PLEXUS

Limitless building connectivity

# Cybersecurity Statement

PLEXUS

# Platform Overview

## Plexus Connectivity

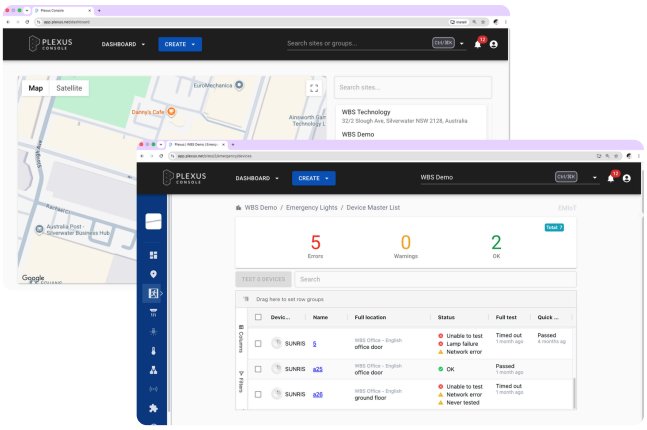
Plexus is a cloud-powered building IoT platform that interconnects intelligent devices through a self-healing dual-radio mesh network. All devices and data are managed through a unified web console and mobile application.

### Plexus Devices

Plexus compatible monitoring devices are a range of IoT sensors and safety fixtures that connect wirelessly to the Plexus mesh network.

### Plexus Gateway

The cloud bridge for each building network. Supports up to 2,000 devices, includes a backup battery, and connects via Ethernet, WiFi, or 4G — falling back through each option automatically if the preferred connection is unavailable.




### Plexus Console

The web application portal for all Plexus data and management functions — sensor data, emergency lighting test reports, audit logs, remote configuration, OTA firmware updates, and virtual floor plan tracking. Accessible at https://app.plexus.net.au

# Security Architecture

## Device-to-Device Communications

Plexus-compatible devices communicate via one of two radios:

| 2.4 GHz BLE | 900 MHz LoRa |
| --- | --- |
| Used for short-range device-to-device communications and for local configuration via the mobile app. BLE is designed to coexist with WiFi and has low interference with other BLE devices, making it well suited to dense building environments. | A proprietary sub-gigahertz radio technology delivering exceptional range and building penetration at low power consumption. The ~900 MHz band is typically congestion-free. *Note: Plexus uses a proprietary mesh protocol and does not use LoRaWAN.* |

### Mesh Topology

Rather than a conventional star topology where all devices connect directly to a central hub, creating a single point of failure, the Plexus mesh allows network packets to hop across multiple devices to find the optimal path to an available gateway. This purely wireless routing is flexible and resilient to interruptions and physical obstructions.

### Encryption

All data transmitted across the Plexus mesh is encrypted with AES-128, preserving both the integrity (data cannot be tampered with) and confidentiality (data cannot be read or intercepted) of all communications.

## Gateway-to-Cloud Communications

All communications between a Plexus gateway and the Plexus cloud platform use MQTT (Message Queuing Telemetry Transport), a lightweight publish-subscribe protocol built on TCP. MQTT sessions are encrypted using TLS and authenticated using X.509 client certificates provisioned by AWS. The MQTT broker is hosted on AWS in the ap-southeast-2 (Sydney) region.

Gateways can obtain an IP address via DHCP or be assigned a static IP. Both Ethernet and WiFi interfaces have stable MAC addresses, supporting sites that require MAC address allowlisting.

# Cloud Platform Security

All Plexus backend services are hosted on AWS in the ap-southeast-2 (Sydney, Australia) region, ensuring full Australian data sovereignty.

## Data Management

### Data at Rest — AES-256

All data is stored on AWS RDS (Relational Database Service) instances encrypted with AES-256. Automated daily database backups are taken for disaster recovery.

### Data in Transit — HTTPS / TLS

All Plexus Console assets are served over HTTPS with certificates generated by AWS Certificate Manager (ACM), providing encryption across all browser sessions.

## Authentication

Authentication is handled by Google Firebase Auth. The Plexus Platform does not store any user passwords or personal information. Authentication tokens are submitted using JWT (JSON Web Token) Bearer Tokens. For full Firebase privacy and security details see: https://firebase.google.com/support/privacy

## Infrastructure

The Plexus Console is hosted on AWS Fargate, distributed across two availability zones, delivering 99%+ uptime. AWS CloudFront caches frequently accessed content on Australian servers for low-latency access.

# Access Control & Audit

### Role-Based Access

Building visibility is restricted to approved, authenticated users only. Administrators manage role-based read/write permissions per building and per user, enforcing least-privilege access across all sites.

### Audit Logging

All user actions are tracked in a per-device audit log with unlimited retention, capturing configuration changes, timestamps, and the identity of the editor. This enables rapid root-cause analysis and supports compliance and incident investigation.

### OTA Firmware Updates

Devices are patched via secure over-the-air (OTA) updates pushed through the Plexus Console, eliminating the need for on-site visits for routine security maintenance.

# TECHNICAL SECURITY REFERENCE

| Security Domain | Implementation |
|---|---|
| **Device communication** | AES-128 (BLE and LoRa mesh) |
| **Gateway-to-cloud protocol** | MQTT over TLS |
| **Gateway-to-cloud authentication** | X.509 client certificates (AWS-provisioned) |
| **Data at rest** | AES-256 on AWS RDS |
| **Console data in transit** | HTTPS via AWS ACM certificates |
| **Account authentication** | Firebase Auth — JWT Bearer Tokens |
| **Cloud infrastructure** | AWS — ap-southeast-2 (Sydney) |
| **Platform uptime** | 99%+ — dual AWS availability zone deployment |
| **Database backups** | Automated daily backups for disaster recovery |
| **Audit logging** | Per-device, unlimited retention, with timestamp and editor identity |
| **User access control** | Role-based, per-building, read/write permissions |
| **Network topology** | Self-healing dual-radio mesh (BLE + LoRa) |
| **Max devices per gateway** | 2,000 |
| **OTA firmware updates** | Supported via Plexus Console |
| **Security research partner** | UNSW NetSyS Laboratory |

## Security Governance

The Plexus network was developed in research partnership with the University of New South Wales (UNSW), with the UNSW NetSyS laboratory providing security hardening expertise. Plexus received R&D grants from both the Australian Government and the Australian Research Council, and was awarded the ACS Gold Digital Disruptor award in 2018. All products are designed in Australia.