MiR Network and Wi-Fi Guide

Date: 03/2023

Version: 2.8 (en)

Copyright and disclaimer

Mobile Industrial Robots A/S (MiR) makes no warranties, expressed or implied, in respect of this document or its contents. In addition, the contents of this document are subject to change without prior notice. Every precaution has been taken in the preparation of this document. Nevertheless, MiR assumes no responsibility for errors or omissions or any damages resulting from the use of the information contained.

MiR authorizes you to view, copy, print, and distribute materials available in this document provided that:

- The materials are used for internal informational purposes only.
- A MiR copyright notice appears on every copy of the material and any portion thereof.
- No materials or related graphics are modified or altered in any way. Any rights not expressly granted herein are reserved by MiR.

Original instructions (English)

Contact the manufacturer:

Mobile Industrial Robots A/S
Emil Neckelmanns Vej 15F
DK-5220 Odense SØ

www.mobile-industrial-robots.com
Phone: +45 20 377 577
Email: support@mir-robots.com

CVR: 35251235

Table of contents

1. About this guide

This guide describes necessary and recommended setups of your network infrastructure, both wired and wireless, for your MiR solution to work optimally.

MiR products are highly dependent on the network quality and especially the Wi-Fi, since Wi-Fi is integral to facilitate communication with the robots and the rest of the setup. A poor Wi-Fi setup will result in:

- Latency between user or fleet commands and robot execution
- Unreliable connection to the robot or fleet interface
- Unreliable connection and slow synchronization between robots and MiR Fleet
- Poor resource management with MiR Fleet
- Poor Collision avoidance coordination between robots connected to MiR Fleet

1.1 Version history

This table shows current and previous versions of this document.

Revision	Description
2.8	**Date:** 2023-03-27 • Styling corrections. Affects the whole guide. • Added new front page.
2.7	**Date:** 2023-02-17 • Added Wi-Fi generations to each network standard. Affects the whole guide. • Added section: Wi-Fi watchdog. • General improvements throughout the manual.

Revision	Description
2.6	**Date:** 2022-08-11 • Added information that only some robots' internal antennas are only designed for 2.4 GHz. Affects section: Robot modifications. • Updated the styling in the version history table. Affects section: Version history.
2.5	**Date:** 2022-04-28 • Updated port overview. Affects section: Ports. • Updated network performance. Affects section: Evaluating the network performance. • Added section: Network architecture.
2.4	**Date:** 2021-10-28 • Added warnings against modifying robot and violating compliance. Affects section: Improving your Wi-Fi setup. • Updated for robots that no longer have an internal access point.
2.3	**Date:** 2021-04-13 • Improved description of using hidden SSIDs. Affects section: SSID and roaming considerations • Added diagram of required ports.

Revision	Description
2.2	**Date:** 2020-09-15 • Added clarification of data rate and bandwidth requirements. Affects section: Requirements for WLAN. • Added recommendation to not use hidden SSIDs. Affects section: SSID and roaming considerations • Minor corrections throughout the manual.
2.1	**Date:** 2020-05-08 • Added ports required for AI camera and HTTPS communication. Affects section: Ports
2.0	**Date:** 2020-15-05 • Changed title from *MiR network requirements* to *MiR network and Wi-Fi guide*. • Added sections describing how to evaluate and improve your Wi-Fi setup for MiR products.
0.7	**Date:** 2020-12-02 • Protocol requirement note added. Affects section: Network security • Subnet note added. Affects section: IP configuration.
0.6	**Date:** 2019-23-10 • Minor updates and additions to requirements for WLAN. Affects section: Requirements for WLAN.

Revision	Description
0.5	**Date:** 2019-13-02 • MiR500 and MiR Fleet added to scope. • Changes to sections Network security and Ports.
0.4	**Date:** 2018-20-08 • Full rework of manual, including new sections.
0.3	**Date:** 2018-21-02 • Protocol errors corrected. Affects section: Ports
0.2	**Date:** 2017-06-11 • Release review.
0.1	**Date:** 2017-13-09 • First edition.

1.2 Where to find more information

On MiR Support Portal you can find the following resources under **Documentation**:

- **Risk assessment guide** describes how to conduct a risk assessment and provides some risk assessed use cases.
- **Commissioning guide** provides examples and guidelines to commission your robot successfully.
- **Operating guides** describe how to set up and use MiR accessories or supported functions that are mainly hardware-based, such as charging stations and shelf functions.

- **Getting started guides** describe how to set up MiR accessories that are mainly software-based, such as MiR Fleet.
- **Interface guides** contain descriptions of all the elements of the robot interface and MiR Fleet interface. Interface guides are available in multiple languages.
- **Best practice guides** provide helpful information you can use when commissioning or operating your robot.
- **REST API references** for MiR robots, MiR Hooks, and MiR Fleet. HTTP requests can be used to control robots, hooks, and MiR Fleet.
- **MiR network and Wi-Fi guide** specifies the performance requirements of your network and how you must configure it for MiR robots and MiR Fleet to operate successfully.
- **Cybersecurity guide** provides important information and instructions to increase the cybersecurity of your MiR product.
- **How-to guides** are short guides providing instruction for maintenance, replacement, commissioning, and other tasks related to MiR products.
- **Troubleshooting guides** can help you determine the cause of an issue you are experiencing with your MiR product and how to resolve it.

2. Network requirements

For your MiR application to function optimally, there are certain configurations and requirements that must be fulfilled. The following sections describe how the network must be set up.

2.1 Network architecture

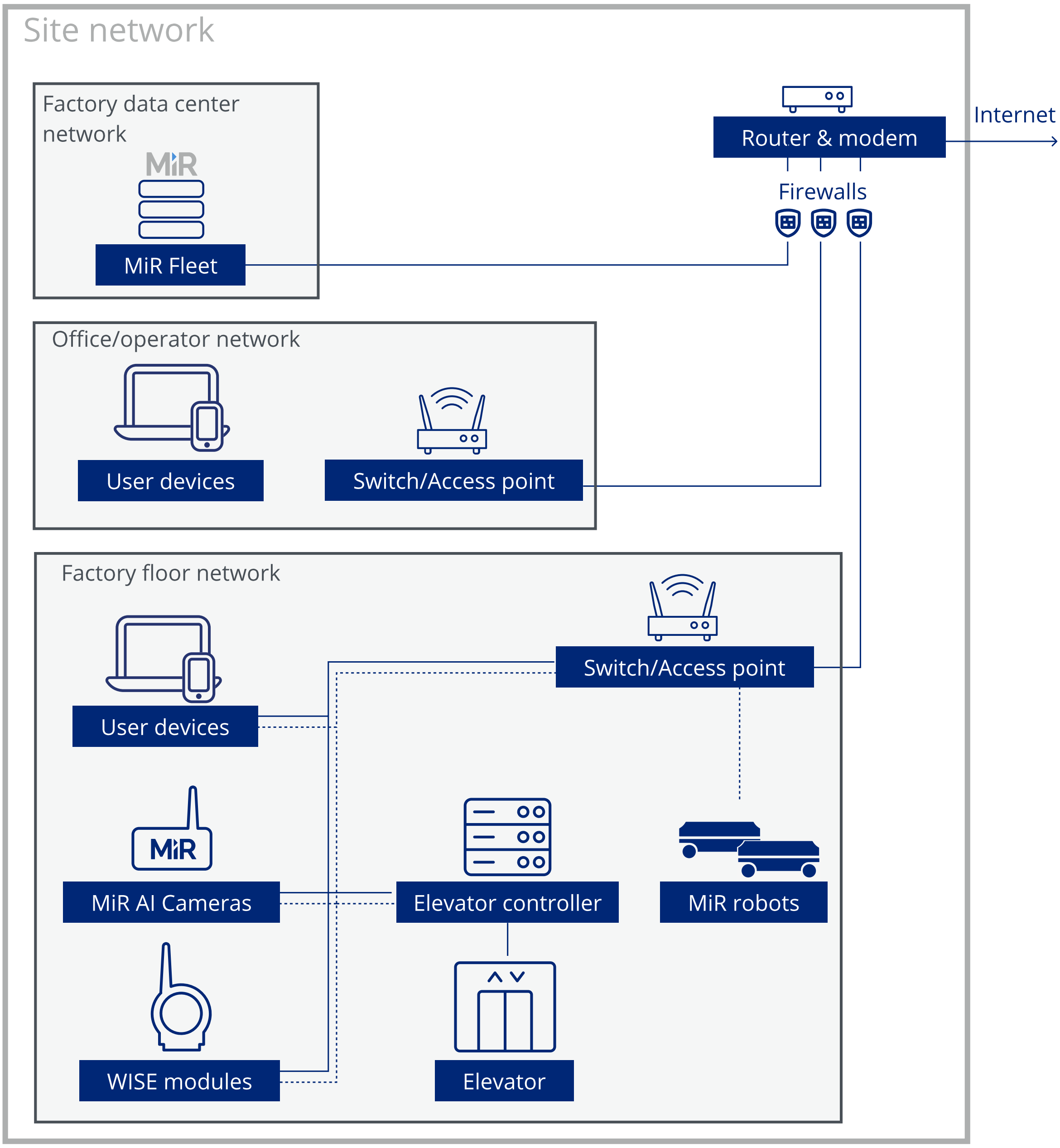
This section describes the basic network architecture you should employ for your MiR system.

Local site network

On the local network level, your setup should be something similar to Figure 2.1. This permits anyone on the site network to communicate with the MiR robots. The key elements are:

- A main router that connects all of the site's sub-networks.
- Each sub-network should have a least one access point or switch to connect devices to. This is used to connect all devices in that network to the main router.
- If you use MiR Fleet, it should connect directly to the main router if possible.
- Robots must be able to connect wirelessly to the access points that cover the area they operate in.
- Additional elevators, WISE modules, MiR AI Cameras, and other user devices can use a wired or wireless connection to an access point or switch that connects it to the main router.

Figure 2.1 Diagram of the local network at your site with MiR robots.



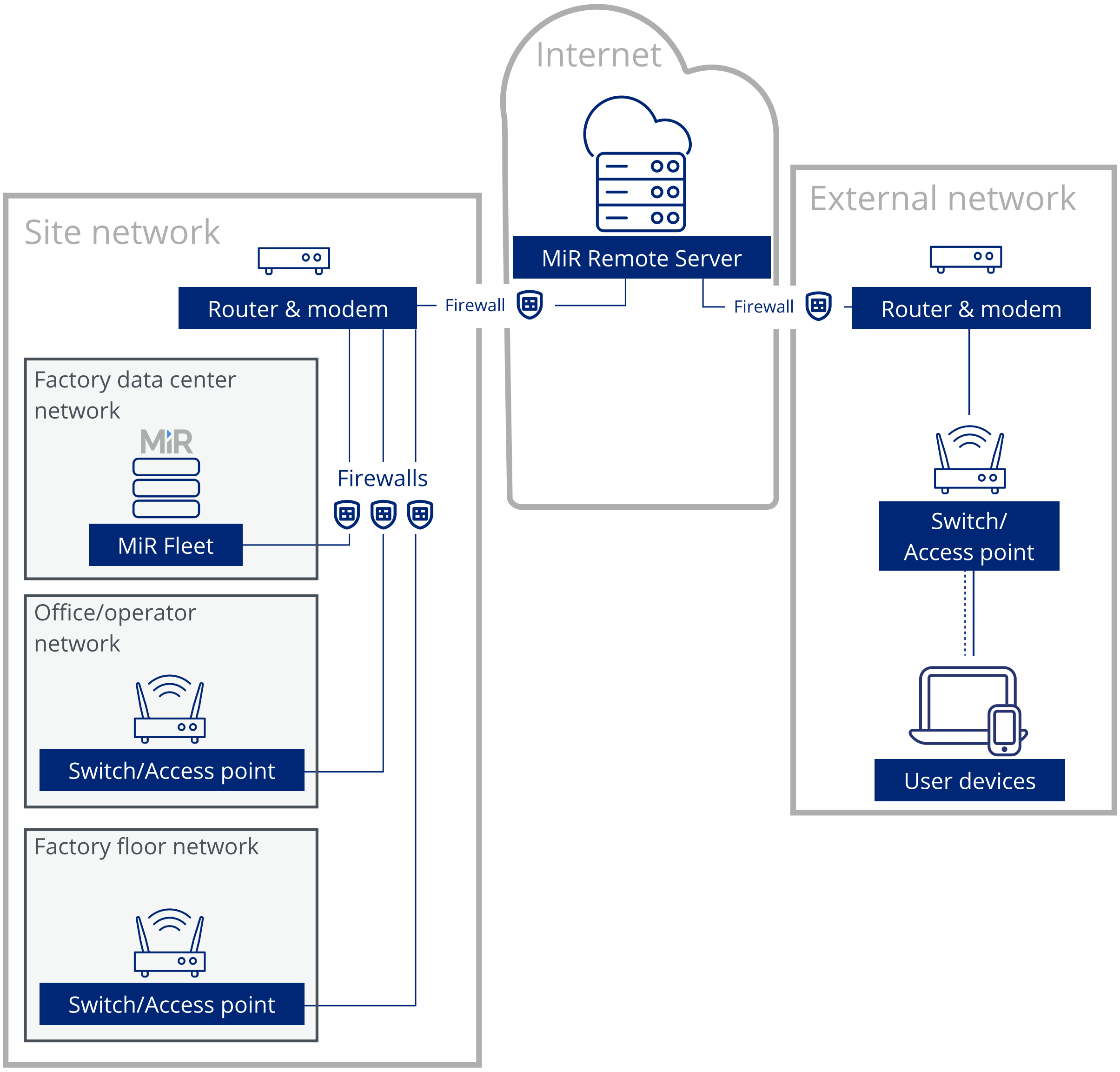
Connection to external network

If you want to be able to control or monitor MiR robots while off-site or use features such as Remote support, your local site network must connect to the internet.

For Remote support to work, your robot must be able to establish an outbound communication to the MiR Remote Server. Once established, MiR Technical Support can access your robot and help troubleshoot the issue.

If you want to access your robots while off-site, you can set up a VPN to connect to your site network.

Figure 2.2 Diagram of how MiR's Remote support or other network can connect to your MiR setup.



2.2 Requirements for WLAN

For the robots to operate well, it is important that your network fulfills certain requirements. Depending on your setup, the requirements may differ, but for a Wi-Fi setup used by both MiR robots and other devices, it is often suitable to meet the requirements outlined in "Requirements for WLAN" above.

Table 2.1 Guideline for network requirements

Parameter	Description	Requirement
Signal strength	The signal strength from the robots' perspectives when connected to the best access point.	Min. -67 dBm
Secondary signal strength	The signal strength from the robots' perspectives when connected to the second best access point.	Min. -75 dBm
Signal to noise ratio	Signal to noise ratio from the robots' perspectives.	Min. 20 dBm
Data rate	Rate of data communicated to and from each robot. This is the transfer speed of communications.	Min. 20 Mbps
Channel interference	Number of access points per channel available when signal strength is lowered to -85 dBm	Max. 2 AP/ch at -85 dBm
Latency (round trip time, ping)	Time taken to send and receive messages from robots by, for example, pinging them.	Max. 200 ms

Parameter	Description	Requirement
Bandwidth	The amount of data that can be transmitted over time. Must support 1 Mbps for each robot on the network. The data rate and bandwidth requirements should be interpreted as that the network must support robots sending and receiving 1 Mb of data every second with a transfer rate of at least 20 Mbps.	Min. 1 Mbps/robot
Packet loss	Percentage of communication packets that can be lost.	Max. 2%

Additionally, your network must fulfill the following requirements:

- There must be full Wi-Fi coverage throughout the traveling path of all robots. You can evaluate this using heatmaps—see "Wi-Fi heatmap" on page 22.
- There must be a WLAN controller to secure that roaming happens at the correct time and without any authentication errors. Make sure that the company network access points are controlled by the same controller.
- The access points must be set up to communicate and share roaming information.
- Make sure that load balancing on the access points is disabled. The robots must be able to roam freely.
- Airtime balancing must be disabled if possible. This setting changes how much time a device gets on the network depending on the signal strength. Low-signal devices get less time than high-signal devices. This means that a robot that is far away will be allowed less data than a robot that is close by.

ⓘ The robots are able to perform some tasks under worse conditions than mentioned above. However, key features in MiR Fleet such as Collision avoidance, Auto charging and staging, Limit-robots zones, data synchronization between robots, and fleet mission execution will not work optimally or at all.

Network capacity

To meet the requirements, you must ensure that your network has the capacity to handle the number of devices connected to it. Determine the following:

1. The number of devices that are connected to the network.
2. How much data the devices are transferring at the same time on a busy work day.
3. How many access points are required to ensure that all devices are connected and can transfer data without using over 50% of the access points' capacity.

If anything more than 60% of the Wi-Fi channel is being used, MiR robots will be affected by latency and packet loss.

2.3 Requirements for MiR Fleet

- MiR Fleet should be connected to the network through a wired connection.
- MiR Fleet must be in the same physical location as the robot. Geographical distance will cause delay between MiR Fleet and robots.

2.4 Wireless network standards

MiR robots can use the following wireless network standards:

- **802.11a (Wi-Fi 2)**
- **802.11b (Wi-Fi 1)**
- **802.11g (Wi-Fi 3)**
- **802.11n (Wi-Fi 4)**
- **802.11ac (Wi-Fi 5)**

In software 2.13.0.2 or higher, you can enable **Improved Wi-Fi settings** where it is possible to modify which frequencies each robot uses on either 2.4 GHz or 5 GHz bands. If you have not specified any channels, MiR robots connect to the best possible channel it has access to.

2.5 IP configuration

By default, the robot is set up to use DHCP, but the robot can also be set up with a static IP from the robot interface. If you use this option, you can specify the IP, netmask, DNS, and gateway for the robot's Wi-Fi connection.

When connected to MiR Fleet, each robot must have a unique static IP or a reserved DHCP assigned IP as MiR Fleet uses the IP to identify the robots.

MiR products only work with IPv4. The system is not compatible with IPv6, which is therefore disabled internally.

Due to the robot's internal network configuration, MiR robots are unable to work on an external network with subnet 192.168.12.0/24.

If you are running software 2.13.1.1 or higher, you also have the option to set the robot's default gateway IP address without a Wi-Fi connection being activated. This is useful when you want to utilize an external router or 5G CPE that is connected to the robot via Ethernet to extend the robot's wireless capabilities. For more information, see the guide *How to connect a robot using a 4G or 5G cellular modem*.

2.6 Ports

All the listed ports are needed for certain functionalities in MiR products. If any of the listed functionalities are to be used on an external network, these ports must be opened.

All ports use the TCP/IP protocol and are all inbound communications except the connection to MiR Remote.

Table 2.2 Ports used by MiR robots and MiR Fleet

Service	Port	Accessible	Description
Required for SW 2.10.0 and higher			

Service	Port	Accessible	Description
HTTPS, REST API, and WSS	443	WLAN and direct connection (Ethernet cable or Wi-Fi via the router hotspot)	Used to access the robot interface and for communication through REST protocol (robot and fleet interface actions, MiR Fleet, WISE modules) through HTTPS.
WebSocket	9090	WLAN and direct connection (Ethernet cable or Wi-Fi via the router hotspot)	Used for ROSbridge. Communication between certain robot functions and the robot interface.
Required for SW 2.9.0.1 and lower			
HTTP	80	WLAN and direct connection (Ethernet cable or Wi-Fi via the router hotspot)	Used to access the robot interface through HTTP.
REST API	8080	WLAN and direct connection	Used for communication through the REST protocol (robot and fleet interface actions, MiR Fleet, WISE modules) through HTTP.

Service	Port	Accessible	Description
WebSocket	9090	WLAN and direct connection (Ethernet cable or Wi-Fi via the router hotspot)	Used for ROSbridge. Communication between certain robot functions and the robot interface.
Optional for all SW versions			
Recovery page	8888	Direct connection (Ethernet cable or Wi-Fi via the router hotspot)	Used to access the recovery robot interface. This interface allows you to connect the robot to a Wi-Fi network, connect it remotely for technical support, or restore to an old version of the software or the database.
Modbus	502	WLAN and direct connection (Ethernet cable or Wi-Fi via the router hotspot)	Required if Modbus is used through the company’s network.
SSH	22	WLAN and direct connection (Ethernet cable or Wi-Fi via the router hotspot)	Used for access through SSH (Secure Shell) for MiR personnel.

Service	Port	Accessible	Description
MiR Remote	80	WLAN	When you select **Connect to MiR Remote** in your robot's interface, an outbound connection is made to the MiR Remote server address ssh.mir-robots.com. Once established, inbound communications via this connection must also be permitted.
MiR AI camera	1908	Direct connection (Ethernet cable or Wi-Fi via the router hotspot)	Used for communication to MiR AI Cameras. You will also need port 80 to be open.
Elevator - OPC UA	4841	Direct connection (Ethernet cable or Wi-Fi via the router hotspot)	Used for communication with elevators with OPC UA drivers.
Elevator - Hitachi	4840	Direct connection (Ethernet cable or Wi-Fi via the router hotspot)	Used for communication with elevators with Hitachi drivers.

Communication examples

The following are simple examples of common communications established with or between MiR products. Depending on how you have segmented your network, it may be necessary to implement network policies to accommodate the MiR product communication traffic patterns to ensure they work as expected.

Connecting to the robot or MiR Fleet interface through HTTPS (SW 2.10.0 or higher)

You initialize this communication by contacting the robot or MiR Fleet web server on port 443/TCP.

When the interface loads, the web browser initializes a WebSocket Secure connection from your device to the robot or MiR Fleet via port 443/TCP. If you are connecting to the MiR Fleet interface, the browser will also initialize the WebSocket Secure connection to each robot connected to MiR Fleet.

MiR Fleet communication to the robot through HTTPS (SW 2.10.0 or higher)

MiR Fleet initializes the communication to MiR robots on port 443/TCP. All communication between MiR Fleet and the connected robots is done via REST.

Connecting to the robot or MiR Fleet interface through HTTP (SW 2.9.0.1 or lower)

You initialize this communication by contacting the robot or MiR Fleet web server on port 80/TCP.

When the interface loads, the web browser initializes a WebSocket connection from your device to the robot via port 9090/TCP. If you are connecting to the MiR Fleet interface, the browser will also initialize the WebSocket connection to each robot connected to MiR Fleet.

MiR Fleet or MiR robots connecting to MiR Remote

You initialize the communication when you select **Connect to MiR Remote** in the user interface. When you select **Connect to MiR Remote**, the robot or MiR Fleet will attempt to establish an outbound communication to the MiR Remote Server hosted at ssh.mir-robots.com via port 80/TCP.

2.7 DNS

MiR robots can work with company-specific DNS servers. By default, the robots have the Google DNS: 8.8.8.8 and 8.8.4.4.

2.8 Network security

MiR robots support different security protocols for wireless networks. All compatible protocols are listed below:

- WPA/WPA2 Personal
- WPA/WPA2 Enterprise:
  - LEAP
  - PEAP
  - EAP-TLS: Certificates only accepted in .pem or .p12 format.

WPA/WPA2 Enterprise requires the server to support TLS 1.2 or higher. MiR robots will not connect to the network using TLS 1.0 or older SSL encryption.

MiR robots can also connect to a hidden SSID. However, you should avoid using them.

3. Planning your network

MiR strongly recommends consulting a Wi-Fi specialist to help determine and implement a sufficient wireless network infrastructure for your MiR application.

The following sections provide guidance for how you can plan and determine a suitable Wi-Fi network setup.

3.1 Site map and access point positions

The placement of access points is dependent on multiple factors. The wireless signal can easily be degraded or lost if there are walls, shelves, or other obstacles in the way.

MiR recommends that a network report is drawn up.

The ideal report should document every detail of the network, such as:

- Current access point positions
- Current performance
- Signal coverage
- Interference
- Channel allocation
- Radio frequencies used (2.4 GHz/5 GHz)
- SSID(s) offered

The report should evaluate the network needs and how they can be achieved. For example, if additional or a new generation of network equipment is needed, access points need to be relocated or equipped with different antennas, channel allocation should be altered, or more advanced configuration of the WLAN controller is required.

MiR recommends consulting a map of the entire site and identifying the positions of current access points or determining the ideal location for new access points. To help determine where access points would be best positioned, label the map with information such as:

- Infrastructure that may pose issues to the wireless signals, such as concrete walls and metal structures especially.
- For each access point note down:
  - The SSID (or SSIDs) exposed by the access point
  - The channel used
  - The radio frequency: 2.4 GHz or 5 GHz
- Devices or machinery that generate radio frequencies that may interfere with the access point signals, such as microwave ovens, cordless phones, and Bluetooth-enabled devices.
- The number of physical obstacles that are often within each room or building, and whether there are people there who are likely to have personal devices such as phones or tablets. These devices and the density of people can also affect the wireless performance.

3.2 Wi-Fi heatmap

Consult a Wi-Fi expert to execute a site survey including a heatmap that you can use to identify any area with weak coverage. It is important that there is a strong Wi-Fi signal everywhere across the site where MiR robots operate.

If you have MiR robots that are already operating on your site, you can use an error log from a MiR robot or MiR Fleet to generate a Wi-Fi heatmap based on their connection to the network. For more information about how to evaluate this, see "Evaluating the network performance" on page 32 or the guide *How to use MiR Log Analytics*.

If there are areas that are not covered, see "Improving your Wi-Fi setup" on page 23 for suggestions on how you can improve your Wi-Fi setup.

4. Improving your Wi-Fi setup

If you have determined that your Wi-Fi setup is not sufficient, there are multiple methods to improve your Wi-Fi coverage. MiR recommends consulting a Wi-Fi specialist to identify the best way to improve your setup. The following sections outline suggestions that you and the Wi-Fi specialist can consider to improve the Wi-Fi coverage.

If it is only some of your robots that have connection issues in certain areas, consider modifying those robots as described in "Robot modifications" on page 29. Applying any modification to the robot violates the compliance of the robot and it must be reevaluated to ensure compliance with national requirements

4.1 Radio frequency interference

If you have identified any access points that are located close to devices that generate radio frequency, you should consider the following:

- Monitor whether MiR robots experience issues around the radio frequency source. If they do, try to move the access point further away from the radio frequency source and see if this improves the performance of the robots in the area.
- Shield the noise source so it does not radiate frequency interference.
- Consider switching radio frequency (from, for example, 2.4 GHz to exclusively using 5 GHz).
- Try to arrange access points so they are within direct line of sight of each other.

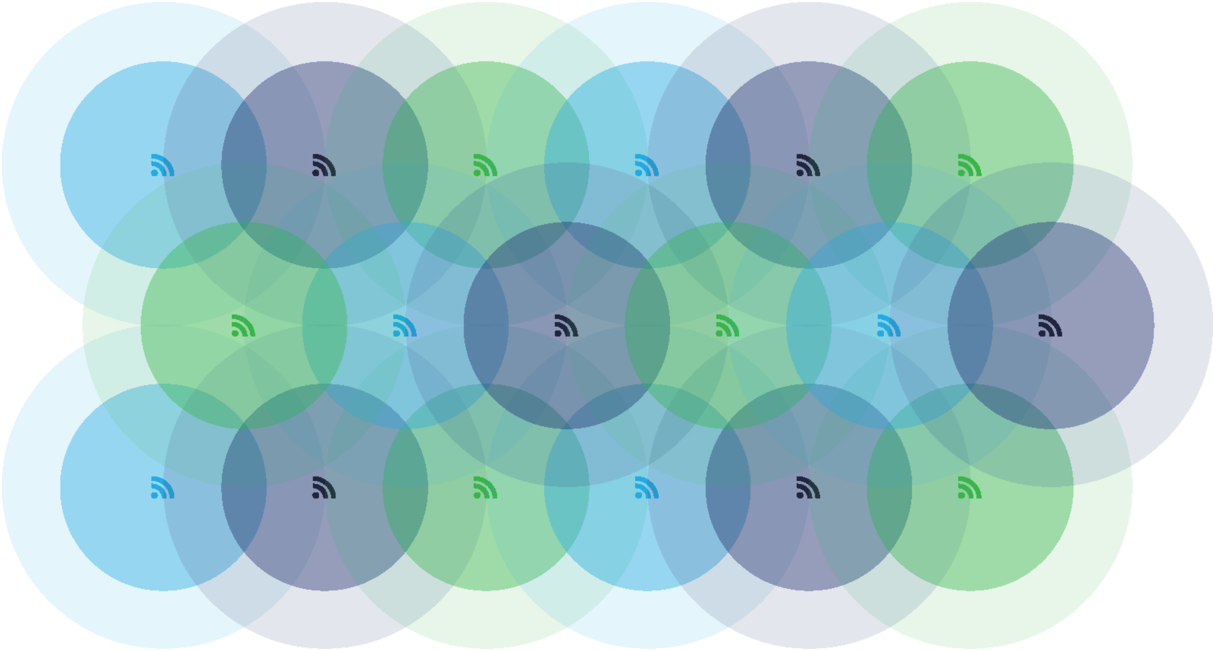
Note that it does not matter whether it is the access point or the robot that is close to the interference source; if either of them are close to the interference, communication can be disrupted.

4.2 Channel planning and overlapping coverage cells

Although radio frequency can interfere with the Wi-Fi signals, the Wi-Fi signals are affected more often by other Wi-Fi signals. To minimize this interference, it is important to arrange and configure your access points as follows:

- Make sure that neighboring access points run on different channels.
- Ensure there is only enough overlap between access point coverage areas to ensure a safe handover when a robot reassociate from one access point to the other.

Figure 4.1 Illustration of a simplified scenario where access points cover a circular area in a site without any interference from structures or other devices. In this case three Wi-Fi channels are used, and the access points are configured so there is the greatest distance possible between access points on the same channel.

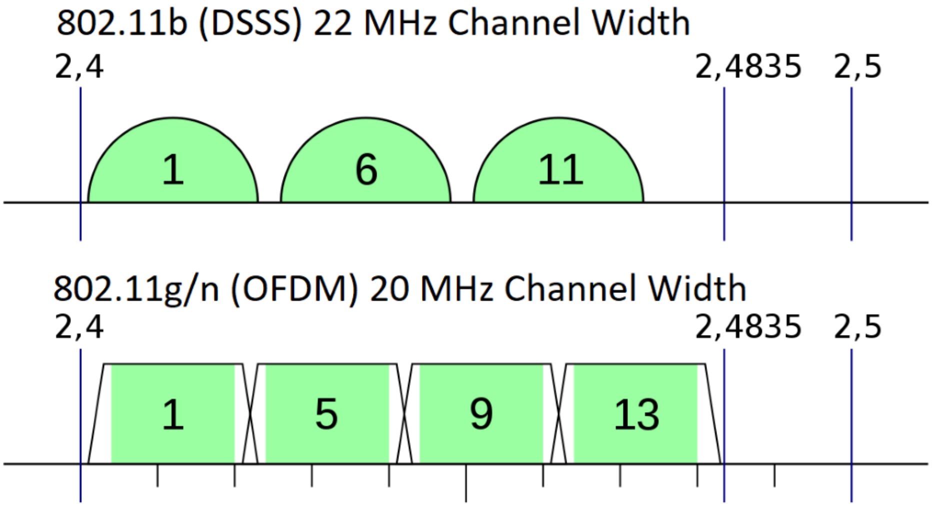


Channel planning 2.4 GHz

When you are using a 2.4 GHz band, always use a channel width of 20 MHz per access point, and avoid using channels where the frequencies overlap. Since channels are divided by only 5 MHz, you should only use channels with four or five channel intervals to avoid channels interfering.

In principle, 802.11n (Wi-Fi 4) allows assigning two channels (40 MHz) per access point, but that interferes with too many channels and is only useful in simple cases with few access points.

Figure 4.2 Channel separations on 802.11b (Wi-Fi 1) and 802.11g (Wi-Fi 3) standards.


802.11b (DSSS) 22 MHz Channel Width
2,4
2,4835
2,5
1
6
11
802.11g/n (OFDM) 20 MHz Channel Width
2,4
2,4835
2,5
1
5
9
13

There are two possible channel selections:

- If you are within the North American region, there are 1-11 channels available. To avoid interference between channels, only use channels 1, 6, and 11.
- If you are using 802.11b (Wi-Fi 1), the channels have a width of 22 MHz. To avoid interference between channels, only use channels 1, 6, and 11.
- If you are outside of North America and are not using 802.11b (Wi-Fi 1), there are often 1-13 channels available. To avoid interference between channels, only use channels 1, 5, 9, and 13.

Channel planning 5 GHz

There are significantly more channels available on a 5 GHz band. The available channels are region dependent. To determine which channels you can use in your region, consult a Wi-Fi specialist or your local governmental body in charge of the regulatory domain for 5GHz.

All channels on a 5 GHz band have a frequency width of 20 MHz or a multiple of 20 MHz. Channels on a 5 GHz band are also divided by 5 MHz intervals, meaning that only every four channels are defined to ensure there is no overlap between channel frequencies.

If a sufficient number of channels is available to avoid interference, it can be advantageous to use two channels (40 MHz) per access point. When an access point uses two channels, it is able to transfer data twice as fast to and from the connected robots. Keep in mind, if each access point uses two channels, the number of available frequencies is halved. You must ensure that you can keep the coverage area of access points that are using the same channels separated—see Figure 4.1.

For access points where the channel utilization is especially high, you can also use four channels (80 MHz) per access point. This can be efficient if only a few clients with high bandwidth requirements are connected. This is often not required for MiR products.

Increasing Wi-Fi capacity with channel planning

To improve the Wi-Fi capacity you can adjust your channel configuration as follows:

- If there are a sufficient number of available channels, you can add more access points that are not using interfering channels, or increase the bandwidth used by each access point.
- If all available channels are in use, you can minimize the area of interference by reducing the transmission power per access point. This will also shrink the coverage area. Make sure these do not drop below the required value.
- To focus the signal strength within the coverage areas without increasing the signal strength in interference areas, you can use directional antennas.
- Both 2.4 GHz and 5 GHz have advantages and disadvantages.
  - **2.4 GHz:** Has longer range and is better at penetrating metal and concrete, but it is limited to three main channels and transmits data at lower speeds. Fewer channels result in signal noise, and most production environments have a very high noise floor on the 2.4 GHz band. Many technologies can create noise on the 2.4 GHz band, such as USB and Bluetooth.
  - **5.0 GHz**: Has shorter range and not as good performance traveling through obstacles as 2.4 GHz, but there are more main channels available, and it transmits data at higher speeds. The exact number of channels depends on the region you are in.

4.3 Minimum data rate

Setting the minimum data rate can improve a robot's ability to roam well between access points and improve the utilization of the Wi-Fi capacity. The default minimum data rate for legacy 802.11b (Wi-Fi 1) is 1 Mbps and for newer standards it is 6 Mbps. The following points describe why you may want to change the minimum data rate:

- Access points transmit beacons at the lowest available data rate per SSID. With a low data rate, a significant percentage of the capacity is wasted on transmitting beacons. With a high data rate, the beacons are transmitted faster and utilize less of the network capacity.
- Increasing the minimum data rate will make robots search for access points where they can transfer data faster. Many Wi-Fi clients stick to an access point for as long as possible before changing, even if they can connect to access points with a stronger signal.

- The Wi-Fi utilization is also improved, since robots do not spend as much time transferring data at low rates through access points where their connection is poor. With better roaming, the robots will spend more time transferring data through access points with a faster data rate.

At sites with good and stable Wi-Fi coverage, it can be an advantage to increase the minimum data rate to 12-24 Mbps. High density 5 GHz deployments may have an even higher optimal minimum data rate.

On sites where the Wi-Fi coverage often varies, for example in warehouses where the Wi-Fi is affected by changing inventory, it may be necessary to keep the minimum data rate low, to ensure that robots are always able to connect to an access point.

4.4 SSID and roaming considerations

If you are using multiple SSIDs, you should consider the following:

- Access points can transmit multiple SSIDs where each SSID provides a logical separation between different networks. All SSIDs and access points on the same frequency share the same physical channel. Traffic on one SSID will degrade the performance (latency, packet loss, and data rate) on other SSIDs on the same channel. For this reason, critical SSIDs should therefor use their own channel, while secondary SSIDs can use another.
- Each SSID broadcasts a beacon at the minimum data rate. If the minimum data rate is high, adding additional SSIDs does not impair the capacity significantly, but at low minimum data rates, the number of SSIDs should be limited to the ones you really need.

When configuring roaming (changing to an access point with a better signal), you should consider the following:

- For roaming to work, the access points must use the same SSID, use the IP addresses of the same network segment, and be in the same VLAN.
- To ensure the robots transition to other access points smoothly, there must be good secondary coverage. In other words, when a robot moves away from one access point, the signal strength from the next access point must be good before the signal quality from the first degrades—see "Network requirements" on page 9.
- The network should support fast reauthentication to other access points. You can limit the security measures to very basic WPA2-PSK to increase the authentication speed, but there are also other options for caching the keys for authentication, which are just as fast and do not sacrifice security.

- Hidden SSIDs should be avoided when stable and optimal roaming performance is desired. While connected to an access point, a robot listens passively for beacons from other access points and creates a list of options to roam to. Hidden SSIDs don't broadcast their name in beacons, making it impossible for the robot to construct this list in advance. In order to roam in such an environment, the robot has to disconnect from its current access point and perform an active scan by sending probe requests to all the access points. Only after that, can the robot construct the list of options and pick the best candidate to connect to. Since this process requires disconnection and active scanning, it can take several seconds to complete, causing complete loss of communication in the meantime.

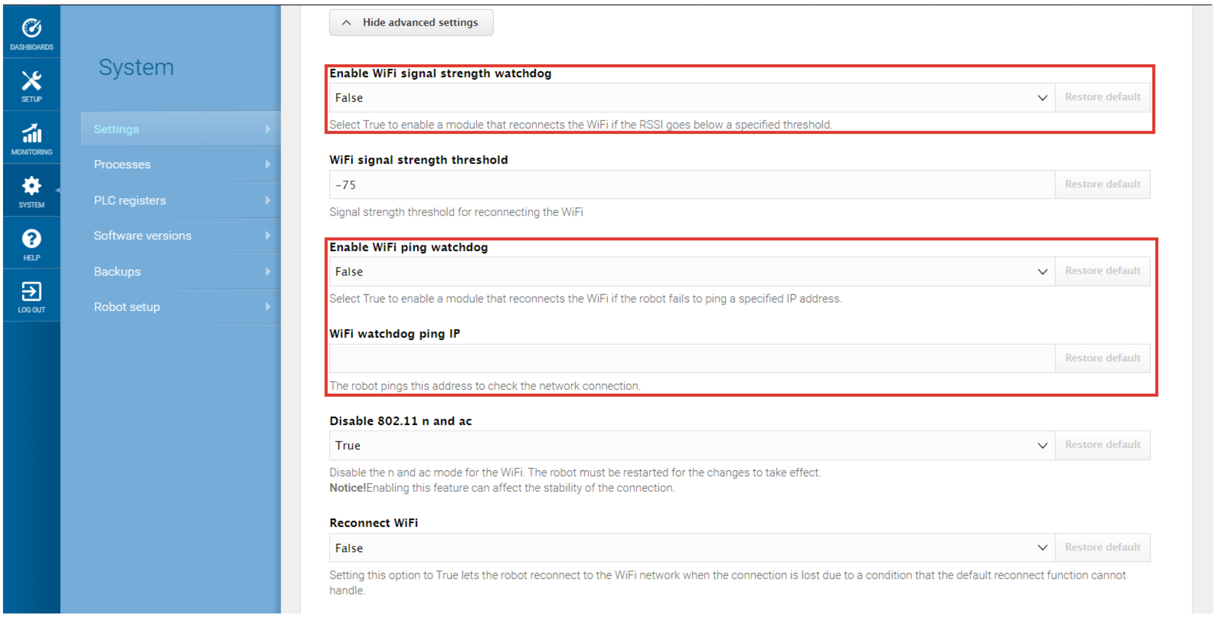
4.5 Wi-Fi watchdog

The purpose of the Wi-Fi watchdog functions is to trigger a reassociate (roaming) event because the robot's Wi-Fi daemon isn't accomplishing its task satisfactory or in time.

Wi-Fi daemon is a piece of software that manages (connects, roams, disconnects) Wi-Fi connections. The term daemon covers a program that runs continuously and handles periodic service requests that a computer system expects to receive.

MiR robots have two Wi-Fi watchdog functions that can be enabled in the robot interface under **System > Settings > Wi-Fi > Show advanced settings**:

- Enable Wi-Fi signal strength watchdog
- Enable Wi-Fi ping watchdog



Enable WiFi signal strength watchdog
False
Select True to enable a module that reconnects the WiFi if the RSSI goes below a specified threshold.

WiFi signal strength threshold
-75
Signal strength threshold for reconnecting the WiFi

Enable WiFi ping watchdog
False
Select True to enable a module that reconnects the WiFi if the robot fails to ping a specified IP address.

WiFi watchdog ping IP

The robot pings this address to check the network connection.

Disable 802.11 n and ac
True
Disable the n and ac mode for the WiFi. The robot must be restarted for the changes to take effect.
Notice!Enabling this feature can affect the stability of the connection.

Reconnect WiFi
False
Setting this option to True lets the robot reconnect to the WiFi network when the connection is lost due to a condition that the default reconnect function cannot handle.

Do not enable the signal strength watchdog and the ping watchdog simultaneously as they function better when only one is used.

Enable Wi-Fi signal strength watchdog

The Enable Wi-Fi signal strength watchdog function enables a module that reconnects the Wi-Fi if the RSSI (Received Signal Strength Indicator) goes below a specified threshold. The function monitors the RSSI level and compares it to the default or user configured threshold value. When the value dips below the threshold, a reassociate (roaming) event is triggered.

Be aware that if the threshold has been set to an unobtainable value, it will cause the RSSI watchdog to trigger reassociation events (forced roaming). In that case, the Wi-Fi connection gets temporarily terminated continuously for no reason.

Enable Wi-Fi ping watchdog

The Enable Wi-Fi ping watchdog function enables a module that reconnects the Wi-Fi if the robot fails to ping a specific IP address. The function uses ICMP (Internet Control Message Protocol) packages to determine if the Wi-Fi link is strong enough to carry a minimum size payload.

Be aware that if you configure the ping watchdog to ping against the server hosting the Fleet, you are not only testing if the Wi-Fi link is sound, but also the connection to the rest of the network and the server hosting the Fleet.

In many cases where the ping watchdog causes a lot of reassociation events (forced roaming), it is because the ping destination is unreachable for some reason. Most often the Wi-Fi link is healthy, and the issue is somewhere else, for example, the router, switch, or server. In that case, the Wi-Fi connection gets temporarily terminated continuously for no reason.

4.6 Robot modifications

> **NOTICE**
> A MiR robot is only approved for use with the antennas it is designed with. Harmful electromagnetic interference with other products is potentially the result of using an antenna with stronger gain.
>
> Ensure compliance with national requirements if you decide to replace or modify an antenna or mount an additional antenna on the robot.

There are a few modifications you can apply to robots to improve their connection to the network:

- Robots are equipped with internal antennas—see the user guide for your robot for the antenna locations. If your robot is carrying a payload that obscures the antenna radiation pattern (often dense and large objects), consider applying the following actions to improve the connection:
  - Reposition the payload to be at least 40 mm away from the antennas.
  - If your top module enables it, mount an external antenna where interference from the payload is minimized. It is the responsibility of the modifier to ensure that the robot still complies to national requirements. See the *Optional features* list for antennas provided by MiR.
- The internal antennas used by MiR100, MiR200, MiR500, and MiR1000 are only designed for 2.4 GHz. It can be beneficial to replace them with an antenna more suited for your wireless network. This will violate the compliancy of the robot and will require a reevaluation of the compliancy. It is the responsibility of the modifier to ensure that the robot complies to national requirements.
- Some robots have an internal wireless access point that broadcasts a hotspot you can use to connect to the robot.

  ⓘ The internal access point has been removed in newer robots. If your robot does not broadcast a Wi-Fi hotspot, you can disregard this solution.

  If your robot does have an internal access point, it can interfere with other access points. Consider applying the following actions to improve the connection:
  - Turn off the access point on the robot to eliminate the interference. If you need to access the web-interface of that robot for either maintenance or to control it manually, you will need to connect to it via an Ethernet cable.
  - Dedicate a frequency to the robot access points that only they can use or a band that the robot's access point can use, meaning the opposite band of what the site's WLAN uses.

  ⓘ To modify the robot access points, contact MiR Technical Support for assistance.

- Software 2.13.0.2 released several changes in the Wi-Fi handling and Wi-Fi settings. To improve the connection, you can consider updating your robot to this software version of higher. After updating, under **System > Settings > Wi-Fi**, you can enable the new Wi-Fi system. When the new system is enabled, you can edit your Wi-Fi connections to scan more often and specify which channels the robot should scan on for better connections. For more information, see the guide *How to connect a MiR robot to a Wi-Fi network*.

5. Evaluating the network performance

If you meet the network requirements outlined in "Network requirements" on page 9 and are still experiencing issues with the Wi-Fi connection to your MiR robots, you can use the MiR Log Analytics tool to analyze the network from the robots' perspectives. You can use the tool to see a network heatmap that can help you identify problematic areas in your network, and you can review the communication data collected by MiR Fleet and your MiR robots. For more information about how to use the tool, see the guide *How to use MiR Log Analytics*.

Some of the main things you can look for in the data from MiR Log Analytics are:

- From a MiR Fleet error log, check that the cycle time is under 1 second all across the map. Any places where the cycle time is higher, indicates an area where the network connection may be poor. If the entire map has a high cycle time for MiR Fleet, but individual robots have a good connection to the network, it is also possible that MiR Fleet is receiving too many requests. In this case, you must review which devices are communicating with MiR Fleet and reduce the requests from devices that are not MiR robots.
- From a MiR Fleet error log, you can also filter the heatmaps to show the performance of individual robots. This is a fast way to determine if there are any robots in particular that have difficulty connecting to the network. In this case, you can try to modify the robot to improve its connection—see "Robot modifications" on page 29.
- If you do determine that a certain robot has poor network connection and the suggestions in "Robot modifications" on page 29 do not help, you can download an error log from the robot and use MiR Log Analytics to determine any other likely causes. See *How to use MiR Log Analytics* for more information about what you can determine from the data.

If you cannot determine why your MiR setup isn't performing as expected, contact MiR Technical Support and include an error log from MiR Fleet and any robots that aren't performing as expected. Make sure to generate the error log shortly after you experience any performance issues. Do not turn off your MiR products before generating the error log, otherwise useful troubleshooting data may be lost.

6. Check list

To summarize the content of this guide, when planning or modifying your Wi-Fi network it is recommended to do the following:

1. Ensure your network meets the requirements in "Network requirements" on page 9, or a set of network requirements determined by a Wi-Fi specialist for your setup.

2. If possible, disable load balancing and airtime balancing on your access points.

3. Determine if your network capacity is suitable for the number of devices connected to your network.

4. If you are using MiR Fleet, make sure that:
   - MiR Fleet is connected to the network through a wired connection.
   - MiR Fleet is in the same physical location as the robot. Geographical distance will cause delay between MiR Fleet and robots.

5. Make sure your network uses one of the following network standards:
   - 802.11a (Wi-Fi 2)
   - 802.11b (Wi-Fi 1)
   - 802.11g (Wi-Fi 3)
   - 802.11n (Wi-Fi 4)
   - 802.11ac (Wi-Fi 5)

6. If you are configuring the IP value, make sure to use IPv4.

7. Make sure you are not using subnet 192.168.12.0/24 with MiR robots.

8 Make sure the following ports are open:

- Port 80
- Port 443
- Port 8080
- Port 9090

9 Make sure you are using one of the following security protocols:

- WPA/WPA2 Personal
- WPA/WPA2 Enterprise:
  - LEAP
  - PEAP
  - EAP-TLS: Certificates only accepted in .pem or .p12 format

10 If you are using WPA/WPA2 Enterprise, make sure the network server supports TLS 1.2 or higher.

11 Determine if there are areas in your site where there is high interference from the structure, personnel, and other devices.

12 Generate a Wi-Fi heatmap to view the coverage of your access points to determine if there are areas where you need more access points, or the existing ones need to be reconfigured.

13 Check that devices generating radio frequency are not interfering with the signal from nearby access points.

14 Set up your access points so access points using the same channel do not have overlapping coverage areas.

15 Use either a 2.4 GHz or 5 GHz band.

16 Use every four channels to avoid interference.

17 Use directional antennas to focus the signals from the access points.

> **NOTICE**
> A MiR robot is only approved for use with the antennas it is designed with. Harmful electromagnetic interference with other products is potentially the result of using an antenna with stronger gain.
>
> Ensure compliance with national requirements if you decide to replace or modify an antenna or mount an additional antenna on the robot.

18 Reduce the power per access point to reduce the coverage area, but make sure the signal strength does not drop below the required value.

19 If your site has a stable and good Wi-Fi coverage, increase the minimum data rate 12-24 Mbps.

20 If you have a low minimum data rate (around 1-6 Mbps), reduce the number of SSIDs.

21 Make sure all access points the robot uses offer the same SSID, use the same VLAN, and use IP addresses within the same network segment.

22 Avoid using hidden SSIDs on your network.

23 Make sure the network supports fast reauthorization to other access points.

24 Make sure the payload of the robot is not interfering with the antenna signal by:

- Mounting an external antenna.

> **NOTICE**
> A MiR robot is only approved for use with the antennas it is designed with. Harmful electromagnetic interference with other products is potentially the result of using an antenna with stronger gain.
>
> Ensure compliance with national requirements if you decide to replace or modify an antenna or mount an additional antenna on the robot.

- Repositioning the payload at least 40 mm from the antenna.

25 For robots that can broadcast a Wi-Fi hotspot from their internal access point, you can turn off the access points on the robots to eliminate interference, or dedicate a channel that only the robot access points can use.

26 Re-evaluate all of the above points regularly as Wi-Fi is not a static thing. Performance changes with the usage pattern, the number of clients, the type of clients, and with changes to the physical environment.