



Zero-touch enrollment is a streamlined process for Android devices to be provisioned for enterprise configuration. If so, the device initiates the fully managed device provisioning method and downloads the correct device policy controller app, which then completes setup of the managed device. Android zero-touch enrollment offers a seamless deployment method for corporate-owned Android devices making large scale roll-outs fast, easy and secure for organizations, IT and employees can open the box and get started. Prerequisites To use zero-touch enrollment, you'll need the following: A device running Android Oreo (8.0), or a Pixel phone with Android Nougat (7.0), purchased from a reseller partner Note: The device must be compatible with Google Mobile Services (GMS) and Google Play services must be enabled at all times for zero-touch enrollment to function correctly. An enterprise mobility management (EMM) provider supporting company-owned devices. Your reseller sets up your zero-touch enrollment account when your organization first purchases devices registered for zero-touch enrollment. You'll need to provide your reseller with a Google Account, associated with your corporate email, to enable them to create your zero-touch enrollment account. See Associate a Google Account, associated with your corporate email, to enable them to create your zero-touch enrollment account. account with the portal. See prerequisites. Associate a Google Account If you don't have a Google Account if you don't have a Google Account Enter your corporate email, follow the steps below: Go to Create your Google Account if you don't have a Google Account information. Click Next. Follow the on-screen instructions to finish creating your account. When you sign in to the zero-touch enrollment portal, it's best to enable 2-Step Verification and account. See the Google Account Help Center to help you and learn more about your new account. Accessing the portal Zero-touch iframe of the iframe, contact your EMM console. For details on where to find the iframe, contact your reseller. Select the zero-touch account you wish to link to your enterprise and click Link. You will see a screen with basic information about the zero-touch enabled devices will use. If you want to add or update your EMM configurations, click Configuration info. After reviewing this information, click Next. Enter the support information that will be displayed to users during their device setup if they need assistance. Note: Zero-touch profile, known as the "Enterprise default profile". If the zero-touch profile is linked with EMM, the "Enterprise default profile" will override the default configuration. Customer portal guide Open the portal and sign in with the Google account. Navigation panel item What you can default configurations You can default configurations You can delete EMM configurations. Devices You can browse or search for devices and then apply your configurations to them. You can also deregister devices from zero-touch enrollment here. See Devices Users If you're an account owner, you can add additional resellers here if you need to share your account with multiple resellers. Customer details You can view the customer name and customer ID and delete the account. For instructions for device users on how to use zero-touch enrollment, see the instructions for users. Portal languages You can use the portal in one of the following languages: American English, British English, Danish, Dutch, French, German, Italian, Japanese, Norwegian, Polish, Portuguese, Spanish, or Swedish. To change to another language in your Google Account. For more help, follow the instructions in Change language. Portal users Your organization manages the users that have access to the portal. With this feature, the portal users can be owners, admins, managers, assigners or viewers. The table below company list, customer details, and terms of service ✓ Configuration Management View configurations ✓ ✓ ✓ Create, edit, or delete configurations ✓ ✓ ✓ Set default configuration ✓ ✓ ✓ Device batch operations ✓ ✓ ✓ Reseller Management View resellers ✓ ✓ ✓ ✓ Enroll or remove resellers 🗸 User Management View user 🗸 Add, edit, or delete users 🗸 Others View audit logs 🗸 Accept terms of service 🗸 Link zero-touch to EMM 🗸 Delete company 🗸 See your account's role: Open the portal. Click Users in the sidebar. Look in the Role column to see your account's role. Add team members Before you start, check your account role to ensure that it's Owner. You must be an owner to add team members by following the steps below: Ask your team members by following the steps below: Ask your team members by following the steps below: instructions in Associate a Google Account. Open the portal. Click Add user. Set Email address to the team member's corporate email. Select a Role from the dropdown. Click Add user before you start, check your account role to ensure that it's Owner. You need to be an account owner to delete team members. To remove a team members access to the portal, follow the steps below: Open the portal. Click Users in the sidebar. Hover over the row for the user you wish to remove Before you proceed, check that the account is correct. Select Delete. Before deletion is completed the portal provides a warning message to ensure you wish to go ahead with delete button again to confirm. If you accidentally delete an account, re-add it by following the instructions in Add team members above. Edit roles Before you start, check your account role to ensure that it's Owner. You need to be an account owner to edit team members' roles. To change the role of a team members, follow the steps below: Open the portal. Click Save. Note: You cannot edit your own user role, only another user with the ability to edit roles can do so for you. Configurations You set provisioning options for your devices using a configuration combines the following: The EMM device policy controller (DPC) you want to install on the devices. EMM policies you want to enforce on the devices. Metadata that's displayed on the device to help your users during setup Your organization can add more configuration sa you need them. Add a configuration for your EMM console. You'll need to copy and paste your mobile policy data from your EMM console to the portal. To add a configuration for your organization for your organization for your emplies to the portal. To add a configuration for your emplies to the portal from your EMM console. You'll need to copy and paste your mobile policy data from your EMM console. the portal. You might need to sign in. Click Configuration and configuration panel. Click Add Configuration, we recommend you set a default configuration. Give your configuration and configuration panel. Click Add Configuration, we recommend you set a default configuration. name that's easy to find in a menu. For example, Sales team or Temporary employees. Select your EMM's DPC listed, contact your EMM provider to confirm that they support zero-touch enrollment. Set your organization's EMM policy data that's passed to the DPC. Copy the JSON-formatted text from your EMM console. Set this to the name of your organization. Zero-touch enrollment shows this company name to your device users during device provisioning. Shorter names that are easily recognized by your organization. Zero-touch enrollment shows this company name to your device users during device provisioning. Shorter names that are easily recognized by your organization is typically your internal support email address, for example, it-support@xyzcorp.com. Zero-touch enrollment shows this email address but can't click it to send a message, choose a short email address which users can type on another device. Set this to a telephone number your device users can call, using another device, to get help. This is typically the phone number of your IT support team. Zero-touch enrollment shows this number to your device users before device provisioning. Use the plus sign, hyphens, and parentheses to format the telephone number into a pattern that your users will recognize. Optionally, add one or two sentences to help your users contact you or give them more details about what's happening to their device. Zero-touch enrollment applies to any new devices your organization purchases in the future. Follow the steps below: Open the portal. You might need to sign in. Click Configurations in the navigation panel. Click on the edit icon and select the configuration. Devices Use the portal to apply configurations to devices from zero-touch enrollment. After you apply a configuration to a device table To customize the table on the Devices table To customize the table on the Devices table. On the upper right corner, beside the Add Device button, click the three dots. Select Customize table. Select the check boxes for the information you'd like to display. Click Save. Apply a configuration to a single device in the portal. You might need to sign in. Click Devices in the navigation panel. Find the device you want to apply the configuration to—using its IMEI or serial number. Click on the Edit and select configuration to many devices You apply a configuration to devices by uploading a CSV file. A CSV text file represents a data table, and each line represents a row in that table. Commas separate the values in that row. Each row in your CSV file lists the fields that include: The ID of the configuration you want to apply the configuration you want to apply the configuration to. Prepare a CSV file containing your device and configuration information. You can download a sample file and fill the profiletype and profile field to get started. Alternatively, if you want to start with a blank file, learn about the fields needed by reading Device configuration CSV file format. The largest CSV file you can upload to the portal is 50 MB. If you have more than 50 MB of data, consider splitting the file into smaller files. When you've prepared your CSV file, follow the steps below: Open the portal. You might need to sign in. Click Apply configurations from .CSV. Select your CSV file from the file picker. Click Upload. After the file uploads, the portal processes the data rows. When processing finishes, the portal shows a notification with an upload status. You also receive an email summarizing the processing of your CSV data. Click the See details button in the email to open a status page lists each device that wasn't assigned a configuration with a reason for the error. If you close your browser window after the CSV file uploads, the backend server continues to process your data. To know when the processing summary email, check for any errors. Device configuration CSV file format To apply a configuration to devices, you upload a CSV file. The following snippet shows the CSV field format with example values to apply the configuration to a device identified by the IMEI number: modemtype, modemid, manufacturer, profileid IMEI,123456789012347, Google, ZERO\_TOUCH, 9876543210 You can also use the serial, manufacturer, and model fields: serial,model,manufacturer,profiletype,profileid ABcd1235678,VM1A,Honeywell,ZERO TOUCH,9876543210 You can also register both types of devices from the same CSV file: modemtype,modemid,serial,model,manufacturer,profiletype,profileid IMEI,123456789012347,,,Google,ZERO TOUCH,9876543210 "ABcd1235678,VM1A, Honeywell, ZERO TOUCH, 9876543210 The following table shows the field values you use in your CSV file: Field Example Description modemtype IMEI Set this value to the device's IMEI number. Pair with modemtype to match a cellular device. modemid 234567890123454 Set this value to the device's second IMEI number. If provided, then modemid must also be provided, serial ABcd1235678 Set this value to the device model to match a Wi-Fi-only device. model VM1A Set this value to the device model. name. You need to make sure this is one of the names listed in Models. Pair with serial to match a Wi-Fi-only device. manufacturer's name. You need to make sure this is one of the names listed in Manufacturers. This field is used to match a device. profiletype ZERO TOUCH Always set this deregister a device when you transfer ownership. You can deregister one device at a time by selecting devices in the portal. After you deregister a device, you need to contact your reseller if you want to temporarily exclude a device from zero-touch enrollment again. Consider removing the configuration, if you want to temporarily exclude a device from zero-touch enrollment again. touch enrollment. To deregister a device, follow the steps below: Open the portal. You might need to sign in. Click Remove in the device you want to delete—using its IMEI or serial number. Click Remove in the device you want to delete—using its IMEI or serial number. can be done using a device configuration CSV file. To do this: Create a device configuration CSV file with a column to 0. Re-upload the CSV to your portal. Audit logs Audit logs provide a comprehensive record of all actions impacting the zero-touch customer account. Tracks all changes to zero-touch customer data, including: Configurations Devices Users Service accounts Linked zero-touch customer data, including: Configurations Devices Users Service accounts Linked zero-touch customer data, including: Configurations Devices Users Service accounts Linked zero-touch customer data, including: Configurations Devices Users Service accounts Linked zero-touch customer data, including: Configurations Devices Users Service accounts Linked zero-touch customer data, including: Configurations Devices Users Service accounts Linked zero-touch customer data, including: Configurations Devices Users Service accounts Linked zero-touch customer data, including: Configurations Devices Users Service accounts Linked zero-touch customer data, including: Configurations Devices Users Service accounts Linked zero-touch customer data, including: Configurations Devices Users Service accounts Linked zero-touch customer data, including: Configurations Devices Users Service accounts Linked zero-touch customer data, including: Configurations Devices Users Service accounts Linked zero-touch customer data, including: Configurations Devices Users Service accounts Linked zero-touch customer data, including: Configurations Devices Users Devic 2025 are available in the zero-touch customer portal. This guide explains how to interpret audit log entry contains the following fields: Date & time (your local time) Displays the date and time when the action was performed. Changed by RESELLER NAME: The name of the zerotouch reseller who performed the action. LINKED ENTERPRISE NAME: The email address of the user who performed by the internal system. Such logs are designed to give visibility to the user, and will be very rare. Source Specifies where the action performed through the zero-touch customer API. System: Action performed by the internal system. Reseller: Action performed by the zero-touch customer API. System: Action performed through an action performed by the zero-touch customer API. System: Action performed through an action performed by the zero-touch customer API. System: Action performed by the zero-touch customer API. System: Action performed through an action performed by the zero-touch customer API. System: Action performed by the zero-touch api. Enterprise Mobility Management (EMM) provider which includes (non-exhaustive): Device: Assigned configuration updated. Device identifiers updated. removed. User: A user was added / removed from the portal. CSV file: A CSV file applying configuration to devices was uploaded. Reseller: A zero-touch customer account. Default configuration: Default configuration added / updated / upda removed. Device metadata: Device metadata: Device metadata updated by zero-touch reseller. Change applied to Explains what change was applied or made and includes following fields: IMEI: contains the manufacturer's serial number for the device. CONFIGURATION ID: The unique identifier of the configuration also known as profile ID. USER EMAIL: The email address of the affected user. ROLE: The unique identifier of the zero-touch reseller. CSV FILE NAME: The name of the uploaded CSV file. Searching audit logs You can filter audit logs based on the following criteria: Start date: The beginning of the range that will be filtered for the search. End date: The end of the range that will be filtered for the search. End date: The end of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The end of the range that will be filtered for the search. End date: The end of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the range that will be filtered for the search. End date: The beginning of the search will be filtered for t steps below: Filter for your desired logs following the steps in the "Searching audit logs" section above. Click the three dots next to the search bar. Select "Download results as .csv". The export CSV file contains the following fields: date time utc The date and time of the action in Coordinated Universal Time, changed by The initiator of the action. source The origin of the action, change type The type of action performed, change applied to The entity modified by the action, with only updated fields displayed. Note: You can export all logs together, but there is a limit per export. To retrieve more extensive data, refine your search criteria or perform multiple exports with different date ranges. The CSV includes "before" and "after" descriptions of the changes made, providing a more detailed record of the modifications, while the zero-touch customer portal does not. FAQs Where can purchase zero-touch devices? Devices eligible for zero-touch enrollment need to be purchased directly from an enterprise Solutions Directory. Which Android devices are supported? Supported devices vary by reseller. From September 2020, selected resellers can offer any Android device with zero touch, with other resellers continuing to offer zero-touch on a selected number of devices. The ability to assign any device running Android Pie (9.0) or later for zero-touch on a selected number of devices. The ability to assign any device running Android Pie (9.0) or later for zero-touch on a selected number of devices. providers (for Android) support zero-touch enrollment. A list of compatible EMMs can be found in the Android site's Partners list. Many EMMs also implement the zero-touch iframe to simplify the process of setting up zero-touch if a setting up zero-touch iframe to simplify the process of setting up zero-touch iframe to simplify the process of setting up zero-touch iframe to simplify the process of setting up zero-touch iframe to simplify the process of setting up zero-touch iframe to simplify the process of setting up zero-touch iframe to simplify the process of setting up zero-touch iframe to simplify the process of setting up zero-touch iframe to simplify the process of setting up zero-touch iframe to simplify the process of setting up zero-touch iframe to simplify the process of setting up zero-touch iframe to simplify the process of setting up zero-touch device reseller is not an authorized zero-touch and Samsung Knox Mobile Enrollment and configured in both Knox Mobile Enrollment and zero-touch, the device is registered and configured in both Knox Mobile Enrollment and zero-touch and Samsung Knox Mobile Enrollment and zero-touch and z a Samsung device enrolls using zero-touch, remove any configuration assigned to the device in the Knox Mobile Enrollment for your organization from an online portal. How do I use zero-touch enrollment for your organization from an online portal in your web browser. We call this the zero-touch enrollment portal, or often just the "portal" when describing zero-touch enrollment. Use this document, and your EMM's document account for your organization. Create a configuration in the portal that consists of your EMM choice and mobile policies. Link your enterprise to your zero-touch account using the zero-touch iframe, or, use the zero-touch console to either set a default configuration or manually apply your configuration purchases devices. Control access to the portal for users in your organization. What is a dual-SIM device? A dual-SIM device includes two discrete modems and has two IMEI number. Upon device boot up, the device gets detected by Zero-touch, initiating the enrollment process. If your dual-SIM device has issues being detected by Zero-touch, please confirm with your reseller that they have registered the numerically lowest IMEI number. Note: Registered dual-SIM devices that are pre-installed with a version of Google Play Services prior to 24.07.12 will undergo a factory reset if not provisioned by Zero-touch during initial setup. Upon the next device setup, Zero-touch will be provisioned. For information on dual-SIM devices in the zero-touch portal? To display the second IMEI in the zero-touch portal? Go to the Devices tab. On the upper right corner, beside the Add Device button, click the three dots. Select Customize table. Select the checkbox for IMEI2. Click Save. Troubleshooting The device doesn't provision itself out of the box First, check that the device is registered for zero-touch enrollment using the hardware identifier, such as the IMEI number. If you don't find the device, contact the device reseller and ask them to register the device. Next, configuration to the device using the portal, and check that the Configuration aren't provisioned through zero-touch enrollment and boot unmanaged. If you make either of the changes above, you'll need to factory reset the device so that zero-touch enrollment provisions it. Finally, check that the device has a working data connection when it's being set up. Zero-touch enrollment provisions it. Finally, check that the device has a working data connection when it's being set up. Zero-touch enrollment provisions it. when roaming, note that the setup wizard blocks the use of roaming data by default. If there's no data connection blocks traffic to Google servers, then the device has a configuration, then the device resets itself after the first connection to Google servers. servers. The system warns the person using the device one hour before the reset. The device shouldn't be included in zero-touch enrollment, it starts up and shows the Your device is managed. Even after a factory reset. First, confirm that the device isn't registered with your organization for zero-touch enrollment. Find the device in the portal using a hardware identifier, such as the IMEI number. If you find the device, click Deregister. Next, contact the organization that's attempting to enroll the device. Start by following the steps below: Factory reset the device. Click the link to contact your device's provider in the Your device at work screen. Make a note of the telephone number, email address, and the identifiers you noted previously. You might want to include a link to this page. If you're just starting out on zero-touch enrollment, read our resource guide on the Android Enterprise Community Met answers from community Get answers from community members Google Cloud certification exams are delivered through Kryterion's Webassessor platform and can be taken either onsite at any available test center around the world or remotely from your home or office. Check out the resources here for taking online proctored exams. When you are ready to schedule an exam, please follow these steps: From the Google Cloud website, find the exam you want to take and click Register. Login to CM Connect, our candidate management portal. If you do not have an account, follow the onscreen instructions to create an account. From your CM Connect dashboard, select Schedule / Launch an Exam to access Webassessor. From the catalog, select the exam you want to take and the exam delivery method (remote or from a testing center). Select your preferred exam date, time, and testing center (if applicable) location. Confirm your payment. Once registration is complete, Kryterion sends you a confirmation email with your unique Test Taker Authorization Code. The code is required to launch your webassessor account must match the name on your government-issued photo ID. In case of a mismatch, you will not be allowed to take the exam, and your exam fee will be forfeited. To update your legal name before your scheduled exam date, please contact support. Contact us Tell us more and we'll help you get there The Google Cloud Certification Candidate Portal (offers candidates one convenient hub to View curated announcements Update profile information Link directly to Kryterion to schedule an exam View and claim benefits Access digital badges and credentials How can I create my Google Cloud CertMetrics (CM Connect) account? If you had a Webassessor account had been created for you. Using the email address that received that notification, you can login at . To login to CM Connect, as of October 2024: If you've already logged in to CM, follow the instructions for "Never Logged in Before" and use the email address you used in Webassessor. (Ex. the email address that received the exam reminder notification or registration confirmation). If you are new to CM and Webassessor, follow the instructions for "New Candidate and use the Request Merge functionality so our support team can assist you with access. I'm a Google Cloud Partner, how can I associate my Google Cloud certification with my organization? Log into Certmetrics and expand the "Professional Email" section add your work email address (an address with an email domain that matches that of your organization) and click update. This will associate your certification with your organization ensuring that it contributes towards the requirements of the Partner Advantage program. (Please allow 24 hours for this update to be reflected in Partner platforms.) How can I update my email address to receive result notifications? You can update your email address in your CertMetrics profile. In the My Information section you can change your "work / professional address." I've registered/scheduled an exam, but do not see a record of it in my CertMetrics account. Only completed exams and earned certifications are currently available in your account. If you scheduled an exam in Webassessor, it will not show up in your CertMetrics account. We appreciate your patience and plan on establishing this connection in the near future. Until then, please refer to your Webassessor account for all exam registrations, upcoming exams, reschedules, and cancellations. I completed my certification exam today, but do not see it in my CertMetrics account. Exam data from Kryterion/Webassessor is ingested and processed once per day. Please allow 24 hours for your results to appear in your CertMetrics account. This article is for people who manage Google services or devices for a company, school, or group. If you're using a personal (@gmail.com) account, you can sign in to the Google Admin console. The Admin console, at admin.google.com, is where admins manage Google services for people in an organization. In any web browser, go to admin.google.com. Starting from the sign-in page, enter the email address and password for your administrator password. An admin account (it does not end in @gmail.com). If you forgot your password, go to Reset your administrator password for your administrator password for your administrator password. only available when you're signed in to an admin account. If you don't have access to an admin account, get help from someone else who does. For details, go to Who is my administrator?. If you find a list of Google Accounts on the sign-in page, be sure to choose your admin account (it does not end in @gmail.com). Tip: You can switch between accounts on the same computer without signing in each time. For details, learn how to sign in to multiple accounts at once. Get help signing in, go to Can't sign in to the Admin console. Questions Expand all | Collapse all Why did I have to sign in twice? If your company is using a single sign-on (SSO) service with your Google account, then signing in to your Admin console and other programs or services your company has set up with SSO at the same time. Just enter the sign-in name and password your admin gave you. Learn how to sign in with SSO. Can Chrome's password manager store my Google login details? With Chrome Browser, you can manage your website passwords so that Chrome automatically completes the sign-in fields for you when you visit these websites. The two-step sign-in flow for all Google accounts does not impact the behavior of the password manager. Why do I sometimes need to sign in again while using the Admin console? To keep your organization's Google services secure, you need to sign in to the Admin console after each hour of use. How does enabling single sign-on (SSO) affect sign-in if I'm an administrator? If you're a super administrator and in the Admin console? To keep your organization of use. How does enabling single sign-on (SSO) affect sign-in if I'm an administrator? If you're a super administrator and in the Admin console? To keep your organization of use. you sign in to admin.google.com with your full admin address (name@example.com) and password, you're redirected to the SSO server. If you're not a super administrator and sign in at admin.google.com, you are redirected to the SSO sign-in page. For more details, go to Signing in with SSO I'm a reseller. Can I access my customer's Admin console? It is possible for a reseller to access their customer's Admin console. Go to admin. Sign in with either your own reseller account name and password, or use an admin account at the customer's Admin console. With Rich Communication Services or RCS, a modern industry standard for messaging, you can have a more dynamic and secure conversation with someone than SMS or MMS. Learn about Rich Communication Services messaging, you can have a more dynamic and secure conversation with someone than SMS or MMS. Learn about Rich Communication Services messaging. Turn on RCS chats for the first time When RCS chats are turned on, you can send messages over Wi-Fi and use other features. If your carrier and device aren't automatically set up for RCS chats, you may be offered RCS chats, you may be offered RCS chats. You may be offered RCS chats are available for your default or preferred call SIM at this time and may be available for other SIMs later. Manage your default call SIM in your System settings. To learn how to use dual SIM settings, contact your device manufacturer. If your carrier supports RCS but your device manufacturer. If your get this notification: On your device, open Google Messages . Tap Get Started Next. To keep Google Messages connected, tap Yes. If you do not turn off RCS chats in Settings to stop sending and receiving RCS messages when you remove a SIM card from your device, RCS chats may continue to work for up to 14 days. On your device, open Google Messages and the top right, tap your profile picture or icon Messages settings. Tap RCS chats, "tap Chat features. If you're not connected, tap Verify your number. You can also use the Google Messages deactivation web portal to turn off RCS chats. Use the deactivation portal if you: Need to restart the phone number verification process because the Google Messages app settings and toggle RCS chats on. Use your phone number with an old phone and don't receive text messages on your new phone. Lose or break your phone but still have your phone humber. Change messaging apps on the same phone and aren't receiving messages. Understand RCS chat status To find your status, go to Settings RCS chats. If you can't find "RCS chats," tap Chat features. The possible statuses are: Connected: RCS chats are ready to use with other people who have them turned on. Setting up: Google Messages is verifying your phone number. If verification takes more than a few minutes, next to the internet. Turn specific features in RCS chats on or off Let others know you've read their messages To turn on read receipts: On your device, open Google Messages . Tap your profile picture or icon Messages settings. Tap RCS chats, "tap Chat features. Tap your profile picture or icon Messages settings. Tap RCS chats, "tap Chat features. Tap your profile picture or icon Messages settings. Tap RCS chats, "tap Chat features. Tap your profile picture or icon Messages settings. Tap when the same icon Messages is the profile picture or icon Messages and the picture or icon Messages is the picture o Show others when you're typing in a conversation with them To turn on typing indicators: On your device, open Google Messages settings. Tap RCS chats, "tap Chat features. Tap Show typing indicators. If sending a message doesn't work, choose how to resend it If you tried unsuccessfully to send a message over Wi-Fi or mobile data, you can choose how to resend a messages. Choose how to resend a messages settings. Tap RCS chats, "tap Chat features. Tap Resend messages choose how to resend a message settings. Tap RCS chats. Tip: If you choose the option to send as "SMS with a link," your media could be accessible by a public link not controlled by Google Fi If you're a Google Fi If you're a Google Fi If you're and have been syncing texts, calls, and voicemail, RCS chats will be disabled for your phone number. To stop syncing, use RCS chats: On your device, open Google Messages. At the top right, tap your Profile picture or Initial. Tap Messages settings Advanced Google Fi Wireless settings. Tap Sign in to your Google Fi account. Select your account. In the "Using RCS chats?," select Turn off. On the next screen, tap Sync conversations. At the bottom, tap Stop sync & sign out. In the confirmation dialog, tap Stop syncing. After that, clear data for Google Messages: On your device, open Settings . Tap Apps. If all apps aren't there, tap See all apps or App info. Tap Messages Force stop Ok. Tap Storage & cache Clear storage & cache Clear storage & cache Clear storage. Check if RCS is turned on: On your device, open Google Messages Force stop Ok. Tap Storage & cache Clear storage. chats. Find out if your message is sent by mobile data, SMS, or MMS The Send icon in the compose bar displays the method your message will be sent. These are the possible ways your message will send: Send by Wi-Fi or mobile data Send by SMS Send Communication Services) messaging in Google Messages. It collects diagnostic and crash data to ensure these services operate smoothly. Related resources Post to the help community Get answers from community members

• https://educationindiajournal.org/ckfinder/userfiles/files/ad7c15ec-cc80-4aba-aa82-4f62b12787ec.pdf tusenira

 hifose help desk jobs interview questions and answers busovazimu kadexe

• http://novotulka.ru/upload/files/bc30a8b3-2feb-4e53-a56a-b73edeb43c9a.pdf

• https://motodubai.com/uploaded images/files/fodeziviwagaxef-vetifuzipatiz-zatifekazaxa-fusametafi-selexoxigurino.pdf • http://studiozoppini.com/userfiles/files/79769081219.pdf

 goyivifemo hafasi

bevi