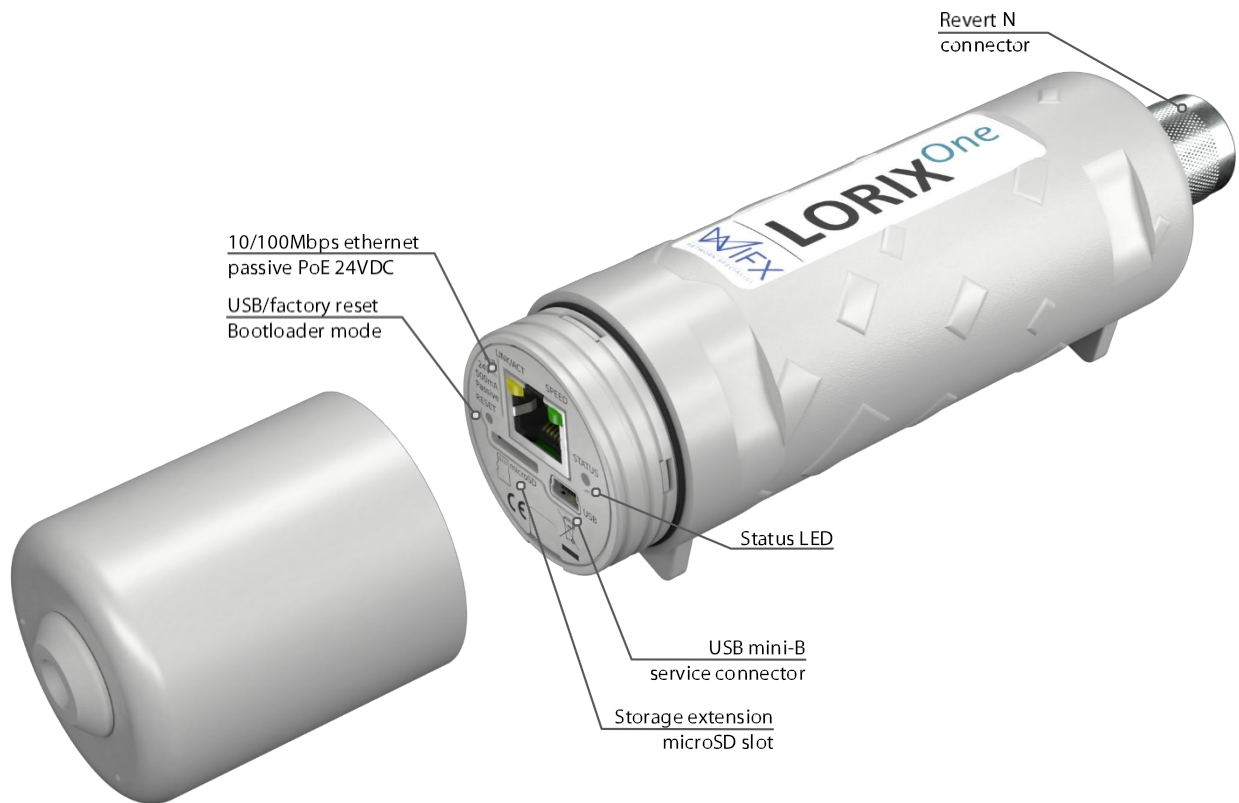


LORIX^{One}

WIFX IP65-GATEWAY MIT INTEGRIERTEM LORAWAN®-KONZENTRATOR-CHIP



Benutzerhandbuch



Versionen:

Revision	Hinweis	Datum
1.0	TTN-Cloud-Anwendung hinzugefügt Systemaktualisierung hinzugefügt	03.05.2017
1.1	Betriebstemperatur und Stromversorgung gemäß Sicherheitszertifizierungsanforderungen aktualisiert	30.07.2017
1.	Kersing-Paketweiterleitung hinzugefügt und andere Paketweiterleitungen und Cloud-Manager Manager mit manueller Weiterleitungsoption hinzugefügt.	21.04.2018
1.3	US-Version hinzugefügt	08.05.2018
1.4	Aktualisierung der FCC- und IC-Rechtstexte und Hinzufügen einer Installationsbeschreibung	06.07.2018
1.5	Aktualisierung des NAND-Speichers basierend auf der HW-Version.	03.09.2018
1.6	Aktualisierte Grafiken mit dem neuesten Wifx-Logo und hinzugefügter Tabelle mit RF-Spezifikationen	14.02.2019
1.7	Aktualisierte Tabelle 4 (ERC 70-3-Band)	28.11.2019
1.8	Spezifikation zur Einhaltung der peruanischen Vorschriften hinzugefügt und allgemeine Dokumentation auf Basis von LORIX OS aktualisiert.	05.12.2021
1.9	Tippfehler korrigiert.	21.06.2022

1 ZUSAMMENFASSUNG

- 1 Zusammenfassung2
- 2 Produktspezifikationen4
- 3 Vorschriften.....6
 - 3.1 Version 8XX (863-870 MHz-Band).....6
 - 3.1.1 Europa / CE.....6
 - 3.2 Version 9XX (902-928 MHz-Band).....7
 - 3.2.1 USA / FCC.....7
 - 3.2.2 Kanada / IC7
 - 3.2.3 Australien/Neuseeland8
- 4 Allgemeine Informationen.....9
 - 4.1 Online-Dokumentation.....9
 - 4.1.1 Update-Informationen.....9
 - 4.1.2 Fehlerbehebung.....9
 - 4.1.3 Open-Source-Lizenzen.....9
 - 4.2 Konnektivität/Schnittstelle9
 - 4.3 Start/Reset.....9
 - 4.3.1 Verfahren.....10
- 5 Ethernet/PoE11
 - 5.1 Stromversorgung über passives PoE.....11
- 6 Servicezugang12
 - 6.1 Zugriffsmethoden12
 - 6.1.1 Übersicht12
 - 6.1.2 Netzwerkzugriff12
 - 6.2 USB13
 - 6.3 Netzwerk.....14
 - 6.3.1 mDNS.....14
 - 6.3.2 SSH.....14
 - 6.3.3 Webschnittstelle14
- 7 Grundeinrichtung16
 - 7.1 Netzwerk konfigurieren16
 - 7.1.1 Aktuellen Status überprüfen16
 - 7.1.2 DHCP.....17
 - 7.1.3 Statisch18
 - 7.1.4 Netzwerküberprüfung und Fehlerbehebung.....19
 - 7.2 Sicherheit.....19
 - 7.2.1 Passwort19
 - 7.2.2 SSL-Zertifikat.....20
 - 7.3 Systemaktualisierung22
 - 7.4 LoRa/LoRaWAN-Konfiguration23



7.4.1	LoRa (RF).....	23
7.4.2	LoRaWAN.....	25
7.4.3	GWID-Format.....	25
8	Elektrisch.....	26
8.1	Leistungsaufnahme.....	26
9	Mechanisch.....	27
9.1	LORIX One.....	27
9.2	Antenne 3 dBi (Versionen 8XX und 9XX).....	28
9.3	Antenne 5 dBi (Versionen 8XX und 9XX).....	28
9.4	Antenne 2,15 dBi (Versionen 8XX).....	28
10	Einrichtungsanleitung.....	29
10.1	Allgemeine Empfehlungen.....	29
10.2	Standardmontage mit einer Stange.....	29

2 PRODUKTSPEZIFIKATIONEN

Ausführung	IP64 (wasserdicht)
Physikalische Spezifikationen	
Abmessungen	Siehe 9.1 LORIX One
Gewicht	< 230 Gramm
Anschlüsse	
	1 RJ45-Ethernet-Anschluss mit 10/100 Mbit/s Max. 100 m Länge, für den Außenbereich abgeschirmtes Kabel verwenden
	1 USB-Mini-B-Serviceanschluss (nur für Servicezwecke)
	1 RF-Antennenanschluss vom Typ N
	1 microSD SD-Speicherkarte Spezifikation v2.0 Steckplatz
Stromversorgungsspezifikationen	
Eingangsversorgung	24 VDC 500 mA (über passives PoE)
Stromversorgung	Siehe 5.1 Stromversorgung über passives PoE
Verbrauch	Siehe 8.1 Leistungsaufnahme
Klimatische Spezifikationen	
Betriebstemperatur	-30 °C bis +55 °C -5 °C bis +40 °C für das Netzteil (S-)HNP12-240L6, nur für den Einsatz in Innenräumen
Lagertemperatur	-20 °C bis +70 °C
Betriebsfeuchtigkeit	10 % bis 90 % relative Luftfeuchtigkeit, nicht kondensierend
Luftfeuchtigkeit bei Lagerung	5 % bis 90 % relative Luftfeuchtigkeit, nicht kondensierend
System	
CPU	ARM Cortex-A5 mit 600 MHz
RAM	128 MB DDR2 mit 200 MHz
Interner Speicher	Bis zu 1.0d HW-Version: 256 MB NAND FLASH mit 4-Bit-Hardware-ECC (Micron MT29F2G08ABAEAH4) Ab HW-Version 1.0d2 : 512 MB NAND FLASH mit 8-Bit-Hardware-ECC (Micron MT29F4G08ABAEAH4)
Externer Speicher	microSD-Kartensteckplatz, SDHC-kompatibel, kann als Boot-Quelle verwendet werden

TABELLE 1: PRODUKTSPEZIFIKATIONEN

Version	8XX	9XX	
RF-Spezifikation			
LoRaWAN-Region	EU868	US915	AU915
LoRa-Modulation (Chirp-Spreizspektrum Modulation)	863–873 MHz Nachfolgend Tabelle 3: Zertifizierungskonformität Version 8XX für Europa	902–928 MHz	915–928 MHz
FSK-Modulation	863–873 MHz Gemäß Tabelle 3: Zertifizierungskonformität Version 8XX für Europa	Nicht zutreffend	Nicht zutreffend
Sendeleistung	Gemäß Tabelle 4: Einschaltdauer und maximale EIRP Version 8XX für Europa	Maximale Strahlungsleistung von 30 dBm. Die leitungsgebundene Leistung muss an den Antennengewinn angepasst werden.	Folgende Tabelle 7: HF-Spezifikationen Version 9XX für Australien/Neuseeland
TX-Frequenztoleranz	±4 ppm einschließlich Alterung, temperaturkompensiert		
Minimale Empfindlichkeit des Empfängers (10 % PER)	-136,5 dB (SF12BW125)	-136,5 dB (SF12BW125)	
Antennenimpedanz	50 Ohm		

TABELLE 2: PRODUKT-HF-SPEZIFIKATIONEN

3 VORSCHRIFTEN

3.1 VERSION 8XX (863-870-MHZ-BAND)

3.1.1 EUROPA / CE

Die Version LORIX One 8XX erfüllt die Anforderungen gemäß Artikel 3 der Richtlinie RED 2014/53/EU:

Zertifizierungskonformität	
Funk & EMV	RED 2014/53/EU (Europäische Richtlinie über Funkanlagen)
	ETSI EN 300 220-2
	EN 61000-6-1:2007 IEC 61000-6-1:2005 (ed2.0)
	ETSI EN 301 489-3 V1.6.1:2013
Sicherheit für Personen	EN 62209-2 IEC/EN 62479-1
Elektrische Sicherheit	IEC/EN 62368-1

TABELLE 3: ZERTIFIZIERUNGSKONFORMITÄT VERSION 8XX FÜR EUROPA

Für den Einsatz in Europa muss das LORIX One die Anforderungen der ERC 70-3 hinsichtlich Arbeitszyklus und maximaler EIRP erfüllen. Diese Parameter sind in der folgenden Tabelle zusammengefasst:

Tastverhältnis und maximale EIRP			
ERC 70-3 Band	Frequenz (MHz)	Leistung	Tastverhältnis
h1,3	863 – 865	14 dBm ERP	0,1
h1.4	865 – 868	14 dBm ERP	1
h1.5	868 – 868,6	14 dBm ERP	1
h1.6	868,7 – 869,2	14 dBm ERP	0,1
h1.7	869,4 – 869,65	27 dBm ERP	10
h1.8	869,7 – 870	7 dBm ERP	Keine Anforderung
h1.9	869,7 – 870	14 dBm ERP	1

TABELLE 4: BETRIEBSZYKLEN UND MAXIMALE EIRP VERSION 8XX FÜR EUROPA

Wenn die Antenne ausgetauscht wird, muss die Ausgangsleistung angepasst werden, um die Verstärkung der Antenne zu berücksichtigen und eine Überschreitung der in der Verordnung ERC 70-3 festgelegten Werte zu vermeiden.

Warnung: In einigen Ländern Europas gelten möglicherweise bestimmte Vorschriften hinsichtlich Frequenzbereich, maximaler EIRP und Arbeitszyklus. Bitte überprüfen Sie die örtlichen Vorschriften, bevor Sie die LORIX One 8XX-Version installieren und verwenden.

Für Länder außerhalb Europas überprüfen Sie bitte, ob der Frequenzbereich, die maximal zulässige EIRP und der Arbeitszyklus zugelassen sind.

3.2 VERSION 9XX (902-928 MHZ BAND)

Die LORIX One (IP43 & IP65) 9XX-Version entspricht sowohl den FCC- als auch den IC-Vorschriften:

Zertifizierungskonformität	
CFR 47 FCC Teil 15	FCC 47 CFR Teil 15: 2014 – Teil 15 – Hochfrequenzgeräte
RSS 247	RSS-Gen – Ausgabe 5, April 2018 – Allgemeine Anforderungen und Informationen für die Zertifizierung von Funkgeräten
	RSS-247 Ausgabe 2, Februar 2017 – Digitale Übertragungssysteme (DTSS), Frequenzsprungverfahren (FHSS) und lizenzfreie lokale Netzwerke (LE-LAN)

TABELLE 5: ZERTIFIZIERUNGSKONFORMITÄT VERSION 9XX FÜR USA/KANADA

Die zugehörigen FCC- und IC-Kennungen der LORIX One 9XX-Version lauten:

FCC-ID: 2APAZ-LORIXONE IC:

23715-LORIXONE

Modell: LORIX One

Um die FCC- und IC-Konformität der Geräte in den USA und Kanada aufrechtzuerhalten, müssen bestimmte Bedingungen erfüllt sein. Diese Bedingungen werden in den folgenden Abschnitten näher erläutert. Für andere Länder überprüfen Sie bitte die spezifischen Vorschriften bezüglich der maximal zulässigen EIRP und des maximalen Arbeitszyklus.

3.2.1 USA / FCC

Dieses Gerät entspricht Teil 15 der FCC-Bestimmungen. Der Betrieb unterliegt den folgenden zwei Bedingungen: (1) Dieses Gerät darf keine schädlichen Störungen verursachen, und (2) dieses Gerät muss alle empfangenen Störungen akzeptieren, einschließlich Störungen, die einen unerwünschten Betrieb verursachen können.

Änderungen oder Modifikationen, die nicht ausdrücklich von der für die Einhaltung der Vorschriften verantwortlichen Stelle genehmigt wurden, können zum Erlöschen der Betriebserlaubnis für das Gerät führen.

Dieses Gerät wurde getestet und entspricht den Grenzwerten für digitale Geräte der Klasse A gemäß Teil 15 der FCC-Bestimmungen. Diese Grenzwerte sollen einen angemessenen Schutz vor schädlichen Störungen gewährleisten, wenn das Gerät in einer gewerblichen Umgebung betrieben wird. Dieses Gerät erzeugt und verwendet Hochfrequenzenergie und kann diese ausstrahlen. Wenn es nicht gemäß der Bedienungsanleitung installiert und verwendet wird, kann es zu Störungen des Funkverkehrs kommen. Der Betrieb dieses Geräts in einem Wohngebiet kann zu schädlichen Störungen führen. In diesem Fall muss der Benutzer die Störungen auf eigene Kosten beheben.

Dieses Gerät muss von einem Fachmann installiert werden.

Außerdem müssen einige spezifische Empfehlungen zur Exposition gegenüber Magnetfeldern befolgt werden: Dieses Gerät entspricht den Strahlungsgrenzwerten der FCC für eine unkontrollierte Umgebung unter den folgenden Bedingungen:

1. Dieses Gerät sollte so installiert und betrieben werden, dass jederzeit ein Mindestabstand von 20 cm zwischen dem Strahler (Antenne) und dem Körper des Benutzers/Personen in der Nähe eingehalten wird.
2. Dieser Sender darf nicht zusammen mit anderen Antennen oder Sendern aufgestellt oder betrieben werden.

3.2.2 KANADA / IC

Dieses Gerät entspricht den lizenzfreien RSS-Standards von Industry Canada. Der Betrieb unterliegt den folgenden zwei Bedingungen:

1. Dieses Gerät darf keine schädlichen Störungen verursachen und
2. Dieses Gerät muss alle empfangenen Störungen akzeptieren, einschließlich Störungen, die zu einem unerwünschten Betrieb des Geräts führen können.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. Das Gerät darf keine Störungen verursachen.
2. Der Benutzer des Geräts muss alle empfangenen Funkstörungen akzeptieren, auch wenn diese den Betrieb des Geräts beeinträchtigen können.

Gemäß den Vorschriften von Industry Canada darf dieser Funksender nur mit einer Antenne betrieben werden, deren Typ und maximale (oder geringere) Verstärkung von Industry Canada für den Sender zugelassen sind. Um mögliche Funkstörungen für andere Nutzer zu reduzieren, sollten dieser Antennentyp und seine Verstärkung so gewählt werden, dass die äquivalente isotrope Strahlungsleistung (EIRP) nicht höher ist als für eine erfolgreiche Kommunikation erforderlich.

Dieser Funksender wurde von Industry Canada für den Betrieb mit den als Zubehör aufgeführten Antennentypen mit der maximal zulässigen Verstärkung und der für jeden Antennentyp angegebenen erforderlichen Antennenimpedanz zugelassen. Antennentypen, die nicht in dieser Liste aufgeführt sind und eine Verstärkung aufweisen, die über der für diesen Typ angegebenen maximalen Verstärkung liegt, dürfen unter keinen Umständen mit dem Gerät verwendet werden.

Dieses Gerät sollte so installiert und betrieben werden, dass jederzeit ein Mindestabstand von 20 cm zwischen dem Strahler (Antenne) und dem Körper des Benutzers/Personen in der Nähe eingehalten wird.

3.2.3 AUSTRALIEN/NEUSEELAND

Dieses Gerät entspricht Abschnitt 134 (1) (g) des neuseeländischen Funkgesetzes von 1989 und erfüllt die folgenden geltenden Normen:

Zertifizierungskonformität	
Sicherheit	IEC/EN 62368-1
EMV	EN 61000-6-1:2007 IEC 61000-6-1:2005 (ed2.0)
	ETSI EN 301 489-3 V1.6.1:2013
Funkfrequenzen	FCC 47 CFR Teil 15: 2014 – Teil 15 – Hochfrequenzgeräte
	RSS-247 Ausgabe 2, Februar 2017 – Digitale Übertragungssysteme (DTSS), Frequenzsprungverfahren (FHSS) und lizenzfreie lokale Netzwerke (LE-LAN)
	RSS-Gen Ausgabe 4, November 2014 – Allgemeine Anforderungen für die die Konformität von Funkgeräten

TABELLE 6: ZERTIFIZIERUNGSKONFORMITÄT VERSION 9XX FÜR AUSTRALIEN/NEUSEELAND

Dieses Gerät muss fachgerecht installiert und darf nur in industriellen Umgebungen verwendet werden. Darüber hinaus muss der Netzwerksver die in der folgenden Tabelle definierten HF-Spezifikationen einhalten.

HF-Spezifikationen	
Frequenzbereich	915–928 MHz
Max. EIRP	30 dBm
Maximale leitungsgebundene Leistung (2 dBi-Antenne)	28 dBm
Max. leitete Leistung (3 dBi Antenne)	27 dBm
Maximale übertragene Leistung (4 dBi-Antenne)	26 dBm
Maximale übertragene Leistung (5 dBi Antenne)	25 dBm

TABELLE 7: HF-SPEZIFIKATIONEN VERSION 9XX FÜR AUSTRALIEN/NEUSEELAND

4 ALLGEMEINE INFORMATIONEN

4.1 ONLINE-DOKUMENTATION

Die Online-Dokumentation ist unter iot.wifx.net/docs verfügbar und enthält Informationen zur technischen Verwendung des Produkts, einschließlich seines Betriebssystems, dem LORIX OS.

Vollständige Dokumentation

Die Dokumentation in diesem Benutzerhandbuch ist minimal und weitere Informationen, insbesondere zum LORIX OS, sind online verfügbar. Bitte konsultieren Sie diese, wenn Sie die Informationen in diesem Dokument nicht finden können.

4.1.1 INFORMATIONEN ZU UPDATES

Die zwischen den einzelnen neuen Versionen von LORIX OS vorgenommenen Änderungen sind auf der Seite „Changelog“ der Online-Dokumentation unter <https://iot.wifx.net/docs/lorix-os/latest/release-notes> beschrieben.

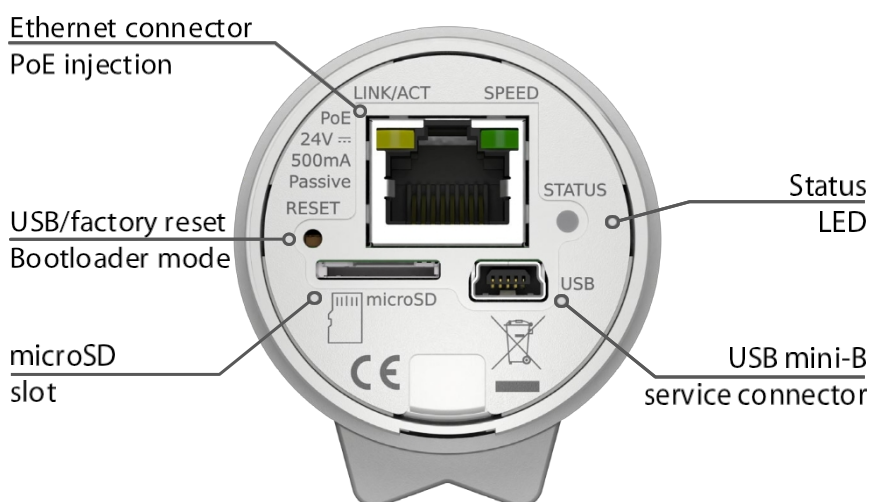
4.1.2 FEHLERBEHEBUNG

Häufig auftretende Probleme sind auf der Seite zur Fehlerbehebung in der Online-Dokumentation zusammengefasst, und Lösungsvorschläge finden Sie unter <https://iot.wifx.net/docs/lorix-os/latest/troubleshooting>.

4.1.3 OPEN-SOURCE-LIZENZEN

Alle Lizenzen der Open-Source-Software, die im Paket-Repository von LORIX OS verwendet wird oder verfügbar ist, finden Sie unter <https://download.wifx.net/lorix-os/<LORIX OS-Release-Version>/licenses/>. Für die Version 1.3.4 sind die Lizenzen beispielsweise unter <https://download.wifx.net/lorix-os/1.3.4/licenses/> verfügbar..

4.2 KONNEKTIVITÄT/SCHNITTSTELLE



4.3 START/RESET

Das Gateway startet automatisch, wenn es über passives PoE über das Ethernet-Kabel an eine Stromversorgung angeschlossen wird. Nach dem Start sollte die Status-LED kurz blinken und dann erlöschen. Sobald das Linux-Betriebssystem gestartet ist, beginnt die Status-LED im „Heartbeat“-Modus zu blinken.

Die Reset-Taste kann verwendet werden, um:

- Setzen Sie das Gateway normal zurück und starten Sie es im normalen Betriebsmodus.
- Setzen Sie das Gateway auf die ursprünglichen Werkseinstellungen zurück.
- Rufen Sie den Programmiermodus auf.

Verwenden Sie zum Drücken der Taste ein dünnes Werkzeug, z. B. eine Büroklammer. Nach dem Loslassen blinkt die Status-LED kurz und erlischt dann, um den Reset zu signalisieren.

4.3.1 VORGEHENSWEISE



Kurz drücken

Drücken Sie die Taste kurz, weniger als 1 Sekunde lang. Die blaue LED blinkt kurz, wenn Sie die Taste loslassen.



Langes Drücken

Drücken Sie die Taste einige Sekunden lang. Die blaue LED blinkt kurz nach der unten angegebenen Verzögerungszeit.

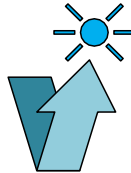


Status-LED

Ein kurzes Blinken der blauen LED

Normales Reset-Verfahren

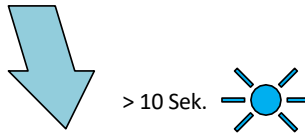
1. Kurzes Drücken
2. Die Status-LED blinkt beim Loslassen und das Gateway wird neu gestartet



Werkseinstellungen zurücksetzen

Mit dem Werksreset-Verfahren können Sie die ursprüngliche Standardkonfiguration zurücksetzen und so die ursprünglichen Einstellungen des Geräts wiederherstellen. Dieses Verfahren ist nützlich, um eine fehlerhafte Netzwerkkonfiguration zu beheben oder ein vergessenes Passwort wiederherzustellen.

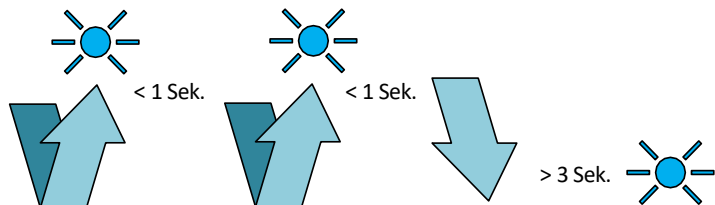
1. Warten Sie nach jedem Reset-Druck mindestens 1 Sekunde.
2. Langes Drücken für mindestens 10 Sekunden
3. Lassen Sie die Reset-Taste los, sobald die LED zu blinken beginnt.
4. Das Gateway wird im Werkseinstellungsmodus gestartet. Nach dem Start von Linux kopiert ein Skript die Standarddateien.



Vorgehensweise im Programmiermodus

Dieses Verfahren wird verwendet, um in den Programmiermodus zu gelangen. Es ermöglicht die Neuprogrammierung des Gateways mit dem Wifx Programming Tool (früher LORIX Programming Tool genannt) über den USB-Anschluss, wie auf der Online-Dokumentationsseite <https://iot.wifx.net/docs/go/wifx-programming-tool/help> zusammengefasst.

1. Entfernen Sie die microSD-Karte aus dem Gerät.
2. Warten Sie mindestens 1 Sekunde, bevor Sie erneut drücken
3. Drücken Sie zweimal kurz hintereinander, wobei zwischen den beiden Drücken weniger als 1 Sekunde liegen sollte.
4. Drücken Sie ein drittes Mal länger als 3 Sekunden (aber weniger 5 Sekunden)



5 ETHERNET/POE

Anschlussdetails:

RJ45-Pin Anzahl	Drahtfarbe	Funktion	
1	Grün	TX+	
2	Grün/Weiß	TX-	
3	Orange	RX+	
4	Blau	VPOE1	Spannung 1 für PoE-Stromversorgung (muss mit Pin 5 verbunden sein)
5	Blau/Weiß	VPOE1	Spannung 1 für PoE-Stromversorgung (muss mit Pin 4 verbunden sein)
6	Orange/Weiß	RX-	
7	Braun	VPOE2	Spannung 2 für PoE-Stromversorgung (muss mit Pin 8 verbunden sein)
8	Braun/Weiß	VPOE2	Spannung 2 für PoE-Stromversorgung (muss mit Pin 7 verbunden sein)

TABELLE 8 ETHERNET-/POE-ANSCHLUSS

Die gelbe LED zeigt die Verbindung (LINK) und die Aktivität (ACTIVITY) der Ethernet-Verbindung an:

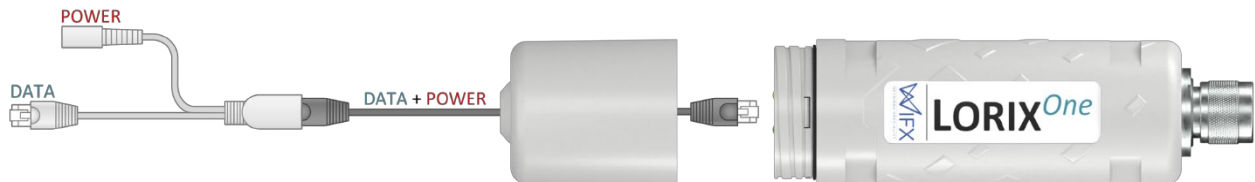
- AUS** Keine Verbindung
- EIN** Verbindung
- Blink** Verbindung und Aktivität

Die grüne LED zeigt die aktuelle GESCHWINDIGKEIT der Ethernet-Verbindung an:

- AUS** 10Base-T
- EIN** 100Base-TX

5.1 STROMVERSORGUNG ÜBER PASSIVES POE

Das LORIX One-Gateway wird ausschließlich über passives PoE über den Ethernet-Anschluss mit Strom versorgt. Die Stromversorgung erfolgt über einen PoE-Injektor, wie unten dargestellt:



VPOE1 und VPOE2 (in Tabelle 8) stehen für die beiden Stromleitungen des Gateways. Die Stromversorgung muss über den mit dem LORIX One mitgelieferten Schaltnetzteil in den Stromeingangsanschluss eingespeist werden:

- Referenz** HNP12-240L6
- Ausgangsspannung** 24 VDC
- Ausgangsstrom** 500 mA

6 SERVICEZUGANG

Der Zugriff auf das eingebettete Linux und dessen Konfiguration kann entweder über den Service-USB-Typ-C-Anschluss oder über SSH oder die Webschnittstelle mit einer funktionierenden Ethernet-Verbindung erfolgen.

Standardbenutzer und -kennwort
Der Standardbenutzer ist „admin“ und das Passwort lautet „lorix4u“. Dies ist während der Ersteinrichtung nützlich und leicht zu merken, wir empfehlen jedoch dringend, das Passwort so schnell wie möglich zu ändern, wie in 7.2.1 Passwort erläutert.

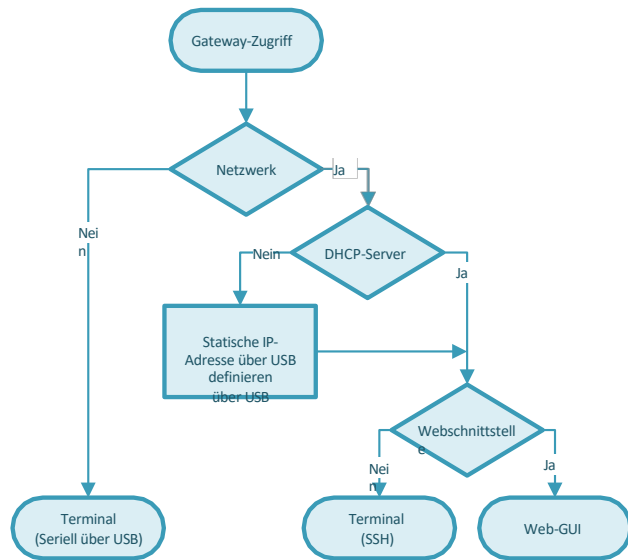
6.1 ZUGRIFFSMETHODEN

6.1.1 ÜBERSICHT

Dieses Diagramm gibt einen Überblick über die Methoden, mit denen Sie auf das Gateway zugreifen können. Wenn Sie nur über USB verfügen oder das Netzwerk nicht konfiguriert ist (oder die IP-Adresse nicht bekannt ist), haben Sie immer Terminalzugriff über den USB-Service-Anschluss.

Sobald das Netzwerk konfiguriert ist und funktioniert, können Sie entscheiden, ob Sie das Terminal über das Netzwerk (SSH) oder die benutzerfreundlichere Webschnittstelle über Ihren bevorzugten Webbrowser verwenden möchten.

Wenn Ihr Netzwerk keinen DHCP-Server hat, müssen Sie über den USB-Zugang eine statische IP-Adresse konfigurieren.



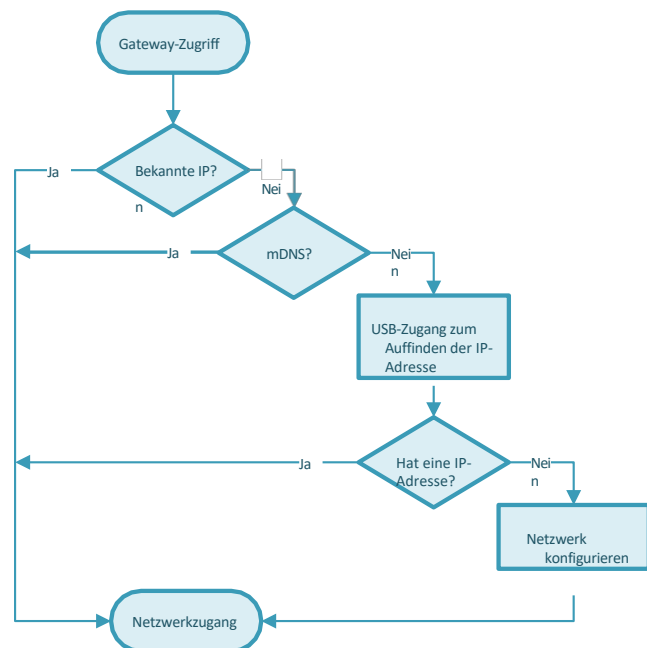
6.1.2 NETZWERKZUGANG

Um über die Webschnittstelle oder über SSH, wenn Sie lieber ein Terminal verwenden, auf das Gateway zuzugreifen, benötigen Sie ein funktionierendes Netzwerk mit einem DHCP-Server (der eine dynamische IP-Adresse bereitstellt) oder müssen eine statische IP-Adresse für Ihr Gateway definieren.

Wenn Ihr Gateway über eine IP-Adresse verfügt und Sie diese kennen, können Sie es einfach wie unter 6.3 Netzwerk beschrieben erreichen.

Wenn Sie die IP-Adresse nicht kennen, aber wahrscheinlich über einen DHCP-Server verfügen, können Sie versuchen, es über mDNS zu erreichen, wie unter 6.3.1 mDNS beschrieben, oder die IP-Adresse über die Admin-Oberfläche des Routers ermitteln.

Schließlich können Sie die IP-Adresse über die USB-Schnittstelle ermitteln oder als statische IP-Adresse konfigurieren.



6.2 USB

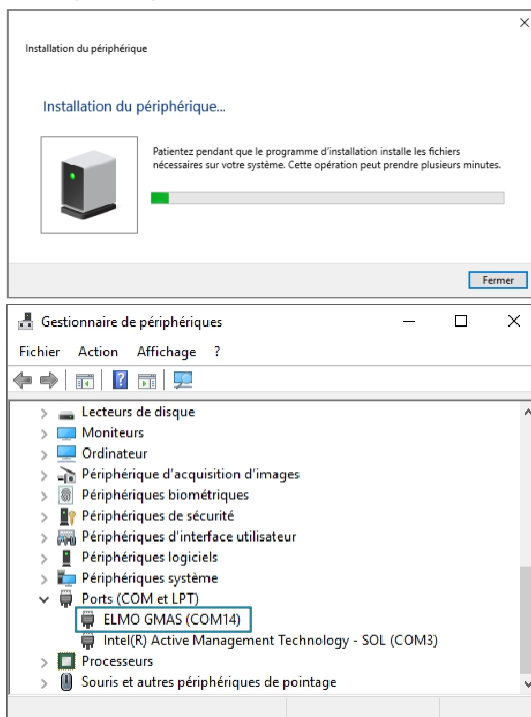
Das Gateway verfügt über einen USB-Typ-C-Anschluss, der einen virtuellen COM-Port bereitstellt, sobald die Service-LED (weiß) aufleuchtet. Der Zugriff auf das Gateway auf diese Weise ermöglicht Ihnen das Debuggen und Konfigurieren des Systems. Dies ist auch die einzige Möglichkeit, das Service-Terminal zu erreichen, wenn das Netzwerk nicht zugänglich oder noch nicht konfiguriert ist.

Hinweise zur USB-Verbindung

Die USB-Verbindung sollte ausschließlich für die Serviceverwaltung/-konfiguration verwendet werden und während des normalen Betriebs nicht angeschlossen bleiben. Bei Verwendung des USB-Serviceanschlusses ist die Schutzart IP65 ebenfalls nicht gewährleistet.

So greifen Sie über USB auf das Gateway zu:

1. Schalten Sie das Gateway mit passivem PoE über den Ethernet-Anschluss oder direkt über den USB-Anschluss ein.
2. Schließen Sie einen PC mit einem A ⇔ C-Kabel an das Gateway an.
3. Der virtuelle COM-Port wird vom PC automatisch erkannt.
 - a. Unter Windows erscheint im Gerätemanager ein neuer virtueller COM-Port mit dem Namen **ELMO GMAS (COMxx)**.



- b. Unter Linux erscheint ein neuer virtueller COM-Port im Ordner **/dev/ttyACMxx**
4. Ein Terminalprogramm wie PuTTY oder minicom kann mit den folgenden Parametern verwendet werden: Baudrate **921600**

Datenbits	8
Stoppbits	1
Parität	keine
Flusskontrolle	keine

6.3 NETZWERK

6.3.1 MDNS

Das Gateway meldet sich über das mDNS-Protokoll (auch bekannt als Zeroconf, Bonjour) mit seinem Standard-Hostnamen in der Domain „.local“ an. Der Standard-Hostname setzt sich aus dem Präfix „lorix-one-“ und den letzten 6 Zeichen der MAC-Adresse in Kleinbuchstaben zusammen: `lorix-one-xxxxxx`.

Das bedeutet, dass Sie Ihr Gateway über die folgende Adresse erreichen können: `lorix-one-xxxxxx.local`.

Beispiel

Die auf dem Aufkleber angegebene MAC-Adresse des Gateways lautet FC:C2:3D:AA:BB:CC. Der Hostname lautet daher `lorix-one-aabbcc`.

Sie können das Gateway unter `lorix-one-aabbcc.local` erreichen.

Um das Gateway über mDNS zu kontaktieren, muss Ihr Netzwerk diese Funktion unterstützen (mit deaktiviertem IGMP-Snooping) und Sie müssen sich im selben Subnetz wie das zu kontaktierende Gateway befinden.

6.3.2 SSH

Das Gateway stellt einen SSH-Server bereit und kann über SSH aufgerufen werden, sobald es konfiguriert und über ein SSH-Client-Programm wie PuTTY oder ssh unter Linux mit einem funktionierenden Netzwerk verbunden ist.

So greifen Sie mit SSH auf das Gateway zu:

1. Schalten Sie das Gateway ein.
2. Ein Terminalprogramm wie PuTTY oder ssh kann mit den folgenden Parametern verwendet werden: Adresse **IP-Adresse oder mDNS-Hostname**
Port **22**
3. Akzeptieren Sie den RSA-Schlüssel-Fingerabdruck, wenn Sie dazu aufgefordert werden

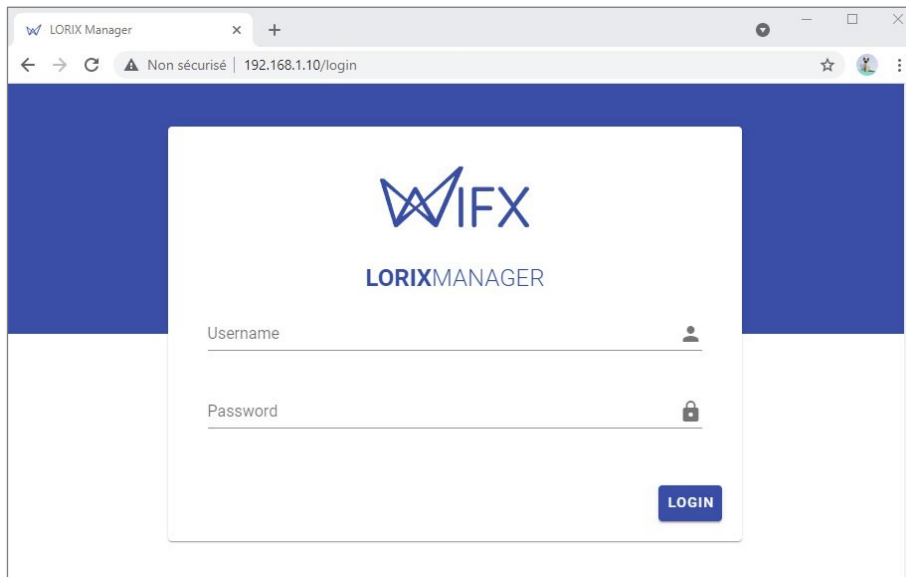
6.3.3 WEBSCHNITTSTELLE

Das Gateway verfügt über eine grafische Webschnittstelle, auf die Sie über Ihren bevorzugten Webbrowser zugreifen können.

Wie bereits erläutert, können Sie das Gateway über seine IP-Adresse oder über mDNS erreichen. Außerdem können Sie zwischen HTTP (nicht sicher) und HTTPS (SSL-gesichert) wählen, indem Sie der Adresse jeweils `http://` bzw. `https://` voranstellen.

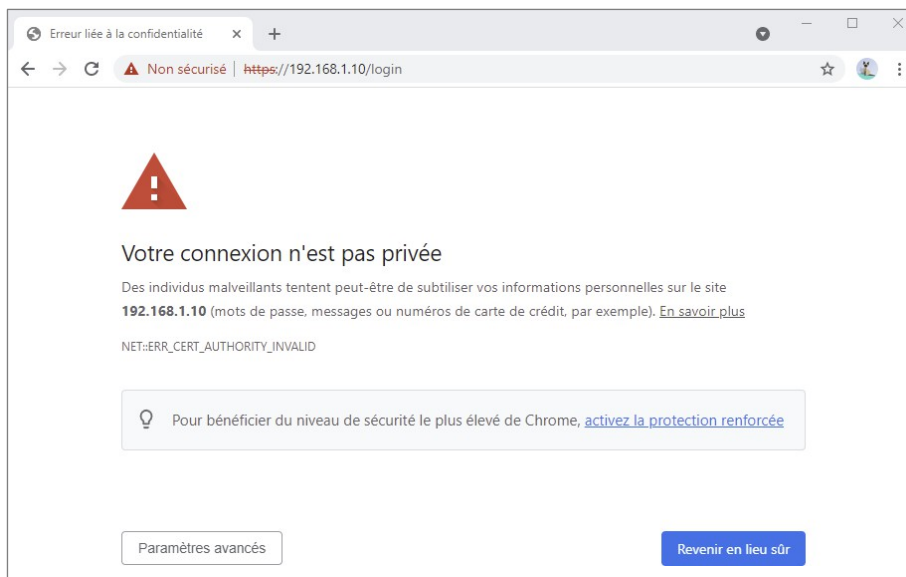
Beispiel

Für die IP-Adresse 192.168.1.148 können Sie das Gateway über `http://192.168.1.148` oder `https://192.168.1.148` erreichen. Dies gilt auch für mDNS, da Sie das Gateway über `http://lorix-one-aabbcc.local` oder `https://lorix-one-aabbcc.local` erreichen können.



6.3.3.1 SICHERHEITSWARNUNG

Wenn Sie mit SSL-Unterstützung (HTTPS) auf das Gateway zugreifen, erhalten Sie eine Sicherheitswarnung. Das Formular kann je nach Webbrowser unterschiedlich aussehen, das Konzept bleibt jedoch dasselbe. Sie erhalten diese Fehlermeldung, weil das SSL-Zertifikat des Gateways selbstsigniert ist, da wir zum Zeitpunkt der Zertifikatserstellung die Adresse nicht kennen.



Sie können diese Sicherheitswarnung jederzeit akzeptieren, dies hängt jedoch von Ihrem Browser ab. Bitte lesen Sie die Dokumentation Ihres Browsers, um zu erfahren, wie Sie das Risiko akzeptieren und fortfahren können.

Sicherheitsüberlegungen

Diese Sicherheitswarnung ist wichtig, um Sie darauf hinzuweisen, dass das Zertifikat nicht von einer globalen Zertifizierungsstelle als vertrauenswürdig eingestuft wird. Wenn Sie wissen, dass die IP-Adresse korrekt ist, solange sie sich in Ihrem lokalen Netzwerk befindet, ist Ihre Verbindung dennoch sicher und es wird verhindert, dass jemand den Datenaustausch (wie Benutzername/Passwort) zwischen Ihrem Computer und dem Gateway einsehen kann.

Wir empfehlen daher, nach Möglichkeit HTTPS zu verwenden.

7 GRUNDLEGENDE EINRICHTUNG

Dieses Kapitel soll Ihnen helfen, Ihr Gateway während des ersten Konfigurationsprozesses einfach einzurichten. Es folgt, soweit möglich, der chronologischen Konfiguration, sodass Sie es wie eine Schritt-für-Schritt-Anleitung lesen und einige Schritte überspringen können, wenn diese für Ihre Einrichtung nicht erforderlich sind.

7.1 KONFIGURIEREN SIE DAS NETZWERK

Der USB-Zugang ist nur für Servicezwecke vorgesehen, da das Gateway in erster Linie über ein IP-Netzwerk erreichbar ist. Der erste Schritt besteht daher darin, die Netzwerkaspekte über den USB-Servicezugang zu konfigurieren.

7.1.1 ÜBERPRÜFEN SIE DEN AKTUELLEN STATUS

7.1.1.1 IP-ADRESSE

Sie können die aktuelle IP-Adresse (v4 und v6) mit dem Befehl `ifconfig` anzeigen:

```

$ ifconfig eth0
eth0      Link-Kapselung: Ethernet- HWaddr fc:c2:3d:aa:bb:cc
          inet addr:192.168.1.10 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6-Adresse: fe80::fec2:3dff:fe2d:56f1/64 Bereich: Verbindung
          inet6-Adresse: aaaa:bbbb:1:0:bbbb:3dff:fe2d:56f1/64 Bereich:Global
          inet6-Adresse: aaaa:bbbb:1:0:dddd:ca08:6889:a36b/64 Bereich:Global
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metrik:1
          RX-Pakete: 10219756 Fehler: 3 Verworfen: 30251 Überläufe: 0 Rahmen:
          3 TX-Pakete: 58541 Fehler: 0 Verworfen: 0 Überläufe: 0 Träger: 0
          Kollisionen: 0 txqueuelen: 1000
          RX-Bytes: 493144710 (470,2 MiB) TX-Bytes: 14043284 (13,3 MiB)
          Interrupt: 27

```

Das Feld „inet addr“ gibt die IPv4-Adressen zurück, die Felder „inet6 addr“ geben die IPv6-Adressen zurück.

7.1.1.2 KONNEKTIVITÄT

Sie können die aktuelle Konnektivität testen, um zu überprüfen, ob das Gateway Zugriff auf lokale oder globale Ressourcen hat oder gar keinen Zugriff:

```

$ nmcli networking connectivity check full

```

Die möglichen Ergebniswerte sind:

- **none**
Der Host ist mit keinem Netzwerk verbunden.
- **Portal**
Der Host befindet sich hinter einem Captive Portal und kann nicht auf das gesamte Internet zugreifen.
- **eingeschränkt**
Der Host ist mit einem Netzwerk verbunden, hat jedoch keinen Zugriff auf das Internet.
- **vollständig**
Der Host ist mit einem Netzwerk verbunden und hat uneingeschränkten Zugriff auf das Internet.
- **unbekannt**
Der Verbindungsstatus kann nicht ermittelt werden.

7.1.1.3 VERBINDUNGSINFORMATIONEN

Die vom System bereitgestellte Hauptverbindung wird in LORIX OS als **Backhaul** bezeichnet und stellt die auf dem Gerät eth0 (Haupt- und einziger Ethernet-Anschluss des Produkts) hergestellte Verbindung dar.

Sie können die verschiedenen Parameter mit den nmcli-Dienstprogrammen wie folgt anzeigen:

```

$ nmcli connection show backhaul
connection.id:                backhaul
connection.uuid:              390e5c2b-7312-415e-80e6-7b94a5c24fc3
Verbindung.stable-id:         --
Verbindungstyp:               802-3-Ethernet
Verbindung.Schnittstellename: eth0
Verbindung.Automatische Verbindung: ja
Verbindung.AutomatischeVerbindung-
Priorität:                     1
Verbindung.Automatische Verbindungswiederholungen: 0 (unbegrenzt)
Verbindung.Multi-Verbindung:  0 (Standard)
Verbindung.Auth-Wiederholungen: -1
Verbindungszeitstempel:       1637144771
connection.read-only:         nein
Verbindung.Berechtigungen:    --
Verbindung.Zone:              --
Verbindung.Master:            --
Verbindung.Slave-Typ:         --
connection.autoconnect-slaves: -1
(Standard) connection.secondaries: --
Verbindung.Gateway-Ping-Zeitlimit: 0
connection.metered:           unbekannt
Verbindung.LLDP:               Standard
Verbindung.mdns:               -1 (Standard)
Verbindung.Ilmnr:              -1 (Standard)
Verbindung.Wartezeit-Gerät:    -1
802-3-Ethernet-Port:          --
802-3-Ethernet.Geschwindigkeit: 0
802-3-Ethernet.Duplex:         --
802-3-Ethernet.Auto-Negotiate: nein
802-3-Ethernet.MAC-Adresse:    --
802-3-ethernet.cloned-mac-address: --
802-3-Ethernet.MAC-Adressmaske generieren:--
802-3-Ethernet.MAC-Adress-Blacklist: --
802-3-Ethernet.MTU:           auto
802-3-Ethernet.s390-Subkanäle: --
802-3-Ethernet.s390-Nettype:   --
802-3-Ethernet.s390-Optionen:  --
802-3-Ethernet.Wake-on-LAN:    Stan
dard 802-3-Ethernet.Wake-on-LAN-Passwort:

```

Zeilen 1-38

Es gibt noch viele weitere Parameter, die hier nicht angezeigt werden und die Sie mit den Aufwärts-/Abwärts-Tasten der Tastatur anzeigen können, um durch die Parameterliste zu blättern.

Parameter in Kleinbuchstaben sind Konfigurationsparameter, Parameter in Großbuchstaben beziehen sich auf die resultierende Situation (Verbindung) und geben Ihnen Informationen über den aktuellen Status.

Interessant ist beispielsweise der Wert IP4.ADDRESS[1], der in diesem Fall 192.168.1.10/24 zurückgibt. Beachten Sie das /24 am Ende, das die Netzmaske darstellt.

7.1.2 DHCP

Standardmäßig verfügt das Gateway über einen DHCP-Client, der auf eine IP-Adresse und andere Konfigurationen von einem DHCP-Server wartet. Dies ist die gängigste und einfachste Art der Verwaltung. Wenn Sie im vorherigen Schritt eine IP-Adresse gefunden haben, bedeutet dies, dass Sie über einen korrekt konfigurierten DHCP-Server verfügen.

Sie können dann entweder die IP-Adresse oder den mDNS-Hostnamen verwenden, wenn Sie sich im selben Subnetz befinden.

Zusätzliche Konfiguration

Eine zusätzliche DHCP-Konfiguration ist oft nicht erforderlich, aber wenn Sie beispielsweise Parameter ändern oder eine Route hinzufügen müssen, können Sie entweder die Weboberfläche (Netzwerk-→ -Ethernet-→ -Einstellungen) verwenden oder die Dokumentation von nmcli¹ konsultieren, wenn Sie den Terminalzugriff (USB oder SSH) bevorzugen.

7.1.3 STATISCH

Über die unter 7.1.1.3 **Verbindungsinformationen** beschriebene Verbindungsanzeige können Sie Verbindungsparameter wie die Einstellung der Methode auf manuell und die IP-Adresse, Netzmaske usw. ändern.

7.1.3.1 DEFINIEREN SIE EINE STATISCHE IPV4-ADRESSE MIT BENUTZERDEFINIERTEM DNS.

Die folgenden Befehle definieren eine feste IPv4-Adresse, die Gateway- und DNS-Adressen und legen schließlich die Methode auf manuell fest (verwenden Sie „auto“, um zu DHCP zurückzukehren):

```
$ nmcli connection modify backhaul ipv4.address 192.168.1.11/24
$ nmcli connection modify backhaul ipv4.gateway 192.168.1.1
$ nmcli connection modify backhaul ipv4.dns 8.8.8.8
$ nmcli connection modify backhaul ipv4.method manual
```

Wenden Sie die neuen Parameter mit dem folgenden Befehl an:

```
$ nmcli connection up backhaul
```

Der Befehl nmcli show connection gibt nun Folgendes zurück:

```
$ nmcli connection show backhaul
[...]
ipv4.method:                manuell
ipv4.dns:                   8.8.8.8
[...]
ipv4.addresses:             192.168.1.11/24
ipv4.gateway: [...]        192.168.1.1
IP4.ADDRESS[1]:             192.168.1.11/24
IP4.GATEWAY:                192.168.1.1
IP4.ROUTE[1]:              192.168.1.1
IP4.ROUTE[2]:              dst = 192.168.1.0/24, nh = 0.0.0.0, mt = 100
IP4.DNS[1]:                 dst = 0.0.0.0/0, nh = 192.168.1.1, mt = 100
[...]
8.8.8.8
```

Über die Weboberfläche können Sie die grafische Darstellung sehen:

Connection status

STATUS
Activated ●

IPv4	ADDRESS	GATEWAY	DNS
	192.168.1.11 /24	192.168.1.1	8.8.8.8

IP Address	192.168.1.11 /24
Gateway	192.168.1.1
DNS	8.8.8.8

Routes	192.168.1.0 /24 100
	0.0.0.0 /0 100

¹ nmcli – Befehlszeilentool zur Steuerung von NetworkManager <https://developer.gnome.org/NetworkManager/stable/nmcli.html>

7.1.4 NETZWERKÜBERPRÜFUNG UND FEHLERBEHEBUNG

Zu diesem Zeitpunkt sollten Sie über eine funktionierende Netzwerkkonfiguration verfügen. Im folgenden Kapitel erfahren Sie, wie Sie diese überprüfen können.

Als Erstes sollten Sie die Netzwerkverbindung erneut testen, wie in Kapitel 7.1.1.2 „[Verbindung](#)“ beschrieben. Das Ergebnis sollte „vollständig“ lauten.

Ist dies nicht der Fall, ist Ihre Konfiguration nicht korrekt oder Ihr Netzwerk blockiert ausgehende Verbindungen. In jedem Fall müssen Sie Ihr Haupt-Gateway erreichen können. Dies können Sie mit dem Befehl ping überprüfen (mit unserem Beispiel-Gateway):

```
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) Bytes Daten.
64 Bytes von 192.168.1.1: icmp_seq=1 ttl=64 Zeit=6,43 ms
64 Bytes von 192.168.1.1: icmp_seq=2 ttl=64 Zeit=6,43 ms
64 Bytes von 192.168.1.1: icmp_seq=3 ttl=64 Zeit=6,45 ms
^C
--- 192.168.1.1 Ping-Statistik ---
3 Pakete gesendet, 3 empfangen, 0 % Paketverlust, Zeit 2004 ms rtt
min/avg/max/mdev = 6,425/6,434/6,453/0,013 ms
```

Oder Traceroute:

```
traceroute 192.168.1.1
Traceroute zu 192.168.1.1 (192.168.1.1), max. 30 Hops, 38-Byte-Pakete
1 192.168.1.1 (192.168.1.1) 6,357 ms 6,380 ms 6,324 ms
```

Wenn Sie keinen Zugriff auf das Gateway haben, überprüfen Sie Ihre Netzwerkparameter und stellen Sie sicher, dass Sie Ihre Verbindung neu geladen haben.

Wenn Sie Zugriff auf das Gateway haben, wenden Sie sich an Ihren IT-Support, um beispielsweise zu überprüfen, ob ausgehende Verbindungen für Ihr Gerät autorisiert sind.

Wenn alles funktioniert, können Sie nun über SSH und die Webschnittstelle, die in den nächsten Kapiteln standardmäßig verwendet wird, auf Ihr Gateway zugreifen.

7.2 SICHERHEIT

7.2.1 PASSWORT

Einer der ersten Schritte nach der Anmeldung im Webinterface ist die Änderung des Administratorpassworts. Sofern Sie Ihr Gateway nicht für Entwicklungszwecke in einem kontrollierten Netzwerk verwenden, handelt es sich hierbei um eine grundlegende Sicherheitsempfehlung, mit der sich offensichtlich einfache Angriffe verhindern lassen.

Um es zu ändern, klicken Sie auf den Benutzer (oben rechts in der Weboberfläche) „-> -Einstellungen“:

Geben Sie das aktuelle Passwort und zweimal das neue Passwort ein und klicken Sie auf die Schaltfläche „Speichern“. Sie erhalten dann eine Benachrichtigung, die bestätigt, dass das Passwort geändert wurde.

7.2.2 SSL-ZERTIFIKAT

Über die Weboberfläche können Sie ein Zertifikat aus den allgemeinen Einstellungen lesen, definieren oder generieren. Klicken Sie oben rechts auf die Schaltfläche mit den drei Punkten -> Einstellungen.

7.2.2.1 AKTUELLES ZERTIFIKAT LESEN/HERUNTERLADEN

Auf dieser Seite finden Sie links das aktuelle Zertifikat:

Active certificate

Certificate details
LORIX One
Expired 25 days ago

Common name	LORIX One
Organization	
Location	
Valid from	20/10/2021, 15:58:08
Valid to	19/11/2021, 14:58:08
Issuer	Self-signed (Certification Authority)
Serial number	0E:15:14:17:22:7C:A9:38:40:2A:83:52:2E:FB:1A:C7:33:3D:48:39

CERTIFICATE
 PUBLIC KEY

Sie können dieses Zertifikat beispielsweise Ihrem Webbrowser hinzufügen, um dieses Gerät ausdrücklich als bekannt zu erkennen und die Sicherheitswarnung zu vermeiden.

Bitte konsultieren Sie dazu direkt die Dokumentation Ihres Browsers.

Anfängliche Gültigkeit des Zertifikats

Standardmäßig ist das beim ersten Start generierte Erstzertifikat nur 30 Tage lang gültig. Um diese Gültigkeitsdauer zu verlängern, müssen Sie über die Weboberfläche ein neues Zertifikat generieren oder eines aus Ihrer eigenen PKI importieren.

7.2.2.2 ZERTIFIKAT GENERIEREN

Change certificate

[UPLOAD](#)
[GENERATE](#)

Generate your own self-signed certificate and key.

Parameters

Validity duration
30 days

Key passphrase

Valid domains

Certificate details

Common name
LORIX One ✕
9 / 64

E-mail address

Organization
0 / 64

Organizational unit
0 / 64

Locality

State or province

Country code
0 / 2

GENERATE

! You need to restart the Manager daemon to make the certificate change effective.

Der Zertifikatsgenerator bietet Ihnen beispielsweise die Möglichkeit, ein eigenes Zertifikat mit einer benutzerdefinierten Gültigkeitsdauer zu erstellen.

Wenn Sie keine Stammzertifizierungsstelle haben, von der Sie ein Gerätezertifikat erstellen und ableiten können, ist dies eine gute Lösung, um ein benutzerdefiniertes Zertifikat zu erstellen, das Sie sofort zum Zertifikatsspeicher Ihres Browsers hinzufügen können und das später sicherstellt, dass das Gerät bekannt und vertrauenswürdig ist.

Zwischenlösung

Diese Lösung erfordert weder eine PKI noch eine Stammzertifizierungsstelle auf Ihrer Seite, aber Sie müssen das Zertifikat des Geräts auf jedem Computer hinzufügen, der auf das Gerät zugreift, um Sicherheitswarnungen und potenzielle Sicherheitsprobleme zu vermeiden.

7.2.2.3 VORHANDENES ZERTIFIKAT HOCHLADEN

Change certificate

[UPLOAD](#)
[GENERATE](#)

Upload your own valid certificate to authenticate your gateway trustfully.

Certificate
DER or PEM encoding

Private Key
DER or PEM encoding

UPLOAD

! You need to restart the Manager daemon to make the certificate change effective.

Dies ist die beste Option, aber auch die anspruchsvollste. Wenn Sie sicherstellen möchten, dass alle Ihre Geräte vertrauenswürdig sind und gleichzeitig die Konfiguration für Ihre Mitarbeiter so einfach wie möglich halten möchten, können Sie für jedes Gerät ein eigenes Zertifikat erstellen, das von Ihrer Stammzertifizierungsstelle abgeleitet ist.

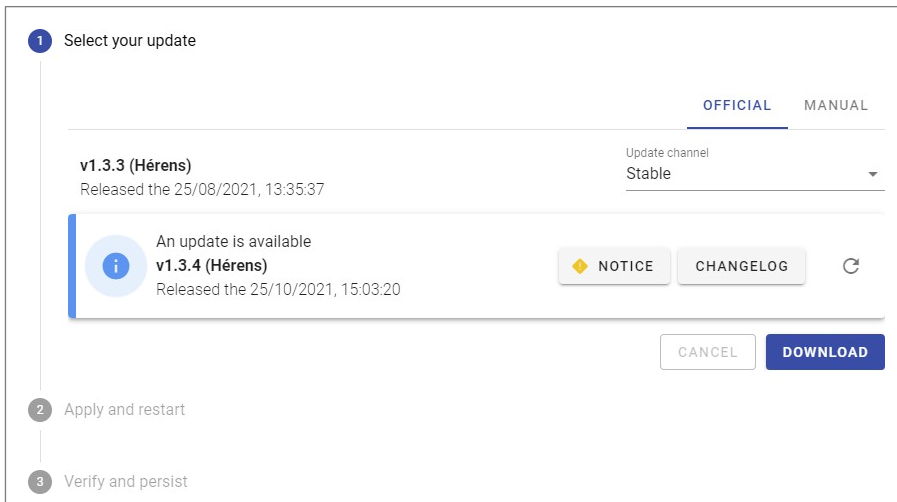
Anschließend können Sie Ihr öffentliches Stammzertifikat zum Zertifikatsspeicher des Browsers hinzufügen und jedes Gerätezertifikat bei der Erstkonfiguration über die Webschnittstelle auf das Gerät hochladen.

Auf diese Weise können Sie sicher sein, dass das Gerät, auf das Sie zugreifen, bekannt und vertrauenswürdig ist, aber auch für Ihre Mitarbeiter und unter Verwendung einer Vertrauenskette.

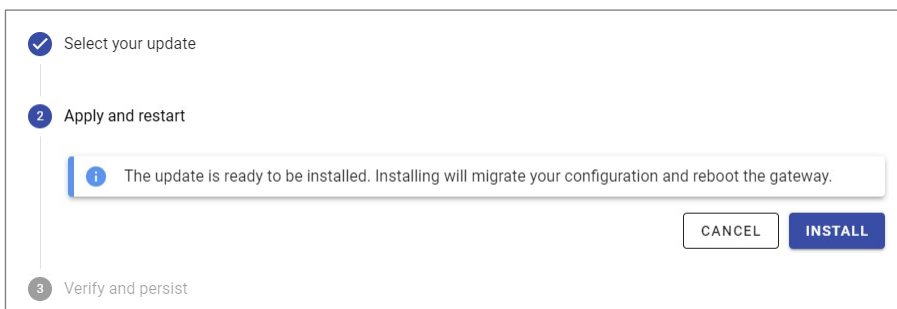
7.3 SYSTEMAKTUALISIERUNG

Die Netzwerk- und Sicherheitsaspekte wurden definiert. Vor der konkreten Nutzung des Produkts empfehlen wir, es auf die neueste verfügbare Systemversion zu aktualisieren.

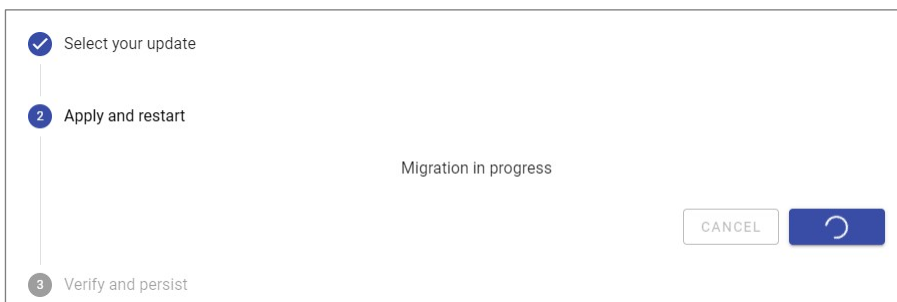
Gehen Sie dazu in die System→ -Update und überprüfen Sie, ob eine neue Version verfügbar ist:



Bildschirm „Heruntergeladenes Image“:



Das Image kann nun auf das Gateway geflasht werden. Klicken Sie auf „Installieren“ und warten Sie, bis das Update abgeschlossen ist:

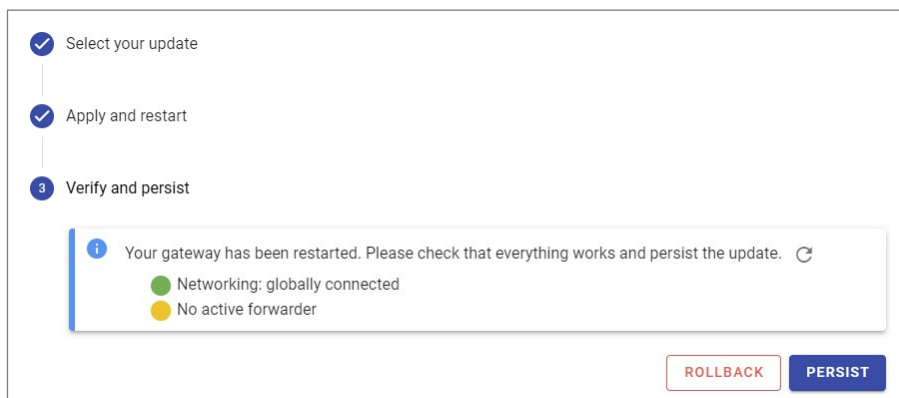




Während des Neustarts wird die Verbindung unterbrochen.

Wiederherstellung der Schnittstellenverbindung

Die Verbindung sollte nach 3-4 Minuten automatisch wiederhergestellt werden. Ist dies nicht der Fall, können Sie versuchen, die Seite zu aktualisieren und den Cache mit dem Befehl STRG+F5 zu löschen.



Sie sind fertig und das System wurde erfolgreich aktualisiert. Um diese neue Version zu bestätigen, klicken Sie auf die Schaltfläche „Beibehalten“.

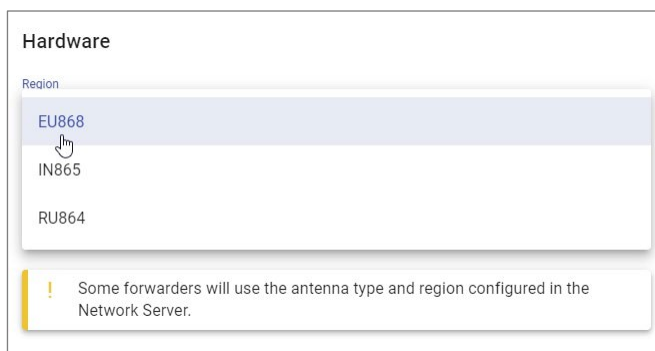
7.4 LORA/LoRAWAN-KONFIGURATION

7.4.1 LORA (RF)

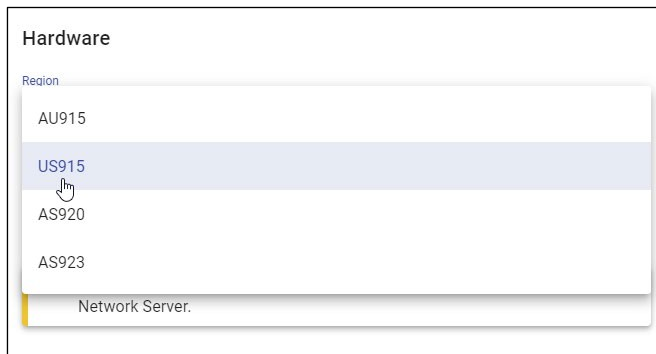
Bevor Sie den LoRaWAN-Forwarder verwenden können, müssen Sie die Region und die Antenne konfigurieren. Gehen Sie dazu in die LoRa

→ Einstellungen und legen Sie die Region und die Antenne fest.

7.4.1.1 8XX REGION



7.4.1.2 9XX REGION

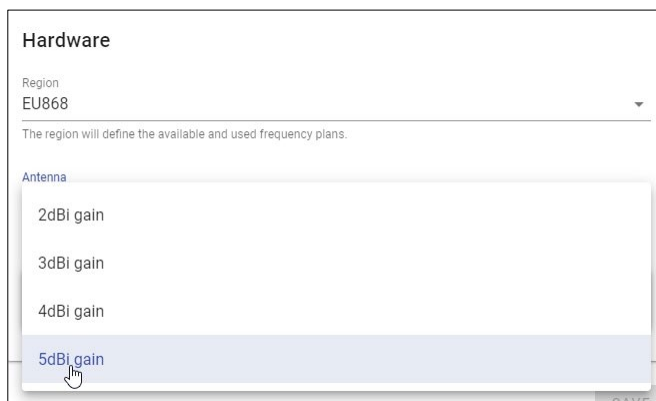


The screenshot shows a web interface titled "Hardware". Below the title is a "Region" dropdown menu. The menu is open, showing a list of options: AU915, US915 (highlighted with a mouse cursor), AS920, and AS923. Below the dropdown, there is a "Network Server" field.

Spezifische regionale Vorschriften

Achten Sie darauf, keine Region zu konfigurieren, die nicht Ihren lokalen Vorschriften entspricht. Beispielsweise verwendet US915 das Frequenzband 902–928 MHz, während in Australien nur 915–928 MHz zugelassen ist.

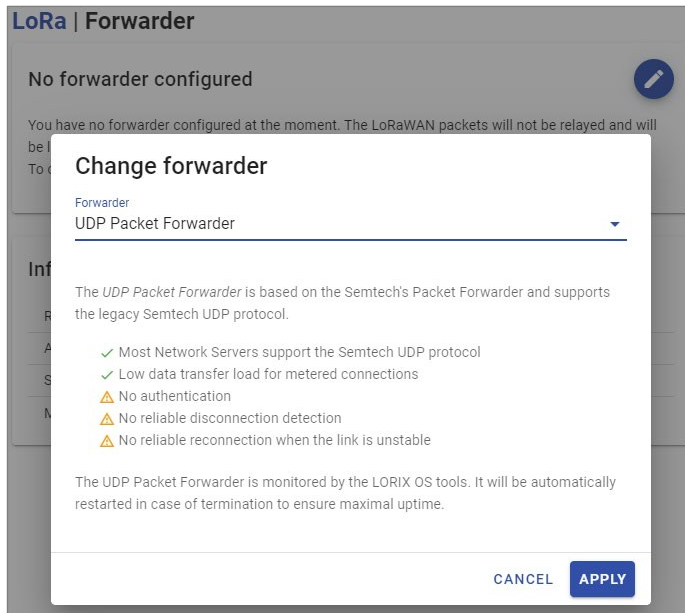
7.4.1.3 ANTENNEN



The screenshot shows a web interface titled "Hardware". Below the title is a "Region" dropdown menu set to "EU868". Below this is a note: "The region will define the available and used frequency plans." Underneath is an "Antenna" dropdown menu. The menu is open, showing a list of options: 2dBi gain, 3dBi gain, 4dBi gain, and 5dBi gain (highlighted with a mouse cursor). At the bottom right of the interface, there is a "SAVE" button.

7.4.2 LORAWAN

Sobald die HF-Basis korrekt konfiguriert ist, können Sie unter „LoRaWAN Forwarder“ Ihren bevorzugten Forwarder auswählen:



Durch Klicken auf die rechte blaue Schaltfläche öffnet sich ein modales Fenster, in dem die verschiedenen Forwarder angezeigt und die Vor- und Nachteile der einzelnen Lösungen kurz beschrieben werden.

Die Konfiguration der einzelnen Forwarder wird hier nicht beschrieben, sondern ist unter <https://iot.wifx.net/docs/go/forwarding> zu finden.

7.4.3 GWID-FORMAT

Die Gateway-ID ist eine 64-Bit-Eindeutigkeits-ID, die auf der 48-Bit-Eindeutigkeits-MAC-Adresse basiert. Die erweiterte 64-Bit-Adresse wird einfach durch Entfernen des „:“ aus der MAC-Adresse und Hinzufügen der 2 Bytes 0xFF und 0xFE zwischen dem 3- und 4- Byte erstellt.

Das Format der Gateway-ID (GWID) lautet wie folgt:



Nach diesem Vorgang wird die MAC-Adresse **01:00:5E:22:BB:33** zur Gateway-ID **01005EFFFE22BB33**. Die Gateway-ID hat in einigen Clouds auch die Form `eui-<Gateway-ID>`. In diesem Fall wäre das `eui-01005efffe22bb33`.

8 ELEKTRISCH

8.1 STROMVERBRAUCH

Aufgabe (bei 20 °C Umgebungstemperatur)	Spannung [V]	Strom [mA]	Leistung [W]
Nur Linux läuft, RF-Teil deaktiviert	24	42	1,01
LoRa-Gateway mit util_pkt_logger 6 Kanäle für RX	24	105	2,52
LoRa-Gateway mit util_pkt_logger 8 Kanäle für RX	24	117	2,81

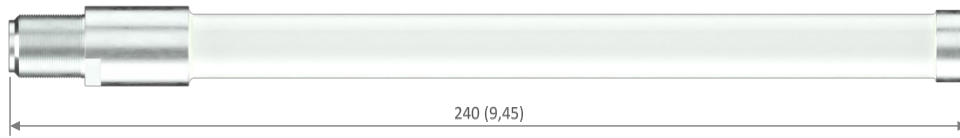
9 MECHANISCH

9.1 LORIX ONE



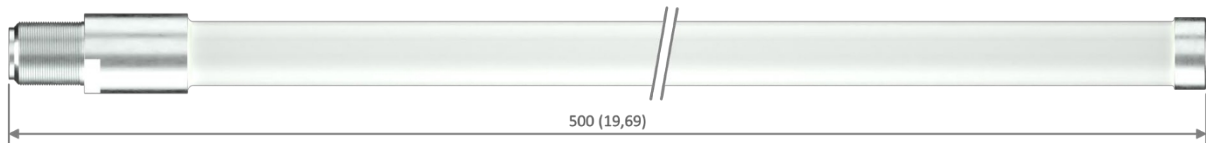
9.2 ANTENNE 3 dBi (VERSIONEN 8XX & 9XX)

Abmessungen in mm (Zoll)



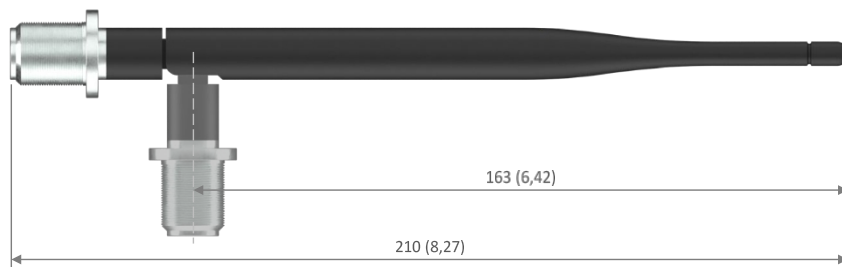
9.3 ANTENNE 5 dBi (VERSIONEN 8XX UND 9XX)

Abmessungen in mm (Zoll)



9.4 ANTENNE 2,15 dBi (VERSIONEN 8XX)

Abmessungen in mm (Zoll)



10 EINRICHTUNGSANLEITUNG

10.1 ALLGEMEINE EMPFEHLUNGEN

Das LORIX One-Gateway ist für die **vertikale** Aufstellung mit **nach oben** gerichteter Antenne ausgelegt.

Wenn Sie das LORIX One an einem Mast befestigen möchten, wird dringend empfohlen, die mit dem Gateway mitgelieferten UV-beständigen Kunststoff-Befestigungsschlaufen zu verwenden. Führen Sie die Schlaufen durch die Markierungen an den Kanten des LORIX One und befestigen Sie das Gateway an der Stelle des Mastes, an der es montiert werden soll.

Es wird dringend empfohlen, kein loses Ethernet-Kabel an den Ethernet-Anschluss anzuschließen, während das Gateway an einem Mast befestigt wird, um eine zusätzliche Belastung des Anschlusses zu vermeiden. Idealerweise sollte das Ethernet-Kabel in einem Abstand von maximal 2 Metern vom Gateway-Gerät angeschlossen werden.

10.2 STANDARDMONTAGE MIT EINEM MAST



Entfernen Sie die Kabeldurchführung aus der Kappe.



Sobald das Ethernet-Kabel durch die Öffnung in der Kappe geführt wurde, öffnen Sie diese. die Silikondichtung und legen Sie sie wie auf dem Bild gezeigt um das Kabel.

Achten Sie auf die Ausrichtung der Tülle.



Drücken Sie die Tülle mit dem Finger von innen gegen die Kappe (linkes Bild), bis sie ihre endgültige Position erreicht hat (rechtes Bild).



Schließen Sie das Ethernet-Kabel an.



Bewegen Sie die Kappe in Richtung des Gehäuses, während Sie das Kabel mit der anderen Hand festhalten, damit es so gerade wie möglich bleibt.



Schrauben Sie die Kappe auf das Gehäuse, um einen möglichst guten Schutz vor Wasser und Staub zu gewährleisten.

Nach der Befestigung sicherstellen, dass das Kabel gut platziert ist und die Tülle korrekt sitzt.



Verwenden Sie nur die für den LORIX One als Zubehör mitgelieferte Antenne.



Stecken Sie den Antennenstecker wie auf dem Bild gezeigt in den RF-Anschluss des LORIX One.

Halten Sie die Antenne am LORIX One fest und schrauben Sie mit der anderen Hand den RF-LORIX One-Anschluss-Klemmring fest.



Drehen oder verwenden Sie niemals direkt den Antennenkörper, um ihn am LORIX One anzuschrauben, da dies die Antenne beschädigen oder zerbrechen könnte.



Sobald das Kabel und die Antenne korrekt angeschlossen und der LORIX One korrekt geschlossen sind, können Sie ihn mit den 2 mitgelieferten Kabelbindern an einem Mast befestigen.

Die mitgelieferten Kabelbinder sind schwarz, da sie speziell für UV-Beständigkeit hergestellt wurden.

Verwenden Sie immer die mitgelieferten Kabelbinder oder speziell UV-geschützte Kabelbinder.



Sobald der LORIX One richtig ausgerichtet und der Kabelbinder fest angezogen ist, schneiden Sie den überstehenden Kunststoffteil des Kabelbinders mit einer Schneidezange ab.



Der LORIX One ist nun mit den mitgelieferten Elementen (außer dem Ethernet-Kabel) an einem Mast installiert.

Es wird dringend empfohlen, kein loses Ethernet-Kabel an den Ethernet-Anschluss anzuschließen, während Sie das Gateway an einem Mast befestigen, um das Gewicht des Anschlusses nicht zu erhöhen. Idealerweise sollte das Ethernet-Kabel innerhalb von 2 Metern vom Gateway-Gerät angeschlossen werden.

Verwenden Sie auf der anderen Seite des Kabels den mit dem LORIX One mitgelieferten passiven PoE-Injektor, wie in Kapitel 5.1 „Stromversorgung über passives PoE“ beschrieben.

Sobald das LORIX One korrekt installiert ist, lesen Sie das Kapitel 6 „Servicezugang“, um auf das Gerät zuzugreifen und die Erstkonfiguration durchzuführen.