Cybersecurity Guide (en)

Date: 11/2021

Revision: v.1.0

Copyright and disclaimer

All rights reserved. No parts of this document may be reproduced in any form without the express written permission of Mobile Industrial Robots A/S (MiR). MiR makes no warranties, expressed or implied, in respect of this document or its contents. In addition, the contents of the 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.

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 document

This guide contains information and instructions you must follow to ensure the cybersecurity of your MiR product.

Cybersecurity in the context of MiR products means protecting IT (Information Technology) and OT (Operational Technology) assets from unauthorized access, use, disruption, modification, or destruction. This guide describes the main cybersecurity related risks and how you minimize them when commissioning the product.

This guide has been written generically for all MiR products. It is made clear which instructions apply for which MiR products.

1.1 Where to find more information

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

- **Quick starts** describe how you start operating MiR robots quickly. It comes in print in the box with the robots. Quick starts are available in multiple languages.
- **User guides** provide all the information you need to operate and maintain MiR robots and how to set up and use top modules and accessories, such as charging stations, hooks, shelf lifts, and pallet lifts. User guides are available in multiple languages.
- **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.
- **Reference guides** contain descriptions of all the elements of the robot interface and MiR Fleet interface. Reference 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 WiFi 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.

1.2 Version history

This table shows current and previous versions of this document.

Revision	Release date	Description
1.0	2021-11-16	First edition.

2. Important security warnings

Before reading the rest of the document, ensure that you understand and have considered the following security warnings.

SECURITY WARNING

MiR products exchange critical data over the IT network that they are connected to. An attacker with access to this network can attempt to adversely affect the product. It is the responsibility of the commissioner to ensure that MiR products are connected to a secured network.

- Conduct a security risk assessment and implement adequate network security controls before commissioning the product.

SECURITY WARNING

An attacker with physical access to MiR products can attempt to tamper with them. Physical tampering can result in a complete loss of confidentiality, integrity, and availability of the products.

- Operate and store MiR products in areas with restricted physical access.

SECURITY WARNING

MiR robots shipped before July 2020 contained insecure default configurations.

- If your robot was shipped before July 2020, please contact your distributor for the guide *How to set up MiR products to improve the IT security*.

3. Managing users and passwords

Applicable for all products

Managing your users and passwords is the main way you can control access to your product.

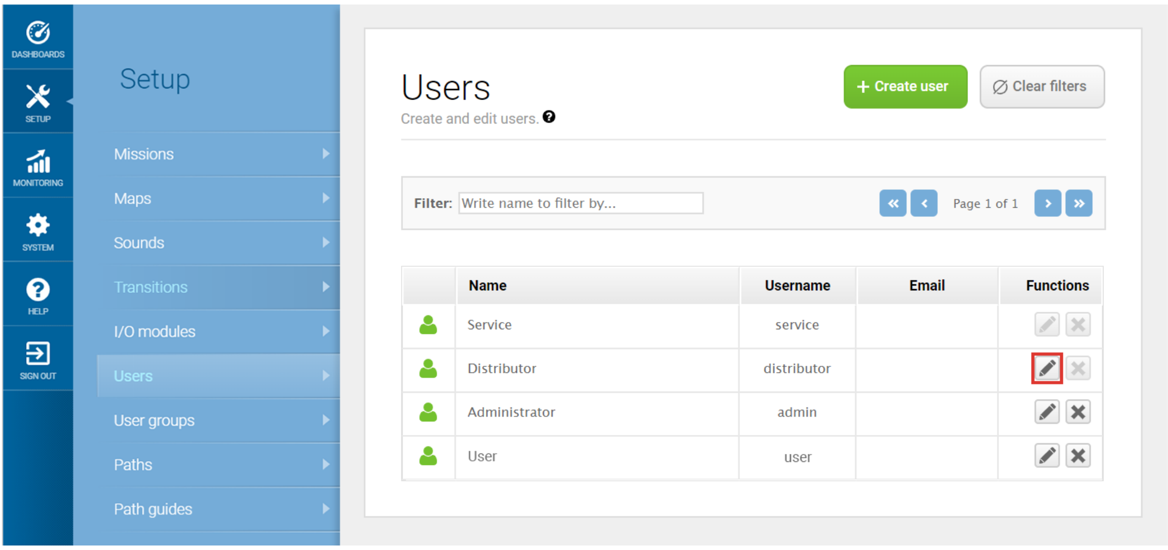
> **SECURITY WARNING**
>
> Unauthorized access to MiR products can result in safety hazards and loss of confidentiality, integrity, and availability.
>
> - Consider the recommendations in this section and implement them if possible with your setup.
> - MiR is not responsible for user and permission management and can not be held liable for damages resulting from improperly configured access control.

There are three default users with predefined passwords for you to start using. These are described in the *MiR Robot Reference Guide* along with instructions to create new users, user groups, and passwords. MiR advises you to:

- Change the default password for all predefined users if you choose to make use of them. Make sure to choose a strong password since MiR products do not enforce any password rules nor expire the password.
- Delete predefined users that you do not want to use.
- Review and adjust the permissions for the predefined users as needed. The default settings may be too permissive for your environment.
- Create new user groups if more levels of access are necessary.
- Create dedicated user accounts under the relevant user group for each person accessing your MiR product, and ensure that the users change the password on their first sign-in. We do not recommend to have several users share the same account.
- Only enable users with a minimum level of access to use a pin code to sign in. This could, for example, be users who can only run existing missions and do not have permission to change anything on the robot. For users with a higher level of access that enables them to modify site components or the robot's settings, we highly recommend to use a strong password to sign in.

3.1 Changing the password of existing users

1. Sign in to the robot interface, go to **Setup > Users**, and select ✎**Edit** for the user you want to change the password for.



Users

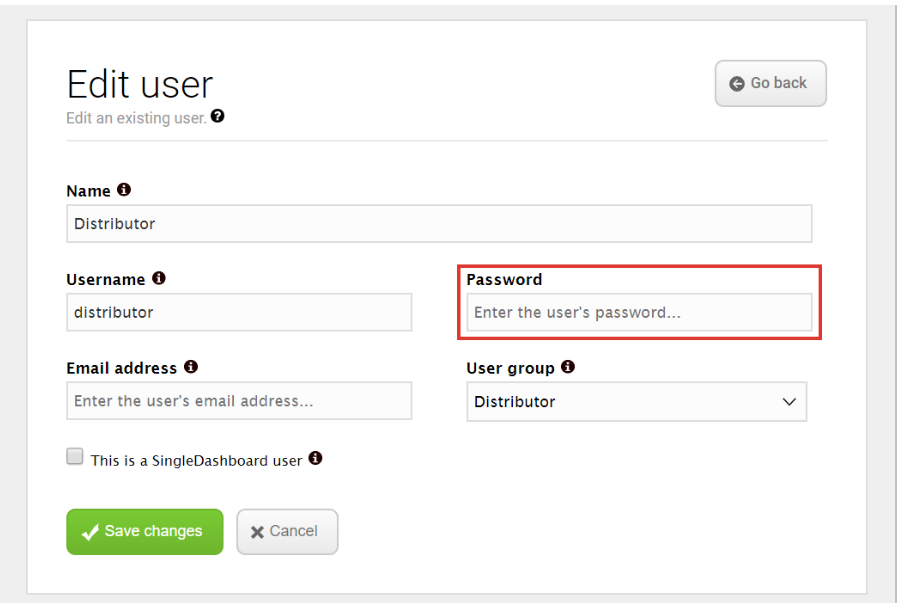
Create and edit users.

Filter: Write name to filter by...

Page 1 of 1

	Name	Username	Email	Functions
●	Service	service		✎ ✕
●	Distributor	distributor		✎ ✕
●	Administrator	admin		✎ ✕
●	User	user		✎ ✕

2. Enter a new password for the user under **Password**.



Edit user

Edit an existing user.

Name: Distributor

Username: distributor

Password: Enter the user's password...

Email address: Enter the user's email address...

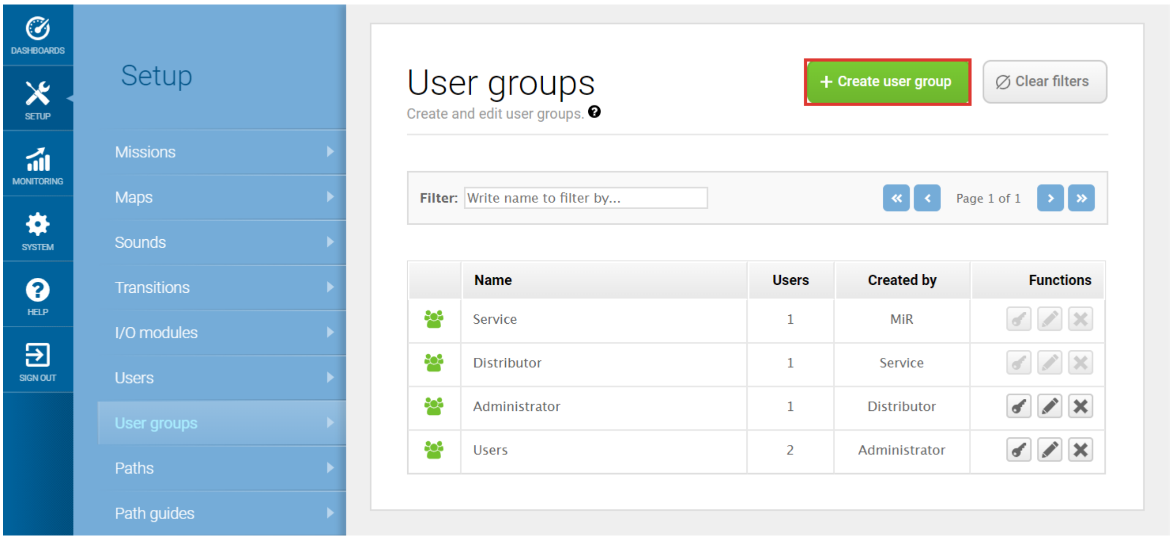
User group: Distributor

□ This is a SingleDashboard user

3. Repeat these steps for other users with a default password that you can access.

3.2 Creating a new user group and editing permissions

1. Sign in to the robot interface, go to **Setup > User groups**, and select **+ Create User group**.



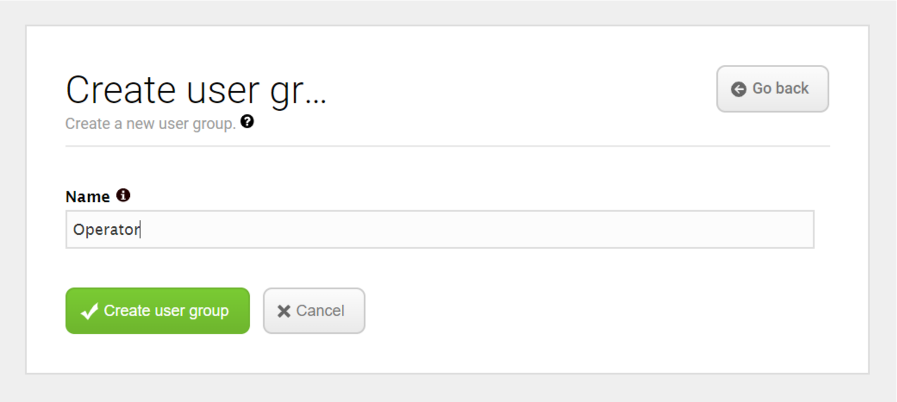
User groups

Create and edit user groups.

Filter: Write name to filter by...

	Name	Users	Created by	Functions
	Service	1	MiR	
	Distributor	1	Service	
	Administrator	1	Distributor	
	Users	2	Administrator	

2. Enter the name of the user group you want to create, and select ✓ **Create user group**.

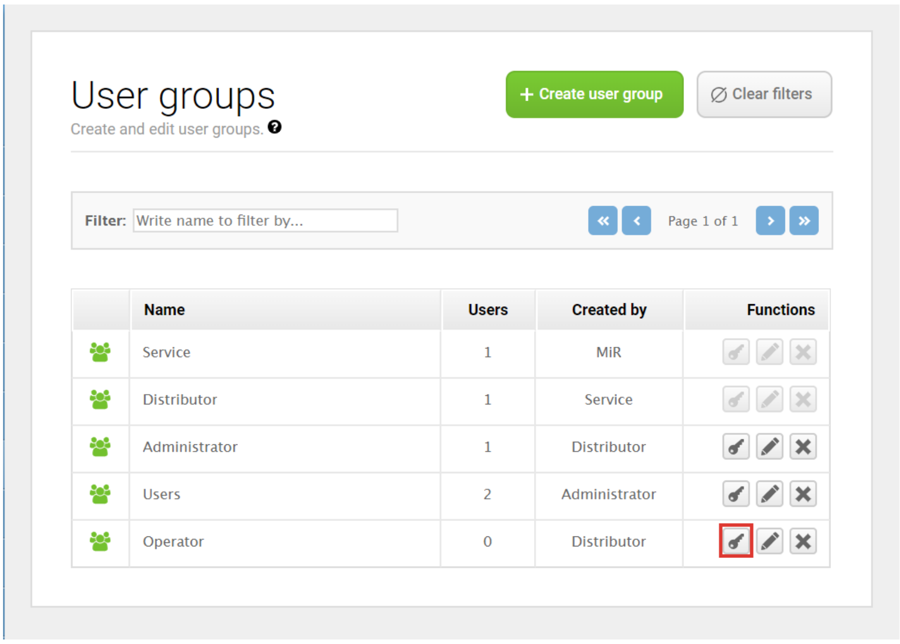


Create user gr...

Create a new user group.

Name: Operator

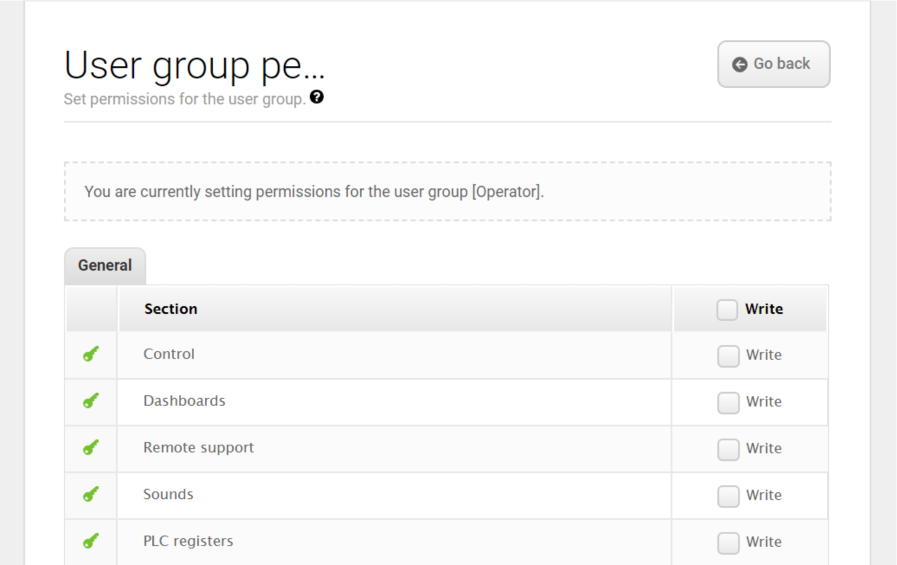
3. Edit which features the user group can access by selecting **Permissions**.



User groups
Create and edit user groups.
+ Create user group
Clear filters
Filter: Write name to filter by...
Page 1 of 1

	Name	Users	Created by	Functions
	Service	1	MiR	
	Distributor	1	Service	
	Administrator	1	Distributor	
	Users	2	Administrator	
	Operator	0	Distributor	

4. Select the features in the robot or MiR Fleet interface that users in this group should be able to edit.



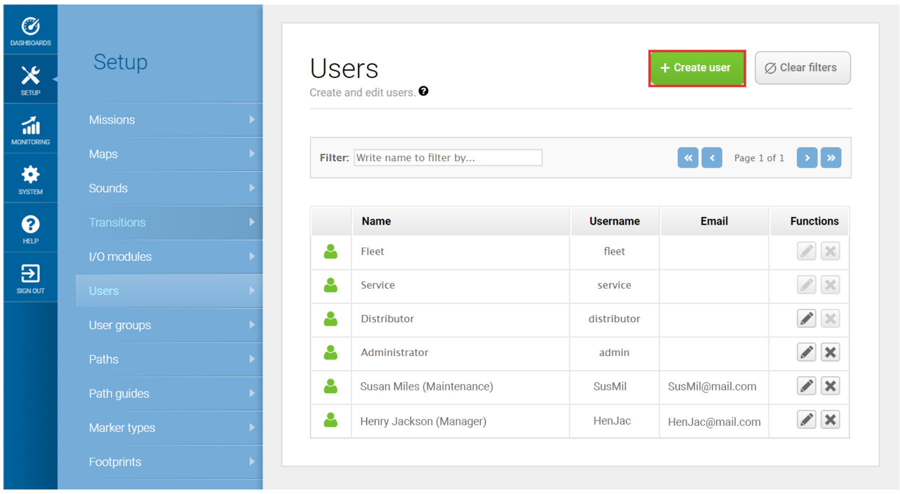
You are currently setting permissions for the user group [Operator].

	Section	□ Write
	Control	□ Write
	Dashboards	□ Write
	Remote support	□ Write
	Sounds	□ Write
	PLC registers	□ Write

You have now created a new user group with limited accessibility.

3.3 Creating new users

1. Sign in to the robot interface, go to **Setup > Users**, and select **+ Create user**.



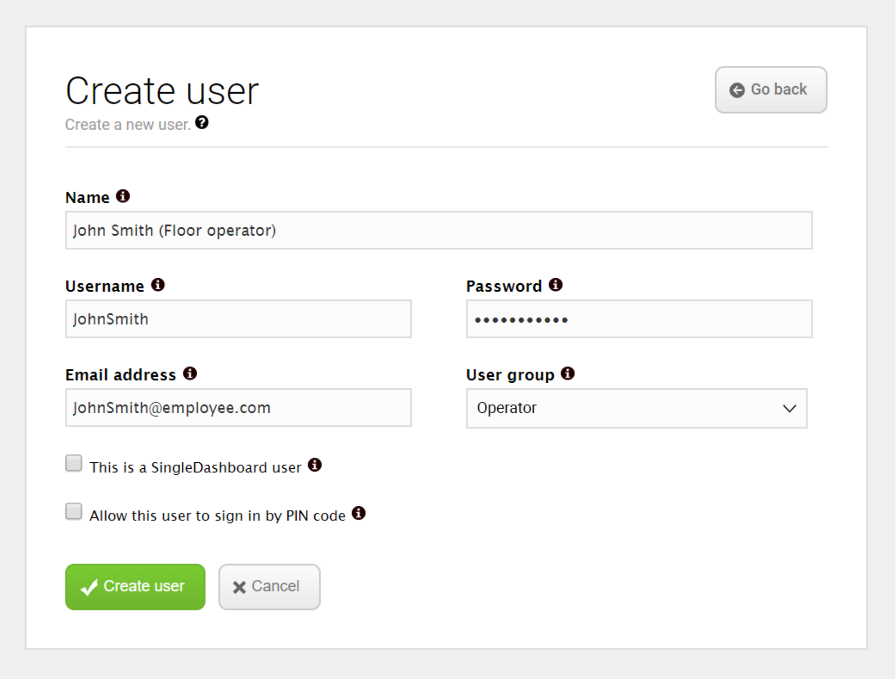
Users

Create and edit users.

Filter: Write name to filter by...

Name	Username	Email	Functions
Fleet	fleet		
Service	service		
Distributor	distributor		
Administrator	admin		
Susan Miles (Maintenance)	SusMil	SusMil@mail.com	
Henry Jackson (Manager)	HenJac	HenJac@mail.com	

2. Fill in the fields for the new user. Users can only edit the information and password if their user group permits it.



Create user

Create a new user.

Name: John Smith (Floor operator)

Username: JohnSmith

Password: •••••••••••

Email address: JohnSmith@employee.com

User group: Operator

□ This is a SingleDashboard user

□ Allow this user to sign in by PIN code

3. Only allow users with very limited access to sign in by PIN code.

4. Select ✓ **Create user**. This user can now sign in with the credentials entered in the previous step.

4. Internal WiFi access point

Applicable for all MiR250, MiR500, and for MiR1000 robots, and MiR100 and MiR200 HW 6.0 and lower.

Only some robots are shipped with an internal WiFi access point that you can connect to. These are the robots that broadcast a WiFi hotspot that you can connect to with a WiFi device.

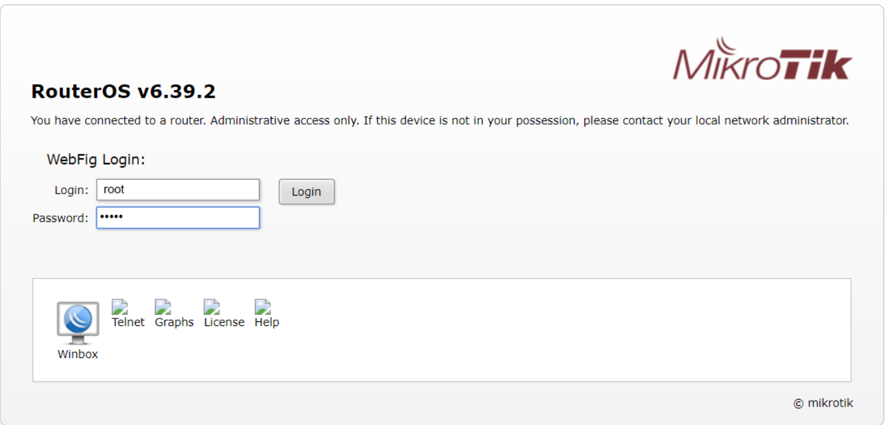
> **SECURITY WARNING**
>
> The local WiFi access point of the robot is only meant to be used for initial configuration. Leaving the access point operational, even if it is password protected, poses a risk to the robot's cybersecurity.
>
> - Disable the access point after commissioning for secure operation of the robot.

The WiFi router configuration page is protected by its own password. You can change this password if desired. However, since the WiFi access point must be turned off during operation, this is generally not required. If you choose to change the password, you must do so before disabling the access point.

To disable the internal WiFi access point and change the router's configuration page password, follow these steps:

1. Connect to your robot's WiFi.
2. Open a browser, and go to the address **192.168.12.1/webfig**. This is the interface to the robot's router.

3. Enter the following default credentials to sign in to the router:
   - **Username:** root
   - **Password:** mirex



RouterOS v6.39.2

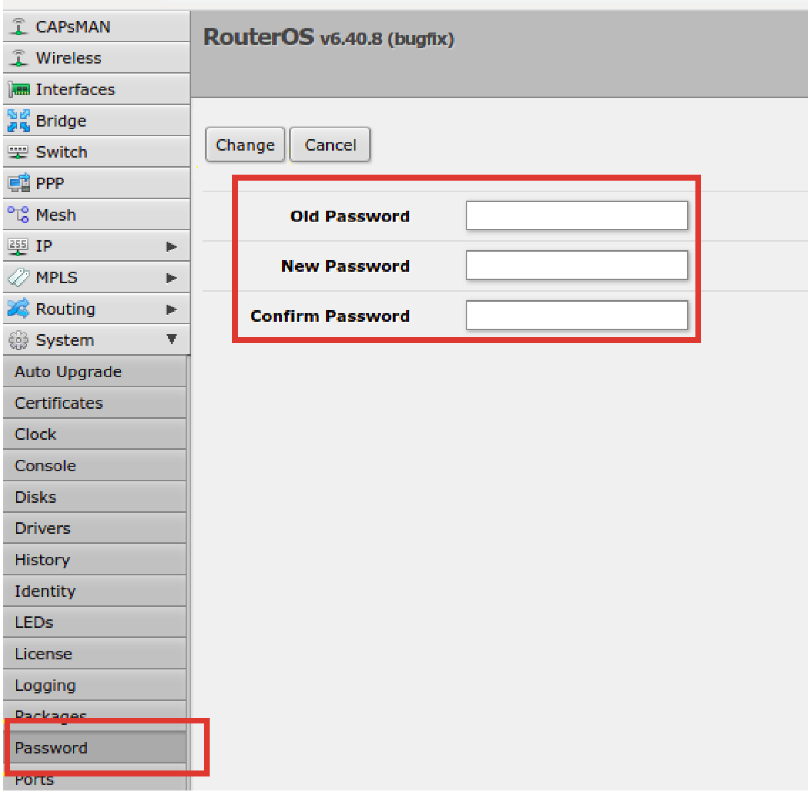
You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

WebFig Login:

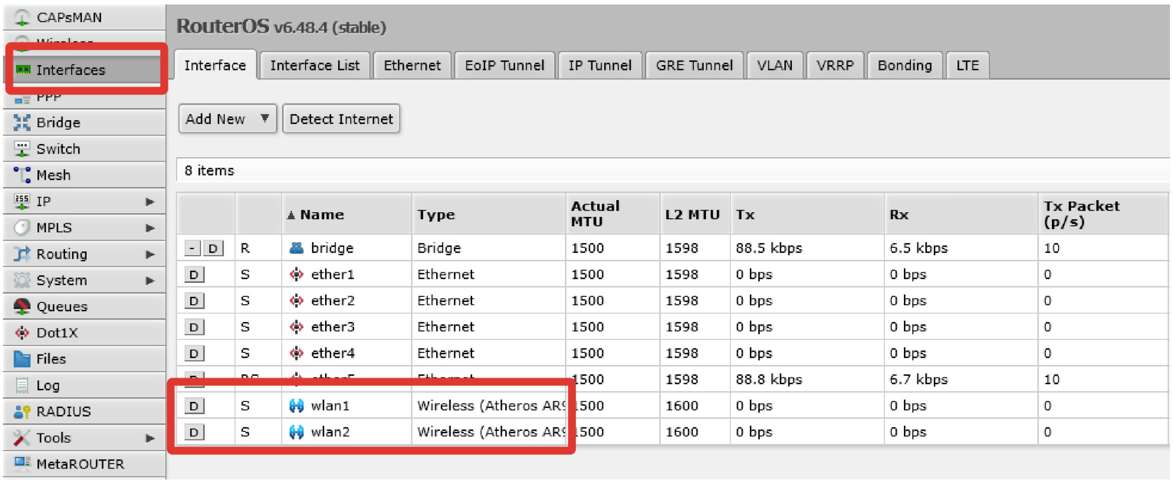
Login: root

Password: •••••

4. To change the password used to sign in to the router's configuration page, go to **System > Password**, and enter a more secure password.



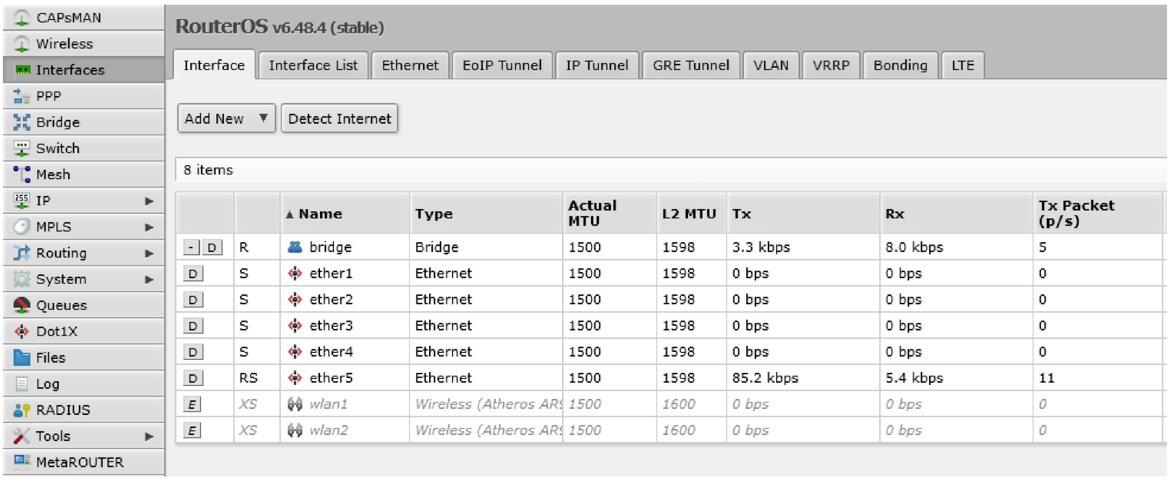
5. To disable the internal access point, go to **Interfaces**, and select **D** for the two wireless interfaces to disable them.



8 items

		▲ Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)
- D	R	bridge	Bridge	1500	1598	88.5 kbps	6.5 kbps	10
D	S	ether1	Ethernet	1500	1598	0 bps	0 bps	0
D	S	ether2	Ethernet	1500	1598	0 bps	0 bps	0
D	S	ether3	Ethernet	1500	1598	0 bps	0 bps	0
D	S	ether4	Ethernet	1500	1598	0 bps	0 bps	0
D	RS	ether5	Ethernet	1500	1598	88.8 kbps	6.7 kbps	10
D	S	wlan1	Wireless (Atheros AR!	1500	1600	0 bps	0 bps	0
D	S	wlan2	Wireless (Atheros AR!	1500	1600	0 bps	0 bps	0

The access point is now disabled.



8 items

		▲ Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)
- D	R	bridge	Bridge	1500	1598	3.3 kbps	8.0 kbps	5
D	S	ether1	Ethernet	1500	1598	0 bps	0 bps	0
D	S	ether2	Ethernet	1500	1598	0 bps	0 bps	0
D	S	ether3	Ethernet	1500	1598	0 bps	0 bps	0
D	S	ether4	Ethernet	1500	1598	0 bps	0 bps	0
D	RS	ether5	Ethernet	1500	1598	85.2 kbps	5.4 kbps	11
E	XS	wlan1	Wireless (Atheros AR!	1500	1600	0 bps	0 bps	0
E	XS	wlan2	Wireless (Atheros AR!	1500	1600	0 bps	0 bps	0

5. External WiFi access point

Applicable for all MiR600 and MiR1350 robots and for MiR100 and MiR200 HW 7.0 and higher.

Some robots can only be configured by either connecting an Ethernet cable to them or connecting an external WiFi access point. MiR provides a MiR Access Point dongle that can be used for this purpose.

> **SECURITY WARNING**
>
> A person with physical access to the robot may connect to it using an Ethernet cable, gaining access to the internal robot network. This level of access is equivalent to connecting to a robot’s internal or external WiFi access point and exposes sensitive internal interfaces.
>
> - Operate the robot in areas with restricted physical access.
> - After commissioning, close the external Ethernet port using an Ethernet lock.

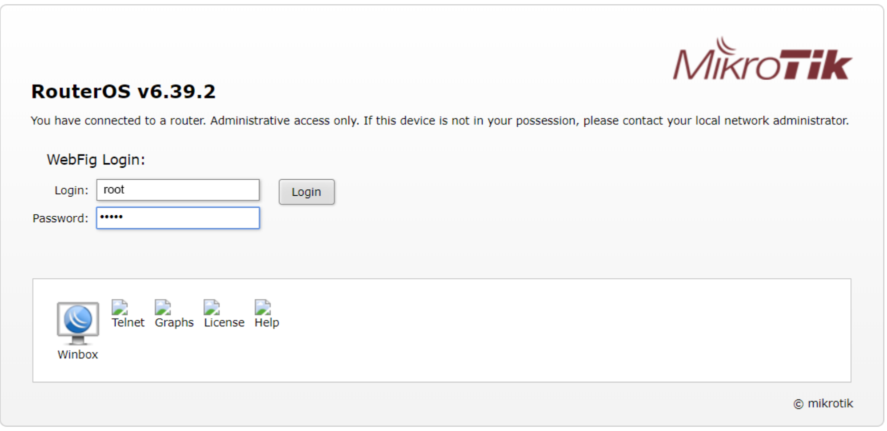
> **SECURITY WARNING**
>
> An external WiFi access point is only meant to be used for initial configuration. Leaving the access point connected to the robot, even if it is password protected, poses a risk to the robot's cybersecurity.
>
> - If you connect an access point to the robot, disconnect the access point after commissioning for secure operation of the robot.
> - Use an Ethernet cable instead of an access point to connect to your robot if possible.

The MiR Access Point configuration page is protected by its own password. You can change this password if desired. However, since the access point must be disconnected during operation, this is generally not required.

To change the access point's configuration page password, follow these steps:

1. Connect to the MiR Access Point's WiFi network.
2. Open a browser, and go to the address 192.168.12.2/webfig. This is the interface to the configuration page for MiR Access Point.

3. Enter the following default credentials to sign in to the access point:
    - **Username:** root
    - **Password:** mirex



RouterOS v6.39.2

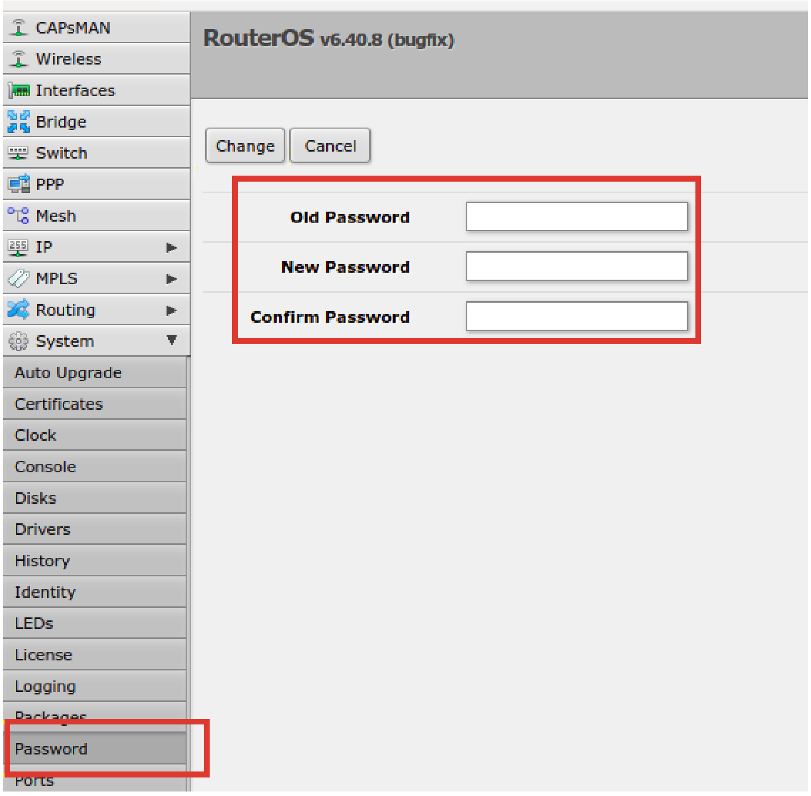
You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

WebFig Login:

Login: root

Password: •••••

4. Go to **System > Password**, and enter a more secure password.



RouterOS v6.40.8 (bugfix)

Old Password

New Password

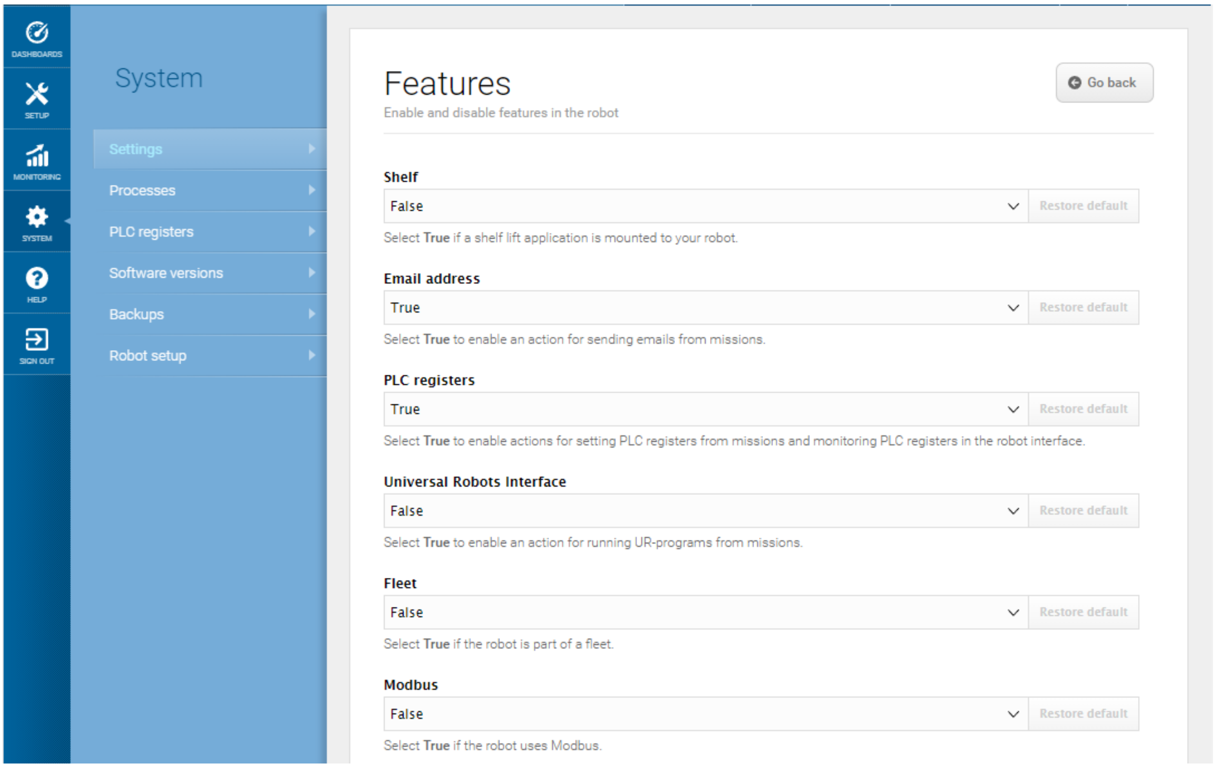
Confirm Password

6. Restrict unused functionality

Applicable for all robots, not for MiR Fleet

We strongly recommend that you disable all unused features in MiR robots.

To disable a feature, sign in to the robot interface, and go to **System > Settings > Features**. A list of all features available to your robot are shown and you can enable or disable them as necessary.



Features

Enable and disable features in the robot

Shelf

False

Select **True** if a shelf lift application is mounted to your robot.

Email address

True

Select **True** to enable an action for sending emails from missions.

PLC registers

True

Select **True** to enable actions for setting PLC registers from missions and monitoring PLC registers in the robot interface.

Universal Robots Interface

False

Select **True** to enable an action for running UR-programs from missions.

Fleet

False

Select **True** if the robot is part of a fleet.

Modbus

False

Select **True** if the robot uses Modbus.

7. BIOS and boot from USB protection

Applicable for all robots, not for MiR Fleet.

The BIOS on the robot is configured to boot up the robot computer from any connected USB drive. You can take measures to prevent attackers from using a USB drive to reconfigure the robot . It is the responsibility of the commissioner to change the default BIOS settings.

7.1 Protecting from USB boot

MiR robots will always attempt to boot from a connected USB drive if one is present. Only MiR100 and MiR200 have an easily accessible USB port in the front-right corner. We recommend taking measures to restrict access to this port.

To protect you robot from booting up from any connected USB drive, you can close the exposed port using a USB lock. This prevents unauthorized users from connecting USB devices to the robot.

Alternatively, you can disable the boot from USB function, but this impacts serviceability and may result in the robot being non-restorable in the event of failure.

Disabling USB boot requires a modification in the robot's software and in the BIOS. You must contact MiR Technical Support for the necessary assistance to correctly disable USB boot. If you do so, we recommend implementing password protection on the BIOS to prevent attacker from reverting your changes–see **Protecting the BIOS below**.

7.2 Protecting the BIOS

You can protect access to the robot’s BIOS with a password. To do this, connect a screen and a keyboard to the robot’s USB or HDMI ports and interrupt the boot sequence to enter the BIOS.

For MiR250, MiR500, MiR600, MiR1000, and MiR1350, you must access the robot computer and connect the keyboard and screen to the ports there. See your robot's user guide to see how to access the front compartment where the robot computer is mounted.

For MiR100 and MiR200, the service port in the front right corner has an HDMI and USB port you can use to connect to the robot computer. In some robot configurations, these service ports are disconnected from the robot computer, and you will need to remove the top and front cover to access the robot computer directly instead.

Depending on the model and hardware revision of your robot, the following instructions apply:

- **For MiR250, MiR500. MiR600, MiR1000, and MiR1350**
  Turn on the robot, and press the Delete key to interrupt the boot sequence and enter the BIOS.
- **MiR100 HW version 4.0 and lower and MiR200 HW version 2.0 and lower**
  Turn on the robot, and press the F2 key to interrupt the boot sequence and enter the BIOS.
- **MiR100 HW version 4.0 and higher and MiR200 HW version 2.0 and higher**
  Turn on the robot, and press the Delete key to interrupt the boot sequence and enter the BIOS.

Once in the BIOS configuration interface, you can set a password for the BIOS.

8. Software security patches

To improve the security of MiR, MiR supplies security patches to the operating system in new MiR software update files. When you install a security patch, it takes approximately 10-15 minutes longer to update a MiR product.

8.1 Understanding MiR software versions

MiR uses the **Major.Minor.Patch.Hot fix** format to version software. For example, 2.8.1.1 means that the software is based on the second major release, the eighth minor release of the major version, the first patch release of the minor version, and, in this example, a single hot fix is included too.

- **Major releases** include the most significant changes that affect the entire robot software.
- **Minor releases** often include new features and smaller changes that only affect parts of the software.
- **Patch releases** focus on fixing small issues in the software and introducing quality improvements.
- **Hot fix releases** are only created when a patch release has introduced a critical issue that needs to be fixed immediately.

8.2 Security patch policy

MiR applies the following policy when supplying security patches:

- New security patches are distributed per every minor release.
- All patch releases under a minor release include the previous security patches also. In other words, if you chose not to install the first software version in a minor release, such as version 2.9.0, the security patches will still be installed when you update to 2.9.1 or higher.