

Haftungsausschluss

Rechtlicher Hinweis

Dieser Leitfaden und seine Inhalte (der „Leitfaden“) werden von NXGEN bereitgestellt. Alle Rechte am Leitfaden und am darin verkörperten geistigen Eigentum — einschließlich, aber nicht beschränkt auf Marken, Handelsnamen, Logos und ähnliche Kennzeichen im oder am Leitfaden — sind gesetzlich geschützt. Sämtliche Rechte, Ansprüche und Anteile am Leitfaden und an damit verbundenen Schutzrechten verbleiben bei NXGEN und seinen Lizenzgebern.

Der Leitfaden wird unentgeltlich, „wie besehen“ und ausschließlich zu Informationszwecken bereitgestellt, ohne jegliche Gewährleistung. Er ist weder dazu bestimmt noch geeignet, ein Rechtsverhältnis zwischen dem Leser und NXGEN oder seinen verbundenen Unternehmen zu begründen, einschließlich, aber nicht beschränkt auf Verpflichtungen von NXGEN oder seinen verbundenen Unternehmen gegenüber dem Leser.

Die Verpflichtungen von NXGEN und seinen verbundenen Unternehmen in Bezug auf von einem Kunden erworbene NXGEN-Produkte oder -Dienstleistungen richten sich ausschließlich nach den Bedingungen des Vertrags, unter dem diese Produkte oder Dienstleistungen erworben wurden.

Zur Klarstellung

Der Leser trägt das gesamte Risiko hinsichtlich der Nutzung, der Ergebnisse und der Leistung des Leitfadens. Soweit gesetzlich zulässig, schließt NXGEN alle Gewährleistungen aus, ob gesetzlich, ausdrücklich oder stillschweigend — einschließlich, aber nicht beschränkt auf stillschweigende Gewährleistungen der Marktgängigkeit, der Eignung für einen bestimmten Zweck, des Rechtsbestands und der Nichtverletzung von Rechten Dritter — sowie jegliche Haftung oder Gewährleistung aus Vorschlägen, Spezifikationen oder Mustern im Zusammenhang mit dem Leitfaden.

Teltonika

Updated 11 August 2026

Einführung

Teltonika-IoT-Router dienen als Konnektivitäts-Backbone für die GCXONE-Tower-Überwachung und bieten Echtzeit-Mobilfunkstatus, GPS-Tracking, I/O-Statusänderungen und Signalqualitätsdaten von entfernten Tower-Standorten. Dieser Leitfaden führt Sie durch den gesamten Onboarding-Prozess für einen Teltonika-IoT-Router – vom Hinzufügen des Geräts in GCXONE und der Eingabe der erforderlichen Anmeldeinformationen bis hin zur Konfiguration von Alarmregeln für Netzwerkverlust, Geo-Fencing, SIM-Datennutzung und Störsendererkennung.

What Teltonika Geräte Monitor

Once connected to GCXONE, Teltonika routers continuously report the following categories of telemetry:

- Network connectivity status and signal quality (RSRQ, RSRP)
- SIM card data usage against configured monthly limits
- Physical input/output (I/O) port state changes — digital, analog, isolated, relay
- GPS position relative to the assigned site boundary (geo-fencing)
- Jammer detection based on sudden signal degradation patterns

Tip

Teltonika kümmert sich um die Kommunikation, GPS-Verfolgung und Edge-Telemetrie-Routing für den Turm. Dies macht es zum Rückgrat der Konnektivitätsüberwachung – ohne es kann GCXONE Netzwerkausfälle, Signalstörungen oder unbefugte Gerätebewegungen nicht erkennen.

Voraussetzungen

Stellen Sie vor Beginn des Geräte-Onboardings sicher, dass die folgenden Informationen und

Zugriffsrechte verfügbar sind:

REQUIREMENT	DETAILS
GCXONE Access	Admin or Operator role with Configuration module access
Device Credentials	Administrative username and password for the Teltonika router
IP Address	Public or VPN-accessible IP address of the Teltonika device
Serial Number	The unique hardware serial number of the router
Control Port	HTTP port used for device communication (e.g.
Site Created	The site this device will be assigned to must already exist in GCXONE

Caution

Stellen Sie sicher, dass der Teltonika-Router online und vom GCXONE-Server aus erreichbar ist (direkte IP oder über VPN) und dass die angegebenen Administratoranmeldeinformationen über vollständigen API-Zugriff verfügen.

Teltonika Config Guide with GCX-ONE

Befolgen Sie diese Schritte, um einen Teltonika IoT-Router zu GCXONE hinzuzufügen. Das Gerät wird unter einer vorhandenen Site registriert und beginnt sofort nach der Konfiguration mit der Meldung von Telemetriedaten.

Schritt 1 — Navigate to the Site

Navigieren Sie in GCXONE zu der Site, auf der das Teltonika-Gerät physisch installiert ist. Dies ist die übergeordnete Entität, unter der das Gerät registriert wird.

- Go to Konfiguration → Standorte

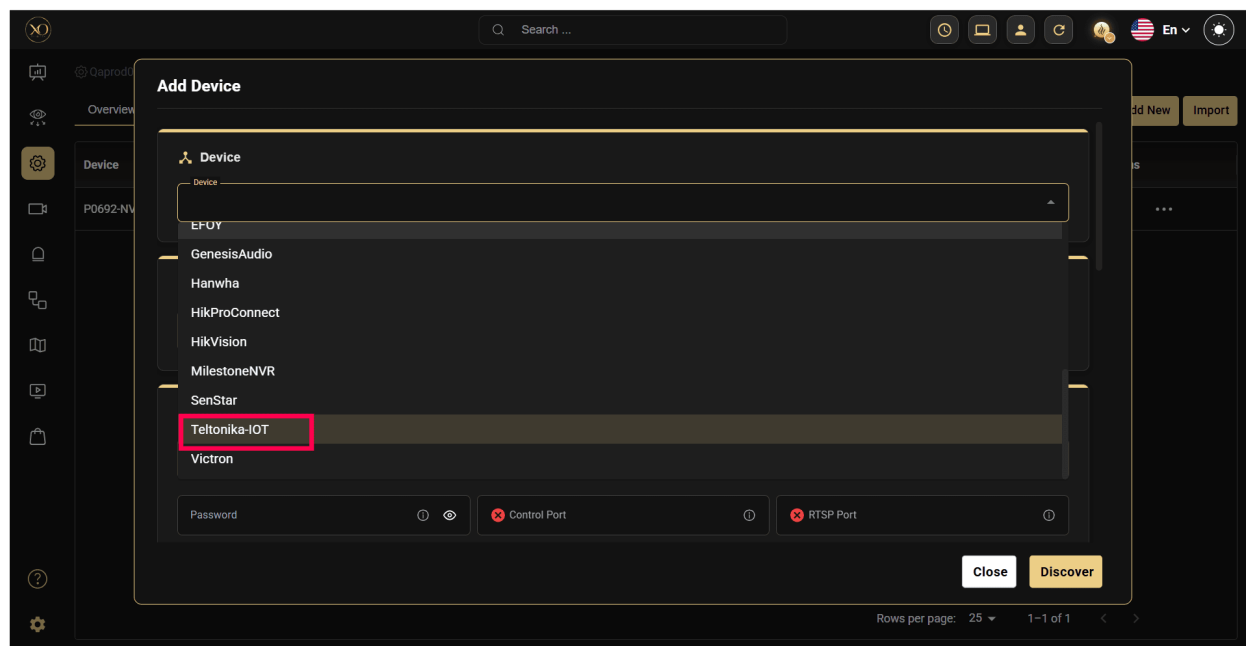
- Locate and open the target site
- Klicken Sie auf Bearbeiten, um das Konfigurationsfenster der Site zu öffnen

Schritt 2 — Open the Device Dialog

Navigieren Sie in der Site-Konfiguration zum Abschnitt „Geräte“ und klicken Sie auf „Gerät hinzufügen“, um den Dialog zur Geräteerstellung zu öffnen.

Schritt 3 — Select Device Typ

Öffnen Sie im Gerätedialog das Dropdown-Menü „Gerätetyp“ und wählen Sie Teltonika IoT aus, um die entsprechenden Konfigurationsfelder zu laden.



Victron

Schritt 4 — Enter Device Details

Füllen Sie alle erforderlichen Felder aus, um eine sichere Verbindung zwischen GCXONE und dem Teltonika-Router herzustellen. Jedes Feld wird im Folgenden ausführlich beschrieben.

Victron

FIELD	DESCRIPTION	NOTES
Device Type	Select 'Teltonika IoT' from the dropdown	Must match exactly — determines which telemetry model is used
Device Name	A unique	descriptive name for this device in GCXONE
IP Address	Public or VPN-accessible IP address of the Teltonika router	Must be reachable from the GCXONE server; use VPN if the device is behind NAT
Serial Number	The hardware serial number printed on the router	Found on the device label or in the Teltonika device management portal
Control Port	HTTP port for device communication	Default is typically port 80; confirm with your network configuration
Username	Administrative login username for the router	Must have full access to all device parameters and APIs
Password	Administrative login password for the router	Stored securely within GCXONE; use a strong

Schritt 5 — Speichern and Verify Connection

Nachdem Sie alle Felder ausgefüllt haben, klicken Sie auf Speichern. GCXONE wird sofort versuchen, mit den bereitgestellten Anmeldeinformationen eine Verbindung mit dem Teltonika-Router herzustellen.

A successful connection results in:

- Das Gerät erscheint in der Geräteliste der Site mit einer aktiven Statusanzeige
- Live-Telemetriedaten beginnen in GCXONE einzufließen (Signalstärke, Netzwerkstatus, I/O-Zustände)
- Das Gerät wird für die Alarmregelkonfiguration verfügbar

Caution

Wenn die Verbindung fehlschlägt, überprüfen Sie, ob die IP-Adresse erreichbar, der Port offen und die Anmeldeinformationen korrekt sind. Stellen Sie sicher, dass keine Firewall-Regeln den Zugriff von GCXONE auf das Gerät blockieren

Alarm Rules Konfiguration

GCXONE verwendet eine JSON-basierte Alarmregelkonfiguration, um zu definieren, welche Telemetrieparameter überwacht werden, welche Schwellenwerte Warnungen auslösen und wie diese Warnungen in CMS-Integrationen identifiziert werden.

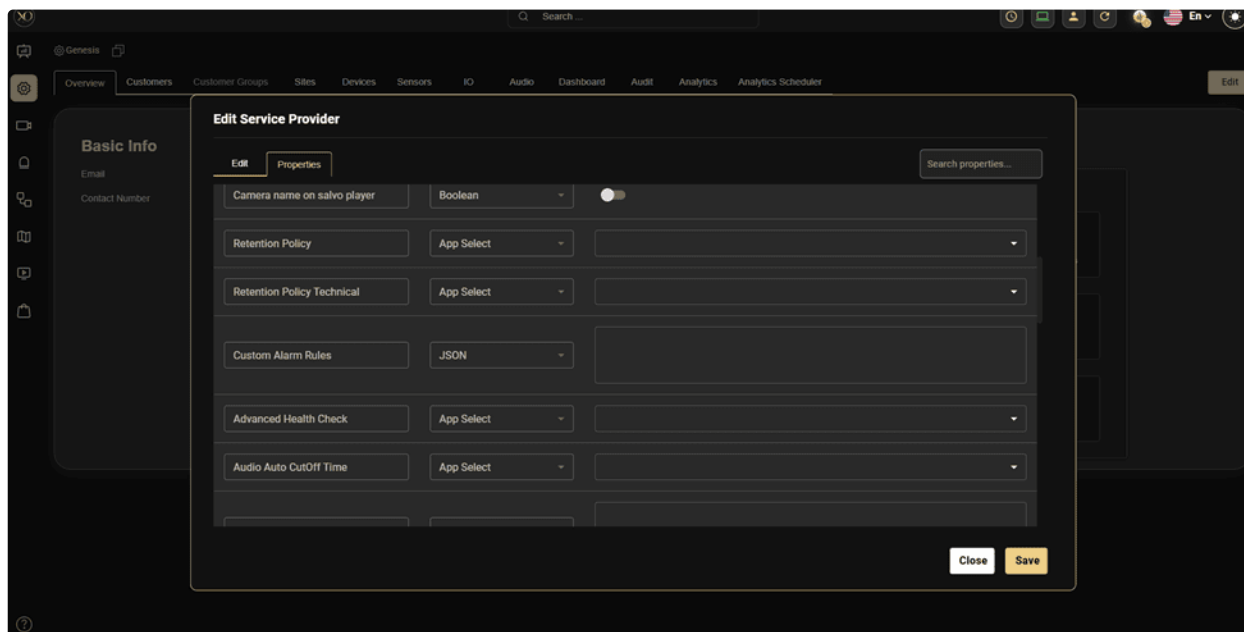
Alarmregeln können auf Standortebene oder Geräteebene konfiguriert werden.

Teltonika-Konnektivitätsregeln werden zur präzisen Steuerung normalerweise auf Geräteebene angewendet.

How to Apply Alarm Rules

1. Navigieren Sie in GCXONE zur Zielsite oder zum Zielgerät.
2. Klicken Sie auf Bearbeiten und gehen Sie zum Abschnitt Zusätzliche Eigenschaften.
3. Locate the property named Custom Alarm Rules.
4. Öffnen Sie das Hamburger-Menü der Eigenschaft (:) und wählen Sie „Standard anwenden“, um den vorkonfigurierten Regelsatz zu laden. Alle Regeln sind standardmäßig inaktiv.

5. Ändern Sie den JSON, um bestimmte Regeln zu aktivieren, indem Sie für die relevanten Parameter „active“: true festlegen.
6. Legen Sie Ihre Schwellenwerte, Ereigniscodes und Gruppencodes nach Bedarf fest.
7. Klicken Sie auf Speichern. GCXONE beginnt sofort mit der Bewertung eingehender Telemetriedaten anhand der konfigurierten Regeln.



Victron

Tipp

Standardmäßig sind alle Alarmregeln inaktiv. Sie müssen für jede Regel, die GCXONE überwachen soll, explizit „active“: true festlegen. Dies verhindert versehentliche Warnungen während der Ersteinrichtung.

Rule Structure

Jede Alarmregel folgt einer konsistenten JSON-Struktur. Das Verständnis der allgemeinen Felder hilft beim Anpassen von Regeln:

FIELD	DESCRIPTION

active	Boolean (true/false). Set to true to enable monitoring for this rule. When false
eventCode	Unique string identifier used by GCXONE to communicate this alarm type to CMS integrations (IMMIX
groupCode	Logical grouping identifier for Tower Monitoring workflows. Used for filtering

Tip

Ereigniscodes werden für systemübergreifende CMS-Benachrichtigungen verwendet (z. B. IMMIX, Evalink). Gruppencodes sind GCXONE-interne Kennungen für Tower-Alarm-Workflows. Für eine vollständige Integration müssen beide vorhanden sein.

Teltonika Connectivity Alarm Rules

Die folgenden Alarmregeln sind für Teltonika-IoT-Geräte im Abschnitt „Konnektivitätsüberwachung“ der benutzerdefinierten Alarmregeln-JSON verfügbar. Jede Regel überwacht einen bestimmten Aspekt des Netzwerkzustands, der physischen E/A oder der Sicherheit.

1. Input/Output Status Change Rule

Überwacht physische Zustandsänderungen an Teltonika-E/A-Ports. Diese Regel gilt für digitale, analoge, isolierte und Relaiseingänge und -ausgänge – wichtig für die Erkennung von Türöffnungen, Stromereignissen, externen Sensorauslösungen und Gerätezustandsänderungen.

Standard JSON Konfiguration

```
"IOStatusChange": {
  "input": {
    "AnalogCurrentLoop": {"active": false, "low": 4, "high": 20},
    "AnalogInput": {"active": false, "low": 11, "high": 14},
```

```

"DigitalInput": {"active": false, "ranges": ["Low level", "High level"],
"alertOn": "High Level"},

"IsolatedInput": {"active": false, "ranges": ["Low level", "High level"],
"alertOn": "High Level"},

"PowerSocketInput": {"active": false, "ranges": ["Low level", "High level"],
"alertOn": "High Level"},

"eventCode": "input.statechange",
"groupCode": "tower.input.statechange"
},

"output": {
"IsolatedOutput": {"active": false, "ranges": ["Low level", "High level"],
"alertOn": "High Level"},

"Relay": {"active": false, "ranges": ["open", "closed"], "alertOn": "open"},
"PowerSocketOutput": {"active": false, "ranges": ["Low level", "High level"],
"alertOn": "High Level"},

"eventCode": "output.statechange",
"groupCode": "tower.output.statechange"
}
} Input Types

```

INPUT TYPE

DESCRIPTION AND PARAMETERS

AnalogCurrentLoop	Monitors 4–20 mA current loop sensors. Set low/high to the acceptable current range. Alerts when current falls outside this range.
AnalogInput	Monitors analog voltage inputs (e.g.
DigitalInput	Binary state monitoring. Set alertOn to the state that should trigger an alarm (e.g.
IsolatedInput	Electrically isolated digital input. Same configuration as DigitalInput. Used when isolation from the main circuit is required.
PowerSocketInput	Monitors power socket state (Low/High level). Set alertOn to the triggering state. Suitable for mains power detection.

Output Types

OUTPUT TYPE	DESCRIPTION AND PARAMETERS
IsolatedOutput	Monitors the state of an isolated output channel. Set alertOn to 'High Level' to alert when the output is active.
Relay	Tracks relay state (open/closed). Set alertOn to 'open' to alert when the relay is not energized. Useful for contactor or lock monitoring.
PowerSocketOutput	Monitors power socket output state. Alert when the output reaches the configured alertOn state.

2. SIM Card Data Package Usage Rule

Verfolgt den monatlichen mobilen Datenverbrauch für die SIM-Karte des Teltonika-Routers.

Löst eine Warnung aus, wenn die Datennutzung den konfigurierten Prozentsatz des monatlichen Gesamtkontingents erreicht – so werden unerwartete Überschreitungsgebühren oder Dienstunterbrechungen verhindert.

Standard JSON Konfiguration

```
"simCardDataPackage": { "active": false, "simBillingStartDate": 1, "simDataPackageGB": 10, "usageWarningPercent": 80, "eventCode": "sim.data.usage.warning", "groupCode": "tower.connectivity.simdata.alert"}
```

Konfiguration Parameters

PARAMETER NAME	DESCRIPTION	EXAMPLE VALUE
simBillingStartDate	Billing cycle start date of the SIM plan (currently inactive)	1
simDataPackageGB	Total mobile data allocated per month (in GB)	10
usageWarningPercent	Warning threshold as a percentage of total data usage	80
eventCode	CMS alarm identifier for this event type	sim.data.usage.warning
groupCode	Internal tower alarm group for filtering and routing	tower.connectivity.simdata.alert

Example Behavior

- Wenn „simDataPackageGB“ auf 10 und „usageWarningPercent“ auf 80 eingestellt ist, löst GCXONE eine Warnung aus, wenn die kumulierte SIM-Datennutzung im Abrechnungszeitraum 8 GB überschreitet.
- Die Warnung wird automatisch gelöscht, wenn die Datennutzung zu Beginn des neuen Abrechnungszeitraums zurückgesetzt wird.
- Passen Sie den Schwellenwert für die Frühwarnung auf Websites mit begrenzten Konnektivitätsalternativen niedriger an (z. B. 70 %).

3. Cellular Network Loss Rule

Erkennt, wenn der Teltonika-Router die Verbindung zum Mobilfunknetz verliert oder das Signal auf ein inakzeptables Niveau abfällt. Warnt Bediener sofort vor möglichen Kommunikationsausfällen vor Ort.

Standard JSON Konfiguration

```
"cellNetworkLoss": {
  "active": false,
```

```
"eventCode": "modem.signal.warning",
"groupCode": "tower.connectivity.signal.alert"
}
```

Example Behavior

- GCXONE löst eine Warnung aus, wenn das Mobilfunksignal unter den akzeptablen Schwellenwert fällt oder die Konnektivität vollständig unterbrochen wird.
- Die Warnung wird automatisch gelöscht, sobald das Signal wieder ein akzeptables Niveau erreicht.
- Diese Regel hat keine Schwellenwertparameter – sie basiert auf der integrierten Signalqualitätsbewertung von GCXONE für den vom Router gemeldeten Modemstatus.

4. Geo-Fencing Rule

Überwacht die GPS-Position des Teltonika-Routers relativ zu seinem zugewiesenen Standortstandort. Löst eine Warnung aus, wenn sich das Gerät über den konfigurierten Radius hinaus bewegt – und erkennt so eine mögliche Turmverschiebung, einen Diebstahl oder eine unbefugte Bewegung.

Standard JSON Konfiguration

```
"geoFencing": {
"active": false,
"radiusMetersWarning": 500,
"eventCode": "geo.fence.breach",
"groupCode": "tower.connectivity.geofence.alert"
}
```

PARAMETER NAME	DESCRIPTION	EXAMPLE VALUE

radiusMetersWarning	Radius (in meters) from the defined geo-fence center (typically	the site's geo location) within which the tower must remain
eventCode	CMS alarm identifier for geo-fence breach events	geo.fence.breach
groupCode	Internal tower alarm group identifier	tower.connectivity.geofence.alert

Example Behavior

- Die Geo-Zaun-Grenze ist auf die Koordinaten zentriert, die in der Konfiguration des übergeordneten Standorts in GCXONE definiert sind.
- Wenn die vom Teltonika-Router gemeldete GPS-Position mehr als 500 Meter von der Standortmitte entfernt ist, wird eine Sicherheitswarnung generiert.
- Die Warnung wird automatisch gelöscht, wenn das Gerät innerhalb der definierten Grenze zurückkehrt.
- Reduzieren Sie den Radius für dauerhafte Festinstallationen; Verwenden Sie einen größeren Radius für mobile oder halbmobile Tower-Einsätze.

5. Jammer Detection Rule

Erkennt potenzielle Hochfrequenz-Störungsversuche aufgrund einer plötzlichen Signalverschlechterung und einer schlechten Referenzsignal-Empfangsqualität (RSRQ). Die Erkennung von Störsendern ist für sicherheitsrelevante Mastinstallationen von entscheidender Bedeutung, bei denen Signalstörungen auf vorsätzliche Störungsversuche hinweisen können.

Standard JSON Konfiguration

```
"jammerDetection": {
  "active": false,
  "criteria": {
    "signalDropThreshold": 25,
```

```

"minSignalLevel": -113,

"rsrqThreshold": -20

},

"eventCode": "modem.jammer.detected",

"groupCode": "tower.connectivity.jamming.alert"

}

```

PARAMETER NAME	DESCRIPTION	EXAMPLE VALUE
signalDropThreshold	Percentage drop in signal strength considered as a potential jamming event	25
minSignalLevel	Minimum acceptable signal level (in dBm); if signal goes below this	jamming is suspected
rsrqThreshold	Minimum acceptable RSRQ (Reference Signal Received Quality); poor RSRQ may indicate interference	-20
eventCode	CMS identifier for jammer detection events	modem.jammer.detected
groupCode	Tower alarm group identifier	tower.connectivity.jamming.alert

Example Behavior

- GCXONE wertet sowohl den absoluten Signalpegel (RSRQ) als auch die Signaländerungsrate (Abfallprozentsatz) aus, um echte Störungen von normalen Signalschwankungen zu unterscheiden.
- Eine Warnung wird ausgelöst, wenn der Signalabfall 25 % überschreitet ODER der RSRQ unter -20 fällt und der Signalpegel gleichzeitig unter -113 dBm liegt.
- The alert clears automatically once normal signal stability is restored.

Tip

Die Schwellenwerte für die Erkennung von Störsendern müssen möglicherweise entsprechend den örtlichen HF-Umgebungsbedingungen angepasst werden. Standorte in städtischen Gebieten mit natürlichen Signalschwankungen erfordern möglicherweise einen höheren signalDropThreshold, um Fehlalarme zu reduzieren.

Konfiguration Reference

a. Complete Teltonika Connectivity Alarm Rules JSON

Im Folgenden finden Sie die vollständige Standard-JSON-Konfiguration für alle Teltonika-Konnektivitätsalarmregeln. Kopieren Sie dies in die Eigenschaft „Benutzerdefinierte Alarmregeln“ und ändern Sie sie nach Bedarf für Ihre Bereitstellung.

```
"connectivityMonitoring": {  
  "IOStatusChange": {  
    "input": {  
      "AnalogCurrentLoop": {"active": false, "low": 4, "high": 20},  
      "AnalogInput": {"active": false, "low": 11, "high": 14},  
      "DigitalInput": {"active": false, "ranges": ["Low level", "High level"],  
        "alertOn": "High Level"},  
      "IsolatedInput": {"active": false, "ranges": ["Low level", "High level"],  
        "alertOn": "High Level"},  
      "PowerSocketInput": {"active": false, "ranges": ["Low level", "High level"],
```

```
"alertOn": "High Level"},

"eventCode": "input.statechange",

"groupCode": "tower.input.statechange"

},

"output": {

"IsolatedOutput": {"active": false, "ranges": ["Low level", "High level"],

"alertOn": "High Level"},

"Relay": {"active": false, "ranges": ["open", "closed"], "alertOn": "open"},

"PowerSocketOutput": {"active": false, "ranges": ["Low level", "High level"],

"alertOn": "High Level"},

"eventCode": "output.statechange",

"groupCode": "tower.output.statechange"

}

},

"simCardDataPackage": {

"active": false,

"simBillingStartDate": 1,

"simDataPackageGB": 10,

"usageWarningPercent": 80,
```

```
"eventCode": "sim.data.usage.warning",  
  
"groupCode": "tower.connectivity.simdata.alert"  
  
},  
  
"cellNetworkLoss": {  
  
"active": false,  
  
"eventCode": "modem.signal.warning",  
  
"groupCode": "tower.connectivity.signal.alert"  
  
},  
  
"geoFencing": {  
  
"active": false,  
  
"radiusMetersWarning": 500,  
  
"eventCode": "geo.fence.breach",  
  
"groupCode": "tower.connectivity.geofence.alert"  
  
},  
  
"jammerDetection": {  
  
"active": false,  
  
"criteria": {  
  
"signalDropThreshold": 25,  
  
"minSignalLevel": -113,
```

```
"rsrqThreshold": -20
},
"eventCode": "modem.jammer.detected",
"groupCode": "tower.connectivity.jamming.alert"
}
}
```

b. Event Codes and Group Codes Summary

Quick reference for all Teltonika connectivity event codes and group codes:

RULE	EVENT CODE	GROUP CODE
I/O Input State Change	input.statechange	tower.input.statechange
I/O Output State Change	output.statechange	tower.output.statechange
SIM Data Usage Warning	sim.data.usage.warning	tower.connectivity.simdata.alert
Cellular Network Loss	modem.signal.warning	tower.connectivity.signal.alert
Geo-Fence Breach	geo.fence.breach	tower.connectivity.geofence.alert
Jammer Detection	modem.jammer.detected	tower.connectivity.jamming.alert

c. Konfiguration Bewährte Verfahren

- Always start with Apply Standard to load the complete preconfigured rule set before making changes.
- Enable rules incrementally — start with critical rules (network loss, jammer detection) before enabling threshold-sensitive rules like I/O state changes.
- Testen Sie Alarmregeln in einer Staging-Umgebung oder auf einem einzelnen Gerät, bevor Sie sie an allen Standorten bereitstellen.
- Legen Sie „usageWarningPercent“ für SIM-Daten auf 70–80 % fest, um den Betreibern genügend Zeit zum Handeln zu geben, bevor der Plan ausgeschöpft ist.

- Verwenden Sie für Geo-Fencing an dauerhaften Standorten einen kleinen Radius (100–200 m).
Verwenden Sie für temporäre Einsätze 500 m oder mehr.
- Dokumentieren Sie Ihre Ereigniscodes und Gruppencodes in Ihrer CMS-Konfiguration, um eine korrekte Alarmweiterleitung sicherzustellen.

Fehlerbehebung

Device Won't Connect

SYMPTOM / CHECK	RESOLUTION
Connection fails immediately after Save	Verify the IP address is reachable from the GCXONE server. Try pinging the IP from the server or checking VPN connectivity.
Authentication error	Confirm the username and password are correct and have administrative access. Log in directly to the Teltonika admin interface to verify credentials.
Port-related connection failure	Check that the configured Control Port is correct and not blocked by a firewall. Default is port 80.
Device shows offline after initial connection	Check whether the Teltonika router's IP address has changed (DHCP). Consider using a static IP or DHCP reservation.

Alarm Rules Not Triggering

SYMPTOM / CHECK	RESOLUTION
No alerts received for a breached threshold	Verify the rule has "active": true in the JSON. Check that the Custom Alarm Rules JSON is valid (no syntax errors).
eventCode not appearing in CMS	Confirm the event code is configured in your CMS integration. Check the CMS channel mapping in GCXONE under the site's integration settings.
False positive alerts (too many alerts)	Adjust thresholds. For analog inputs
Geo-fence alerts for a fixed site	Verify the site's GPS coordinates in GCXONE are correctly set to the actual tower location. Increase radiusMetersWarning if GPS reporting has variance.

SIM Data Rule Not Activating

- Stellen Sie sicher, dass der Teltonika-Router SIM-Datennutzungsmetriken an GCXONE meldet.

- Verify that simDataPackageGB matches your actual SIM plan size.
- Das Feld simBillingStartDate ist derzeit inaktiv – die Datennutzungsverfolgung verwendet vorerst den Kalendermonat.

Für weitere Unterstützung wenden Sie sich an Ihren NXGEN-Vertreter oder lesen Sie den vollständigen GCXONE Tower Monitoring Konfigurationsleitfaden, der neben der Teltonika IoT-Konnektivität auch die Überwachung von Victron Energy und EFOY Fuel Cell abdeckt.