HARTING

Pushing Performance

People | Power | Partnership

Application Notes

MICA Getting Started

2. Edition 2019

Version 5.0. Subject to alterations without notice.

Contents

1 Connecting Your MICA to Power 4

2 Logging In 5
- 2.1 Using Name Resolution 5
- 2.2 Using the 10.10.10.10 Fall Back Address 5
- 2.3 Connecting to a MICA Wireless for the First Time 5
- 2.4 First Login 5

3 Working with Containers 6
- 3.1 Starting Containers 6
- 3.2 Opening the UI of a Container 7
- 3.3 Stopping a Container 7

4 MICA Configuration and Maintenance 8
- 4.1 Network Configuration 8
- 4.2 Time and Date 10
- 4.3 Changing Passwords 11
- 4.4 Firmware Reset 11
- 4.5 Firmware Upgrade 11
- 4.6 Generating a System Report 12

5 Container Configuration and Maintenance 12
- 5.1 Container Installation 12
- 5.2 Container Update 12
- 5.3 The Context Menu 12
- 5.4 Accessing the Container UI 12
- 5.5 Container Network Settings 13
- 5.6 Container Reset 13
- 5.7 Container Duplication 13
- 5.8 Container Export 13
- 5.9 Container Overlay Export 13

6 MICA Software Architecture 14
- 6.1 Container Architecture 14
- 6.2 MICA Network Topology 14

7 Troubleshooting 16

1 Connecting Your MICA to Power

FIG. 1: MICA BASIC WITH M12 A-CODED GPIO AND M12 X-CODED POWER OVER ETHERNET (POE).

FIG. 2: MICA WIRELESS WITH M8 POWER SUPPLY.

Depending on the MICA variant your MICA can be powered using Power over Ethernet (PoE) or 24V DC. The documentation included with your MICA explains how to connect your MICA to power and to your computer.

Warning: Make sure to use an appropriate power source. Some commercially available PoE injectors do not follow the IEEE 802.3af norm and can damage devices like the MICA through voltage peaks up to 80V. If you are unsure which PoE Injector to use, please contact your HARTING partner or MICASupport@HARTING.com

---

The MICA boots automatically when connected to power and loads its web interface. During the boot sequence, the power LED will be illuminated in red and switch to green once the boot process is complete.

2 Logging In

2.1 Using Name Resolution

In most network environments the MICA will show up under the name listed on the type shield at the bottom of the device. Depending on your particular combination of browser, operating system, and network settings, you can log into the MICA web interface using either *https://micaname or* https://micaname.local.

2.2 Using the 10.10.10.10 Fall Back Address

If the MICA cannot connect to a DHCP server, for example because it is connected directly to a PC, you can access its web interface under https://10.10.10.10. To do this, your PC needs to be in the same network segment as the MICA. You can do this, for example, by setting its IP address to 10.10.10.7 and its network mask to 255.255.255.240.

If you have not set the MICA base system to a static IPv4 address, you can also use 10.10.10.10 to log into a MICA that no longer shows up in a network due to some fault or misconfiguration. To engage this fallback mode, disconnect the MICA from power, connect it directly to a PC that is not connected to an IPv4 network, and power the MICA back on.

2.3 Connecting to a MICA Wireless for the First Time

When the MICA Wireless is initially connected to power, it starts in Access Point mode with the IP address 10.10.10.10 and WPA2 enabled. The SSID and WPA2 password are listed on the type shield on the bottom of the MICA. Use these to connect to the MICA from your PC or tablet and to perform the initial configuration. For more information about configuring a MICA Wireless, please refer to the *MICA Wireless User Guide* available on www.harting-mica.com.

2.4 First Login

To log into your MICA for the first time, use the username *admin* and the password listed on the type shield. We strongly recommend that you change the password immediately after logging in.

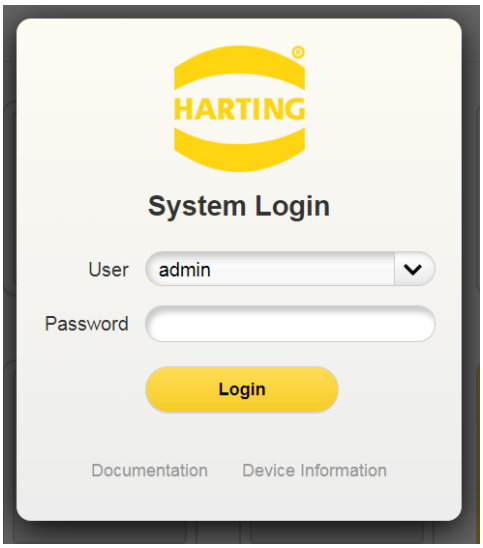

FIG. 3: LOGIN SCREEN

You can also access the MICA API documentation and some basic device information about your device (including the serial number and MAC address) from this screen without having to log in.

Warning: Make sure to store your password in a safe place. HARTING is not able to recover lost passwords. If you have lost your password, contact your HARTING service provider or MICASupport@HARTING.com for instructions how to return your MICA for a factory reset.

3 Working with Containers

All MICA applications consist of one or more LXC containers, which are small independent virtual machines. The MICA web interface lists all installed containers and three general tools called *Install*, *Settings*, and *Information*.

FIG. 4: MICA WEB INTERFACE

3.1 Starting Containers

Before you can interact with a container, it has to be started. To start a container, choose *Start App* from the context menu. You can open the context menu by right-clicking a container icon or by long pressing it on a touch screen. Once the container is active, its icon changes from gray to yellow.

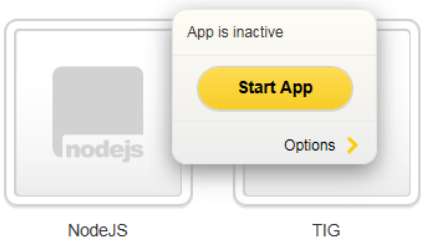

FIG. 5: STARTING CONTAINERS

3.2 Opening the UI of a Container

To open the user interface of a started container, click its icon. If the container has a web user interface, it will be displayed in your browser. If the container does not have a web interface, an informational message will be shown.

3.3 Stopping a Container

To stop a container, choose *Stop App* from its context menu. You can open the context menu by right-clicking a container icon or by long pressing it on a touch screen. Once the container is stopped, the icon changes from yellow to gray.

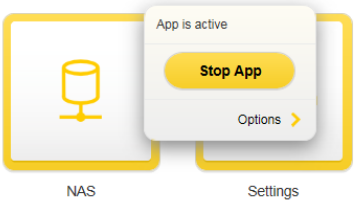

FIG. 6: STOPPING CONTAINERS

4 MICA Configuration and Maintenance

The MICA base system can be configured using the *Settings* panel. All actions inside the *Settings* panel require admin privileges.

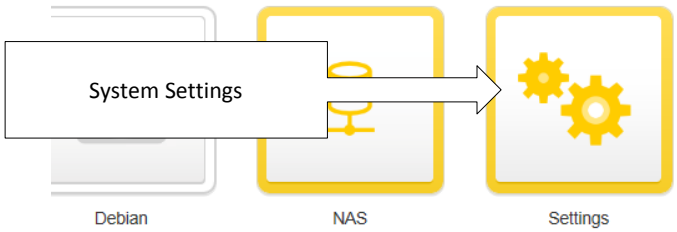

FIG. 7: SYSTEM SETTINGS

4.1 Network Configuration

Network settings can be configured under *Settings* → *Network*.

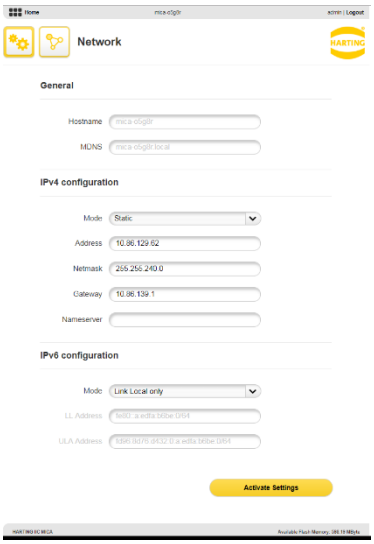

FIG. 8: MICA BASE SYSTEM NETWORK SETTINGS

4.1.1 General Settings

The MICA host name and MDNS name are set in the factory and cannot be changed in the UI.

4.1.2 IPv4 Configuration

IPv4 is disabled by default with the exception of the Fallback address 10.10.10.10 (see Troubleshooting).

To activate IPv4, either select *DHCP* to have the MICA obtain an IPv4 address automatically, or select *Static* and enter an IP address, network mask and, if necessary, a gateway and a DNS server.

Click *Activate Settings* to restart the MICA with the new settings.

Warning: If you assign an invalid IPv4 address, or an IPv4 address that is not reachable in your network, the MICA will not be accessible over the IPv4 network. In this case, follow the troubleshooting instructions in chapter 7.

4.1.3 IPv6 Configuration

By default the MICA base system has an IPv6 Link Local address as well as a ULA address. The Link Local address can be derived by combining the HARTING IPv6 prefix and the last 9 digits of the MAC address listed on the type shield of the MICA.
For example:

1. MAC address 00:**0A:ED:D8:0B:10**
2. IPv6 Link Local address: fe80::**a:ed:d8:0B:10**:0

This address is set in the factory and cannot be changed.

To assign additional static IPv6 addresses, choose *Static* in the drop down menu and add the desired address, gateway, and prefix.

Click *Activate Settings* to restart the MICA with the new settings.

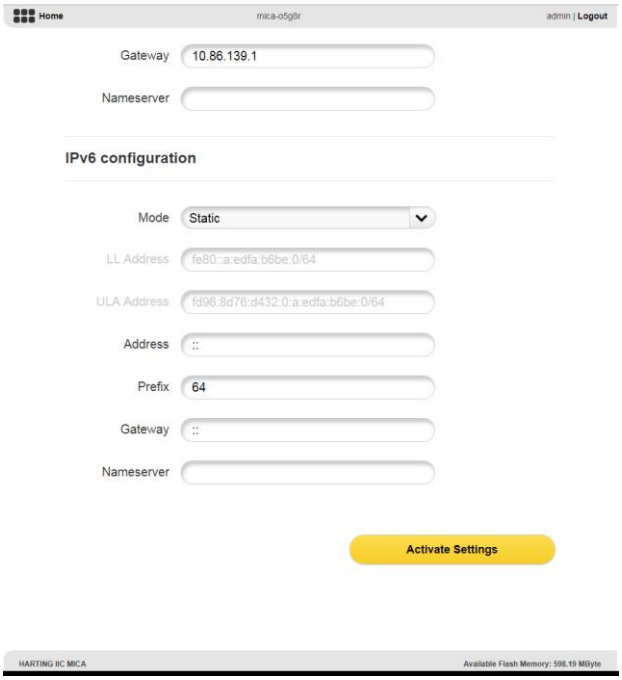

FIG. 9: MICA BASE SYSTEM IPV6 SETTINGS

4.1.4 Partial DHCP

MICA base system version 5 and higher also let you configure name servers and gateways manually even if the MICA is connected to a DHCP server. This can be useful for some specific network environments.

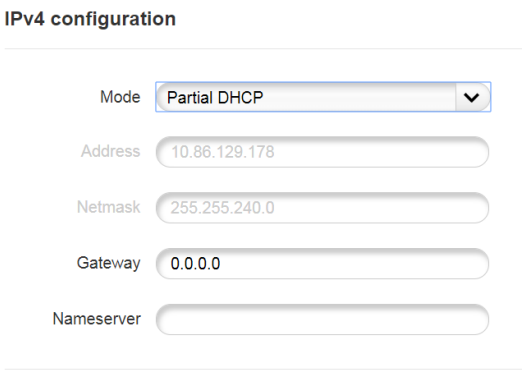

FIG. 10: PARTIAL DHCP

To override DHCP settings, select Partial DHCP from the IPv4 Mode drop down and enter IPv4 addresses for the gateway, the name server, or both.

4.2 Time and Date

You can adjust the time and date under *Settings* → *Time & Date*. The MICA real time clock is buffered for 72 hours. If the MICA is disconnected from power for more than 72 hours, the time and date will be reset to the production date.

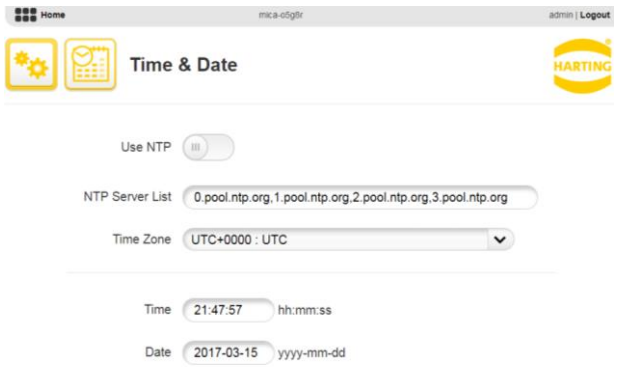

FIG. 11: TIME AND DATE SETTINGS

If your MICA has access to a time server we recommend that you activate NTP. By default, the MICA contacts the primary NTP server pools. If you want to use a different time server, enter it in the NTP Server List. The time zone has to be set manually.

It may take a couple of seconds for the MICA to synchronize with the NTP server. The MICA shows the last time it successfully synced the real time clock with an NTP server or “not synced” if the synchronization failed.

If you cannot use a time server, you can enter the time and date manually.

4.3 Changing Passwords

For security reasons your MICA shipped with a random generated administrator password which is listed on the type shield on the bottom of the device. We strongly recommend that you change the password immediately after logging in to your MICA for the first time.

Every MICA comes with three user privilege levels—*user, containeradmin,* and *admin*—to provide protection against accidental or deliberate misconfiguration or deletion/installation of containers. Typically, operators should only be given access at the lowest privilege level they need to fulfill their jobs.

For the user levels *user* and *containeradmin* the default password is the same as the user name.

Each user (*user, containeradmin, admin*) can change their own password. Admin users can change all passwords. To change a password, go to *Settings* → *Accounts*, choose the user, enter a new password and confirm the password. Up to and including MICA base system version 3, passwords must only contain ASCII characters, version 4 and higher support UTF-8 user names and passwords.

Warning: Make sure to store your password in a safe place. HARTING is not able to recover lost passwords! If you have lost your password, contact your HARTING service provider or MICASupport@HARTING.com for instructions how to return your MICA for a factory reset.

4.4 Firmware Reset

To reset the MICA to default settings, go to *Settings* → *Firmware* → *Reset* and click OK in the confirmation dialog. The MICA will reboot with factory defaults. After a firmware rest all containers are stopped and have to be restarted. Container settings and data stored in containers are not affected by a firmware reset.

Warning: A firmware reset also resets all MICA base system network settings, including static IP addresses. To access your MICA after a firmware reset, see chapter 2.

4.5 Firmware Upgrade

The most up to date MICA firmware is available on http://mica-container.com and http://www.harting-mica.com. Once you have downloaded the archive to your local PC or network, click *Install* to start the upgrade process. Then select the appropriate archive and click *Update.* After displaying a confirmation dialog, the MICA installs the new firmware and reboots. Container and user data are not affected by a firmware update.

Depending on your operating system and browser, you might have to perform a force refresh of your browser window after the MICA restarts to reconnect to the MICA:

Warning: During a firmware upgrade do not disconnect the MICA from power or close your browser session.

4.6 Generating a System Report

To get a comprehensive overview of your MICA and all installed containers, you can generate a system report from the *Information* panel by clicking *Device Summary* under *MICA Resources* and saving the generated JSON file.

5 Container Configuration and Maintenance

5.1 Container Installation

To install a container, click *Install* in the web GUI, select the desired container archive in the file dialog, and click *Execute*. The MICA will show the installation process.

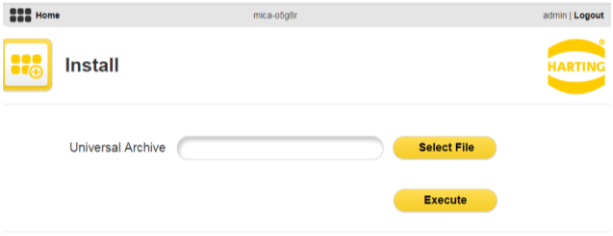

FIG. 12: INSTALL

After installation, you need to start the container manually before it can be used.

5.2 Container Update

To update a container, click *Install* in the web GUI, select the desired container archive in the file dialog, and click *Execute*. The MICA will show the upgrade process.

Container updates do not affect user data stored in the container.

5.3 The Context Menu

All container management operations are available in the container context menu. You can open the context menu by right-clicking a container icon or by long pressing it on a touch screen.

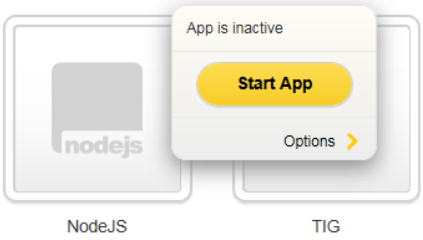

FIG. 13: CONTEXT MENU

5.4 Accessing the Container UI

If a container provides its own user interface, you can access it by clicking on a running container. If the container does not provide an interface, an informational message will be shown.

You can also access a container directly by entering the URL *https://micaname/#1_containername* in your browser.

If the container has been designed according to the HARTING development guidelines, *https:// micaname /#1_containername/api* will open a page describing the functionality and application programming interface of the container and *https://micaname.local/#1_containername/readme* will display the container readme.

5.5 Container Network Settings

The MICA base system automatically assigns an IPv6 link local and ULA address that lets the container communicate locally. To assign additional IP addresses choose *Options* → *Settings* from the context menu. Most settings are analogous to the settings for the MICA base system (see section 4.1).

5.5.1 Additional Network Interface

Additional Network Interface lets you specify additional network interfaces on a HARTING MICA and configure various container types as gateway containers to let applications use these additional network interfaces as default gateways. Note that standard container-to-container communication and communication between the MICA base system and containers will always use the primary network interface. For more information, see the *Additional Network Interfaces* application note on www.harting-mica.com.

5.6 Container Reset

To reset a container to factory settings, choose *Options* → *Reset* and click OK in the confirmation dialog.

Warning: A container reset deletes the overlay (see section 6.1) and thereby deletes all user data and configurations. We strongly recommend to create a backup before resetting a container. To do this, either duplicate the container on the MICA itself, or merge the container and export it to your PC or a network drive.

5.7 Container Duplication

To duplicate a container, choose *Options* → *Duplicate* from the context menu and enter a name for the duplicated container. *Duplicate* makes an identical copy of the root file system and the overlay (see section 6.1) of the original container and stores it on the MICA. The duplicated container has the same reset behavior as the original container in that a container reset will reset the container to the factory defaults of the original container.

The main use of *Duplicate* is creating a snapshot of a container. You can use this snapshot to quickly try out a new configuration, or to have a backup of the container on the MICA itself, for example before performing a container update.

5.8 Container Export

To export a container, first choose *Options* → *Merge* and then *Options* → *Export* from the context menu. Then select a location to save the exported container to and name the file.

The primary use of *Export* is to create a container for distribution or to store a backup outside the MICA. *Merge* combines the root file system and the overlay (see section 6.1) of the original container into a new root file system and *Export* saves the merged container as a .tar archive.

In contrast to *Duplicate* a reset of an exported container returns it to the state it had when it was exported.

5.9 Container Overlay Export

To export just the container overlay (see section 6.1), choose *Options* → *Export*. Then select a location to save the exported overlay to and name the file.

The primary use of an overlay export is backing up or distributing user data and container configurations.

6 MICA Software Architecture

All MICA applications consist of one or more LXC[1] containers, which are managed by the MICA base system.

Containers are virtual machines used for developing and running applications. Administrators and users can start, stop, configure, install, uninstall, duplicate and export containers.

The MICA base system contains the operating system and Linux kernel. It manages users, network access, hardware access, and the container lifecycle. The MICA base system is not accessible to users other than through the web interface.

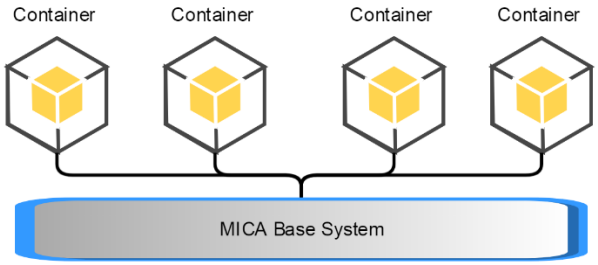

FIG. 14: CONTAINERS AND MICA BASE SYSTEM

Communication between containers happen via IP protocols with websockets or wss being the lowest level communication protocol. In many cases, container developers choose higher level protocols like MQTT or OPC-UA.

6.1 Container Architecture

Each MICA container has a two-tiered file system: the *root file system* and the *overlay.* The root file system stores all the application code and the default container configuration. During installation, the MICA creates an additional overlay file system that stores user data and changes to the default configuration. This architecture allows swapping out the root file system—for example when performing an update—without affecting user data and settings.

6.2 MICA Network Topology

The MICA base system and the installed containers form a network that is managed by the MICA base system. The MICA base system automatically assigns an IPv6 Link Local and an IPv6 ULA address to itself and each container, which are used to communicate internally. Administrators can assign additional IPv4 and IPv6 addresses both to containers and the MICA base system. If an administrator configures the MICA base system and containers to use DHCP, they will acquire IPv4 addresses from the specified DHCP server.

[1] For more information on LXC, see https://linuxcontainers.org/

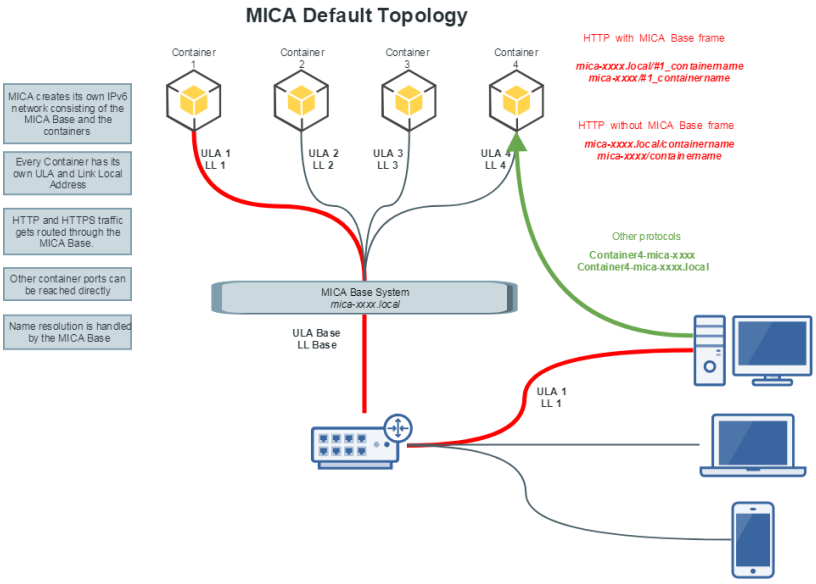

FIG. 15: MICA NETWORK TOPOLOGY

The MICA base system also performs name resolution while containers have their own MDNS and LLRP responders. This means that containers can be addressed via *micaname/containername*. For example, *https://mica-test/gpio* (or *https://mica-test.local/gpio* on Linux and Mac OS) will bring up the default web page of the container named gpio running on mica-test.

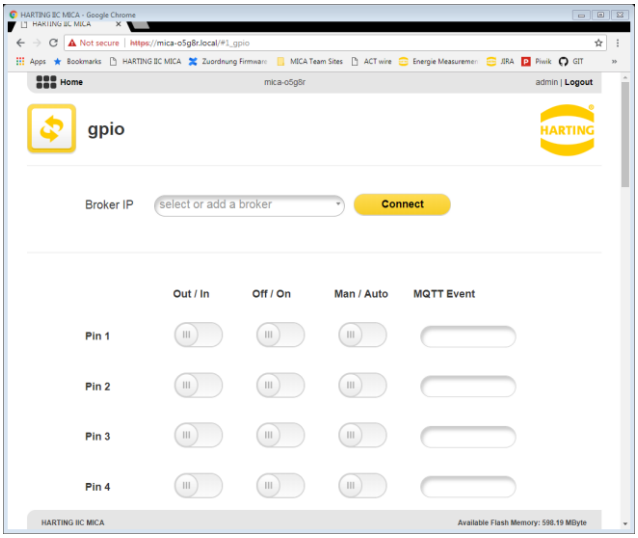

FIG. 16: CONTAINER HOMEPAGE

Adding *#1_* to the URL will bring up the default website of the container as an iFrame in the MICA Base web GUI.

Starting with MICA base system firmware version 4, MICA supports aliased communication. Aliased communication lets containers connect to the MICA base system and other containers on the same MICA using the aliases *mica* and the containername, respectively.

7 Troubleshooting

Problem	Solution
MICA doesn't start. Power LED is dark.	1. Check the power connection. 2. If possible, connect the MICA to an alternative power source (e.g. 24V instead of PoE).
MICA doesn't start. Power LED is red.	1. The MICA cannot connect to the network. Check your network connection. 2. Disconnect the MICA from the power source for at least 30 seconds. 3. Connect the MICA directly to a PC and follow the instructions to connect using the fallback address as described in section 2.2.
MICA does not show up in the network.	1. Check that the MICA is connected to power. 2. Verify that the power LED and network LEDs are green or blinking yellow. 3. Check your network connection. 4. Restart the MICA and wait until the network LEDs blink yellow. 5. Check if any network security settings prevent the MICA from connecting to the network (for example MAC filters or required passwords). 6. Check that the MICA is in a network segment that is reachable from your computer. 7. If you are using a VPN, disable the VPN, restart your computer and try to connect to the MICA. 8. If your network supports IPv6, try connecting to the link local or ULA address. 9. Disconnect the MICA from the power source for at least 30 seconds. 10. Connect the MICA directly to a PC and follow the instructions to connect using the fallback address as described in section 2.2.[2]
MICA cannot be reached by name	Due to LLRP caching in Windows, the MICA might not be available by name in Internet Explorer and Chrome after a failed connection attempt for up to 5 minutes—or the value *NegativeCacheTime* is set to in the Windows registry—until Windows performs a DNS cache refresh. 1. In Chrome, the MICA is reachable via *micaname.*local: 2. In IE and Chrome, the MICA is reachable via its IP address. 3. Clearing the DNS cache with *ipconfig /flushdns* resolves this problem.
Lost password	For security reasons, the MICA is designed in a way that HARTING cannot recover passwords. Contact you HARTING service provider or MICASupport@HARTING.com for instructions how to return your MICA to HARTING for a factory reset. A factory reset will erase **all** user and application data.

[2] If you are using a MICA Wireless, follow the instructions in the MICA Wireless User Guide available at https://www.harting-mica.com.