Carte SIM et eSIM IoT qui ne se connecte pas : guide de dépannage complet

Introduction

Lorsqu'un objet connecté caméra 4G, traceur GPS, centrale d'alarme, routeur industriel refuse de se connecter au réseau cellulaire lors de sa première mise en service, l'origine du problème se trouve dans trois causes dominantes : un code PIN actif que l'objet ne peut pas saisir, une configuration APN absente ou erronée, ou l'absence d'autorisation d'itinérance (roaming) sur la SIM.

Les autres dysfonctionnements (déconnexions intempestives, échec de téléchargement de profil eSIM, faible signal) découlent généralement de problèmes secondaires : steering opérateur, incompatibilité de bandes de fréquences, ou défaut d'antenne. Ce guide traite chaque cas par ordre de fréquence, avec les procédures de diagnostic exploitables sur le terrain.

1. Problème n°1 : la carte SIM refuse de se connecter (erreur d'authentification)

Réponse directe : Dans 80 % des cas, l'erreur d'authentification provient d'un code PIN encore actif sur la carte SIM. Il faut désactiver ce code via un smartphone avant d'insérer la SIM dans l'objet connecté.

1.1 La cause principale : le code PIN actif

La majorité des objets connectés industriels (caméras IP cellulaires, traceurs GPS, balises, centrales d'alarme) ne disposent d'aucune interface de saisie pour entrer un code PIN. Lorsqu'une SIM protégée par PIN est insérée, le modem reste bloqué en état `SIM PIN required` et ne procède jamais à l'enregistrement réseau (commande AT correspondante : `AT+CPIN?` retournant `+CPIN: SIM PIN`).

Certains équipements haut de gamme permettent de pré-renseigner un code PIN dans leur configuration logicielle, mais cette option reste rare et expose à un blocage définitif (code PUK) en cas d'erreur de saisie répétée. La pratique standard consiste à désactiver totalement la demande de PIN sur la SIM avant son insertion finale.

1.2 Procédure de désactivation du code PIN

1. Insérer la carte SIM dans un smartphone classique (Android ou iOS) compatible avec le format physique (2FF, 3FF ou 4FF).
2. Saisir le code PIN initial lors du démarrage du téléphone (généralement fourni sur le support cartonné de la SIM).
3. Ouvrir les paramètres : sur Android, *Paramètres → Sécurité → Verrouillage de la SIM* ; sur iOS, *Réglages → Cellulaire → PIN de la SIM*.

4. Désactiver l'option « Verrouiller la SIM » ou « PIN de la SIM ». Le téléphone redemandera le code PIN actuel pour confirmer.
5. Éteindre le téléphone, retirer la SIM, l'insérer dans l'objet connecté, puis redémarrer ce dernier.

Si la SIM est bloquée par trois saisies erronées du PIN, un code PUK à 8 chiffres devient nécessaire. Il est fourni par l'émetteur de la SIM (opérateur ou MVNO IoT) via son espace client ou sa plateforme de gestion CMP.

1.3 Autres causes possibles d'erreur d'authentification

- **SIM non activée côté opérateur** : la carte est physiquement présente mais son IMSI n'est pas encore enregistré sur le HLR/HSS. Vérifier le statut sur la CMP (statut attendu : *Active*, non *Inventory* ou *Test ready*).
- **SIM mal insérée ou contacts oxydés** : retirer, nettoyer les contacts dorés avec un chiffon sec, repositionner.
- **Incompatibilité de tension** : certaines SIM industrielles MFF2 fonctionnent en 1,8 V uniquement, certaines anciennes en 3 V. Vérifier la fiche technique du modem.
- **SIM expirée ou résiliée** : commande AT `AT+CIMI` retourne l'IMSI mais l'enregistrement échoue avec `+CREG: 0,3` (registration denied).

2. Problème n°2 : l'objet capte le réseau mais la data ne fonctionne pas (erreur APN)

Réponse directe : Quand le modem affiche un bon signal et un opérateur visible mais que les données ne passent pas, la cause quasi systématique est un APN (Access Point Name) absent ou incorrect. La configuration doit être saisie manuellement, l'auto-détection échouant sur la plupart des SIM IoT/MVNO.

2.1 Pourquoi l'APN doit-il être configuré manuellement ?

L'APN est la passerelle logique qui relie le modem cellulaire au réseau de destination (Internet public ou réseau privé du client). Les smartphones grand public détectent automatiquement le bon APN grâce à une base de données interne croisant le MCC (Mobile Country Code) et le MNC (Mobile Network Code) de la SIM. Cette base ne contient pas les APN des MVNO IoT, dont les SIM utilisent souvent des MCC/MNC non répertoriés ou partagés.

Les modems IoT (Quectel, u-blox, Sierra Wireless, Telit, SimCom) suivent une logique différente : ils utilisent l'APN explicitement défini dans leur configuration (commande AT `AT+CGDCONT`) ou laissé vide. En l'absence d'APN ou avec un APN erroné, le modem s'enregistre sur le réseau cellulaire (signal présent, opérateur détecté) mais aucun contexte PDP n'est établi : aucun trafic IP ne transite.

2.2 Méthodes de configuration manuelle de l'APN

Selon le type d'équipement, trois méthodes coexistent :

- **Interface web du routeur ou de la caméra** : se connecter à l'adresse IP locale par défaut (typiquement 192.168.1.1 ou 192.168.8.1), section « WAN cellulaire » ou « Cellular », renseigner le champ APN, éventuellement le nom d'utilisateur et le mot de passe (souvent vides pour les SIM M2M).
- **Application mobile dédiée du fabricant** : courante sur les caméras 4G, les traceurs grand public et les centrales d'alarme. La SIM est configurée par Bluetooth ou Wi-Fi direct depuis le smartphone d'installation.
- **SMS de configuration** : sur les traceurs GPS et certaines alarmes, on envoie un SMS structuré au numéro de la SIM IoT. Le format dépend du fabricant : `admin123456 apn,iot.provider.com,,#` est un format typique chez les traceurs chinois (mot de passe administrateur, commande, APN, utilisateur, mot de passe).
- **Commandes AT en accès direct** : sur les modems industriels, via port série ou USB : `AT+CGDCONT=1,"IP","iot.provider.com"`, puis `AT+CGACT=1,1` pour activer le contexte PDP.

2.3 Tableau de synthèse des APN typiques

Type de réseau	Nom de l'APN type	Usage
Opérateur grand public (illustratif)	`orange`, `sl2sfr`, `mmsbouygtel.com`, `free`	Navigation Internet mobile sur SIM B2C contractuellement inadapté à l'IoT
MVNO IoT public générique	`iot.[provider].com`, `m2m.[provider].com`, `global.data`	APN public partagé entre tous les clients du MVNO ; IP publique dynamique
APN privé client	`[clientname].private`, `[customcode].vpn`	Passerelle dédiée vers le SI du client via VPN IPsec ou MPLS, IP fixe possible
APN fixe IP (statique)	`iotfix.[provider].com`, `static.m2m`	IP publique fixe pour objets joignables depuis l'extérieur (caméras, automates)
APN LTE-M / NB-IoT dédié	`iot.nb`, `lpwa.[provider]`	Passerelle dimensionnée pour les profils basse consommation et faible débit

Les noms exacts d'APN sont communiqués par le fournisseur de connectivité IoT lors de la livraison des SIM. En cas de doute, la commande AT `AT+CGDCONT?` permet de vérifier l'APN actuellement chargé, et `AT+COPS?` de confirmer l'opérateur sur lequel la SIM est enregistrée.

2.4 Validation de l'établissement de la session data

- **État du contexte PDP** : `AT+CGACT?` doit retourner `+CGACT: 1,1` (contexte 1 actif).
- **Attribution d'une IP** : `AT+CGPADDR=1` retourne l'adresse IP attribuée par le réseau. Une absence d'IP indique un APN erroné ou un refus du réseau.
- **Test ping** : depuis le routeur cellulaire, lancer un ping vers `8.8.8.8` ou `1.1.1.1`. L'échec malgré un PDP actif indique un blocage côté APN privé (firewall opérateur).

3. Problème n°3 : dysfonctionnements spécifiques aux eSIM et profils eUICC

Réponse directe : Une eSIM IoT qui ne s'active pas a généralement échoué lors du téléchargement OTA de son profil opérateur, faute de couverture initiale suffisante ou d'autorisation côté plateforme de gestion. Le diagnostic se fait sur la CMP en vérifiant le passage du statut *Test* ou *Available* à *Enabled*.

3.1 Échec de téléchargement du profil OTA

L'eSIM eUICC est livrée avec un *bootstrap profile* minimal permettant uniquement de joindre le serveur SM-DP+ (Subscription Manager Data Preparation) afin d'y télécharger le profil opérateur final. Trois conditions doivent être réunies pour que le téléchargement aboutisse :

- **Couverture cellulaire minimale** sur le réseau autorisé par le bootstrap profile. Un objet placé dans un local technique sans signal ne peut pas réaliser son provisioning initial. Il faut effectuer la première mise sous tension en extérieur ou près d'une fenêtre.
- **Joignabilité du serveur SM-DP+** depuis le réseau de bootstrap. Certains réseaux d'entreprise bloquent les flux sortants vers les adresses des SM-DP+ ; le test doit être conduit sur une connectivité non filtrée.
- **Autorisation du téléchargement côté CMP** : le profil opérateur cible doit être affecté à l'eUICC concernée (identifiée par son EID eUICC Identifier composé de 32 chiffres).

3.2 Vérification du statut sur la CMP

La plateforme de gestion (CMP) du fournisseur de connectivité expose plusieurs statuts pour chaque profil eUICC. La progression attendue est la suivante :

Statut	Signification	Action requise
Available / *Released*	Profil créé chez l'opérateur, non encore lié à un EID	Affecter le profil à l'EID de l'objet
Linked / *Allocated*	Profil affecté à un EID, en attente de téléchargement	Mettre sous tension l'objet en zone couverte
Downloaded	Profil téléchargé sur l'eUICC, non encore activé	Déclencher l'activation depuis la CMP
Enabled / *Active*	Profil actif, l'objet utilise ce profil pour se connecter	Aucune ; état nominal
Disabled	Profil présent mais inactif (un autre profil est utilisé)	Activer si nécessaire
Deleted	Profil supprimé de l'eUICC	Provisionner un nouveau profil si besoin

3.3 Diagnostic complémentaire au niveau du modem

- **Lecture de l'EID** : commande AT `AT+CCID` ou `AT+SQNEID` selon le constructeur, pour confirmer que l'eUICC est physiquement reconnue.
- **Liste des profils chargés** : sur les modems compatibles LPA (Local Profile Assistant), commande `AT+SQNGETPROFILES` ou équivalent constructeur.
- **Logs du modem** : activer le niveau verbose et capturer la séquence de communication avec le SM-DP+ (handshake TLS, téléchargement du profil chiffré).

4. Problème n°4 : déconnexions intempestives ou absence totale de signal

Réponse directe : Les déconnexions répétées proviennent généralement d'un steering of roaming agressif sur les SIM grand public ou d'une incompatibilité de bandes de fréquences sur le matériel importé. Une SIM IoT multi-opérateur sans steering et un équipement supportant les bandes locales résolvent ces deux cas.

4.1 Le piège du « steering of roaming »

Le steering of roaming désigne la pratique par laquelle l'opérateur émetteur d'une SIM force le terminal à se réenregistrer périodiquement sur ses partenaires d'itinérance privilégiés, même quand un autre réseau offre un meilleur signal localement. Sur une SIM grand public en zone frontalière ou rurale, ce mécanisme se traduit par :

- Des bascules récurrentes entre opérateurs avec coupure de session data à chaque rejet.
- Des tentatives répétées de se rattacher à un opérateur trop éloigné, échouant après plusieurs minutes.
- Une autonomie batterie dégradée (le modem émet en permanence à pleine puissance).

Une SIM IoT multi-opérateur sans steering s'enregistre sur le réseau présentant la meilleure qualité radio mesurée (RSRP, RSRQ) et n'en change qu'en cas de dégradation effective. Sur ce type de SIM, la commande `AT+COPS=0` active la sélection automatique de réseau, et `AT+COPS?` affiche en continu le PLMN actuellement utilisé.

4.2 Compatibilité des bandes de fréquences

Un équipement IoT importé hors zone CE (Asie, Amérique du Nord) peut être incompatible avec les bandes utilisées en Europe. Les bandes critiques pour la couverture rurale et indoor sont notamment :

Bande LTE	Fréquence	Utilisation en France
B1	2100 MHz	4G urbaine standard
B3	1800 MHz	4G principale, capacité élevée
B7	2600 MHz	4G urbaine, haut débit
B8	900 MHz	4G de couverture rurale
B20	800 MHz	4G de couverture étendue, pénétration indoor
B28	700 MHz	4G et 5G en zones rurales et indoor profond
n78	3500 MHz	5G urbaine principale

Un appareil ne supportant pas B20 ni B28 sera inopérant dans la plupart des zones rurales françaises. Vérifier impérativement la fiche technique du modem (souvent listée sous la forme `LTE Cat-4 B1/B3/B7/B8/B20/B28`) avant l'achat. Pour le LTE-M et le NB-IoT, les bandes principalement déployées en France sont B8 (900 MHz) et B20 (800 MHz).

4.3 Mesure du signal et interprétation

- **RSSI** (commande `AT+CSQ`) : valeur de 0 à 31 (99 = inconnu). Au-delà de 15, le signal est exploitable ; en-dessous de 10, des déconnexions sont probables.
- **RSRP** (LTE) : référence absolue, exprimée en dBm. Au-dessus de -85 dBm = excellent ; -85 à -100 dBm = bon ; -100 à -110 dBm = correct ; en-dessous de -110 dBm = marginal.
- **RSRQ** (LTE) : qualité du signal, en dB. Au-dessus de -10 dB = bon ; en-dessous de -15 dB = mauvais (interférences ou cellule saturée).

4.4 Signification des LED de diagnostic

L'interprétation exacte dépend du fabricant, mais les conventions suivantes sont largement partagées sur les modules IoT cellulaires :

État de la LED	Signification standard	Action
Éteinte	Module hors tension ou en veille profonde	Vérifier l'alimentation et le câblage
Rouge fixe	Pas de carte SIM détectée ou erreur matérielle	Vérifier l'insertion et la propreté des contacts
Rouge clignotant	SIM détectée mais authentification échouée (PIN, IMSI rejeté)	Vérifier le statut PIN et l'activation côté CMP
Orange / jaune clignotant lent	Recherche de réseau en cours	Patienter, vérifier l'antenne et le signal
Vert clignotant lent (~1 Hz)	Enregistré sur le réseau, contexte data non actif	Vérifier la configuration APN
Vert clignotant rapide (~5 Hz)	Transfert de données en cours	État normal en activité
Vert fixe	Connecté au réseau, session data établie, aucun trafic	Aucune ; état nominal
Bleue (selon constructeur)	Connexion 5G ou LTE-M / NB-IoT active	Aucune ; état nominal

Sur les caméras 4G, le code couleur est souvent affiché directement dans l'interface logicielle ou l'application mobile sous forme d'indicateur de qualité (1 à 5 barres). Préférer la lecture du RSRP en dBm quand cette valeur est exposée.

5. Checklist ultime de vérification avant déploiement

Réponse directe : Avant de fixer définitivement un objet connecté sur son site d'exploitation, il convient de valider successivement la configuration logicielle (PIN, APN, eSIM), la qualité radio (signal, bande), l'antenne (raccordement, protections retirées) et la connectivité IP (test

ping et accès distant). Sauter une étape conduit dans la quasi-totalité des cas à une intervention terrain coûteuse.

5.1 Liste de vérification terrain

- Code PIN de la SIM désactivé via un smartphone, ou eSIM provisionnée et statut *Enabled* confirmé sur la CMP.
- APN renseigné manuellement selon les paramètres fournis par le fournisseur de connectivité (nom, utilisateur, mot de passe, type d'IP).
- Itinérance des données (data roaming) activée dans la configuration du modem si la SIM est multi-opérateur option indispensable même en usage national sur SIM IoT.
- SIM ou eSIM activée côté plateforme CMP, avec un forfait suffisant ou un pool de data partagée alimenté.
- Antennes externes vissées à la main puis à la clé (couple typique 0,5 à 1 N·m), tous les capuchons et films plastiques de protection retirés des connecteurs SMA/RP-SMA.
- Polarisation et orientation des antennes optimisées (diversité spatiale entre antenne principale et antenne MIMO, séparation minimale de 10 cm).
- Bandes de fréquences supportées par l'équipement vérifiées contre la couverture locale (B20 et B28 indispensables en zone rurale française).
- Test de signal sur site final : RSRP > -100 dBm et RSRQ > -13 dB recommandés pour un usage stable.
- Test de ping réussi vers une adresse publique (`8.8.8.8`) depuis l'équipement, confirmant l'établissement du contexte PDP.
- Pour les équipements joignables (caméras, automates), test d'accès distant effectif depuis l'extérieur via l'IP fixe ou le tunnel VPN.
- Vérification du basculement multi-opérateur en désactivant temporairement l'opérateur primaire (mode avion d'un téléphone test sur la même cellule, ou observation des changements de PLMN dans les logs).
- Mise à jour du firmware du modem cellulaire et du firmware applicatif (caméra, traceur) à la dernière version stable validée par le fabricant.
- Configuration des alertes sur la CMP : seuils de consommation, inactivité prolongée, dépassement géographique éventuel.
- Documentation locale du déploiement : ICCID, IMSI, IMEI, EID (si eUICC), APN, numéro de téléphone éventuel, archivés et reliés à l'inventaire client.

Le respect intégral de cette checklist élimine la quasi-totalité des incidents de déploiement et permet aux interventions ultérieures de se concentrer sur les véritables anomalies (panne matérielle, dégradation de l'environnement radio, modification du parc opérateur).