

X2000 Gateway – Plug-and-Play Instruction Manual



These instructions must be read thoroughly before installation or operation. This instruction manual was accurate at the time of printing.

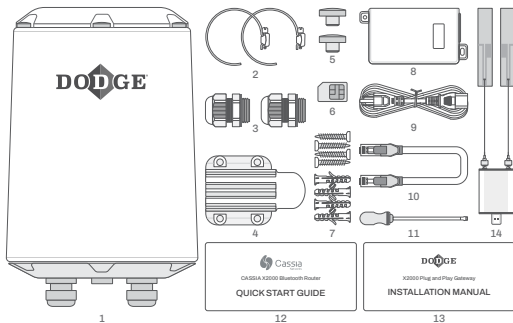
TABLE OF CONTENTS

- 1 GENERAL2**
- 2 INSTALLATION4**
 - 2.1 Prerequisites for installation4
 - 2.2 Recommended location 6
 - 2.3 Network and power connection summary 8
 - 2.4 Gateway configuration confirmation 9
- 3 TROUBLESHOOTING15**
- 4 SECURITY19**
 - 4.1 Enable HTTPS access19
 - 4.2 Password update requirements 25
 - 4.3 SSH access and redirect 25
- 5 OPTIFY™26**
- 6 SUPPORT27**

1 GENERAL

The X2000 Gateway – Plug-and-Play is used to upload Dodge® sensor data automatically to the OPTIFY platform. The gateway requires no configuration to communicate with OPTIFY as it supports connection to OPTIFY through a 4G mobile network with a preinstalled cellular USB dongle.

The package includes:



- | | | |
|----------------------------|------------------------------|--------------------------|
| 1.X2000 Router (1) | 2.Pole Mounting Straps (2) | 3.Cable Glands (2) |
| 4.Mounting Bracket (1) | 5.Extra Top Screw Covers (2) | 6.SIM Card (1) |
| 7.Anchor with Screws (2*4) | 8.PoE Injector (1) | 9.Power Cord (1) |
| 10.Ethernet Cable (1) | 11.Slotted Screwdriver (1) | 12.Quick Start Guide (1) |
| 13.Installation Manual (1) | 14.Modem with Antennas (1) | |

Figure 1 - Package contents

For more information about these components, refer to the quick start guide (see Figure 1). For general information about the gateway, please refer to the user manual at https://www.cassianetworks.com/download/docs/Cassia_User_Manual.pdf

2 INSTALLATION

2.1 Prerequisites for installation

Internet connection

The X2000 Gateway – Plug-and-Play connects to the internet via a preinstalled cellular USB dongle. Please ensure the gateway is installed in a location with adequate signal strength to reliably connect to a cellular network.

NOTE: OPTIFY is hosted in the United States (east coast) via Microsoft Azure Cloud Service.

- Access controller (global)
 - gw.dodgeoptify.com
- OPTIFY platform (global)
 - dodgeoptify.com
- OPTIFY Azure IoT Services (global)
 - dodge.azure-devices.net
 - global.azure-devices-provisioning.net
 - dodge-provisioning.azure-devices-provisioning.net

Power supply

- The gateway can be powered either via a Power over Ethernet (PoE) network or using a 12 V 2 A DC adapter
- For PoE, use the included PoE injector and Ethernet cable to power the gateway
- PoE is 802.3af/at compliant
- To power the gateway using a 12 V 2 A DC adapter, you will need to provide this adapter

Ethernet cable

- Cat5 or Cat6 Ethernet cable is needed to power the gateway when not using a 12 V 2 A DC power supply

Computer

- Computer with a Wi-Fi adapter is needed to verify the gateway is ready to communicate with the OPTIFY platform. A tablet or mobile phone can also be used.
- Google Chrome is the recommended web browser to use

USB cellular modem/dongle

- The gateway has a preinstalled USB cellular modem/dongle

Mounting

- A flat-head screwdriver can be used for pole mounting
- A Phillips-head screwdriver and a drill (optional if needed) can be used for wall mounting
- Mounting the gateway is not mandatory but is recommended so the unit is secured in its intended location

2.2 Recommended location

Height

- The recommended mounting height for the gateway is 10 ft (3 m)—100 ft (30 m) from ground level. Mounting at a lower height is possible but may reduce the connection range.

Orientation

- The gateway has the best reception in the direction where the Dodge logo is located on the side of its case. If the gateway has trouble connecting to a specific sensor, it is recommended to rotate the gateway to point in that direction.

Grounding

- If installing the gateway outdoors, install a grounding cable to the bottom of the gateway as shown in Figure 2.

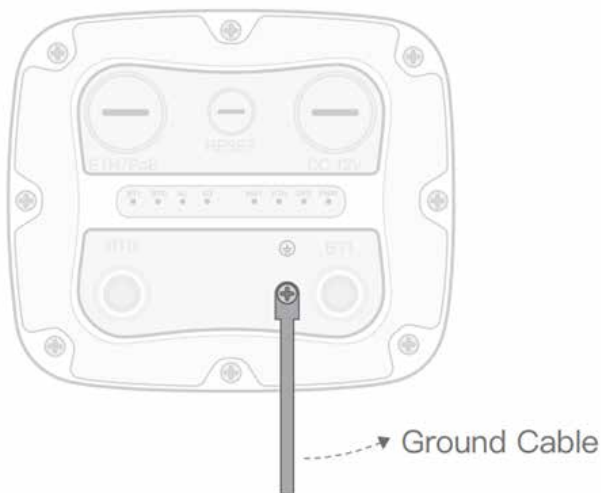


Figure 2 - Grounding cable location

2.3 Network and power connection summary

The gateway includes a USB mobile dongle with a SIM card for connection to cellular networks. Power the gateway using the provided PoE injector and Ethernet cable as shown in Figure 3. Alternatively, a 12 V 2 A adapter can be used to power the gateway as shown in Figure 4.

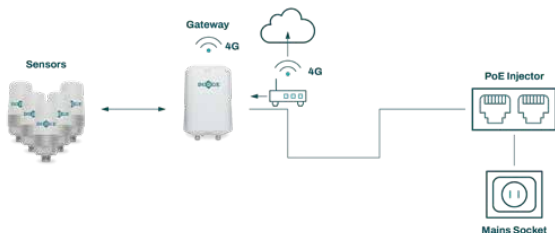


Figure 3 - Mobile network power configuration

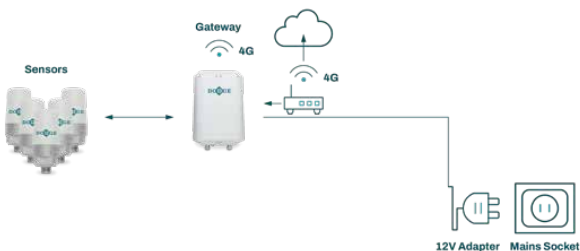


Figure 4 - Mobile network power configuration with 12 V adapter

2.4 Gateway configuration confirmation

When the gateway is powered on, the power LED at the bottom of the gateway will turn green. The bootup takes about 30—60 seconds.

After bootup, the gateway will turn on its Wi-Fi hotspot. Connect to the Wi-Fi hotspot to change configuration settings (e.g., computer, mobile phone, or tablet).

The Wi-Fi hotspot connection's SSID, or name, will be “cassia-XXXXXX”, where the last 6 characters will match the last 6 characters of the gateway's MAC address. The MAC address can be found on the bottom of the gateway.

The password for the Wi-Fi hotspot connection will be the same as the SSID. Once your device is connected to the gateway's Wi-Fi hotspot connection, open an internet browser. Type 192.168.40.1 in the address field, then press enter. The configuration login page will open (see Figure 5).

The default password will need to be changed after the first login. When prompted, create a new password. The default credentials are:

- Username: admin
- Password: admin

! **NOTE:** the new password should include a combination of numbers, letters, and special characters and must be between 8—20 characters in length. Take note of password for future use.

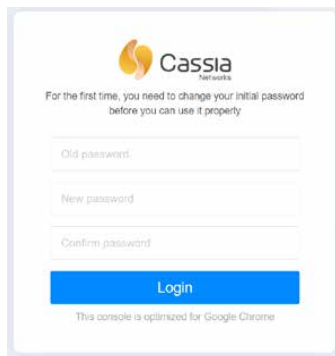
The image shows a web browser window displaying the Cassia Networks login page. At the top center is the Cassia Networks logo, which consists of a stylized orange 'C' icon followed by the text 'Cassia Networks'. Below the logo, a message reads: 'For the first time, you need to change your initial password before you can use it properly'. There are three input fields stacked vertically: 'Old password', 'New password', and 'Confirm password'. Below these fields is a prominent blue button with the text 'Login' in white. At the very bottom of the page, a small note states: 'This console is optimized for Google Chrome'.

Figure 5 - Login page

Once logged in, the status page (Figure 6) is shown to display the current operating mode and connection status of the gateway. The AC Online Time shows how long the gateway has been connected to the AC server. If no time is shown, it means the gateway does not have a connection to the AC server. Connection to the AC server is required for the transfer of sensor data.

Status	Basic	Container	Events	Other
Model	X2000			
MAC	CC:1B:E0:E2:58:AC			
Working Mode	AC Managed			
AC-Gateway Protocol	MQTT			
Uplink	Cellular			
Uplink Signal Strength	GOOD			
ETH IP	10.85.13.161			
WLAN IP	192.168.40.1			
Cellular IP	10.82.85.70			
Country/Region	United States			
Firmware Version	2.1.1.2207292108			
Up Time	147hrs 19min 54sec			
AC Online Time	147hrs 18min 59sec			
Chip0	Active Scan			
Chip1	Idle			
CPU Usage	11.74%			
Memory Usage	20.99%			
Storage Usage	19.47MB / 111.20MB			

Figure 6 - Status page with access controller connection

The Basic page, as shown in Figure 8, is where the configuration is managed. The following values on the Basic page are common for all X2000 Plug-and-Play gateways, regardless of mobile network:

- Gateway name: Not required but recommended

Do not make any changes to the following values:

- Gateway mode: AC Managed Gateway
- Tx power: 19
- External antenna: None
- Statistics report interval: 5 Minutes
- AC server address: gw.dodgeoptify.com
- AC-Gateway protocol priority: MQTT
- Connection priority: Cellular
- Enable OAuth2 Token for Local API: Off
- Remote assistance: On

For security reasons, we recommend that you change the gateway Wi-Fi password. This can be done under the Wi-Fi section. Please make note of the new password.

You can also change the SSID (name of the Wi-Fi hotspot of the gateway) if desired.

Wi-Fi

Operating Mode

Hotspot(Setup Only) ▼

SSID

cassia-E24754

Password

IP

192.168.40.1

Netmask

255.255.255.0

Figure 7 - Changing the Wi-Fi hotspot password

NOTE: If you forget your login credentials or make a mistake while configuring the Wi-Fi network's SSID or password, please contact Dodge support using the information at the end of this document.

NOTE: Do not make any changes the Cellular Modem section shown in Figure 8.

Status

Basic

Container

Events

Other

Gateway Name

Gateway Name

Gateway Mode

AC Managed Gateway

Tx Power

18

External Antenna

None

Statistics Report Interval

3 Minutes

AC Server Address

gw.digiparty.com

AC Gateway Protocol Priority

HTTP

Connection Priority

Cellular

Enable OAuth2 Token For Local API

Off

Remote Assistance

On

Wired

IP Allocation

DHCP

DNS1

DNS2

Wi-Fi

Operating Mode

Hotspot(Setup Only)

SSID

3883A-6-25AC

Password

IP

192.168.40.1

Netmask

255.255.255.0

Cellular Modem

USB Modem Type

None

Apply

Cassia

Figure 8 - Basic page

3 TROUBLESHOOTING

If the AC Online Time is not shown within a few minutes:

- Check the configuration and internet connection
- Be sure that the gateway mode is set to “AC Managed Gateway” on the basic page
- Reboot the gateway by powering it off, then on

Connection to the internet can be verified with debug tools on the Other page:

- Under debug tools, select “ping”
- For the address type a known web address, such as “google.com”
- Select “5s” then click “Start”
- A success message will appear if the gateway is connected to the internet

If the gateway does not generate the Wi-Fi hotspot for setup:

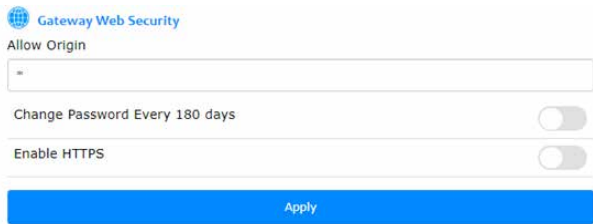
- Check the power supply and verify the green LEDs on the bottom of the gateway are on

Scanning for Bluetooth devices

The correct gateway placement can be checked by scanning for Bluetooth devices within the gateway’s range. The gateway’s location or orientation might need to be changed if all desired sensors are not visible for the gateway or if the sensors are showing weak signal levels.

To enable scanning, the router's mode on the basic page needs to be changed from "AC Managed Gateway" to "Standalone Gateway". Once changed, the gateway will automatically reboot and will be operational again in 30—60 seconds.

In addition, you must type an asterisk (*) in the "Allow Origin" field under "Gateway Web Security" on the Other page. Click apply to save this change.



Gateway Web Security

Allow Origin

Change Password Every 180 days

Enable HTTPS

Apply

Figure 9 - Gateway web security on the Other page

Open the following web page on a Wi-Fi enabled computer using Google Chrome: <http://www.bluetooth.tech/debugger/>

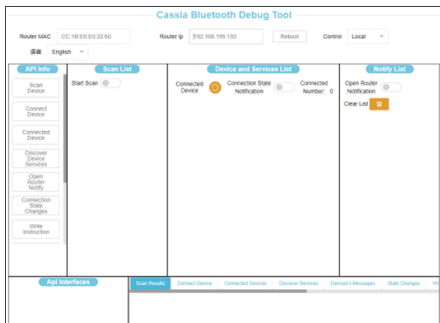


Figure 10 - Gateway Bluetooth debug tool

Once the debug tool is loaded, connect your computer to the Wi-Fi network generated by the gateway.

Type in the gateway's MAC address into the Router MAC field and the IP address (192.168.40.1) into the Router IP field.

Press “start scan”.

The debug tool will start to list all Bluetooth devices within range. For all scanned devices, the tool shows the MAC address and the RSSI value. Sometimes the name is not available, but it is listed if known.

If the debugger is not displaying any Bluetooth devices after starting the scan, please refer to the debugger troubleshooting guide available here: bluetooth.tech/debugger2/dist/Debugger2-Troubleshooting.pdf

RSSI values can be generally categorized into the following groups:

- RSSI value between 0 and -70: good
- RSSI value between -70 and -80: weak (the sensor data might be read periodically)
- RSSI value -80 or less: poor (most of the time the sensor cannot be read)

If the desired sensors are showing RSSI values of -70 or less, adjusting the gateway's location or orientation is recommended.

! **NOTE:** Remember to change the gateway mode back to AC Managed Gateway. If this mode is not changed, the gateway will not establish the connection to the AC server and the sensor data is not being read.

4 SECURITY

4.1 Enable HTTPS access

The gateways allows users to configure an SSL certificate (https) for accessing the gateway through an encrypted channel.

The SSL certificate and key will be delivered in the privacy enhanced mail (PEM) format, or a certificate signed by an internal public key infrastructure (PKI) can be used. An example of how to create and import a self-signed certificate is outlined below.

Certificate generation

A certificate can be created with the OpenSSL tool and the example shows creating the certificate with Ubuntu 22.01.2 WSL system using the built-in tool.

The tool uses command line interface (CLI) with appropriate arguments. Use the following command to generate a certificate:

- `openssl -req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out gateway.crt -keyout private.key`

The command generates two files:

- `gateway.crt` (public certificate with a public key)
- `gateway.key` (private key for the certificate)

The following arguments are specified:

- Cryptographic algorithm: rsa
- Key length: 4096
- Type of certificate: x509
- Type of certificate signature: sha256
- Validity period: 365 days

You will also be prompted to provide additional data such as country name, location, and other information. The data will be included in your certificate but only the Common Name is required. The Common Name may be the IP address or DNS name if the DNS name is used to resolve and assign an appropriate name for the gateway.

Example data

- Country Name (2 letter code) [AU]:PL
- State or Province Name (full name) [Some-State]: Masovian
- Locality Name (eg, city) []: Warsaw
- Organization Name (eg, company) [Internet Widgits Pty Ltd]: Dodge OPTIFY Security
- Organizational Unit Name (eg, section) []: OPTIFY Platform
- Common Name (e.g. server FQDN or YOUR name) []: 192.168.192.53
- Email Address []: security@dodgeoptify.com

```
ubuntu@dodgeptify:~$ openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out gateway.crt -keyout private.key
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
if you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Masovian
Locality Name (eg, city) []:Warsaw
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Dodge OPTIFY Security
Organizational Unit Name (eg, section) []:OPTIFY Platform
Common Name (e.g. server FQDN or YOUR name) []:192.168.192.53
Email Address []:security@dodgeoptify.com
ubuntu@dodgeptify:~$
```


**Figure 11 - Additional information for
HTTPS security certificate**

 gateway.crt Type: Security Certificate	Date modified: 3/1/2023 8:28 AM Size: 2.11 KB
 private.key Type: KEY File	Date modified: 3/1/2023 8:28 AM Size: 3.10 KB

Figure 12 - Generated files for HTTPS security certificate

The generated files can be uploaded on the Other page:

- Under the Gateway Web Security section, turn on Enable HTTPS and two new buttons should appear
- Upload the certificate and key files to the appropriate areas
- Click “Apply”

 Gateway Web Security

Allow Origin

Change Password Every 180 days ☐

Enable HTTPS ☒

SSL Private Key (*.key)
 private.key

SSL Certificate (*.crt)
 gateway.crt

Figure 13 - Gateway web security section to enable HTTPS

You will be reconnected to a secure connection (HTTPS).

NOTE: If a self-signed certificate is used, your browser will display a message stating the connection is not private or trusted but this is not an issue.

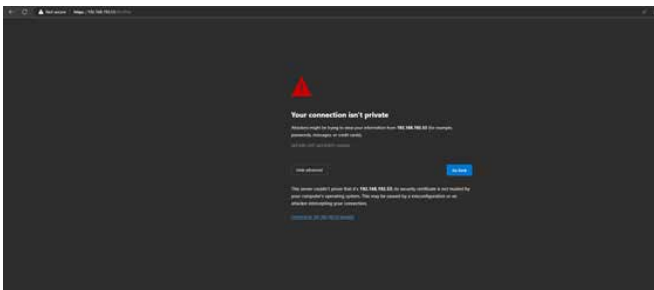


Figure 14 - Verifying the certificate

To verify your self-signed certificate, click on “Not secure” in the browser address bar and confirm the certificate.

! **NOTE:** The process of approving a self-signed certificate may depend on the specific browser used.

The data presented should match your certificate data. Advanced users can also verify the fingerprint as needed for their security requirements.

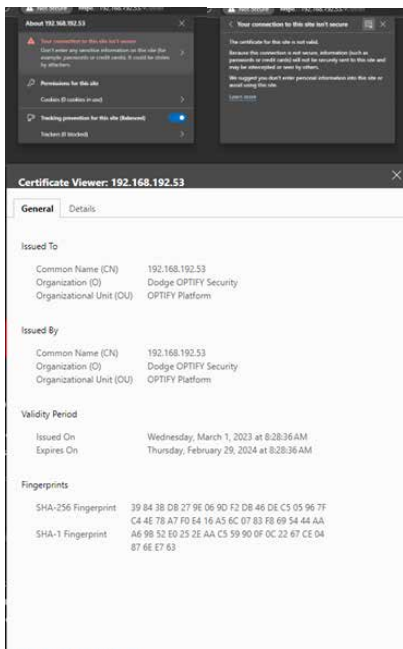


Figure 15 - Certificate data

After completing SSL (HTTPS) setup, you should use the address, <https://<gateway address>>, when connecting to the gateway as an address leading with “http” will not work.

4.2 Enable administrator password update requirements

If needed, you can require the administrator password for the management panel to be updated every 180 days. To enable this feature, go to the Other page:

- In the Gateway Web Security section, toggle the button for “change password every 180 days”

Gateway Web Security

Allow Origin

Change Password Every 180 days

Enable HTTPS

SSL Private Key (*.key)

Select File private.key

SSL Certificate (*.crt)

Select File gateway.crt

Apply

Figure 16 - Gateway web security section to enable password change requirements

4.3 SSH access and redirect

The gateway can allow SS access locally and from the cloud. This access is only to be used by Dodge employees for troubleshooting reasons and you should not enable this feature.

5 OPTIFY

After a gateway is configured and online, it will need to be commissioned in the OPTIFY platform to read data from sensors. Once a gateway is commissioned, sensors must be assigned to it within OPTIFY as a gateway will only read data from assigned sensors.

Commissioning a gateway in OPTIFY can be done using the OPTIFY web portal or mobile app. The web portal is available at dodgeoptify.com. The mobile app is available on the App Store for iOS devices and the Google Play Store for Android devices.

To learn how to commission a gateway and assign sensors in OPTIFY through the web portal or mobile app, follow the appropriate QR code below to the instructions.

Commission a gateway



Manually assign a sensor



Automatically assign a sensor



6 SUPPORT

For additional support, please contact the Dodge IIoT Technologies team:

- Email: engineering@support.dodgeindustrial.com
- Phone: +1 864 284 5700 ext. 6
- Availability: Monday—Friday, 8 am—5 pm EST

Scan for the latest digital instructions:



Dodge Industrial, Inc.
1061 Holland Road
Simpsonville, SC 29681
+1 864 297 4800

