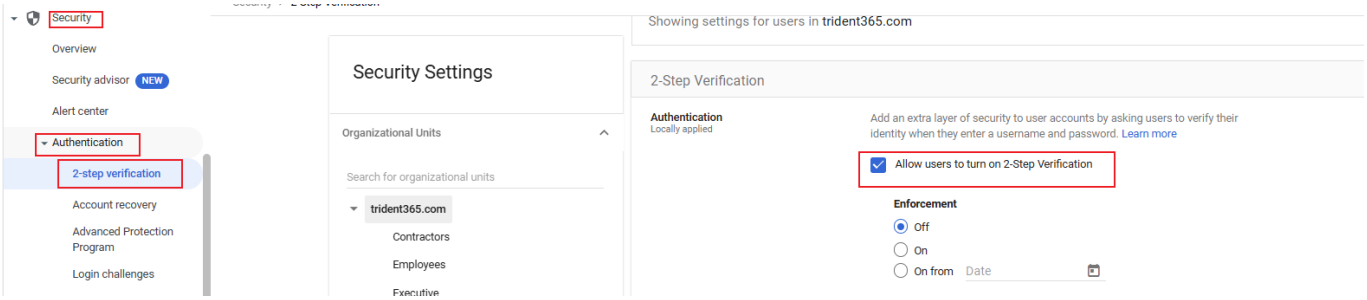
第3章 GWS安全

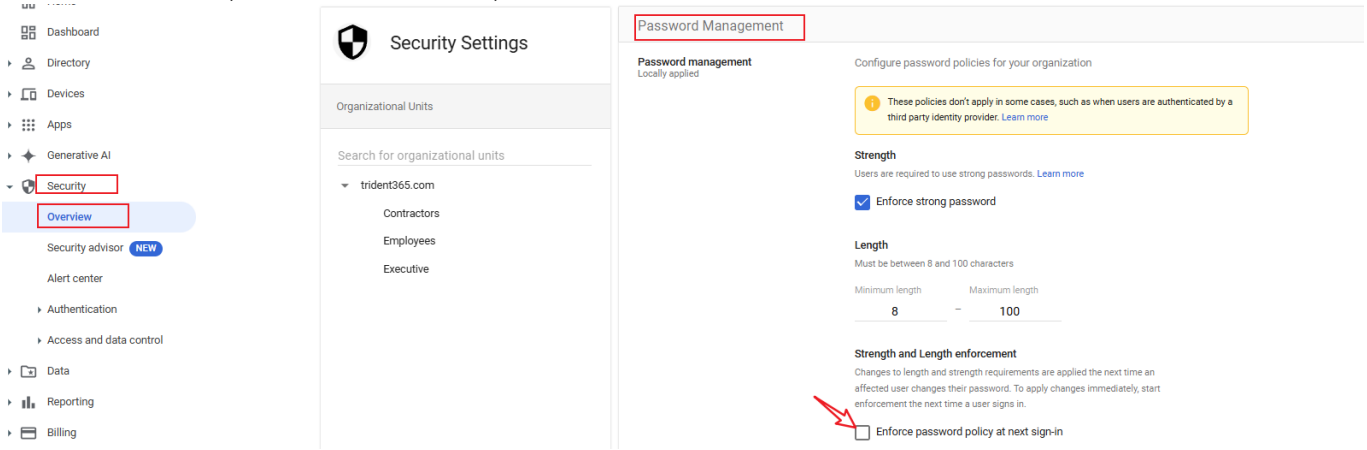
练习1

准备GWS域名，已经完成，略

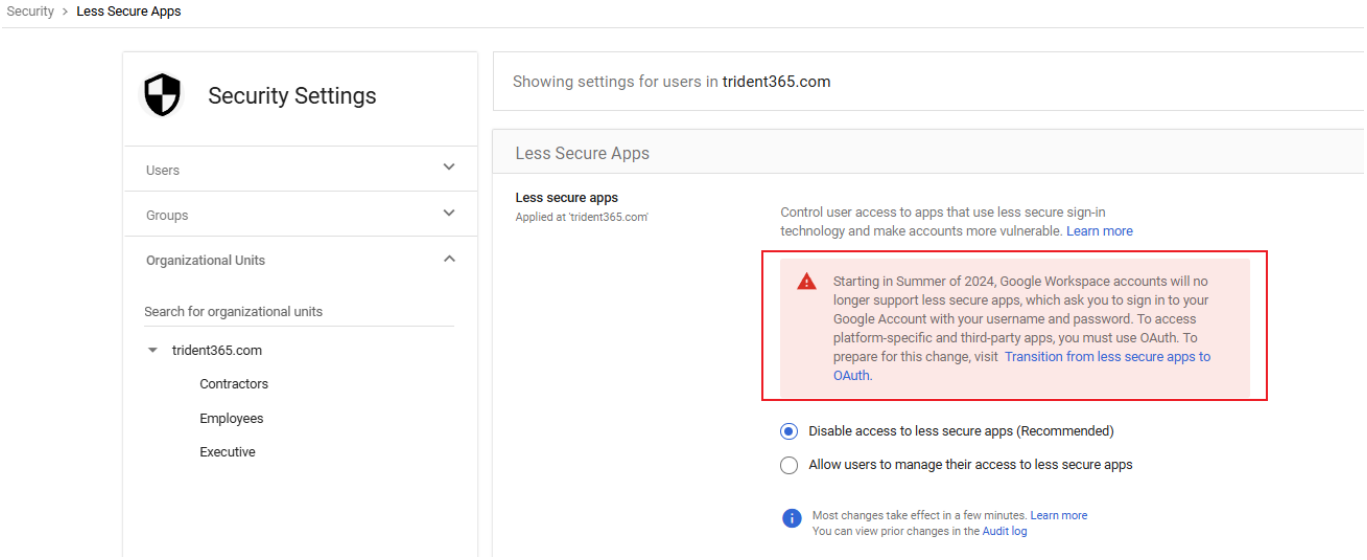
配置通用安全设定



默认2FA是打开的，用户可以自行设定，但不是必须的。

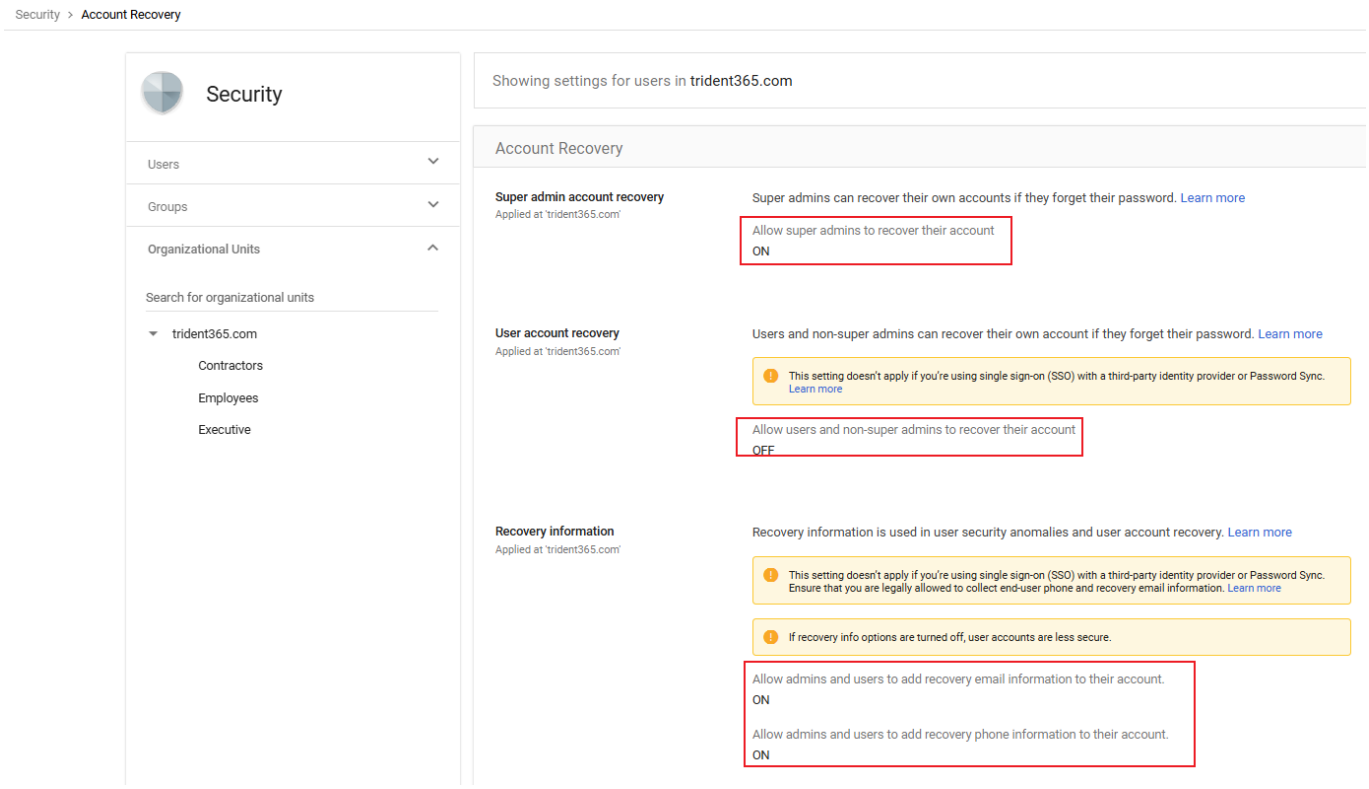


如果要变更PW方针，可以勾选下次登录时执行，这个方针适用单位是OU或以上。



这里刚好有一个更新，2025年1月之后，所有第三方APP

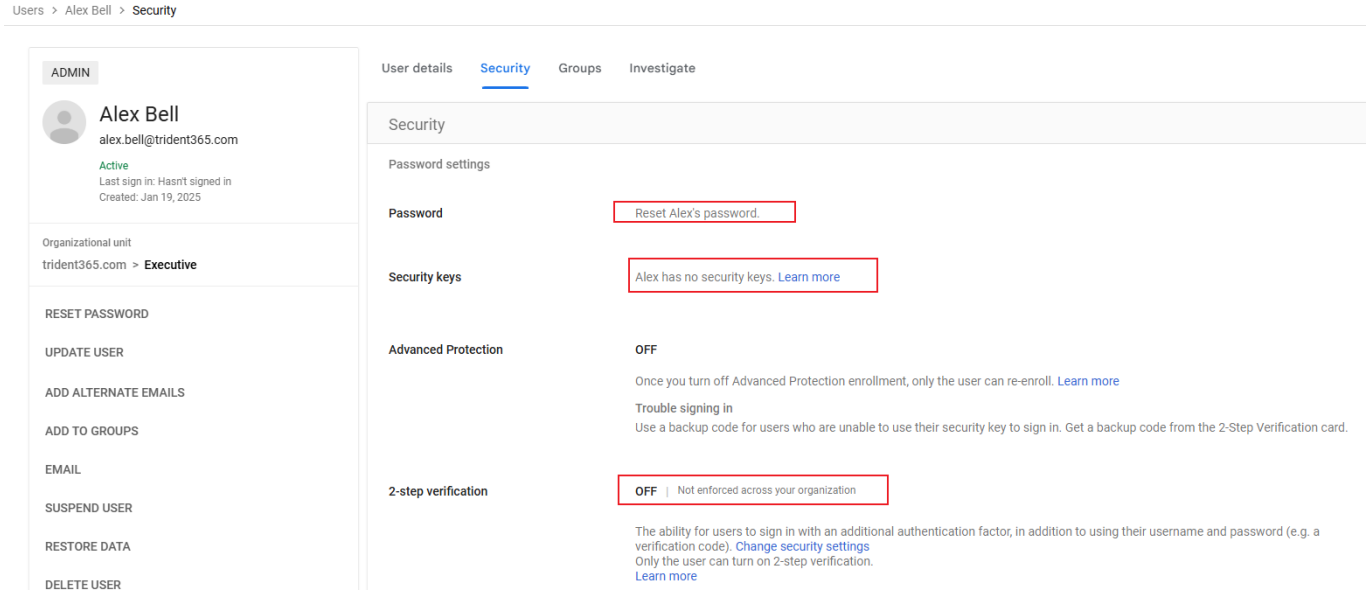
https://support.google.com/a/answer/14114704?hl=ja&sjid=8401829336969536596-AP 还有一个设置是恢复账户□Console里设置了权限，默认只有超级管理员可以恢复用户账号密码

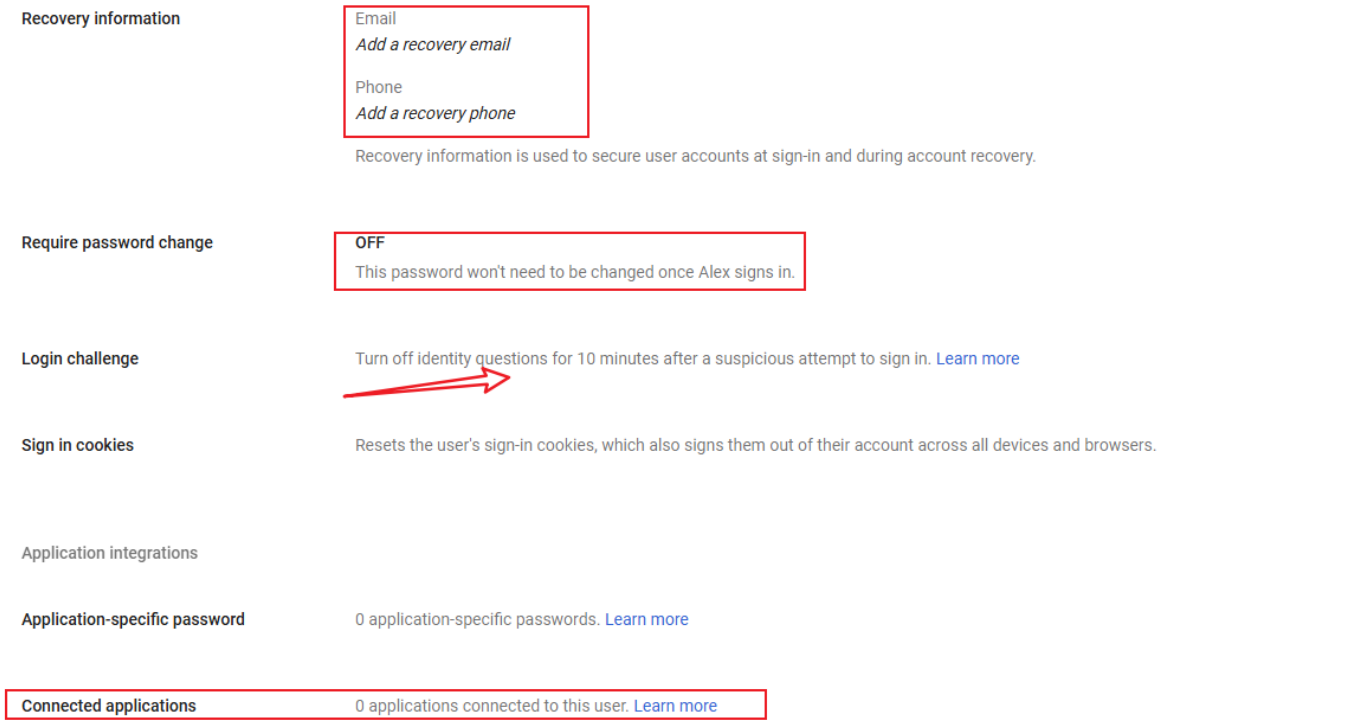


这里把Allow users and non-super admins to recover their account设为ON保存。

练习2

查看用户安全设置

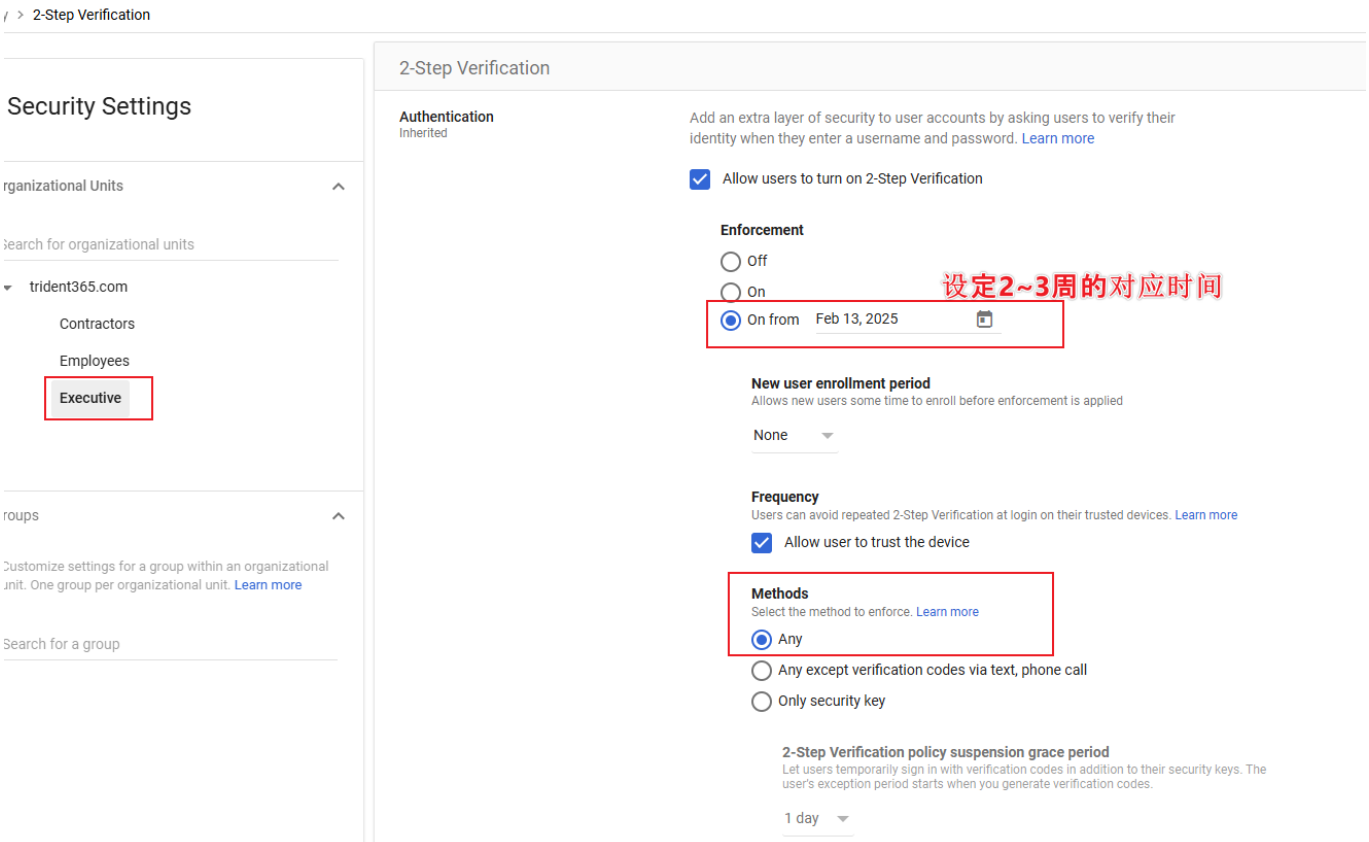




作为管理员，可以强制用户重置密码，也可以为他添加恢复用邮箱和电话号码。另外，当用户登录活动可疑时，如果不能正确验明身份，则账户会被锁，这时管理员可以暂时关闭验证，以让用户本人可以正常登录，修改密码。 还可以查看该账号连携了哪些APP 100名以上用户的IT管理员检查清单：https://support.google.com/a/answer/9211704

练习3

强制2FA



然后找一个高管的邮箱，比如Alex登录后，会出现提示

对于已经使用SSO登录的公司来说，不需要设置

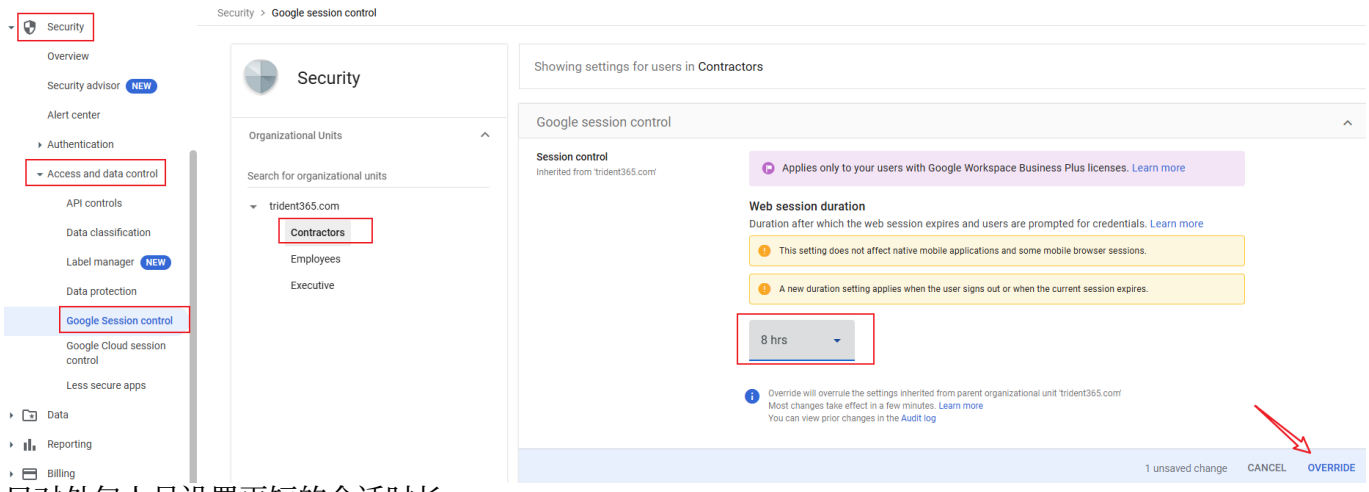
有4种方式

1. 通行密钥和安全密钥
2. Google提示（如手机端的Gmail
3. 身份验证器（二维码或是OTP等）
4. 电话号码（验证码或语音电话）

参考链接https://support.google.com/a/answer/9176657 我们可以单独建立一个Group对OU关闭2FA但对Group是打开。

练习4

我们可以控制用户访问谷歌服务的会话时长，从1小时到默认的14天。



只对外包人员设置更短的会话时长。

测试1

The IT manager at your organization wants to know the advantages of using 2-step verification for your organization. What should you say? (Choose 2)

1. **It'll greatly reduce the risk of unauthorized access if a user's password is compromised**
2. We wouldn't have to manage individual user IDs and passwords for each user
3. It would be a great opportunity to make sure everyone is the organization has a security key
4. **It'll reinforce our domain’s password security by requiring our users to enter an additional code or use a security key to sign in**

What are some best practices for reinforcing and monitoring the security of your domain?

1. **All the options**
2. Disable access to less secure apps
3. Set up 2-step verification
4. View and manage your users' security settings

Where do you go to manage your users' password strength?

1. **Security > Password management**
2. Reports > Security
3. Users > Account
4. Security > Password monitoring

The IT manager at your organization hasn't had a chance to explore the admin console yet but wants to know what individual security settings he can manage for a user. What are some examples you could give him? (Choose 3)

1. Review a user's administrative access
2. **Require a password change**
3. **Temporarily disable the user's login challenge for 10 minutes**
4. **Determine if the user is enrolled in 2-step verification**

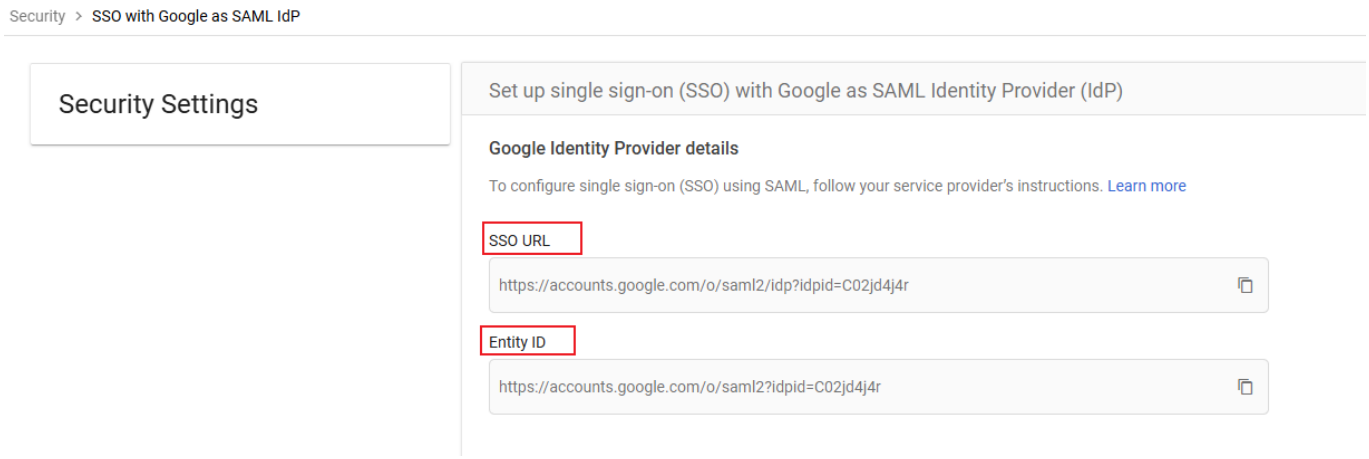
Your organization has decided to enforce 2-step verification in 2 weeks. What actions should you keep

in mind when enforcing 2-step verification? (Choose 3)

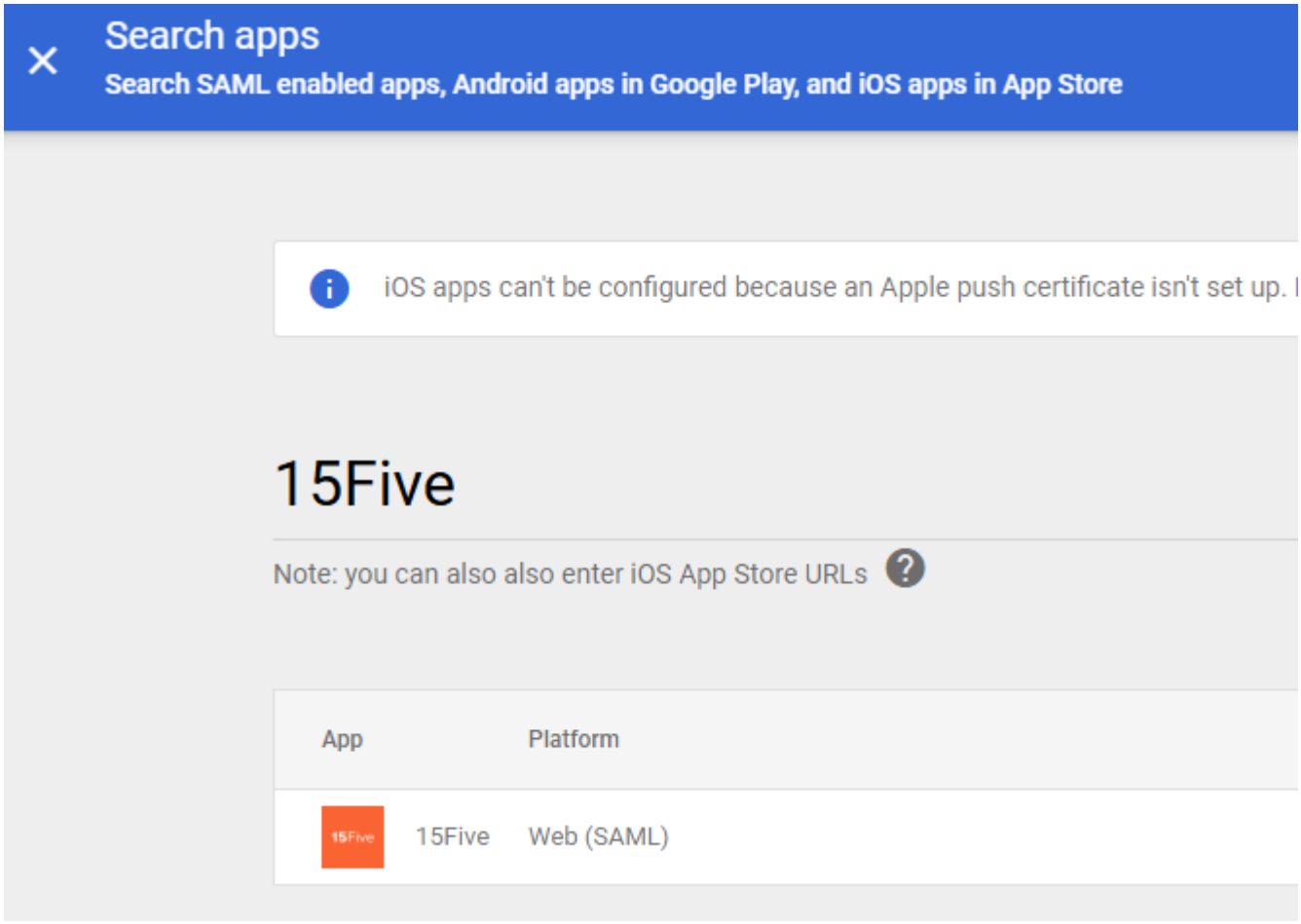
1. **You'll want to provide a lead time for users to enroll before enforcement**
2. Enforcing 2-step verification will not affect your users as they can still opt-out.
3. **When you create new user accounts after enforcement, you will want to allow them a grace period before they need to enroll otherwise they will be locked out of their accounts**
4. **You'll want to confirm that all of your users are enrolled before enforcement**

SSO介绍

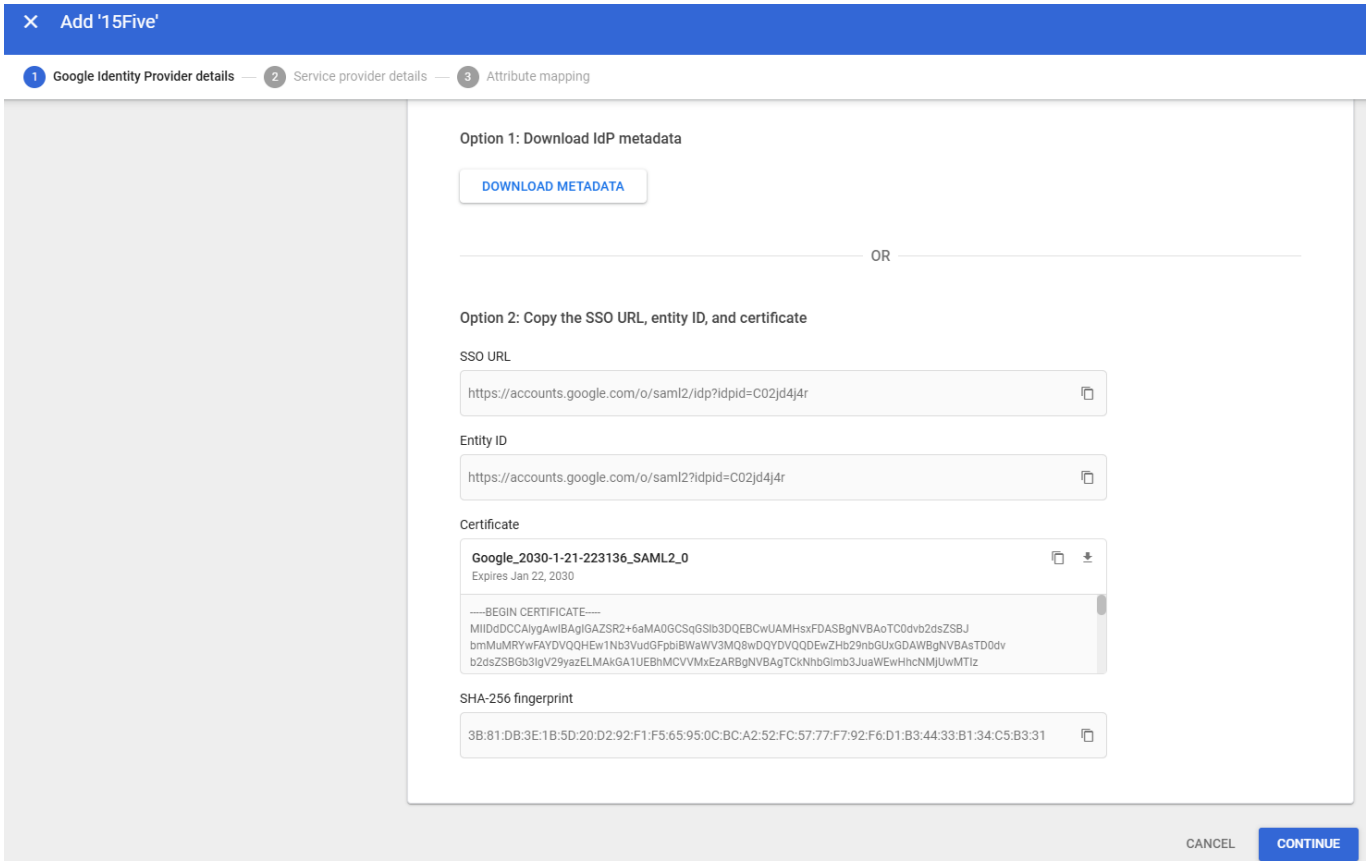
练习1



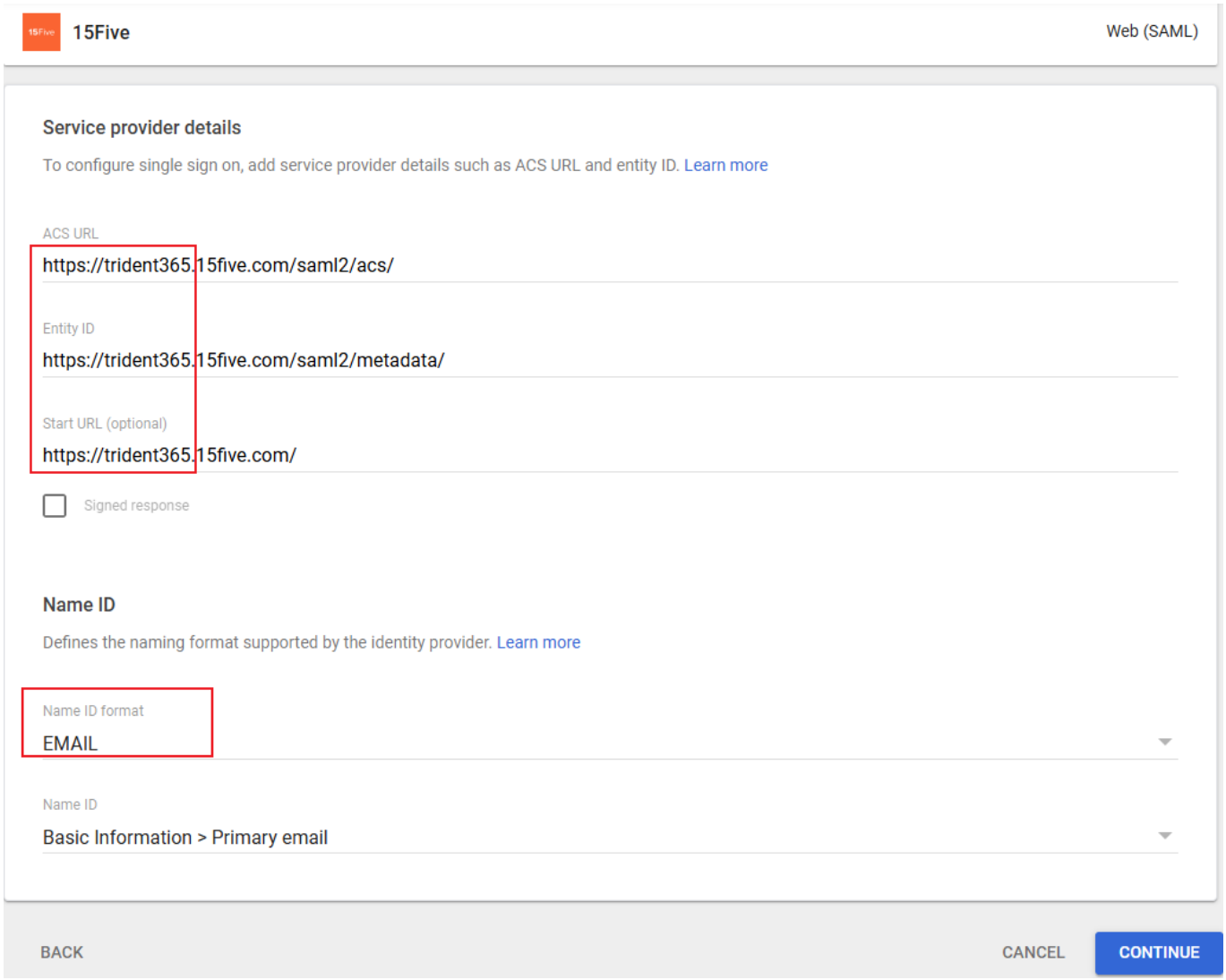
如果要使用SAML来实现SSO，则需要同第三方服务商确认SSO的URL和EntityID信息， App>Search for apps,根据练习要求，搜索15Five



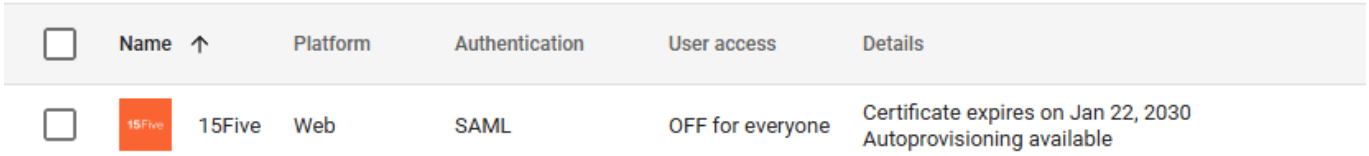
下载Metadata



详细设定指导的URL https://support.google.com/a/answer/7649387?hl=en#setup

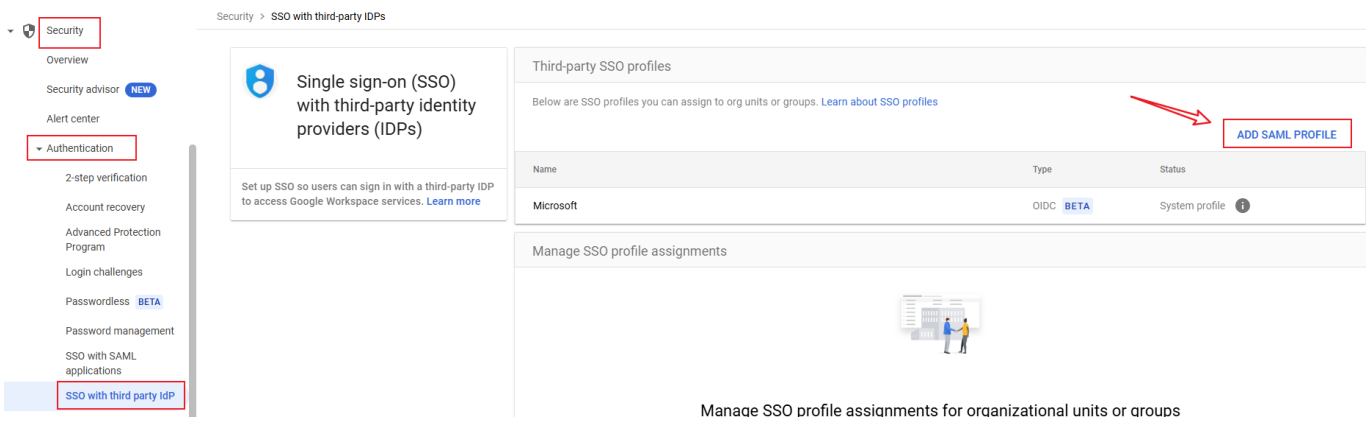


把域名补全，然后ID格式选择Email，继续



完成后，按照指导URL一步步操作才能用。因为公司用的HenngeOne，所以GWS上的操作也可以免了。。

练习2



这里要上传证书，需要OpenSSL，而且只能在Chrome浏览器，不能用其他的。 没有证书，所以练习略过。

Secure LDAP

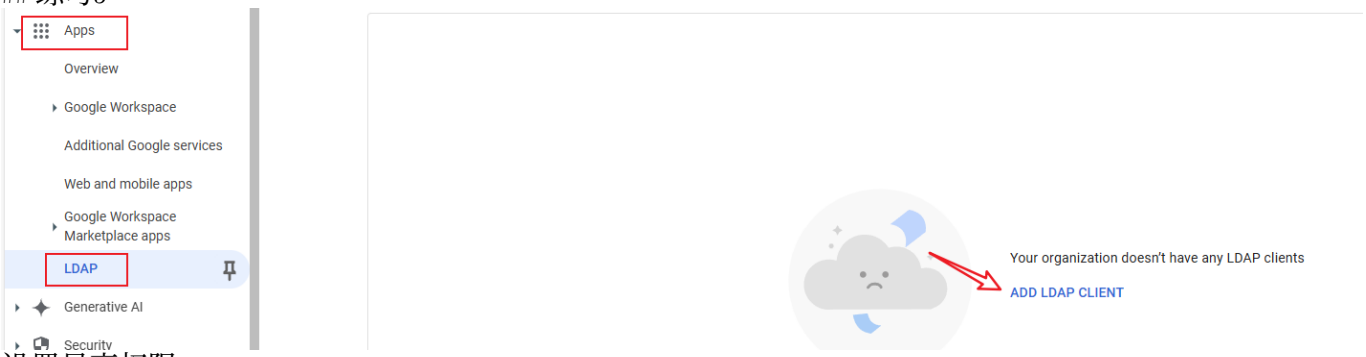
同时管理SaaS和传统程序，需要LDAP服务，除了微软的AD外，还有谷歌的Secure LDAP

Use your Google directory as an LDAP server for authentication, authorization and directory

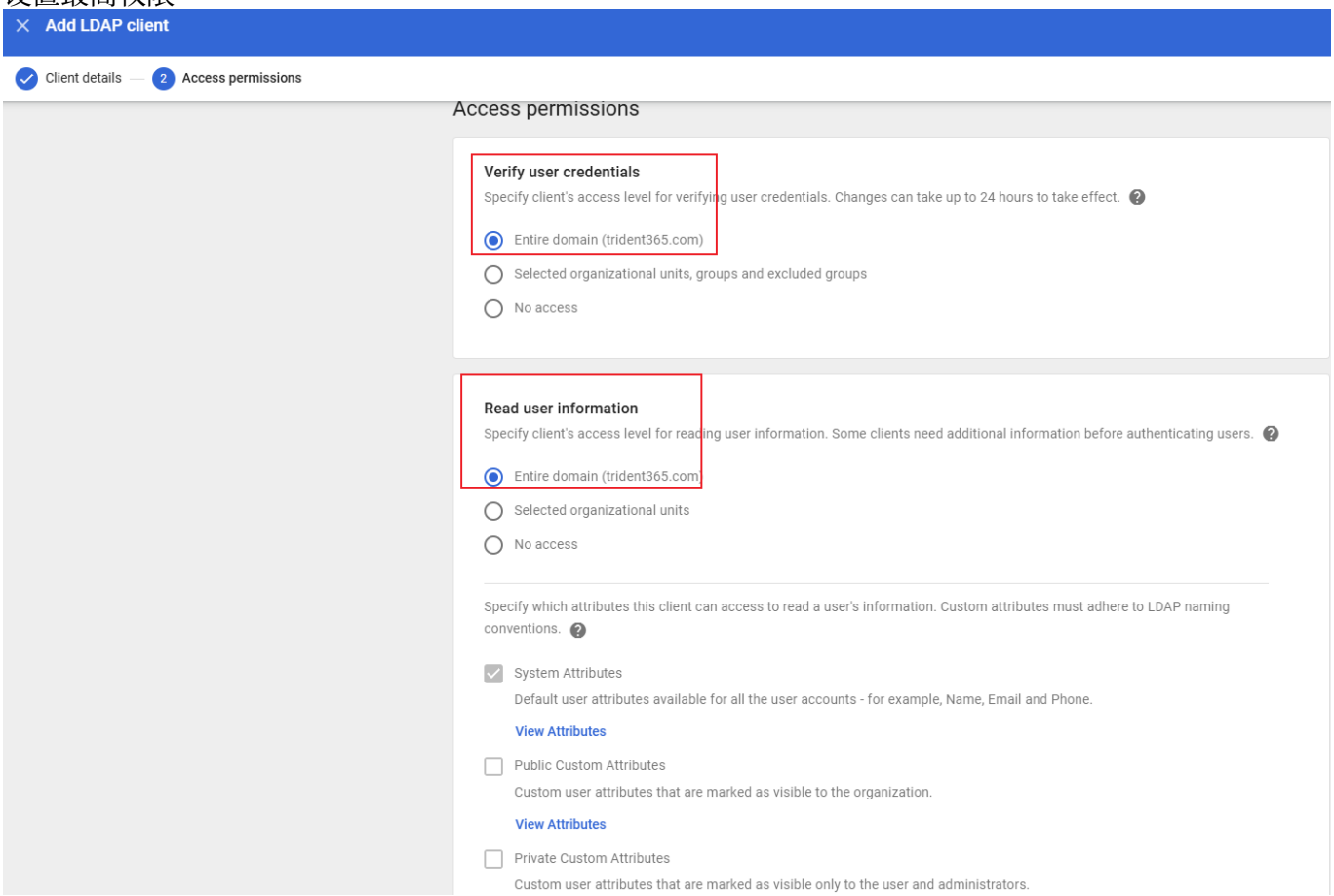
步骤

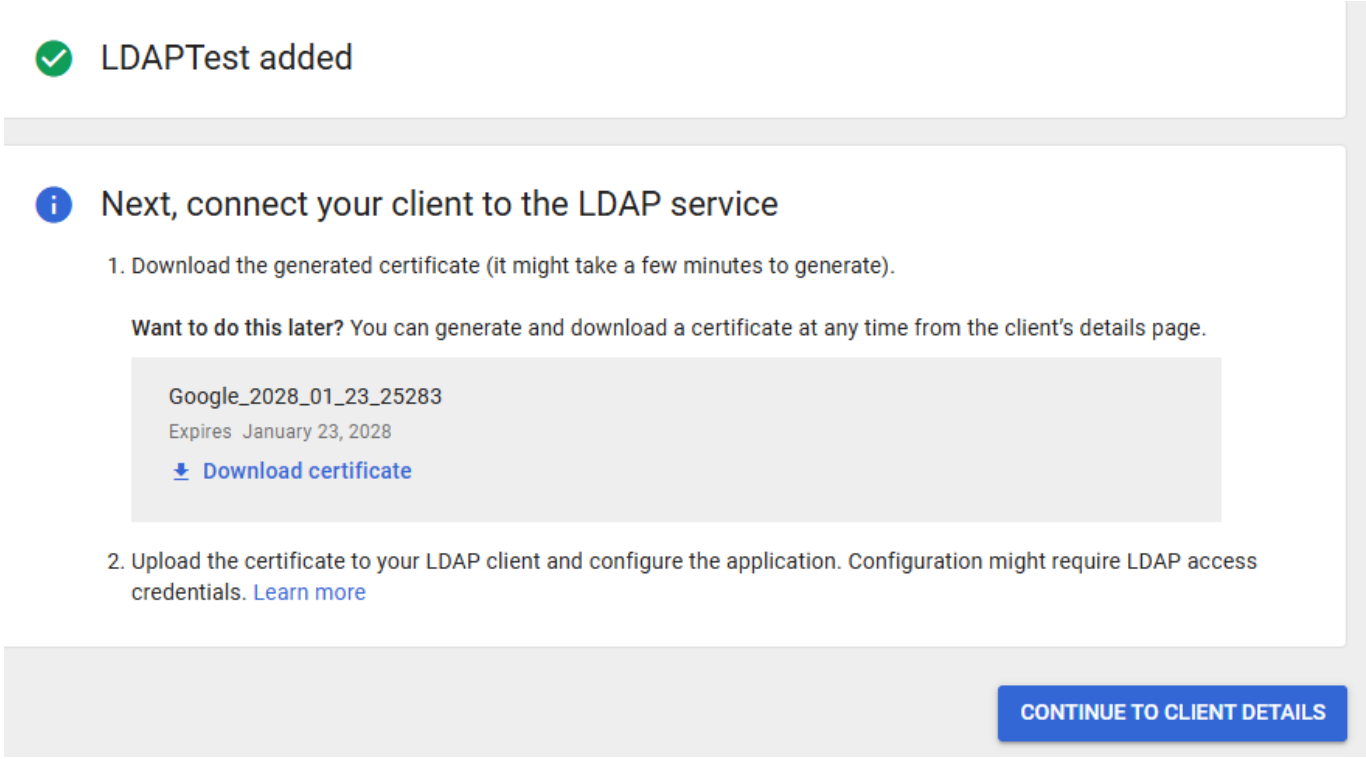
- Create LDAP client in the Admin console
- Configure your LDAP client to connect to the secure LDAP service

练习3



设置最高权限





相关资料： https://support.google.com/a/topic/9173976 https://support.google.com/a/answer/9089736
类似于加入AD域的操作。

测试2

What of the following are true of the Secure LDAP service? (Choose 3)

1. User's authenticate against a local directory to gain access to Google Workspace services
2. **It reduces maintenance as directory information is consolidated into one directory**
3. **It allows you to connect your LDAP-based applications and services to Google Workspace**
4. **Users authenticate against the Google Workspace directory to gain access to LDAP compliant applications and services**

When adding a pre-integrated SAML application to your Google Workspace account, which of the following must you add/upload the Service Provider's configuration? (Choose 3)

1. Change Password URL
2. **Google Certificate**
3. **Entity ID URL**
4. **SSO URL**

When using a third party IdP which of the following is disabled/hidden in Google Workspace?

1. Password reuse policy
2. Password recovery
3. **Require password change**
4. Password monitoring

Your IT manager has just informed you that your organization has an account now with Asana and would like you to enable Single Sign On with the application. Where in the admin console would you

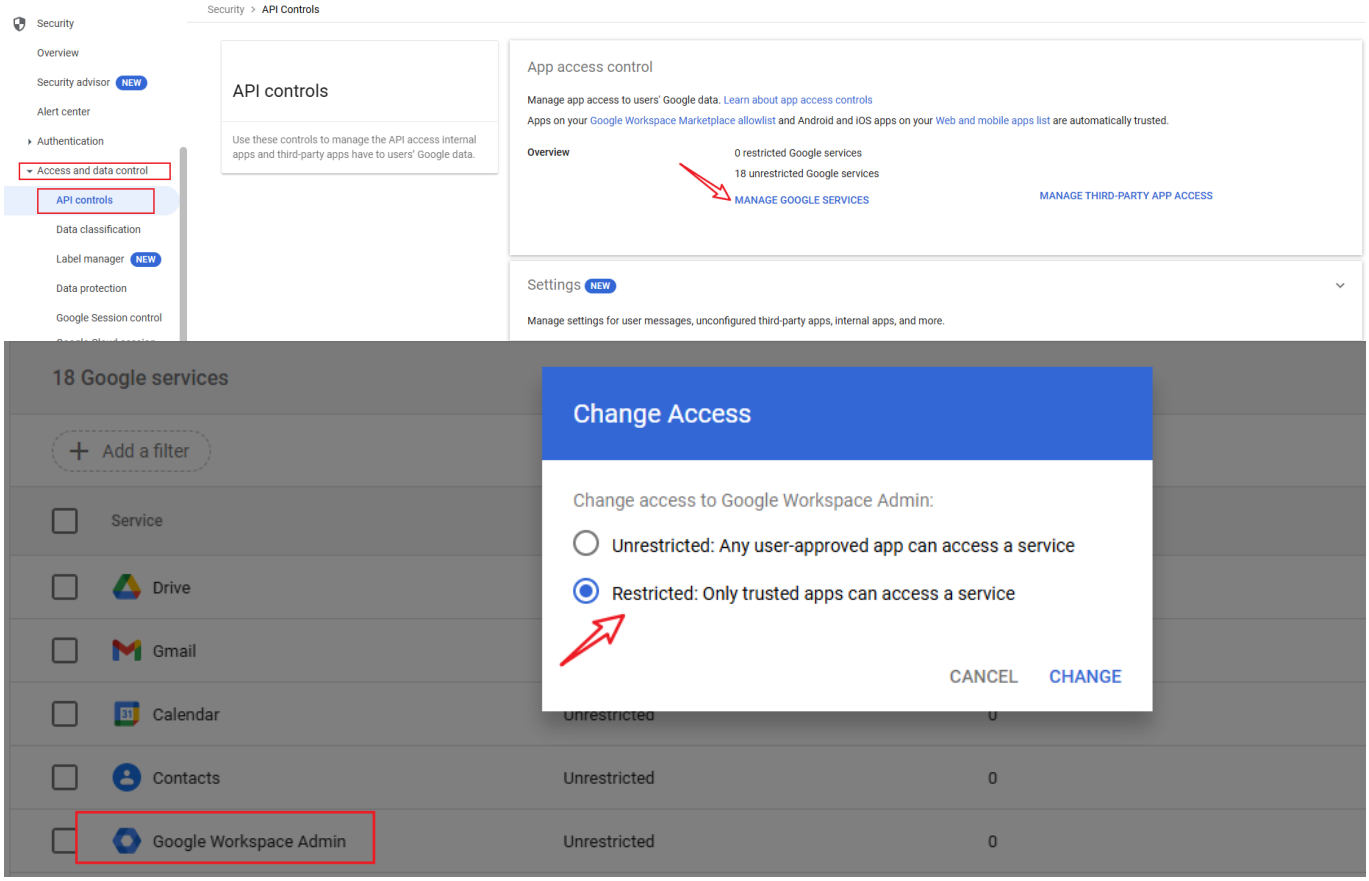
go to configure a third-party pre-integrated cloud application, like Asana, as your service provider?

1. **Apps > Web and mobile apps > Add App > Search for apps. Then search for Asana from the list of predefined applications**
2. Security > Set up single sign-on (SSO) for SAML applications and provide the necessary information
3. Apps > Web and mobile apps > plus sign (+) > SETUP MY OWN CUSTOM APP from the Enable SSO for SAML Application window
4. Apps > Settings > Third-party integrations. Then search for Asana.

App安全

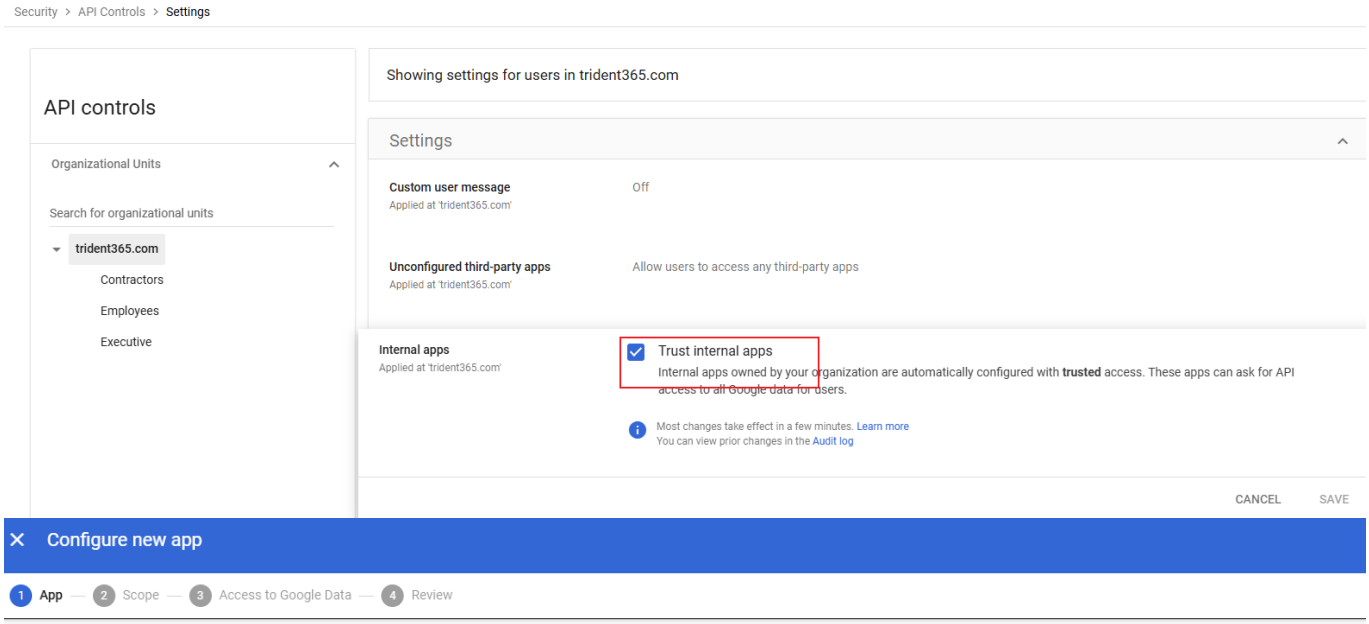
1. Control access from the Admin SDK API
2. Block access to a specific service
3. Create a trusted application list
4. Explore the GWS Marketplace

练习1

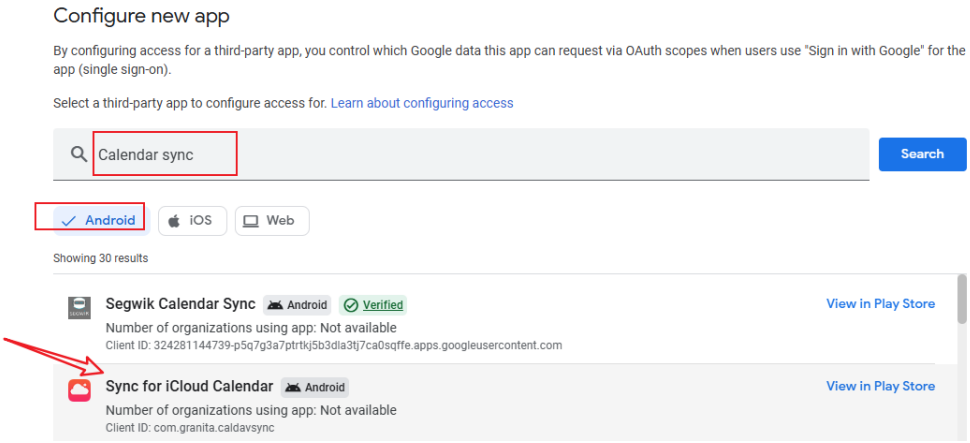


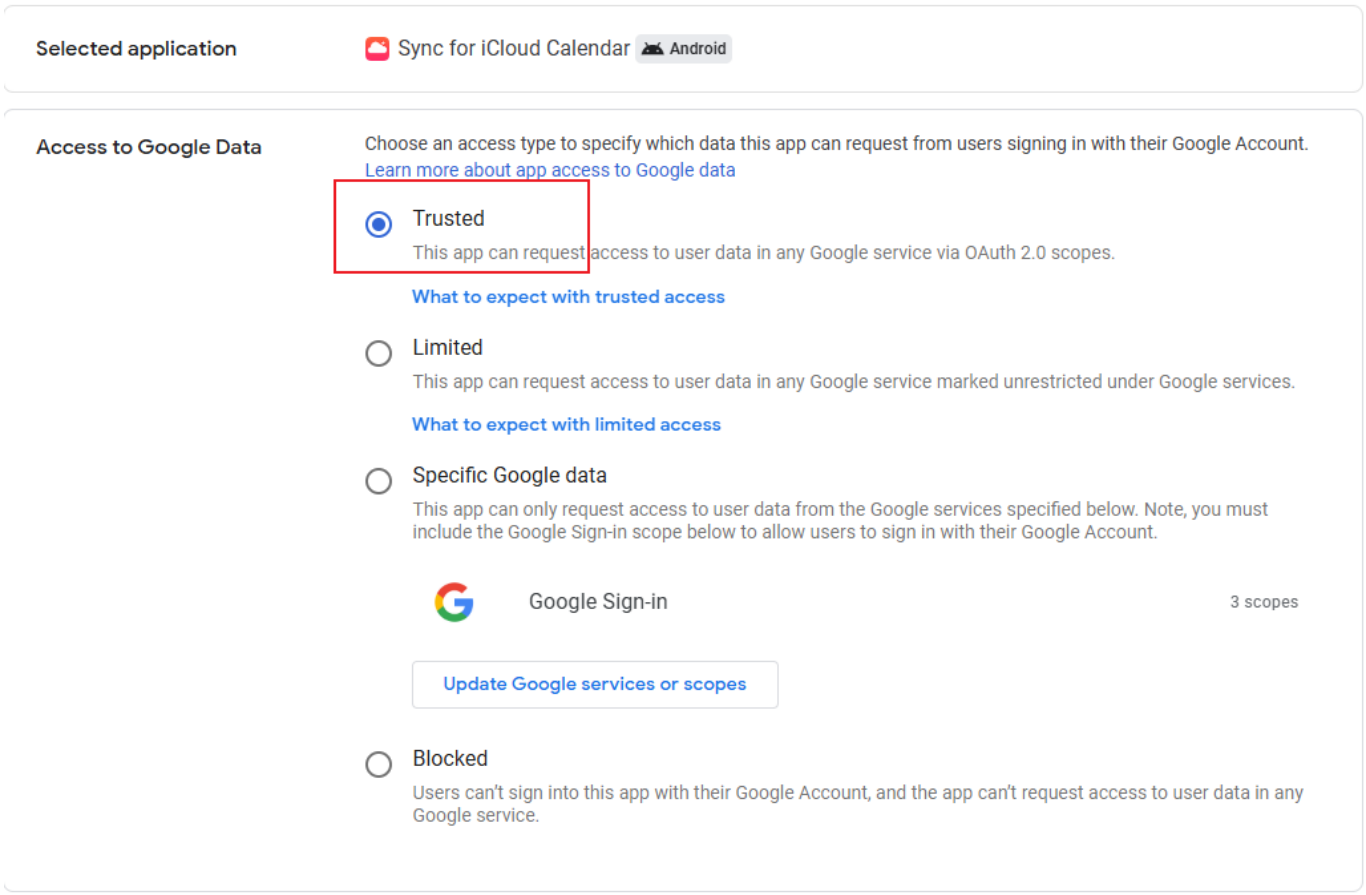
练习2

有许多第三方APP会连到GWS上，作为管理员要进行控制。

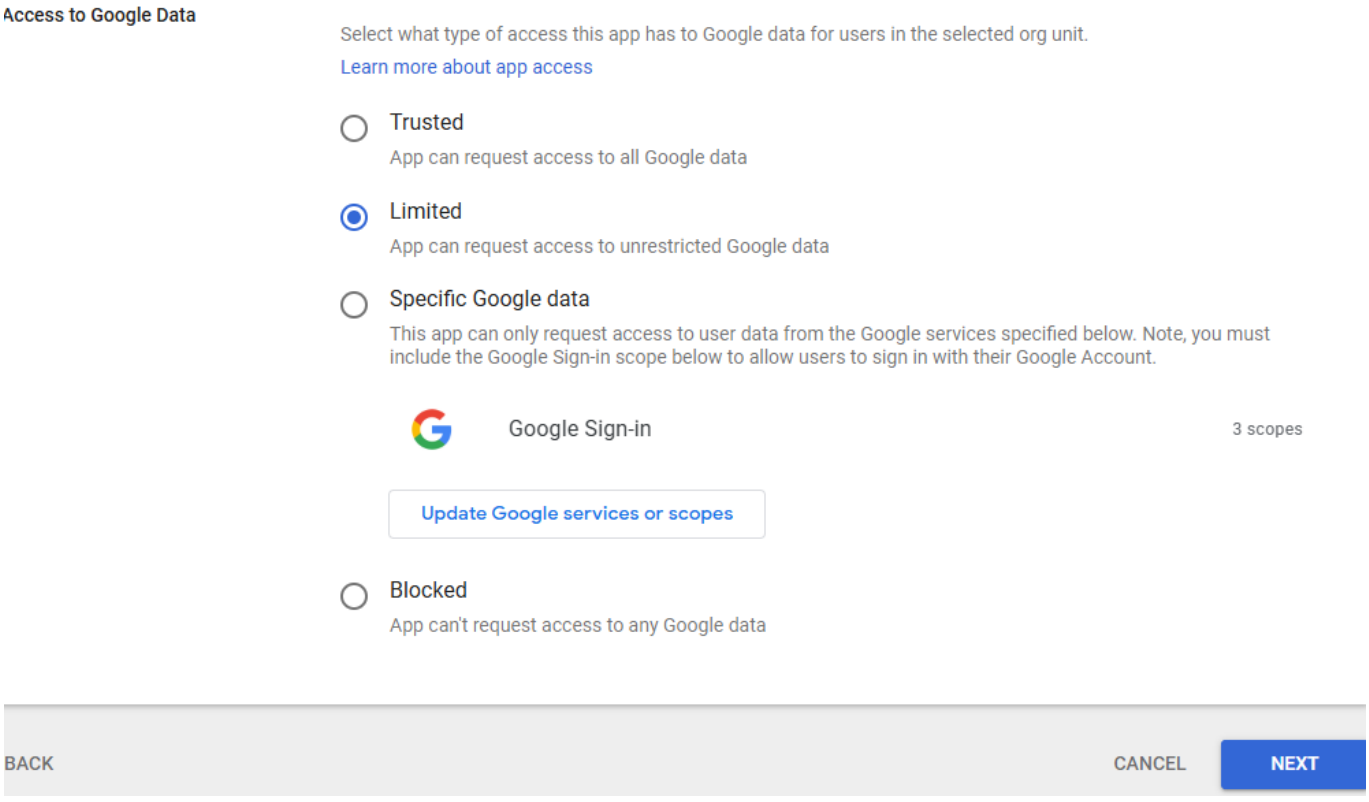

Security > API Controls > Settings
API controls
Organizational Units
Search for organizational units
trident365.com
Contractors
Employees
Executive
Showing settings for users in trident365.com
Settings
Custom user message
Applied at 'trident365.com'
Off
Unconfigured third-party apps
Applied at 'trident365.com'
Allow users to access any third-party apps
Internal apps
Applied at 'trident365.com'
Trust internal apps
Internal apps owned by your organization are automatically configured with trusted access. These apps can ask for API access to all Google data for users.
Most changes take effect in a few minutes. Learn more
You can view prior changes in the Audit log
CANCEL
SAVE

Configure new app
1 App
2 Scope
3 Access to Google Data
4 Review


Configure new app
By configuring access for a third-party app, you control which Google data this app can request via OAuth scopes when users use "Sign in with Google" for the app (single sign-on).
Select a third-party app to configure access for. Learn about configuring access
Calendar sync
Search
Android
iOS
Web
Showing 30 results
Segwik Calendar Sync
Android
Verified
View in Play Store
Number of organizations using app: Not available
Client ID: 324281144739-p5q7g3a7ptrtkj5b3dla3tj7ca0sqffe.apps.googleusercontent.com
Sync for iCloud Calendar
Android
View in Play Store
Number of organizations using app: Not available
Client ID: com.granita.caldavsync



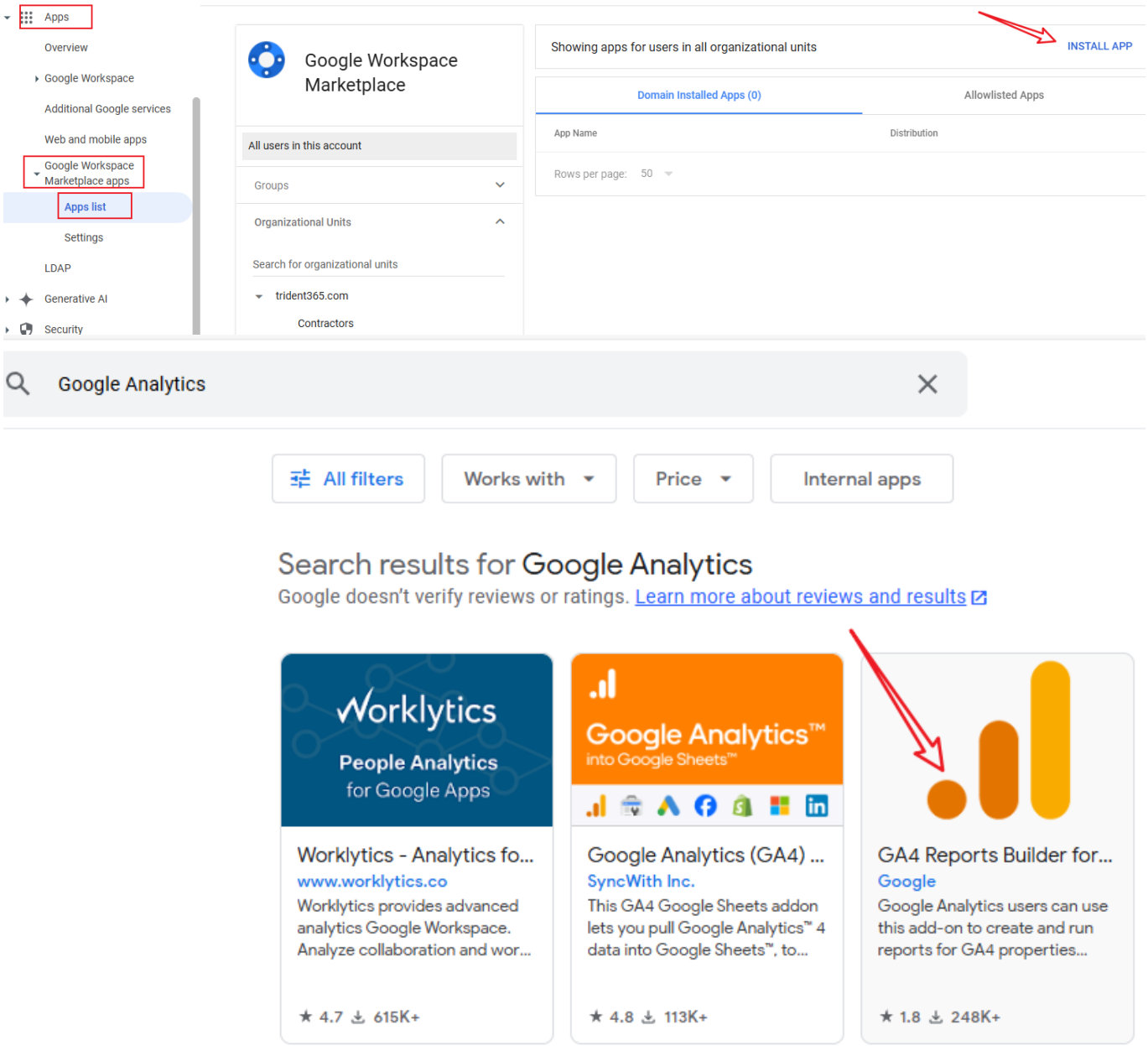
最后点FINISH，然后再把它限制



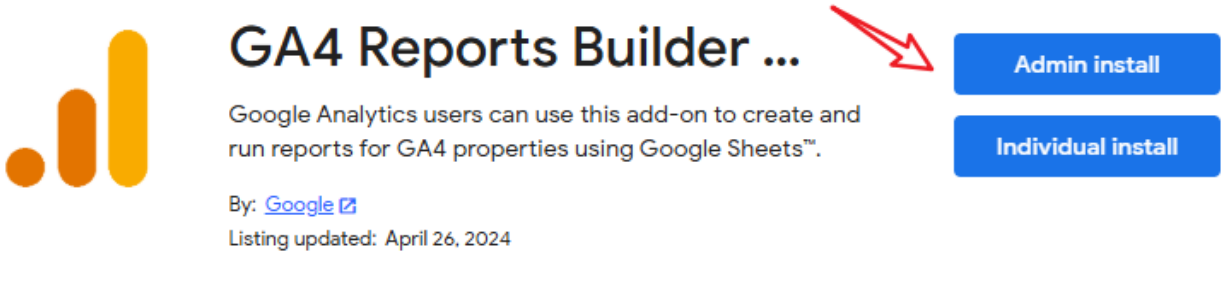
1.如果你想禁用API访问，但想使用某些已经安装的应用，则把这些应用放到TrustedList中，然后再禁用API 2.当用户想安装被禁用的APP，会收到错误信息

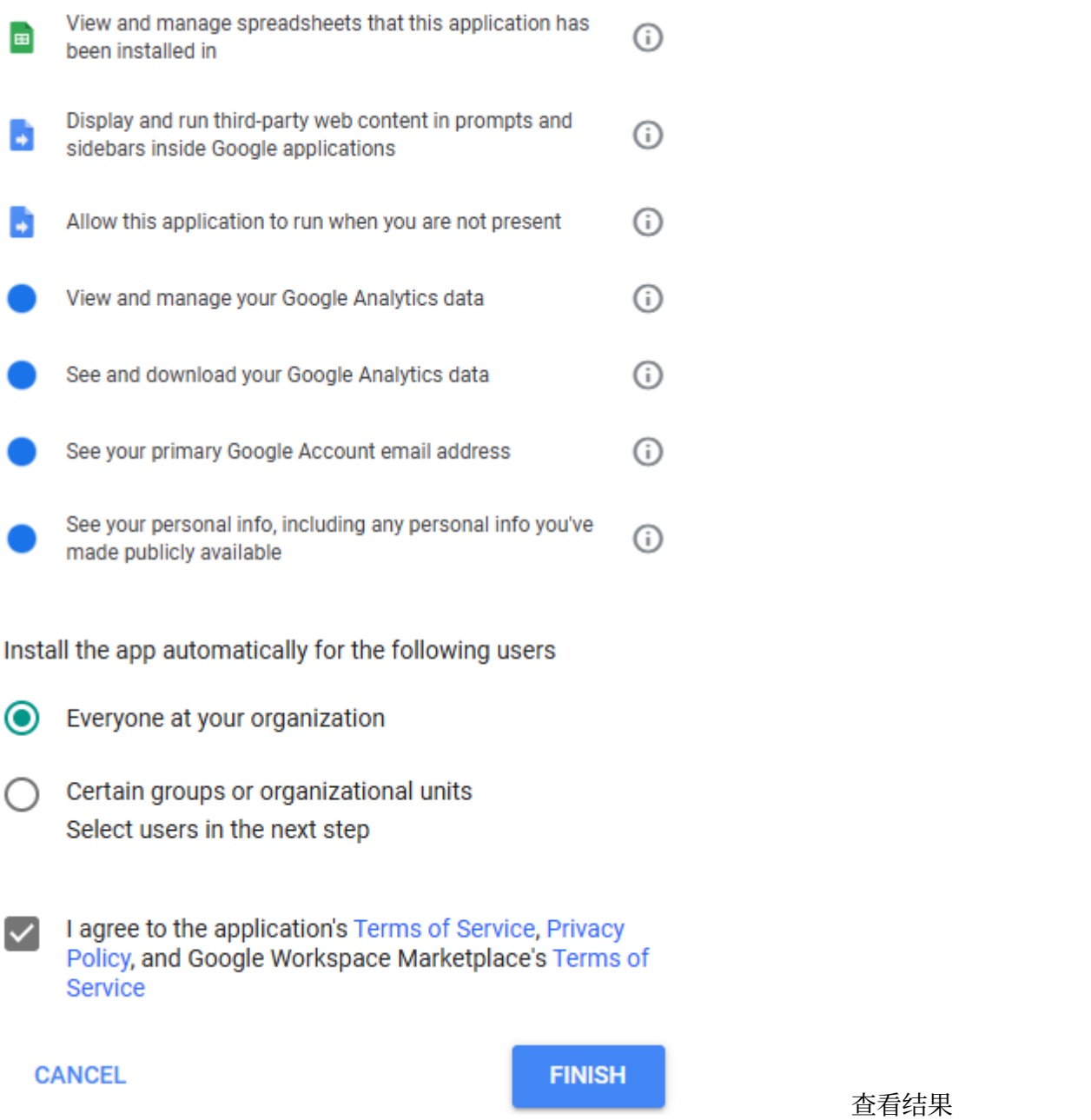
参考链接：https://support.google.com/a/answer/7281227

练习3

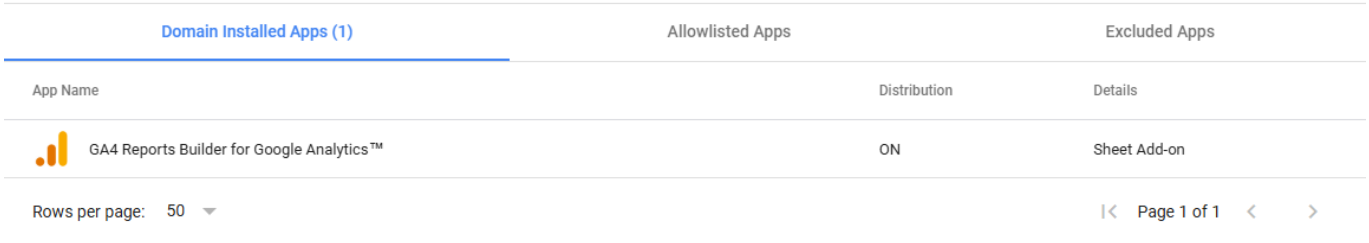


安装GA4

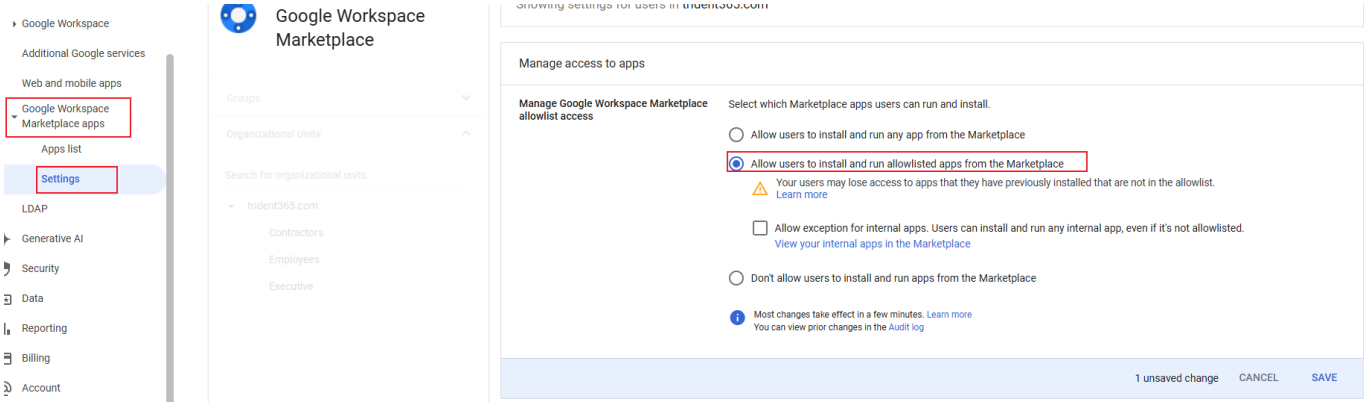




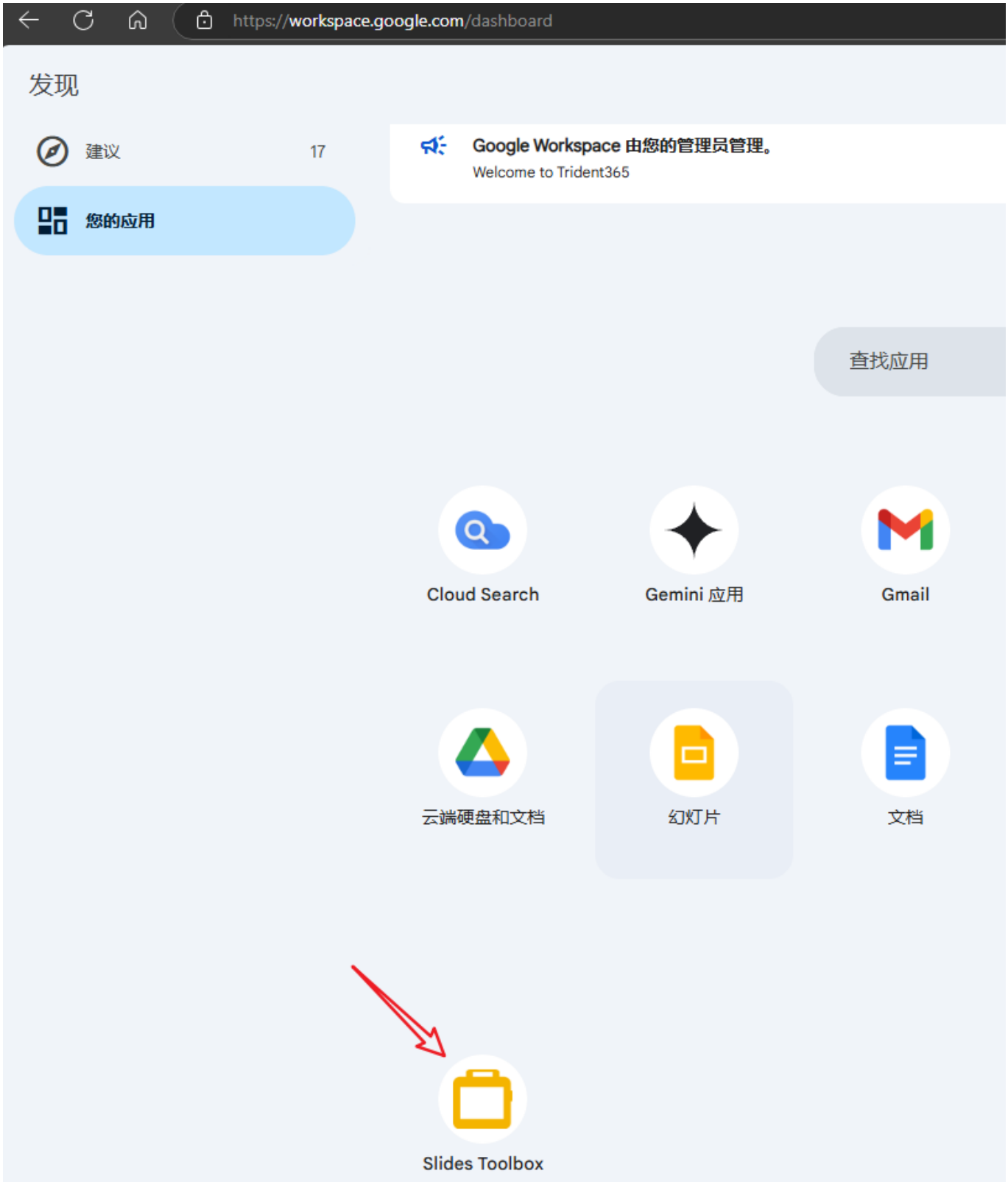
查看结果



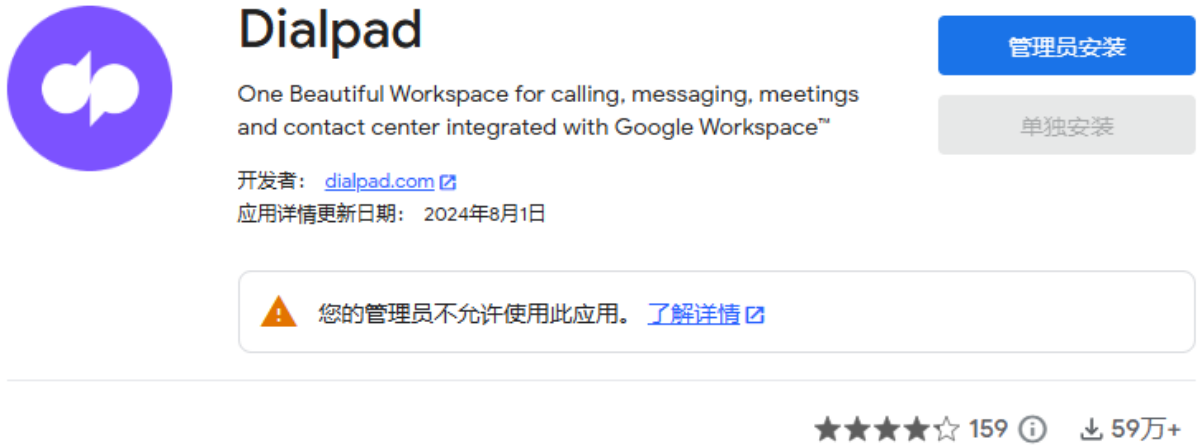
然后设置，只允许用户安装白名单的APP



再添加白名单APP□练习中要求添加Google Apps Script,但我没找到，于是改为Slides Toolbox 换成某一个用户的账号登录，查看URL apps.google.com/user/hub,发现已经出现了



再打开Market，任意安装一个APP，会跳出提示



测试3

What happens to already installed applications if you block API access from the Security > API Permissions section?

1. Already installed applications that use the blocked API will continue to work until the application needs a new OAuth token
2. **Already installed applications will stop working and OAuth tokens will be revoked**
3. Already installed applications that use the blocked API will continue to work indefinitely
4. Already installed applications that use the blocked API will continue to work until the user next signs in to Google Workspace

What is the expected behavior when a user tries to install a Marketplace app that has not been allowed?

1. **Users can not attempt to install an application that is not on the allowlist because they only see allowed apps in the Marketplace**
2. When the user attempts to install the app they will see a message advising that the app cannot be installed because it has not been allowed
3. Users can install an app that is not in the allowlist but they cannot grant it access to their data so it will not work
4. The app will appear to install, but it will not function correctly.

You have been asked to create a allowlist of Marketplace apps to restrict which apps a user can install onto their devices. What must you do first?

1. **Change the Marketplace settings to allow users to install only allowed applications from Google Workspace Marketplace**
2. Complete a Domain install for each application that you want to allow
3. Get your users to Install the Marketplace allowlist app onto each device
4. Add the names of all the trusted applications to each user's device policy

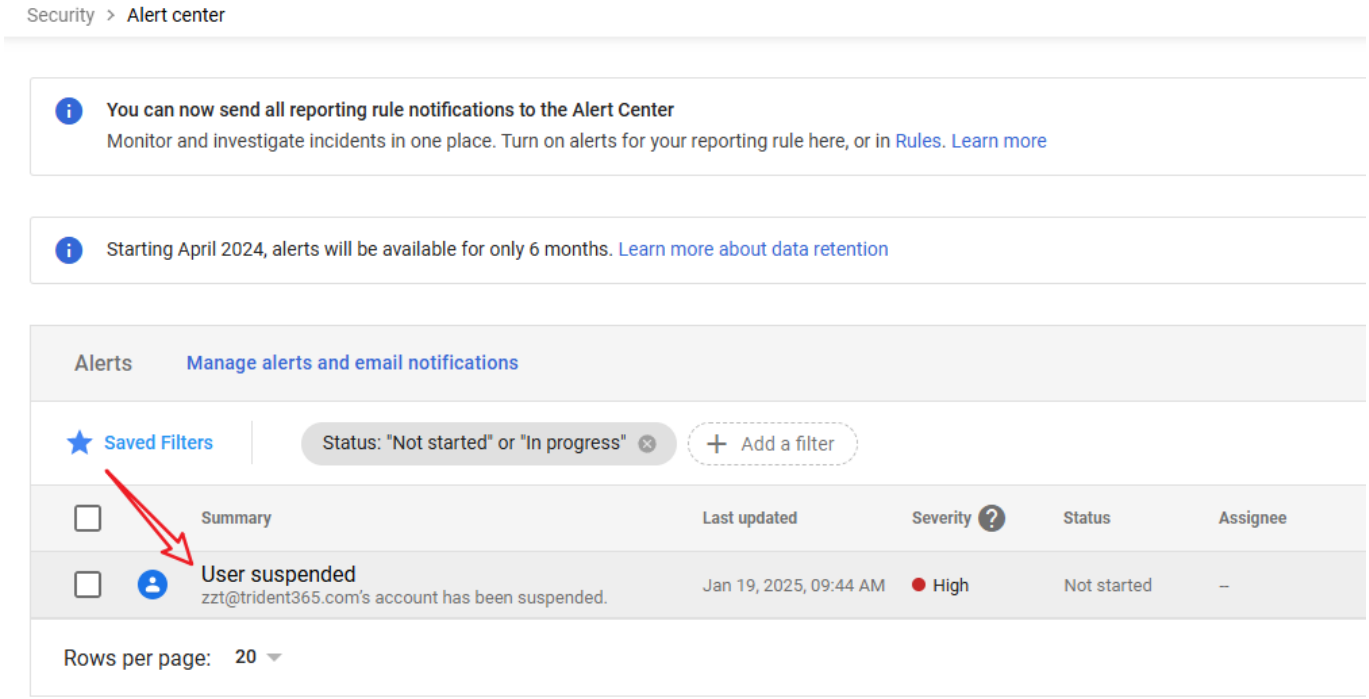
Your organization wants to prevent any external application from accessing Gmail and Drive data. How would you ensure such access is prevented?

1. Disable API access from the Gmail and Drive service settings

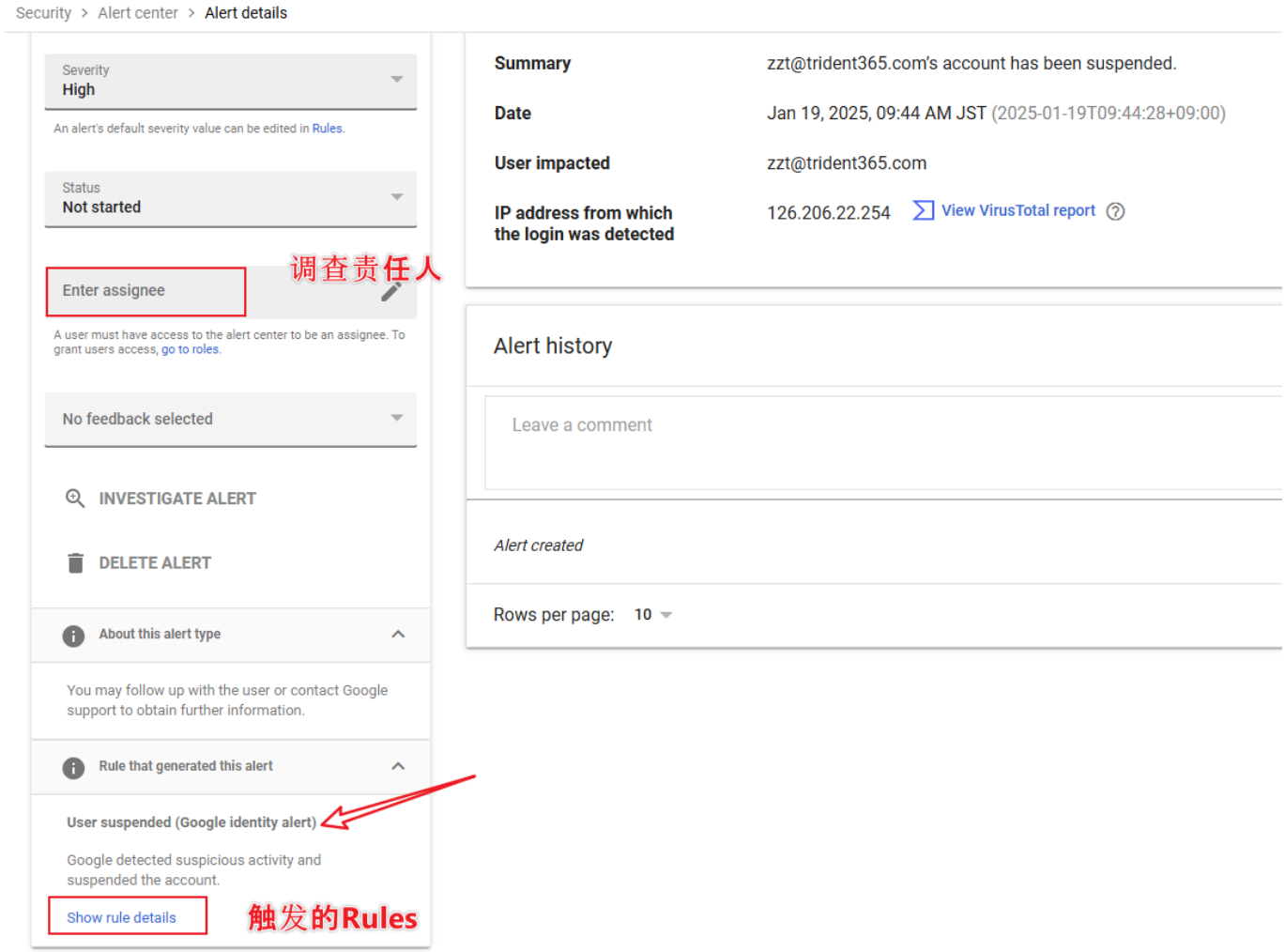
2. **From Security > Access and Data Control > API Controls, ensure Trust domain owned apps is enabled. From Security > Access and Data Control > API Controls > MANAGE GOOGLE SERVICES, restrict access to the Gmail and Drive services.**
3. From Security > API Permissions, ensure Trust domain owned apps is disabled. From Security > API Permissions > MANAGE GOOGLE SERVICES, restrict access to the Gmail and Drive services.
4. Disable Gmail and Drive API access from the top level organization settings

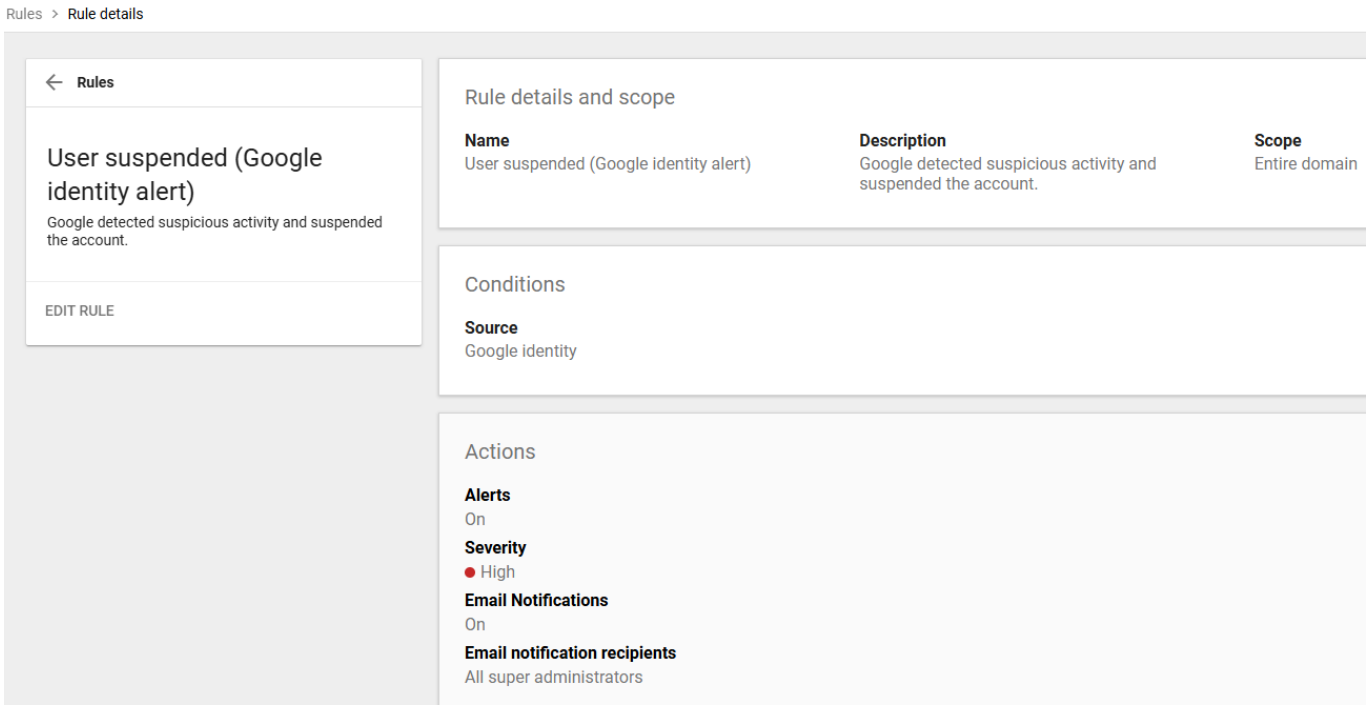
练习1

Security>Alert Center

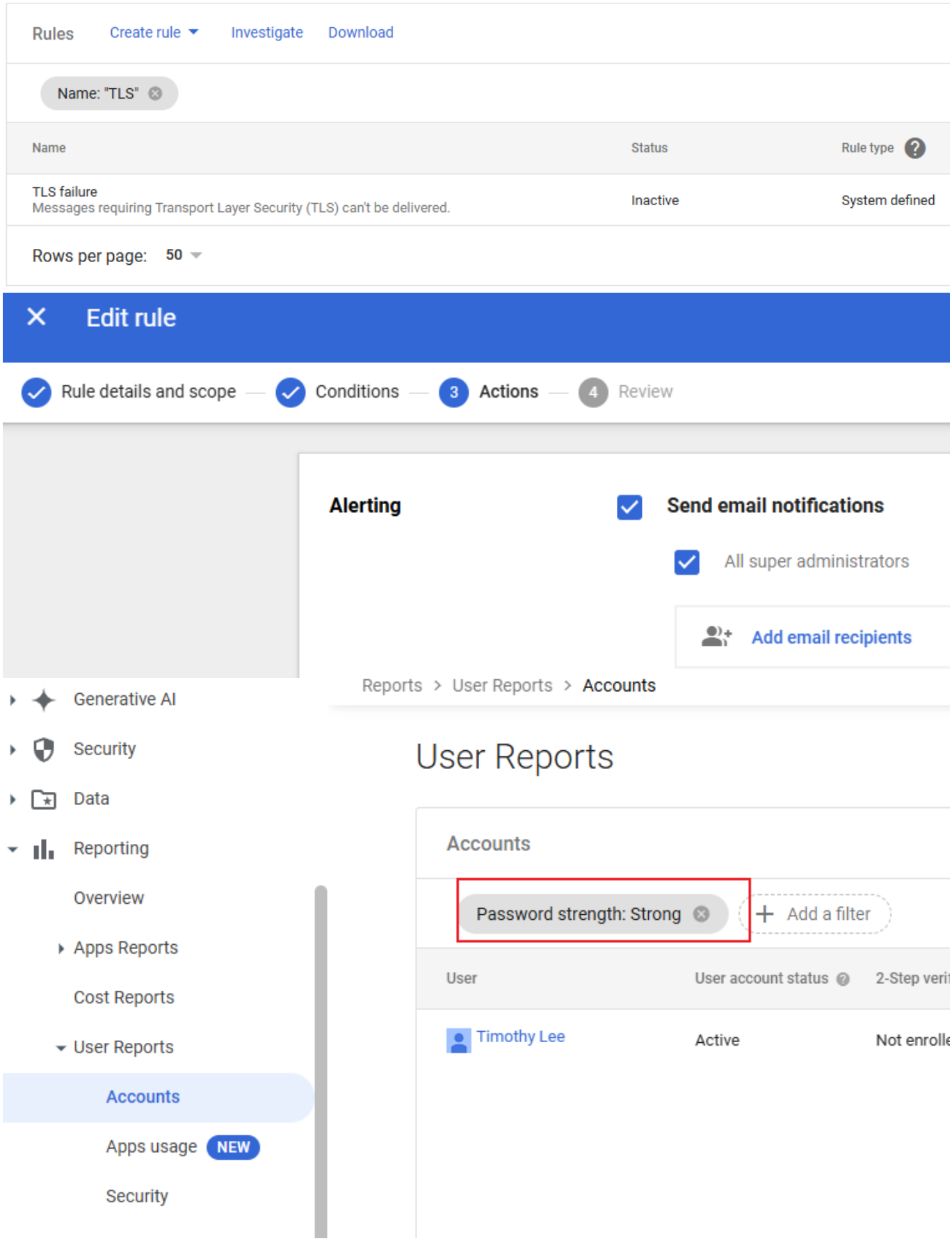


发现有一个高危警报User suspended





找到TLS Failure



系统预设的Rule只能设置Email通知（被触发时）

练习2

Reporting>User reports>Accounts,使用密码强度来筛选，查看结果

Security Center

1. Security best practice
2. Analytics
3. Actionable insights

还可以查看各类设置的状态，比如

1. Automatic email forwarding
2. Device encryption
3. Drive sharing settings

查看各类报警，比如

1. External file share activity
2. Authenticated messages
3. Suspicious device activities
4. Failed password attempts

Dashboard里则有各种图表，另外，还可以查看Log

1. Access device-log data
2. Access data about Gmail messages
3. Access Gmail log data
4. Access Drive log data

举例来说，我们可以通过Query来确认，是否有如下行为

1. Delete specific messages
2. Mark messages as spam or phishing
3. Send message to quarantine
4. Send message to users' inboxes

这些与MS家的EDR中的Query有些类似，要学会写Query语句

From:
https://www.trident365.com/ - **三叉戟**

Permanent link:
https://www.trident365.com/doku.php?id=resources:courses:gws_c3&rev=1737622945

Last update: **2025/01/23 18:02**