NOZOMI NETWORKS

Guardian Air
Installation Guide

Legal notices

Information about the Nozomi Networks copyright and use of third-party software in the Nozomi Networks product suite.

Copyright

Third Party Software

Nozomi Networks uses third-party software, the usage of which is governed by the applicable license agreements from each of the software vendors. Additional details about used third-party software can be found at https://security.nozominetworks.com/licenses.

Contents

Chapter 1. Introduction

Guardian Air overview

Guardian Air is a wireless security sensor for operational technology (OT) and Internet of Things (IoT) environments. It monitors in real-time activities from prominent wireless frequencies, to provide immediate visibility to connected assets and attack surfaces. Guardian Air seamlessly integrates with Vantage for unified visibility of wired, wireless and endpoint assets across your OT and IoT environments.

General

Guardian Air is the first wireless security sensor purpose-built for *operational technology (OT)* and *Internet of Things (IoT)* environments. It monitors all prominent frequencies to provide customers with the much-needed visibility of the wirelessly connected assets. Guardian Air can detect the appearance of rogue infrastructure such as:

- Cellphone towers
- Spoofing devices
- *long range wide area network (LoRaWAN)*
- Building automation protocols
- Drones, and related equipment

Data from Guardian Air sensors is sent to Vantage for analysis alongside network and endpoint data. This consolidated analysis provides a holistic view of your *OT* and *IoT* environments.

Continuous visibility and monitoring

While many *OT* security solutions only see wireless assets once they are connected to the wired network, the Guardian Air sensor continuously monitors all prominent wireless frequencies. These include:

- Bluetooth
- Wi-Fi
- Building automation protocols
- Drones, and
- Long range technology such as cellular and *LoRaWAN*

Guardian Air operates in a wide variety of frequencies, which allows it to provide real-time monitoring and detailed information of assets such as rogue installations or drones. Drones can be utilized to perform attacks, take pictures of critical facilities or carry equipment for attacks or for the exfiltration of valuable information. With Guardian Air, you can detect the presence of drones and the equipment attached to them, enabling security teams to take corrective action.

Ongoing detection of wireless-specific threats

The nature of wireless connections means that cyber adversaries don't need to be in close proximity to exploit an asset’s vulnerabilities. Guardian Air provides ongoing threat detection of wireless-specific threats, such as:

- Brute force attacks
- Spoofing
- Bluejacking

For example, Guardian Air can detect de-authentication attacks and triangulate the location of the devices performing the attacks. Alarms can be set to notify security teams enabling them to take immediate countermeasures, improve defenses and minimize impacts to critical operations.

Description

A description of the key characteristics of the Guardian Air sensor.

General

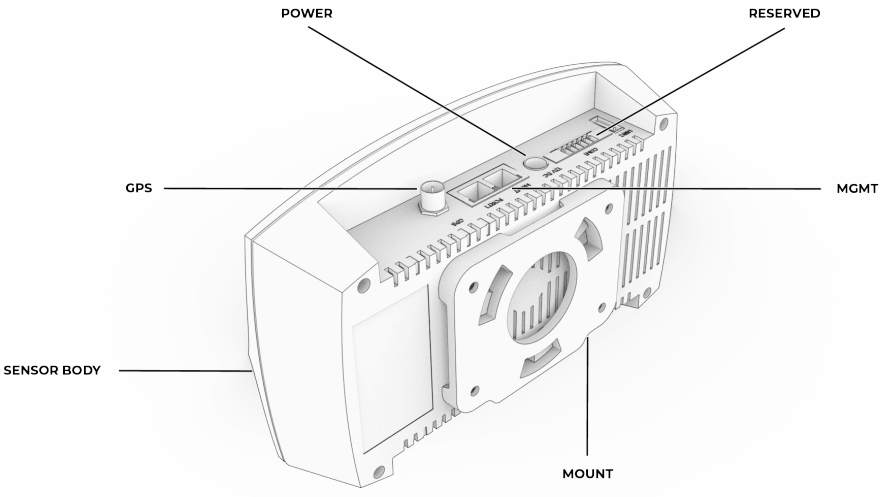


Figure 1. Guardian Air

The Nozomi Networks Guardian Air sensor is a sleek, compact device designed for deployment in *industrial control systems (ICS)* environments. Its design focuses on simplicity and functionality, ensuring seamless integration into diverse *OT* setups. The sensor features a durable, hard plastic body, that ensures resilience in challenging industrial environments.

The top of the sensor has:

- A power button
- A reset button
- An *light-emitting diode (LED)* status indicator
- A reserved port that is not used at this time

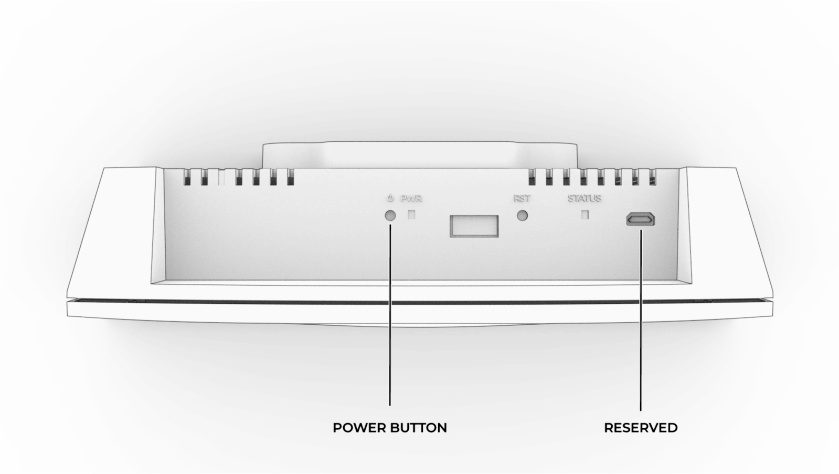


Figure 2. Guardian Air - top view

The bottom of the sensor has:

- A MGMT (management) port
- A *Global Positioning System (GPS)* connector
- A 12 *Volts Direct Current (VDC)* power connector
- A *universal serial bus (USB)* connector
- Three reserved ports that are not used at this time

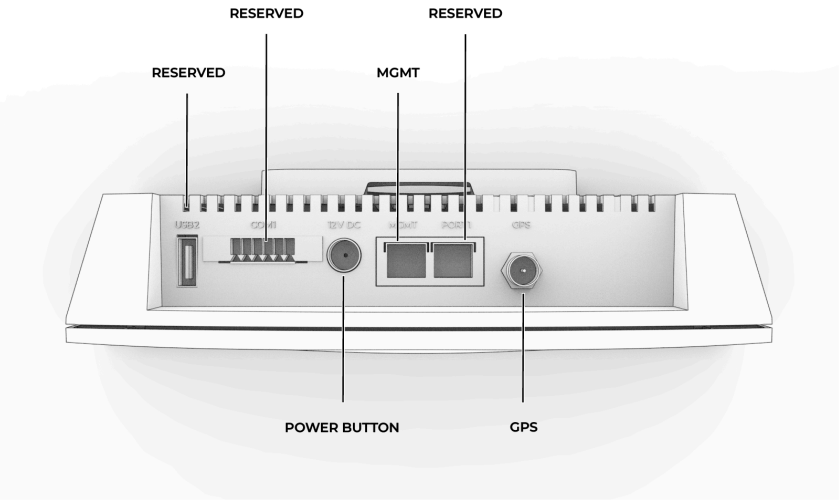


Figure 3. Guardian Air - bottom view

Electrical supply

You can connect electrical power to the sensor through:

- A *power over ethernet (PoE)* compatible switch
- The supplied 12 *Volts Direct Current* external power supply

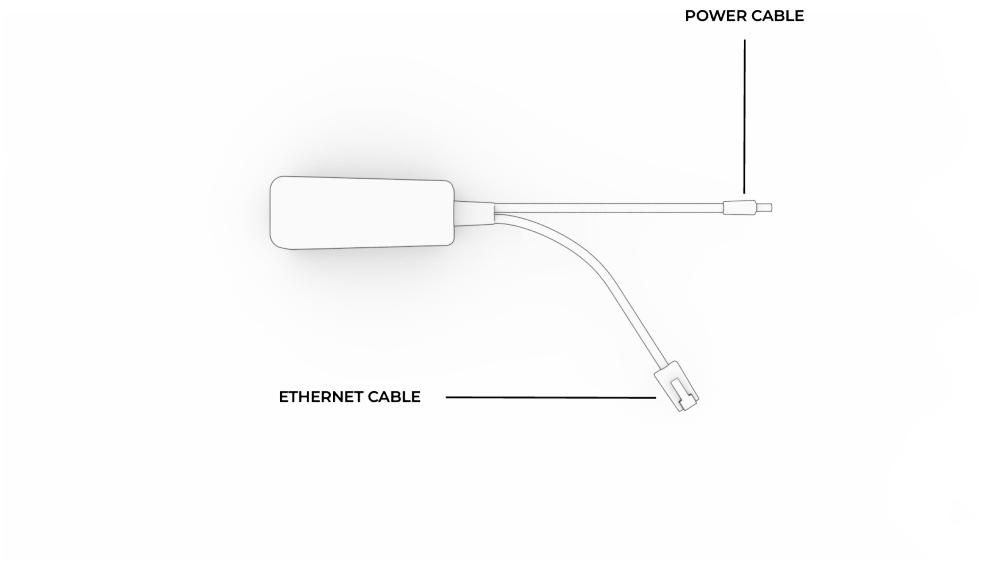


Figure 4. Power over Ethernet (PoE) connector

Operation

Learn how Guardian Air operates and what the different colors of the status indicator mean.

⚠ CAUTION	
	Overheating To prevent the sensor from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature. See below.

Operating environment	Temperature: -20°C - +50°C
	Humidity: 10% - 90%
Storage environment	Temperature: -40°C - +85°C
	Humidity: 5% - 90%

Power cycling

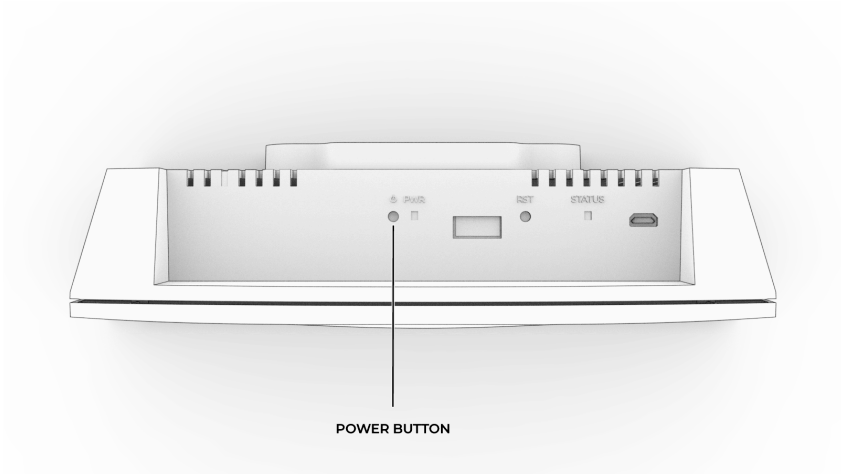


Figure 5. Power button

You can power cycle the appliance in two ways:

- Press the power button with a pen or a pointed object
- Disconnect the power cable and then connect it again

LED indicators

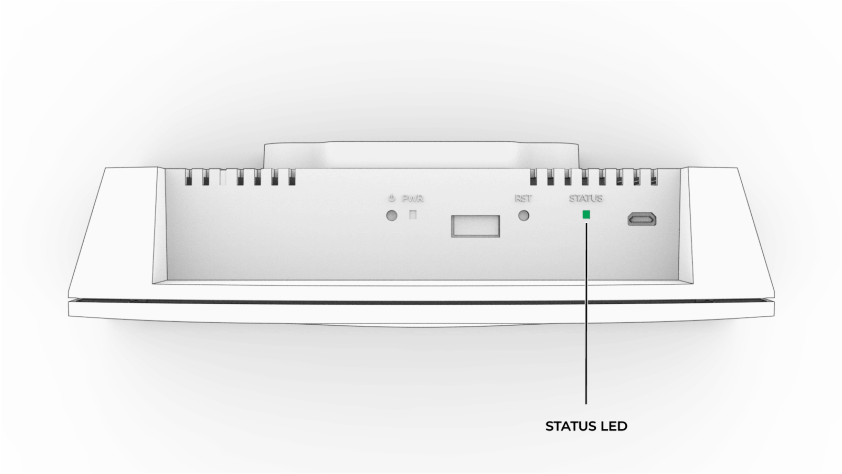


Figure 6. Status LED

Fixed yellow ● the sensor has not obtained an *internet protocol (IP)* address.

Flashing yellow ☀ the sensor had obtained an *IP* address, but it is not able to connect to Nozomi Networks services.

Flashing green ☀ the sensor is ready to be connected to Vantage.

Fixed green ● the sensor is operating correctly.

Chapter 2. Wireless protocols

Wi-Fi monitoring

Guardian Air passively monitors Wi-Fi traffic to discover access points, client devices, and wireless networks, and to detect Wi-Fi-based attacks.

Overview

Guardian Air uses a Realtek 8821CU Wi-Fi adapter to capture 802.11 management frames. The sensor performs channel hopping across the 2.4 GHz and 5 GHz frequency bands to achieve broad coverage across active Wi-Fi channels. Guardian Air synchronizes the data to Vantage for analysis and alert generation.

What Guardian Air discovers

During Wi-Fi monitoring, Guardian Air collects the following information for each detected network and device.

Table 1. Discovery data

Data point	Description
service set identifier (SSID)	The network name broadcast in beacon and probe response frames.
basic service set identifier (BSSID)	The *media access control (MAC)* address of the access point.
Channel	The operating channel of the network.
Frequency band	2.4 GHz or 5 GHz.
Security protocol	The encryption standard in use: open, *Wired Equivalent Privacy (WEP)*, *Wi-Fi Protected Access (WPA)*, *Wi-Fi Protected Access 2 (WPA2)*, or *Wi-Fi Protected Access 3 (WPA3)*.
Cipher suite	The cipher suites supported by the network, as advertised in the access point's information elements.
management frame protection (MFP)	Whether *MFP* is enabled on the network.
pairwise master key identifier (PMKID)	Presence of a *PMKID* in the network's RSN information element, which may enable offline attacks depending on network configuration.
Remote Authentication Dial-In User Service (RADIUS) authentication	Whether the network uses 802.1X *RADIUS*-based authentication (*WPA*-Enterprise).

Table 1. Discovery data (continued)

Data point	Description
Client devices	*MAC* addresses and probe requests from devices associated with or searching for Wi-Fi networks.

Attack detection

Guardian Air includes a Wi-Fi detection engine that identifies the following attack patterns.

Table 2. Attack detection results

Attack type	Description
Beacon flood	A high volume of beacon frames broadcast to overwhelm client device scanning and degrade Wi-Fi usability.
Random beacon flood	A beacon flood using randomized *SSIDs* to evade simple signature-based filters.
Probe request flood	A flood of probe request frames sent to discover networks or disrupt client scanning.
Flipper Zero beacon flood	A signature-based detection of beacon floods using recognizable *SSID* sequences associated with Flipper Zero and similar devices.
Deauthentication attack	Multiple deauthentication frames detected in a short period, aimed at disconnecting clients from access points. Guardian Air reports a `Deauth Attack Attempt` when *MFP* is enabled on the network, or a `Deauth Attack Success` when *MFP* is not enabled.
Packet injection	Wireless injection detected through traffic heuristics, such as high-frequency packet anomalies or replay activity.
SSID cross-site scripting (XSS) injection	An *SSID* in a captured packet contains script code, indicating a *XSS* injection attempt or malformed fields.
Region/country mismatch	A device uses a frequency that is only authorized in a different regulatory region than where the sensor is deployed.
Repeated connection attempts	A device has failed to connect to an access point multiple times, typically due to an incorrect password.

Table 2. Attack detection results (continued)

Attack type	Description
Malicious device (Pwnagotchi)	Detection of a Pwnagotchi device or its attack engine becoming active, including changes to deauthentication or association attack settings.

Hardware

Wi-Fi monitoring uses the Realtek 8821CU *USB* Wi-Fi adapter (interface `wlan0`). The adapter supports the 2.4 GHz and 5 GHz frequency bands. Guardian Air operates the adapter in monitor mode to capture all 802.11 frames without associating to any network.

Bluetooth monitoring

Guardian Air passively monitors Bluetooth Low Energy (BLE) advertising traffic to discover nearby devices and detect BLE-based spoofing attacks.

Overview

Guardian Air uses a Nordic Semiconductor nRF module to capture *Bluetooth Low Energy (BLE)* advertising frames. *BLE* advertising is the mechanism that Bluetooth devices use to announce their presence before pairing. By capturing these frames, Guardian Air builds a picture of all *BLE* devices operating in the environment without connecting to any of them. Guardian Air synchronizes the data to Vantage for analysis and alert generation.

What Guardian Air discovers

During *BLE* monitoring, Guardian Air collects the following information for each detected device.

Table 3. Discovery data

Data point	Description
MAC address	The device address reported in the advertising frame. May be a public address, a static random address, or a *resolvable private address (RPA)* that rotates over time.
Device name	The advertised local name of the device, if present in the advertising data.
Manufacturer	The manufacturer identifier derived from the company *identifier (ID)* field in the advertising payload, if manufacturer-specific data is present.
Advertising type	The type of advertising frame: connectable undirected (`ADV_IND`), connectable directed (`ADV_DIRECT_IND`), non-connectable (`ADV_NONCONN_IND`), scan response (`SCAN_RSP`), or extended advertisement (`ADV_EXT_IND`).
Service UUID	The Bluetooth service class *universally unique identifier (UUID)* advertised by the device, used to indicate potential device type or capability.
Signal strength (*received signal strength indicator (RSSI)*)	The received signal strength in dBm, used to estimate proximity.

Attack detection

Guardian Air includes a *BLE* detection engine that uses signature-based detection to identify known payload patterns associated with advertisement spoofing tools such as the Flipper Zero. These tools send crafted *BLE* advertising packets that trigger notifications or dialogs on nearby devices.

Table 4. Attack detection results

Attack type	Description
Bluetooth settings flood	Repeated *BLE* advertisements using the *human interface device (HID)* service *UUID* (`0x1812`), designed to trigger repeated Bluetooth settings prompts on nearby devices. Generated by Flipper Zero and similar tools.
Apple device popup	Crafted *BLE* packets that mimic Apple accessory advertisements, causing unsolicited pairing popups on iOS and macOS devices.
Apple action modal	*BLE* packets that trigger Apple action sheets, such as AirDrop or AirPods prompts, on nearby Apple devices.
Android device connect	Crafted *BLE* advertisements that trigger connection prompts on Android devices.
Samsung Buds popup	*BLE* packets that mimic Samsung Galaxy Buds advertisements, triggering setup popups on Samsung devices.
Samsung Watch pairing	*BLE* packets that mimic Samsung Galaxy Watch advertisements, triggering pairing prompts on Samsung devices.
Windows `device found`	*BLE* packets that trigger Windows `device found` notifications on nearby Windows computers.
SweynTooth — malformed connection request	A malformed *BLE* connection request that exploits the SweynTooth vulnerability, known to cause crashes on affected devices.
Flipper Zero device detection	A Flipper Zero device is detected on the *BLE* network. Detection confidence varies with the signature.
Packet injection/spam	Excessive or irregular *BLE* advertising packets detected, often characteristic of spam tools or jamming devices.

Hardware

BLE monitoring uses a Nordic Semiconductor nRF module connected via *USB* (interface `ttyble0`). The module operates in the 2.4 GHz ISM band and captures *BLE* advertising frames across the three primary advertising channels (channels 37, 38, and 39).

IEEE 802.15.4 monitoring

Guardian Air monitors IEEE 802.15.4 radio traffic to identify Zigbee, ISA-100.11a, WirelessHART, and other low-power mesh network activity in the 2.4 GHz band.

Overview

Guardian Air uses a Nordic Semiconductor nRF module to monitor *Institute of Electrical and Electronics Engineers (IEEE)* 802.15.4 radio traffic. *IEEE* 802.15.4 is the physical and media access control layer used by several low-power, low-data-rate wireless protocols common in *OT* and building automation environments. Guardian Air performs channel hopping across all 16 channels in the 2.4 GHz band to observe traffic and infer devices from addresses seen in captured frames. Guardian Air synchronizes the data to Vantage for analysis.

Supported protocols

Guardian Air identifies the following application-layer protocols carried over *IEEE* 802.15.4.

Table 5. Supported application protocols

Protocol	Description
Zigbee	A mesh networking protocol widely used in building automation, smart lighting, and *IoT* devices. Guardian Air parses Zigbee network layer frames to extract network addresses. Topology visibility is partial and depends on observed traffic.
ISA-100.11a	An industrial wireless standard used in process automation and oil and gas environments. Guardian Air uses pattern-based detection to identify ISA-100.11a frames from field devices and access points.
WirelessHART	An industrial wireless protocol based on the Highway Addressable Remote Transducer (HART) protocol, used in process automation environments. Guardian Air identifies WirelessHART frames and extracts node and network information.
6LoWPAN	*Internet Protocol version 6* over Low-Power Wireless Personal Area Networks. Used by Thread and other protocols to enable *IP* connectivity on constrained devices. Guardian Air detects 6LoWPAN header compression patterns.

What Guardian Air discovers

During *IEEE* 802.15.4 monitoring, Guardian Air collects the following information for each detected network and device.

Table 6. Discovery data

Data point	Description
personal area network (PAN) ID	The *PAN* identifier that groups devices into a single wireless network.
Source address	The short (16-bit) or extended (64-bit) *IEEE* 802.15.4 address of the transmitting device.
Destination address	The address of the intended recipient of each frame.
Channel	The *IEEE* 802.15.4 channel (11 to 26) on which the frame was captured.
Frame type	The *MAC* frame type: beacon, data, acknowledgement, or *MAC* command.
Security	Whether the frame has the 802.15.4 security header enabled, indicating encrypted payload.
Signal strength (*RSSI*)	The received signal strength of the frame in dBm.

Channels monitored

Guardian Air hops across all 16 channels defined in the *IEEE* 802.15.4 2.4 GHz channel plan: channels 11 through 26. Each channel is 2 MHz wide, with 5 MHz spacing, covering the range 2405 MHz to 2480 MHz.

Hardware

IEEE 802.15.4 monitoring uses a Nordic Semiconductor nRF module connected via *USB* (interface `tty8021540`). This module is separate from the nRF module used for *BLE* monitoring.

LoRaWAN monitoring

Guardian Air monitors LoRaWAN radio traffic to observe join and data message activity and to infer end device presence on long-range wireless networks.

Overview

LoRaWAN is a low-power, wide-area network protocol used extensively in *IoT* deployments for long-range communication between sensors and gateways. Guardian Air uses a dedicated LoRa radio module to capture LoRaWAN packets on supported frequency bands. Gateways are not directly identifiable from LoRa PHY frames; downlink transmissions indicate network infrastructure activity. Because LoRaWAN frequency plans vary by region and country, Guardian Air applies a country-specific configuration to monitor the correct frequency bands. Guardian Air synchronizes the data to Vantage for analysis and alert generation.

What Guardian Air discovers

During LoRaWAN monitoring, Guardian Air collects the following information from each captured transmission. LoRaWAN payloads are end-to-end encrypted; monitoring is limited to message metadata and frame structure.

Table 7. Discovery data

Data point	Description
Device EUI (*device extended unique identifier (DevEUI)*)	The globally unique 64-bit identifier assigned to a LoRaWAN end device, present in join request frames.
Device address (DevAddr)	The 32-bit network address assigned to an end device after a successful join. Present in uplink and downlink data frames.
Network ID (NetID)	The network *ID* present in join-accept frames, used to identify the LoRaWAN network server operator.
Message type	The LoRaWAN message type: join request, join accept, confirmed uplink data, unconfirmed uplink data, confirmed downlink data, unconfirmed downlink data, or rejoin request.
Signal strength (*RSSI*)	The received signal strength of the packet in dBm.
Noise floor	The ambient RF noise level measured alongside the received packet, used to calculate signal-to-noise ratio.

Attack detection

Guardian Air analyzes LoRaWAN frame metadata to detect anomalies that may indicate replay attacks or protocol manipulation.

Table 8. Attack detection results

Attack type	Description
Invalid frame counter value	A LoRaWAN frame counter regression is detected, which may indicate a replay attack or a security issue with the end device.
Incorrect frame payload length	A mismatch between the declared and actual payload length in a LoRaWAN packet, which may indicate data manipulation or a protocol violation.

Frequency configuration

LoRaWAN operates on different frequency bands depending on the region. Guardian Air applies a country-specific configuration to monitor the correct frequencies, set during sensor onboarding in Vantage. The following table lists the frequency plan applied for each supported country.

Table 9. LoRaWAN frequency plans by country

Frequency plan	Frequency range	Supported countries
EU868	863 to 870 MHz	Albania, Andorra, Austria, Bahrain, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Kuwait, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Montenegro, Netherlands, North Macedonia, Poland, Portugal, Qatar, Romania, San Marino, Saudi Arabia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, United Arab Emirates, United Kingdom, Vatican City
EU868 (Macau variant)	863 to 870 MHz	Macau
US915	902 to 928 MHz	Canada, Colombia, Guatemala, United States
AU915	915 to 928 MHz	Australia, Brazil, New Zealand
AS923-1	920 to 925 MHz	Japan, Singapore
KR920	920 to 923 MHz	South Korea

Hardware

LoRaWAN monitoring uses a dedicated LoRa radio module (interface `ttylora0`). The module is separate from the Wi-Fi and Bluetooth modules, and operates exclusively on LoRa frequencies as defined by the active regional configuration.

Cellular monitoring

Guardian Air scans cellular networks using modem measurement capabilities to identify nearby cells, track the cellular environment, and detect anomalies that may indicate rogue base stations.

Overview

Guardian Air uses a SIMCom SIM7600G-H2 cellular modem to scan *Long-Term Evolution (LTE)* (4G) and *Universal Mobile Telecommunications System (UMTS)* (3G) cell activity in the sensor's vicinity. The modem synchronizes with cells and decodes broadcast channels to collect cell measurements, but does not attach to any network or transmit user data. Guardian Air uses this modem-driven scanning to collect information about the serving cell and neighboring cells. This data enables Vantage to identify anomalies that may indicate rogue base stations or unexpected changes in the cellular environment.

What Guardian Air discovers

Guardian Air collects the following information for each detected cell, covering both the serving cell and neighboring cells.

Table 10. Discovery data

Data point	Description
Network mode	Whether the cell is an *LTE* (4G) or *UMTS* (3G) base station.
mobile country code (MCC)	The three-digit code identifying the country of the mobile network operator.
mobile network code (MNC)	The two- or three-digit code identifying the mobile network operator within a country.
Cell ID	The unique *ID* of the base station cell.
Frequency band	The *LTE* or *UMTS* frequency band in use. Guardian Air resolves band numbers and their corresponding frequency ranges from the *E-UTRA absolute radio frequency channel number (EARFCN)* (*LTE*) or *UTRA absolute radio frequency channel number (UARFCN)* (*UMTS*) channel number.
tracking area code (TAC)	The *LTE* tracking area code used for location registration (*LTE* only).
physical cell ID (PCI)	The physical layer cell identifier used to distinguish cells on the same frequency (*LTE* only).
Signal strength (*RSSI*)	The received signal strength of the cell in dBm.

Table 10. Discovery data (continued)

Data point	Description
reference signal received power (RSRP)	The average power of *LTE* reference signal resource elements, used as a measure of signal quality (*LTE* only).
reference signal received quality (RSRQ)	The ratio of *RSRP* to total received power, indicating signal-to-interference quality (*LTE* only).
Cell role	Whether the cell is the serving (selected) cell in idle mode or a neighbor cell detected during scanning.
Operator name	The name of the mobile network operator, where available.

Attack detection

Guardian Air uses cellular scan data to detect anomalies that may indicate unauthorized network infrastructure.

Table 11. Attack detection results

Attack type	Description
Rogue cell tower	A cell with stronger signal and mismatched parameters is detected, possibly indicating a rogue or fake base station.

Frequency bands monitored

Guardian Air detects *LTE* cells across a broad range of frequency bands, from sub-700 MHz low-band spectrum to 3.8 GHz high-band spectrum. The modem resolves the frequency range from the *EARFCN* value reported for each cell. Examples of monitored bands include Band 1 (2110 to 2170 MHz) and Band 3 (1805 to 1880 MHz). Additional examples include Band 7 (2620 to 2690 MHz), Band 20 (791 to 821 MHz), and Band 28 (758 to 803 MHz), among others.

For *UMTS* (3G), Guardian Air uses the *UARFCN* value to identify the cell's operating frequency.

Hardware

Cellular monitoring uses the SIMCom SIM7600G-H2 module (interface `cellular`). This module also provides *GPS* capability when used for location services. No SIM card is required for cellular monitoring because the sensor operates in scan-only mode.

Z-Wave monitoring

Guardian Air monitors Z-Wave radio traffic to observe device activity in building automation and smart facility environments.

Overview

Z-Wave is a sub-GHz wireless protocol used in building automation, access control, *heating, ventilation, and air conditioning (HVAC)*, and smart facility systems. Guardian Air uses a dedicated Z-Wave module to monitor Z-Wave radio traffic in the frequency band appropriate to the sensor's configured region. The module captures observable Z-Wave frames without joining any Z-Wave network. Z-Wave payloads are typically encrypted (S0 or S2 security); monitoring is limited to frame metadata and unencrypted traffic. Guardian Air synchronizes the data to Vantage for analysis.

What Guardian Air discovers

During Z-Wave monitoring, Guardian Air collects the following information from captured frames.

Table 12. Discovery data

Data point	Description
Frame direction	The direction of the frame as reported by the Z-Wave module: received (RX) from other devices, or transmitted (TX) by the module itself (for example, acknowledgements).
Payload	Parsed frame metadata and, where unencrypted, command class data used to identify device types and behavior.
Signal strength (*RSSI*)	The received signal strength of the frame in dBm, used to estimate device proximity.
Channel hop index	The Z-Wave channel on which the frame was captured. Z-Wave Long Range uses a separate channel from classic Z-Wave.
Frame length	The byte length of the Z-Wave frame payload.
cyclic redundancy check (CRC) status	Whether the frame passed *CRC* validation, confirming frame integrity.

Frequency configuration

Z-Wave operates on sub-GHz frequencies that vary by region to comply with local radio regulations. Guardian Air applies the regional configuration during sensor onboarding in Vantage. The following table lists the frequency and region applied for each supported country.

Table 13. Z-Wave frequency regions by country

Region	Frequency	Supported countries
EU	868.4 MHz	Albania, Andorra, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Kuwait, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Montenegro, Netherlands, North Macedonia, Poland, Portugal, Qatar, Romania, San Marino, Saudi Arabia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, United Arab Emirates, United Kingdom, Vatican City
US	908.4 MHz / 916 MHz	Canada, Colombia, Guatemala, United States
ANZ	919.8 MHz / 921.4 MHz	Australia, Brazil, New Zealand
JP	922.5 MHz / 923.9 MHz	Japan
RU [1]	869.0 MHz	Macau
KR	920.9 MHz	Singapore, South Korea

Hardware

Z-Wave monitoring uses a dedicated Z-Wave module connected to the serial interface `ttymxc3`. Guardian Air processes only frames that pass *CRC* validation, ensuring that corrupted or partial frames do not generate false device discoveries.

1. The RU region code is defined by the Z-Wave Alliance and does not correspond to Russia. It is applied to Macau based on compatible frequency regulations.

OpenDroneID monitoring

Guardian Air monitors OpenDroneID (ODID) beacon traffic broadcast by drones to identify unmanned aircraft in the area and detect spoofing or anomalous behavior.

Overview

OpenDroneID (ODID) is a broadcast Remote Identification standard defined by ASTM F3411 that requires drones to transmit identification and telemetry data over Wi-Fi beacon frames. Guardian Air captures these beacons using the Wi-Fi adapter and decodes the *ODID* message packs to extract drone identity, location, and flight data. Guardian Air synchronizes the data to Vantage for analysis and alert generation.

What Guardian Air discovers

During *ODID* monitoring, Guardian Air collects the following information for each detected drone.

Table 14. Discovery data

Data point	Description
UA ID (Remote ID)	The unmanned aircraft identifier broadcast in the Basic ID message, used to uniquely identify the drone.
ID type	The type of identifier, such as serial number, registration ID, or UTM-assigned ID.
UA type	The type of unmanned aircraft, such as helicopter, aeroplane, or multirotor.
Protocol version	The ASTM F3411 protocol version in use: F3411-19 (1.0), F3411-20 (1.1), or F3411-22 (2.0).
Status	The operational status of the drone as reported in the location message.
Latitude and longitude	The geographic coordinates of the drone, extracted from the location vector message.
Altitude and height	The geodetic altitude, barometric altitude, and height above takeoff or ground as reported by the drone.
Direction and speed	The horizontal direction, horizontal speed, and vertical speed of the drone.
Signal strength (*RSSI*)	The received signal strength of the beacon in dBm, used to estimate proximity.

Attack detection

Guardian Air analyzes *ODID* telemetry data to detect anomalies that may indicate spoofing, replay attacks, or unauthorized drone activity.

Table 15. Attack detection results

Attack type	Description
Improbable *RSSI* change	A sudden and abnormal change in the drone's *RSSI* value between consecutive packets, which may indicate spoofing or packet injection.
Wrong telemetry sequence number	The telemetry counter in a received packet is lower than or inconsistent with the previous value, which may indicate a replay attack or packet injection.
Drone above height limit	The drone reports a height above 500 meters, which is suspicious and may indicate spoofed telemetry.
Unrealistic number of drones	More drones appear within a short time window than is plausible, which may indicate that an attacker is sending crafted packets to simulate a fleet of drones.

Hardware

ODID monitoring uses the same Realtek 8821CU Wi-Fi adapter (interface `wlan0`) as Wi-Fi monitoring. Guardian Air identifies *ODID* beacons by matching the CEN *Organizationally Unique Identifier (OUI)* in the vendor-specific information element of 802.11 beacon frames.

ESP-NOW monitoring

Guardian Air monitors ESP-NOW wireless traffic to detect exploitation attempts targeting Espressif ESP-NOW based devices.

Overview

ESP-NOW is a connectionless communication protocol developed by Espressif for low-bitrate, peer-to-peer data exchange between ESP32 and ESP8266 devices. ESP-NOW frames are transmitted as Wi-Fi action frames without requiring an access point or network association. Guardian Air captures ESP-NOW traffic using the Wi-Fi adapter in monitor mode and analyzes frame patterns for known vulnerabilities. Guardian Air synchronizes the data to Vantage for analysis and alert generation.

What Guardian Air discovers

During ESP-NOW monitoring, Guardian Air collects the following information from each captured frame.

Table 16. Discovery data

Data point	Description
Source address	The *MAC* address of the transmitting device.
Destination address	The *MAC* address of the intended recipient, or broadcast address for group communication.
Signal strength (*RSSI*)	The received signal strength of the frame in dBm.

Attack detection

Guardian Air detects exploitation attempts targeting known vulnerabilities in the ESP-NOW protocol implementation.

Table 17. Attack detection results

Attack type	Description
Out-of-bounds buffer read (CVE-2024-42484)	An ESP-NOW frame containing invalid group info data is detected. The frame's payload size is smaller than the declared group info structure, which can cause a buffer read out-of-bounds and potentially crash the receiving device. Some ESP-NOW protocol versions do not sanitize group info data and are vulnerable to this attack.
Replay attack (CVE-2024-42483)	A burst of ESP-NOW frames toward a single destination is detected at an unusually high rate. This pattern may indicate an attacker attempting to saturate the receiver's cache to replay previously captured frames. The ESP-NOW protocol does not implement protection against replay attacks.

Hardware

ESP-NOW monitoring uses the same Realtek 8821CU Wi-Fi adapter (interface `wlan0`) as Wi-Fi monitoring. Guardian Air identifies ESP-NOW frames by matching the Espressif *OUI* in Wi-Fi action frames.

Chapter 3. Requirements

Requirements

The requirements for Guardian Air.

To use Guardian Air, you will need:

- Vantage
- An Ethernet cable

Chapter 4. Setup

Connect a Guardian Air sensor to Vantage

To connect a Guardian Air sensor to Vantage, use either a power over Ethernet-compatible switch or an external power supply. This procedure includes network setup steps and sensor registration using a QR code. Successful connection is indicated by a green status light and confirmation in the Vantage interface.

Before you begin

If you are not connected to a *dynamic host configuration protocol (DHCP)* enabled network, do one of these procedures first:

- Configure an HTTP proxy (on page 53)
- Configure a static IP address (on page 59)

If your *DHCP* does not provide a *network time protocol (NTP)* service then Guardian Air will use default *NTP* servers that the *operating system (OS)* provides. If you can't connect to those servers, then do the Configure an NTP server (on page 56) procedure.

About this task

There are two possible methods to connect the sensor:

- With a *PoE*-compatible switch
- Without *PoE*-compatible switch

Procedure

1. Connect the sensor.

   Choose from:

   - With a *PoE*-compatible switch. Go to 2 (on page 41).
   - Without a *PoE*-compatible switch. Go to 3 (on page 42).

2. ⚠ CAUTION

   Electrical power source
   If the power source is different from the one provided, it must be LPS/PS2 rated 12VDC 3A maximum.

   Connect with a *PoE*-compatible switch.

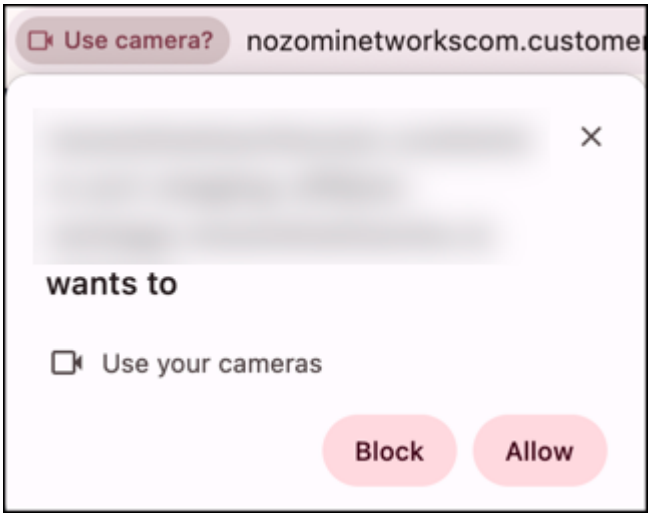
   a. Connect an Ethernet cable to the *PoE* splitter.
   b. Connect the *PoE* power connector into the power plug.
   c. Connect the Ethernet cable into the **MGMT** port.

3. Connect without a *PoE*-compatible switch.
   a. Connect the provided external power supply to the power plug.
   b. Connect a standard Ethernet cable to the **MGMT** port.

   The ethernet cable must be connected to a network with *DHCP* enabled, and firewall rules/policies need to allow connectivity to:
   - https://*.guardianair.nozominetworks.io
   - Your Vantage instance *uniform resource locator (URL)*
4. Make sure that the green *LED* is flashing green.

   A flashing green *LED* indicates that the sensor is ready to be connected to Vantage.
5. Go to your Vantage instance and select the most appropriate organization.
6. In the Vantage's **Sensors** page, add your sensor.
7. Select **Guardian Air**.

   Result: A dialog shows.
8. To allow Vantage to access your camera to scan the pairing QR code, select **Allow.**



9. Scan the QR code.

   You can find the QR code:
   - In the Quick Start Guide
   - On the bottom of the sensor
10. Follow the steps and select a **Site** and a **Network Domain**.
11. Wait until the status *LED* indicator changes to fixed green and Vantage reports success.

    This process can take a few minutes.

Results

The sensor has been connected to Vantage.

Related information

Configure an HTTP proxy (on page 53)
Configure an NTP server (on page 56)
Configure a static IP address (on page 59)

Install a Guardian Air sensor

Guardian Air is designed to be mounted on a wall or ceiling. Follow this procedure to install your Guardian Air sensor.

Before you begin

You will need the correct size and type of screws for your installation surface. The screws should have a diameter of 4 mm (5/32 in) and a minimum length of 30 mm (1.2 in).

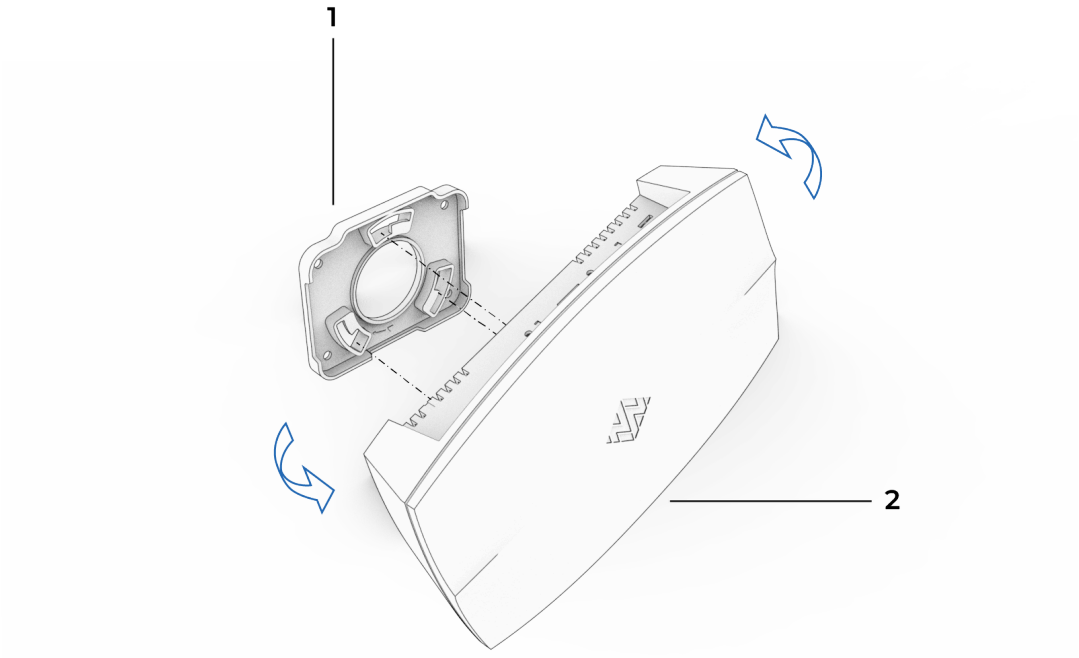
Procedure

1. Choose where you want to install the Guardian Air sensor.

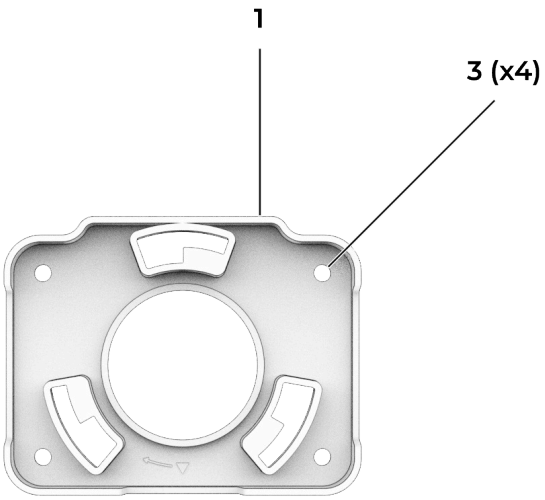
   Choose from:

   - A wall-mounted installation
   - A ceiling-mounted installation

2. Choose the correct screws for the surface that you want to install Guardian Air.
3. Hold the Guardian Air sensor (sensor) (2) in position and turn the mount (1) counterclockwise to remove it.

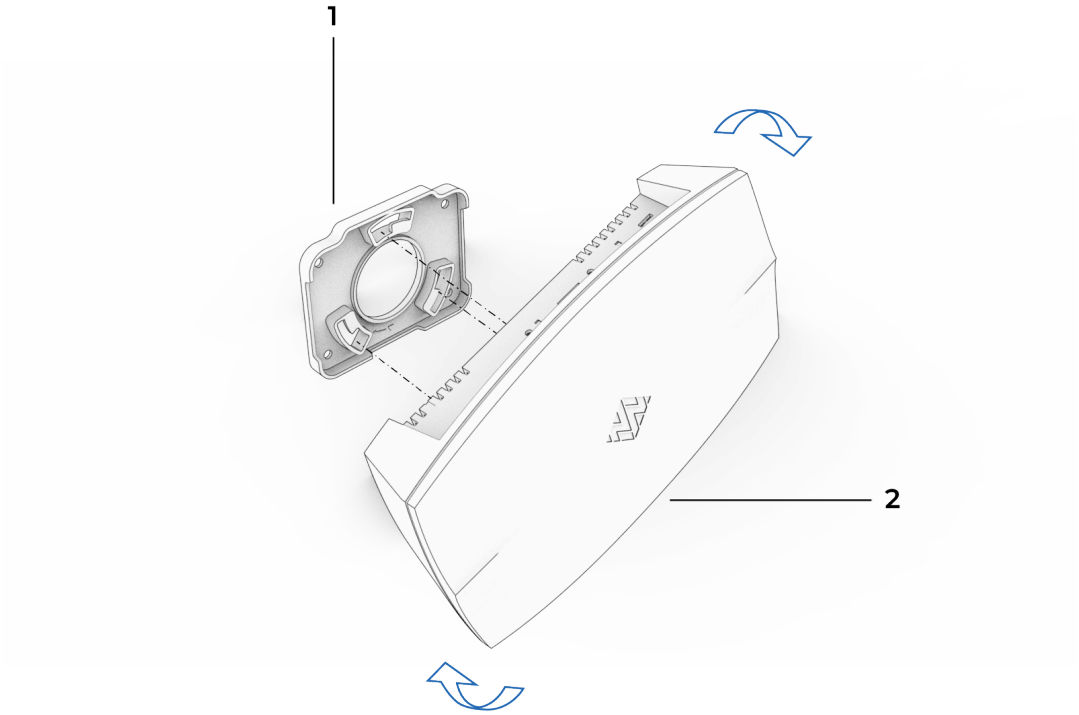


4. Put the mount (1) in position on the wall or ceiling.



5. Make a mark at the position of the four holes (3).
6. Remove the mount (1).
7. Drill the four holes (3) to the correct depth for your screws.

8. Put the mount (1) in position and install the four screws.
9. Align the sensor (2) with the mount (1) and turn it clockwise until it locks into position.



Chapter 5. Configuration

v1.0.14 and after

Custom settings configuration

To customize the settings of a Guardian Air device, you can load a configuration file from a FAT32-formatted USB drive. Supported parameters include static IP address, gateway, DNS, proxy servers, and NTP servers for time synchronization.

Overview

Within certain limitations, it is possible to customize the configuration of a Guardian Air device. To do this, you must copy a configuration file to a FAT32-formatted *USB* pendrive. Then, before you power-on the device, you must connect the *USB* pendrive to one of the *USB* ports on the device.

The only available section is network which, as its name suggests, includes configuration parameters related to networking. For example:

```
[network]
address=172.16.4.195/26
gateway=172.16.4.193
dns=172.16.4.193
http_proxy=http://10.41.48.40:3128
https_proxy=http://10.41.48.40:3128
ntp_servers=time.google.com,time.aws.com,time.cloudflare.com
```

Parameters

`address`: a valid *classless inter-domain routing (CIDR) Internet Protocol version 4* address that represents the static *IP* address to be assigned to the network interface associated to the management Ethernet port

`gateway`: a valid *IPv4* address that represents the gateway to be assigned to the network interface associated to the management Ethernet port

`dns`: a valid *IPv4* address that represents the *domain name server (DNS)* server to be used by the network interface associated to the management Ethernet port

`http_proxy`: a valid *URL* that represents the *hypertext transfer protocol (HTTP)* proxy server to be used by all the running applications that need to communicate with cloud services

`https_proxy`: a valid *URL* that represents the *hypertext transfer protocol secure (HTTPS)* proxy server to be used by all the running applications that need to communicate with cloud services

`ntp_servers`: a comma-separated list of valid hostnames, compliant with RFC 1123, or *IPv4* addresses, that represent *NTP* servers to be used for time synchronization

Configure custom settings

Use a USB drive to apply custom network settings to a Guardian Air device. Define static IP address, gateway, DNS, and proxy server parameters in a configuration file. Load the file during device startup to configure networking manually.

Before you begin

Make sure that:

- Your Guardian Air device is running firmware version 1.0.14 or later
- You have a *USB* drive formatted as FAT32

About this task

Within certain limitations, it is possible to customize the configuration of a Guardian Air device. To do this, you must copy a configuration file to a FAT32-formatted *USB* pendrive. Then, before you power-on the device, you must connect the *USB* pendrive to one of the *USB* ports on the device.

For more details, see Custom settings configuration (on page 49).

Procedure

1. Connect a *USB* pendrive to a desktop or laptop computer.

   Note:
   The *OS* installed is not important.

2. Format the *USB* pendrive.
3. Assign the label **NOZOMI** to the *USB* pendrive.
4. On the *USB* pendrive, create a file with the name: `configuration.ini`
5. Open the `configuration.ini` file.
6. In the `configuration.ini` file, enter this text:

   ```
   [network]
   ```

7. Enter a line for each parameter that you want to customize. For example,

   ```
   [network]
   address=172.16.4.195/26
   gateway=172.16.4.193
   dns=172.16.4.193
   http_proxy=http://10.41.48.40:3128
   https_proxy=http://10.41.48.40:3128
   ntp_servers=time.google.com,time.aws.com,time.cloudflare.com
   ```

8. Save the `configuration.ini` file.
9. Safely eject the *USB* pendrive.

10. If the Guardian Air device is powered on, disconnect the electrical power cable.
11. Connect the *USB* pendrive to one of the *USB* ports on the Guardian Air device.
12. To turn on electrical power to the Guardian Air device, connect the electrical power cable.
13. Wait until the status *LED* indicator starts to flash green.
    This means that the Guardian Air custom network configuration has been correctly applied, and the system is able to connect to the Nozomi Networks cloud service.
14. If the *LED* does not flash green, see the Troubleshooting (on page 69) section.
15. Safely eject the *USB* pendrive.

Results

Guardian Air is now configured with your custom settings.

What to do next

Do the Connect a Guardian Air sensor to Vantage (on page 41) procedure.

Related information

Revert custom settings (on page 52)

Revert custom settings

Remove the previously configured custom settings from a Guardian Air device. This procedure restores the default network configuration. It is useful for troubleshooting or reconfiguring the device for a different network environment.

About this task

Do this procedure if you need to revert the Guardian Air device to its original network configuration. This is useful when changing network settings, troubleshooting connectivity issues, or removing a previously configured *HTTP* proxy.

Procedure

1. Connect the *USB* pendrive you used to do the configuration to a desktop or laptop computer.

   > **Note:**
   > The *OS* installed is not important.

2. Open the `configuration.ini` file.
3. Remove all the text from the file.
4. Save the `configuration.ini` file.
5. Safely eject the *USB* pendrive.
6. Make sure that the Guardian Air device is powered off. If it is on, disconnect the electrical power cable.
7. Connect the *USB* pendrive to one of the *USB* ports on the Guardian Air device.
8. To turn on electrical power to the Guardian Air device, connect the electrical power cable.
9. Wait until the status *LED* indicator shows fixed yellow.
   This should take less than one minute.
   A fixed yellow light means that the Guardian Air original network configuration has been restored, and the system is unable to connect to the Nozomi Networks cloud service.
10. Safely eject the *USB* pendrive.

Results

After completing this procedure, the Guardian Air device reverts to its default network configuration.

Up to v1.0.13

Configure an HTTP proxy

Use a universal serial bus (USB) pendrive to manually configure hypertext transfer protocol (HTTP) proxy settings on a Guardian Air device. This setup enables network connectivity through a proxy when automatic configuration using the dynamic host configuration protocol (DHCP) is unavailable. Proxy details must be saved in a specific file format on the USB device.

Before you begin

Make sure that:

- Your Guardian Air device is running firmware version 1.0.7 or later
- You have a *USB* drive formatted as FAT32

About this task

You can use a *USB* pendrive to manually configure a *HTTP* proxy on a Guardian Air device. Before you do this procedure, we recommend that you upgrade to the latest version of Guardian Air. To do this, you will need to connect your Guardian Air to a network that already has a *DHCP* server. This will let you do the automatic upgrade.

Procedure

1. Connect a *USB* pendrive to a desktop or laptop computer.

   Note:
   The *OS* installed is not important.

2. Assign the label **NOZOMI** to the *USB* pendrive.
3. On the *USB* pendrive, create a file with the name: `environment`
4. In the `environment` file, enter this text:

   ```
   HTTP_PROXY="<HTTP-proxy-URL>"
   HTTPS_PROXY="<HTTP-proxy-URL>"
   ```

5. Replace the text: `<HTTP-proxy-URL>` with the *URL* of the *HTTP* proxy to be configured. Include the port and the slash at the end. For example, `http://10.41.48.40:3128/`
6. Save the `environment` file.
7. Safely eject the *USB* pendrive.
8. If the Guardian Air device is powered on, disconnect the electrical power cable.
9. Connect the *USB* pendrive to one of the *USB* ports on the Guardian Air device.
10. To turn on electrical power to the Guardian Air device, connect the electrical power cable.

11. Wait until the status *LED* indicator starts to flash green.
    This means that the Guardian Air custom network configuration has been correctly applied, and the system is able to connect to the Nozomi Networks cloud service. This connection is either direct, or through the configured *HTTP* proxy.
12. If the *LED* does not flash green, see the Troubleshooting (on page 70) procedure.
13. Safely eject the *USB* pendrive.

Results

Guardian Air is now configured with the *HTTP* proxy settings, which allows it to connect to the Nozomi Networks cloud.

What to do next

Do the Connect a Guardian Air sensor to Vantage (on page 41) procedure.

Related information

Revert an HTTP proxy configuration (on page 55)
Failure to connect after HTTP proxy configuration (on page 70)

Revert an HTTP proxy configuration

Remove the previously configured hypertext transfer protocol (HTTP) proxy settings from a Guardian Air device. This procedure restores the default network configuration. It is useful for troubleshooting or reconfiguring the device for a different network environment.

About this task

Do this procedure if you need to revert the Guardian Air device to its original network configuration. This is useful when changing network settings, troubleshooting connectivity issues, or removing a previously configured *HTTP* proxy.

Procedure

1. Connect the *USB* pendrive you used to do the configuration to a desktop or laptop computer.

   > **Note:**
   > The *OS* installed is not important.

2. Open the `environment` file.
3. Remove all the text from the file.
4. Save the `environment` file.
5. Safely eject the *USB* pendrive.
6. Make sure that the Guardian Air device is powered off. If it is on, disconnect the electrical power cable.
7. Connect the *USB* pendrive to one of the *USB* ports on the Guardian Air device.
8. To turn on electrical power to the Guardian Air device, connect the electrical power cable.
9. Wait until the status *LED* indicator shows fixed yellow.
   This should take less than one minute.
   A fixed yellow light means that the Guardian Air original network configuration has been restored, and the system is unable to connect to the Nozomi Networks cloud service.
10. Safely eject the *USB* pendrive.

Results

After completing this procedure, the Guardian Air device reverts to its default network configuration. The *HTTP* proxy settings are removed, and the device is unable to connect to the Nozomi Networks cloud service until new network settings are configured.

Configure an NTP server

Use a universal serial bus (USB) pendrive to manually configure a network time protocol (NTP) server on a Guardian Air device. This setup is useful when automatic configuration using the dynamic host configuration protocol (DHCP) is not available. The NTP server addresses must be specified in a configuration file saved on the USB device.

Before you begin

Make sure that:

- Your Guardian Air device is running firmware version 1.0.11 or later
- You have a *USB* drive formatted as FAT32

About this task

You can use a *USB* pendrive to manually configure a *NTP* server on a Guardian Air device. Before you do this procedure, we recommend that you upgrade to the latest version of Guardian Air. To do this, you will need to connect your Guardian Air to a network that already has a *DHCP* server. This will let you do the automatic upgrade.

Procedure

1. Connect a *USB* pendrive to a desktop or laptop computer.

   > **Note:**
   > The *OS* installed is not important.

2. Assign the label **NOZOMI** to the *USB* pendrive.
3. On the *USB* pendrive, create a file with the name: `timesyncd.conf`

   Use a plain text editor to create configuration files. For example, Visual Studio Code or Sublime Text.
4. In the `timesyncd.conf` file, enter this text:

   ```
   [Time]
   NTP=<NTP-address> <NTP-address>
   FallbackNTP=<NTP-address> <NTP-address>
   ```

5. Replace the text: `<NTP-address>` with the IPv4 *CIDR* address that you want to assign to the device. For example: `172.16.4.195/26`

   Both `NTP` or `FallbackNTP` sections can be:

   - Empty
   - Contain a single value, or
   - Contain a list of values that are separated by spaces

6. Save the `timesyncd.conf` file.
7. Safely eject the *USB* pendrive.

8. If the Guardian Air device is powered on, disconnect the electrical power cable.
9. Connect the *USB* pendrive to one of the *USB* ports on the Guardian Air device.
10. To turn on electrical power to the Guardian Air device, connect the electrical power cable.
11. Wait until the status *LED* indicator starts to flash green.
    This means that the Guardian Air custom network configuration has been correctly applied, and the system is able to connect to the Nozomi Networks cloud service. This connection is either direct, or through the configured *HTTP* proxy.
12. If the *LED* does not flash green, see the Troubleshooting (on page 71) procedure.
13. Safely eject the *USB* pendrive.

Results

Guardian Air is now configured with the *NTP* server settings.

What to do next

Do the Connect a Guardian Air sensor to Vantage (on page 41) procedure.

Related information

Revert an NTP server configuration (on page 58)

Failure to connect after NTP server configuration (on page 71)

Revert an NTP server configuration

Remove the previously configured network time protocol (NTP) server settings from a Guardian Air device. This procedure restores the default network configuration. It is useful when troubleshooting or preparing the device for a new network setup.

About this task

Do this procedure if you need to revert the Guardian Air device to its original network configuration. This is useful when changing network settings, troubleshooting connectivity issues, or removing previously configured *NTP* server settings.

Procedure

1. Connect the *USB* pendrive you used to do the configuration to a desktop or laptop computer.

   Note:
   The *OS* installed is not important.

2. Open the `timesyncd.conf` file.
3. Remove all the text from the file.
4. Save the `timesyncd.conf` file.
5. Safely eject the *USB* pendrive.
6. Make sure that the Guardian Air device is powered off. If it is on, disconnect the electrical power cable.
7. Connect the *USB* pendrive to one of the *USB* ports on the Guardian Air device.
8. To turn on electrical power to the Guardian Air device, connect the electrical power cable.
9. Wait until the status *LED* indicator shows fixed yellow.
   This should take less than one minute.
   A fixed yellow light means that the Guardian Air original network configuration has been restored, and the system is unable to connect to the Nozomi Networks cloud service.
10. Safely eject the *USB* pendrive.

Results

After completing this procedure, the Guardian Air device reverts to its default network configuration. The *NTP* server settings are removed, and the device is unable to connect to the Nozomi Networks cloud service until new network settings are configured.

Configure a static IP address

Use a universal serial bus (USB) pendrive to manually configure a static internet protocol (IP) address on a Guardian Air device. This approach is used when automatic configuration using the dynamic host configuration protocol (DHCP) is not available. The IP address, gateway, and domain name system (DNS) settings must be defined in a configuration file stored on the USB device.

Before you begin

Make sure that:

- Your Guardian Air device is running firmware version 1.0.7 or later
- You have a *USB* drive formatted as FAT32

About this task

You can use a *USB* pendrive to manually configure a static *IP* address on a Guardian Air device. Before you do this procedure, we recommend that you upgrade to the latest version of Guardian Air. To do this, you will need to connect your Guardian Air to a network that already has a *DHCP* server. This will let you do the automatic upgrade.

Procedure

1. Connect a *USB* pendrive to a desktop or laptop computer.

   Note:
   The *OS* installed is not important.

2. Assign the label **NOZOMI** to the *USB* pendrive.
3. On the *USB* pendrive, create a file with the name: `eth0-manual.network`
   Use a plain text editor to create configuration files. For example, Visual Studio Code or Sublime Text.
4. In the `eth0-manual.network` file, enter this text:

```
[Match]
Type=ether
Name=eth0
KernelCommandLine=!nfsroot
KernelCommandLine=!ip

[Network]
Address=<IPv4-CIDR-address>
Gateway=<Gateway-IPv4-address>
DNS=<DNS-IPv4-address>
```

5. Replace the text: `<IPv4-CIDR-address>` with the IPv4 *CIDR* address that you want to assign to the device. For example: `172.16.4.195/26`
6. Replace the text: `<Gateway-IPv4-address>` with the IPv4 address of the gateway. For example: `172.16.4.193`
7. Replace the text: `<DNS-IPv4-address>` with the IPv4 address of the *DNS* server.
8. Save the `eth0-manual.network` file.
9. Safely eject the *USB* pendrive.
10. If the Guardian Air device is powered on, disconnect the electrical power cable.
11. Connect the *USB* pendrive to one of the *USB* ports on the Guardian Air device.
12. To turn on electrical power to the Guardian Air device, connect the electrical power cable.
13. Wait until the status *LED* indicator starts to flash green.
    This means that the Guardian Air custom network configuration has been correctly applied, and the system is able to connect to the Nozomi Networks cloud service. This connection is either direct, or through the configured *HTTP* proxy.
14. If the *LED* does not flash green, see the Troubleshooting (on page 72) procedure.
15. Safely eject the *USB* pendrive.

Results

Guardian Air is now configured with the static *IP* address settings, which allows it to connect to the Nozomi Networks cloud.

What to do next

Do the Connect a Guardian Air sensor to Vantage (on page 41) procedure.

Related information

Revert a static IP configuration (on page 61)
Failure to connect after static IP configuration (on page 72)

Revert a static IP configuration

Remove the previously configured static internet protocol (IP) address settings from a Guardian Air device. This procedure restores the device's original network configuration. It is useful when troubleshooting connectivity issues or preparing the device for a new deployment.

About this task

Do this procedure if you need to revert the Guardian Air device to its original network configuration. This is useful when changing network settings, troubleshooting connectivity issues, or removing a previously configured static *IP* address.

Procedure

1. Connect the *USB* pendrive you used to do the configuration to a desktop or laptop computer.

   Note:
   The *OS* installed is not important.

2. Open the `eth0-manual.network` file.
3. Remove all the text from the file.
4. Save the `eth0-manual.network` file.
5. Safely eject the *USB* pendrive.
6. Make sure that the Guardian Air device is powered off. If it is on, disconnect the electrical power cable.
7. Connect the *USB* pendrive to one of the *USB* ports on the Guardian Air device.
8. To turn on electrical power to the Guardian Air device, connect the electrical power cable.
9. Wait until the status *LED* indicator shows fixed yellow.
   This should take less than one minute.
   A fixed yellow light means that the Guardian Air original network configuration has been restored, and the system is unable to connect to the Nozomi Networks cloud service.
10. Safely eject the *USB* pendrive.

Results

After completing this procedure, the Guardian Air device reverts to its default network configuration. The static *IP* address settings are removed, and the device is unable

to connect to the Nozomi Networks cloud service until new network settings are configured.

Chapter 6. Cleaning

Clean a Guardian Air sensor

It is important that you clean the sensor correctly.

Procedure

1. **⚠ DANGER**

   Electrical power
   Before you clean the sensor, disconnect it from electrical power.

   Disconnect the electrical power cable from the sensor.

2. **⚠ DANGER**

   Liquids
   Do not use water, or other liquids to clean the sensor. Only use a clean, dry cloth.

   Use a clean, lint-free cloth to clean the external body of the sensor.
3. Connect the electrical power cable to the sensor.

Chapter 7. Troubleshooting

Status indicator shows fixed yellow

Possible cause

Your *DHCP* server is not connected correctly.

Procedure

Check your *DHCP* server.

If none of the previous solutions work, please contact our Customer Support team.

Status indicator shows flashing yellow

Possible cause

The sensor has obtained an *IP* address, but cannot connect to Nozomi Networks services.

Procedure

Do a check of your firewall.

If none of the previous solutions work, please contact our Customer Support team.

Failure to connect after HTTP proxy configuration

Diagnose and resolve connection failures that occur after configuring a hypertext transfer protocol (HTTP) proxy on a Guardian Air device. Causes may include incorrect file entries or issues with the network configuration. Use this guide to identify and correct common setup problems.

Possible cause

Your *DHCP* server is not connected correctly.

Procedure

Check your *DHCP* server.

Possible cause

You did not write the configuration files correctly.

Procedure

1. Turn off the power to the Guardian Air.
2. Connect a *USB* pendrive to a desktop or laptop computer.
3. Read the `environment` file to make sure that it is correct.
4. If you found a mistake in the file, correct the mistake.
5. Do the Configure an HTTP proxy (on page 53) procedure again.

If none of the previous solutions work, please contact our Customer Support team.

Related information

Configure an HTTP proxy (on page 53)

Failure to connect after NTP server configuration

Troubleshoot connectivity problems that occur after configuring a network time protocol (NTP) server on a Guardian Air device. Issues may be caused by incorrect file entries or network setup errors. This topic guides you through checking and correcting the configuration.

Possible cause

Your *DHCP* server is not connected correctly.

Procedure

Check your *DHCP* server.

Possible cause

You did not write the configuration files correctly.

Procedure

1. Turn off the power to the Guardian Air.
2. Connect a *USB* pendrive to a desktop or laptop computer.
3. Read the `timesyncd.conf` file to make sure that it is correct.
4. If you found a mistake in the file, correct the mistake.
5. Do the Configure an NTP server (on page 56) procedure again.

If none of the previous solutions work, please contact our Customer Support team.

Related information

Configure an NTP server (on page 56)

Failure to connect after static IP configuration

Identify and fix connection issues that occur after assigning a static internet protocol (IP) address to a Guardian Air device. Problems may result from file errors or network misconfiguration. This topic provides steps to verify and correct the settings.

Possible cause

Your *DHCP* server is not connected correctly.

Procedure

Check your *DHCP* server.

Possible cause

You did not write the configuration files correctly.

Procedure

1. Turn off the power to the Guardian Air.
2. Connect a *USB* pendrive to a desktop or laptop computer.
3. Read the `eth0-manual.network` file to make sure that it is correct.
4. If you found a mistake in the file, correct the mistake.
5. Do the Configure a static IP address (on page 59) procedure again.

If none of the previous solutions work, please contact our Customer Support team.

Related information

Configure a static IP address (on page 59)

Glossary

BLE

Bluetooth Low Energy (BLE) is a short-range wireless communication protocol designed for low-power devices. It operates in the 2.4 GHz ISM band and is used for device discovery and data exchange in IoT, medical, and industrial applications.

BSSID

A Basic Service Set Identifier (BSSID) is the MAC address of a Wi-Fi access point. It uniquely identifies a wireless access point within a network.

Classless Inter-Domain Routing

CIDR is a method for IP routing and for allocating IP addresses.

CRC

A Cyclic Redundancy Check (CRC) is an error-detection code used to verify the integrity of transmitted data. A CRC value is calculated from the payload and appended to each frame. The receiver recalculates the CRC and compares it to the transmitted value to detect transmission errors.

cURL

cURL is a command-line tool and library used to transfer data to or from a server. It supports many protocols, including HTTP, HTTPS, FTP, and more. In API contexts, curl is commonly used to test and interact with endpoints by sending requests and receiving responses.

DevEUI

A Device Extended Unique Identifier (DevEUI) is a globally unique 64-bit identifier assigned to a LoRaWAN end device. It is present in join request frames and used to uniquely identify a device on a LoRaWAN network.

Domain Name Server

The DNS is a distributed naming system for computers, services, and other resources on the Internet, or other types of Internet Protocol (IP) networks.

Dynamic Host Configuration Protocol

DHCP is a network protocol that automatically assigns IP addresses and other configuration settings to devices, simplifying network management, reducing manual setup, preventing IP conflicts, and supporting scalable network configurations.

EAPOL

Extensible Authentication Protocol over LAN (EAPOL) is a network authentication protocol used in IEEE 802.1X implementations. In Wi-Fi networks, EAPOL frames carry the authentication handshake between a client device and an access point during the WPA and WPA2 connection process.

EARFCN

An E-UTRA Absolute Radio Frequency Channel Number (EARFCN) is a channel number that uniquely identifies an LTE downlink carrier frequency. EARFCN values map to specific frequency bands and are used to determine which LTE frequency band a cell is operating on.

File Allocation Table

FAT is a file system architecture used in computers for managing disk space. It maintains a table to track the allocation of files on a disk, supporting efficient data storage, access, and management

Global Positioning System

GPS is a satellite-based navigation system that provides real-time location and time information, enabling accurate positioning, navigation, and tracking for various devices and applications worldwide.

gRPC

gRPC is an open-source remote procedure call framework that lets a client application call methods on a server application as if they were local calls. It uses Protocol Buffers as its interface definition language and typically runs over HTTP/2.

HID

A Human Interface Device (HID) is a category of device that interacts directly with humans, such as a keyboard, mouse, or game controller. In the Bluetooth protocol stack, the HID service (UUID 0x1812) identifies these devices and is commonly spoofed in Bluetooth advertising attacks.

HVAC

Heating, ventilation, and air conditioning (HVAC) refers to the systems used to regulate temperature, humidity, and air quality in buildings. HVAC systems are a common use case for building automation protocols such as Z-Wave and BACnet.

Hypertext Transfer Protocol

HTTP is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

Hypertext Transfer Protocol Secure

HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL.

Identifier

A label that identifies the related item.

IEEE

The Institute of Electrical and Electronics Engineers (IEEE) is a professional organization that publishes technical standards for electronics, computing, and telecommunications, including the 802 series of networking standards.

Industrial Control Systems

An ICS is an electronic control system and related instrumentation that is used to control industrial processes.

Internet of Things

The IoT describes devices that connect and exchange information through the internet or other communication devices.

Internet Protocol

An Internet Protocol address, or IP address, identifies a node in a computer network that uses the Internet Protocol to communicate. The IP label is numerical.

IPv4

Internet Protocol version 4 is a widely used network protocol that identifies devices using 32-bit numerical addresses.

IPv6

Internet Protocol version 6 is the most recent version of the Internet Protocol, designed to replace IPv4. It uses 128-bit numerical addresses to identify devices, allowing for a vastly larger address space.

Light-emitting Diode

An LED (Light Emitting Diode) is an electronic component that emits light when an electric current passes through it, offering energy-efficient, long-lasting illumination for displays, indicators, and lighting applications.

LoRaWAN

LoRaWAN (Long Range Wide Area Network) is a wireless communication protocol designed for low-power, long-range communications. It's specifically intended for Internet of Things (IoT) devices and applications, enabling them to transmit small packets of data over vast distances efficiently.

LTE

Long-Term Evolution (LTE) is a 4G cellular standard that defines the radio interface and network architecture for high-speed mobile broadband communications. LTE is specified by the 3rd Generation Partnership Project (3GPP).

MCC

A Mobile Country Code (MCC) is a three-digit code that identifies the country of a mobile network operator. MCC values are defined by the ITU and are used alongside Mobile Network Codes to identify cellular networks worldwide.

Media Access Control

A MAC address is a unique identifier for a network interface controller (NIC). It is used as a network address in network segment communications. A common use is in most IEEE 802 networking technologies, such as Bluetooth, Ethernet, and Wi-Fi. MAC addresses are most commonly assigned by device manufacturers and are also referred to as a hardware address, or physical address. A MAC address normally includes a manufacturer's organizationally unique identifier (OUI). It can be stored in hardware, such as the card's read-only memory, or by a firmware mechanism.

MFP

Management Frame Protection (MFP) is a security mechanism defined in IEEE 802.11w that protects Wi-Fi management frames from forgery and replay attacks. Networks with MFP enabled are more resistant to deauthentication and disassociation attacks.

MNC

A Mobile Network Code (MNC) is a two- or three-digit code that identifies a mobile network operator within a country. MNC values are used alongside Mobile Country Codes to uniquely identify cellular networks.

Network Time Protocol

The NTP is a networking protocol to synchronize clocks between computer systems over variable-latency, packet-switched data networks.

ODID

OpenDroneID (ODID) is a broadcast Remote Identification protocol defined by the ASTM F3411 standard. It requires unmanned aircraft to transmit identification and telemetry data over wireless protocols such as Wi-Fi and Bluetooth.

Operating System

An operating system is computer system software that is used to manage computer hardware, software resources, and provide common services for computer programs.

Operational Technology

OT is the software and hardware that controls and/or monitors industrial assets, devices and processes.

OUI

An Organizationally Unique Identifier (OUI) is a 24-bit or 28-bit identifier assigned by IEEE to a device manufacturer. It forms the first portion of a MAC address and is used to identify the vendor of a network device.

PAN

A Personal Area Network (PAN) identifier (PAN ID) is a short identifier used in IEEE 802.15.4 wireless networks to distinguish individual networks sharing the same radio channel. Devices belonging to the same network share a common PAN ID.

PCI

A Physical Cell ID (PCI) is a number used in LTE networks to identify a cell at the physical layer. PCI values (0 to 503) allow devices to distinguish between cells operating on the same frequency within a local area.

PMKID

A Pairwise Master Key Identifier (PMKID) is a field included in *extensible authentication protocol over LAN (EAPOL)* frames during the WPA2 handshake. A PMKID vulnerability in certain WPA2 implementations allows an attacker to obtain the PMKID without capturing the full four-way handshake, enabling offline dictionary attacks against the network passphrase.

Power over Ethernet

PoE is a technology that allows electrical power to be transmitted alongside data over standard Ethernet cables. This enables network devices such as IP cameras, wireless access points, and VoIP phones to receive power directly from the network cable, eliminating the need for separate power sources and simplifying installation.

Pre-Shared Key

A pre-shared key (PSK) is a shared secret established in advance between parties, used for authentication in wireless security protocols such as WPA and WPA2.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting for users who access a network. In Wi-Fi (WPA-Enterprise) deployments, RADIUS servers authenticate clients using IEEE 802.1X before granting network access.

Resolvable private address

A resolvable private address (RPA) is a Bluetooth Low Energy device address that changes periodically to prevent long-term tracking. RPAs can be resolved back to a device's true identity by a bonded peer using a shared identity resolving key (IRK).

RSRP

Reference Signal Received Power (RSRP) is an LTE measurement that indicates the average power of reference signal resource elements in a received signal. RSRP is used to assess LTE signal quality and serving cell selection.

RSRQ

Reference Signal Received Quality (RSRQ) is an LTE measurement that expresses the ratio of RSRP to the total received power, indicating overall signal-to-interference quality. RSRQ is used alongside RSRP to assess LTE network quality.

RSSI

Received Signal Strength Indicator (RSSI) is a measurement of the power level of a received radio signal, expressed in decibels relative to 1 milliwatt (dBm). RSSI is used across wireless protocols including Wi-Fi, Bluetooth, LoRaWAN, and cellular to estimate signal quality and device proximity.

SSID

A Service Set Identifier (SSID) is the name of a Wi-Fi network, broadcast in beacon and probe response frames. SSIDs can be up to 32 characters long and are used by client devices to identify and connect to wireless networks.

TAC

A Tracking Area Code (TAC) is an identifier used in LTE networks to group cells into tracking areas for location registration and paging. The TAC helps the network identify which tracking area a device is registered to.

Transport Layer Security

TLS is a cryptographic protocol that provides communications security over a computer network. The protocol is widely used in applications such as: HTTPS, voice over IP, instant messaging, and email.

UARFCN

A UTRA Absolute Radio Frequency Channel Number (UARFCN) is a channel number that identifies a UMTS (3G) carrier frequency. UARFCN values are used to determine the frequency band on which a UMTS cell is operating.

UMTS

Universal Mobile Telecommunications System (UMTS) is a 3G cellular standard based on wideband code division multiple access (W-CDMA) radio technology. UMTS is specified by the 3rd Generation Partnership Project (3GPP) and is the predecessor to LTE.

Uniform Resource Locator

An URL is a reference to a resource on the web that gives its location on a computer network and a mechanism to retrieving it.

Universally unique identifier

A UUID is a 128-bit label that is used for information in computer systems. When a UUID is generated with standard methods, they are, for all practical purposes, unique. Their uniqueness is not dependent on an authority, or a centralized registry. While it is not impossible for the UUID to be duplicated, the possibility is generally considered to be so small, as to be negligible. The term globally unique identifier (GUID) is also used in some, mostly Microsoft, systems.

Universal Serial Bus

Universal Serial Bus (USB) is a standard that sets specifications for protocols, connectors, and cables for communication and connection between computers and peripheral devices.

Volts Direct Current

VDC refers to the voltage of a direct current (DC) electrical supply, where electrons flow in one direction, powering devices like electronics, sensors, and various other components.

WEP

Wired Equivalent Privacy (WEP) is a deprecated Wi-Fi security protocol defined in IEEE 802.11. WEP uses RC4 stream cipher encryption and is considered cryptographically broken. It has been superseded by WPA and WPA2.

WPA

Wi-Fi Protected Access (WPA) is a Wi-Fi security protocol introduced as an interim replacement for WEP. WPA uses TKIP encryption and provides stronger security than WEP, but has since been superseded by WPA2 and WPA3.

WPA2

Wi-Fi Protected Access 2 (WPA2) is a Wi-Fi security protocol defined in IEEE 802.11i. WPA2 uses AES-based CCMP encryption and is the most widely deployed Wi-Fi security standard. It has been largely superseded by WPA3 for new deployments.

WPA3

Wi-Fi Protected Access 3 (WPA3) is the current generation Wi-Fi security protocol, introduced in 2018. WPA3 provides stronger encryption than WPA2 and introduces Simultaneous Authentication of Equals (SAE) to protect against offline dictionary attacks.

XSS

Cross-site scripting (XSS) is a type of security vulnerability in which an attacker injects malicious script code into data fields or content that is rendered by other users or systems.