AGINOVA

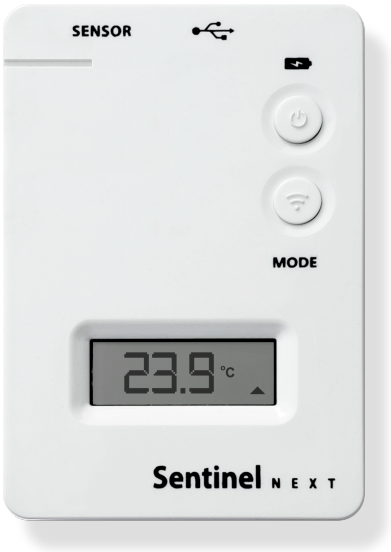
Remote Monitoring Specification

Sentinel NEXT 1S

Product Number: **XTEMP-3101-0000**

Specifications

Dimensions (HxWxD)	89mm x 60mm x 20mm (3.50” x 2.36” x 0.78”)
Weight	102g (3.60 Oz)
Connectors	10-pin Sensor Connector; micro USB for Charging
Battery	Integrated 1000mAh Rechargeable Li-Ion Battery
Wi-Fi Protocols	IEEE 802.11b/g/n
Wi-Fi Models Supported	Wi-Fi Direct, Infrastructure, Remote
Wi-Fi Encryption	WEP, WPA/WPA2, WPA2-Enterprise Personal (PEAPv0/MSCHAPV2, EAP-TTLS)
On Board Data Storage	>2 months with a Once/Minute Sampling Rate
Operating Temperature	0°C to 40°C on Charger -20°C to 60°C on Battery only
Non-operating Temperature	-30°C to 70°C
Relative Humidity	10% to 90%
Certifications	FCC, CE
Ports Used	443(tcp) for Communication 123 (udp) for Time server (Default: pool.ntp.org)
Protocol to Cloud	Sensor communication MQTTS (MQTT over TLS) OTAP and Debugging HTTPS



7552 Central Parke Blvd. Mason, OH 45040
Tel: +1 513 204 5837 / Fax: +1 732 879 0248
www.AGINOVA.com

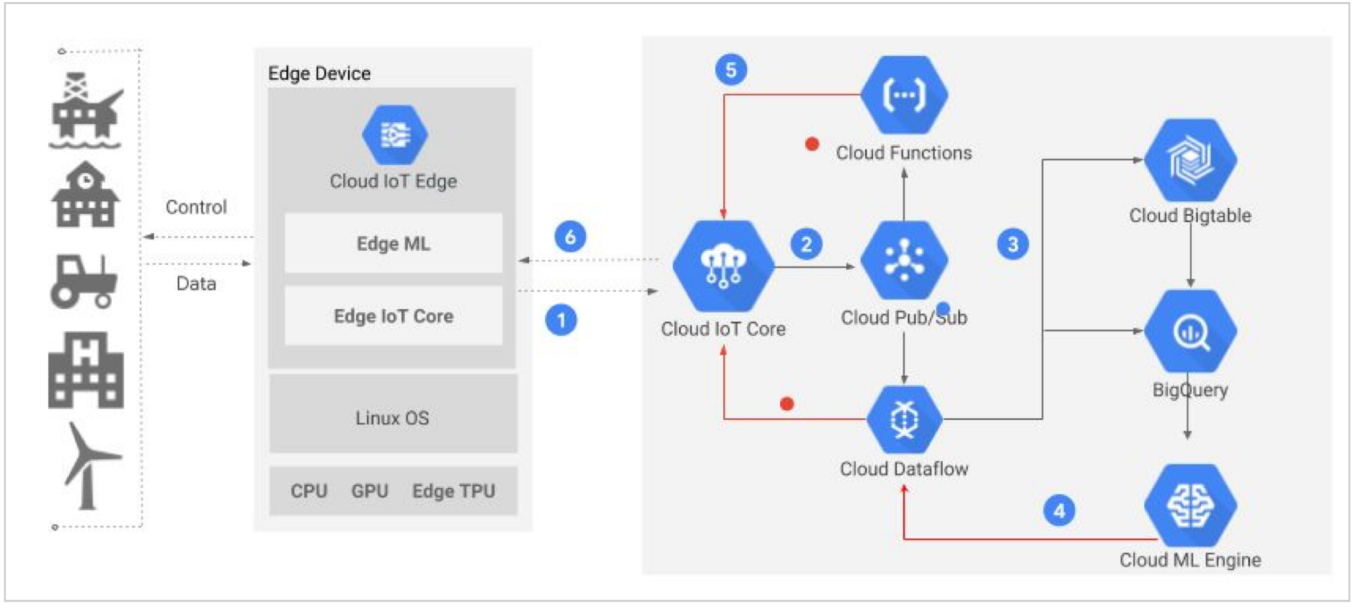
AGINOVA

Cloud Provider Google
Sensor Communication WiFi Infrastructure
Protocol MQTTS (secure connection for devices and sensors) ; HTTPS (Debugging and OTAP)

IDS/IPS : Intrusion detection https://cloud.google.com/intrusion-detection-system
WAF: Cloud Armor https://cloud.google.com/armor/
Vulnerability Test: https://cloud.google.com/security-command-center
TLS Version: 1.2
Data: meets 21 CFR Part 11

Cloud Features Metrics and dashboards allowing visibility into the performance of your services with alerting. Health check monitoring for web applications and applications that can be accessed from the internet with uptime monitoring. Support for logs and logs routing with error reporting and alerting.
Audit logs for visibility into security-related events in your Google Cloud account.
Production debugging and profiling.

Aegis Application User Management System
Sensor Management System
Sensor Data Storage and Reporting
Sensor Health Monitoring
Aggregate Reports for Anomaly Detection



Architecture Google IoT Core

7552 Central Parke Blvd. Mason, OH 45040
Tel: +1 513 204 5837 / Fax: +1 732 879 0248
www.AGINOVA.com

AGINOVA

IT Infrastructure Specifications

1. Enable Publish and Subscribe over MQTT

Sensors connect to the MQTT Bridge using TLS transport to communicate with the Cloud IoT Core.

The following URL and ports should be enabled on the network Firewall:

mqtt.googleapis.com:443

2. Enable Clock Synchronization

Sentinel units periodically synchronize their internal clock using the NTP protocol.

0.pool.ntp.org

Please allow packets over the UDP protocol to destination port 123, for all sensors.

3. Enable OTA (Over The Air Firmware Updates)

Sensors can have their firmware updated remotely, and will need to be able to access the Google Cloud Storage with TLS security (port 443):

storage.googleapis.com:443

4. Test the Network with the Sentinel Config App (Android/iOS)

Once the changes above have been made on the network Firewall, you can download and install the Sentinel Config app from the Google Play Store or iOS App Store:

https://play.google.com/store/apps/details?id=com.aginova.sentinelconfig

https://apps.apple.com/ie/app/sentinel-config/id1457672545

After launching the app, simulate a sensor by pressing the MQTT TEST button. This will check whether the Publish & Subscribe over the MQTT Bridge of the Cloud IoT Core is successful, and it will test clock synchronization with the NTP Pool time servers.

7552 Central Parke Blvd. Mason, OH 45040
Tel: +1 513 204 5837 / Fax: +1 732 879 0248
www.AGINOVA.com