Click Here

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 As an administrator, you can use the Google Admin console to manage all your Google Workspace services. Use it to add or remove users, manage billing, set up mobile devices, and more. You can find the Admin console at admin.google.com. Before you begin: If youre on a Google Workspace trial and need to verify your domain, change your MX records, and set up billing, go toSet up Google Workspace for your organization. Start on the Home page with these features To get started, sign in to your Admin console. Note: Your administrator privileges determine which features are available to you and which tasks you can perform. For example, an admin with the Users privilege can only perform actions on users, so they don't see all the features, such as Billing. For more information, go to Administrator privilege definitions. Feature What you can do with it Users Add or remove users, put users in organizational units, and assign admin roles to users to help you manage your Google Workspace services. Go to Add new users or email addresses. Billing Add payment methods, print your invoices, upgrade your Google Workspace edition, or cancel your subscription. Go to Billing and payments. Discover Discover tips and new ways of working to help you get the most out of Google Workspace. Product updates Read the latest blog posts from the Google Workspace Updates blog. Domains Verify your domain, add a domain alias or other domains, and more. Go to Add or change domains. Alerts View the latest alerts from the Admin console alert center. Go to About the alert center. Chrome Enterprise Core Set up Chrome Enterprise Core, enroll browsers, configure browser policies, and manage their extensions. Go to Chrome Enterprise Core. Groups Create company-wide groups and mailing lists to collaborate. Go to Get started managing groups for an organization. Devices Manage mobile devices and computers for your organizations Google Workspace account. Go to Manage devices with Google endpoint management. Organizational units Set up a structure to apply settings and appsto groups or departments. Go to How the organizational structure works. Reporting View reports and audit logs to examine potential security risks and analyze user and administrator activity. Go to Monitor usage & security with reports. Directory Sync Synchronize your LDAP user and group data with your Google Cloud directory. Go toGet started with Directory Sync. Apps Manage settings for Google Workspace apps and services, such as Gmail and Calendar. Go to Set up services for your business. Admin roles Add other users as administrators and select their permissions. Go to About administrator roles. Account settings Customize your organization's details and set your communication preferences. Review and accept compliance agreements (GDPR, HIPAA). Profile Preferences Personalization Add your logo to Google Workspace Legal and compliance Data regions Choose a geographic location for your data Account Management Custom URLs Customize a Google Workspace service URL Support Get support from Google by chat, phone, or email, or search for specific help topics. Go to Contact Google Workspace support. Security Manage security settings in Google Workspaceenforce 2-Step Verification, monitor and enforce passwords, and more. Go to Security and data protection. Buildings and resources Set up Calendar so users can book shared resources in your company, such as equipment or conference rooms. Go to Create buildings, features & Calendar resources. Rules Secure your organization's data, files, and devices. Go to Create and manage rules from the Rules page. Storage Manage Google Workspace storage for your organization. Go toReview storage use across your organization. As an administrator, you can transfer your users' dataemail, calendars, documents, sites, and morefrom an existing account to a new one. You can also choose to merge data from several accounts into one account. In some cases, you transfer the users' data. In other cases, users move their own data. Note: If you transfer a lot of data all at once, it might take some time for the data to appear. Transfer data for multiple users Administrators who need to transfer data for multiple users between Google Workspace accounts can use these methods: Transfer data as a user or member of a small team If youre an end user or a member of a small team, you can transfer your own data using these methods: Related topics Supported editions for this feature: Business Starter (except as noted), Business Standard, and Business Plus; Enterprise Standard and Enterprise Plus; Education Fundamentals, Education Standard, and Education Plus; Essentials, Enterprise Essentials, and Enterprise Essentials Plus; Nonprofits; GSuite Business. Compareyouredition If you're a manager of a shared drive, go here instead. As an administrator, you can change the members and their access level for any shared drive in your organization. You can also change the sharing settings for a shared drive, and the default sharing settings for all new shared drives. For example, if youre concerned about a specific user having access to a shared drive, you can remove them or change their access level. Note: If you have Business Starter and sign up for Frontline Plus, you cant manage shared drives. To continue to manage shared drives for your non-Frontline users, upgrade to a Business Standard or higher edition. Add or remove members of a shared drive As an administrator, you might need to add members to a shared drive through the admin console if the shared drive has no members or no managers. Or, you might need to remove members from a shared drive if they shouldnt have access to the contents. Note: You can assign up to 100 groups to a shared drive and up to 600 members (between groups and individual users). A shared drive can have no more than 50,000 individual members through groups and individuals. Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. Click Manage shared drives. Point to the shared drive you want to update and click Manage members. If you have many shared drives, you can filter the list by shared drive name or other attributes. To find shared drives that have no members, click Add a filterNo members. To find shared drives that have no managers, click Add a filterNo managers. To add a person or group: Enter the email address. Select an access level. Select if you want to notify people, and if you do, optionally include a message. Click Send (if you chose to notify people) or Share (if you chose not to notify people). To remove a person or group: Next to the person or group name, click the access level. Click Remove access. Note: When you remove a member from a shared drive, they also lose access to any files and folders in the shared drive that were directly shared with them. Click Save. Change the access level of a shared drive member As an administrator, you can change the access level for a member of a shared drive, even if youre not a manager of the shared drive. For example, if youre concerned about a specific user having Manager access to a shared drive, you can reduce their access level. Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. Click Manage shared drives. Point to the shared drive with the member you want to update and click Manage members. If you have many shared drives, you can filter the list by shared drive name or other attributes. In the row for the member you want to update, click their current access level, then click the new access level. Click Done. Not supported for Business Starter. All shared drive sharing settings are set to allow. As an administrator, you can set the default sharing settings for shared drives by the organizational unit theyre assigned to. You can also prevent members with Manager access from changing those settings. For example, if you don't want users in an organizational unit to share content outside your organization, you can block external sharing and prevent managers from changing that setting. Important: The default sharing settings apply only to new shared drives. If you have existing shared drives that you want to change sharing settings for, go to the next section. Note:The sharing permissions for shared drives don't restrict who the Google Forms form requests can be shared with. Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. ClickSharing settingsShared drive creation. (Optional) To apply the setting to a department or team, at the side, select an organizational unit. Show me how Set the default sharing settings for new shared drives, and choose whether shared drive managers can override those settings. Options: Allow members with manager access to override the settings belowWhen unchecked, managers cant change these sharing settings for individual shared drives. In most cases, you might want to allow shared drive managers to change the settings so that they arent prevented from collaborating with external users or other teams. Allow users outside your organization to access files in shared drivesWhen unchecked, external users can't have access, even if you allow users to share files outside of your organization. This setting also blocks shared drive managers from adding external users as members. If users arent allowed to share any items in Drive outside of your organization, this setting has no effect because it cant override the sharing setting. Allow people who aren't shared drive members to be added to filesWhen unchecked, shared drive members can't give non-members view, comment, or edit access to files in shared drives, or sharing these files with a link. Allow content managers to share foldersWhen unchecked, only managers can share folders. Allow viewers and commenters to download, print, and copy filesWhen unchecked, shared drive members who have viewer or commenter access can't download, copy, or print files in shared drives. Note: Files and folders in shared drives retain this setting when they're moved out of shared drives. In the case of folders, the setting can't be reverted after the file is in My Drive. Click Save. Or, you might click Override for an organizational unit.To later restore the inherited value, click Inherit. Changes can take up to 24 hours but typically happen more quickly.Learn more Change sharing settings for a shared drive Not supported for Business Starter. You can only reset so all sharing is allowed. Before you begin: Review the contents of the shared drive to understand what should and shouldnt be shared. Shared drive sharing settings are overridden by Drive sharing settings if the Drive settings are more restrictive. For more information about sharing settings and shared drives, see Manage data policies for specific shared drives. To update sharing settings for a shared drive: Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. Click Manage shared drives. Point to the shared drive you want to update and click Settings. If you have many shared drives, you can filter the list by shared drive name or other attributes. Update the sharing settings. Your changes are automatically saved as you update. (Optional) To prevent shared drive managers from overriding your new settings, uncheck the first box. Click Done. Changes can take up to 24 hours but typically happen more quickly.Learn more Restrict who can move content to external shared drives You can control who can move files and folders outside of your organization when moving content from: A shared drive in your organization to: A shared drive owned by another organization Someones My Drive in another organization Someones My Drive in your organization to a shared drive owned by another organization Click Sharing settingsSharing options. Select the desired organizational unitor group. In Distributing content outside of yourorganization,select an option: Anyone People with Manager access to a shared drive can move files from that shared drive to a Drive location in a different organization. Learn more People in the selected organizational unit or group can move content from their My Drive to a shared drive owned by a different organization (for example, another business, group, or school). Learn more Only users in your organization People with Manager access to a shared drive can move files from that shared drive to a Drive location in a different organization. Users in the selected organizational unit or group can move content from their My Drive to a shared drive owned by a different organization. No one Files on a shared drive cannot be moved to a Drive location in a different organization. No one in the selected organizational unit or group can move content from My Drive to a shared drive owned by a different organization. No one in the selected organizational unit or group can create files on a shared drive owned by another organization. ClickSave. Important: If you select a child organizational unit or group, this setting only controls moving content from someones My Drive to a shared drive in a different organization (for example, another business or school). If the top-level organizational unit permits the user to share files outside their organization, but the child organizational unit does not, the user cant share files outside their organization. It can take up to 24 hours to see changes. During this time, old and new settings might be intermittently enforced. Review user activity in shared drives To review when files, settings, or members of shared drives changed and who made the changes, you can use the Drive audit log. Review and appeal disabled shared drives If Google detects that a shared drive contains content that violates the Terms of Service, it may disable the shared drive. Your content isnt deleted, but users can't access it until the shared drive is reinstated by Google upon your appeal. If you believe that the shared drive was disabled in error, you can submit a request for a review. You have 29 days to appeal. If you dont appeal, the disabled shared drive is automatically deleted. Your appeal for the shared drive is reviewed. If approved, the shared drive is reinstated. Artikel ini ditujukan bagi pengguna yang mengelola layanan atau perangkat Google untuk perusahaan, sekolah, atau grup. Jika Anda menggunakan akun pribadi (@gmail.com), buka Pusat Bantuan Akun Google. Jika memiliki akses ke akun administrator (atau admin), Anda dapat login ke konsol Google Admin. Konsol Admin, di admin.google.com, adalah tempat adminmengelola layanan Google untuk pengguna dalam sebuah organisasi. Di browser web apa pun, buka admin.google.com. Mulai dari halaman login, masukkan alamat email dan sandi untuk akun admin Anda (yang tidak diakhiri dengan @gmail.com). Jika Anda lupa sandi Anda, buka halaman Mereset sandi administrator Anda. Akun admin memiliki hak istimewa untuk mengelola layanan bagi orang lain di organisasi Anda.Konsol Admin hanya tersedia jika Anda login ke akunadmin. Jika Anda tidak memiliki akses ke akun admin, dapatkan bantuan dari orang lain yang memilikinya. Untuk mengetahui detailnya, bukahalaman Siapaadministratorsaya?. Jika Anda menemukan daftar Akun Google di halaman login, pastikan Anda memilih akun admin Anda (yang tidak diakhiri dengan @gmail.com). Tips: Anda dapat beralih antar-akun di komputer yang sama tanpa perlu login setiap kalinya. Untuk mengetahui detailnya,pelajari cara login ke beberapa akun sekaligus. Mendapatkan bantuan untuk login Jika Anda lupa sandi Anda, buka halaman Mereset sandi administrator Anda. Jika Anda masih mengalami masalah saat login, buka halaman Tidak dapat login ke konsol Admin. Pertanyaan Luaskan semua|Ciutkan semuaMengapa saya harus login dua kali? Jika perusahaan menggunakan layanan Single Sign-On (SSO) dengan akun Google Anda, Anda akan diarahkan ke halaman login kedua saat login ke akun dari admin.google.com. Dari sini, Anda dapat login ke konsol Admin dan program atau layanan lain yang sudah disiapkan perusahaan Anda dengan SSO secara bersamaan. Cukup masukkan nama dan sandi login yang diberikan oleh admin. Pelajari cara login dengan SSO.Dapatkah pengelola sandi Chrome menyimpan detail login Google saya? Dengan Browser Chrome, Anda dapat mengelola sandi situs Anda agar Chrome otomatis mengisi kolom login untuk Anda saat Anda mengunjungi situs tersebut. Proses login dua langkah untuk semua akun Google tidak akan memengaruhi perilaku pengelola sandi.Mengapa terkadang saya harus login lagi saat menggunakan konsol Admin? Untuk menjaga layanan Google organisasi Anda tetap aman, Anda harus login ke konsol Admin setelah tiap jam penggunaan.Bagaimana pengaruh pengaktifan Single Sign-On (SSO) terhadap proses login jika saya adalah administrator? Jika Anda adalah administrator super dan login ke admin.google.com menggunakan alamat admin lengkap (nama@example.com) dan sandi, Anda akan dialihkan ke konsol Admin. Google tidak mengalihkan Anda ke server SSO. Jika Anda bukan administrator super dan login ke admin.google.com, Anda akan dialihkan ke halaman login SSO. Untuk mengetahui detail selengkapnya, buka Login dengan SSOSaya adalah reseller. Dapatkah saya mengakses konsol Admin pelanggan? Reseller dapat mengakses konsol Admin pelanggan. Buka admin.google.com/customer_domain. Login menggunakan nama akun dan sandi reseller, atau gunakan akun admin di domain pelanggan. Untuk mengetahui detail selengkapnya, buka Mengakses konsol Admin pelanggan Bagaimana cara meningkatkannya? You can set up SSO with Google as your service provider in a number of ways, depending on your organizations needs.Google Workspace supports both SAML-based and OIDC-based SSO. If your users use domain-specific service URLs to access Google services (for example, , you can also manage how these URLs work with SSO. If your organization needs conditional SSO redirection based on IP address, or SSO for super admins, you also have the option to configure the legacy SSO profile. Set up SSO with SAML Before you begin To set up a SAML SSO profile, youll need some basic configuration from your IdPs support team or documentation: Sign-in page URL This is also known as the SSO URL or SAML 2.0 Endpoint (HTTP). This is where users sign in to your IdP. Sign-out page URL Where the user lands after exiting the Google app or service. Change password URL The page where SSO users will go to change their password (instead of changing their password with Google). Certificate X.509 PEM certificate from your IdP. The certificate contains the public key which verifies sign-in from the IdP.Certificate requirements The certificate must be a PEM or DER formatted X.509 certificate with an embedded public key. The public key must be generated with the DSA or RSA algorithms. The public key in the certificate must match the private key used to sign the SAML response. Youll usually get these certificates from your IdP. However, you can also generate them yourself. Create a SAML SSO profile Follow these steps to create a third-party SSO profile. You can create up to 1000 profiles in your organization. Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. In Third-party SSO profiles, click Add SAML profile. Enter a name for the profile. (Optional) If you have an XML metadata file from your IdP, click upload XML file to provide IdP information, then continue with Step 8 Fill in the Sign-in page URL and other information obtained from your IdP. Enter a change password URL for your IdP. Users will go to this URL (rather than the Google change password page) to reset their passwords. Click Upload certificateto upload your certificate file. You can upload up to two certificates, giving you the optionto rotate certificates when necessary. Click Save. In the SP Details section, copy and save the Entity ID and ACS URL. Youll need these values to configure SSO with Google in your IdP admin control panel. (Optional)If your IdP supports encrypting assertions, you can generate and share a certificate with your IdP to enable encryption. Each SAML SSO profile can have up to 2 SP certificates. Click the SP Details section to enter edit mode. Under SP certificate, click Generate certificate. (The certificate will display after you save it.) Click Save. The certificate name, expiration date, and contents are displayed. Use the buttons above a certificate to either copy the certificate contents or download as a file, then share the certificate with your IdP. (Optional) If you need to rotate a certificate, return to SP Details and click Generate another certificate, then share the new certificate with your IdP. Once youre sure your IdP is using the new one, you can delete the original certificate. Configure your IdP To configure your IdP to use this SSO profile, enter the information from the Service Provider (SP) Details section of theprofile into the appropriate fields in your IdP SSO settings. Both the ACS URL and Entity ID are unique to this profile.Configure the legacy SSO profile The legacy SSO profile is supported for users who have not migrated to SSO profiles. It only supports usage with a single IdP. Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. In Third-party SSO profiles, click Add SAML profile. At the bottom of the IdP details page, click Go to legacy SSO profile settings. On the Legacy SSO profile page, check the Enable SSO with third-party identity provider box. Fill in the following information for your IdP: Enter the Sign-in page URL and Sign-out page URL for your IdP. Note: All URLs must be entered and must use HTTPS, for example . Click Upload certificate and locate and upload the X.509 certificate supplied by your IdP. For more information, see Certificate requirements. Choose whether to use a domain-specific issuer in the SAML request from Google. If you have multiple domains using SSO with your IdP, use a domain-specific issuer to identify the correct domain issuing the SAML request. Checked Google sends an issuer specific to your domain: google.com/a/example.com (where example.com is your primary Google Workspace domain name) Unchecked Google sends the standard issuer in the SAML request: google.com (Optional) To apply SSO to a set of users within specific IP address ranges, enter a network mask. For more information see Network mapping results. Note: you can also set up partial SSO by assigning the SSO profile to specific organizational units or groups. Enter a change password URL for your IdP. Users will go to this URL (rather than the Google change password page) to reset their passwords. Note: If you enter a URL here, users are directed to this page even if you dont enable SSO for your organization. Click Save. After saving, the legacy SSO profile is listed in the SSO profiles table. Configure your IdP To configure your IdP to use this SSO profile, enter the information from the Service Provider (SP) Details section of the profile into the appropriate fields in your IdP SSO settings. Both the ACS URL and Entity ID are unique to this profile. Format ACS URL domain.com}/acs Where {domain.com} is your organization's Workspace domain name Entity ID Either of the following: google.com google.com/a/customerprimarydomain (if you choose to use a domain-specific issuer when configuring the legacy profile). Disable the legacy SSO profile In the Third-party SSO profiles list, click Legacy SSO profile. In the Legacy SSO profile settings, uncheck Enable SSO with third-party identity provider. Confirm that you want to continue, then click Save. In the SSO profiles list, the Legacy SSO profile now shows as Disabled. Organizational units that have the Legacy SSO profile assigned will display an alert in the Assigned profile column. The top level organizational unit will display None in the Assigned profile column. In Manage SSO profile assignments, the Legacy SSO profile shows as inactive. Migratefrom legacy SAML to SSO profiles If your organization is using the legacy SSO profile, we recommend migrating to SSO profiles, which offer several advantages including OIDC support, more modern APIs, and greater flexibility in applying SSO settings to your user groups. Learn more. Set up SSO with OIDC Follow these steps to use OIDC-based SSO: Choose an OIDC optioneither create a custom OIDC profile, where you provide information for your OIDC partner, or use the pre-configured Microsoft Entra OIDC profile. Follow the steps in Decide which users should use SSO to assign the pre-configured OIDC profile to selected organizational units/groups. If you have users within an organizational unit (for example in a sub-organizational unit) who dont need SSO, you can also use assignments to turn SSO off for those users. Note: The Google Cloud Command Line Interface does not currently support reauthentication with OIDC. Before you begin To set up a custom OIDC profile, youll need some basic configuration from your IdPs support team or documentation: Issuer URL The complete URL of the IdP authorization server. An OAuth client, identified by its Client ID and authenticated by a Client secret. Change password URL The page where SSO users will go to change their password (instead of changing their password with Google). Also, Google needs your IdP to do this: The email claim from your IdP must match the users primary email address on the Google side. It must use the authorization code flow. Create a custom OIDC profile (beta) Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. In Third-party SSO profiles, click Add OIDC profile. Name the OIDC profile. Enter OIDC details: Client ID, Issuer URL, Client secret. Click Save. On the OIDC SSO settings page for the new profile, copy the Redirect URI. Youll need to update your OAuth client on your IdP to respond to requests using this URI. To edit settings, hover over the OIDC Details, then click Edit . Use the Microsoft Entra OIDC profile Make sure youve configured the following prerequisites for OIDC in your organizations Microsoft Entra ID tenant: The Microsoft Entra ID tenant needs to be domain verified. End users must have Microsoft 365 licenses. The username (primary email) of the Google Workspace admin assigning the SSO profile must match the primary email address of your Azure ADtenant admin account. Decide which users should use SSO Turn SSO on for an organizational unit or group by assigning an SSO profile and its associated IdP. Or, turn SSO off by assigning None for the SSO profile. You can also apply a mixed SSO policy within an organizational unit or group, for example turning SSO on for the organizational unit as a whole, then turning it off for a sub-organizational unit. If you haven't created aSAMLor OIDC profile, do that before continuing. Or, you can assign the preconfigured OIDC profile. Click Manage SSO profile assignments. If this is your first time assigning the SSO profile, click Get started. Otherwise, click Manage assignments. On the left, select the organizational unit or group to which youre assigning the SSO profile. If the SSO profile assignment for an organizational unit or group differs from your domain-wide profile assignment, an override warning appears when you select that organizational unit or group. You cant assign the SSO profile on a per-user basis. The Users view lets you check the setting for a specific user. Choose an SSO profile assignment for the selected organizational unit or group: To exclude the organizational unit or group from SSO, choose None. Users in the organizational unit or group will sign in directly with Google. To assign another IdP to the organizational unit or group, choose Another SSO profile, then select the SSO profile from the dropdown list. (SAML SSO profiles only) After selecting a SAML profile, choose a sign-in option for users who go directly to a Google service without first signing in to the SSO profile's third-party IdP. You can prompt users for their Google username, then redirect them to the IdP, or require users to enter their Google username and password. Note: If you choose to require users to enter their Google username and password, the Change password URL setting for this SAML SSO profile (available at SSO Profile > IDP details) is ignored. This ensures that users are able to change theirGoogle passwords as needed. Click Save. (Optional) Assign SSO profiles to other organizational units or groups as needed. After you close the Manage SSO profile assignments card, youll see the updated assignments for organizational units and groups in the Manage SSO profile assignments section. Remove an SSO profile assignment Click a group or organizational unit name to open its profile assignment settings. Replace the existing assignment setting with the parent organization unit setting: For organizational unit assignmentsclick Inherit. For group assignmentsclick Unset. Note: Your top organizational unit is always present in the profile assignment list, even if the Profile is set to None. See also Google, Google Workspace, and related marks and logos are trademarks of Google LLC. All other company and product names are trademarks of the companieswith which they are associated. 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 Post to the help community Get answers from community members As aGoogle Workspace admin, you can automatically redirect or forward incoming messages sent to one person in your organization, to one or more other recipients. Do this by creating address maps in your Admin console. On this page Options and examples Exclude original recipient (redirect)Someone leaves your organization and you want to redirect their future messages to their replacement, or to an account set up for this purpose. Messages aren't delivered to the original recipient. Include original recipient (forward)Someone takes a leave of absence. During their leave, you want them to keep getting their email so they have it whentheyre back. Butyou also want to forward their messagesto the person whos doing their work while theyre gone. Map addresses in bulkFor example, you might need to map your organizations' old addresses to new addressesafter an acquisition. Tip: Learn more about forwarding vs. redirecting. Redirect or forward one address at a time Messages you redirect or forward appear to come directly from the original sender. The To: address in redirected messagesincludes the original recipient address only. In your Google Admin console... Go to Menu Apps > Google Workspace Gmail > Routing(not"Default routing"). On the left, selectthe top-level organizational unit. Scroll down toEmail forwarding using recipient address map, and click Configure or Add Another Rule. At the top of the Add setting box, enter a descriptive name for the address map. In step 1 of the Add setting box, click Add. In the Addressfield,enter the original recipient email address. In theMap to addressfield,enter the email address you want to forward messagesto. Repeat this step to add more mappings. Or see below to mapaddresses in bulk. Under Messages to affect: choose an option: All incoming messages: Apply the forwarding setting to all messages received by your domain, including messages sent within your domain. Only external incoming messages: Apply the forwarding setting only to messages received from senders outside your domain. Also route to original destination: Check this box to send the message to the original recipient, in addition to the new recipients. Add X-Gm-Original-To header: Check this box to keep the original recipient information in the message header. You might want to do this if you manage anyemailbased on message headers.Message header information can also be useful for troubleshooting email delivery. At the bottom of the Add setting box,clickSave. Your new address map appears as a row on the Routing page.Each row represents one address map. Changes can take up to 24 hours but typically happen more quickly.Learn more Back to top Redirect or forward addresses in bulk You can more easily map a large number of address by entering them as comma-delimited entries, such as from spreadsheet. The maximum number of recipient addresses for all address maps is 5,000. For example,you can add 1 address map with 5,000 recipient addresses, 50 address maps with 100 recipients each, or 1,000 address maps with 5 recipients each. Follow the steps above to create an address map. Then in step 6, do the following: ClickBulk Add. Enter the original email address followed by a comma, then enter the new recipient address. Add a new line with the Return or Enter key. Repeat Steps 1-3 until youve added all addresses. At the bottom of the bulk add box, clickAdd aliases. Continue with step 9 above. Depending on your email sending practices, we may reduce the recipient address limit for your domain. This can affect recipient limits for your address maps.We recommend you follow ourbest practices for sending mail to Gmail users. Back to top Watch a video Forward messages with address maps Back to top Alternatives to address maps Depending on your goals, these options might be more effective than using address maps. Click each option to see the steps: Let users automatically forward their own Gmail emailsIf you turn on automatic forwarding, a user can forward messages from their account. They can temporarily forward their own messages to a colleague, or to another account they own. Add an email alias for a userAn alias is an alternate email addresswhere a user can receive email. Messages sent to the alias are automatically sent to the user's primary email account. Let users delegate their Gmail accountEmail delegation lets people give others access to their Gmail account. For example, an executive assistant with delegate access can read, send, and receive messages for the executive they support. Back to top Forwarding limits Your organizations message forwarding limits are based on your overall sending practices. The maximum number of forwarding operations per organization are: 30 million in a 24-hour period 600k per 1-minute window Forwarding also includes redirects. If you exceed these limits, your users might get an error when they try to send a message. Depending on your email sending practices, we might reduce forwarding limits for your Google Workspace account. If we limit forwarding and redirecting, your accounts address maps might also be limited. We recommend you always follow these Email sender guidelines when sending mail to Gmail users. Back to top

Admin clerk job interview questions and answers. Office admin job interview questions and answers. General admin job interview questions and answers. Admin job interview questions and answers pdf. Admin job interview questions and answers for freshers. Nhs admin job interview questions and answers pdf. School admin job interview questions and answers. Admin assistant job interview questions and answers. Admin manager job interview questions and answers. Hr admin job interview questions and answers.