Volvo Car USA LLC **Technical Journal**

Technical Journal Title Unintentional VIDA Wi-Fi Connection Leading to 12V Battery Drain		Ref. No. TJ 36426.1.2	
Issuer (Dept.) Technical Service		Issue Date 1/4/24	Status Date 1/4/24
Car Market United States and Canada	Partner 3 US 7510 Volvo Car USA	Function Group 3111	
Function Description Battery, complete		Page Page 1 of 52	

Attachment

File Name	File Size
Service Journal 1000046.pdf	1.8612 MB
Service Journal 32310.pdf	0.0762 MB
Stethoscope.jpg	0.0703 MB
VOE Adapter Plugged-In.png	0.7915 MB

Rows beginning with * are modified
Note! If using a printed copy of this Technical Journal, first check for the latest online version.

DESCRIPTION:

TCAM = Telematics Connectivity Antenna Module

Vehicles equipped with a TCAM can unintentionally populate in VIDA through Wi-Fi connection. When this happens, the 12V battery can drain.

Please follow the steps under Service.

CSC Customer Symptom Codes

Code	Description
LM	12 V main battery/Dead battery
LN	12 V main battery/Weak or low electrical power

DTC Diagnostic Trouble Codes

Vehicle Type

Type	Eng	Eng Desc	Sales	Body	Gear	Steer	Model Year	Plant	Chassis range	Struc Week Range
224							2023-9999		-	202222-999952
225							2023-9999		-	202222-999952
227							2023-9999		-	202222-999952
235							2022-9999		-	202122-999952
236							2022-9999		-	202122-999952
238							2022-9999		-	202122-999952
246							2022-9999		-	202122-999952

Type	Eng	Eng Desc	Sales	Body	Gear	Steer	Model Year	Plant	Chassis range	Struc Week Range
256							2023-9999		-	202222-999952
536							2021-9999		-	202037-999952
539							2022-9999		-	202139-999952

SERVICE:

Software Solution was made available with V2.8 SW, which was released 23w16. Please ensure vehicle is on V2.8+ SW.

CCD = Center Console Display

In order to avoid unintentional connections to VIDA Wi-Fi, please note the following:

1. Leave the vehicle in Transport mode as long as possible (until the vehicle is ready for delivery)

THIS IS THE MOST EFFECTIVE WAY TO PREVENT UNINTENTIONAL VIDA WI-FI CONNECTIONS AND 12V BATTERY DRAIN

If you must take the vehicle out of Transport mode (therefore placing it into Normal mode), please note the following:

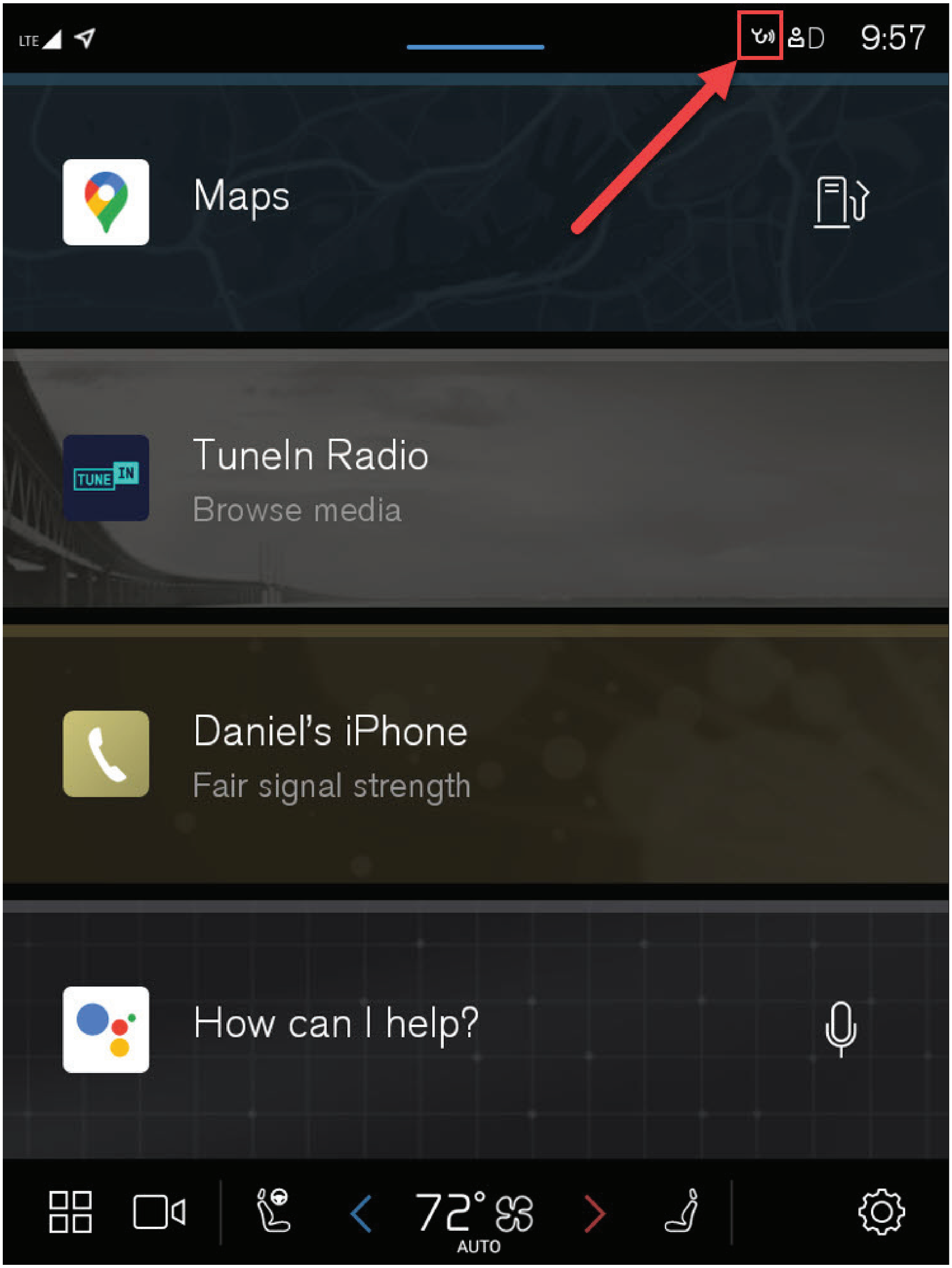
1. The vehicle will attempt to connect to VIDA Wi-Fi whenever the LOCK button on the key fob is pressed 3 or more times repeatedly.
   a. To prevent unintended activation of VIDA Wi-Fi (and therefore unintended 12V battery drain), do NOT press the LOCK button 3 times consecutively (as is often done when retailer personnel are trying to locate a vehicle)
2. A stethoscope icon will appear in the top-right corner of the CCD (see attached “Stethoscope.png”) when the vehicle is attempting to connect (or has already successfully connected) to VIDA Wi-Fi
3. In order to disconnect VIDA Wi-Fi, you have 3 options:
   a. Plug a VOE adapter (PN 9513108 OR PN 9513062 from Service Journal 32310) into the OBD-II port for 5 seconds—**no computer connection is necessary**
      i. Reference attached picture “VOE Adapter Plugged-In.png”
   b. Connect the vehicle to VIDA (manually or through VIDA Wi-Fi) and then Disconnect from VIDA (according to Service Journal 1000046)
   c. Drive the vehicle out of range of the Wi-Fi access point

Note: This is valuable information for everyone in the retailer (especially the sales team)—please share this information!

VEHICLE REPORT:

Yes, please submit a Vehicle Report if the service solution described in this TJ has no effect. Use concern area “Vehicle Report” and sub concern area “Support needed”, use function group 3113.

To view TJ attachments continue to next page. This TJ has four attachments.



LTE
9:57
Maps
TuneIn Radio
Browse media
Daniel's iPhone
Fair signal strength
How can I help?
72°
AUTO

Service Journal 32310 - Version 1

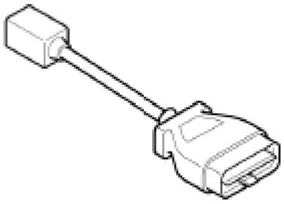
9513108 VOE Adapter

Tools & Equipment - Diagnostic Tools

VOE Adapter updated.
9513108 VOE Adapter replace 9513062 VOE Adapter.
Adapter for onboard diagnostic (OBD).

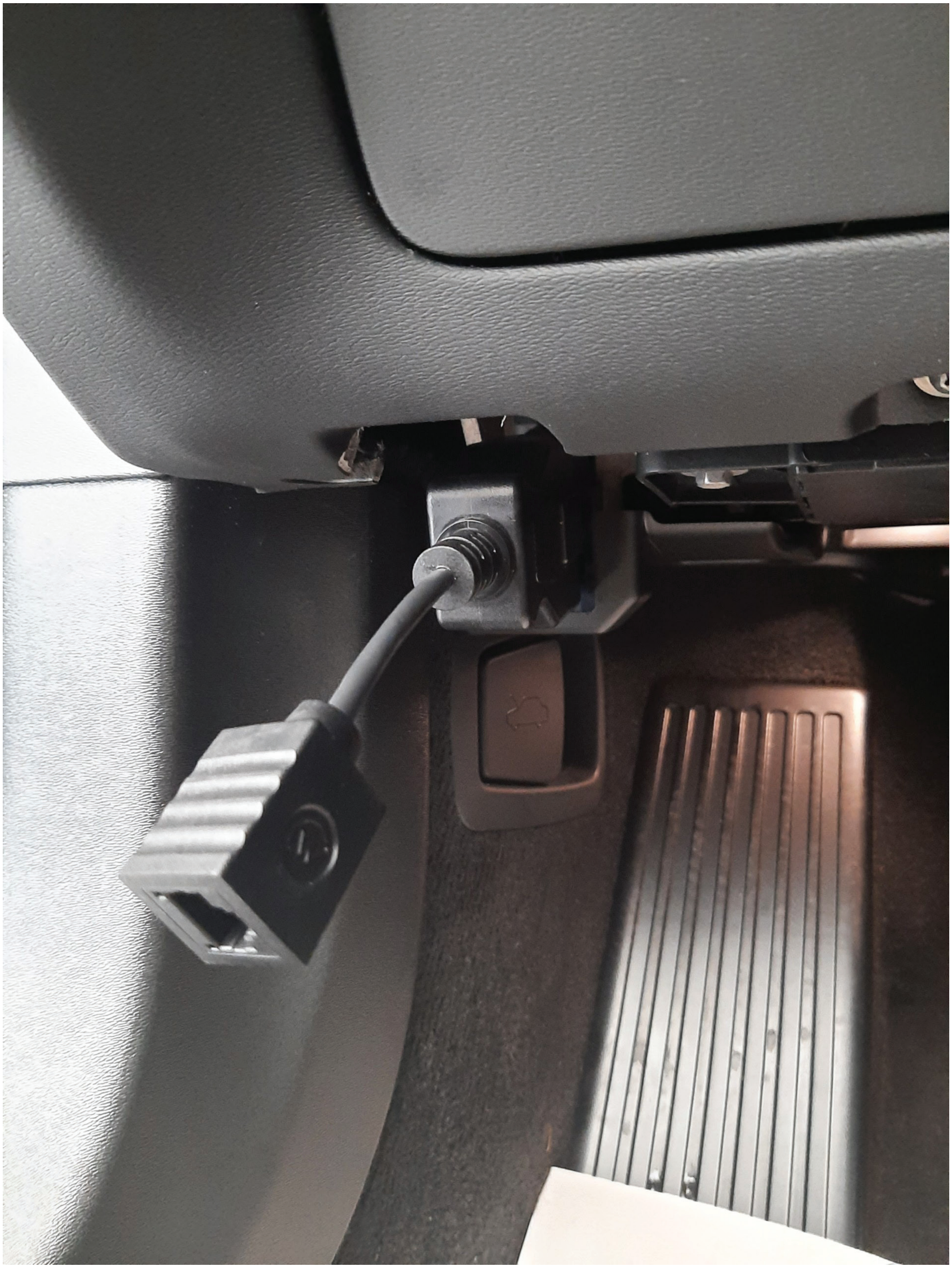
Use 9513108 for software download.

9513062 can still be used for other work/readouts on cars.



Ulf Ljungberg - Jan 23, 2017 06:50

Volvo Car Corporation



VOLVO CARS GLOBAL WI-FI SERVICE

CONTENTS

SUPPORT DOCUMENT FOR HELPDESKS

1 TARGET GROUPS FOR THIS DOCUMENT

Support organizations that are involved in supporting dealers using Volvo Cars Global Wi-Service, both during and after the implementation of the service.

2 PURPOSE OF THIS DOCUMENT

The purpose of this document is to, on the one hand, give the helpdesks an insight about new functionalities in VIDA & VIDA Admin and Workshop Wi-Fi functionality is added to the systems and, on the other hand, to guide through the Fault Tracing of eventual Symptom.
Do not print this document since it might be updated regularly and the document also contains links to other sections within the document.

3 THE VOLVO CARS GLOBAL WI-FI SERVICE

3.1 Overview

Volvo Cars, as an industry leader in car connectivity, has developed a Wi-Fi service designed to match with its connected car infrastructure and requirements for Wi-Fi connectivity.

This Wi-Fi service contains two different Wi-Fi connections:

- **Volvo Cars Diagnostic Wi-Fi (mandatory) SSID = VCCarDW**
    - Connects the car to the dealer's local network.
    - Enables a new and very efficient process for diagnostic and downloads at Volvo workshops.
- **Volvo Cars Vehicle Connectivity Wi-Fi (optional) SSID VCVCW**
    - Connects the car to Internet using the dealer's local network.
    - Provides dealers with a very simple and efficient way to demonstrate connectivity features in the showroom
    - Prepares connected cars for delivery to customer.

The Volvo Cars Global Wi-Fi service will be delivered as a mandatory subscription for the dealer. The service includes a set of pre-configured access points to be installed at the dealership for extending the IT infrastructure at dealerships.

3.2 TIE Service Journals for Volvo Cars Global Wi-Fi Service

SJ 1000046- Support document for Helpdesks - Volvo Cars Global Wi-Fi Service

Target groups for this SJ:
Support organizations that are involved in supporting dealers using Volvo Cars Global Wi-Service, Both during and after the implementation of the service.

SJ 1000044 - Volvo Cars Global Wi-Fi Service – Basic Fault Tracing – VIDA and Vehicle.
Target groups for this SJ:
For dealers for initial troubleshooting prior writing a report as for helpdesks to ensure everything has been done to exclude the vehicle itself as the reason for a fault.
Also to be used by all supporting Volvo Cars Global Wi-Fi Service.

SJ 1000045 - Technical overview and design - Volvo Cars Global Wi-Fi Service

Target group of this SJ:

The aim of the attached document in this SPJ is to provide extensive and in-depth knowledge about the Volvo Cars Global Wi-Fi Service. It provides information on requirements for the Wi-Fi service and how to adapt an existing dealership network to dealership Wi-Fi. The primary target group is IT technicians at the dealerships and/or NSCs.

SJ 1000039- Verification Tool - Volvo Cars Global Wi-Fi Service

Target group of this SJ:

Is intended to be used by the IT department or the IT partner at the dealership. When preparing an order for the Volvo Cars Global Wi-Fi Service the tool is helpful to verify compliance with the requirements on the IT infrastructure.
It can later on also be used for fault tracing when there is a need to check that the IT infrastructure is still supporting Volvo Cars Global Wi-Fi Service, or not.

SJ 1000040- Validation Tool - Volvo Cars Global Wi-Fi Service

Target group of this SJ:

Is intended to be used by the NSC to verify the XML file created by the Verification Tool by the dealer when placing an order for Volvo Cars Global Wi-Fi Service or when there is an issue after an implementation.

SJ 1000038 - Introduction - Volvo Cars Global Wi-Fi Service

Target group of this SJ:
To be used by all as an introduction to Volvo Cars Global Wi-Fi Service

SJ 1000049- Wi-Fi Self-assessment and test report - Volvo Cars Global Wi-Fi Service

Target group of this SJ:

To be used by workshops that have installed the service.
It will include a list of tests that should be done in order to verify the service.

3.3 Requirements and Standards

In order to ensure the functionality, it is necessary to ensure that below requirements have been fulfilled.

SJ – 1000692 - Workshop System Requirements & Guidelines - VIDA in 2015 (Dealers)

Also ensure that the latest version of VIDA Prerequisite is installed.

For users in countries except for China, the latest version can be downloaded here:
http://vidainstaller.volvocars.biz/client-installer/VIDASetup.exe

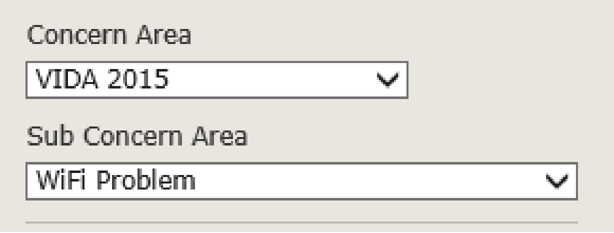
For users in China, the latest file can be downloaded here:
http://vidainstaller-cncc.volvocars.biz/client-installer-cn/VIDACNSetup.exe

Notes:
The installation requires that you are logged in as an Administrator on your computer.

The computer might restart after the installation and the installation might continue after the restart.

4 HOW TO ESCALATE MAJOR ISSUES

If **many workshops suddenly experience issues at the same time** when using Volvo Cars Global Wi-Fi Service, then it is most likely caused by an ongoing major incident.
Please then forward feedback from affected workshops by forwarding TIE reports to central using below Concern Are and Sub Concern Area.



Concern Area: VIDA 2015

Sub Concern Area: WiFi Problem

Please ensure that the following information is included in the TIE-report.

Description of the issue and business impact, e.g.

- Vehicles does not appear in VIDA.
- Vehicle can be found in VIDA, but an error occurs when trying to connect to the vehicle.
- Other than above.

Please describe the symptom as clear as possible with impact.

- Number of workshops affected.
- Time of occurrence (date and time.)
- If the vehicle appears in VIDA, but an issue occurs when trying to connect to the vehicle, then also attach below log files created by VIDA.

✓ **VIDAusername_VIN.log**
✓ **VIDAusername_VIDATrace.log**

Examples of:

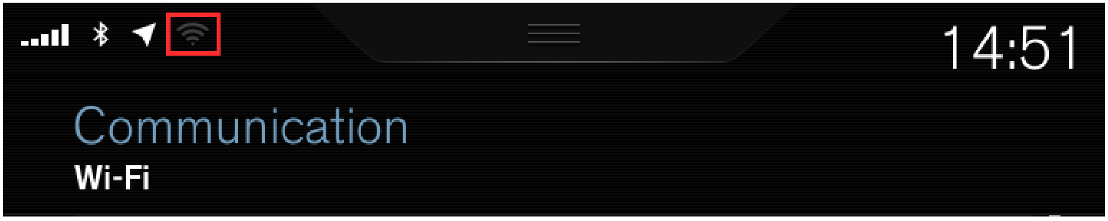
- Network names according to Meraki (e.g SE-STO-6SE1234)
- Partner IDs according to VIDA Admin (e.g 6SE1234)
- VIN numbers if available.

5 HOW TO CONNECT

To establish a Wi-Fi connection between the vehicle and VIDA the technician or service advisor needs to enable the functionality in the vehicle first.

This is done by clicking the lock-button of the remote-key 3 times in range of the vehicle. Those 3 clicks needs to be done within 5 seconds and minimum 1 second between each click.

A Wi-Fi symbol will then first appear in the CCD in grey according to below example

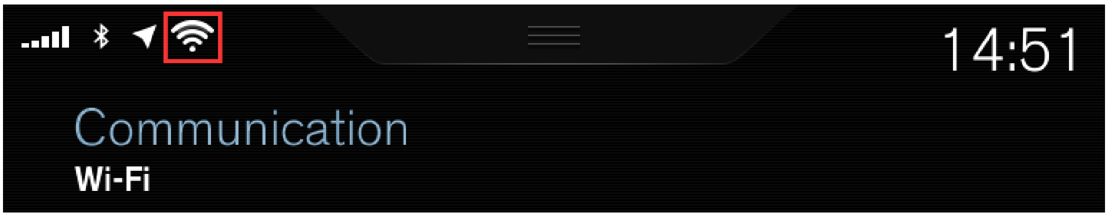


14:51

Communication

Wi-Fi

The Wi-Fi symbol will after 5-10 seconds change from grey to white when a successful connection has been established.



14:51

Communication

Wi-Fi

This sequence will be recognized by the vehicle. When the infrastructure is set up accordingly to the requirements and the vehicle is in range of Wi-Fi coverage, it then will be displayed and available in VIDA´s "Connected Vehicles" tab.

Notes

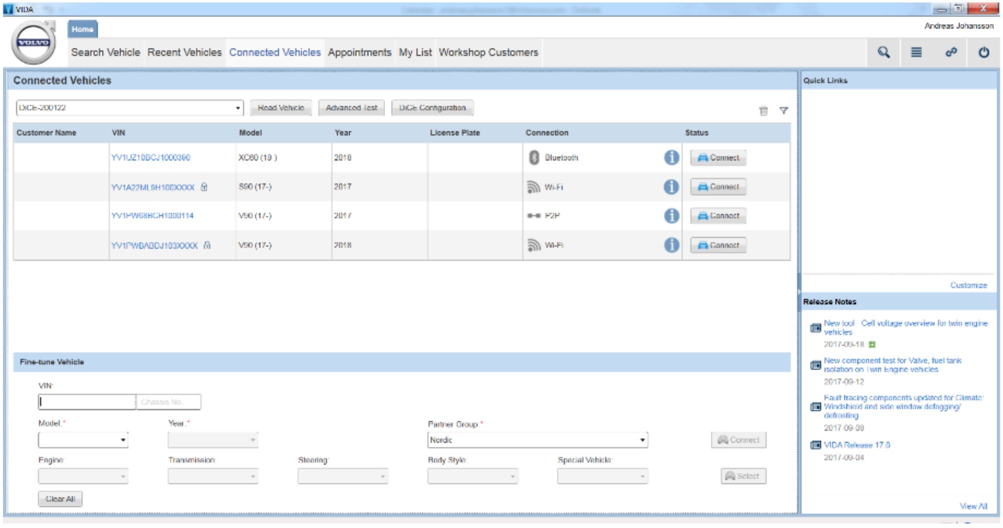
The vehicle will in VIDA remain in the "Connected Vehicles" tab for 20 minutes, if no session is started by VIDA within this time the vehicle will disconnect from the Wi-Fi.

A Dice or a VOE Adapter used for P2P cannot be connected to the vehicle since that will disable the Wi-Fi feature.

6 VIDA

6.1 Wi-Fi connected vehicles

Wi-Fi connected vehicles will appear in the "Connected Vehicles" tab with a Wi-Fi symbol in the connection column.
After the vehicle has established a connection to the Volvo Cars Diagnostic Wi-Fi service, it will take about 10-15 sec until the vehicle appears in VIDA.



Connected Vehicles

DiCE-200122

Customer Name	VIN	Model	Year	License Plate	Connection	Status
	YV1UZ10BCJ1000390	XC60 (18-)	2018		Bluetooth	Connect
	YV1A22ML9H100XXXX	S90 (17-)	2017		Wi-Fi	Connect
	YV1PW68BCH1000114	V90 (17-)	2017		P2P	Connect
	YV1PWBABDJ103XXXX	V90 (17-)	2018		Wi-Fi	Connect

Fine-tune Vehicle

VIN: Chassis No.

Model: * Year: * Partner Group: * Nordic

Engine: Transmission: Steering: Body Style: Special Vehicle:

Release Notes

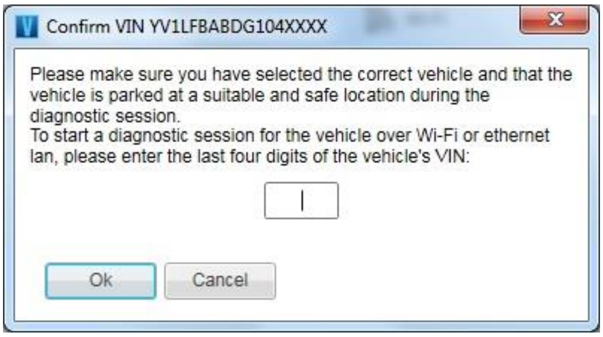
New tool - Cell voltage overview for twin engine vehicles
2017-09-18

New component test for Valve, fuel tank isolation on Twin Engine vehicles
2017-09-12

Fault tracing components updated for Climate: Windshield and side window defogging/defrosting
2017-09-08

VIDA Release 17.8
2017-09-04

By clicking the "Connect"-Button the connection a pop-up window will appear where the last 4 digits of the Vehicle Identification Number (VIN) of the specific car needs to be entered.



Confirm VIN YV1LFBABDG104XXXX

Please make sure you have selected the correct vehicle and that the vehicle is parked at a suitable and safe location during the diagnostic session.
To start a diagnostic session for the vehicle over Wi-Fi or ethernet lan, please enter the last four digits of the vehicle's VIN:

The VIN of a vehicle available via Wi-Fi is not totally displayed. The full VIN number can be looked up via DMS, TIE, vehicle papers or on the vehicle directly.

When the connection has been established the technician is able to do most of the work like (readout, software download, fault tracing, etc.) instead of using a cable-connection.

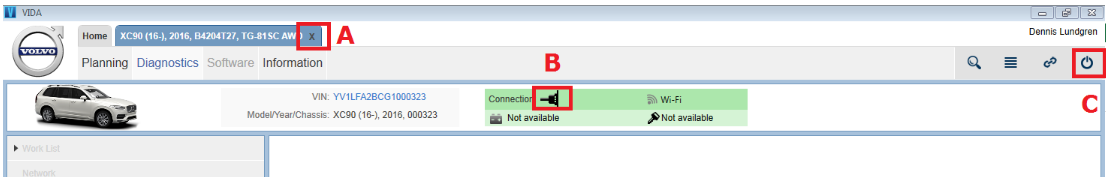
Note

Reload of VCM should not be performed via Wi-Fi since it will not be possible to establish a Wi-Fi connection due to lack of certificates in the ECU. Instead an Ethernet Cable (P2P) needs to be used.
Replacement of CEM need to be performed by using Ethernet Cable (P2P).

6.2 How to disconnect

To close an active connection with a vehicle the technician can do the following:

A) Close vehicle – tab
B) Select the Connection symbol
C) Close VIDA



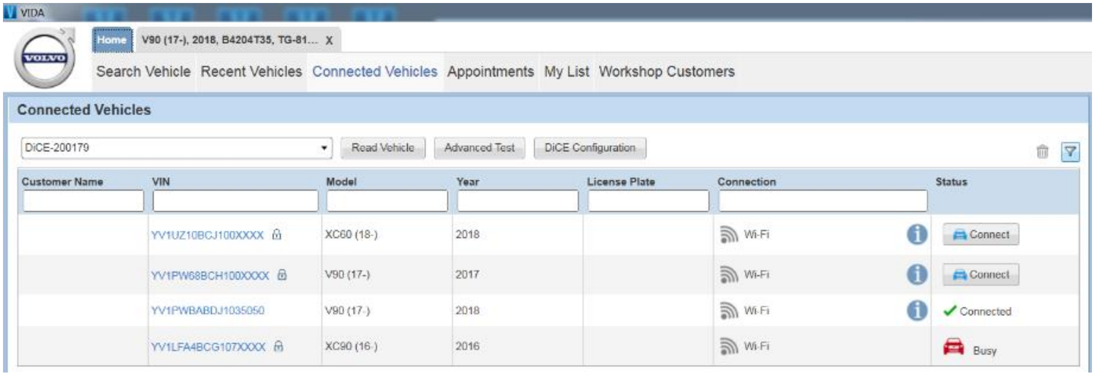
Note

A secure disconnect is required otherwise the vehicle will remain in a connected – mode and the battery of the vehicle might drain.

It is also important to disconnect vehicles when ready with them to avoid too many vehicles in the Connected-Vehicle Tab.

6.3 How to filter

The filter functionality in VIDA can be helpful when there are a lot of (Wi-Fi available) vehicles on-site at the dealership.



Customer Name	VIN	Model	Year	License Plate	Connection	Status
	YV1UZ10BCJ100XXXX	XC60 (18-)	2018		Wi-Fi	Connect
	YV1PW68BCH100XXXX	V90 (17-)	2017		Wi-Fi	Connect
	YV1PWBABDJ1035050	V90 (17-)	2018		Wi-Fi	✓ Connected
	YV1LFA4BCG107XXXX	XC90 (16-)	2016		Wi-Fi	Busy

It is possible to filter for:

- Customer Name
- VIN
- Model
- Year
- License Plate
- Connection (type)

7 VIDA ADMIN

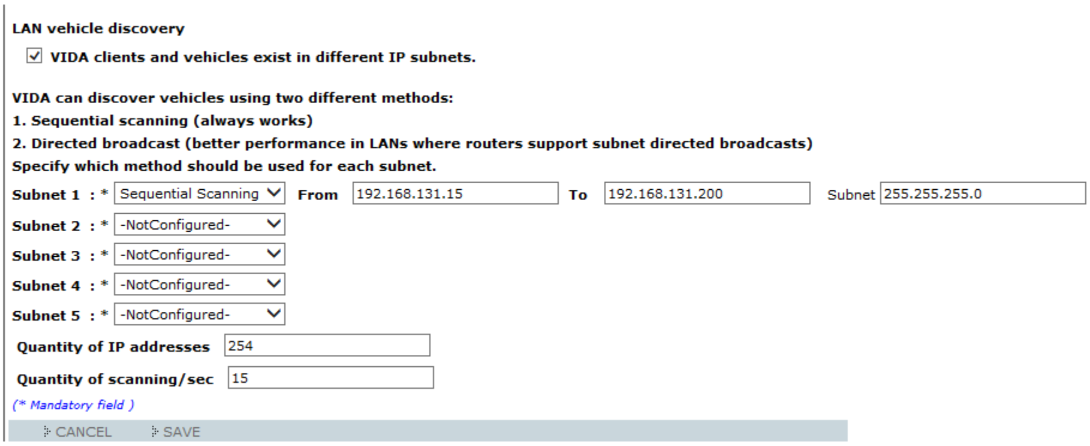
7.1 What are the functionalities in VIDA Admin?

VIDA clients and cars can be located in different IP subnets. Therefor the new functionality in VIDA Admin is needed, to set the IP settings according to the dealer network, when VIDA clients and vehicle are located in different networks/subnets.

More information can be found in:

SPJ 34226 - Technical overview and design - Volvo Cars Global Wi-Fi Service

VIDA needs to be restarted after any changes have been done in VIDA Admin in order for the changes to take effect in VIDA.



LAN vehicle discovery

☑ **VIDA clients and vehicles exist in different IP subnets.**

VIDA can discover vehicles using two different methods:
1. Sequential scanning (always works)
2. Directed broadcast (better performance in LANs where routers support subnet directed broadcasts)
Specify which method should be used for each subnet.

Subnet 1 : *	Sequential Scanning	**From**	192.168.131.15	**To**	192.168.131.200	Subnet	255.255.255.0
Subnet 2 : *	-NotConfigured-						
Subnet 3 : *	-NotConfigured-						
Subnet 4 : *	-NotConfigured-						
Subnet 5 : *	-NotConfigured-						

Quantity of IP addresses 254

Quantity of scanning/sec 15

(Mandatory field)*

8 ACCESS POINTS

8.1 Prerequisites

Access Points mounted at correct location and connected according to the installation Guide.

During normal working conditions, the LED indicator on the AP will be:

- Green - AP in Gateway mode with no clients
- Blue - AP in Gateway mode with clients

Led patterns that will require actions:

- Blinking Orange - AP can't find uplink
- Led not lit – No power supply or broken AP

Other LED patterns that doesn't require any actions:

- Orange - AP is booting
- Rainbow - AP is initializing/scanning
- Blinking Blue - AP is upgrading

8.2 How to fault trace and determine if an AP is broken or not.

(AP is not active according to Meraki Dashboard)

Symptom 1 – LED is not lit on AP:

1. **Test of PoE/PoE injector.**

   Locate the Switch or PoE injector to where the non-functional AP is connected to.
   Disconnect the ethernet cable used for the none functional AP at the Switch or PoE injector and move it to another ethernet outlet that has been connected to a functional AP.

   a. LED on the AP starts now starts to lit:
      Meaning that the ethernet cable between the AP and the Switch or PoE Injector is OK.
      But there is an issue with the power supply from the Switch or the PoE injector where the AP was previously connected to.

   b. LED on the AP is still not lit:
      Continue checkpoint 2.

2. **Test of Ethernet Cable**
   (Checkpoint 1 has been followed and LED on the AP is still not lit)

   Move the non-functional AP and connect it to an Ethernet cable that has been connected to a functional AP.

   a. LED on the AP starts now start to lit:
      The ethernet cable initially used for the none working AP is broken.
      Replace the ethernet cable and try again.

   b. LED on the AP is still not lit:
      The AP seems to be broken and should maybe be replaced.
      See How to request a replacement of a broken AP
      Note, Reconnect the non-functional AP in case it will be possible, and a need to perform further fault tracing.

- **Symptom 2 – The LED will permanently remain lit with Orange color.**

1. Disconnect and Connect the Ethernet cable connected to the none functional AP in order to restart the AP.

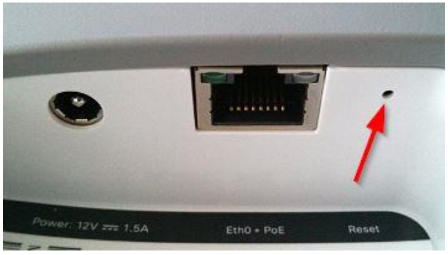
   a. The LED will now go from permanently Orange *(during startup)* to either green or blue. The AP seems to be OK and something unexpected happened during previous start-up of the AP.
   Wait 5-10 minutes and check the status of the AP in Meraki dashboard.

   b. *(Checkpoint 1 has been followed but the LED on the AP is still permanently lit with orange color.*

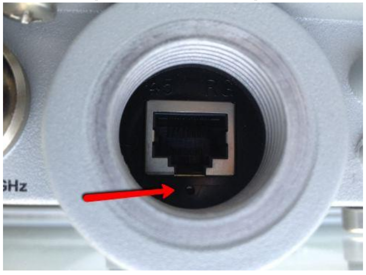
   Perform a factory reset of the AP while connected to power supply:

   Cisco Meraki devices can be reset to factory defaults using the reset button on the device. This requires a paper clip or object with a long thin tip. Insert the tip of the paper clip into the reset button, press, and hold it until the LED light turns off.

   The reset button is located adjacent to the power and Ethernet ports on the AP. Exact location will vary by model. Example for model:
   MR33 (Indoor AP)



   MR72 (Outdoor AP)

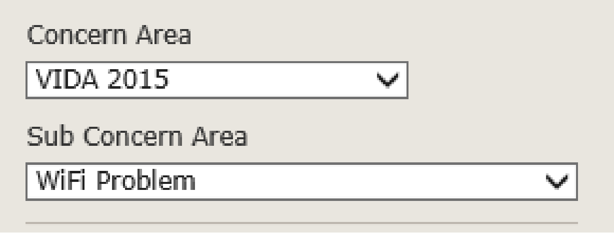


   This will reset the device to factory defaults and reboot. Please be patient as this could take up to 5 - 10 minutes. If the reset resolved the issue, then the light of the LED will finally switch to either green or blue.

   c. *(Checkpoint 1 and 1b has been followed but the LED on the AP is still permanently lit with orange color.*
   The AP seems to be broken and should maybe be replaced.
   See [How to request a replacement of a broken AP]
   Note, Reconnect the non-functional AP in case it will be possible, and a need to perform further fault tracing.

8.3 How to request a replacement of a broken AP.

Create and forward a TIE report to central using below Concern Are and Sub Concern Area.



Concern Area
VIDA 2015

Sub Concern Area
WiFi Problem

Include the following information in the free text field in case the AP will be replaced.

- Partner ID of the affected workshop.
- Serial number of the none working AP.
- Full company address to where a new AP could be delivered to.
- Name to a contact person.
- Email to the contact person.
- Phone number to the contact person.
- Optional, special instructions from the workshop and where to pick up the none functional access point. Such as time or special place for the pickup.

Also include the check list that is available in the same Service Journal as this document (Service Journal 1000046)

Updated 2020-11-25 – ***AP-Check-List - Volvo Cars Global Wi-Fi Service-ver1.xlsx*** has been replaced by ***AP-Check-List - Volvo Cars Global Wi-Fi Service-ver2.docx***

AP-Check-List - Volvo Cars Global Wi-Fi Service-ver2.docx will now also have input fields for additional information that needs to be included.

The checklist is based on the checks that is being described in this document according to 7.2 How to fault trace and determine if an AP is broken or not.

8.4 Return instruction for a none functional Access point.

Communication cornering replacement of a none functional access point will be done in the TIE report that has been sent to central concerning the none functional access point.

A none functional access point will be replaced with the same or equivalent model supporting the same functionality.

The none functional access point should be returned within 30 days after the new access point has been received.

Courier might contact the workshop before pickup depending on rules/country.

How to return the none functional access point.

- A prepaid return label will become available in the TIE report concerning the none functional access point or in the box that will be shipped with the new access point. Some other documents that also needs to be included in the return might also be sent from central depending on requirements /country.

- Date for the pick-up of the none functional access point will be communicated from central in the TIE report.

- The none functional access point should be placed in the same box that arrived with the new access point.)

- Seal the box and place the return shipping label on the box.

- Please also note the tracking number on the return label if a tracking number exists. Required in case there is a need to track the return.

9 MERAKI DASHBOARD

Request to access to Meraki Dashboard can be found in TIE SPJ 33048.

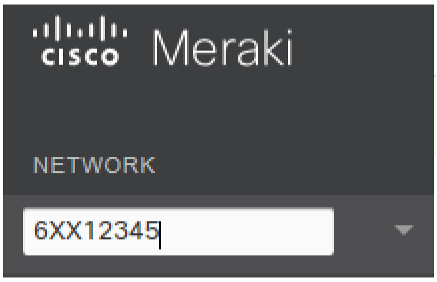
Login URLs for Meraki Dashboard:

When supporting workshops other than China. https://dashboard.meraki.com

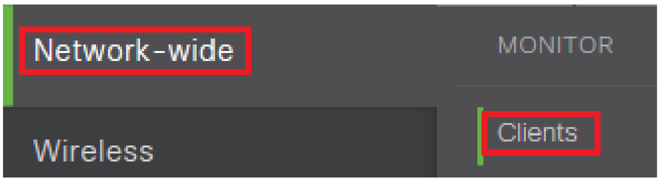
When supporting workshops in China. https://dashboard.meraki.cn

Below will only show some basic steps and what to look for in Meraki Dashboard when there is a need to perform fault tracing.

Enter the Partner ID that you would like to look at and select the workshop after it is shown under the search field.

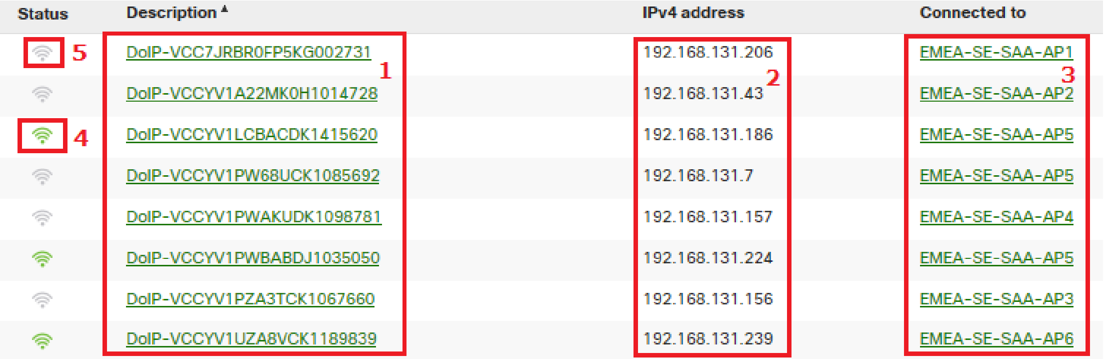


Then select Network-wide > Clients.



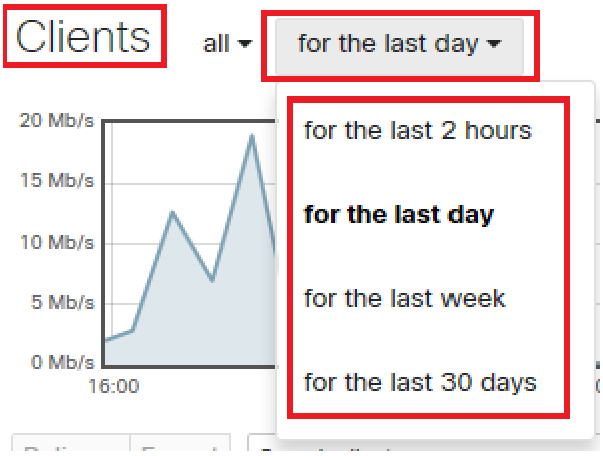
You will now see a view that will show what clients that have been connected to APs used for "Volvo Cars Global Wi-Fi Service"

(1) **DoIP-VCC**XXXXXX means that the client is a vehicle.
(2) The IP address provided for the vehicle.
(3) What AP the vehicle is or has been connected to.
(4) The vehicle is connected.
(5) The vehicle is no longer connected.

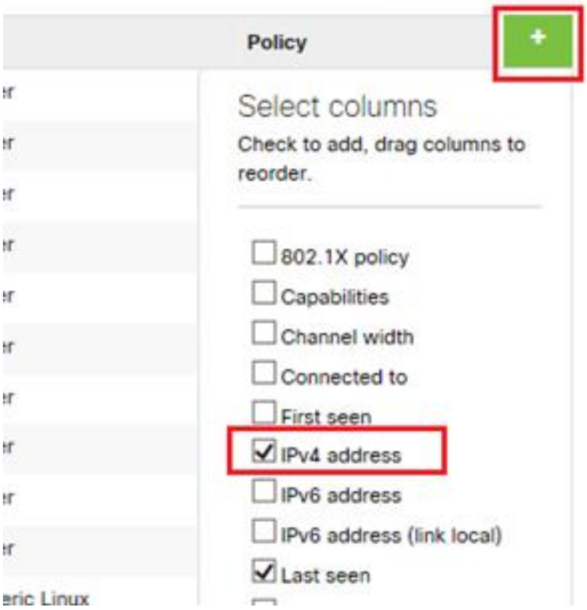


Status	Description ▴	IPv4 address	Connected to
	DoIP-VCC7JRBR0FP5KG002731	192.168.131.206	EMEA-SE-SAA-AP1
	DoIP-VCCYV1A22MK0H1014728	192.168.131.43	EMEA-SE-SAA-AP2
	DoIP-VCCYV1LCBACDK1415620	192.168.131.186	EMEA-SE-SAA-AP5
	DoIP-VCCYV1PW68UCK1085692	192.168.131.7	EMEA-SE-SAA-AP5
	DoIP-VCCYV1PWAKUDK1098781	192.168.131.157	EMEA-SE-SAA-AP4
	DoIP-VCCYV1PWBABDJ1035050	192.168.131.224	EMEA-SE-SAA-AP5
	DoIP-VCCYV1PZA3TCK1067660	192.168.131.156	EMEA-SE-SAA-AP3
	DoIP-VCCYV1UZA8VCK1189839	192.168.131.239	EMEA-SE-SAA-AP6

Default you will see the status for the last day.
But it can be changed by using below option.



If the column IPv4 address or any other column is missing, then it can be added by selecting the Plus sign according to below.

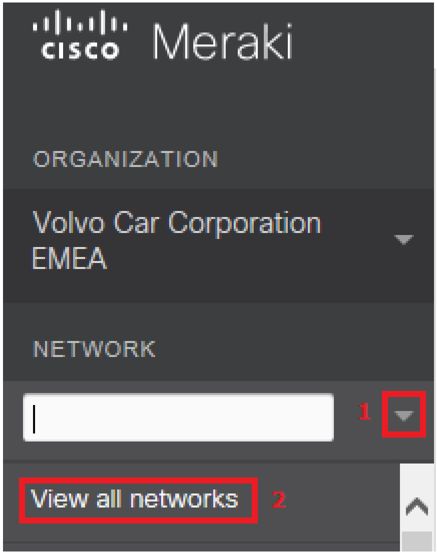


Check to add, drag columns to reorder.

- □ 802.1X policy
- □ Capabilities
- □ Channel width
- □ Connected to
- □ First seen
- ☑ IPv4 address
- □ IPv6 address
- □ IPv6 address (link local)
- ☑ Last seen

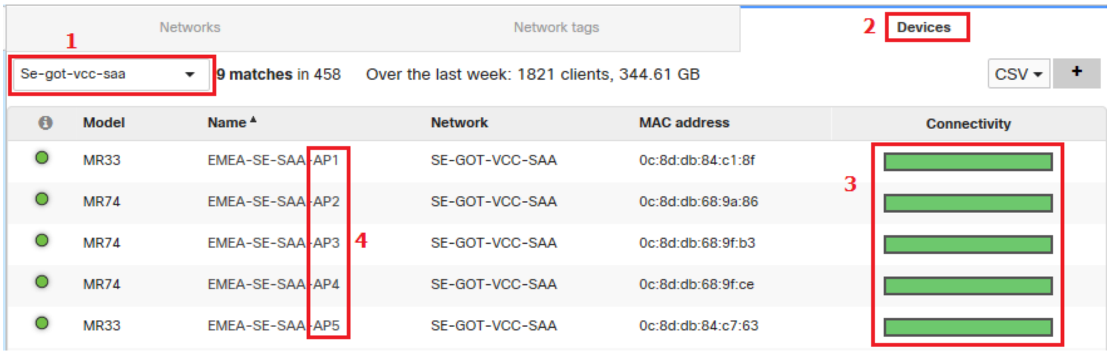
You can also see the status of all access points for a workshop and their history and current status towards the cloud used for "Volvo Cars Global Wi-Fi Service"

First, select below options:



Next:

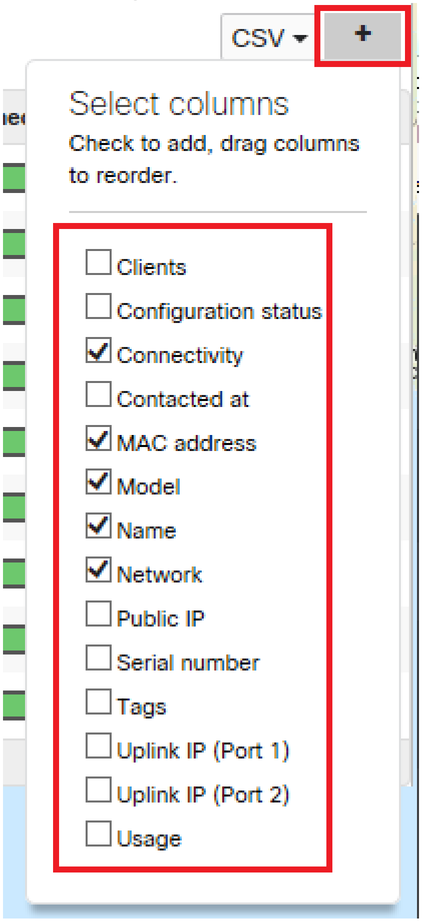
(1) Enter the Partner ID for the workshop that you would like to check.
(2) Select "Devices".
(3-4) Then you will see status for each access point and for that last week.



9 matches in 458 Over the last week: 1821 clients, 344.61 GB

	Model	Name ▲	Network	MAC address	Connectivity
●	MR33	EMEA-SE-SAA-AP1	SE-GOT-VCC-SAA	0c:8d:db:84:c1:8f	🟩
●	MR74	EMEA-SE-SAA-AP2	SE-GOT-VCC-SAA	0c:8d:db:68:9a:86	🟩
●	MR74	EMEA-SE-SAA-AP3	SE-GOT-VCC-SAA	0c:8d:db:68:9f:b3	🟩
●	MR74	EMEA-SE-SAA-AP4	SE-GOT-VCC-SAA	0c:8d:db:68:9f:ce	🟩
●	MR33	EMEA-SE-SAA-AP5	SE-GOT-VCC-SAA	0c:8d:db:84:c7:63	🟩

If any column is missing, then it can be added by selecting the + sign icon according to below.



Select columns

Check to add, drag columns to reorder.

- □ Clients
- □ Configuration status
- ☑ Connectivity
- □ Contacted at
- ☑ MAC address
- ☑ Model
- ☑ Name
- ☑ Network
- □ Public IP
- □ Serial number
- □ Tags
- □ Uplink IP (Port 1)
- □ Uplink IP (Port 2)
- □ Usage

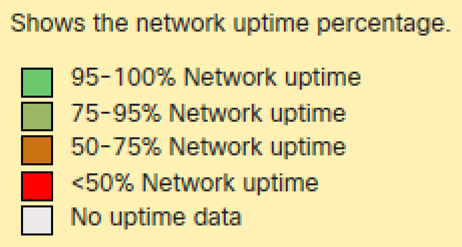
10 FAULT TRACING – VEHICLE(S) DOES NOT APPEAR IN VIDA

10.1 Vehicle(s) does not appear in VIDA after locking the vehicle 3 times.

You are recommended to start by using Fault Tracing Chart
The “Fault Tracing Chart” will have links to below sections 9.1.1 – 9.1.6 that will include more details if needed.

10.1.1 Are all Access Points (AP) that are expected to operate showing green or not in Meraki Dashboard?

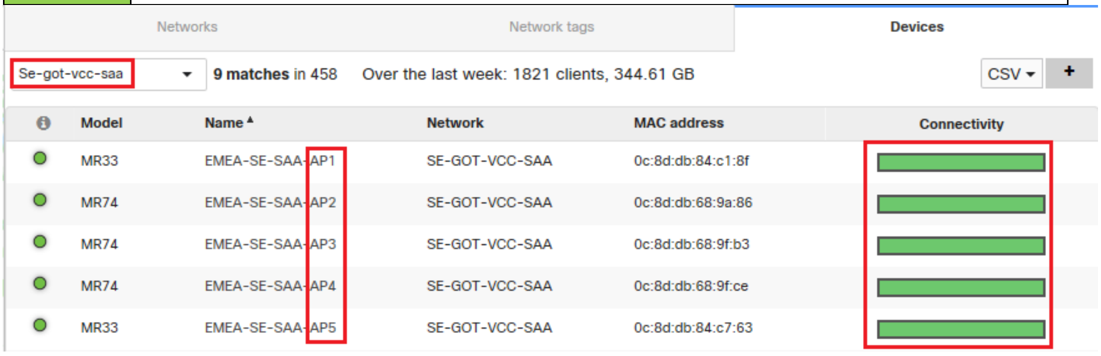
Also see Meraki Dashboard



Shows the network uptime percentage.

🟩 95-100% Network uptime
🟩 75-95% Network uptime
🟧 50-75% Network uptime
🟥 <50% Network uptime
□ No uptime data

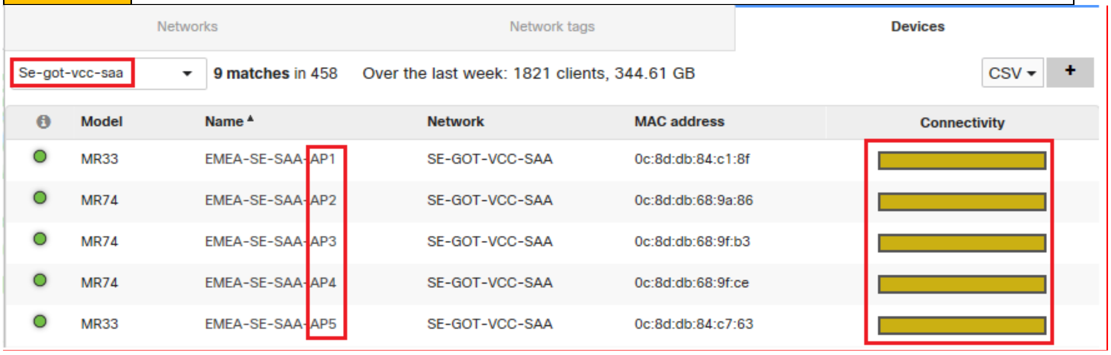
Green	The AP is able to connect to internet and the cloud used for the AP.



9 matches in 458 Over the last week: 1821 clients, 344.61 GB

	Model	Name	Network	MAC address	Connectivity
●	MR33	EMEA-SE-SAA-AP1	SE-GOT-VCC-SAA	0c:8d:db:84:c1:8f	🟩
●	MR74	EMEA-SE-SAA-AP2	SE-GOT-VCC-SAA	0c:8d:db:68:9a:86	🟩
●	MR74	EMEA-SE-SAA-AP3	SE-GOT-VCC-SAA	0c:8d:db:68:9f:b3	🟩
●	MR74	EMEA-SE-SAA-AP4	SE-GOT-VCC-SAA	0c:8d:db:68:9f:ce	🟩
●	MR33	EMEA-SE-SAA-AP5	SE-GOT-VCC-SAA	0c:8d:db:84:c7:63	🟩

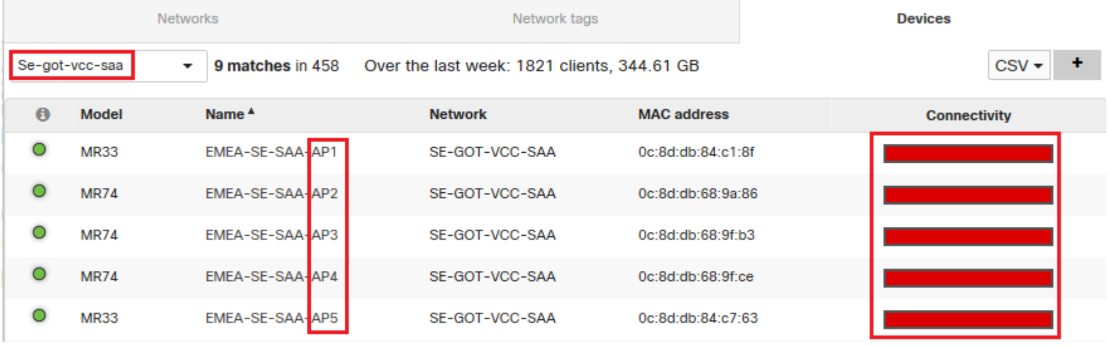
Orange	The AP is able to connect to internet and the cloud used for the AP, but has one or more active alerts.



9 matches in 458 Over the last week: 1821 clients, 344.61 GB

	Model	Name	Network	MAC address	Connectivity
●	MR33	EMEA-SE-SAA-AP1	SE-GOT-VCC-SAA	0c:8d:db:84:c1:8f	🟨
●	MR74	EMEA-SE-SAA-AP2	SE-GOT-VCC-SAA	0c:8d:db:68:9a:86	🟨
●	MR74	EMEA-SE-SAA-AP3	SE-GOT-VCC-SAA	0c:8d:db:68:9f:b3	🟨
●	MR74	EMEA-SE-SAA-AP4	SE-GOT-VCC-SAA	0c:8d:db:68:9f:ce	🟨
●	MR33	EMEA-SE-SAA-AP5	SE-GOT-VCC-SAA	0c:8d:db:84:c7:63	🟨

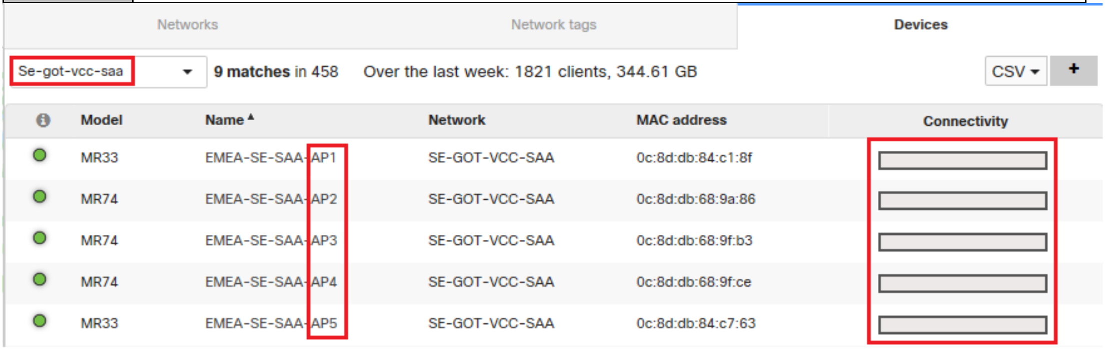
Red	The AP is **NOT** able to connect to internet and the cloud used for the AP.



9 matches in 458 Over the last week: 1821 clients, 344.61 GB

	Model	Name	Network	MAC address	Connectivity
●	MR33	EMEA-SE-SAA-AP1	SE-GOT-VCC-SAA	0c:8d:db:84:c1:8f	🟥
●	MR74	EMEA-SE-SAA-AP2	SE-GOT-VCC-SAA	0c:8d:db:68:9a:86	🟥
●	MR74	EMEA-SE-SAA-AP3	SE-GOT-VCC-SAA	0c:8d:db:68:9f:b3	🟥
●	MR74	EMEA-SE-SAA-AP4	SE-GOT-VCC-SAA	0c:8d:db:68:9f:ce	🟥
●	MR33	EMEA-SE-SAA-AP5	SE-GOT-VCC-SAA	0c:8d:db:84:c7:63	🟥

Grey	The AP has not yet been connected or it has not been able to connect to internet and cloud used for the AP during the last 7 days.



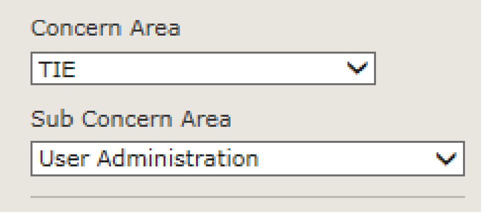
9 matches in 458 Over the last week: 1821 clients, 344.61 GB

	Model	Name	Network	MAC address	Connectivity
●	MR33	EMEA-SE-SAA-AP1	SE-GOT-VCC-SAA	0c:8d:db:84:c1:8f	□
●	MR74	EMEA-SE-SAA-AP2	SE-GOT-VCC-SAA	0c:8d:db:68:9a:86	□
●	MR74	EMEA-SE-SAA-AP3	SE-GOT-VCC-SAA	0c:8d:db:68:9f:b3	□
●	MR74	EMEA-SE-SAA-AP4	SE-GOT-VCC-SAA	0c:8d:db:68:9f:ce	□
●	MR33	EMEA-SE-SAA-AP5	SE-GOT-VCC-SAA	0c:8d:db:84:c7:63	□

If any AP is shown as Grey in Meraki dashboard at the time when the workshop faced an issue, then it could mean:

1. The AP has been offline unexpectedly for more than 7 days and fault tracing should be done.
2. Or the workshop has just ordered an additional AP that has not yet been mounted or connected and the status is then expected to be shown as grey until it has been installed and connected properly.

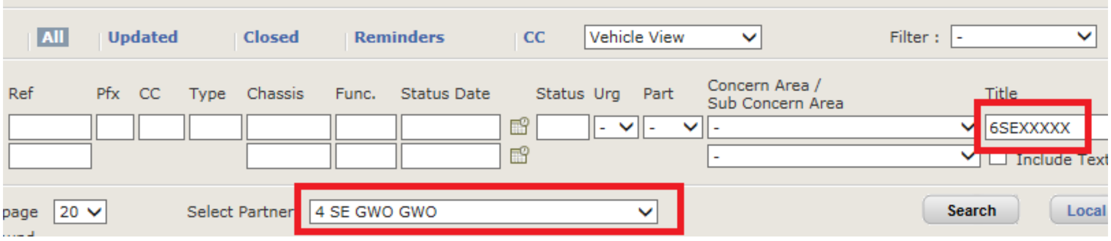
In TIE, try to find an additional order for an additional access point.
Note. In TIE you also need to have access to Partner ID **4 SE GWO** in order to see Wi-Fi orders done by workshops.
If you don't have access to Partner ID **4 SE GWO,** then you need to request access by creating a TIE report using below template and state the reason for the request and that you need to have "VCC_Reader access"



Concern Area: TIE

Sub Concern Area: User Administration

When you have access to **4 SE GWO**
Make a search under the section TIE Report and use the Partner ID as input for the search.



Vehicle View
Filter : -
Title: 6SEXXXXX
page 20
Select Partner 4 SE GWO GWO

If an order is found that is new, then you can maybe expect that it has not yet been delivered or installed in the workshop.
It will take about 3 weeks to deliver a new AP after an order has been accepted, and then it also needs to be installed when it has arrived, which might take some time.
If no new order is found, then you can expect that the access point should have been shown as Green, and not Red or Grey.

If an access point is shown as Red or Grey but is expected to show Green:
Then check and adjust local infrastructure until they show green according to below.

<u>Possible reasons for failures that needs to be checked by local IT.</u>

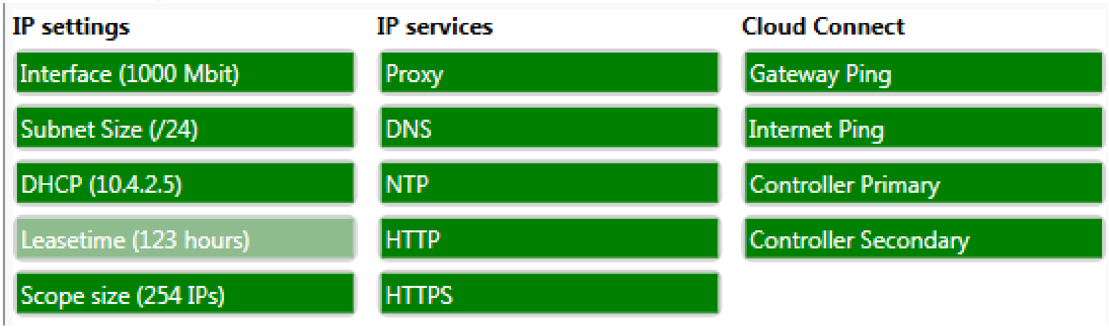
- The Switch connected to the access point is not providing power to the access point.
- The Ethernet cable between the switch and the access point is broken or not connected properly.
- POE injector is not providing power or is broken.
- Access point broken.
- Local router, switch or firewall is preventing the access points to access Internet. Check that there is no local proxy/firewall within the network that are blocking required ports according to:

SPJ – 1000692 - Workshop System Requirements & Guidelines - VIDA in 2015 (Dealers)

A check can also be done by connecting a computer to the same network as the APs are connected to and to run the verification tool on that computer.
SPJ 1000039 - Verification Tool - Volvo Cars Global Wi-Fi Service.

If needed consult with local IT if some of the results in the verification tool is showing Red.
The user guide available in SPJ *1000039* will include guidance when some of the tests are not shown as green.

Inform the workshop to perform necessary actions in case not all tests are shown as green.

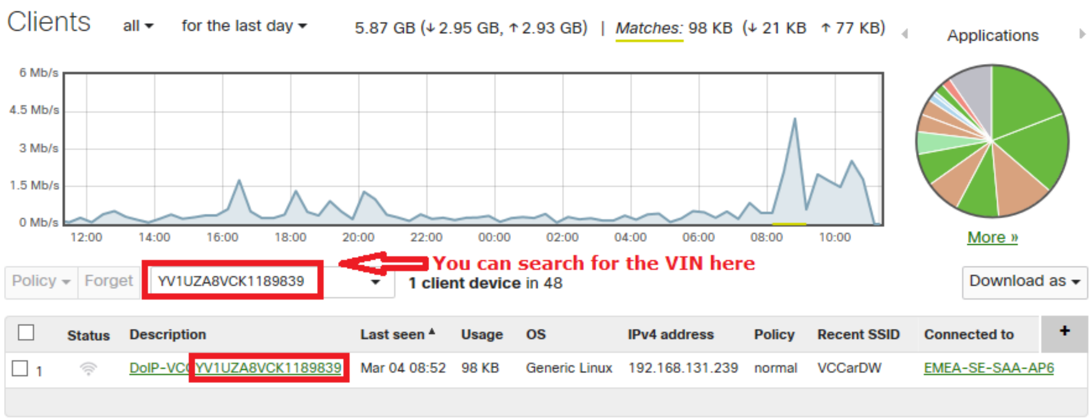


IP settings	IP services	Cloud Connect
Interface (1000 Mbit)	Proxy	Gateway Ping
Subnet Size (/24)	DNS	Internet Ping
DHCP (10.4.2.5)	NTP	Controller Primary
Leasetime (123 hours)	HTTP	Controller Secondary
Scope size (254 IPs)	HTTPS	

After a conclusion has been made and possible actions has been taken, then please proceed back to the Fault Tracing Chart

10.1.2 Is the VIN present in Meraki Dashboard?

Also see Meraki Dashboard



YV1UZA8VCK1189839

You can search for the VIN here

1 client device in 48

☐	Status	Description	Last seen ▲	Usage	OS	IPv4 address	Policy	Recent SSID	Connected to
☐ 1		DoIP-VC(YV1UZA8VCK1189839	Mar 04 08:52	98 KB	Generic Linux	192.168.131.239	normal	VCCarDW	EMEA-SE-SAA-AP6

After a conclusion has been made, then please proceed back to the Fault Tracing Chart

10.1.3 Can a MAC ID be found in Meraki Dashboard that starts with 00:10:02:XX:XX:XX at the time when Wi-Fi was activated in the vehicle?

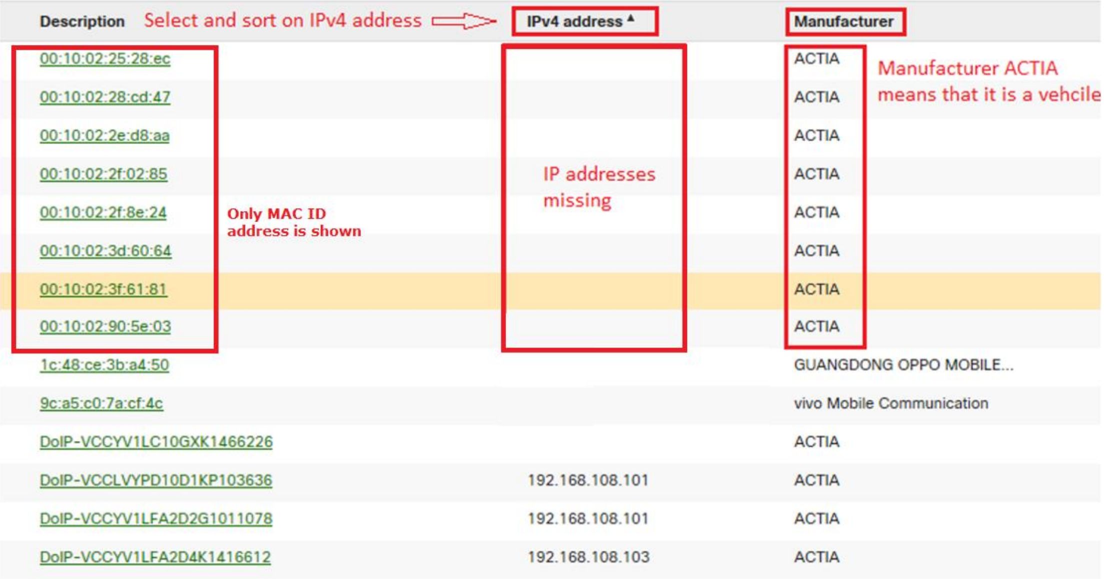
In Meraki Dashboard, select the affected workshop by searching for the Partner ID for the affected workshop.

Go to Network-wide > Clients.

Check if there are any vehicles that have been trying to establish a connection, without the possibility to get an IP address and were the description is only showing the Mac ID address from the vehicle.

A MAC ID address for a vehicles always starts with **00:10:02**:XX:XX:XX
And the Manufacture is shown as ACTIA.

Can a MAC ID be found in Meraki Dashboard that starts with **00:10:02**:XX:XX:XX at the time when Wi-Fi was activated in the vehicle?


Select and sort on IPv4 address
Only MAC ID address is shown
IP addresses missing
Manufacturer ACTIA means that it is a vehcile

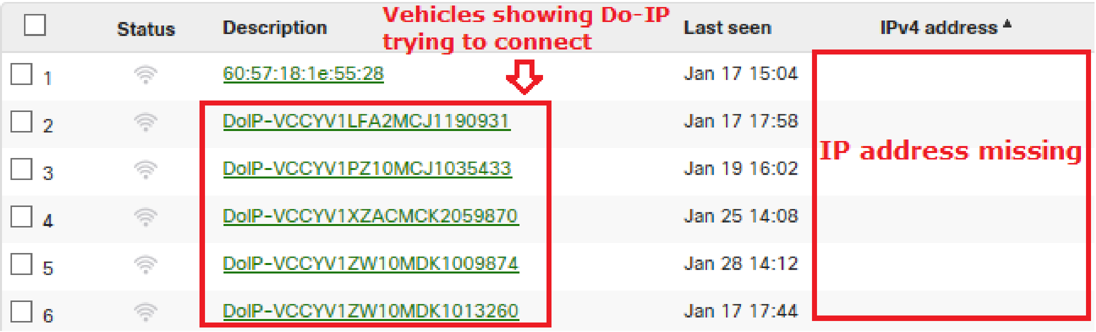
Description	IPv4 address ▲	Manufacturer
00:10:02:25:28:ec		ACTIA
00:10:02:28:cd:47		ACTIA
00:10:02:2e:d8:aa		ACTIA
00:10:02:2f:02:85		ACTIA
00:10:02:2f:8e:24		ACTIA
00:10:02:3d:60:64		ACTIA
00:10:02:3f:61:81		ACTIA
00:10:02:90:5e:03		ACTIA
1c:48:ce:3b:a4:50		GUANGDONG OPPO MOBILE...
9c:a5:c0:7a:cf:4c		vivo Mobile Communication
DoIP-VCCYV1LC10GXK1466226		ACTIA
DoIP-VCCLVYPD10D1KP103636	192.168.108.101	ACTIA
DoIP-VCCYV1LFA2D2G1011078	192.168.108.101	ACTIA
DoIP-VCCYV1LFA2D4K1416612	192.168.108.103	ACTIA

After a conclusion has been made, then please proceed back to the Fault Tracing Chart

10.1.4 Is an IP-address present or not for the VIN in Meraki Dashboard.

Select and sort on IPv4 address and check if any vehicles are not getting an IP address at the day when the issue occurred.
If a vehicle is shown with DoIP-VINVCCXXXXXX, then it means that the vehicle has a valid certificate in the ECU VCM, but the missing IP address could be caused by lack of IP addresses from the local DHCP.

Contact local IT and inform them to ensure a working DHCP function.

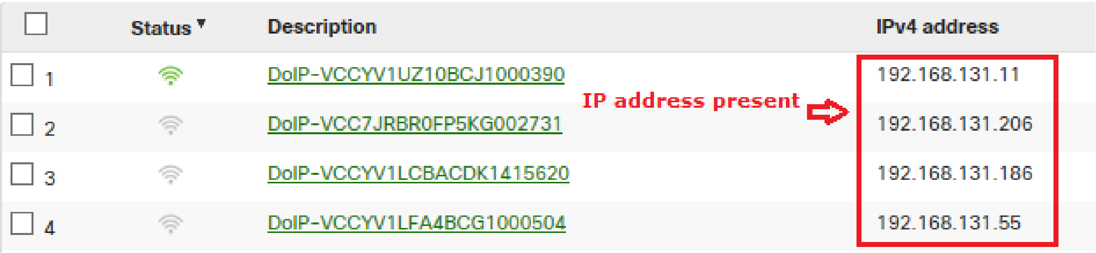


□	Status	Description	Last seen	IPv4 address ▲
□ 1	📶	60:57:18:1e:55:28	Jan 17 15:04	
□ 2	📶	DoIP-VCCYV1LFA2MCJ1190931	Jan 17 17:58	
□ 3	📶	DoIP-VCCYV1PZ10MCJ1035433	Jan 19 16:02	
□ 4	📶	DoIP-VCCYV1XZACMCK2059870	Jan 25 14:08	
□ 5	📶	DoIP-VCCYV1ZW10MDK1009874	Jan 28 14:12	
□ 6	📶	DoIP-VCCYV1ZW10MDK1013260	Jan 17 17:44	

Vehicles showing Do-IP trying to connect

IP address missing

How it can look when an IP address is present for a vehicle.



□	Status ▼	Description	IPv4 address
□ 1	📶	DoIP-VCCYV1UZ10BCJ1000390	192.168.131.11
□ 2	📶	DoIP-VCC7JRBR0FP5KG002731	192.168.131.206
□ 3	📶	DoIP-VCCYV1LCBACDK1415620	192.168.131.186
□ 4	📶	DoIP-VCCYV1LFA4BCG1000504	192.168.131.55

IP address present

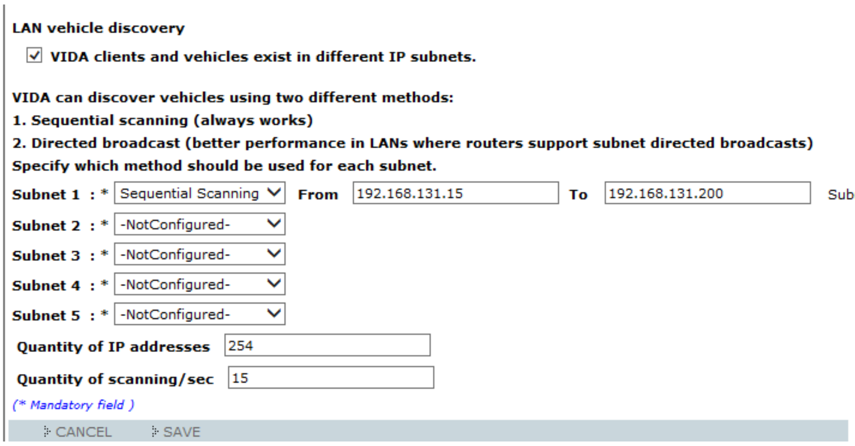
After a conclusion has been made and possible actions have been taken, then please proceed back to the Fault Tracing Chart

10.1.5 If needed, adjust settings in VIDA Admin if different subnets are intended to be used for Volvo Cars Diagnostic WI-Fi and computers used for VIDA.

If local IT states that different Subnets are intended to be used for Volvo Cars Diagnostic WI-Fi.
Then it also has to be configurated in VIDA Admin.

More information can also be found in:

SPJ 1000045 - Technical overview and design - Volvo Cars Global Wi-Fi Service



LAN vehicle discovery

☑ **VIDA clients and vehicles exist in different IP subnets.**

VIDA can discover vehicles using two different methods:
1. Sequential scanning (always works)
2. Directed broadcast (better performance in LANs where routers support subnet directed broadcasts)
Specify which method should be used for each subnet.

Subnet 1 : * Sequential Scanning **From** 192.168.131.15 **To** 192.168.131.200 Subnet 255.255.255.0
Subnet 2 : * -NotConfigured-
Subnet 3 : * -NotConfigured-
Subnet 4 : * -NotConfigured-
Subnet 5 : * -NotConfigured-
Quantity of IP addresses 254
Quantity of scanning/sec 15

(Mandatory field)*

After a conclusion has been made and possible actions has been taken, then please proceed back to the Fault Tracing Chart

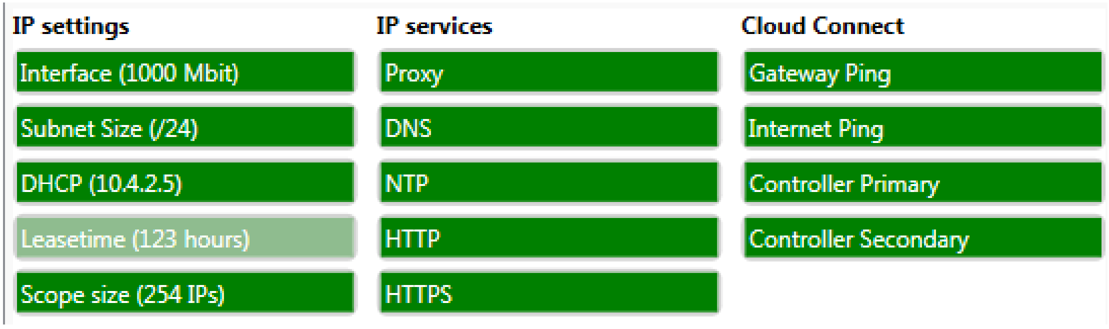
10.1.6 Check and if needed adjust local infrastructure such as firewalls and blocking of ports.

Check that there is no local proxy/firewall within the network or on computers used by VIDA that are blocking required ports according to:

SPJ – 1000692 - Workshop System Requirements & Guidelines - VIDA in 2015 (Dealers)

A check can be done by connecting a computer to the same network as the APs and to run the verification tool on that computer.
SPJ 1000039 - Verification Tool - Volvo Cars Global Wi-Fi Service.

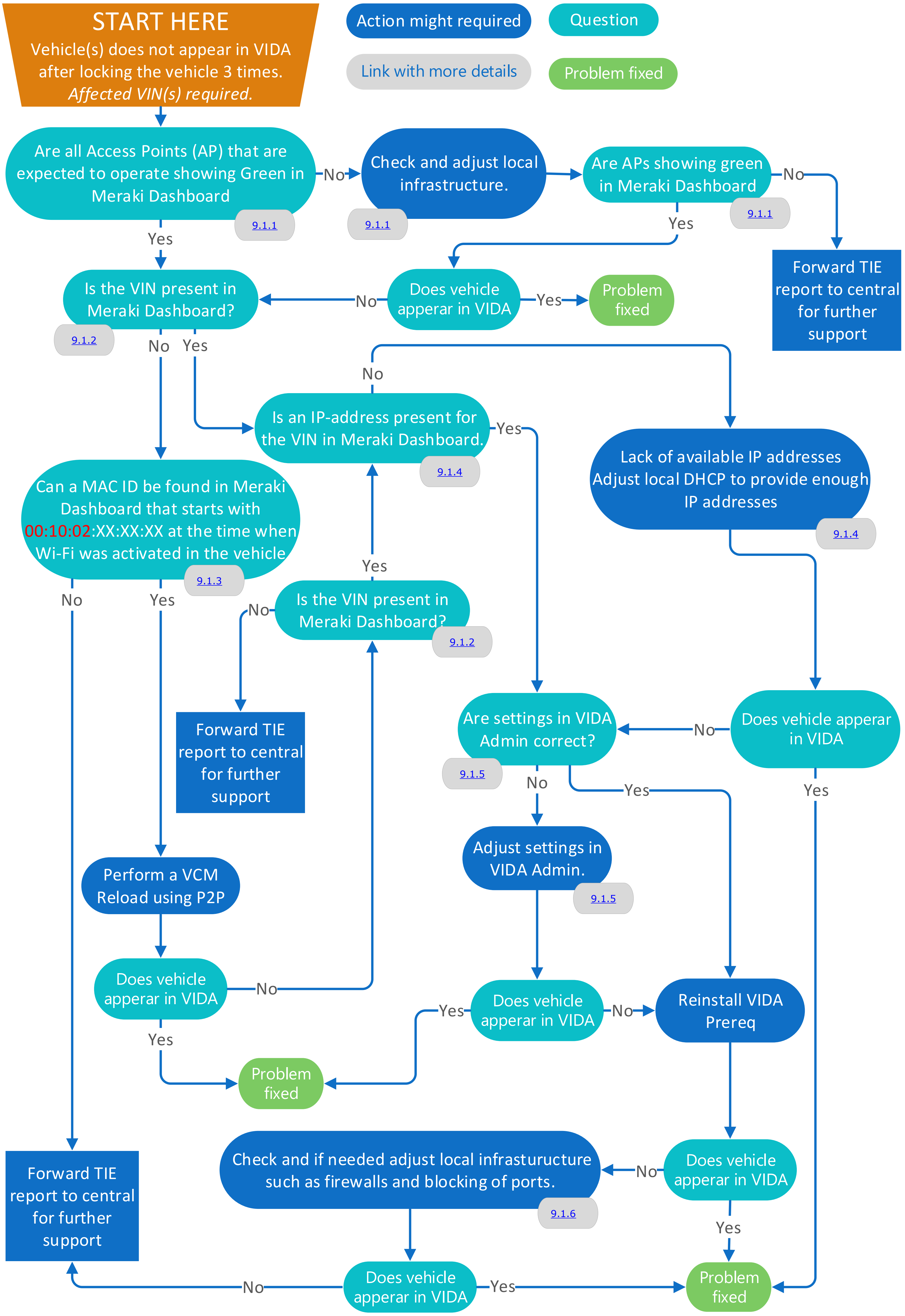
If needed consult with local IT if some of the results in the verification tool is showing Red.
The user guide available in SPJ 1000039 will include guidance for when some of the tests are not shown as green.
Inform the workshop to perform necessary actions in case not all tests are shown as green.



IP settings	IP services	Cloud Connect
Interface (1000 Mbit)	Proxy	Gateway Ping
Subnet Size (/24)	DNS	Internet Ping
DHCP (10.4.2.5)	NTP	Controller Primary
Leasetime (123 hours)	HTTP	Controller Secondary
Scope size (254 IPs)	HTTPS	

After a conclusion has been made and possible actions has been taken, then please proceed back to the Fault Tracing Chart

11 FAULT TRACING CHART - VEHICLE(S) DOES NOT APPEAR IN VIDA AFTER LOCKING THE VEHICLE 3 TIMES.



START HERE

Vehicle(s) does not appear in VIDA after locking the vehicle 3 times. *Affected VIN(s) required.*

Action might required

Question

Link with more details

Problem fixed

Are all Access Points (AP) that are expected to operate showing Green in Meraki Dashboard (9.1.1)

No → Check and adjust local infrastructure. (9.1.1) → Are APs showing green in Meraki Dashboard (9.1.1)

No → Forward TIE report to central for further support

Yes → Does vehicle apperar in VIDA

Yes → Problem fixed

No → Is the VIN present in Meraki Dashboard? (9.1.2)

Are all Access Points … Yes → Is the VIN present in Meraki Dashboard? (9.1.2)

No → Can a MAC ID be found in Meraki Dashboard that starts with 00:10:02:XX:XX:XX at the time when Wi-Fi was activated in the vehicle (9.1.3)

Yes → Is an IP-address present for the VIN in Meraki Dashboard. (9.1.4)

No → Lack of available IP addresses Adjust local DHCP to provide enough IP addresses (9.1.4) → Does vehicle apperar in VIDA

Yes → Problem fixed

No → Are settings in VIDA Admin correct? (9.1.5)

Is an IP-address present … Yes → Are settings in VIDA Admin correct? (9.1.5)

No → Adjust settings in VIDA Admin. (9.1.5) → Does vehicle apperar in VIDA

Yes → Problem fixed

No → Reinstall VIDA Prereq

Are settings in VIDA Admin correct? Yes → Reinstall VIDA Prereq → Does vehicle apperar in VIDA

Yes → Problem fixed

No → Check and if needed adjust local infrastructure such as firewalls and blocking of ports. (9.1.6) → Does vehicle apperar in VIDA

Yes → Problem fixed

No → Forward TIE report to central for further support

Can a MAC ID be found … No → Forward TIE report to central for further support

Yes → Perform a VCM Reload using P2P → Does vehicle apperar in VIDA

Yes → Problem fixed

No → Is the VIN present in Meraki Dashboard? (9.1.2)

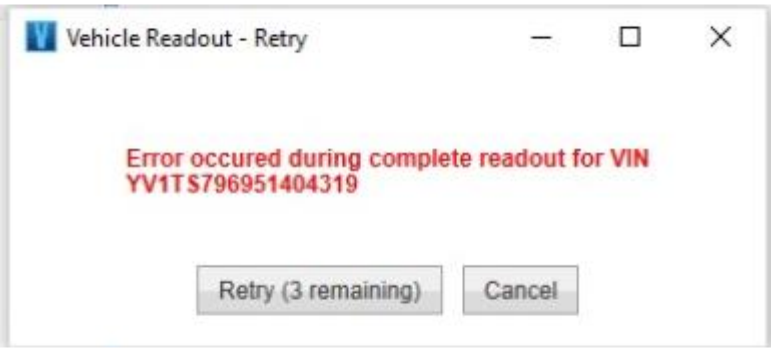
Yes → Is an IP-address present for the VIN in Meraki Dashboard.

No → Forward TIE report to central for further support

12 FAULT TRACING - ERROR SHOWN WHEN TRYING TO CONNECT TO THE VEHICLE.

12.1 Vehicle appears in VIDA, but an error message is shown when trying to connect to the vehicle.

Below error message is shown in VIDA instead of a successful readout of the vehicle.



Vehicle Readout - Retry

Error occured during complete readout for VIN YV1TS796951404319

12.1.1 Perform a battery reset of the vehicle.

If above error message is shown, then start with performing a battery reset of the vehicle.
It is important that you first turn ignition mode to off.

- Disconnect the negative pole of the main battery in the trunk.
- Wait 1 minute in order for the car to get fully discharged.
- Reconnect the negative pole of the main battery in the trunk.

After a conclusion has been made and possible actions has been taken, then please proceed back to the Fault Tracing Chart

12.1.2 Check and if needed adjust local infrastructure such as firewalls and blocking of ports.

Check that there is no local proxy/firewall within the network or on computers used by VIDA that are blocking required ports according to:

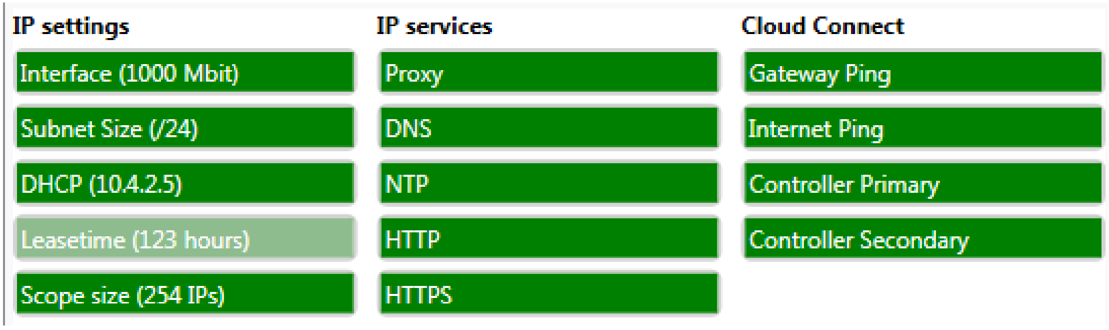
SPJ – 1000692 - Workshop System Requirements & Guidelines - VIDA in 2015 (Dealers)

Especially port TCP 13400.

A check can be done by running the verification tool on the computer where the issue occurs.

SPJ 1000039 - Verification Tool - Volvo Cars Global Wi-Fi Service.

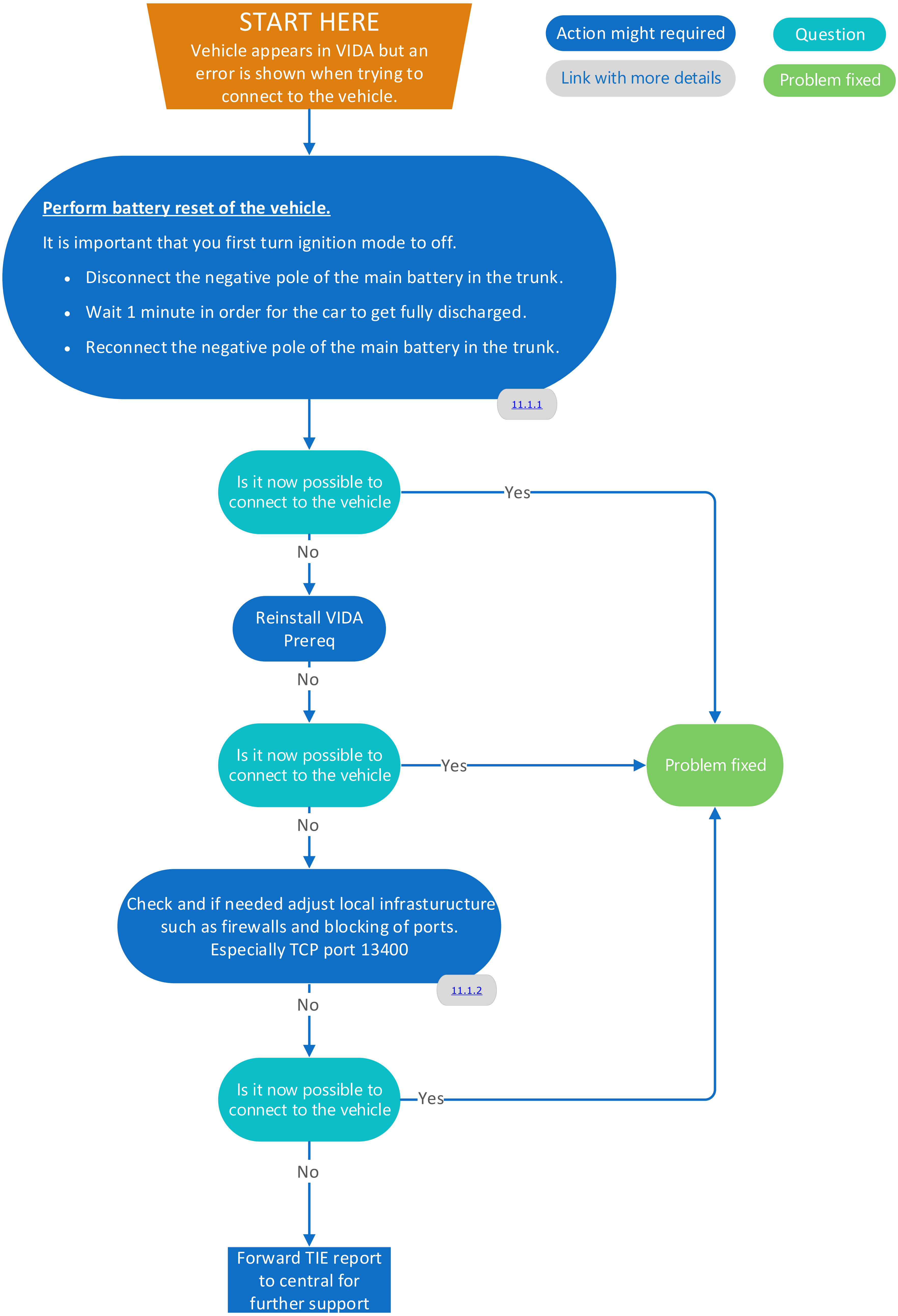
If needed consult with local IT if some of the results in the verification tool is showing Red.
The user guide available in SPJ 1000039 will include guidance when some of the tests are not shown as green.
Inform the workshop perform necessary actions in case not all tests are shown as green.



IP settings	IP services	Cloud Connect
Interface (1000 Mbit)	Proxy	Gateway Ping
Subnet Size (/24)	DNS	Internet Ping
DHCP (10.4.2.5)	NTP	Controller Primary
Leasetime (123 hours)	HTTP	Controller Secondary
Scope size (254 IPs)	HTTPS	

After a conclusion has been made and possible actions has been taken, then please proceed back to the Fault Tracing Chart

13 FAULT TRACING CHART - ERROR SHOWN WHEN TRYING TO CONNECT TO THE VEHICLE.



Action might required

Question

Link with more details

Problem fixed

START HERE

Vehicle appears in VIDA but an error is shown when trying to connect to the vehicle.

Perform battery reset of the vehicle.

It is important that you first turn ignition mode to off.

- Disconnect the negative pole of the main battery in the trunk.
- Wait 1 minute in order for the car to get fully discharged.
- Reconnect the negative pole of the main battery in the trunk.

11.1.1

Is it now possible to connect to the vehicle

Yes → Problem fixed

No

Reinstall VIDA Prereq

No

Is it now possible to connect to the vehicle

Yes → Problem fixed

No

Check and if needed adjust local infrasturucture such as firewalls and blocking of ports. Especially TCP port 13400

11.1.2

No

Is it now possible to connect to the vehicle

Yes → Problem fixed

No

Forward TIE report to central for further support

14 POOR PERFORMANCE – VEHICLE CONNECTION AND INSTALLATION OF SW

14.1 A bad Radio Frequency (RF) environment can result in connection issues and high SWDL Failure rate.

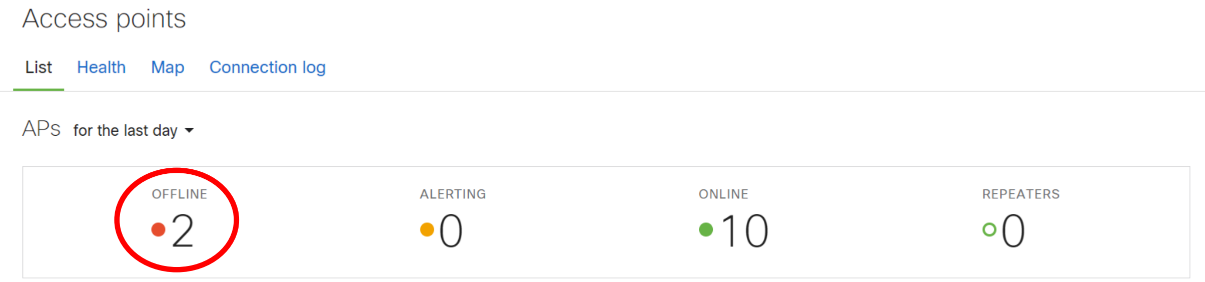
Guide for discovering RF problems in Meraki Dashboard.

Maintaining a good wireless environment is essential for benefiting the most from Volvo Cars Global Wi-Fi service. As more RF devices (access points, smartphones, laptops, etc.) are present in the workshop environment, complexity increases and the potential for degraded performance is larger.

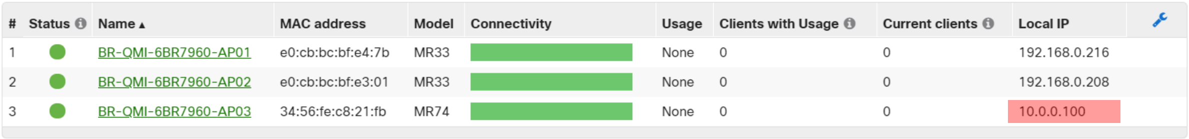
Individuals providing support to workshops can use this guide in order to find RF issues in Meraki Dashboard. A bad RF environment can result in connection issues and high SWDL failure rate with no clear root cause. There's no guarantee that solving RF issues will resolve the workshop's problems, but it can improve the Wi-Fi performance.

1. **Access point connection:**

   Navigate to **Wireless -> Access Points** and verify that all access points are **ONLINE**. The Access Points table should show all access points with a valid local IP address (depends on the network setup). Here are some examples of workshops with issues:



   AP possibly connected to wrong network:

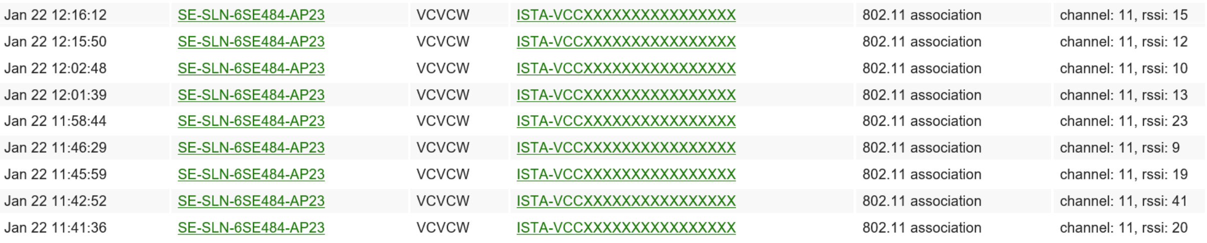


#	Status	Name ▴	MAC address	Model	Connectivity	Usage	Clients with Usage	Current clients	Local IP
1	●	BR-QMI-6BR7960-AP01	e0:cb:bc:bf:e4:7b	MR33	🟩	None	0	0	192.168.0.216
2	●	BR-QMI-6BR7960-AP02	e0:cb:bc:bf:e3:01	MR33	🟩	None	0	0	192.168.0.208
3	●	BR-QMI-6BR7960-AP03	34:56:fe:c8:21:fb	MR74	🟩	None	0	0	10.0.0.100

   Recommendation to workshop: Make sure all access points are installed in the right position and location. They should also be connected to the right local network and always have internet connection.

2. **Low signal strength:**

   Navigate to **Network-wide -> Event log** and for the field **"Event type include:"** select the option **"802.11 association"**. Associations with RSSI (received signal strength indication) values lower than **25** indicate that there can be issues with the workshop's signal strength. The **"Access Point:"** field can be used to identify which access point is having problems. For example, in the image below, vehicles connected the access point AP23 show a low RSSI. This can be due to the vehicles being too far from the AP, there might be obstructions between the vehicle and the AP or the AP TX-power is too low.



Jan 22 12:16:12	SE-SLN-6SE484-AP23	VCVCW	ISTA-VCCXXXXXXXXXXXXXXXX	802.11 association	channel: 11, rssi: 15
Jan 22 12:15:50	SE-SLN-6SE484-AP23	VCVCW	ISTA-VCCXXXXXXXXXXXXXXXX	802.11 association	channel: 11, rssi: 12
Jan 22 12:02:48	SE-SLN-6SE484-AP23	VCVCW	ISTA-VCCXXXXXXXXXXXXXXXX	802.11 association	channel: 11, rssi: 10
Jan 22 12:01:39	SE-SLN-6SE484-AP23	VCVCW	ISTA-VCCXXXXXXXXXXXXXXXX	802.11 association	channel: 11, rssi: 13
Jan 22 11:58:44	SE-SLN-6SE484-AP23	VCVCW	ISTA-VCCXXXXXXXXXXXXXXXX	802.11 association	channel: 11, rssi: 23
Jan 22 11:46:29	SE-SLN-6SE484-AP23	VCVCW	ISTA-VCCXXXXXXXXXXXXXXXX	802.11 association	channel: 11, rssi: 9
Jan 22 11:45:59	SE-SLN-6SE484-AP23	VCVCW	ISTA-VCCXXXXXXXXXXXXXXXX	802.11 association	channel: 11, rssi: 19
Jan 22 11:42:52	SE-SLN-6SE484-AP23	VCVCW	ISTA-VCCXXXXXXXXXXXXXXXX	802.11 association	channel: 11, rssi: 41
Jan 22 11:41:36	SE-SLN-6SE484-AP23	VCVCW	ISTA-VCCXXXXXXXXXXXXXXXX	802.11 association	channel: 11, rssi: 20

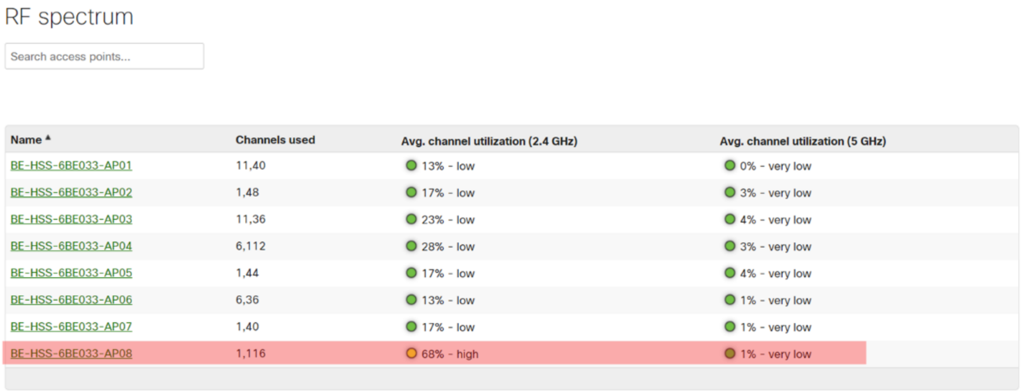
Recommendation to workshop: Analyze the location of the vehicles in relation to the access points:

a. Is there any obstacle between the vehicles and the access point such as: a wall, beams or glass?
b. Verify that the location of the vehicles is covered by the access points according to the site survey.

3. Interference from other Wi-Fi devices:

Several Wi-Fi devices in the proximity of the workshop or the access points will result in a high channel utilization and a crowded RF environment. There are two main ways of detecting this in Meraki:

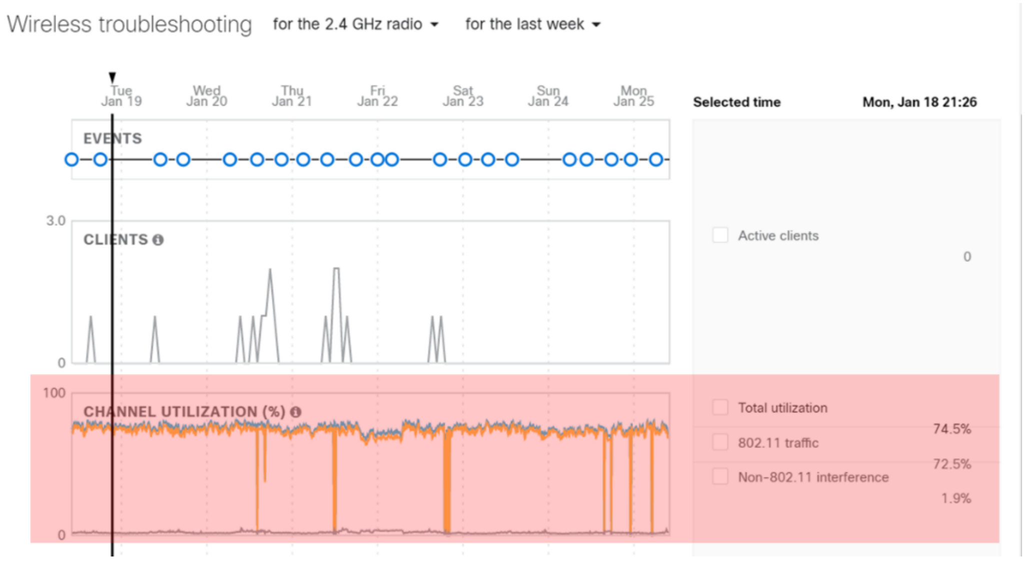
Option 1: Navigate to **Wireless -> RF Spectrum** and look at the **Avg. channel utilization (2.4 GHz)**. A channel utilization of more than **70%** can generate problems in the communication. Click on the AP to see more information on what channels are used the most and how the RF spectrum looks like.



RF spectrum

Name ▲	Channels used	Avg. channel utilization (2.4 GHz)	Avg. channel utilization (5 GHz)
BE-HSS-6BE033-AP01	11,40	● 13% - low	● 0% - very low
BE-HSS-6BE033-AP02	1,48	● 17% - low	● 3% - very low
BE-HSS-6BE033-AP03	11,36	● 23% - low	● 4% - very low
BE-HSS-6BE033-AP04	6,112	● 28% - low	● 3% - very low
BE-HSS-6BE033-AP05	1,44	● 17% - low	● 4% - very low
BE-HSS-6BE033-AP06	6,36	● 13% - low	● 1% - very low
BE-HSS-6BE033-AP07	1,40	● 17% - low	● 1% - very low
BE-HSS-6BE033-AP08	1,116	● 68% - high	● 1% - very low

Option 2: Navigate to **Wireless -> Access points** and click on an access point. In the access point view click on the **RF** tab at the top of the window. Select **"for 2.4 GHZ radio"** and **"for the last week"**. Check the channel utilization graph and see if there is high **802.11 traffic**. Analyze why the access point is seeing channel utilization: is it a constant high channel utilization? Is the channel utilization proportional to the number of clients connected to the AP and network usage? Are there specific time intervals with higher utilization? See figure below.



Wireless troubleshooting for the 2.4 GHz radio ▾ for the last week ▾

Selected time Mon, Jan 18 21:26

□ Active clients 0

□ Total utilization 74.5%

□ 802.11 traffic 72.5%

□ Non-802.11 interference 1.9%

Most of the time the workshops do not have control over all the Wi-Fi devices in their proximity as they can come from places/devices outside the workshop area, however, there are some thing that they can to improve the 2.4 GHz band channel utilization:

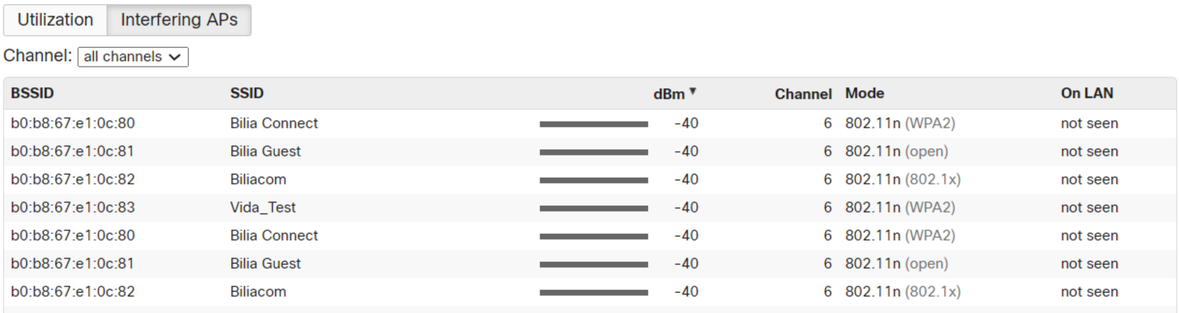
Recommendations to workshop:

- Make sure the access points are installed far from other devices that can cause Wi-Fi RF interference such as: other access points, routers, IP phones, repeaters.
- Band steering – As vehicles will only communicate on the 2.4 GHz band, other devices capable of using the 5GHz band should be steered into it to avoid overcrowding the 2.4GHz band.
- Connect the VIDA-client computers to the internet using ethernet cables whenever possible and investigate if there are other devices that use Wi-Fi but can be connected by cable. (e.g. surveillance cameras, HDMI wireless casting devices).

4. Local SSID management:

Every SSID broadcasting from the local access points (private or Volvo Cars Global Wi-Fi service) generates an overhead in the channel utilization which leads to poor wireless network performance. There are two ways of finding issues with SSIDs in Meraki:

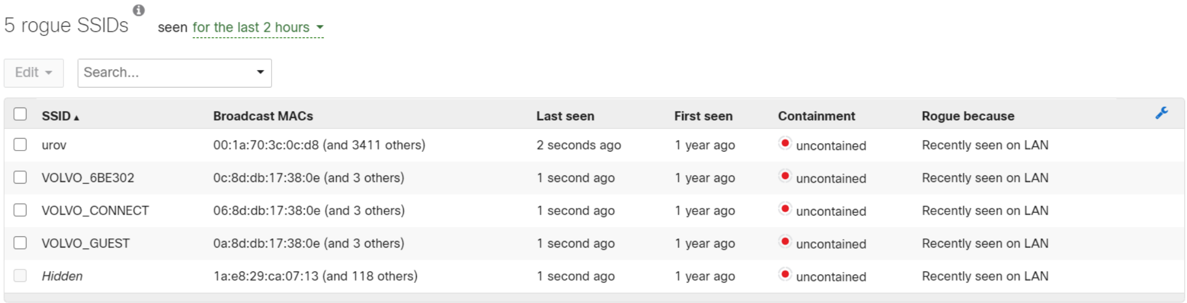
Option 1: Navigate to **Wireless -> RF Spectrum** click on an access point and click on **“Interfering APs”**. Sort the list by **“dBm”** to see how much interference is the SSID causing to the access points. SSIDS with strength greater than **-60dBm** (notice the negative sign) can be causing problems. Sort by **“SSID”** and check if there are SSIDs with the same or similar name but different **“Mode”** (authentication), if SSIDs are managed by the workshop, they could optimize the number of different SSIDs. If the Volvo Cars Global Wi-Fi Services SSIDs (VCCarDW and VCVCW) can be seen in the list with high **dBm** it can indicate that the access points are too close and could be interfering with each other if they are in the same channel.



Channel: all channels

BSSID	SSID	dBm ▾	Channel	Mode	On LAN
b0:b8:67:e1:0c:80	Bilia Connect	-40	6	802.11n (WPA2)	not seen
b0:b8:67:e1:0c:81	Bilia Guest	-40	6	802.11n (open)	not seen
b0:b8:67:e1:0c:82	Biliacom	-40	6	802.11n (802.1x)	not seen
b0:b8:67:e1:0c:83	Vida_Test	-40	6	802.11n (WPA2)	not seen
b0:b8:67:e1:0c:80	Bilia Connect	-40	6	802.11n (WPA2)	not seen
b0:b8:67:e1:0c:81	Bilia Guest	-40	6	802.11n (open)	not seen
b0:b8:67:e1:0c:82	Biliacom	-40	6	802.11n (802.1x)	not seen

Option 2: Navigate to **Wireless -> Air Marshall,** wait a few seconds for the Air Marshall to load the data. Click on **"Rogue SSIDs"** to see those SSIDs that are part of the LAN (managed by the workshop). The image below shows a workshop whose APs are announcing the same SSID in 3411 ways, this can lead to high channel utilization and turn into Wi-Fi service issues.


5 rogue SSIDs seen for the last 2 hours

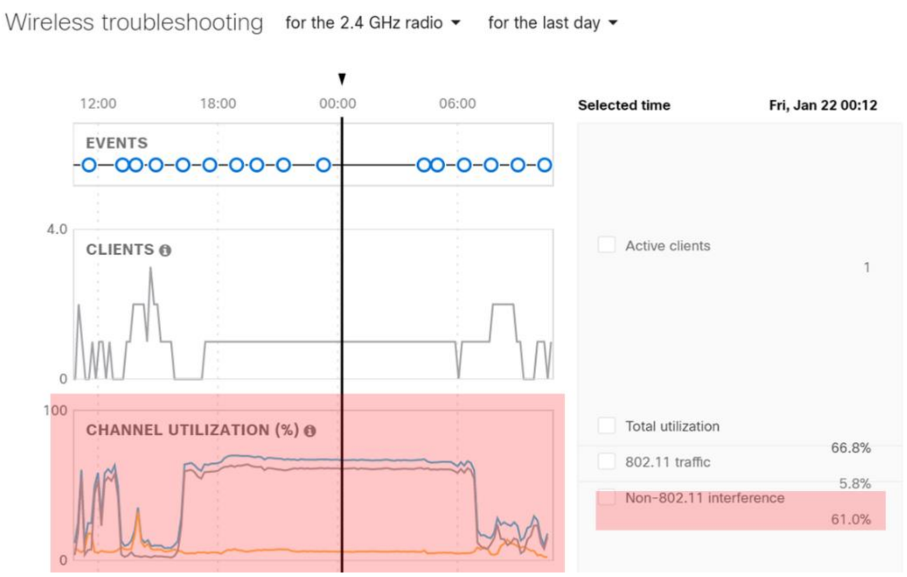
☐	SSID ▴	Broadcast MACs	Last seen	First seen	Containment	Rogue because
☐	urov	00:1a:70:3c:0c:d8 (and 3411 others)	2 seconds ago	1 year ago	● uncontained	Recently seen on LAN
☐	VOLVO_6BE302	0c:8d:db:17:38:0e (and 3 others)	1 second ago	1 year ago	● uncontained	Recently seen on LAN
☐	VOLVO_CONNECT	06:8d:db:17:38:0e (and 3 others)	1 second ago	1 year ago	● uncontained	Recently seen on LAN
☐	VOLVO_GUEST	0a:8d:db:17:38:0e (and 3 others)	1 second ago	1 year ago	● uncontained	Recently seen on LAN
☐	*Hidden*	1a:e8:29:ca:07:13 (and 118 others)	1 second ago	1 year ago	● uncontained	Recently seen on LAN

Click on **"Other SSIDs"** to see if there is an overflood of any other SSID (not connected to the LAN) that can be reported to the workshop to see if they can take any measure.

Recommendation to workshop: As rule of thumb, only one SSID should be created for each type of authentication required (open, WPA, 802.1x) and combine any SSIDs that use the same type authentication.

5. Non Wi-Fi interference:

To discover non Wi-Fi interference issues in Meraki, navigate to **Wireless -> Access points** and click on an access point. In the access point view click on the **RF** tab at the top of the window. Select **"for 2.4 GHZ radio"** and **"for the last week"**. Check the channel utilization graph and see if there is high **Non-802.11 interference**. Analyze to see if there's any time pattern in the channel utilization graph.



Wireless troubleshooting for the 2.4 GHz radio ▾ for the last day ▾

Selected time Fri, Jan 22 00:12

□ Active clients 1

□ Total utilization 66.8%

□ 802.11 traffic 5.8%

□ Non-802.11 interference 61.0%

Recommendation to workshop: The following devices can also cause RF interference degrading the performance of the wireless network. These devices should be kept as far as possible from the workshop area:

- Microwave ovens
- Cordless phones
- Bluetooth devices
- Wireless video cameras
- Wireless peripherals
- Zigbee devices
- Fluorescent lights

15 EXAMPLES OF KNOWN ISSUES AND HOW TO RESOLVE THEM.

15.1 Vehicles does not appear in VIDA for some internal VCC users having Windows 10.

Problem description:

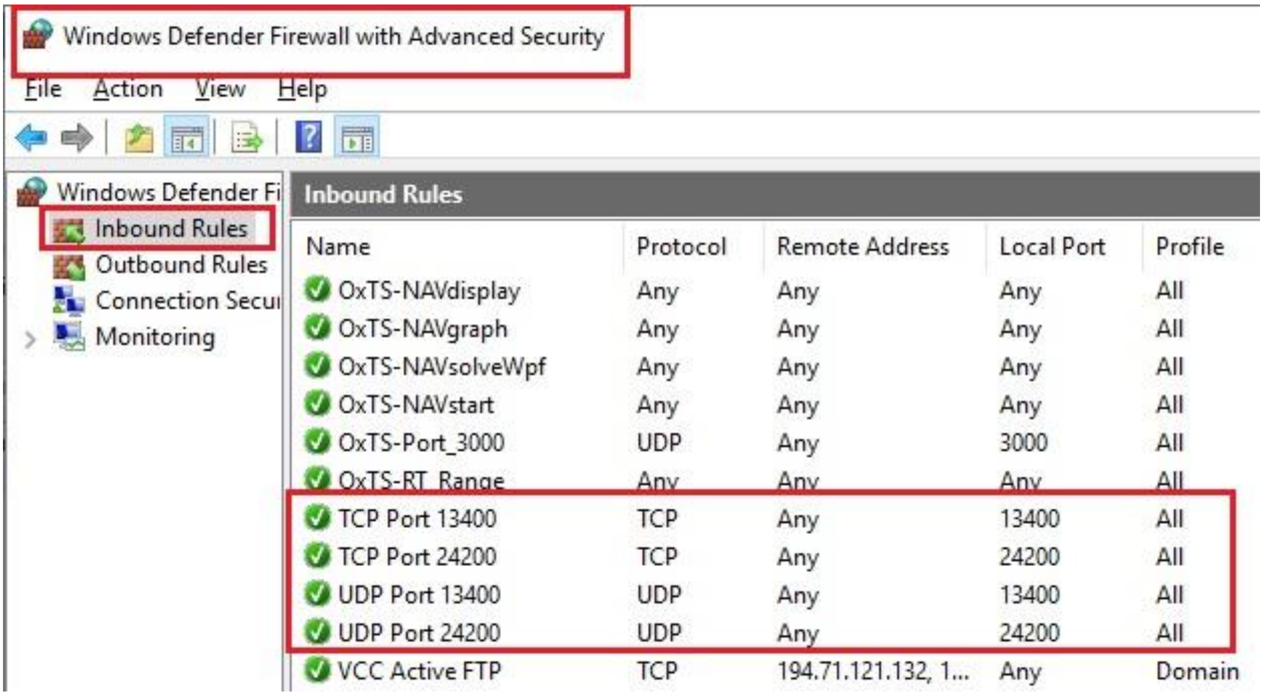
Vehicles does not appear in VIDA for some internal users having Windows 10

Possible Reason for the issue:

Communication (TCP and UDP port 24200 and 13400) blocked on computer.
This affects only Windows 10 due to a difference in how Windows 7 and 10 Windows handles the configuration of Ports in the local firewall.
The issue will also cause the same issue when trying to connect to the vehicle using P2P

How to Identify the reason for the issue:

Below firewall rules are missing



Inbound Rules

Name	Protocol	Remote Address	Local Port	Profile
OxTS-NAVdisplay	Any	Any	Any	All
OxTS-NAVgraph	Any	Any	Any	All
OxTS-NAVsolveWpf	Any	Any	Any	All
OxTS-NAVstart	Any	Any	Any	All
OxTS-Port_3000	UDP	Any	3000	All
OxTS-RT_Range	Any	Any	Any	All
TCP Port 13400	TCP	Any	13400	All
TCP Port 24200	TCP	Any	24200	All
UDP Port 13400	UDP	Any	13400	All
UDP Port 24200	UDP	Any	24200	All
VCC Active FTP	TCP	194.71.121.132, 1...	Any	Domain

How to resolve the issue:

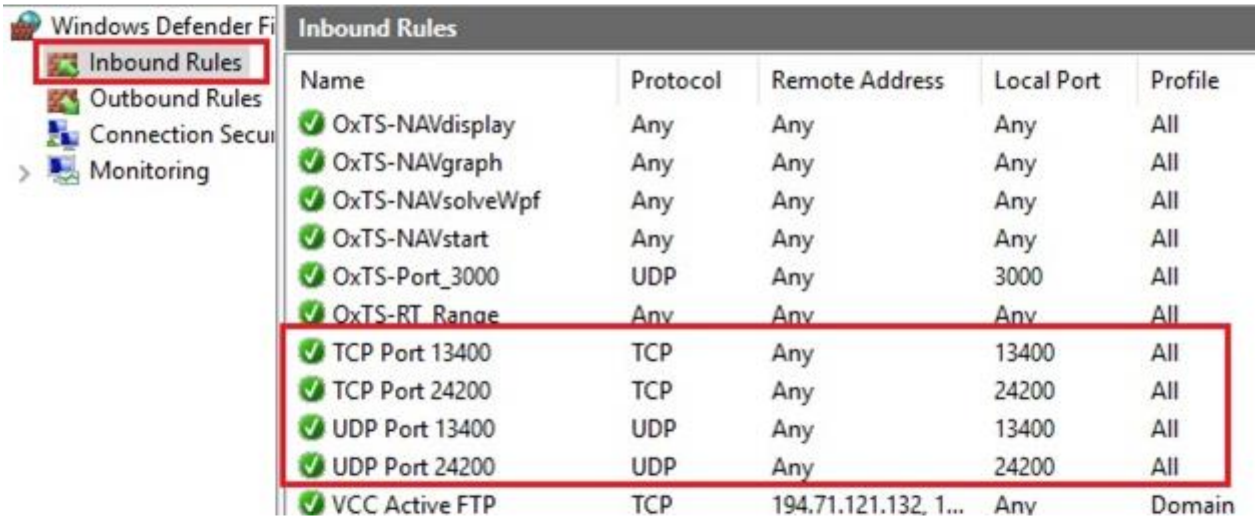
Order VIDA through Service-Now even if VIDA is already installed and even if VIDA has been ordered through Service-Now in the past.

Use below URL when ordering VIDA Prod
https://volvocars.service-now.com/sp?id=sc_home

Search for VIDA and select the one called only VIDA.

Verification:

Vehicles appears in VIDA and below firewall rules have been added to the computer after the request has been approved and the computer has been restarted.
Can only be verified if you have admin rights on user level and also on the affected computer.



Inbound Rules

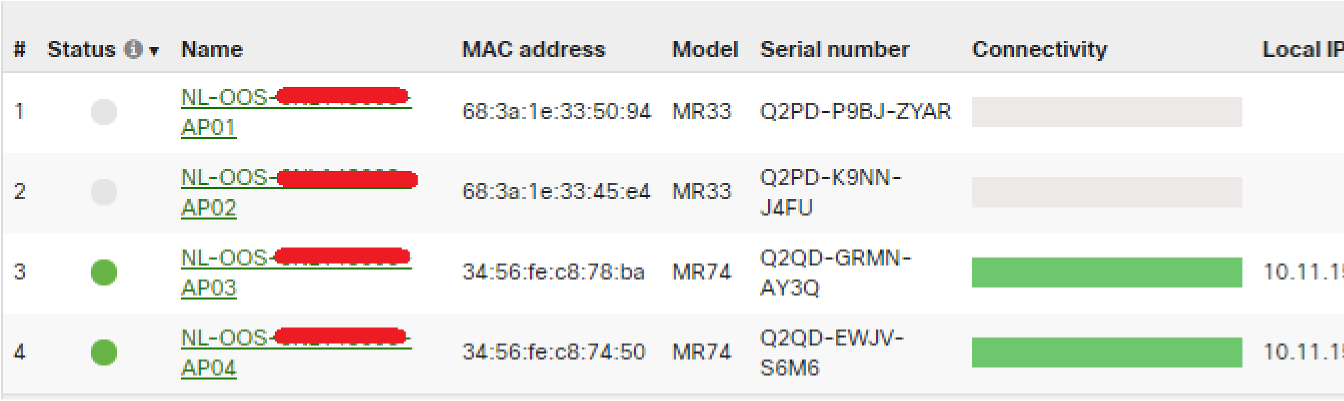
Name	Protocol	Remote Address	Local Port	Profile
OxTS-NAVdisplay	Any	Any	Any	All
OxTS-NAVgraph	Any	Any	Any	All
OxTS-NAVsolveWpf	Any	Any	Any	All
OxTS-NAVstart	Any	Any	Any	All
OxTS-Port_3000	UDP	Any	3000	All
OxTS-RT_Range	Any	Any	Any	All
TCP Port 13400	TCP	Any	13400	All
TCP Port 24200	TCP	Any	24200	All
UDP Port 13400	UDP	Any	13400	All
UDP Port 24200	UDP	Any	24200	All
VCC Active FTP	TCP	194.71.121.132, 1...	Any	Domain

15.2 LED on access point is blinking orange and status also shown as grey in Meraki Dashboard.

Problem description:

LED on 2 Access points are blinking Orange while 2 other access points at the same workshop are operational.

They are also shown as grey in Meraki Dashboard and without IP address.



#	Status	Name	MAC address	Model	Serial number	Connectivity	Local IP
1	○	NL-OOS-[redacted] AP01	68:3a:1e:33:50:94	MR33	Q2PD-P9BJ-ZYAR	⬜	
2	○	NL-OOS-[redacted] AP02	68:3a:1e:33:45:e4	MR33	Q2PD-K9NN-J4FU	⬜	
3	●	NL-OOS-[redacted] AP03	34:56:fe:c8:78:ba	MR74	Q2QD-GRMN-AY3Q	🟩	10.11.1
4	●	NL-OOS-[redacted] AP04	34:56:fe:c8:74:50	MR74	Q2QD-EWJV-S6M6	🟩	10.11.1

An orange blinking LED on the access point means that the access point is not able to establish a connection to Internet or the cloud used for the service "Volvo Cars Global Wi-Fi Service"

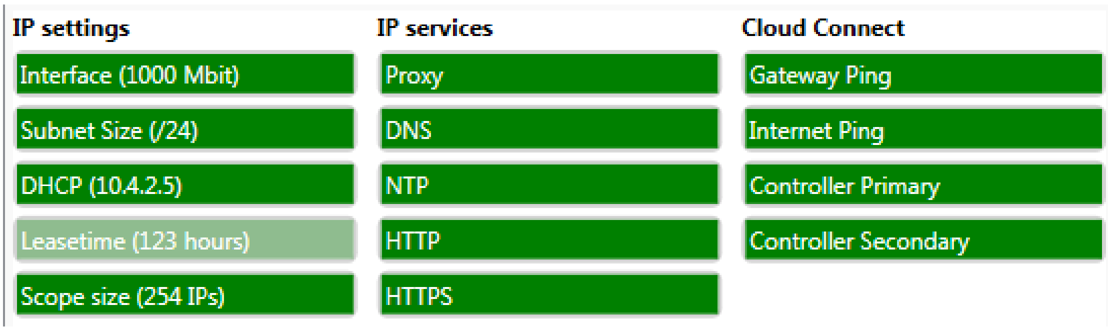
The reason is most likely locally in this case since 2 other access points at the same workshop are able to connect to the cloud used for the service "Volvo Cars Global Wi-Fi Service"

Possible Reason for the issue:

- Access to Internet or the cloud used for the service "Volvo Cars Global Wi-Fi Service" is being blocked by local firewall for the affected access points.
- Affected access point is not obtaining an IP address.
- Broken ethernet cable between the access point at the switch/router to where the access point is connected.

How to Identify the reason for the issue:

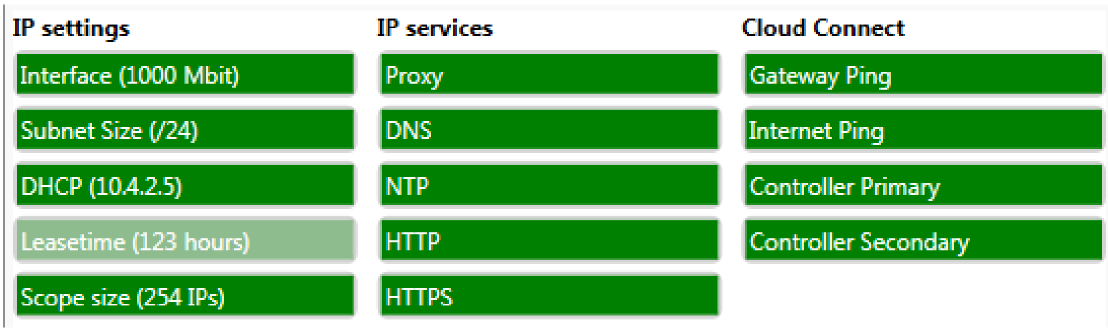
- Disconnect and connect the Ethernet cable connected to the none functional AP in order to restart the AP. If the issue still exists, go to next step:
- At the switch or router used for the access point, disconnect the ether cable used for the access point and connect another ethernet cable to the same port that is being used for the access point.
  Connect the other end of the ethernet cable to a computer that normally has access to Internet.
  On this computer, install the Verification tool used for "Volvo Cars Global Wi-Fi Service"
  Run the Verification tool and check that all tests are shown as green.
  The verification tool including information about each test can be found in TIE Service Journal 1000039.



IP settings	IP services	Cloud Connect
Interface (1000 Mbit)	Proxy	Gateway Ping
Subnet Size (/24)	DNS	Internet Ping
DHCP (10.4.2.5)	NTP	Controller Primary
Leasetime (123 hours)	HTTP	Controller Secondary
Scope size (254 IPs)	HTTPS	

How to resolve the issue:

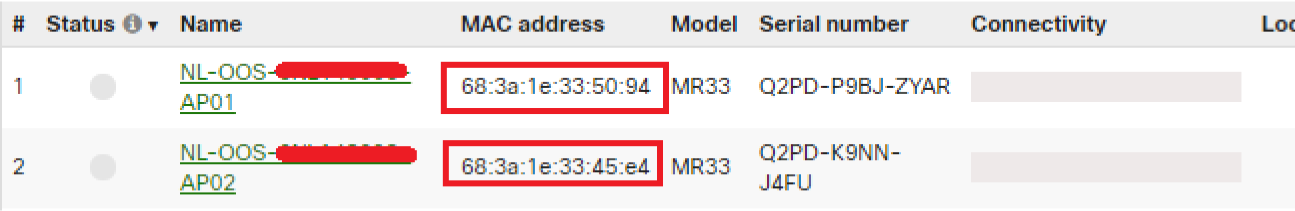
If some of the tests fails when running the verification tool, then ensure that required ports are not being blocked by any local firewall, required port-numbers are being described in the “User guide” that is available in TIE Service Journal 1000039.



IP settings	IP services	Cloud Connect
Interface (1000 Mbit)	Proxy	Gateway Ping
Subnet Size (/24)	DNS	Internet Ping
DHCP (10.4.2.5)	NTP	Controller Primary
Leasetime (123 hours)	HTTP	Controller Secondary
Scope size (254 IPs)	HTTPS	

If all tests are shown as green in the verification tool, but the AP is still blinking orange.
Then also check below before forwarding a TIE report to central.

- Connect another functional ethernet cable between the none functional access point and the switch/router used for the access point. If the issue still exists, go to next step:
- Check with local IT if the AP is being blocked or not on MAC ID address level. Ask them to check in their local firewall if any MAC address from the none functional access point are trying to access their network or not. If needed they need to unblock the access and ensure that an IP address becomes available for the affected MAC address.
  The MAC address for each access point can be found in Meraki Dashboard according to below:



#	Status	Name	MAC address	Model	Serial number	Connectivity	Loc
1	●	NL-OOS-[redacted] AP01	68:3a:1e:33:50:94	MR33	Q2PD-P9BJ-ZYAR		
2	●	NL-OOS-[redacted] AP02	68:3a:1e:33:45:e4	MR33	Q2PD-K9NN-J4FU		

Verification:

- The LED on the access point will finally lit with green color (blue if a device if connected)

  And

- Status on the affected access point will switch from grey to green in Meraki Dashboard.
  And they will get a Local and Public IP address.

16 CHANGE LOG

Changelog

Version	Date	Change
Version 1.0	2019-01-25	First version created
Version 1.1	2019-03-19	Fault tracing charts added For when a vehicle does not appear in VIDA Details for each checkpoint --- For when a vehicle appears in VIDA, but not be possible to connect to the vehicle. Details for each checkpoint --- Basic info about Meraki dashboard and access points added. --- Basic info about the Access points created.
Version 1.2	2020-03-20	How to fault trace and determine if an AP is broken or not. ---- How to request a replacement of a broken AP. --- Known issues and how to resolve them.
Version 1.3	2020-03-26	Below added one page 13 and 14 Page 13 Note, Reconnect the non-functional AP in case it will be possible, and a need to perform further fault tracing. Page 14 Note, Reconnect the non-functional AP in case it will be possible, and a need to perform further fault tracing.
Version 1.4	2020-05-14	13.2 LED on access point is blinking orange and status also shown as grey in Meraki Dashboard.
Version 1.5	2020-05-28	Page 5 - Information about Guest Wi-Fi removed.

		Page 6 – SPJ number replaced by TIE NG SJ number SPJ number 33048 has been replaced by TIE NG number 1000046 SPJ number 33761 has been replaced by TIE NG number 1000038
Version 1.6	2020-06-04	Update on page 16: 7.3 How to request a replacement of a broken AP. Below has been added: - Optional, special instructions from the workshop and where to pick up the none functional access point. Such as time or special place for the pickup. New on page 17: 7.4 Return instruction for a none functional Access point.
Version 1.7	2020-10-14	Update on page 16 Information added with a reference to a check list that should be filled in when sending in a request for replacing a none functional access point.
Version 1.8	2020-11-25	Update on page 16 ***AP-Check-List - Volvo Cars Global Wi-Fi Service-ver1.xlsx*** has been replaced by ***AP-Check-List - Volvo Cars Global Wi-Fi Service-ver2.docx*** ***AP-Check-List - Volvo Cars Global Wi-Fi Service-ver2.docx*** will now also have input fields for additional information that needs to be included.
Version 1.9	2021-02-15	Update on page 35- 38 A bad Radio Frequency (RF) environment could be the reason for poor performance or cause issues when installing software into vehicles when using WI-Fi. New section added describing how to detect a possible bad RF environment. POOR PERFORMANCE – VEHICLE CONNECTION AND INSTALLATION OF SW

Version 1.10	2021-04-14	New on page 8 4 - HOW TO ESCALATE MAJOR ISSUES