centrica
Business Solutions

May 2021

Centrica Business Solutions

PowerRadar® Security Overview

Updated May 2021 (for bridge firmware V470 or higher)

Table of Contents

About us	**2**
Our sensor security principles	**3**
Sensor to Bridge data flow	**4**
Bridge to Cloud data flow	**5**
Choosing the right cloud connectivity mode	**6**
Confirming the bridge-cloud connection security	**8**
Our cloud security principles	**9**
Inbound bridge servers	**10**
Our privacy policy	**10**
Frequently asked questions	**10**

1. About us

Centrica Business Solutions is part of Centrica plc, a global energy and services company, dedicated to satisfying the changing needs of our customers:

- Well-established, 200-year old, FTSE 100 company
- £28bn revenues in 2016
- 28m Centrica customer accounts mainly in the UK, Ireland and North America
- 12,000 Centrica engineers and technicians

Centrica Business Solutions provides innovative, end-to-end distributed energy solutions to organisations enabling them to improve operational efficiency, increase resilience and drive their business vision forward.

Panoramic Power is the brand name for our energy insight solution powered by our hardware sensors and bridges.

PowerRadar® is the brand name for the *Centrica Business Solutions* cloud platform.

Our energy insight solution, driven by Panoramic Power hardware and the PowerRadar cloud platform, lets our customers see exactly how their business uses energy – right down to device level. It gives our customers the energy intelligence they need to reduce wasted power and improve their operational efficiency.

At *Centrica Business Solutions* we understand the sensitivity and criticality of data and network security. Therefore, we have taken relevant measures to secure our devices that are deployed to your network and around your critical assets.. We secure, manage and monitor account access and activities across the entire deployment process.

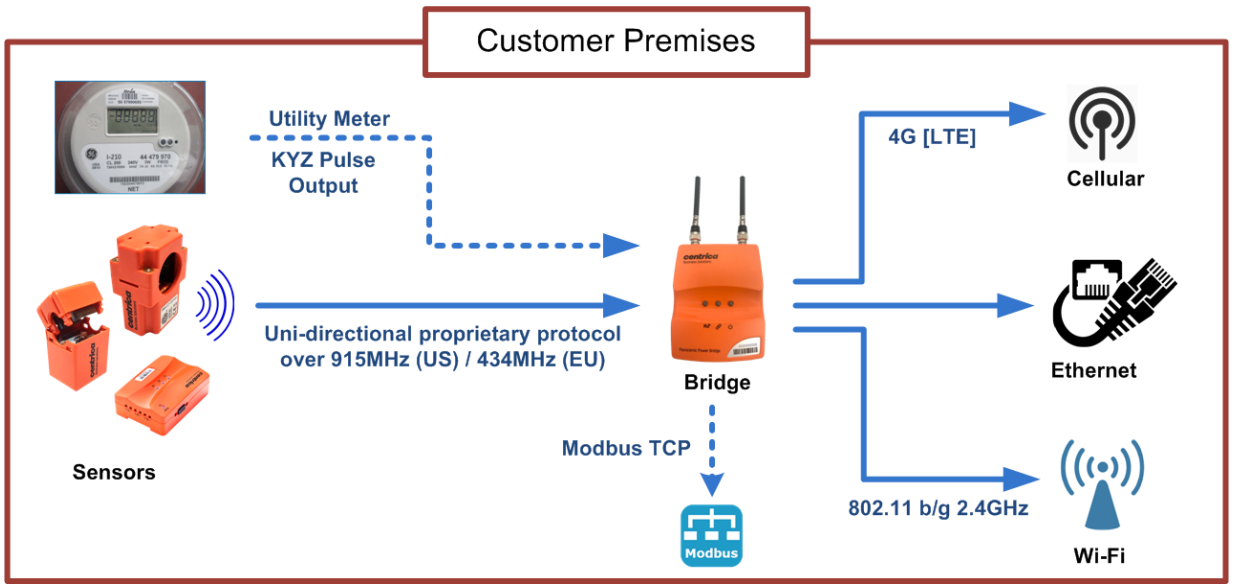
2. Our sensor security principles

To achieve a secure environment to our customers, we have adopted a few security guidelines:

- **Data sensitivity classification -** The Panoramic Power sensors measure and transmit energy readings at a predefined interval. The coded information only contains the sensor ID and the electrical measurements (current, voltage, power, etc.). Any machine or device-specific information such as the type and name of the monitored devices, site name etc. is maintained separately in the PowerRadar secured cloud servers. By enforcing this separation between business data and real-time energy measurements, we eliminate information disclosure or leakage in the unlikely event that the outbound transmission of the data packet is intercepted.
- **Non-intrusive sensors -** Panoramic Power's current sensors (PAN-10, 12 & 14) use the electromagnetic field generated by the wire to self-power, measure and transmit the current reading. Due to their non-intrusive nature, the sensors do not interact or affect the performance of the devices they are monitoring.
- **Outbound data flow -** The data flow of our sensors and bridges in the installed facility is outbound, decreasing the attack surface of the system.

The rest of this document describes the data flow and the security measures we employ.

3. Sensor to Bridge data flow



Panoramic Power sensors transmit small unidirectional packets over a proprietary protocol in the ISM 915MHz (US) or434 MHz (EU) band. Transmissions are sent 5 to 6 times a minute to a bridge unit.

Sensors cannot receive any incoming communication from the bridge or from any other device. Sensor to bridge transmissions include the sensor ID and the circuit current (Amp) reading and do not include any customer information such as circuit name and type, site name, etc. The effective distance between the sensor and the bridge is typically 16 feet (5 meters) but may be shorter depending on the installed environment.

4. Bridge to Cloud data flow

The bridge collects the sensor transmissions and conveys them to the PowerRadar cloud. The bridge can convey the sensors' transmissions using one of the following options:

- Wi-Fi (802.11b/g, 2.4GHz)
- Ethernet
- Cellular (GSM/UMTS)

When using Wi-Fi, the following security protocols are supported: WPA,WPA2, WPA2 Enterprise (username-password mode), WEP64 and WEP128.
WPA2 Enterprise using client-certificate authentication is currently not supported.

The protocol used for bridge-cloud communications depends bridge hardware and firmware version. As shown in the table below:

Bridge Hardware Version	Firmware Version	Bridge-Cloud Protocol Used
Gen1 or Gen2	any	TCP port 8051
Gen3 or Gen4	2xx	TCP port 8051
Gen3 or Gen4	4xx 7xx	TLS V1.2 over port 443 or TCP port 8051

During normal operations, the bridge communicates with the PowerRadar server using outbound communications. A dedicated configuration mode, switched by pressing a designated button on the bridge, enables bridge configuration via browser and a built-in web server[1].

Bridge firmware upgrades are done via physical connection, inserting a USB stick with the latest firmware into the bridge USB port. Bridges with firmware version V470 and above also support secure over-the-air firmware updates but this functionality can be turned off in the bridge.

Choosing a secure location for the bridge is imperative to preventing unauthorised access to physical ports on the bridge.

[1] Firmware version V470 added the (non default) option to enable bridge configuration also in normal (non config) operating mode.

5. Choosing the right cloud connectivity mode

Ethernet, Wi-Fi, or Cellular connectivity

We provide flexibility for bridge-cloud connectivity. It is ultimately the customer's decision which method to use.

For maximum security, many IT organizations prefer to completely isolate sensor and bridge traffic from the corporate IT network. This can be done using the built-in cellular modem and creates a clear *'air gap'* barrier between the Panoramic Solution and the corporate IT network. Choosing this option also frees the IT organization from managing the connection (e.g. managing firewall rules, managing Wi-Fi password updates, etc).

TCP Vs. TLS connectivity to the cloud

Our latest bridge firmware versions (V409 and above) support two cloud connectivity modes:

- via TCP port 8051
- via TLS V1.2 port 443

Selection between TLS or TCP is done when choosing the cloud address and port in the bridge configuration page.

Protocol	Address to use in the bridge	Port
TCP	col.panpwrws.com	8051
TLS	bridges.powerradar.energy[2]	443

TCP connectivity over port 8051 is provided for backwards compatibility. We strongly recommend using the TLS connectivity method in new installations since it is more secure.

[2] For backwards compatibility, *bridges.**panpwrws.com*** is also supported (and points to the same server) as bridges.**powerradar.energy**.

IT organizations that use the corporate Wi-Fi or Ethernet networks must ensure adequate outbound firewall access.

When using TCP port 8051 for communications with the Powerradar cloud:

- Outbound TCP port 8051
- **From**: any on-premises Panoramic Power bridge
- **To**: col.panpwrws.com (Both IP addresses: 50.17.231.3 and 54.163.225.201)

When using TLS for communications with the Powerradar cloud:

- Outbound TCP port 443
- **From**: any on-premises Panoramic Power bridge
- **To**: bridges.powerradar.energy (IP address may change over time)

To operate properly, the bridge must use accurate time-of-day. The bridge acquires the time via usage of the NTP protocol using public NTP servers. If the NTP port (outbound UDP port 123) is closed, the bridge will acquire[3] the time from the PowerRadar cloud.

- Outbound UDP port 123
- **From**: any on-premises Panoramic Power bridge
- **To**: The relevant public NTP server

It is also possible to provide a custom NTP server address. This should be used when connecting to an NTP server located within the private network.

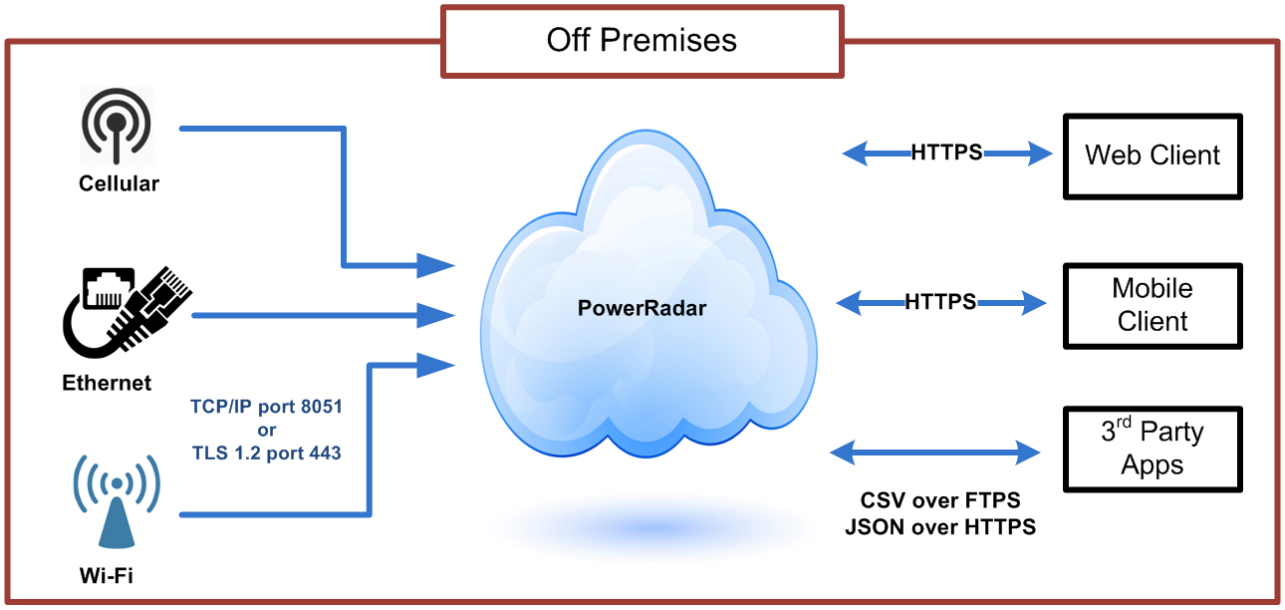
[3] V409 has a known issue that when NTP fails (due to closed ports, for example), the bridge can not connect to the cloud. This is not happening in earlier versions and is fixed in V410 and above

6. Confirming the bridge-cloud connection security

Gen3/4 bridges running firmware version V409 and above, encrypt all bridge-to-cloud communications by default using TLS. Powerradar's **Settings > Bridges** page now contains an indication of the security level of the connection in the model column.

The bridge-cloud connection is authenticated[4] and encrypted (using TLS).

The bridge-cloud connection is authenticated[5] but is not encrypted.



[4] Server side authentication is TLS based, client (bridge) authentication is CHAP based.

[5] Client (bridge) authentication is provided using CHAP.

7. Our cloud security principles

The Centrica Business Solutions PowerRadar solution is hosted at Amazon AWS and utilizes the shared security model enforced by Amazon. Under this model:

- **AWS** is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.
- ***Centrica Business Solutions*** is responsible for management of the guest operating system (including updates and security patches), all application software and utilities installed on the instances, and the configuration of the AWS-provided firewall.

For more information about Amazon AWS security and compliance, please refer to : http://aws.amazon.com/compliance/

Our implementation adheres to strict security standards, covered and audited by Centrica IT security. This includes but is not limited to:

- **Encrypting all web traffic** - All web traffic is encrypted using HTTPS.
- **Web Application Firewall (WAF)** - WAF is used to protect incoming web traffic.
- **Virtual Private Cloud (VPC)** - Hosting all production services in a Virtual Private Cloud (VPC) with strict access controls.
- **Minimal Access Privileges** - Our web and mobile applications were designed for least-privileges access, where users are assigned with privileges to the minimal set of sites or accounts necessary to perform their job, as defined by their account administrator.
- **Optimized Amazon OS** - All of our systems use Amazon's optimized flavor of Linux, which is dedicated and optimized for use with AWS. The AWS security team constantly tests and provides hotfixes which we upgrade regularly.
- **Automated Intrusion Detection & Prevention** - We constantly monitor suspicious activity via automatic access and activity log analysis.
- **Periodical Penetration Testing and Hardening** - We proactively test our system for vulnerabilities and continuously harden the system as new threats appear

8. Inbound bridge servers

Communications with the PowerRadar cloud is out-bound only. the bridge does implement a few (inbound) internal services. All of them are disabled by default when in normal (non config) operating mode.

Service	**Port**	**When enabled**
Web UI Server	HTTP, Port 80	**Default**: Only in config mode **Optional**: Can be extended to always available
Telnet	Telnet, Port 20	Only in config mode
Modbus Server	Modbus, Port 502	Disabled by default. Only when stand-alone mode (Modbus TCP) is enabled

9. Our privacy policy

We at *Centrica Business Solutions* know that you care how your data and information is used and shared, and we appreciate your trust that we will do so carefully and sensibly.
Our full privacy policy can be downloaded on this link.

10. Frequently asked questions

This section contains answers to some frequent questions we get related to our sensors, cloud and security.

What is the wireless communications protocol used with the sensors?

Our sensors transmit small unidirectional data packets via a proprietary protocol in the ISM 915MHz (US) or 434 MHz (EU) band.

What is the range of the sensor to the bridge?

For reliable communication between the sensors and bridge, the bridge should not be more than 16 feet (5 meters) away from the panel. Bridge Wi-Fi range is up to about 150 feet (45 meters) but is subject to local Wi-Fi conditions.

Are the sensor transmission one-way out or two-way? What are the polling rates?

Sensor transmission is one-way. Sensors cannot receive any incoming communication from the bridge or from any other device. Transmissions are sent 5 to 6 times per minute to a bridge unit.

How does the bridge get updated if the various protocols change?

Firmware updates to the bridge are done using a USB stick with the latest version.

Our latest bridge firmware version (V470 and above) added the ability to automatically receive over-the-air firmware updates from the PowerRadar server. This is an optional feature that can be turned off.

How do you secure over the air firmware updates ?

Over-the-air firmware update is an optional feature added to bridge firmware version V470 and above. When turned on, the bridge checks periodically if a new firmware version is available, downloads and installs it.

This process is done over a secure TLS channel where the bridge verifies the PowerRadar server certificate. Further, the firmware version itself is cryptographically signed and the signature is verified by the bridge prior to the installation.

How do the sensors connect/authenticate with the bridge?

Sensors broadcast their measurements to the bridge using a proprietary protocol. No authentication/connection is needed due to the low power, the close proximity of the communications and the restricted scope of data being transmitted.

Can the sensors receive firmware updates, and if so, what is the frequency?

The sensors do not need firmware updates.

Is the bridge a proprietary device?

Yes, the bridge is a *Centrica Business Solutions* proprietary device that receives data transmission from Panoramic Power sensors. However, the bridge uses standard Wi-Fi/LAN/cellular communication to send sensor transmissions to the cloud.

What data elements are sent to the web for analysis?

The sensor ID, the measurement data and internal bridge statistics (such as number of reconnects, noise level, etc).

How is bridge configuration done?

Bridge configuration is done via a dedicated web interface, which is enabled by default only when the bridge is in ‘config mode’. It is possible to enable the web UI also in normal operating mode. The web interface is protected by a password. It is important to change the bridge password periodically to increase its security.