Pushing Performance

People | Power | Partnership

HARTING MICA Base 5 Release Notes

1. Edition 2019

Contents

1 General Notes

To upgrade to MICA Base 5, MICA Base 2 or later has to be installed. If your MICA has an earlier version of the MICA Base, you first need to upgrade it to version 2, and then to version 5.

Please perform a browser refresh after upgrading the firmware.

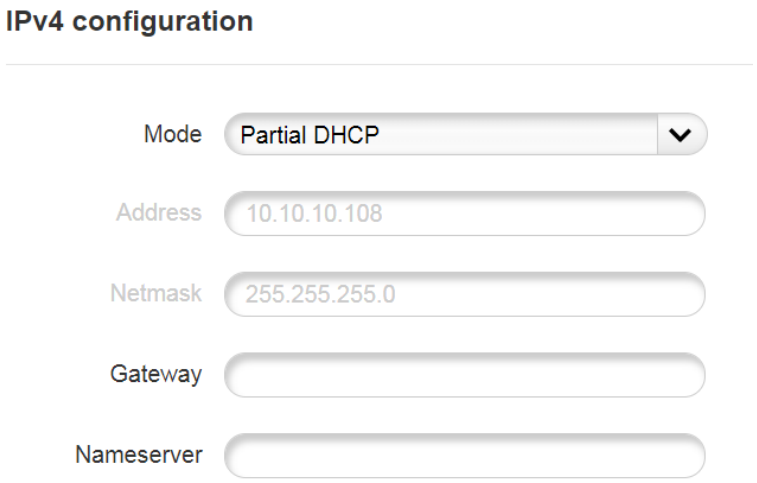
Warning: Firmware upgrades are NOT REVERSIBLE.

---

2 New Features

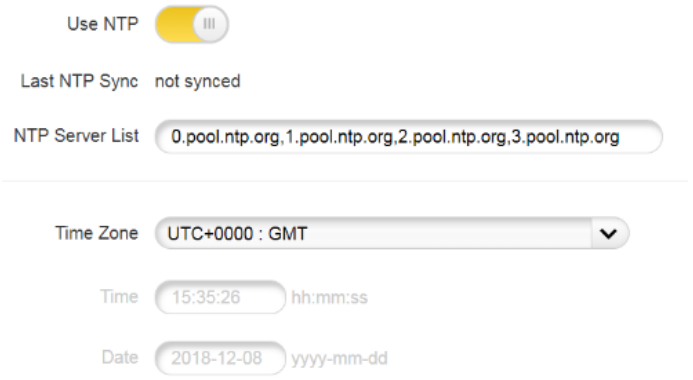
2.1 Manual Entry of Name Servers and Gateways

Gateways and name servers can now be set manually in DHCP environments using the Partial DHCP mode in both the base system and containers.



2.2 Last Sync for NTP

The MICA now shows the last time it successfully synced the real time clock with an NTP server or “not synced” if the synchronization failed.



2.3 No Firmware Update from Version 1.7 and Lower

Firmware updates from version 1.7 and lower are now disabled.

2.4 Selector for Basic Information

The new *.base_info* selector returns basic MICA information without the need for a SSO login.

2.5 Selector for Container Metrics

The new *.metrics* selector returns CPU and memory usage of a containers.

```
{
    "method" : "get_container",
    "params" :
    {
        "selector": ".metrics",
        "name": "gpio"
    }
}
```

Leaving the name parameter blank returns a list with the values for all containers running on the MICA.

2.6 Firmware Reset

Unresponsive MICA can now be reset using a µSD card or USB 3 memory stick. For instructions contact mica-support@harting.com.

Note: Opening the card cover on the MICA voids the factory warranty because it may compromise the waterproofness and protection class of the MICA.

---

3 New Features Specific to MICA Wireless

3.1 Access Point Scan Limited to Band

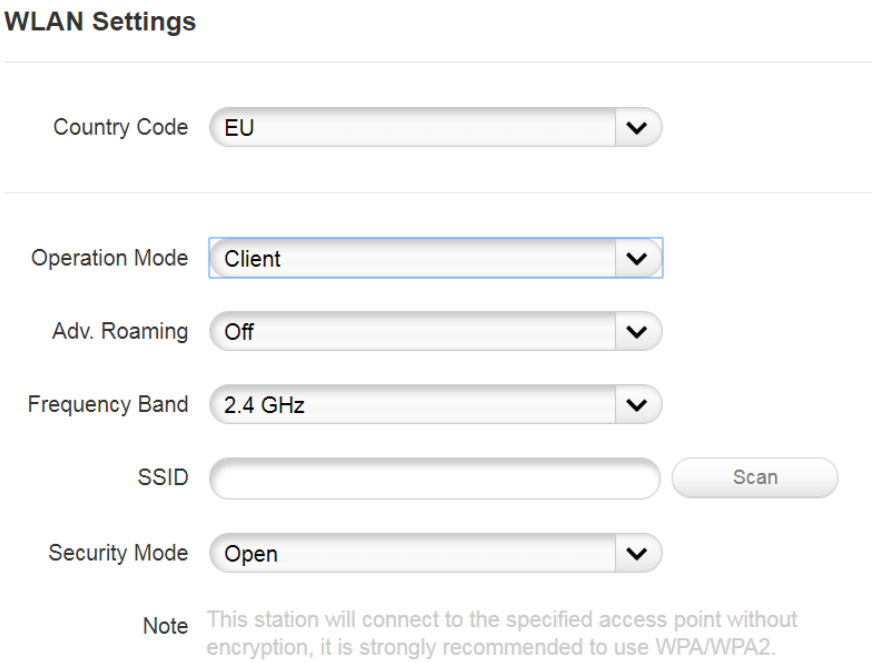
The access point scan can now be limited to either the 2.4GHz or the 5GHz band for customers who restrict WiFi band access.

3.2 Co-existence Mode for WiFi AP and BLE

The use of BLE while the MICA Wireless is running in access point mode is now supported.

3.3 SSID Scan in Access Point Mode

SSID scans can be performed in access point mode by selecting Client Mode from the drop down menu and launching a scan. This feature is not available when BLE is enabled.



4 Bug fixes

4.1 Occasional Startup Problems of the WEB UI

Firmware 5 contains a number of changes to address problems with starting the Web UI after container deletion and other operations.

4.2 Internal Name Resolution

Firmware 5 fixes some rare problems with internal name resolution and container to base system communication using IPv6.

4.3 More Graceful Handling of Dropped WiFi Packets

Firmware 5 handles dropped WiFi packets more gracefully than Firmware 4: it now waits for a few seconds before warning about connection problems and closing the WiFi connection.

4.4 Other issues

- Improved support for Microsoft Edge on Windows 10.
- Fixes for some issues concerning the startup of the WiFi and LTE modules of MICA Wireless after restarts and reboots of the MICA.
- Various security and stability enhancements.

5 Known limitations

- Due to a LLMR caching issue in Windows 7, the MICA might not be available by name in Internet Explorer and Chrome after a failed connection attempt for up to 5 minutes—or whatever *NegativeCacheTime* is set to in the Windows registry—until Windows performs a DNS cache refresh.
    - In Chrome, the MICA is reachable via *micaname.*local:
    - In IE and Chrome, the MICA is reachable via its IP address.
    - Clearing the DNS cache with *ipconfig /flushdns* resolves this problem.
- Container gateway functionality is not yet supported for IPv6.
- While advanced roaming is active, it is recommended not to launch scans for additional access points.

6 Notes

6.1 RPC

As a reminder: Firmware 2 contained a major redesign of the JSON RPC interface. Deprecated RPC calls will be disabled in a future firmware version after 2, so developers *must* migrate their containers to the new RPC format before 3/31/2019.

- New JSON RPC calls are only available via Websockets. These are get_base, set_base, get_container, set_container, changepasswd, sign_in, get_clients and set_client.
- If you want to use Deprecated RPC via HTTP make sure to also use old SSO authentification via get_auth_token. Keep in mind, that it is not intended to use Deprecated RPC via websockets.
- The following RPC are only reasonably available via websockets:
    - getStatusMessageCount
    - getStatusMessage
    - setResponseMessage
    - update
    - get_container
    - set_container
    - get_base
    - set_base
- if you want to use old RPC API methods with websockets, pass auth token as an empty string (do not forget to sign_in() before)
- Using RPC via HTTP requires to use deprecated SSO authentication via get_auth_token()
- transfer_chunk, reset_cert and some other calls are possible without authentification
- Old Busybox Based Container Web-GUI that use websocket SSO service (eg. GPIO, Python Demo, Mobile) sometimes might not come up. Restarting the container resolves this problem, alternatively you might use a workaround by modifying the "/etc/init.d/network"-file of your busybox container with

    .

    .

    .

    IPV6=$IPV6:0

```
if [ ! "$(cat /etc/resolv.d/20lo_dyn | grep $IPV6)" ]; then
echo "nameserver $IPV6" >> /etc/resolv.d/20lo_dyn
fi

+ # workaround for unreachable Base
+ping -c 1 $IPV6

# append config files
cat /etc/hosts.d/* | while read line
do
.
.
.
```

- Containers need to implement their own mdns responder to allow calling by name