

WISEGATE MIOTY GATEWAY INBETRIEBNAHMEHANDBUCH



Dieses Inbetriebnahmehandbuch enthält alle erforderlichen Informationen zur Installation, Konfiguration und zum Betrieb des Sentinum Gateways in Kombination mit der MIOTY-CLI.

Es beschreibt den vollständigen Prozess – von der Ersteinrichtung und Softwareinstallation bis hin zur Integration in das Service Center sowie den grundlegenden Schritten zur Fehlerbehebung.

Damit bildet es die Grundlage für den zuverlässigen Betrieb moderner IoT-Netzwerke.

Table of content

1. WARN- UND SICHERHEITSHINWEISE.....	3
2. SYSTEMVORAUSSETZUNGEN UND VORBEREITUNG	4
2.1. LIEFERUMFANG	4
2.2. ERFORDERLICHE WERKZEUGE UND RESSOURCEN.....	4
3. Hardware Installation.....	5
3.1. Montageüberprüfung	5
3.2. STROMVERSORGUNGSPRÜFUNG	5
3.3. NETZWERKVERBINDUNG	5
4. SOFTWAREINSTALLATION.....	6
4.1. INSTALLATION DER MIOTY-CLI	6
4.2. GATEWAY KONFIGURATION	8
5. SERVICE-CENTER-KONFIGURATION	11
5.1. ZUGRIFF AUF DIE WEB-OBERFLÄCHE	13
5.2. ÜBERPRÜFUNG DER BSSCI-VERBINDUNG IM SERVICE CENTER.....	14
6. FEHLERBEHEBUNG	15
7. SICHERHEIT UND WARTUNG.....	16
8. Anhang.....	17
8.1. GLOSSAR.....	17
8.2. LINKS.....	17
8.3. SUPPORT	17

1. WARN- UND SICHERHEITSHINWEISE

Warnungen und wichtige Hinweise zu möglichen Gefahren oder Beschädigungen, um die Sicherheit von Personen, der Umgebung sowie des Gateways zu gewährleisten.

Zusätzlich werden wichtige Informationen für den störungsfreien Betrieb der Geräte bereitgestellt.

Bitte beachten:

- Beachten Sie sämtliche Sicherheitshinweise in diesem Handbuch.
- Stellen Sie sicher, dass die Installationsumgebung den vorgegebenen Temperatur- und Feuchtigkeitsgrenzen entspricht.
- Das Gateway ist für den Außeneinsatz bis zu einer Höhe von 2 000 m über dem Meeresspiegel ausgelegt.
- Halten Sie einen Mindestabstand von 20 cm zwischen den Antennen und Personen ein.
- Schalten Sie das Gateway nicht ein, wenn ein HF-Steckverbinder offen oder nicht terminiert ist.
- Halten Sie einen ausreichenden Abstand zu anderen elektronischen Geräten ein.
- Stellen Sie sicher, dass die Stromversorgung den SELV/PELV-Normen entspricht.
- Betreiben Sie das Gerät nicht in explosionsgefährdeten oder gefährlichen Umgebungen.

Bei unsachgemäßer Installation des Geräts:

- Kann die einwandfreie Funktion nicht gewährleistet werden.
- Kann das Gerät dauerhaft beschädigt werden.
- Besteht Verletzungsgefahr für Personen.

2. SYSTEMVORAUSSETZUNGEN UND VORBEREITUNG

Dieses Kapitel beschreibt die erforderlichen Komponenten, Werkzeuge und Voraussetzungen zur Konfiguration des WiseGate Gateways mit der MIOTY-CLI.

Stellen Sie sicher, dass alle Komponenten und die erforderliche Software verfügbar sind, bevor Sie mit der Einrichtung beginnen.

2.1. LIEFERUMFANG

Bevor Sie mit der Konfiguration beginnen, überprüfen Sie, ob die folgenden Komponenten im Lieferumfang enthalten sind:

- Sentinum Gateway
- Sentinum Gateway
- Netzteil
- M12-Anschlusskabel
- Montageclip oder Haltebügel
- Produkt dokumentation (e.g., docs.sentinum.de)

Bitte beachten:

Sollte eine Komponente fehlen oder beschädigt sein, wenden Sie sich vor Beginn der Konfiguration an den Sentinum-Support.

2.2. ERFORDERLICHE WERKZEUGE UND RESSOURCEN

Für die vollständige Konfiguration werden die folgenden Werkzeuge und Zugänge benötigt:

- MIOTY-CLI-Software: Herunterladbar aus dem Sentinum-GitHub-Repository oder von der Herstellerseite.
- Terminal software: Zum beispiel: PuTTY (Windows).
- Internetzugang: Erforderlich für die Gateway-Konfiguration, Updates und den Zertifikatsdownload.
- Sentinum Service Center-Konto: Mit gültigen MQTT-BSSCI-Zugangsdaten zur Einrichtung der Verbindung mit dem Service Center

Bitte beachten:

Sentinum Service Center-Konto: Mit gültigen MQTT-BSSCI-Zugangsdaten zur Einrichtung der Verbindung mit dem Service Center

3. HARDWARE INSTALLATION

Bevor Sie mit der MIOTY-CLI-Konfiguration beginnen, stellen Sie sicher, dass:

- Das Gateway ist ordnungsgemäß installiert, mit Strom versorgt und mit dem Netzwerk verbunden.
- Die Hardwareinstallation wurde bereits gemäß der Sentigate-Quick-Start-Anleitung durchgeführt.

Dieser Abschnitt dient ausschließlich als Überprüfung der Einsatzbereitschaft vor der eigentlichen Konfiguration.

3.1. MONTAGEÜBERPRÜFUNG

Bitte beachten:

- Stellen Sie sicher, dass das Gateway sicher und fest an einem geeigneten Ort montiert ist (z. B. Wand, Mast oder Schaltschrank).
- Achten Sie auf eine ausreichende Luftzirkulation und den Umgebungsschutz gemäß den Gerätespezifikationen.
- Die Montagehalterung oder der Befestigungsbügel muss das Gateway stabil und vibrationsfrei fixieren..

3.2. STROMVERSORGUNGSPRÜFUNG

- Schließen Sie das Netzteil an das Gateway an.
- Warten Sie, bis die LED-Anzeigen den Betriebsstatus anzeigen:
 - **Grün blinkend:** Gerät ist betriebsbereit.
 - **Rot:** Fehlerzustand – überprüfen Sie die Stromversorgung oder die Netzwerkverbindung, bevor Sie fortfahren.

Lassen Sie das Gerät den Startvorgang vollständig abschließen, bevor Sie MIOTY-CLI-Befehle ausführen.

3.3. NETZWERKVERBINDUNG

- Schließen Sie ein **Ethernet-Kabel** zwischen dem **Gateway** und dem **lokalen Netzwerk** an.
- Überprüfen Sie, ob die **Netzwerkschnittstelle aktiv** ist und das Gateway **eine IP-Adresse** erhalten hat.
 - Die IP-Adresse kann je nach Netzwerkrichtlinie automatisch über DHCP zugewiesen oder manuell (statisch) konfiguriert werden.

Eine stabile und uneingeschränkte Netzwerkverbindung ist erforderlich, um auf die MIOTY-CLI zuzugreifen und die Kommunikation mit dem Sentinum Service Center sicherzustellen.

4. SOFTWAREINSTALLATION

In diesem Abschnitt wird beschrieben, wie das MIOTY-CLI-Tool auf dem Gateway installiert und überprüft wird.

Die MIOTY-CLI ermöglicht die Konfiguration und Kommunikation zwischen der mioty®-Basisstation des Gateways und dem Sentinum Service Center.

4.1. INSTALLATION DER MIOTY-CLI

Stellen Sie über SSH eine Verbindung zum Gateway her:

- Öffnen Sie eine Terminalverbindung zur IP-Adresse des Gateways über Port 22.
Beispiel:
 - Unter Windows verwenden Sie PuTTY.
- Melden Sie sich mit den zugewiesenen Zugangsdaten des Gateways an.

```

      .
     .
    .
   .
  .
 .
.

system info:
Distro.....: RAKPiOS 0.9.2 (bookworm)
Kernel.....: Linux 6.6.74+rpt-rpi-v8

Uptime.....: up 8 minutes
Load.....: 0.11 (1m), 0.19 (5m), 0.14 (15m)
Processes...: 160 (root), 8 (user), 168 (total)

CPU.....: Pi Compute Module 4 Rev 1.1 (4 vCPU)
Memory.....: 226Mi used, 1.6Gi avail, 1.8Gi total
CPU temp....: 30.1°C

IP.....: 192.168.0.157 172.30.1.1

disk usage:
/
[=====] 22% used out of 15G
/boot/firmware
[=====] 13% used out of 535M

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
last login: Wed Aug 20 15:43:25 2025 from 192.168.0.91
rak@rakpios:~$
```

Überprüfen Sie, ob die MIOTY-CLI bereits installiert ist:

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

- Wenn eine Versionsnummer angezeigt wird, ist die MIOTY-CLI bereits installiert.
- Wird der Befehl nicht erkannt, laden Sie das Installationspaket herunter und installieren Sie es:

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

Nach der Installation überprüfen Sie, ob die MIOTY-CLI aktiv ist:

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

```
rak@rakpios:~$ mioty-cli up
Bring up connection to edge card
ERROR: run 'setup' first to configure the connection

Mioty™ CLI
Utility to configure and manage Miromico's Miro EdgeCard for Mioty™ board.

Host configuration:

  mioty-cli setup      --> setups connection and firewall rules
  mioty-cli remove     --> deletes connection
  mioty-cli up         --> brings up connection to edge card
  mioty-cli down       --> brings down connection to edge card

Edge card configuration:

  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     --> gets params from builtin base station
  mioty-cli set <param> <value> --> sets a param of the builtin base station
  mioty-cli cert <file> --> pushes a certificate file to card
  mioty-cli reset      --> resets base station params to factory values
  mioty-cli ssh        --> ssh to the EdgeCard
  mioty-cli dashboard  --> create tunnel to access EdgeCard dashboard
  mioty-cli credentials --> shows default credentials based on uniqueBaseStationId

Tool management:

  mioty-cli version    --> show the current script version
  mioty-cli install    --> installs tool to user path
  mioty-cli update     --> updates tool to the latest version

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

Das Terminal zeigt die Befehlsübersicht der **MIOTY-CLI** an – dies bestätigt die erfolgreiche Installation.

Übersicht der MIOTY-CLI-Befehle

Funktionsbeschreibung

Die MIOTY-CLI ist ein Dienstprogramm zur Konfiguration und Verwaltung der Miro EdgeCard von Miromico für die mioty®-Basisstation.

Host-Konfigurationsbefehle

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 Konfigurationsbefehle

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
```

Werkzeugverwaltungsbefehle

```
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
```

Bitte beachten:

- Das Gateway muss während der Installation über eine aktive Internetverbindung verfügen.
- Trennen Sie während der Installation weder die Stromversorgung noch die Netzwerkverbindung.
- Falls der Netzwerkzugriff auf GitHub eingeschränkt ist, laden Sie das Installationspaket manuell herunter und übertragen Sie es per SCP oder USB auf das Gateway.

4.2. GATEWAY KONFIGURATION

Nachdem die MIOTY-CLI installiert wurde, fahren Sie mit der Gerätekonfiguration fort.

Führen Sie den Setup-Befehl aus, um die Verbindung sowie die Firewall-Regeln zu initialisieren.

Im nächsten Schritt erfolgt die Einrichtung des Geräts:

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

```
rak@rakpios:~$ mioty-cli setup
Setting up connection and firewall rules
Miromico GWC-62-MY-868 card detected using eth2
Connection 'mioty' (5606e369-8e9f-4f76-aebf-9a29aef0e68b) successfully added.
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/38)
rak@rakpios:~$
```

Nun müssen die kundenspezifischen Parameter angepasst werden.

Dies erfolgt mit dem Befehl `set <param> <value>`:

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

Um die Parameter anzuzeigen.

```
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:~$
```

Passen Sie kundenspezifische Parameter mit dem Befehl set an:

```
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 diesem Beispiel wurde der Parameter basestationName mit dem folgenden Befehl auf RAK geändert:

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

Wichtig: Ändern Sie die Base Station ID nicht – sie ist eine eindeutige, weltweit vergebene IEEE-Kennung, die jedem Gerät nur einmalig zugewiesen wird.

Um auf die Dashboard-Benutzeroberfläche zuzugreifen, führen Sie den folgenden Befehl aus:

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

Erst nach Ausführung dieses Befehls kann auf die Basisstation im Browser über die IP-Adresse :8888 zugegriffen werden.

```

rak@rakpios:~$ mioty-cli dashboard

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

root@mioty-bsm:~#

```

```

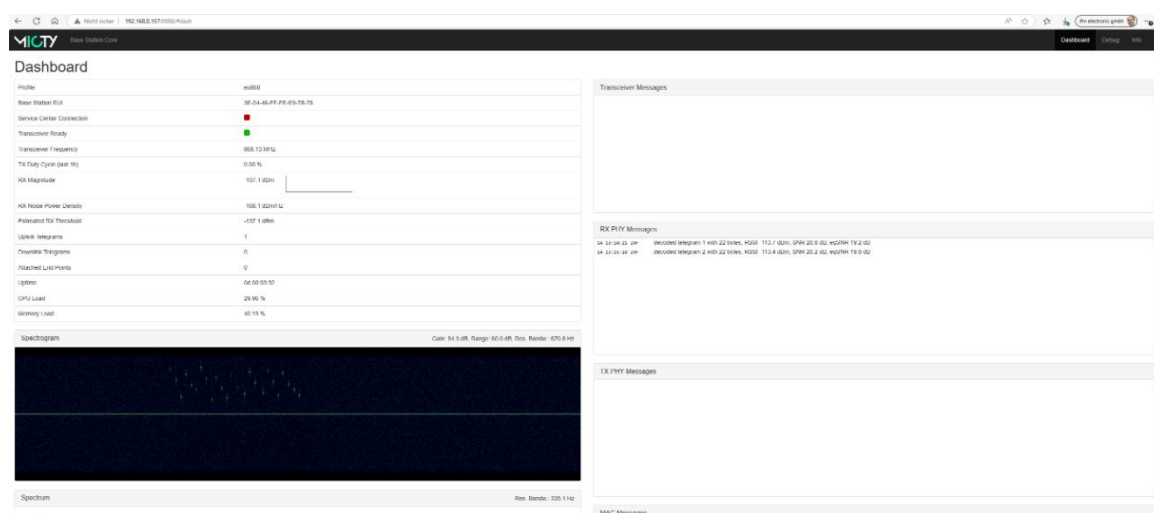
rak@rakpios:~$ mioty-cli dashboard

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+W9jpG0MT2xV70.
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:~#

```

Das Dashboard erscheint beim ersten Öffnen wie folgt:



Unter „Transceiver ready“ sollte ein grünes Feld sichtbar sein; unter „Service Center Connection“ wird zunächst noch ein rotes Feld angezeigt. Die EUI entspricht der UID aus dem Parametersatz.

```
mioty-cli getall
```

5. SERVICE-CENTER-KONFIGURATION

Für eine stabile Verbindung zum Service Center müssen die entsprechenden Service-Center-Zertifikate auf der Basisstation hinterlegt werden.

Dazu müssen die folgenden Zertifikatsdateien (mit Standardbenennung) verfügbar sein:

ca_cert.pem	service_center_cert.pem	service_center_key.pem
-------------	-------------------------	------------------------

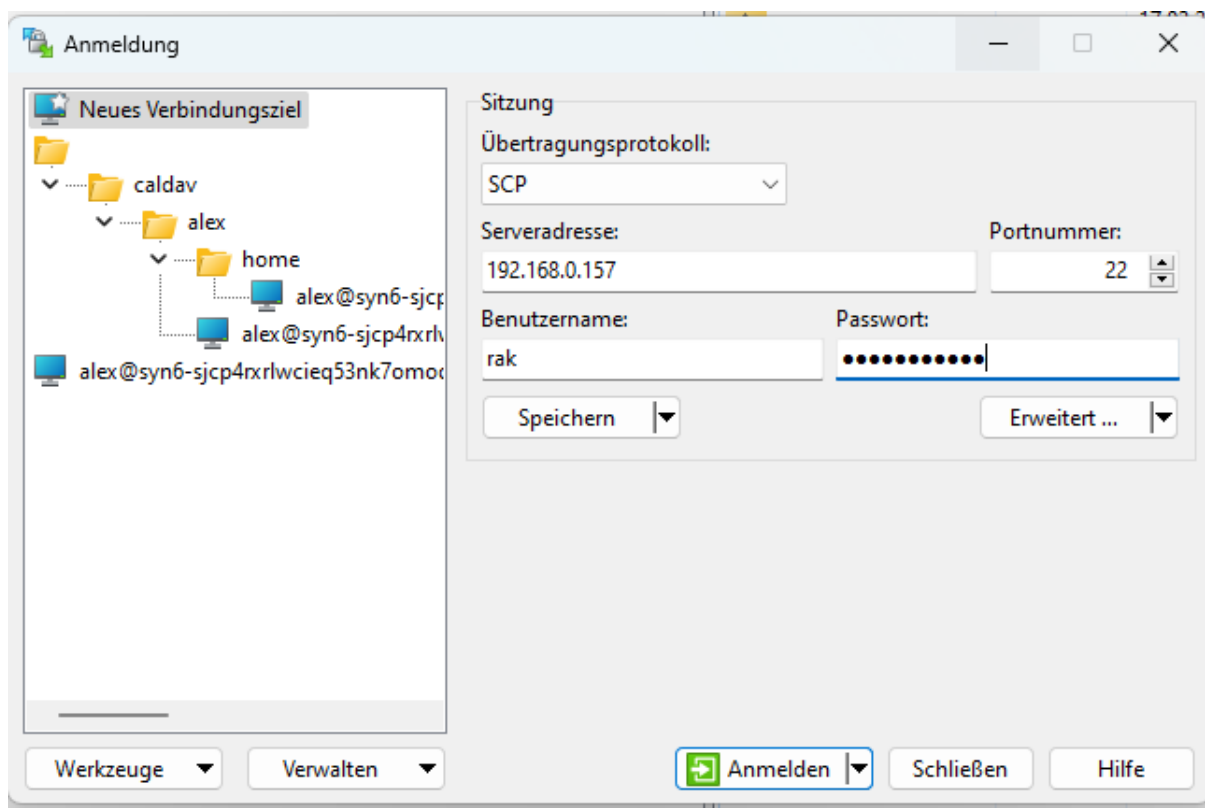
Diese Dateien müssen umbenannt und anschließend per SSH auf die Basisstation übertragen werden.

Das Gateway erwartet dabei die folgende Dateibenennung:

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

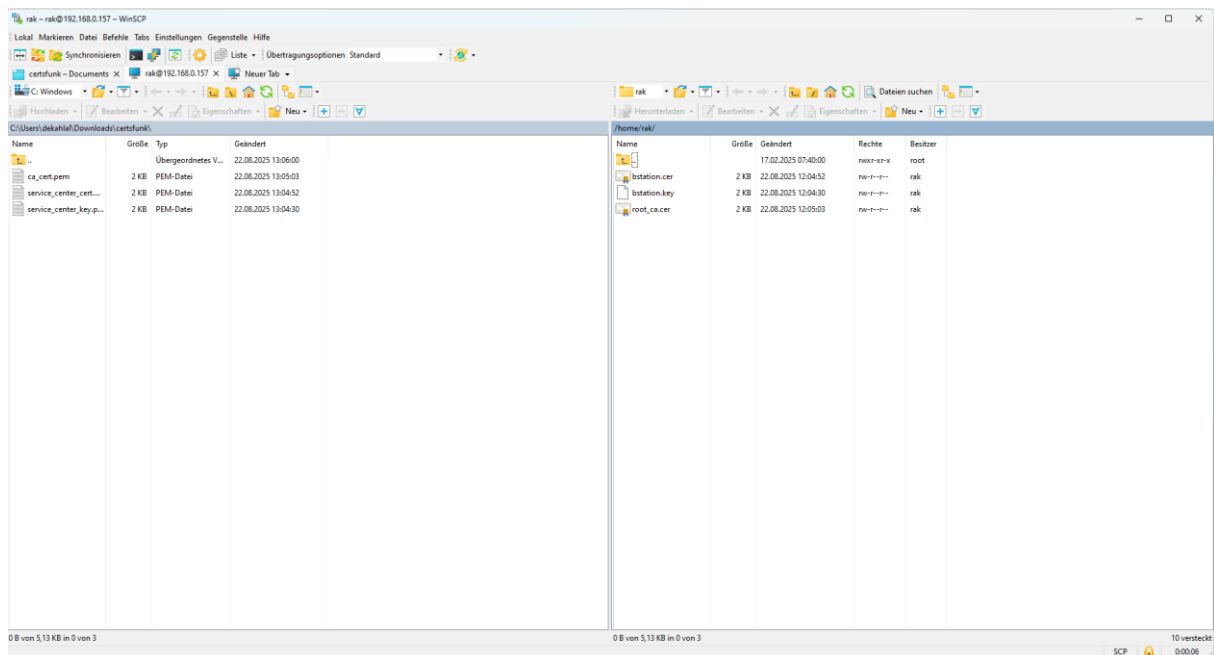
Die Daten können anschließend – typischerweise mit **WinSCP** – auf die Basisstation übertragen werden.

Öffnen Sie dazu einen „New Session“-Tab und verbinden Sie sich mit der IP-Adresse des Geräts unter Verwendung des Benutzernamens und Passworts des Linux-Kontos



Nach erfolgreicher Anmeldung wird auf der rechten Seite die Verzeichnisstruktur der Basisstation angezeigt; auf der linken Seite müssen Sie zu dem Ordner mit den Zertifikaten navigieren.

Links sind noch die Standardnamen der Zertifikate zu sehen, während auf der rechten Seite (auf der Basisstation) die hochgeladenen Zertifikate bereits umbenannt wurden.



Anschließend können Sie zur Terminalumgebung zurückkehren.

Die Zertifikate müssen nun aktiv geladen werden. Dies erfolgt mit dem folgenden Befehl::

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

```
rak@rakpios:~$ ls
bstation.cer  bstation.key  root_ca.cer
rak@rakpios:~$ mioty-cli cert bstation.cer

bstation.cer                                     100% 1549    442.2KB/s   00:00
rak@rakpios:~$ mioty-cli cert bstation.key

bstation.key                                     100% 1704    373.2KB/s   00:00
rak@rakpios:~$ mioty-cli cert root_ca.cer

root_ca.cer                                     100% 2009    444.3KB/s   00:00
rak@rakpios:~$ █

rak@rakpios:~$ mioty-cli restart

Restarting base station
rak@rakpios:~$ █
```

Starten Sie anschließend die Basisstation neu mit dem folgenden Befehl:

```
mioty-cli restart
```

Verwenden Sie `mioty-cli getall` , um zu überprüfen, ob die korrekte Adresse und der richtige Port der Service-Center-Installation eingetragen sind (z. B. 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
```

Wenn dort noch „loriot“ eingetragen ist, müssen die Parameter mit folgendem Befehl angepasst werden:

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

5.1. ZUGRIFF AUF DIE WEB-OBERFLÄCHE

Um das Dashboard mit Benutzeroberfläche aufzurufen, führen Sie den folgenden Befehl aus:

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

Erst nach Ausführung dieses Befehls kann die Basisstation im Browser über die IP-Adresse :8888 aufgerufen werden.

```
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:IOlQKyJe3aHeoluuBxKlHZ10HI+zA+W9jpGOMTZxV70.
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:~#
```

Wenn alle Parameter korrekt eingegeben wurden, erscheint das Feld „Service Center Connection“ nun grün.

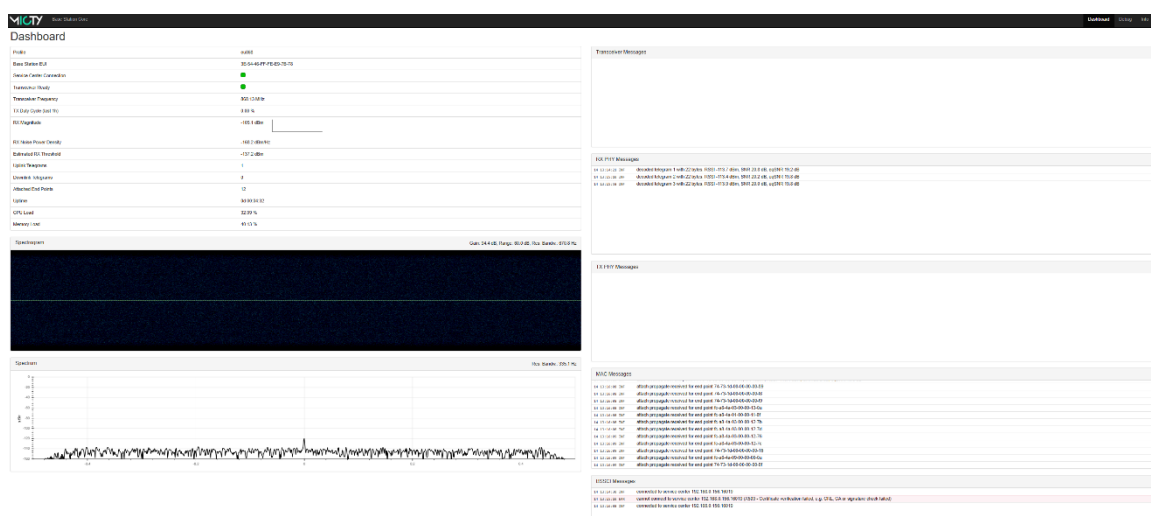
Falls das Feld nicht grün wird, öffnen Sie den **Debug**-Tab in der oberen rechten Ecke und ändern Sie in den Detail-einstellungen den folgenden Parameter:

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

Das Dashboard sollte beim ersten Öffnen wie folgt angezeigt werden:

MICTY	Device Modeler - Core		
message			
systemConfigLoad		OK	
systemConfigSave			OK
systemConfigFile			
# 36			
message			
routMac			
routPhysChan			
routMdlr			
outputLdchan			
baseStationName	TTXOF-DWV-AFY-001		
baseStationName	mduf_3ch		
baseStationVendor	Mitsumi		
batt			
dutyCycle	0		
gsmAntenna	0		
gsmAntenna	0		
gsmCompRate	0		
intraCarrierSampleRate	0		
outtraCarrierSampleRate	0		
serviceCenterAudio	192 198 0 156		
serviceCenterConnect	false		
serviceCenterCpuTimeout	200000		
serviceCenterPinger			
serviceCenterPort	18010		
serviceCenterSslPublicKey	C=US,E=ttx@ttc.com		
serviceCenterSerialNumber	10462-7003		
serviceCenterTimeOut	5000		
softwareEmbedded	[E, W]		
tsAlertInactivity	true		
tsAutoRejoinCall	false		
tsCCall	****		
tsCallT	****		
tsCall	****		
tsVerifyHostname	false		
tsVerify	true		
uniqueAddressGlobalId	3E-54-46-FF-FE-E6-7B-78		

Anschließend klicken Sie auf „Dashboard“, woraufhin das Feld grün angezeigt wird.



5.2. ÜBERPRÜFUNG DER BSSCI-VERBINDUNG IM SERVICE CENTER

Die neu hinzugefügte Basisstation wird nun im Service Center angezeigt.

BSSCI Service Center

DashboardSensorsConfigurationCertificatesLogs

BSSCI Service Center Dashboard

Service Status

Failed to load service status

Quick Actions

Manage Sensors

Configuration

View Logs

Base Station Status

Connected Base Stations: 3

EUI: 70b3d59cd00009f6
Address: 192.168.208.1:49172
EUI: 9c65f9fffe6be145
Address: 192.168.208.1:49180
EUI: 3e5446fffee97b78
Address: 192.168.208.1:46126

Connecting Base Stations: 0

No connecting base stations

Recent Logs

Damit ist der Onboarding-Prozess erfolgreich abgeschlossen, und die Basisstation ist nun aktiv mit dem Sentinum Service Center verbunden.

6. FEHLERBEHEBUNG

Dieser Abschnitt bietet Anleitungen zur Identifizierung und Behebung häufiger Probleme während des MIOTY-CLI-Betriebs und der Kommunikation mit dem Service Center.

PROBLEM	MÖGLICHE URSACHE	EMPFOHLENE MASSNAHME
VERBINDUNG VOM GEGENÜBER ZURÜCKGESETZT	TLS-Handshake- oder Zertifikatsfehler	Überprüfen Sie die TLS-Zertifikate auf Gültigkeit und korrekte Installation. Starten Sie den MIOTY-Dienst mit <code>mioty-cli neu</code> .
FILEDATEIENDE	Unterbrochener Datenstrom	Prüfen Sie die Datei <code>/var/log/mioty.log</code> für Detailinformationen. Stellen Sie eine stabile Netzwerkverbindung sicher
KEINE DATENÜBERTRAGUNG	Fehlkonfiguration des Netzwerks oder des Service Centers	Testen Sie die Verbindung zwischen Gateway und Service Center. Bestätigen Sie die korrekte IP-Adresse und den Port mit <code>mioty-cli getall</code> .

Protokolle können ebenfalls mit dem Befehl `journalctl -u mioty` eingesehen werden.

7. SICHERHEIT UND WARTUNG

Regelmäßige Sicherheits- und Wartungsmaßnahmen sind erforderlich, um die langfristige Stabilität und Datenintegrität des Gateways sicherzustellen.

Passwortschutz

- Ändern Sie alle Standardpasswörter unmittelbar nach der Installation.
- Definieren und vergeben Sie Benutzerrollen, um Zugriffsrechte gezielt zu steuern.

Firmware-Updates

- Überprüfen Sie regelmäßig das Sentinum-Portal auf verfügbare Firmware-Updates.
- Führen Sie Updates über die Weboberfläche oder die CLI gemäß den Sentinum-Update-Anweisungen durch

Datensicherung und Wiederherstellung

- Exportieren Sie die aktuelle Konfiguration, bevor Sie größere Änderungen oder Updates durchführen.
- Dokumentieren Sie den Wiederherstellungsprozess, um im Falle eines Systemausfalls eine schnelle Wiederinbetriebnahme zu ermöglichen.

8. ANHANG

8.1. GLOSSAR

- **mioty** - Funkprotokoll für Low-Power-Wide-Area-Netzwerke (LPWAN)
- **MQTT** - Leichtgewichtiges Nachrichtenprotokoll, das häufig in IoT-Systemen verwendet wird

8.2. LINKS

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

8.3. SUPPORT

Technischer Kontakt: Simon Schrapfer

Projektkoordination: Manuel Hart