

Service Description

emnify GmbH

May 10, 2023

Version 1.9



Contents

1	Purpose of this document	4
2	emnify IoT eSIM	4
2.1	eSIM technology	4
2.1.1	M2M eSIM	4
2.1.2	Consumer eSIM	4
2.2	Form factors	5
2.3	Quality Grades	6
2.4	Compliance and software features	6
2.5	Multi-IMSI applet	6
3	emnify IoT SuperNetwork	7
3.1	Cellular IoT connectivity	7
3.1.1	Global coverage	7
3.1.2	Dedicated IoT specific multi-network access	8
3.1.3	Radio access types and frequency bands	8
3.1.4	2G (GSM/GPRS/EDGE)	8
3.1.5	3G (UMTS/WCDMA/HSPA/HSDPA)	9
3.1.6	4G (LTE/LTE-A/LTE-CATXX)	9
3.1.7	LPWAN: LTE-M/NB-IoT	9
3.1.8	5G (New Radio)	10
3.2	emnify local connectivity	10
3.2.1	Regional Breakout	10
3.2.2	emnify regional breakouts	11
4	emnify connectivity platform	11
4.1	emnify Portal	11
4.1.1	Dashboards	12
4.1.2	Device Details	12
4.1.3	Device Policies	12
4.1.4	Location Information	13
4.1.5	SIM orders	13
4.1.6	SIM lifecycle management	13
4.1.7	User management	13
4.2	emnify APIs	14
4.2.1	REST API	14
4.2.2	GraphQL	15
4.2.3	Data Streamer	15
4.2.4	SDK	15
4.2.5	No-Code	15
4.2.6	Events	15

5	Communication services	16
5.1	Data	16
5.1.1	Public internet breakout	16
5.1.2	Virtual Private Network	16
5.1.3	Inter-device communication	18
5.1.4	Regional breakout	18
5.2	SMS	18
5.2.1	SMS MO/MT	19
5.2.2	P2P SMS	19
5.2.3	A2P SMS	19
5.2.4	SMS short codes	20
6	Network security services	21
6.1	SASE overview	21
6.2	Virtual Private Network options	21
6.2.1	Private static IP	21
6.2.2	Cloud Connect – secure data transport	21
6.2.3	OpenVPN – remote access	22
6.3	Custom DNS	22
6.4	IMEI lock	23
6.5	Centralized policies	23
6.5.1	Service policies	23
6.5.2	Coverage policies	23
7	Support	24
7.1	Service Options	24
7.2	Incident Management	24
7.3	Roaming	25
7.4	Customer Success Manager	25

1 Purpose of this document

This document outlines emnify's service offering for IoT solution providers who use emnify's cloud native IoT communication platform to bring their devices online, as well as integrate and manage global device connectivity. Throughout the document any of these types of customers are referenced as Enterprises.

The document outlines key service offerings, available functionalities of the emnify platform including private IoT networking, integration, and quota management, as well as emnify's customer support.

2 emnify IoT eSIM

A SIM card is basically a microprocessor that allows a device to connect to cellular networks. Nevertheless, it has its own operation system, file system, and apps that differentiate it from other SIM cards. The emnify IoT eSIM has been specifically designed and programmed to serve enterprises that want to deploy their devices in any part of the world. It's important to consider that the SIM cards in IoT devices – in contrast to consumer SIM cards used in smartphones – cannot be swapped out when delivered to a customer site. With state of the art technology such as the M2M eUICC standard and software applications such as the multi-IMSI applet, the emnify IoT eSIM ensures reliable connectivity.

2.1 eSIM technology

2.1.1 M2M eSIM

Every new SIM you order from emnify is an M2M eSIM (compliant with SGP.01, SGP.02, and SGP.016). The M2M eSIM is also referred to as an eUICC (Embedded universal integrated circuit card). Unlike a regular SIM (UICC), an eUICC can be updated over the air. Because M2M eSIMs can be updated with new configurations or profiles, this eliminates the need for SIM swaps.

2.1.2 Consumer eSIM

emnify also offers consumer eSIMs for phones, tablets, and smart watches. The consumer eSIM can be downloaded to a device by scanning a QR code. For information about consumer eSIM technology, please [contact us](#)¹.

¹Contact emnify via <https://www.emnify.com/talk-to-us>

2.2 Form factors

emnify M2M eSIMs are available in the following form factors.

Form factor	Dimensions
2FF (Mini SIM)	15 x 25 x 0.75 mm
3FF (Micro SIM)	12 x 15 x 0.75 mm
4FF (Nano SIM)	8.8 x 12.3 x 0.75 mm
MFF2 (eSIM)	5 x 6 x 0.75 mm, 8 pin

MFF2 eSIMs can be soldered onto a device and are not readily removable. Visit the emnify SIM Shop where you can choose between these packages:

- Triple-cut commercial
 - Mini (2FF)
 - Micro (3FF)
 - Nano (4FF)
- Dual-cut commercial
 - Mini (2FF)
 - Micro (3FF)
- Single-cut Mini Industrial (2FF)
- Single-cut Micro Industrial (3FF)
- Embedded MFF2

In use cases where devices are mobile, we highly recommend choosing the form factor that fits the device exactly, not multi-cut ones that include a smaller form factor than is needed. Not only are such pluggable SIMs more durable, but their contact with the device is also firmer.

2.3 Quality Grades

emnify eSIMs come in three different quality grades: **Commercial eUICC**, **Industrial eUICC**, and **MFF2**.

		Commercial eUICC	Industrial eUICC	MFF2
Form Factor	Embedded/solderable	-	-	MFF2
	Removable Card	Triple-cut or Dual-Cut	2FF or 3FF	-
Chip Type	Operational and storage temperature	25°C to +85°C (JESD22-A104)		40°C to +105°C (JESD22-A104)
	Operating voltage	1.62V to 5.5V		
	Interface	ISO-7816, T=0		
	Chipset NVM size	704 Kbytes		
	Chipset RAM size	20 Kbytes		
NVRAM characteristics	Write Endurance	500k erase per page 10M cycles with OS High Endurance		
	Data retention	15 years @ 85°C		
	Moisture/Reflow conditions	-	MSL3 (J-STD020)	
	Humidity	-	HA as per ETSI TS 102.671 / (JESD22-A101D)	
	Corrosion	-	-	CX as per ETSI TS 102.671 (JESD22-A107)
	Vibration	-	-	VX as per ETSI TS 102.671 (JESD22-B103)
	Shock	-	-	SX as per ETSI TS 102.671 (JESD22-B104)
	Common Criteria Certificate	CCN-CC-5/2019		

2.4 Compliance and software features

The following compliance standards and software features apply to all quality grades of emnify eSIMs.

emnify eUICC Compliance	GSMA	SGP.01 Embedded SIM Remote Provisioning Architecture	1.1
		SGP.02 Embedded UICC Technical Specification	3.2
		SGP.16 M2M Compliance Process	1.1
	TCA	eUICC Profile Package Interoperable Format Technical Specification	2.1
Software Features	Embedded Universal Integrated Circuit Card (eUICC)	Maximum number of profiles	10
		ISD-A and ISD-R system applets	Supported
		EAP-SIM and EAP-AKA authentication protocols	Supported
	LPWAN features	Suspend and resume SIM state ETSI TS 102 221	Supported
		Poll Interval Negotiation ETSI TS 102 221	
	OTA Capabilities on ISD-P: Remote file management – RFM Remote applet management – RAM	HTTPS	Supported
		TLS 1.2	Supported
		AES algorithm (128-bit, 192-bit, and 256-bit keys)	Supported
Compliance	GlobalPlatform	All Secure Channel Protocols	Supported
	Java Card	Standard Java Card APIs	Supported
		GlobalPlatform API	Supported
		ROHS	Yes
		REACH	Yes

2.5 Multi-IMSI applet

emnify eSIM cards are equipped with a multi-IMSI applet that runs in the background using minimal resources without any negative impact on the device's performance. This technology is similar to a mobile phone using dual-SIM technology. An emnify eSIM has cellular provider information from multiple SIM cards already included. While emnify has

roaming agreements and local contracts with operators around the world, emnify also uses partner operators to increase the network coverage footprint in order to provide a fallback when preferred networks experience outages.

The multi-IMSI applet works in the following manner. emnify has its own operator identity (IMSI²) as well as the partner operator's IMSI stored on the SIM card. In most countries, an IMSI / partner operator will have access to multiple networks. The applet maintains a list of preferred IMSIs to take advantage of such alternate sources of connectivity. For example, this list defines that IMSI X will have the highest priority for access in country A. However, if the device can't connect, another operator, IMSI Y, will be next on the list of priorities. So when a device then moves to country A, the applet dynamically overwrites the active IMSI with IMSI X based on the preferred IMSI list. Then when operator X has a service outage, the SIM automatically falls back to IMSI Y to ensure the device can maintain connectivity.

The selection of the preferred IMSI for each country is based on multiple factors, including:

- If permanent roaming is permitted in that country
- IMSI that has the most network partners in the country
- IMSI that has the best availability of radio access types (LTE, NB-IoT, LTE-M) or features (PSM/eDRX)

3 emnify IoT SuperNetwork

3.1 Cellular IoT connectivity

Cellular is the most widely-used wireless network technology for connecting things. It is superior to other wireless technologies with regard to network availability and security. Cellular solutions improve the end-customer experience by instantly delivering data at the customer site without local integration. Not only is this solution ideal for mobile use cases but also for stationary devices.

3.1.1 Global coverage

emnify uses an approach to aggregate the roaming footprint of multiple operators with the goal of offering access to every network in the world. Mobile operators utilize roaming in foreign countries so their subscribers can stay connected when traveling. Often operators do not have roaming agreements with all countries or only have a roaming agreement for one network – which is sufficient for roaming travelers but not ideal for devices that could be anywhere in the country. emnify works with multiple partner operators across the globe to be able to offer more networks at a commercially viable rate.

²IMSI (International Mobile Subscriber Identity), a unique number used to identify a GSM subscriber.

The emnify multi-IMSI applet makes it completely transparent for the device to identify which roaming agreement of which operator is being utilized.

3.1.2 Dedicated IoT specific multi-network access

emnify is dedicated to IoT connectivity even without having any base stations of its own. Instead, emnify has direct roaming agreements with more than 400 networks for the sole purpose of connecting IoT devices. Additionally, emnify works with network partners to increase the number of available networks with the goal of allowing devices to connect through any cellular network. Consequently, emnify's IoT eSIM can connect to more than 540 networks around the world.

3.1.3 Radio access types and frequency bands

The emnify IoT SuperNetwork and IoT eSIM supports all devices and modules using the following radio access technologies.

- 2G (GSM/GPRS/EDGE)
- 3G (UMTS/WCDMA/HSPA/HSDPA)
- 4G (LTE/LTE-A/LTE-CATXX)
- 5G (New Radio)
- LTE-M (CAT-M1)
- NB-IoT (CAT-NB1, CAT-NB2)

When a device wants to connect with any of these radio technologies, the network needs to support this technology as well as the device needs to support the network-specific frequency band for this technology.

3.1.4 2G (GSM/GPRS/EDGE)

As one of the most dominant IoT technologies still in use, emnify IoT SuperNetwork provides 2G service. Although the throughput is limited (GPRS max. 120 kbps, EDGE max. 1 Mbps) it is more than sufficient for many IoT use cases.

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

In the 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.](#)

3.1.5 3G (UMTS/WCDMA/HPSA/HSDPA)

The IoT SuperNetwork also provides 3G services like UMTS, WCDMA, HSDPA, HSUPA.

3G/UMTS is being phased out by several network operators to make room for newer technologies. See also the article on [GMS and UMTS networks that are being discontinued.](#)

3.1.6 4G (LTE/LTE-A/LTE-CATXX)

The emnify IoT SuperNetwork provides 4G network service complying with all LTE categories such as CAT-1, CAT-3, CAT-4, CAT-6, CAT-9, and CAT-12.

For broadband use cases, higher category LTE device categories offer more bandwidth. This means that CAT-1 offers a low cost alternative for specific IoT use cases where bandwidth is not a priority.

3.1.7 LPWAN: LTE-M/NB-IoT

The emnify IoT SuperNetwork provides the largest coverage of cellular Low-Power Wide Area Networks (LPWAN) - namely LTE-M and NB-IoT. Our blog post [LTE-M vs NB-IoT: 5 Considerations for Your IoT Solutions](#) compares their technical differences. Check our website for a list of [LTE-M networks](#) and [NB-IoT networks](#).

LTE-M and NB-IoT available on the IoT SuperNetwork provide

- 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 – (+14 dB for LTE-M and +20 dB 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

3.1.8 5G (New Radio)

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

1. Enhanced Mobile Broadband (eMBB)
 - With faster throughput upto 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

The emnify IoT SuperNetwork supports 5G Non-Standalone (5G NSA) networks which are mainly deployed to provide enhanced Mobile Broadband (eMBB). In 5G NSA deployments the air interface uses 5G technology but the core network is still 4G.

In August 2020 emnify announced its first 5G roaming agreements. Since then emnify has entered into agreements with more than a dozen network operators worldwide.

3.2 emnify local connectivity

Traditional operators and MVNOs always have a home network – and infrastructure – in a country or market where they provide their service. emnify's IoT SuperNetwork doesn't have a "home" country. Instead, it is comprised of a cloud-based infrastructure that is deployed in 4 regions in order to provide local connectivity to each market.

3.2.1 Regional Breakout

When network operators have their infrastructure in one home country, all data from SIM cards of this operator are first routed back to their home country, even if the device is on a different continent. This is called Home Routing.

3.2.2 emnify regional breakouts

emnify's distributed data plane enables device data to breakout locally, keeping the customer data within the same region. Moreover, it also helps reduce network latency. You can either select a specific breakout region or the network automatically selects the breakout region closest to the device. This can be done on the emnify Portal » **Device Policies** » **New service policy** which is applicable to a group of devices.

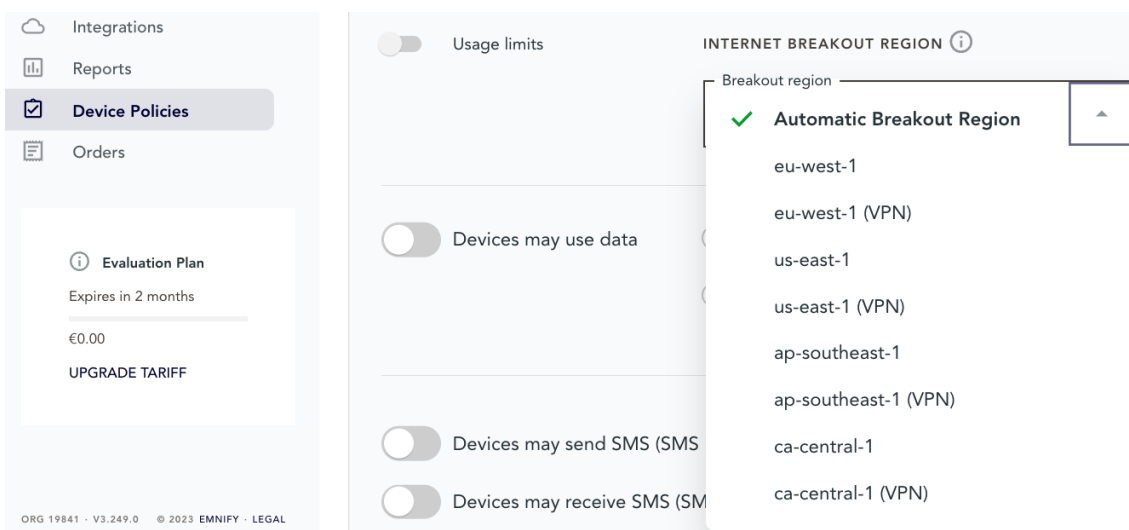


Figure 1: Selecting a **Breakout region** in the emnify Portal

4 emnify connectivity platform

emnify's connectivity platform allows you to manage and monitor the connectivity services provided by emnify's IoT eSIMs via its web-based portal and APIs. Additionally, the platform provides network security services to protect devices against misuse and integration with cloud services.

4.1 emnify Portal

The web-based [emnify Portal](https://portal.emnify.com)³ is the Operation Center for the IoT SuperNetwork.

The Portal allows Enterprise customers to monitor and manage all aspects of device communication – from viewing real-time volume and costs, managing the SIM lifecycle and defining service policies to troubleshooting connectivity issues and executing and managing integrations. The web portal provides a fully responsive design, supporting Desktop, Mobile phones and Tablets.

³The emnify Portal is available via <https://portal.emnify.com>

4.1.1 Dashboards

The Portal provides detailed reports about data and SMS traffic, costs for individual devices or the full organization, and in which networks the service has been used.

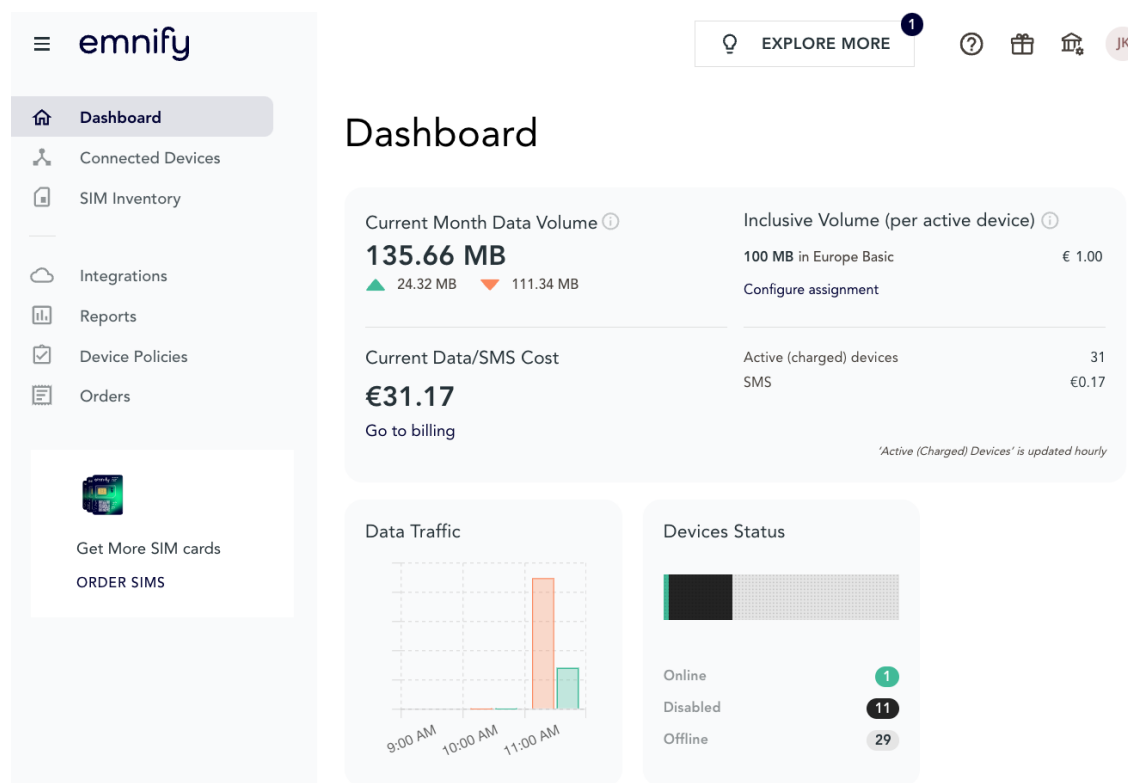


Figure 2: The default dashboard

4.1.2 Device Details

The portal provides an overview of all relevant information, such as real-time connection status, statistics, and detailed connectivity events which include location updates and PDP session creation logs for each device.

4.1.3 Device Policies

An Enterprise can define multiple service policies and coverage policies. When devices are assigned to their respective policies each policy functions as a device group. Configuring a device group's access, traffic limits, and data plan applies the settings to all devices in the group, which reduces the burden of device management for large deployments.

4.1.4 Location Information

Based on the location of the cell tower to which the device is connected, the emnify Portal displays a map indicating the device's location.

4.1.5 SIM orders

With the emnify Portal's self-service feature, an Enterprise can order emnify IoT eSIMs in any form factor with worldwide shipping destinations. When expedited shipping is chosen, SIM cards usually ship within the next business day.

4.1.6 SIM lifecycle management

When emnify IoT eSIM cards are shipped they are in an inactive state which means no fees are incurred. An Enterprise can either change an eSIM's status to active, which will start the billing process for that eSIM, or put it in factory test mode. In factory test mode, the device can be used without incurring any charges until a certain threshold of data usage is reached. Once the free data usage limit is reached, the eSIM automatically transitions to the active state. All subsequent data usage will be included in the current billing cycle. SIMs can be suspended any time in order to eliminate charges for future billing cycles.

4.1.7 User management

The emnify Portal provides the following user management functionality.

User roles

Each user can be assigned one of three different roles: Observer, User, or Admin.

- **Observer** can see all the information but cannot change configurations
- **User** can see and change configurations, except adding IP address ranges and adding/deleting users
- **Admin** can manage users and IP address ranges

Multi-Factor Authentication

The default login method is the username/password login. For increased security, each user can enable and disable the use of Multi-Factor Authentication (MFA). When chosen, an additional one-time passcode must be provided which can be retrieved using an authenticator app.

Single Sign-On

The emnify Portal supports signing on with a single ID which is also used for other SSO supporting applications. The following authentication providers are supported: Microsoft Azure, Google OIDC. Additional authentication providers can be offered on request.

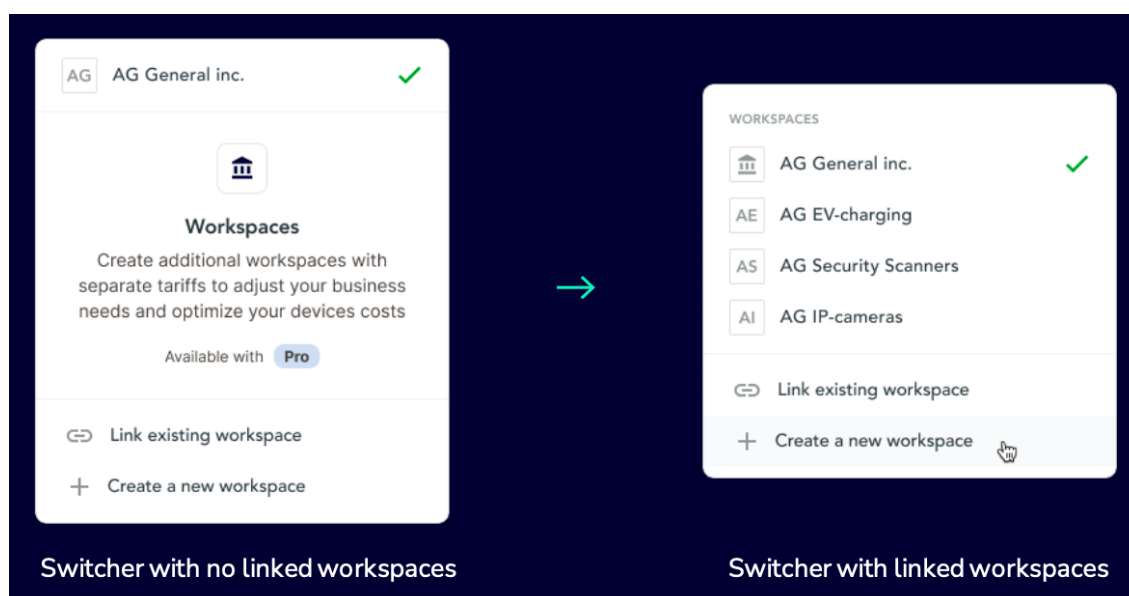


Figure 3: Workspaces

Workspaces

Workspaces is available for PRO package Enterprises. It is well-suited for Enterprises with complex business structures or those with a diverse set of products and services.

With the Workspaces service enabled, Enterprises can create multiple workspaces that are linked to their organization. Workspaces might be created based on markets (different countries/currencies), individual product lines /service types, or business units, e.g., subsidiaries. Each workspace functions as an independent entity that can be independently managed, or if linked, be centrally managed while being separately billed and inaccessible to regular users from other linked workspaces.

4.2 emnify APIs

4.2.1 REST API

All communication management capabilities available in the emnify Portal are exposed via a REST API. One typical use case for integrating the REST API is synchronizing the SIM activation and deactivation with the lifecycle of devices in the field. Another use case is enabling end-customers to see which network is in use and allow them to block specific networks.

The [emnify REST API](#)⁴ is based on the OpenAPI Specification OAS3.

⁴See the emnify REST API documentation: <https://cdn.emnify.net/api/doc/index.html>

4.2.2 GraphQL

GraphQL is a query language that enables you to define API call responses to match your use case and technical needs.

While the REST API returns the entire parameter set for a specific API endpoint, GraphQL returns only the parameters needed with a single request, even when the REST API would require requests to multiple endpoints to deliver the same results. Using the GraphQL API can speed up response times significantly. It also ensures predictable results when the API evolves with additional parameters in the future.

4.2.3 Data Streamer

The emnify platform provides a real-time event-based feed for ingestion into cloud services, business intelligence applications, and billing platforms. Enterprise customers can get real-time usage and cost records, detailed signaling, as well as policy events and alerts. This connectivity data provides a comprehensive view of an Enterprise's devices, network, and application data.

4.2.4 SDK

The emnify software development kits (SDKs) allow developers to manage their IoT devices using an intuitive set of APIs, including SIM state management and device connectivity operations. emnify SDKs are Open Source and currently available for Java and Python. For other languages, developers can use the REST API and GraphQL for creating custom applications.

4.2.5 No-Code

[Zapier](https://zapier.com)⁵ is a service that allows you to connect more than 4,000 applications – including emnify – to automate workflows without needing any software development skills. With the available integrations you can automate tasks based on triggers. All Data Streamer events are available as triggers. For instance, a specific event might be defined as a trigger for sending an SMS. Another type of event might be chosen as the trigger for either activating or deactivating a SIM card.

4.2.6 Events

The emnify system generates several types of events. These events allow you to track notable system occurrences based on behavior. Events are often used as triggers for custom business processes, for monitoring, and as input for custom billing systems. They provide information about lifecycle transitions and configuration changes.

⁵Zapier: <https://zapier.com>

5 Communication services

5.1 Data

5.1.1 Public internet breakout

An internet breakout is where data passes from a private network to the public internet. For cellular networks, the internet breakout is the home operator's central location – the one that sold the SIM card.

The default data service on the emnify IoT SuperNetwork uses a public internet breakout which means devices can connect to services using public IPs. However, a Carrier-Grade NAT protects devices by making them inaccessible from the public internet. Whenever a device opens a data session, it is assigned a temporary public IP address that the destination uses for responding to the device. Consequently, public internet breakout IP addresses can change between data sessions.

5.1.2 Virtual Private Network

Private APN

In legacy telecommunications infrastructure, devices need to provide a private Access Point Name (APN) to be assigned a static IP address for connecting to a secure virtual private network (VPN) on which it can communicate with the application server.

The emnify IoT SuperNetwork doesn't require private APNs for connecting to a secure VPN. Devices can use the same standard "em" APN for both regular or secure VPN connectivity. Optionally, emnify offers customized subdomain APN names to reflect Enterprise branding.

Private static IP

Every device using an emnify IoT eSIM receives a private static IP address from an IP address range allocated solely to that specific organization and never shared. By definition, private static IP addresses are inaccessible from the public internet. However, the organization can use OpenVPN or emnify Cloud Connect to remotely access its devices on the virtual private network (VPN) or to send data downstream to them.

OpenVPN

emnify's communication platform hosts an OpenVPN service that allows you to establish a private network between a device and any remote client location. The remote client can be on the application server or any machine that wants to access the device remotely (such as operational staff).

Your IoT device doesn't need a private APN, OpenVPN software, or dynamic DNS resolution to use the OpenVPN service. Through the emnify IoT eSIM, each device will have a static private IP address that you can use to identify and address the device.

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

Cloud Connect

The data traffic of regular SIM cards is secured within the mobile network but traverses the public internet between the mobile network and the application. With this network topology, the device and application are not only susceptible to attacks but it also makes it extremely difficult to establish remote device sessions.

emnify's Cloud Connect offers two distinct solutions to overcome these challenges:

- Amazon AWS Transit Gateway
- Internet Protocol Security (IPsec) VPN for other cloud providers like Microsoft Azure, Google Cloud, etc., or for on-premises applications

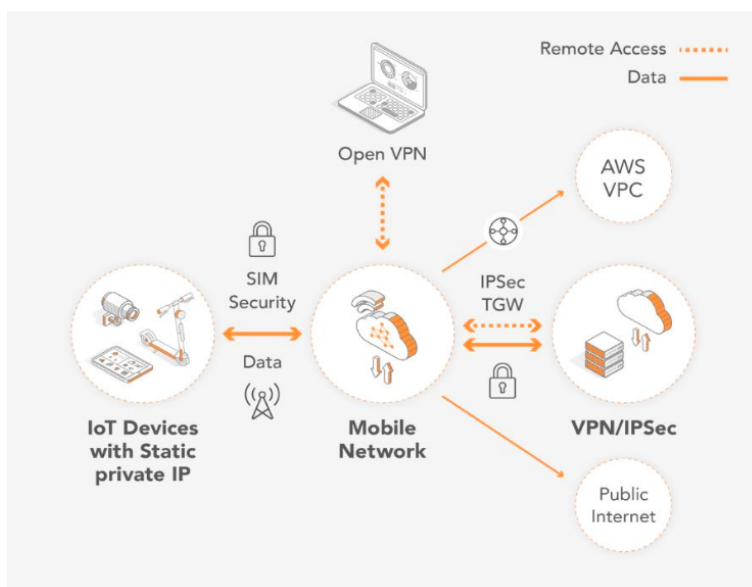


Figure 4: VPN options and public breakout

Amazon AWS Transit Gateway can be used by Enterprise customers who have their infrastructure on Amazon Web Services. AWS Transit Gateway provides a secure channel from the emnify AWS VPC to the Enterprise's VPC. Data stays within AWS networks and does not require any public internet breakout to connect devices to the application in AWS.

The **IPsec** VPN solution provides a channel between an Enterprise's devices and their application infrastructure on Microsoft Azure, Google Cloud, or on-premises servers, for secure data exchange and remote access. The IPsec VPN connection is provided through a managed AWS service (AWS Transit Gateway with VPN gateway) using two redundant VPN tunnels as the standard setup to ensure high availability of the IPsec

VPN connection. Static and dynamic VPNs using BGP are supported. The IPsec VPN connection can be established via the emnify Portal or REST API within a matter of minutes.

5.1.3 Inter-device communication

Devices using the emnify IoT eSIM are connected to the emnify IoT SuperNetwork. As an optional service, devices registered within the same account can communicate with each other using their private static IP addresses. The inter-device communication service is possible for devices within the same group and IP address range without the need of an overlay network over the public Internet. For information about this service, please [contact us](#)⁶.

5.1.4 Regional breakout

With traditional operator SIM cards device data is always routed back to the country of the operator, even when it entails routing between continents. By definition, "home routing" makes the deployment of a *distributed* IoT solution impossible because the operator network already centralizes the traffic.

The emnify IoT SuperNetwork supports building a distributed IoT application service based on regional breakouts. These breakouts are available in major Amazon Web Services (AWS) regions:

- US East (N. Virginia) us-east-1
- Canada (Central) ca-central-1
- Asia Pacific (Singapore) ap-southeast-1
- Europe (Ireland) eu-west-1

In the default dynamic configuration, data is sent to the region closest to the device. Or, the Enterprise can manually select a region that a specific group of devices will have their data sent to.

The public internet breakout and VPN / Cloud Connect service are available in each region. The use of regional breakouts allows Enterprises to keep data local to their devices, ensuring not only lower latency and packet loss, but also to comply with end customer data processing agreements or local regulations.

5.2 SMS

The emnify platform includes a Short Message Servicing Center (SMSC) that manages all SMS communication and interfaces.

⁶Contact emnify via <https://www.emnify.com/talk-to-us> or email: info@emnify.com

SMS messages can play a pivotal role in remote IoT device management and automation. Since SMS works without a data connection, it's a reliable way to communicate with remote IoT devices.

By designing devices to accept SMS parameters, most manufacturers have eased the burden of configuring a fleet of devices, both for the initial connectivity configuration as well as for post-deployment configuration changes.

By leveraging SMS for specific tasks that would otherwise require power-hungry data connections, devices can operate more efficiently by conserving battery power.

With SMS in place for your remote configuration, you can also use it to trigger additional actions on a device. For example, if you wanted to perform an update, you could use SMS to trigger a firmware OTA update.

5.2.1 SMS MO/MT

The emnify platform supports:

- SMS Mobile Originating (MO): messages sent / originating from a device
- SMS Mobile Terminating (MT): messages received / terminating at a device

Mobile Terminating SMS can be sent from another device (P2P SMS), via the emnify Portal or via the REST API (see A2P SMS).

Mobile Originated SMS are visible in the emnify Portal or via the REST API (see A2P SMS)

5.2.2 P2P SMS

P2P stands for Peer-to-Peer messaging. For example, an SMS sent from a phone to a device with an emnify SIM or vice versa would be P2P SMS.

The emnify IoT SuperNetwork supports P2P SMS over an international phone number (MSISDN) that is assigned to each SIM.

emnify allows MO and MT SMS from external SMS devices. Devices can be reached over the assigned MSISDN number from any regular mobile phone.

5.2.3 A2P SMS

Application-to-Person (A2P) Short Message Service (SMS) refers to text messages sent from a software program to person or a SMS sent from a person to an application. Messages from an application are often automated and trigger based on a set of rules or conditions. Messages to an application involve a request or command.

The emnify IoT SuperNetwork also supports Application-2-Peer (A2P) SMS. This means SMS messages can be sent or received via an API or the emnify Portal.

The emnify platform supports the following methods to send and receive A2P SMS: SMPP, emnify Portal, REST API, and Zapier.

In the Internet of Things (IoT), end users and manufacturers rely on A2P SMS to do things like remotely set the Access Point Name (APN), reconfigure devices, "wake up" a device to go online, or send small measurement data to the application.

SMPP

The emnify platform supports the Short Message Peer-to-Peer protocol v3.4. An external application – also referred to as an External Short Message Entity (ESME) – can connect to the emnify SMS center and then send and receive SMS directly to/from the device. Most GPS platforms that support SMS offer SMPP as an integration option. Any communication then goes directly over the emnify platform via A2P SMS avoids the more costly P2P SMS over-the-top solutions.

SMS via the emnify REST API

Besides the SMPP interface, the emnify platform also provides a simple to use REST API that supports sending and receiving SMS messages programmatically.

Mobile terminating SMS:

For SMS MT the source address can be freely specified. Additionally, multiple SMS messages can be concatenated. There is also support for different data coding schemes.

Mobile originated SMS:

SMS MO can be retrieved by an application via an SMS webhook that forwards every SMS sent from the device. The webhook provides SMS MO sent by the device and SMS MT delivery receipts.

SMS console in the emnify Portal

The emnify Portal also provides an SMS console which allows an SMS to be sent to the device with a configurable source address. In addition, the UI lists all SMSs that are received and sent by the device.

5.2.4 SMS short codes

The emnify platform supports SMS Short codes for automating processes. In a consumer world, SMS short codes are used for sending marketing messages, or for example to top off a data plan via SMS. On the emnify platform, SMS short codes are supported with up to 7 digits or alphanumeric addresses from which the application or IoT device can create a specific response, independent of the actual SMS payload.

6 Network security services

Given the globally distributed nature of the devices, smaller footprints and lack of resources, it can get difficult to individually secure IoT devices.

emnify uses a SASE approach to simplify securing devices – using several services specifically to protect customer data, filtering malicious content and preventing unauthorized access.

6.1 SASE overview

Secure Access Service Edge (SASE) introduces a new architecture where networking and security functions are bundled in a cloud-delivered service. You can apply the same security standards across all your devices independent of the location. Moreover, you can integrate security features in your solutions right from the beginning.

Some of the features that SASE for IoT architecture includes are as follows:

- Dynamic Data Routing with Software-Defined Wide Area Network (SD-WAN) emnify utilizes a SD-WAN to route data to the closest cloud region using the Regional Breakout concept. In this way, latency and data stability is improved, and the end customer can be sure that data does not leave the continent and jurisdiction.
- Cloud Access Security Broker (CASB) emnify allows centrally defining policies for the devices such as: networks that can be accessed, allowed IP addresses through which authorized users can remotely access devices. All configuration is done in the central platform and applied wherever the device is.

6.2 Virtual Private Network options

A Virtual Private Network (VPN) enables encrypted, targeted transmission of data over public networks such as the internet. It establishes protected and self-contained networks with various devices. A common use case is the connection of home offices or mobile employees.

6.2.1 Private static IP

Assigning a device a private static IP address prevents computers or other devices outside the local network from directly connecting to it.

6.2.2 Cloud Connect – secure data transport

AWS Transit Gateway

Connect devices securely to AWS VPC without using public Internet. Some of the features and benefits are:

- Devices and the application infrastructure reside within the same private network.
- Remotely access devices from AWS infrastructure via telnet / SSH.
- Device data does not traverse public internet.
- VPC / EC2 instances do not need public IP addresses.
- Fully scalable and managed AWS service.

IPsec

If your application is not on AWS but on any other cloud services or on-premise, you can utilize Cloud Connect for establishing an IPsec VPN connection.

With emnify you can set up an IPsec tunnel to securely transfer your data into your application server.

6.2.3 OpenVPN – remote access

OpenVPN is provided as a self-service for enterprise customers to get remote access to their devices from any OpenVPN client. Customer VPN clients are authenticated with the credentials and application tokens of their emnify account to get remote access to devices. OpenVPN establishes a single tunnel to the VPN gateways which are delivered in active-passive redundancy with automatic failover in case one VPN gateway becomes unavailable.

6.3 Custom DNS

When a device establishes a connection, it uses a Domain Name Service (DNS) server 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 an IP address like `192.0.2.1`.

Cellular providers typically provide a DNS service. By default, emnify routes all DNS queries over Google's public DNS `8.8.8.8`.

For some devices and modules, it is possible to configure the DNS service. For example, Quectel uses the `AT+QIDNSCFG` command, SIMcom `AT+CDNSCFG` command. This is useful to be able to use your own or private DNS servers to secure and have better control over the solution.

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 emnify Portal » **Device Policies** » **New service policy** » **More options**

Utilizing a private DNS server which is not reachable via the public internet requires to set up a private network with the machine or a network where the private DNS server is located. This can be done using Cloud Connect either with Amazon Transit Gateway or IPsec. A tutorial on how to set up a DNS firewall based on a private DNS using Amazon Route 53 is available [here](#).

6.4 IMEI lock

For device manufacturers, SIM card theft is an issue because pluggable SIM cards can be removed from a device and then used to gain free internet access. The IMEI lock feature prevents the use of SIM card in any other device by bounding the SIM to an IMEI. The IMEI is a unique device identifier. When the automatic IMEI lock is configured, the emnify platform will bind the SIM cards to the first device that establishes a data connection. All future device connections will only be allowed from this device.

6.5 Centralized policies

Within the emnify platform, there is a separation between SIM card and the device, also referred to as "endpoint". This allows you to configure policies on the device level rather than SIM level. The device policies can be applied on a device group as well as at an individual level.

6.5.1 Service policies

Service policies define which services are available for a group of devices. These policies include:

- Available radio access types (2G, 3G, 4G, NB-IoT)
- Monthly data and SMS limit
- SMS API configuration
- Custom DNS
- Breakout Region
- Available SMS service (MO/MT/P2P/A2P)
- Activation of Quota and Prepaid Management

6.5.2 Coverage policies

Coverage policies define which tariff and network coverage is available for a group of devices. This enables you to optimize the tariff based on the intended coverage.

The coverage policies include:

- The applied tariff for the group of devices
- The available networks organized in rate zones

7 Support

emnify is dedicated to your success with our service. We provide you with a choice of different plans, a globally-based customer success team, and support with global roaming to ensure that you have connectivity wherever you need it.

7.1 Service Options

emnify offers a variety of support plans designed to ensure that your devices operate reliably in our network. The **Standard** support plan is included for all customers at no additional cost. It is the default service plan when registering through our website using the emnify Portal. For a detailed description of the standard services, please refer to our Terms of Service.

The **Business** and **Enterprise** plans offer premium customer service and can be bundled with your emnify subscription. They are designed to reduce operational costs by detecting issues before they disrupt your business operations and by resolving incidents faster.

Feature	Standard	Business	Enterprise
Operating hours	Mon-Fri 09:00-18:00 CET	24x7x365	24x7x365
Method of contact	Tickets must be opened via webform. Replies via email are possible.	Tickets must be opened via webform. Replies via email are possible.	Webform, email, and phone
Help Center & Knowledge Base	Yes	Yes	Yes
Pre-scheduled event support	Not included	Yes	Yes
Dedicated Support Agent	Not included	Not included	Yes (EU-CET, US-EST or US-PST business hours)
Trace requests	–	1 simultaneous trace Max 1 request/day Max duration 24 hours/trace	3 simultaneous traces Max 1 request/day Max duration 24 hours/trace
Guaranteed response times: Critical incident Operational incident General issue / question	7 business days	3 hours, 24x7x365 6 business hours 9 business hours	1 hour, 24x7x365 3 hours, 24x7x365 6 business hours
Target time to restore service: Critical incident Operational incident	–	12 hours 10 business days	4 hours 4 business days
SLO	Mobile Core: 98.5% Internet Breakout/VPN: 98.5% API/GUI: 98.5%	Mobile Core: 99.5% Internet Breakout/VPN: 99.5% API/GUI: 99.5%	Mobile Core: 99.95% Internet Breakout/VPN: 99.9% API/GUI: 99.5%
Root cause analysis	Yes (Critical incidents)	Yes (Critical incidents)	Yes (Critical and operational incidents)
Length of service	Monthly (automatic renewal)	Monthly (automatic renewal)	Minimum 12 months

7.2 Incident Management

emnify's network operation center (NOC) monitors the health of all cellular networks and services that emnify offers 24x7. The NOC proactively identifies any degradation of service. In case of an incident, it starts the incident management process that alerts a team of on-call engineers to start an investigation.

When an incident is triggered due to network-related events, the responding team will diagnose the fault and escalate the incident to emnify's carrier and roaming partners if necessary. Optionally, any network causing a service disruption will be blocked so that devices can connect to alternate networks.

During an incident, emnify updates the Status page for all services in order keep customers informed in real time about the status of the incident and its impact.

For critical and operational incidents, emnify conducts a root cause analysis (RCA) and issues a postmortem that provides details about the incident, which changes have been applied, and which measures are planned to guard against future incidents.

The incident management process is reviewed annually and certified by a third party as part of emnify's SOC2 audit.

7.3 Roaming

Unlike typical mobile network operators (MNOs), emnify will also provide 24/7 support when your device is in roaming scenarios. The emnify network operation center (NOC) has visibility of all networks in the world and can detect network service degradation. emnify will also investigate and follow up even when only your fleet of devices is affected.

Based on the direct and IoT/M2M specific roaming relationships with network operators, emnify has service-level agreements (SLAs) to resolve critical and operational incidents within specific timelines.

So you will never need to worry about roaming when your IoT devices are moved to another location, even if it is to another country or continent. Support for the global deployment of IoT devices is a key feature of emnify's Global IoT Network.

7.4 Customer Success Manager

In addition to emnify's 24x7 support and network operation center (NOC), each customer has access to a Customer Success Manager (CSM). CSMs comprise a globally distributed team with local working hours. They are fluent in emnify's main supported languages: English, Spanish, Italian, French, and German. The CSM team proactively engages with their customers to help them obtain value from the product and guide them through their journey. They also conduct onboardings to get their customers acquainted with the platform and help with setting up integrations.