

Clause de non-responsabilité

Avertissement juridique

Ce guide et son contenu (le « Guide ») sont fournis par NXGEN. Tous les droits sur le Guide et sur la propriété intellectuelle qu'il incorpore — y compris, sans s'y limiter, les marques, noms commerciaux, logos et signes similaires figurant dans ou sur le Guide — sont protégés par la loi. L'ensemble des droits, titres et intérêts relatifs au Guide et aux droits de propriété intellectuelle qui s'y rapportent appartiennent et demeurent à NXGEN et à ses concédants.

Le Guide est fourni gratuitement, « en l'état » et à titre d'information uniquement, sans garantie d'aucune sorte. Il n'est ni destiné ni propre à établir une quelconque relation juridique entre le lecteur et NXGEN ou ses sociétés affiliées, y compris, sans s'y limiter, une quelconque obligation de NXGEN ou de ses sociétés affiliées envers le lecteur.

Les obligations de NXGEN et de ses sociétés affiliées concernant les produits ou services NXGEN achetés par un client sont régies exclusivement par les termes du contrat au titre duquel ces produits ou services ont été achetés.

Pour clarification

Le lecteur assume l'intégralité du risque quant à l'utilisation, aux résultats et aux performances du Guide. Dans toute la mesure permise par la loi applicable, NXGEN décline et exclut toutes garanties, qu'elles soient légales, expresses ou implicites — y compris, sans s'y limiter, les garanties implicites de qualité marchande, d'adéquation à un usage particulier, de titre et de non-contrefaçon des droits de tiers — ainsi que toute responsabilité ou garantie découlant de suggestions, spécifications ou échantillons liés au Guide.

Teltonika

Updated 11 August 2026

Introduction

Les routeurs IoT Teltonika servent de colonne vertébrale de connectivité pour la surveillance des tours GCXONE, fournissant l'état cellulaire en temps réel, le suivi GPS, les changements d'état des entrées/sorties et la qualité du signal depuis des sites de tours distants. Ce guide explique tout le processus d'intégration d'un routeur IoT Teltonika — de l'ajout de l'appareil dans GCXONE et la saisie des identifiants requis, à la configuration des règles d'alarme pour la perte réseau, la géo-repérage, l'utilisation des données SIM et la détection des brouilleurs.

Quels Teltonika Devices surveillent

Une fois connectés à GCXONE, les routeurs Teltonika rapportent en continu les catégories suivantes de télémétrie :

- État de la connectivité réseau et qualité du signal (RSRQ, RSRP)
- Utilisation des données de la carte SIM selon des limites mensuelles configurées
- Changements physiques d'état des ports d'entrée/sortie (E/S) — numérique, analogique, isolé, relais
- Position GPS par rapport à la limite du site attribuée (géo-repérage)
- Détection de brouilleurs basée sur des schémas de dégradation soudaine du signal

Tip

Teltonika gère la communication, le suivi GPS et le routage de télémétrie en périphérie pour la tour. Cela en fait l'épine dorsale de la surveillance de la connectivité — sans elle, GCXONE ne peut pas détecter les pannes réseau, les interférences de signal ou les mouvements non autorisés des appareils.

Prérequis

Avant de commencer l'intégration des appareils, assurez-vous que les informations et accès suivants sont disponibles :

EXIGENCE	DÉTAILS
Accès GCXONE	Rôle administrateur ou opérateur avec accès au module de configuration
Identifiants des appareils	Nom d'utilisateur administratif et mot de passe pour le routeur Teltonika
Adresse IP	Adresse IP publique ou accessible via VPN de l'appareil Teltonika
Numéro de série	Le numéro de série matériel unique du routeur
Port de contrôle	Port HTTP utilisé pour la communication avec les appareils (par exemple
Site créé	Le site auquel cet appareil sera assigné doit déjà exister dans GCXONE

Caution

Assurez-vous que le routeur Teltonika est en ligne, accessible depuis le serveur GCXONE (IP directe ou via VPN), et que les identifiants administratifs fournis bénéficient d'un accès complet à l'API.

Guide de configuration Teltonika avec GCX-ONE

Suivez ces étapes pour ajouter un routeur IoT Teltonika à GCXONE. L'appareil sera enregistré sur un site existant et commencera à signaler la télémétrie immédiatement après la configuration.

Étape 1 — Naviguer jusqu'au site

Dans GCXONE, naviguez jusqu'au site où l'appareil Teltonika est physiquement installé. C'est l'entité mère sous laquelle l'appareil sera enregistré.

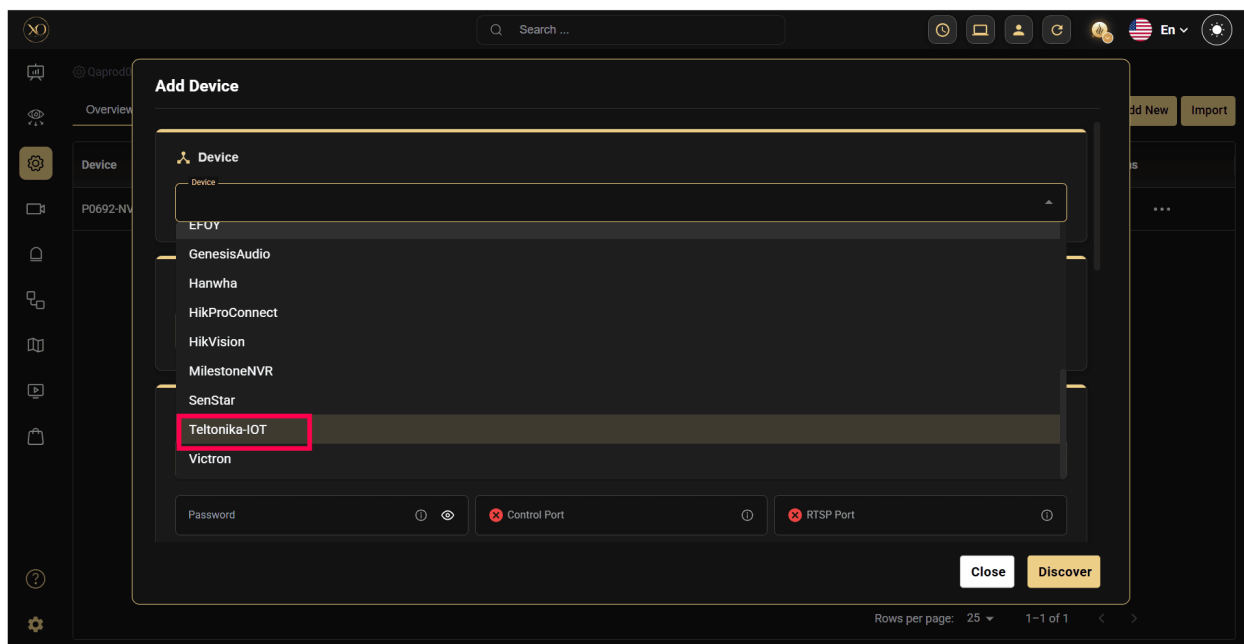
- Aller dans Configuration → sites
- Localisez et ouvrez le site cible
- Cliquez sur Modifier pour ouvrir le panneau de configuration du site

Étape 2 — Ouvrir la boîte de dialogue Appareil

Dans la configuration du site, allez dans la section Appareils et cliquez sur Ajouter un appareil pour ouvrir la boîte de dialogue de création d'appareil.

Étape 3 — Sélectionner le type d'appareil

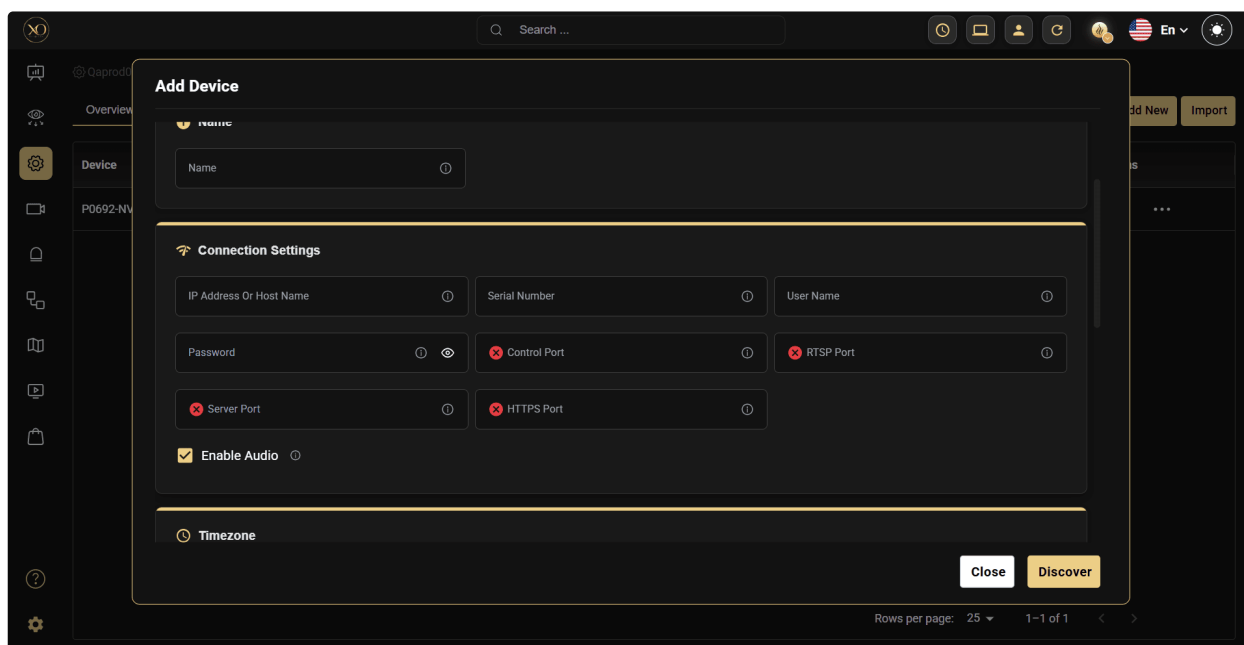
Dans la boîte de dialogue de l'appareil, ouvrez la liste déroulante Type d'appareil et sélectionnez Teltonika IoT pour charger les champs de configuration appropriés.



Victron

Étape 4 — Saisir les détails de l'appareil

Remplissez tous les champs requis pour établir une connexion sécurisée entre GXONE et le routeur Teltonika. Chaque champ est décrit en détail ci-dessous.



Victron

TERRAIN	DESCRIPTION	NOTES

Type de dispositif	Sélectionnez « Teltonika IoT » dans le menu déroulant	Doit correspondre exactement — détermine quel modèle de télémétrie est utilisé
Nom de l'appareil	Un nom unique et descriptif pour cet appareil dans GCXONE	Utilisez une convention de nommage qui identifie le site et l'appareil
Adresse IP	Adresse IP publique ou accessible via VPN du routeur Teltonika	Doit être joignable depuis le serveur GCXONE ; utiliser le VPN si l'appareil est en retard sur NAT
Numéro de série	Le numéro de série matériel imprimé sur le routeur	Disponible sur l'étiquette de l'appareil ou dans le portail de gestion des appareils Teltonika
Port de contrôle	Port HTTP pour la communication avec les appareils	Par défaut
Nom d'utilisateur	Identifiant administrateur pour le routeur	Doit avoir un accès complet à tous les paramètres et API de l'appareil
Mot de passe	Mot de passe de connexion administrateur pour le routeur	Stocké en toute sécurité dans GCXONE ; Utilisez un mot de passe fort et unique

Étape 5 — Enregistrer et vérifier la connexion

Après avoir saisi tous les champs, cliquez sur Enregistrer. GCXONE tentera immédiatement d'établir une connexion avec le routeur Teltonika en utilisant les références fournies.

Une connexion réussie aboutit à :

- L'appareil apparaissant dans la liste des appareils du site avec un indicateur d'état actif
- Les données télémétriques en direct commencent à affluer dans GCXONE (force du signal, état du réseau, états d'E/S)
- L'appareil devient disponible pour la configuration des règles d'alarme

Caution

Si la connexion échoue, vérifiez que l'adresse IP est joignable, que le port est ouvert et que les identifiants sont corrects. Vérifiez qu'aucune règle de pare-feu ne bloque l'accès de GCXONE à l'appareil

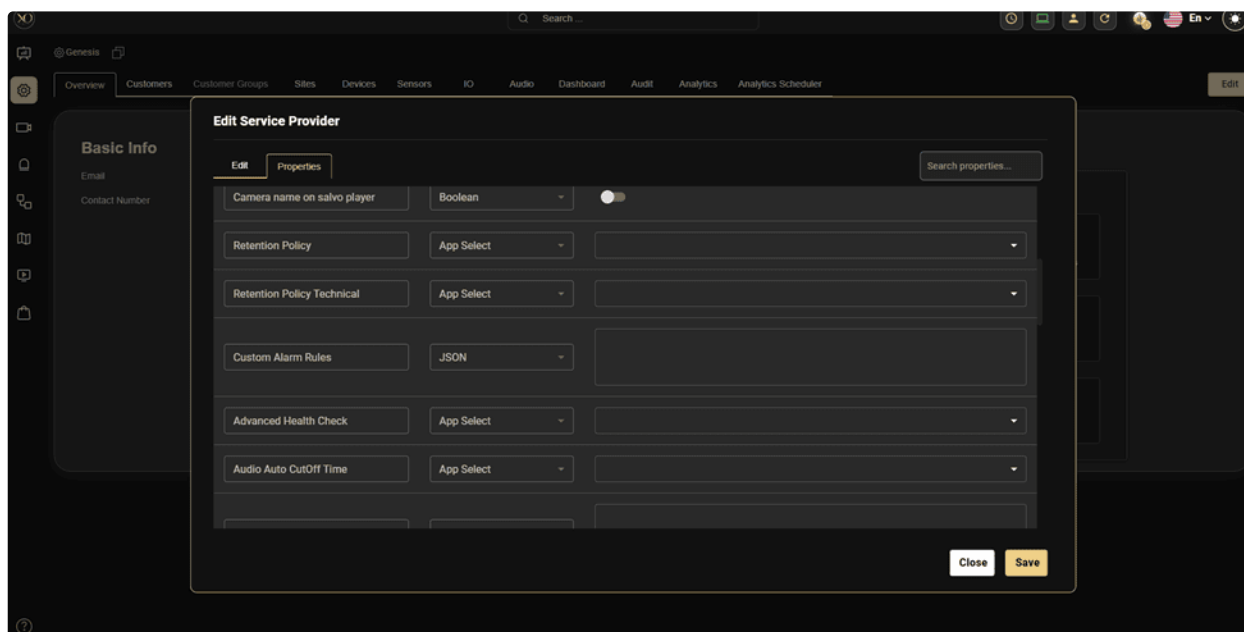
Configuration des règles d'alarme

GCXONE utilise une configuration de règles d'alarme basée sur JSON pour définir quels paramètres de télémétrie sont surveillés, quels seuils déclenchent les alertes, et comment ces alertes sont identifiées dans les intégrations CMS.

Les règles d'alarme peuvent être configurées au niveau du site ou du niveau de l'appareil. Les règles de connectivité Teltonika sont généralement appliquées au niveau de l'appareil pour un contrôle précis.

Comment appliquer les règles d'alarme

1. Naviguez vers le site ou l'appareil cible dans GCXONE.
2. Cliquez sur Modifier et allez dans la section Propriétés supplémentaires.
3. Trouvez la propriété appelée Custom Alarm Rules.
4. Ouvrez le menu hamburger (:) de la propriété et sélectionnez Appliquer par défaut pour charger le jeu de règles préconfiguré. Toutes les règles sont inactives par défaut.
5. Modifiez le JSON pour permettre des règles spécifiques en définissant « active » : true pour les paramètres concernés.
6. Définissez vos seuils, codes d'événements et codes de groupe selon les besoins.
7. Cliquez sur Enregistrer. GCXONE commencera immédiatement à évaluer la télémétrie entrante par rapport aux règles configurées.



Victron

Conseil

Par défaut, toutes les règles d'alarme sont inactives. Vous devez explicitement définir « active » : vrai pour chaque règle que vous souhaitez que GCXONE surveille. Cela évite les alertes accidentelles lors de la configuration initiale.

Structure des règles

Chaque règle d'alarme suit une structure JSON cohérente. Comprendre les champs courants aide à personnaliser les règles :

TERRAIN	DESCRIPTION
Actif	Booléen (vrai/faux). Réglez sur true pour permettre la surveillance de cette règle. Lorsqu'elle est fausse
eventCode	Identifiant de chaîne unique utilisé par GCXONE pour communiquer ce type d'alarme aux intégrations CMS (IMMIX
groupCode	Identifiant de groupement logique pour les flux de travail de surveillance de tour. Utilisé pour filtrer

Tip

Les codes d'événement sont utilisés pour la notification CMS inter-système (par exemple, IMMIX, Evalink). Les codes de groupe sont des identifiants internes GCXONE pour les flux de travail d'alarme de tour. Les deux doivent être présents pour une intégration complète.

Règles d'alarme de connectivité Teltonika

Les règles d'alarme suivantes sont disponibles pour les appareils IoT Teltonika dans la section Surveillance de la connectivité du JSON des règles d'alarme personnalisées. Chaque règle surveille un aspect spécifique de la santé du réseau, des E/S physiques ou de la sécurité.

1. Règle de changement de statut d'entrée/sortie

Surveille les changements d'état physique sur les ports d'E/S Teltonika. Cette règle couvre les entrées et sorties numériques, analogiques, isolées et relais — essentielles pour détecter l'ouverture des portes, les événements d'alimentation, les déclencheurs externes des capteurs et les changements d'état des équipements.

Configuration JSON par défaut

```
« IOSTatusChange » : {
  « entrée » : {
    « AnalogCurrentLoop » : {"active » : false, « low » : 4, « high » : 20},
    « AnalogInput » : {"active » : false, « low » : 11, « high » : 14},
    « DigitalInput » : {"active » : false, « ranges » : ["Low level », « High level"],
    « alertOn » : « Haut Niveau"},
```

```
« IsolationedInput » : {"active » : false, « ranges » : ["Low level », « High level"],
« alertOn » : « Haut Niveau"},
« PowerSocketInput » : {"active » : false, « ranges » : ["Low level », « High level"],
« alertOn » : « Haut Niveau"},
« eventCode » : « input.statechange »,
« groupCode » : « tower.input.statechange »
},
« sortie » : {
« IsolatedOutput » : {"active » : false, « ranges » : ["Low level », « High level"],
« alertOn » : « Haut Niveau"},
« Relay » : {"active » : false, « ranges » : ["open », « closed"], « alertOn » :
« open"},
« PowerSocketOutput » : {"active » : false, « ranges » : ["Low level », « High level"],
« alertOn » : « Haut Niveau"},
« eventCode » : « output.statechange »,
« groupCode » : « tower.output.statechange »
}
```

} Types d'entrées

TYPE D'ENTRÉE	DESCRIPTION ET PARAMÈTRES

AnalogCurrentLoop	Surveille des capteurs de boucle de courant de 4 à 20 mA. Réglez bas/haut à la plage de courant acceptable. Alertes lorsque le courant dépasse cette portée.
AnalogInput	Surveille les entrées de tension analogiques (par exemple
DigitalInput	Surveillance de l'état binaire. Réglez AlertOn sur l'état qui devrait déclencher une alarme (par exemple
EntréeIsolée	Entrée numérique électriquement isolée. Même configuration que DigitalInput. Utilisé lorsque l'isolation du circuit principal est requise.
PowerSocketInput	Surveille l'état de la prise électrique (niveau bas/haut). Activez l'alerte sur l'état de déclenchement. Adapté à la détection de l'alimentation électrique.

Types de sortie

TYPE DE SORTIE	DESCRIPTION ET PARAMÈTRES
SortieIsolée	Surveille l'état d'un canal de sortie isolé. Réglez alertOn sur « High Level » pour alerter lorsque la sortie est active.
Relais	L'état du relais des pistes (ouvert/fermé). Activez l'alerte sur « ouvrir » pour alerter lorsque le relais n'est pas sous tension. Utile pour la surveillance des contacteurs ou des serrures.
PowerSocketOutput	Surveille l'état de sortie de la prise électrique. Alertez lorsque la sortie atteint l'état configuré alertOn.

2. Règle d'utilisation des paquets de données de carte SIM

Suit la consommation mensuelle de données mobiles pour la carte SIM du routeur Teltonika. Déclenche un avertissement lorsque l'utilisation des données atteint le pourcentage configuré de l'allocation mensuelle totale — évitant ainsi des frais de dépassement imprévus ou des interruptions de service.

Configuration JSON par défaut

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

Paramètres de configuration

NOM DU PARAMÈTRE	DESCRIPTION	VALEUR D'EXEMPLE
simBillingDate de début	Date de début du cycle de facturation du forfait SIM (actuellement inactif)	1
simDataPackageGB	Total des données mobiles allouées par mois (en GB)	10
UtilisationAvertissementPourcentage	Seuil d'avertissement en pourcentage de l'utilisation totale des données	80
eventCode	Identifiant d'alarme CMS pour ce type d'événement	sim.data.usage.warning
groupCode	Groupe d'alarme interne de tour pour le filtrage et le routage	tower.connectivity.simdata.alert

Exemple de comportement

- Avec simDataPackageGB réglé à 10 et usageWarningPercent à 80, GCXONE déclenche une alerte lorsque l'utilisation cumulée des données SIM dépasse 8 Go pendant la période de facturation.
- L'alerte se réinitialise automatiquement lorsque l'utilisation des données est réinitialisée au début du nouveau cycle de facturation.
- Ajustez le seuil à la baisse (par exemple, 70 %) pour l'alerte précoce sur les sites aux alternatives de connectivité limitées.

3. Règle de perte de réseau cellulaire

Détecte lorsque le routeur Teltonika perd la connectivité du réseau mobile ou que le signal chute à un niveau inacceptable. Alerte immédiatement les opérateurs en cas de défaillances potentielles de communication sur le site.

Configuration JSON par défaut

```
« cellNetworkLoss » : {
  « actif » : faux,
  « eventCode » : « modem.signal.warning »,
```

```
« groupCode » : « tower.connectivity.signal.alert »  
}
```

Exemple de comportement

- GCXONE déclenche une alerte lorsque le signal cellulaire descend en dessous du seuil acceptable ou que la connectivité est complètement supprimée.
- L'alerte se dissipe automatiquement une fois que le signal revient à un niveau acceptable.
- Cette règle n'a pas de paramètres seuils — elle repose sur l'évaluation de la qualité du signal intégrée à GCXONE pour l'état du modem rapporté.

4. Règle de la géo-clôture

Surveille la position GPS du routeur Teltonika par rapport à son emplacement attribué. Déclenche une alerte si l'appareil dépasse le rayon configuré — détectant un déplacement potentiel de la tour, un vol ou un mouvement non autorisé.

Configuration JSON par défaut

```
« geoFencing » : {  
  « actif » : faux,  
  « AlerteMètresRayons » : 500,  
  « eventCode » : « geo.fence.breach »,  
  « groupCode » : « tower.connectivity.geofence.alert »  
}
```

NOM DU PARAMÈTRE	DESCRIPTION	VALEUR D'EXEMPLE
Avertissements RadiusMeters	Rayon (en mètres) à partir du centre de géo-clôture défini (typiquement	la géolocalisation du site) dans lequel la tour doit se trouver

eventCode	Identifiant d'alarme CMS pour les événements de brèche de géoclôture	geo.fence.breach
groupCode	Identifiant de groupe d'alarme interne à la tour	tour.connectivité.geofence.alerte

Exemple de comportement

- La limite de la géo-clôture est centrée sur les coordonnées définies dans la configuration du site parent dans GCXONE.
- Si la position GPS rapportée par le routeur Teltonika dépasse 500 mètres du centre du site, une alerte de brèche est générée.
- L'alerte se réprime automatiquement lorsque l'appareil revient dans la limite définie.
- Réduire le rayon pour les installations fixes permanentes ; Utilisez un rayon plus large pour le déploiement de tours mobiles ou semi-mobiles.

5. Règle de détection du brouilleur

Détecte les tentatives potentielles de brouillage radiofréquence basées sur une dégradation soudaine du signal et une mauvaise qualité de référence du signal reçu (RSRQ). La détection des brouilleurs est cruciale pour les déploiements de tours sensibles à la sécurité où les interférences de signal peuvent indiquer des tentatives délibérées de perturbation.

Configuration JSON par défaut

```
« BrouilleurDedetection » : {
  « actif » : faux,
  « critères » : {
    « signalDropThreshold » : 25,
    « minSignalLevel » : -113,
```

```
« rsrqThreshold » : -20

},

« eventCode » : « modem.jammer.detected »,

« groupCode » : « tower.connectivity.jamming.alert »

}
```

NOM DU PARAMÈTRE	DESCRIPTION	VALEUR D'EXEMPLE
signalDropThreshold	Baisse en pourcentage de la puissance du signal considérée comme un événement potentiel de brouillage	25
minSignalLevel	Niveau minimal acceptable de signal (en dBm) ; Si le signal descend en dessous de cette limite	on soupçonne un brouillage
rsrqThreshold	RSRQ minimal acceptable (Qualité de Signal de Référence Reçu) ; RSRQ médiocre peut indiquer des interférences	-20
eventCode	Identifiant CMS pour les événements de détection de brouilleurs	modem.jammer.detected
groupCode	Identifiant de groupe d'alarme de tour	tour.connectivité.jamming.alerte

Exemple de comportement

- GCXONE évalue à la fois le niveau absolu du signal (RSRQ) et le taux de variation du signal (pourcentage de chute) afin de distinguer le brouillage véritable de la variation normale du signal.
- Une alerte est déclenchée lorsque la chute du signal dépasse 25 % OU que le RSRQ descend en dessous de -20 et que le niveau du signal est en dessous de -113 dBm simultanément.
- L'alerte se dissipe automatiquement une fois la stabilité normale du signal rétablie.

Tip

Les seuils de détection des brouilleurs peuvent nécessiter un réglage en fonction des conditions locales de l'environnement RF. Les sites situés en zones urbaines présentant une variation naturelle du signal peuvent nécessiter un seuil de chute plus élevé pour réduire les faux positifs.

Référence de configuration

a. Règles complètes d'alarme de connectivité Teltonika JSON

Voici la configuration JSON par défaut complète pour toutes les règles d'alarme de connectivité Teltonika. Copiez cela dans la propriété Custom Alarm Rules et modifiez-les selon les besoins pour votre déploiement.

```
« connectivityMonitoring » : {  
  
  « IOStatusChange » : {  
  
    « entrée » : {  
  
      « AnalogCurrentLoop » : { "active" : false, « low » : 4, « high » : 20 },  
  
      « AnalogInput » : { "active" : false, « low » : 11, « high » : 14 },  
  
      « DigitalInput » : { "active" : false, « ranges » : [ "Low level", « High level" ],  
  
      « alertOn » : « Haut Niveau },  
  
      « IsolationedInput » : { "active" : false, « ranges » : [ "Low level", « High level" ],  
  
      « alertOn » : « Haut Niveau },  
  
      « PowerSocketInput » : { "active" : false, « ranges » : [ "Low level", « High level" ],  
  
      « alertOn » : « Haut Niveau },
```



```
« eventCode » : « input.statechange »,

« groupCode » : « tower.input.statechange »

},

« sortie » : {

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

« alertOn » : « Haut Niveau"},

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

« open"},

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

« alertOn » : « Haut Niveau"},

« eventCode » : « output.statechange »,

« groupCode » : « tower.output.statechange »

}

},

« simCardDataPackage » : {

« actif » : faux,

« simBillingDateStartDateT » : 1,

« simDataPackageGB » : 10,

« usageWarningPercentpercent » : 80,

« eventCode » : « sim.data.usage.warning »,
```

```
« groupCode » : « tower.connectivity.simdata.alert »  
  
},  
  
« cellNetworkLoss » : {  
  
« actif » : faux,  
  
« eventCode » : « modem.signal.warning »,  
  
« groupCode » : « tower.connectivity.signal.alert »  
  
},  
  
« geoFencing » : {  
  
« actif » : faux,  
  
« AlerteMètresRayons » : 500,  
  
« eventCode » : « geo.fence.breach »,  
  
« groupCode » : « tower.connectivity.geofence.alert »  
  
},  
  
« BrouilleurDedetection » : {  
  
« actif » : faux,  
  
« critères » : {  
  
« signalDropThreshold » : 25,  
  
« minSignalLevel » : -113,  
  
« rsrqThreshold » : -20
```

```

},
« eventCode » : « modem.jammer.detected »,
« groupCode » : « tower.connectivity.jamming.alert »
}
}

```

b. Résumé des codes d'événement et des codes de groupe

Référence rapide pour tous les codes d'événements de connectivité Teltonika et les codes de groupe :

RÈGNE	CODE DE L'ÉVÉNEMENT	CODE DE GROUPE
Changement d'état d'entrée d'E/S	Entrée.change-état	tour.entrée.état-change
Changement d'état de sortie d'E/S	output.statechange	tour.output.statechange
Avertissement d'utilisation des données SIM	sim.data.usage.warning	tower.connectivity.simdata.alert
Perte du réseau cellulaire	modem.signal.warning	tour.connectivité.signal.alerte
Brèche de la géo-clôture	geo.fence.breach	tour.connectivité.geofence.alerte
Détection du brouilleur	modem.jammer.detected	tour.connectivité.jamming.alerte

c. Bonnes pratiques de configuration

- Commencez toujours par Appliquer par défaut pour charger l'ensemble complet des règles préconfigurées avant d'effectuer des modifications.
- Activez les règles de manière incrémentale — commencez par des règles critiques (perte réseau, détection de brouilleurs) avant d'activer des règles sensibles au seuil comme les changements d'état d'E/S.
- Testez les règles d'alarme dans un environnement de staging ou sur un seul appareil avant de déployer sur tous les sites.

- Réglez utilisationWarningPercentpercentage pour les données SIM à 70–80 % afin de laisser aux opérateurs suffisamment de temps pour agir avant que le plan ne soit épuisé.
- Pour le géorepérage sur des sites permanents, utilisez un petit rayon (100–200 m). Pour les déploiements temporaires, utilisez 500 m ou plus.
- Documentez vos codes d'événement et de groupe dans votre configuration CMS pour garantir un bon routage des alarmes.

Configuration OpenVPN sur le routeur Teltonika

Du côté NXGEN, nous vous fournirons un fichier de configuration OpenVPN (ovpn) ainsi qu'un segment IP LAN à attribuer au réseau client.

Configuration étape par étape

1. Changer l'IP LAN par défaut du routeur Teltonika pour l'IP fournie par l'équipe NXGEN

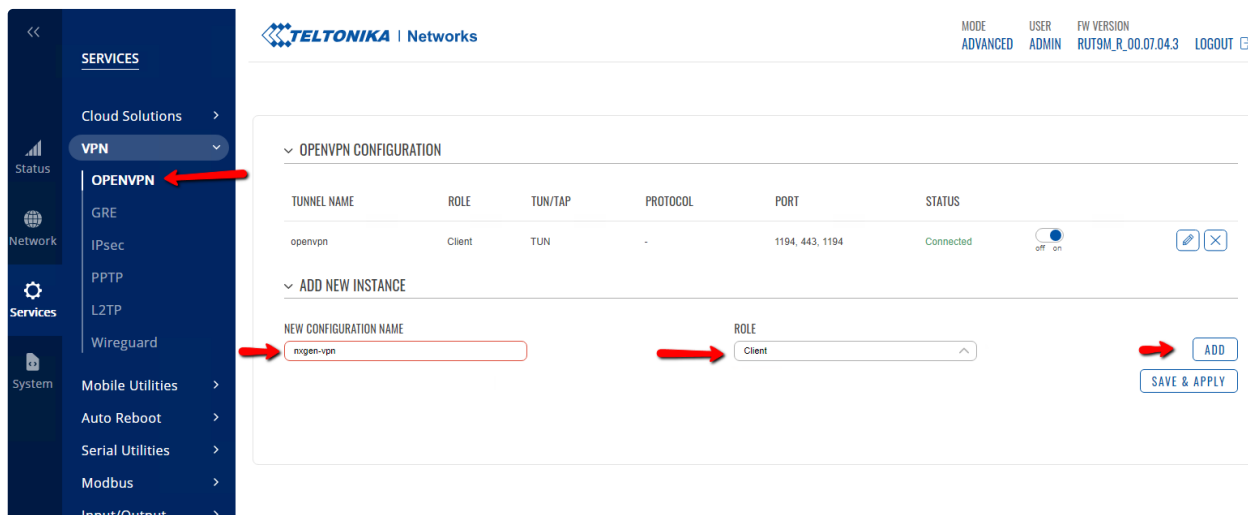
- Ouvre la console web du routeur.
- Naviguer vers Réseau -> Interfaces -> Général -> Modifier le LAN.
- Voici la sauvegarde IP LAN et Subnet ->.

The screenshot shows the Teltonika Networks web interface. On the left, a sidebar menu is visible with the 'NETWORK' section expanded, showing 'Mobile', 'Interfaces', 'Static Leases', 'Wireless', 'Failover', 'Firewall', 'VLAN', 'Routing', and 'DNS'. The 'Interfaces' section is selected, and the 'General' tab is active. The main content area displays a table of network interfaces. The first interface, 'lan', is highlighted with a red arrow pointing to its configuration options (edit, delete, and status toggle). The table lists the following interfaces:

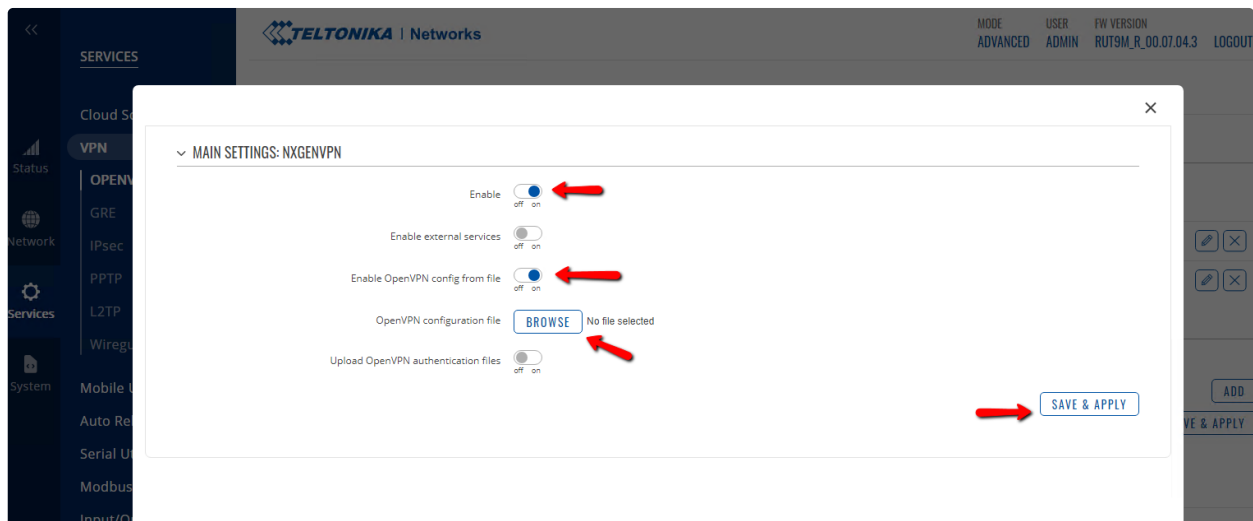
ID	Name	Status	Failover	Type	IP	Protocol	MAC	Uptime	Tx	Rx	Actions	Status Toggle
1	lan	Up	Disabled	Wired	10.175.102.1/24	static	20:97:27:0B:27:3B	26d 21h 50m 2s	8.82 GB	303.10 GB	[Edit] [Delete]	off on
2	vpn1	Down	Disabled	Wired	-	none	-	-	0.00 B	0.00 B	[Edit] [Delete]	off on
3	wan	Down	Disabled	Wired	-	dhcp	20:97:27:0B:27:3C	-	255.55 MB	0.00 B	[Edit] [Delete]	off on
4	wan6	Down	Disabled	Wired	-	dhcpv6	20:97:27:0B:27:3C	-	255.55 MB	0.00 B	[Edit] [Delete]	off on
5	mob1sta1	Up	Disabled	Mobile	10.137.165.227/32	internet	SIM: 1	11h 10m 15s	296.51 GB	7.06 GB	[Edit] [Delete]	off on

2. Importer le fichier de configuration OpenVPN vers le routeur fourni par l'équipe NXGEN

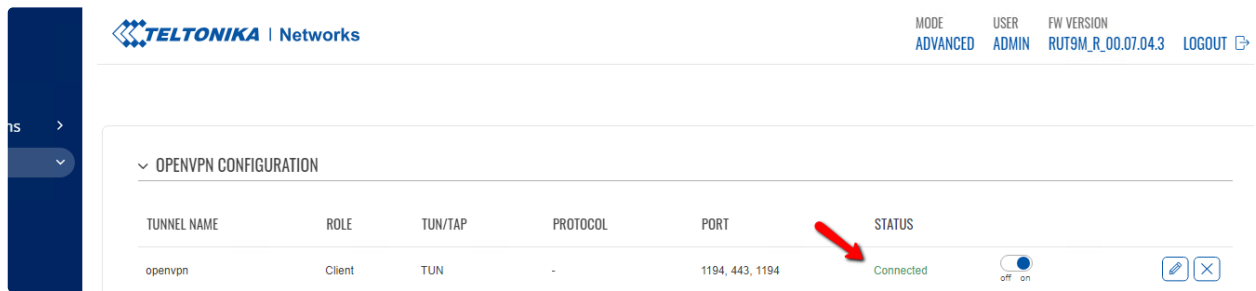
- Sur la console web, naviguez dans Services -> VPN -> OPENVPN.
- Dans l'option Ajouter une nouvelle interface, indiquez « Nom VPN » et définissez le rôle sur « Client » -> Ajouter.



- Sélectionnez « Activer le fichier de configuration OpenVPN » -> Parcourez et attachez le fichier ovpn.
- Sélectionnez Activer et Sauvegarder.

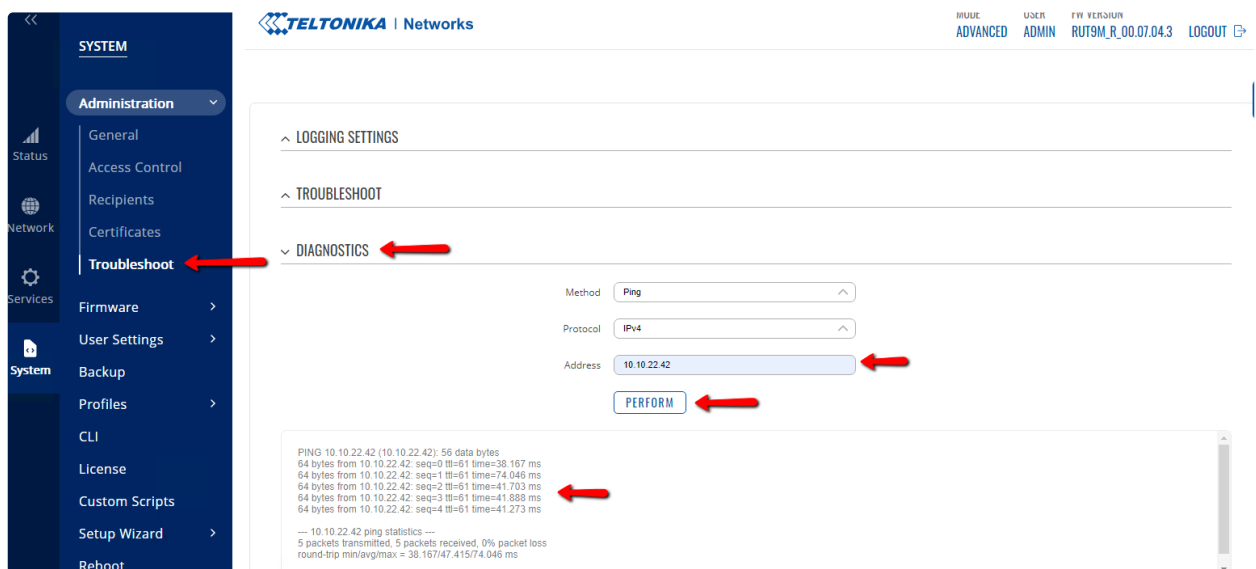


- Après quelques minutes, le statut passe à « Connecté ».



3. Tester la connectivité :

- Naviguez dans System -> Administration -> Dépannage.
- Dans Diagnostic, sélectionnez la méthode « Ping » -> Entrez IP « 10.10.22.42 » -> Exécuter.



- La connexion VPN est configurée avec succès si vous obtenez une réponse de ping réussie.

Dépannage

L'appareil ne se connecte pas

SYMPTÔME / VÉRIFICATION	RÉSOLUTION
La connexion tombe immédiatement après la sauvegarde	Vérifiez que l'adresse IP est accessible depuis le serveur GCXONE. Essayez de pinguer l'IP depuis le serveur ou de vérifier la connectivité VPN.
Erreur d'authentification	Confirmez que le nom d'utilisateur et le mot de passe sont corrects et que vous avez accès administratif. Connectez-vous directement à l'interface d'administration de Teltonika pour vérifier les identifiants.

Défaillance de connexion liée au port	Vérifiez que le port Control configuré est correct et non bloqué par un pare-feu. Par défaut
L'appareil apparaît hors ligne après la connexion initiale	Vérifiez si l'adresse IP du routeur Teltonika a changé (DHCP). Envisagez d'utiliser une IP statique ou une réservation DHCP.

Règles d'alarme qui ne se déclenchent pas

SYMPTÔME / VÉRIFICATION	RÉSOLUTION
Aucune alerte reçue pour un seuil dépassé	Vérifiez que la règle a « active » : vrai dans le JSON. Vérifiez que le JSON des règles d'alarme personnalisées est valide (aucune erreur de syntaxe).
OccurrenceCode n'apparaît pas dans CMS	Confirmez que le code de l'événement est configuré dans votre intégration CMS. Vérifiez la cartographie des canaux CMS dans GCXONE sous les paramètres d'intégration du site.
Fausse alertes positives (trop d'alertes)	Ajustez les seuils. Pour les entrées analogiques
Alertes géo-clôture pour un site fixe	Vérifiez que les coordonnées GPS du site dans GCXONE sont correctement réglées sur l'emplacement réel de la tour. Augmenter les rayonsMètresAvertissement si le signalement GPS présente une variation.

Règle des données SIM qui ne s'active pas

- Assurez-vous que le routeur Teltonika rapporte les indicateurs d'utilisation des données SIM à GCXONE.
- Vérifiez que simDataPackageGB correspond à la taille réelle de votre forfait SIM.
- Le champ simBillingStartDate est actuellement inactif — le suivi de l'utilisation des données utilise pour l'instant le mois calendaire.

Pour un soutien complémentaire, contactez votre représentant NXGEN ou consultez le guide complet de configuration GCXONE Tower Monitoring qui couvre la surveillance Victron Energy et EFOY Fuel Cell en plus de la connectivité IoT Teltonika.