Insights Security Sheet

Insights provides your engineers with the following features:

- KPIs to improve product quality and process efficiency
- Data to optimize robot performance
- SMS alerts for specific robot events
- Remote Access to the robot
- Online help from robotics experts

Your production managers will be able to:

- Monitor long term trends in robot performance
- Improve planning and overall productivity
- Measure the return on investment of their robot cells

Industrial Internet of Things (IIoT) brings tremendous benefits to your company. But in the fashion of every IIoT component, connecting a robot to your corporate network without securing it might represent a risk for your data, equipment and even workers.

Edge Gateway

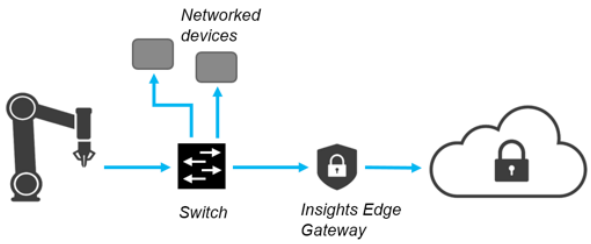
Robotiq provides a pre-configured firewall: the Insights Edge Gateway. The Edge Gateway blocks all ports except the following to ensure connection to the Insights cloud service:

Protocol	Port	Host address	Use
MQTT	443	aws-iot-prod.robotiq.com	Publish robot data to the cloud service
HTTPS	443	www.amazon.com	Test Internet connectivity
HTTPS	443	insights-api.robotiq.com	Communicate with the Insights API
NTP	123	us.pool.ntp.org	Synchronize the robot with a time server
DNS	53	DNS server	Resolve the IP addresses
STUN & TURN	443	remote-access-turn.robotiq.com	Remote Access functionalities

In order for Insights to work with your robots, you might need to open the described ports on your corporate firewall.

The gateway only allows outbound connection from the robot. This means only the robot can initiate a connection with the cloud service. All inbound connections to the Edge Gateway are blocked. A limited, temporary, encrypted and secure communication is established for the Remote Access feature. The gateway position in the network affects the communication between devices:

You can connect the gateway directly between the robot and Internet. Doing so will block any other device to communicate with the robot.



You can connect the gateway next to a network switch. You can also decide to secure a subnetwork that contains other devices (a PLC, CNC machine, etc.). This will allow those devices to communicate with each other while blocking all other connections with another network level that are not allowed by the Edge Gateway.

You may have to modify the default Edge Gateway configuration in order to place it on the same subnetwork. Every robot cell network topology is different. Therefore, make sure your network setup meets your security requirements.

Note that if you decide to connect your robots to the Internet without using the Edge Gateway, you expose their ports to the subnetwork to which they are connected. Robotiq recommends you perform a risk assessment to ensure proper security.

Data Security

All data sent from the robot to the Insights cloud service and from the cloud service to the user dashboard are encrypted. The database can only be accessed via the Insights cloud server, hosted by Amazon.

When pairing a robot to an account, a temporary pairing code is generated for a specific robot serial number. A handshake is performed between the pairing code and robot serial number in order to authenticate the robot and coordinate it with the right user account.

You can further increase the security of Insights by enabling the 2-factor authentication for your personal account. When an account has not been used for 30 days, the application will prompt you to re-enter your password.

Need to know more? Refer to our Insights documentation available at *support.robotiq.com*:

- Privacy policy & licence agreement
- Quick Start Guide
- Instruction Manual

Contact support@robotiq.com if you have further questions!