Continue

Cmo podemos mejorar esta pgina? 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. 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 arent automatically set up for RCS chats, you may be offered RCS chats. You might be asked to provide your phone number. Important: You may occasionally receive a text from Jibe Mobile from Google to verify your phone number. 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 isnt automatically set up for RCS chats, you may get a notification to "Do more with Google Messages." If you get this notification: On your device, open Google Messages . Tap Get Started Next. To keep Google Messages connected, tap Yes. If you can't turn on RCS chats, learn how to troubleshoot. Turn RCS chats on or off Important: 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 . At the top right, tap your profile picture or icon Messages settings. Tap RCS chats. Turn RCS chats on or off. Tips: If you can't find "RCS chats," tap Chat features. If youre 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 shows "Trying to verify" for some time. Tip: After you use the deactivation portal, go back into 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 number. 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 status, tap Retry. Disconnected: RCS chats are temporarily unavailable. Check that you're connected to the internet. Turn specific features in RCS chats on or offLet 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. Tip: If you can't find "RCS chats," tap Chat features. Tap Send read receipts. To find out when others have read your message, they must turn on read receipts in Settings.Show others when you're typing in a conversation with them To turn on typing indicators: On your device, open Google Messages . Tap your profile picture or icon Messages settings. Tap RCS chats. Tip: If you can't find "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 message: On your device, open Google Messages . Tap your profile picture or icon Messages settings. Tap RCS chats. Tip: If you can't find "RCS chats," tap Chat features. Tap Resend messages. Choose how to resend a message. Important: 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. Syncing with Google Fi If youre a Google Fi user 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. Check if RCS is turned on: On your device, open Google Messages . At the top right, tap your Profile picture or Initial. Tap Messages settings RCS Chats Turn on RCS 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 messages will send: Send by Wi-Fi or mobile data Send by SMS Send by MMS About Carrier Services Carrier Services provides services to support RCS (Rich 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 Zero-touch enrollment is a streamlined process for Android devices to be provisioned for enterprise management. On first boot, devices check to see if theyve been assigned an 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. Zero-touch makes it simple to configure devices online and have them shipped with enforced management so employees can open the box and get started. Prerequisites To use zero-touch enrollment, youll need the following: A device running Android Pie (9.0) or later, a compatible 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 A zero-touch account created by an authorized zero-touch reseller partner Get started Start by purchasing zero-touch enrollment 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 below. Don't use your personal Gmail account with the portal. See prerequisites. Associate a Google Account If you don't have a Google Account associated with your corporate email, follow the steps below: Go to Create your Google Account. Enter your name. Set Your email address to your corporate email. Don't click Create a new Gmail address instead. Complete the remaining 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 on an account like this that's used for administrative purposes. 2-step verification adds an extra layer of security to your account. See the Google Account Help Center to help you and learn more about your new account.Accessing the portal Zero-touch iframe Open the zero-touch iframe in your EMM console. For details on where to find the iframe, contact your EMM provider. On the landing page of the iframe, click Next. Log in with the Google account you provided to 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 configuration that your 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 profiles, including newly registered devices by resellers, are automatically configured with the enterprise 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 portaland sign in with the Google account. Navigation panel item What you can do with this Configurations You can create, edit and delete EMM configurations here. You can also set a default configuration for any devices added to zero-touch enrollment going forward. See 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 youre an account owner, you can add, edit, or delete users to manage portal access for your organization. Resellers 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. Note: Once the account is deleted, you will need to reach out to the reseller to create a new 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, update the preferred 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 compares the capabilities of each role: Role capabilities Portal tasks Owner Admin Manager Assigner Viewer View company list, customer details, and terms of service Configuration Management View configurations Create, edit, or delete configurations Set default configuration Device Management View devices Assign or unassign configuration Remove devices 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 Follow the steps below to check 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. Give portal access to new team members by following the steps below: Ask your team member to associate a Google Account with their corporate email. Your team member can follow the instructions in Associate a Google Account. Open the portal. Click Users in the sidebar. Click Add user. Set Email address to the team member's corporate email. Select a Role from the dropdown. Click Add. The portal doesn't notify your team members that they have access so you must remember to inform them yourself. Delete team members 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 member's 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 deletion. You must click the 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 member, follow the steps below: Open the portal. Click Users in the sidebar. Click Edit for the account you want to change. Select a Role from the dropdown. 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. Each 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 configurations as you need them. Add a configuration Before you add a configuration, check that you have access to your EMM console. Youll need to copy and paste your mobile policy data from your EMM console to the portal. To add a configuration for your organization's devices, follow the steps below: Open the portal. You might need to sign in. Click Configurations in the navigation panel. ClickAddConfiguration. Use the notes below to help you complete the new configuration panel. Once you've created a configuration, we recommend you set a default configuration. Give your configuration a name that describes its purpose. Choose a short, descriptive name that's easy to find in a menu. For example, Sales team or Temporary employees. Select your EMM's DPC app. If you don't see 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's employees work best. Set this to an email address your device users can contact to get help. This is typically your internal support email address, for example, it-support@xyzcorp.com. Zero-touch enrollment shows this email address to device users before device provisioning. Because device users can see the 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 whats happening to their device. Zero-touch enrollment shows this message before the device is provisioned. Assign a default configuration Choose a default configuration that 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 you want applied to new devices in the Default configuration panel. Click Save. Note:If the zero-touch account is linked with EMM, the "Enterprise default profile" will override the default configuration. Devices Use the portal to apply configurations to devices or deregister devices from zero-touch enrollment. After you apply a configuration to a device, the device automatically provisions itself on first boot, or next factory reset. Customize the Devices table To customize the table on the Devices tab: Go to the Devices tab. On the upper right corner, beside the Add Device button, click the three dots. Select Customize table. Select the check boxes for the information youd like to display. Click Save. Apply a configuration to a single device You can apply a configuration one device at a time by selecting devices in the portal. Follow the steps below: Open the portal. You might need to sign in. Click Devices in the navigation panel. Find the device you want to apply the configuration tousing its IMEI or serial number. Click on the Edit and select configuration you want to apply or select None to temporarily remove the device from zero-touch enrollment. Click Save. Apply a 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. A hardware identifier of the device 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 profileid 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 Devices in the navigation panel. Click More in the Devices table header. 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. The 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 portal finishes processing your data, check your email inbox for the status email. When you receive 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,profiletype,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 IMEI using uppercase characters. Pair with modemid to match a cellular device. modemid 123456789012347 Set this value to the devices IMEI number. Pair with modemtype to match a cellular device. modemid2 234567890123454 Set this value to the devices second IMEI number. If provided, then modemid must also be provided. serial ABcd1235678 Set this value to the device's case-sensitive serial number. Pair with 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 Google Always set this value to the device manufacturers 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 value to ZERO_TOUCH using uppercase characters. profileid 54321 Always set this value to the numeric ID of the configuration you want to apply to the device. To see the ID for a configuration, check that the table's ID column in the Configurations page. Deregister a device You can deregister devices from zero-touch enrollment. You might need to 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 register the device into zero-touch enrollment again. Consider removing the configuration, if you want to temporarily exclude a device from zero-touch enrollment. To deregister a device, follow the steps below: Open the portal. You might need to sign in. Click Devices in the navigation panel. Find the device you want to deleteusing its IMEI or serial number. Click Remove in the device row. Click Remove in the confirmation panel. Bulk deregister devices Deregistering multiple devices in bulk can be done using a device configuration CSV file. To do this: Create a device configuration CSV file including every device you wish to deregister. Replace the 'profileid' column in this CSV file with a column titled 'owner', and set the values in this 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 resellers Terms of service CSV file uploads Linked EMM account Important: For privacy reasons, audit logs are retained for a maximum of one year. Only logs after March 2025 are available in the zero-touch customer portal. This guide explains how to interpret audit logs and utilize their features. Understanding audit log fields Each 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 zero-touch reseller who performed the action. LINKED ENTERPRISE NAME: The name of the enterprise account associated with the action. USER EMAIL: The email address of the user who performed the action. System: Indicates that the action was 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 originated. Customer portal: Action performed through the zero-touch customer portal. Customer API: Action performed through the zero-touch customer API. System: Action performed by the internal system. Reseller: Action performed by the zero-touch reseller. EMM provider: Action performed through an Enterprise Mobility Management (EMM) provider which includes zero-touch iframe. Change type Describes the nature of the action which includes (non-exhaustive): Device: Assigned configuration updated. Device identifiers updated. Device added to / removed from the zero-touch customer account. Configurations: Configuration created / modified / removed. User: A user was added / removed from the portal. CSV file: A CSV file applying configurations to devices was uploaded. Reseller: A zero-touch reseller was removed from the zero-touch customer account. A zero-touch reseller was enrolled to the zero-touch customer account. Default configuration: Default configuration added / updated / removed. 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 GSM network identity number for the device. SERIAL NUMBER: 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 user's role within the zero-touch customer account. RESELLER NAME: The name of the zero-touch reseller. RESELLER ID: 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. IMEI or serial number: Search for logs related to a specific device. Exporting audit logs To export audit logs as a CSV file, follow the 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. state_before_change The entity's state prior to the action, with only updated fields displayed. state_after_change The entity's state following 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 I purchase zero-touch devices? Devices eligible for zero-touch enrollment need to be purchased directly from an enterprise reseller or Google partner and not through a consumer store. Reseller partners are listed in Android's 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 enrollment will expand to all resellers by the end of 2020. Which EMMs support zero-touch enrollment? Most EMM 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 devices after you purchase them from a reseller. To see if this feature is available, contact your EMM provider. What if my device reseller is not an authorized zero-touch reseller? What if my device is registered with zero-touch and Samsung Knox Mobile Enrollment? If a device is registered and configured in both Knox Mobile Enrollment and zero-touch, the device will enroll using Knox Mobile Enrollment and apply the configuration defined in that service. To ensure that a Samsung device enrolls using zero-touch, remove any configuration assigned to the device in the Knox Mobile Enrollment portal. How do I use zero-touch enrollment? You manage 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 EMMs documentation, to help you complete the following steps: Purchase your devices from a reseller who sets up a zero-touch enrollment 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 to a range of devices . You can also use the portal to: Activate and deactivate the resellers from whom your organization 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 numbers. Its recommended for the resellers to register dual-SIM devices with the numerically lowest 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 issues and their resolutions regarding zero-touch devices, please read known issues. How can I view the second IMEI for 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 doesnt provision itself out of the box First, check that the device is registered for zero-touch enrollment using the portal. Find the device using the hardware identifier, such as the IMEI number. If you dont find the device, contact the device reseller and ask them to register the device. Next, confirm that you applied a configuration to the device. Find the device using the portal, and check that the Configuration column of the table isnt listed as No config. Devices without a configuration arent provisioned through zero-touch enrollment and boot unmanaged. If you make either of the changes above, youll 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 needs a connection to Google servers. The connection can be ethernet, Wi-Fi, or cellular data. If you're using cellular data when roaming, note that the setup wizard blocks the use of roaming data by default. If there's no data connection, or if the connection blocks traffic to Google servers, then the zero-touch enrollment flow is skipped. If zero-touch enrollment is skipped but the device has a configuration, then the device resets itself after the first connection to Google servers. The system warns the person using the device one hour before the reset. The device shouldnt be included in zero-touch enrollment When your device is registered for zero-touch enrollment, it starts up and shows the Your device at work panel explaining the device is managed. Even after a factory reset. First, confirm that the device isnt 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 thats attempting to enroll the device. Start by following the steps below: Factory reset the device. Click the link to contact your devices provider in the Your device at work screen. Make a note of the telephone number, email address, and the identifiers in Device information. Ask the organization to deregister the device from zero-touch enrollment. Include 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. Post to the help community Get answers from community members 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 as of October 2023, you were notified, via do-not-reply@certmetrics.com, at your primary email address that a CertMetrics 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'vealready logged into CM and/or created an account, use those login credentials. If you are new 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 Register." If you no longer have access to the email addressyou used in Webassessor, register as a new candidate and use the Request Merge functionality so our support team can assist you with access. Im a Google Cloud Partner, how can I associate my Google Cloud certification with my organization? Log into Certmetrics and expand the Profile sectionon the left hand menu. Click on Professional Affiliation In the Work / Professional Email sectionadd your work email address (an address with an email domain that matches that of your organization) and click update. This willassociate 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 theMy Informationsection you can change your "primary email address" and in theProfessional Affiliationsection you can change your "work / professional email 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, go instead to the Google Account Help Center. If you have access to an administrator (or admin) account, you can sign in to the Google Admin console. The Admin console, at admin.google.com, is where adminsmanage 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 admin account (it does not end in @gmail.com). If you forgot your password, go toResetyour administrator password. An admin account has privileges to manage services for other people in your organization.The Admin console is only available when you're signed in to an adminaccount. If you don't have access to an admin account, get help from someone else who does. For details, go toWhoismyadministrator?. 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 If you forgot your password, go to Reset your administrator password. If you're still having trouble signing in, go to Can't sign in to the Admin console. Questions Expandall|CollapseallWhy 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 account from admin.google.com sends you to a second sign-in page. From here, you sign 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 admingave 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 you sign in to admin.google.com with your full adminaddress (name@example.com) and password, you're redirected to the Admin console. Google does not redirect you 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 SSOI'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.google.com/customer_domain. Sign in with either your own reseller account name and password, or use an admin account at the customer's domain. For more details, go to Access a customer's Admin console

Gateway portal. Gateway definition. Gateway port definition.