



Manuel

Modem Routeur 3G

(NEGO421)



REFDOC – V2.6 – 10/2019



+33 (0)4 93 19 37 37
+33 (0)4 93 19 37 30 - hot-line@wit.fr
7, avenue Raymond Féraud - CS 31003 - 06205 NICE Cedex 3



@ wit@wit.fr
www.wit.fr
www.wit-square.fr

 **Document mis à jour le 10/2019**

Sommaire

1.	Architecture.....	3
2.	Besoin	4
3.	Mise en œuvre.....	5
4.	Paramétrage du MTR (Firmware 5.0.0).....	6
5.	Statistiques	16
6.	Multitech device Manager.....	18
7.	Informations techniques	19
7.1	Paramétrage d’usine	19
7.2	Redémarrage et réinitialisation de l’appareil	19
7.3	Les voyants	20
7.4	Installation de la carte SIM.....	20
7.5	Mise à jour du logiciel	21

1. Architecture

Le modem routeur MultiTech® type MultiConnect® rCell 100 Series Router (modèles : MTR-H5, MTR-H6, MTR-G3, MTR-EV3, MTR-C2, MTR-LAT1, MTR-LEU1, MTR-LVW2) permet de se connecter, en utilisant le réseau 3G (HSPA), à distance sur un serveur Web qui ne dispose pas d'une liaison internet directe.

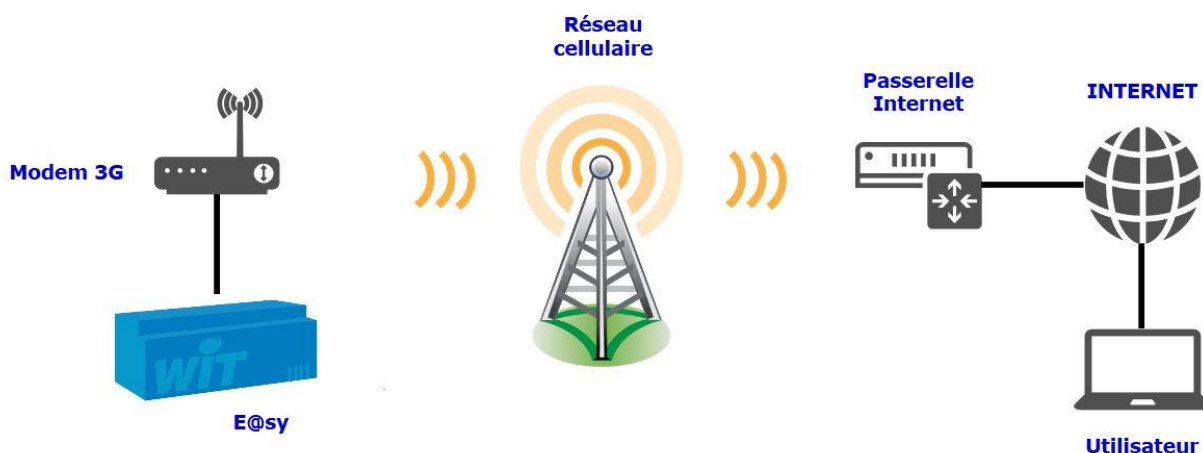
Le fonctionnement dans ce mode nécessite une carte SIM pourvue d'un compte actif auprès d'un fournisseur de service cellulaire avec un abonnement 3G ou HSUPA / HSDPA.

Rappel :

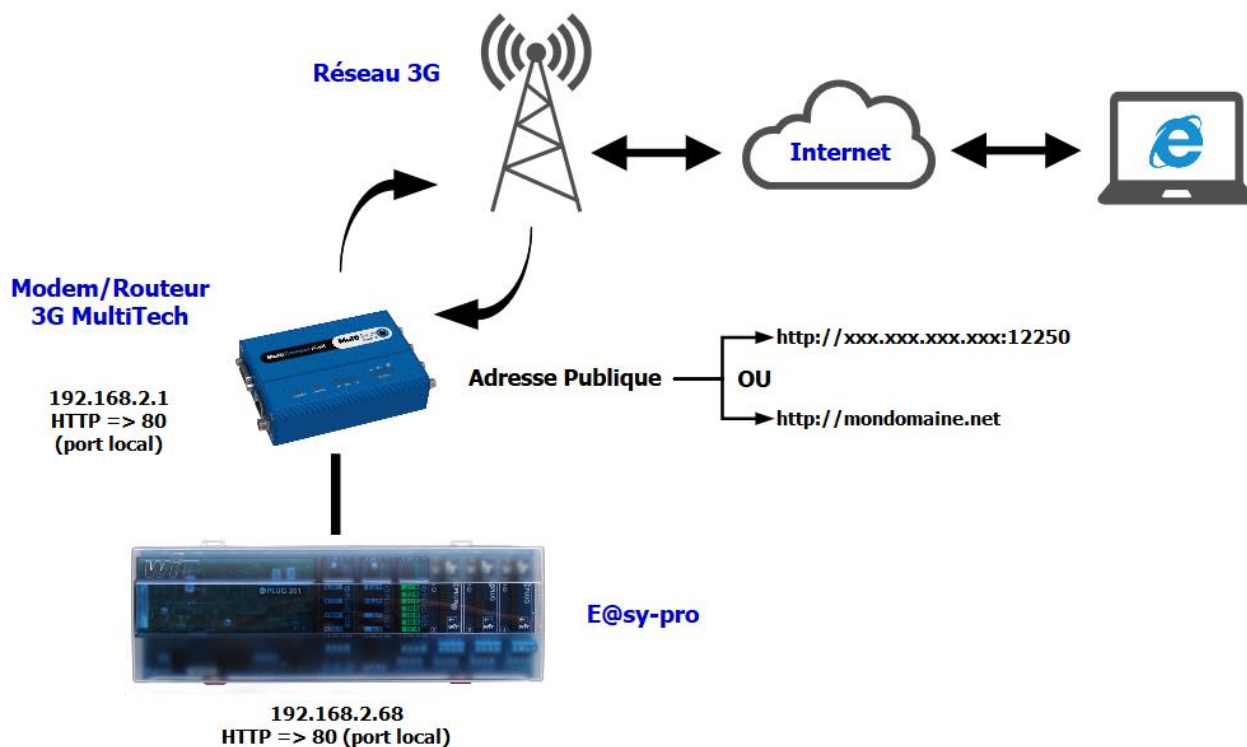
2,5G	GPRS	Global Packet Radio Service
3G	UMTS	Universal Mobile Telecommunications System
3,5G ou 3G+	HSPA	High Speed Packet Access

Le fournisseur d'accès donne une APN (Access Point Name) qui doit fournir au modem une adresse IP publique :

Fournisseur	APN	IP
Orange	orange.m2m ou internet-entreprise	publique
Orange	orange.m2m.spec	privée
Bouygues	fipbouygtel.com	publique
SFR	m2mpremium	publique



2. Besoin



L'objectif est d'accéder à un e@sy depuis un PC connecté au réseau internet en utilisant le réseau 3G (ou HSDPA).

Dans le réseau local on définit l'adresse IP de l'e@sy et du modem (qui doivent être le même domaine).

Le modem MultiConnect rCell est paramétré en conséquence pour faire sa fonction de routeur.

L'adresse IP Publique fournit par l'APN du fournisseur est dynamique, elle est susceptible de changer dans le temps. Il vaut mieux alors prendre un abonnement DNS qui permet la connexion par un nom plutôt qu'à partir d'une adresse IP.

L'utilisation du port entrant en 12250 est un exemple. Il est possible en spécifiant des ports différents d'accéder à d'autres équipements présents dans le réseau local (Caméra IP, autre e@sy, etc).

Dans la table de routage le port public 12250 devra être routé sur le port 80 de l'e@sy-pro.

L'e@sy est raccordé en permanence au réseau, il est donc capable de gérer des connexions sortantes comme s'il était sur un réseau local (SMTP, WOP, TRSII etc).

3. Mise en œuvre

La mise en service du système nécessite d'installer une carte SIM puis d'effectuer le paramétrage du Modem/Routeur MTR.

- Insérer la **carte** SIM dans le modem routeur.
- Raccorder l'antenne.
- **Alimenter le modem routeur.**
- Brancher le câble Ethernet.

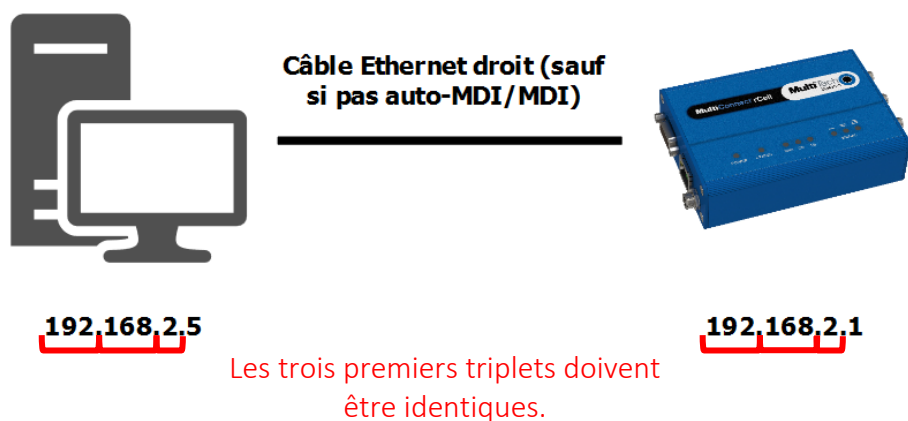
* Utiliser un cordon Ethernet croisé pour relier le MTR au PC.

Connexion :

L'adresse IP par défaut du modem routeur est : **192.168.2.1** (voir chapitre sur informations techniques).

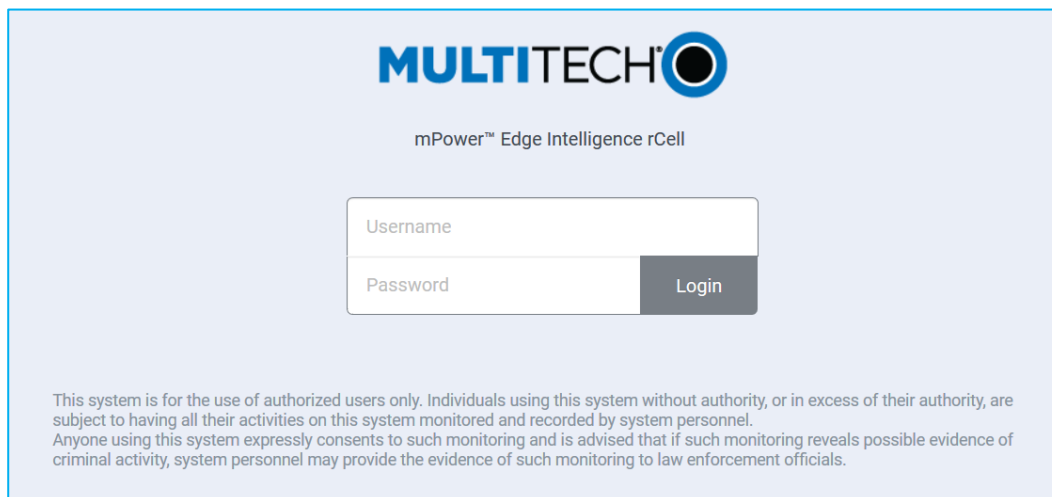
Pour pouvoir vous connecter au modem et y accéder, il vous faudra changer certains paramètres de la carte réseau de votre ordinateur (en lui attribuant une adresse IP fixe ayant le même masque que l'IP du modem), par exemple :


- Adresse IP : **192.168.2.5**
- Masque : 255.255.255.0
- Passerelle : **192.168.2.1**




4. Paramétrage du MTR (Firmware 5.0.0)

Etape 1 Après avoir connecter avec un câble Ethernet le modem sur votre réseau local. Rendez-vous sur l'interface utilisateur de votre modem via votre explorateur internet (Edge, Mozilla Firefox, ...) en renseignant dans la barre d'adresse l'adresse IP du constructeur : 192.168.2.1, vous verrez alors l'affichage suivant (la mise en page diffère à partir de la version 4.1.0) :



 Lors de la première connexion (« Commissioning mode »), le modem vous demandera de renseigner un nom d'utilisateur et un mot de passe.

 A partir du Firmware 4.0.5, il est obligatoire de renseigner un code d'accès personnalisé lors de la première authentification.

Si la connexion s'effectue en HTTPS, il est possible qu'un certificat de sécurité vous soit demandé. Pour contourner la connexion en HTTPS, et passer via le HTTP, vous devez cliquer sur « Paramètres avancés » puis « Ajouter une exception » ou « Continuer vers le site » selon le navigateur :



Vous avez tenté d'accéder à **192.168.2.1**, mais le serveur a présenté un certificat émis par une entité non approuvée par le système d'exploitation de votre ordinateur. Cela peut signifier que le serveur a généré son propre certificat de sécurité, auquel cas Google Chrome ne peut pas s'y fier pour valider les informations d'identification. Il se peut également qu'un pirate informatique tente d'intercepter vos communications.

[Continuer vers le site 192.168.2.1 \(dangereux\)](#)

Etape 2 Une fois entrée dans l’interface du produit, vous verrez sur la page qui s’affiche « HOME » un bon nombre d’informations concernant le routeur (référence du modèle, adresse IP, ...).



Au niveau du tableau « Device », si vous constatez que votre version est en deçà de la 5.0.0, profitez-en pour mettre à jour votre appareil.

Voici le lien de téléchargement : <https://www.multitech.com/models/92507260LF>

Lors du premier démarrage, le modem vous invitera dans un mode de paramétrage rapide « First-Time Setup ». La première fenêtre vous présentera trois modes d’utilisation du produit : **Network Router**, **PPP-IP Passthrough** et **Serial Modem**. Après avoir choisi l’un des modes proposés, vous serez amené à compléter les étapes restantes ou à les ignorer (vous pouvez revenir à tout moment sur les paramètres rencontrés en « First-Time Setup » via les onglets du menu déroulant situé à gauche).

Network Router	Mode par défaut, il paramètre le produit en tant que routeur de réseau cellulaire.
PPP-IP Passthrough	Le mode utilise le DHCP pour transmettre l'adresse IP qui a été attribuée à une interface PPP par un FAI (fournisseur réseau), à un autre périphérique exécutant un client DHCP. Dans ce mode, l'appareil n'autorise qu'un bail DHCP.
Serial Modem	Le mode crée une connexion série avec l'appareil qui peut être configurée en vitesse et contrôle de flux. Le port série parle à la radio cellulaire pour envoyer et recevoir des messages.

Dans la suite de ce document, nous avons choisi le mode « Network Router » pour configurer l’appareil. Pour en savoir plus sur les autres modes, nous vous invitons à consulter la documentation Multitech intitulée « mPower™ Edge Intelligence - MTR Software Guide ».



Si vous souhaitez changer de mode, il vous sera nécessaire de réinitialiser l’appareil aux configurations d’usine. Pour cela, vous pouvez utiliser le bouton « Reset » de l’appareil ou aller dans le menu « Saving and Restoring Settings ».

Je vous invite à débiter le paramétrage en cliquant sur l’onglet « Setup » du menu déroulant situé à gauche de votre écran. Toujours dans cet onglet, cliquez sur l’item « Network Interfaces », vous verrez alors la fenêtre suivante :

Home

Save And Restart

Setup

Network Interfaces

WAN Configuration

Global DNS

NETWORK INTERFACES CONFIGURATION ⓘ

Reset To Default

Name	Direction	Type	IP Mode	IP Address	Bridge	Options
eth0	LAN	ETHER	–	–	br0	✎
ppp0	WAN	PPP	PPP			✎
br0	LAN	BRIDGE	Static	192.168.2.1/24	br0	✎

Cette fenêtre affiche une liste d'interfaces réseaux :

Slave Interface	Cette section vous permet de créer une passerelle (bridge) entre les interfaces réseau. Toutes les interfaces réseau LAN sont ajoutées par défaut dans la passerelle « br0 ». Lorsqu'une interface « bridge » est ajoutée, il est possible de lui affecter un nombre quelconque d'interfaces LAN de type Ethernet (eth0) et Wi-Fi AP (wlan1). Attention, une seule interface passerelle est autorisée et supportée.
Ethernet Interface	L'interface Ethernet peut être configurée en LAN ou WAN, cette dernière peut utiliser des adresses IPv4 statiques ou obtenir dynamiquement une adresse IPv4 via le DHCP en mode client DHCP.
PPP interface	L'interface PPP ne peut être utilisée qu'en WAN. L'interface PPP répertoriée au sein de la page « Network Interfaces » ne peut être modifiée qu'au niveau de son mode. Les options disponibles sont les modes PPP et PPP – Addresses only .

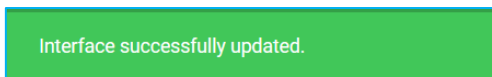
Ici nous souhaitons donner une adresse IP statique au modem pour l'automate puisse dialoguer avec lui. De plus, nous souhaitons dialoguer localement avec l'automate en Ethernet (LAN). Pour cela, nous devons seulement modifier les informations présentes au niveau de la passerelle « br0 » (il vous faudra cliquer sur l'icône « crayon »). Vous obtenez alors l'affichage suivant :

Admettons que l'adresse IP de votre automate sur le réseau soit 192.68.2.135, afin que les deux appareils puissent dialoguer, il faut qu'ils soient sur le même sous-réseau. Dans la pratique, cela veut dire que les trois premiers quadruplés de l'IP doivent être identiques sur les deux appareils, si on reprend l'exemple précédent, cela donne : 192.68.2.X. Le dernier quadruplé X doit être différent de celui de l'automate (donc différent de 135 en suivant notre exemple) et compris entre 0 et 255 (attention, aux adresses réservées et déjà utilisées). Si le modem n'est pas la passerelle du réseau, il faut indiquer dans le champ « Gateway » l'adresse IP de la passerelle correspondante (ce champ est disponible qu'après désélection de la passerelle **br0** dans l'interface **eth0**).



Veillez ne pas modifier le masque sous-réseau prédéfini sur le modem et l'automate (intitulé « Mask » sur le modem) ! Vérifier également qu'ils soient identiques sinon ils ne partageront pas le même sous-réseau.

Dès que vous avez terminé vos modifications, il vous faut valider les changements apportés en cliquant sur le bouton « Submit ».



Un message en haut à droite de l'écran vous indiquera si l'action a bien marché.



Vous apercevrez au passage que le bouton « Save and Restart » passe en rouge indiquant qu'une sauvegarde et un redémarrage sont nécessaires pour que les nouveaux paramètres soient pris en compte. Vous cliquerez sur ce bouton seulement lorsque toutes les modifications auront été faites.

Etape 3 Cliquer sur l'onglet « Cellular » puis sur l'item « Cellular Configuration » et renseigner les paramètres de votre abonnement 3G lié à la carte SIM insérée.

Selon les paramètres de votre abonnement SIM, il sera nécessaire de renseigner les champs suivants :

Paramètres	Signification
SIM Pin	Il s'agit du code PIN de votre carte SIM
APN « Access Point Name »	Nom du point d'accès réseau fourni par votre opérateur
Authentication Type*	Moyen d'authentification : PAP, CHAP et PAP-CHAP
Username	Nom d'utilisateur lié à l'abonnement SIM
Password	Mot de passe lié à l'abonnement SIM

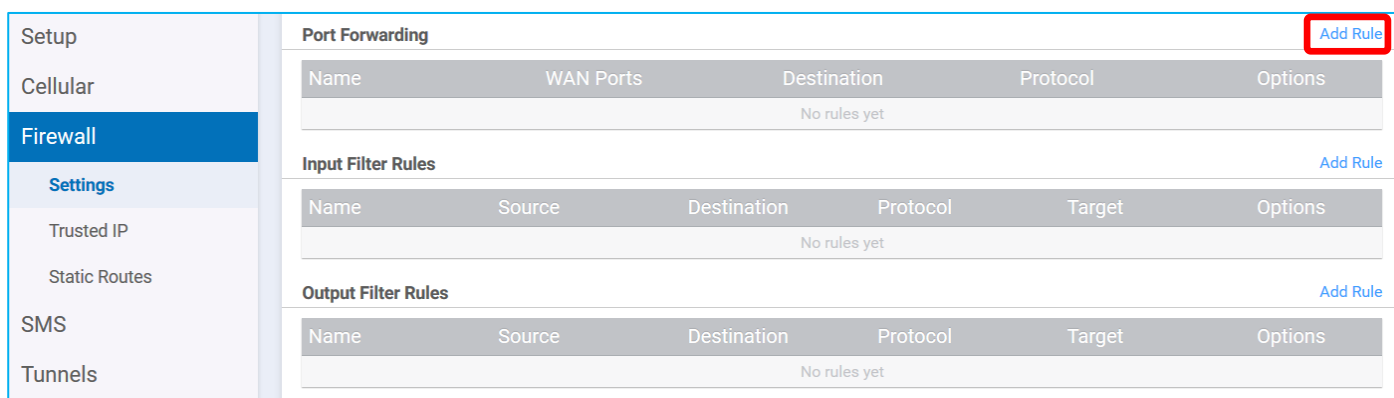
* Protocole réseau servant l'authentification d'un utilisateur sur un serveur internet. Les deux types de protocole sont :

1. PAP (Password Authentication) : le nom d'utilisateur et mot de passe sont transmis en clair au serveur.
2. CHAP (Challenge Handshake Authentication Protocol) : ce protocole négocie une forme sécurisée d'authentification cryptée à l'aide de MD05 (Message Digest 5).

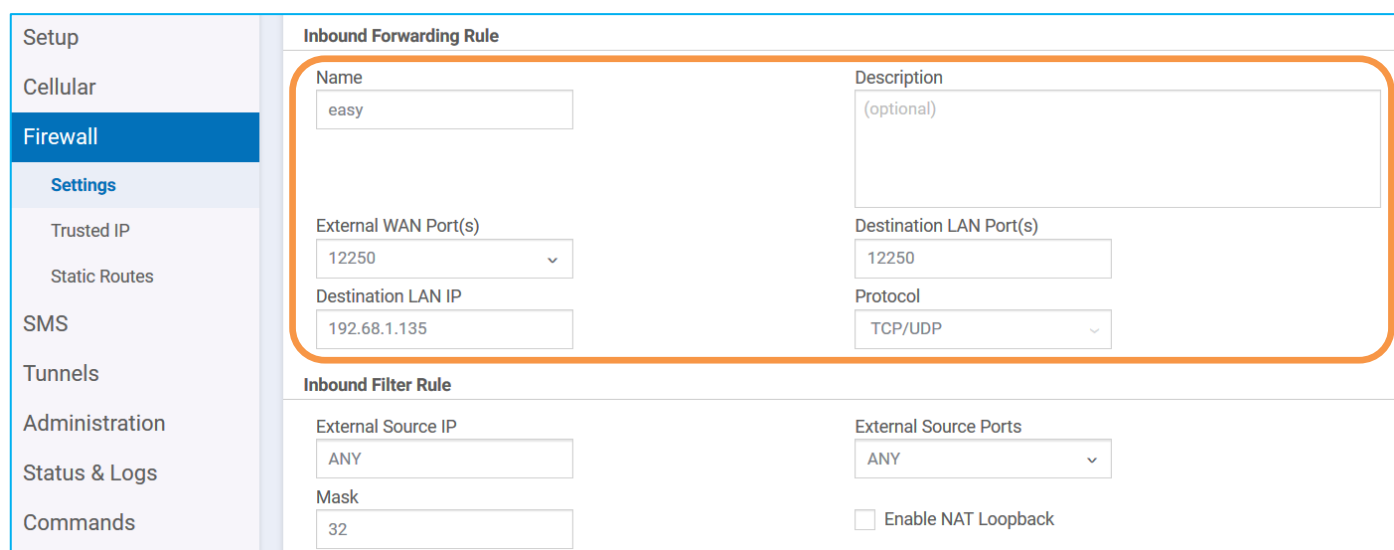
Exemple pour le réseau Orange :

- ➡ APN ➡ Internet- entreprise ou orange.m2m ou orange.m2m.spec
- ➡ Username ➡ orange
- ➡ Network Password ➡ orange



Etape 4 Cliquer sur « Firewall » puis sur l'onglet « Settings ». Dans cette nouvelle page, vous apercevrez trois zones de paramétrage : **Port Forwarding**, **Input Filter Rules** et **Output Filter Rules**. Ici c'est la première qui nous intéresse, elle permet de définir les règles de redirection des ports. Ces règles servent à indiquer les appareils du réseau local que l'on souhaite joindre de l'extérieur. Pour ajouter un nouvel appareil, cliquez sur le bouton « Add Rule ».



Après avoir effectué cette action, une nouvelle page de paramétrage devrait normalement apparaître (voir ci-dessous).

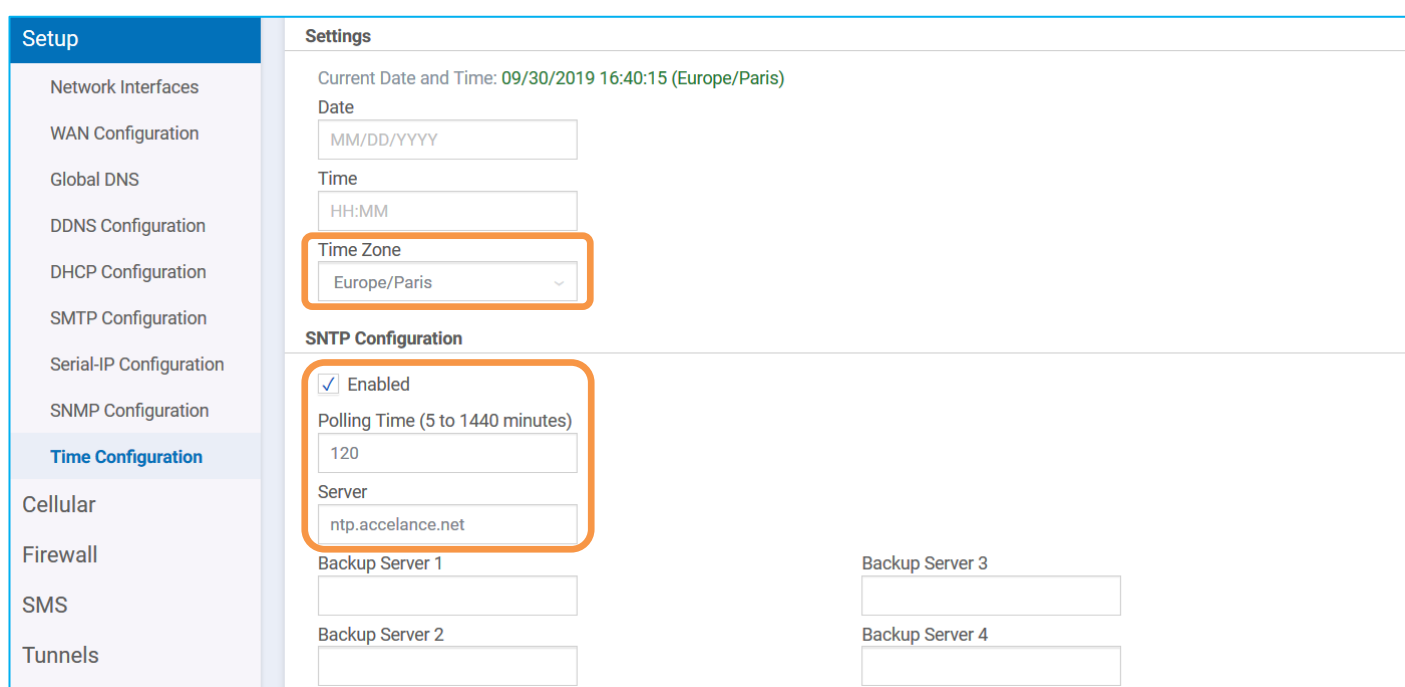


Les informations principales à renseigner sont le nom de la règle, le port extérieur WAN (le port de destination LAN est automatiquement rempli avec la même valeur), l'adresse IP LAN de destination (celle de l'appareil avec lequel on souhaite dialoguer) et enfin le protocole de transport souvent TCP/UDP (le premier est orienté « connexion » (informations sur l'émetteur du paquet et accusé de réception) et le second est « non connexion » (il est plus léger et unidirectionnel, pas d'informations sur l'émetteur)).

 Il est possible de modifier les paramètres d'une règle en cliquant sur l'icône , vous retrouverez le même aperçu que précédemment

Etape 5 Revenez dans le menu déroulant et cliquez maintenant sur « Setup ». Allez ensuite dans « Time Configuration » afin de mettre le modem à l'heure.

NB : Cette étape est facultative



Setup	Settings
Network Interfaces	Current Date and Time: 09/30/2019 16:40:15 (Europe/Paris)
WAN Configuration	Date MM/DD/YYYY
Global DNS	Time HH:MM
DDNS Configuration	Time Zone Europe/Paris
DHCP Configuration	SNTP Configuration
SMTP Configuration	<input checked="" type="checkbox"/> Enabled
Serial-IP Configuration	Polling Time (5 to 1440 minutes) 120
SNMP Configuration	Server ntp.accelance.net
Time Configuration	Backup Server 1
Cellular	Backup Server 2
Firewall	Backup Server 3
SMS	Backup Server 4
Tunnels	

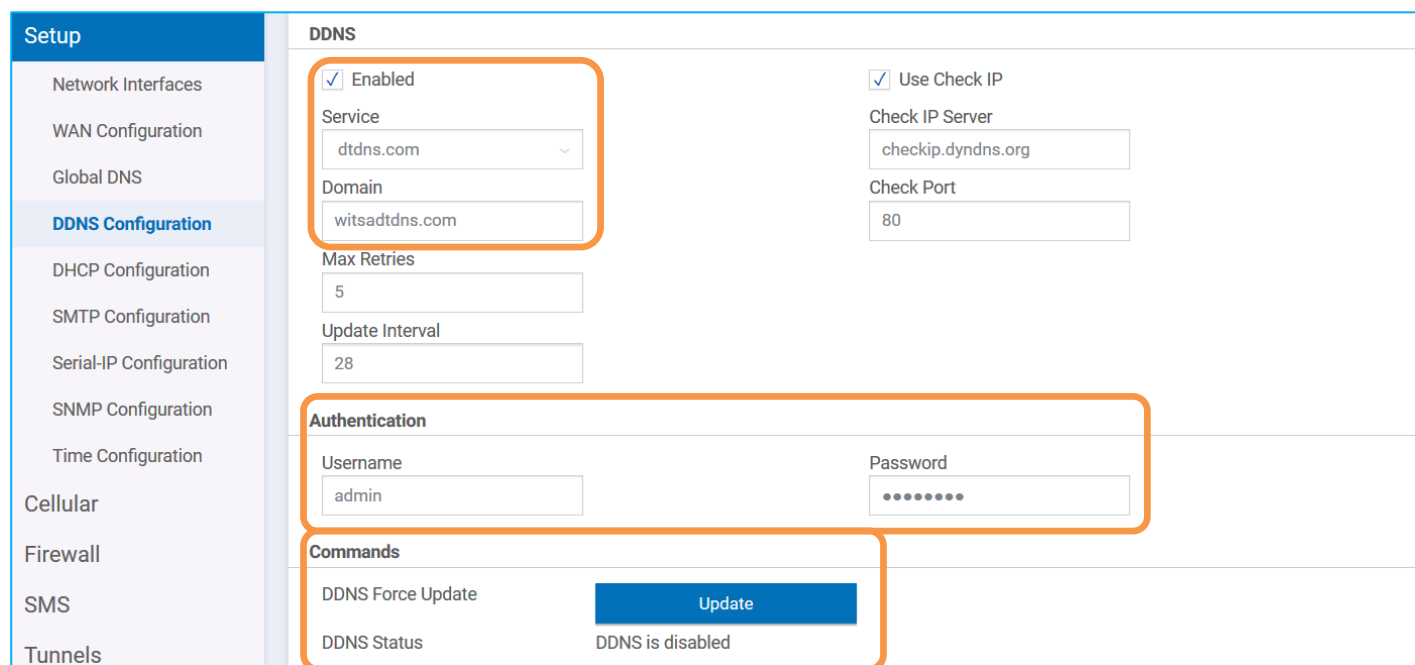
Si vous souhaitez synchroniser l'horloge du modem via le réseau, il vous faudra renseigner l'onglet « SNTP Configuration » en indiquant le nom (ou adresse IP) du serveur type SNTP/NTP puis la valeur du « Polling Time » qui correspond à l'intervalle de temps entre chaque requête effectuée par le client, autrement dit le temps entre chaque mise à jour de l'horloge (par défaut à 120 minutes).



N'oubliez de cocher « **Enable** » pour activer la synchronisation automatique !

Etape 6 Cliquez sur « Setup » puis « DDNS Configuration » afin de paramétrer le DynDNS (DNS dynamique). Pour rappel, le DNS (Domain Name System) est un processus permettant de lier une adresse IP à un nom de domaine (ex : « 192.13.21.3 » ⇔ « www.wit.fr »). Dans le cas du DNS dynamique, un nom de domaine est relié à une adresse IP dynamique, c'est-à-dire que cette dernière change régulièrement (toutes les 24h) pour des raisons de sécurité.

NB : Cette étape est facultative.



The screenshot shows the DDNS configuration page. The 'Enabled' checkbox is checked. The 'Service' dropdown is set to 'dtdns.com' and the 'Domain' text box contains 'witsadtdns.com'. The 'Max Retries' is set to 5 and the 'Update Interval' is 28. The 'Use Check IP' checkbox is checked, with the 'Check IP Server' set to 'checkip.dyndns.org' and the 'Check Port' set to 80. In the 'Authentication' section, the 'Username' is 'admin' and the 'Password' is masked with dots. In the 'Commands' section, there is a blue 'Update' button and the 'DDNS Status' is 'DDNS is disabled'.

Lorsque l'adresse IP sur le réseau 3G (WAN) n'est pas fixe, il est nécessaire de passer par un service d'adressage dynamique. Pour cela, il faut au préalable souscrire à un abonnement chez un fournisseur d'accès à Internet (FAI) proposant ce type de service, ainsi vous pourrez vous connecter sur le produit en toutes circonstances.

Dans l'exemple ci-dessus un abonnement a été souscrit chez www.dtdns.net

Les caractéristiques d'un abonnement sont généralement :

- **Nom de domaine** : witsadtdns.net
- **Username (nom d'utilisateur)** : admin
- **Password** : masqué ici

Après avoir mis à jour (**Update**) le DDNS et cliquez sur « Submit » puis « Save and Restart », vous verrez que le service passe de « disabled » à « enabled » pour vous dire que la connexion avec le serveur DynDNS est bien établie.

Etape 7 Pour administrer à distance le modem/routeur (c'est-à-dire pour s'y connecter à distance), veuillez-vous rendre dans le menu « Administration » puis « Access Configuration ».

NB : Cette étape est facultative. **Si vous utilisez l'agent de Téléalarme SMS vers Modem Multitech au sein du produit** → Ne pas tenir compte de la configuration ci-dessous mais se fier à celle du manuel de l'agent.

The screenshot shows the configuration interface for a WIT modem. The left sidebar contains a menu with 'Administration' selected, and 'Access Configuration' highlighted. The main content area is titled 'Web Server' and includes several sections:

- HTTP Redirect to HTTPS:** Includes checkboxes for 'Enabled', 'Via LAN', and 'Via WAN', and a 'Port' field set to 80.
- HTTPS:** Includes a checked 'Via WAN' checkbox and a 'Port' field set to 443.
- Authorization:** Includes a 'Session Timeout (minutes)' field set to 60.
- SSH Settings:** Includes a checked 'Enabled' checkbox, a 'Port' field set to 22, and checked 'Via LAN' and 'Via WAN' checkboxes.
- SSH Security:** Includes a 'Show ↓' link.
- ICMP Settings:** Includes a checked 'Enabled' checkbox, checked 'Respond to LAN', and unchecked 'Respond to WAN' checkboxes.
- SNMP Settings:** Includes checked 'Via LAN' and unchecked 'Via WAN' checkboxes.
- Modbus Slave:** Includes an unchecked 'Enabled' checkbox, checked 'Via LAN', and a 'Port' field set to 1502.
- IP Defense:** Includes three sub-sections:
 - DoS Prevention:** Includes a checked 'Enabled' checkbox, a 'Per Minute' field set to 60, and a 'Burst' field set to 100.
 - Ping Limit:** Includes a checked 'Enabled' checkbox, a 'Per Second' field set to 10, and a 'Burst' field set to 30.
 - Brute Force Prevention:** Includes a checked 'Enabled' checkbox, an 'Attempts' field set to 3, and a 'Lockout Minutes' field set to 5.

Enabling HTTPS access via WAN may allow remote users to access the Web UI via the cellular link. Due to continuous background data refreshing, the web UI may incur additional cellular data charges.

In addition, allowing HTTPS access to public networks may increase the likelihood of cyber attacks.

Please consider enabling Brute Force Prevention and DoS Prevention in the IP Defense section.

Il faut également activer les options de la rubrique « IP Defense » comme indiqué ci-dessus afin de garantir une meilleure sécurité de la connexion entrante. En effet, lorsque vous sélectionnez le HTTPS via WAN, un message de prévention apparaît pour vous indiquer les recommandations en termes de sécurité.

Etape 8 Dernière étape avant la sauvegarde et redémarrage du modem, c'est la validation du **Keep Alive** pour la partie téléphonique. Pour cela, allez successivement dans les onglets « Cellular » puis « Cellular Configuration ».



Cette étape est impérative pour éviter toutes déconnexions du modem.

<ul style="list-style-type: none"> Setup <li style="background-color: #0070C0; color: white;">Cellular <li style="background-color: #0070C0; color: white;">Cellular Configuration Wake Up On Call Radio Status Firewall SMS Tunnels Administration Status & Logs Commands Help 	<div style="border: 1px solid #ccc; padding: 5px;"> <p>General Configuration</p> <p><input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Diversity</p> <p>Connect Timeout: <input type="text" value="90"/> <input type="checkbox"/> Dial-On-Demand</p> <p>Dialing Max Retries: <input type="text" value="0"/></p> <hr/> <p>Modem Configuration</p> <p>Dial Number: <input type="text" value="*99***1#"/> Init String 1: <input type="text" value="AT+CSQ"/></p> <p>Connect String: <input type="text" value="CONNECT"/> Init String 2: <input type="text"/></p> <p>Dial Prefix: <input type="text" value="ATDT"/> Init String 3: <input type="text"/></p> <p>SIM Pin: <input type="text" value="0000"/> Init String 4: <input type="text"/></p> <p>APN: <input type="text" value="orange"/></p> <hr/> <p>Authentication</p> <p>Authentication Type: <input type="text" value="CHAP"/> Username: <input type="text" value="orange"/></p> <p style="text-align: right;">Password: <input type="text" value="....."/></p> <hr/> <p>Keep Alive</p> <div style="border: 2px solid orange; padding: 5px;"> <p>ICMP/TCP Check</p> <p><input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Radio Reboot Enabled</p> <p>Interval (seconds): <input type="text" value="180"/> Keep Alive Type: <input type="text" value="ICMP"/></p> <p>Hostname: <input type="text" value="8.8.8.8"/> ICMP Count: <input type="text" value="4"/></p> </div> <hr/> <p>Data Receive Monitor</p> <p><input checked="" type="checkbox"/> Enabled</p> <p>Window (minutes): <input type="text" value="60"/></p> </div>
---	---

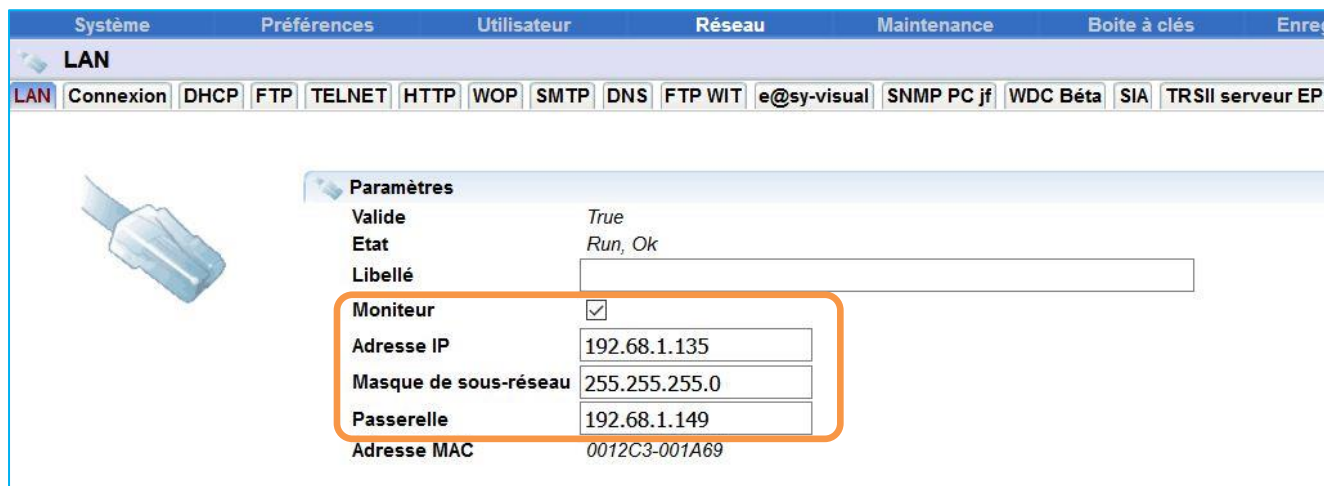
Cette option permet de vérifier périodiquement si le lien cellulaire est toujours actif, si au contraire il est coupé, le modem tentera de le rétablir. Le protocole ICMP (Internet Control Message Protocol) est utilisé pour véhiculer des messages de contrôle et d'erreur entre les machines qui communiquent (ping, traceroute, ...). Ainsi l'activation du « Keep Alive » permettra de maintenir la connexion ouverte et évitera le raccrochage du modem/routeur.

Etape 9 Pensez à bien sauvegarder l'ensemble des modifications que vous apportez en cliquant sur le bouton « Save and Restart ».

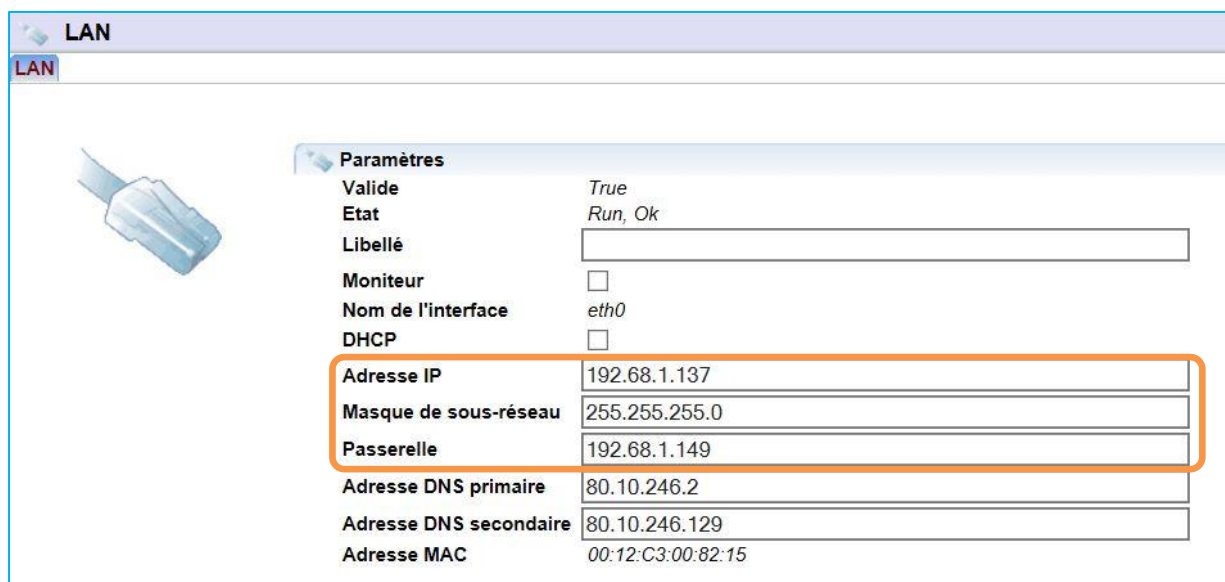


Etape 10 Pour finir, il est nécessaire de renseigner côté E@sy®/Redy® certaines informations sur la fiche de paramétrage du réseau.

Pour un E@sy®, il faudra aller dans **Configuration → Réseau → LAN** puis changer la passerelle en indiquant l'adresse IP du modem/routeur :



Pour un Redy®, il faudra aller dans **Configuration → Réseau → LAN** puis changer la passerelle en indiquant l'adresse IP du modem/routeur :



Désormais le Multiconnect® rCell 100 series est joignable à l'adresse suivante (exemple) :

```
http://DOMAIN_NAME.dtdns.net:ENTRY_PORT
```

Soit pour l'exemple ci-dessus :

```
http://witsa.dtdns.net:12250
```

5. Statistiques

Elles vous permettent d’avoir des informations sur le système (modèle, version du firmware, l’adresse MAC, mémoire occupée, mémoire libre, téléchargement des logs, ...), de suivre les paquets qui sont envoyés et reçus par le modem en fonction du service (Ethernet, Cellular, ...).

Etape 1 Pour avoir accès à ces informations, rendez-vous sur la page « Status & Log » puis cliquez sur le premier onglet de la liste « Statistics ».

STATISTICS ?

System Ethernet Cellular Serial GRE IPsec OpenVPN

Model Number: MTR-H6
 Firmware Information: 5.0.0-MTR 2019-05-10T10:00:08
 System Uptime: 05:28:54
 Mac-Address: 00:08:00:88:8F:19

Memory Usage

	Total	Used	Free	Available	Shared	Buff/Cache
Memory	119.88 MB	24.18 MB	51.45 MB	80.31 MB	10.32 MB	44.25 MB
Swap	0 Bytes	0 Bytes	0 Bytes			
Total	119.88 MB	24.18 MB	51.45 MB			

System Log [show ↓](#)

[Download Logs](#)

STATISTICS ?

System Ethernet Cellular Serial GRE IPsec OpenVPN

Start Date: 07/30/2019 End Date: 09/30/2019 [Clear History](#) [Show Cumulative Usage](#)

Legend: Sent (Green), Received (Blue)

0 bytes

30/07/2019 01/08/2019 03/08/2019 05/08/2019 07/08/2019 09/08/2019 11/08/2019 13/08/2019 15/08/2019 17/08/2019 19/08/2019 21/08/2019 23/08/2019 25/08/2019 27/08/2019 29/08/2019 31/08/2019 02/09/2019 04/09/2019 06/09/2019 08/09/2019 10/09/2019 12/09/2019 14/09/2019 16/09/2019 18/09/2019 20/09/2019 22/09/2019 24/09/2019 26/09/2019 28/09/2019 30/09/2019

Link

Local IPv4 Address: Not Acquired
 Remote IPv4 Address: Not Acquired
 MTU: -

Received		Sent	
Total	0 Bytes	Total	0 Bytes
Today	0 Bytes	Today	0 Bytes

Etape 2 Cliquez ensuite sur l'onglet « Services », vous pourrez visualiser sur cette page l'ensemble des services utilisés et leurs états.

Home	<p>SERVICE STATISTICS ?</p> <table border="1"> <thead> <tr> <th>Service Name</th> <th>Configuration</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>DDNS</td> <td>Disabled</td> <td>DDNS is disabled</td> </tr> <tr> <td>SNTP</td> <td>Disabled</td> <td>SNTP is disabled</td> </tr> <tr> <td>TCP/ICMP Keep Alive</td> <td>Disabled</td> <td>PING Keep alive is disabled</td> </tr> <tr> <td>Dial-On-Demand</td> <td>Disabled</td> <td>PPP is not running</td> </tr> <tr> <td>SMTP</td> <td>Disabled</td> <td>SMTP is disabled</td> </tr> <tr> <td>SMS</td> <td>Enabled</td> <td>SMS service has stopped</td> </tr> <tr> <td>Failover</td> <td>Enabled</td> <td>Failover service is running</td> </tr> </tbody> </table> <p>Last Updated: 17:29:11</p>	Service Name	Configuration	Status	DDNS	Disabled	DDNS is disabled	SNTP	Disabled	SNTP is disabled	TCP/ICMP Keep Alive	Disabled	PING Keep alive is disabled	Dial-On-Demand	Disabled	PPP is not running	SMTP	Disabled	SMTP is disabled	SMS	Enabled	SMS service has stopped	Failover	Enabled	Failover service is running
Service Name		Configuration	Status																						
DDNS		Disabled	DDNS is disabled																						
SNTP		Disabled	SNTP is disabled																						
TCP/ICMP Keep Alive		Disabled	PING Keep alive is disabled																						
Dial-On-Demand		Disabled	PPP is not running																						
SMTP		Disabled	SMTP is disabled																						
SMS		Enabled	SMS service has stopped																						
Failover		Enabled	Failover service is running																						
Save And Restart																									
Setup																									
Cellular																									
Firewall																									
SMS																									
Tunnels																									
Administration																									
Status & Logs																									
Statistics																									
Services																									

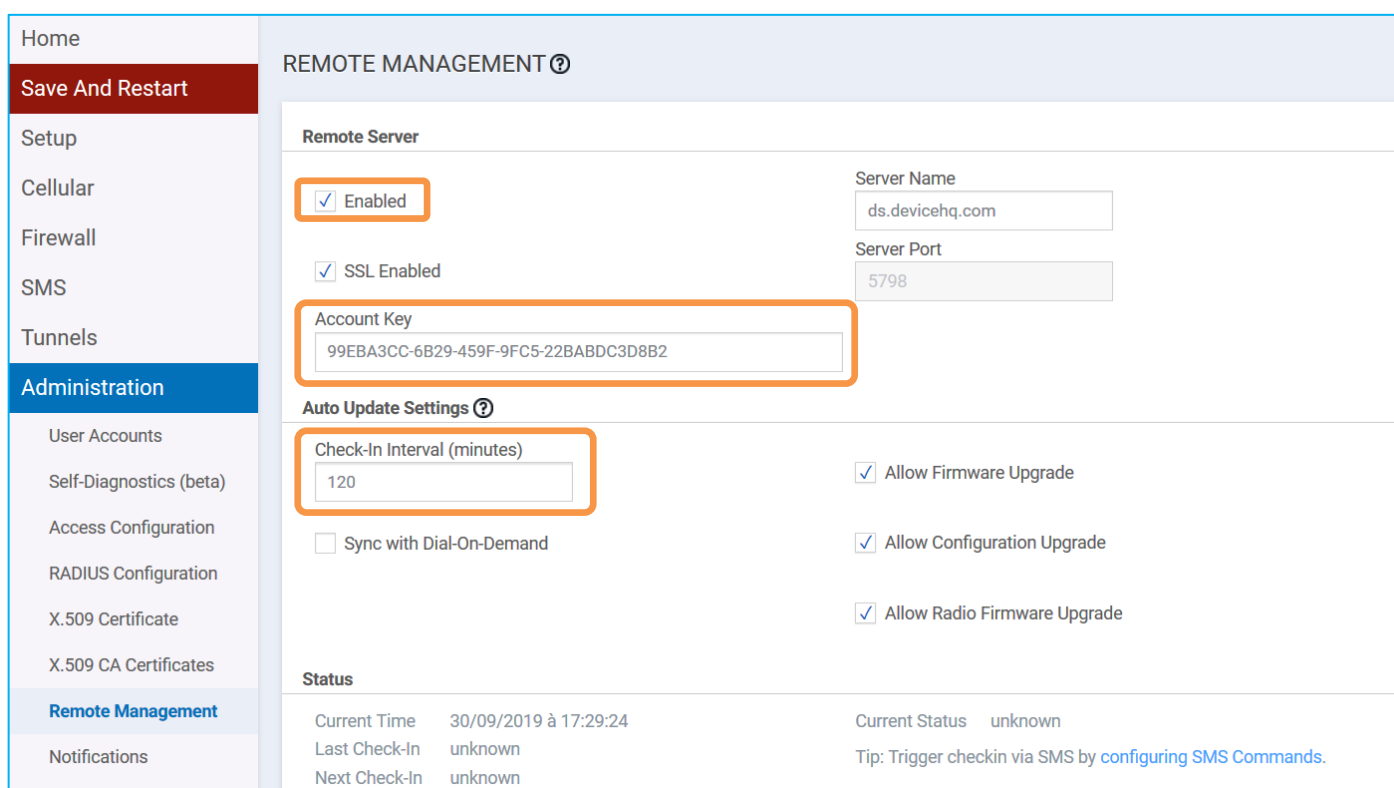
6. Multitech device Manager

Le fabricant propose gratuitement une solution cloud pour suivre les dernières générations de modems Multitech. Pour bénéficier de ce service, il vous suffit de vous inscrire sur la plateforme [DeviceHQ™](https://www.multitech.com/brands/devicehq) (<https://www.multitech.com/brands/devicehq>).

En parcourant la page dédiée, vous trouverez un bouton « **DeviceHQ Log In** » qui vous renverra sur la page d'authentification de la plateforme. Si vous n'avez pas de compte, vous pouvez en créer un en cliquant sur le lien « **Register Account** ».

Après vous être connecté ou inscrit, vous pourrez obtenir une clef (d'API) qu'il vous faudra renseigner dans le paramétrage du modem (dans le champ **Account Key**).

Pour activer côté modem le service, rendez-vous sur la page « Remote Management » accessible depuis l'onglet « Administration ».



The screenshot shows the 'REMOTE MANAGEMENT' configuration page. The sidebar on the left includes 'Administration' and 'Remote Management'. The main content area has the following sections:

- Remote Server:**
 - Enabled
 - SSL Enabled
 - Server Name: ds.devicehq.com
 - Server Port: 5798
 - Account Key: 99EBA3CC-6B29-459F-9FC5-22BABDC3D8B2
- Auto Update Settings:**
 - Check-In Interval (minutes): 120
 - Sync with Dial-On-Demand
 - Allow Firmware Upgrade
 - Allow Configuration Upgrade
 - Allow Radio Firmware Upgrade
- Status:**
 - Current Time: 30/09/2019 à 17:29:24
 - Last Check-In: unknown
 - Next Check-In: unknown
 - Current Status: unknown
 - Tip: Trigger checkin via SMS by [configuring SMS Commands](#).

Valider la fonction « Enabled », insérer la clé fournie dans le champ « Account Key » et régler l'intervalle d'appel « Check-in Interval ».

Grâce à ce service, vous pourrez faire un suivi du fonctionnement des appareils mais également faire une mise à jour du Firmware des appareils, forcer le redémarrage d'un modem, etc...

7. Informations techniques

7.1 Paramétrage d'usine



Pour les principales valeurs d'usine que vous retrouverez au dos du produit (normalement) ou au sein de la Data Sheet, vous avez :

Adresse IP	192.168.2.1
Identifiant	admin
Mot de passe	admin

7.2 Redémarrage et réinitialisation de l'appareil

Pour **redémarrer le produit** sans affecter le paramétrage :


1. Trouvez le bouton situé dans un trou intitulé « Reset » (pour éviter une mauvaise manipulation)
2. Utiliser une épingle pour appuyer sur le bouton, maintenez-le enfoncé pendant moins de 3 secondes puis relâchez-le.
3. L'appareil redémarre.


Pour **réinitialiser le produit aux valeurs par défaut définies par l'utilisateur** :

1. Trouvez le bouton situé dans un trou intitulé « Reset » (pour éviter une mauvaise manipulation)
2. Utiliser une épingle pour appuyer sur le bouton, maintenez-le enfoncé pendant 3 à 29 secondes puis relâchez-le.
3. L'appareil redémarre.

Pour **réinitialiser le produit aux valeurs d'usine** (suppression des valeurs « utilisateur ») :

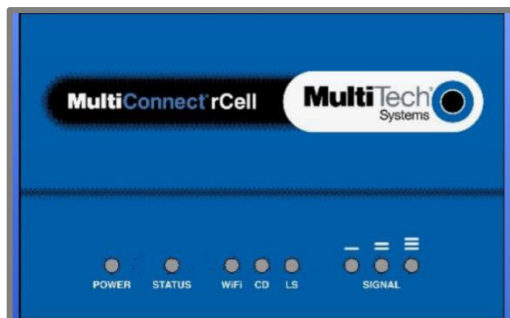
1. Trouvez le bouton situé dans un trou intitulé « Reset » (pour éviter une mauvaise manipulation)
2. Utiliser une épingle pour appuyer sur le bouton, maintenez-le enfoncé pendant au moins 30 secondes puis relâchez-le.
3. L'appareil redémarre en mode « Commissioning ».

 Après cette manipulation irréversible, tous vos paramètres seront réinitialisés aux valeurs par défaut fournies par le constructeur. Tous les comptes « utilisateur » seront supprimés de l'appareil.

 Si vous devez mettre à jour votre produit sur la dernière version Firmware, il doit se trouver préalablement en version 3.4.5.

7.3 Les voyants

Le panneau supérieur possède les voyants suivants :



- **POWER** : Allumé fixe (vert) indique la présence de l'alimentation.
- **STATUS** : La led verte est fixe lorsque l'appareil est en cours de démarrage, lors d'une sauvegarde de la configuration, d'un redémarrage, ou d'une mise à jour du Firmware. Lorsque le voyant clignote, le routeur est prêt à l'emploi.
- **CD (Carrier Detect)** : Allumé, il indique que la connexion au réseau a été établie.

➤ **LS (Link Status)** :

Eteint → Pas de transmission de données.

Allumé fixe → Connecté et échange de données de transmission et de réception.

Clignotement lent (-0.2 Hz) → Enregistré ou connecté, mais trafic ralenti.

Clignotement rapide (-3 Hz) → Pas enregistré ou en recherche de connexion.

➤ **SIGNAL** : puissance du signal de réception.

Voyant « Signal »	Puissance du signal (dBm)	Qualité du signal
Eteint	$0 \leq \text{RSSI} < 6$	Pas de réseau ou extrêmement faible
1 barre	$7 \leq \text{RSSI} < 14$	très faible
2 barres	$15 \leq \text{RSSI} < 23$	faible
3 barres	$24 \leq \text{RSSI} \leq 31$	très bon

7.4 Installation de la carte SIM

Veuillez procéder de la manière suivante pour intégrer votre carte SIM au sein du modem :

1. Ouverture du logement

- Débrancher l'alimentation du modem et tous les câbles.

2. Insérer la carte SIM

- Appuyer doucement sur la carte SIM pour qu'elle s'enclenche dans son logement.



7.5 Mise à jour du logiciel

Les dernières versions logicielles du modem sont téléchargeables en suivant ce lien :

 <https://www.multitech.com/models/92507260LF>

Nota : **Software 5.0.0 Upgrade** de mai 2019 améliorant l'interface du produit (notamment plus d'options disponibles pour le paramétrage réseau) et certains aspects de sécurité. Release Note : ftp://ftp.multitech.com/wireless/mtr/mtr-release-notes_5.0.0.txt



Pour migrer aux versions Firmware 3.7.3 à 5.0.0, il est nécessaire d'installer au préalable la première version du logiciel → 3.4.5



A partir du Firmware 4.0.5, il est indispensable de renseigner un mot de passe personnalisé. Ce dernier doit avoir certaine complexité :

- Au minimum 8 caractères dont 3 au minimum de différents types
- 1 caractère alphabétique majuscule (A-Z) au minimum
- 1 caractère alphabétique minuscule (a-z) au minimum
- 1 caractère numérique (0-9) au minimum
- 1 caractère spécial (!, ?, \$, #, %, /, \, [,], {, }, ...)