle On	Normal	0.00	0

(Device screen header: ST Eye | SYSTEM | INFEEDS | BRANCHES | OUTLETS | SENSORS)

steye68   Bluetooth MAC Address 00:07:80:6F:15:3F

Outlets

Device View – Outlets Tab *(continued…)*

Outlets Expanded View

If the PRO2 unit is POPS-enabled, the Outlets list will also display values for Current Capacity and Reactance.

Device View – Sensors Tab

Provides a separate list of Temper.

Subsections for Temperature and Humidity Sensors

Shows the current status and readings of environmental sensors.

Sensors are shown in Celsius or Fahrenheit (depending on Scale used),

If no sensors are found, the Sensors screen will be blank.

Configuring Bluetooth® Parameters Using Sentry Firmware

The following Bluetooth parameters are available in the firmware and can be configured (using GUI or CLI) by the administrative-user account as described:

Firmware Bluetooth Parameters	
Parameter	**Description and Valid Values/Range**
Enable	The PRO2 using Sentry firmware 8.0 is shipped with Bluetooth® enabled by default.
Name	Descriptive name of the Bluetooth module that displays at the top of the list of discovered modules on the Android device. The default is blank; maximum length is 31 characters.
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.
Discoverability	Settings that determine the current status of the pushbutton on the Bluetooth module. • Enabled – 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. • Disabled – The Bluetooth module is never in discoverable mode.
Transmission Power	Designated transmission power (dbm) for the Bluetooth module. Lowering the transmission power reduces the effective range of the module. Range is -6 to 4 dbm; default is 0.

From the GUI:

Step 1. Go to **System > Bluetooth:**
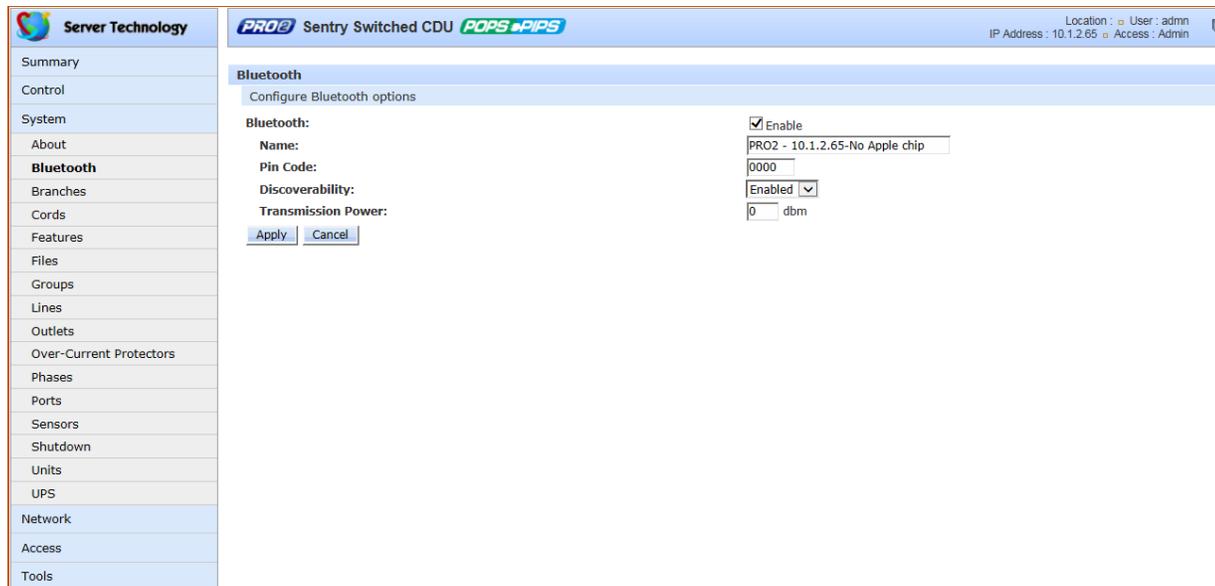
Step 1. Enable/disable Bluetooth, and configure name, pin code, discoverability, and transmission power as described above.

Step 2. Click **Apply**.

From the CLI:

At the Switched CDU: (or Smart CDU:) prompt, type the following commands:

Enable/disable the Bluetooth wire-free solution:

Type **set bluetooth** followed by **enabled** or **disabled** and press **Enter**.

Provide a custom name for the Bluetooth module:

Type **set bluetooth name** and press **Enter**.   Default is blank; maximum length is 31 characters.

Set the pin code:

Type **set bluetooth pincode** and press **Enter**. Default is 9611; must be 4-digits; range is 0000 to 9999.

Configure discoverability status of the Bluetooth module:

Type **set bluetooth discover** followed by **disabled**, **enabled**, or **limited,** and press **Enter**.

Designate transmission power for the Bluetooth module:

Type **set bluetooth transpwr** and press **Enter**. Default is 0; range is -6 to 4 dbm.

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 |