

IT REQUIREMENTS FOR T-ONE 2.1 - 2311

IT requirements for system installation, including hardware, OS, and network configuration.

About the IT requirements collection.....	3
Other IT requirements versions.....	3
1. Hardware requirements for T-ONE 2.1.....	4
1.1. General requirements.....	4
1.2. Requirements for up to 30 Autopilots.....	4
1.3. Requirements for more than 30 Autopilots.....	5
1.4. Back to IT requirements.....	5
2. Software requirements for T-ONE 2.1.....	6
2.1. Software requirements.....	6
2.2. Required software.....	6
2.3. Optional software.....	7
2.4. Ubuntu requirements for T-ONE 2.1.....	7
2.5. Red Hat Enterprise Linux requirements for T-ONE 2.1.....	7
2.6. SUSE Linux Enterprise Server requirements for T-ONE 2.1.....	8
3. Client requirements.....	9
3.1. Web browser requirements for T-ONE 2.1.....	9
3.2. CallMe screen requirements in T-ONE 2.1.....	9
4. SSL/TLS requirements for T-ONE 2.1.....	11
4.1. Requirements.....	11
4.2. Back to IT requirements.....	11
5. Network requirements for T-ONE 2.1.....	12
5.1. Network ports.....	12
5.2. Wired network.....	12
5.3. Wireless network.....	12
5.4. External connection.....	12
5.5. Back to IT requirements.....	12
5.6. Wireless network requirements for T-ONE 2.1.....	12
5.7. Network ports used by T-ONE 2.1.....	15
5.8. WLAN technology in Autopilots with CVC600.....	18
5.9. WLAN technology in Autopilots with CVC700.....	20
6. Native redundancy support in T-ONE 2.1.....	21
6.1. Customer backup requirements.....	21
6.2. Back to IT requirements.....	21
7. Making changes to IT infrastructure for T-ONE 2.1	22
7.1. Back to IT requirements.....	22

About the IT requirements collection

Note: Before deploying and using T-ONE 2.1, the customer must follow the requirements defined in this collection.

Other IT requirements versions

T-ONE 2.1

See: *Integration specifications and IT requirements archive for T-ONE 2.1*.

T-ONE 1.X

See: *IT requirements for T-ONE 1.X - all versions*.

IMPORTANT: Without database backups, data is lost in case of a hardware or software failure. Toyota strongly recommends that the customers set up backup systems, following best practices.

WARNING: Before making changes to the server environment in an existing T-ONE system, contact TMHLS. Changes can negatively affect system performance, require new licenses, or cause failures and unexpected behaviour. See, *Making changes to IT-infrastructure*.

1. Hardware requirements for T-ONE 2.1

IMPORTANT: New versions of T-ONE may have new hardware requirements. Always consult the *release notes* before updating T-ONE.

1.1. General requirements

IMPORTANT: The hardware is owned and maintained by the customer.

Each system installation **requires two virtual or physical servers, one server with Windows and one server with Linux** as operating system (OS).

1.1.1. Software requirements

Hardware requirements are listed below. Further requirements are listed in 2. *Software requirements for T-ONE 2.1*.

1.2. Requirements for up to 30 Autopilots

1.2.1. Windows server machine requirements

The windows server machine runs System manager and KepWare (optional) when I/O integration is used.

If C: is used for installation, it is recommended to store logs on a separate drive.

- Minimum 8 GB RAM.
- Minimum 4 Core CPU @ 2.3 GHz with AVX activated.

Example: 2,3 GHz Intel XEON® E5-2673 v4 (Broadwell)

- Hard drive with a minimum of 150 GB capacity (install of software stack and logs).
- Toyota staff credentials with administration rights.
- Follow instructions: 5.7. *Network ports used by T-ONE 2.1*.
- An USB port (for physical servers).

1.2.2. Linux server machine

The Linux server machine runs T-ONE services.

Note: A separate volume for backups is recommended.

- Minimum 16 GB RAM.
- Minimum 4 Core CPU @ 2.3 GHz with AVX activated.

Example: 2,3 GHz Intel XEON® E5-2673 v4 (Broadwell)

- A hard drive with a minimum of 250 GB capacity (install of software stack, order data, and logs).

The required minimum mount point sizes for a default installation are:

```
* /opt 1GB
* /var 200GB
```

- **From T-ONE 2.0 to T-ONE 2.1-2209:**

Confirm that there is at least 10 GB free disk space in the home folder to download, unpack, and install the T-ONE setup package.

- **From T-ONE 2.1-2211 and onwards:**

Confirm that there is at least 10 GB free disk space (for example in the home folder or the /tmp directory) to download, unpack, and install the setup package.

- Toyota staff credentials with administration rights (Root level access during installation) is needed.
- Follow the network requirements: *5.7. Network ports used by T-ONE 2.1.*

1.3. Requirements for more than 30 Autopilots

Simulations and tests are needed before adding more than 30 Autopilots to the system.

1.4. Back to IT requirements

Go to: *IT requirements for T-ONE 2.1 - 2311.*

2. Software requirements for T-ONE 2.1

2.1. Software requirements

IMPORTANT: Do not install software on the T-ONE 2.1 server that isn't part of the T-ONE stack. Irrelevant software can cause higher CPU load or disk usage, which can lead to errors.

IMPORTANT: Do not install Docker with *Snap*.

- All required software listed in this document must be licensed, installed, and maintained by the customer.
- All Windows hosted services must be configured for automatic restart, to ensure immediate system start-up after a reboot of the Windows host machine. See, *Expected services when T-ONE 2.1 is operational*.

2.1.1. Hardware requirements and installation guidelines

See 1. *Hardware requirements for T-ONE 2.1* and *System installation guidelines T-ONE 2.1*.

2.2. Required software

If more than one version is available in the following lists, install one of the versions.

2.2.1. Linux server

The Linux server machine runs T-ONE services.

- **Linux Server OS**
 - Ubuntu 20.04 LTS or 22.04 LTS, see 2.4. *Ubuntu requirements for T-ONE 2.1*.
 - RedHat Enterprise Linux (RHEL) 8.6, or later. See 2.5. *Red Hat Enterprise Linux requirements for T-ONE 2.1*.
 - SUSE Linux Enterprise Server 15.4, or later. See 2.6. *SUSE Linux Enterprise Server requirements for T-ONE 2.1*.
- **Additional Linux software**
 - jq
 - sed
 - curl
 - awk
 - Ntp client
 - Docker engine 20.10.11 or later versions
 - Docker compose 1.29.2, 2.2.3 or later releases

IMPORTANT: jq, sed, curl, awk, Ntp client, Docker engine, and Docker compose must be installed on the Linux server by the customer before installing T-ONE.

2.2.2. Windows server

The windows server machine runs System manager and KepWare (optional) when I/O integration is used.

- **Windows Server operating system**

- Windows Server 2019
- Windows Server 2022

- **A web browser**

See 3.1. *Web browser requirements for T-ONE 2.1.*

- **Security certificates**

Certificates for SSL/TLS and OPC UA must be available during installation. See, 4. *SSL/TLS requirements for T-ONE 2.1 and I/O service and OPC UA certificates and security*.

2.3. Optional software

- **LDAP compliant directory service**

If a directory service for user management is preferred, the customer must provide an LDAP compliant directory service (for example Active Directory).

2.4. Ubuntu requirements for T-ONE 2.1

2.4.1. Support

Toyota supports the LTS releases of Ubuntu.

Support follows the Ubuntu life cycle. For more information, see <https://wiki.ubuntu.com/Releases>.

2.4.2. NTP client

An *NTP client* must be installed and configured.

Note: The setup script *setup.sh* in **tone-setup/t-one/scripts/ubuntu** takes care of all requirements except configuring ntp.

2.4.3. Back to IT requirements

Go to: *IT requirements for T-ONE 2.1 - 2311*.

2.5. Red Hat Enterprise Linux requirements for T-ONE 2.1

2.5.1. Support

Support follows the Redhat Enterprise Linux (RHEL) 8 life cycle. For more information, see <https://access.redhat.com/support/policy/updates/errata>.

2.5.2. Podman not supported

Running podman as standalone or beside docker engine is **not supported**. Podman must be removed.

2.5.3. Disable Firewalld

Firewalld interferes with docker network and must be disabled.

2.5.4. NTP client

An *NTP client* must be installed and configured.

Note: The setup script (setup.sh) in **tone-setup/t-one/scripts/rhel** installs all requirements except configuring ntp.

2.5.5. Back to IT requirements

Go to: *IT requirements for T-ONE 2.1 - 2311*.

2.6. SUSE Linux Enterprise Server requirements for T-ONE 2.1

2.6.1. Support

Toyota supports the SUSE Linux Enterprise Server (SLES).

Support follows the SLES life cycle. For more information, see <https://www.suse.com/products/server/>.

2.6.2. NTP client

An *NTP client* must be installed and configured.

Note: The setup script *setup.sh* in **tone-setup/t-one/scripts/sles** takes care of all requirements except configuring ntp.

2.6.3. Back to IT requirements

Go to: *IT requirements for T-ONE 2.1 - 2311*.

3. Client requirements

3.1. Web browser requirements for T-ONE 2.1

The user interface (UI) as well as any external screens for transport initiation are displayed in web browsers. UI and external screens can run on the server machine itself, or on a separate computer or device.

3.1.1. Supported browsers and versions

The following browsers and versions have been tested and fully support T-ONE. Other browsers may also support T-ONE but have not been tested.

Browser	Supported versions in T-ONE 2.1
Chrome	Latest
Firefox	Latest
Microsoft Edge	Latest

3.1.2. Limitations

3.1.2.1. Concurrent connections to a host

IMPORTANT: Web browsers support a limited number of concurrent connections to a host.

The browsers can only display a limited number of T-ONE UI tabs at a time, depending on what browser and what browser version is used, as the web browsers support a different number of connection at a time. For example, Chrome can handle 6 concurrent connections to a host.

3.1.2.2. User interface translations

IMPORTANT: An internet connection is needed to access other languages than English on a client (computer or tablet).

English is the standard language used in T-ONE. To access other languages in the UI, the client (computer or tablet) must have an internet connection.

3.1.3. Back to IT requirements

Go to: *IT requirements for T-ONE 2.1 - 2311*.

3.2. CallMe screen requirements in T-ONE 2.1

Any device that runs a web browser that is following the *3.1. Web browser requirements*, can display CallMe screens. The requirements in this article refer to tablets.

For more information on CallMe screens, see *CallMe screens in T-ONE 2.1 - feature description*.

3.2.1. Minimum requirements for using CallMe screens on tablets:

- At least 2 GB RAM
- At least 16 GB internal storage
- Operating system: IOS, Android, or Windows.

WARNING: Apple iPads are **not recommended** for industrial automation as they can only run in networks which permit internet access.

- 3.1. *Web browser requirements for T-ONE 2.1.*
- Wi-Fi compatible with 5. *Network requirements for T-ONE 2.1.*

For a complete catalogue of peripheral devices supplied by Toyota, see *SharePoint*.

3.2.2. Host connections

IMPORTANT: Web browsers support a limited number of concurrent connections to a host.

The amount of concurrent host connections depends on the browser and the browser version. Chrome supports 6 connections. One browser can only display a limited number of tabs with CallMe screens.

3.2.3. Back to IT requirements

Go to: *IT requirements for T-ONE 2.1 - 2311*.

4. SSL/TLS requirements for T-ONE 2.1

4.1. Requirements

The security of the system, including user authentication, depends on encrypted communication between components.

To ensure secure systems, **the appropriate security certificates must be installed.** Certificates are acquired from third party certificate providers or through customers IT-department.

Note: The certificates must be provided and managed by the customer.

A certificate with the following required certificate capabilities:

- Server authentication certificate: RFC3280 id-kp-serverAuth: 1.3.6.1.5.5.7.3.1
- Client authentication certificate: RFC3280 id-kp-clientAuth: 1.3.6.1.5.5.7.3.2

For information on how to install certificates, see *T-ONE 2.1 system installation guidelines*.

4.2. Back to IT requirements

Go to: *IT requirements for T-ONE 2.1 - 2311*.

5. Network requirements for T-ONE 2.1

5.1. Network ports

All network ports listed in 5.7. *Network ports used by T-ONE 2.1* must stay open.

5.2. Wired network

Wired connections, when required, must conform to industry standards at a speed of at least 1Gbs. (Virtual) Network adapter must follow the Gigabit Ethernet standard as defined by the IEEE 802.3z specification.

5.3. Wireless network

See 5.6. *Wireless network requirements for T-ONE 2.1*.

5.4. External connection

Remote Desktop access to the server, including the ability to upload and download files, must be available for Toyota staff at all times. This is required to secure a stable system and to enable immediate intervention in case of failure.

To enable remote access to the server, the customer must provide a Virtual Private Network (VPN) connection, including:

- **VPN** account and access information to a selected group of TMH users
- **Instructions** for access and installation
- **Links** to applications needed
- **Additional software** and/or hardware if such is needed for the use of the VPN connection

5.5. Back to IT requirements

Go to: *IT requirements for T-ONE 2.1 - 2311*.

5.6. Wireless network requirements for T-ONE 2.1

Applies to: NDC8

The Autopilot is constantly moving and connecting to different Access Points (APs). If a vehicle loses WLAN connectivity, it will continue to move for a short distance, then stop. The Autopilot vehicle cannot move to a new location to attempt to reestablish lost communication.

The network therefore needs to be optimized to handle vehicle mobility. The vehicle handles this by itself, but if your WLAN has blind spots, or if there is substantial interference, the ability to roam will be strongly reduced. The effect of this is increased vehicle downtime.

Note: If you need assistance planning and verifying a WLAN network, contact the TMHLS office.

5.6.1. Standards

The WLAN must conform to the standard IEEE 802.11 n/ac. For more information, see *WLAN technology in Autopilots*.

5.6.2. Performance

It is the customer's responsibility to provide seamless wireless connectivity throughout the area of operation. The area of operation (factory or warehouse floor) must have complete and constant Wi-Fi coverage:

1. A minimum bandwidth of 52 Mbps. (As a rule of thumb, one vehicle generates about 7500 bytes of traffic per second to System Manager. This does not include the transfer of black box information.
2. A minimum signal strength of -66 dBm at receiving end (Autopilot vehicle)
3. A (SIR) Signal to Interference of -18 dBi or better.

Lowest requirement is According to 802.11n (MCS5)

1. One Spatial stream
2. Guard interval (GI) 800ns/0,8 @ 20 MHz Channel bandwidth
3. MCS5, 52 Mb/s, SNR 18, RSSI -66 dBm
4. FT-802.11r enabled on Autopilot SSID and Roaming between APs must be verified by the customer
5. A maximum response time between server and Autopilot of 30 ms. It may be higher while a vehicle is roaming or scanning for an access point.
6. WLAN network must be **optimized to handle roaming between APs** in the entire area of operation.

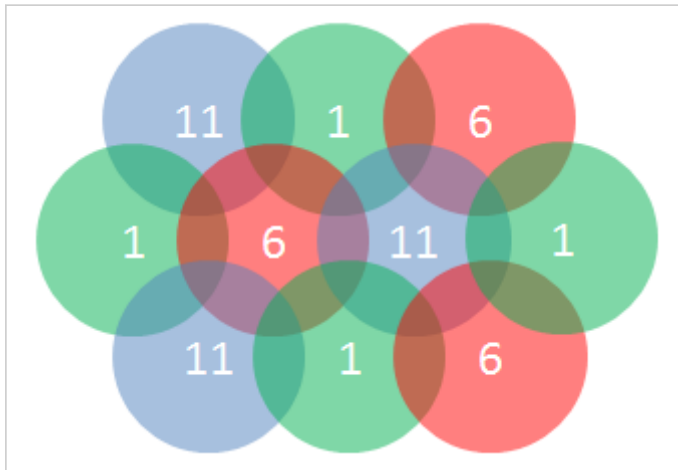
Note: The performance criteria is verified during the WLAN Commissioning phase, it is required that the customer provides a Network engineer that can monitor and verify that the AGV's meet the above performance.

IMPORTANT: The customer must verify the quality of their WLAN Network, to ensure adequate coverage and minimum interference according to the Performance requirements in the entire area of operation. This means that the customer has to verify SIR (Signal to Interference Rate), Minimum RSSI value (Received Signal Strength Indicator) and Handover between APs (That mobility of the AGVs in the WLAN network are secured and functioning).

Remove any interfering equipment from the area of operation. That could be none DECT 6.0 Phones, cordless phones or microwave ovens.

5.6.3. Access points

Access points should be placed and channels assigned such that two adjacent APs (access points) never share the same channel.



To reduce the amount of overhead in the network, Toyota recommends a maximum of three SSIDs (Service Set Identifiers) for each access point in 2.4 GHz networks.

The following requirements apply to both 2.4 GHz and 5 GHz networks:

- At least 2 APs must be available for the Autopilot vehicle, with signal strength as specified above.
- Follow recommendations from the WLAN product manufacturer regarding placement, antenna mounting, etc.
- Wi-Fi infrastructure must be uniform, regarding APs, firmware level, etc.
- Roaming between APs must be verified for non 802.11K/V/R compliant equipment.
- Maintain a map of all access points with channels, MAC addresses, IP addresses, and physical positions. This must be made available to Toyota on request, for troubleshooting.

5.6.3.1. 2.4 GHz networks

In a 2.4 GHz network, use only channels 1, 6 and 11 or 12/13.

Note: Only use channels 1, 6, and 11 in the operating area, even for other purposes than Autopilot control. All other channels have frequency overlap with at least one of the channels 1, 6, or 11. Overlapping frequency space will cause increased noise and degraded communications.

5.6.3.2. 5 GHz networks

Only with CVC700 unit or external WLAN Bridge.

- U-NII 1: Channels 36, 40, 44, 48
- U-NII 2a: Channels 52, 56, 60, 64
- U-NII 2c: Channels 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144
- U-NII 3: Channels 149, 153, 157, 161, 165

For a 5 GHz network, there are no restrictions on the channels being used since the frequency space does not overlap. However, they must match the setup in the vehicle controller (CVC700).

Note: You may need more access points on a 5 GHz network because it is more sensitive to solid objects than a 2.4 GHz network.

5.6.4. Back to IT requirements

Go to: *IT requirements for T-ONE 2.1 - 2311* or *IT requirements for T-ONE 2.0*.

5.7. Network ports used by T-ONE 2.1

IMPORTANT: The network must be open for all outbound traffic from the T-ONE servers.

The tables in this article list ports that must or can be opened up in the network firewall. **The requirements for the ports are listed under each table heading below.**

The reason to why some ports **must** be open and some ports **can** be open is:

- Some ports must always be open in production.
- Some ports are only required during commissioning or support.
- Some ports can be ignored if a particular feature is not used.

Command line tool

Toyota provides a command line tool for checking the status of relevant ports on the network, available in the **PortStatus 2.x.zip** and **PortStatus SM Only.zip** files on *SharePoint*.

Table explanations

In the tables below, the following sources and targets are used:

- **T-ONE Linux server** - The server running the T-ONE services.
- **Windows server** - The server running System Manager and optional KepWare (when I/O integration is used).
- **T-ONE web app** - The T-ONE GUI, running in a browser on a client machine.
- **Autopilot** - The vehicles that are executing transports/missions.
- **CWay clients** - Any machines which the CWay application runs on.
- **I/O cabinet** - The PLC in the Söderberg I/O cabinet used to route I/O signals to and from T-ONE.
- **WMS** - The customer's WMS.
- **AE machine** - The application engineer's laptop. Used for configuration, diagnostics, etc.

5.7.1. Basic requirements

The following ports **must** always be open for a T-ONE 2.1 system in production:

Source	Target	Port/Protocol	Description	Application protocol
--------	--------	---------------	-------------	----------------------

T-ONE web app	T-ONE Linux server	443/TCP	HTTPS access to the T-ONE web UI from a browser. This port must be open if running web UI client on other machine than T-ONE server.	HTTPS
T-ONE Linux server	Windows server	30000, 30001/TCP	Windows server, the System Manager and T-ONE system communication.	Proprietary
Autopilot	Windows server	30010/TCP	The vehicle controller reply channel to System Manager.	Proprietary
CWay clients	Windows server	30030-30044/TCP	The number of ports depends on the number of clients. Required only if CWay runs on a separate machine.	Proprietary

5.7.2. Feature dependent requirements

The following ports **must** be open for specific optional features:

Source	Target	Port/ Protocol	Description	Application protocol
AD connection				
T-ONE Linux server	Domain controller	<Domain controller>	Port for communication with the external domain controller.	
Barcode, handheld and stationary scanners				
T-ONE Linux server	Scanner	3888/TCP	Open if using SICK scanners.	SOPAS over socket
CDI				
Windows server	Smartness	5672/TCP	Used by T-Hive Vehicle bridge - Smartness Vehicle Adaptor to connect to RabbitMQ.	AMQP
DataCollector				
Windows server	Smartness	5677/TCP	Default port to DataCollector.	HTTP
OPC UA				

T-ONE Linux server	OPC UA server	49320/TCP	Default port for enabling OPC UA with a Kepware server.	Secured by TLS
Shuttles				
T-ONE Linux server	Radioshuttle(s)	2000-N/TCP	One port per shuttle is required.	Proprietary
TwinCat				
Windows Server	I/O Cabinet	48898/TCP	TwinCAT server to Twincat client in I/O cabinet. Used to forward I/O communications, eg fire alarm, doors, etc.	ADS API
T-ONE Live				
T-ONE Linux server	Windows server	30045/TCP	Vehicle coordinates from System Manager to T-ONE to display vehicle movement in the Live view.	Proprietary
WMS Integration				
WMS	T-ONE Linux server	443/TCP	Default port for web service interface REST-API when T-ONE is host.	HTTPS
T-ONE Linux server	WMS	<WMS as host>	Connection to the customer's Warehouse Management System (WMS) is set up through a subscription call to REST-API. See API specification.	HTTP/HTTPS

5.7.3. Ports required for commissioning and support

The following ports are **not required to be open during production, but must be open when needed for support and troubleshooting.**

Source	Target	Port/Protocol	Description	Application protocol
--------	--------	---------------	-------------	----------------------

AE machine / Windows server	Autopilot	80/TCP	Communication with vehicle web server.	HTTP
AE machine / Windows server	Autopilot	443/TCP	Communication with vehicle from engineering tools (Vehicle Application Designer, VMT PC, Natural Surveyor, Vehicle Diagnostic Tool, Web Browser) if using secure mode and Licence Manager.	HTTPS
AE machine/ Windows server	Autopilot	5432/TCP	Reflector Surveyor, Vehicle Diagnostic Tool.	Proprietary
Windows server	Autopilot	8071/UDP	System Manager Broadcast. Name resolution broadcast, from vehicle to System Manager, or from VAD/ OpenPCS/LD/R to vehicle. Response is sent on a random port 100-6000. Alternatively, the application engineer can connect to the vehicle using ethernet cable.	Proprietary
AE machine	Autopilot	44000/TCP	OpenPCS. Used to monitor vehicle PLC in real time.	
Windows server	I/O cabinet	48899/UDP	Used to download configuration to I/O cabinet.	
AE machine/ Windows server	Autopilot	5677/TCP	Vehicle Application Designer, VMT PC, Reflector Surveyor, Vehicle Diagnostic Tool. Required during production for scheduled blackbox fetching.	Proprietary

5.7.4. Back to IT requirements

Go to: *IT requirements for T-ONE 2.1 - 2311*.

5.8. WLAN technology in Autopilots with CVC600

Applies to: *LAE250* Applies to: *SAE160* Applies to: *RAE160/200/250* Applies to: *OAE120CB*
Applies to: *TAE500*

The following WLAN support is built into Autopilot vehicles as *Standard*.

Wireless client	Embedded Wi-Fi (WPA supplicant) CVC600
Frequency bands	2.4 GHz, 5 GHz
Channels	1, 6, 11 (for 2.4 GHz). U-NII 1, 2, 2e and 3 (for 5 GHz) is available for the CVC600 hardware revision 18446-01N or later. Only for use outside of EU.
Sticky client	No
Pre-shared key authentication support	Yes
Static IP address	Yes, one per vehicle

Datasheet: https://www.u-blox.com/sites/default/files/OWS451-OWL253-ElectricalMechanical_DataSheet_%28UBX-15021499%29.pdf

IMPORTANT: As *Standard*, Autopilots support only 2.4 GHz WLAN. The standard 5 GHz WLAN built into the CVC600 vehicle controller is currently not approved for AGV communication in the EU. If 5 GHz communication is required, a *Moxa WLAN bridge* should be ordered as an *Option*.

5.8.1. Standards

The Wi-Fi network must conform to the standard IEEE 802.11b/g/n. technology in the automated vehicle.

- 802.11 b 11MBit/s (ISM channel: 2,4 GHz)
- 802.11 g 54 Mbit/s (ISM channel: 2,4 GHz)
- 802.11 n 65 Mbit/s (ISM channel: 2,4 GHz or UNII channel: 5 GHz(single-stream))

5.8.2. Encryption

The following encryption modes are supported:

- WEP (64/128) (not recommended due to low security)
- WPA-PSK (TKIP or AES/CCMP or TKIP+WEP128)
- WPA2-PSK (TKIP or AES/CCMP or TKIP+WEP128)

IMPORTANT: TMHE products do not support WPA/WPA2 mixed mode.

Note: Other needs than mentioned above, for example 802.1x and/or EU certified 5 GHz communication, might require an external bridge which must be ordered as an *Option*. It is important to involve TMHMS in the solution to secure the CE-marking.

5.9. WLAN technology in Autopilots with CVC700

Applies to: *LAE250* Applies to: *SAE160* Applies to: *RAE160/200/250* Applies to: *OAE120CB* Applies to: *TAE500*

The following WLAN support is built into Autopilot vehicles as *Standard*.

Wireless client	Embedded Wi-Fi (WPA supplicant) CVC700
Frequency bands	2.4 GHz, 5 GHz
Channels	1, 6, 11 (for 2.4 GHz), 1, 2a, 2c, 3 (5 GHz)
Sticky client	No
Pre-shared key authentication support	Yes
Static IP address	Yes, one per vehicle

Standards

Communication with the Autopilot is managed over WLAN according to IEEE 802.11 a/b/g/n/ac standard, the Autopilot is equipped with antennas supporting both 2.4 GHz and 5 GHz communication.

- 802.11 a 54MBit/s (UNII channel: 5 GHz)
- 802.11 b 11MBit/s (ISM channel: 2,4 GHz)
- 802.11 g 54 Mbit/s (ISM channel: 2,4 GHz)
- 802.11 n 65 Mbit/s (ISM channel: 2,4 GHz or UNII channel: 5 GHz(single-stream))
- 802.11 ac 433 Mbit/s (UNII 1, 2a, 2c, 3 (5 GHz)
- MU-MIMO Support (Multi-user, multiple-input, multiple-output technology) 2gen 802.11ac both client and AP needs to support the same standard (spatial stream switching).

Encryption The following encryption modes are supported:

- WEP (64/128) (not recommended due to low security)
- WPA-PSK (TKIP & AES/CCMP)
- WPA2-PSK (TKIP & AES/CCMP)

IMPORTANT: TMHE products do not support WPA/WPA2 mixed mode.

Note: Other needs than mentioned above, might require an external bridge which must be ordered as an *Option*. It is important to involve TMHMS in the solution to secure the CE-marking.

Back to IT requirements

Go to: *IT requirements for T-ONE 2.1 - 2311, Integration specifications and IT requirements archive for T-ONE 2.1* or *IT requirements for T-ONE 1.X - all versions*.

6. Native redundancy support in T-ONE 2.1

IMPORTANT: Redundancy in terms of mirrored T-ONE installations (failover) is **not supported**.

MongoDb, MS SQL, and Elasticsearch are backed up to a local folder on the Linux host specified during the installation.

SQL and MongoDB backups are by default kept for 7-days and then discarded.

Elasticsearch keeps data based on retention policies.

6.1. Customer backup requirements

The customer must secure the T-ONE backup volume with a backup system.

For more information on setting up and restoring backups, see *Setting up and restoring backups in T-ONE 2.1*.

6.2. Back to IT requirements

Go to: *IT requirements for T-ONE 2.1 - 2311*

7. Making changes to IT infrastructure for T-ONE 2.1

Before making changes to the server environment in an existing T-ONE system, IT requirements must adhere to the installed T-ONE version. Changes that do not adhere to the IT requirements can negatively affect system performance, or cause failures and undesired behaviour.

IMPORTANT: Kollmorgen License Manager replaces fingerprint checks.

Examples of server environment changes

Changes include, but are not limited to:

- Updating to a **later version** of the operating system.
- Changing **firewall settings** in a way that conflicts with the ports required for operation of the system, as described in *5.7. Network ports used by T-ONE 2.1*.
- Changing the **hardware** in a way that makes it not adhere to requirements, as listed in *1. Hardware requirements for T-ONE 2.1*.

7.1. Back to IT requirements

Go to: *IT requirements for T-ONE 2.1 - 2311*.