11. Cybersecurity Threat Assessment

Description

This section provides information to help you strengthen the robot against potential cybersecurity threats. It outlines requirements for addressing cybersecurity threats and provides security hardening guidelines.

11.1. General Cybersecurity

Description

Connecting a Universal Robots robot to a network can introduce cybersecurity risks. These risks can be mitigated by using qualified personnel and implementing specific measures for protecting the robot's cybersecurity.
Implementing cybersecurity measures requires conducting a cybersecurity threat assessment.
The purpose is to:

- Identify threats
- Define trust zones and conduits
- Specify the requirements of each component in the application

WARNING

Failure to conduct a cybersecurity risk assessment can place the robot at risk.

- The integrator or competent, qualified personnel shall conduct a cybersecurity risk assessment.

NOTICE

Only competent, qualified personnel shall be responsible for determining the need for specific cybersecurity measures and for providing the required cybersecurity measures.

11.2. Cybersecurity Requirements

Description

Configuring your network and securing your robot requires you to implement the threat measures for cybersecurity.
Follow all the requirements before you start configure your network, then verify the robot setup is secure.

Cybersecurity

- Operating personnel must have a thorough understanding of general cybersecurity principles and advanced technologies as used in the UR robot.
- Physical security measures must be implemented to allow only authorized personnel physical access to the robot.
- There must be adequate control of all access points. For example: locks on doors, badge systems, physical access control in general.

WARNING

Connecting the robot to a network that is not properly secured, can introduce security and safety risks.

- Only connect your robot to a trusted and properly secured network.

Network configuration requirements

- Only trusted devices are to be connected to the local network.
- There must be no inbound connections from adjacent networks to the robot.
- Outgoing connections from the robot are to be restricted to allow the smallest relevant set of specific ports, protocols and addresses.
- Only URCaps and magic scripts from trusted partners can be used, and only after verifying their authenticity and integrity

Robot setup security requirements

- Change the default password to a new, strong password.
- Disable the "Magic Files" when not actively used (PolyScope 5).
- Disable SSH access when not needed. Prefer key-based authentication over password-based authentication
- Set the robot firewall to the most restrictive usable settings and disable all unused interfaces and services, close ports and restrict IP addresses

11.3. Cybersecurity Hardening Guidelines

Description

Although PolyScope includes many features for keeping the network connection secure, you can harden security by observing to following guidelines:

- Before connecting your robot to any network, always change the default password to a strong password.

  NOTICE

  You cannot retrieve or reset a forgotten or lost password.

  - Store all passwords securely.

- Use the built-in settings to restrict the network access to the robot as much as possible.
- Some communication interfaces have no method of authenticating and encrypting communication. This is a security risk. Consider appropriate mitigating measures, based on your cybersecurity threat assessment.
- SSH tunneling (Local port forwarding) must be used to access robot interfaces from other devices if the connection crosses the trust zone boundary.
- Remove sensitive data from the robot before it is decommissioned. Pay particular attention to the URCaps and data in the program folder.
  - To ensure secure removal of highly sensitive data, securely wipe or destroy the SD card.

For information about setting an admin password and local port forwarding, see the Hamburger Menu.

You can also read Secure Setup on www.universal-robots.com/articles

11.4. Passwords

Description

You can create and manage different types of password in PolyScope. An initial password must be set to access the full safety settings. The following password types are described below:

- Administrator
- Operational

11.5. Password Settings

To set a Password

You must set a password to Unlock all safety settings that make up your Safety Configuration. If no safety password is applied, you are prompted to set it up.

1. In your PolyScope header right corner, press the **Hamburger** menu and select **Settings**.
2. On the left of the screen, in the blue menu, press **Password** and select **Safety**.
3. In **New password**, type a password.
4. Now, in **Confirm new password**, type the same password and press **Apply**.
5. In the bottom left of the blue menu, press **Exit** to return to previous screen.

You can press the **Lock** tab to lock all Safety settings again or simply navigate to a screen outside of the Safety menu.

11.6. Administrator Password

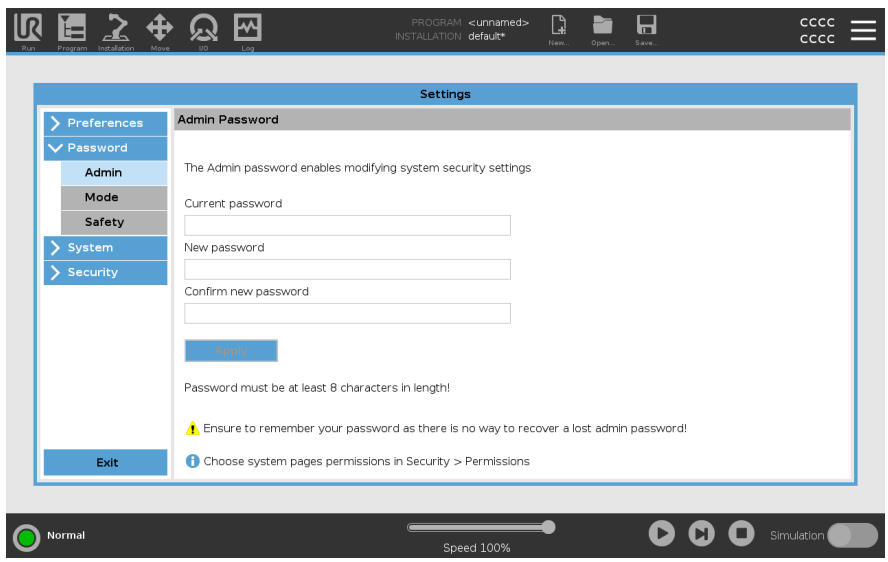
Description

Use the Administrator (Admin) Password to change the security configuration of the system, including network access.
The Admin password is equal to the password used for the root user account on the Linux system running on the robot, which may be needed in some network use cases such as SSH or SFTP.

WARNING

You cannot recover a lost Admin password.

- Take the appropriate steps to ensure your admin password is not lost.



To set the Admin Password

1. In the Header, tap the Hamburger menu icon and select **Settings**.
2. Under **Password**, tap **Admin**.
3. Under **Current password**, put in the default password: **easybot**.
4. Under **New password**, create a new password.
   Creating a strong, secret password obtains the best security for your system.
5. Under **Confirm new password**, repeat your new password.
6. Tap **Apply** to confirm your password change.

Safety

The Safety password prevents unauthorized modification of the Safety settings.

11.7. Operational Password

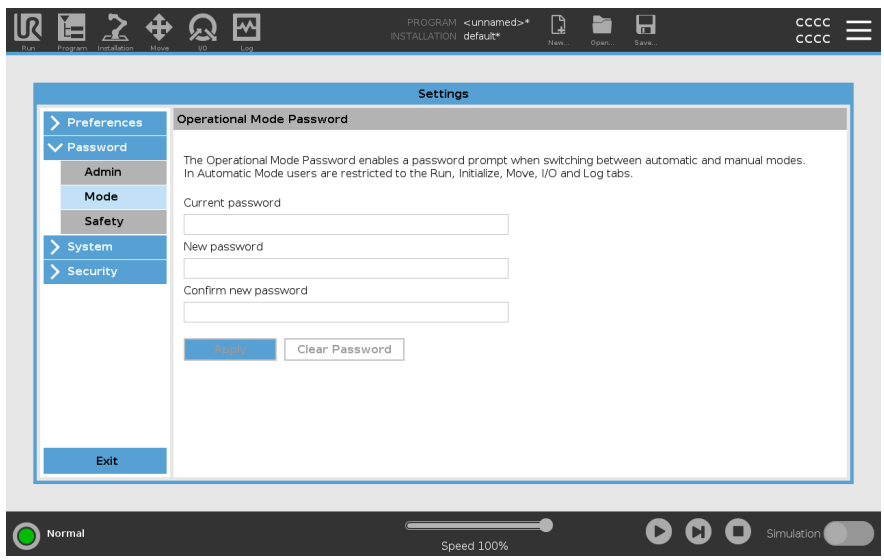
Description

The Operational Mode Password, or mode password, creates two different user roles on PolyScope:

- Manual
- Automatic

When the mode password is set, programs and installations can only be created and edited in Manual mode. Automatic mode only allows the operator to load pre-made programs . Once a password has been set, a new Mode icon appears in the Header.

Switching operational modes, from Manual to Automatic and from Automatic to Manual, causes PolyScope to prompt for the new password.



To set the Mode Password

1. In the Header, tap the Hamburger menu icon and select **Settings**.
2. Under **Password**, tap **Mode**.
3. Under **New password**, create a new password.

   Creating a strong, secret password obtains the best security for your system.
4. Under **Confirm new password**, repeat your new password.
5. Tap **Apply** to confirm your password change.