

Dickson Connect™ Gateway

LoRa-enabled gateway for
DicksonOne and OCEAView
monitoring platforms

Firmware 3.x



Notices and safety

Read this first

Please read these simple guidelines before using your Dickson product. It may be dangerous or against local laws or regulations to not follow them.

Disclaimer and limitation of liability

Dickson assumes no liability for any loss or claims by third parties which may arise through the use of this product. Users must not use the product in any manner not specifically indicated by Dickson. In the case that the device is used in any manners not specified by Dickson, the protection provided by the device may be compromised. The proper use of the device is of the responsibility of the user.

Dickson shall not be held liable for improper use of this product. This document is non-contractual and subject to change without notice.

Safety instructions

The latest safety instructions document is available for download from the Dickson website. Flash this QR code to access the document:



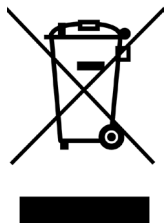
https://docs.oceaview.com/dickson_safety.pdf

Certifications and compliance

Please see [Chapter 5 – Appendix – Certifications and compliance, p. 38,](#) for a complete list of certifications and compliance references.

WEEE compliance

This device complies with the essential requirements and other relevant provisions of the Waste Electrical and Electronic Equipment Directive 2002/96/EC (WEEE Directive).



Environmental protection

Please respect local regulations concerning disposal of packaging, unused wireless devices, and their accessories, and promote their recycling.



RoHS compliance

This device is compliant with the restriction of the use of certain hazardous substances in electrical and electronic equipment Directive 2002/95/EC (RoHS Directive). Do not dispose of this product with household trash. Dickson recycles this product under certain conditions. Please contact us for more information.

Dickson Europe

Montpellier – France
+33 499 13 67 30
contact@dicksondata.fr

Dickson North America

Addison, IL – USA
+1 (630) 543-3747
contact@dicksondata.com

Dickson Asia-Pacific

Petaling Jaya – Malaysia
+603 749 40758
contact@dicksondata.my

© 2025 Dickson. All rights reserved. Dickson, DicksonOne, OCEAView, the Dickson logo, RFL, Cobalt X, Cobalt X1, and Cobalt X2 are the exclusive property of Dickson. WisGate Edge Lite 2 is the property of RAKwireless Technology Limited. All other brands mentioned are the property of their respective owners. This is a non-contractual document. Features and specifications mentioned here are subject to change. Document updated for gateway firmware v3.1.

May 2025

Ref: ING-INS-203-EN

Rev. 04

Table of Contents

1 Introduction	5
1.1 Features	6
1.1.1 Functionality	6
1.1.2 Connectivity	6
1.1.3 Hardware.....	6
1.1.4 Package contents	6
1.2 How it works	7
2 Setting up your gateway	8
2.1 Getting started.....	9
2.1.1 Changing the Wi-Fi access point key	13
2.2 Setting up LoRaWAN	14
2.2.1 Select your platform and environment	14
2.2.2 Select your country to set the radio frequency	17
2.3 Settings for your WAN network(s).....	18
2.3.1 Configuring Ethernet settings	19
2.3.2 Using the gateway as a Wi-Fi access point	20
2.3.3 Configuring Wi-Fi settings	22
2.3.4 Configuring cellular settings	24
2.3.5 Setting up fallback communication channels.....	25
2.4 Testing your LoRaWAN connection	26
3 Settings	28
3.1 General settings.....	28
3.2 Backup and restore.....	29
3.3 Firmware	30
3.3.1 Updating firmware manually via the gateway (DicksonOne and OCEAView).....	30
3.3.2 Updating firmware manually with DicksonOne.....	31
3.3.3 Updating firmware automatically with DicksonOne.....	32
3.4 User preferences	33
4 Troubleshooting.....	34
4.1 FAQ	34
4.2 LED indicators.....	37
5 Appendix – Certifications and compliance.....	38

1 Introduction

Thank you for choosing the Dickson LoRaWAN wireless monitoring solution. This document describes how to set up and use the Dickson Connect LoRaWAN gateway, a key part of your network infrastructure for collecting data from data loggers.

This gateway supports the following Dickson monitoring solutions:

- DicksonOne Cloud
- OCEAView Cloud and On-premises

After the first few steps of the initial startup procedure described in this guide, gateway operation is nearly identical for both solutions. Please check the user guides for DicksonOne and OCEAView for details about registering a gateway in your system to get the most out of your product.

The Dickson Connect LoRaWAN gateway forwards information such as sensor readings and alarms from supported Dickson data loggers to your monitoring platform. This gateway supports Ethernet, Wi-Fi, and/or cellular network connections, depending on regional availability.



Figure 1 – Dickson Connect LoRaWAN gateway

1.1 Features

1.1.1 Functionality

- Collects and forwards data from data loggers to Dickson's OCEAView and DicksonOne monitoring platforms
- Supports Dickson Cobalt and RFL LoRaWAN-equipped data loggers
- Integrated administrator interface for setup and firmware updates

The firmware in this gateway is customized by Dickson for WisGate Edge Lite 2 by RAKwireless Technology Limited. When performing firmware upgrades manually, you must only use firmware provided by Dickson.

1.1.2 Connectivity

- LoRaWAN long-range wireless technology
 - Free-field range up to about 15 km/10 miles
 - Frequency: worldwide (Europe, Asia-Pacific, Americas)
- Ethernet RJ45 (10/100 M); Wi-Fi (IEEE 802.11b/g/n, 2.4 GHz); Cellular (optional)

Note: Wi-Fi and cellular connectivity options are not available for the gateway model sold in China.

1.1.3 Hardware

- External LoRaWAN antenna
- Power: DC 12 V - 2 A (110-240 V AC adapter included) or Power-over-Ethernet (PoE)
- Dimensions: 66 x 127 x 36 mm
- Weight: 0.3 kg
- Operating temperature: -10 °C to 55 °C
- Ingress protection: IP30, for indoor use
- Enclosure material: plastic
- Wall-mountable, supports DIN rail
- ROHS 3, REACH

1.1.4 Package contents

- Dickson Connect LoRaWAN gateway
- AC adapter (110-240 V)
- LoRaWAN antenna
- Ethernet cable
- Mounting kit with screws

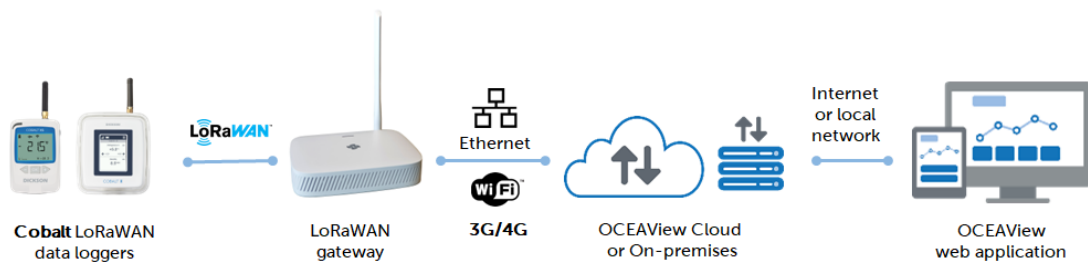
1.2 How it works

Installed at your site, the Dickson Connect LoRaWAN gateway forwards data to and from compatible Dickson data loggers within wireless range.

Its role is to continually transfer data via the Internet or local network to the configured monitoring platform, which users access via the web application.

The diagrams below summarize how the gateway fits into Dickson's two solutions.

OCEAView



DicksonOne

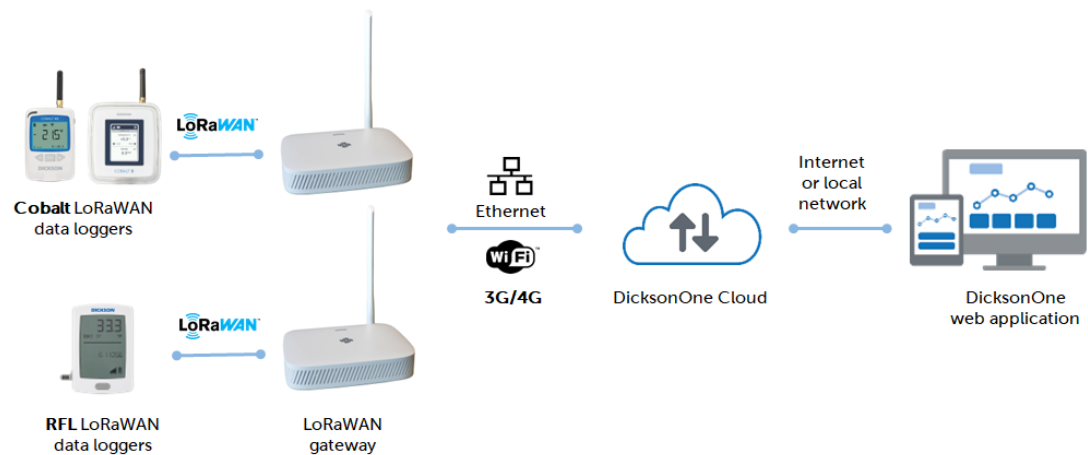


Figure 2 – Gateway connecting data loggers to the monitoring platform



The Dickson Connect LoRa gateway supports Cobalt and RFL data loggers, but it is not possible to use both types with a single gateway at the same time. If you need to use both types of data loggers with your account, you must install two gateways.

2 Setting up your gateway

This section explains how to get the gateway up and running in your environment.

Here is a summary of the process:

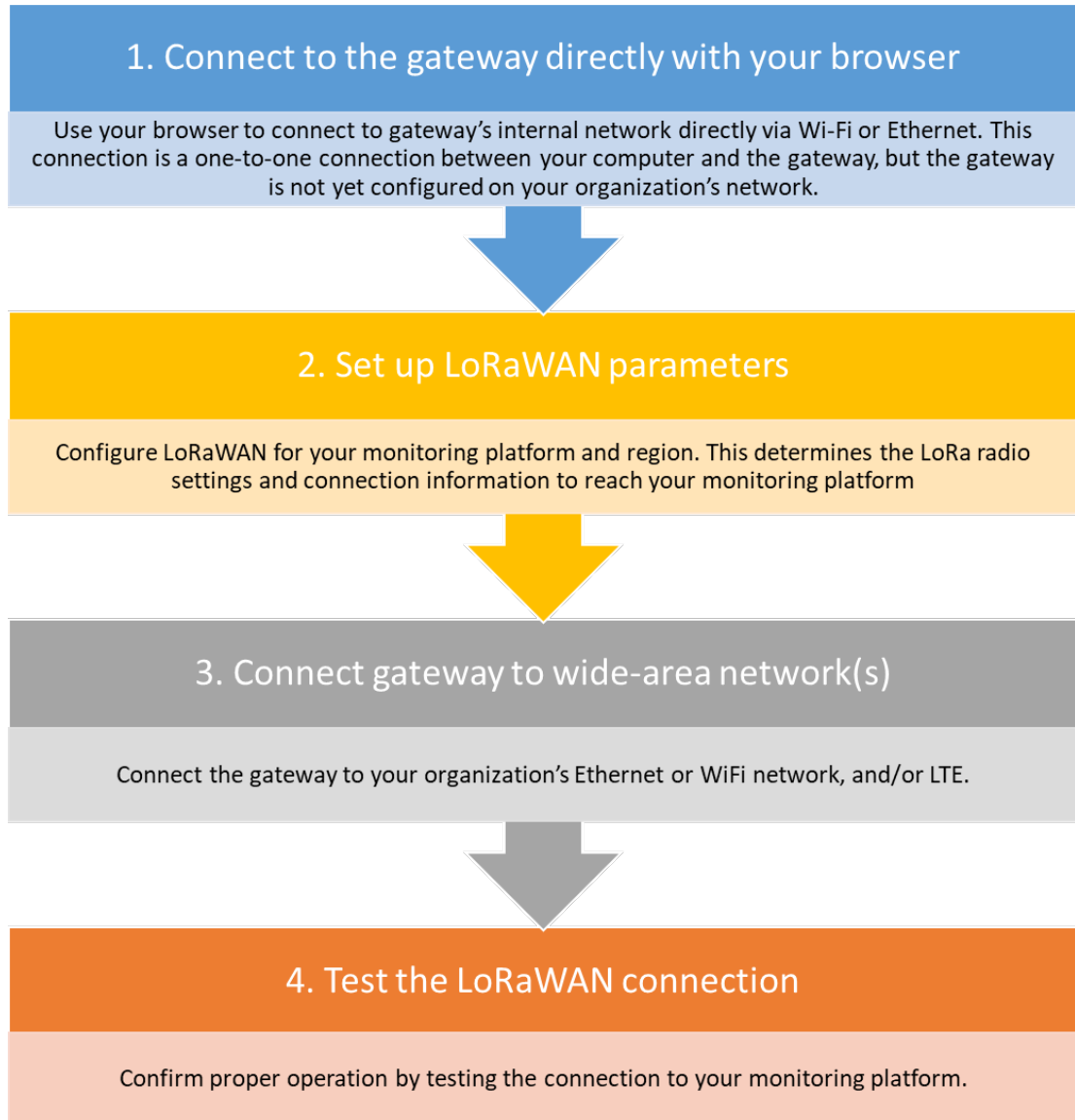


Figure 3 – Configuration process summary

2.1 Getting started

1. Before connecting power to the gateway, attach the provided LoRaWAN antenna to the connector on the back of the gateway.
2. Hand-tighten the antenna by rotating the ring clockwise on the connector.



Figure 4 – Attach LoRaWAN antenna to connector

3. To use AC power:

- Plug the AC adapter into a power socket.
- Plug the power cable into the gateway **1** to boot the device.

To use Power-over-Ethernet (PoE):

- Connect an Ethernet cable (configured for PoE) to the RJ-45 plug marked ETH(PoE) **1** to boot the device.



Figure 5 – Plug AC power cable into DC 12V input

When the gateway is started and ready to use, the “breathing LED” on top of the gateway **2** blinks slowly green, on and off.

4. Access the gateway interface from your computer via Wi-Fi or Ethernet:

Option 1: Connect via Wi-Fi *(not available in China)*

When the gateway finishes booting for the first time, it is automatically configured to run as a Wi-Fi access point. Later, when you are done setting up WAN settings to communicate on your network, the access point is turned off for security reasons (starting with firmware version 3.0.0.0). You may choose to reactivate it if you want.

To connect to your gateway running as an access point:

- Use your computer's Wi-Fi network selection to connect to the gateway, whose network name is "DKSN-####", where "####" represents the last four digits of the unit's serial number. You will find the serial number on the label on the bottom of the gateway:

Label on gateway:



Wi-Fi networks seen by your computer:

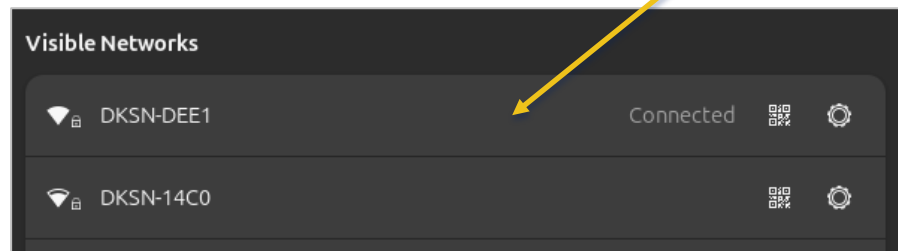


Figure 6 – Gateway serial number is part of its Wi-Fi network name

- When prompted for the network access key, enter "Dickson%####", where #### are the same four numbers as above.
- Use your browser to open one of the following URLs, based on the monitoring platform you are using:

<http://gw.oceaview.lan>

<http://gw.dicksonone.lan>

Note: The connection to the gateway is safe, even if your browser displays a security warning. Make sure you include "Error! Hyperlink reference not valid." when you enter the URL.

Option 2: Connect with an Ethernet cable

Follow these steps to connect to the gateway with an Ethernet cable:

- Plug an Ethernet network cable into the Ethernet port on the back of the gateway **1**.

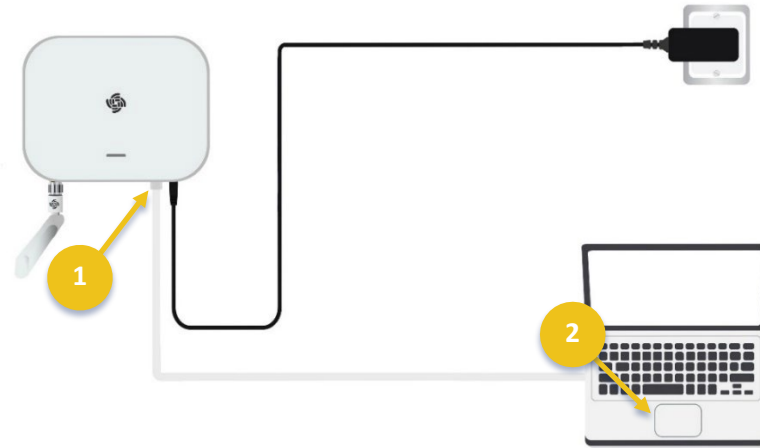


Figure 7 – Connecting your computer to the gateway via Ethernet

- Plug the other end of the cable into your computer **2**. Assign the following IP information temporarily in your computer's network settings (don't forget to change it back when you are done configuring the gateway):

IP: 192.168.2.199

Mask: 255.255.255.0

- Use your browser to connect to the gateway's default IP address:
<http://192.168.2.1>



For best results, we recommend that you use Google Chrome.

5. When you first connect, you will be prompted to set a password for the default “root” user account:

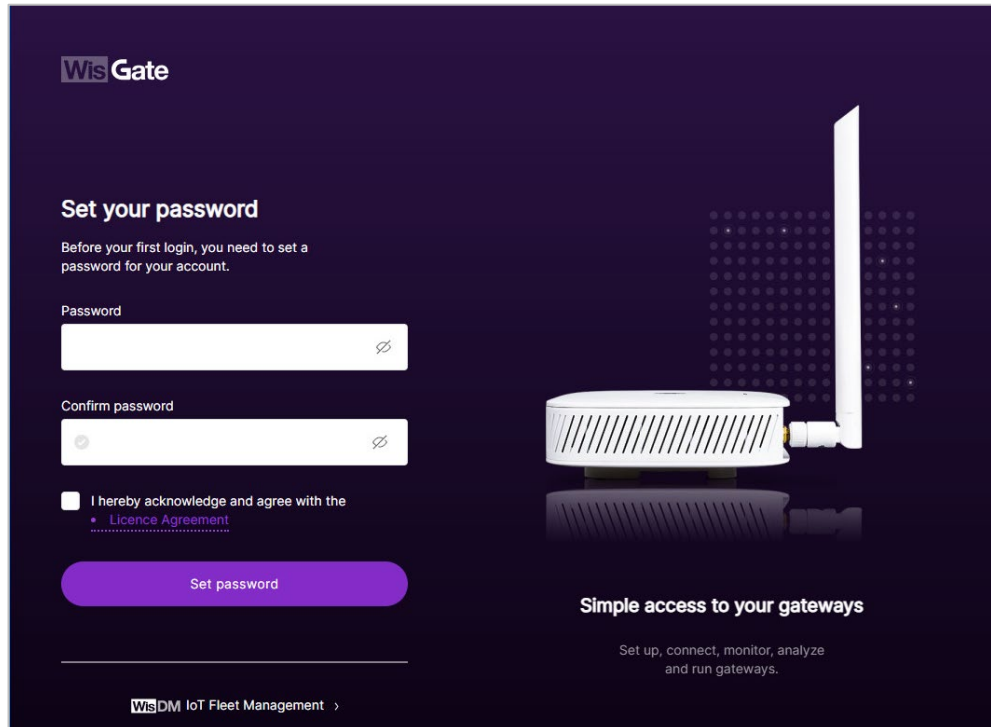
The screenshot shows the 'Wis Gate' web interface for setting a password. The title is 'Set your password'. Below it, a message states: 'Before your first login, you need to set a password for your account.' There are two input fields: 'Password' and 'Confirm password', both with a strength indicator icon on the right. Below the fields is a checkbox labeled 'I hereby acknowledge and agree with the' followed by a link 'Licence Agreement'. A large blue button labeled 'Set password' is positioned below the checkbox. To the right of the form is a 3D rendering of a white LoRa gateway device with a vertical antenna. At the bottom right, the text 'Simple access to your gateways' is displayed above the subtext 'Set up, connect, monitor, analyze and run gateways.' The footer at the bottom left reads 'WisDM IoT Fleet Management' with a right-pointing arrow.

Figure 8 – Setting the password for the “root” account



This password applies to the username “root” (which you will use on subsequent logins).

The password must be at least 12 characters long, with at least one special character, one number, and one letter.

6. Enter the same password in both fields, click to accept the terms of the license agreement, then click on **Set password**.
7. You will be logged into the interface automatically.
8. Next time you connect to the gateway, login with the username “root” and the password you created, then click on **Login**.

2.1.1 Changing the Wi-Fi access point key



Your gateway initially boots up as a Wi-Fi access point to make it easy for you to connect to the configuration interface. For security reasons, we recommend that you change the access point key (not to be confused with the system login name and password).

If you do not change the access point key or leave the prefix as “Dickson”, Wi-Fi access point functionality will be deactivated automatically after you set up your WAN connection(s).. If you want to use that feature, you must enable it later.

1. After logging in, click on **Network** () ➔ **LAN** ➔ **Wi-Fi** > **Settings**
2. Click in the **Key** field and enter a new key.
3. Click on **Save** at the bottom of the screen when done.

Note: if you are connected to your gateway via Ethernet and you do not intend to use Wi-Fi access point functionality, you can click on the **Disabled** button to turn off Wi-Fi.

2.2 Setting up LoRaWAN

The next step in the setup process is to configure network connections. In this guide, we focus on the settings that are relevant for using the gateway with DicksonOne and OCEAView. You may leave all other settings in the interface at their default values. More information (excluding Dickson customizations) can be found in the WisGate Edge Lite 2 documentation by RAKwireless Technology.

2.2.1 Select your platform and environment

Upon your first connection to the gateway, you must specify the monitoring platform and environment you are using.

1. Click on **Select platform** 

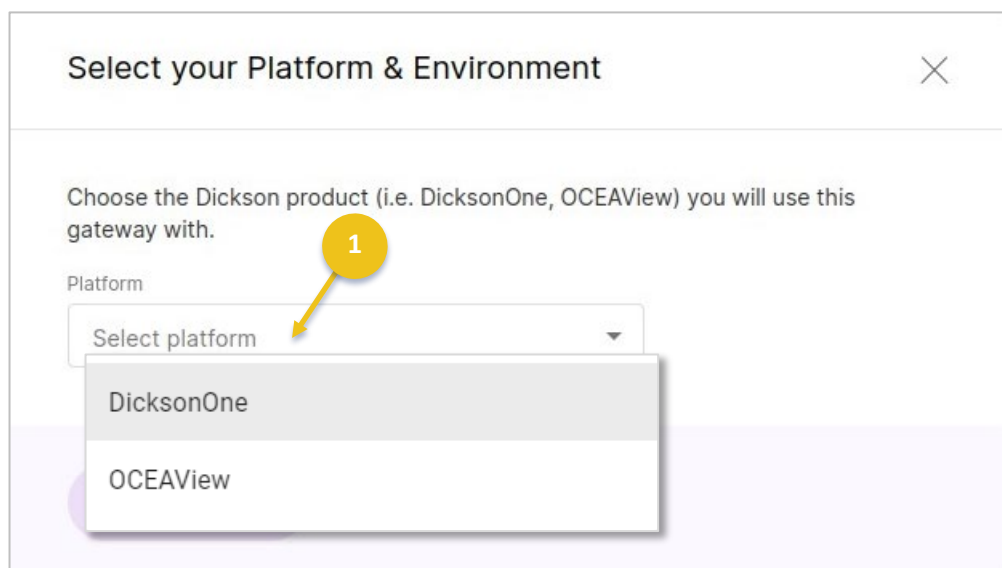


Figure 9 – Select your monitoring platform

Note: this option can be accessed via the menu by selecting  (Configuration) → Change platform:

2. Choose either OCEAView or DicksonOne.

DicksonOne: RFL US, RFL Mapping US, RFL EU, Cobalt US, Cobalt EU

The screenshot shows a dialog box titled "Select your Platform & Environment" with a close button (X) in the top right corner. Inside the dialog, there is a text prompt: "Choose the Dickson product (i.e. DicksonOne, OCEAView) you will use this gateway with." Below this is a "Platform" dropdown menu. A yellow arrow points to the "DicksonOne" option, which is currently selected. Below the platform selection, there is another text prompt: "Choose which environment you are using for the selected platform." This is followed by an "Environment" dropdown menu. The dropdown is open, showing a list of options: "RFL US", "RFL Mapping US", "RFL EU", "Cobalts US", and "Cobalts EU".

OCEAView: North America, Europe, Asia, and Custom (On-premises solutions)

The screenshot shows the same "Select your Platform & Environment" dialog box, but with "OCEAView" selected in the "Platform" dropdown menu. A yellow arrow points to this selection. The "Environment" dropdown menu is also open, showing a list of options: "North America", "Europe", "Asia", and "Custom". At the bottom of the dialog, there is a "Confirm" button.

Figure 10 – Platform and environment selection

3. Click in the **Environment** field and choose the appropriate option. This determines the LoRaWAN connector and data center to which the gateway connects.

The options are as follows:

Monitoring solution	Menu option	Data loggers	Data center location
DicksonOne	RFL US	RFL	North America
	RFL Mapping US		North America
	RFL EU		Europe
	Cobalt US	Cobalt	North America
	Cobalt EU		Europe
OCEAView	North America	Cobalt	North America
	Europe		Europe
	Asia		Asia
	Custom		On-premises

When you make your choice, the **Server address** in the section **LoRa Packet Forwarder parameters** is adapted automatically according to your platform and environment settings.

For OCEAView On-premises solutions, you must fill in the **Server address** field manually (see also section 2.4 – *Testing your LoRaWAN connection*, p. 26). The LoRa Connector mechanism is generally located on the same computer as the OCEAView On-premises server.



The network test performed when you press the **Test LoRa Server reachability** button cannot be successful until your gateway is set up on your organization's network as described in section 2.3 – *Settings for your WAN network(s)*, p. 18.

4. Press **Confirm** at the bottom of the screen when done.



As of this writing, a single gateway does not support the use of Dickson RFL and Cobalt data loggers at the same time. If

you need to use both types of data loggers, you will need two gateways, one for each.

2.2.2 Select your country to set the radio frequency

The gateway will automatically prompt you to specify your regional details. The options displayed here are based on the LoRaWAN radio hardware installed in your gateway. You can change these settings at any time if necessary.

1. Use the pull-down menu to select the appropriate options. The first field, Country, is always **Worldwide, WW**.

Change your country [X]

Selecting the correct country will assure you are operating under the local law requirements. The transmit power of your gateway will be set to the local regulation maximum and the LBT feature will be turned on if required.

Country
Worldwide, WW

Region
[Dropdown]

☐ I confirm that I have chosen the country where the gateway is located. I acknowledge that countries have different rules applicable to the radio band of a gateway and if I chose the wrong country, I may be in breach of the local legislation. I further agree to indemnify and hold the manufacturer, seller, and their respective affiliates harmless in case I choose the wrong country and thus violate the applicable law.

Confirm

Figure 11 – Select and confirm your regional details

2. Click in the **Region** field 1 to select the appropriate information, then click on **Confirm**. You may also need to confirm third field labeled “Variations”. The table below shows the potential options:

Country	Available regions	Radio frequency	Variations
Worldwide, WW	Europe/Africa	868 MHz	–
	India	865 MHz	
	Russia	864 MHz	
	Australia/Brazil USA/Canada/Mexico	915 MHz	–
	Korea	920 MHz	
	Other	923 MHz	Asia, Indonesia / Vietnam, Cuba, Israel

	China	470 MHz	–
--	-------	---------	---

3. Click on **Save** at the bottom of the screen when done.

2.3 Settings for your WAN network(s)

Until the gateway is able to access your network(s), the LED bar **1** on top of the gateway blinks red.

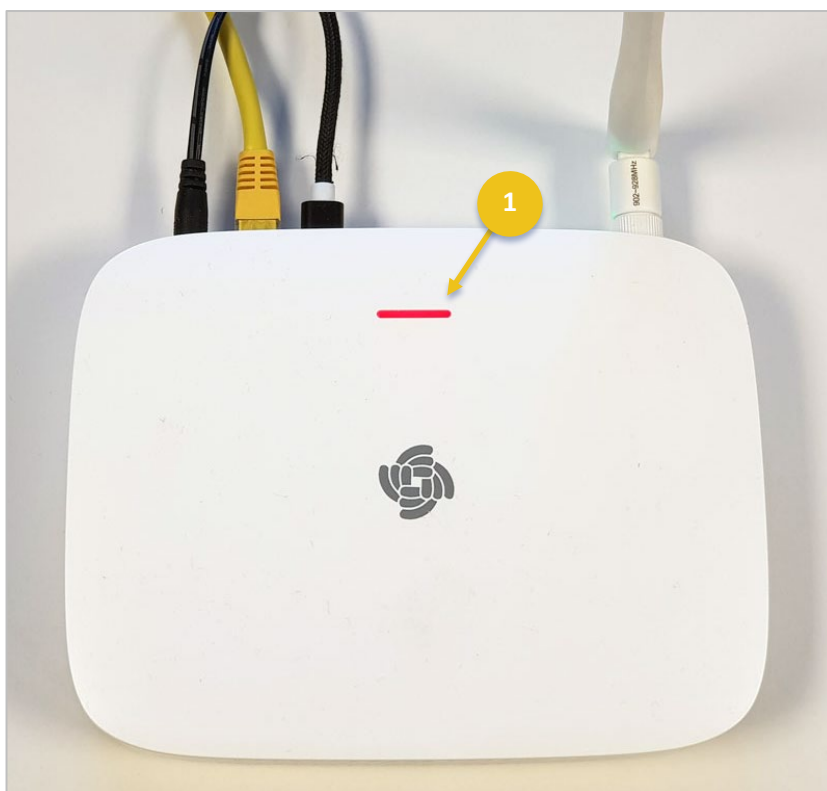


Figure 12 – Blinking Red LED indicates no network access

The next step is therefore to configure the gateway's WAN connections to communicate using your Ethernet, Wi-Fi, and/or cellular network(s).

2.3.1 Configuring Ethernet settings

1. Click on **Network** () → **WAN** → **Ethernet** → **Settings**

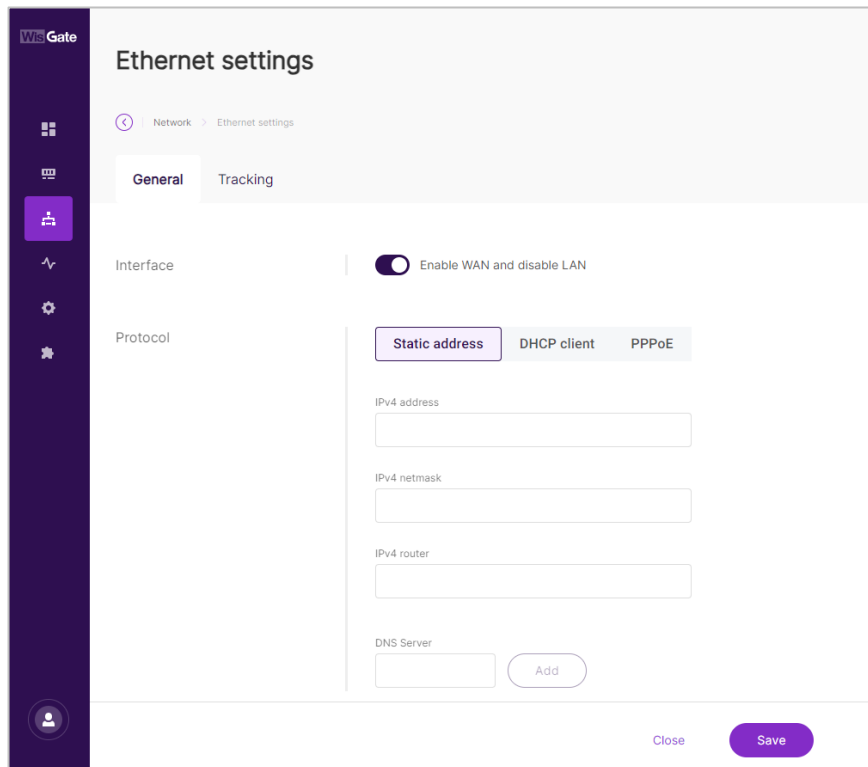


Figure 13 –Ethernet settings for your network

2. Set **Enable WAN and disable LAN** to on ().

Note: "WAN" refers to communications from the gateway to your monitoring platform; "LAN" refers to local communications between the gateway and your computer used during the initial setup process.

3. Click on the **Static address** or **DHCP client** according to your needs:

Static IP address

If you would like to set a static IP address, enter the information to match your network in the fields **IPv4 address**, **IPv4 netmask**, **IPv4 router**, **DNS server**.

DHCP client

If you want the gateway to get its IP address from your network's DHCP server, click on the **DCHP client** tab. This is often referred to as Dynamic IP.

Here, you may either enable **Use DNS servers advertised by your router** (), or disable this option in order to add the IP address of your DNS server. In either case, the gateway must be able to reach the OCEAView platform as well as one or more Network Time Protocol (NTP) servers via the Internet.

4. Click on **Save** to apply your settings, or on **Close** to leave this page without saving changes. After a few moments the LED on top of the gateway will blink blue to indicate that the connection is established..
5. Remember to plug the gateway and your computer (if necessary) into your Ethernet network when you are done.

2.3.2 Using the gateway as a Wi-Fi access point



Unless you changed the Wi-Fi access point key as mentioned earlier, Wi-Fi access point functionality is automatically deactivated when you save your WAN settings as described in the previous section.

If you want to be able to connect to the gateway via Wi-Fi (and you did not change the default key), you must re-enable access point functionality.

To activate the gateway as a Wi-Fi access point (LAN connection):

1. Connect to the gateway via Ethernet either with its static IP address or check with your system administrator to obtain the IP address if the gateway is set up to use DHCP.
2. Login with the username "root" and the password you defined.
3. Click on **Network** () → **LAN** → **Wi-Fi** → **Settings**
4. Click on **Enabled** to activate the Wi-Fi access point for LAN use.

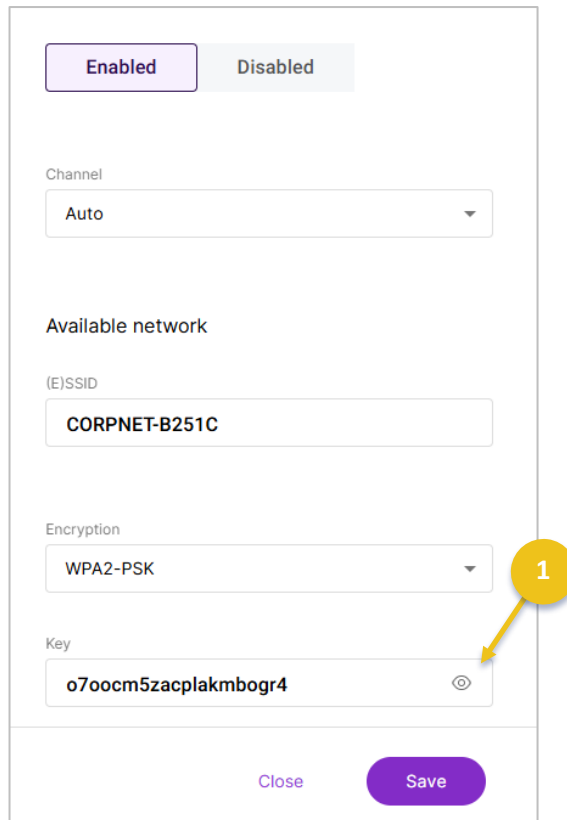


Figure 14 – Activating Wi-Fi for LAN access

5. Click on the eye  to show the contents of the Wi-Fi access point **Key** field key.

You will see that a 20-character random key has been generated, replacing the default key. Use this key when connecting wireless devices to the gateway via Wi-Fi.



We highly recommend that you keep track of your configuration settings and the access point key, if applicable.

If, for some reason, you can no longer login to the gateway interface, you will have to perform a factory reset (as described in the FAQ section of this user guide) and reconfigure the gateway.

2.3.3 Configuring Wi-Fi settings

To use Wi-Fi for the WAN connection, you must integrate your gateway into your organization's Wi-Fi network.



Wi-Fi connectivity is not available for this gateway in China.

To set up Wi-Fi:

1. Click on Network () → WAN → Wi-Fi → Settings

Wi-Fi settings

Network > Wi-Fi settings

General Tracking

Interface

Enabled Disabled

Available (E)SSID networks

Scan

Click scan to find available Wi-Fi networks or enter network (E)SSID manually.

Encryption

No Encryption

Protocol

Static address DHCP client

☒ Use DNS servers advertised by router

Disabling will ignore DNS servers advertised by the router.

Close Save

Figure 15 –Wi-Fi settings for your network

- | | |
|---|--|
| Enabled / Disabled | Use these buttons to turn Wi-Fi on or off. |
| Scan | Click on Scan to search and select a nearby Wi-Fi network. |
| Encryption | Choose WPA-PSK, WPA2-PSK, or WPA-PSK/ WPA2-PSK Mixed Mode according to your needs. |
| Static address or DHCP client | You may enter IP address information manually or allow the gateway to use DHCP to automate IP address configuration. |
| Use DNS servers advertised by router | Activate this option or enter DNS server information manually. |
2. Click on **Save** to apply your settings, or on **Close** to leave this page without saving changes.

2.3.4 Configuring cellular settings

To use a cellular connection for the WAN connection, you must specify the APN (Access point Name), the name of the gateway between the carrier's network and the Internet.



Cellular connectivity is not available for this gateway in China.

1. Click on **Network** () → **WAN** → **Cellular** → **Settings**
2. The APN depends on the communication frequency used in your region:

868 MHz: `iot.1nce.net`

915 MHz: `SUPER`

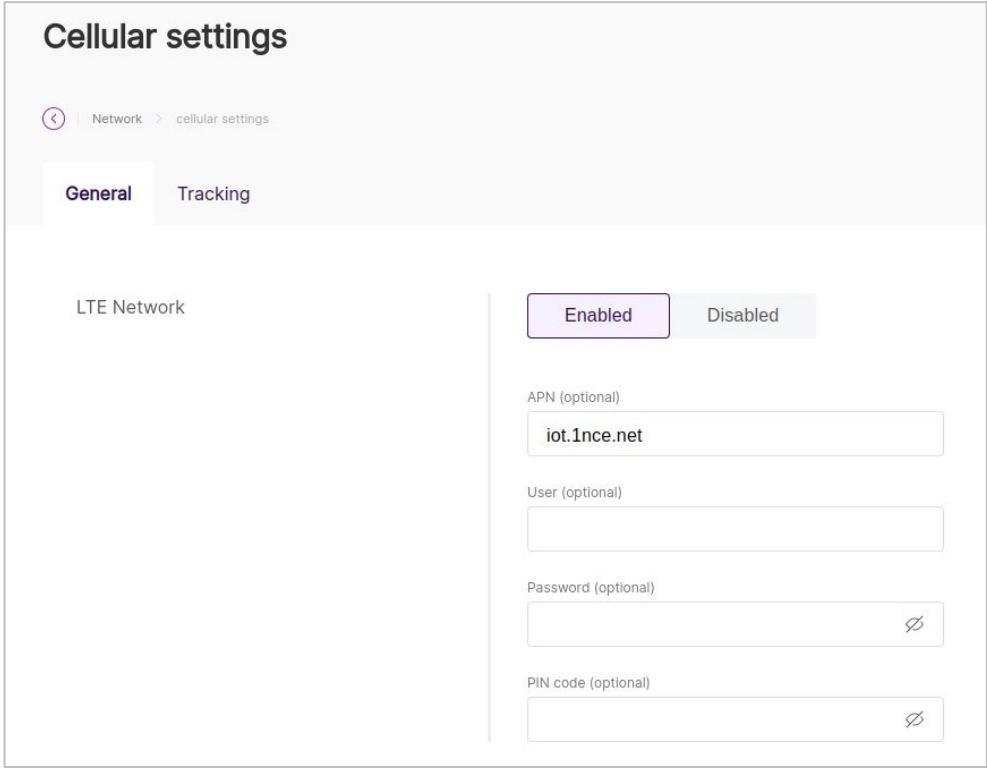


Figure 16 – Cellular network settings

3. Click on **Save** at the bottom of the screen when done.

2.3.5 Setting up fallback communication channels

Depending on your organization's layout and network, you may choose to use Ethernet, Wi-Fi, or cellular connectivity in your WAN configuration. You may also choose to set up several connectivity options as fallbacks in case one network encounters problems.

One of the channels serves as the primary connection method, and one or both of the others serve as fallbacks to ensure connectivity in case of failure.

To setup connectivity priorities for your system:

1. Click on **Network** () → **WAN** → **Change Priority**

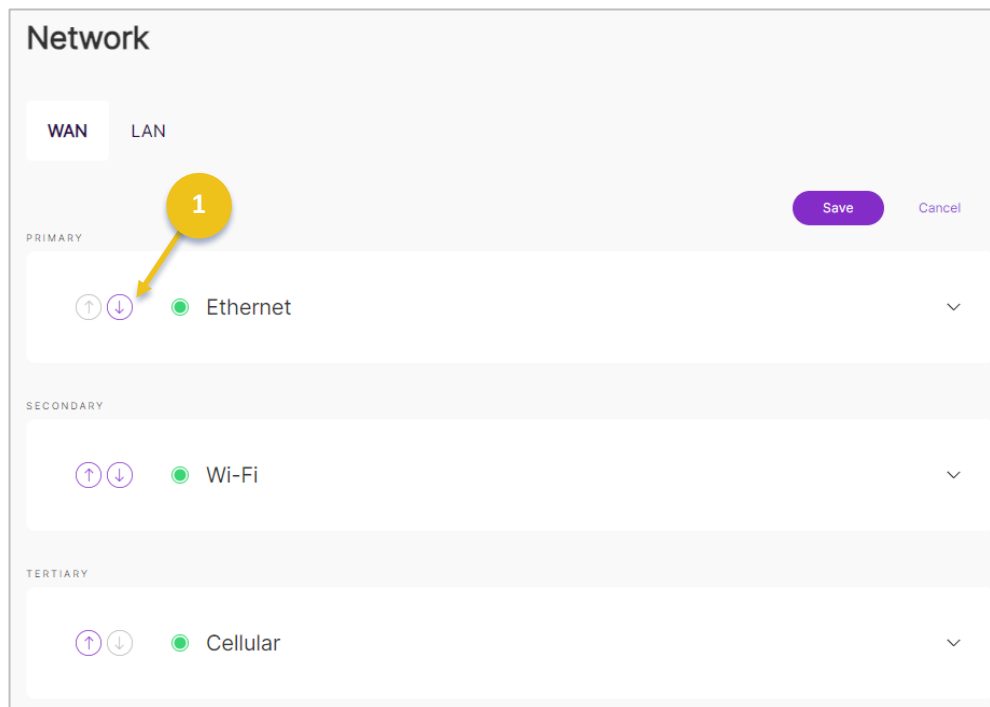


Figure 17 – Configuring connection fallback order

2. Use the up and down arrows ( ) () to change the order of your connectivity options.
3. Click on **Save** to keep your changes when you are done, or on **Cancel** to discard any changes.

2.4 Testing your LoRaWAN connection

After setting up your LoRaWAN and network connections, you can test your configuration to make sure the gateway reaches your monitoring platform correctly.



The server address for LoRaWAN connections is filled in automatically based on your platform and environment settings.

To check your connection or change settings:

1. In the left-hand menu bar, click on **LoRa** ().
2. In the section **LoRa Packet Forwarder parameters**, the Server address is adapted automatically according to your platform and environment settings.

For OCEAView On-premises solutions, you must fill in the **Server address** field manually.

Figure 18 – Enter or confirm the server address and test the connection to your OCEAView platform

OCEAView Cloud

Server addresses

connect-us.oceaview.com

connect-eu.oceaview.com

connect-asia.oceaview.com

Server port: 1700

Keepalive interval (s): 10

OCEAView On-premises

If you are using the OCEAView On-premises solution (with **Environment** set to **Custom**), enter the server and port information corresponding to your system. Set the **Keepalive interval** to 10 seconds.

DicksonOne

Server addresses

RFL data loggers

dicksonone.nam1.cloud.thethings.industries

dicksonone.eu1.cloud.thethings.industries

Cobalt X data loggers

us.d1.oceaview.com

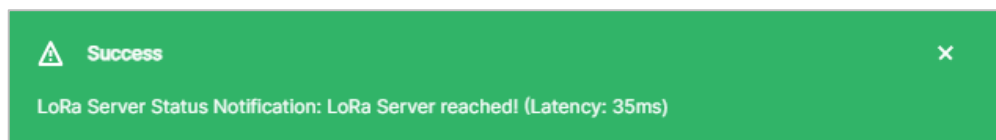
eu.d1.oceaview.com

Server port: 1700

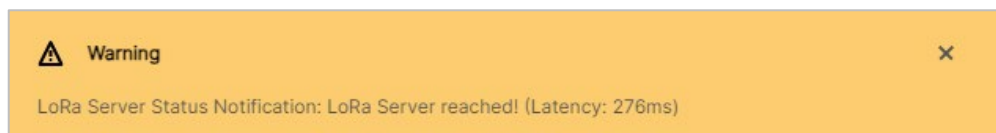
Keepalive interval (s): 10

3. Use the **Test LoRa server reachability** button to test the network connection between your gateway and the monitoring platform. This test must be successful for your solution to function correctly, with a latency value typically well under 200 ms. (a warning message is displayed in orange if latency is over 100 ms.).

 - Connection is good with acceptable response time:



- Connection is successful but with slow response time:



- Connection with server was not successful:

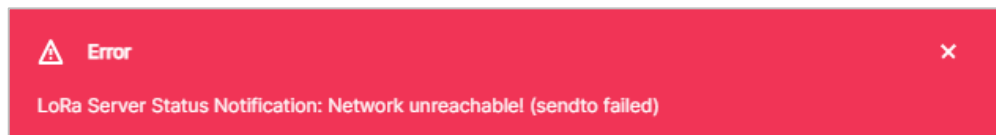


Figure 19 – Possible connection test results

4. Click on **Save changes** when done, if necessary, or click on any menu option in the left-hand menu bar to leave this page without saving changes.

3 Settings

The **Settings** menu () offers several configuration options and functions.

3.1 General settings

Gateway name You may change the “friendly name” for the device in your network. Simply type in a new name and press **Save**.

System log Your gateway keeps a log that can be used (with Technical Support) for debugging purposes. By default, the log is stored internally, but you may choose to point to an external log server.

Buffer size Maximum size of the log file to be saved.

Log expiration How long the log file is stored.

External system log server IP address
Address of the external system log server. Please check with Technical Support or your IT team if you need to use this feature.

Port – Corresponding port of the system log server.

Time synchronization Enables/disables time synchronization from a Network Time Protocol (NTP) server. In the NTP server candidates area, you can add or remove NTP candidates. You may add a new candidate by clicking on **Add new server candidate**.

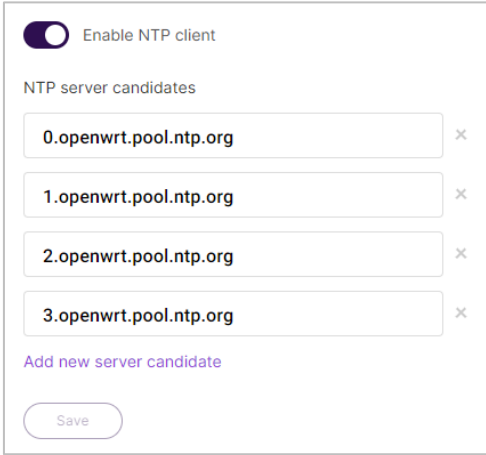


Figure 20 – Typical NTP settings

Reboot You may use the **Reboot** button to reboot the gateway. Any unsaved changes will be discarded. Any data loggers currently communicating may lose their connection during the time it takes to reboot. They will recover automatically.

3.2 Backup and restore

Settings

General settings **Backup and restore** Firmware

Backup

Use this option to create a backup image of the current configuration settings for the gateway.

☐ Set password to protect the backup archive

[Generate and download backup](#)

Restore

To restore the configuration file, you can upload a previously generated backup here.

Drop your archive file here or [choose file](#)

[Restore](#)

Reset

This action will reset the gateway to its factory default settings, and your configuration will be lost permanently.

[Reset](#)

Figure 21 – Back and restore tab

Backup

You may create a complete backup of your current gateway configuration by clicking on the **Generate and download backup** button. The system creates and downloads an archive file (tar.gz format) with all current settings. This file may be used to restore your settings with the **Restore** function.

Restore

You may upload an archive file by clicking on **choose file**, or drag-and-drop an archive file to restore previous settings.

Reset

You may click on the **Reset** button to restore the gateway's original factory settings. After you click on **Reset**, you will be prompted to confirm your action.

3.3 Firmware

3.3.1 Updating firmware manually via the gateway (DicksonOne and OCEAView)

This tab shows the gateway's current firmware version and allows you to update it manually if necessary.

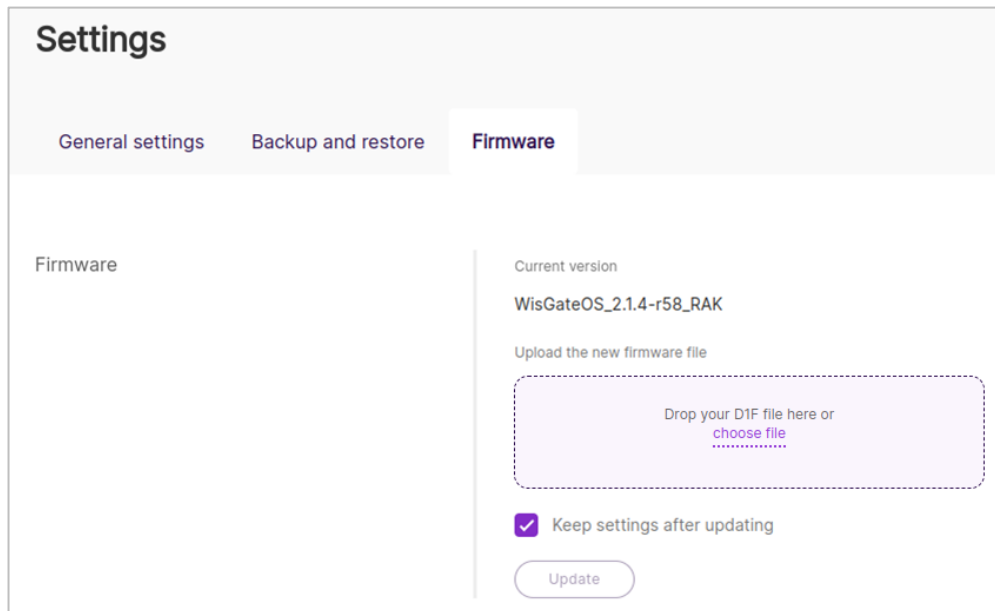


Figure 22 – Firmware management tab

To update the firmware:

1. Obtain a new "D1F" encrypted file from the Dickson technical support team.



You must only use firmware provided by Dickson. If you try to load other firmware files, an "Invalid firmware" message is displayed and the process does not continue.

2. Once you have the file on your computer, you may click on the link **choose file** to locate it, or drag and drop the file directly into the purple zone on the screen.
3. To keep your existing settings after the firmware update, make sure that the checkbox **Keep settings after updating** is selected.



The **Keep settings after updating** check box is selected by default. If it is unchecked, the gateway will be restored to factory settings after the firmware update.

4. Press **Update** and follow any on-screen instructions to launch the process.

3.3.2 Updating firmware manually with DicksonOne

The DicksonOne monitoring platform enables you to update your gateway manually with new firmware when it becomes available. We recommend updating firmware so that your gateway benefits from the latest improvements.

To update firmware manually:

1. Log in to DicksonOne using an account with Owner privileges.
2. Select **Manage** → **Gateways** from the left-hand menu.
3. In the list, click on the gateway you want to configure, then click on the **Firmware** (1) tab:

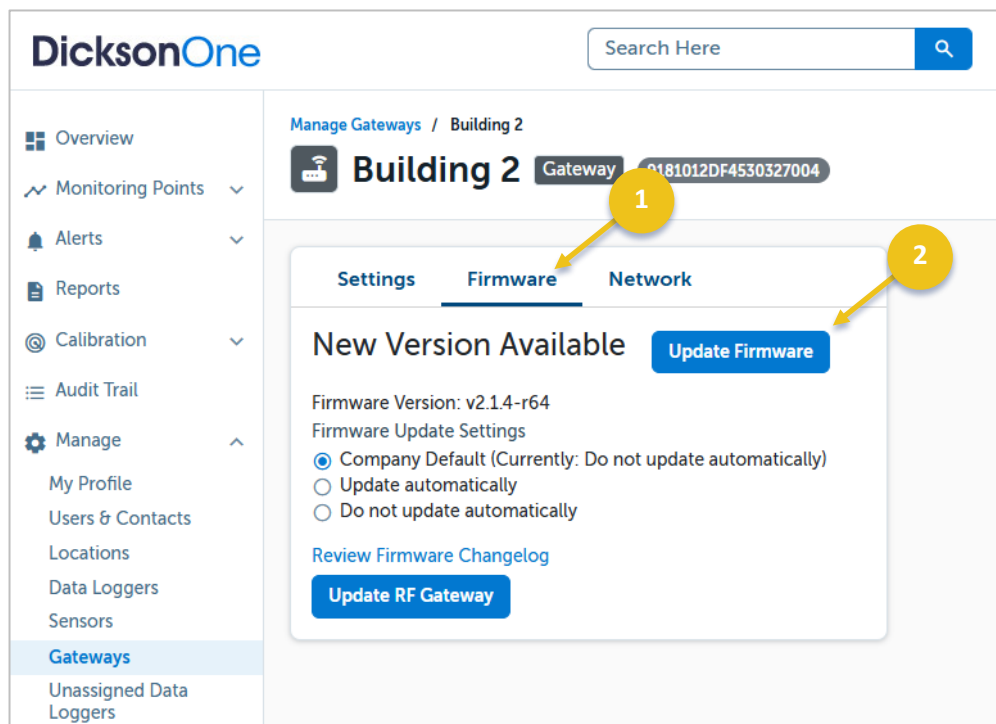


Figure 23 – Manual update on DicksonOne

4. If your system is not configured to update firmware automatically, an **Update Firmware** button (2) is displayed when new firmware becomes available.
5. Click on **Update Firmware** and follow any on-screen instructions if you want to install the new firmware in your gateway.

3.3.3 Updating firmware automatically with DicksonOne

DicksonOne includes a configuration option that enables the gateway to be updated automatically with new firmware when it becomes available. This ensures that your gateway always benefits from the latest improvements without requiring any action on your part.

To set up your gateway for automatic firmware updates:

1. Log in to DicksonOne using an account with Owner privileges.
2. Select **Manage** → **Gateways** from the left-hand menu.
3. In the list, click on the gateway you want to configure, then click on the **Firmware** (1) tab:

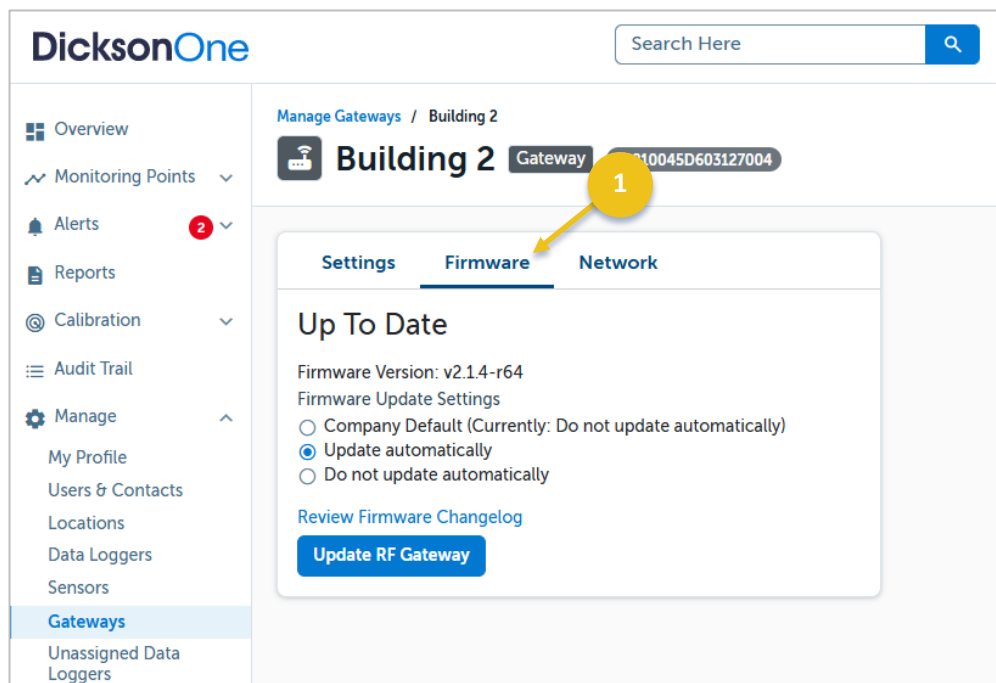
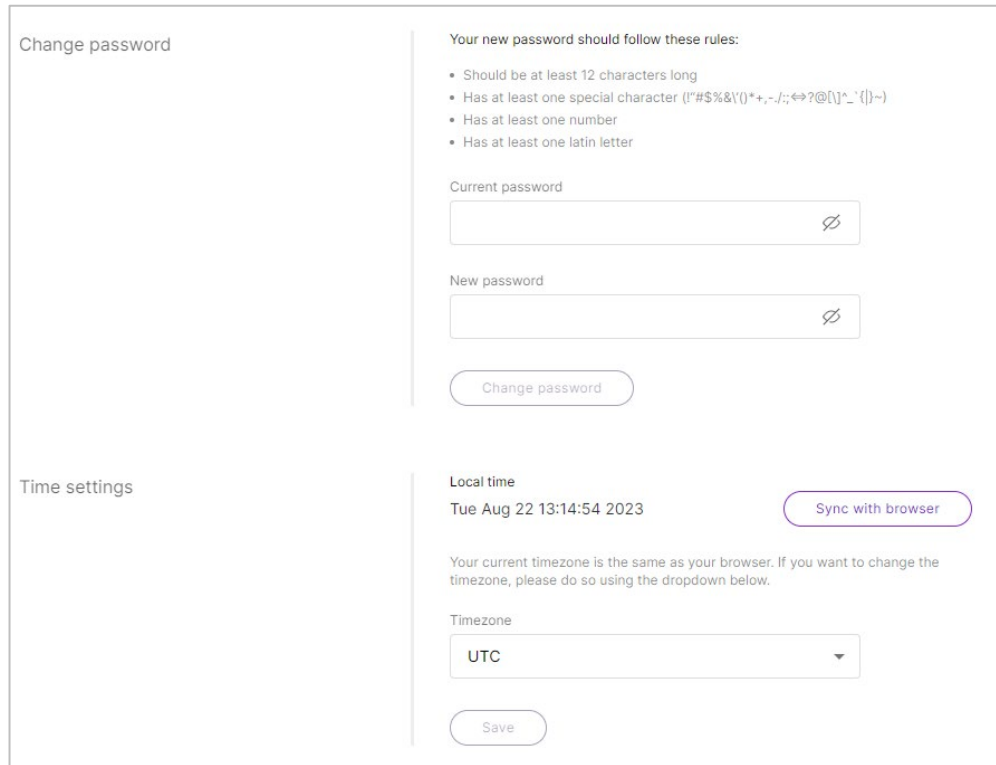


Figure 24 – Automatic update settings on DicksonOne

4. If you want updates to occur automatically, click on the **Update automatically** button.
5. Click on **Update RF Gateway** to apply any changes you make here. Changes are not saved if you leave this page without clicking this button.

3.4 User preferences

At the bottom of the left-hand menu bar, you may click on the icon () to logout from the Web interface or access **User preferences**.



The screenshot displays the 'User preferences' interface. It is divided into two main sections: 'Change password' and 'Time settings'. The 'Change password' section includes a list of password rules: 'Should be at least 12 characters long', 'Has at least one special character (!"#\$%&\'()*+,-./:;<=>?@[\\]^_`{|}~)', 'Has at least one number', and 'Has at least one latin letter'. Below these rules are two password input fields labeled 'Current password' and 'New password', each with a toggle icon on the right. A 'Change password' button is located below the 'New password' field. The 'Time settings' section shows the 'Local time' as 'Tue Aug 22 13:14:54 2023' with a 'Sync with browser' button. Below this, it states 'Your current timezone is the same as your browser. If you want to change the timezone, please do so using the dropdown below.' There is a 'Timezone' dropdown menu currently set to 'UTC' and a 'Save' button at the bottom.

Figure 25 – User preferences tab

The options here are:

Password

You may change the password you assigned when first logging in to the gateway interface. Enter the new password into the two fields and press the **Change password** button to assign it.

The username remains "root".

Time settings

You can set the gateway to the local time used by your computer's browser, and/or modify the time zone if necessary.

4 Troubleshooting

4.1 FAQ

If you are having difficulties with your configuration, look at these frequently asked questions before contacting technical support.

How can I test my LoRaWAN network connection?

In the **LoRa** setup screen, there is a **Test LoRa server reachability** button. When you click on that button, you should receive acknowledgment that the connection is up and running.



The latency indicated by this function must not be higher than 200 ms.

If the latency is too high, first check to make sure you entered the correct LoRa server URL. For example, if you are in North America, make sure to choose the North America option. If you choose Europe or Asia by mistake, it is possible that the latency would be too high for proper operation.

Otherwise, you may need to check with your IT department or Internet Service Provider to see why the connection is slow.

I would like to see how well LoRaWAN wireless coverage works at my site. Is there an easy way to perform tests?

Dickson Cobalt X data loggers include a **Range test** feature that enables you to test the LoRaWAN connection between a data logger and the gateway. For more information, or to conduct a more complete site survey, please contact your Dickson representative.

Can I test LoRaWAN wireless coverage at my site without connecting the gateway to the Internet?

You can use a Cobalt X data logger to test on-site coverage without an Internet connection (that is, just the LoRaWAN part), with the following configuration on the Cobalt X:

1. Select **Menu → Advanced → LoRaWAN → Network → Customer**.
2. Select the region and enter this 8-digit number via the keypad: "00000000".
3. In the LoRa section on the gateway, change the "Server Address" to 127.0.0.1 (an IP address that will not successfully connect to anything from your gateway), then click on **Save changes**.

4. You may then use the **Range test** feature on the X2 data logger to test LoRaWAN connectivity with your gateway.

I forgot my gateway's IP address or username/password and cannot connect to the administrator interface. Is there a way to restore factory settings?

The Dickson Connect LoRaWAN gateway has a reset button that can be pressed to restore factory settings. For example, you may choose to do this if you forgot the IP address you entered in network configuration, or if you forgot the username/password and can no longer connect to the administration interface.

To perform a factory reset:

1. Insert a blunt tool (such as a paper clip) to press and hold the button recessed inside the "Reset" hole on the back of the gateway.
2. Continue pressing the button for more than 5 seconds to restore factory settings. Note: pressing less than 5 seconds simply reboots the gateway.
3. Release the button and wait while the gateway reboots. The breathing LED turns off briefly, then blinks red until the boot sequence is complete, at which point it blinks green again.
4. You may then connect to the gateway using the default settings (and default IP address).

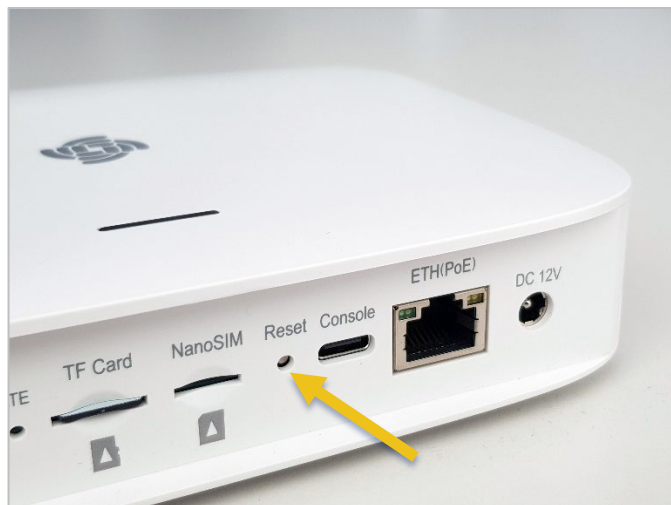


Figure 26 – Restoring gateway factory settings

I was making changes in my gateway's network configuration, and after a while the interface seemed unstable or unresponsive. What should I do?

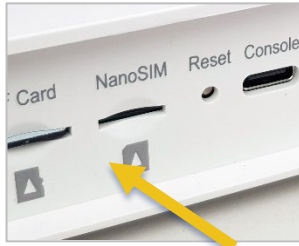
In rare cases, if you make a number of network changes successively using the gateway's administration interface (in particular with WAN Ethernet deactivated), the device can become unstable. If this occurs, you should press the Reset button (as shown in the above image) for about five seconds to perform a factory reset and then reconfigure the gateway.

Is it possible to have the gateway firmware updated automatically?

There is an automatic update feature when using DicksonOne (as described in section 3.3.3 – *Updating firmware automatically with DicksonOne*, p. 32). When using OCEAView, firmware updates must be performed manually using the administrator interface.

How do I insert the SIM card for my LTE connection?

Insert the SIM card into the slot on the back of the gateway marked "NanoSIM". The printed icon below the slot indicates the orientation of the SIM card.



Reboot the gateway for the SIM card to be taken into account.

Can I use the Dickson Connect gateway simultaneously for LoRa and as a Wi-Fi access point?

Yes, you can set up the LoRa gateway to also serve as a Wi-Fi access point to your network. See section 2.3.2 – *Using the gateway as a Wi-Fi access point*, p. 20.

4.2 LED indicators

LEDs	Status Indication Description
PWR LED	Power indicator - the LED is on when device power is on
Breathing LED	Indicates the current status of the gateway.
ETH LED	On: Uplink Off: Downlink Flicker: Data transmitting and receiving
LoRa LED	On: LoRa active Off: LoRa inactive Flicker: LoRa packet sending and receiving
WLAN LED	AP mode: - On: AP is up - Off: AP is down - Flicker: data sending and receiving STA Mode: - Slow flicker - Disconnected - On: connected - Flicker: data sending and receiving
LTE LED (functional only on models equipped with cellular data functionality)	Slow flicker (1800 ms high / 200 ms low): network searching Slow flicker (200 ms high / 1800 ms low): idle Fast flicker (125 ms high / 125 ms low): ongoing data transfer

5 Appendix – Certifications and compliance

Caution: Any changes or modifications made to this product not expressly approved in writing by Dickson could void the user's authority to operate the equipment.



United States – FCC statement

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operation: FCC Part 15 §107 - §109 - §207 - §247 (Ed 2008).

FCC RF Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.



Innovation, Science
and Economic
Development
Canada

Canada – ISED Statement

This device complies with ISED's license-exempt RSSs. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Le présent appareil est conforme aux CNR d'ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. Le dispositif ne doit pas produire de brouillage préjudiciable, et
 2. Ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.
-

Europe – Conformity with European regulations



This device is compliant with the essential requirements and other relevant requirements of the following directives.

- 2014/53/EU Radio Equipment Directive (RED)
- 2014/30/EU EMC Directive
- 2014/35/EU Low Voltage Directive
- 2011/65/EU Restriction of Hazardous Substances Directive



South Korea – KC certification

상호 또는 성명: Shenzhen Rakwireless Technology CO., Ltd

기자재명칭(제품명칭) : WisGate RAK7268C

제조사 : Shenzhen Rakwireless Technology CO., Ltd

등록번호 : R-R-SrT-RAK7268C



Australia – ACMA certification



New Zealand – R-NZ certification



China – CMIIT ID: 2021DP12529

DICKSON

Environmental Monitoring + Compliance Experts

Dickson North America
Addison, IL - USA

+1 (630) 543-3747
contact@dicksondata.com

Dickson Europe
Montpellier - France

+33 (0)4 99 13 67 30
contact@dicksondata.fr

Dickson Asia-Pacific
Petaling Jaya - Malaysia

+603 749 40758
contact@dicksondata.my

www.dicksondata.com