

InfinID Technologies, Inc.

V-Tag Gateway Setup VG200-1

November 14, 2022

Table of Contents

1.0 Gateway Overview.....	3
1.1 Introduction.....	3
1.2 Standard V-Tags	3
1.3 Beacon V-Tags.....	4
2.0 Power and LED Indicators.....	5
2.1 Power	5
2.2 LED Indicators.....	5
2.3 Gateway Configuration Mode.....	5
2.4 Gateway Factory Reset	5
3.0 Additional Gateway Features.....	6
3.1 Two-way cloud communication	6
3.2 Gateway Web Server	6
3.3 Automatic firmware updates.....	6
3.4 Gateway IP Address Discovery	7
3.5 Gateway Security Mode.....	7
4.0 Gateway Configuration using AssetWorx! App.....	8
5.0 Gateway Configuration using V-Tag Gateway Setup App.....	15
6.0 Uploading Client Certificates	22

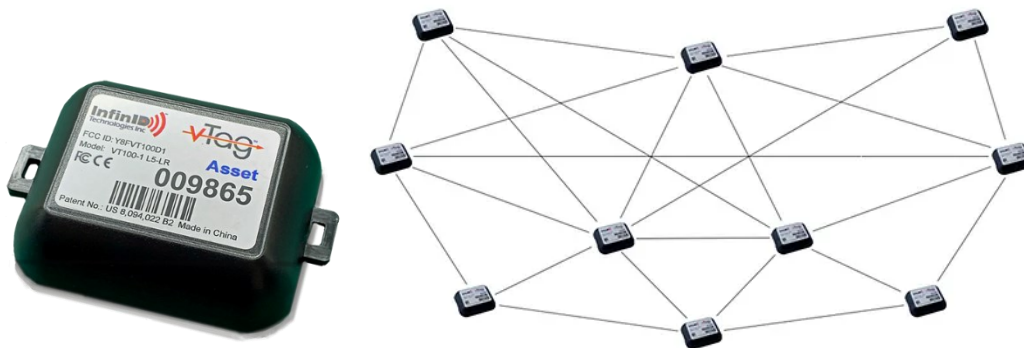
1.0 Gateway Overview

1.1 Introduction

The VG200-1 gateway is used to receive messages from standard V-Tags or beacon V-Tags and push those messages to a server in the cloud or to a local server.



1.2 Standard V-Tags



Standard V-Tags create a mesh network for relaying messages. A movement message may be relayed from an asset tag through a network of fixed tags to a listening gateway. The fixed tags also serve as reference points for locations.

1.3 Beacon V-Tags

An example of a beacon V-Tag is shown below:



Beacon V-Tags transmit a beacon message every 15 second which is picked up by a nearby gateway. The gateways also serve as reference points for reporting tag locations.

⚠ The gateway must be configured to be in “Security Mode” to report beacon messages.

2.0 Power and LED Indicators

2.1 Power

The gateway may be powered using PoE (Power-Over-Ethernet) or via USB-C. Power consumption for the gateway is: 2W (5V @ 0.4A). The gateway supports both IEEE 802.3af (PoE) and IEEE 802.3at (PoE+).

2.2 LED Indicators

There are three LED indicators. In normal operations, the LEDs have the following meaning:

POWER	Green	Unit is powered on
NETWORK	Green	The gateway has an IP address obtained over Ethernet or Wi-Fi
SERVER	Orange	The last transaction with the cloud server was successful

If the last transaction with the cloud server failed, the SERVER light will blink.

When powering up or immediately after a reset, the NETWORK light will flash five times.

2.3 Gateway Configuration Mode

If you briefly insert a paper clip in the hole next to the LEDs, this puts the gateway into configuration mode. The green NETWORK light will flash continuously. The orange SERVER light will be off. Configuration mode automatically terminates upon completion of configuration or after 10 minutes of no activity.

2.4 Gateway Factory Reset

If you insert a paper clip in the hole next to the LEDs for 5 seconds, the unit will reset to factory defaults. The NETWORK light and SERVER light will alternately flash for 10 seconds, and then the unit will reset.

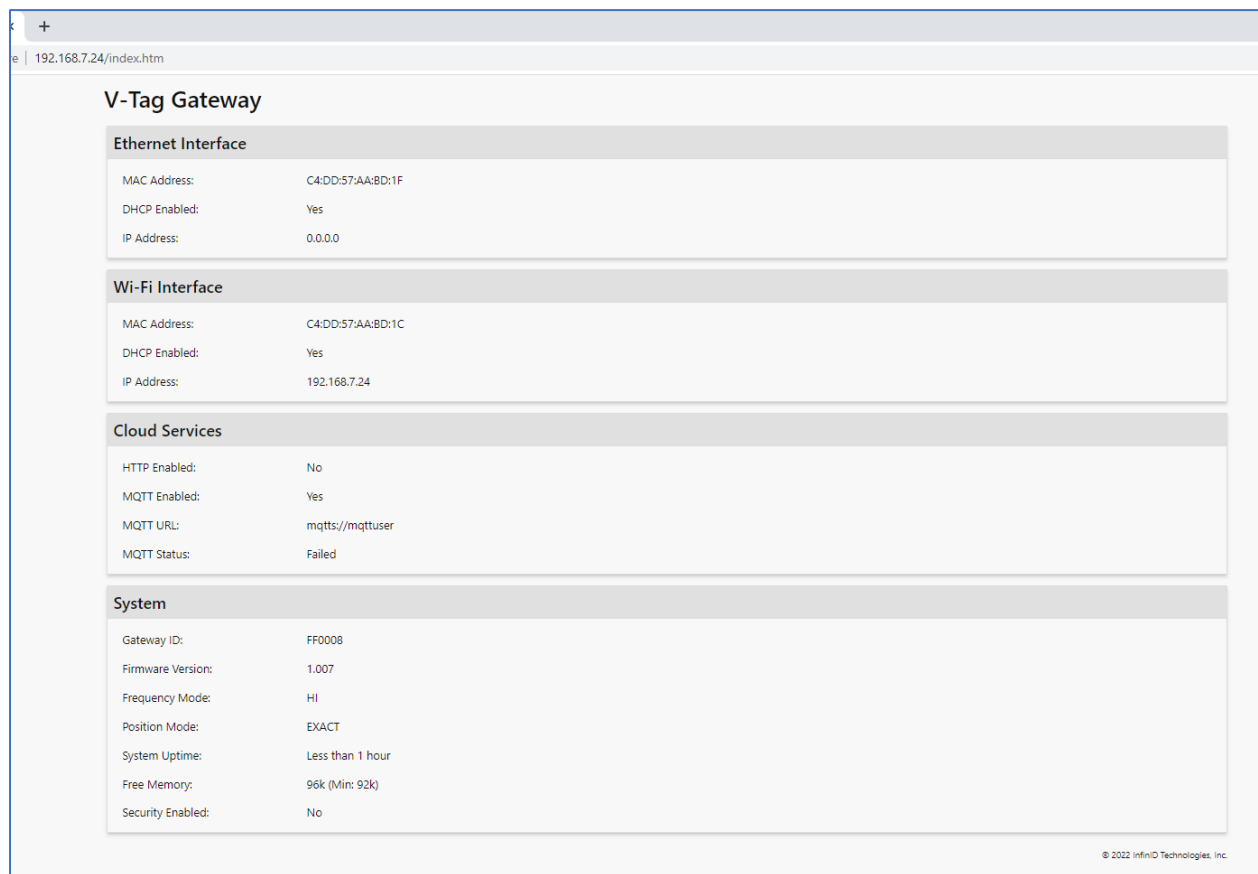
3.0 Additional Gateway Features

3.1 Two-way cloud communication

The gateway supports pushing messages to the cloud using HTTP or MQTT. If MQTT is used, the communication can be two-way to support messages from the cloud to the gateway. The most common command sent from the cloud to the gateway is the `BUZZ` command which is used to activate the buzzer in an asset tag, if so equipped.

3.2 Gateway Web Server

The gateway has an embedded web server which can be useful for checking gateway health. The embedded web server can be accessed at [http:// IP_ADDRESS/](http://IP_ADDRESS/) where `_IP_ADDRESS_` is the IP address of the gateway.



The screenshot shows a web browser window with the address bar displaying `192.168.7.24/index.htm`. The page title is "V-Tag Gateway". The interface is divided into four main sections: Ethernet Interface, Wi-Fi Interface, Cloud Services, and System. Each section contains a table of status information.

Ethernet Interface	
MAC Address:	C4:DD:57:AA:BD:1F
DHCP Enabled:	Yes
IP Address:	0.0.0.0

Wi-Fi Interface	
MAC Address:	C4:DD:57:AA:BD:1C
DHCP Enabled:	Yes
IP Address:	192.168.7.24

Cloud Services	
HTTP Enabled:	No
MQTT Enabled:	Yes
MQTT URL:	mqtt://mqttuser
MQTT Status:	Failed

System	
Gateway ID:	FF0008
Firmware Version:	1.007
Frequency Mode:	HI
Position Mode:	EXACT
System Uptime:	Less than 1 hour
Free Memory:	96k (Min: 92k)
Security Enabled:	No

© 2022 InfiniD Technologies, Inc.

3.3 Automatic firmware updates

By default, the gateway checks once a day for firmware updates. This check can be disabled in the initial configuration screen.

3.4 Gateway IP Address Discovery

The gateway broadcasts its IP address using Zeroconf/Bonjour/mDNS. This allows for discovery of the gateway IP address using an App such as Flame on iOS or Service Browser on Android. This can be useful if the gateway has joined the network but the gateway IP address is not known.

3.5 Gateway Security Mode

By default, the gateway does not report the 15 second beacon messages from V-Tags since this would generate a lot of unnecessary network traffic. However, if a gateway is placed at an entrance or an exit, it can be configured to be in security mode. If an asset tag enters this area, the activity will be reported. Security mode can be enabled in the initial configuration screen. A security mode reporting threshold from 0 dBm (very strong signal only) to -100 dBm (very weak signal) can be configured.

- ⚠ The gateway **must** be configured to be in “Security Mode” to report beacon messages from beacon tags. See Chapter 1 “Gateway Overview”.

4.0 Gateway Configuration using AssetWorx! App

The AssetWorx! App is used to configure the gateway when connecting to AssetWorx! software. At the conclusion of gateway configuration, the App creates a record within AssetWorx! containing the gateway details. The AssetWorx! App is available as an Android App in the Google Play Store or as an iOS App in the Apple App Store. See Chapter 5 if you do **not** plan to use AssetWorx! software.

Download the AssetWorx! App and launch it. You will need to provide the URL of the AssetWorx! cloud server or AssetWorx! local server when first launched. You will also be asked to login. Then select “More -> Setup Gateway”. Place the gateway into configuration mode by briefly inserting a paperclip into the hole next to the LEDs. The gateway should appear in the list of gateways to be configured. Select the gateway from the list.



The first configuration screen allows for configuration of system options.

← Add Gateway System Options

ASSETS LOCATIONS CHECKOUT MORE

System Options

HTTP Web Server

Enabled

Security Mode

Off

Automatic Updates

On

Security Mode Threshold

-100

Firmware Version

1.007

Ethernet MAC Address

C4:DD:57:AA:BD:1F

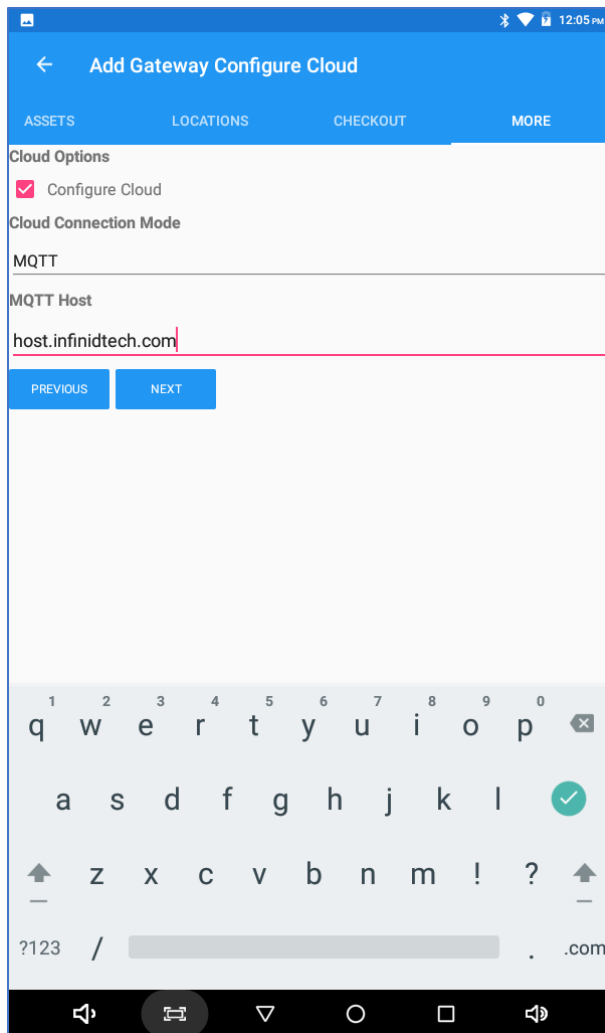
Wi-Fi MAC Address

C4:DD:57:AA:BD:1C

CANCEL NEXT

The HTTP Web Server is a web server that reports gateway status. It was described in Chapter 3 “Additional Gateway Features”. It may be enabled or disabled. The Security Mode option provides for the reporting of beacon messages from tags. It was also described in Chapter 3 “Additional Gateway Features”. It is normally left disabled for standard V-Tags. It should be enabled if beacon V-Tags have been purchased. By default, the gateway checks once a day for firmware updates. This feature can be disabled to conform with company policy.

The second configuration screen allows for configuration of cloud options.



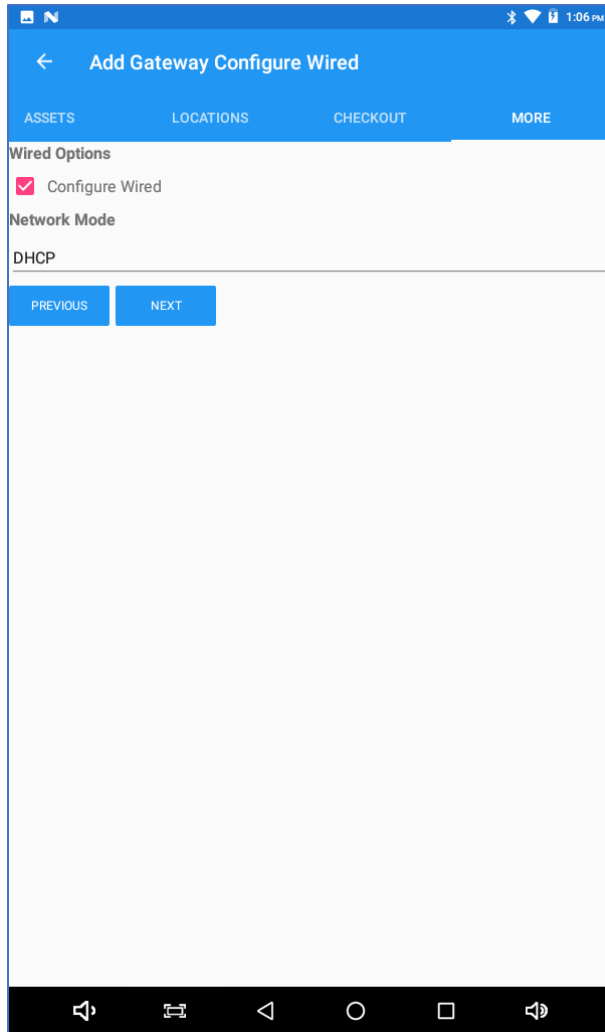
The gateway can use either HTTP or MQTT to push information to the cloud. MQTT has an advantage over HTTP since it supports two-way communications. The HTTP or MQTT host name (*not URL*) is specified on this screen.

The third configuration screen allows for configuration of Wi-Fi.

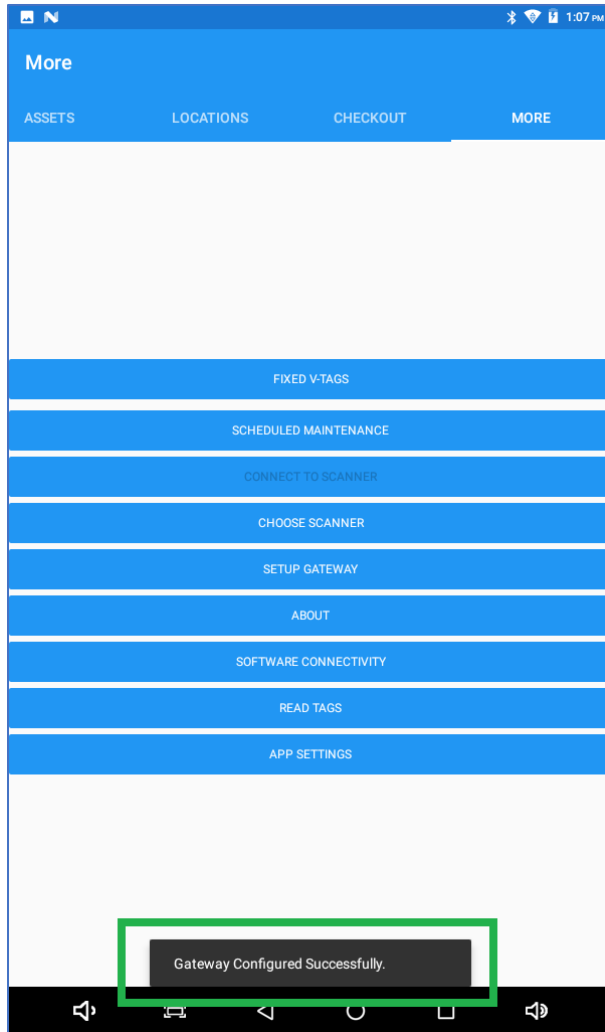
If consumer grade Wi-Fi is being used, the options are straightforward. The SSID can be either entered manually or selected from a list of Broadcast SSID names. The Wi-Fi password can be entered. If DHCP is selected, the gateway gets its IP address from a DHCP server. If Static IP is selected, the gateway IP address, netmask, routing gateway and DNS servers must be manually entered.

Many enterprises use a Radius Server and Enterprise Wi-Fi standards to enhance security. There are essentially two authentication options. (A) If client certificates are used, a client certificate for each gateway must be uploaded using the procedure in Chapter 6 “Uploading Client Certificates”. If enterprise server certificates must additionally be validated by the client, then a Root CA Certificate must be uploaded using the procedure in Chapter 6. (B) The second option for authentication is client login. This is easier to configure and simply requires a username and password to be specified. The password is specified using the password field earlier on the page. The anonymous identity is used during the Radius Server negotiations before encryption has been established. It is typically left blank causing the gateway to send the username “anonymous” during the early stages of negotiations. The private key password is also typically left blank unless the client private key file has been encrypted prior to client certificate upload.

The fourth configuration screen allows for configuration of Ethernet.



If DHCP is selected, the gateway gets its IP address from a DHCP server. If Static IP is selected, the gateway IP address, netmask, routing gateway and DNS servers must be manually entered.



After completing the configuration, you should get a message indicating the gateway was configured successfully, as shown above. The App will also automatically add a record for the gateway into AssetWorx!

5.0 Gateway Configuration using V-Tag Gateway Setup App

The V-Tag Gateway Setup App is used to configure the gateway when **not** using AssetWorx! software. The V-Tag Gateway Setup App is available as an Android App in the Google Play Store or as an iOS App in the Apple App Store. See Chapter 4 “Gateway Configuration using AssetWorx! App” instead if you plan to use AssetWorx! software.

Download the V-Tag Gateway Setup App and launch it. Place the gateway into configuration mode by briefly inserting a paperclip into the hole next to the LEDs. The gateway should appear in the list of gateways to be configured. Select the gateway from the list.



The first configuration screen allows for configuration of system options.

← Add Gateway System Options

System Options

Automatic Updates

On

HTTP Web Server

Enabled

Security Mode

Off

Security Mode Threshold

-100

Firmware Version

1.007

Ethernet MAC Address

C4:DD:57:AA:BD:1F

Wi-Fi MAC Address

C4:DD:57:AA:BD:1C

CANCEL NEXT

By default, the gateway checks once a day for firmware updates. This feature can be disabled to conform with company policy. The HTTP Web Server is a web server that reports gateway status. It was described in Chapter 3 “Additional Gateway Features”. It can be enabled or disabled. The Security Mode option provides for the reporting of beacon messages from tags. It was also described in Chapter 3 “Additional Gateway Features”. It is normally left disabled for standard V-Tags. It should be enabled if beacon V-Tags have been purchased.

The second configuration screen allows for configuration of cloud options.

Cloud Options

☒ Configure Cloud

Cloud Connection Mode

MQTT

MQTT Host

host.com

MQTT Username

mqttuser

MQTT Password

022cf657-b9ed-433b-bff4-9dc727a193ba

☐ Use Client Certificate

PREVIOUS NEXT

The gateway can use either HTTP or MQTT to push information to the cloud. MQTT has an advantage over HTTP since it supports two-way communications. The HTTP or MQTT host name (*not URL*) is specified on this screen. The server login credentials are also specified on this screen. If client certificates are needed for authentication, a client certificate for each gateway must be uploaded using the procedure in Chapter 6 “Uploading Client Certificates”.

The third configuration screen allows for configuration of Wi-Fi.

Configure Wi-fi

Wi-Fi Options

☒ Configure Wi-Fi

SSID Mode

Broadcast

SSID

A_Network

Wi-Fi Password

.....

Network Mode

DHCP

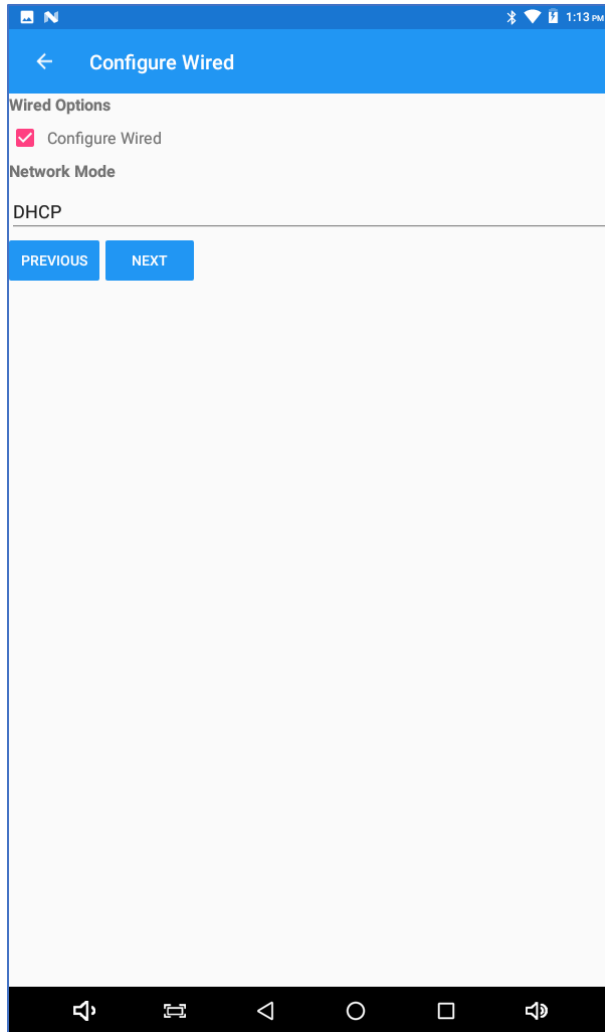
☐ Use Enterprise Wi-Fi

PREVIOUS NEXT

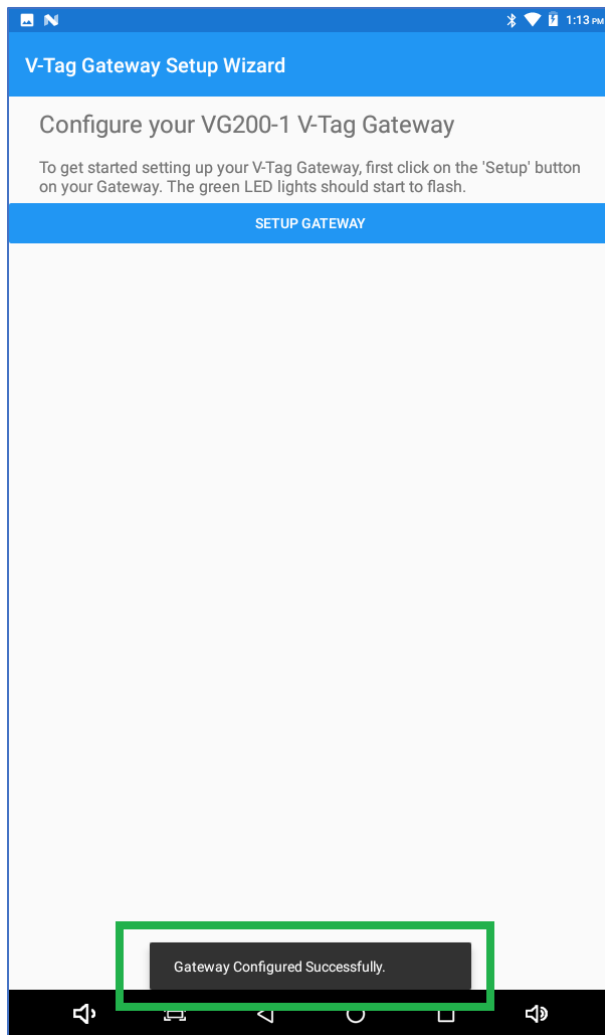
If consumer grade Wi-Fi is being used, the options are straightforward. The SSID can be either entered manually or selected from a list of Broadcast SSID names. The Wi-Fi password can be entered. If DHCP is selected, the gateway gets its IP address from a DHCP server. If Static IP is selected, the gateway IP address, netmask, routing gateway and DNS servers must be manually entered.

Many enterprises use a Radius Server and Enterprise Wi-Fi standards to enhance security. There are essentially two authentication options. (A) If client certificates are used, a client certificate for each gateway must be uploaded using the procedure in Chapter 6 “Uploading Client Certificates”. If enterprise server certificates must additionally be validated by the client, then a Root CA Certificate must be uploaded using the procedure in Chapter 6. (B) The second option for authentication is client login. This is easier to configure and simply requires a username and password to be specified. The password is specified using the password field earlier on the page. The anonymous identity is used during the Radius Server negotiations before encryption has been established. It is typically left blank causing the gateway to send the username “anonymous” during the early stages of negotiations. The private key password is also typically left blank unless the client private key file has been encrypted prior to client certificate upload.

The fourth configuration screen allows for configuration of Ethernet.



If DHCP is selected, the gateway gets its IP address from a DHCP server. If Static IP is selected, the gateway IP address, netmask, routing gateway and DNS servers must be manually entered.



After completing the configuration, you should get a message indicating the gateway was configured successfully, as shown above.

6.0 Uploading Client Certificates

Client certificates are used in the following situations:

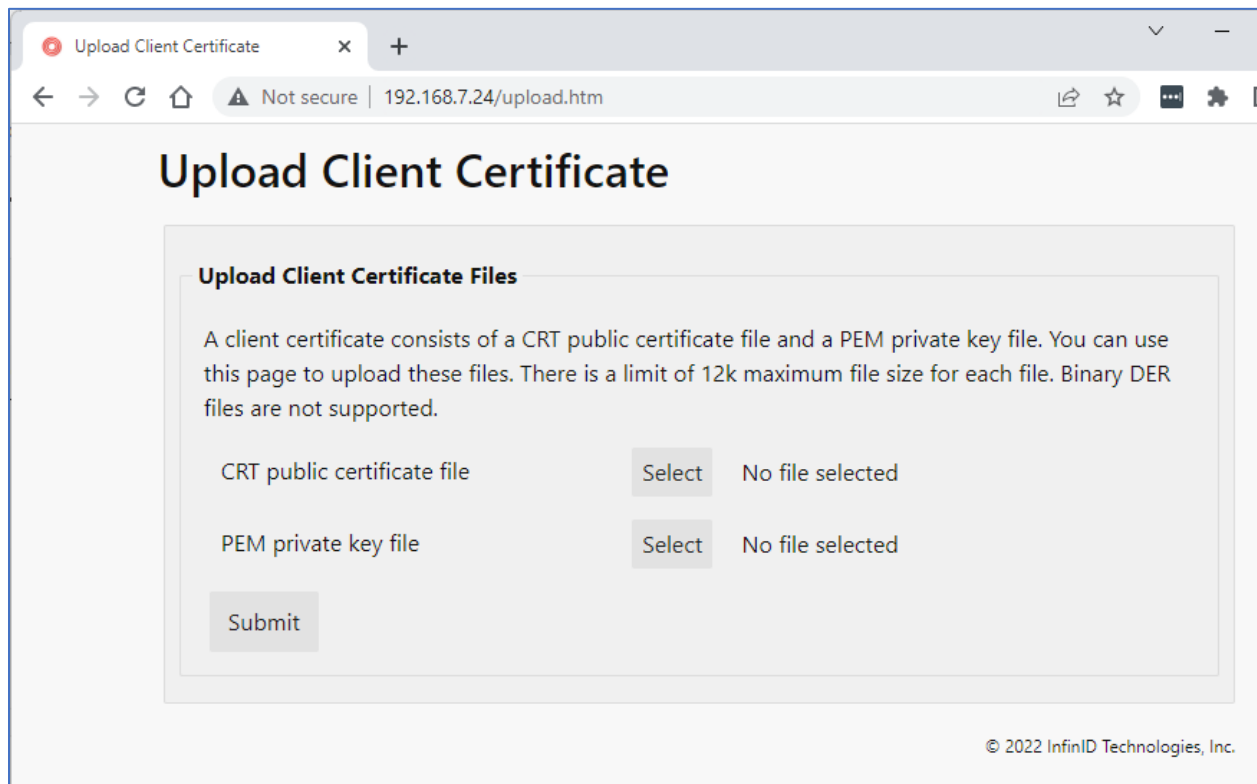
- Optionally for HTTP Push when not using AssetWorx!
- Optionally for MQTT Push when not using AssetWorx!
- Optionally for Enterprise Wi-Fi connections

Client certificates may be uploaded to the gateway while the gateway is in configuration mode. The following URL's are available:

[http:// IP ADDRESS/upload.htm](http://IP_ADDRESS/upload.htm) (Client Certificate)

[http:// IP ADDRESS/upload2.htm](http://IP_ADDRESS/upload2.htm) (Root CA Certificate)

Here `_IP_ADDRESS_` is the IP address of the gateway. Sample screens are given below.



The screenshot shows a web browser window with the title 'Upload Client Certificate'. The address bar shows '192.168.7.24/upload.htm' with a 'Not secure' warning. The main heading is 'Upload Client Certificate'. Below it, a section titled 'Upload Client Certificate Files' contains a text block explaining that a client certificate consists of a CRT public certificate file and a PEM private key file, with a 12k maximum file size limit and that Binary DER files are not supported. There are two file selection rows: 'CRT public certificate file' and 'PEM private key file', each with a 'Select' button and the text 'No file selected'. A 'Submit' button is located at the bottom left of the form area. The footer of the page reads '© 2022 InfinID Technologies, Inc.'

