



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

Copyright © 2013-2025, Nozomi Networks. All rights reserved. Nozomi Networks believes the information it furnishes to be accurate and reliable. However, Nozomi Networks assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of Nozomi Networks except as specifically described by applicable user licenses. Nozomi Networks reserves the right to change specifications at any time without notice.

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.....	5
Guardian Air overview.....	7
Description.....	9
Operation.....	13
Chapter 2. Requirements.....	15
Requirements.....	17
Chapter 3. Setup.....	19
Connect a Guardian Air sensor to Vantage.....	21
Install a Guardian Air sensor.....	24
Chapter 4. Configuration.....	27
v1.0.14 and after.....	29
Custom settings configuration.....	29
Configure custom settings.....	30
Revert custom settings.....	32
Up to v1.0.13.....	33
Configure an HTTP proxy.....	33
Revert an HTTP proxy configuration.....	35
Configure an NTP server.....	36
Revert an NTP server configuration.....	38
Configure a static IP address.....	39
Revert a static IP configuration.....	41
Chapter 5. Cleaning.....	43
Clean a Guardian Air sensor.....	45
Chapter 6. Troubleshooting.....	47
Status indicator shows fixed yellow.....	49
Status indicator shows flashing yellow.....	49
Failure to connect after HTTP proxy configuration.....	50
Failure to connect after NTP server configuration.....	51
Failure to connect after static IP configuration.....	52
Glossary.....	53



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

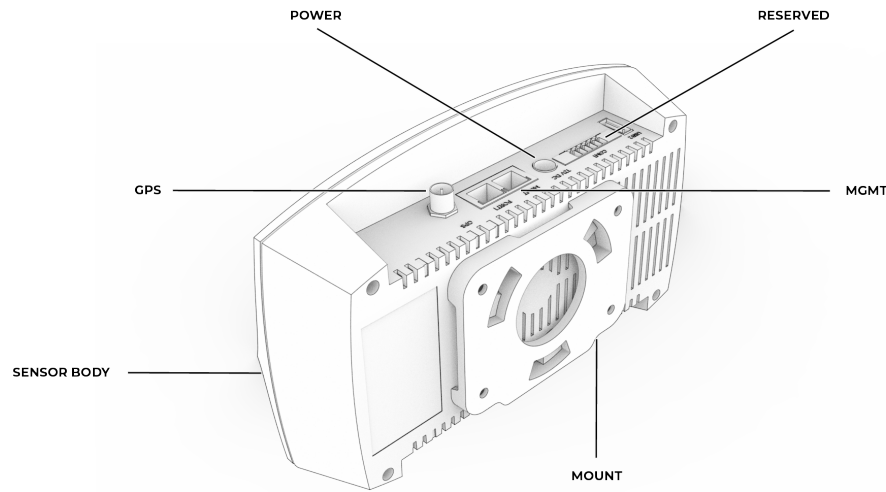


Figure 1. Guardian Air

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

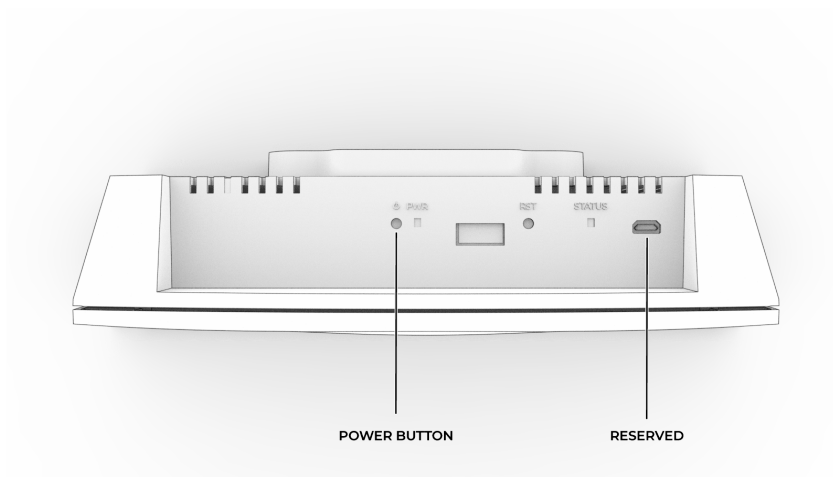


Figure 2. Guardian Air - top view

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

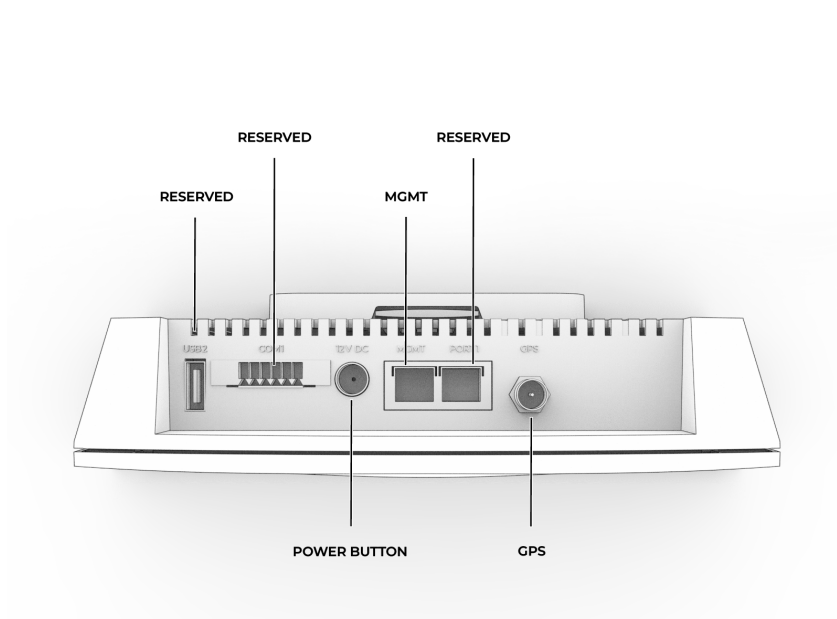


Figure 3. Guardian Air - bottom view

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

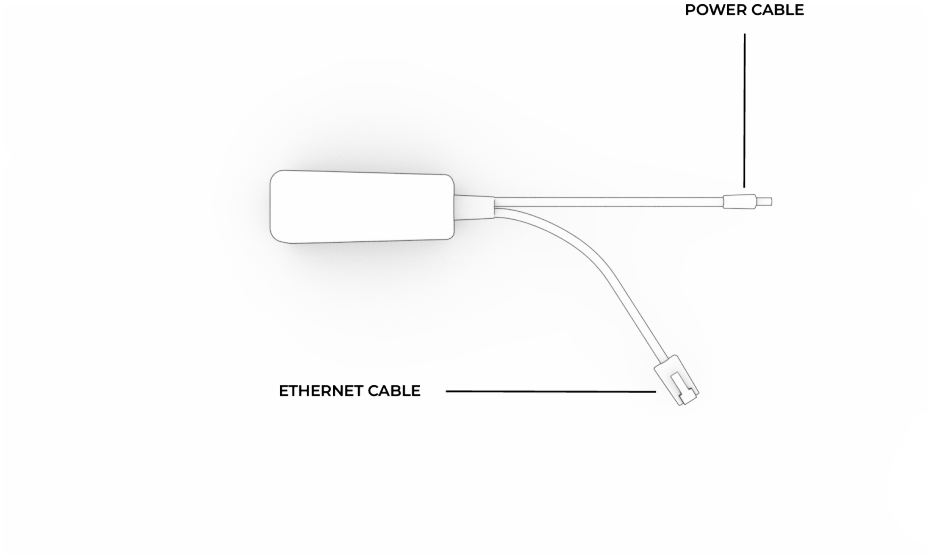


Figure 4. Power over Ethernet (PoE) connector

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

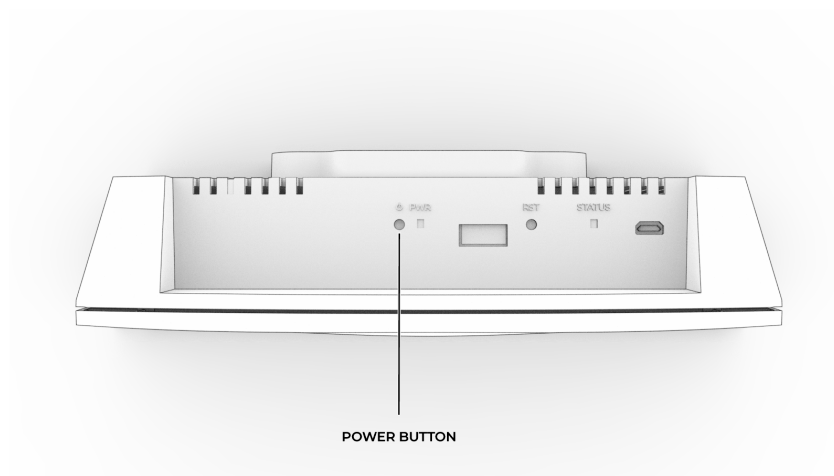


Figure 5. Power button

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

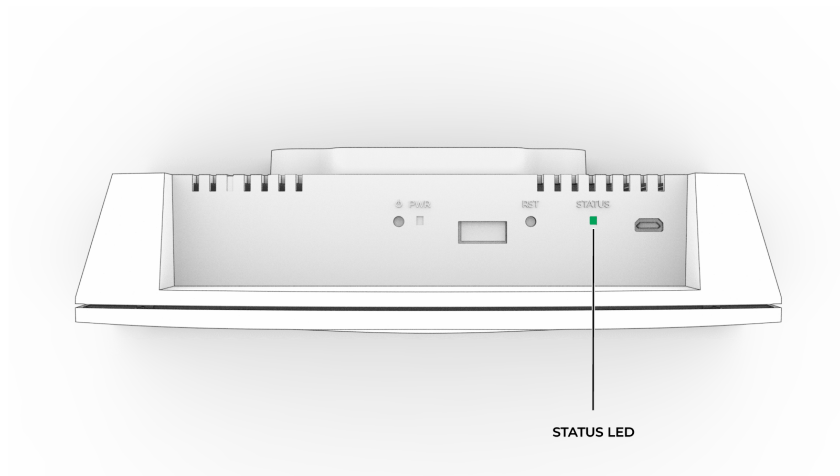


Figure 6. Status LED

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. 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

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 \(on page 33\)](#)
- [Configure a static IP address \(on page 39\)](#)

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 \(on page 36\)](#) 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 \(on page 21\)](#).
- Without a [PoE](#)-compatible switch. Go to [3 \(on page 22\)](#).

- 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.

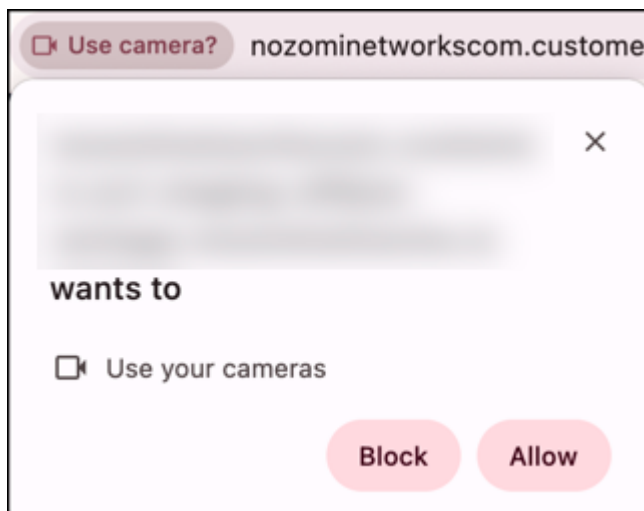
3. Connect without a *PoE*-compatible switch.
 - a. Connect the provided external power supply to the power plug.
 - b. Connect a standard Ethernet cable to the **MGMT** port.The ethernet cable must be connected to a network with *DHCP* enabled, and firewall rules/policies need to allow connectivity 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 \(on page 33\)](#)

[Configure an NTP server \(on page 36\)](#)

[Configure a static IP address \(on page 39\)](#)

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).

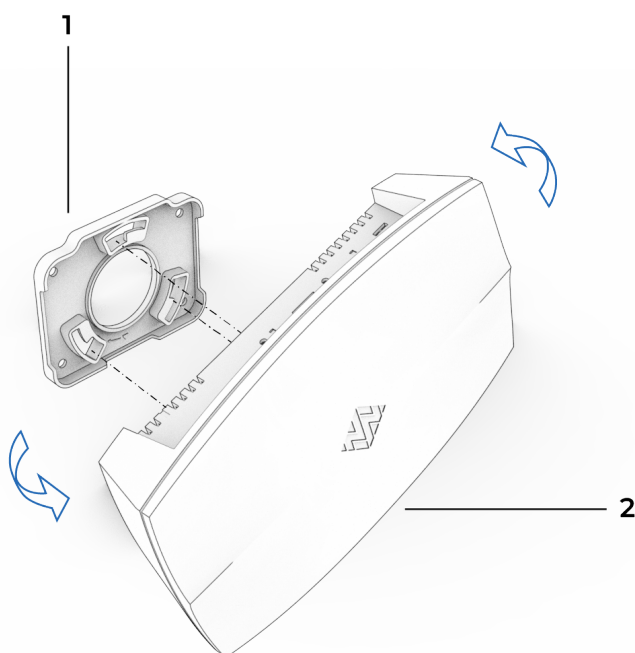
Procedure

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

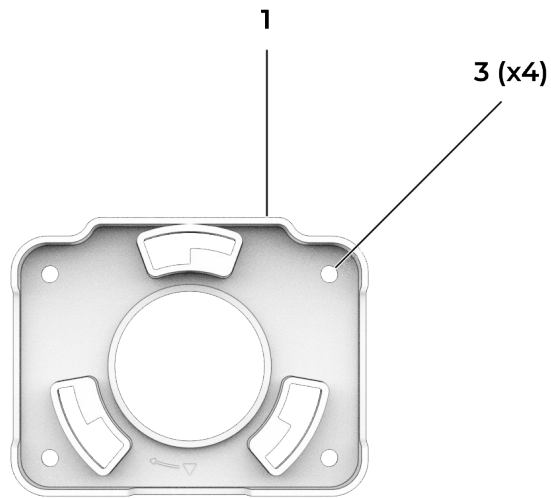
Choose from:

- 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.

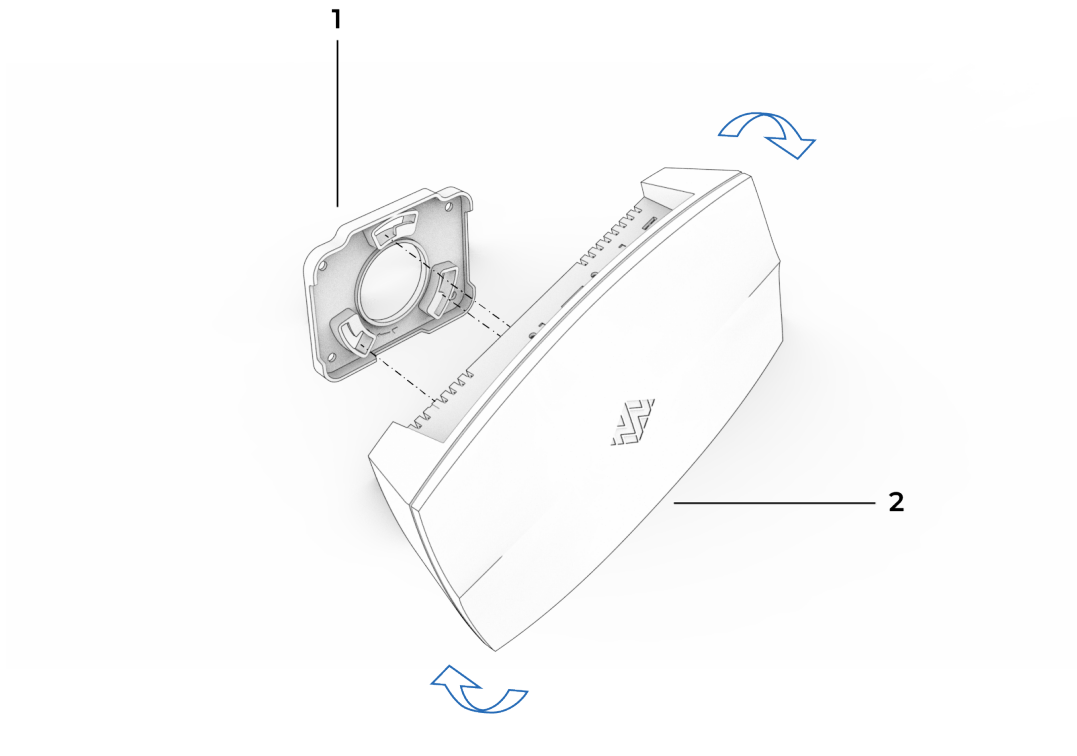


4. Put the mount (1) in position on the wall or ceiling.



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



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 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 \(on page 29\)](#).

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 \(on page 49\)](#) 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 \(on page 21\)](#) procedure.

Related information

[Revert custom settings \(on page 32\)](#)

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 \(on page 50\)](#) 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 \(on page 21\)](#) procedure.

Related information

[Revert an HTTP proxy configuration \(on page 35\)](#)

[Failure to connect after HTTP proxy configuration \(on page 50\)](#)

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 \(on page 51\)](#) 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 \(on page 21\)](#) procedure.

Related information

[Revert an NTP server configuration \(on page 38\)](#)

[Failure to connect after NTP server configuration \(on page 51\)](#)

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 \(on page 52\)](#) 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 \(on page 21\)](#) procedure.

Related information

[Revert a static IP configuration \(on page 41\)](#)

[Failure to connect after static IP configuration \(on page 52\)](#)

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 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 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 \(on page 33\)](#) procedure again.

If none of the previous solutions work, please contact our [Customer Support](#) team.

Related information

[Configure an HTTP proxy \(on page 33\)](#)

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 \(on page 36\)](#) procedure again.

If none of the previous solutions work, please contact our [Customer Support](#) team.

Related information

[Configure an NTP server \(on page 36\)](#)

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 \(on page 39\)](#) procedure again.

If none of the previous solutions work, please contact our [Customer Support](#) team.

Related information

[Configure a static IP address \(on page 39\)](#)

Glossary



Classless Inter-Domain Routing

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

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.

cURL

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.

IPv4

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

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.

Network Time Protocol

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

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.