

# X2000 Gateway – Standard 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	GE	NERAL	2
2	INS	TALLATION	3
	2.1	Prerequisites for installation	4
	2.2	Recommended location	9
	2.3	Gateway configuration	11
	2.4	PoE connection	17
	2.5	LAN/ethernet cable connection	18
	2.6	Wi-Fi connection	20
	2.7	USB mobile dongle connection	22
	2.8	Firewall configuration	
	2.9	Verifying the configuration	25
3	TRO	OUBLESHOOTING	26
4	SEC	CURITY CONSIDERATIONS	32
	4.1	Enable HTTPS access	32
	4.2	Password update requirements	
	4.3	SSH access and redirect	38
5	OP	TIFY <sup>™</sup>	39
6	SUI	PPORT	
-			

# 1 GENERAL

The X2000 Gateway (part number 749972) is used to automatically upload Dodge<sup>®</sup> sensor data to the OPTIFY platform. For the gateway to communicate with OPTIFY, it needs to be configured for internet access. The following internet connections are supported:

- Local Area Network (LAN)/EtherNet network together with a
   Power over Ethernet (PoE) injector
- 2.4 GHz/5 GHz Wi-Fi network
- 4G mobile network with a specific USB dongle

#### The package includes:



## 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

cassianetworks.com/download/docs/Cassia\_User\_Manual.pdf

# 2 INSTALLATION

# 2.1 Prerequisites for installation

#### Internet connection

- The default DNS server address is the Google DNS server for global customers (8.8.8.8)
- If a firewall is used, the following ports need to be opened:

URL	Port type	Port number	Gateway communication partner	Service details
gw.dodgeoptify.com	тср	8883	Access Controller (AC)	MQTT for Cassia Access Controller
gw.dodgeoptify.com	ТСР	9999	Access Controller (AC)	SSH port to provide troubleshooting services for gateways
gw.dodgeoptify.com	TCP/ HTTP	80	Access Controller (AC)	HTTP service for gateway software and firmware updates
gw.dodgeoptify.com	TCP/ HTTPS	443	Access Controller (AC)	HTTPS service for gateway software and firmware updates
global.azure-devices- provisioning.net	ТСР	8883	Azure IoT Device Provisioning Service	MQTT for gateway provisioning application
dodge.azure-devices.net	ТСР	8883	Azure IoT Hub	MQTT communication between AC and router
api.dodgeoptify.com	TCP/ HTTPS	443	OPTIFY Platform	HTTPS for OPTIFY API
dodge-provisioning. azure-devices- provisioning.net	ТСР	8883	Azure IoT Device Provisioning Service	MQTT for gateway provisioning application
Customer DNS URL	TCP/ UDP	53	DNS Server	DNS lookup for AC address (optional if specified in gateway network configuration)

**NOTE:** The above table is from the gateway's perspective. All communication is out of the gateway to the communication partner.

**NOTE:** Check to confirm there are no TLS splitting solutions on the way (certificate switching) or TLS blocking for the gateway.

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

Access controller (global)

I

- gw.dodgeoptify.com
- OPTIFY platform (global)
  - dodgeoptify.com
- The mobile network needs to have adequate signal strength. In demanding locations, a USB extension cable or external antenna might be needed for the USB modem/dongle.
- OPTIFY Azure IoT Services (global)
  - dodge.azure-devices.net
  - global.azure-devices-provisioning.net
  - dodge-provisioning.azure-devices-provisioning.net

#### **Power supply**

- In case the PoE network is not available, a PoE injector is needed for the power supply
- PoE is 802.3af/at compliant
- The gateway can also be powered with a 12 V 2 A DC power supply

#### Ethernet cable

• The following table outlines the number of Ethernet cables required in different X2000 configurations

Power source	Connection method	<b>Required Ethernet cables</b>	
PoE network	PoE network	1	
PoE injector	LAN/Ethernet network	2	
PoE injector	Wi-Fi	1	
PoE injector	Cellular modem	1	
12 V 2 A DC adapter	LAN/Ethernet network	1	
12 V 2 A DC adapter	Wi-Fi	0	
12 V 2 A DC adapter	Cellular modem	0	

#### Computer

- Computer with a Wi-Fi adapter is needed to configure the gateway. 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 bult-in drivers for several USB dongles. For the list of supported dongles, please check the USB mobile dongle connection section.
- A SIM card with an internet data plan
- The gateway also supports the use of any USB-powered
  Wi-Fi modem

#### 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 to secure the unit 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, be sure to install a grounding cable to the bottom of the gateway as shown Figure 2.



## Figure 2 - Grounding cable location

# 2.3 Gateway configuration

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 configuration. Connect to the Wi-Fi hotspot with the device used for configuration (e.g., computer, mobile phone, or tablet).

The Wi-Fi connection's SSID, or name, will be "cassia-XXXXXX" where the last 6 digits will match the last 6 digits of the gateway's MAC address. The MAC address can be found on the bottom of the gateway. The password for the Wi-Fi connection will be the same as the SSID.

Once your device is connected to the gateway's Wi-Fi hotspot, open an internet browser. Type 192.168.40.1 in the address field, then press enter. The Cassia configuration page will open.

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.

or the first lim	Networks
t	pefore you can use it property
Old puersw	ord
New pass	word
	eseword
	Login

## Figure 3 - Cassia login page

Once logged in, the status page is shown to display the current operation 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:18:	E0:E2:58:AC
Working Mode			AC Managed
AC-Gateway Protocol			MQTT
Uplink			Cellular
Uplink Signal Strength			GOOD
ETH IP			0.85.13.161
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		19.47ME	3/111.20MB

## Figure 4 - Status page

The Basic page is where the configuration is managed. The following values are common for all network configurations (PoE, LAN, Wi-Fi, and Mobile):

- Gateway name: Not required but recommended
- 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: See below
- Enable OAuth2 Token for Local API: Off
- Remote assistance: On

Connection priority is where a prioritized connection method is selected in case there are several in use. Select the priority according to the connection in use:

- Wired for PoE and LAN connections
- Wireless for a Wi-Fi connection
- 3G/4G for a mobile USB dongle connection

For security reasons, we recommend that you change the gateway Wi-Fi password for wired or 3G/4G connections. 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 5 - Changing the Wi-Fi hotspot password

Analysis     Analysis       Analysis     A	Status Basic	Container	Events	Other
And and a mone of the ansate o				0.014
Sance in and Sance in a second	Decemby Martie			
Advances of the set of	Contrast de la			
No. No. Sector     Image: Sector       No. No. Sector     Image: Sector       Sector     Sector       Sector <td< td=""><td>Sacranty Mode</td><td></td><td></td><td></td></td<>	Sacranty Mode			
b and a set of a set	AC Ranapat Galavay			
III and a second	ta Power			
Sine        Sine <td>19</td> <td></td> <td></td> <td></td>	19			
tone            tone            Shate            Shate       <	External Anterna			
Sensition         web           C Sarow (Control of Sensition Control of Sens	None			
	Ratistics Report Interval			
C Astrone Accordence C Astrone Accordence C calculary in Protocial Francis C calculary in Protocial Francis C calculary in Protocial Francis C calculary in Protocial Area C calculary C	5 Minutes			
pic dagatakanan (catalanak mataka famatakanan mitit catalanak mataka famatakanan catalanak matakanan catalanak matakanan catalanakanan catalanak matak	IC Server Address			
ic datasy frated franky ic datasy frated franky ic datasy frated franky ic datasy frated franky ic datasy frated fra Lead M1 ic datasy ic datasy frated fra Lead M1 ic datasy ic datasy frated	gri 4odgeoptify.com			
Indite Analysis of the analysi	sc Gateway Protocol Priorit	<b>v</b> .)		
andetten frestrik Gene Gene Gene Gene Gene Gene Gene Gen	110177			14
induis of the second of the se	Jannection Phonity			
Inde Califord Tools for (and Mf Cir Cir Cir Cir Cir Cir Cir Cir	Ohlar			. e
an or	Enable OAuth2 Token For Lo	cal APE		
innut Autoor Other and Autoor Autocom	ONA			19
os	Remote Assistance			
	05			
	0459			
Docatory (Mode Status	🚔 win			
	Doerating Mode			
SSD SSD Sanactine : Sanactine	Hittpot(Tetup Oilly)			
IBBAR DINC : IBBAR DINC : IB	SSID			
Venesori d Venesori d Veneso	03832-6255AC			
With the second secon	Pasaword			
a States 48 A States 48 A States 51 A B Collume Modern Type States 51 A States				
102.05.05.05.1 before A Statistic Statist Children Hype Rose v	2			
Network	192.556.40.1			
ensole ania de Robert Type Robert Type Ver	leştmaşk:			
i colure Hoden dd Hoden Type Now v	255.255.255.4			
d8 Hoden Type filme ↓	Called at Modern			
litos 🗸	uš8 Modem Type			
	ficoe			.*
		ALC: NO	_	-

## Figure 6 - Basic page

# 2.4 PoE connection

If a PoE network is available, the gateway can be configured for use without any additional power supply.



## Figure 7 - PoE network configuration

**NOTE:** For more information about the figure components, please refer to the quick start guide.

From the Basic page, select:

- Connection Priority: wired
- IP Allocation: DHCP or static (in case the IP allocation is given)

Press "Apply" at the bottom of the screen.

# 2.5 LAN/Ethernet cable connection

If a LAN/Ethernet network is available, the gateway can be configured for use with a PoE injector as the power supply. Alternatively, a 12 V—2 A adapter can be used to power the gateway.



## Figure 8 - LAN network configuration



## Figure 9 - 12 V LAN network configuration

**NOTE:** For more information about the figure components, please refer to the quick start guide.

From the Basic page, select:

- Connection Priority: wired
- IP Allocation: DHCP or static (in case the IP allocation is given)

Press "Apply" at the bottom of the screen.

# 2.6 Wi-Fi connection

The gateway can be configured to use an existing Wi-Fi network with a PoE injector as the power supply. If using a PoE injector, make sure the Ethernet cable is connected to the PoE port of the injector. Alternatively, a 12 V—2 A adapter can be used to power the gateway.



Figure 10 - Wi-Fi network configuration



Figure 11 - Wi-Fi network configuration with 12 V adapter

From the Basic page, select:

- Connection Priority: Wireless
- Enter the Wi-Fi network SSID (name)
- Enter the Wi-Fi network password
- Under Wi-Fi, change Operating Mode from "Hotspot" to "Client"
- IP Allocation: DHCP or Static (in case the IP allocation is given)

Press apply at the bottom of the screen.

NOTE: Once the apply button is pressed, the gateway Wi-Fi adapter stops sharing the Wi-Fi hotspot and changes the connection to the configured Wi-Fi network. In case the DHCP is used, the gateway now has a new IP address. The new IP address is needed to reconnect to the gateway (e.g., to check the Status page or scan the devices within the gateway's range). Your local IT department can find the gateway's IP address by accessing the Wi-Fi router device list or by performing a network scan for IP addresses. In the case of a static IP being used, the address is known.

**NOTE:** Connect your computer, tablet, or mobile phone to the same Wi-Fi network the gateway is connected to. Open your web browser and type the new IP address into the address field, then press enter. Access to the gateway configuration pages is established again.

**NOTE:** If there was an error in the SSID, password, or IP address configurations, you cannot access the gateway anymore. In this case, the gateway isn't shown in the Wi-Fi router device list or a network scan. To resolve, press and hold the reset button on the bottom of the gateway for 10—15 seconds to reset the gateway back to factory default values.

## 2.7 USB mobile dongle connection

A mobile network can be used with a specific USB dongle. In addition, a PoE injector (power supply), a supported USB dongle, and a SIM card are needed. Alternatively, a 12 V—2 A adapter can be used to power the gateway.



## Figure 12 - Mobile network configuration



## Figure 13 - Mobile network connection with 12 V adapter

Insert the USB dongle with the SIM card into the USB port at the top of the gateway. The PIN query needs to be disabled from the SIM card.

From the Basic page, select:

- Connection Priority: Cellular
- USB dongle type: Select the correct dongle type being used
- Type the access point name (APN) the SIM card's carrier is using
- Type the username and password for the APN if needed

Press apply at the bottom of the screen, then reboot the gateway by removing the power supply for a few seconds and reconnecting it.

**NOTE:** With a USB dongle, the gateway needs to be in a location with good network coverage. If the signal strength is weak, a USB extension cable or additional external antenna for the USB dongle might be needed. **NOTE:** If a Wi-Fi modem is used, connect the modem to the USB port on the top of the gateway, then follow the instructions under section 2.6 Wi-Fi connection.

**NOTE:** For supported USB dongle modems, please consult Cassia's user manual. Please note that some countries might have regulations that forbid the use of certain types of hardware providers (i.e., check if Huawei can be used in the United States).

# 2.8 Firewall configuration

If there is a firewall in the network the gateway is using, specific ports needed to be opened.



## Figure 14 - Firewall configuration



**NOTE:** The firewall should allow communication between the gateway and the access controller as well as the gateway and the OPTIFY platform respectively. If needed, refer to the required ports in section 2.1

# 2.9 Verifying the configuration

Once the configuration is done, it can be verified from the Status page. When the connection is established to the access controller, the AC Online Time will show.

Model	x200
MAC	CC:18:09:02:47:0
Working Mode	AC Manager
AC-Gateway Protocol	мал
Uplink	We-P
Uplink Signal Strength	0.000
ETH IP	192.168.1.19
WLAN SP	192.168.1.19
Cellular IP	
Country/Region	United State
Firmware Version	2.1.1.220729210
Up Time	10min 1se
AC Online Time	1266
CNUD	Active Scan
Chip1	lide
CPU Usage	25.189
Hemory Usage	11.919
Storage Usage	3.21M8 / 111.20M

## Figure 15 - Gateway connected to gw.dodgeoptify.com

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

- Check the configuration and internet connection
- Reboot the gateway by powering it off, then on

# **3 TROUBLESHOOTING**

# If you forget your login credentials or make a mistake while configuring the Wi-Fi networks's SSID or password:

- Press and hold the reset button on the bottom of the gateway for 10—15 seconds to reset the gateway back to factory default values. This button is located under a cap labeled "reset".
- This will require reconfiguring the gateway to communicate with the access controller

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

- Check the power supply and verify the green LED on the bottom of the gateway is on
- If the gateway is configured to use a Wi-Fi network, it does not generate a Wi-Fi hotspot
- Press and hold the reset button on the bottom of the gateway for 10—15 seconds to reset the gateway back to factory default values

#### If the gateway does not connect to the AC server:

- Check access to the internet
- If a USB dongle is used, check if the model is supported by the gateway and that the dongle has established a connection to a mobile network
- Check the firewall settings for the network being used to ensure the necessary ports for outbound communication are open (refer to the Prerequisites for installation section)
- Check to confirm there are no TLS splitting solutions on the way (certificate switching) or TLS blocking for the gateway

Connection to access controller can also be verified with debug tools on the other page:

- Under debug tools, select "NetCat"
- For Address type "gw.dodgeoptify.com"
- For Protocol select "TCP"
- For Timeout select "5s"
- For Port enter "8883"
- Press start
- A success message will appear if the entered port is open for communication

NetCat	~
Address	
gw.dodgeoptify.com	
Protocol	
TCP	~
fimeout(Second)	
3	~
Port	
8083	
Start	

## Figure 16 - Gateway debug tools on the other page

NOTE: NetCat can also be used to check ports 9999, 80, and 443.

**NOTE:** The inverse host lookup will fail, this is not an indication of whether the port is open.

#### 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 17 - Gateway web security section on the other page

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

		Cassia	Bluetooth	Debug Tool			
Router MAC	CC:18:E0:E0:22:60	Router Ip	192.168.199.150	Reboo	Contro	ol Local ~	
57 M E	nglish 👻						
API Info	Scan Li	st.	Device	and Services List		No	lify List
Scan Device	Start Scan	Con	nected O Con Ivice N	inection State	Connected Number: 0	Open Router Notification	•
Connect Device						Clear List 👕	
Connected Device							
Discover Device Services							
Open Router Notify							
Connection State Changes							
White Instruction							
Ap	i Interfaces	Scan Results Con	nect Device Conne	cted Devices Discover	Services Dev	rices's Messages	State Changes W

Figure 18 - Gateway Bluetooth debug tool

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

**NOTE:** For gateways configured to a Wi-Fi network, connect your computer to the same Wi-Fi network as 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.

**NOTE:** For gateways configured to a Wi-Fi network, type the new IP address into the field. For more information, refer to the Wi-Fi connection section in the manual.

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

I

- 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 CONSIDERATIONS**

# 4.1 Enable HTTPS access

Cassia gateways allow 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 of 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

abantadioSpecify-5 openal req -em -emery release -1500 -1525 -days 355 -oodes out gatemay.ct keyout private key 	University × + +
You are about to be asked to enter information that will be incorporated info your certificate request. What you are about to enter in what is called a Distinguished Name or a DN. There are quite a few fields buy our cal leave some blank For some fields there will be a default value, if you enter '', the field will be be fet blank. Contry Name (2 letter code) [AU]:PL State or Province Name (Coll mano) [Some-State]:Nasovin State or Province Name (Coll mano) [Some-State]:Nasovin State or Province Name (Coll mano) [Some-State]:Nasovin	abathéédésetify:-5 opensil ma -man -manény ma:4098 -1599 -hb256 -days 365 -nodes -out patemay.crt keyest private key
Organizational Unit Name (eg. Section) []007fFy Platform Genema Name (eg. server FROM en vOM name) []192.166.192.53 Email Address []recurityHedgeorify.com AuncHedgeoryFify]	Yea are about to be asked to enter information that will be incorporated into your certificate request. Must you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields both you can leave some Blank For some fields there will be a default value, if you enter '.', the field will be left blank. Exantry Name (2) Letter code) [AU]:PL State or Province Name (full name) [Some-State]:Masovian Locality Name (eq, campa) [Internet Widgits Pty Ltd]:Dodge OPTIFY Security Organization Name (eq, server FORM or YORT may Distribute State) Organization Name (eq, server FORM or YORT may Distribute State) Organization Name (eq, server FORM or YORT may Distribute State) Organization Name (eq, server FORM or YORT may Distribute State) Distribute State State) [J:192.106.192.53 What hyddodgeoptify:ce

## Figure 19 - Additional information for HTTPS security certificate



## Figure 20 - 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 S Allow Origin	Security		
Enable HTTPS	Every 180 days		
SSL Private Key (*	.key)		
Select File	private.key		
SSL Certificate (*.o	crt)		
Select File	gateway.crt		
		Apply	

## Figure 21 - 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 22 - 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.

Annuel 2012 Mar 2012 SA 2012 SA     Annuel 2014 SA 2014 SA     Annuel 2014 SA 2014 SA 2014 SA     Annuel 2014 SA	All	<ul> <li>Construction and the close of source of the close of</li></ul>	
C			
General Details	2.196.192.33		
Issued To			
Common Name (CN) Organization (O) Organizational Unit (O	192.168.192.53 Dodge OPTIFY OPTIFY Platfor	Security	
Issued By			
Common Name (CN) Organization (O) Organizational Unit (O	192.168.192.53 Dodge OPTIFY U) OPTIFY Platfor	Security m	
Validity Period			
Issued On Expires On	Wednesday, M Thursday, Febr	arch 1, 2023 at 8:28:36 AM uary 29, 2024 at 8:28:36 AM	
Fingerprints			
SHA-256 Fingerprint	39 84 38 D8 27 9E C4 4E 78 A7 F0 E4 A6 98 52 E0 25 2E A 87 6E E7 63	56 90 E2 00 440 DE C5 05 99 7F 16 55 EC 07 81 86 95 54 44 AA 14 C5 59 90 0F 0C 22 67 CE 04	

## Figure 23 - Certificate data

After completing SSL (HTTPS) setup, you must 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 S	ecurity		
Change Password	Every 180 days		
Enable HTTPS			
SSL Private Key (*.	key)		
Select File	private.key		
SSL Certificate (*.c	rt)		
Select File	gateway.crt		
		Apply	

## Figure 24 - Gateway web security section to enable password change requirements

# 4.3 SSH access and redirect

The gateway can allow SSH 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**



#### Automatically assign a sensor



#### Manually 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



© DODGE INDUSTRIAL, INC. AN RBC BEARINGS COMPANY All Rights Reserved. Printed in USA. MN7004 REV- 05/24