periMICA

Perinets Modular Industrial Computing Architecture

User Guide

Perinet
Seamless IoT Connectivity

Abstract

The award-winning Modular Industry Computing Architecture has been taken up and redesigned by Perinet. Thanks to the flexible, modular approach, the periMICA edge computer can be adapted as needed. Depending on the application and environment, different hardware modules and software apps can be combined from a construction kit and extended with own hardware and software elements.

The successful combination of industry-standard hardware and open source-based software has been retained in order to take over decentralized tasks in the field. The platform is based on a secure Linux system, applications run in independent software containers. In addition to the compact and robust IP67 aluminium housing, periMICA will also be available as an IP20 version for installation in the control cabinet.

Doc-No.: PRN.100.392 rev: 2

July 22, 2022

Document Information

Title	periMICA
Subtitle	Perinets Modular Industrial Computing Architecture
Type	User Guide
Status	Release
Version	2
Date	July 22, 2022
Disclosure Restriction	

Contents

1 Overview

The periMICA is an edge computer which can run typical functions needed in an (I)IoT application in the field. Specifically functions like data preprocessing/aggregation, local function control, showing dashboards or forwarding data to higher level IT-systems.

The periMICA hosts lightweight virtual machines, so-called containers, and allows you to setup your applications with the same techniques used nowadays in the cloud. You can see the periMICA as a datacenter in a box, which greatly supports shifting the functionality of your application between cloud and field, according to your needs.

Perinet also provides containers for functionalities needed on field level in (I)IoT applications, typically, e.g. a local MQTT broker. It is therefore the first stop for data traveling from sensors or actuators to the cloud. The sensors and actuators are connected preferably via network, as shown in Figure 1, in combination with our other products. In the same time, the periMICA is ideal as bus master for non-Ethernet sensors as well.

Everything from network infrastructure down to sensor & actuator:

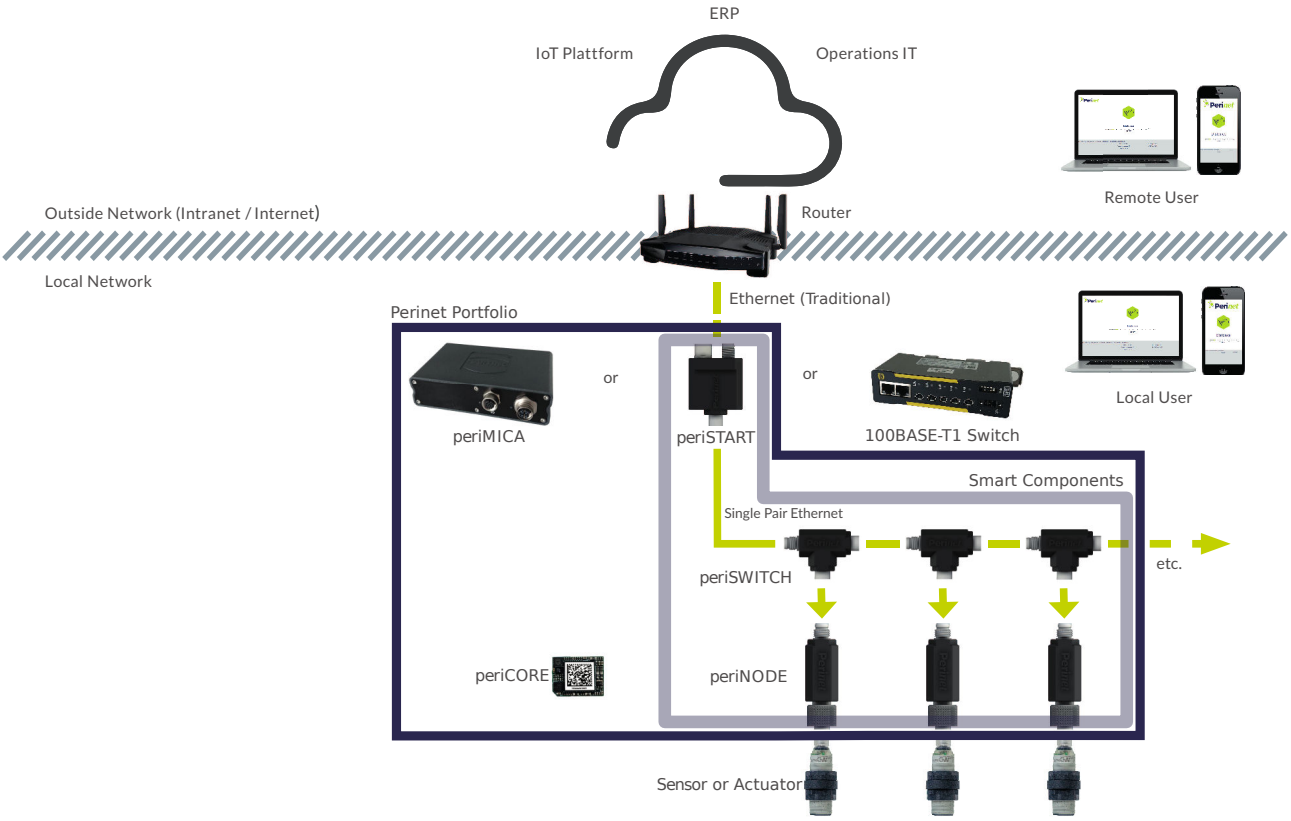


Figure 1: Perinet Seamless IoT Connectivity System

The periMICA is also a perfect base for your own product development, due to its modular hardware & software architecture. This allows you to develop specialized products in low and mid quantities for reasonable costs.

2 Starting Up

Mounting

1. Unpack the device and verify the scope of delivery.
2. Check all delivered components for damage.
3. Mount and ground the device with the optional DIN rail adapter or wall mounting kit (available separately).

Electrical Connection

Info

Ensure correct polarity when connecting the power supply. The device may only be operated with safety extra-low voltage (SELV) according to IEC 60950-1 / EN 60950-1 / VDE 0805-1 or with protective extra-low voltages (PELV) according to EN 50178.

The supply voltage must be secured with a 10A circuit breaker. Only use power supply units according to IEC 60 364-4-41 or HD 384.4.41 S2 (VDE 0100 part 410).

The device is grounded via a screw on the back and via the DIN rail or wall mounting kit.

Connection

Option 1: Powered via 24 VDC supply. In this case, connect the device to the A-coded M12 connector according to the pin assignments. Then connect the X-coded M12 connector to a switch or computer with RJ45.
Option 2: Powered via Power over Ethernet. In this case, connect the device to a PoE-capable switch with a suitable X-coded M12 cable.

Commissioning

1. Check to ensure that the device is mounted securely.
2. Turn the power supply on. The power LED (beside the connector) initially flashes green during the boot process, then is on solid green after a successful system start. A fault is present if the LED lights up red.
3. Check the data transfer activity. Monitor the LEDs on the connector.
4. If the fault cannot be rectified, remove the device as described under "ASSEMBLY" > "Dismantling" and return it to the manufacturer with a description of the fault.

Status LEDs

LED displays	Meaning
Green LED on the connector is flashing	Device is booting
Green LED on the connector is on solid	Device is ready
Red LED on the connector is on solid	Fault
Orange LED on the connector is on flashing / on solid	Link is active

3 periMICA Hardware Architecture

The periMICA hardware architecture is based on a modular concept. The flexibility of the hardware architecture makes the periMICA a perfect fit to your application specific needs, as the hardware modules are designed to be interchangeable, to adapt to a specific environment.

The periMICA housing is following the same modular concept and it can either have an IP67 certification or an IP20 certification, depending on the needs of your application. The housing is made of aluminum, which makes the device robust and lightweight.

All periMICA devices have the same commercial name ("periMICA modular edge computer") and the same manufacturer part number (PRN.000.025). To distinguish among different periMICA variants, each variant receives an up-counting specification number that describes its configuration and makes it possible to re-order the periMICA with the same specification.

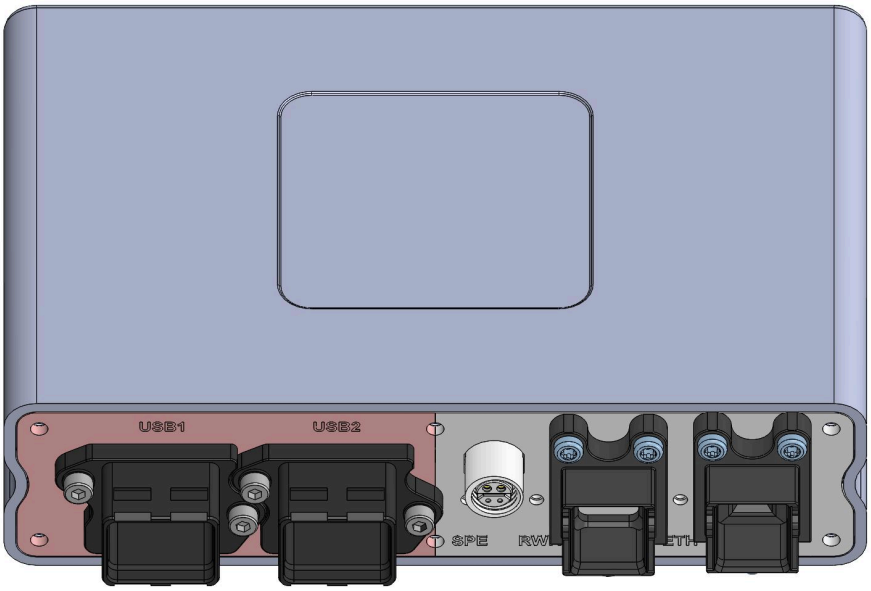


Figure 2: periMICA Housing

The housing dimensions are always the same for all the different variants of the periMICA. From the outside, the periMICA can be divided into two halves, as you can see in Figure 2 above. The left half (light pink) is used as the function side where the application that needs a special interface is connected to and the right half (grey) is used to supply the periMICA with power and connect it to the local infrastructure.

The inside of the computer is made of three printed circuit boards (PCBs) that define the interfaces and functionality. The three PCBs are categorized into supply module, processor module and functions module. Each of the modules is interchangeable with another module of the same category. The three PCBs are shown in Figure 3.

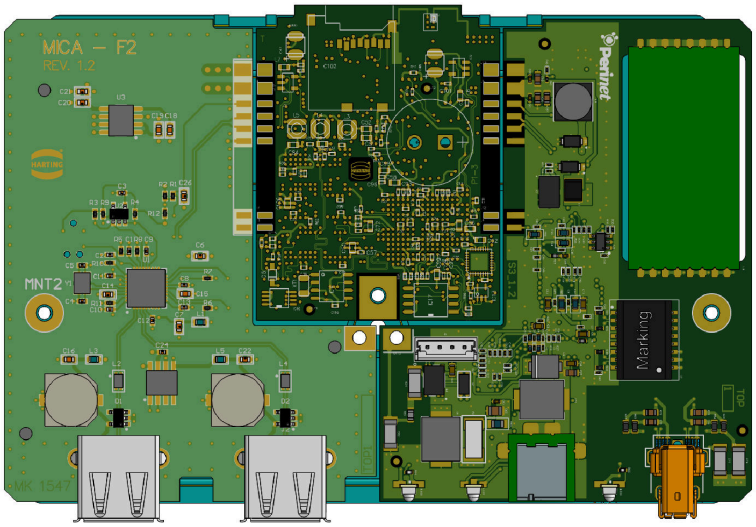


Figure 3: periMICA Modules
On the left is the function module, in the middle the processor module and on the right the supply module

The processor module uses the Universal Serial Bus (USB) protocol to communicate to the other modules. To grant the exchange ability between the modules, an interface is standardized by Perinet GmbH. This interface can be used by everybody to develop their own modules and adapt the periMICA modular edge computer to their own application.

Electrical Specifications

The global termination Table 1 below is an overview of a few technical parameters that are globally defined for all the periMICAs. Each device needs to be compliant at least to this global termination data. The supply module can have even higher restrictions.

Global termination data	
Operating voltage	24V DC
Max DC voltage	60V DC
Surge protection	yes
Supply circuit	SELV/PELV with Circuit Breaker 10A
Power consumption	max 15 Watts
Over-current protection	yes
Inverse-polarity protection	yes

Table 1: Global termination data

Technical parameter	Value
Ambient temperature	-25°C ... +75°C
Storage temperature	-25°C ... +85°C
Relative humidity	5 ... 95% non condensing (operation) 5 ... 95% non condensing (storage/transport)
Protection Class	IP67 (mated condition) IP20
Relative humidity	5 ... 95% non condensing

Table 2: Technical parameters

Mechanical Specifications

Material properties	
Material housing	aluminum (powder-coated)
Dimensions (mm)	132x86x35 without connectors
RoHS	compliant
REACH	compliant
REACH Annex XVII substances	no
REACH ANNEX XIV substances	no
REACH SVHC substances	no

Table 3: Material properties

4 periMICA Variants with Additional Connections

In this section we present a few of the modules that are currently available for the periMICA modular edge computer and their purpose. As described in the previous chapter, the periMICA contains three modules, each with its own functionality. The power supply module is responsible for powering the periMICA device and providing an interface to the local infrastructure, the processor module is the computing unit of the periMICA and the function module is used for the application specific adaption of the periMICA.

4.1 Supply Module

The supply module is used as a power source and creates the connection to the local environment, from where the operator can reach and configure the periMICA. Each supply module has a power LED that indicates the status of the device.

Color	periMICA status
green	ready
red	during boot

4.1.1 S1 Module

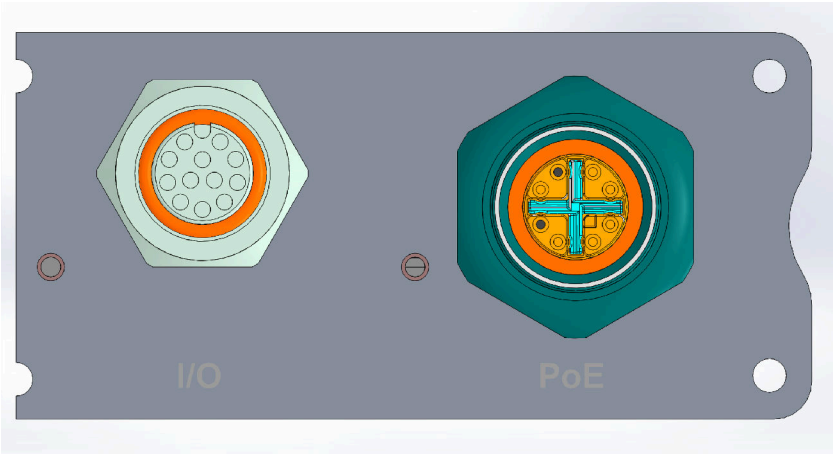
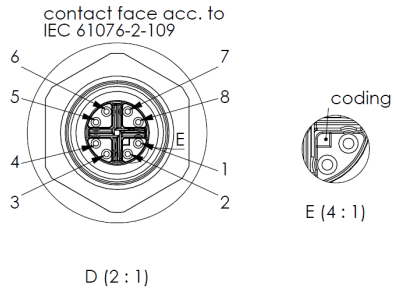


Figure 4: periMICA S1 Module
From left to right: power LED, I/O-connector, act LED and PoE connector.

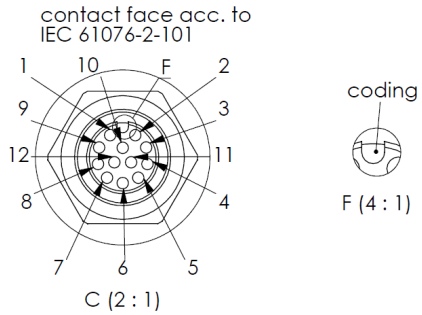
This supply module provides a Fast Ethernet (100BASE-TX) connection via the PoE connector (M12 X-Coded push-pull). The **act** (activity) LED indicates the transmission and reception of Ethernet frames, i.e. the periMICA has a valid link.

The computer can be powered over the PoE connector via Power over Ethernet (IEEE 802.3af) or over the I/O connector (M12 A-Coded 12 pin) with 24 volt direct current. For the pin-out, please refer to M12 A-Coded.



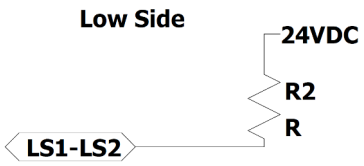
M12 X-Coded

Pin	Description	T568A/PoE		T568B/PoE	
1	RX+	WH/GN	DC-	WH/OR	-
2	RX-	GN	DC-	OR	-
3	TX+	WH/OR	DC+	WH/GN	-
4	-	BU	-	BU	DC+
5	-	WH/BU	-	WH/BU	DC+
6	TX-	OR	DC+	GN	-
7	-	WH/BR	-	WH/BR	DC-
8	-	BR	-	BR	DC-

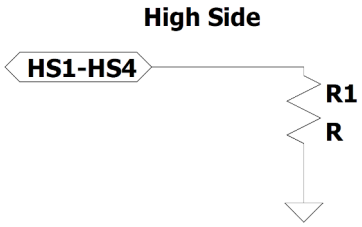


M12 A-Coded

Pin	Signal	Description
1	GPIO7	LS2
2	GPIO6	LS1
3	GPIO4	SWO1
4	GPIO0	HS1
5	GPIO2	HS3
6	GPIO1	HS2
7	GPIO3	HS4
8	GPIO5	SWO2
9	GPIO5	SWS2
10	GPIO4	SWS1
11	24V IN	Power In (+)
12	GND	Power In (-)

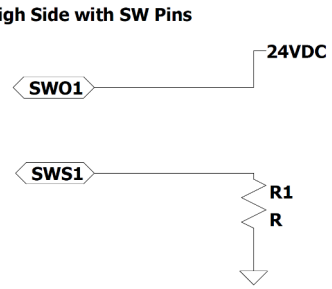


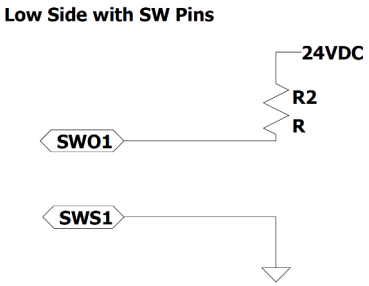
LS stands for low side switch and is used to be connected between the load and GND for switching the load on and off. All LS pins are connected internally to GND.



HS stands for high side switch and should be connected between the 24 volt direct current and the load for proper operation. All HS pins are internally connected to 24V DC.

The SWO pins have no inner connection to GND or 24V DC. The operator can decide if he wants to use these pins as high side or low side switches.





Warning: *Please note that the GPIOs from the I/O connector are not supported with the base system software version 21-01.*

Electrical Specifications

Absolute maximum ratings	Value
PoE connector	
Fast Ethernet cable length	100 meter
Max DC current	0.5A
Max DC voltage	57V
I/O connector	
DC voltage	60V
DC current	2A

Table 4: Absolute maximum ratings S1 module

4.2 Processor Module

The processor module is the heart of the periMICA modular edge computer as it runs the firmware and connects the modules. The processor module is used to host and run your application. A short overview of the currently available processor modules and their main features is presented next.

The Flash is the main memory for the Linux-based base system. The periMICA base system uses two partitions and each partition takes around 256 megabytes, i.e. in total around 512 Megabytes can be subtracted from the Flash storage.

4.2.1 P1 Module

Processor	1GHz ARMv7 Cortex A8
RAM	1GB
Flash	4 GB
Interface	USB 2.0

4.2.2 P2 Module

Processor	Dual Core 1.3GHz ARMv7 Cortex A9
RAM	2GB
Flash	16 GB
Interface	USB 2.0/3.0

4.3 Function Module

The function module is used to expand the periMICA functionality, by adding application specific interfaces. The newly added interface can either be a specific one like RS485 or a more generic bus interface. The idea behind the function module is to connect the application from where you want to collect or read the data and send it via Ethernet.

4.3.1 F2 Module

The F2 USB function module is used to add USB devices to the periMICA. An USB to Ethernet dongle could be connected to the periMICA for a second Ethernet interface. The USB device can later be assigned to a container. The USB function module has two USB 2.0 Type A interfaces. The HARTING push pull (Figure 5) sockets are optional. With the push pull sockets in the function module, the periMICA can be IP67 compliant, otherwise it has only IP20 compliance.

Warning: *Please be aware that only when both interfaces are plugged in, the device is IP67 compliant. If only one USB interface is needed, please add a cover for the other USB interface. Without the push-pull sockets, the periMICA only has an IP20 certification.*

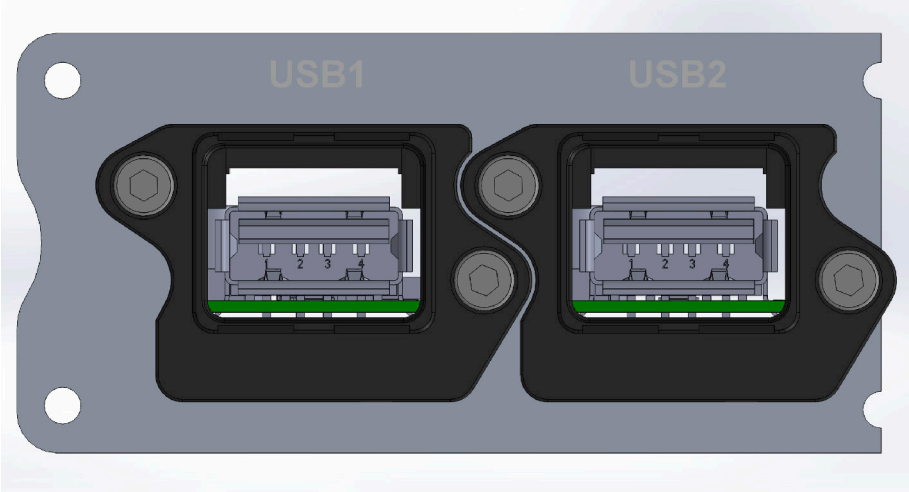


Figure 5: periMICA F2 Module

While the IP67 USB connector accepts most USB A plugs, we recommend using a HARTING IP67 push-pull cable for water and dust protection.

USB devices connected to the USB port will show up in the ***Settings → Devices*** screen in the Web UI of the periMICA base system. Devices can be added to a specific container as needed. After this step, it is then possible to directly start developing an application with the specific hardware in your container.

Because all periMICA modules are connected internally via USB, the USB function module is the one recommended to start with for your development.

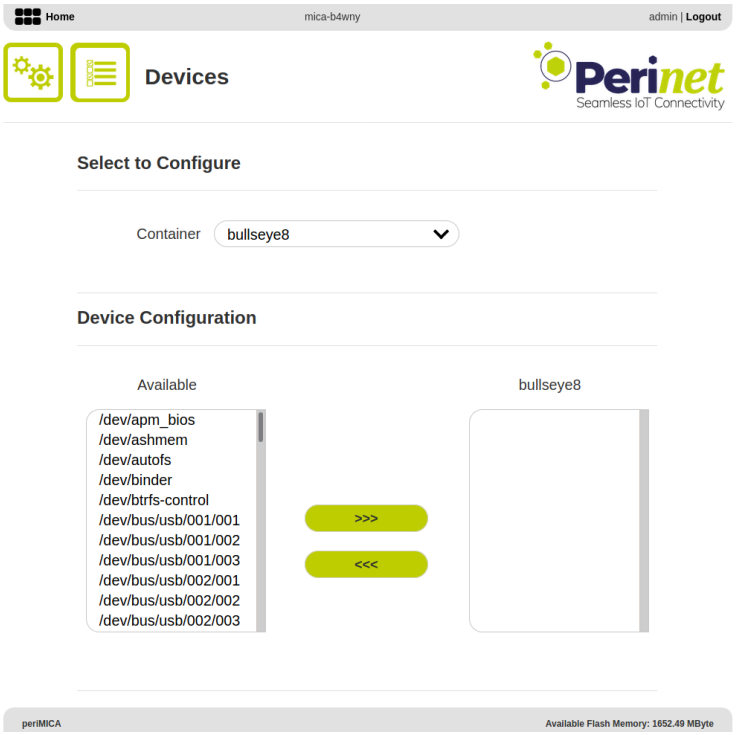


Figure 6: periMICA Devices

The periMICA base system supports hot plugging and will recognize most USB devices when they are plugged into a running periMICA. If your USB device is not auto-detected, try power cycling the periMICA device.

Electrical Specifications

Absolute maximum ratings	Value
USB cable length	1 meter
Max DC current	0.5 A per Port
Max DC voltage	5 VDC ± 10 %
soft-start feature	yes per Port
short circuit protection	yes per Port

Table 5: Absolute maximum ratings USB module

5 periMICA Software Architecture

periMICA is a host for virtual machines, used for developing and running applications.

All periMICA applications consist of one or more LXC containers, which are managed by the periMICA base system (Figure 7). Administrators and users can start, stop, configure, install, uninstall, duplicate and export containers.
For detailed information on LXC, please visit `https://linuxcontainers.org/`.

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

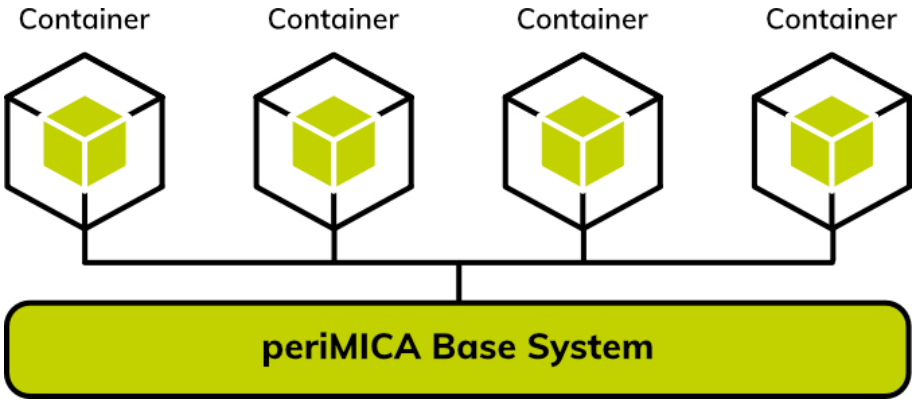


Figure 7: Containers and periMICA Base System

From networking perspective, periMICA containers are independent hosts. Basically, container developers can implement communication protocols of their choice, like MQTT, https and so on. On top of that, containers can access periMICA base system services via web sockets without password login, unlike other periMICA clients. For configuration purposes, each periMICA container is shipped by default with a https server just like periNODEs.

For details on how to deploy your own application with the Debian container for periMICA, please see our *Debian Container User Guide* [**Debian Container User Guide**].

5.1 Container Architecture

Each periMICA container has a two-tiered file system: the root file system and the overlay. The root file system stores the application code and the default container configuration. During installation, the periMICA 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.

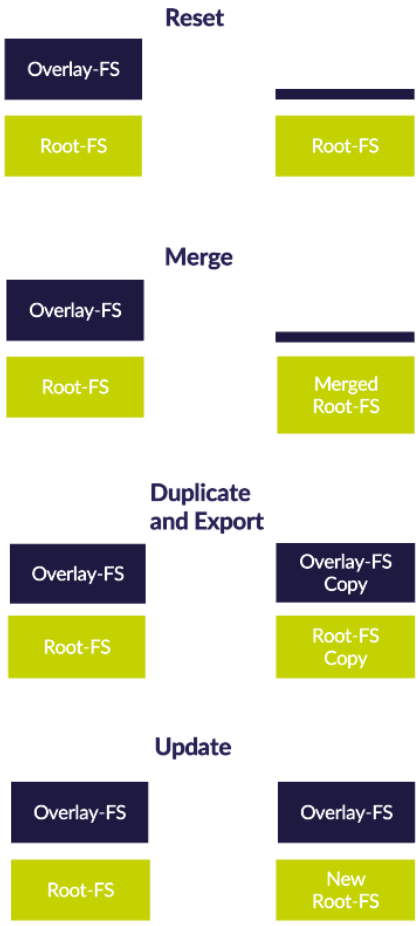


Figure 8: Container Lifecycle Functions

5.2 Network Topology

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

The periMICA base system also performs name resolution, because containers have their own MDNS responders. This means that containers can be addressed via ***containername-periMICAname.local***.

For example, `https://gpio-perimica-test.local/` will bring up the default web page of the container named ***gpio*** running on ***perimica-test***.

6 First Steps

6.1 Connecting your periMICA to Power

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

Figure 9: Connecting periMICA with PoE Injector

Warning: *Make sure to use an appropriate power source. Some commercially available PoE injectors do not follow the IEEE 802.3af standard and can damage devices like periMICA through voltage peaks of up to 80V. If you are unsure which PoE Injector to use, please contact our support (see Contact & Support).*

periMICA 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.

6.2 Logging In

The periMICA is accessible under the name listed on the label at the bottom of the device (Figure 10).

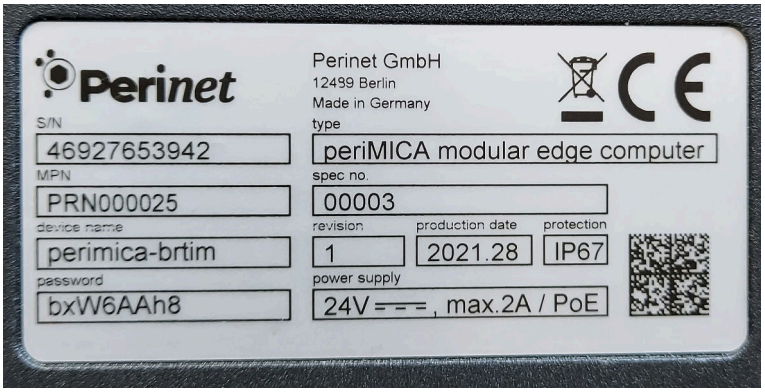


Figure 10: periMICA Label

Please log into the periMICA web interface using `https://perimicaname.local`:

Figure 11: periMICA Browser Access

First Login

To log into your periMICA for the first time, use the username ***admin*** and the password listed on the label (Figure 10).

We strongly recommend that you change the ***admin*** password as well as the passwords for ***containeradmin*** and ***user*** immediately after logging in for the first time.

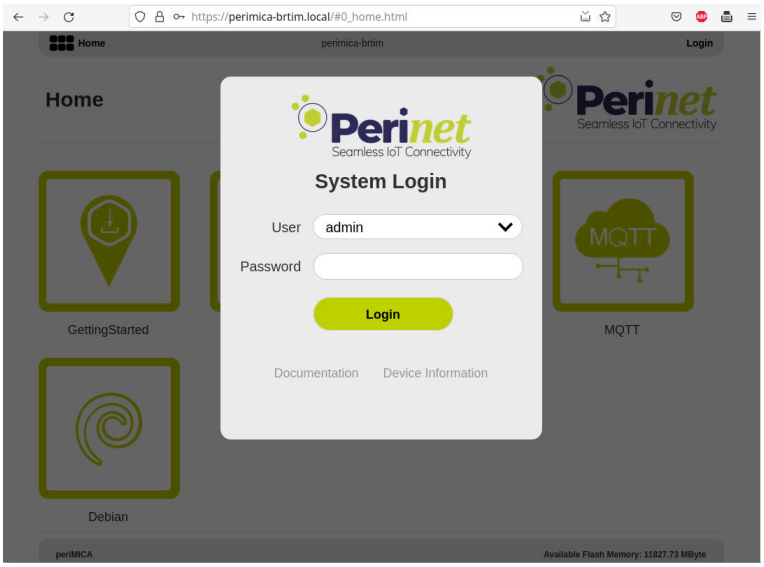


Figure 12: periMICA Login

You can access the periMICA 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.

Note: Make sure to store your password in a safe place. In case of lost credentials, a Factory Reset (Section 7.3) of the periMICA will restore the initial credentials.

7 periMICA Basics

The periMICA Home screen (Figure 13) displays a section with different periMICA application containers and a section containing the settings, installer and information of the base system.

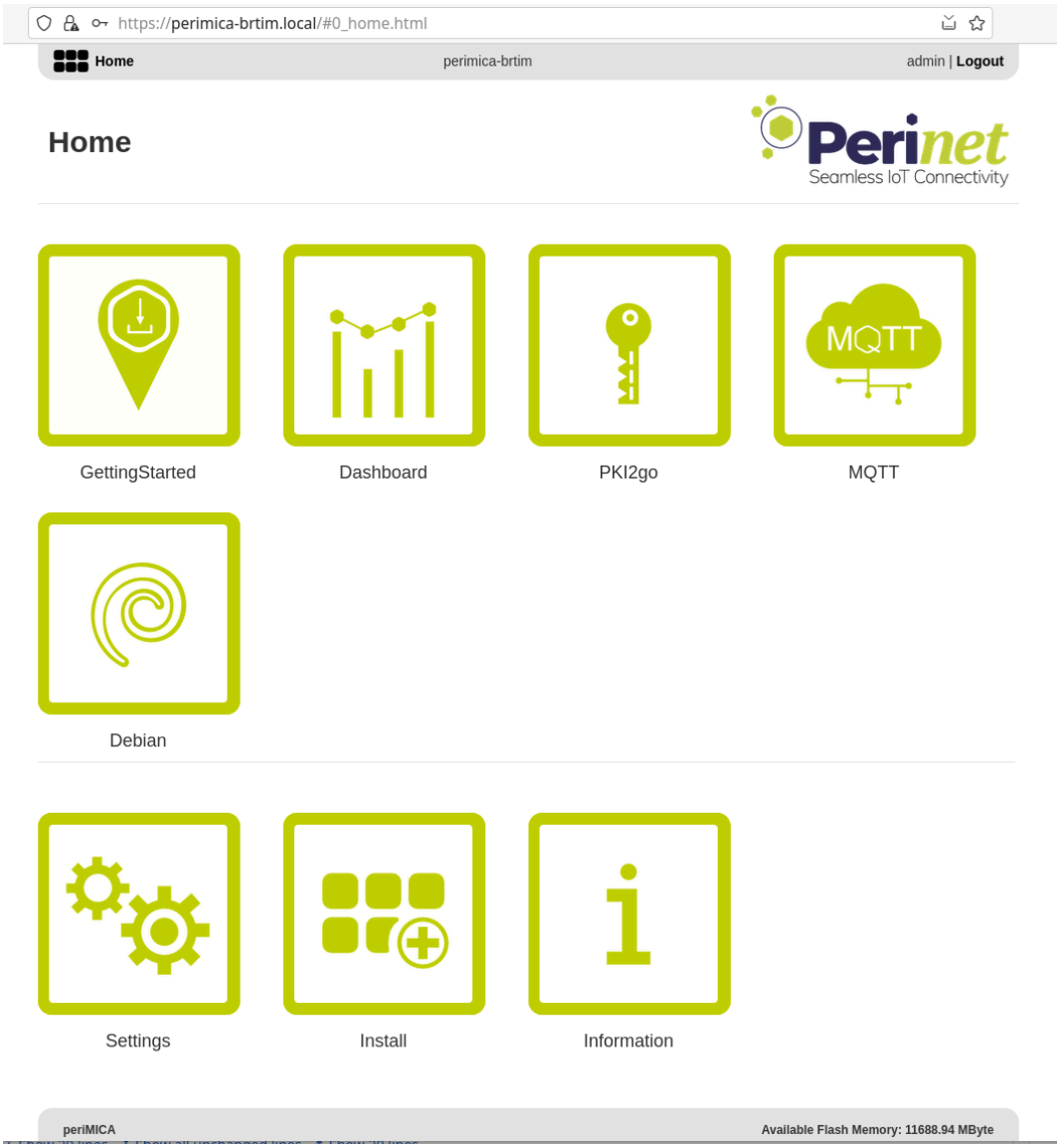


Figure 13: periMICA Home Screen

In this chapter, we will focus on the basic settings and operations that can be done in periMICA base system.

7.1 Time and Date

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

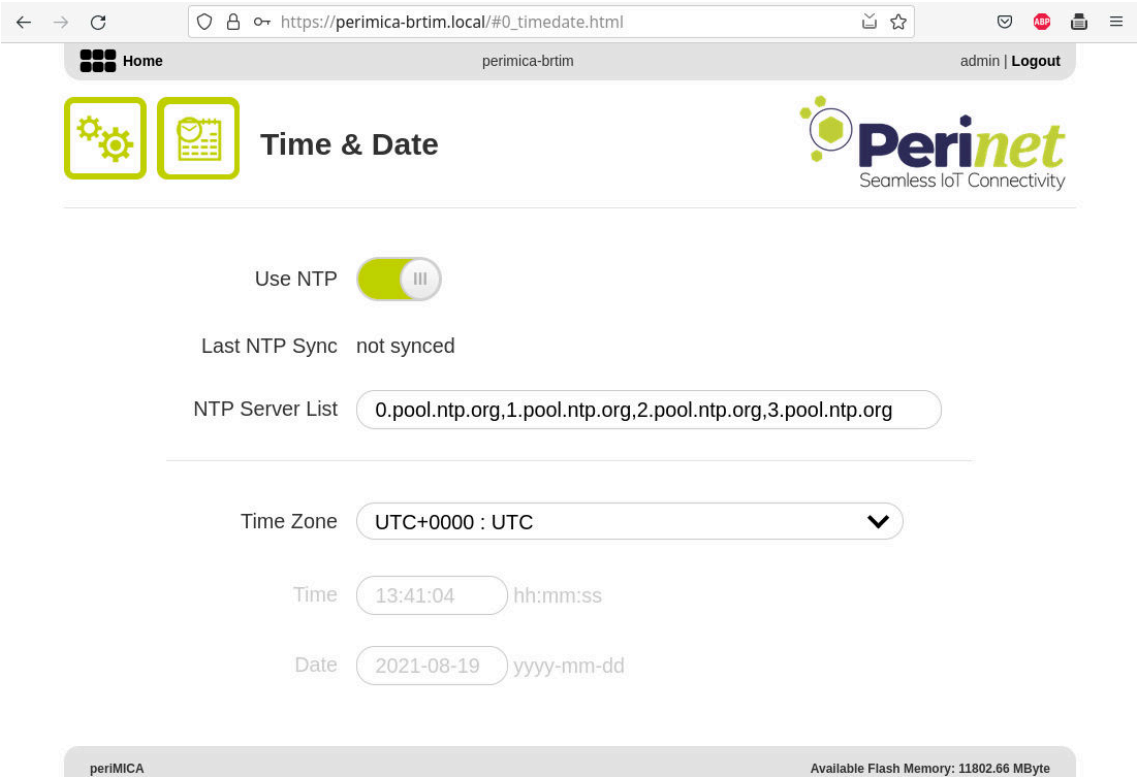


Figure 14: periMICA Time and Date

If your periMICA has access to a time-server, we recommend that you activate NTP. By default, the periMICA 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 must be set manually.

It may take a couple of seconds for the periMICA to synchronize with the NTP server. The periMICA 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.

7.2 Changing Passwords

For security reasons, your periMICA is shipped with a randomly generated administrator password, which is listed on the type shield on the bottom of the device. We strongly recommend that you change the password imme•diately after logging in to your periMICA for the first time.

Every periMICA has three user privilege levels —***user***, ***containeradmin*** and ***admin***— to provide protection against accidental or deliberate misconfiguration or deletion/installation of con-

tainers. Typically, operators should only be given access at the lowest privilege level they need to fulfill their jobs.

Each user (*user*, *containeradmin*, *admin*) can change their own password. Admin users can change all passwords. To change a password, go to ***Settings → Accounts***, select the user, enter a new password and confirm the password. Usernames and passwords support UTF-8 characters.

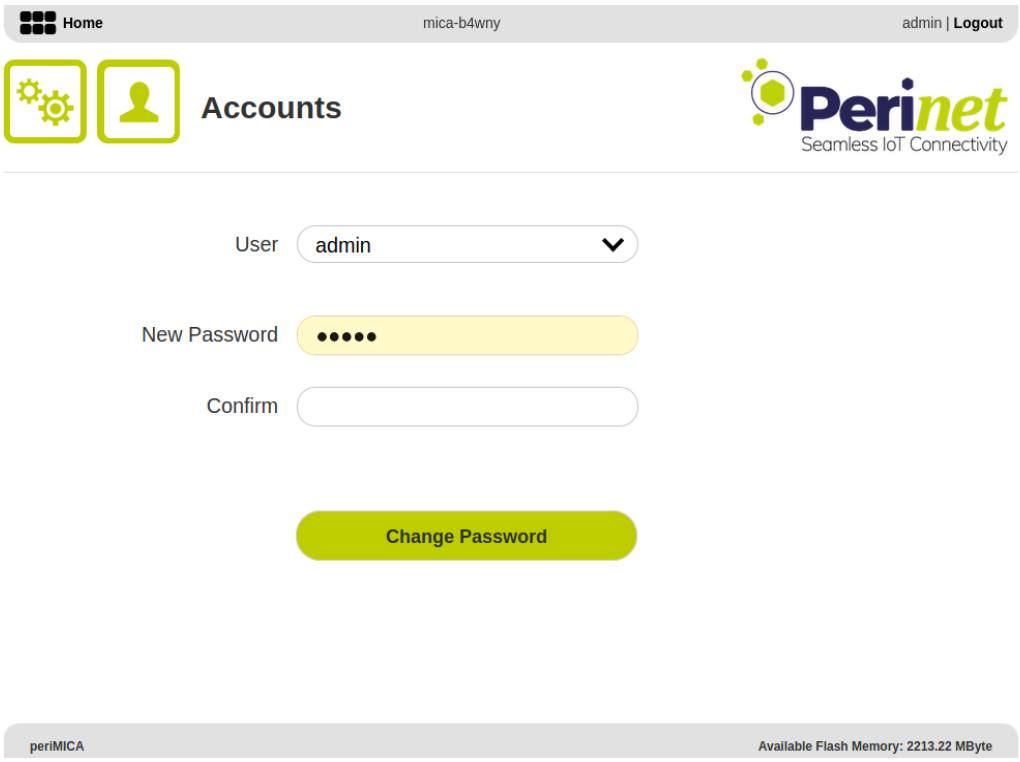


Figure 15: periMICA Account Settings

We strongly recommend that you change passwords for all users immediately after logging in to your periMICA for the first time. Passwords are reset during Factory Reset (see Section 7.3).

7.3 Factory Reset

A Factory Reset will restore the default settings of the periMICA device, including network settings as well as credentials. To access your periMICA after a Factory Reset see Section 6.2 for further details.

The periMICA device implements two procedures to perform a Factory Reset, via the Web User Interface and with SD Card / USB Stick. The latter can be executed without credentials.

7.3.1 Factory Reset via WebUI

To reset the periMICA to its default settings, go to ***Settings → Firmware → Reset*** and click ***OK*** in the confirmation dialogue. The periMICA will reboot with factory defaults. After a factory

reset, all containers are stopped and must be restarted. Container settings and data stored in containers are not affected by a factory reset.

7.3.2 Factory Reset via SD Card / USB

It is possible to reset the periMICA via SD Card or USB dongle (depending on periMICA variant) To perform the Factory Reset procedure via SD Card or USB dongle execute the following steps:

- Power down the periMICA device.
- Open the back lid with a TX8 screwdriver
- A SD Card (SD Card slot) or a USB dongle (USB-C port) has to be prepared. Please make sure that your device is formatted with FAT32 (the default for most devices). Afterwards create a text file named `control` inside root directory with the following content:

```
{"command":"fw_reset"}
```

- Connect the SD Card (SD Card slot) or the USB dongle (USB-C port) to the slot beneath the back lid of the periMICA device.
- Wait until the periMICA LED is blinking red/green and turning red again, remove the SD Card / USB dongle and close the back lid again.

Warning: Opening the back lid of the periMICA can affect the IP67 protection of your device.

7.4 Firmware Update

The most up to date periMICA firmware is available on `https://docs.perinet.io/`. Once you have downloaded the archive to your local PC or network, click ***Install*** to start the update process. Then select the appropriate archive and click ***Execute***. After displaying a confirmation dialogue, the periMICA 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 forced refresh of your browser window after the periMICA restarts, to reconnect to the device.

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

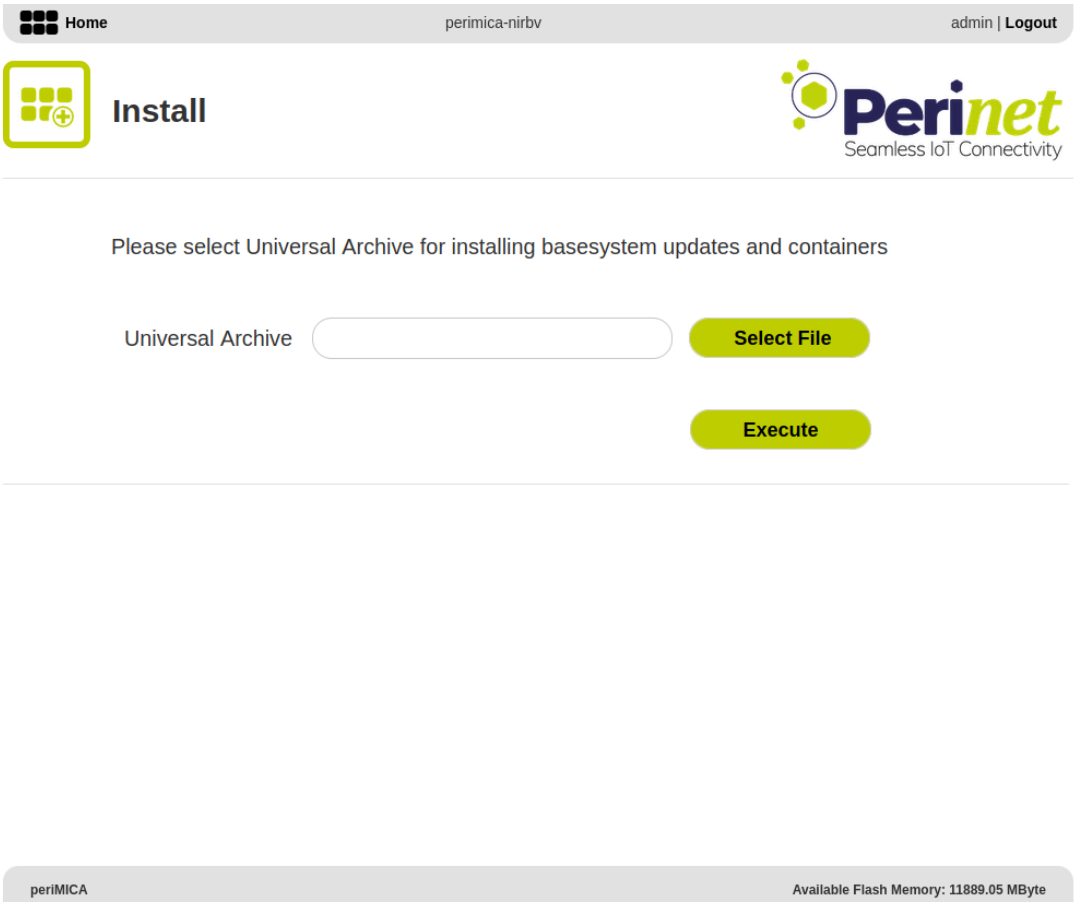


Figure 16: The periMICA Install Dialogue.

7.5 Remote API

The periMICA can be controlled via remote API using JSON-RPC. Go to ***Information → Documentation*** for detailed documentation.

7.6 Working with Containers

The periMICA web interface lists all installed containers and three general tools called ***Settings***, ***Install*** and ***Information***.

7.6.1 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.

Figure 17: Container Context Menu

7.6.2 Install Container

periMICA containers can be downloaded from `https://docs.perinet.io/`.

To install a container, click ***Install*** in the web GUI, select the desired container archive in the file dialog and click ***Execute***. The periMICA will show the installation process: **??**. After installation, the container needs to be started manually before it can be used.

7.6.3 Start Container

Before you can interact with a container, it must be started. To start a container, select ***Start*** from the context menu. You can open the context menu by right-clicking a container icon. Once the container is active, its icon changes from **gray** to **green**.

7.6.4 Open Container GUI

To open the graphical user interface of a started container, click on 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 error message will be shown.

You can also access a container directly by entering the URL `https://<containername>-<perimicaname>.local/` in your browser.

7.6.5 Stop Container

To stop a container, select ***Stop*** from its context menu. You can open the context menu by right-clicking a container icon. Once the container is stopped, the icon changes from **green** to **gray**.

7.6.6 Reset Container

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

Warning: *A container reset deletes the overlay and thereby deletes all user data and configurations. We strongly recommend creating a backup before resetting a container. To do this, either duplicate the container on the periMICA itself or merge the container and export it to your PC or a network drive.*

7.6.7 Duplicate Container

To duplicate a container, select ***Options → Duplicate*** from the context menu and enter a name for the duplicated container. ***Duplicate*** makes an identical copy of the base file system and the overlay of the original container and stores it on the periMICA. 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 to create 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 periMICA itself, for example before performing a container update.

7.6.8 Export Container

To export the container overlay and base, select ***Options → Export***. Then select a location to save the exported container to and name the file.

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

7.6.9 Merge Container

The overlay of a container can be merged into the base file system, by selecting ***Options*** → ***Merge*** from the context menu. Merging prevents the deletion of files during a container reset. During development, this function can be used to make container modifications persistent.

Merge and Export

To export a container, first select ***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 periMICA. ***Merge*** combines the base file system and the overlay of the original container into a new base 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.

7.6.10 Update Container

To apply a container update, select ***Options*** → ***Update*** from the context menu and select the desired container archive in the file dialog. The periMICA will show the upgrade process and ask for the container to update after uploading it.

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

8 Networking

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

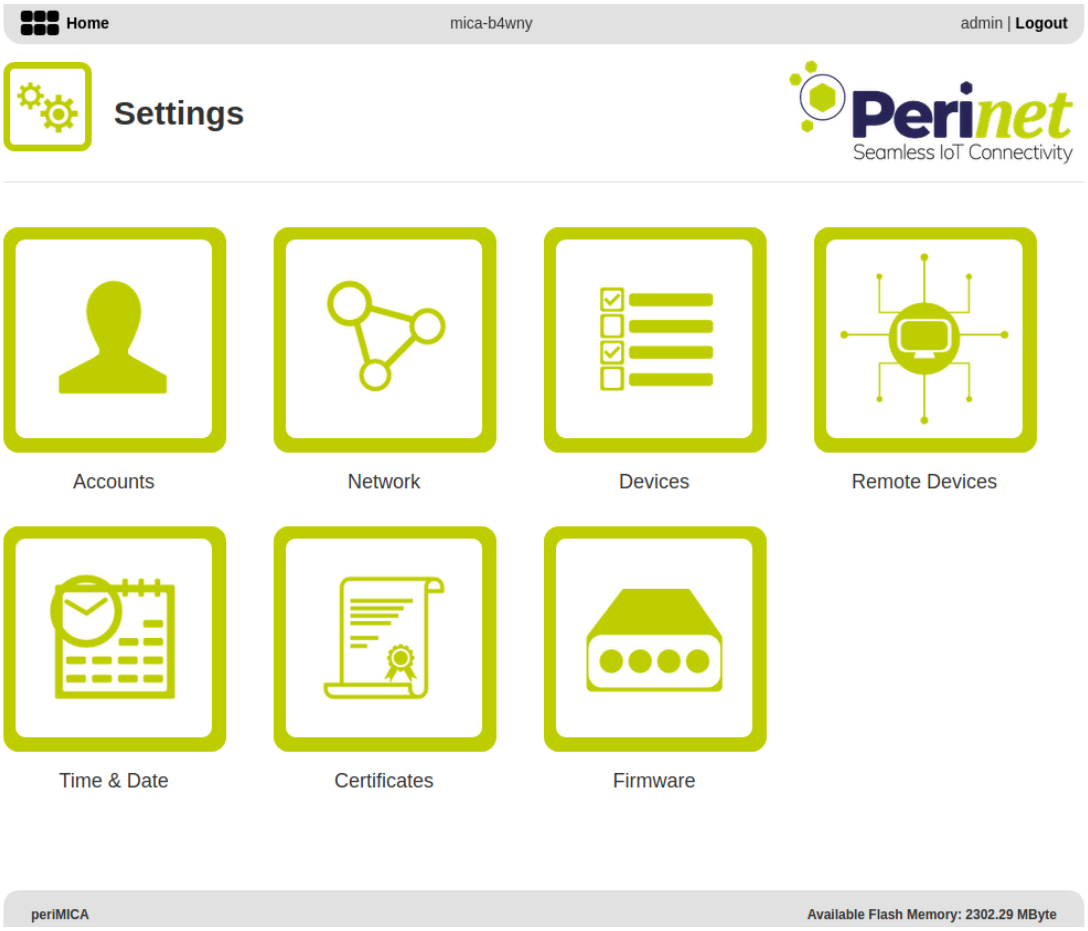


Figure 18: periMICA Settings

8.1 periMICA Basic Network Configuration

Network settings can be configured under ***Settings*** → ***Network***. In most cases, you only need to configure the primary network and do not have to worry about advanced settings.

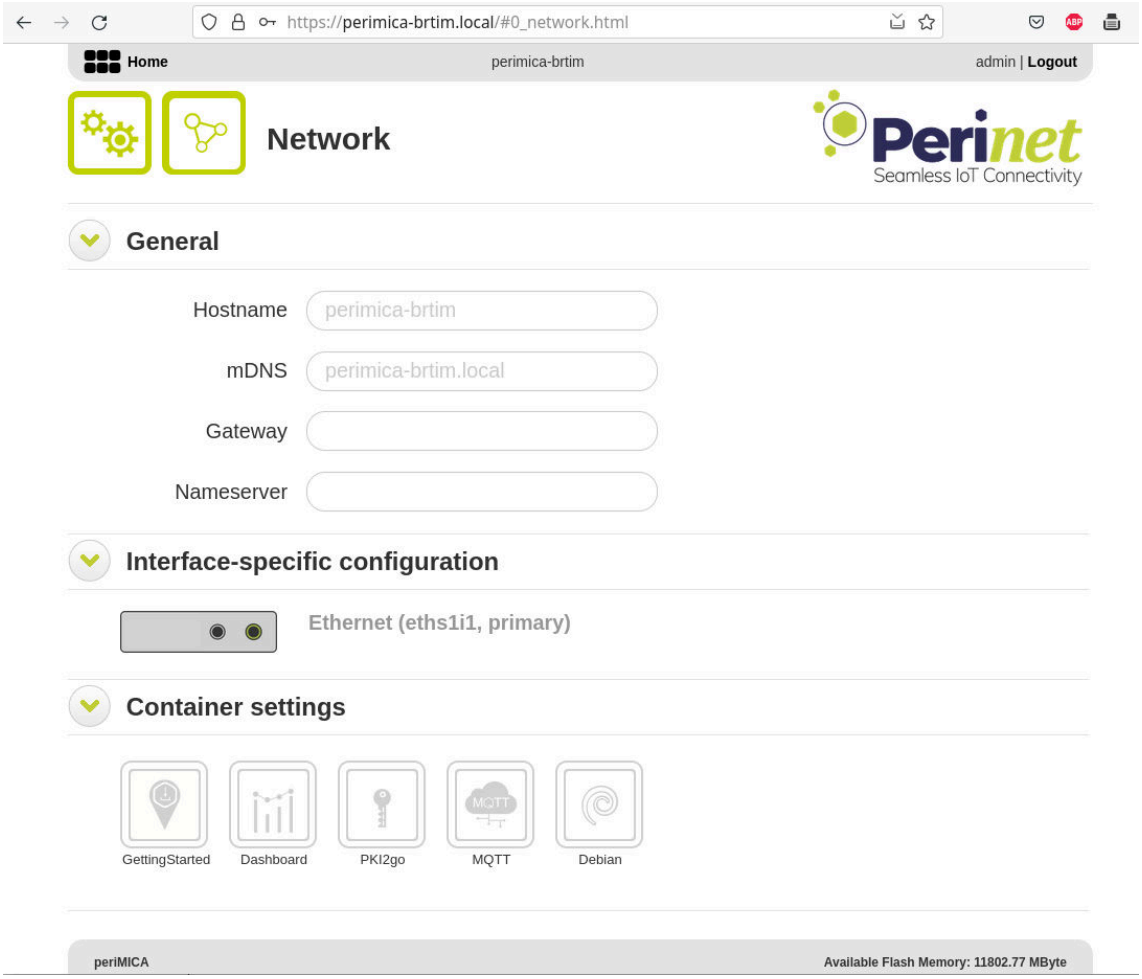


Figure 19: periMICA Network Settings

8.1.1 General Settings

The periMICA ***Hostname*** and ***mDNS*** are set in the factory and cannot be changed.

The currently used gateway and name servers are displayed in the ***Gateway*** and ***Nameserver*** fields. These settings can be changed in the ***Interface-specific Configuration*** section.

8.1.2 Interface-specific Configuration

In this section, you can configure all built-in network interfaces. The periMICA has just one primary interface according to the flat network model, however you can add more Ethernet interfaces, e.g. via Ethernet to USB dongles and let a container control this interface (e.g. for separating networks).

WiFi to USB dongles are not supported by the periMICA base system.

Note: *You cannot deactivate all network interfaces at the same time, since periMICA would no longer be accessible.*

To view and edit the settings of an interface, click the icon on the left or on the interface name (Figure 20):

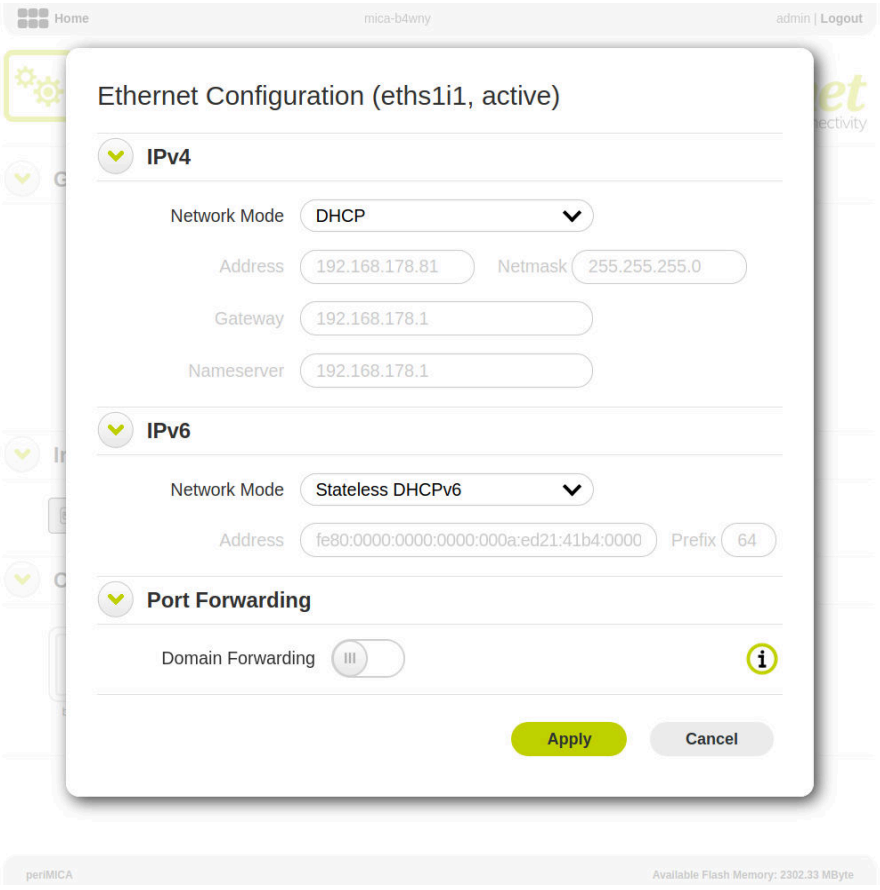


Figure 20: periMICA Network Interface Settings

8.1.3 IPv6 Configuration

By default, the periMICA base system has an IPv6 link-local address starting with *fe80*. This link-local address can be derived by combining the Perinet IPv6 prefix and the last 9 digits of the MAC address listed on the type shield of the periMICA. 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 configure IPv6, you can select from one of four settings:

- Select ***Auto-Configuration*** if you want the periMICA to obtain IPv6 addresses and gateway via Stateless address auto-configuration.
- Select ***Stateless DHCPv6*** if you want the periMICA to obtain IPv6 addresses, gateway and name server information automatically. (Default)
- Select ***Stateful DHCPv6*** if you want the periMICA to obtain IPv6 addresses via DHCPv6.
- Select ***Static*** to enter an IPv6 address, network mask and, if necessary, a gateway and a name server manually.

Click ***Apply*** to apply the new settings.

8.1.4 IPv4 Configuration

The periMICA base system IPv4 networking is set to DHCP by default, except for the fallback address, if no DHCP Server is available (see *Troubleshooting*).

To configure IPv4, you can select from one of four settings:

- Select ***Disabled*** to disable IPv4.
- Select ***DHCP*** if you want periMICA to obtain an IPv4 address, gateway and name server information automatically. (Default)
- Select ***Partial DHCP*** if you want the periMICA to obtain an IPv4 address automatically but want to set the gateway and name server manually.
- Select ***Static*** to enter an IP address, network mask and, if necessary, a gateway and a name server manually.

Click ***Apply*** to apply the new network settings.

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

8.1.5 Forwarding

In case IPv4-only clients need to access containers, the periMICA base system forwards the traffic to containers, through **domain forwarding**. With this mechanism, the periMICA base

system announces the periMICA container on IPv4 (mDNS) and forwards any request for

```
https://<periMICA-container>-<periMICA>.local/
```

to the corresponding container.

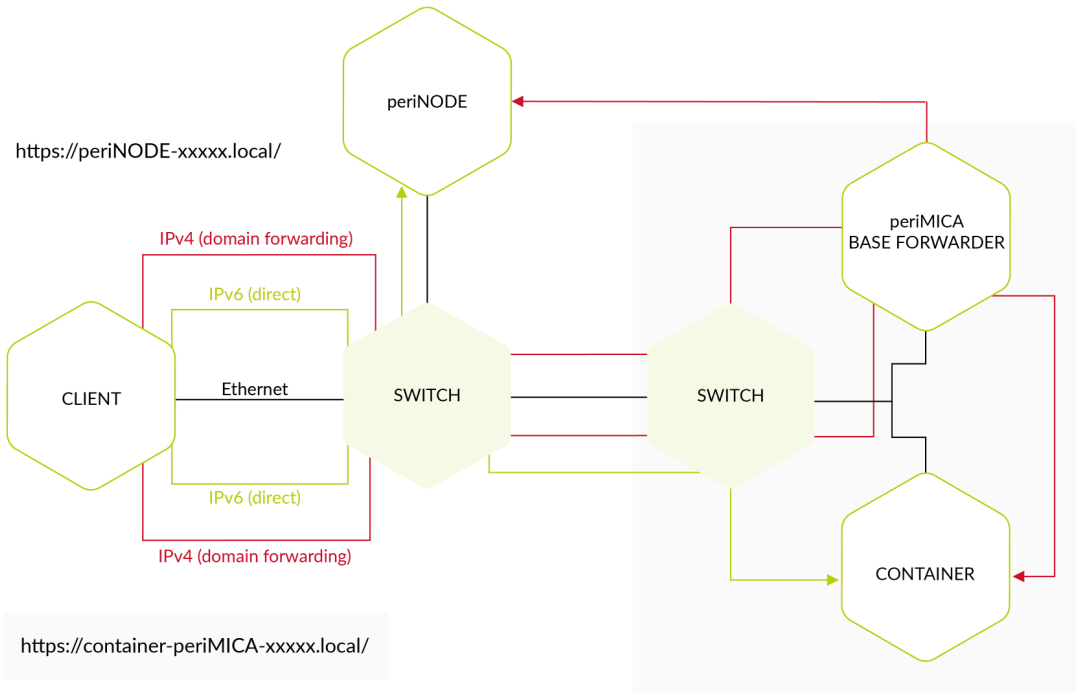


Figure 21: periMICA Domain Forwarding

In order to activate this feature, login to the periMICA Web UI and go to ***Settings → Network***. Under ***Interface-specific configuration***, click on your periMICA network interface and expand **Forwarding**. Now enable/disable the forwarding feature by clicking on the corresponding button and ***Apply*** (Figure 20).

Note: *Domain forwarding is only working for http(s) and websocket connections.*

8.2 Container Network Settings

8.2.1 IPv6

Using IPv6 in networks allows communication without configuration or usage of DHCP servers, because the IPv6 protocol automatically assigns by default a link-local address to each network participant. In the case of periMICA containers, the periMICA base system takes care of assigning these addresses to containers on startup of the containers.

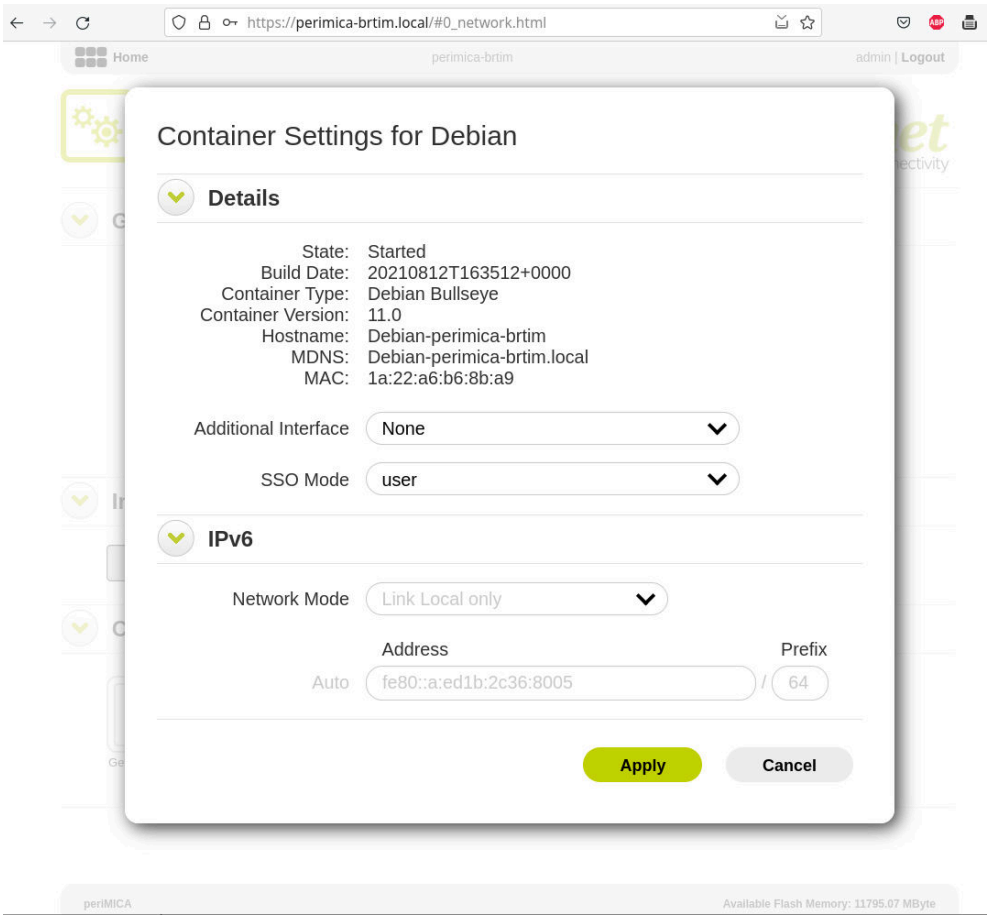


Figure 22: periMICA Container Network Settings

In case you have an IPv4-only client, you can nevertheless access containers, due to the forwarding of the network traffic performed by the periMICA base system. Please see chapters *Forwarding* and *Remote Devices* for more information.

8.2.2 Additional Interface

Adding network interfaces via USB to a periMICA can be done through a periMICA container. The idea is to first assign the corresponding network device to a container and after that to configure the specific device by logging-in via SSH to this container. In order to assign a network interface via Web UI, right-click on the periMICA container icon. Expand **Options**

and go to ***Settings***. Next, expand **Details** and select the desired interface under ***Additional Interface*** (Figure 22).

8.3 Remote Devices

Figure 23: periMICA Remote Devices

The ***Remote Devices*** feature extends the domain forwarding mechanism for network devices that need to be accessed in IPv4-only networks, without supporting IPv4 themselves. For example, periNODE devices are providing just an IPv6 link-local address. The periMICA base system can be used, just like it does implicitly for periMICA containers, to translate the IPv6-only device into IPv4 networks.

Therefore, please access the periMICA Web UI and go to ***Settings → Remote Devices***. Available network devices will be automatically discovered and shown in the ***Available*** list. Pushing the ***<Refresh*** button updates the list, by triggering a new network discovery. Forwarded devices can be enabled and disabled by pushing the >>> and <<< buttons, respectively. Once added, the remote device will also be shown on the periMICA home screen and can then be accessed by clicking on the device icon, automatically redirecting to:

`https://<remote-device>.local/`

Note: *As the Remote Devices feature is based on the same domain forwarding mechanism that is used for periMICA containers, only http(s) and websocket connections can be accessed.*

9 Generating a System Report

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

9.1 Logs and System Information

The periMICA log errors, as well as memory and CPU usage for up to ten days in two system level logs are available from the ***Information*** screen of the web GUI. These logs are kept during system restarts and will only be erased by firmware resets.

To download the Error Log, click the ***Error Log*** link. This will download a ***csv*** file containing the errors which were thrown by the Linux kernel and certain additional components. The errors are time stamped with the system time on the periMICA. Note that the time stamps can jump if the periMICA gets connected to and disconnected from networks.

To download a set of zipped ***csv*** files listing the CPU and memory usage of the periMICA, its base system and each container, click the ***Performance Log*** link on the ***Information*** page. Each ***csv*** file contains time stamped values for the memory used and the cumulative CPU time used by the component. To calculate momentary CPU use, you can subtract consecutive values. Both logs are being rolled over after approximately ten days.

Note: *If you are contacting technical support, please include the error log, performance log and the device summary with your email to support@perinet.io. This greatly speeds up the processing of your query.*

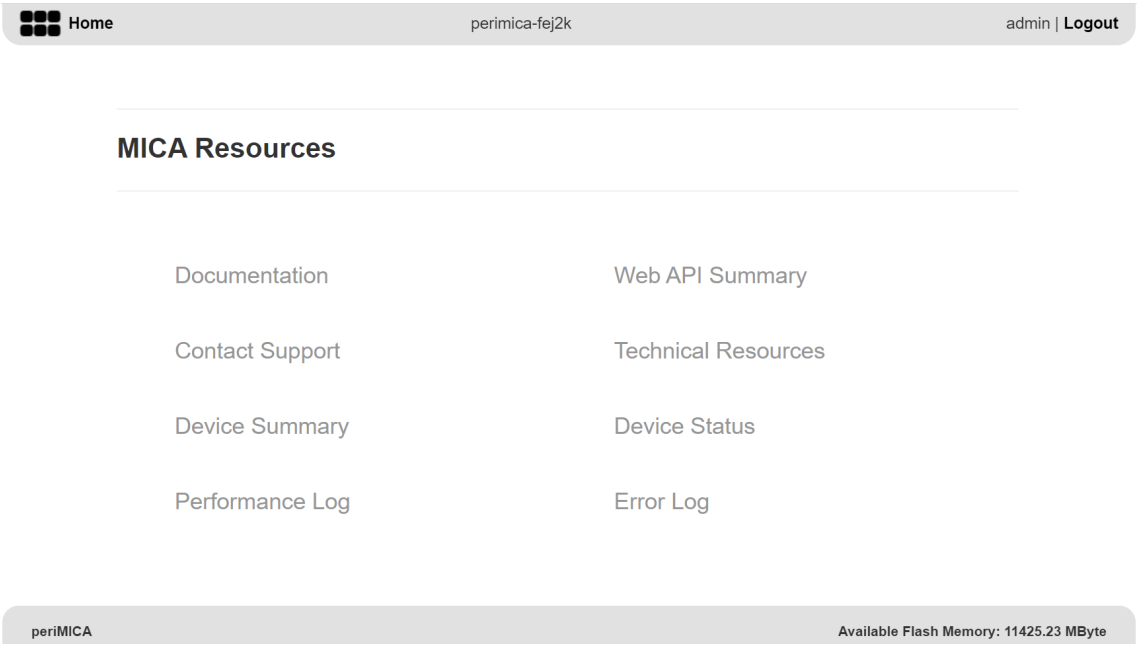


Figure 24: periMICA Information

10 Supported Browsers

Browser / OS	Edge	Chrome	Firefox	Safari
Windows 10 (19044.1645)	yes* (102.0.1245.44)	yes* (102.0.5005.115)	yes (101.0.1)	n/a
macOS (11.3.1)	yes, with forwarding (92.0.902.73)	yes, with forwarding (91.0.4472.114)	yes (89.0.2)	yes (14.1)
Ubuntu 21.10	yes, with forwarding (101.0.1210.53)	yes, with forwarding (101.0.4951.64)	yes (101.0.1)	n/a

Table 6: periMICA supported browsers

() Tested version in brackets

* ***Note:*** *There is a known issue when using Edge and Chrome browsers on Windows: the first time a container is accessed, a delay of about 15 seconds could occur before the container web UI is loaded.*

11 Troubleshooting

11.1 Solving Common Issues

Problem	Solution
periMICA doesn't start, Power LED is dark	- Check the power connection. - If possible, connect the periMICA to an alternative power source (e.g. 24V instead of PoE).
periMICA does not start, Power LED is red	- The periMICA cannot connect to the network. Check your network connection. Disconnect the periMICA from the power source for at least 30 seconds. Connect the periMICA directly to a PC and follow the instructions to connect using the fallback address 169.254.10.10. Your PC should use an IPv4 link-local address automatically (169.254.0.0-169.254.255.255). If not, please set an IP address manually, for example 169.254.10.1 and network mask 255.255.0.0.
periMICA does not show up in the network	- Check that the periMICA is connected to power. - Verify that the power LED and network LEDs are green or blinking yellow. - Check your network connection. - Restart the periMICA and wait until the network LEDs blink yellow. - Check if any network security settings prevent the periMICA from connecting to the network (for example MAC filters or required passwords). - Check that the periMICA is in the same local network segment as your computer (or VPN). - If you are using a VPN, disable the VPN, restart your computer and try to connect to the periMICA. - If your network supports IPv6, try connecting to the link local address. - Disconnect the periMICA from the power source for at least 30 seconds.

	- Connect the periMICA directly to a PC and follow the instructions to connect using the fallback address 169.254.10.10. Your PC should use an IPv4 link-local address automatically (169.254.0.0-169.254.255.255). If not, please set an IP address manually, for example 169.254.10.1 and network mask 255.255.0.0.
periMICA cannot be reached by name	Due to LLMNR caching in Windows, the periMICA 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. - In Chrome, the periMICA is reachable via *micaname.local*. - In IE and Chrome, the periMICA is reachable via its IP address. - Clearing the DNS cache with *ipconfig /flushdns* resolves this problem.
Lost password	For security reasons, the periMICA is designed in a way that Perinet cannot recover passwords. Contact your Perinet service provider or *support@perinet.io* for instructions on how to return your periMICA to Perinet for a factory reset. A factory reset will erase all user and application data.

Table 7: Troubleshooting

12 Labeling and Ordering Information

12.1 Product Marking

12.1.1 Device Label

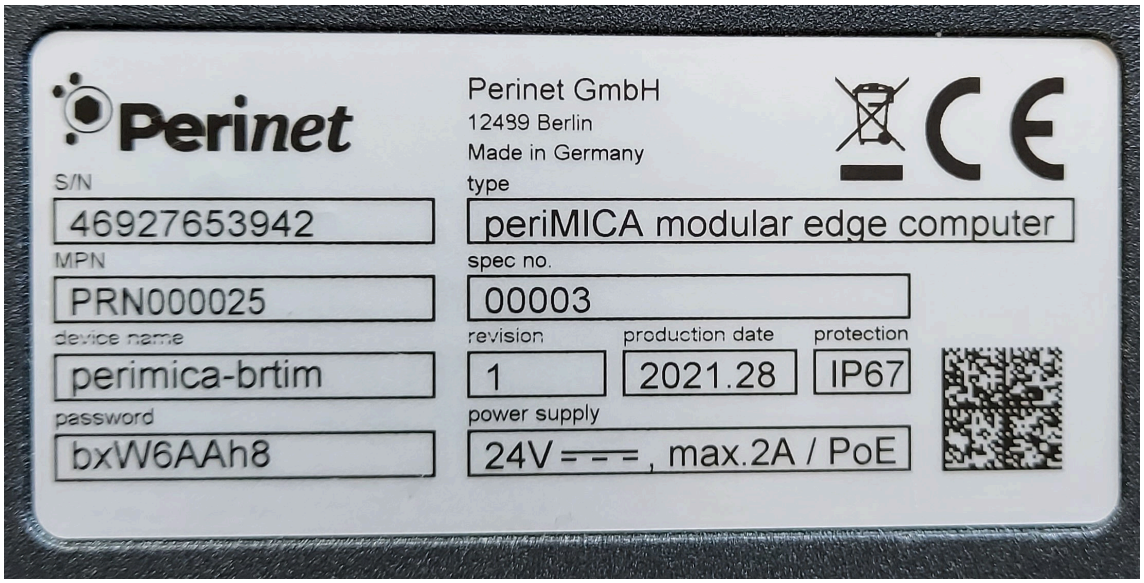


Figure 25: periMICA Device Label

The periMICA device label contains all the relevant information that a user needs. The most important are the periMICA **device name** and the random **password** for the login.

The data matrix present on the label encodes the same parameters, separated by a pipe "|".

12.1.2 Carton Label

Figure 26: periMICA Carton Label

The carton label shows the serial number and the specification number of the periMICA modular edge computer.

12.2 Ordering Information

The periMICA has a single manufacturer part number (PRN.000.025) that is used for all the periMICA variants and configurations.

To distinguish among the different variants, the periMICA has a **spec no.** on both labels. The specification number is a unique increment, that will be created for every new distinct variant that is ordered. If a customer orders a periMICA with a specification that has been already produced, then this existing number will be used. The specification number encodes the exact hardware, firmware and the containers (see ***periMICA Software Architecture***), i.e. a customer can specify the desired periMICA variant and what should be installed on the device. Later orders of the exact same device can be made using the same specification number.

Spec no.	Hardware modules	Software configuration
00001	S1 Module, P1 Module	Base Firmware: 21-02 Container:
00002	S1 Module, P1 Module, F2 Module	Base Firmware: 21-02 Container:
00003	S1 Module, P2 Module	Base Firmware: 21-02 Container: GettingStarted-21-01, Dashboard-21-01, PKI2go-21-01, MQTT-21-01, Debian-21-01
00004	S1 Module, P2 Module, F2 Module	Base Firmware: 21-02 Container:
00005	S1 Module, P2 Module	Base Firmware: 21-02 Container:

Table 8: periMICA ordering information

General commercial information:

Commercial data	
Packaging parts	1
Net weight	669 gram
Country of origin	Germany
European customs tariff number	84714100

Table 9: Commercial data

13 Contact & Support

For customer support, please call us at **+49 30 863 206 701** or send an e-mail to *support@perinet.io*.

For complete contact information visit us at `www.perinet.io`

14 Safety Instructions

This section contains information that you must observe for your personal safety and to avoid damage of property. The instructions for your personal safety are highlighted by a warning triangle, while information on damage of property alone is given without a warning triangle. Depending on the hazard level, the warnings are shown in decreasing order as follows.

⚠ DANGER	means that death or serious injury will occur if the appropriate precautions are not taken.
⚠ WARNING	means that death or serious injury may occur if the appropriate precautions are not taken.
⚠ CAUTION	with warning triangle, means that minor injury may occur if the appropriate precautions are not taken.
CAUTION	without warning triangle, means that property damage may occur if the appropriate precautions are not taken.
ATTENTION	means that an undesirable result or condition may occur if the corresponding precaution is not taken.
INFO	information on needed measures to guard against system failures.

Table 10: Safety instructions

If several hazard levels occur, the warning notice for the highest level is always used.
If the warning triangle is used in a warning against personal injury, then a warning against property damage can also be added to the same warning.

14.1 Power Supply

⚠ DANGER

Connection of the 24 V device only via safety extra-low voltage/protective extra-low voltage

The device is designed for operation with a directly connectable safety extra-low voltage (Safety Extra-Low Voltage, SELV) or Protective Extra-Low Voltage (PELV).

Failure to observe this warning may result in electric shock or damage to property.

Therefore, only safety extra-low voltages (SELV) according to IEC 60950-1 / EN 60950-1 / VDE 0805-1 or protective extra-low voltages (PELV) according to EN 50178 may be connected to the supply connections.

ATTENTION

Connecting the 24 V device to a safety extra-low voltage (SELV) turns it into a protective extra-low voltage (PELV). The connection point between ground and PE is established by the device according to the IEC 61851 standard.

14.2 Protection

CAUTION

Property damage

Property damage caused by electrostatic charging.

- Follow the measures necessary for the handling of components prone to electrostatic charging.

⚠ WARNING

Unwanted heat generation or fire due to insufficient fuse protection

The internal fuses of the device are designed for device protection only. The system installer or operator is responsible for the necessary line protection.

14.3 Repair

Repairs are not permitted. Defective devices must be disposed of in accordance with environmental requirements.

CAUTION

Dangers due to unauthorized opening of the device

Unauthorized opening of the device can cause considerable damage to property or danger to the user.

CAUTION

Voiding of the manufacturer's warranty due to unauthorized modifications to the device

Modifications to the equipment are not permitted. Failure to comply will invalidate the manufacturer's warranty expires.

Only put undamaged components in operation.

INFO

Perinet expressly notes that devices to which this document pertains are unsuitable for use as part of or in connection with medical implants or as important components of life support systems, where failure could lead to severe injuries to people. The components used and the proven level of reliability don't meet the necessary requirements for such applications. In order to avoid damage to devices and equipment as well as injuries to or death of people, the user or application developer must implement suitable, well thought out measures to guard against system failures.

The rights of third parties may be violated through use in the transport market of devices which are described in this document. Perinet can provide no warranty whatsoever that the rights of third parties aren't violated through use of the devices. If you are planning on this sort of use, please contact Perinet in order to clarify any potential questions regarding patent or property rights.

14.4 Qualification of the Personnel

The devices may only be mounted, installed, commissioned and maintained by persons who are familiar with the handling of such devices and who are qualified for the described activities.

This qualification includes:

- Training regarding the installation, connection, earthing, commissioning and maintenance of electrical devices (EN 50 110-1/-2 / VDE 0105 part 100).
- Training regarding the current standards of electrical engineering and safety technology.
- First aid training.

15 Use of Open Source Software

15.1 General

Our product also includes so-called open source software, which has been produced by third parties and published for the free use by everyone. The open source software is subject to special open source software licenses and the copyright of third parties. Every customer can use the open source software freely according to the license terms. The rights of the customer to use the open source software beyond the purpose of our product are defined in detail by the the respective open source software licenses concerned. The customer may use the open source software as provided for in the respective valid license, beyond the purpose for which the open source software is intended in our product. In the event that there is a conflict between our license terms for our product and the respective open-source software license, the relevant open source software license shall take precedence over our our license terms, insofar as the respective open source software is affected by this.

The use of the open source software used is free of charge. We do not charge any user fees or comparable fees for the use of the open source software included in our product. The use of the open-source software by the customer in our product is not a part of the profit we make on the contractual fee.

From the available list you can see all open source software programs that are included in our product. The most important open source software licenses are listed in the Licenses section at the end of this publication.

Where programs included in our product are licensed under the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), the Clarified Artistic License, or any other open source software license that requires that the source code must be made available, and if this software is not already included with our software has not already been supplied with our product on a data carrier in the source code, we will send the source code at any time upon request. Should the delivery on a data carrier is requested, the software will be sent against payment of a flat rate of 10.00 €. Our offer to send the source code on request ends automatically 3 years after delivery of our product to the customer. Inquiries are in this respect if possible by sending the serial number of our product to the following address:

Perinet GmbH
Rudower Chaussee 29
12489 Berlin
Germany
Phone: +49 30 86 32 06 701
E-Mail: support@perinet.io

15.2 Special Liability Regulations

We do not assume any warranty and liability if the open source software programs included in our product are used by the customer in a way that no longer corresponds to the purpose of the contract underlying the purchase of our product. This applies in particular to any use

of the open source software programs outside of our product. For the use of the open source software beyond the purpose of the contract, the warranty and liability provisions that are included in the applicable open source software license for the corresponding open source software, as listed below. In particular, we shall not be liable for software in our product or the entire software configuration in our product is changed. The underlying contract of the purchase of our product, only applies to the unmodified open source software and the unmodified software configuration in our product.

15.3 Open Source Software Used

Please contact our support department (*support@perinet.io*) for a list of the open source software used in this product.

A List of Figures

B List of Tables

C Glossary

D References

E Revision History

Revision	Date	Author(s)	Description
1	September 9, 2021	msen	Initial release
2	July 22, 2022	dber, shoe	Release of S3 power supply module, Add Factory Reset description (Section 7.3)

List of Figures

List of Tables