Simplifying eSIM
iPad Setup with Jamf
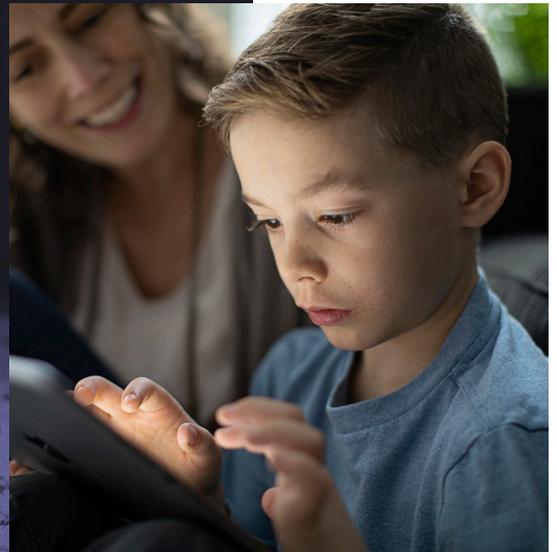
Table of Contents

.

Introduction

eSIM and Apple Mobile Devices

Traditionally, cellular devices included a slot where a small Subscriber Identity Module ("SIM") card could be inserted. Most of the time, devices came with a card already installed to link the device to a cellular carrier and service plan. Some modern devices are switching to use an embedded SIM ("eSIM") that can store the this information. Unlike SIMs, eSIMs don't take up any physical space inside the device -- they're stored digitally in an encrypted file system on the iPad. Since they're not linked to a specific carrier, eSims can simplify initial procurement and make it easier to switch from one carrier to another.

The following Apple reference lists the iPad models and countries/carriers that support eSIM: https://www.apple.com/ipad/cellular/.

Activating Cellular Service with eSIM without Jamf

Unless a device has been pre-configured, eSIM devices don't know which carrier will be providing their cell service when they're first turned on. There are no icons at the top of the screen to indicate cell service has been set up like there are when a carrier-specific physical SIM is installed.

When a consumer purchases a device with an included cellular plan, the retailer may configure the device for them. Or they can go into the cellular settings page on the device and pick a plan to purchase for themselves. In cases where the device was purchased directly from the carrier, Apple may already know that the device has a carrier and the device might provision its cell service automatically.

When an organization adds devices to its cellular plan, there are a number of manual methods available for setting up cell service with an eSIM. Most carriers have a have a web page with instructions for the methods they support. They may provide a URL and activation Code that you can enter manually, a QR code to scan, an Apple App Store app, etc.

But going through the cellular configuration process is a lot of extra work if you're setting up a large number of devices and requires that you have physical access to the device. In these cases, we can use a Jamf School or Jamf Pro MDM command to instruct the device (or many devices at once) to contact your carrier's eSIM servers and configure themselves. We'll show you how in the next section.

When an organization needs to add eSIM devices to their cellular account, they'll need to provide the Mobile Equipment Identity ("IMEI") number and eSIM ID Number ("EID"). If you don't already have a list of these, ask your Apple Rep to provide them. They can work with their SE team to create a list as soon as your iPads have shipped and their serial numbers are known. You can pass the list on to your cellular provider so they have the device information associated with your account and set up in their eSIM

servers when you're ready to configure the devices. Ask your carrier if there's any time limit on how long you have to download an eSIM profile to your devices.

If you don't have a list of the cellular IDs for a device, you can find the IMEI and eSIM numbers on the outside of the iPad's box. You can read them in with a barcode scanner if one is available. It may also be helpful to include the device serial number in your list so the device can be referenced if you have to followup with your carrier should a device require troubleshooting.
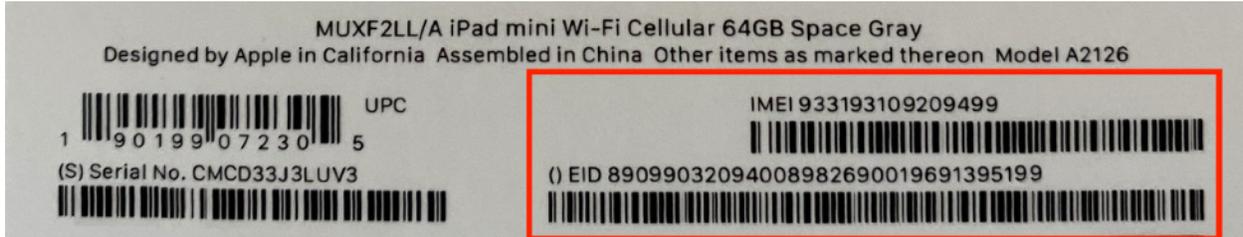
The same information is also available on the device itself under "Settings > General > About".

Apple's https://support.apple.com/en-us/HT209044 page has detailed information on these provisioning methods as well as tips for using an eSIM on a dual-SIM phone as might be the case when a corporate device has a separate SIM for personal or international use. Note that while some iPad models offer both a physical SIM slot and eSIM, they do not have dual-radio capabilities like some iPhones do -- on an iPad, only one SIM can be active at a time.

The images below show the Cellular Data pane as it appears on an eSIM iPad that doesn't yet have an activated cellular data plan. The image to the right shows the data plan purchase page for a carrier, in this example, T-Mobile.
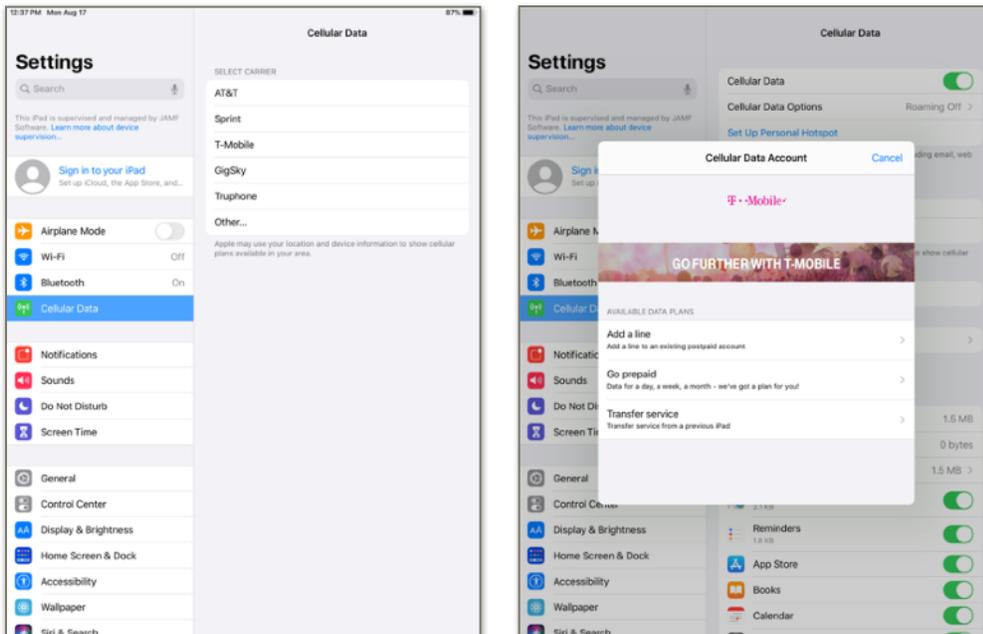
Automated Cellular Activation for iPad

Manual configuration of cellular settings in Settings is practical for consumer devices but too time-consuming when setting up large numbers of devices. Two Jamf products offer support for automated eSIM activation. Jamf School is purpose-built for management of educational devices. Jamf Pro is often used in other organizations, or by schools with large or complex management requirements.

Typical Provisioning Workflow

In a common mass-deployment scenario, an organization is going to be distributing iPads to end-users for home use. They often want to configure the devices at a central location or service provider depot to make sure everything is correct before handing out or shipping the device. In education, the student may be young and not an expert troubleshooter. In business, IT may not want employees to have the trouble of shipping a device back to IT if there's something wrong.

Boxes of new devices have been delivered by Apple (or their reseller), cellular service has been purchased, and the cellular carrier has added the EID numbers for the device eSIMs to your organization's data plan account. To get the devices ready for the users, we'll first need to enroll the devices in a Mobile Device Manager ("MDM") like Jamf Pro or Jamf School. Once that's done, we can manage the cellular setup from a central console without ever having to touch them.

There are a few ways to enroll devices in MDM when doing mass-deployment:

Automated Enrollment – In this method, Apple School Manager (or Business Manager) already knows your organization owns the devices so they'll tell them to connect to your MDM automatically the first time they're powered on.

Apple Configurator – This is a free program available on the Mac App Store. It allows you to connect many iOS or iPadOS devices to a Mac via a multi-port USB hub and can install the initial software and settings you want. It's fast since it doesn't all need to happen over a WiFi network.

Once the device is enrolled in Jamf Pro or Jamf School, it's easy to install more settings and software, or to push mobile device commands to large numbers of devices, for example, "Refresh Cellular Plan". This command tells the iPads to connect to your carrier to download an eSIM so they can start getting cellular data. That's a lot easier than setting up cell service on all your devices by hand.

Some helpful references:

- Apple School Manager Guide / Apple Business Manager Guide
- Jamf School Deployment Guide
- Deploying iOS and tvOS Devices Using Apple Configurator 2 and Jamf Pro
- Enrolling macOS, iOS, and tvOS Devices in Jamf Pro Using Automated MDM Enrollment

Activating eSIMs with Jamf School

Activating a Single Device

Once a set of devices have been enrolled Jamf School, we can view them under "Devices". If we click on a device to view its details then select "Network Information", we can see that the cellular plan information is blank because cell service hasn't been activated yet.
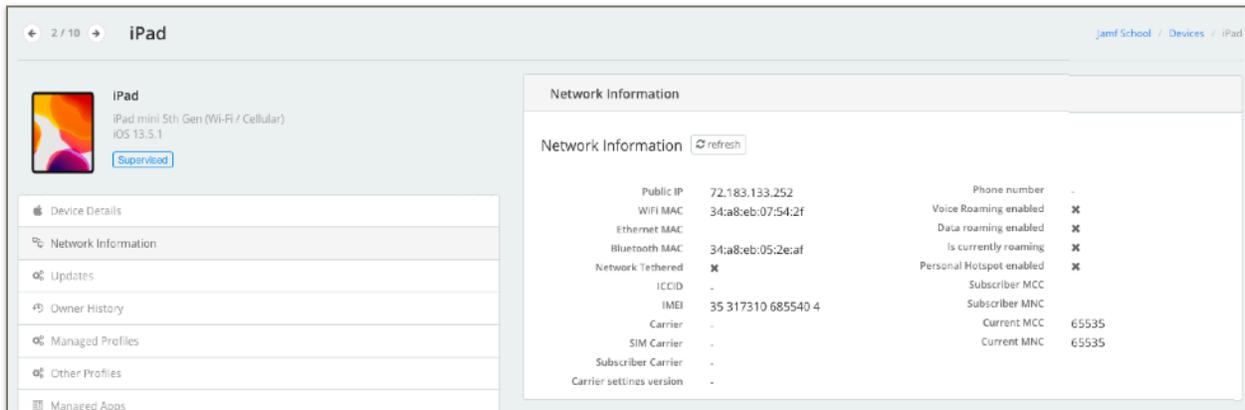
You can tell the device to contact your cellular carrier and activate its cell service by clicking the "Refresh cellular plans" button under "Quick Actions" in the lower-left of the detail page.
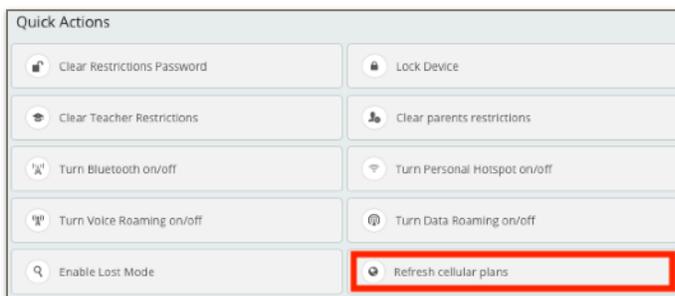
When this button is pressed, a dialog box will appear. Enter the eSim Server URL for your carrier. If you're using network tethering, select the "Requires network tether" checkbox. Ref: Setting up a shared Internet connection for iPhone and iPad.
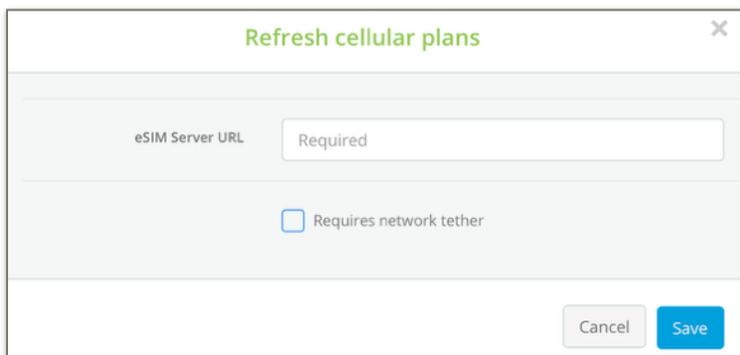
Activating Multiple Devices

To quickly activate the cellular data plan on multiple devices, open the device listing and click the checkboxes next to the devices you want to activate. A filter on "Device Model" and/or "Location" may be helpful when locating your cellular iPad devices. Once you've indicated the devices to be configured, select "Refresh Cellular Plans" from the "More" drop-down menu.

As with activations from the detail page for a single device, Jamf School will prompt you for your carrier's "eSIM Server URL". This will be provided by your carrier. (See the Notes section at the end of this document for some examples.)

When this button is pressed, a dialog box will appear. Enter the eSim Server URL for your carrier. If you're using network tethering, select the "Requires network tether" checkbox. Ref: Setting up a shared Internet connection for iPhone and iPad.
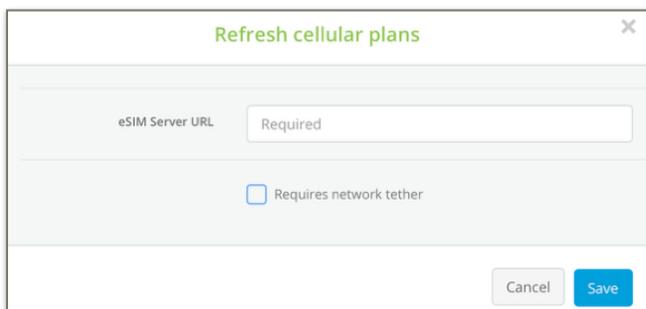
Click the "Save" button once you've filled in the information. Jamf School will send an MDM command to each of the selected devices. This command will direct the Apple OS to identify itself to the carrier's eSIM server. The carrier will match this to your account and reply to the device with its activation

information (i.e., an "eSIM Profile"). The device will then connect to the cellular network without requiring any manual steps on the device.

There are a number of indications that the eSIM has been configured. On the iPad itself, the presence of cell service is indicated by the LTE signal strength indicator at the top of the screen, and the cell carrier and details of your configuration are shown in Settings.
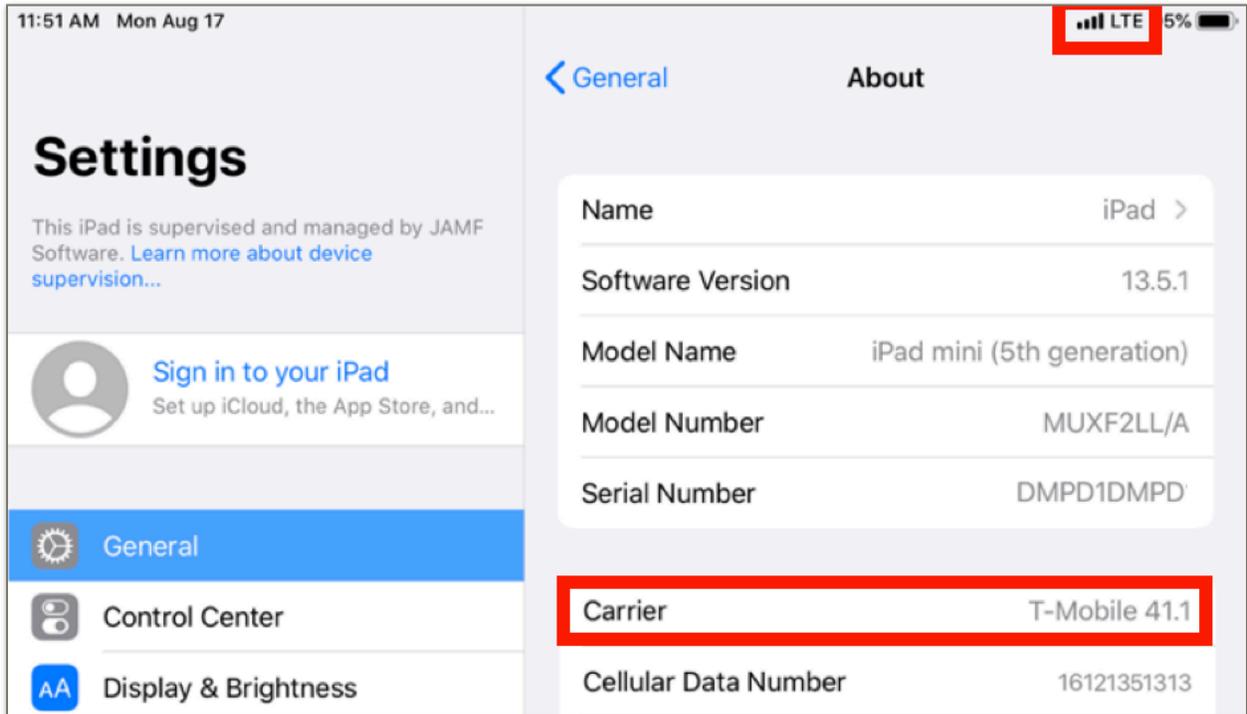
Much of the same data is also now available in the Network section of the device details page in Jamf School.
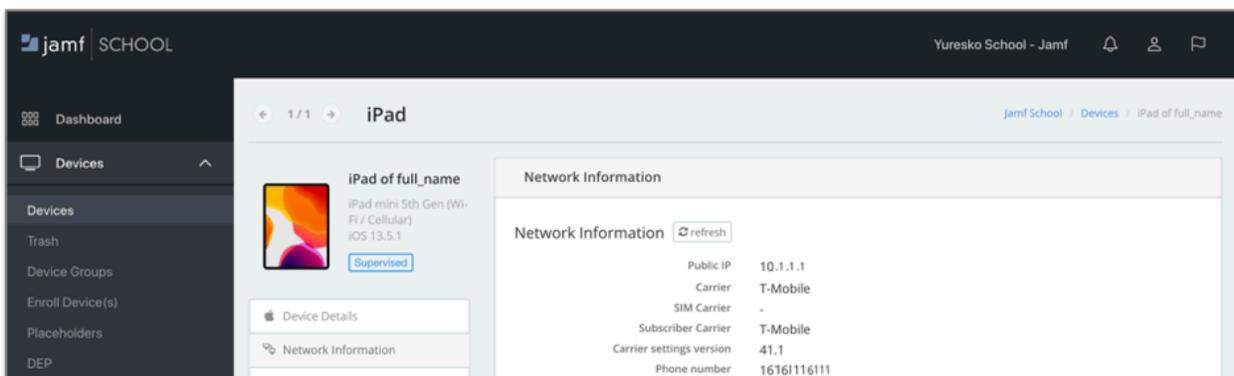
You can test out the cellular connection by turning off wifi on the iPad (if it's connected) and then opening a web page in Safari.

Activating eSIM Cellular Service with Jamf Pro

When a brand-new device is enrolled in Jamf Pro, we can open its inventory details ("Devices > Search Inventory" > click on the device item in the list > Network section) and see that it's a cellular device because it has values in for things like the IMEI number. We haven't downloaded an eSIM on this device yet so the Carrier Network fields say, "iPad".

The cellular fields will be blank for devices that don't have cellular capability. If we want to activate the cellular data services on this device, switch to the "Management" tab and click the "Refresh Cellular Plans" button.
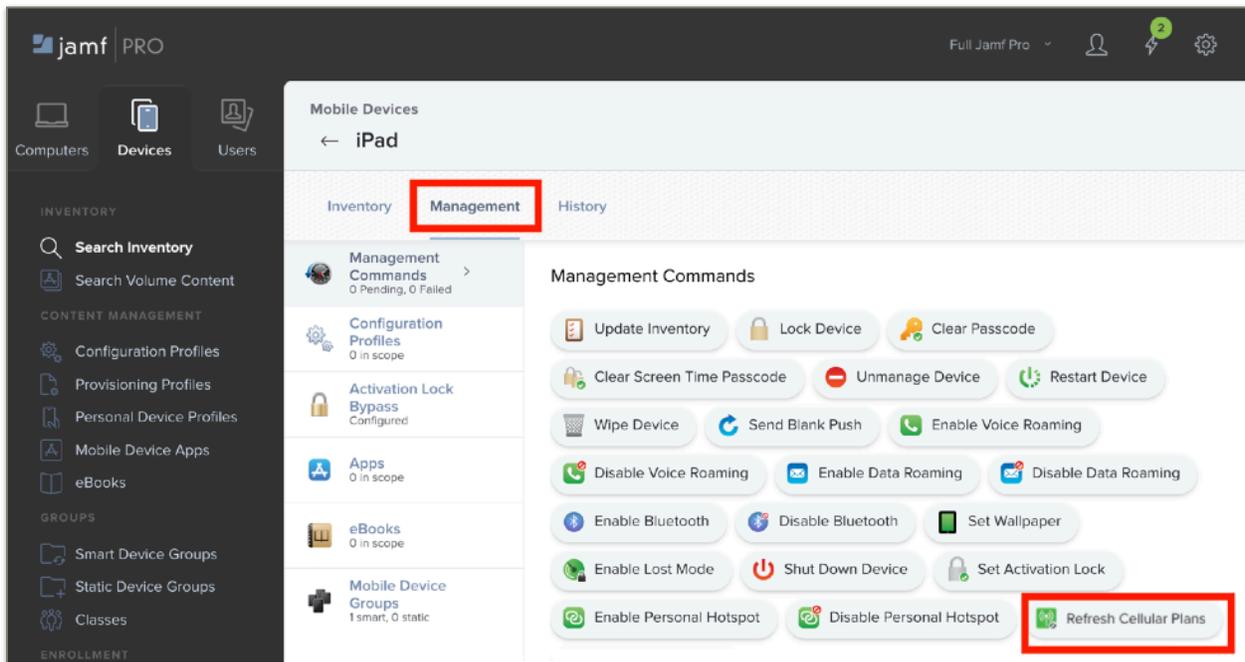
You'll be prompted for the "eSIM Server URL". A few examples are listed in the Notes section at the end of this document but check with your carrier to make sure you have the right one.
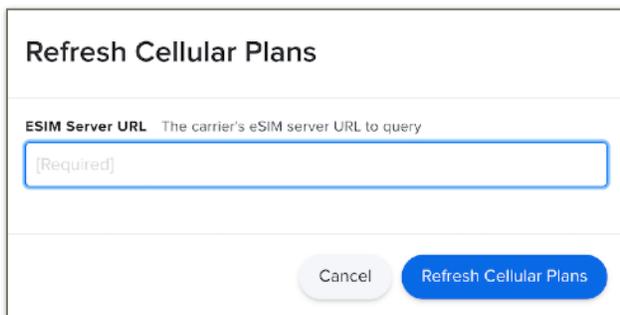
Upon completion, the device will be activated and show cellular bars in the upper corner of the home screen. You can view details about the cell service in "Settings > General" on the device and you'll see the carrier information filled in on the device's network inventory details page in Jamf Pro. If you don't, refresh the device's inventory information using the button in the Management tab.

Listing the Devices that Need to have their Cell Service Activated

Suppose we spent a morning enrolling a large group of new iPads into Jamf Pro using either the Apple Automated Enrollment or Configurator methods and we want them to activate their cell service while we go to lunch. We can create a group of the devices to be activated and then tell Jamf Pro we want them to be setup for cell service all at once. It's a lot faster than clicking into each one individually and hitting the refresh cellular plans button in the management tab.

To begin, go to "Devices" and click the "+New" button for Advanced Mobile Device Searches.
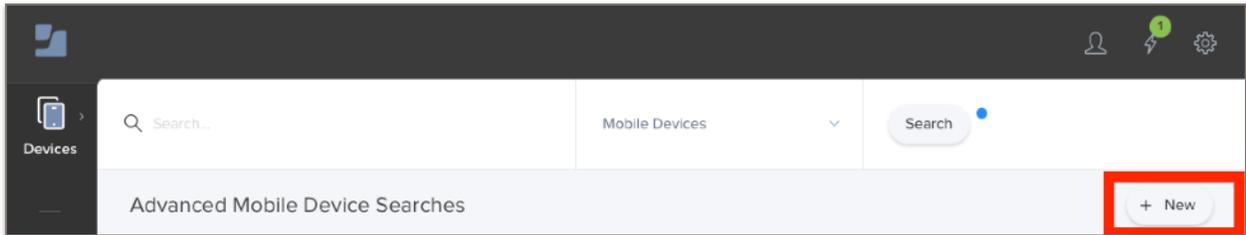
If you're going to be doing some additional batches of device enrollments later, you can save the search for later re-use by clicking the "Save this search" checkbox and supplying a name.
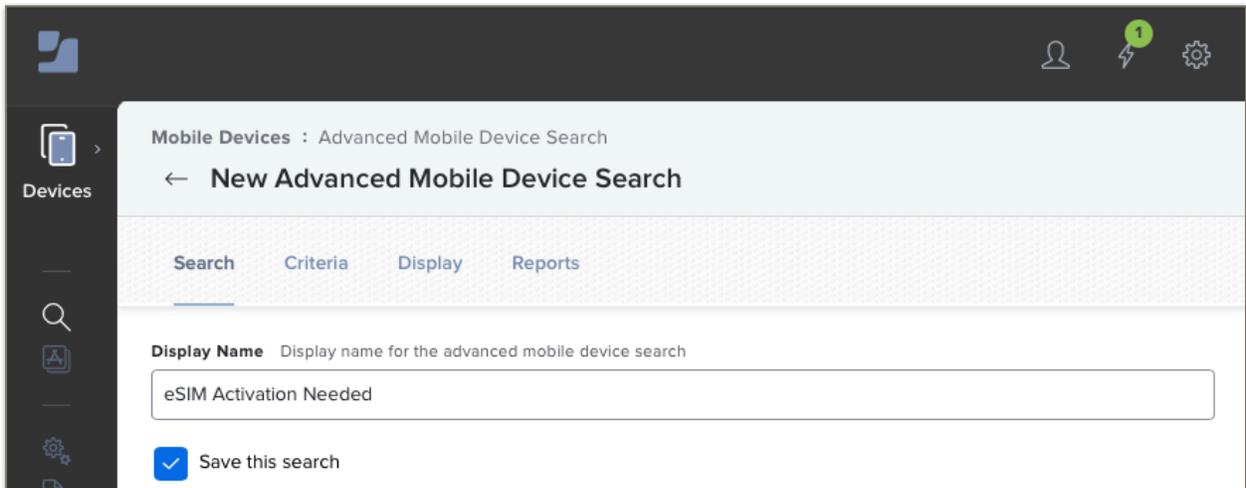
Next we'll fill in the "criteria" tab. When we looked at the network inventory details for an iPad that had been enrolled with Jamf Pro but had not yet been configured for cell service, we noted that that the "Current Network Carrier" field was set to "iPad". We can use this behavior to quickly create a set of all devices that need to be setup with their cell service plan.
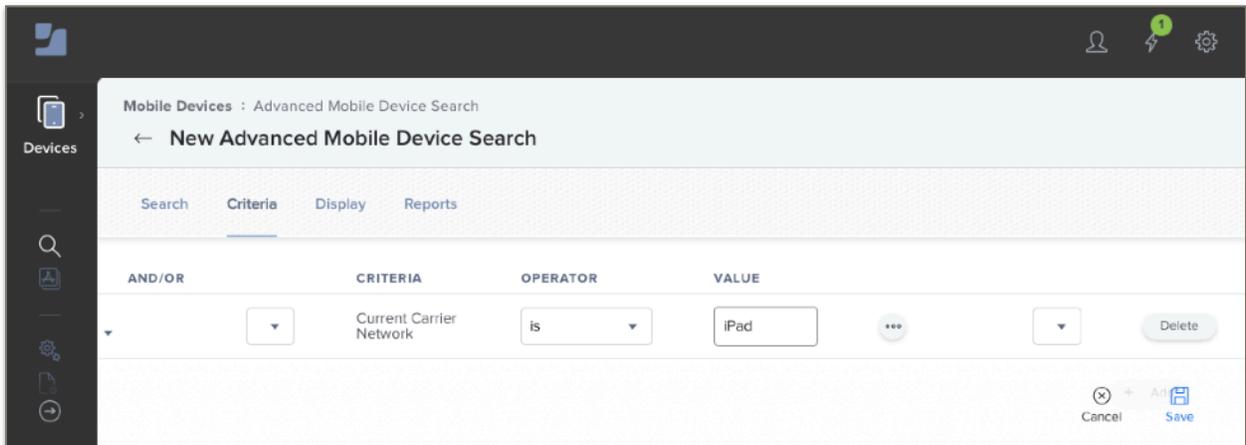
Once a device is activated with a carrier and inventory information has been updated, that field will change to the carrier's name and the devices will automatically drop out of the advanced search results.

Advanced Mobile Device Searches

In the preceding section, we created a simple advanced search to create a list of all iPads that still need to be activated. That would cover the majority of deployment scenarios, but there might be some more complicated cases. Jamf Pro has options to cover almost anything.

For example, if you're working over the course of a few days to set up lots of different iPads and only wanted to active a batch of "iPad Pros 11-inch (2nd generation)" that you enrolled today, your criteria might be:

This strategy is helpful because there may be cases where a device have activated its cell service but has not yet reported an updated inventory to Jamf Pro. In this case, just filtering for carrier = "iPad" could capture devices that already have their cell service running. In the above example, we're filtering on date and if this is the first time we've pushed out a cell plan reset commands, we'll know we're only updating the devices that are ready for it.

Suppose there are a few iPads that will only be used in the office and you don't intend to activate their cellular data plan. We could add a few "is not equal to" lines to exclude them by name, user, or serial number. If there were many such devices, we could create a "No Cell Service Needed" static group and add an "is not a member of" line to our advanced search to exclude them.

What if we're deploying lots of different models and the setup work is happening at many different sites? That might be the case with a large eduction deployment with staff at each of a district's schools setting devices up at the same time. We could create a separate "Activation Needed" advanced search for each location and filter on external IP address (if every school had a different one). If we are including a school abbreviation somewhere in the device names that we're applying with Apple Configurator, we could add a "Device name/contains/<school code>" line.

If you're doing a 1:1 deployment and assigning the devices to specific users, you can even use information like department of group membership from a directory service like Active Directory.

Bulk Cell Plan Activation in Jamf Pro

Once you have your Advanced Search criteria the way you want, click the "Save" button and then the "View" button at the bottom of the page to show the list of all the devices that meet your "Activation Needed" criteria. From the device listing screen, click the "Actions" button. Jamf Pro will display a list of things you can do to a group of devices. Select "Send Remote Commands" and click the "Next" button.
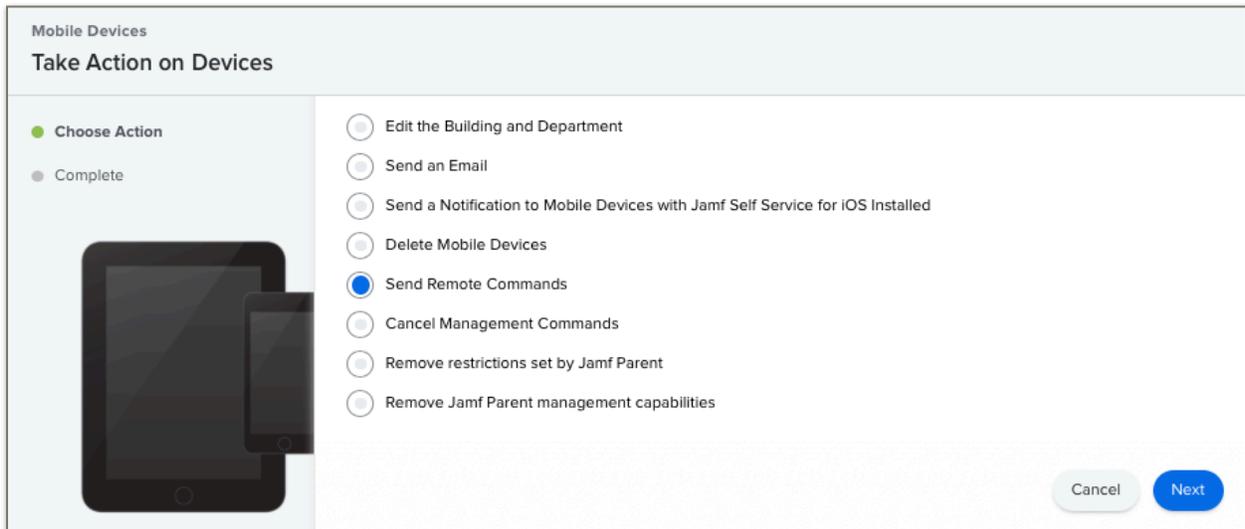
Select "Refresh Cellular Plan" and enter the eSIM Server URL provided by your carrier. Then click "Next".
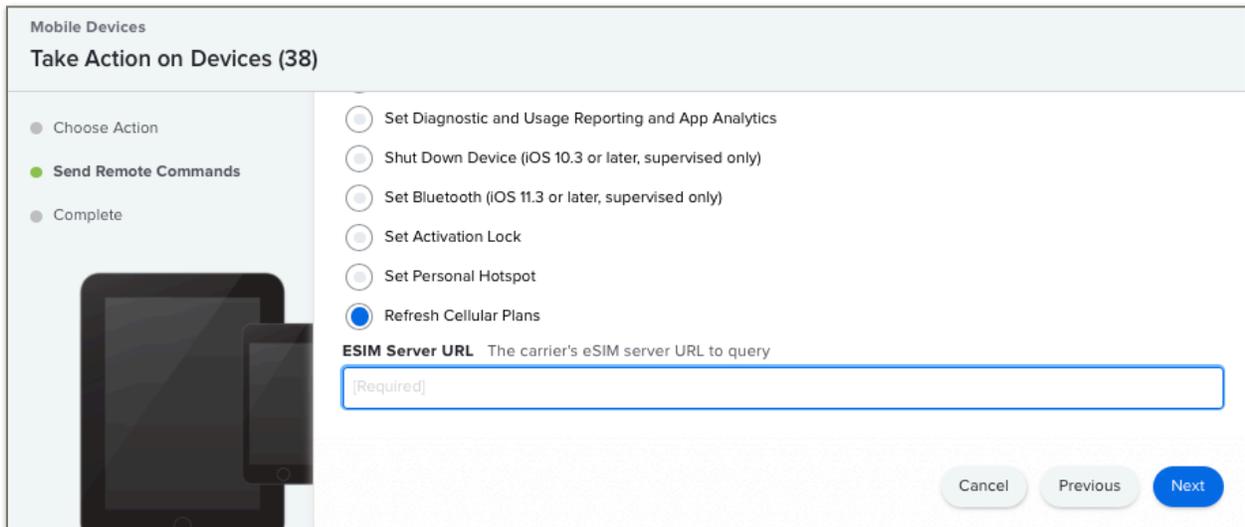
Jamf Pro will send the command to each device in the group. The devices will contact the carrier eSIM server you specified and retrieve their cell plan settings (the "eSIM Profile"). Then they can connect to the cellular network without requiring any manual steps on the device.

When checking the iPads, we'll see the cell service signal strength in the upper-right corner of the screen and the carrier will be listed if we go into Settings > About on the iPad.
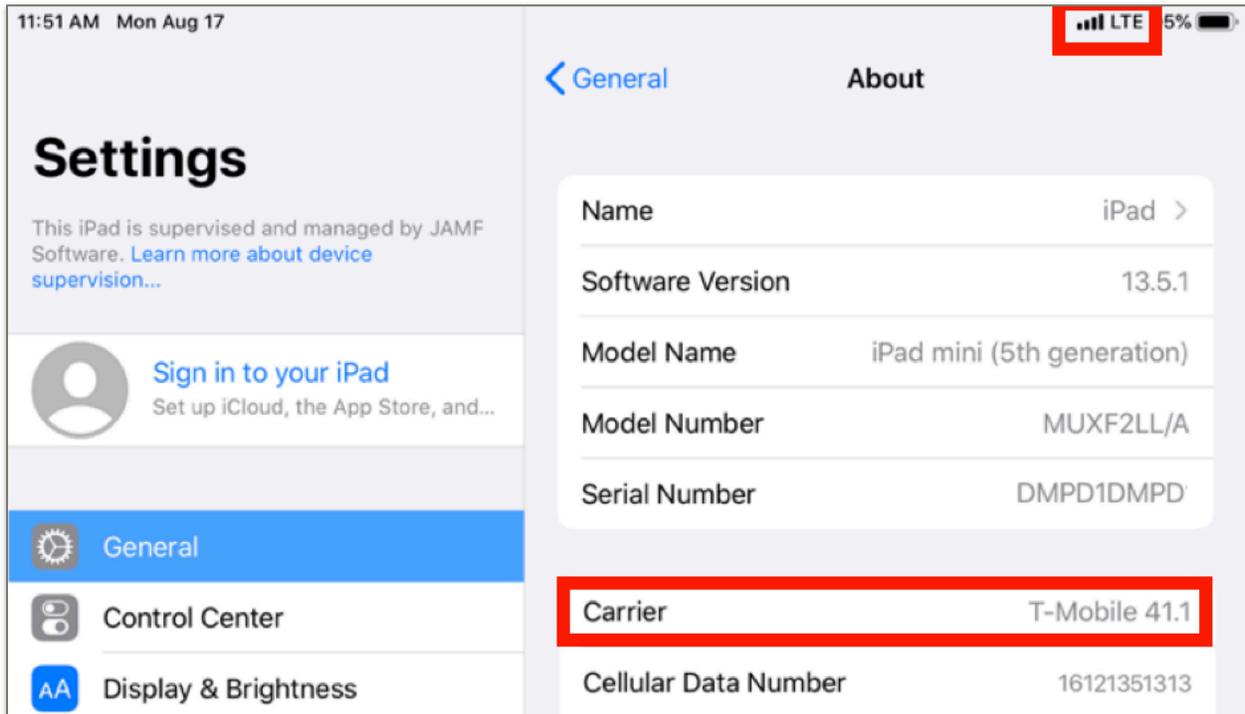
Once the device has submitted its next inventory, the details for the cell service will appear in Jamf Pro's device details page, including Carrier and Phone Number information.
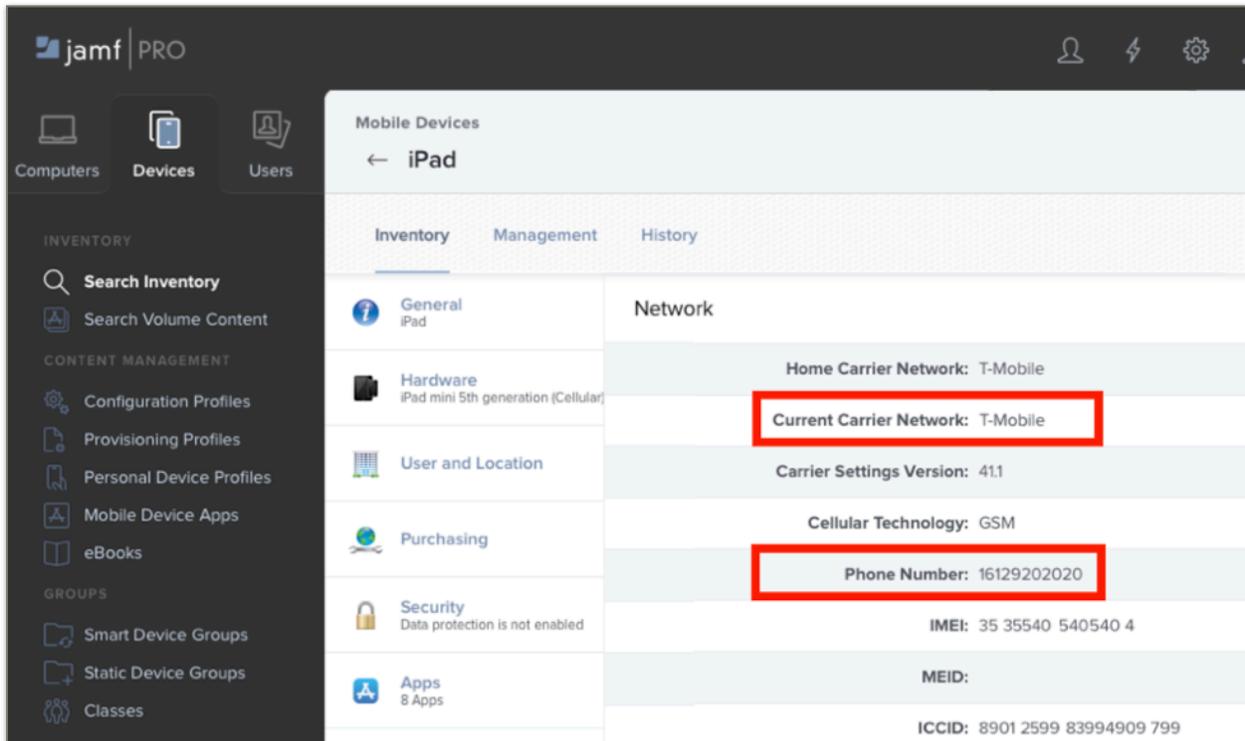
eSIM Implications for Device Reset

Device Reset and "Retain Cellular Plan" in iPadOS

Carriers may expire or remove device information from their eSIM servers once an eSIM profile has been downloaded, so unless you're changing to a new carrier, eSIM provisioning on an iPad should be considered a one-time event. We'll need to make sure the eSIM profile isn't accidentally erased. We can use Jamf to:

1. Prevent users from altering their cell plan.
2. Prevent users from deleting their eSIM via Settings's "erase all content and settings" option.

If cellular settings are unintentionally removed from a previously-activated eSIM device, either on the device itself in Settings, by sending a device wipe command via MDM, or by wiping the device with Apple Configurator, trying to reinstate it by sending the "Refresh cellular plan" MDM command probably won't work. The device is no longer in the carrier provisioning systems. The user will see see a popup message on the iPad stating, *"Cellular Plan Cannot Be Added; This code is no longer valid. Contact your carrier for more information."* You'll need to contact your carrier and give them the device's IMEI and EID numbers so they can re-stage the eSIM profile for the device on their eSIM server. Once that's done, they may instruct you to restart the device. Then you should be able to re-activate the device's cellular service.

Because of all the carrier intervention required to get cell services back onto a device, we need to take precautions to prevent users from removing their cell plan inadvertently.

Restricting the user's ability to change cellular settings — Jamf School

We can create a restrictions configuration profile to ensure that users do not remove the cellular plan settings from their devices.

If you already have a standard restrictions profile for your devices, you can elect to edit it to add the cellular restrictions. Or, to create a new profile, go to "Profiles > Profiles > Create Profile".
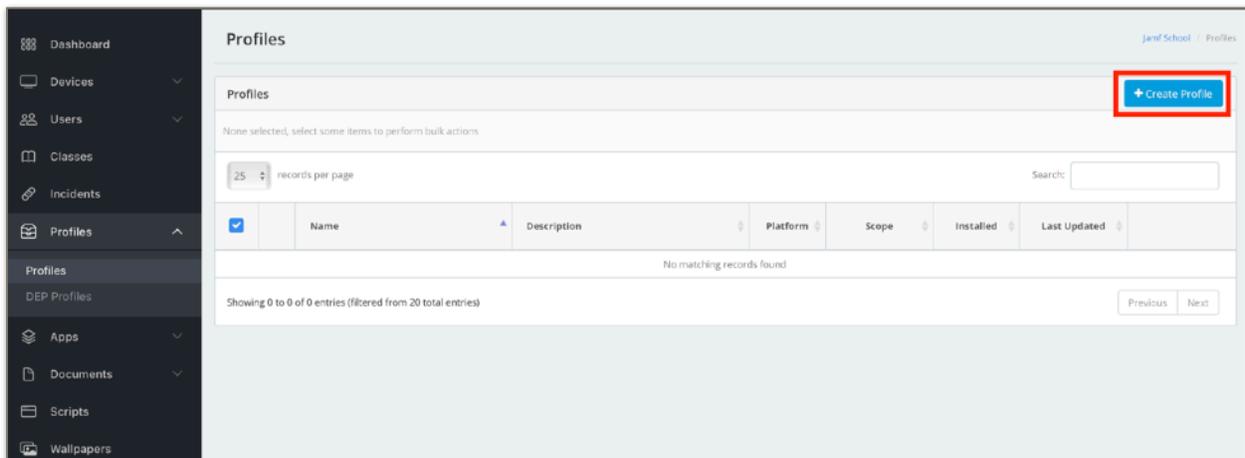
Select "iOS"
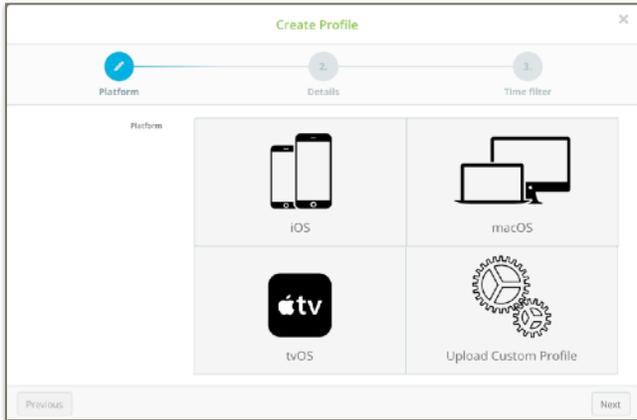
Select Device Enrollment, click "Next"
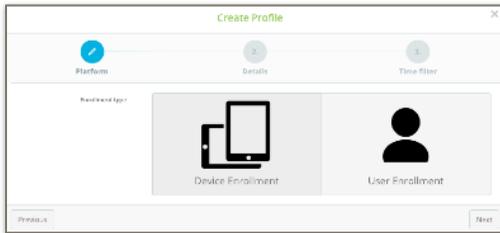
On the Details screen, provide a name for the Configuration Profile; you can also choose to add a description. Click "Next"
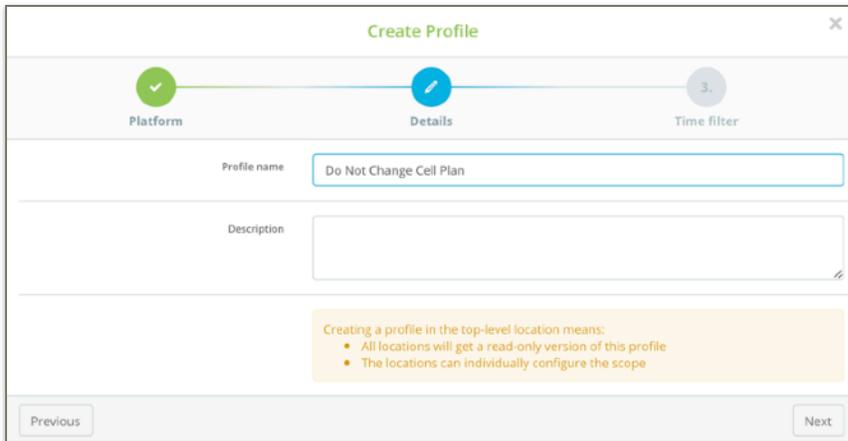
The final configuration step in the New Profile wizard is "Time Filter". We will not use this option when setting cellular restrictions. Click "Finish".
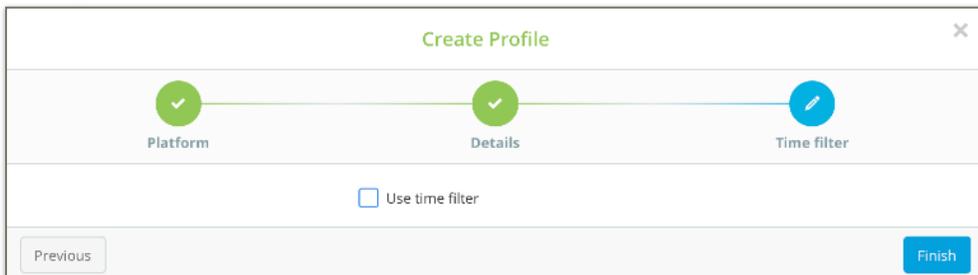
The newly created profile will now be in view. Click the "Restrictions" payload and then click "Configure".
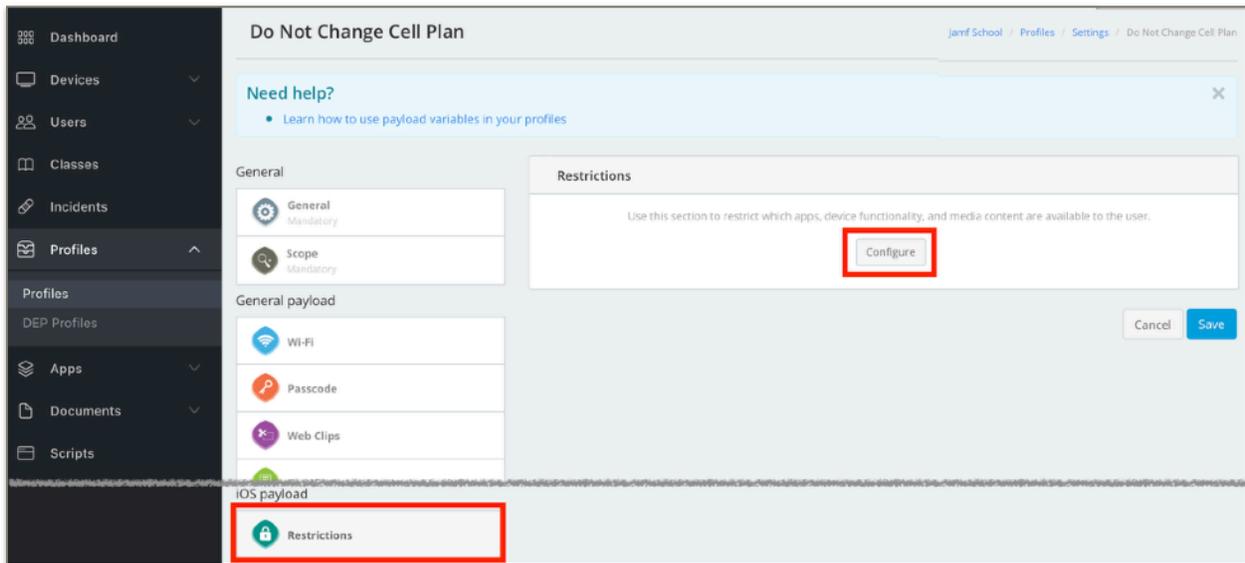
On the Functionality options page, scroll down to the "User modifications" section and uncheck "Allow adding or removing a cellular plan", "Allow modifying cellular plan", and "Allow the use of the 'Erase All Content and Settings' setting". Blocking the user from erasing their iPad is a good idea because they might do it incorrectly and remove their eSIM. It's safer to have an admin use Jamf School to erase the device if it's ever required. That way the admin can decide if the eSIM should be retained or not.
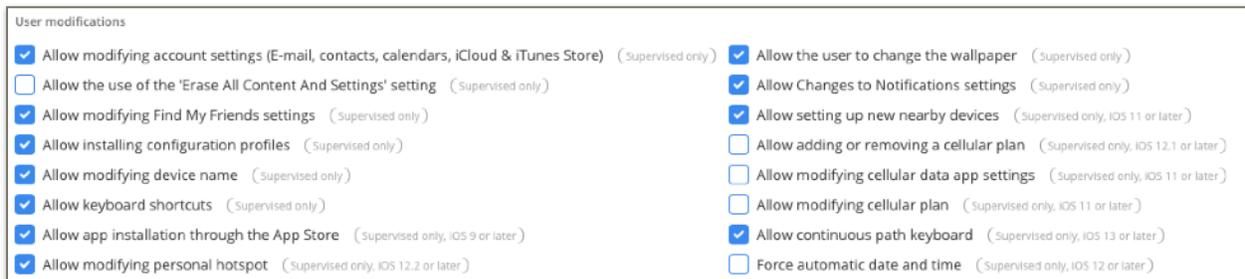
In the example above, the administrator has also unchecked the "Allow modifying cellular data app setting" option. This prevents the user from making changes to the apps that can use cellular data. Any app that can't use cellular data would have to run over WiFi. The Network Usage Rules payload will be used to determine which apps can use cellular data. The admin may elect to allow all apps to use cellular data as in the example below, or can set "Custom Data Usage" to allow only specific apps. For example, they might allow all apps to use cellular data except the YouTube app since a video app might consume a great deal of bandwidth.
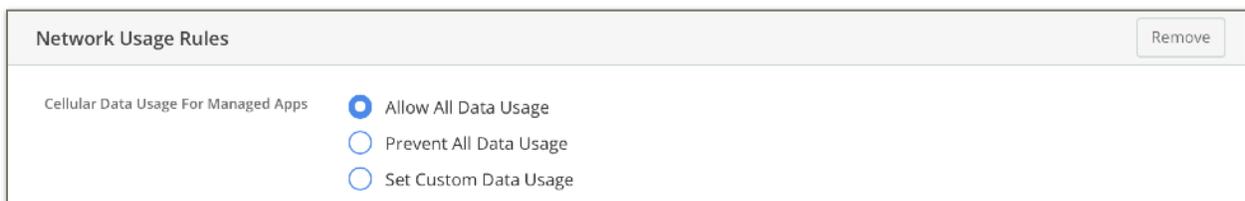
Click on the "Scope" option to choose the devices that need these settings. This profile could be scoped to the device models that are cellular-capable. It's OK if you accidentally push it to others -- it will have no effect on devices that don't have a cellular plan. Also, it's safe to push this profile to devices even before the cellular service has been activated because the "Refresh Cellular Plan" MDM command is not affected by these restriction settings. Save the profile once you've set your desired device scope.
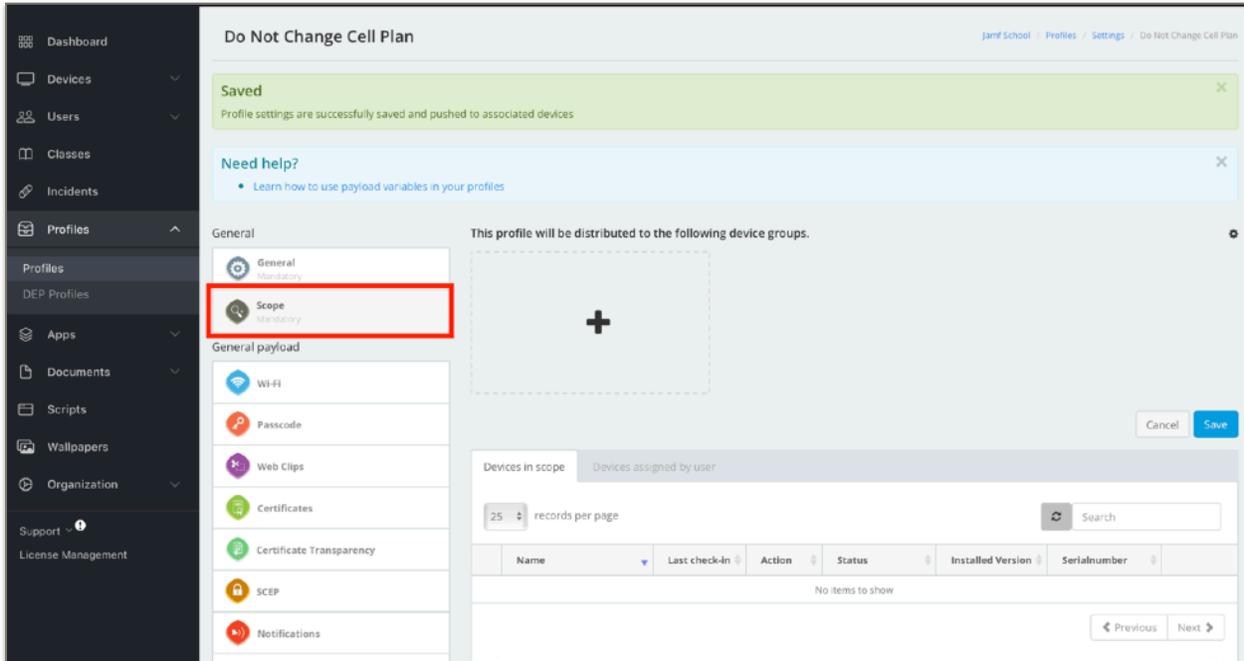
Restricting the user's ability to change cellular settings — Jamf Pro

We can create a restrictions configuration profile to ensure that users do not remove the cellular plan settings from their devices.

If you already have a standard restrictions profile for your devices, you may elect to edit it to add the cellular restrictions. Or, to create a new profile, go to "Devices > Configuration Profiles > New".
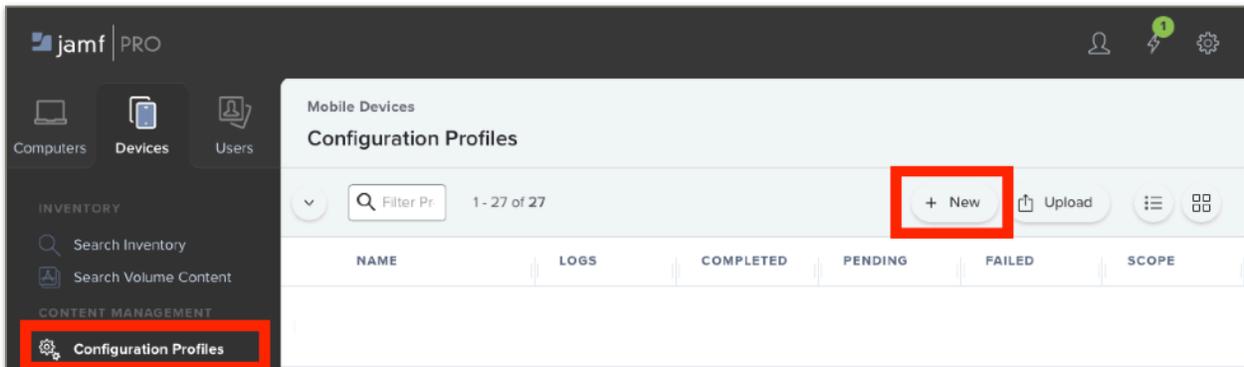
Give the profile a name in the General pane.
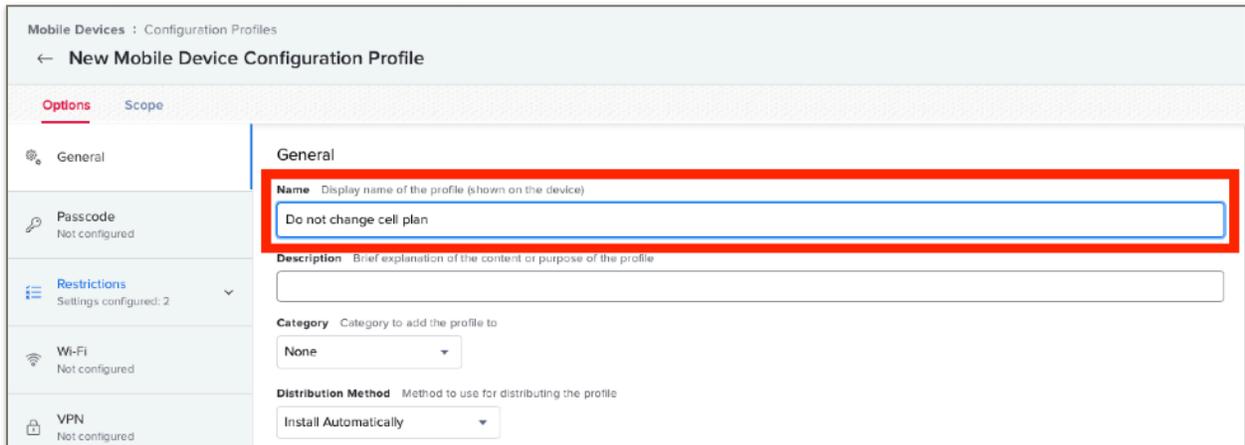
Next, switch to the "Restrictions > Functionality" pane and restrict "Modify cellular plan" and "Modify eSIM settings".
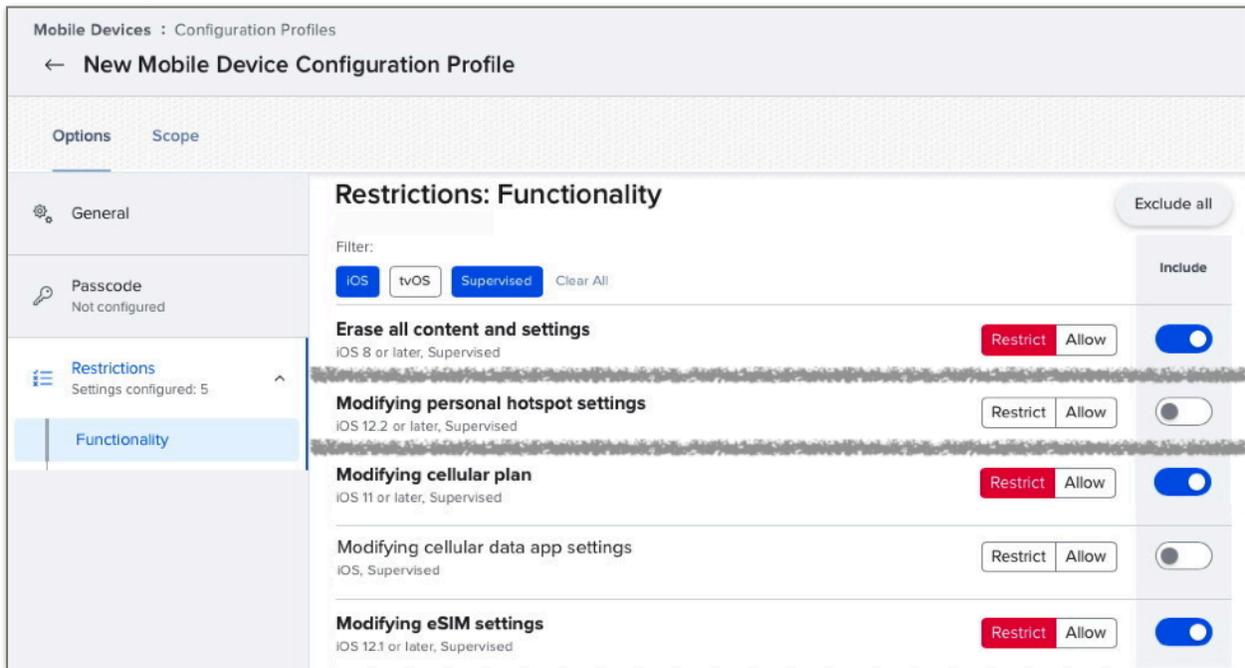
In the example shown, we are also preventing the user from erasing the device because if not done correctly, the eSIM can be deleted as well.

This example also places no restrictions on "Modifying cellular data app settings". This might be a good approach on a corporate device where we are allowing users to install things like YouTube or Netflix but encouraging them to turn off cellular data for these apps in favor of using WiFi. In education, we might choose to turn this restriction on, and also restrict students' ability to install their own apps from the App Store. Then the admin can specify which of the apps we're installing should use cellular data and which should not. These settings are managed in the "Network Usage Rules" payload.

The Hotspot restriction is another cellular-related option, though not specific to eSIM. This is usually unnecessary because the availability of this feature is typically managed by the carrier based on the cellular service plan purchased for the device.

Switch to the scope tab to select the devices that need these settings. This profile can be scoped to all mobile devices... it will have no effect on devices that do not have a cellular plan, or to a smart group with criteria of Mobile Carrier is not equal to "iPad" and is not equal to (no value). Save the profile once when you've completed the setup. The users will not be able to alter their cellular settings. It's safe to push this profile to devices even before the cellular service has been activated. The "Refresh Cellular Plan" MDM command is not affected by this setting.

Avoid auto-erase after a number of incorrect passcode attempts

Unless your organization has an information security policy that requires it, do not set the option in the passcode payload that will wipe a device after a certain number of failed passcode attempts as this will also delete the eSIM settings.

Erasing Content and Settings

Removing Content and settings from an eSIM device

iPad OS allows users to erase content and settings. If an eSIM is present on the device, iPadOS will offer two options. If the device is going to a new user but it will be on the same cellular plan, select the "Erase All & Keep Cellular Plans" option. If you're going to be disposing of the device, transferring ownership, no longer want the device to have cellular service, or need to switch to a new cellular account, select the "Erase All" option.

By default, end-users have access to the erase command on their iPad and may not understand that they may need to retain their cellular plan. For this reason, consider using a restrictions profile to prevent an end user from erasing their own device. If a device erase is ever needed, an administrator can use the MDM command instead.
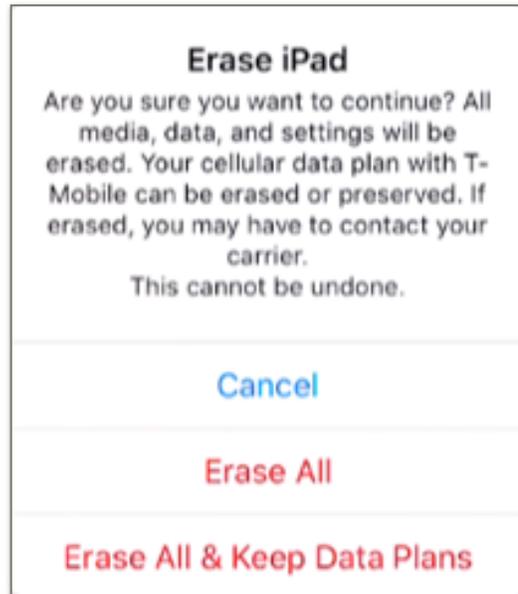
Sending the Device Wipe command to an eSIM device in Jamf School

To send a remote wipe command to a device (or to a series of devices) in Jamf School, check its box in the device listing and select Wipe Devices from the Advanced menu. In the resulting options menu, be sure that "Preserve Data Plan" is checked if you want the device to remain on your cellular service account.
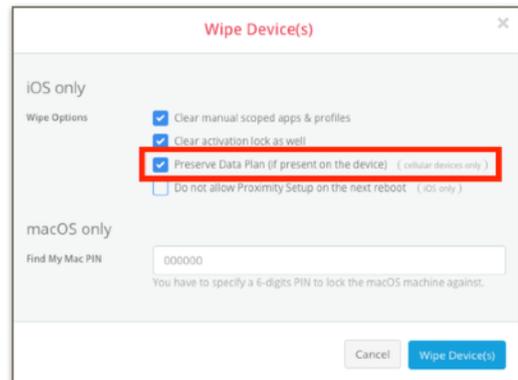
Sending the Device Wipe command to an eSIM device in Jamf Pro

If you're using Jamf Pro to wipe a device with a remote action, be sure to check the "Retain Cellular Data Plan" option unless you no longer want the device to have cell service with your carrier. This command can be sent to an individual device from the Management tab in its inventory detail page or as a mass-action to a group of devices in an Advanced Search or Mobile Device Group.
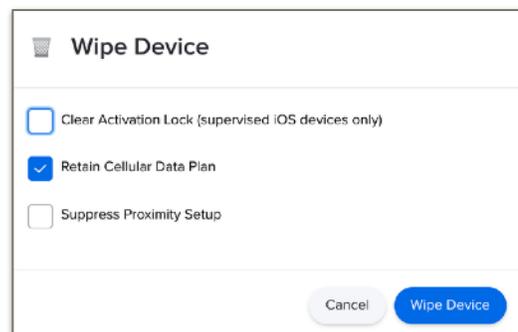
Bulk Activation Considerations

Apple's enrollment and app delivery systems can scale to handle huge demand surges, as can the cell carriers' device activation infrastructure. Your organization's wifi network and internet connection are more limited however, and so is the capacity of the cell tower covering your site. We should give some thought to what we're asking our networks to do when considering a device setup workflow.

Even if you're enrolling very large numbers of devices, they're typically being configured in batches. So in most real-world workflows, network demand required for MDM enrollment and cellular service activation is distributed over time. We won't expect to see too many problems. But downloading iPadOS updates and apps can require significant bandwidth, and an MDM will be busy negotiating device check-ins and Apple Push/App Store transactions during this period. We might have some issues if we try to activate cell service on too many devices at once, or while the devices are busy doing other things.

Examples:

- A school sent the refresh cellular command to 500 devices that had been enrolled via Automated Enrollment. It took an hour for the devices to activate their cell service. In this case, the network admin noticed that the wifi network and the school's connection to the Internet was saturated. The devices were downloading the many apps that the admin had scoped to the devices so they were competing for bandwidth.

- A Jamf admin pushed new versions of their company's in-house apps to 30,000 devices at the same time. A few cubes over, another admin was pushing the Refresh Cellular Plan command to some new devices she was setting up. She didn't know about the app installs and couldn't tell why her commands didn't seem to be going through. The admins found that both their management tasks and the app installations went much better when they broke their app installs into 5,000-device chunks with a few minutes break in-between.

- A group of IT staff members reserved a large conference room to use for their device setup project and recruited a team of assistants. Things went well at first but they ran into trouble after turning on a couple dozen devices. They discovered that the network administrator had placed a limit on the number of devices that could be connected to the conference room's wifi access point.

- An organization decided to switch cellular providers and sent the Refresh Cellular Plan command to all their devices at once so they would activate with the new carrier. The switchover took longer than expected and failed on some devices.

The main point here is that a setup workflow for hundreds of devices may need to include some extra time for downloads and processing. It's best to wait until data-intensive activities like OS/app updates are completed before sending the refresh cellular plan command and we shouldn't try to activate 1,000 devices all at once on the first try. We may have better success if we activate a few devices to start and then increase the device count on subsequent batches as we observe success.

The use of Apple Caching Service can dramatically reduce the load on your organization's internet connection when Apple OS and App installations are needed. Ref: *https://support.apple.com/guide/mac-help/what-is-content-caching-on-mac-mchl9388ba1b/mac*

Cellular-related Popup Notifications

The following message may be seen in iPadOS.

"Carrier Settings Update"

Carriers may occasionally ask Apple to adjust some cellular radio and network settings on cellular-capable devices after they've been purchased. You might see a prompt informing you that such an update is available as you're activating your iPads. Select the "Update" or "OK" option if you see this prompt. Ref: https://support.apple.com/en-us/HT201270

"Cellular Plan is Ready to be Installed"

Once your carrier has entered the IMEI and EIDs for your devices into their system, you might see a prompt on an iPad saying that it's ready to set up cellular data. You can activate the cellular plan on these devices if you're doing manual setups. But if you're configuring lots of devices and don't want to tap the activation by hand, disregard this message and instead use the "Refreshing Cellular Plan" mass-action command in Jamf School or Jamf Pro.

"No SIM Card Installed"

It's OK if you see this message on an eSIM device. It just means that in addition to the eSIM, there's also a slot for a physical SIM card and it's empty. Once the eSIM is downloaded, you will see that the device has cellular service via the eSIM in "Settings->General->About" or by looking for the vertical signal-strength bars at the top of the home screen. Ref: https://support.apple.com/en-us/HT201420

"Unable to Update Cellular Plan"

We've seen this when there was a content filter on the customer network that blocked access to the carrier's eSIM server URL. See the Troubleshooting section of this document for more details.

"Unable to Complete Cellular Plan Change"

This occurs when the MDM has sent the Refresh Cellular Plans to a device that is already activated. It won't hurt anything on the device if you accidentally send the command, but you should avoid doing so if a user already has the device so they aren't confused by the message.

"Cellular Plan Cannot Be Added; This code is no longer valid."

This happens if you send a "Refresh cellular plan" MDM command after removing the cellular settings on a previously activated eSIM device. The device's information is no longer active in the carrier's automated systems. You'll need to contact your carrier and give them the device's IMEI and EID numbers so they can re-enable the device in their eSIM servers. Once that's done, they may instruct you to restart the device. Then you should be able to re-activate the device's cellular service.

Troubleshooting

Cell Service is not activating after sending the Refresh Cellular Plan command

1. Ensure your carrier had added your device IMEI and EID numbers to their eSIM server.

2. Check for a typo in the eSIM Server URL you sent to the device(s). Ensure it matches the URL provided by your carrier and does not include a trailing "/".

3. Ensure device is turned on/charged.

4. Check that the device is on Wifi or has a tethered data connection so that it can communicate with Apple, Jamf, and your cell carrier.

5. A content filter (e.g., Cisco Umbrella, Lightspeed, etc.) on your network may be blocking access to your carrier's eSIM URL. In this case, you will see an "*Unable to Update Cellular Plan*" error message on the device when you push the refreshCellularPlan MDM command. To check, navigate to the carrier's eSIM Server URL in Safari. If you see a message saying that your content filter blocked the connection, contact your network administrator. If your network is allowing traffic to flow to the eSIM server, you will instead see a message stating that the "Connection Is Not Private". This warning is expected and indicates a successful test because eSIM servers use a private certificate trusted only for eSIM activation.

6. Perform the activation in a location where cellular service is available from your carrier.

7. Verify that there aren't any backlogged/pending MDM commands, macOS updates, or app installs.
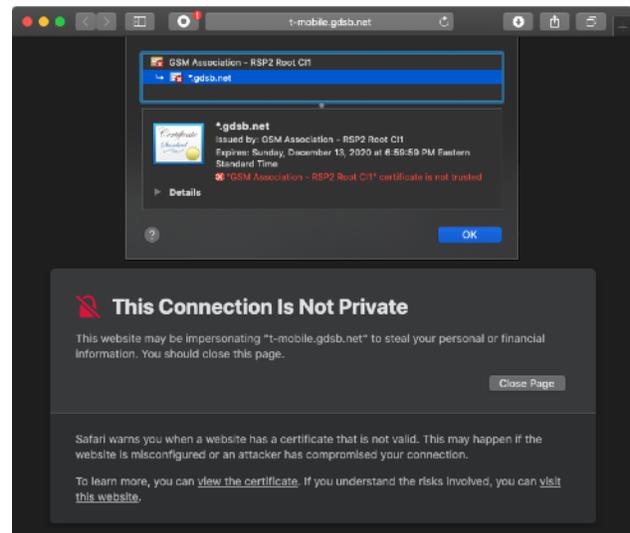
Notes

Example eSIM Server URLs ("SM-DP+" Servers) for use with "Refresh Cellular Plan"

Note that these are only examples. Carriers may change their eSIM Server URLs from time to time and may have different servers for different eSIM versions, service lines, or regions. You should use the URL provided by your carrier.

Do not include a trailing "/" when entering these URLs into Jamf.

Carrier	URL
Verizon	https://2.vzw.otgeuicc.com
AT&T	https://cust-001-v4-prod-atl2.gdsb.net
T-Mobile	https://t-mobile.gdsb.net

Switching Carriers

An iPad can have multiple eSIMs. When an iPad initializes its cellular radio, it will default to the most recently-provisioned eSIM. If you need to switch to a new carrier for a device, use the same "Refresh Cellular Plan" command that we previously discussed when explaining initial device setups. You may need to restart the device for the new eSIM to take effect.

Some Terms Related to eSIM iPad Provisioning

We've tried to avoid using excessive lingo in this document, but the following terms might come up when discussing eSIM iPads.

Cellular Networking

4G / 4G LTE "Fourth Generation/Long Term Evolution" is a mobile communications standard released in 2008 to improve speed and reliability. This is the most common cellular networking standard in use today.

5G "Fifth Generation" is a new mobile communications standard. Carriers and cellular device manufacturers are currently working on implementing 5G. It is anticipated the the significant speed improvement offered will lead to many new applications for mobile technology.

SIM A "Subscriber Identity Module" is a small plastic card that contains a chip to store the international mobile subscriber identity (IMSI) number and its key to used to identify and authenticate subscribers when they connect to a carrier network. They are usually specific to a particular carrier so changing service often requires a new SIM card.

eSIM An "embedded SIM" stores the same information as a physical SIM, but the data is written to memory within the device, eliminating the need for a carrier-specific physical SIM card.

EID The "Electronic Identifier Document" is a unique number that identifies an eSIM.

IMEI The "International Mobile Equipment Identity" number is used to identify a physical device to cellular networks. The number identifies the hardware and is not tied to any particular carrier or subscriber. The IMEI can be found on an iPad or iPhone in the Settings App—General—About. On an iPhone, you can access the information my simply dialing phones "*#06#". The IMEI is one of the values a cellular data carrier needs to provision an eSIM.

SM-DP+ "Subscription Manager - Data Preparation Plus" servers distribute the eSIM profiles needed to utilize a carrier's cellular data network. Data carriers will collect IMEI and EID numbers from subscribers and "provision" an eSIM for each device on their server. When you push an SM-DP+ URL to a device using the Refresh Cellular Plan MDM command, the device will contact the SM-DP+ server to download its eSIM profile. In this document, we have referred to these servers as "**eSIM Servers**".

Apple Technologies and Services

Apple Business Manager ("ABM") is accessed via a [web portal](#) and integrates with Jamf Products. It allows IT administrators to assign devices to Jamf for automated enrollment, to purchase apps and content, and to configure managed Apple IDs.

Apple School Manager ("ASM") is similar to Apple Business Manger and adds the ability to integrate with a Student Information System to support the Apple Classroom app. Ref: https://help.apple.com/deployment/education/

Apple Configurator 2 is a macOS application used to prepare iOS, iPadOS and tvOS devices for use. Apple Configurator connects to these devices via a USB connection and assists in the deployment of settings, apps, and other data. Apple Configurator is available from the [Apple App Store](#).

Automated Enrollment combines features of an Apple device management program, Apple's OSs, and Jamf to [automatically enroll](#) an organization's devices in management when during the Setup Assistant flow on a new device.

Hot Spot/Tethering is provided by a cellular device that shares its data connection with nearby devices, or by a network-connected Mac computer. A hot spot will act as an ad hoc wireless network on either Wi-Fi or BlueTooth PAN (Personal Area Network). Tethering allows data connections to be shared with another device via a cable and can be useful in the initial setup of new devices that do not yet have a configured Wi-Fi network.

Let Jamf be a part of your Apple education success.

Put this workflow in place and empower your students and educators with the best Apple has to offer.

Get Started