



Technical Support Troubleshooting Guide

Wireless Vehicle Bus Adapter

Digi Technical Support

November 2019

Ver. 1.1

Technical Support Troubleshooting Guide – Wireless Vehicle Bus Adapter

Contents

1	Introduction	3
1.1	Overview	3
1.2	Assumptions	3
1.3	Corrections	3
1.4	Version	3
1.5	Useful Equipment for Troubleshooting.....	3
2	Troubleshooting Reference – Getting Started Guide.....	4
3	Hardware Troubleshooting Supplement	5
3.1	Verifying Power to Wireless Vehicle Bus Adapter (WVA)	5
3.2	Verifying WVA is at Factory Default Configuration	6
3.3	Verifying Ability to Connect to WVA’s Wi-Fi Access Point.....	7
4	Configuration Troubleshooting Supplement.....	9
	Key Considerations for WVA Configuration	9
4.1	Accessing the Device Configuration and Management WebUI	9
4.2	Configuring a Time Source – Unable to Update Firmware error	12
4.3	Troubleshooting Time Related Issues	13
4.4	Updating to the latest WVA OS/Firmware	14
4.5	Wireless Network Configuration: Infrastructure or Wi-Fi Direct?.....	14
4.6	Troubleshooting Wi-Fi Network Connectivity Issues	15
4.7	Internal Wi-Fi Diagnostics Monitor	17
4.8	Troubleshooting Digi Remote Manager (DRM) Connection Issues.....	18
4.9	Issues with Python Script usage on the WVA.....	20
4.10	Issues Receiving Vehicle Data: Alarm and Event Channel Usage.....	21
5	Obtaining Troubleshooting Data and WVA Logfiles.....	23
5.1	WebUI - Home page.....	23
5.2	WebUI - Adapter Status	24
5.3	WebUI - System Log areas.....	24
5.4	Admin Tools: /ws web services information	25
5.5	Digi Remote Manager Properties pages:	25

1 INTRODUCTION

1.1 Overview

This guide is intended to supplement the WVA Getting Started Guide's Troubleshooting section, to provide additional troubleshooting insight and background based on lessons learned from field use of the Wireless Vehicle Bus Adapter (WVA). This guide can also be used to determine if RMA/repair may be necessary during the Wireless Vehicle Bus Adapter's 3yr. warranty period.

1.2 Assumptions

This guide has been written for use by technically competent personnel with an understanding of Wi-Fi (802.11b/g/n) communications, and of the requirements for any specific application(s), hardware, and/or Operating System(s) in use with the WVA. This guide also assumes the user has a basic ability to access and navigate the product's WebUI using a Web Browser, and that a person installing a WVA into a Vehicle is knowledgeable about the Vehicle itself, its interfaces and operation, or has access to personnel who are knowledgeable about the vehicles which the WVA will be installed into.

1.3 Corrections

Feedback and corrections to this document, or content-related requests are welcome and can be addressed to: tech.support@digi.com, subject: Attn: WVA Troubleshooting Guide feedback.

1.4 Version

Version Number	Status
0.1	Draft
1.0	Initial Release – Sept 2016
1.1	Update – Nov 2019

1.5 Useful Equipment for Troubleshooting

The following equipment is useful when troubleshooting Wireless Vehicle Adapter issues:

- 1) WVA's QR Code/PASS key Label (or close-up image of the QR Code/PASS key label on a phone)
– QR Code label or PASS key is required to connect to the WVA Access Point for the first time
- 2) Known working WVA (for verifying vehicle bus power or to swap out a bad WVA if necessary)
- 3) PC/Laptop, Mobile phone, or Tablet with Wi-Fi enabled and Admin access for network config – Wi-Fi troubleshooting apps and QR code reader useful
- 4) Wireless Vehicle Bus Adapter Wire Harness (for testing WVA outside of Vehicle/Truck)

Digi Accessory page: <https://www.digi.com/products/models/76000931>

2 TROUBLESHOOTING REFERENCE – GETTING STARTED GUIDE

Getting Started Guide – Basic Troubleshooting Reference:

- [Power LED is dark](#)
- [Device is not discovered by Digi Device Discovery](#)
- [Cannot open web interface or access web services](#)
- [Cannot receive data from the CAN bus](#)
- [WVA does not connect to a Wi-Fi infrastructure Access Point](#)
- [Wi-Fi access issues](#)
- [Cannot discover device using Wi-Fi Direct](#)
- [Cannot associate with WVA over Wi-Fi Direct in push-button mode](#)
- [Cannot associate with WVA over Wi-Fi Direct in PIN mode](#)
- [Wireless signal strength issues](#)

Other Useful Wireless Vehicle Bus Adapter Links:

- [WVA Developer Guide](#)
- [WVA Firmware Page](#)
- [WVA TLS 1.2 Support](#)
- [Understanding TCP and UDP port usage on the WVA](#)

3 HARDWARE TROUBLESHOOTING SUPPLEMENT

Reference: Connect the Hardware:

https://www.digi.com/resources/documentation/digidocs/90001929/default.htm#Task/T_connect_hardware.htm

The Wireless Vehicle Bus Adapter (WVA) is a rugged, compact, 1708/J1939 to Wi-Fi plug-in device, which provides easy access to vehicle data via Wi-Fi connection to the WVA and its full-featured API using secure RESTful web services commands. The WVA installs in minutes by connecting directly to the 9-Pin Deutsch diagnostic port of the vehicle, which also serves as the WVA power source:

Reference: Deutsch 9-Pin pinout:

https://www.digi.com/resources/documentation/digidocs/90001930/default.htm#reference/r_hardware_connector_pinout.htm

Important Note: Some newer Vehicle/Trucks models have started using interfaces for vehicle data other than the **9-Pin Deutsch connector**. These connectors may have an alternate diagnostic port where data may also be available (examples: CAN3, RP1226 VECU, future interface standards). These interfaces are **untested by Digi for use with the WVA**, so results may be **unpredictable**.

A WVA **should never be plugged into an interface other than a Deutsch 9-Pin**, unless the **Truck Manufacturer** or Body Builder Manual for that particular Truck Model/Type (or **authorized vehicle shop**) **has been consulted** for compatibility information, or whether Vehicle Manufacturer warranty might be voided by connecting the WVA into an incompatible interface/ adapter cable.

Digi assumes no responsibility for damage to vehicle or WVA device due to a WVA being plugged into a vehicle with an interface other than the Deutsch 9-Pin:

WVA Product page: <https://www.digi.com/products/networking/gateways/wireless-vehicle-bus-adapter>

3.1 Verifying Power to Wireless Vehicle Bus Adapter (WVA)

Vehicle ignition should be to Off prior to installing a WVA into the vehicle Deutsch 9-Pin connector/vehicle bus interface. If cable adapter or Truck vehicle interface wiring changes are needed, they should only be done when vehicle battery is disconnected.

When WVA is connected into a 9-Pin Deutsch J1708/J1939 vehicle bus connector and Vehicle **Ignition is turned back On**, the **Power LED** (see below for location) should be lit **solid Green**.

Exception: During firmware update, **Green Power LED flickers** slightly while firmware is updating.



Figure 3-1: Wireless Vehicle Bus Adapter Power LED

Technical Support Troubleshooting Guide – Wireless Vehicle Bus Adapter

If WVA Power LED (see Example below for location) isn't lit solid Green on an installed WVA:

1. Remove any in-line Y-cable or “dogbone” adapter in use between the Truck's Deutsch 9-Pin connector and WVA. If a cable/adapter was removed: Install WVA directly into 9-Pin Deutsch connector then re-check Power LED. If Power LED is now lit, Adapter cable may be bad.
2. If WVA Power LED is still dark, and a known-working/spare WVA is available, swap the suspect WVA unit with the known-working spare, to see if the spare WVA works when plugged in. If spare unit works, RMA the suspect unit. If no spare unit is available, continue onto step 3.
3. If WVA Power LED is still dark and a Digi WVA Wiring Harness is available, plug the suspect WVA into the Wiring Harness to see if WVA Power LED is lit. If a Wiring Harness is unavailable, try plugging suspect WVA into a different Truck. If Power LED is still dark, RMA the suspect unit.

Note: If an RMA is necessary, the Serial Number and WVA MAC are both needed, and can be found on the underside of the WVA Mounting Ring. For RMA purposes, the “WVA Serial Number” might be either the S/N# or the WVA MAC (both were used at different times). The S/N and MAC font are small – taking a picture of the Serial Number/MAC location on the underside of the WVA mounting ring is useful to identify the device.

3.2 Verifying WVA is at Factory Default Configuration

Reference: Reset the WVA to Factory Defaults:

https://www.digi.com/resources/documentation/digidocs/90001929/default.htm#Task/T_factoryreset.htm

At Factory Default, the WVA will broadcast its printed MAC address as the Wi-Fi SSID of its Access Point. The wva-<MAC> Access Point provides a Wi-Fi interface for further configuration of the WVA via the Web User Interface (WebUI).

Factory Default procedure using the Reset Switch

1. Locate Reset Switch on the faceplate, beneath a raised area under the Digi logo



Figure 3-2: Location of Factory Reset Button

Technical Support Troubleshooting Guide – Wireless Vehicle Bus Adapter

2. Depress Reset Switch for a minimum of 10 seconds to Factory Default the WVA.

Note: The reset_delay value for the Reset button is programmable via RCI, web services (/ws/config/button), or changing the WVA's config file and reloading it with the new value. Depressing the switch for longer than the specified Factory Default of 10 seconds might be necessary if a longer reset_delay value was configured in order to avoid accidental factory default during field use.

3. After the Factory Default procedure is performed, the WVA automatically reboots.

Note: The reset_delay value for the button is programmable via RCI, web services (/ws/config/button), or by changing the WVA's config file. Depressing the switch for longer than the specified factory default value would be necessary, if a longer value was configured on the device to avoid accidental factory default during field use.

After a few moments, the wva-<MAC> Access Point should be seen in a Wi-Fi scan from the Laptop, Mobile Phone, or Tablet. The wva-<MAC> Access Point can take a few moments to show up in the Wi-Fi scan, so several Wi-Fi scans may be needed before the built-in wva-<MAC> Access Point appears.

If a Wi-Fi scan shows a *DIRECT-xx-<wva-mac address>* device instead of a wva-<MAC> Access Point SSID, it indicates that the WVA is configured for a Wi-Fi-Direct connection. Re-do Factory Default procedure on the WVA (section 3-2) in order to re-enable the wva-<MAC> Access Point SSID for the device.

If the wva-<MAC> Access Point still doesn't show up after several scans after verifying the WVA has been Factory Defaulted, verify warranty status with Digi Technical Support and RMA the device for repair if still under warranty.

3.3 Verifying Ability to Connect to WVA's Wi-Fi Access Point

Reference: Connect to the WVA:

https://www.digi.com/resources/documentation/digidocs/90001929/default.htm#Task/T_connect_to_wva.htm

A Wi-Fi connection must be established initially to the wva-<MAC> Access Point (interface: wlan1), so that the WVA can be further configured for operation using the WVA's Web User Interface (WebUI).

Connecting to the wva-<MAC> Access Point by scanning the QR Code:

The easiest way to establish a Wi-Fi connection with the WVA's wva-<MAC> Access Point is by scanning the QR code using a QR Code reader app on a Tablet or Mobile Phone:

- 1) Enable Wi-Fi on the Tablet/Mobile Phone device from which you'll be connecting with the WVA
- 2) Open the Wi-Fi area on the Tablet/Mobile Phone and "forget" any existing Wi-Fi connections that your device is already connected to (also, disable automatic Wi-Fi connections).

Technical Support Troubleshooting Guide – Wireless Vehicle Bus Adapter

- 3) Scan the QR Code (from QR Code label which shipped with the WVA) using a QR Code reader



Figure 3-3: Example QR Code label

- a. A “Configure Wi-Fi” box pops up with the WVA’s SSID, example: wva-00:40:9D:5C:49:98
- b. Select “OK” to connect to the WVA’s Access Point automatically.

Note: If a “Wi-Fi Networks” list appears instead of a box saying “Internet unavailable” which lists the WVA’s SSID (indicates successful connection to the WVA’s Access Point), return to step 2 and “forget” any existing Wi-Fi network connection, then retry step 3.

If a QR Code reader app (or the QR Code itself) is not available, the QR Code Label also contains a PASS key, which can also be used to connect to the WVA Access Point via manual configuration.

Connecting to the wva-<MAC> Access Point using the WVA PASS key:

- 1) Run a Wi-Fi scan – select/click the wva-<MAC> SSID for the intended WVA from the list
- 2) When the Wi-Fi PIN entry box pops up, click the link to “**Connect using a security key instead**”:

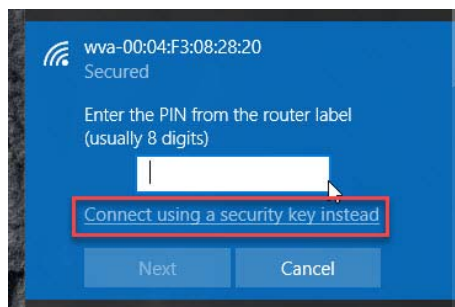


Figure 3-4: Wi-Fi PIN configuration box

- 3) Enter the WVA Passkey from the QR code label as the network security key



Figures 3-5, 3-6: Accessing WVA Access Point using WVA Passkey as network security key

Technical Support Troubleshooting Guide – Wireless Vehicle Bus Adapter

- 4) If the Wi-Fi connection with the WVA is successful, the PC, Tablet, or Mobile Phone will be connected to the WVA's wlan1 interface in order to enable further configuration via the WebUI

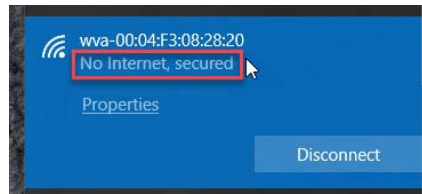


Figure 3-7: Successful connection to WVA Access Point

- If the QR Code is unavailable and the WVA Passkey is refused when customer tries connecting to the WVA Access Point, the WVA Passkey can be verified by contacting Digi Tech Support.

Note: If the PASS key itself isn't available, the font isn't legible, or what appears to be printed as the PASS key isn't working, the PASS key can be obtained through Digi Tech Support. Requestor should provide proof of WVA ownership by providing a photo of the S/N# and MAC listed on the underside of the WVA mounting ring.

4 CONFIGURATION TROUBLESHOOTING SUPPLEMENT

Key Considerations for WVA Configuration

The following section covers various configuration areas of the WVA, some of which are required for proper use of the product in a field environment, others which are optional.

Once the WebUI of the WVA is accessed for the first time, a time source **must** be configured, because items such as a firmware are not allowed until a date/time has been set on the WVA. With the date/time configured, firmware should be updated to the most recent version available from the Tech Support website, after which the remainder of WVA configuration can continue.

4.1 Accessing the Device Configuration and Management WebUI

1. If a Wi-Fi enabled Windows system is being used to connect to the WVA for the first time, the Digi Device Discovery Tool can be run from the Windows desktop to verify the Wi-Fi connection with the WVA's Access Point (AP):

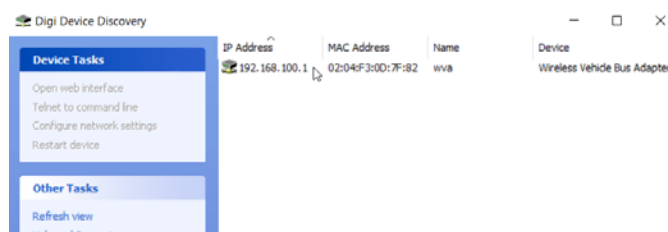


Figure 4-1: Successful Discovery of WVA AP from Windows 10 laptop

Digi Device Discovery Tool link: www.digi.com/support/knowledge-base/device-discovery-troubleshooting-tips

Technical Support Troubleshooting Guide – Wireless Vehicle Bus Adapter

2. **Select** the discovered WVA, then under **Device Tasks** menu - select **Open web interface**:

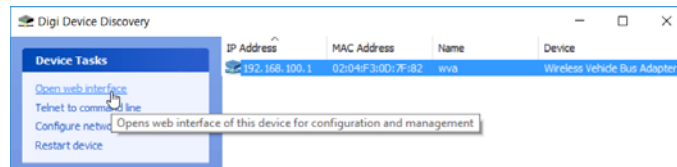


Figure 4-2: Opening WVA WebUI directly from Digi Device Discovery Tool

*** Skip to step 4

3. If a Tablet or Mobile Phone (or PC/Laptop without Digi Device Discovery Tool) is connecting to the WVA, a simple ping test to 192.168.100.1 can be used to verify connection to the WVA:

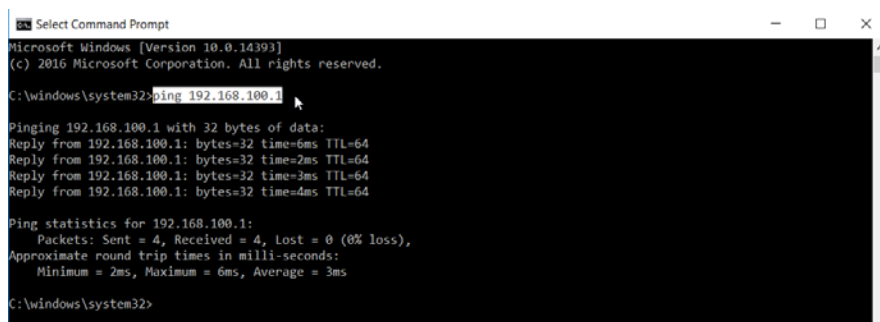


Figure 4-3: Windows 10 Wi-Fi scan showing laptop connected to WVA AP

4. Open Web browser to 192.168.100.1 (default IP address of WVA AP) for WebUI Login Prompt:

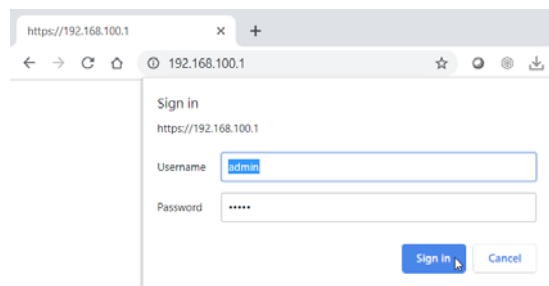


Figure 4-4: WVA WebUI Login Prompt

WVA Factory Default Login:

Username: **admin**

Password: **admin**

Note: If default of admin/admin fails, factory default the WVA (see section 3-2)

Technical Support Troubleshooting Guide – Wireless Vehicle Bus Adapter

5. Upon successful login, a **Privacy Error** page with **Your connection is not private** is displayed. Click on the word **Advanced**, then the **Proceed to 192.168.100.1** link:

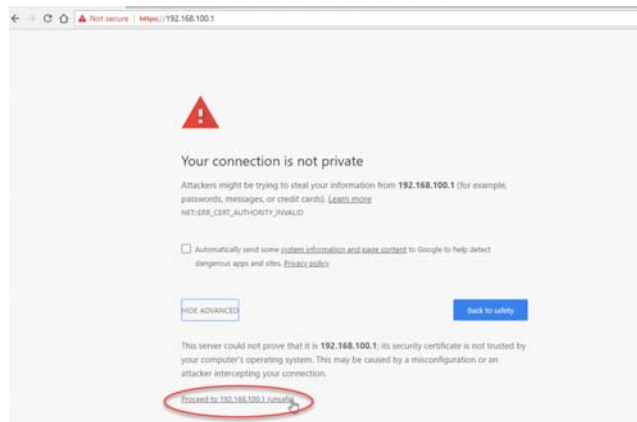


Figure 4-5: Browser's "Not Secure" warning page

6. On successful login, user will land at the WVA Device Configuration and Management page:



Figure 4-6: WVA Device Configuration and Management Home page

4.2 Configuring a Time Source – Unable to Update Firmware error

The WebUI **Home** page (see **Figure 3-5** above) displays the **Date and Time** currently in use on the WVA, adjusted for the configured Timezone. If the displayed Date/Time is incorrect, the WebUI Configuration → Time area can be used to configure the Real Time Clock.

Uncheck the Enable Time Server Synchronization option, then check the Set Time option and set Date/Time for the chosen Timezone (UTC in example below):

Home

Configuration

- Wireless Network
- Wireless Access Point
- Python
- Network Services
- Time
- Device Cloud Connectivity
- Power Management
- CAN Bus
- Admin Password

Administration

- File Management
- Certificate Management
- Backup/Restore
- Firmware Update
- Adapter Status
- System Log
- Legal Notices
- Reboot

Time Configuration

Network Time Protocol (NTP) Settings

☐ Enable Time Server Synchronization

NTP Time Precision:

- ☐ Standard (1 sync per day)
- ☒ High (Up to 1 sync per minute)

Note: High NTP Time Precision requires the device to perform frequent NTP sampling. This may significantly increase network data usage.

NTP Server #1:

NTP Server #2:

NTP Server #3:

NTP Server #4:

Time Settings

Note: Time Server Synchronization must be disabled to set the time.

☒ Set Time:

Month: Day: Year:

Hour: Minute: Second:

Timezone Settings

Timezone:

Figure 4-7: Configuration → Time area of the WebUI – Setting Date/Time/Timezone

When the WVA is first powered, the clock is not configured and displays date/time as **Jan 1 2000 00:00:00**. The clock then begins counting time forward (until current date/time is set).

Setting a valid Date/Time when first connecting to the WVA is so important that **WVA OS/firmware update is denied** without date/time having been set. The **SSL connection into Digi Remote Manager** (when enabled) also requires that a **valid date/time is configured**, so that the certificate being used to establish the **SSL connection into DRM isn't rejected**.

The WVA's System Logs are time-stamped using this Date/Time (as is the Vehicle bus data flowing through the WVA), so keeping accurate Date/Time is important.

Where applications collecting vehicle data through the WVA are concerned, the application should **contain a function for setting correct date/time at least once per day (and after each reboot of the WVA)**, to ensure that date/time is always accurate.

To set the RTC Date/Time of a WVA from a RESTful web services client, a PUT should be sent to /ws/hw/time using the proper Date/Time format (in UTC): `<time>2019-07-31T07:50:32Z</time>`

4.3 Troubleshooting Time Related Issues

The WVA WebUI Home page (see Figure 3-5 on page before previous) provides a quick view of the current Date/Time in use on the WVA.

To check time programmatically via web services, send a GET to /ws/hw/time from a REST client (or enter the web services time location after IP address of the WVA in a web browser, as shown below:

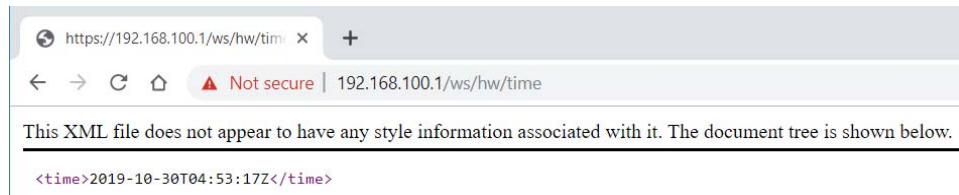


Figure 4-8: Displaying Date/Time in browser via web services

Date/Time issues can often be detected from the WVA WebUI Admin → System Logs, by searching for chrony activity in `digi.log` (or `digi.log.0`), or `digicdsd` activity such as in `eventlog.txt` output below:



Figure 4-9: WebUI's Admin → System Logs Log File Browser area

If Date/Time jumps around by days or months within any of the System Log files, it is typically an indicator that the WVA was configured for NTP time sync then lost internet connectivity for a period of time. Another possibility is that the WVA was without power for an extended period, after which the WVA's internal clock reverted back to its last known RTC date/time.

This is the standard way that "time" functions within the WVA, so the WVA's built-in Real-time clock should be kept updated by the app using the WVA, unless the WVA will have a continuous internet connection available through which frequent NTP Time Synchronization can be used.

4.4 Updating to the latest WVA OS/Firmware

WVA Firmware page: <https://www.digi.com/support/productdetail?pid=5594&type=firmware>

There have been a number of updates since WVA OS/firmware version 3.2.25.10 (last released firmware before the WVA's software stack was overhauled and a number of major enhancements to the product were made. Once the correct Date/Time are configured on the WVA, the OS/firmware of the device should be updated to the latest version available from the Digi Tech Support website:

4.5 Wireless Network Configuration: Infrastructure or Wi-Fi Direct?

Reference Link:

Configuring Wireless Network Settings:

https://www.digi.com/resources/documentation/digidocs/90001929/default.htm#Task/T_config_wireless.htm

Once date/time is configured and the firmware is at the latest version, the next step in WVA configuration is to set it up for a client connection to another network or device, using the

Wi-Fi Infrastructure Mode – WVA connects to an Infrastructure Access Point, such as a Mobile Hotspot running on a Tablet in a vehicle, or an Infrastructure Wi-Fi Access Point (WVA is typically configured as a DHCP client in this mode). Internet access may also be enabled with this type of connection, so this is a good choice if Remote Management will be used with the WVA. The WVA's Access Point also remains available in this mode, so the WVA can still be accessed at 192.168.100.1 for WebUI/Web Services access.

Wi-Fi Direct Mode – Wi-Fi Direct allows a pair of Wi-Fi devices to establish a direct connection with each other, without need for an Access Point. Wi-Fi Direct requires a one-time configuration, where the WVA is setup to establish the Wi-Fi Direct connection, either by pushing the button on the WVA or entering a PIN.

By definition, Wi-Fi Direct is point-to-point between the WVA and another device, so an Internet route for Remote Management isn't readily available. A proxy connector software which routes all traffic on TCP Port 3199 (DRM), UDP port 123 (NTP) traffic), and UDP port 53 (DNS), between the WVA's Wi-Fi Direct connection and the Internet (using Tablet or Mobile Phone Cellular access) can allow for Remote Management and NTP capability.

Note: The WVA's Access Point is disabled when the WVA is configured for Wi-Fi Direct mode. If access to the WVA Access Point is needed after Wi-Fi Direct mode was configured, WVA can be factory defaulted (see section 3-2) to re-enable the wva-<MAC> Access Point for connection.

4.6 Troubleshooting Wi-Fi Network Connectivity Issues

The WVA can be correctly configured for a Wi-Fi Infrastructure Mode or Wi-Fi Direct Mode connection, yet still encounter Wi-Fi network connectivity issues beyond its own control. This could result in the WVA being frequently disconnected from its configured Wi-Fi network connection.

Wi-Fi Signal Strength/Signal Environment Issues

Reference links - RF environment and wireless troubleshooting:

https://www.digi.com/resources/documentation/digidocs/90001929/Default.htm#Reference/TS_wireless_issues.htm

<https://www.digi.com/support/knowledge-base/zigbee-wifi-coexistence>

WVA Data Sheet: https://www.digi.com/pdf/ds_wva.pdf

If a WVA keeps getting disconnected from its configured Wi-Fi network connection, whether in Infrastructure or Wi-Fi Direct Mode, the first thing to consider is the immediate RF environment and what potential sources of interference exist in the area of the WVA-to-Wi-Fi Network connection.

An important thing to consider is where and how the WVA is mounted. For instance, has the WVA been installed inside the dashboard of the vehicle or on a metal surface? If so, the WVA may be in a somewhat constricted area which may cause the WVA to overheat in high temperature days, or the metal surface may act as a ground plane and attenuate the Wi-Fi signal.

Considering that the dash/dashboard area might also be made of metal and connected to electrical Ground (or have in-vehicle instrumentation that is “noisy” in an RF sense), an In-Vehicle installation may have unique challenges where the RF environment is considered. Other important factors to consider where RF Environment is concerned is the distance between the WVA and Wi-Fi network it connects to, what obstructions to RF exist between those points, the signal strength of the WVA, as well as the Signal Strength of the network device which the WVA is connecting to.

The WVA WebUI Admin → Adapter Status page contains info about WVA Signal Strength, and can be refreshed manually or at a 5-second auto-refresh interval:

Home

- Configuration
 - Wireless Network
 - Wireless Access Point
 - Python
 - Network Services
 - Time
 - Device Cloud Connectivity
 - Power Management
 - CAN Bus
 - Admin Password
- Administration
 - File Management
 - Certificate Management
 - Backup/Restore
 - Firmware Update
 - Adapter Status**
 - System Log
 - Legal Notices
 - Reboot

Wireless Vehicle Adapter Status

Current Wireless Network Status

Active SSID:	Frontier652F
Access Point:	28:80:88:69:0E:0E
Signal Level:	-50 dBm
Link Quality:	60/70

Current Vehicle Status

VIN:	N/A
Engine Speed:	N/A
Vehicle Speed:	N/A

CAN Bus Statistics

Bus	Bytes Received	Packets Received	Bytes Sent	Packets Sent
can0	0	0	0	0
can1	0	0	0	0

Refresh Once | Refresh Automatically

Automatic refresh requests a status update every 5 seconds.

Figure 4-10: WVA WebUI's Admin → Adapter Status page – RF info highlighted

Technical Support Troubleshooting Guide – Wireless Vehicle Bus Adapter

Wi-Fi Watchdog

In order to re-connect a WVA to its configured Wi-Fi connection if its been disconnected for whatever reason, a Wi-Fi Watchdog has been added that reboots the WVA if Wi-Fi has been disconnected for a configurable number of minutes (**factory default setting = Enabled for 5 minute watchdog, useable range = 5 – 65535**). Use **Apply** button at bottom of page if config changes were made.

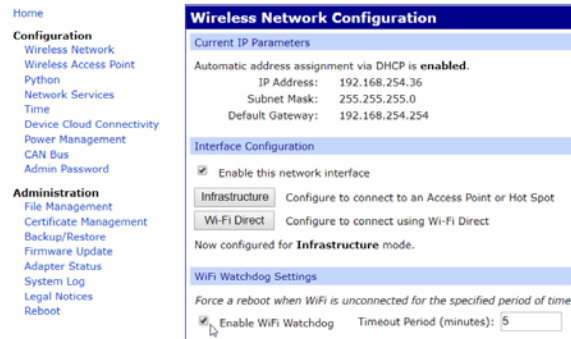


Figure 4-11: WebUI Configuration → Wireless Network, Wi-Fi Watchdog Settings

WPA_Supplicant Logging Verbosity Level

For troubleshooting network connectivity issues, verbose debug logging capability has been built into the WVA in the form of WPA Supplicant Logging (outputs to wifi.log and wifi.log.0).

Wi-Fi logging level can be configured individually for each WVA wlan adapter with web services:

PUT to <https://192.168.100.1/ws/config/logging>

```
<logging>
  <wpa_supplicant_wlan0>0</wpa_supplicant_wlan0>
  <wpa_supplicant_wlan1>0</wpa_supplicant_wlan1>
</logging>
```

The Logging Verbosity Levels can also be configured on Connected devices with Digi Remote Manager:

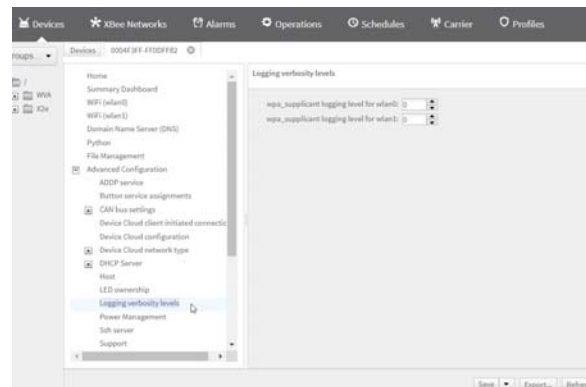


Figure 4-12: WPA_Supplicant Logging Verbosity Level Setting via DRM Properties page

Wi-Fi logging level settings:

- 0 - original Wi-Fi-related output which used to be logged in digi.log (now logged in wifi.log)
- 1 - reduced verbose logging
- 2 - explicit Wi-Fi logging - rolls over the wifi.log file in about 3 min

Note: Logging levels above 0 may result in heavy CPU utilization depending on amount of network activity - leave disabled unless actively debugging a Wi-Fi issue, then download the Wi-Fi log every few minutes to avoid missing important debug info.

4.7 Internal Wi-Fi Diagnostics Monitor

Due to the extreme vibration levels sometimes encountered when a WVA is used in a Heavy Equipment environment, a Wi-Fi Diagnostic Monitor begins running 30 seconds after bootup, then at 5 minute intervals afterward to check if Wi-Fi chip or connector issues have occurred inside the WVA.

Example: If the Wi-Fi driver fails to load or if transmit errors occur, the Amber LED labelled “App” ON the WVA faceplate will flash for 30 seconds, then the WVA will reboot. Every time a failure of either error type occurs, the count of that error type is incremented then written to the file system.

If Wi-Fi operation is intermittent and WVA is sometimes accessible, the user can view information regarding frequency of these errors via the web services interface at ws/errors.

Perform a GET of the /ws/errors output, which appears like this when no errors exist:

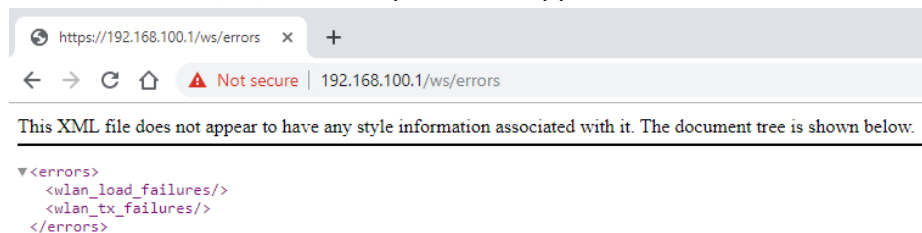


Figure 4-13: WVA web services – GET to /ws/errors via browser – no Wi-Fi Diagnostic Monitor errors

If errors had occurred, the output would be similar to below (# is # of times an error occurred):

```
<errors>

<wlan_load_failures>1</wlan_load_failures>

<wlan_tx_failures>1</wlan_tx_failures>

</errors>
```

If <wlan_load_failures/> or <wlan_tx_failures/> errors occur frequently, contact Digi Technical Support to check warranty status toward RMA/Repair of the WVA if within the 3 yr. warranty period.

4.8 Troubleshooting Digi Remote Manager (DRM) Connection Issues

Digi Remote Manager (DRM) is a comprehensive IoT device monitoring application for secure asset monitoring and control. As such, DRM is the ideal platform for managing the thousands of Wireless Vehicle Bus Adapters which might be installed, in support of ELD compliance monitoring and giving Managers a view into the health of a large Truck Fleet spread across a country or region:

- Fleet Management page: <https://www.digi.com/industries/transportation#Fleet>

When your WVA becomes DRM-connected, the connection history of each WVA device can be monitored, WVA OS/firmware can be kept up to date, WVA configuration changes can simultaneously be made en masse, and all vehicle data coming in from the Fleet's WVA devices can be captured into streams for real-time analysis, or pushed to a central server for long-term data storage or webpage display of Fleet data.

Sign up for a free 30-day Trial account on the Digi Remote Manager Product page:

- <https://www.digi.com/products/iot-software-services/digi-remote-manager>

Configuring the WVA for Connection to Digi Remote Manager

Reference Link: https://www.digi.com/resources/documentation/digidocs/90001929/default.htm#Task/T_config_enable_DC.htm

Since Digi Remote Manager is the perfect way of managing all of a Fleet's WVA devices, a configuration option for DRM connectivity is available in the WebUI (actual Digi Remote Manager DNS name and TCP Port number of outbound SSL socket connection for DRM connectivity are shown below):

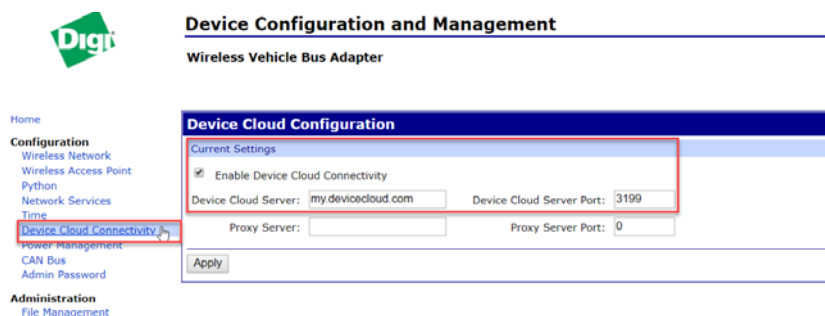


Figure 4-13: WebUI Configuration → Device Cloud Connectivity page

Requirements for successful Remote Management (and NTP Time Sync) usage on WVA:

1. WVA has reliable Wi-Fi network connection which provides Internet access
2. DRM (Device Cloud) connectivity option enabled to DNS name my.devicecloud.com
3. Digi Remote Manager Server Port number is set to 3199
4. Outbound ports TCP port 3199 (EDP/SSL connection to DRM); and UDP ports 123 (if NTP Time Sync used) and/or 53 (DNS name service) aren't being blocked by a firewall.
5. Date/Time is configured (whether Real-Time clock in use or NTP Time Sync is enabled)

Technical Support Troubleshooting Guide – Wireless Vehicle Bus Adapter

Internet Access and Firewall Requirements for Connection to Remote Manager

The following article may be useful when setting up proxy service for the DRM connection, or if firewall rule modifications are needed when using an Infrastructure network connection.

Reference Link: Firewall Concerns for outbound EDP connections:

<https://www.digi.com/support/knowledge-base/firewall-concerns-for-outbound-edp-connections-to>

A Tablet's Mobile Hotspot or a Network Wi-Fi Access Point will typically provide the WVA a reliable network connection with internet access. A Wi-Fi Direct connection on the other hand is a point-to-point Wi-Fi connection between WVA and Tablet without internet access. A Digi Remote Manager connection can't be established without the Tablet providing proxy service for the DRM connection.

Note: A standalone proxy app (or proxy support built into a vehicle data monitoring program running on the Tablet) would need to provide internet access for traffic on TCP port 3199 to enable DRM access. Internet access to UDP port 123 (NTP) and UDP port 53 (DNS) would also be needed when in use, unless WVA access to NTP and UDP service are provided by applications on the Tablet.

Verifying Network Connectivity Status and Progress from the WebUI Home page

Reference Link:

https://www.digi.com/resources/documentation/digidocs/90001929/Default.htm#Task/T_config_open_webui_descriptions.htm

The WVA Home page shows important network information such as the WVA MAC and IP address, also the SSID, MAC, IP address, and the DNS server addresses which are in use. The Network Connectivity Status shows the progress of the network connection as the WVA establishes a network connection, then tunnels through the internet to connect to Digi Remote Manager

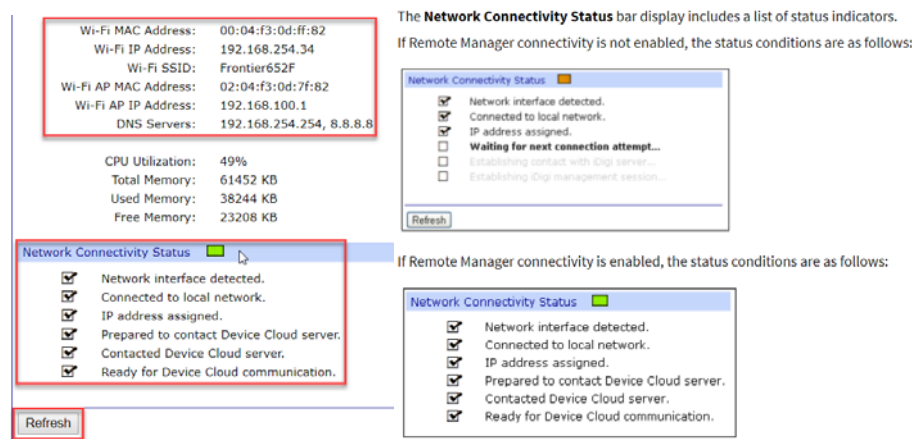


Figure 4-14: WebUI Home page – Network Status information

Network Connectivity Status: Orange = Not Ready / Green = Ready, Refresh updates the display

4.9 Issues with Python Script usage on the WVA

Reference Links:

Getting Started Guide:

https://www.digi.com/resources/documentation/digidocs/90001929/default.htm#Task/T_config_python.htm

Digi Python Mediawiki – WVA DataStream to Device Cloud Python Script Example:

http://cms.digi.com/resources/documentation/digidocs/90001537/Default.htm#references/r_wva_datastream_to_device_cloud.htm

Digi Github – python-wvalib – Python Library and CLI for Accessing WVA Functions:

<https://github.com/digidotcom/python-wvalib>

The WVA contains a Python 2.7 interpreter, which can be used to run powerful scripts that perform functions which aren't built into the product's OS/firmware. The ability to upload the data points coming into the WVA from the vehicle bus, via the internet to Digi Remote Manager where the data becomes part of data streams, is one such function as seen in the example below:

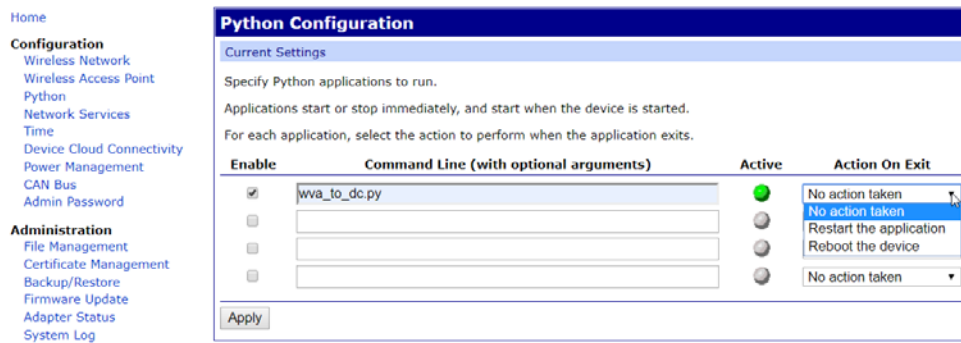


Figure 4-14: Python app wva_to_dc.py configured to upload vehicle data to Digi Remote Manager

In the example python configuration above, python script wva_to_dc.py's Action On Exit option is configured as "No action taken" if the script exits due to an exception or other error.

Python apps should never be used on a field-installed WVA until they are fully tested/debugged in a development environment first, then pass a small pilot test consisting of only a Truck or two parked in the company parking lot that are not in use with field operations. The script can be considered for widespread field use once the script has been fully tested/considered stable, and the operation/effect that the script has on a WVA are fully understood.

Technical Support Troubleshooting Guide – Wireless Vehicle Bus Adapter

Detection of Python Issues

An untested python script configured to Auto-start on a WVA may result in unpredictable behaviour:

- Configuring Action On Exit for “Restart the application” could result in a WVA CPU pegged at 100% usage (or with no available memory) if script is repeatedly crashing over and over
- Configuring Action On Exit for “Reboot the device” option can result in an inaccessible WVA due to the WVA being stuck in a reboot loop when python script starts, crashes (exits), reboots the WVA, on and on.

Factory Default of WVA using the reset switch method returns the WVA to a sane state. The factory default blanks out the Python Auto-start configuration of the WVA, making it possible to gain control of the WVA again. Factory default will not remove python file(s) – they remain in the File Management area under /WEB/python. Python app should be further developed/debugged/verified.

When the symptoms of a python issue aren't quite as obvious, debug info related to python script operation (or python-related issues) can be found in the Admin → System Logs area (see section 5)

4.10 Issues Receiving Vehicle Data: Alarm and Event Channel Usage

Reference links:

https://www.digi.com/resources/documentation/digidocs/90001929/Default.htm#Concept/C_web_interface_page_descriptions.htm

https://www.digi.com/resources/documentation/digidocs/90001930/default.htm#reference/r_webservices_dataflow.htm

https://www.digi.com/resources/documentation/digidocs/90001930/default.htm#reference/r_webservices_resource_index.htm

Vehicle data can be obtained from the WVA in several ways:

1. App can view vehicle data by doing GET of /ws web services data at WVA IP using a browser:
Example: <https://192.168.100.1/ws/vehicle/data/EngineSpeed>
2. App can subscribe to individual endpoints or all vehicle data, which is then received over the Event channel. Reference link:
https://www.digi.com/resources/documentation/digidocs/90001929/Default.htm#Task/T_demoapp_subscribe_to_endpoint.htm
3. App can configure an Endpoint as an Alarm, i.e. when alarm threshold is met, alarm is sent to Event channel. Reference link:
https://www.digi.com/resources/documentation/digidocs/90001929/Default.htm#Task/T_demoapp_configure_endpoint_as_alarm.htm

Information regarding what vehicle data endpoints are available and how to subscribe to those endpoints or configure an alarm for a given endpoint are available at preceding five Reference links above.

RE: Getting vehicle data using the “subscribe endpoint” vs. “subscribe alarm for endpoint” where WVA resource usage is concerned, subscribing an endpoint to an alarm uses less WVA CPU% usage than subscribing to the endpoint itself.

Technical Support Troubleshooting Guide – Wireless Vehicle Bus Adapter

Event Channel configuration:

In order to receive endpoint data about the vehicle, a Vehicle Data Monitoring app would establish a TCP socket connection to the configured Event Channel TCP port. WebUI Web Services → Event channel is disabled at Factory Default, with TCP port at 0/unconfigured.

For use, Event Channel must be enabled with a TCP port configured to an unused TCP Port number within useable range 1025 – 65535 (example below shows Event channel enabled on TCP port 5000):

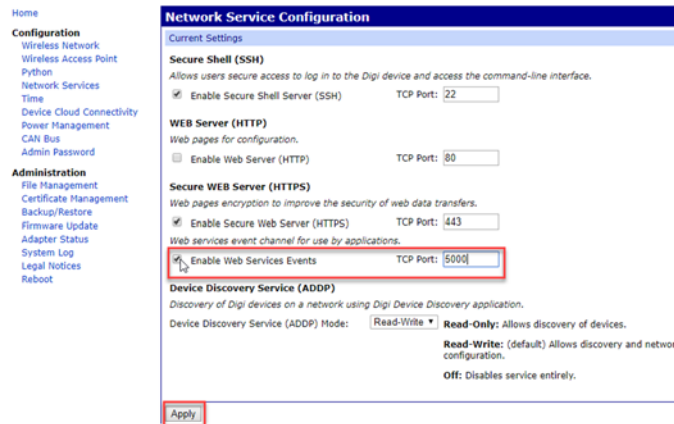


Figure 4-15: WebUI Web Services → Enabling Event channel service

The Event channel can also be configured from /ws web services with a PUT similar to this example:

PUT /ws/config/ws_events HTTP/1.1

Authorization: Basic

Content-Length: 66

Host: 192.168.100.1

Content-Type: application/xml

```
<ws_events>
  <enable>on</enable>
  <port>5000</port>
</ws_events>
```

Receiving Event data:

Once the Event channel is Enabled/configured for a TCP Port within the useable range, a persistent TCP socket connection should be established from the Tablet (where vehicle data monitoring app is located), to the Event channel TCP Port, in order to receive subscribed endpoint or alarm updates.

5 OBTAINING TROUBLESHOOTING DATA AND WVA LOGFILES

There are a number of different areas available to obtain WVA troubleshooting info:

- Web UI pages: Home and Adapter Status pages, System Logs
- Directly from WVA via API query - GET of various elements of /ws web services
- Remotely via Digi Remote Manager Properties page for the WVA – also Data Streams (if data is being sent to DRM via python script)

5.1 WebUI - Home page

The WebUI → Home page contains important info about a number of key WVA configuration areas and overall network/resource status in one location – manually refresh to update view:

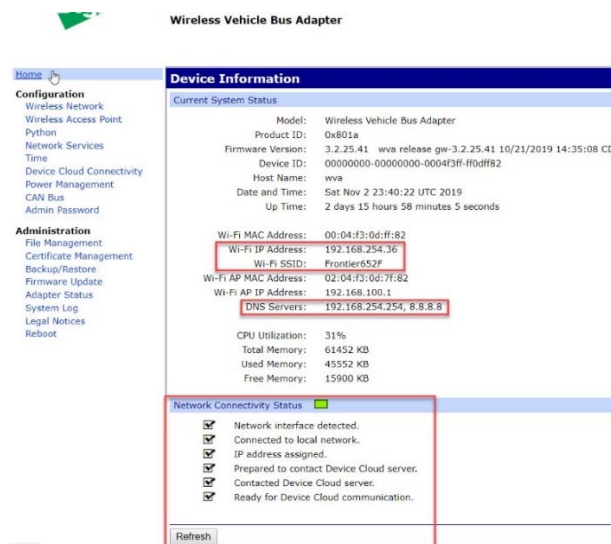


Figure 5-1: WebUI Home page – Current System Status, Network Connectivity Status

5.2 WebUI - Adapter Status

The WebUI → Admin → Status page contains some Wi-Fi connection-related info, as well as info about the vehicle and the amount of data coming in over each CAN bus:

Wireless Vehicle Adapter Status

Current Wireless Network Status

- Active SSID: Frontier652F
- Access Point: 28:80:88:69:0E:0E
- Signal Level: -50 dBm
- Link Quality: 60/70

Current Vehicle Status

- VIN: N/A
- Engine Speed: N/A
- Vehicle Speed: N/A

CAN Bus Statistics

Bus	Bytes Received	Packets Received	Bytes Sent	Packets Sent
can0	0	0	0	0
can1	0	0	0	0

Refresh Once Refresh Automatically
Automatic refresh requests a status update every 5 seconds.

Figure 5-2: WebUI Admin → Adapter Status page

5.3 WebUI - System Log areas

Reference: https://www.digi.com/resources/documentation/digidocs/90001929/Default.htm#Task/T_view_syslog.htm

System logs such as python.log*, digi.log*, and eventlog.txt* can be downloaded from the /WEB/python folder of Admin → File Management, or viewed live using the Admin → System Log File Browser shown in the example below (Get File button is used to load System Log files into the Log File Browser – Refresh button is used for updating the data being viewed in the Browser – Save All is used to copy the output to a file):

System Message Log File Browser

Log File

Select Log File: python.log Get File

Message Filters for Displayed Log File

☒ pylog

Clear All Mark All

Messages in Log File "python.log"

Refresh Save All

Nov 2 23:18:24	local17.info	pylog: 192.168.254.36, Frontier652F, 28:80:88:69:0E:0E, 2.412 GHz, -49 dBm, (3582, 100.00%), (3579, 99.92%), 3582, connected
Nov 2 23:19:28	local17.info	pylog: 192.168.254.36, Frontier652F, 28:80:88:69:0E:0E, 2.412 GHz, -49 dBm, (3583, 100.00%), (3580, 99.92%), 3583, connected
Nov 2 23:20:32	local17.info	pylog: 192.168.254.36, Frontier652F, 28:80:88:69:0E:0E, 2.412 GHz, -48 dBm, (3584, 100.00%), (3581, 99.92%), 3584, connected
Nov 2 23:21:36	local17.info	pylog: 192.168.254.36, Frontier652F, 28:80:88:69:0E:0E, 2.412 GHz, -47 dBm, (3585, 100.00%), (3582, 99.92%), 3585, connected
Nov 2 23:22:39	local17.info	pylog: 192.168.254.36, Frontier652F, 28:80:88:69:0E:0E, 2.412 GHz, -49 dBm, (3586, 100.00%), (3583, 99.92%), 3586, connected
Nov 2 23:23:43	local17.info	pylog: 192.168.254.36, Frontier652F, 28:80:88:69:0E:0E, 2.412 GHz, -48 dBm, (3587, 100.00%), (3584, 99.92%), 3587, connected
Nov 2 23:24:47	local17.info	pylog: 192.168.254.36, Frontier652F, 28:80:88:69:0E:0E, 2.412 GHz, -49 dBm, (3588, 100.00%), (3585, 99.92%), 3588, connected
Nov 2 23:25:51	local17.info	pylog: 192.168.254.36, Frontier652F, 28:80:88:69:0E:0E, 2.412 GHz, -48 dBm, (3589, 100.00%), (3586, 99.92%), 3589, connected

Figure 5-3: Use of Admin → System Log option to view logfiles in the Log File Browser

Technical Support Troubleshooting Guide – Wireless Vehicle Bus Adapter

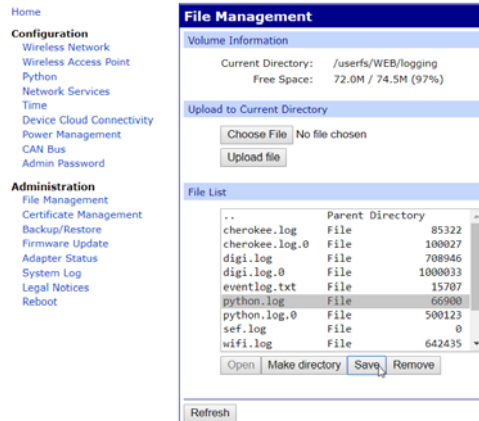


Figure 5-4: Downloading System Logs from /WEB/logging folder via Admin → File Management

5.4 Admin Tools: /ws web services information

Reference:

https://www.digi.com/resources/documentation/digidocs/90001930/default.htm#reference/r_webservices_resource_index.htm

Information regarding all aspects of WVA operation can be obtained using /ws web services.

Interfaces which specifically show information related to the WVA itself include: /hw, /state, /config, and/filesystem.

When a web services request is made of the WVA, the WVA will respond with the appropriate HTTP response. The page lists the possible HTTP response codes and their meanings:

Reference:

https://www.digi.com/resources/documentation/digidocs/90001930/default.htm#reference/r_webservices_http_response_codes.htm

5.5 Digi Remote Manager Properties pages:

Reference:

https://www.digi.com/resources/documentation/digidocs/90001930/default.htm#reference/r_webservices_resource_index.htm

Much information about WVA configuration settings and operation can be obtained through the Digi Remote Manager Properties pages, for WVA devices that are configured for Remote Management.

MAC Address	Device ID	Device Name	IP Address	Device Type	Description	Firmware Level	Health Status
00409D:848757	00000000-00000000-00409DFF-FF848757	...	192.168.43.130	Wireless Vehicle Bus Adapter		3.2.25.35	Unknown
0004F3:0DFF82	00000000-00000000-0004F3FF-FF0DFF82	...	192.168.254.32	Wireless Vehicle Bus Adapter		3.2.25.41	Unknown
0004F3:081AF8	00000000-00000000-0004F3FF-FF081AF8	...	192.168.254.39	Wireless Vehicle Bus Adapter		3.2.25.40	Unknown

Figure 5-5: DRM – Device Management → Devices view

Technical Support Troubleshooting Guide – Wireless Vehicle Bus Adapter

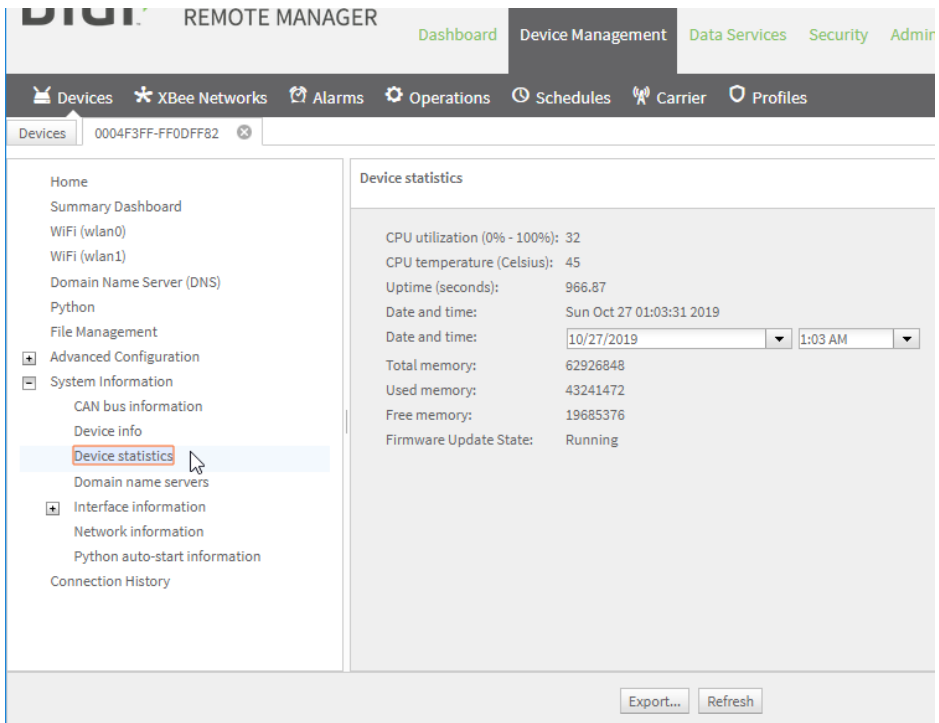


Figure 5-6: DRM- WVA Properties page – System Information – Device Statistics

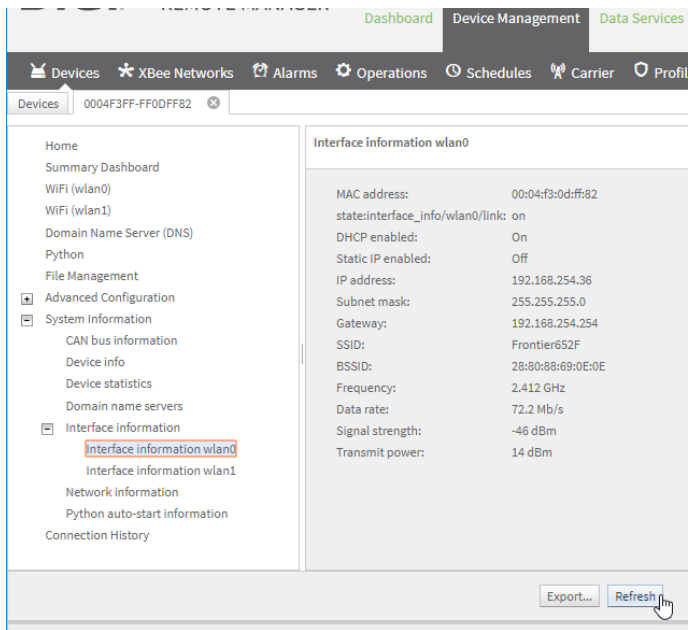


Figure 5-7: DRM- WVA Properties page – System Info – Interface Info – wlan0