Table of Contents

Cellular IoT

EMnify is a IoT communications platform that enables you to connect your IoT solutions over the best networks in the country - anywhere with the EMnify Global IoT SIM. Not only do you get global cellular access but with our cloud-native platform, we provide you with control over your device connectivity and tools so that you can better operate and secure your solution.

- IoT SIM

Using a single SIM, you can have multiple IMSIs, switch between multiple carriers and ensure uninterrupted connectivity. You can learn more about IMSI in Service Stack Overview section

- Highly available platform

Being able to connect to multiple operators over multiple partners increases connectivity availability. EMnify's platform (consisting of a mobile core network and a communication platform dedicated for IoT) has been built up cloud-natively, which means that it is deployed in 3 cloud regions within 2-3 availability zones per region / data centers. Even when one cloud data center becomes unavailable you can still transport your data over the EMnify network.

- Cloud Integration

Given the cloud-native nature of our platform, you can easily integrate your cloud as well as on-premise IoT solutions. We allow you to connect through standard cloud services to establish a secure private network with your devices, get operational connectivity metadata delivered to your favorite << Multi Cloud Data Streamer, streaming analytics service>> or use your low-code environment to automate your device logistics and operation processes.

- EMnify API

With the EMnify API, you can control your SIM cards from your own applications using HTTP requests - for example to align your SIM contract with your device lifecycle, build own prepaid models or to send or receive configuration SMS. The complete functionality available is documented in the API Reference section.

In the following sections of the guide, you will find more information about our technology stack, integrations to several cloud platforms, the EMmnify API as well as several examples to help you in your IoT solutions building journey.

Quickstart

To begin developing your IoT solutions with EMnify, you will need an EMnify account. Sign up for free to a 60-day trial to use all functionalities.

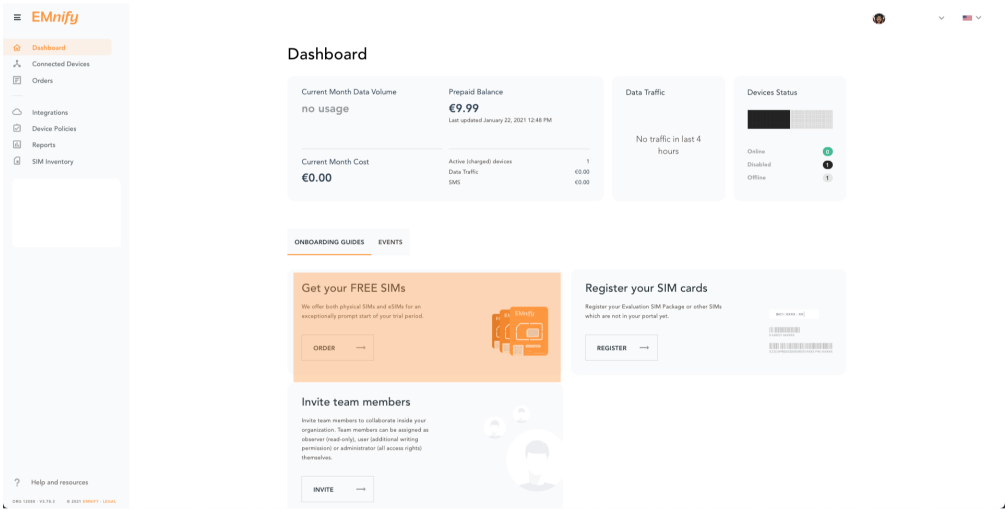
Order a free evaluation SIM package

Before you begin the production of your IoT solution with your EMnify SIM cards, you may want to test the service. You can order your free Evaluation SIM package on the EMnify portal with which

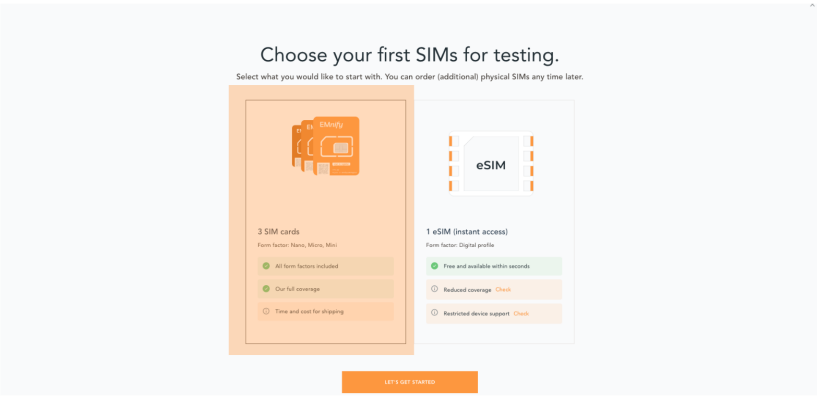
you can test all EMnify services. Whereas you can download the eSIM for your smartphone for free - shipping costs may apply for the 3 physical SIM cards, depending on your location.

Log into your EMnify account and follow these steps:

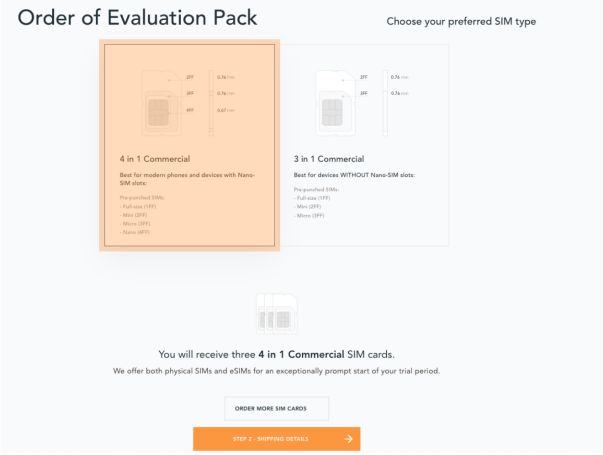
1. On the dashboard, click on order on **Get your FREE SIMs**



2. Select the SIM cards of your choice.

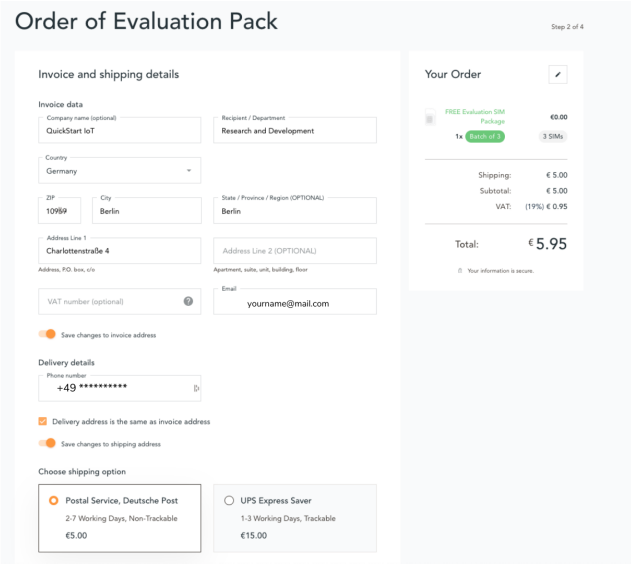


   a. If you select physical SIM cards, you can further choose between 3in1 (no nano SIM) or 4in1 (with nano SIM).

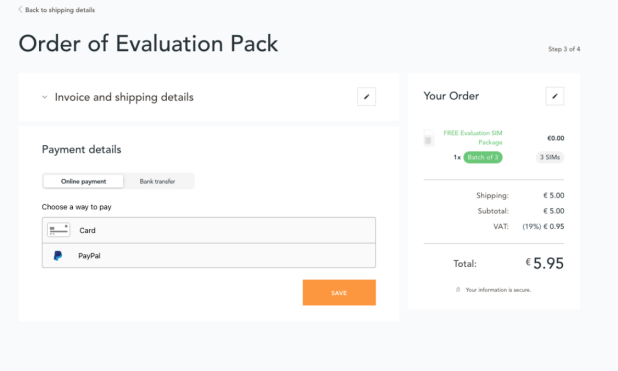


b. If you select the developer eSIM, you can directly download it into your eSIM compatible phone. You can find the instructions to do so in this blog post

3. For the physical SIM cards, proceed to fill in your shipping details.



4. Proceed to pay the shipping charges and you will be notified when the SIM cards will be shipped.



Registering SIMs

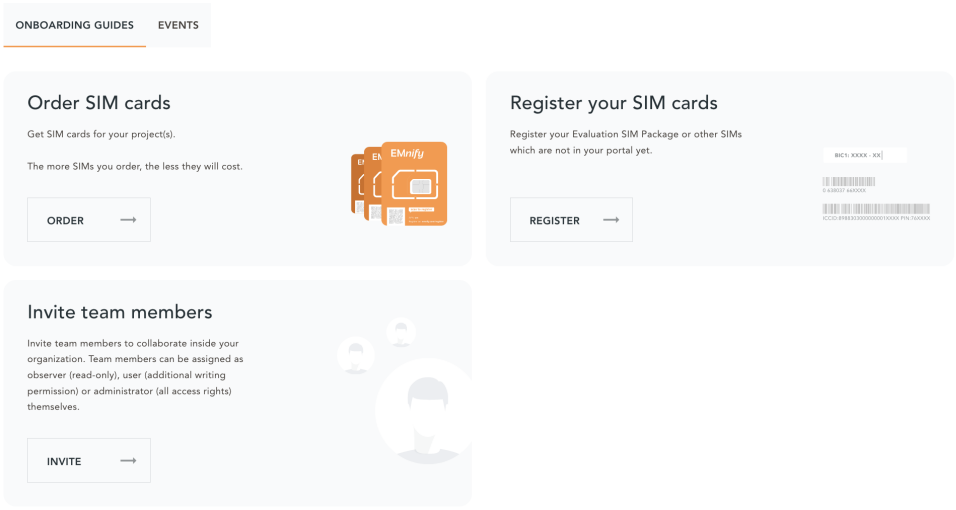
Once you get your EMnify SIMs, you need to register them before you can start using them.

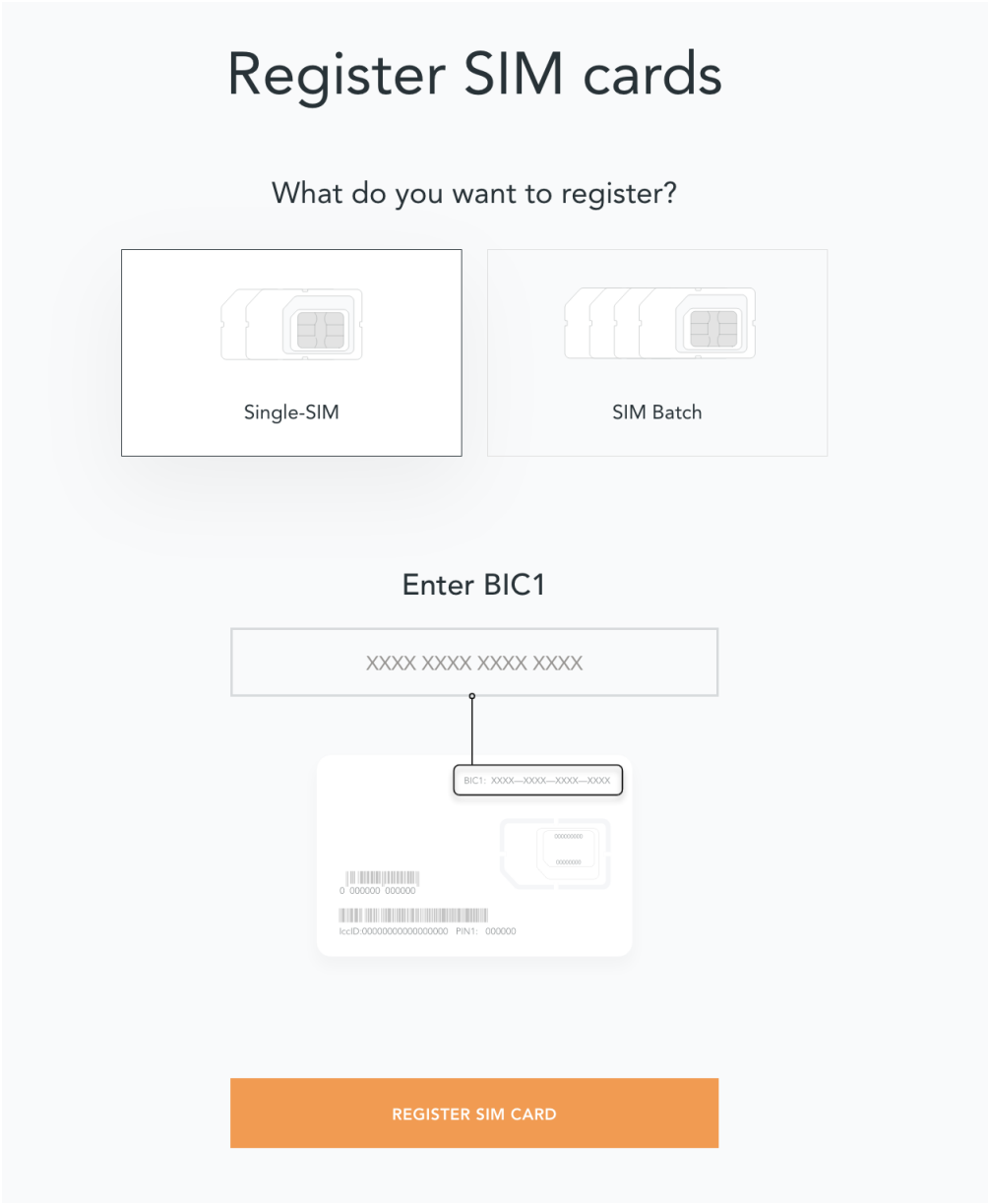
1. If you have the evaluation SIM cards, you will have to register them one by one.

   Scan the QR code on the SIM card and click on register. The scanner will copy the BIC and take you to the EMnify portal to register the SIM.

2. If you do not have a QR reader or want to do this on a desktop without a camera, register using the BIC

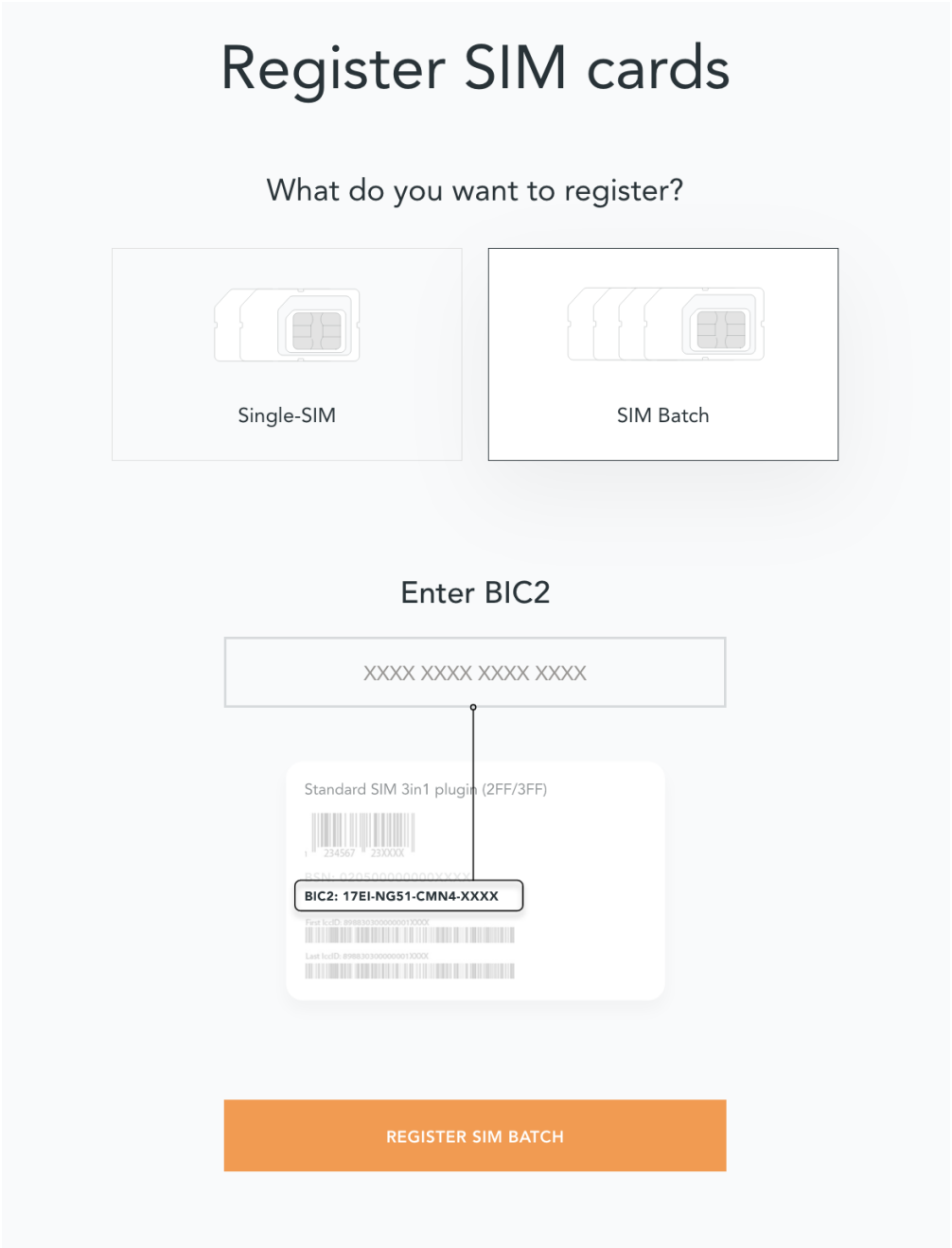
   Login to your link: EMnify account On your dashboard, click **REGISTER** on the card - Register your SIM cards.

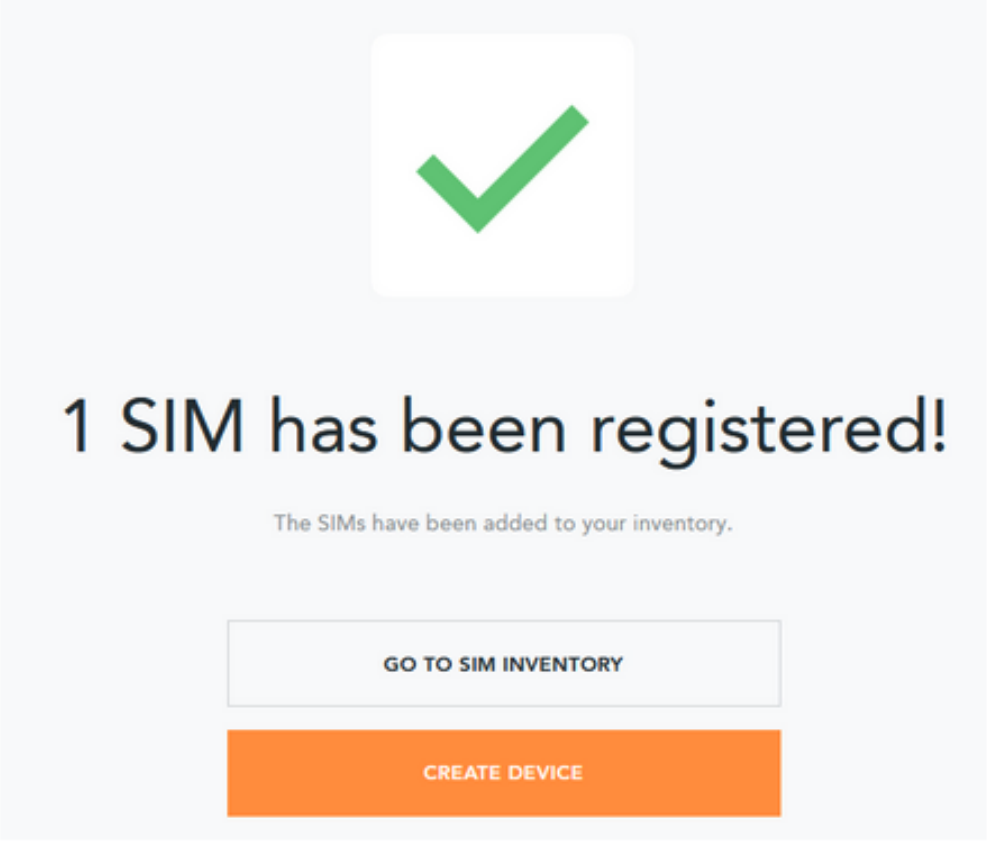




3. Now enter the Batch Identification Code (**BIC** 1) in the prompt. You can find the BIC1 on the back of your SIM card.

4. If you have ordered more than 5 SIM cards, you need to batch register them using the **BIC2**.



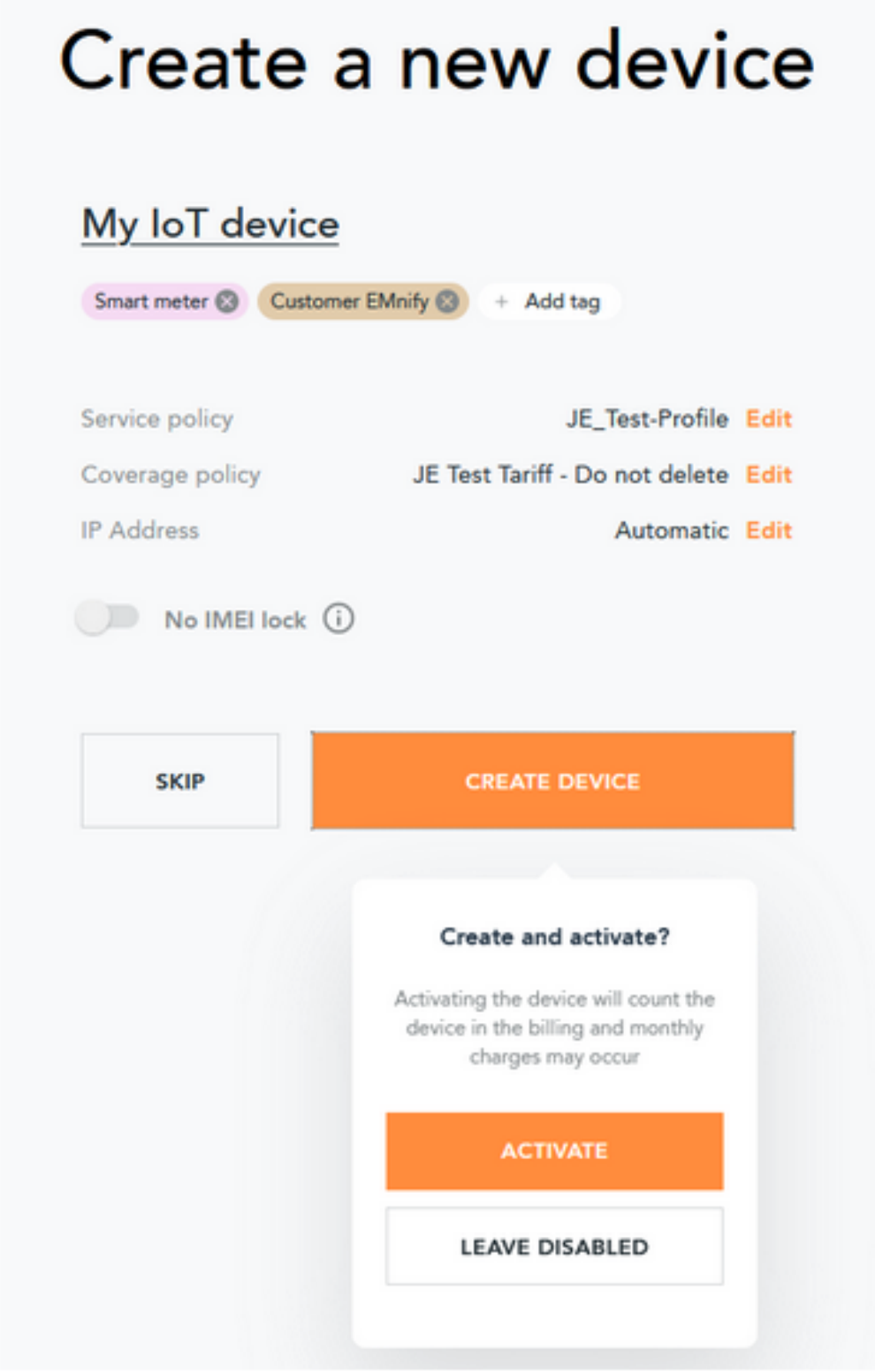


NOTE	If you have a developer eSIM, the downloading process of an eSIM automatically registers it in our portal.

Creating a Device

After you register a SIM, you need to create a virtual representation of the device associated with the SIM.

To create a device, give it a name and assign a service and coverage policy.



If you plan on using your device right away, activate it. If you do not plan on using the device right away, select "leave disabled".

Getting the first device online

Any device equipped with a SIM card requires an APN (Access Point Name) configuration to establish a data session. Some devices and networks auto-detect the APN but for most cases you need to configure it.

APN: `em` (or alternatively use `emnify`)

Further some Android / iOS based devices and cellular modules also need to be configured to allow for roaming.

Select below your device type and model to see how to configure the APN.

Cellular modules	GPS tracker	Industrial Routers
Android	iOS devices	

Cellular modules

Quectel	u-Blox	Fibocom
Telit	Sierra Wireless	Cinterion/Gemalto/Thales
SIMcom	Sequans	

Quectel cellular IoT modules

Applies to all Quectel modules: BG95, BG96, EG25, EG91, EG95, EC21, EC25, M65, M66, M95, MC60, BG77, BG600L

With Quectel modules the APN can be set with the 3GPP standard command AT+CGDCONT

```
AT+CGDCONT=1,"IP","em",,
```

Quectel also utilizes a vendor specific Command AT+QICSGP

```
AT+QICSGP=1,1,"em","","",1
```

According to Quectel the command AT+QICSGP shall be used when the internal TCP/UDP stack should be used – and it also allows to configure which bearer (CSD or GPRS) is used. GPRS must be used.

For managing roaming Quectel also introduced the AT+QCFG command. The suggested setting is:

```
AT+QCFG="roamservice",2,1
```

NOTE	Check your Quectel module AT command guide for more information. Further you can also read about AT commands in our [AT command guide].

u-Blox cellular IoT modules

u-Blox supports the standard 3GPP command to set APNs via AT+CGDCONT

```
AT+CGDCONT=1,"IP","em",,
```

u-Blox also supports a vendor specific command to configure the APN for the initial EPS bearer.

```
AT+UCGDFLT=1,"IP","em"
```

For roaming configuration u-blox modules utilize a vendor specific AT+UDCONF command. This enables automatic search in case the device cannot attach to a specific network.

```
AT+UDCONF=20,2
```

NOTE	Check your u-Blox module AT command guide for more information. Further you can also read about AT commands in our [AT command guide].

General cellular IoT modules

Applies to a cellular module vendors: Fibocom, Telit, Sierra Wireless, SIMcom, Cinterion, Gemalto, Thales, Sequans

The commands for configuring the APN settings are 3GPP standardized and all major cellular module manufacturer support the commands.

The AT+CGDCONT command needs to be utilized to set the APN.

```
AT+CGDCONT=1,"IP","em",,
```

NOTE	Check your AT command guide for further information or read 3GPP Technical Specification 27.007. Further you can also read about AT commands in our [AT command guide].

GPS tracker

Teltonika	Ruptela	Concox
Coban	Meitrack	Elinz
Reachfar	Queclink	Bitrek

TIP	For other GPS vendors please consult the manual and configure the APN to be `em` or `emnify`.

Teltonika GPS APN configuration

Source Teltonika GPS documentation

Applies to FMB110, FMB120, FM130, FMB140, FMC001, FMM001, FMC125, FMC130, FMC640, FMM125, FMM130, FMM640, FMP100, FMB001, FMB002, FMB003, FMB010

Configuring the APN for Teltonika GPS trackers can be done through

1. Teltonika Configurator over a USB, Bluetooth connection
2. Via the SMS console through the EMnify Portal (most simple)
3. via the EMnify SMS API or Zapier Integration (when automating the configuration)

NOTE	Newer Teltonika GPS versions automatically detect the EMnify APN setting

When the GPS tracker is turned on for the first time after the SIM is installed it is showing the status `Attached` in the EMnify portal. At this point the device can receive SMS but not establish a data session unless the APN is setup or detected.

The SMS command to set the APN is:

```
  setparam 2001:em
```

(please note the two leading spaces)

Ruptela GPS APN configuration

Applies to HCV5, LCV5, Pro5, Trace5/NA, FM-Tco4 HCV/HCV 3G, FM-Tco4 LCV/LCV 3G, FM-Pro4/Pro4 3G, FM-Eco4/4+, FM-Eco4 light/light+/3G, FM-Eco4 S Series, FM-Eco4 T Series, FM-Plug4

Source Ruptela Documentation

Configuring the APN for Ruptela GPS trackers can be done through

1. Ruptela Device Center over a USB, Bluetooth connection
2. Via the SMS console through the EMnify Portal (most simple)
3. via the EMnify SMS API or Zapier Integration (when automating the configuration)

When the GPS tracker is turned on for the first time after the SIM is installed it is showing the status `Attached` in the EMnify portal. At this point the device can receive SMS but not establish a data session unless the APN is setup or detected.

The SMS command to set the APN for Ruptela GPS trackers is:

```
[SMSpassword] setconnection em
```

The [SMSpassword] can be setup in the Ruptela device center. IF it is not set then the SMSpassword can be omitted and the command is only

```
setconnection em
```

Concox GPS APN configuration

Applies to JM-VL01, JM-VL02, JM-BL11, JM-VL03, JM-VL04, JM-LL01, JM-LL02, JM-LL301, X3,Wetrack140, Wetrack2, Wetrack lite, Bl10, GT06N, OB22, ET25, HVT001, EG02, JM-VG01U, JM-VG02U, JM-VG04Q, AT1-AT6, CT10, JM-LG01, JM-LG05, TBT100

Configuring the APN for Concox GPS trackers can be done

1. Via the SMS console through the EMnify Portal (most simple)
2. via the EMnify SMS API or Zapier Integration (when automating the configuration)

When the GPS tracker is turned on for the first time after the SIM is installed it is showing the status `Attached` in the EMnify portal. At this point the device can receive SMS but not establish a data session unless the APN is setup.

The SMS command to set the APN for Concox GPS trackers is:

```
APN em#
```

For some Concox models (e.g. TR02) the password (default 666666) needs to be send with the command

```
APN,666666,em#
```

Coban GPS APN configuration

Applies to Coban TK104, GPS303X, GPS103X, GPS306X, LK209, ...

Configuring the APN for Coban GPS trackers can be done

1. Via the SMS console through the EMnify Portal (most simple)
2. via the EMnify SMS API or Zapier Integration (when automating the configuration)

When the GPS tracker is turned on for the first time after the SIM is installed it is showing the status `Attached` in the EMnify portal. At this point the device can receive SMS but not establish a data session unless the APN is setup and the GPRS service is activated.

To turn on GPSR

```
gprs[your_password]
```

The SMS command to set the APN for Coban GPS trackers is:

```
APN[your_password] em
```

The default password is 123456. There are no spaces between gprs/APN and the password.

Meitrack GPS APN configuration

Applies to P88L, P99, MT90, T663L, T333, T366, T399, TS299L, TC68L, TC68SG, T622, K211G, T355G
Configuring the APN for Meitrack GPS trackers can be done

1. via the Meitrack manager when
2. Via the SMS console through the EMnify Portal (most simple)
3. via the EMnify SMS API or Zapier Integration (when automating the configuration)

When the GPS tracker is turned on for the first time after the SIM is installed it is showing the status `Attached` in the EMnify portal. At this point the device can receive SMS but not establish a data session unless the APN is setup.

The SMS command to set the APN for Meitrack GPS trackers is:

```
0000,A81,em,,
```

Where 0000 is the default SMS password.

On other devices the APN setting is done via the A21 command

```
666888,A21,1,server.meigps.com,8800,em,,
```

Where 666888 is the default superpassword (not the SMS password).

Both SMS and Superpassword can be changed and would then need to be replaced in the SMS command.

Elinz GPS APN configuration

Configuring the APN for Elinz GPS trackers can be done

1. Via the SMS console through the EMnify Portal (most simple)
2. via the EMnify SMS API or Zapier Integration (when automating the configuration)

When the GPS tracker is turned on for the first time after the SIM is installed it is showing the status `Attached` in the EMnify portal. At this point the device can receive SMS but not establish a data session unless the APN is setup.

The SMS command to set the APN for Elinz GPS trackers is:

```
APN,em#
```

On other models the APN configuration is a little different

```
apn[password] em
```

Default password 123456.

Reachfar GPS APN configuration

Configuring the APN for Reachfar GPS trackers can be done

When the GPS tracker is turned on for the first time after the SIM is installed it is showing the status `Attached` in the EMnify portal. At this point the device can receive SMS but not establish a data session unless the APN is setup.

Applies to RF-V6+, RF-V8, RF-V8S, RF-V13, RF-V16, RF-V18, RF-V20

The following two SMS commands need to send

```
123456,sos1,[yourphonenumber]# // Bind the tracker to a specific phone number e.g.
49173871878 (instead of +49173871878). 123456 is the default SMS password.
apn,em,plmn,90143#  // Send this SMS from the phone
```

123456 is the default password. After setting the APN the GPS tracker needs to be rebooted.

Applies to RF-V26, RF-V26+, RF-V28, RF-V30, RF-V32, RF-V34, RF-V36, RF-V36, RF-V38, RF-V40, RF-V42, RF-V43□RF-V44, RF-V46

The following two SMS commands need to send

```
pw,123456,center,[yourphonenumber]# // Bind tracker to specific phone. 123456 is the
default password.
apn,em# // Send this SMS from the phone
```

Queclink GPS APN configuration

Configuring the APN for Queclink GPS trackers can be done

1. Via the SMS console through the EMnify Portal (most simple)
2. via the EMnify SMS API or Zapier Integration (when automating the configuration)

When the GPS tracker is turned on for the first time after the SIM is installed it is showing the status `Attached` in the EMnify portal. At this point the device can receive SMS but not establish a data session unless the APN is setup.

The SMS command to set the APN for Queclink GPS trackers is:

```
AT+GTBSI=[password],em,,,,,,,0002$ // The password default is device model,e.g. gl200
```

Bitrek GPS APN configuration

Configuring the APN for Bitrek GPS trackers can be done

1. Via the SMS console through the EMnify Portal (most simple)
2. via the EMnify SMS API or Zapier Integration (when automating the configuration)

When the GPS tracker is turned on for the first time after the SIM is installed it is showing the status `Attached` in the EMnify portal. At this point the device can receive SMS but not establish a data session unless the APN is setup.

The SMS command to set the APN for Bitrek GPS trackers is:

```
setparam 0242 em
```

The Bitrek GPS tracker also utilize a roaming command (setparam 0917) together with a list of enabled networks (setparam 0020-0099). The following SMS commands need to be send

```
setparam 0917 1 // enable romaing in all networks as defined in the next SMS
setparam 0020 <MNC> // MNC is the mobile network code on which the device shall roam
setparam 0021 <MNC>
....
setparam 0099 <MNC>
```

All commands can be concatenated into one SMS (max. 160 characters) by using the ; as a delimiter.

```
setparam 0242 em; setparam 0917 1; setparam 0020 <MNC>; .....
```

Industrial Routers

Applies to RUT240, RUT950, RUT955, RUTX09, RUTX11, RUTX12, RUTX14, RUTXR1, RUT360

Newer firmware version of the Teltonika Routers should automatically detect the EMnify APN. Nevertheless, in case the APN is not correctly detected it can be configured with 3 methods

1. With the Teltonika WebUI over Wifi, Ethernet
2. Via the SMS console through the EMnify Portal (most simple)
3. via the EMnify SMS API or Zapier Integration (when automating the configuration)

1. APN configuration through the Teltonika Router WebUI

   Connect your PC through the routers Wi-Fi using the credentials provided on the device. Open the Teltonika WebUI http://192.168.1.1 and go to the Mobile configuration. Type in “em” in APN – there is no PIN configured on the SIM and no APN username or password required.

2. Teltonika Networks Router APN configuration via SMS console / API or Zapier

   Teltonika Documentation Source

   Make sure that the Router is powered on and the SIM card is inserted and activated. In the EMnify portal the device should show as `Attached`.

   The following SMS command need to be send to the device

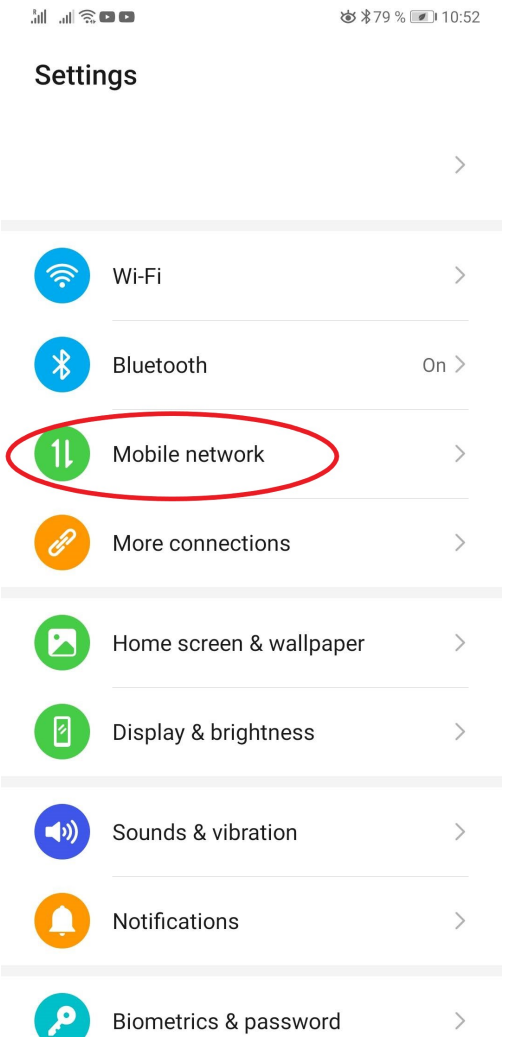
```
cellular apn=em
```

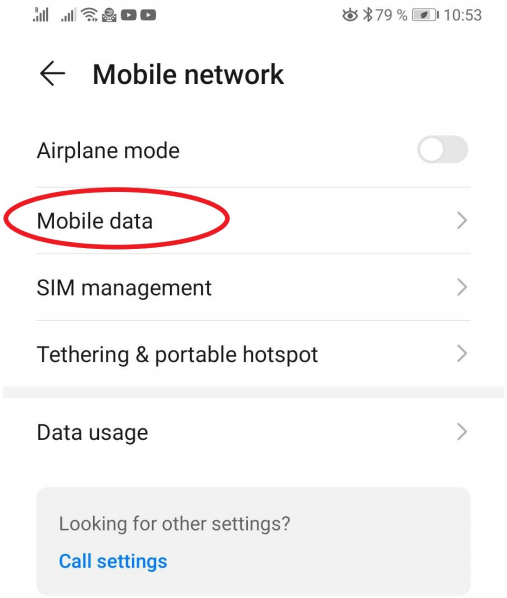
Android

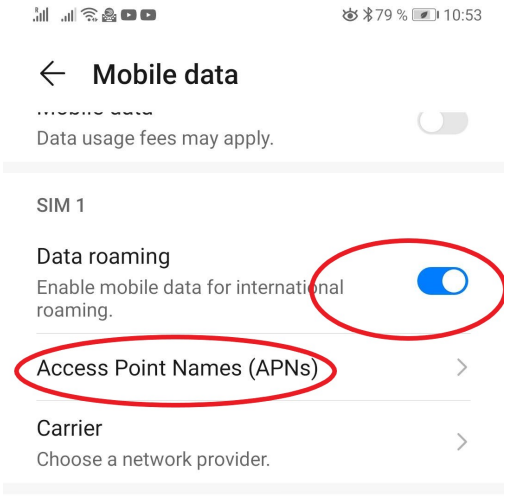
When setting up an Android device with an EMnify SIM you need to follow these 5 steps

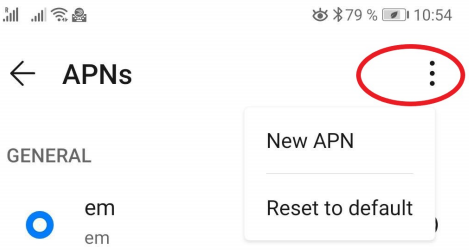
1. Go to Settings → Mobile Network

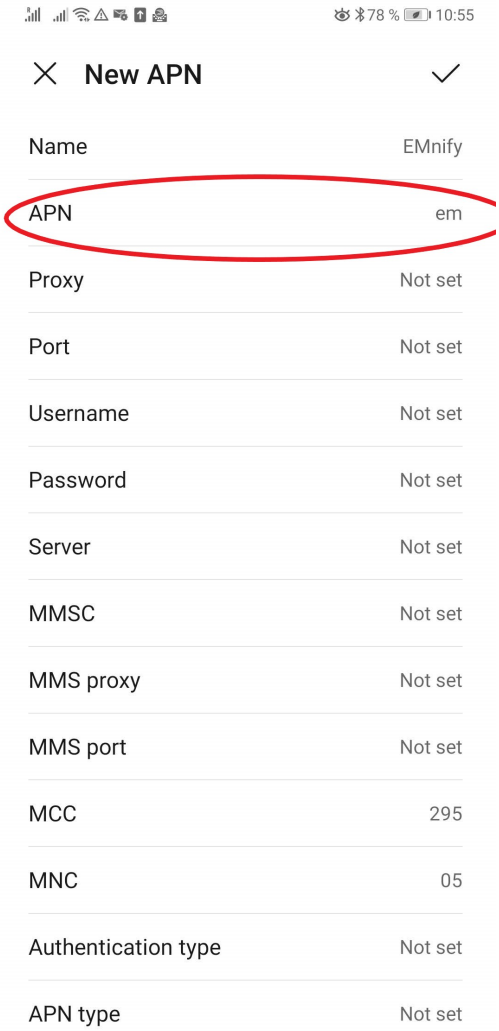
2. Go to Mobile data
3. Enable roaming and go to Access Point Names (APN)
4. Create a new APN with any name and configure the APN with "em"




79 % 10:53
Mobile network
Airplane mode
Mobile data
SIM management
Tethering & portable hotspot
Data usage
Looking for other settings?
Call settings


79 % 10:53
Mobile data
Data usage fees may apply.
SIM 1
Data roaming
Enable mobile data for international roaming.
Access Point Names (APNs)
Carrier
Choose a network provider.

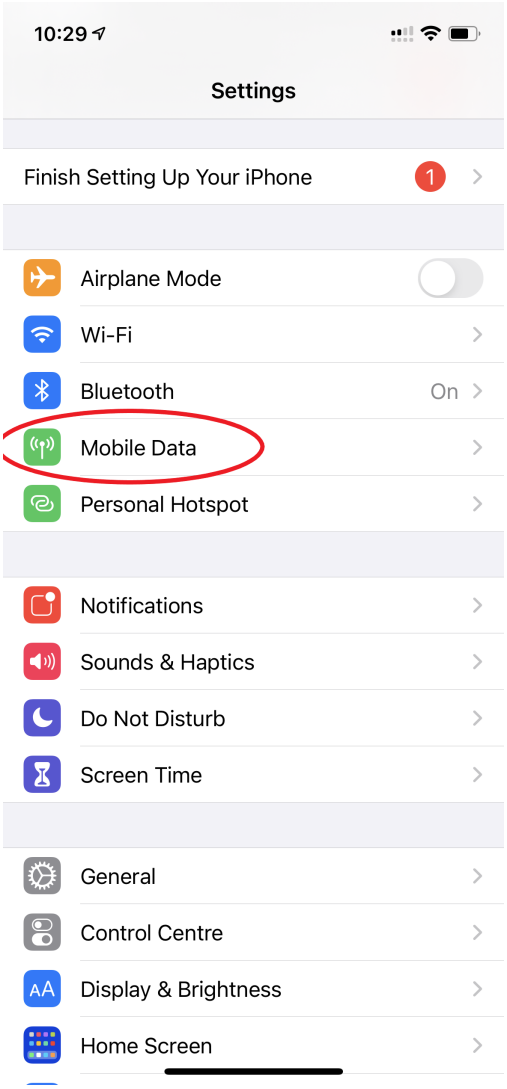

79 %
10:54
APNs
New APN
Reset to default
GENERAL
em
em

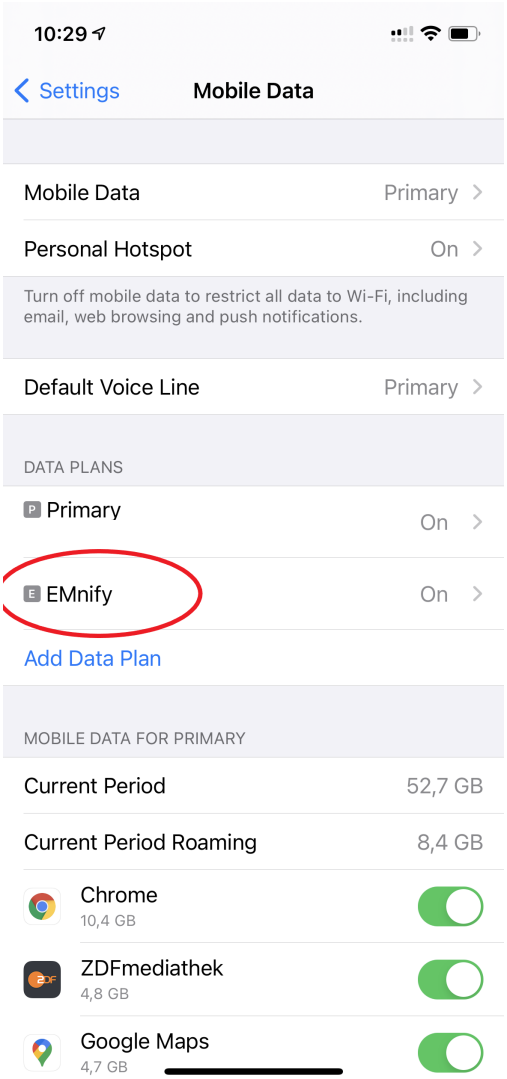


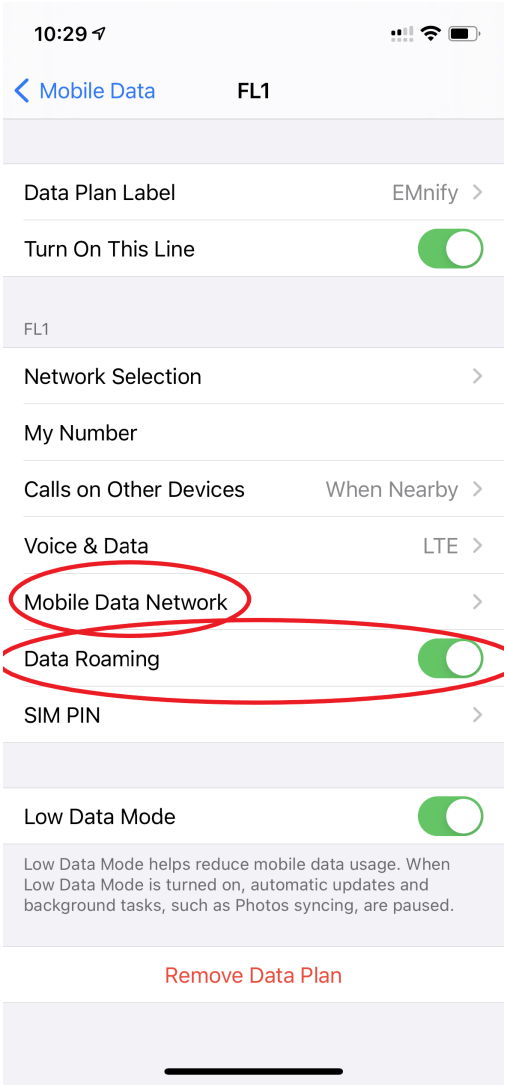
iOS devices

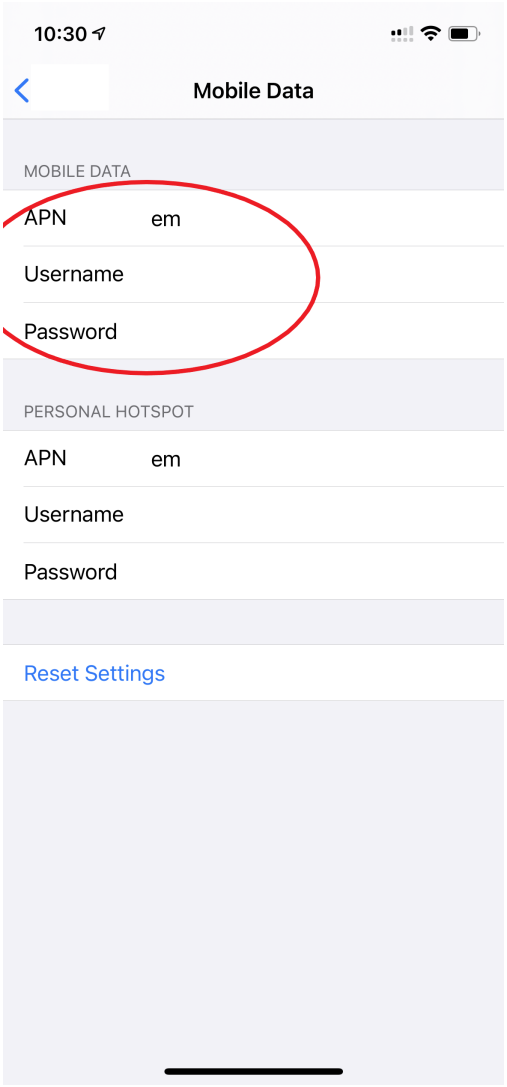
When setting up an iOS device with an EMnify IoT SIM you need to follow 4 steps

1. Go to Settings → Mobile Data
2. Click on the EMnify Data Plan (first one if regular SIM or secondary in case of eSIM)
3. Enable Roaming and Click on Mobile Data Network
4. Set APN to em - leave anything else blank


10:29
Settings
Finish Setting Up Your iPhone
1
Airplane Mode
Wi-Fi
Bluetooth
On
Mobile Data
Personal Hotspot
Notifications
Sounds & Haptics
Do Not Disturb
Screen Time
General
Control Centre
Display & Brightness
Home Screen


10:29
Settings
Mobile Data
Mobile Data
Primary
Personal Hotspot
On
Turn off mobile data to restrict all data to Wi-Fi, including email, web browsing and push notifications.
Default Voice Line
Primary
DATA PLANS
Primary
On
EMnify
On
Add Data Plan
MOBILE DATA FOR PRIMARY
Current Period
52,7 GB
Current Period Roaming
8,4 GB
Chrome
10,4 GB
ZDFmediathek
4,8 GB
Google Maps
4,7 GB


10:29
Mobile Data
FL1
Data Plan Label
EMnify
Turn On This Line
FL1
Network Selection
My Number
Calls on Other Devices
When Nearby
Voice & Data
LTE
Mobile Data Network
Data Roaming
SIM PIN
Low Data Mode
Low Data Mode helps reduce mobile data usage. When Low Data Mode is turned on, automatic updates and background tasks, such as Photos syncing, are paused.
Remove Data Plan



Troubleshooting

When you experience issues while connecting your device for the first time there are several common patterns that can be identified by looking at the connected device section in the portal. If you do not have any entry in the connected devices - go back to Creating a Device and assign the SIM.

The device will show different icons that indicate the status (`Offline`, `Attached`, `Online`, `Blocked`). If no icon is visible, assign a SIM to the device.

For most of the troubleshooting, a look at Details→Events is necessary. A usual event flow should look like this:

1. Update Location - the SIM card is (re)authenticating with a different network element. If successful the device will show as `Attached` and can already receive SMS.
2. Update GPRS location - the SIM card has successfully registered for data sessions with a different network element.
3. Create PDP context - the device has started a data transfer. The device will show `Online` as long is there is no delete PDP context event.
4. Delete PDP context - the device has ended a data transfer. The event details will also show the

data transmitted and the device status will be set to `Offline`

[event flow]

There can be many update locations before or in between the data session.

[offline] The device is offline

- click on Details → ensure that the device is enabled
- click on Details →Events. Validate if there is any location update event created and rejected. The reasoning should indicate the resolution to the problem. If there is no location update event:
- ensure the device is powered on and searches for a network
- ensure that the device is in reception of any supported network

[att] The device shows attached but does not transmit data

- ensure that the APN is correctly set to 'em' or use alternatively 'emnify' as some devices do not support two digit APNs. Guides for different device can be found Getting the first device online
- in case you changed policy settings make sure the radio types (2G,3G,4G) and data access is activated
- ensure mobile data is enabled, as well as international roaming is allowed
- click on Details → Events. Validate if there is any PDP create event and rejected. The reason and resolution is given in the event description.

NOTE	The `Attached` status does not necessarily mean that the device is powered on. If the device first attaches to a network and then powers off - there is no information towards the EMnify network that would allow to detect this.

[online] The device shows online but does not transmit data

- ensure mobile data is enabled, as well as international roaming is allowed
- validate under Details→Events if any `Warn` or `Error` is detected
- for NB-IoT and LTE-M this behaviour can happen when the device automatically connects to a network - rather specify the network that shall be used with using the `AT+COPS`. Also verify that the network is on EMnify's NB-IoT coverage or LTE-M network coverage list
- ensure that your data destination and DNS server (default EMnify uses googles 8.8.8.8 DNS if your device does not specify a DNS) is not blocked for the device

Other general troubleshooting tips

- after configuration changes make sure they are correctly applied on the device (e.g. with a reboot)
- a reset connectivity [reset] on Connected Devices can also reset the network state and allow your device to freshly reattach

- the issue may only be present with one network or in the specific location (e.g. due to high interference for this network). You can use the Operator Blacklist to block the network and force the change to a different network.

Service Stack Overview

IoT SIM

EMnify IoT SIMs are more durable than regular SIM cards and come in different form factors and quality grades. For testing the platform services quickly without any SIM hardware - EMnify offers an eSIM which can be downloaded directly onto a supported smartphone. EMnify also has a multi-IMSI software application directly on the SIM so different operator profiles can be used based on the location of the device. Using this technology EMnify can provide a superset of roaming networks from traditional operators.

Form Factors

The traditional, plugable SIM card comes in 4 different form factors: * 1FF (approximately the size of a credit card - only used in first GSM phones) - 85 x 54 x 0,76mm * 2FF (mini SIM) - 25 x 15 x 0,76mm * 3FF (Micro SIM) - 15 x 12 x 0,76 mm * 4FF (Nano SIM) - 12,3 x 8,8 x 0,67 mm

EMnify offers pre-punched SIM cards in different combinations 2-in-1 (1FF and 2FF), 3-in-1 (1FF,2FF,3FF) and 4-in-1 (1FF,2FF,3FF,4FF). Especially in use cases where the devices are moving it is advisable to use a SIM which exactly fits the device and does not have another smaller form factor punched-out. The SIMs are then more durable and the contact to the device is more firmly.

Another form factor is MFF2 also called embedded SIM with the dimension 6 x 5 x 0.75-0.82mm. The embedded SIms are soldered onto a device and not removable.

Note: Often the term eSIM is used for the MFF2 factor. Nevertheless the eSIM term is also used for SIMs whose operator profiles can be updated over the air. These eUICC based eSIM can be in any of the described form factors - not only in MFF2. While eSIM/eUICC is widely adopted for consumer smartphone and watches - for IoT use cases (where the profile cannot be download via a screen or QR reader) the commercial and deployment model of the required infrastructure prohibits an easy change of operator profiles and is therefore not widely adopted.

Quality Grades

The EMnify SIM cards come in two different quality grades Commercial and Industrial. In below table a comparison to a standard consumer SIM is made.

Parameter	Consumer SIM	Commercial	Industrial
Available form factors	2FF, 3FF, 4FF	2FF, 3FF, 4FF	MFF2, 2FF, 3FF (2-in-1 or 3-in-1)
Temperature Range	-	25° - 85°C	-40° - 105°C
Data Retention	10 years	10 years	15 years at 85°C

Parameter	Consumer SIM	Commercial	Industrial
Write Cycles	100,000	500,000	1,000,000
Memory	64-128kB	128kB	128KB
Corrosion Resistance Jedec JSD22-A107	-	CA	CC
Moisture Resistance Jedec JESD22-A102	-	110°C / 85% RH	130°C / 85% RH
Humidity Resistance Jedec JESD22-A101	-	-	HA
Vibration Jedec JESD22-B103	-	-	VA
Mechnical Shock Jedec JESD22-B104	-	-	SA
Low Power features	-	• Poll Interval negotiation • UICC suspension and resume	• Poll Interval negotiation • UICC suspension and resume

eSIM

EMnify offers an easy entry to test the services and platform by downloading an EMnify eSIM profile to an eSIM compatible phone or tablet. During the trial period every organization has the option to download one profile which can be used instantly.

The eSIM does not use a multi-IMSI applet (as on the physical SIM cards) and therefore has some differences in the network coverage. For a list of supported devices and limitations please refer to the knowledge base

The eSIM can be used to test and verify all EMnify functionalities including:

- availability of networks
- API functionality
- Cloud Connect and Datastreamer integration
- Zapier- No-Code Integrations

Multi-IMSI Application

EMnify IoT SIM cards are equipped with a multi-IMSI applet that contains EMnify's own and partner operator profiles. The different operator profiles are identified by the utilized [IMSI]. Each IMSI / partner operator usually has more than one network accessible per country.

The SIM applet utilizes a preferred IMSI list per country. When a device moves to a different country which has a different preferred IMSI configured (for e.g. because it gives access to more

networks), then the applet dynamically overwrites the previously active IMSI with the preferred IMSI for this country. Likewise, when an operator's service experiences outage, the SIM can automatically fall back to a fallback IMSI to ensure connection remains uninterrupted.

The selection of the IMSI partner that is used for the countries is based on mutliple factors. The preferred IMSI selected based on:

- allowance for permanent roaming in the country
- the most network partners in the country
- the best availability of radio access types (e.g. LTE) or availability of features (PSM/eDRX)

The Multi-IMSI applet is transparent for the device and has no impact on the device operation. In order to analyze which IMSI is currently in use, you can either check in the EMnify portal → Connected devices → Details or also query the device directly using the AT-command `AT+CIMI?`.

Global IoT Network and Platform

Even when IoT devices are more often only deployed at a single location and are not moving, for a vendor selling to multiple countries it is important to have a global connectivity solution, so that there is no need to have different SIM cards in stock or have multiple contracts and tariffs. For mobile use cases there is no other alternative than using an international SIM card.

Therefore, for deploying IoT solutions globally it is important to aggregate multiple operators in the same tariff with one IoT SIM. Another aspect is that the platform and data routing is setup to support a global deployment, while adhering to local data privacy regulations. EMnify's global platform therefore uses a distributed data plane and patented mechanism called regional breakout to address these needs.

Mobile Network Aggregation

Any mobile operator has a footprint of roaming networks in foreign countries. In case any of their subscribers travel, this ensures that they can be reached.

Distributed Data Transport

Regional Breakout

VPN Connectivity

SMS

Voice

RAN Aggregation

Radio Access Types

The EMnify IoT SIM and platform supports all devices and modules using the following radio access technologies

- 2G (GSM/GPRS/Edge) - in more than 370 networks
- 3G (UMTS/WCDMA/HPSA/HSDPA) - in more than 390 networks
- 4G (LTE/LTE-A/LTE-CATXX) - in more than 310 networks
- 5G (NR) - in 5+ networks
- LTE-M (CAT-M1) - in more than 60 networks
- NB-IoT (CAT-NB1, CAT-NB2) - in 12+ networks

When a device wants to connect with any of these radio technologies than the network needs to suport this technology as well as the device needs to support the frequency band which this network utilizes for this technology.

2G (GSM/GPRS/Edge)

GSM/GPRS is still one of the most dominant IoT technologies. Although the throughput is limited (GPRS max. 120kbps, Edge max. 1Mbps) it is more than sufficient for many IoT use cases. The modules are cheap (<10$) and the coverage is widely available throughout the world in more than 200 countries. EMnify provides GSM/GPRS coverage in more than 370 GSM networks.

GSM/GPRS is easy to deploy for IoT use cases because there only 4 frequency bands utilized by operators for GSM/GPRS worldwide.

In Americas

- B2 (1900MHz)
- B5 (850MHz)

In the rest of world

- B3 (1800MHz)
- B8 (900MHz)

Therefore, module manufacturers offer dual-band modules that can be used either in Americas or Rest of World - or Quadband modules that can be deployed globally.

Nevertheless GSM/GPRS is being phased out in several countries to free up frequency band for newer technologies. More than 60 networks have discontinued or announced to discontinue GSM technology.

3G (UMTS/WCDMA/HPSA/HSDPA)

3G technologies like UMTS, WCDMA, HSDPA, HSUPA have been driven by the surge for more data speed. As an evolution of GSM, many parts of the GSM/GPRS core network and signaling are reused, where the most difference is in the radio part.

With more than 170 countries worldwide 3G/UMTS is still widely available. EMnify provides 3G/UMTS coverage in more than 390 networks.

3G modules are easy to deploy - similar to 2G - as there are only 5 different frequency bands utilized by operators worlwide (with exception of Japan and China). Most UMTS modules therefore can be deployed worldwide.

- B1 (2100Mhz) - main UMTS band in the world
- B2 (1900Mhz) - used in Americas
- B4 (1700Mhz) - used in Americas
- B5 (850Mhz) - Australia / Americas
- B8 (900Mhz) - Europe

For Europe a 900/2100 Mhz dual-band module is required. For Americas a 850/1900 Mhz dual-band module is required.

3G/UMTS is also being phased out by several network operators to make space for newer technologies - also check here the article on GMS and UMTS networks that are being discontinued

4G (LTE/LTE-A/LTE-CATXX)

LTE is a 4G technology (another one would be Wimaxx - which never succeeded). With the evolution of LTE there have been different LTE categories established such as CAT-1, CAT-3, CAT-4, CAT-6, CAT-9, CAT-12 - mainly with increasing data throughput per category. While for consumer phones and broadband use cases the increase of throughput is relevant - the increasing costs for the modules have demanded for a lightweight LTE module for IoT use cases - which first led to CAT-1.

LTE CAT-1 offers 10Mbps in downlink and 5Mbps in uplink - and is available with network operators wherever LTE is deployed. Because of its wide availability and the possibility to roam between operators without limitation LTE CAT-1 is widely used in IoT use cases.

Currently EMnify offers connectivity over LTE in more than 310 networks worldwide.

The deployment of LTE devices in a global scale is more challenging than with GSM and UMTS because network operators worldwide have been using more than 27 different frequency bands. Most modules therefore only support specific regions where the device can be deployed.

Some main LTE-bands are

- B3 (1800 MHz) - Europe, Africa, APAC
- B7 (2600 MHz) - used in Americas, Europe, APAC
- B20 (800 MHz) - used in Europe, Asia
- B1 (2100 MHz) - Europe, Asia
- B2 (1900 NHz) - Americas
- B4 (1700 Mhz) - Americas

- B5 (850 Mhz) - North America, APAC

TIP	Validate the frequency bands utilized by the operators in your deployment countries before deciding for a module. You can look up the utilized frequency bands here

LPWAN: LTE-M/NB-IoT

While utilizing LTE infrastructure both NB-IoT and LTE-M are also part of the 5G standardization. Both technologies have been specified to meet the demand for IoT use cases in terms of:

- Reduced cost - to enable mass production of cellular IoT devices
  - removing unnecessary LTE features for IoT such as dual carrier, high modulations
- Low power utilization - for battery powered use cases that require years of operation
  - introducing power saving features such as [PSM] and [eDRX]
  - reducing the max. transmission power to less than 200mA to cater for battery max. current (GSM for example has 2A max power)
- Wider coverage - (+14dB for LTE-M and +20 for Nb-IoT sensitivity) for rural/indoor/underground use cases
  - utilizing extended coverage feature with more retransmissions to ensure data gets delivered
- Smaller module size - to enable smaller device use cases

Because LTE-M and NB-IoT rely on LTE infrastructure they also utilize a multitude of different frequency bands - a total of 26 bands have been specified for their use. To deploy NB-IoT and LTE-M in multiple countries and regions the modules need to support the operator frequency bands.

Cellular LPWAN modules come in different versions

- NB-IoT only or LTE-M only
- LTE-M/NB-IoT combined
- LTE-M/NB-IoT with 2G fallback and optional additional technologies (3G,4G)

As of today, roaming for NB-IoT is very limited between operators because of new charging models being implemented for NB-IoT. For LTE-M roaming usually works over regular LTE roaming - nevertheless some operators have limited the access to their LTE-M networks and the available features (PSM, eDRX).

Check the EMnify LTE-M coverage, availability of PSM/eDRX and proposed frequency bands on our Website.

Power-Save-Mode (PSM)

Jump to:

- Why cellular communication is not ideal for IoT
- How does Power Save Mode work

- Roaming for Power Save mode
- AT Command calculation and examples for PSM settings *

Cellular communication for smartphones usually requires low latency on downlink - in case you are being called your phone should ring right away. Because of this there are two things the device does which require power:

1. continously listening to the radio if there is an incoming call
2. transmitting location information to the network where it should be called - whenever it moves out of a tracking area and periodicly every 54 minutes

For most IoT use cases a downlink-initiated channel is not required - it is usually the device that intiates the communication to send e.g. sensor data. Therefore, a Power Save Mode is introduced that allows the device to go to sleep in case it has nothing to send.

The Power Save mode has these characteristics

- the Power Save Mode is similar to a power off period during which the module only consumes a couple of μA
- the device tells the network for how long it is going periodically into PSM (timer T3412 extended)
- the device/module will not be reachable during PSM from the outside in downlink
- the device can wake up the module and send data (e.g. powerkey, interrupt or pin triggered)
- when the device wakes up it does not need to reattach and reestablishing a PDN connection (unless it has moved to a different tracking area)
- after the device wakes up it stays in idle mode for a configurable time (timer T3324) to listen for downlink messages (e.g. firmware updates)
- the actual time the device is then in Power Save Mode is T3412 extended - T3324

[#PSM_Image].PSM and the 3412 and T3324 timers

NOTE	some modules (e.g. u-blox SARA-R4/SARA-N4) do not go into sleep mode when having a SIM enabled PIN. On EMnify SIMs the PIN is disabled.

Be aware that not all Nb-IoT and LTE-M networks have implemented PSM - and even when PSM is available with the local operator this does not mean that a roaming SIM can use it. This makes it very difficult for devices that are moving - in case they use PSM, and the new network does not support PSM - or only other timer configurations. We therefore regularly test the availability of PSM in our EMnify LTE-M roaming footprint.

The 3GPP defined AT command to configure PSM is `AT+CPSMS`m which sets the T3412 extended and T3324 timers.

An example command is

```
AT+CPSMS=1,,,01001110,00000101
```

PSM will be enabled (1) and the desired value for T3412 extended is 140 hours (01001110) and the desired value for the T3324 timer is 10s (01001110). The network does not necessarily use the desired values but utilizes supported values that are close to the desired values. To read the effective PSM configuration use the command

```
AT+CPSMS?
```

There is a good calculator fon how to set the values for 3412 and T3324 available from Thales.

Module vendors have also implemented module specific commands, e.g. Quectel

- AT+QPSMS extends PSM settings
- AT+QCFG="psm/enter",1 used to put the module immediately into PSM when the RRC connection is released (not waiting for T3324 to expire)
- AT+QPSMEXTCFG modem optimization command with different attributes such as making sure that PSM is randomized between different devices so they do not send data at the same time

extended Discontinuous Reception (eDRX)

- How does eDRX work
- Roaming with eDRX
- AT Command examples for eDRX settings

Whereas PSM is focused on uplink centric use cases, eDRX tries to reduce the power consumption for IoT Use cases that get downlink information. Regular smartphones are not continously listening on the radio for an incoming message but only every 1.28s or 2.56s which is called DRX (discontinous Reception). eDRX allows configuration of custom intervals of up to 40-175mins - depending on which configuration the visited network allows.

[eDRX].PSM and the 3412 and T3324 timers

As with PSM - not all NB-IoT and LTE-M networks support eDRX or the same timer configuration - and even if they do this does not guarantee that a roaming SIM card can utilize eDRX. We therefore also test and publish the eDRX availability on our LTE-M roaming footprint.

The standard 3GPP defined AT-command to configure eDRX is AT+CEDRXS.

As an example the below command enables (1) eDRX for LTE-M (4) and an eDRX cycle of 143.36s (1000).

```
AT+CEDRXS=1,4,"1000"
```

The setting for NB-IoT would be 5 and the timer values are shown in below table

0 0 0 0	5.12 seconds
0 0 1 0	10.24 seconds
0 0 1 1	40.96 seconds
0 1 0 0	5.12 seconds

0 0 1 0	61.44 seconds
0 1 0 1	81.92 seconds
0 1 1 0	102.4 seconds
0 1 1 1	122.88 seconds
1 0 0 0	143.36 seconds
1 0 0 1	163.84 seconds
1 0 1 0	327.68 seconds
1 0 1 1	655,36 seconds
1 1 0 0	1310.72 seconds
1 1 0 1	2621.44 seconds
1 1 1 0	5242.88 seconds
1 1 1 1	10485.76 seconds

The network will respond with the actual effective interval.

```
+CEDRXS: [4,"1000","1000","0111"]
```

5G (NR)

5G is the next major technology standard after LTE - which targets 3 different applications areas:

1. enhanced Mobile Broadband (eMBB)
    - with faster throughput upt 1Gps+ and more capacity in a local area
    - utilizing mmWave bands (5Ghz+) for increased throughput
2. Massive Machine Type communication (mMTC)
    - targeted at IoT application where a multitude of devices are in the same location and need to communicate with low power
    - LTE-M and NB-IoT often seen as decoupled from 5G to get earlier results will fusion with 5G mMTC
3. Ultra Reliable Low Latency Communications (URLLC)
    - for missing critical applications that require low latency and reliable data transmission

As of today 5G is mainly adopted for eMBB use cases - using a 5G non-standalone (NSA) deployment - meaning that the air interface uses 5G technology whereas the core network is still 4G.

EMnify has announced its first 5G roaming agreements in August 2020 and since then has reached agreements with more than a dozen network operators worldwide.

API & UI

Integrations

Services

SIM Life Cycle Management

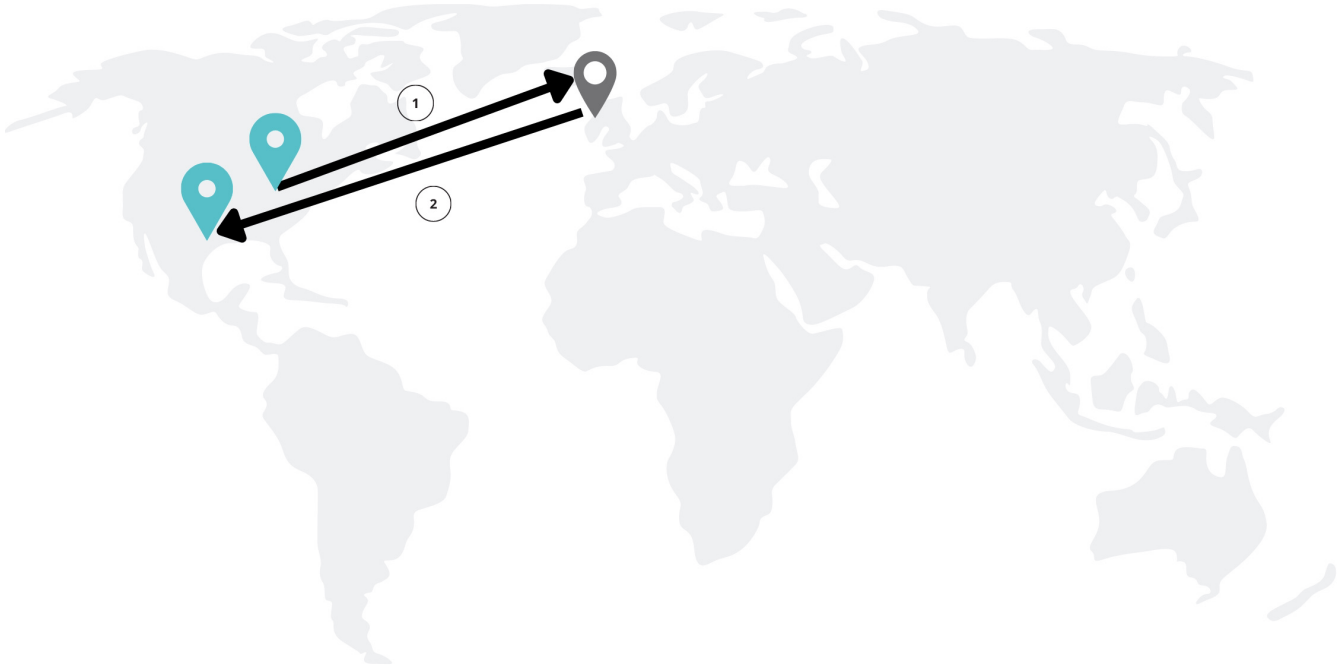
Endpoint Management & Policies

Regional Breakout

Traditional connectivity providers normally have a centrally located network core which increases network latency.

Let’s take an example of a network provider which has its network core in Ireland. And the application as well as the device that is using the nework data is in USA. This data travels from the device in USA, to the network core in Ireland and then back to the application server in USA. This geographical distance between the application server and the core network will increase the network latency. However if the network core were to be in the USA, the network latency will be lesser.

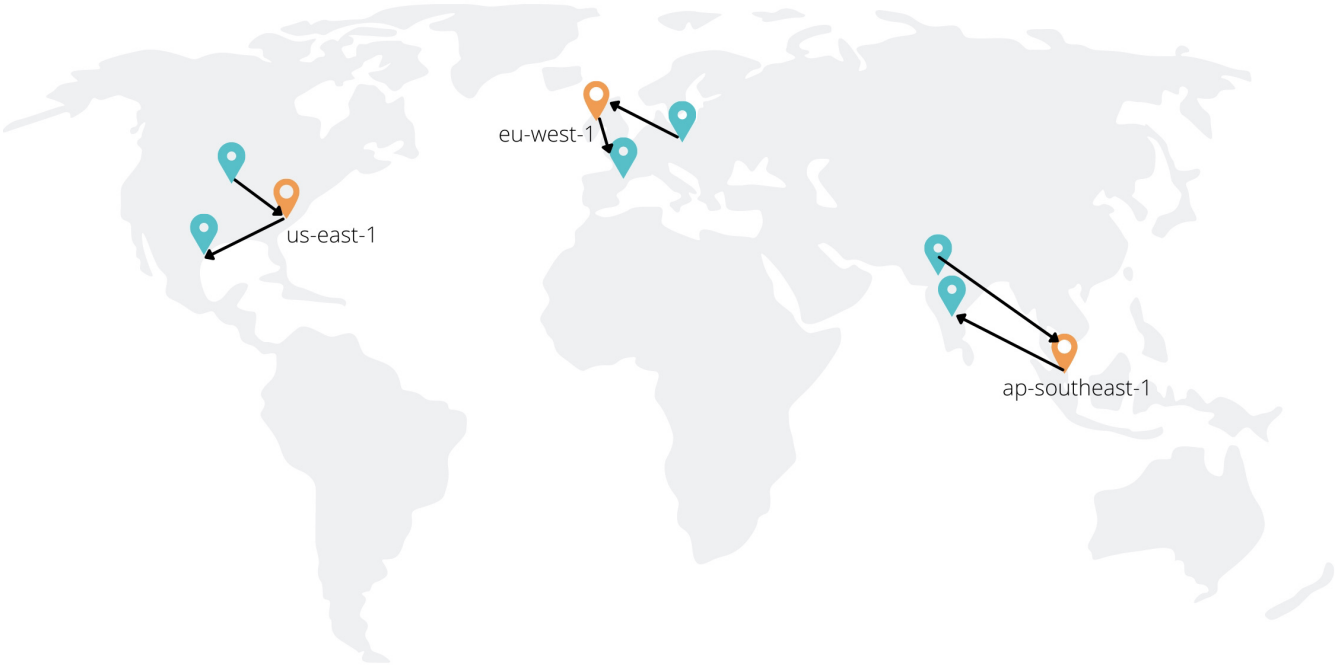
Network Latency due to centrally located core network



EMnify’s Regional Breakout is a solution for this network latency. Because of EMnify’s globally distributed cloud architecture, you can route endpoint traffic- either dynamically depending on the device’s location or through pre-defined system configuration. Choosing "Regional Breakout” in your Device Service Policy will let the system dynamically choose the breakout region, based on the visited network’s location.

Reduction in Network Latency due to EMnify Regional Breakout regions

EMnify Regional Breakout



Multi Cloud Data Streamer

Events

Usage Data

Cloud Connect

Transit Gateway

IPSec

OpenVPN

EMnify's communication platform hosts a OpenVPN service, that allows to establish a private network between the device and any remote client location. The remote client can either be on the application server itself - or also on any machine that wants to remotely access the device.

OpenVPN Overview

To use the OpenVPN service the IoT device does not need any OpenVPN software or dynamic DNS resolution. Through the EMnify SIM every device will get a private static IP address which can be used to identify and address the device.

You can connect from any machine using a OpenVPN client to the OpenVPN service on the EMnify communication platform. The machine can then use the private static IP address of the device to

communicate with it remotely.

OpenVPN System Overview

[OpenVPN System Overview]

At the same time the IoT device can send data through the private tunnel to the IP address of the remote machine.

OpenVPN setup

In order to setup OpenVPN on your machine the following high level steps are required.

1. In the EMnify Portal → Device Policies: Set the service profile to a VPN breakout region, eu-west-1 (VPN)
2. Portal → Integrations → OpenVPN: download the VPN configuration file for your region and operating system
3. Create a credentials.txt with you username / password or organisation_id / application token.
4. load the VPN configuration file and credentials.txt with your OpenVPN client

For detailed instructions please refer to our knowledge base articles

1. OpenVPN Integration MacOS
2. OpenVPN Integration Windows
3. OpenVPN Integration Linux

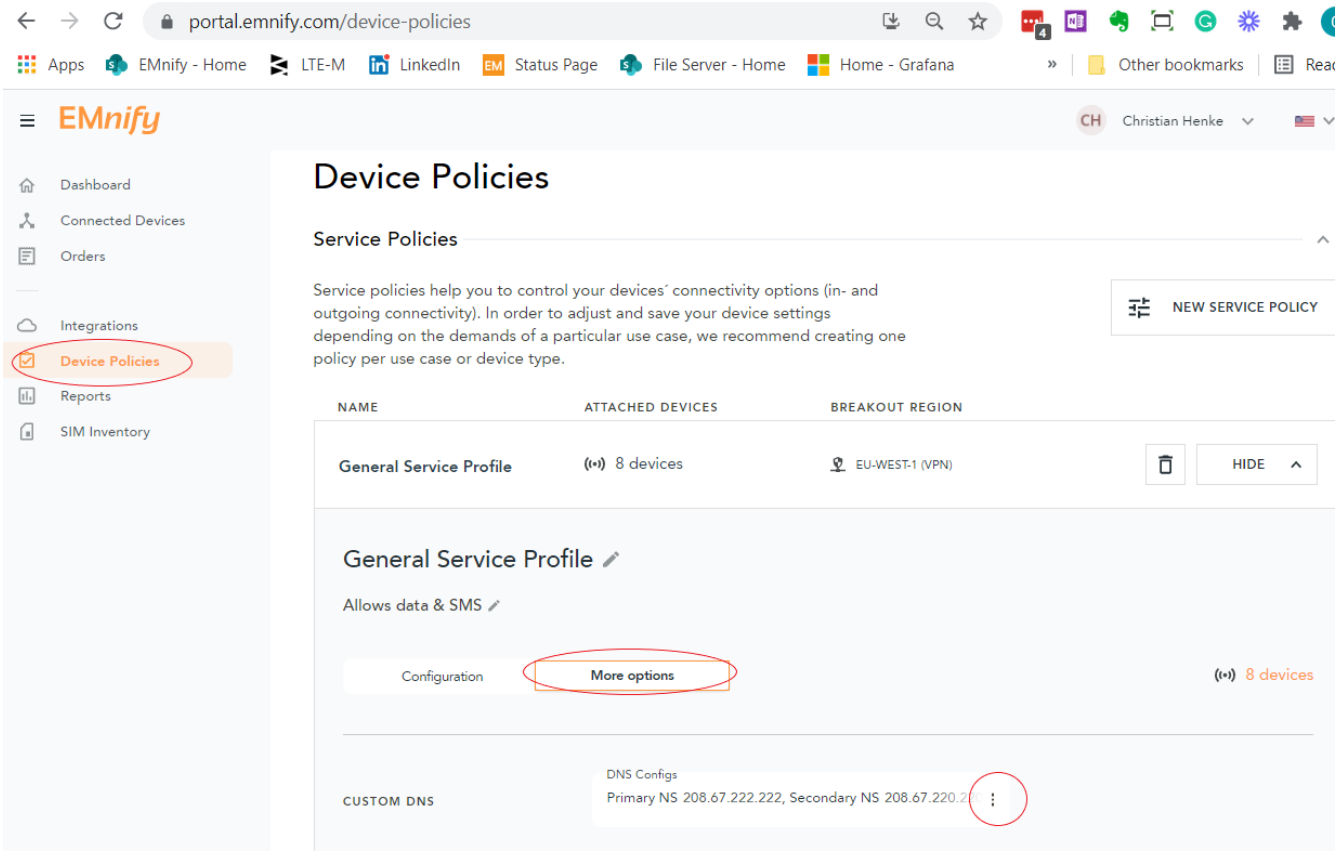
Security

DNS

When a device establishes a connection it uses a Domain Name Service (DNS) to resolve a hostname to an IP address to which it can send data. For example a hostname such as *.iot.example.com will be mapped to the IP address e.g. 120.126.230.60.

The device itself can configure a DNS service that it uses to resolve domain names. If the device does not use a DNS then EMnify will provide a domain name service to the device. By default EMnify will route all DNS queries over Google's public DNS `8.8.8.8`.

Customers can also configure to use their own DNS - no matter if it is a public or a private one. The DNS settings can be changed in the Portal → Device Policies → Service Policies → More Options → DNS



.Custom DNS setting configuration

Utilizing a private DNS server which is not reachable via a public IP, requires to setup a private network with the machine or a network where the private DNS is located. This can be done using Cloud Connect either with Amazon Transit Gateway or IPsec. A tutorial on how to setup a DNS firewall based on a private DNS using Amazon Route 53 is available here

IMEI Lock

Identity and Access Management

Business Intelligence and Analytics

No-Code Workflow Automation

Connectivity as Code

API Authentication

Working with SIMs and Endpoints

SIM State Management

Endpoint Connectivity Status

Sending and receiving SMS

Retrieving Events and Statistics

API Reference

Code Samples

Java SDK

Javascript

Python

Integration Guides

Blue Prints

Automating SIM Life Cycle Management

How to integrate data into operational dashboards

How to build a prepaid service

Integrating Connectivity Status in a Portal

Glossary

Active SIM

A SIM that has network activity at a certain time period (signaling level or teleservices)

APN - Access point name

A gateway between a GSM, GPRS, 3G or 4G mobile network and another computer network, usually the Public Internet.

Application Token

A unique identification key used to access EMnify's VPN services

A2P SMS - Application–to–peer SMS

SMS between an application and a device

Assigned SIM

SIM that had been assigned to an Endpoint

AT+CREG AT command: gives information about the registration status and access technology of the serving cell

AuC - Authentication center

a part of GSM infrastructure, validates any SIM card attempting network connection when a phone has a live network signal.

BIC - Batch Identification Code

a code used to register the EMnify SIM cards on the EUI

BTS - Base Transceiver Station

Callback URL

Computer programming practice of sending executable code to another web address

Carrier-agnostic network

A network that provides routing consistency regardless of the roaming mobile network that the SIM is connected to.

CID profile

A generally unique number used to identify each (BTS) Base transceiver station or sector of a BTS within a (LAC) Location Area Code if not within a GSM network

Connectivity status

This is the connectivity status of an endpoint which can be set to online, attached, offline:

- Online : Endpoint is transmitting data
- Attached : Endpoint is attached to a network but not transmitting any data
- Offline : Endpoint isn't attached to a network

Data package

A data bundle that can be used by all SIM cards until the end of the calendar month

Data RX

Data sent from the device

Data session

A session between opening and closing a data connection to the network

Data TX

Data received by the device

Data Usage (volume)

The data that has been used by an endpoint

DNS Domain Name System

A hierarchical decentralized naming system for computers, services, or any resource connected to the Internet or a private network

Dynamic endpoint reconfiguration

Live changes to the endpoint parameters

Dynamic IP

An IP that changes over time

Dynamic network reconfiguration

Live changes to the network parameters

Endpoint

A representation of the device which has a SIM installed

Endpoint Status

The current state of the endpoint: Enabled/Disabled

eUICC

Embedded Universal Integrated Circuit Card, allows hosting multiple mobile network profiles on the SIM

Event log

A log that stores all Endpoint events

Form factor

Form factor of a SIM card represents the SIM card format (SIM cards vary in size (Mini vs Micro vs Nano), function (embedded vs standard) and quality (industrial grade vs standard)):

- 2FF : mini SIM card
- 3FF : Micro SIM card
- 4FF : Nano SIM card

GGSN - Gateway GPRS Support node

Part of the GSM infrastructure, the GGSN is responsible for the interworking between the GPRS network and external packet switched networks

Globally–distributed infrastructure

Cloud infrastructure which is distributed globally, with several local breakout points for better traffic handling

Global Routing Consistency

A single set of connectivity rules and settings applied when the SIM roams over various

networks

GSM (Global System for Mobile communiations)

a standard developed by the European Telecommunications Standards Institute to describe the protocols for second-generation (2G) digital cellular networks used by mobile devices

HLR - Home location register

A part of GSM infrastructure, a database from a mobile network in which information from all mobile subscribers is stored

http POST request

A request method supported by the HTTP protocol

ICCID - Integrated Circuit Card Identifier

A unique number used to identify a SIM card.

IMEI - International Mobile Equipment Identification number

A unique number used to identify mobile phones

IMEI lock

The practice of strictly associating a SIM to the device with a certain IMEI number

IMSI - International mobile subscriber identity

A unique number used to identify a GSM subscriber

Inactive SIM

A SIM that doesn’t have any network activity at a certain time period

IPSec

A protocol suite for Secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session

IP subnet

A logical subdivision of an IP network

JSON - JavaScript Object Notation

a lightweight data-interchange format. It is easy for humans to read and write. It is easy for machines to parse and generate.

LAC - Location Area Code

A unique 16-digit fixed length location area identity code that identifies a phone number’s location area

MFA Key

A combination generated by external device or a service which is used to authenticate the user

MFF SMD (embedded)

SIM card embedded in the device during manufacturing

MSISDN - Mobile Station International Subscriber Directory Number

A unique number used to identify a mobile phone number internationally

MSC Mobile Switching Center

A part of GSM architecture which controls the network switching subsystem elements

NFV Network Functions Virtualization

The concept of replacing dedicated network appliances, such as routers and firewalls, with software running on commercial off–the–shelf servers

Network–based firewall

Firewalls which are deployed by an entire network

OTA Over–the–air

A method of wireless distribution of the software, configuration settings or encryption keys

OTA Provisioning

A technology which allows making changes to the SIM memory over–the–air

OpenVPN

An open–source software application that implements virtual private network (VPN) techniques for creating secure point–to–point or site–to–site connections in routed or bridged configurations and remote access facilities

P2P SMS Peer–to–Peer SMS

SMS exchanged between devices

PCRF Policy control

the software node designated in real–time to determine policy rules in a multimedia network

PDP context

Data structure present on both the serving GPRS support node (SGSN) and the gateway GPRS support node (GGSN) which contains the subscriber's session information when the subscriber has an active session

Private IP

The IP address that is used/stored in the local network

Public IP

The IP address which is accessible from the public Internet

RESTful API

The Representational State Transfer Application programming interface, which allows you to integrate services with your applications

Release SIM

The act of unbinding a SIM from the endpoint

Routing

The process of selecting a path for a network

SDN Software–Defined Networking

An approach that allows network administrators to programmatically initialize, control, change, and manage network behavior dynamically via open interfaces

Service profile

A profile which defines the services and functionality of an endpoint

SIM batch

A collection of SIM cards that can be registered with a single BIC code

SMS Firewall

A firewall that controls the SMS flow

SIM hosting fee

Monthly fee for an active SIM

SIM Profile

The MNO's ID information which is stored in the SIM's memory

SIM repository

All SIMs assigned to your organization

SIM status

Life cycle of a SIM card

- Purchased SIMs : The SIMs purchased by the customer
- Registered SIMs : The SIMs that the customer registered to his account, but haven't activated yet
- Unregistered SIMs : The SIMs that the customer did not register to his account
- Activated SIMs: The SIMs that have been activated
- Suspended SIMs : The SIMs that have been suspended
- Deleted SIMs : The SIMs that have been deleted from the platform

SMPP - Short Message Peer–to–Peer

A protocol used by the telecommunications industry for exchanging SMS messages between Short Message Service Centers (SMSC) and/or External Short Messaging Entities (ESME)

SMSC - Short message service center

A network element in the mobile telephone network that stores, forwards, converts and delivers Short SMS messages

SMS console

An interface to send A2P SMS from the platform to the SIM card

SMS MO

SMS originating from the device

SMS MT

SMS terminated (received) by the device

Source Address

The address of the SMS sender as displayed on the receiving device

Static IP

An IP that doesn't change over time

Tariff profile

A profile which defines which networks or countries SIM should operate in

Traffic pooling

A term which is used to describe the service model when various endpoints utilize the same data pool

Unassigned SIM

SIM that had been unassigned from an Endpoint

Usage limit

User–defined limit of consumption of a certain service (data, SMS) per endpoint

User–defined coverage

An ability to select which operator customer's SIM connects to

User–Defined Networking

An approach which enables user to create his own virtual mobile network, define service and security policies and provision tariff profiles and data packages

USSD - Unstructured Supplementary Service Data

A protocol used to communicate with the service provider's computers

USSD gateway

The collection of hardware and software required to interconnect two or more disparate networks, including performing protocol conversion

VPN

virtual private network