

Disclaimer

Juridische disclaimer

Deze gids en de inhoud ervan (de "Gids") worden aangeboden door NXGEN. Alle rechten op de Gids en op de daarin vervatte intellectuele eigendom — met inbegrip van, maar niet beperkt tot, merken, handelsnamen, logo's en vergelijkbare tekens in of op de Gids — worden beschermd door de wet. Alle rechten, aanspraken en belangen met betrekking tot de Gids en de bijbehorende intellectuele-eigendomsrechten berusten en blijven bij NXGEN en zijn licentiegevers.

De Gids wordt kosteloos, "zoals deze is" en uitsluitend ter informatie verstrekt, zonder enige garantie. De Gids is niet bedoeld en evenmin geschikt om enige rechtsverhouding tot stand te brengen tussen de lezer en NXGEN of zijn gelieerde ondernemingen, met inbegrip van, maar niet beperkt tot, enige verplichting van NXGEN of zijn gelieerde ondernemingen jegens de lezer.

De verplichtingen van NXGEN en zijn gelieerde ondernemingen met betrekking tot door een klant afgenomen NXGEN-producten of -diensten worden uitsluitend beheerst door de voorwaarden van de overeenkomst waaronder die producten of diensten zijn afgenomen.

Ter verduidelijking

De lezer draagt het volledige risico ten aanzien van het gebruik, de resultaten en de prestaties van de Gids. Voor zover toegestaan door het toepasselijke recht wijst NXGEN alle garanties af, hetzij wettelijk, uitdrukkelijk of stilzwijgend — met inbegrip van, maar niet beperkt tot, stilzwijgende garanties van verhandelbaarheid, geschiktheid voor een bepaald doel, eigendom en niet-inbreuk op rechten van derden — evenals iedere aansprakelijkheid of garantie die voortvloeit uit suggesties, specificaties of voorbeelden met betrekking tot de Gids.

Teltonika

Updated 14 September 2026

Introductie

Teltonika IoT-routers vormen de connectiviteitsbackbone voor GCXONE Torenmonitoring en leveren realtime cellulair status, GPS-tracking, I/O-toestandveranderingen en signaalkwaliteitsdata van afgelegen torenlocaties. Deze gids doorloopt het volledige onboarding-proces voor een Teltonika IoT-router — van het toevoegen van het apparaat in GCXONE en het invoeren van de vereiste inloggegevens, tot het configureren van alarmregels voor netwerkverlies, geo-fencing, SIM-dataverbruik en jammerdetectie.

Wat Teltonika-apparaten monitoren

Zodra de router is verbonden met GCXONE, rapporteert Teltonika continu de volgende categorieën telemetrie:

- Netwerkconnectiviteitsstatus en signaalkwaliteit (RSRQ, RSRP)
- SIM-kaartdataverbruik ten opzichte van geconfigureerde maandelijkse limieten
- Fysieke input/output (I/O)-poorttoestandveranderingen — digitaal, analoog, geïsoleerd, relais
- GPS-positie ten opzichte van de toegewezen site-grens (geo-fencing)
- Jammerdetectie op basis van plotselinge signaaldegradatiepatronen

Opmerking: Teltonika verzorgt communicatie, GPS-tracking en edge-telemetrierouting voor de toren.

Dit maakt het de backbone van connectiviteitsmonitoring — zonder Teltonika kan GCXONE geen netwerkuitval, signaalinterferentie of ongeautoriseerde apparaatbeweging detecteren.

Voorvereisten

Zorg ervoor dat de volgende informatie en toegangsrechten beschikbaar zijn voordat u begint met het onboarden van het apparaat:

VereisteDetailsGCXONE-toegangBeheerders- of Operator-rol met toegang tot de Configuratiemodule-Apparaat-referentiesAdministratieve gebruikersnaam en wachtwoord voor de Teltonika-router-IP-adresPubliek of via VPN toegankelijk IP-adres van het Teltonika-apparaatSerienummerHet unieke hardware-serienummer van de routeControl PoortHTTP-poort die wordt gebruikt voor apparaatcommunicatie (standaardpoort 80)Site gemaaktDe site waaraan dit apparaat wordt toegewezen moet reeds bestaan in GCXONE

Belangrijk: Zorg ervoor dat de Teltonika-router online is, bereikbaar vanaf de GCXONE-server (direct IP of via VPN), en dat de opgegeven administratieve inloggegevens volledige API-toegang hebben.

Teltonika Configuratie-gids met GCXONE

Volg deze stappen om een Teltonika IoT-router toe te voegen aan GCXONE. Het apparaat wordt geregistreerd onder een bestaande site en begint direct met het rapporteren van telemetrie na configuratie.

Stap 1: Navigeer naar de Site

In GCXONE navigeert u naar de Site waar het Teltonika-apparaat fysiek is geïnstalleerd. Dit is de bovenliggende entiteit waaronder het apparaat wordt geregistreerd.

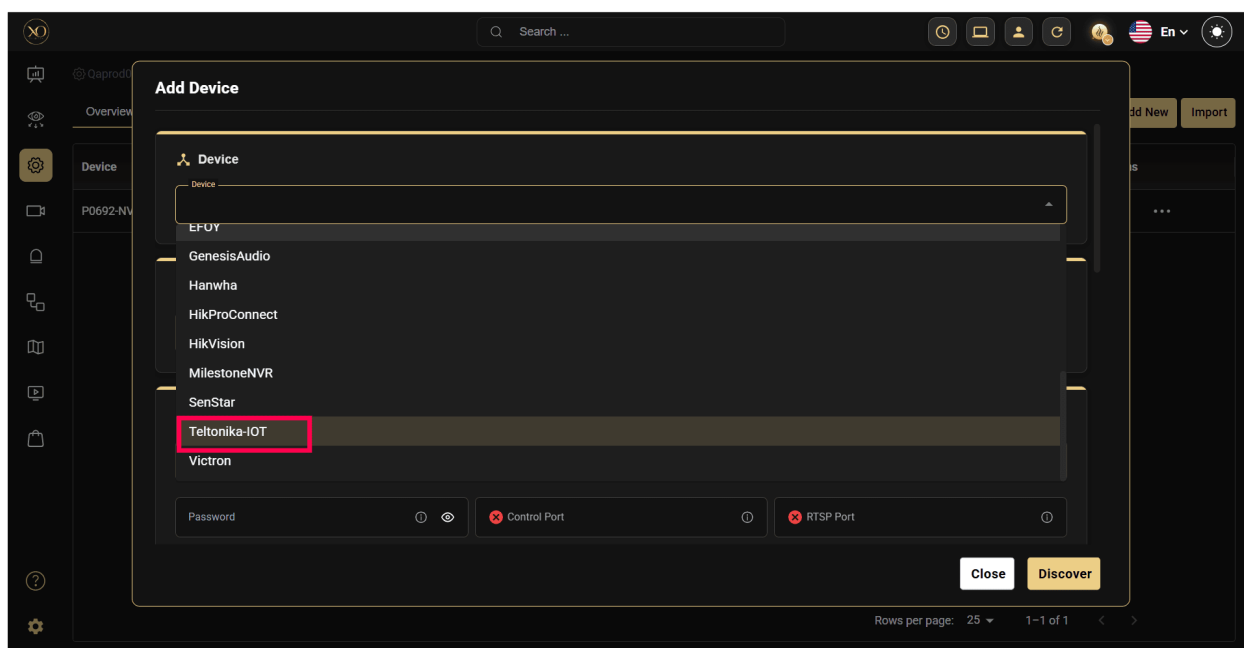
- Ga naar Configuratie → Sites
- Zoek en open de doel-site
- Klik Bewerken om het configuratie-paneel van de site te openen

Stap 2: Open het Apparaat-dialoog

Navigeer binnen de site-configuratie naar de Devices-sectie en klik op Add New om het dialoogvenster voor het aanmaken van een apparaat te openen.

Stap 3: Selecteer Apparaattype

Open in het apparaatedialoog het dropdownmenu Device Type en selecteer Teltonika-IOT om de juiste configuratievelden te laden.



Teltonika-apparaat-type-selectie

Stap 4: Voer Apparaatdetails in

Vul alle verplichte velden in om een beveiligde verbinding tussen GCXONE en de Teltonika-router tot stand te brengen. Elk veld wordt hieronder gedetailleerd beschreven.

Teltonika-apparaat-detailsformulier

VeldBeschrijvingNotitiesApparaattypeselecteer 'Teltonika-IOT' in het dropdownmenuMoet exact overeenkomen — bepaalt welk telemetriemodel wordt gebruiktApparaatnaamEen unieke en beschrijvende naam voor dit apparaat in GCXONEGebruik een naamgevingsconventie die de site en het apparaat identificeert — bijvoorbeeld 'Tower-North-Router-01'IP-adresOpenbaar of via VPN bereikbaar IP-adres van de Teltonika-routerMoet bereikbaar zijn vanaf de GCXONE-server; gebruik VPN als het apparaat zich achter NAT bevindtSerienummerHet hardware-serienummer dat op de router staat gedruktGevonden op het apparaatlabel of in het Teltonika-apparaatbeheerdersportaal-ControlpoortHTTP-poort voor apparaatcommunicatieStandaard is meestal poort 80; bevestig met uw netwerkconfiguratieRTSP poortRTSP-poort voor videostreaming vanaf het apparaatVerplicht veldServer poortServer-communicatiepoort voor het apparaatVerplicht veldHTTPS poortHTTPS-poort voor beveiligde communicatie met het apparaatVerplicht veldGebruikersnaamAdministratieve inlog-gebruikersnaam voor de routerMoet volledige toegang hebben tot alle apparaatparameters en API'sWachtwoordAdministratief inlogwachtwoord voor de routerVeilig opgeslagen in GCXONE; gebruik een sterk en uniek wachtwoord

Stap 5: Onder de verbindingsvelden bevat het dialoogvenster ook een Selecteer entiteitsgroep vervolgkeuzelijst, een Audio inschakelen schakelaar (standaard ingeschakeld), een vereiste Tijdzone, een Apparaat Configuratie sectie (Site puls configuratie), een Geavanceerde instellingen sectie (Event Polling, Heatmap masker configureren, Periodieke Status controle, Event retentie tijd — standaard 30 dagen), en een optionele Locatie sectie (Breedtegraad, Lengtegraad, Plus Code, What3Words).

Stap 6: Opslaan en verbinding verifiëren

Na het invullen van alle velden klikt u op Opslaan. GCXONE zal onmiddellijk proberen een verbinding tot stand te brengen met de Teltonika-router met de opgegeven inloggegevens.

Een succesvolle verbinding resulteert in:

- Het apparaat verschijnt in de apparaatlijst van de site met een actieve statusindicator
- Live telemetriegegevens beginnen te stromen naar GCXONE (signaalsterkte, netwerkstatus, I/O-staten)
- Het apparaat wordt beschikbaar voor configuratie van alarmregels

Belangrijk: Als de verbinding mislukt, controleer dan of het IP-adres bereikbaar is, de poort openstaat en de inloggegevens correct zijn. Controleer of er geen firewallregels GCXONE's toegang tot het apparaat blokkeren.

Alarmregels configuratie

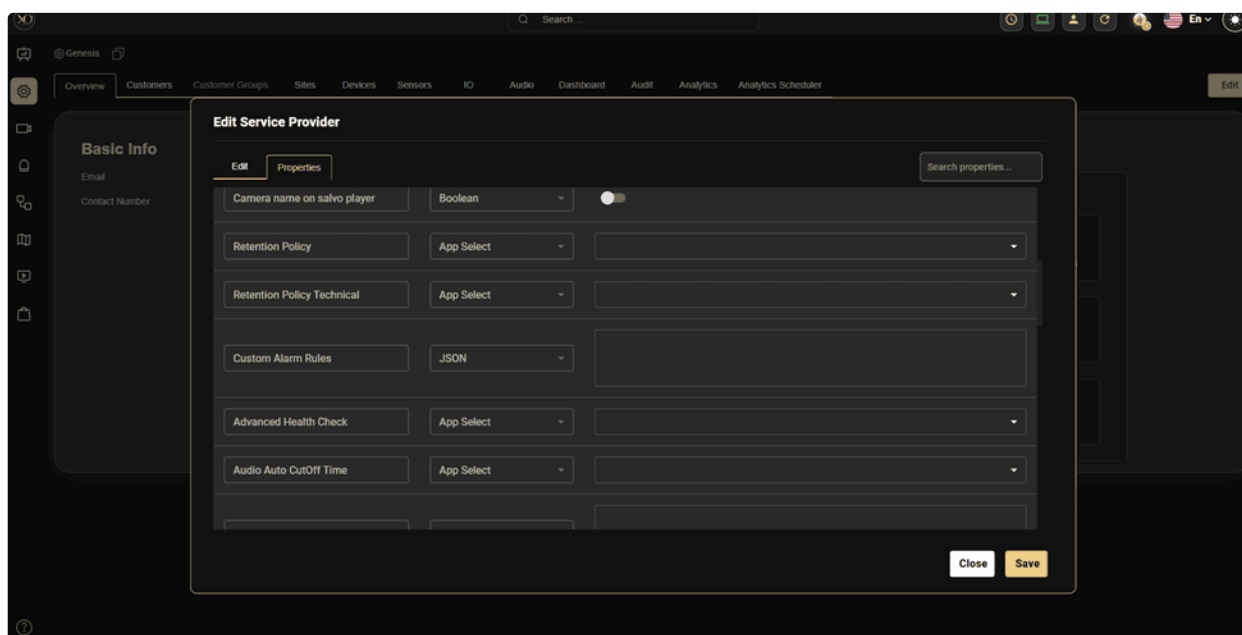
GCXONE gebruikt een JSON-gebaseerde alarmregelconfiguratie om te definiëren welke telemetrieparameters worden gemonitord, welke drempels alarmen activeren en hoe die alarmen worden geïdentificeerd in CMS-integraties.

Alarmregels kunnen worden geconfigureerd op site-niveau of apparaatniveau.

Teltonika-connectiviteitsregels worden doorgaans toegepast op apparaatniveau voor precieze controle.

Hoe alarmregels toe te passen

1. Navigeer naar de gewenste Site of Apparaat in GCXONE.
2. Klik op Bewerken en ga naar de sectie Extra eigenschappen.
3. Zoek de eigenschap met de naam Aangepaste alarmregels.
4. Open de drie puntjes (⋮) van de eigenschap en selecteer Standaard toepassen om de vooraf geconfigureerde regelset te laden. Alle regels zijn standaard inactief.
5. Pas de JSON aan om specifieke regels in te schakelen door "active": true te zetten voor de relevante parameters.
6. Stel uw drempels, gebeurteniscodes en groepscode in naar behoefte.
7. Klik op Opslaan. GCXONE zal onmiddellijk beginnen met het evalueren van binnenkomende telemetrie tegen de geconfigureerde regels.



Aangepaste alarmregels eigenschap

Tip: Standaard zijn alle alarmregels inactief. U moet expliciet "active": true instellen voor elke regel die GCXONE moet monitoren. Dit voorkomt onbedoelde alarmen tijdens de eerste configuratie.

Regelstructuur

Elke alarmregel volgt een consistente JSON-structuur. Het begrijpen van de gemeenschappelijke velden helpt bij het aanpassen van regels:

VeldBeschrijvingactiefBoolean (true/false). Stel in op true om monitoring voor deze regel in te schakelen.

Bij false wordt de regel genegeerdeventCodeUnieke tekenreeks-identificatie die door GCXONE wordt gebruikt om dit alarmtype te communiceren naar CMS-integraties (IMMIX / Evalink / AmWin / LISA).

Deze code verschijnt in uitgaande alarmmeldingengroupCodeLogische groeperingsidentificatie voor Tower-Monitoring-workflows — gebruikt om gerelateerde alarmen te filteren en te organiseren binnen GCXONE's Tower Alarm Manager.

Opmerking: Event-codes worden gebruikt voor cross-system CMS-meldingen (bijv. IMMIX, Evalink).

Group-codes zijn interne GCXONE-identificatoren voor toren-alarm-workflows. Beide moeten aanwezig zijn voor volledige integratie.

Teltonika-connectiviteits-alarmregels

De volgende alarmregels zijn beschikbaar voor Teltonika-IoT-apparaten onder de sectie

Connectiviteitsmonitoring van de Custom Alarm Rules JSON. Elke regel bewaakt een specifiek aspect van netwerkgezondheid, fysieke I/O of beveiliging.

Regel 1: Invoer/Uitvoer-statuswijziging

Bewaakt fysieke statuswijzigingen op Teltonika-I/O-poorten. Deze regel omvat digitale, analoge, geïsoleerde en relais-in- en uitgangen — essentieel voor het detecteren van deuropeningen, stroomgebeurtenissen, externe sensortriggers en apparaatstatuswijzigingen.

Standaard JSON-configuratie

```
"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"
}
}
```

Invoertypen

InvoertypeBeschrijving en parameters AnalogCurrentLoopBewaakt 4–20 mA-stroomlusssensoren. Stel

low/high in op het acceptabele stroomgebied. Waarschuwt wanneer de stroom buiten dit bereik valt.-

AnalogInputBewaakt analoge spanningsinvoeren (bijv. 11–14 V). Stel low/high drempels in. Een alarm wordt

geactiveerd wanneer de spanning buiten het bereik ligtDigitalInputBinaire statusbewaking. Stel alertOn

in op de status die een alarm moet activeren (bijv. 'High Level' voor detectie van een open deur).-

IsolatedInputElektrisch geïsoleerde digitale invoer. Zelfde configuratie als DigitalInput. Wordt gebruikt

wanneer isolatie van het hoofdcircuit vereist isPowerSocketInputBewaakt de status van een stopcontact

(Low/High niveau). Stel alertOn in op de triggerende status. Geschikt voor detectie van netstroom.

Uitvoertypen

UitvoertypeBeschrijving en parameters IsolatedOutputBewaakt de status van een geïsoleerd

uitvoerkanaal. Stel alertOn in op 'High Level' om een alarm te geven wanneer de uitvoer actief isRelay-

Volgt de relaisstatus (open/gesloten). Stel alertOn in op 'open' om een alarm te geven wanneer het

relais niet geactiveerd is. Handig voor monitoring van contactor of slotPowerSocketOutputBewaakt de

uitvoerstatus van een stopcontact. Alarm wanneer de uitvoer de geconfigureerde alertOn-status bereikt.

Regel 2: Gebruik van datapakketten SIM-kaart

Volgt het maandelijkse mobiele dataverbruik van de SIM-kaart van de Teltonika-router. Activeert een waarschuwing wanneer het dataverbruik het geconfigureerde percentage van de totale maandelijkse limiet bereikt — voorkomt onverwachte extra kosten of onderbrekingen van de service.

Standaard JSON Configuratie

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

Configuratieparameters

Parameter	naam	Beschrijving	Voorbeeld	waarde
simBillingStartDate	Facturatiecyclus	startdatum van het		
simDataPackageGB	Totale mobiele data	toegewezen per maand (in		
usageWarningPercent	Waarschuwingsdrempel	als percentage van het totale dataverbruik	80-	
eventCode	CMS alarm-identificatie	voor dit gebeurtenis	typesim.data.usage.warning	groupCode
groupCode	Interne	toren alarmgroep	voor filteren en routeren	tower.connectivity.simdata.alert

Voorbeeldgedrag

- Met `simDataPackageGB` ingesteld op 10 en `usageWarningPercent` op 80, genereert GCXONE een alarm wanneer het cumulatieve SIM-dataverbruik 8GB overschrijdt in de facturatieperiode.
- Het alarm wordt automatisch gewist wanneer het dataverbruik wordt gereset aan het begin van de nieuwe facturatiecyclus.
- Verlaag de drempel (bijv. 70%) voor vroegtijdige waarschuwing op locaties met beperkte connectiviteitsalternatieven.

Regel 3: Verlies van mobiel netwerk

Detecteert wanneer de Teltonika-router de mobiele netwerkconnectiviteit verliest of het signaal onder een onaanvaardbaar niveau daalt. Waarschuwt onmiddellijk operators voor mogelijke communicatiefouten op de locatie.

Standaard JSON Configuratie

```
"cellNetworkLoss": {  
  "active": false,  
  "eventCode": "modem.signal.warning",  
  "groupCode": "tower.connectivity.signal.alert"  
}
```

Voorbeeldgedrag

- GCXONE genereert een alarm wanneer het mobiele signaal onder de aanvaardbare drempel daalt of de connectiviteit volledig verloren gaat.
- Het alarm wordt automatisch gewist zodra het signaal terugkeert naar een aanvaardbaar niveau.
- Deze regel heeft geen drempelparameters — hij vertrouwt op de ingebouwde signaalkwaliteitsevaluatie van GCXONE voor de gerapporteerde modemstatus van de router.

Regel 4: Geo-fencing

Monitort de GPS-positie van de Teltonika-router ten opzichte van de toegewezen locatie van de site.

Genereert een alarm als het apparaat buiten de geconfigureerde radius beweegt — detecteert mogelijke torenverplaatsing, diefstal of ongeoorloofde beweging.

Standaard JSON Configuratie

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

Parameter naam Beschrijving Voorbeeld waarde radiusMeters Warning Radius (in meters) vanaf het gedefinieerde geo-fence-centrum — doorgaans de geo-locatie van de site — waarbinnen de toren moet blijven 500 eventCode CMS alarm-identificatie voor geo-omheining-schendingen geo.fence.breach-groupCode Interne toren-alarm-groepsidentificatie tower.connectivity.geofence.alert

Voorbeeldgedrag

- De geo-omheining is gecentreerd op de coördinaten die in de configuratie van de bovenliggende Site in GCXONE zijn gedefinieerd.
- Wanneer de GPS-positie die door de Teltonika-router wordt gerapporteerd meer dan 500 meter van het site-centrum afwijkt, wordt een schending-alarm gegenereerd.
- Het alarm wordt automatisch gewist wanneer het apparaat weer binnen de gedefinieerde grens terugkeert.
- Verklein de radius voor permanente vaste installaties; gebruik een grotere radius voor mobiele of semi-mobiele toren-implementaties.

Teltonika Dashboard

Elk Teltonika-apparaat heeft een eigen Dashboard-tabblad (Configuratie→ de site van het apparaat → Apparaten → het Teltonika-apparaat → Dashboard) waarop de live-status van VPN- en cellulair (LTE)-verbinding, dataverbruik, modemtemperatuur, SIM- en uptime-details, en de meest recente GPS-positie van het apparaat op een plattegrond worden weergegeven. Een veld Site Radius Meters op dit scherm maakt het mogelijk de geo-omheining-radius direct te bekijken en bij te werken — voer een waarde in meters in en klik op Verzenden, in plaats van de JSON-configuratie handmatig te bewerken. Als de laatst gerapporteerde positie van het apparaat buiten de ingestelde radius ligt, toont het dashboard een waarschuwingsbanner met de huidige afstand tot de site. Een knop Opname Nu vraagt op verzoek een nieuwe GPS-meting aan, en Stel Site in op Huidige GPS werkt de coördinaten van de site bij naar de laatst bekende positie van het apparaat.

Regel 5: Jammerdetectie

Detecteert mogelijke radiofrequentie-jammingpogingen op basis van plotselinge signaaldegradatie en slechte Reference Signal Received Quality (RSRQ). Jammerdetectie is cruciaal voor beveiligingsgevoelige toren-implementaties waar signaalinterferentie kan duiden op opzettelijke verstoringspogingen.

Standaard JSON-configuratie

```
"jammerDetection": {
  "active": false,
  "criteria": {
    "signalDropThreshold": 25,
    "minSignalLevel": -113,
    "rsrqThreshold": -20
  },
  "eventCode": "modem.jammer.detected",
  "groupCode": "tower.connectivity.jamming.alert"
}
```

ParameternaamBeschrijvingVoorbeeldwaarde
 signalDropThresholdPercentage-daling in signaalsterkte dat wordt beschouwd als een potentieel jam-event
 25
 minSignalLevelMinimaal aanvaardbaar signaalniveau (in dBm) waaronder jamming wordt vermoed
 -113
 rsrqThresholdMinimaal aanvaardbare RSRQ (Reference Signal Received Quality); een slechte RSRQ kan duiden op interferentie-

-20eventCodeCMS-identificatie voor jammerdetectie-eventsmodem.jammer.detectedgroupCode-

Toren-alarm-groepsidentificatietower.connectivity.jamming.alert

Voorbeeldgedrag

- GCXONE evalueert zowel het absolute signaalniveau (RSRQ) als de snelheid van signaalverandering (daling-percentages) om echte jamming te onderscheiden van normale signaalvariatie.
- Een alarm wordt geactiveerd wanneer de signaaldaling 25% overschrijdt OF de RSRQ onder -20 valt en het signaalniveau gelijktijdig onder -113 dBm ligt.
- Het alarm wordt automatisch gewist zodra de signaalstabiliteit weer normaal is.

Opmerking: Jammerdetectiedrempels moeten mogelijk worden afgestemd op de lokale

RF-omgevingscondities. Sites in stedelijke gebieden met natuurlijke signaalvariatie kunnen een hogere signalDropThreshold vereisen om valse positieven te verminderen.

Configuratie Referentie

Complete Teltonika Connectivity Alarm Regels JSON

Dit is de volledige standaard JSON-configuratie voor alle Teltonika-connectiviteit alarm regels. Kopieer dit naar de Aangepast Alarm Regels eigenschap en pas het aan naar behoefte voor uw implementatie.

```
"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"
}
}
```

Evenementcodes en Groepcodes Samenvatting

Snelle referentie voor alle Teltonika-connectiviteit evenementcodes en groepcodes:

RegelEvenementcodeGroepcode/O

Ingangstoestandwijziginginput.statechangetower.input.statechange/O

Uitgangstoestandwijzigingoutput.statechangetower.output.statechangeSIM-datagebruik

Waarschuwingssim.data.usage.warningtower.connectivity.simdata.alertMobiel

Netwerkverliesmodem.signal.warningtower.connectivity.signal.alertGeo-Fence

Overtredinggeo.fence.breachtower.connectivity.geofence.alertJammerdetectie-

modem.jammer.detectedtower.connectivity.jamming.alert

Configuratie Best Practices

- Begin altijd met Toepassen Standaard om de volledige vooraf geconfigureerde regelset te laden voordat u wijzigingen aanbrengt.
- Schakel regels geleidelijk in — begin met kritieke regels (netwerkverlies, jammerdetectie) voordat u drempelgevoelige regels zoals I/O-toestandwijzigingen inschakelt.
- Test alarm regels in een testomgeving of op één apparaat voordat u ze naar alle locaties uitrolt.
- Stel usageWarningPercent voor SIM-data in op 70–80% om operators voldoende tijd te geven actie te ondernemen voordat het abonnement is uitgeput.
- Voor geo-fencing op permanente locaties, gebruik een kleine radius (100–200m). Voor tijdelijke inzet, gebruik 500 m of meer.
- Documenteer uw evenementcodes en groepcodes in uw CMS-configuratie om correcte alarm routing te waarborgen.

OpenVPN Configuratie op Teltonika Router

Vanuit de NXGEN-kant leveren wij een OpenVPN (ovpn) configuratiebestand en een LAN-IP-segment dat moet worden toegewezen aan het Klant-netwerk.

Stapsgewijze Configuratie

Stap 1: Verander het Standaard LAN-IP van de Teltonika Router naar het IP dat door het NXGEN-team is opgegeven

- Open de webconsole van de router.
- Navigeer naar Netwerk → Interfaces → Algemeen → Bewerk LAN.
- Voer het LAN-IP en Subnet in → Opslaan.

TELTONIKA | Networks

MODE: ADVANCED USER: ADMIN FW VERSION: RUT9M_R_00.07.04.3 LOGOUT

NETWORK INTERFACES

ID	Name	Status	Failover	Type	IP	Protocol	MAC	Uptime	Tx	Rx	Actions	Toggle
1	lan	Up	Disabled	Wired	10.175.102.1/24	static	20:97:27:08:27:38	26d 21h 50m 2s	8.82 GB	303.10 GB	[Edit] [Delete]	off on
2	vpn1	Down	Disabled	Wired	-	none	-	-	0.00 B	0.00 B	[Edit] [Delete]	off on
3	wan	Down	Disabled	Wired	-	dhcp	20:97:27:08:27:3C	-	255.55 MB	0.00 B	[Edit] [Delete]	off on
4	wan6	Down	Disabled	Wired	-	dhcpv6	20:97:27:08:27:3C	-	255.55 MB	0.00 B	[Edit] [Delete]	off on
5	mobilsta1	Up	Disabled	Mobile	10.137.165.227/32	internet	SIM: 1	11h 10m 15s	296.51 GB	7.06 GB	[Edit] [Delete]	off on

Teltonika LAN IP-configuratie

Stap 2: Importeer het OpenVPN-configuratiebestand dat door het NXGEN-team is geleverd

- Navigeer in de webconsole naar Services → VPN → OPENVPN.
- Selecteer onder Add New Interface de optie, voer de "VPN Name" in en stel de Rol in op "Client" → Add.

TELTONIKA | Networks

MODE: ADVANCED USER: ADMIN FW VERSION: RUT9M_R_00.07.04.3 LOGOUT

SERVICES

VPN

OPENVPN

OPENVPN CONFIGURATION

TUNNEL NAME	ROLE	TUN/TAP	PROTOCOL	PORT	STATUS	Actions
openvpn	Client	TUN	-	1194, 443, 1194	Connected	[Edit] [Delete]

ADD NEW INSTANCE

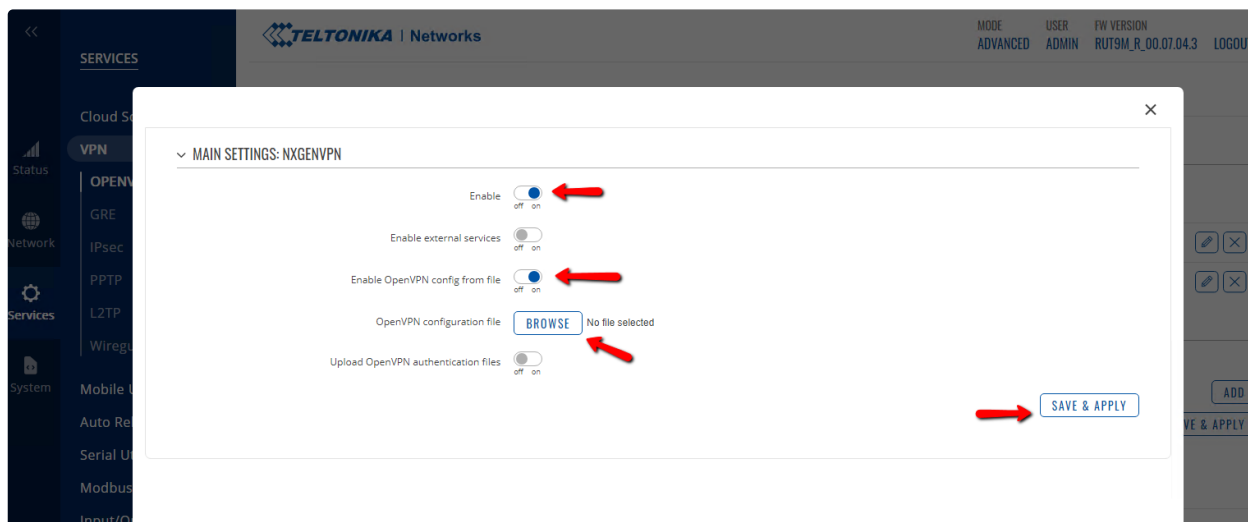
NEW CONFIGURATION NAME:

ROLE:

[ADD] [SAVE & APPLY]

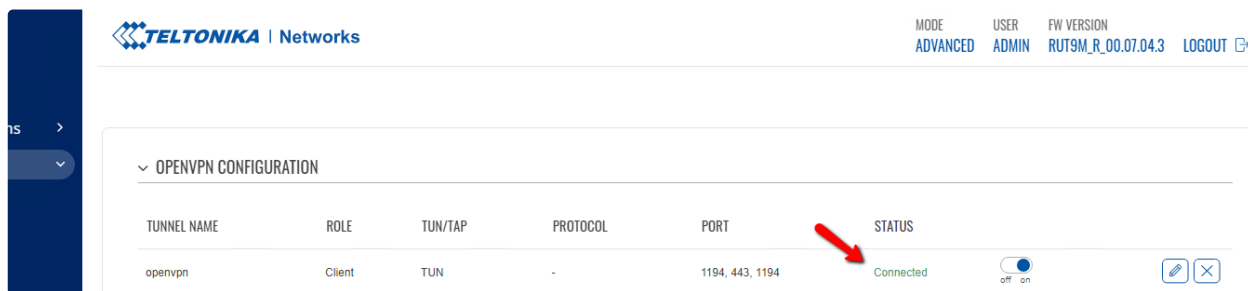
Teltonika OpenVPN-interface-configuratie

- Selecteer "Enable OpenVPN configuration file" → Blader en voeg het ovpn-bestand bij.
- Selecteer Inschakelen en Opslaan.



Teltonika OpenVPN-bestand uploaden

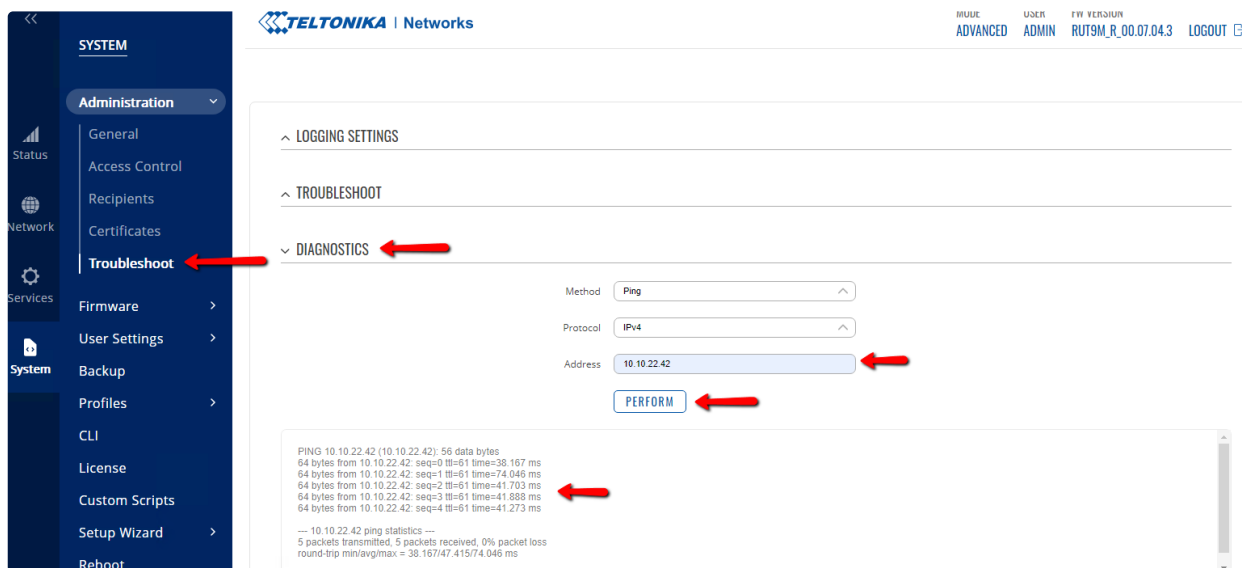
- Na enkele minuten verandert de status naar "Connected".



Teltonika OpenVPN-verbonden status

Stap 3: Test de connectiviteit

- Navigeer naar **Systeem** → **Administration** → **Troubleshoot**.
- Selecteer onder **Diagnostics** de methode "Ping" → Voer IP "10.10.22.42" in → **Uitvoeren**.



Teltonika VPN-pingtest

- De VPN-verbinding is correct geconfigureerd als u een succesvolle ping-respons ontvangt.

Probleemoplossing

Apparaat maakt geen verbinding

Symptoom / ControleOplossingVerbinding mislukt onmiddellijk na OpslaanControleer of het IP-adres bereikbaar is vanaf de GCXONE-server. Probeer het IP vanaf de server te pingen of controleer de VPN-connectiviteit.AuthenticatiefoutBevestig dat gebruikersnaam en wachtwoord correct zijn en administratieve toegang hebben. Log direct in op de Teltonika-admininterface om de inloggegevens te verifiëren.Poortgerelateerde verbindingsfoutControleer of de geconfigureerde Poort correct is en niet geblokkeerd wordt door een firewall. Standaard is poort 80Apparaat toont offline na initiële verbinding-Controleer of het IP-adres van de Teltonika-router is gewijzigd (DHCP). Overweeg een statisch IP of DHCP-reservering te gebruiken.

Alarmregels worden niet geactiveerd

Symptoom / ControleOplossingGeen alarmen ontvangen voor een overschreden drempelControleer of de regel "active": true bevat in de JSON. Controleer of de Aangepaste Alarmregels-JSON geldig is (geen syntaxisfouten).eventCode verschijnt niet in CMSBevestig dat de event-code is geconfigureerd in

uw CMS-integratie. Controleer de CMS-kanaalmapping in GCXONE onder de integratie-instellingen van de site. Valse alarmen (te veel alarmen) Vergroot het laag/hoog bereik voor analoge ingangen; verhoog signalDropThreshold voor jammerdetectie Geo-fence-alarm voor een vaste locatie Controleer of de GPS-coördinaten van de site in GCXONE correct zijn ingesteld op de werkelijke torenlocatie. Verhoog radiusMetersWarning als GPS-rapportage variatie vertoont.

SIM-dateregeling wordt niet geactiveerd

- Zorg ervoor dat de Teltonika-router SIM-datagebruik-metingen rapporteert aan GCXONE.
- Controleer of simDataPackageGB overeenkomt met uw werkelijke SIM-planomvang.
- Het veld simBillingStartDate is momenteel inactief — het bijhouden van dataverbruik gebruikt voorlopig de kalendermaand.

Voor extra ondersteuning kunt u contact opnemen met uw NXGEN-vertegenwoordiger of de volledige GCXONE Toren Monitoren Configuratie-gids raadplegen, die Victron Energy- en EFOY-brandstofcelmonitoring behandelt, naast Teltonika IoT-connectiviteit.