WISEGATE COMMISSIONING GUIDE

This commissioning guide provides all necessary information to install, configure, and operate the Sentinum Gateway in combination with the MIOTY-CLI.

It covers the complete process – from initial setup and software installation to Service Center integration and troubleshooting foundation for modern IoT networks.

Table of content

1. WARNING AND SAFETY INSTRUCTIONS

Warnings and important information about potential hazards or damageinstructions to ensure the safety of you, your surroundings and the gateway !

Important information required for smooth operation of the devices

Please note :

- Observe all safety instructions in this manual.
- Ensure the installation environment complies with the prescribed temperature and humidity limits.
- The gateway is designed for outdoor use up to 2 000 m above sea level.
- Maintain a minimum distance of 20 cm between the antennas and people.
- Do **not** power the gateway if any RF connector is open or unterminated.
- Maintain a minimum distance from other electronic devices.
- Ensure the power supply complies with SELV/PELV standards.
- Do not operate the device in potentially explosive or hazardous environments.

If the device is installed incorrectly:

- It may not function properly.
- It could be permanently damaged.
- It could pose a risk of injury.

2. SYSTEM REQUIREMENTS AND PREPARATION

This chapter outlines the items, tools, and conditions required to configure the WiseGate Gateway with MIOTY-CLI.

Ensure all components and software are available before proceeding with the setup.

2.1. PACKAGE CONTENTS

Before beginning the configuration, verify that the following items are included in your delivery:

- Sentinum Gateway
- Power supply unit
- M12 connection cable
- Mounting clip or bracket
- Product documentation (e.g., docs.sentinum.de)

Please note:
If any component is missing or damaged, contact Sentinum Support before proceeding with configuration

2.2. REQUIRED TOOLS AND RESOURCES

To complete the configuration, the following tools and access are required:

- MIOTY-CLI software: Downloadable from the Sentinum GitHub repository or manufacturer's page.
- Terminal software: Examples: PuTTY (Windows).
- Internet access: Required for gateway configuration, updates, and certificate downloads.
- Sentinum Service Center account: With valid MQTT BSSCI credentials for Service Center connection setup.

Please note:
Ensure your network firewall allows outbound communication from the gateway to the Service Center IP and port before starting configuration.

3. HARDWARE SETUP

Before starting the MIOTY-CLI configuration, ensure that:

- the Gateway is correctly installed, powered, and connected to the network.
- Hardware installation should already have been completed according to the Sentigate Quick Start Guide.

`This section serves only as a readiness check prior to configuration.`

3.1. MOUNTING VERIFICATION

`Please note:`

- Confirm that the gateway is securely mounted in a suitable location (e.g., wall, mast, or control cabinet).
- Ensure proper airflow and environmental protection according to the device specifications.
- The mounting clip or bracket must hold the gateway firmly in place to ensure stable and secure installation.

3.2. POWER SUPPLY CHECK

- Connect the **power adapter** to the gateway.
- Wait for the **LED indicators** to display operational status:
    - **Green blinking:** Device operational and ready.
    - **Red:** Error state – check power or connection before proceeding.

`Allow the device to complete its startup sequence before running MIOTY-CLI commands.`

3.3. NETWORK CONNECTION

- Connect an **Ethernet cable** between the gateway and the local network.
- Verify that the **network interface is active** and that the gateway receives an IP address.
    - The IP address can be assigned **automatically via DHCP** or configured **manually (static IP)** depending on your network policy.

`A stable and unrestricted network connection is required for MIOTY-CLI access and communication with the Sentinum Service Center.`

4. SOFTWARE INSTALLATION

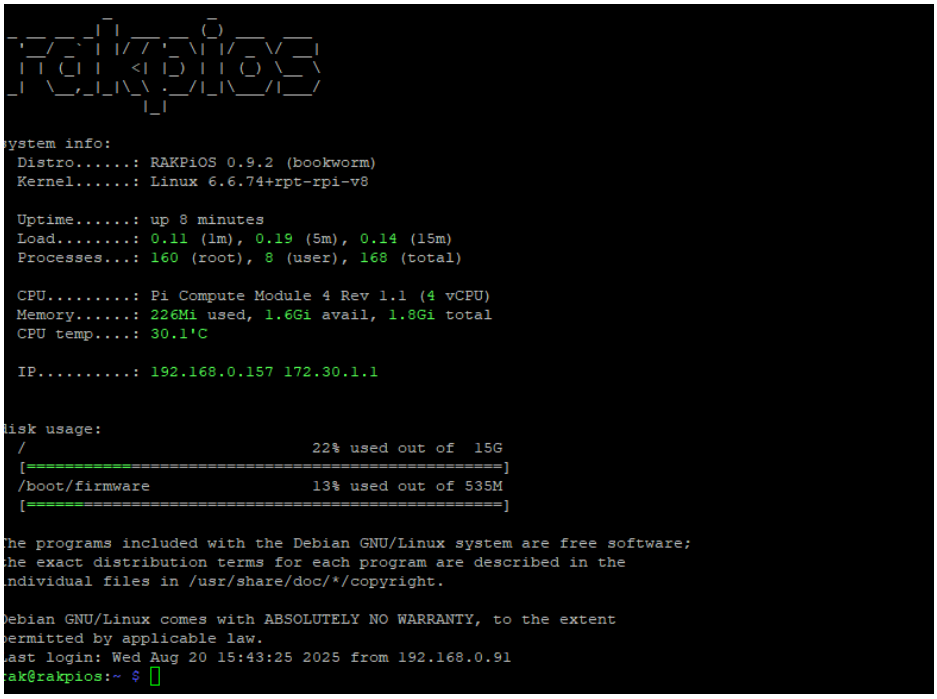
This section describes how to install and verify the MIOTY-CLI tool on the Gateway.

The MIOTY-CLI enables configuration and communication between the gateway's mioty® base station and the Sentinum Service Center.

4.1. INSTALLING THE MIOTY-CLI

Access the gateway via SSH

- Open a terminal connection to the gateway's IP address using port 22.
  Example:
  - On Windows: use PuTTY
- Connect with your assigned gateway login credentials.



Check whether MIOTY-CLI is already installed:

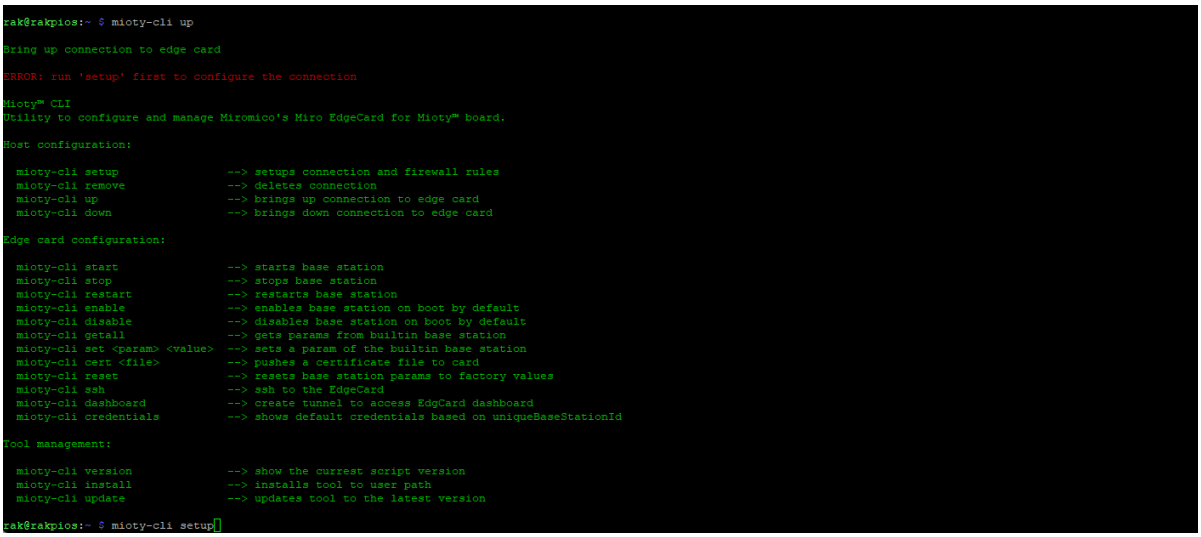
```
rak@rakpios:~$ mioty-cli version
```

- If a version number appears, MIOTY-CLI is already installed.
- If the command is not recognized, download and install the package:

```
git clone https://github.com/sentinum/mioty-cli.git
cd mioty-cli
./install.sh
```

After installation, verify that MIOTY-CLI is active:

```
rak@rakpios:~$ mioty-cli
```



The terminal displays the **MIOTY-CLI command list,** confirming successful installation.

MIOTY-CLI COMMAND OVERVIEW

Utility description:

The MIOTY-CLI is a utility used to configure and manage Miromico's Miro EdgeCard for the mioty® base station.

Host Configuration Commands

```
mioty-cli setup                 --> Sets up connection and firewall rules
mioty-cli remove                --> Deletes connection
mioty-cli up                    --> Brings up connection to EdgeCard
mioty-cli down                  --> Brings down connection to EdgeCard
```

Edge Card Configuration Commands

```
mioty-cli start                 --> Starts base station
mioty-cli stop                  --> Stops base station
mioty-cli restart               --> Restarts base station
mioty-cli enable                --> Enables base station on boot by
                                    default
mioty-cli disable               --> Disables base station on boot by
                                    default
mioty-cli getall                --> Retrieves all parameters from the
                                    base station
mioty-cli set <param> <value>   --> Sets a specific parameter of the base
                                    station
```

```
mioty-cli cert <file>          --> Uploads a certificate file to the
                                   base station
mioty-cli reset                --> Resets parameters to factory values
mioty-cli ssh                  --> SSH connection to the EdgeCard
mioty-cli dashboard            --> Creates tunnel to access the EdgeCard
                                   dashboard
mioty-cli credentials          --> Displays default credentials
```

Tool Management Commands

```
mioty-cli version              --> Displays the current script version
mioty-cli install              --> Installs the tool to user path
mioty-cli update               --> Updates the tool to the latest
                                   version
```

Please note:

- The gateway must have active internet access during installation.
- Do not disconnect power or network connections during installation.
- If the network restricts GitHub access, download the package manually and transfer it via SCP or USB.

4.2. GATEWAY CONFIGURATION

Once MIOTY-CLI is installed, continue with the device configuration.

Run the setup command to initialize the connection and firewall rules:

In the next step, perform the device setup:

```
rak@rakpios:~$ mioty-cli setup
```

Now the customer-specific parameters must be adjusted. This can be done using the command set <param> <value>:

```
rak@rakpios:~$ mioty-cli getall
```

to display the list of parameters.

```
rak@rakpios:~ $ mioty-cli getall

Base station parameters

uniqueBaseStationId : 3E-54-46-FF-FE-E9-7B-78
baseStationName     : mioty-bsm
baseStationVendor   : Miromico
baseStationModel    : EDGE-GWC-MY-868
serviceCenterAddr   : eu3.loriot.io
serviceCenterPort   : 727
tlsAuthRequired     : true
profile             : eu868

rak@rakpios:~ $
```

Adjust customer-specific parameters using the set command:

```
rak@rakpios:~$ mioty-cli set <param> <value>
```

```
Base station parameters

uniqueBaseStationId : 3E-54-46-FF-FE-E9-7B-78
baseStationName     : mioty-bsm
baseStationVendor   : Miromico
baseStationModel    : EDGE-GWC-MY-868
serviceCenterAddr   : 192.168.0.156
serviceCenterPort   : 16019
tlsAuthRequired     : true
profile             : eu868

rak@rakpios:~ $ mioty-cli set baseStationName RAK


rak@rakpios:~ $ mioty-cli getall

Base station parameters

uniqueBaseStationId : 3E-54-46-FF-FE-E9-7B-78
baseStationName     : RAK
baseStationVendor   : Miromico
baseStationModel    : EDGE-GWC-MY-868
serviceCenterAddr   : 192.168.0.156
serviceCenterPort   : 16019
tlsAuthRequired     : true
profile             : eu868
```

In this example, the parameter basestationName was changed to RAK using the command:

```
mioty-cli set basestationName RAK
```

Important: Do not change the Base Station ID – it is a unique IEEE identifier assigned globally and only once per device.

To access the dashboard user interface, you must run the following command:

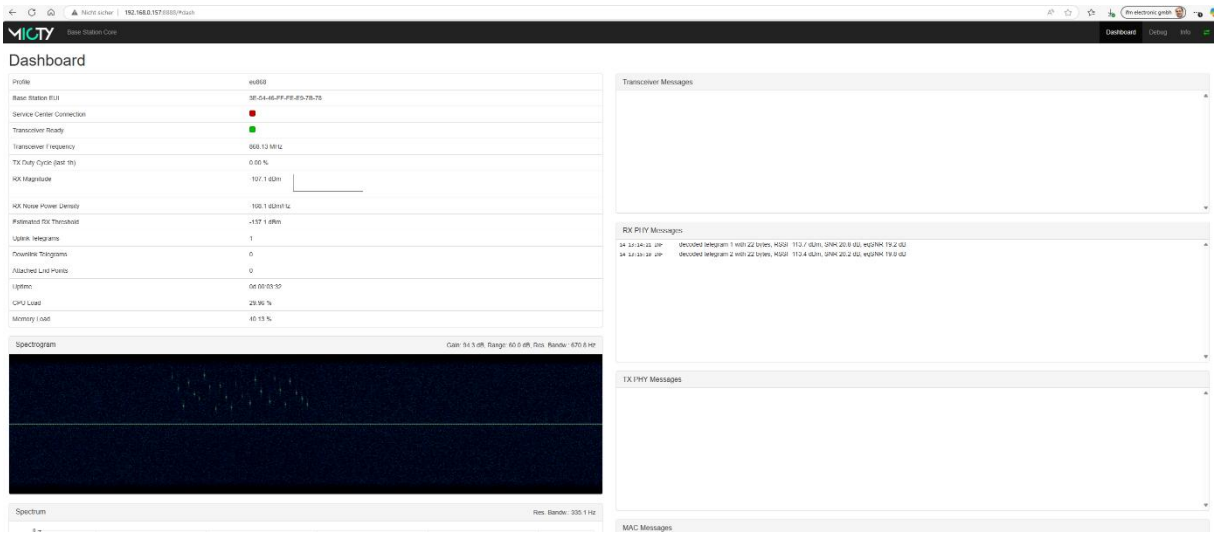
```
rak@rakpios:~$ mioty-cli dashboard
```

Only after this command has been executed can the base station be accessed in a browser via IP address: :8888

```
rak@rakpios:~ $ mioty-cli dashboard

Access dashboard on http://192.168.0.157:8888 once the tunnel is created

root@mioty-bsm:~#
```

```
Access dashboard on http://192.168.0.157:8888 once the tunnel is created

The authenticity of host '172.30.1.2 (172.30.1.2)' can't be established.
RSA key fingerprint is SHA256:IO1QKyJe3aHeoluuBxK1HZ1OHI+zA+W9jpG0MTZxV70.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.30.1.2' (RSA) to the list of known hosts.
root@mioty-bsm:~#
```

The dashboard appears as follows when opened for the first time:



Under Transceiver ready, a green field should be visible; under Service Center Connection, a red field will still be displayed. The EUI corresponds to the UID from the parameter set:

```
mioty-cli getall
```

5. SERVICE CENTER CONFIGURATION

For a Stable Service Center connection, the Service Center certificates must be stored on the base station.

For this purpose, the following Service Center certificates must be available (standard naming):

```
ca_cert.pem      service_center_cert.pem      service_center_key.pem
```

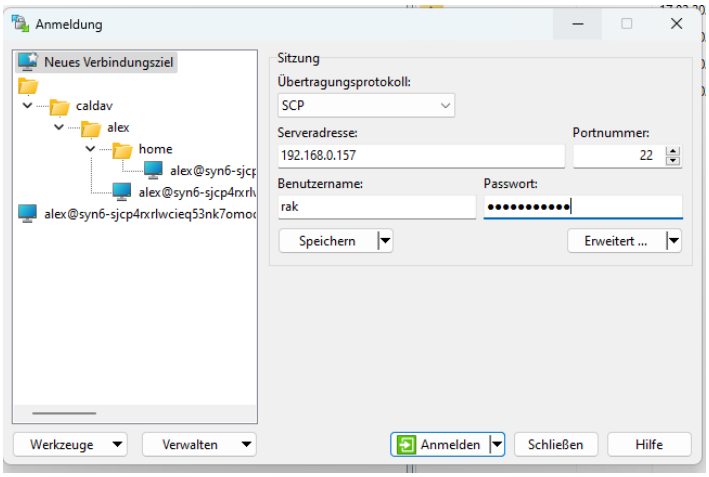
These files must be renamed and transferred to the base station via SSH.

The Gateway expects the following naming:

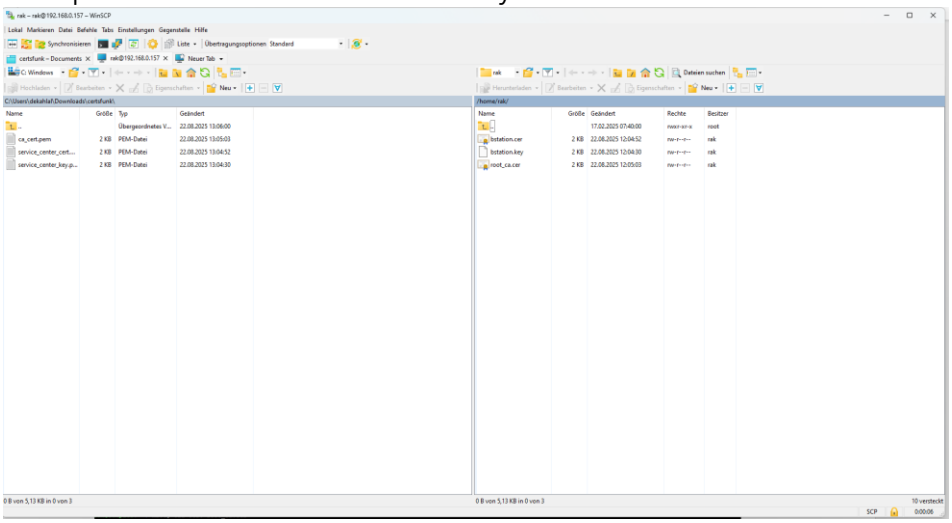
```
ca_cert.pem                  -->   root_ca.cer
service_center_cert.pem      -->  bstation.cer
service_center_key.pem       -->   bstation.key
```

The data can then be transferred to the base station, typically using **WinSCP.**

To do this, open a **'New Session Tab'** and connect to the device's IP address using the username and password for the Linux account.

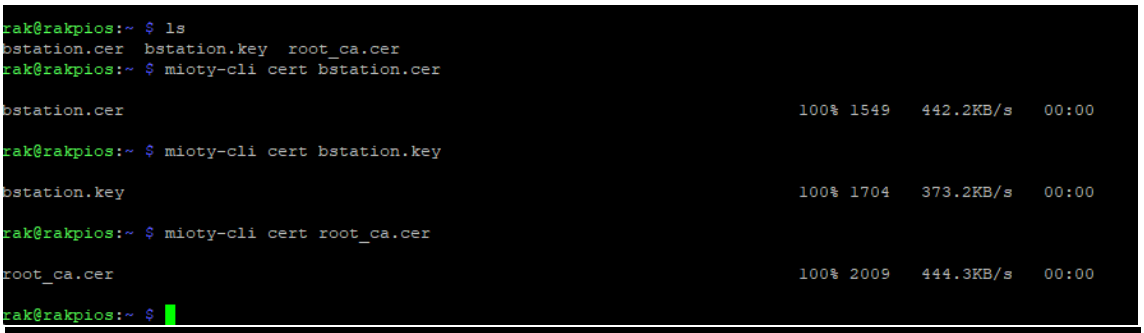


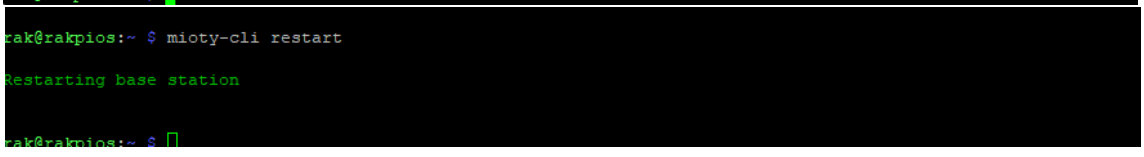
Once logged in successfully, the interface of the base station can be seen on the right; on the left you must navigate to the folder containing the certificates.
Here you still see the standard names of the certificates; on the right, on the base station, the uploaded certificates have already been renamed.



Then you can switch back to the terminal environment.
The certificates must be now actively loaded.This can be done with the command:

```
rak@rakpios:~$ mioty-cli cer <name Zertifikat>
```





Then restart the base station using: `mioty-cli restart`

Use `mioty-cli getall` to check whether the correct address and port of the Service Center installation are entered (for example 192.168.0.156:16019).

```
Base station parameters

uniqueBaseStationId : 3E-54-46-FF-FE-E9-7B-78
baseStationName     : mioty-bsm
baseStationVendor   : Miromico
baseStationModel    : EDGE-GWC-MY-868
serviceCenterAddr   : 192.168.0.156
serviceCenterPort   : 16019
tlsAuthRequired     : true
profile             : eu868

rak@rakpios:~ $ mioty-cli set baseStationName RAK


rak@rakpios:~ $ mioty-cli getall

Base station parameters

uniqueBaseStationId : 3E-54-46-FF-FE-E9-7B-78
baseStationName     : RAK
baseStationVendor   : Miromico
baseStationModel    : EDGE-GWC-MY-868
serviceCenterAddr   : 192.168.0.156
serviceCenterPort   : 16019
tlsAuthRequired     : true
profile             : eu868
```

If *loriot* is still stored there, the parameters must be adjusted with:

```
mioty-cli set <param> <value>
```

5.1. ACCESSING THE WEB INTERFACE

To reach the dashboard with UI, execute:

```
rak@rakpios:~$ mioty-cli dashboard
```

Only after executing this command can, the base station be reached in the browser via the IP address:8888

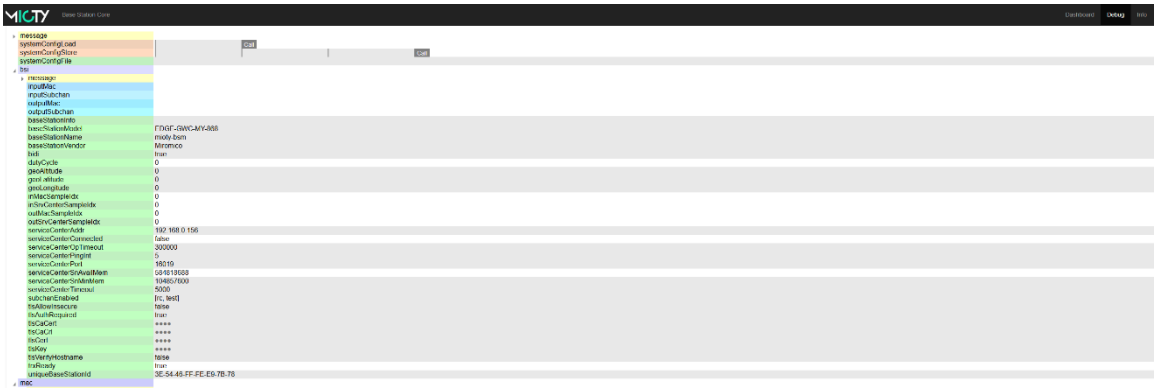
```
rak@rakpios:~ $ mioty-cli dashboard

Access dashboard on http://192.168.0.157:8888 once the tunnel is created

root@mioty-bsm:~#
```

```
Access dashboard on http://192.168.0.157:8888 once the tunnel is created

The authenticity of host '172.30.1.2 (172.30.1.2)' can't be established.
RSA key fingerprint is SHA256:IOlQKyJe3aHeoluuBxKlHZlOHI+zA+W9jpG0MTZxV70.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.30.1.2' (RSA) to the list of known hosts.
root@mioty-bsm:~#
```

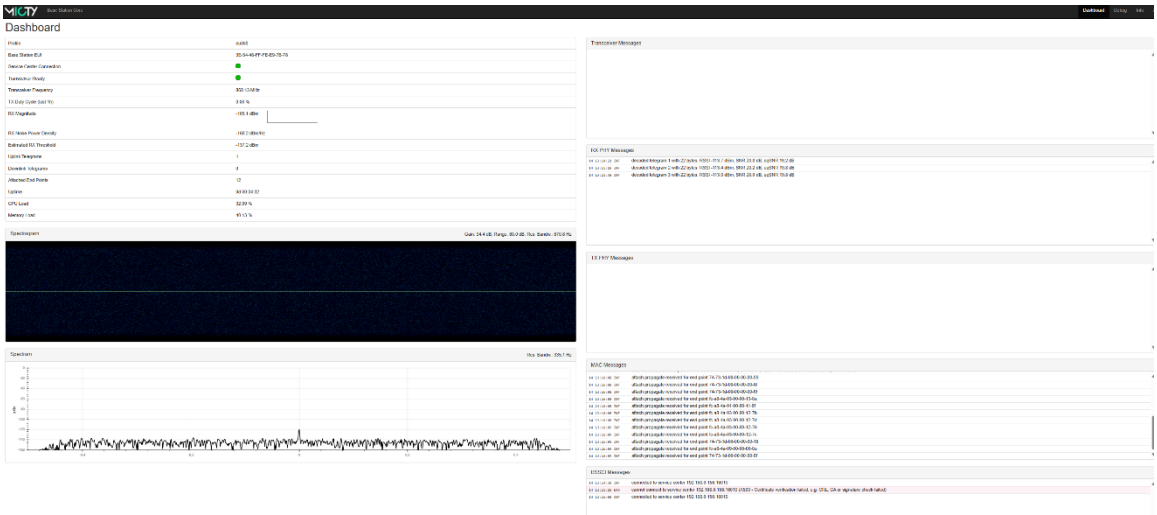
If all parameters have been entered correctly, the **Service Center Connection** field now appears green.
If the Service Center Connection field does not turn green, open the **Debug** tab in the upper-right corner and change the following parameter in the detailed settings:

```
tlsAuthRequired  from  false  ->  true
```

The dashboard should appears as follows when opened for the first time:

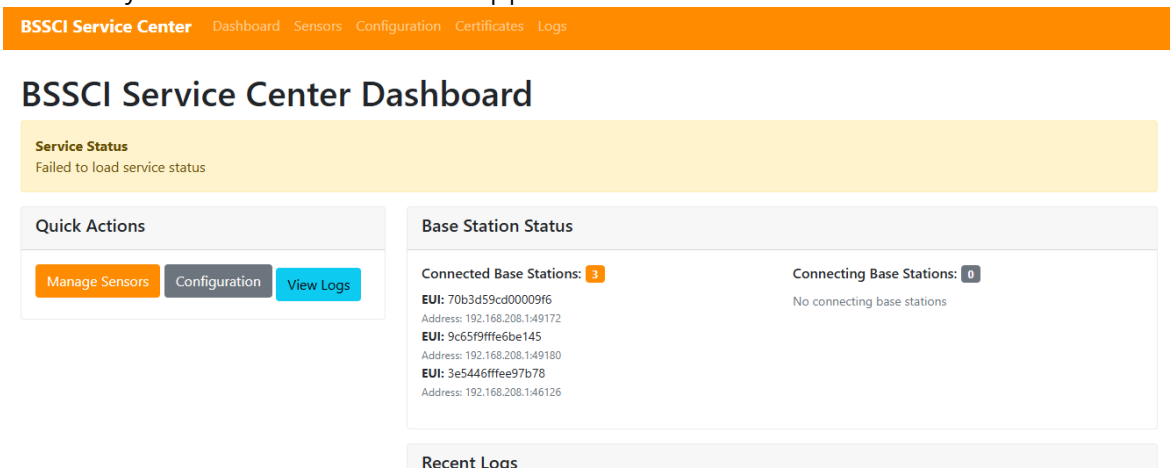


Afterwards, click on Dashboard, and the field is displayed in green.



5.2. CHECK BSSCI CONNECTION AT THE SERVICE CENTER

The newly added base station now appears in the Service Center.



With this, the onboarding process is successfully completed, and the base station is now actively connected to the Sentinum Service Center

6. TROUBLESHOOTING

This section provides guidance for identifying and resolving common issues during MIOTY-CLI operation and Service Center communication.

ISSUE	POSSIBLE CAUSE	RECOMMENDED ACTION
CONNECTION RESET BY PEER	TLS handshake or certificate error	Check TLS certificates for validity and correct installation. Restart the MIOTY service with `mioty-cli restart`.
END OF FILE	Interrupted data stream	Review `/var/log/mioty.log` for details. Verify stable network connection.
NO DATA TRANSMISSION	Network or Service Center misconfiguration	Test connectivity between gateway and Service Center. Confirm correct IP and port using `mioty-cli getall`.

Logs can also be viewed with the command journalctl -u mioty.

7. SECURITY AND MAINTENANCE

Routine security and maintenance actions are required to ensure long-term stability and data integrity of the Gateway.

Password Protection

- Change all default passwords immediately after installation.
- Define and assign user roles to control access permissions.

Firmware Updates

- Check the Sentinum portal regularly for firmware updates.
- Perform updates via the web interface or CLI following the Sentinum update instructions.

Back up and recovery

- Export the current configuration before making major changes or updates.
- Document the recovery process for quick restoration in case of system failure

8. APPENDIX

8.1. GLOSSARY

- **mioty –** Radio protocol for Low Power Wide Area Networks (LPWAN)
- **MQTT –** Lightweight messaging protocol commonly used in IoT systems

8.2. LINKS

- Sentinum Documentation: https://docs.sentinum.de/en/test-3
- MIOTY-CLI GitHub: https://github.com/sentinum/mioty-cli

8.3. SUPPORT

Technical Contact: Simon Schrampfer

Project Coordination: Manuel Hart