

Aviso legal

Descargo de responsabilidad legal

Esta guía y su contenido (la «Guía») son proporcionados por NXGEN. Todos los derechos sobre la Guía y sobre la propiedad intelectual incorporada en ella — incluidos, entre otros, marcas, nombres comerciales, logotipos y signos similares que figuren en la Guía — están protegidos por la ley. Todos los derechos, títulos e intereses sobre la Guía y sobre los derechos de propiedad intelectual relacionados pertenecen y permanecen con NXGEN y sus licenciantes.

La Guía se proporciona de forma gratuita, «tal cual» y únicamente con fines informativos, sin garantía de ningún tipo. No está destinada ni es adecuada para establecer relación jurídica alguna entre el lector y NXGEN o sus filiales, incluidas, entre otras, obligaciones de NXGEN o de sus filiales frente al lector.

Las obligaciones de NXGEN y de sus filiales respecto de los productos o servicios de NXGEN adquiridos por un cliente se rigen exclusivamente por los términos del contrato en virtud del cual se adquirieron dichos productos o servicios.

Para mayor claridad

El lector asume todo el riesgo en cuanto al uso, los resultados y el rendimiento de la Guía. En la máxima medida permitida por la ley aplicable, NXGEN rechaza y excluye todas las garantías, ya sean legales, expresas o implícitas — incluidas, entre otras, las garantías implícitas de comerciabilidad, idoneidad para un fin determinado, titularidad y no infracción de derechos de terceros — así como cualquier responsabilidad o garantía derivada de sugerencias, especificaciones o muestras relacionadas con la Guía.

Teltonika

Updated 11 August 2026

Introducción

Los routers IoT de Teltonika sirven como columna vertebral de conectividad para la monitorización de torres GCXONE, proporcionando estado celular en tiempo real, seguimiento GPS, cambios de estado de E/S y datos de calidad de señal desde sitios remotos de torres. Esta guía explica todo el proceso de incorporación de un router IoT Teltonika: desde añadir el dispositivo en GCXONE e introducir las credenciales requeridas, hasta configurar las reglas de alarma para pérdida de red, geo-vallado, uso de datos SIM y detección de inhibidores.

Qué monitorizan los dispositivos Teltonika

Una vez conectados a GCXONE, los routers Teltonika informan continuamente de las siguientes categorías de telemetría:

- Estado de la conectividad de red y calidad de señal (RSRQ, RSRP)
- Uso de datos de tarjetas SIM frente a límites mensuales configurados
- Cambios físicos de estado de puertos de entrada/salida (E/S) — digital, analógico, aislado, relé
- Posición GPS relativa al límite del sitio asignado (geo-vallado)
- Detección de interferidores basada en patrones de degradación repentina de señales

Tip

Teltonika se encarga de la comunicación, el seguimiento GPS y el enrutamiento de telemetría en el borde para la torre. Esto lo convierte en la columna vertebral de la monitorización de la conectividad: sin él, GCXONE no puede detectar cortes de red, interferencias de señal ni movimientos no autorizados de dispositivos.

Requisitos previos

Antes de iniciar la incorporación del dispositivo, asegúrese de que la siguiente información y acceso estén disponibles:

REQUISITO	DETALLES
Acceso GCXONE	Rol de administrador u operador con acceso a módulos de configuración
Credenciales de dispositivos	Nombre de usuario y contraseña administrativos para el router Teltonika
Dirección IP	Dirección IP pública o accesible por VPN del dispositivo Teltonika
Número de serie	El número de serie único del router por hardware
Puerto de control	Puerto HTTP usado para la comunicación con dispositivos (por ejemplo
Sitio creado	El sitio al que se asignará este dispositivo debe ya existir en GCXONE

Caution

Asegúrate de que el router Teltonika esté en línea, accesible desde el servidor GCXONE (IP directa o vía VPN) y que las credenciales administrativas proporcionadas tengan acceso completo a la API.

Guía de configuración de Teltonika con GCX-ONE

Sigue estos pasos para añadir un router IoT Teltonika a GCXONE. El dispositivo se registrará en un sitio existente y comenzará a reportar telemetría inmediatamente después de la configuración.

Paso 1 — Navegar hasta el sitio

En GCXONE, navega hasta el sitio donde el dispositivo Teltonika está físicamente instalado. Esta es la entidad matriz bajo la cual se registrará el dispositivo.

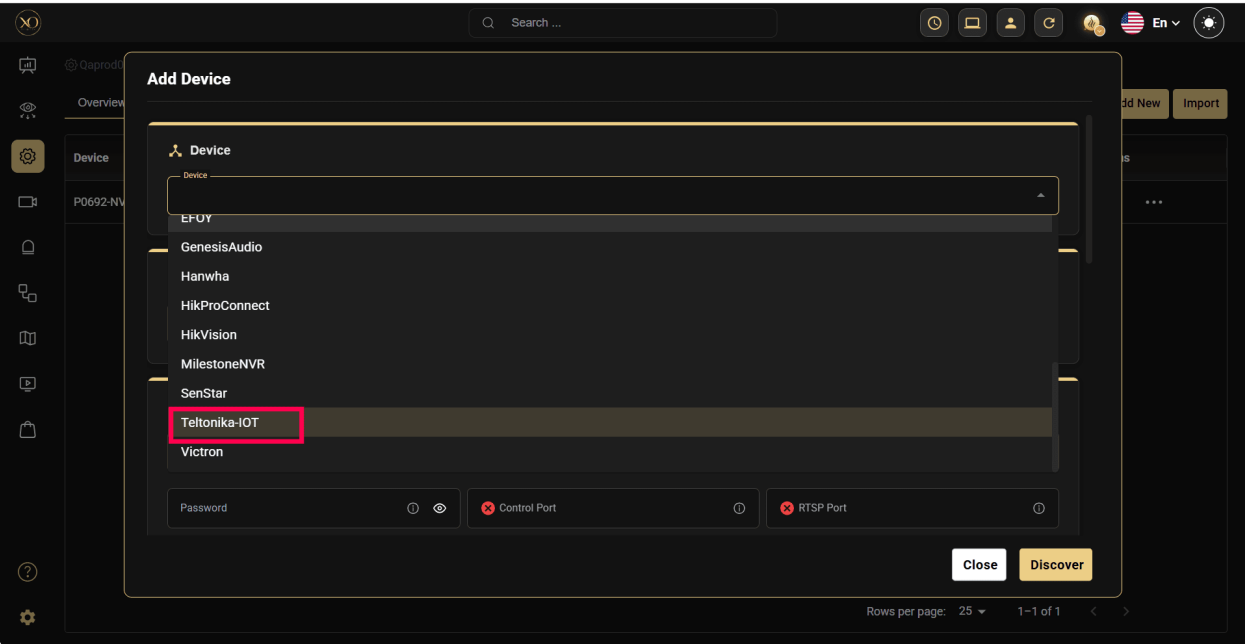
- Ve a Configuración → Sitios
- Localiza y abre el sitio objetivo
- Haz clic en Editar para abrir el panel de configuración del sitio

Paso 2 — Abrir el diálogo de dispositivos

Dentro de la configuración del sitio, navega a la sección Dispositivos y haz clic en Añadir Dispositivo para abrir el cuadro de diálogo de creación de dispositivos.

Paso 3 — Seleccionar el tipo de dispositivo

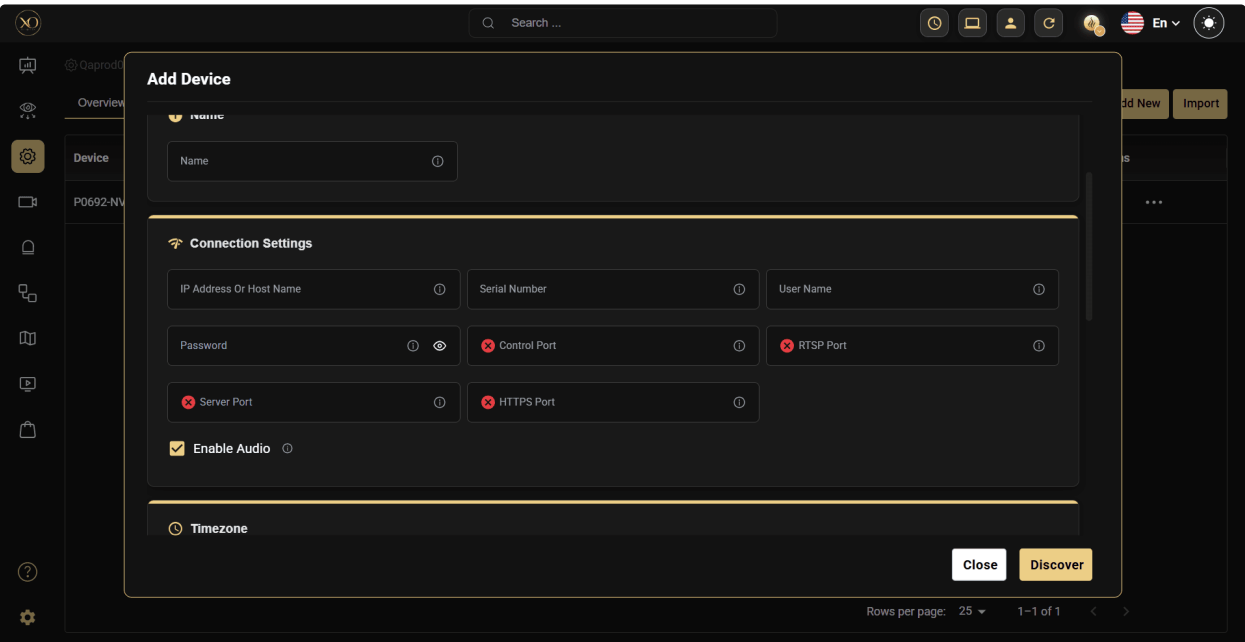
En el cuadro de diálogo de dispositivos, abre el desplegable Tipo de dispositivo y selecciona Teltonika IoT para cargar los campos de configuración correspondientes.



Victron

Paso 4 — Introducir los datos del dispositivo

Rellena todos los campos necesarios para establecer una conexión segura entre GCXONE y el router Teltonika. Cada campo se describe en detalle a continuación.



Victron

CAMPO	DESCRIPCIÓN	NOTAS

Tipo de dispositivo	Selecciona 'Teltonika IoT' en el desplegable	Debe coincidir exactamente — determina qué modelo de telemetría se utiliza
Nombre del dispositivo	Un nombre único y descriptivo para este dispositivo en GCXONE	Utiliza una convención de nombres que identifique el sitio y el dispositivo
Dirección IP	Dirección IP pública o VPN del router Teltonika	Debe ser accesible desde el servidor GCXONE; usar VPN si el dispositivo está detrás de NAT
Número de serie	El número de serie del hardware impreso en el router	Se encuentra en la etiqueta del dispositivo o en el portal de gestión de dispositivos de Teltonika
Puerto de control	Puerto HTTP para la comunicación con dispositivos	El predeterminado suele ser puerto 80; Confirma con la configuración de tu red
Nombre de usuario	Usuario de usuario administrativo del router	Debe tener acceso completo a todos los parámetros y APIs del dispositivo
Contraseña	Contraseña de inicio de sesión administrativa para el router	Almacenado de forma segura dentro de GCXONE; Usa una contraseña fuerte y única

Paso 5 — Guardar y verificar la conexión

Después de introducir todos los campos, haz clic en Guardar. GCXONE intentará inmediatamente establecer una conexión con el router Teltonika utilizando las credenciales proporcionadas.

Una conexión exitosa resulta en:

- El dispositivo aparece en la lista de dispositivos del sitio con un indicador de estado activo
- Datos de telemetría en directo que comienzan a fluir hacia GCXONE (intensidad de la señal, estado de la red, estados de E/S)
- El dispositivo estará disponible para la configuración de reglas de alarma

Caution

Si la conexión falla, verifica que la dirección IP sea accesible, que el puerto esté abierto y que las credenciales sean correctas. Comprueba que ninguna regla de cortafuegos bloquee el acceso de GCXONE al dispositivo

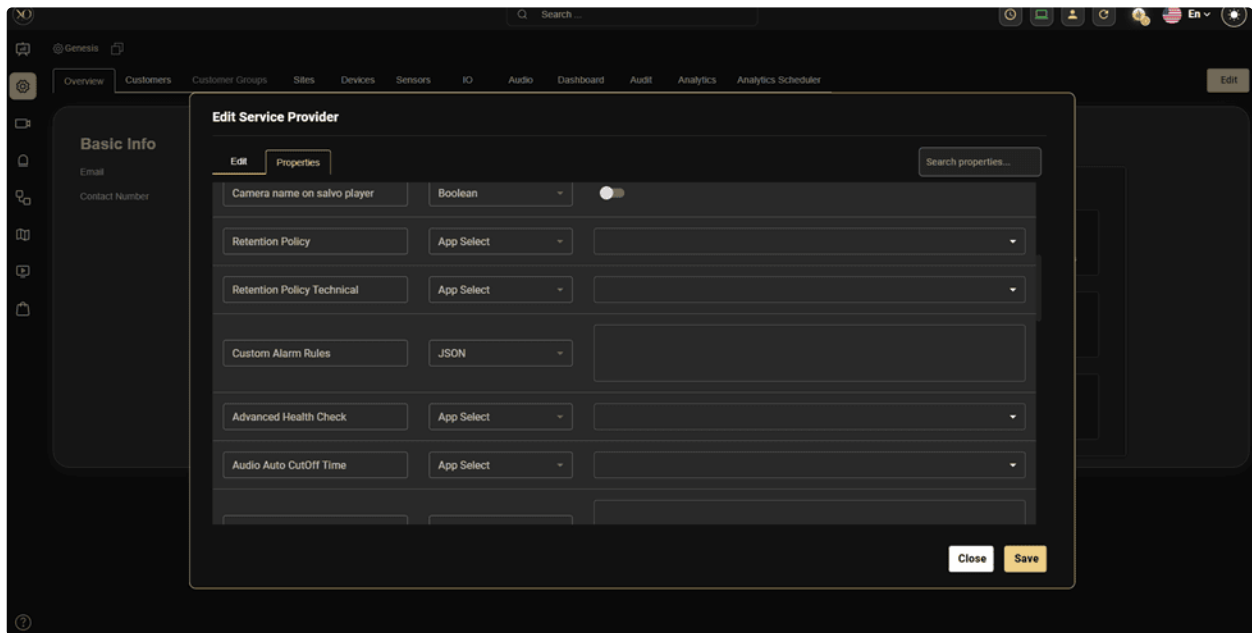
Configuración de las reglas de alarma

GCXONE utiliza una configuración de reglas de alarma basada en JSON para definir qué parámetros de telemetría se monitorizan, qué umbrales activan las alertas y cómo se identifican esas alertas en las integraciones CMS.

Las reglas de alarma pueden configurarse a nivel de sitio o a nivel de dispositivo. Las reglas de conectividad Teltonika se aplican típicamente a nivel de dispositivo para un control de precisión.

Cómo aplicar las reglas de alarma

1. Navega hasta el sitio o dispositivo destino en GCXONE.
2. Haz clic en Editar y ve a la sección de Propiedades Adicionales.
3. Localiza la propiedad llamada Custom Alarm Rules.
4. Abre el menú de hamburguesas (:) de la propiedad y selecciona Aplicar predeterminado para cargar el conjunto de reglas preconfigurado. Todas las reglas están inactivas por defecto.
5. Modifica el JSON para habilitar reglas específicas estableciendo "active": true para los parámetros relevantes.
6. Establece tus umbrales, códigos de evento y códigos de grupo según sea necesario.
7. Haz clic en Guardar. GCXONE comenzará inmediatamente a evaluar la telemetría entrante en función de las reglas configuradas.



Victron

Propina

Por defecto, todas las reglas de alarma están inactivas. Debes establecer explícitamente "activo": verdadero para cada regla que quieras que GCXONE monitoree. Esto evita alertas accidentales durante la configuración inicial.

Estructura de las reglas

Cada regla de alarma sigue una estructura JSON consistente. Entender los campos comunes ayuda a personalizar reglas:

CAMPO	DESCRIPCIÓN
Activo	Booleano (verdadero/falso). Ponlo en true para habilitar la monitorización de esta regla. Cuando es falsa
eventCode	Identificador único de cadena utilizado por GCXONE para comunicar este tipo de alarma a integraciones CMS (IMMIX)
groupCode	Identificador lógico de agrupación para flujos de trabajo de monitorización de torres. Utilizado para filtrar

Tip

Los códigos de evento se utilizan para notificaciones CMS entre sistemas (por ejemplo, IMMIX, Evalink). Los códigos de grupo son identificadores internos de GCXONE para los flujos de trabajo de alarma de torres. Ambos deben estar presentes para una integración completa.

Reglas de Alarma de Conectividad Teltonika

Las siguientes reglas de alarma están disponibles para dispositivos IoT Teltonika en la sección de Monitorización de Conectividad del JSON de Reglas de Alarma Personalizadas. Cada regla supervisa un aspecto específico de la salud de la red, la E/S física o la seguridad.

1. Regla de cambio de estado de entrada/salida

Monitoriza los cambios de estado físico en los puertos de E/S Teltonika. Esta norma cubre entradas y salidas digitales, analógicas, aisladas y de relé — esenciales para detectar aberturas de puertas, eventos de energía, disparadores externos de sensores y cambios de estado del equipo.

Configuración JSON predeterminada

```
"IOStatusChange": {
  "entrada": {
    "AnalogCurrentLoop": {"active": false, "low": 4, "high": 20},
    "AnalogInput": {"active": false, "low": 11, "high": 14},
    "DigitalInput": {"active": false, "ranges": ["Low level", "High level"],
    "alertOn": "Alto Nivel"},
    "InputIsolated": {"active": false, "ranges": ["Low level", "High level"],
```

```

"alertOn": "Alto Nivel"},

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

"alertOn": "Alto Nivel"},

"eventCode": "input.statechange",

"groupCode": "tower.input.statechange"

},

"salida": {

"Salida Aislada": {"activo": falso, "rangos": ["Bajo nivel", "Alto nivel"],

"alertOn": "Alto Nivel"},

"Relé": {"activo": falso, "rangos": ["abierto", "cerrado"], "alertOn": "abierto"},

"PowerSocketOutput": {"activo": falso, "rangos": ["Bajo nivel", "Alto nivel"],

"alertOn": "Alto Nivel"},

"eventCode": "output.statechange",

"groupCode": "tower.output.statechange"

}

} Tipos de entrada

```

TIPO DE ENTRADA	DESCRIPCIÓN Y PARÁMETROS
AnalogCurrentLoop	Monitoriza sensores de bucle de corriente de 4–20 mA. Ajusta bajo/alto al rango de corriente aceptable. Alertas cuando la corriente se aleja de este rango.
AnalogInput	Monitoriza las entradas de voltaje analógicas (por ejemplo

DigitalInput	Monitorización de estado binario. Configura alertOn para el estado que debería activar una alarma (por ejemplo
EntradaAislada	Entrada digital eléctricamente aislada. La misma configuración que DigitalInput. Se utiliza cuando se requiere aislamiento del circuito principal.
PowerSocketInput	Monitoriza el estado del enchufe (nivel bajo/alto). Pon la alerta activada en el estado de activación. Adecuado para la detección de corriente eléctrica.

Tipos de salida

TIPO DE SALIDA	DESCRIPCIÓN Y PARÁMETROS
Salida Aislada	Monitoriza el estado de un canal de salida aislado. Pon alertOn en 'High Level' para avisar cuando la salida esté activa.
Relevo	Estado del relé de las pistas (abierto/cerrado). Pon alerta activado para 'abrir' y alertar cuando el relé no esté energizado. Útil para monitorizar contactores o cerraduras.
PowerSocketOutput	Monitoriza el estado de salida del enchufe de corriente. Avisa cuando la salida alcance el estado de alerta configurado.

2. Regla de uso de paquetes de datos de tarjetas SIM

Rastrea el consumo mensual de datos móviles de la tarjeta SIM del router Teltonika. Activa una advertencia cuando el uso de datos alcanza el porcentaje configurado del total mensual de la asignación — evitando cargos inesperados por excedentes o interrupciones del servicio.

Configuración JSON predeterminada

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

Parámetros de configuración

NOMBRE DEL PARÁMETRO	DESCRIPCIÓN	VALOR DE EJEMPLO

simBillingFecha de inicio	Fecha de inicio del ciclo de facturación del plan SIM (actualmente inactivo)	1
simDataPackageGB	Total de datos móviles asignados al mes (en GB)	10
UsoAvisoPorcentaje	Umbral de advertencia como porcentaje del uso total de datos	80
eventCode	Identificador de alarma CMS para este tipo de evento	sim.data.usage.warning
groupCode	Grupo de alarma interno de torre para filtrado y enrutamiento	torre.conectividad.simdata.alerta

Comportamiento de ejemplo

- Con simDataPackageGB configurado en 10 y usageWarningPercent en 80, GCXONE activa una alerta cuando el uso acumulado de datos de la SIM supera los 8GB durante el periodo de facturación.
- La alerta se elimina automáticamente cuando el uso de datos se reinicia al inicio del nuevo ciclo de facturación.
- Ajusta el umbral más bajo (por ejemplo, un 70%) para la alerta temprana en sitios con alternativas de conectividad limitadas.

3. Regla de Pérdida de Red Celular

Detecta cuando el router Teltonika pierde conectividad a la red móvil o la señal cae a un nivel inaceptable.

Alerta inmediatamente a los operadores sobre posibles fallos en la comunicación en el sitio.

Configuración JSON predeterminada

```
"cellNetworkLoss": {
  "activo": falso,
  "eventCode": "modem.signal.warning",
  "groupCode": "tower.connectivity.signal.alert"
```

}

Comportamiento de ejemplo

- GCXONE activa una alerta cuando la señal celular baja del umbral aceptable o se pierde por completo la conectividad.
- La alerta se disipa automáticamente una vez que la señal vuelve a un nivel aceptable.
- Esta regla no tiene parámetros umbral — se basa en la evaluación de calidad de señal integrada de GCXONE para el estado reportado del módem del router.

4. Regla de Geo-Cercado

Monitoriza la posición GPS del router Teltonika en relación con la ubicación asignada a su sitio. Activa una alerta si el dispositivo se mueve más allá del radio configurado — detectando posible desplazamiento de la torre, robo o movimiento no autorizado.

Configuración JSON predeterminada

```
"geoFencing": {
  "activo": falso,
  "AlertaRadioMetros": 500,
  "eventoCode": "geo.fence.breach",
  "groupCode": "tower.connectivity.geofence.alert"
}
```

NOMBRE DEL PARÁMETRO	DESCRIPCIÓN	VALOR DE EJEMPLO
RadioMedidoresAviso	Radio (en metros) desde el centro de geovalla definido (típicamente	la ubicación geográfica del sitio) dentro del cual debe permanecer la torre

eventCode	Identificador de alarma CMS para eventos de brecha de geovallas	geo.fence.breach
groupCode	Identificador interno de grupo de alarma de torre	torre.conectividad.geofence.alerta

Comportamiento de ejemplo

- El límite de la geo-valla se centra en las coordenadas definidas en la configuración del sitio principal en GCXONE.
- Si la posición GPS reportada por el router Teltonika supera los 500 metros desde el centro del sitio, se genera una alerta de brecha.
- La alerta se elimina automáticamente cuando el dispositivo regresa dentro del límite definido.
- Reducir el radio para instalaciones fijas permanentes; Utiliza un radio mayor para despliegues de torres móviles o semi-móviles.

5. Regla de detección de interferidores

Detecta posibles intentos de interferencia por radiofrecuencia basados en una degradación repentina de la señal y una mala calidad de señal de referencia recibida (RSRQ). La detección de interferidores es fundamental para despliegues de torres sensibles a la seguridad donde la interferencia de señal puede indicar intentos deliberados de interrupción.

Configuración JSON predeterminada

```
"jammerDetection": {
  "activo": falso,
  "criterios": {
    "signalDropThreshold": 25,
    "minSignalLevel": -113,
```

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

NOMBRE DEL PARÁMETRO	DESCRIPCIÓN	VALOR DE EJEMPLO
signalDropThreshold	Disminución porcentual en la intensidad de la señal considerada como un posible evento de interferencia	25
minSignalLevel	Nivel mínimo aceptable de señal (en dBm); Si la señal baja de esto	se sospecha interferencia
rsrqThreshold	RSRQ mínimo aceptable (Calidad de Señal de Referencia Recibida); una RSRQ pobre puede indicar interferencias	-20
eventCode	Identificador CMS para eventos de detección de interferidores	modem.jammer.detected
groupCode	Identificador de grupo de alarma de torre	tower.connectivity.jamming.alert

Comportamiento de ejemplo

- GCXONE evalúa tanto el nivel absoluto de señal (RSRQ) como la tasa de cambio de señal (porcentaje de caída) para distinguir la interferencia genuina de la variación normal de la señal.
- Se activa una alerta cuando la caída de señal supera el 25% O cuando el RSRQ cae por debajo de -20 y el nivel de señal está por debajo de -113 dBm simultáneamente.
- La alerta se elimina automáticamente una vez que se restablece la estabilidad normal de la señal.

Tip

Los umbrales de detección de interferidores pueden necesitar ajustes basados en las condiciones del entorno local de RF. Los emplazamientos en áreas urbanas con variación natural de señal pueden requerir un umbral de caída más alto para reducir los falsos positivos.

Referencia de configuración

a. Reglas completas de alarma de conectividad Teltonika JSON

A continuación se muestra la configuración completa predeterminada de JSON para todas las reglas de alarma de conectividad de Teltonika. Copia esto en la propiedad de Reglas de Alarma Personalizadas y modifícalo según sea necesario para tu despliegue.

```
"connectivityMonitoring": {
  "IOStatusChange": {
    "entrada": {
      "AnalogCurrentLoop": {"active": false, "low": 4, "high": 20},
      "AnalogInput": {"active": false, "low": 11, "high": 14},
      "DigitalInput": {"active": false, "ranges": ["Low level", "High level"]},
      "alertOn": "Alto Nivel"},
    "InputIsolated": {"active": false, "ranges": ["Low level", "High level"]},
    "alertOn": "Alto Nivel"},
    "PowerSocketInput": {"active": false, "ranges": ["Low level", "High level"]},
    "alertOn": "Alto Nivel"},
```

```
"eventCode": "input.statechange",

"groupCode": "tower.input.statechange"

},

"salida": {

"Salida Aislada": {"activo": falso, "rangos": ["Bajo nivel", "Alto nivel"],

>alertOn": "Alto Nivel"},

"Relé": {"activo": falso, "rangos": ["abierto", "cerrado"], "alertOn": "abierto"},

"PowerSocketOutput": {"activo": falso, "rangos": ["Bajo nivel", "Alto nivel"],

>alertOn": "Alto Nivel"},

"eventCode": "output.statechange",

"groupCode": "tower.output.statechange"

}

},

"simCardDataPackage": {

"activo": falso,

"simBillingDateStartDate": 1,

"simDataPackageGB": 10,

"PorcentajeAdvertencia de uso": 80,

"eventCode": "sim.data.usage.warning",
```

```
"groupCode": "tower.connectivity.simdata.alert"

},

"cellNetworkLoss": {

"activo": falso,

"eventCode": "modem.signal.warning",

"groupCode": "tower.connectivity.signal.alert"

},

"geoFencing": {

"activo": falso,

"AlertaRadioMetros": 500,

"eventoCode": "geo.fence.breach",

"groupCode": "tower.connectivity.geofence.alert"

},

"jammerDetection": {

"activo": falso,

"criterios": {

"signalDropThreshold": 25,

"minSignalLevel": -113,

"rsrqThreshold": -20
```

```

},

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

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

}

}

```

b. Resumen de Códigos de Eventos y Códigos de Grupo

Referencia rápida para todos los códigos de eventos de conectividad y códigos de grupo de Teltonika:

GOBIERNO	CÓDIGO DEL EVENTO	CÓDIGO DE GRUPO
Cambio de estado de entrada de E/S	Input.statechange	torre.entrada.estado-cambio
Cambio de estado de salida de E/S	output.statechange	torre.salida.estadoestado
Advertencia de uso de datos SIM	sim.data.usage.warning	torre.conectividad.simdata.alerta
Pérdida de la red celular	modem.signal.warning	torre.conectividad.señal.alerta
Brecha de la valla geoespacial	geo.fence.breach	torre.conectividad.geofence.alerta
Detección de interferidores	modem.jammer.detected	tower.connectivity.jamming.alert

c. Mejores prácticas de configuración

- Siempre empieza con Aplicar Default para cargar el conjunto completo de reglas preconfiguradas antes de hacer cambios.
- Activa las reglas de forma incremental — comienza con reglas críticas (pérdida de red, detección de interferidores) antes de activar reglas sensibles al umbral como los cambios de estado de E/S.
- Prueba las reglas de alarma en un entorno de staging o en un solo dispositivo antes de desplegarlas en todos los sitios.
- Establece el usoAvisoPorcentaje de datos SIM en un 70–80% para dar a los operadores tiempo suficiente para actuar antes de que el plan se agote.

- Para la geovallada en sitios permanentes, utiliza un radio pequeño (100–200 m). Para despliegues temporales, usa 500 m o más.
- Documenta tus códigos de evento y de grupo en la configuración de tu CMS para asegurar un correcto enrutamiento de alarmas.

Configuración de OpenVPN en el router Teltonika

Desde el lado de NXGEN, te proporcionaremos un archivo de configuración OpenVPN (ovpn) y un segmento de IP LAN que debe asignarse a la red del cliente.

Configuración paso a paso

1. Cambiar la IP LAN predeterminada del router Teltonika por la IP proporcionada por el equipo NXGEN

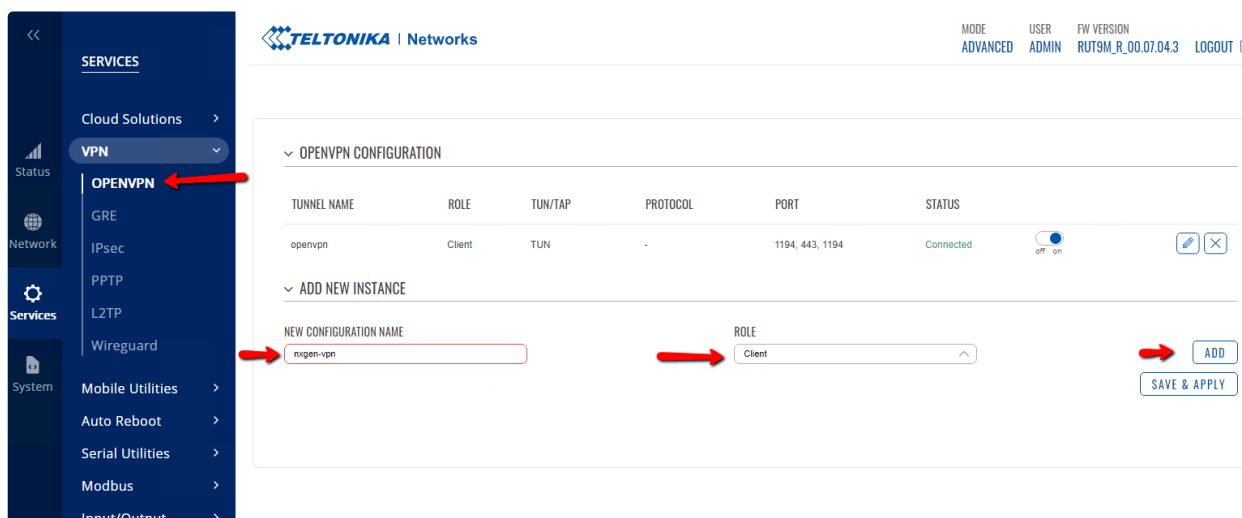
- Abre la consola web del router.
- Navegar a Red -> Interfaces -> General -> Editar LAN.
- Aquí entra el guardado de la IP LAN y la subred de >.

ID	Name	Status	Failover	Type	IP	Protocol	MAC	Uptime	Tx	Rx	Actions	Toggle
1	lan	Up	Disabled	Wired	10.175.102.1/24	static	20:97:27:0B: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

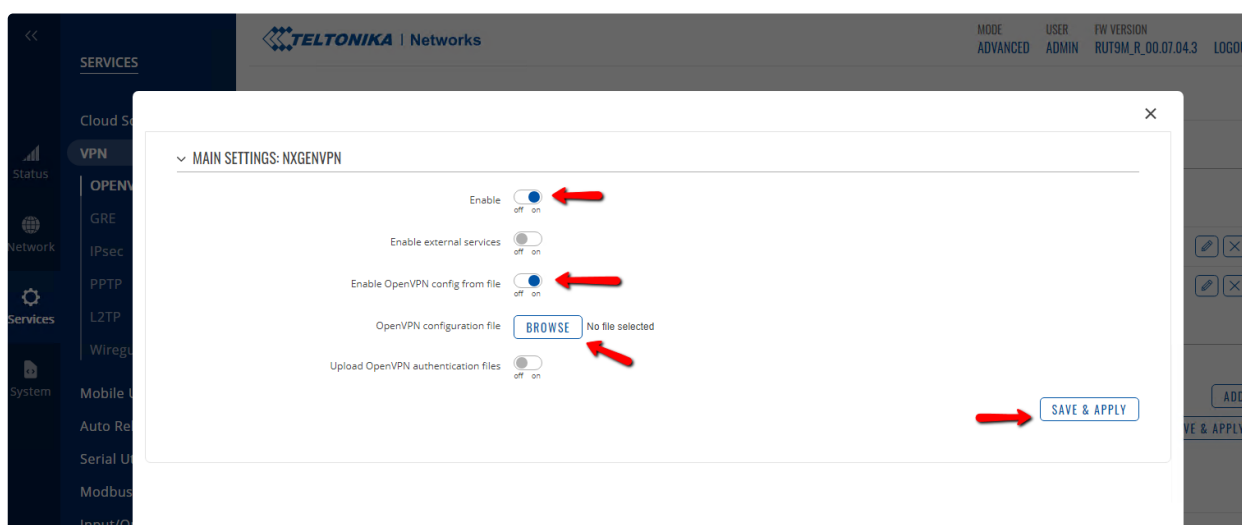
2. Importar el archivo de configuración de OpenVPN al router proporcionado por el equipo de NXGEN

- En la consola web, navega a Services -> VPN -> OPENVPN.

- En la opción Añadir nueva interfaz, proporciona el "Nombre de la VPN" y configura el rol en "Cliente" -> Añadir.



- Selecciona "Activar el archivo de configuración OpenVPN" -> Navega y adjunta el archivo ovpn.
- Selecciona Habilitar y guardar.



- Tras un par de minutos, el estado cambiará a "Conectado".

3. Probar la conectividad:

- Navega a Administración de Sistema > > Solucionar problemas.
- En Diagnóstico, selecciona el método "Ping" -> Introduce IP "10.10.22.42" -> Realizar.

- La conexión VPN se configura correctamente si recibes una respuesta de ping exitosa.

Resolución de problemas

El dispositivo no se conecta

SÍNTOMA / COMPROBACIÓN	RESOLUCIÓN
La conexión falla inmediatamente después de guardar	Verifica que la dirección IP sea accesible desde el servidor GCXONE. Prueba a hacer ping a la IP del servidor o comprobar la conectividad de la VPN.
Error de autenticación	Confirma que el nombre de usuario y la contraseña son correctos y tienes acceso administrativo. Inicia sesión directamente en la interfaz de administración de Teltonika para verificar las credenciales.

Fallo de conexión relacionado con los puertos	Comprueba que el puerto de control configurado esté correcto y no esté bloqueado por un cortafuegos. Por defecto es el puerto 80.
El dispositivo aparece desconectado tras la conexión inicial	Comprueba si la dirección IP del router Teltonika ha cambiado (DHCP). Considera usar una IP estática o una reserva DHCP.

Reglas de alarma que no se activan

SÍNTOMA / COMPROBACIÓN	RESOLUCIÓN
No se han recibido alertas por un umbral de superación	Verifica que la regla tenga "activo": verdadero en el JSON. Comprueba que el JSON de las Reglas de Alarma Personalizadas sea válido (sin errores de sintaxis).
EventCode no aparece en CMS	Confirma que el código del evento está configurado en tu integración CMS. Consulta el mapeo de canales CMS en GCXONE bajo la configuración de integración del sitio.
Falsos positivos (demasiadas alertas)	Ajusta los umbrales. Para entradas analógicas
Alertas de geovallas para un sitio fijo	Verifica que las coordenadas GPS del sitio en GCXONE estén correctamente configuradas con la ubicación real de la torre. Aumentar radioMetrosAviso si la notificación por GPS tiene variaciones.

Regla de datos SIM no se activa

- Asegúrate de que el router Teltonika esté informando las métricas de uso de datos de la SIM a GCXONE.
- Verifica que simDataPackageGB coincida con el tamaño real de tu plan SIM.
- El campo simBillingStartDate está actualmente inactivo — el seguimiento del uso de datos utiliza el mes calendario por ahora.

Para más soporte, contacte con su representante de NXGEN o consulte la Guía completa de Configuración de Monitorización de Torres de GCXONE, que cubre la monitorización de Victron Energy y EFOY Fuel Pil, además de la conectividad IoT de Teltonika.