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 a 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

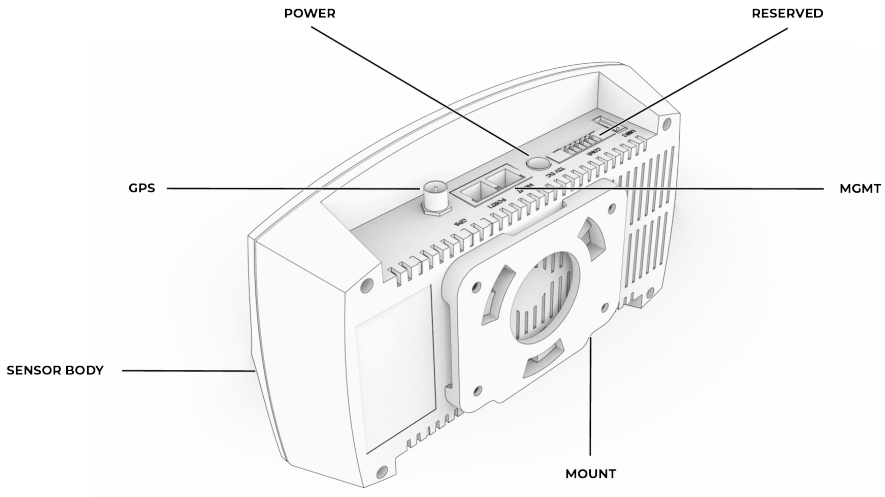


Figure 1. Guardian Air

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

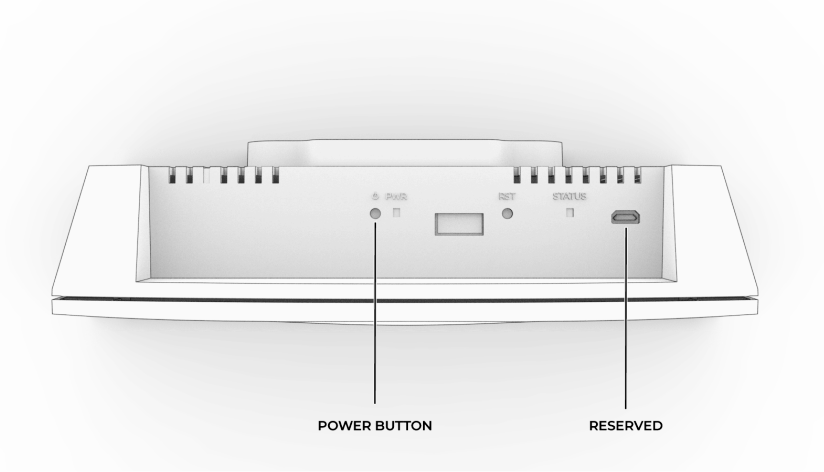


Figure 2. Guardian Air - top view

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

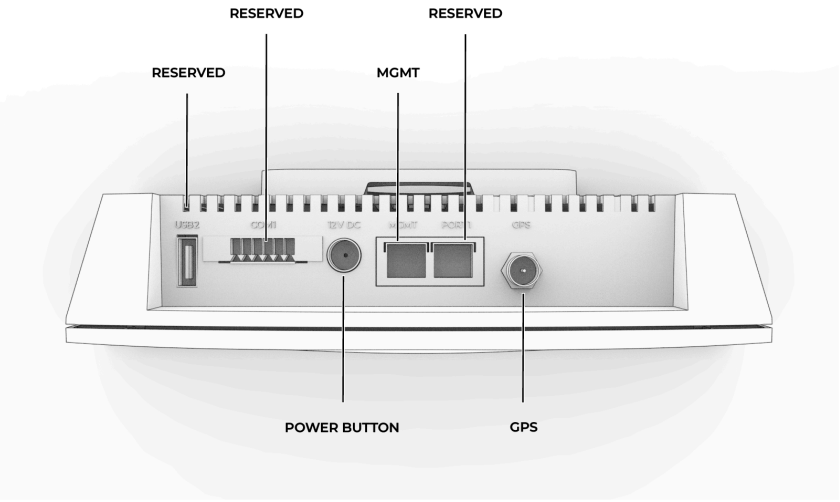


Figure 3. Guardian Air - bottom view

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

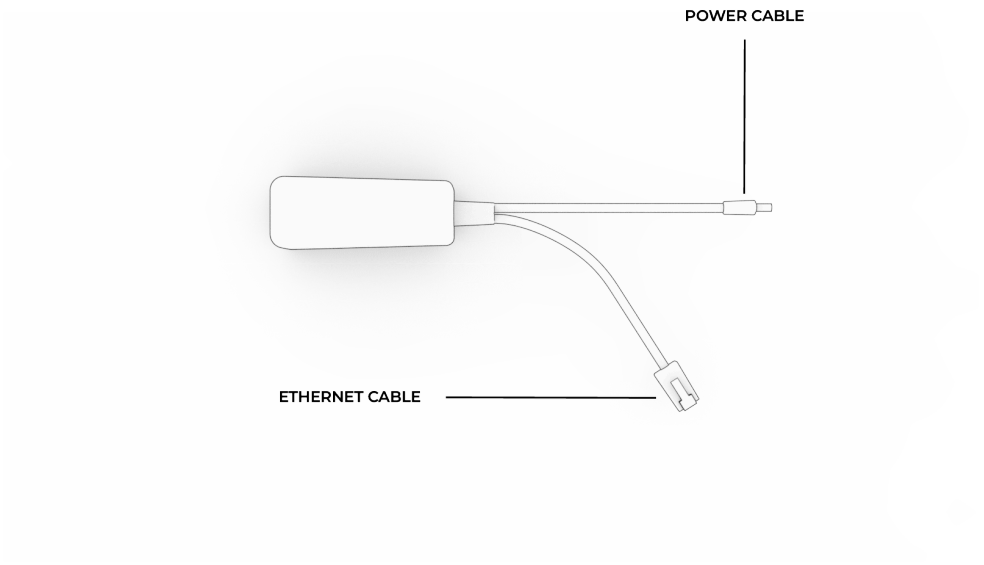


Figure 4. Power over Ethernet (PoE) connector

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

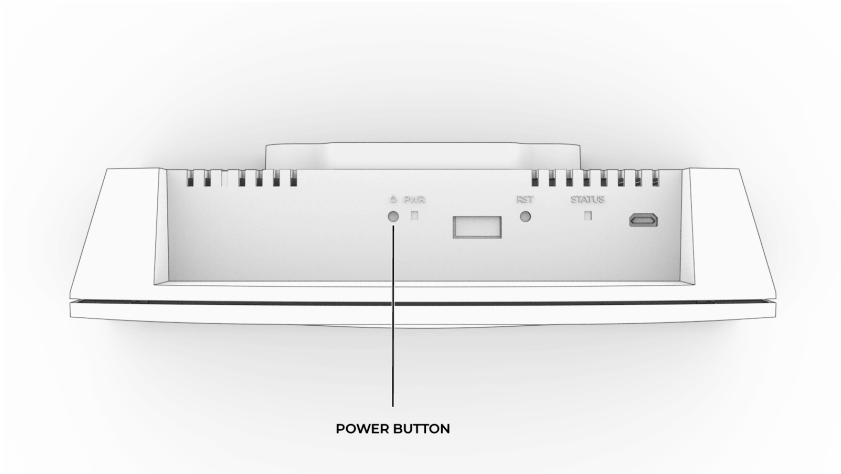


Figure 5. Power button

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

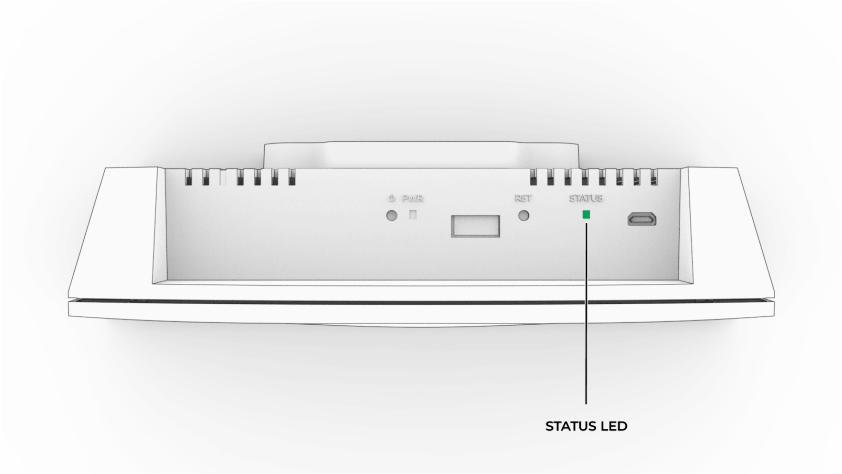


Figure 6. Status LED

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. Requirements

Requirements

The requirements for Guardian Air.

To use Guardian Air, you will need:

- Vantage
- An Ethernet cable

Chapter 3. Setup

Connect a Guardian Air sensor to Vantage

Before you can use your Guardian Air sensor, you will need to connect it to Vantage.

Before you begin

If you are not connected to a *dynamic host configuration protocol (DHCP)* enabled network, do the Configure static IP and HTTP proxy (on page 29) procedure first.

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 21).
   - Without a *PoE*-compatible switch. Go to 3 (on page 21).

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.

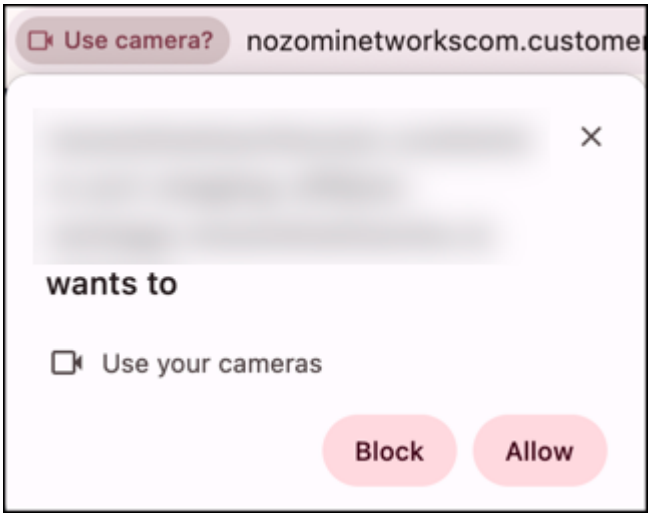
   A flashing green *LED* indicates that the sensor is ready to be connected to Vantage.

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.

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).

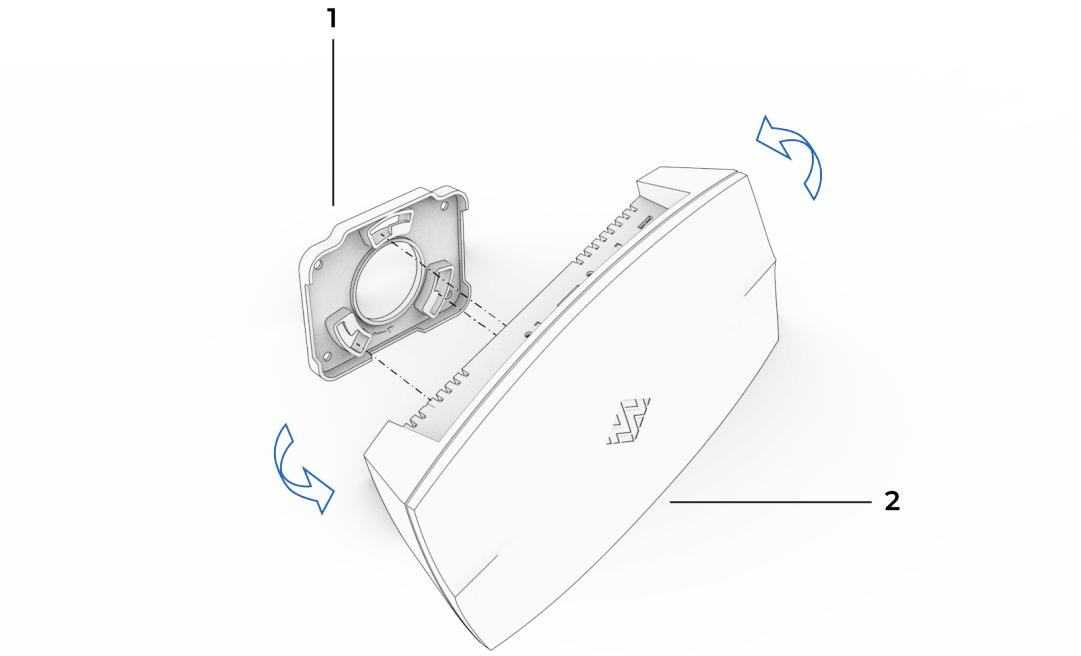
Procedure

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

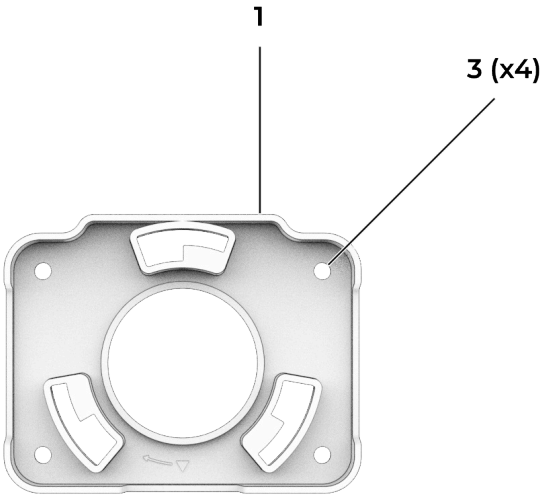
   Choose from:

   - 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.

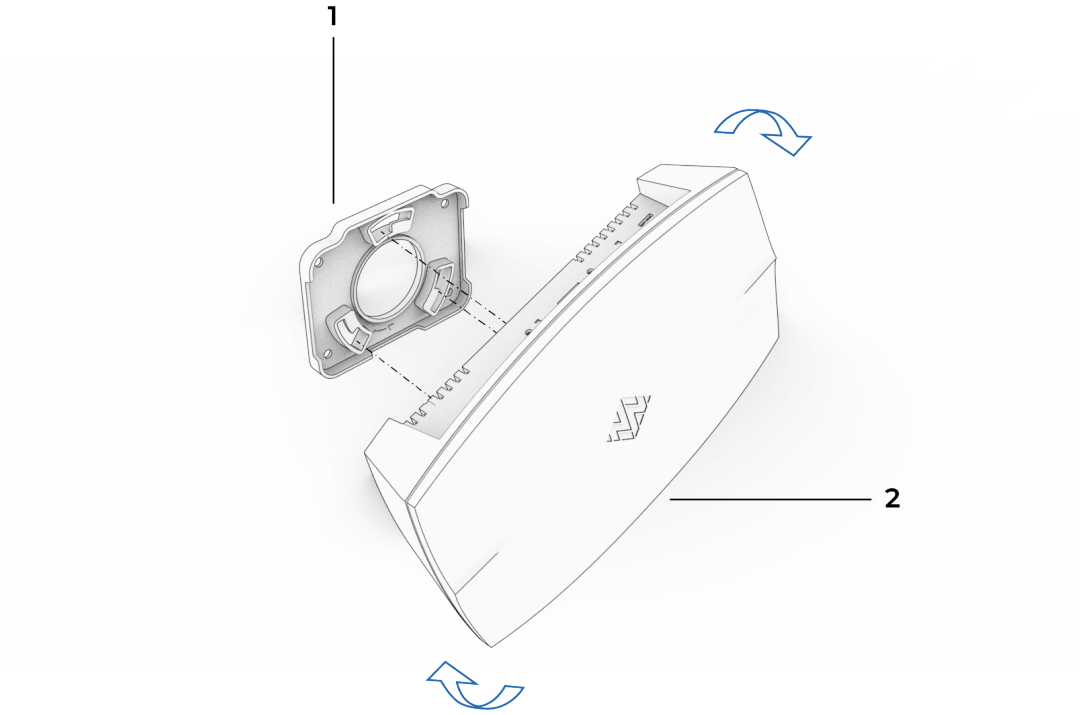


4. Put the mount (1) in position on the wall or ceiling.



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 4. Configuration

Configure static IP and HTTP proxy

If you install a Guardian Air in a network that does not have DHCP, you will need to do a manual configuration.

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* and *hypertext transfer protocol (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 *operating system (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 *classless inter-domain routing (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 *domain name server (DNS)* server.
8. On the *USB* pendrive, create a file with the name: `environment`
9. In the `environment` file, enter this text:

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

10. 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/`
11. Save both the `eth0-manual.network` and the `environment` files.
12. Safely eject the *USB* pendrive.
13. If the Guardian Air device is powered on, disconnect the electrical power cable.
14. Connect the *USB* pendrive to one of the *USB* ports on the Guardian Air device.
15. To turn on electrical power to the Guardian Air device, connect the electrical power cable.
16. 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 directly, or through the configured *HTTP* proxy.
17. If the *LED* does not flash green, see the Troubleshooting (on page 40) procedure.
18. Safely eject the *USB* pendrive.

Results

Guardian Air is now configured with a static *IP* and *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 21) procedure.

Revert the static IP and HTTP proxy configuration

Remove the static IP and HTTP proxy settings to restore the default network configuration on the Guardian Air device.

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* and *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 `eth0-manual.network` file.
3. Remove all the text from the file.
4. Open the `environment` file.
5. Remove all the text from the file.
6. Save the `eth0-manual.network` file.
7. Safely eject the *USB* pendrive.
8. Make sure that the Guardian Air device is powered off. If it is 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 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.
12. Safely eject the *USB* pendrive.

Results

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

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

Chapter 5. 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 6. 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 static IP and HTTP proxy 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 `eth0-manual.network` file to make sure that it is correct.
4. Read the `environment` file to make sure that it is correct.
5. If you found a mistake in one or both of the files, correct the mistake(s).
6. Do the Configure static IP and HTTP proxy (on page 29) procedure again.

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

Glossary

Classless Inter-Domain Routing

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.