
Unleash the power of Apple devices on your Private 5G LAN
Eric Zelenka
Senior Consulting Engineer for 5G & Cellular, Apple
Puneet Shetty
VP of Product, Celona
celona
Celona Propriety & confidential 2023 ©

Eric Zelenka

Senior Consulting Engineer
5G & Cellular

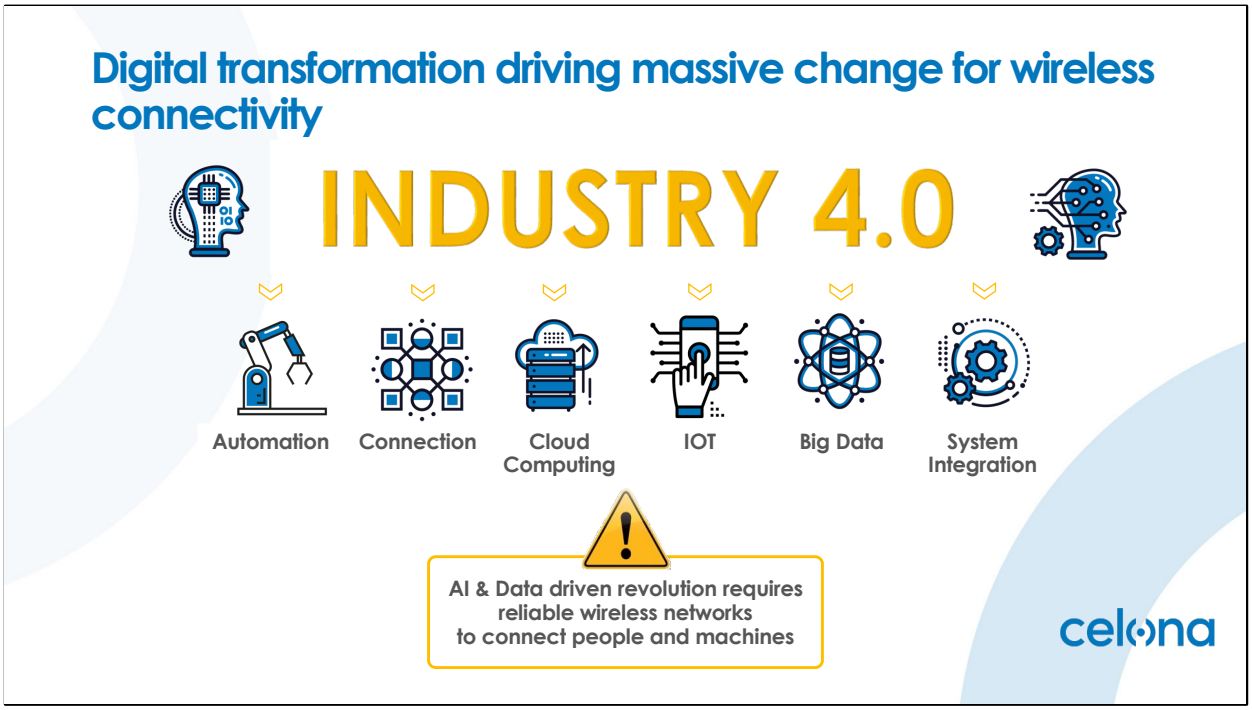
Apple

Puneet Shetty

Vice President of
Product Management

Celona

celona



- Automating operations
- Uplink-heavy applications
- Low-latency protocols
- End-end security
- Seamless mobility
- Predictable performance
- Pervasive coverage

You may believe that with all the advancement over the years, that Wi-Fi has solved most of the issues related to reliability. In your typical carpeted office environment that is mostly true. Wi-Fi has better range and certainly higher speeds than it used to.

So Wi-Fi is actually pretty awesome at home and in the carpeted office environment. But in those environments the client devices are typically stationary and the Wi-Fi access points are mostly separated from each other by the walls between rooms. In this stable environment it is possible to design and implement a mostly reliable wireless network.

But everyone is familiar with unreliable Wi-Fi. So why does this unreliability happen? It happens for a number of reasons:

The spectrum used by Wi-Fi is unlicensed – which means anyone and everyone can use it – and does, and not just for Wi-Fi. Even within your own office environment there are often multiple devices trying to transmit and receive data on the same spectrum your wifi is trying to use
Wi-Fi access points interfere with each other – architecturally, each AP can transmit and receive data at the same time as all the other access points – when they do this they create interference for other APs operating on the same or nearby frequencies. This is especially bad in environments where lots of APs have line of sight to each other which is why operation outdoors and in large open indoor spaces is typically so poor
Wi-Fi was not designed for mobility – Wi-Fi assumes the client is not mobile and not

roaming from one AP to another. Whilst techniques for improving Wi-Fi roaming have been worked on over the years, the fundamental issue is that with Wi-Fi, the client device makes the decision when to drop from one AP and request connection to another. When it does that the new AP has to accept the connection and the client may need to reauthenticate through that AP to whatever service it was connected to. Very often the result is a dropped connection.
Wi-Fi is a first-come, first-served, contention-based system – the more devices that are connected to an access point, the higher the levels of contention which means the higher amount of time and capacity is wasted determining which device will connect next

Wi-Fi performance issues mostly manifest themselves in "large open spaces"….be they indoors or outdoors as shown in the slide pictures. Most customers who work at the operational level are aware of the reliability issues they experience with their "large open space" locations. Show me a warehouse and I can show you a place where the Wi-Fi does not work very well. Show me an outdoor facility and I will show you a place where the Wi-Fi barely works at all.

By contrast:

Cellular was designed with mobility in mind - ensuring that as devices roam from one cellular access point to another – even at high speeds – connections are not dropped.
Cellular networks use licensed spectrum – even for private cellular, a local grant is provided to use spectrum which nothing else nearby is using ensuring no outside interference
Cellular APs do not interfere with each other – as the right to transmission is co-ordinated by the network core and not the end devices, resulting in an optimal RF environment
Cellular devices do not contend with each other for access – as the core determines when a user can transmit, there is optimal usage of the available bandwidth
As a result, Cellular will reliably cover much larger areas than Wi-Fi – upto 5x indoor and 20x or even more outdoors

In addition, because Wi-Fi is a contention based system where the network attempts to cope with end device demands for access, QoS can only be implemented on a best effort basis. There are no guarantees. By contrast, because cellular is controlled from the core, explicit levels of QoS can be implemented and monitored to ensure application SLAs are being met.

One last and very important point – when Wi-Fi gets down to lower bandwidth speeds, because the network has no control over latency and cannot guarantee any minimum amounts of capacity at any instant, the connection will typically drop even though there seems to be some signal. By contrast, cellular can hold on to a connection for much longer because whilst the capacity may be low, the core can guarantee capacity and latency, ensuring the connection is maintained.

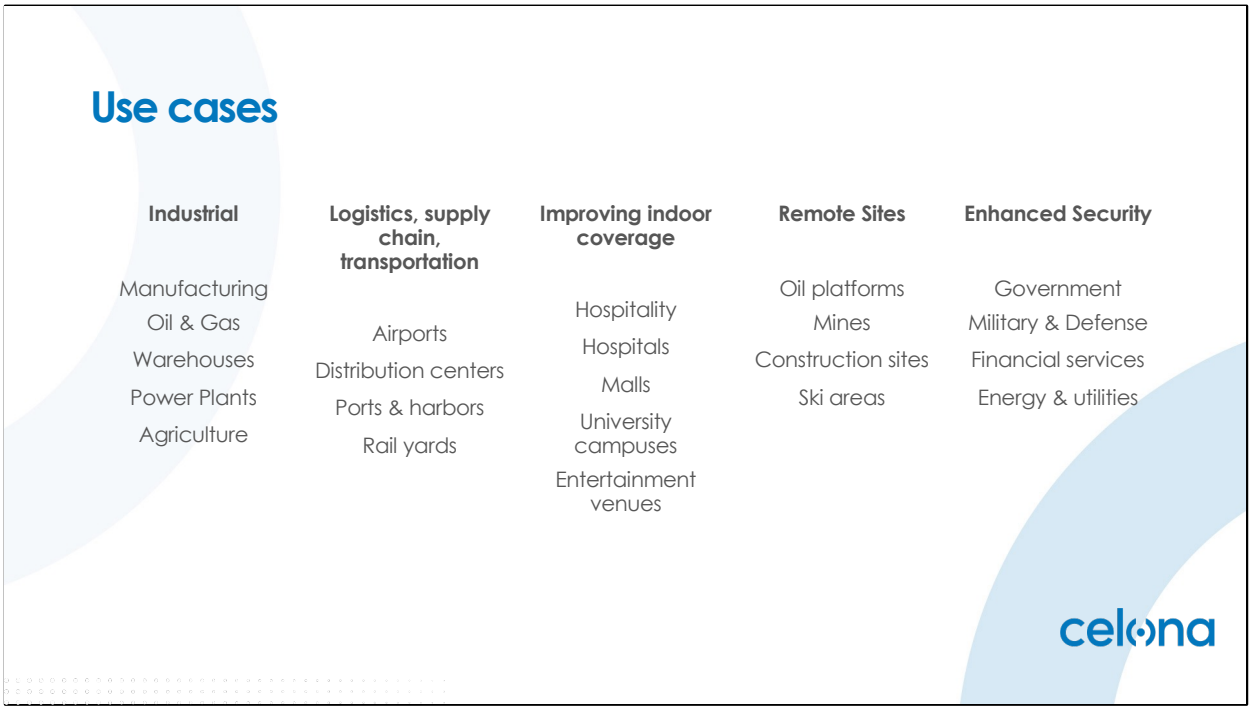
Device Ecosystem: The Pivotal Challenge & Prime Opportunity for Private 5G

celona

iOS and iPadOS 17

Adding support for PCN

celona



We live in an age where technology and access to information really redefine every aspect of our lives from how we live to how we work. And Apple is truly at the forefront of this mobile transformation.

With the iPhone and iPad, Apple has transformed how enterprises work, enabling employees to be more productive and capable than ever before.

Earlier this year, Apple announced support for private cellular networks in iOS and iPad OS 17.

So, enterprises can now take advantage of this 5G technology to build a workplace that's more connected, secure, reliable, and designed for your individual business needs.

With support for private 5G, Apple is truly revolutionizing how enterprises operate and how work is done.

Exciting thing is that 5G is here. You can take advantage of this technology.

With iPhone and iPad support for private 5G, this technology is now ready for widespread deployment in your enterprise. Your business can now take advantage of this 5G technology to, again, have reliable high performance and in a secure wireless network, for your business.

So, let's consider a couple use case and deployment scenarios where private 5G is really an ideal wireless solution. Private 5G is well suited for industrial applications. That demand extensive wireless coverage, both indoor and outdoor.

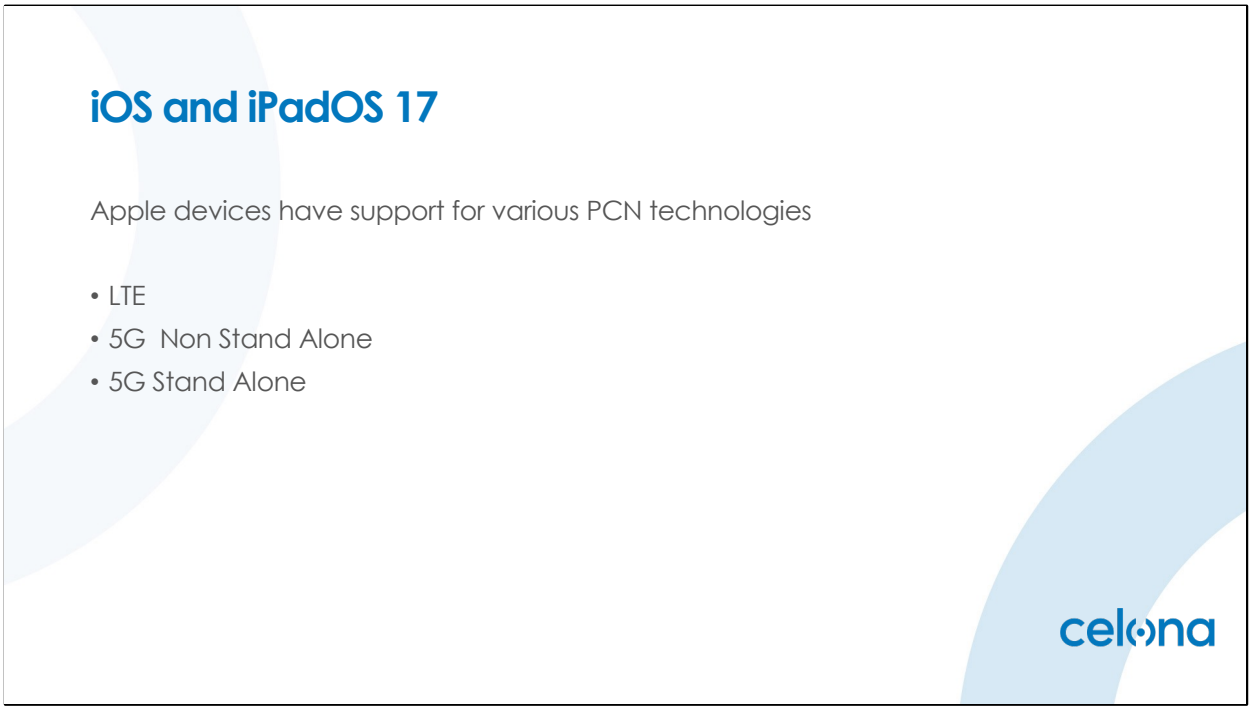
And unwavering network reliability as downtime is simply not an option in these mission critical operations. We look at industries such as manufacturing and oil and

gas, warehousing, power plants. They all require low latency communications. They're all analyzing real time data from sensors and equipment, even personnel who are walking around with iPhones.

Private 5G is exceptionally well suited for logistics and transportation businesses, including airports, distribution centers, ports and rail yards. These businesses typically require, again, coverage both indoor and outdoor across a large and complex facilities. They also again re require those that reliable low latency communications so that it can-do real-time tracking and management of equipment, cargo, vehicles, and so forth.

The deployment of a private 5G network can also be used to solve a challenge many customers have which is poor indoor coverage from a nationwide carrier. Now this is particularly a challenge in hotels casinos, hospitals, university campuses, malls, entertainment venues.
Now think about it. Having excellent seller connectivity, both for voice and data is fundamental. And when people can't use their iPhones indoors to make a call or access data, it leads to all sorts of customer satisfaction issues.
how can a private 5G network improve a carrier's indoor coverage?
Well, the access points you deploy for your private 5G LAN They can serve as a neutral host, allowing you to share your information, your infrastructure with a nationwide carrier.
Your access points effectively vend cellular connectivity for both your private 5G network, as well as nationwide carrier. With your company's internet connection acting as the backhaul.
And the exciting thing is this neutral host technology works great. With iPhone and iPad.
Celona private 5G network is highly advantageous for remote sites. Such as oil platforms, mines, construction sites, even ski areas.
These remote sites are often outside the coverage of a nationwide carrier and may require wireless connectivity over large distances.
Satellite connectivity such as StarLink is actually commonly used for backhauling.
Private 5G networks offer enhanced security and control. Making them particularly suitable for various security conscious use cases, such as many governments, military, and defense applications.
But this also extends into financial services, energy, and utilities.
Utilizing SIM technology ensures only authenticated devices are connected to the network. And so, this can be u this is great because it reduces the risk of unauthorized access and data breaches.
And SIM technology enables encryption of data that's transmitted over the network. So, the information is safeguarded from interception and eavesdropping.
And since this private 5G network is your own infrastructure, which gives you access to your LAN, you can be sure that the data is remaining local. You're not sending data out over a carrier network or even, the public internet.
Now at Apple, we understand that robust wireless connectivity is essential for the operation of your business.
And that's why we've designed iPhone and iPad to support advanced wireless technologies, technologies such as 5G and WIFI.
And now with iOS and iPad OS seventeen, we've added support for private cellular networks.

Giving you more ways to keep your business connected.



iOS and iPad OS 17 support data only private cellular networks using a range of radio access technologies.
This includes 4G LTE, 5G non standalone, and 5G standalone.
So, this gives you the flexibility to deploy the right type of private cellular network for your specific business needs.

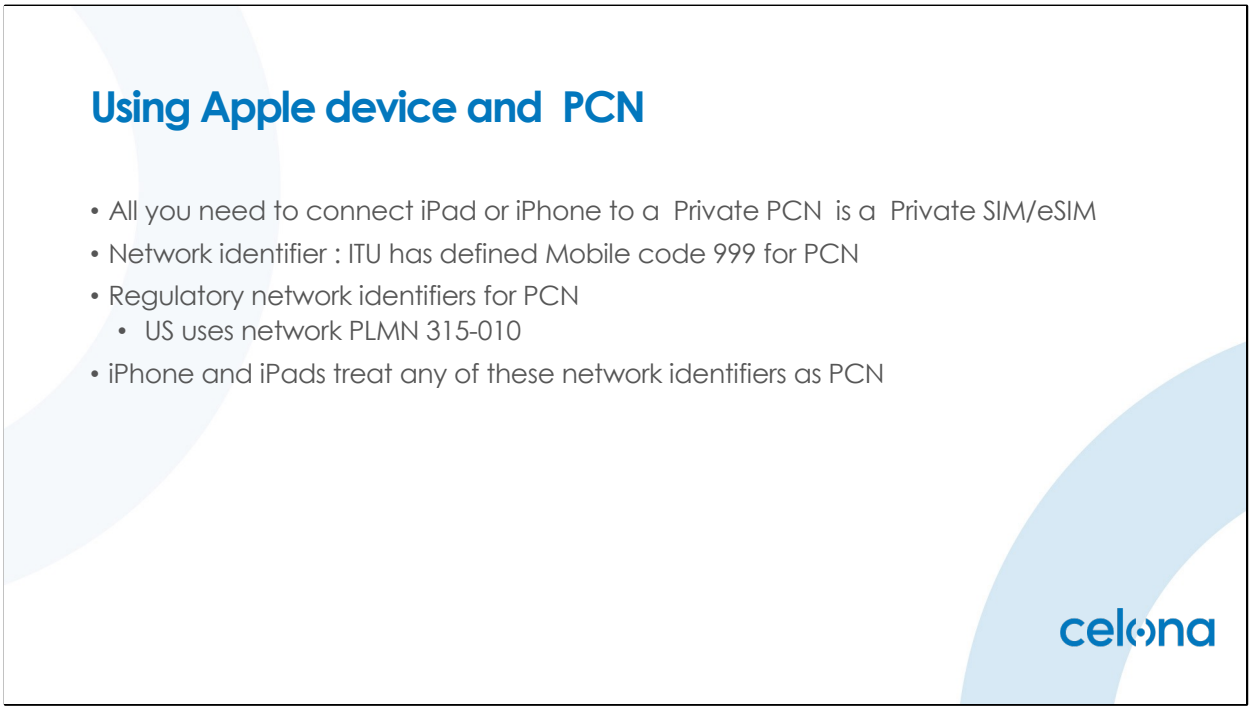
Apple device compatibility with private wireless

- iPhones and iPads support a whole range of Private wireless spectrums around the world including
  - b48 4G/USA
  - n48 5G/USA
  - n77 US/UK/Sweden/Norway
  - n78 ROW
  - n79 Japan
- Use link below to see which apple devices support which spectrum

https://www.apple.com/iphone/cellular/

celona

You also have the flexibility to use iPhone and iPad on a wide range of spectrum. This is a spectrum that's encompassing low band, mid band, and even high band frequencies.
So, there's a lot of different bands, that are commonly being deployed, throughout the world. But the good news here is that your iPhone and your iPad can support a wide range of cellular bands. Now this slide here is not meant to be an exhaustive list of which bands are supported in which countries, but more of an example of some of the more commonly deployed bands that we're seeing on private cellular networks.

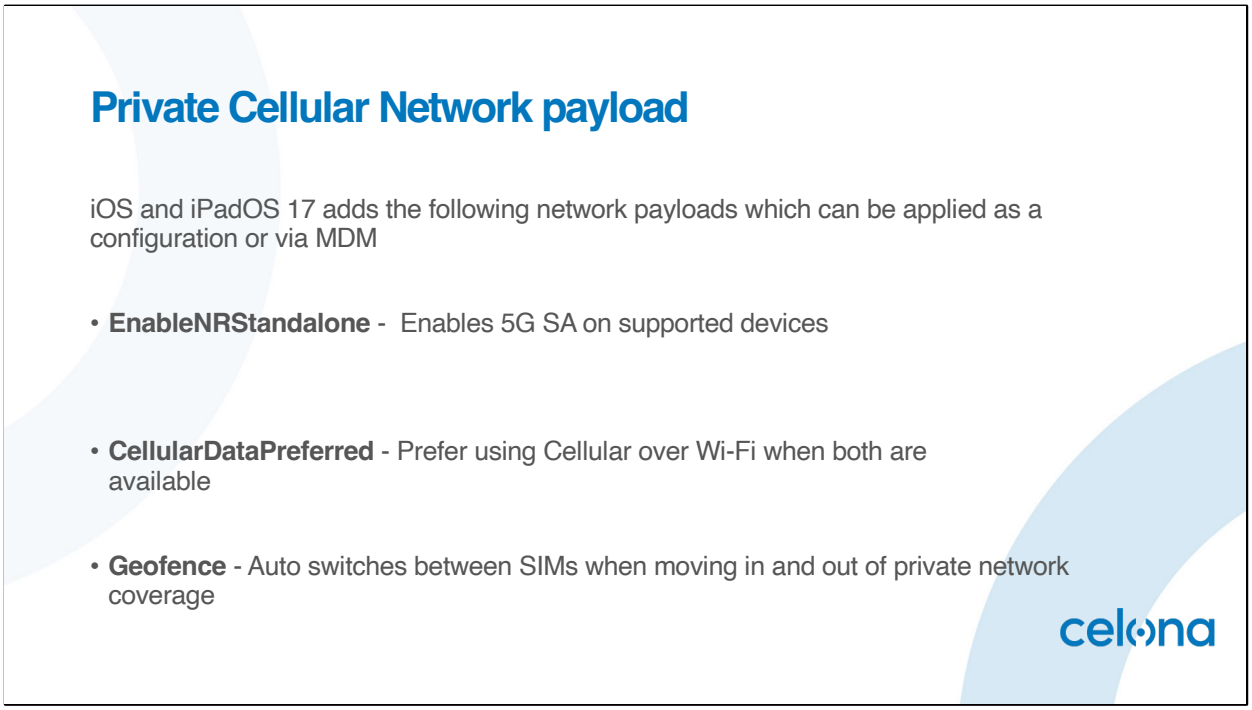


Now all that's needed to connect your iPhone or iPad to a private cellular network, is an e SIM or a physical SIM that's provisioned for your network. So once that SIM is installed, your iPhone or iPad will attach. And that's going to give you 5G access to your LAN. It it's that simple.

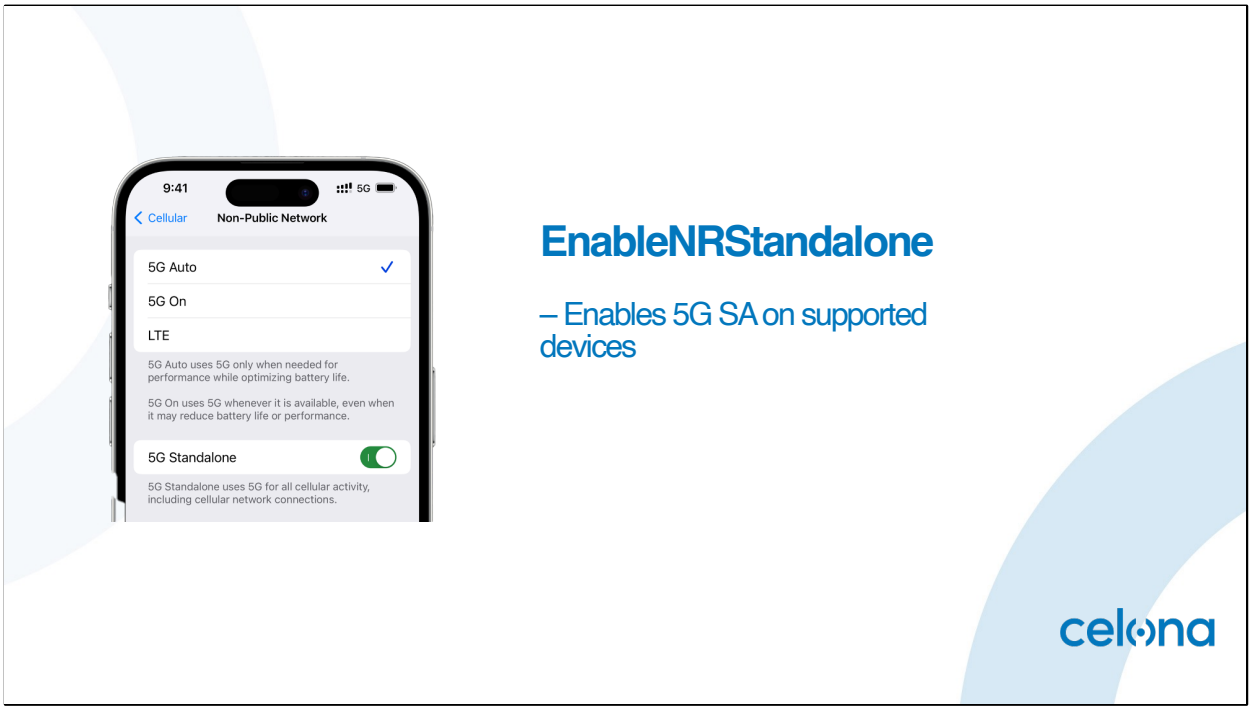
For your iPhone or iPad to take advantage of unique private cellular network features, you must use specific network identifiers. Now the international telecommunications union has the find mobile country code 999 as the standard that should be used for private cellular networks worldwide.

In some countries, though, such as the United States, Germany, and Sweden, there are regulatory network identifiers for private cellular networks.For example, the systems broadband radio service uses the network identifier 315-010

iPhone and iPad will treat any network which uses mobile country code nine or one of these regulatory network identifiers as a private cellular network, allowing your device to be configured to take advantage of some really unique capabilities.

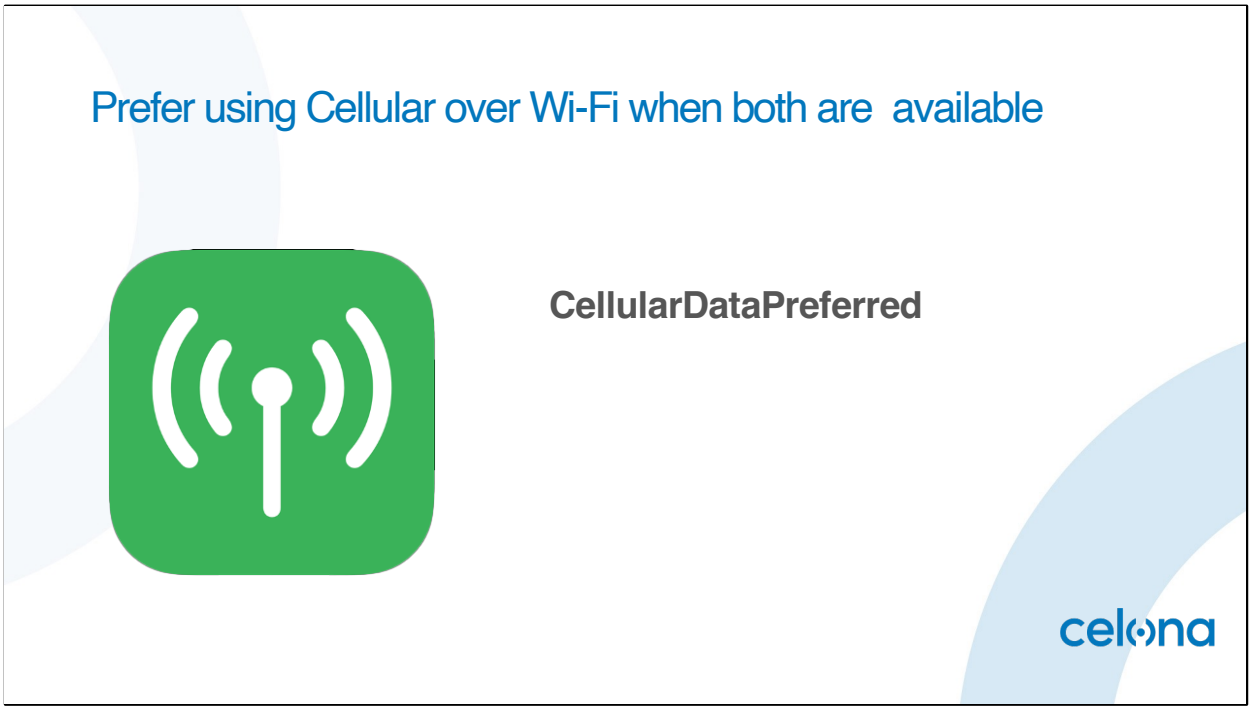


Now iOS and iPad OS support a robust device management architecture.
And we use this architecture streamlined the way businesses deploy, configure, and manage iPhone and iPad.
IOS and iPad OS 17 add support for a new private cellular network payload.
And there are three new management features which are available when using a private cellular network.
This payload can be deployed as a configuration profile or applied to devices using mobile device management.

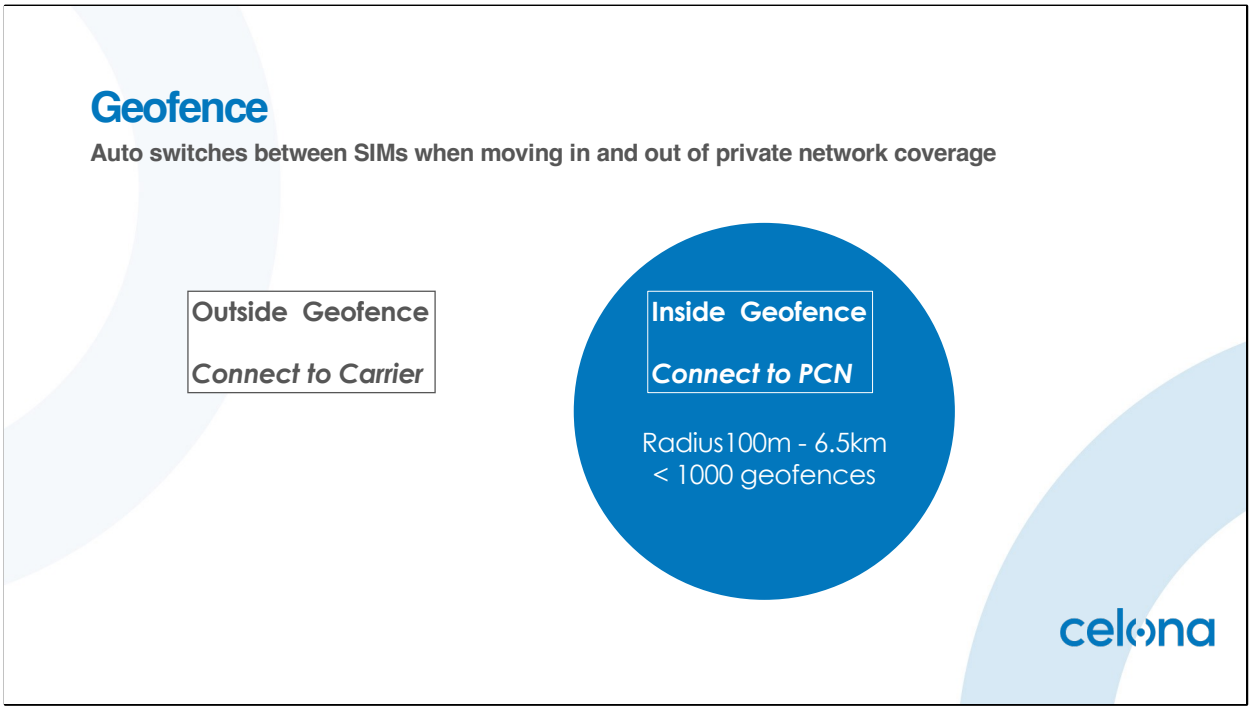


The first of these features is the ability to manage 5G stand alone. Now 5G stand alone is off by default. But users can go into their iPhone. They can, go into settings, they can tap on cellular, and they can manually turn that on.

But to eliminate this step and to tell your iPhone or iPad to always use 5G stand alone, you can configure a new enable and our stand alone key. In your private cellular network payload.



Another new feature available only when using a private cellular network is the ability to prefer cellular over WIFI.
So, with the new cellular data preferred key, your business with a private 5G or LTE network has the option to prefer using cellular over WIFI when both are available.
So, with the setting, your iPhone, your iPad, you can set it to prefer your private cellular network, and applications and data are going to go over that private cellular network. While still allowing WIFI for specific services such as airdrop or even Airplay.

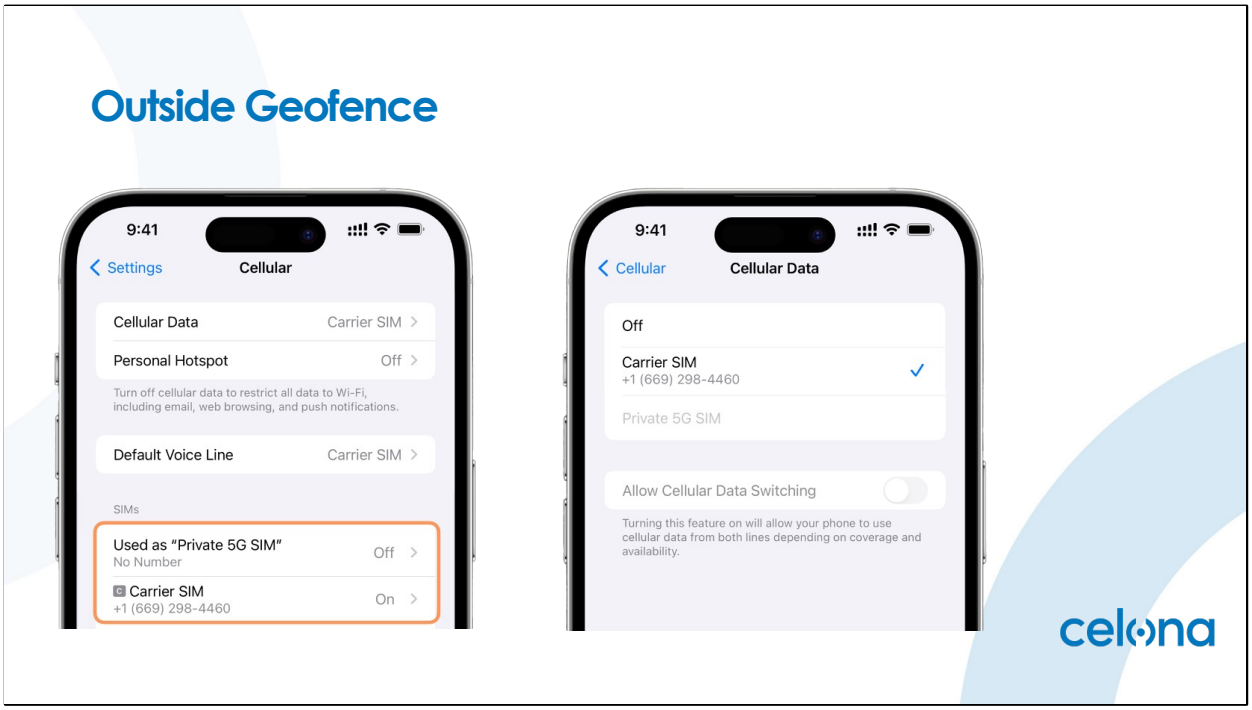


The third new feature available when using a private selling network is to use a geofence to automatically activate your private network SIM.

Now this feature is especially for iPhones when using a dual SIM, where you have one SIM which is your private cell for your private cellular network, and another SIM for a nationwide carrier.

So, by creating a geofence, your iPhone can seamlessly switch between a private network sim and a carrier sim. As you move in and out of the private network coverage.

iOS 17 supports up to one thousand geofences, with each with a radius ranging from one hundred meters to six and a half kilometers.



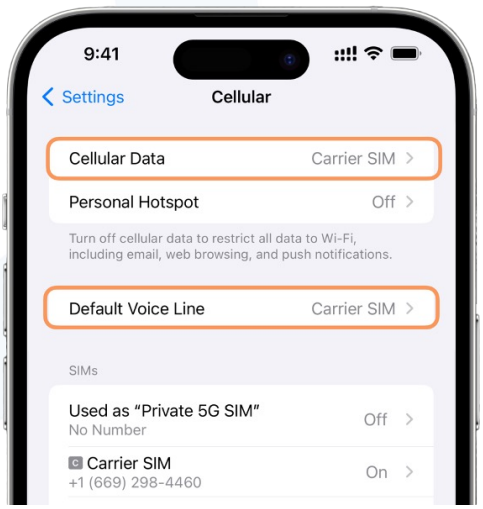
The first thing to notice is that your iPhone is configured and must be configured to use two sims. You're going to have two sims here, one for your private cellular network, and one for your nationwide carrier.

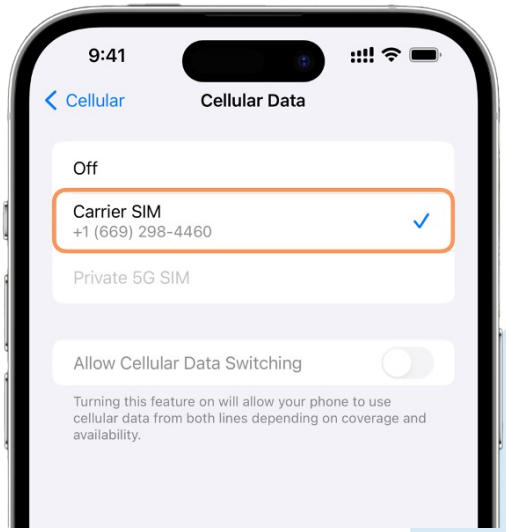
Now while outside the geofence, your private network sim is will be turned off.

Also notice that your nationwide carrier SIM will be used for cellular data invoice.

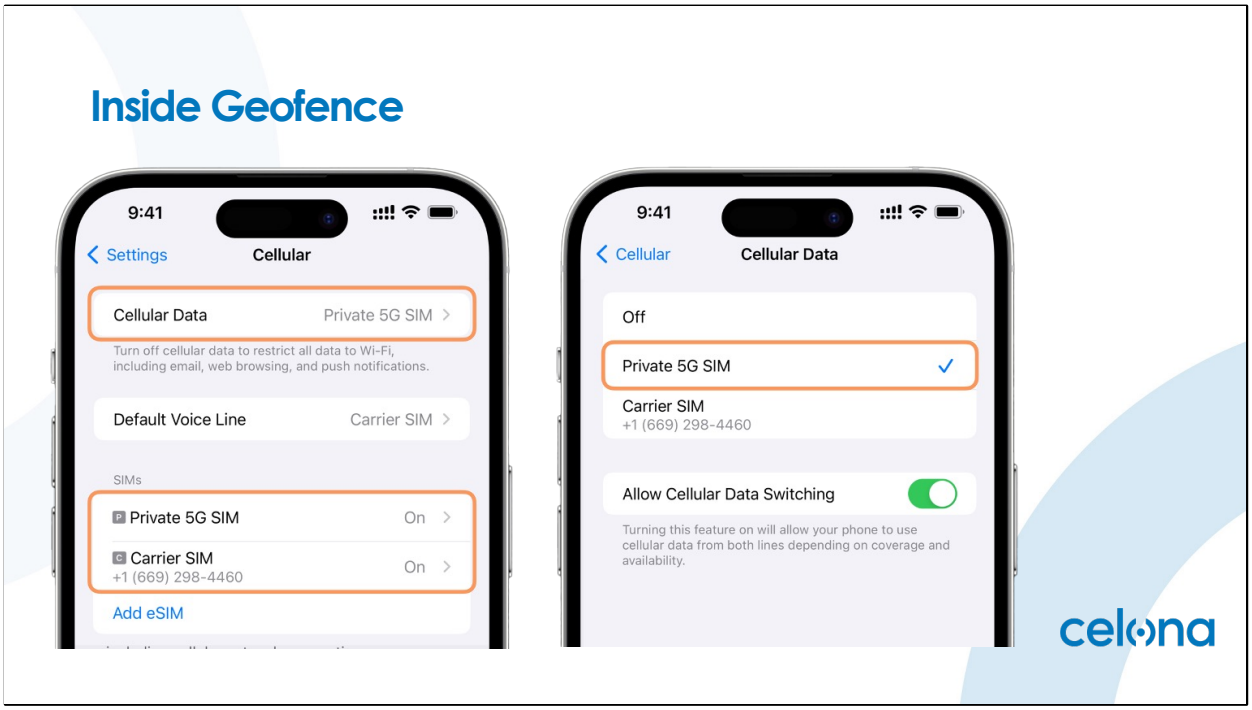
So, you're going to still be able to make phone calls and use your carrier network just like normal for all data while you're outside your private cellular network.

Outside Geofence





celona



When you go inside the private cellular network, you want to use that network for your cellular data.

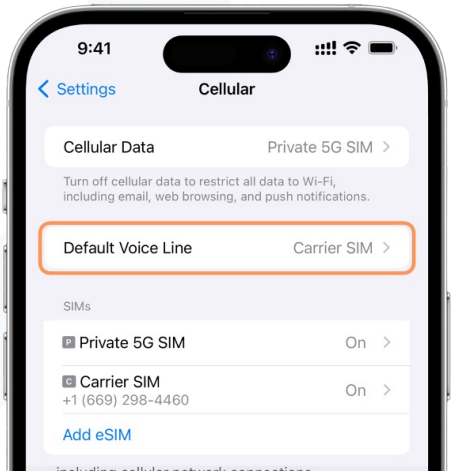
So, when you can by configuring that geofence, your iPhone is going to automatically turn on the private network SIM and set it to use for cellular data.

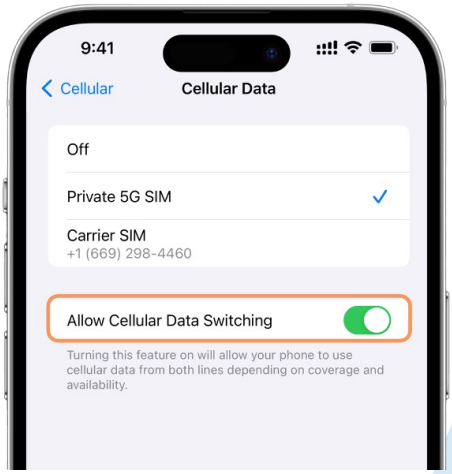
The carrier SIM remains active, and this allows your iPhone to again continue to make calls while you're connected, even to that private cellular network.

Now if there are areas of poor coverage inside the geofence, you can turn on allow cellular data switching.

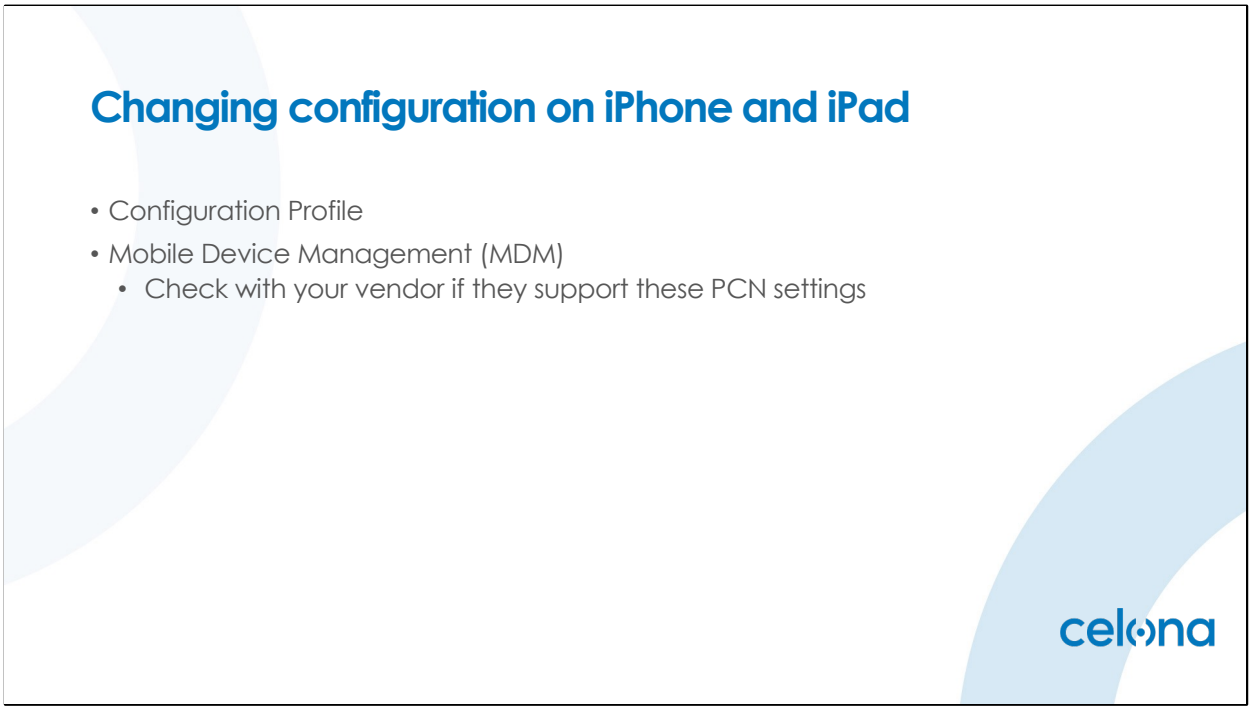
This will enable your carrier sim to be used for cellular data. When the signal quality of your private cellular network is poor.

Inside Geofence





celona

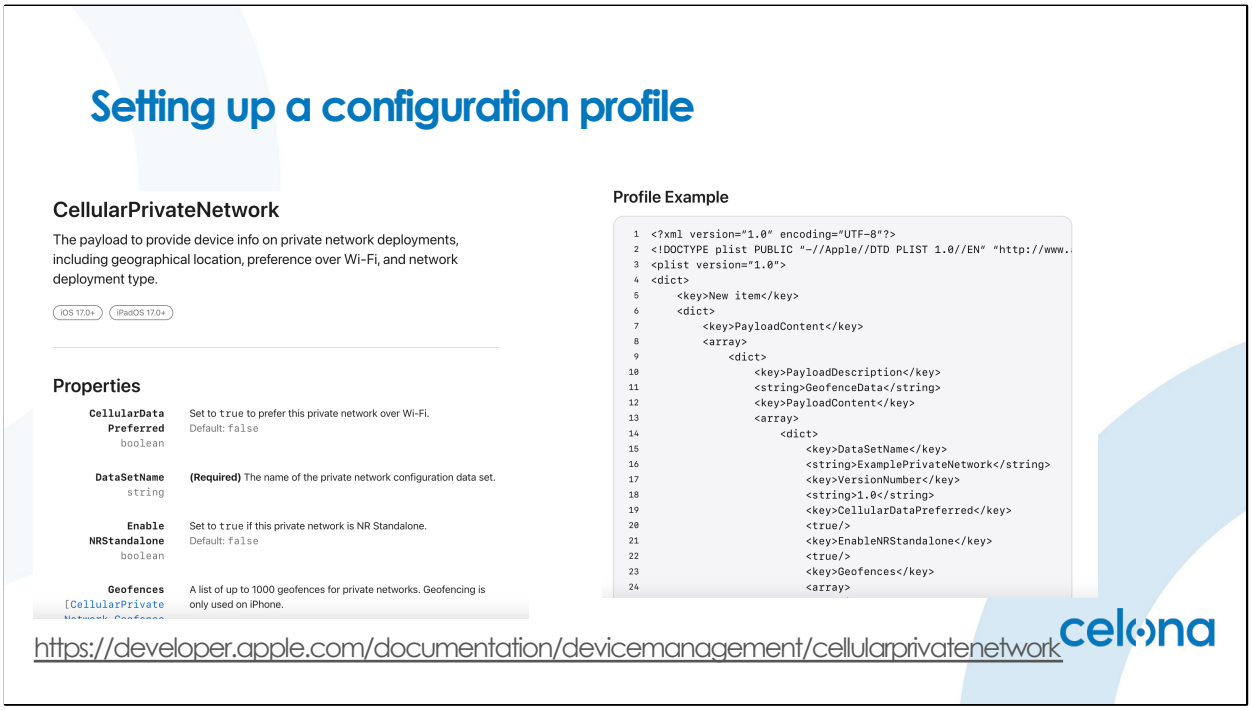


As I mentioned earlier, the private cellular network payload for configuring these options can be deployed as a configuration profile or apply to devices using mobile device management or MDM.

Now if your enterprise is already using mobile device management, check with your vendor to see if they support configuration of these new private cellular network features that were introduced in iOS and iPad OS seventeen.

Most MDM vendors already do or are planning to support these features in the very near future.

If you're not using MDM, you can create a configuration profile instead.



Now a configuration profile is simply a text file with the appropriate settings, and then you save it with a dot mobile config suffix.

You then install this profile on the device You can use Apple configurator, or you can download it from a web server or even send it in an email message.

To create a configuration profile with this private seller network payload, I recommend start by going to the Apple developer website. And you're going to look there for documentation on cellular private network under device management.

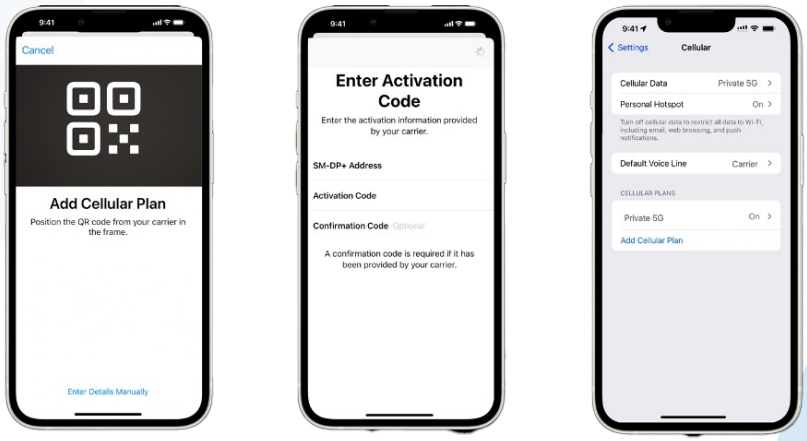
On this page, you're going to find an example profile, which contains the keys for each of these features that we just discussed.

The enable in our standalone, the cellular data preferred, and geofence.

You can copy and paste this into a text editor, Make the appropriate changes for your network, and then again, save it as a file with a dot mobile config suffix.

Apple recommends using esim when deploying a private seller network.
Esim's, prevent bad actors from taking your physical SIM and inserting it into a different device, or taking your device removing the SIM and connecting it to a different network altogether.
Celona can make eSIMs available for your specific devices that you want to connect to your private Cellular network. And you can add these esims to your iPhone or iPad by scanning a QR code, manually entering a server address or using MDM to automate the installation.
Now esims have many advantages over physical sims. They're more secure, they're device specific, and they cannot be physically removed or damaged.
So, this makes them ideal for enterprise deployments.

eSIM onboarding

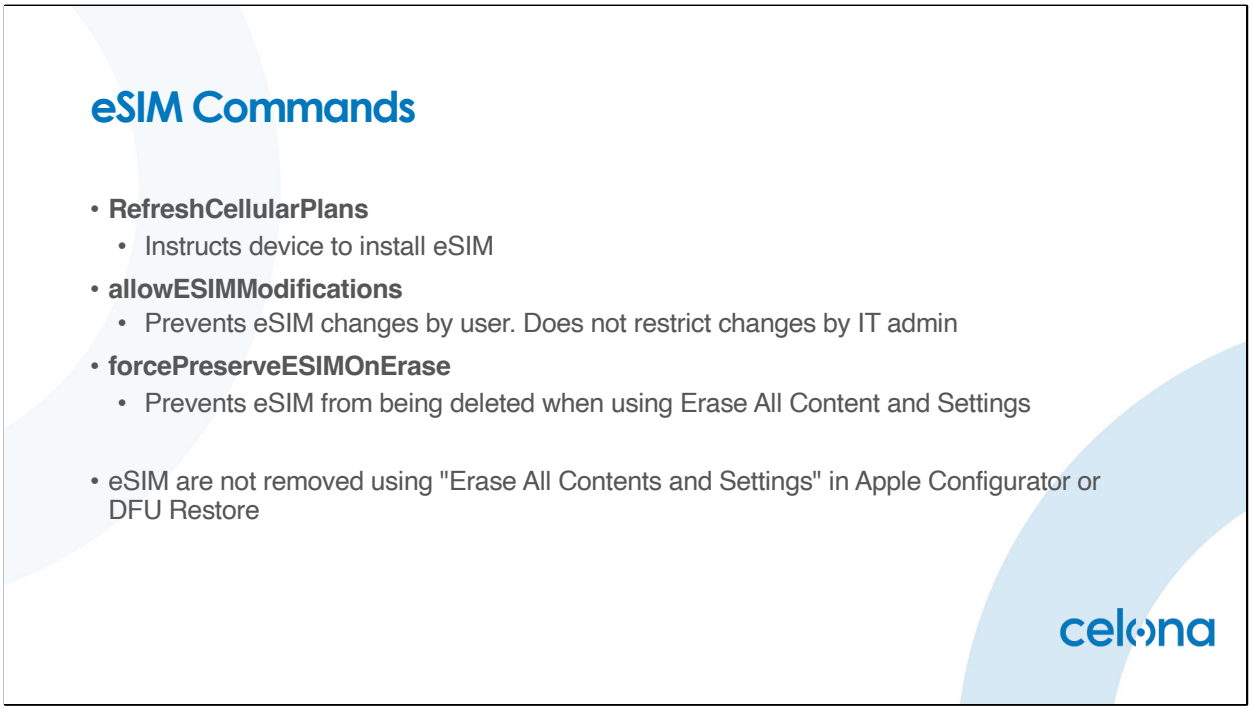


celona

eSIM Advantages

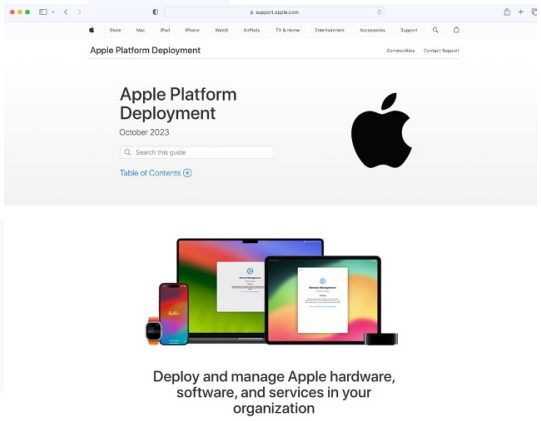
- Cannot be physically removed or damaged
- Secure remote installation and deletion
- Device specific; cannot be cloned or modified Advanced Elliptic Curve Cryptography (ECC)
- Store multiple eSIMs on iPhone and iPad

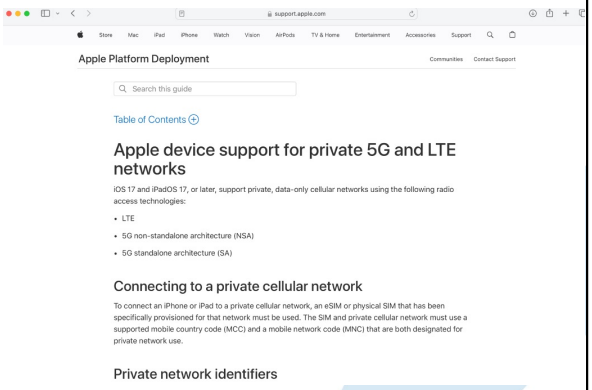
celona



If your enterprise is using MDM, there are a couple of features you can use with eSIMs.
The first is the refresh cellular plans command.
This command simply instructs iPhone or iPad to download and install the esim Celona provided to you.
The second is the allow esim modifications restriction.
This restriction prevents the iPhone or iPad user from making any eSIM changes. They can't add esims, they can't delete esims, or move an esim from one device to another.
This restriction is ideal for enterprise applications.
The third is a new restriction called force preserve e SIM on a race.
This restriction prevents eons from being deleted by the user when using erase all content and settings. Or when you wipe the device after a certain number of incorrect passcode attempts.
Now Apple has designed ESMs to remain on the device even if you need to do a complete reset.
So eSIMs are never deleted. We keep them on the device even if you use Apple configurator to do an erase all content and settings. Or you completely reinstall the operating system using a Dfu restore.
To help enterprises like yourself deploy iPhone and iPad on private cellular networks, Apple has added a new private 5G and LTE section to the Apple platform deployment guide.

Apple deployment platform – support for PCN





https://support.apple.com/guide/deployment/welcome/web

celona

The Apple platform deployment guide is a technical document. It covers a lot of different topics that we discussed today, as well as a lot of information about deploying Apple products and services. In the guide, there's this entire section that we added on Apple device support for private 5G and LTE networks.

And so, you're going to find here, information about device compatibility with private networks, more information on installing esims. Also, some really exciting information about enhanced security and privacy which are enabled on 5G standalone networks.

So, this is an excellent resource to use when you're planning, for your deployment.

Well, as I mentioned at the outset, now that iPhone and iPad support private cellular networks, we think this technology is ready for widespread deployment.

Your enterprise can now take advantage of this 5G technology to build a workplace that's more connected, secure, reliable, and designed for your individual business needs.

Celona 5G LAN…

FOUNDED	April 2019 (Founders from Aruba, Qualcomm, Federated Wireless, Cisco)
HEADQUARTERS	Silicon Valley
CAPITALIZATION	$100 M (three rounds)
INVESTORS	Lightspeed, Norwest NTT VC, Qualcomm Ventures, Cervin, Digital Bridge
IINNOVATION	Pioneer of industry's first enterprise 5G LAN system

STRATEGIC PARTNERS

verizon · NTT · ZEBRA · Google Cloud · COX · comcast

REPRESENTATIVE CUSTOMERS

BMW · Schneider Electric · HSG · STANDARD STEEL · DELCONCA · ALBEMARLE

celona

Private Wireless for the enterprise

- End to end turnkey, converged 4G/5G solution, designed exclusively for the enterprise
- Deterministic performance for critical apps – MicroSlicing™
- Enterprise friendly management and operations
- Integrates with all existing Enterprise network services & security protocols

Decide how, where, and when you need 4G or 5G or both

End to End turnkey
Every component needed
Engineered for the enterprise
With Wi-Fi-like simplicity
Cloud managed
Deploy in hours/days
vs. weeks/months

We are extending 5G LAN to your global enterprises

With mid band support from 3.3 to 4.9 GHz,
Celona's 5G LANs can serve a vast majority of global markets

N48 (3.5-3.7GHz) **N77** (3.8-4.2GHz) **N78** (3.3-3.8GHz) **N79** (4.6-4.9GHz –planned 2H23)

- US – shared/ managed spectrum with 4G/5G support
- Globally – shared/licensed spectrum mostly on 5G
- licensed spectrum allocated to enterprises for a nominal cost
- 20+ countries incl. **US, UK, Germany, Japan, Korea, France**
- Strong device ecosystem including Apple, Zebra, Samsung

celona

- While US is providing a shared spectrum that doesn't require licensing, other countries are offering licensed spectrum at a nominal cost.
- US using the CBRS B48/N48 spectrum for private wireless
- Globally private wireless is skipping to 5G (no option for 4G) around the N77,78,79 spectrums

Device Ecosystem: The Pivotal Challenge & Prime Opportunity for Private 5G

celona

Robust and open 4G/5G device ecosystem

celona.io/devices

5G LAN Certified

Devices that have successfully gone through Celona's complete device certification test suite.

5G LAN Compatible

Devices that have been successfully operated on Celona 4G/5G network yet to go through full device certification.

Consumer Smartphones

Ruggedized Handhelds

Tablets

Laptops/Cameras

Adapters/Dongles

Push-to-talk

IoT Gateways

MANUFACTURERS COVERED

Apple, Digi, Google, Samsung, Zebra, Quanta, Getac, MultiTech, Telit Cradlepoint, Sierra, OnePlus. OneScreen, Quectel, Sequans, Peplink

Apple iOS 17 certified on Celona 5G LAN

iPhone

All iPhone 14 models
All iPhone 13 models
iPhone SE (3rd generation)

iPAD

iPad Pro 12.9-inch (6th generation)
iPad Pro 11-inch (4th generation)
iPad Air (5th generation)
iPad mini (6th generation
iPad (10th generation)

Key Private Network Features (iOS 17) validated on Celona Private 5G network

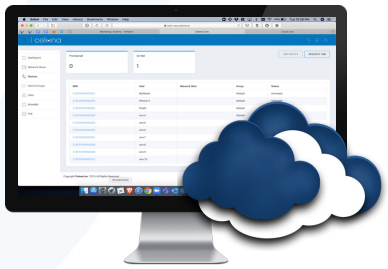
- ✓ 5G Standalone
- ✓ Support for MCC 999 and 315 CBRS networks
- ✓ Prioritizing Cellular over Wi-Fi
- ✓ Geofence activation
- ✓ Zero-touch provisioning using eSIM & MDM
- ✓ Support for n78, n77 & n48 bands across Europe, UK & US

celona

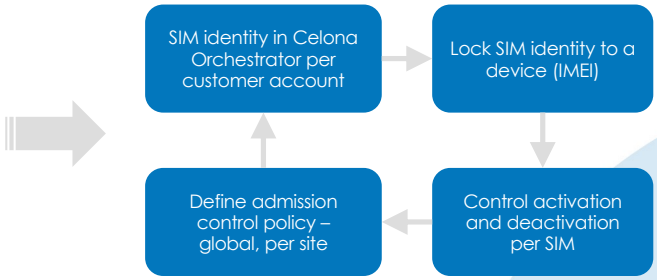
`

Device onboarding made easy

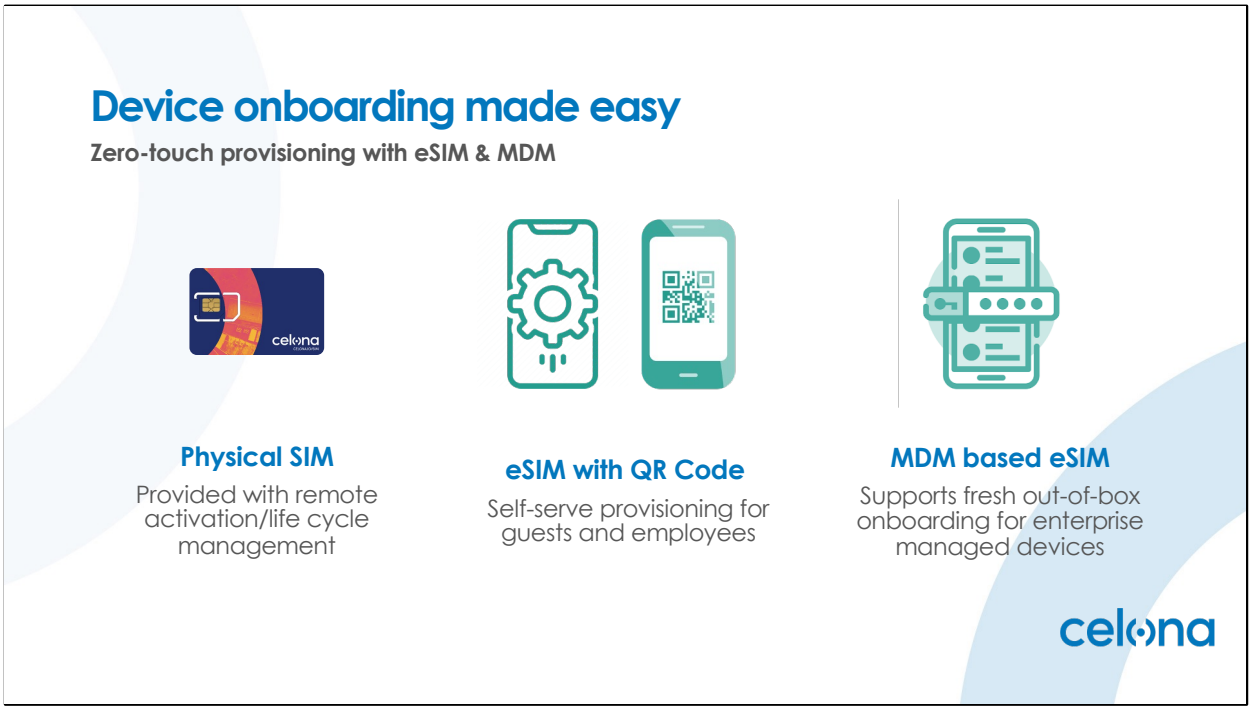
Full SIM lifecycle management



SIM assignment to devices
and ongoing management



celona



>

DIU request: List authentication methods used between UE and authentication framework.

Case Study - Transportation Railyard

Customer Pain Points:

- Delays in certifying trains for commercial operation due to erratic and unstable wireless connectivity impacted revenues/operations
- Connectivity for portable yard air controllers (YACs) to test brake systems

Use Cases:

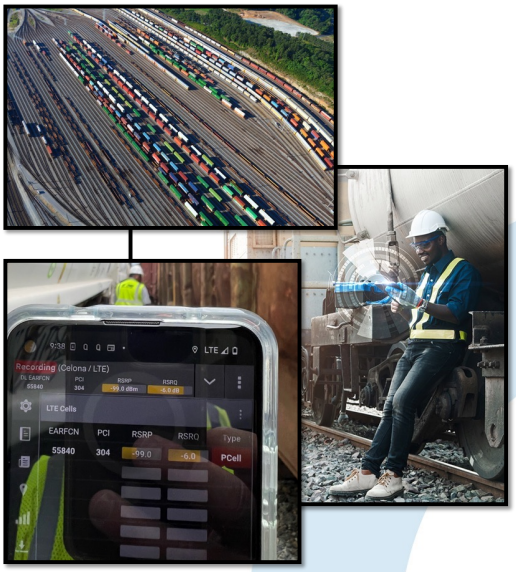
- Dual-SIM Apple iPhones and iPad Pros
- Dual-SIM public to private roaming required for railyard workers

After Celona Deployment:

- Outdoor ***4G/LTE*** coverage using only 4 Celona AP 11 APs (per site) with no wireless dead spots
- eSIM integration with existing MDM system
- Celona Orchestrator for cloud-based administration and SIM mgmt.

Business Outcome

- Up to a 20 dBm improvement in signal strength over existing public cellular service (Wi-Fi wouldn't work in this environment)
- Elimination of wireless disconnects, and session interruptions caused by poor wireless coverage
- Improved productivity of rail yard staff to certify trains for operation



Q&A, and next steps...

Celona 5G LAN certified devices
https://www.celona.io/devices

Download the new report – State of the private wireless market, 2023 and Beyond
https://www.celona.io/the-state-of-private-wireless

Request a complimentary RF planning workshop
https://www.celona.io/rf-planning-workshop

Learn more at
https://docs.celona.io
http://support.apple.com

Q & A

Eric Zelenka

Senior Consulting Engineer
5G & Cellular

Apple

ez@apple.com

celona

Don't miss our next webinar

Topic: Why business technology leaders must consider Private Wireless

Speakers:
Dean Bubley, Founder, Disruptive Analysis
Rajeev Shah , CEO, Celona

Day/Date: January 25th, 2024
Time: 8 AM PT | 11 AM ET | 4 PM GMT
Registration link: https://www.celona.io/webinar-why-tech-leaders-must-consider-private-wireless