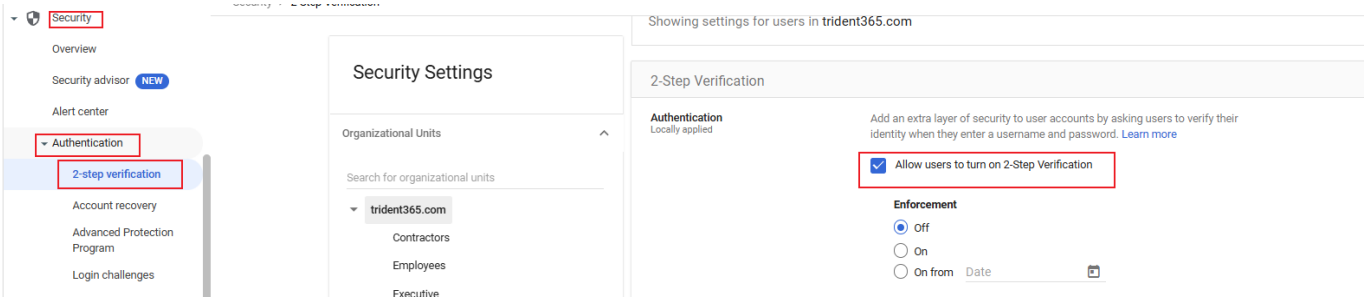
第3章 GWS安全

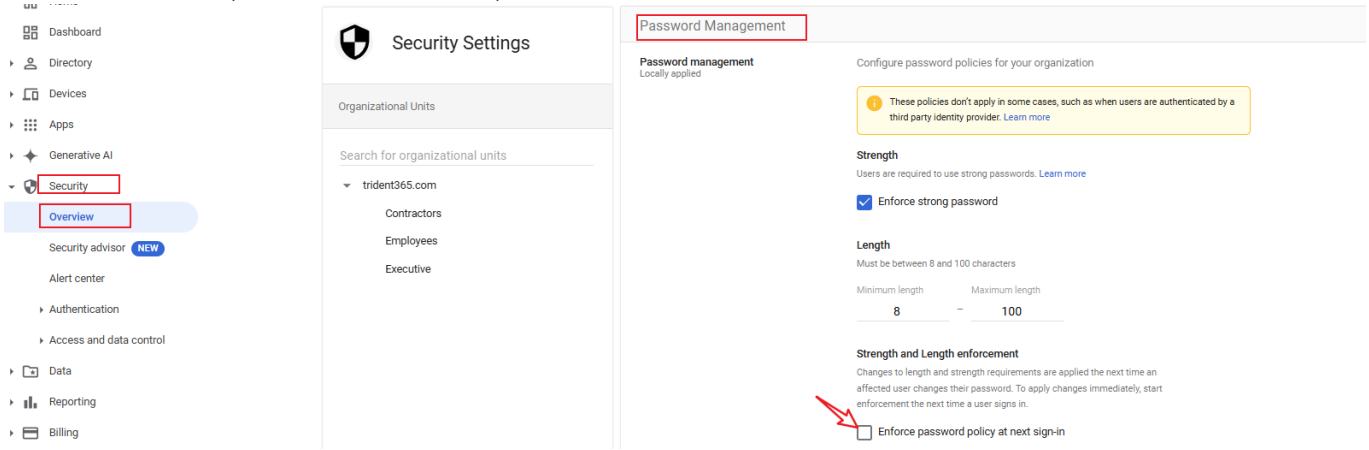
练习1

准备GWS域名，已经完成，略

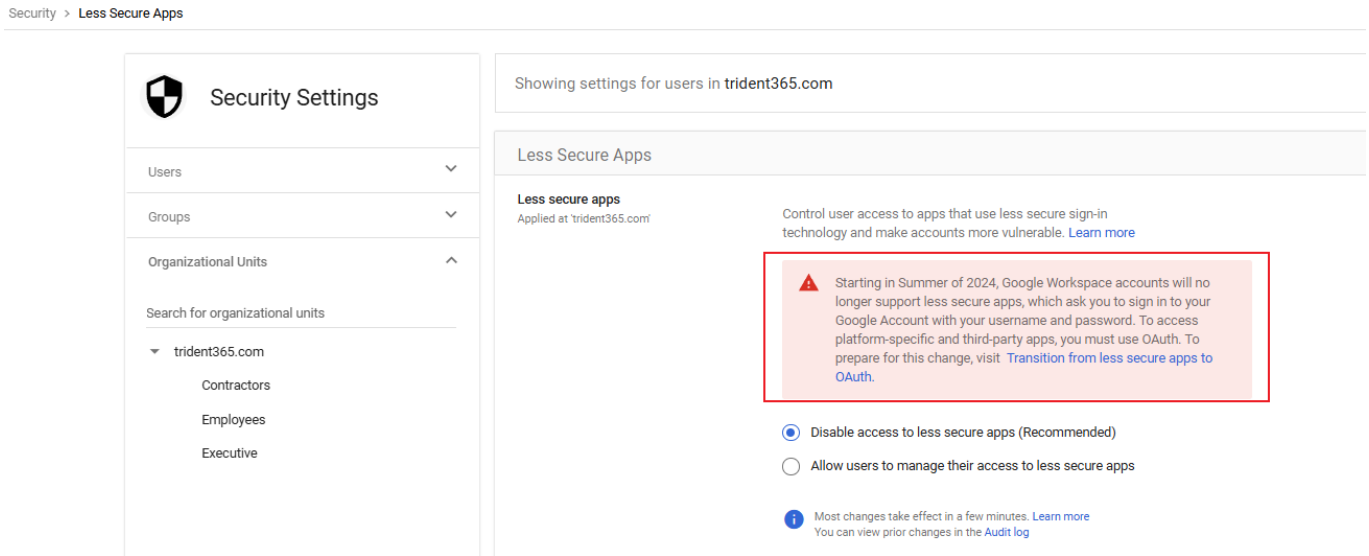
配置通用安全设定



默认2FA是打开的，用户可以自行设定，但不是必须的。

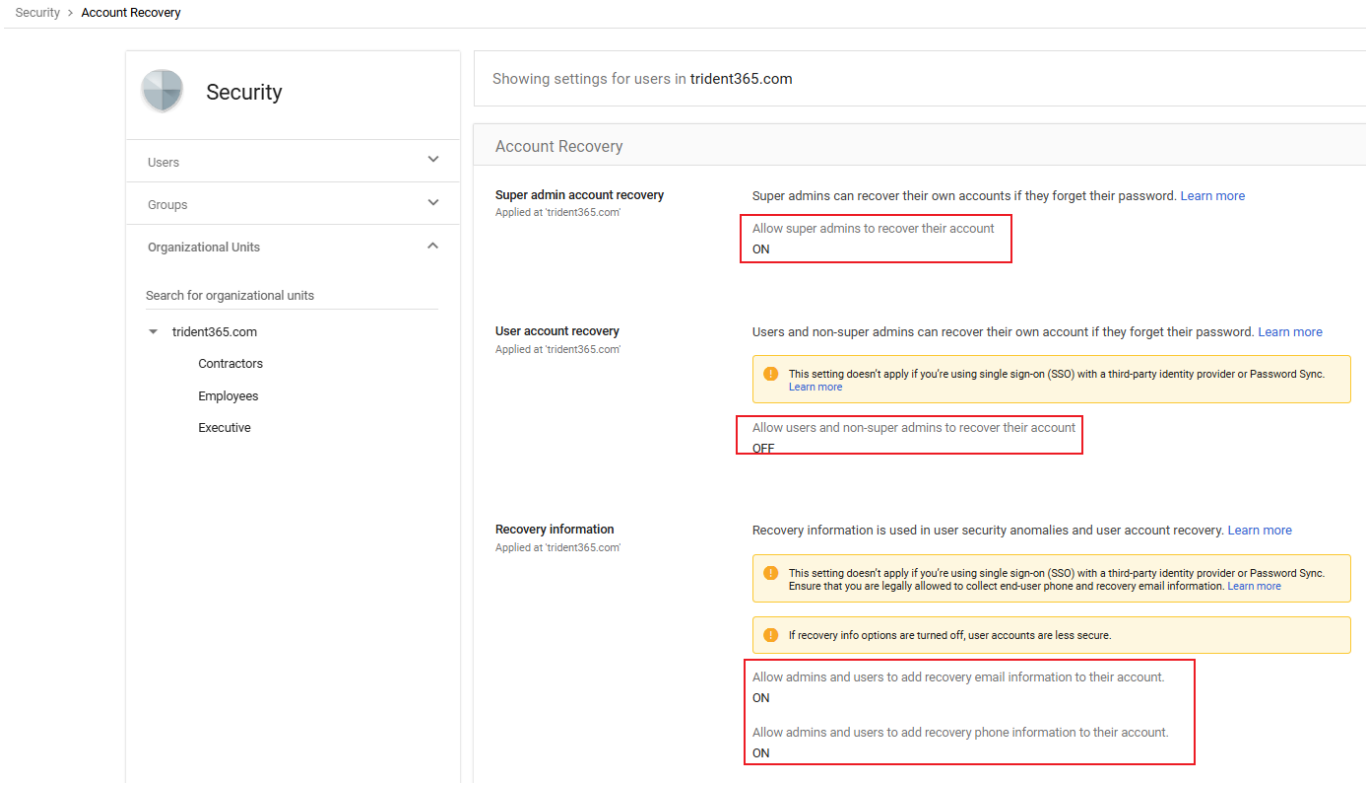


如果要变更PW方针，可以勾选下次登录时执行，这个方针适用单位是OU或以上。



这里刚好有一个更新，2025年1月之后，所有第三方APP

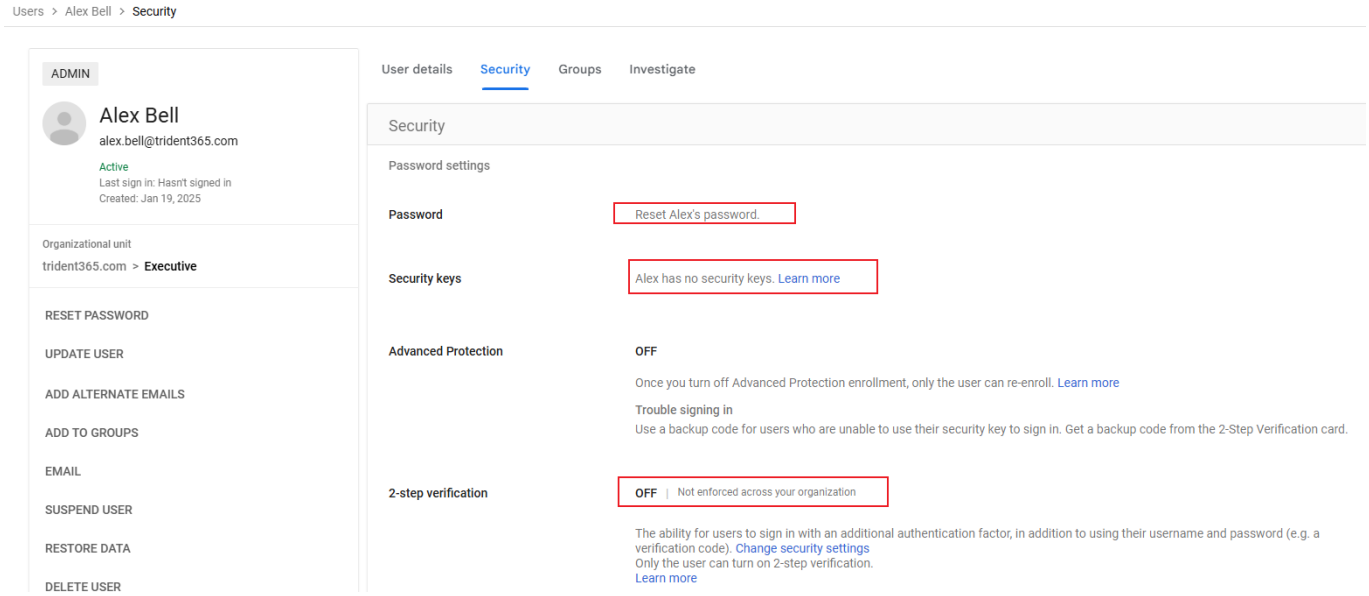
https://support.google.com/a/answer/14114704?hl=ja&sjid=8401829336969536596-AP 还有一个设置是恢复账户Console里设置了权限，默认只有超级管理员可以恢复用户账号密码

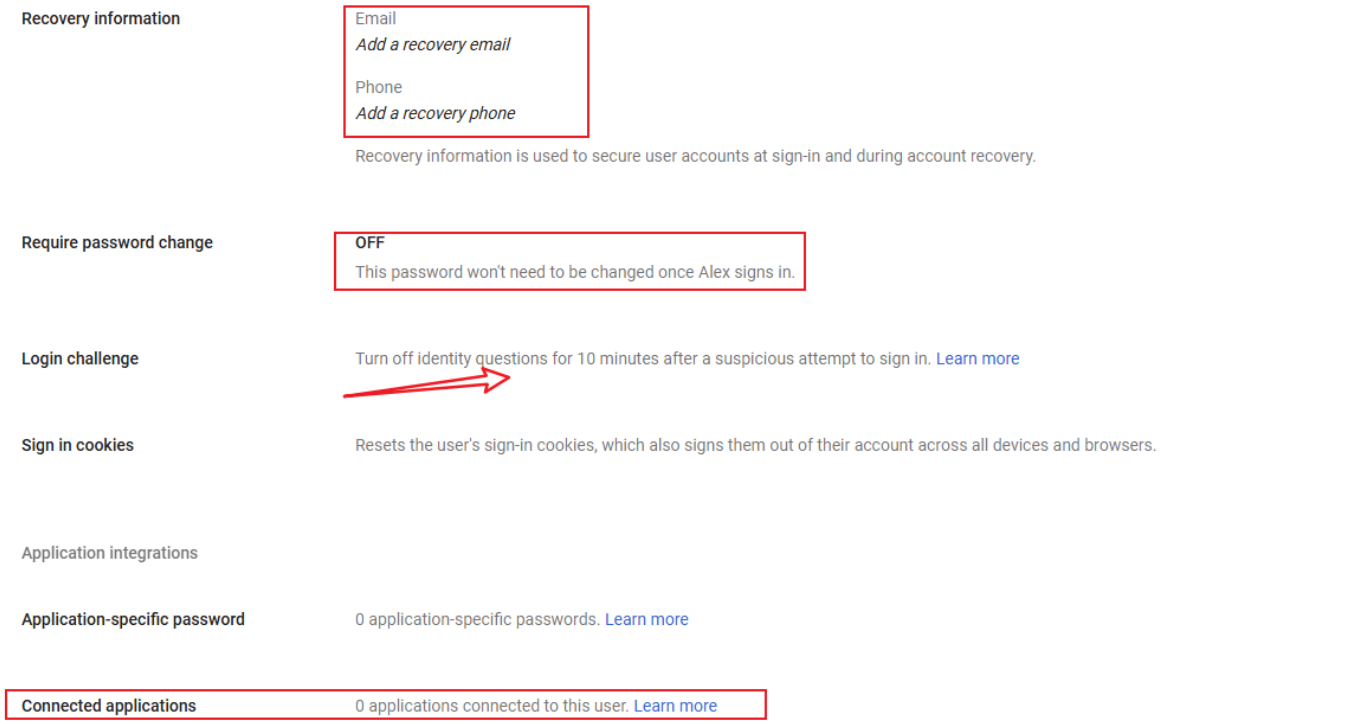


这里把Allow users and non-super admins to recover their account设为ON保存。

练习2

查看用户安全设置

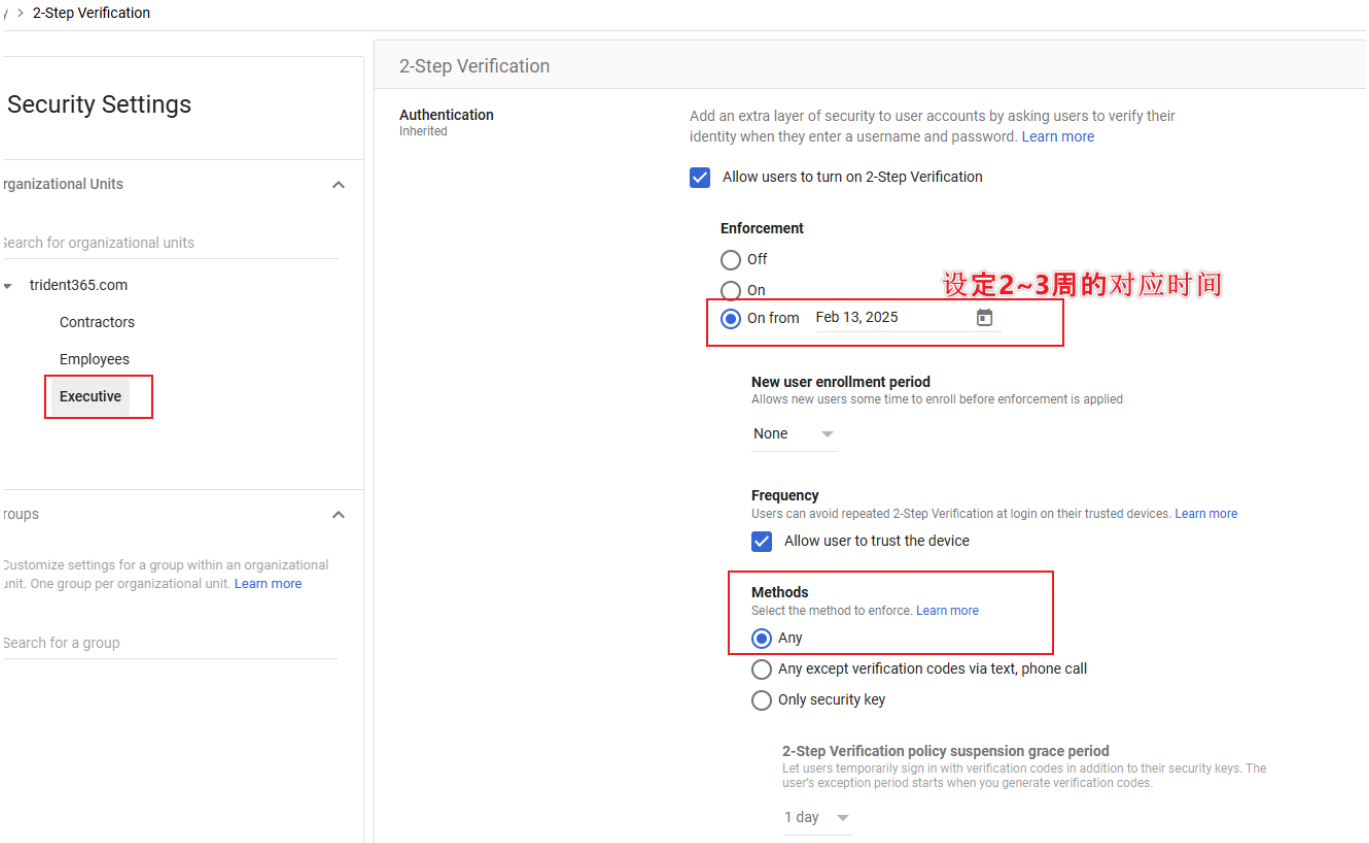




作为管理员，可以强制用户重置密码，也可以为他添加恢复用邮箱和电话号码。另外，当用户登录活动可疑时，如果不能正确验明身份，则账户会被锁，这时管理员可以暂时关闭验证，以让用户本人可以正常登录，修改密码。 还可以查看该账号连携了哪些APP 100名以上用户的IT管理员检查清单：https://support.google.com/a/answer/9211704

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

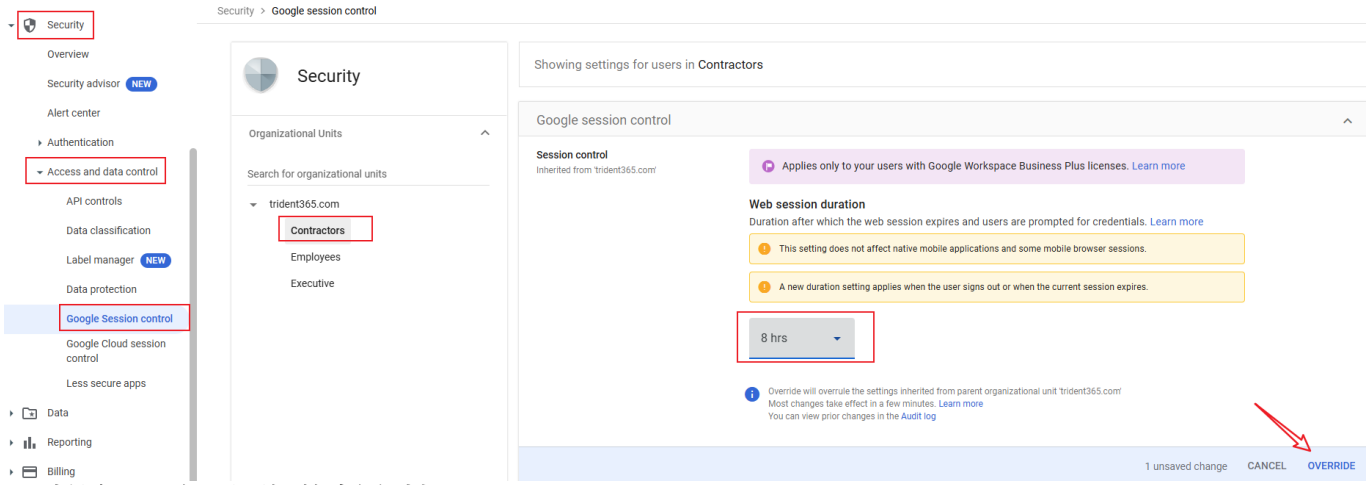
有4种方式

- 通行密钥和安全密钥
- Google提示（如手机端的Gmail）
- 身份验证器（二维码或是OTP等）
- 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)

- **It'll greatly reduce the risk of unauthorized access if a user's password is compromised**
- We wouldn't have to manage individual user IDs and passwords for each user
- It would be a great opportunity to make sure everyone is the organization has a security key
- **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?

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

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

- **Security > Password management**
- Reports > Security
- Users > Account
- 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)

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

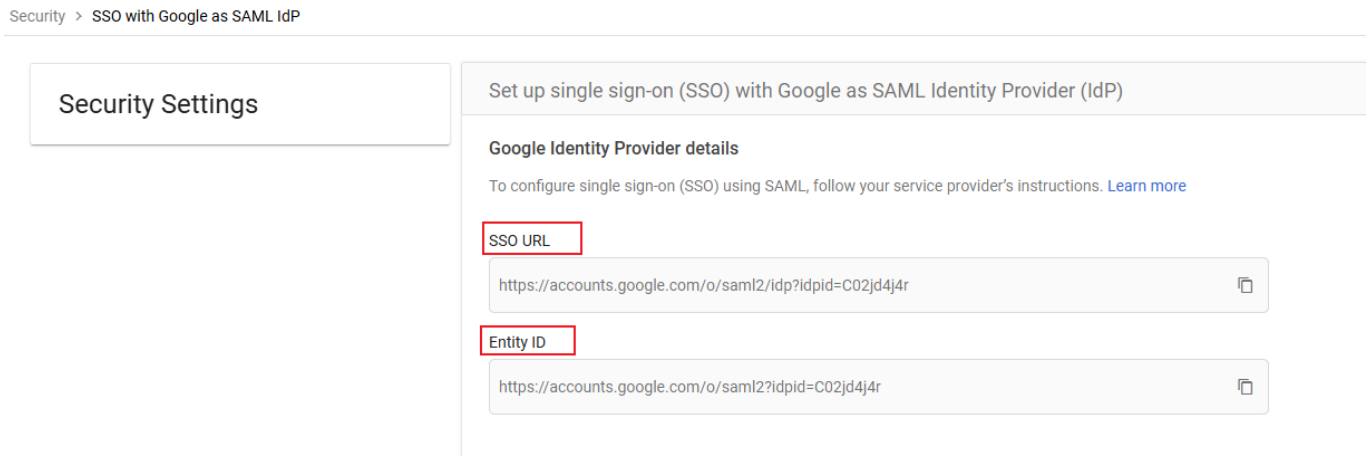
Your organization has decided to enforce 2-step verification in 2 weeks. What actions should you keep

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

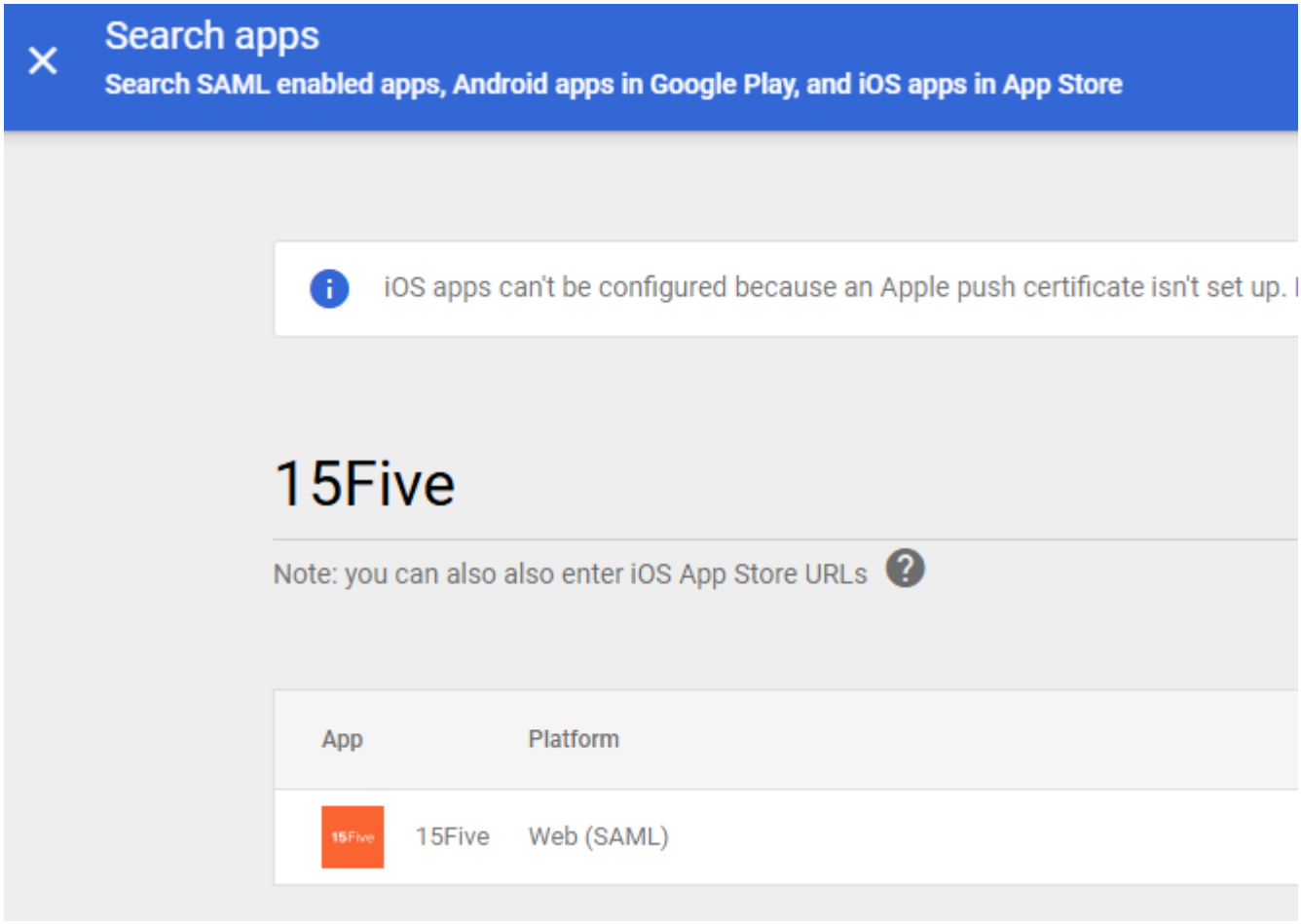
- **You'll want to provide a lead time for users to enroll before enforcement**
- Enforcing 2-step verification will not affect your users as they can still opt-out.
- **When you create new user accounts after enforcement, you will want to allow them a grace period before they need to enroll otherwise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

SSO介绍

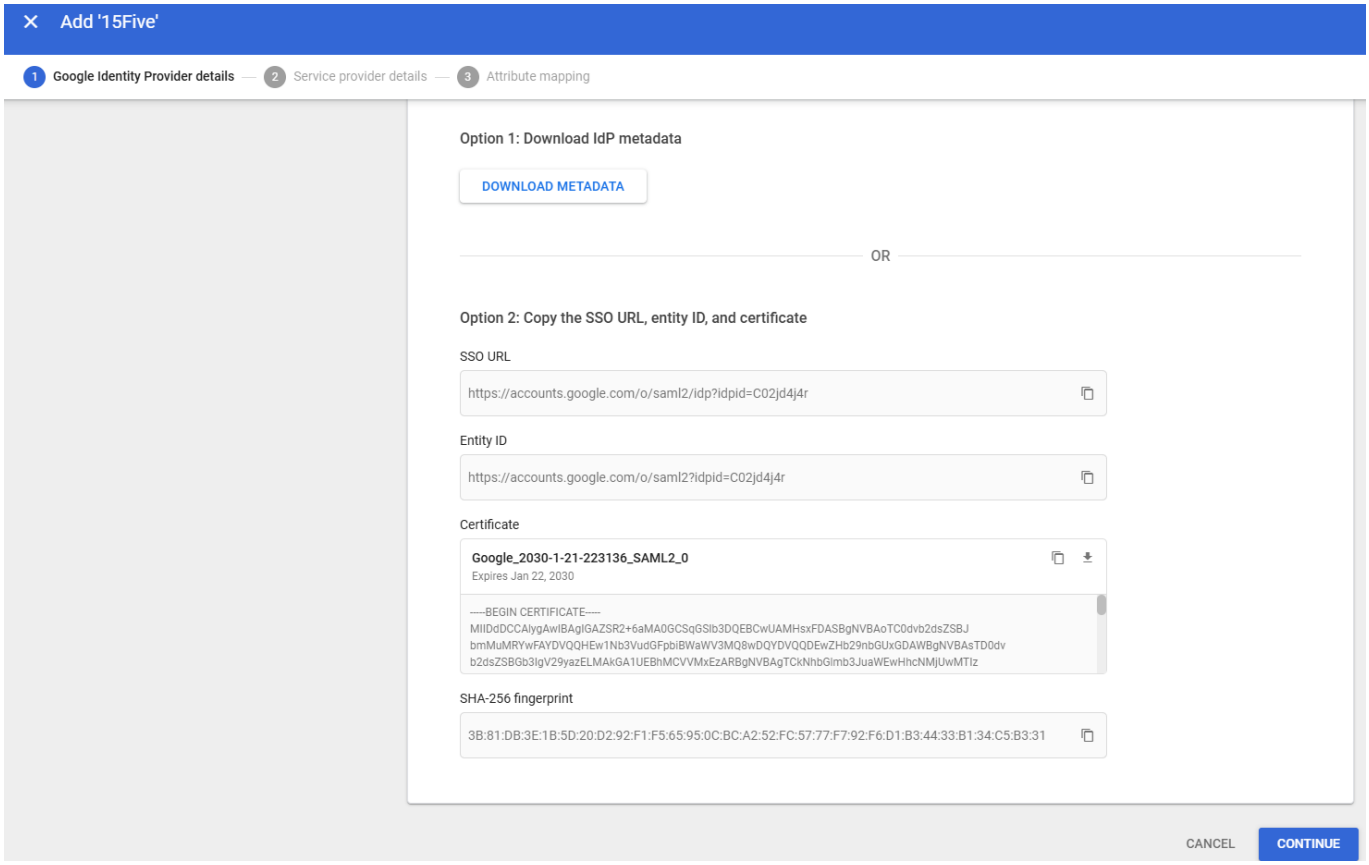
练习1



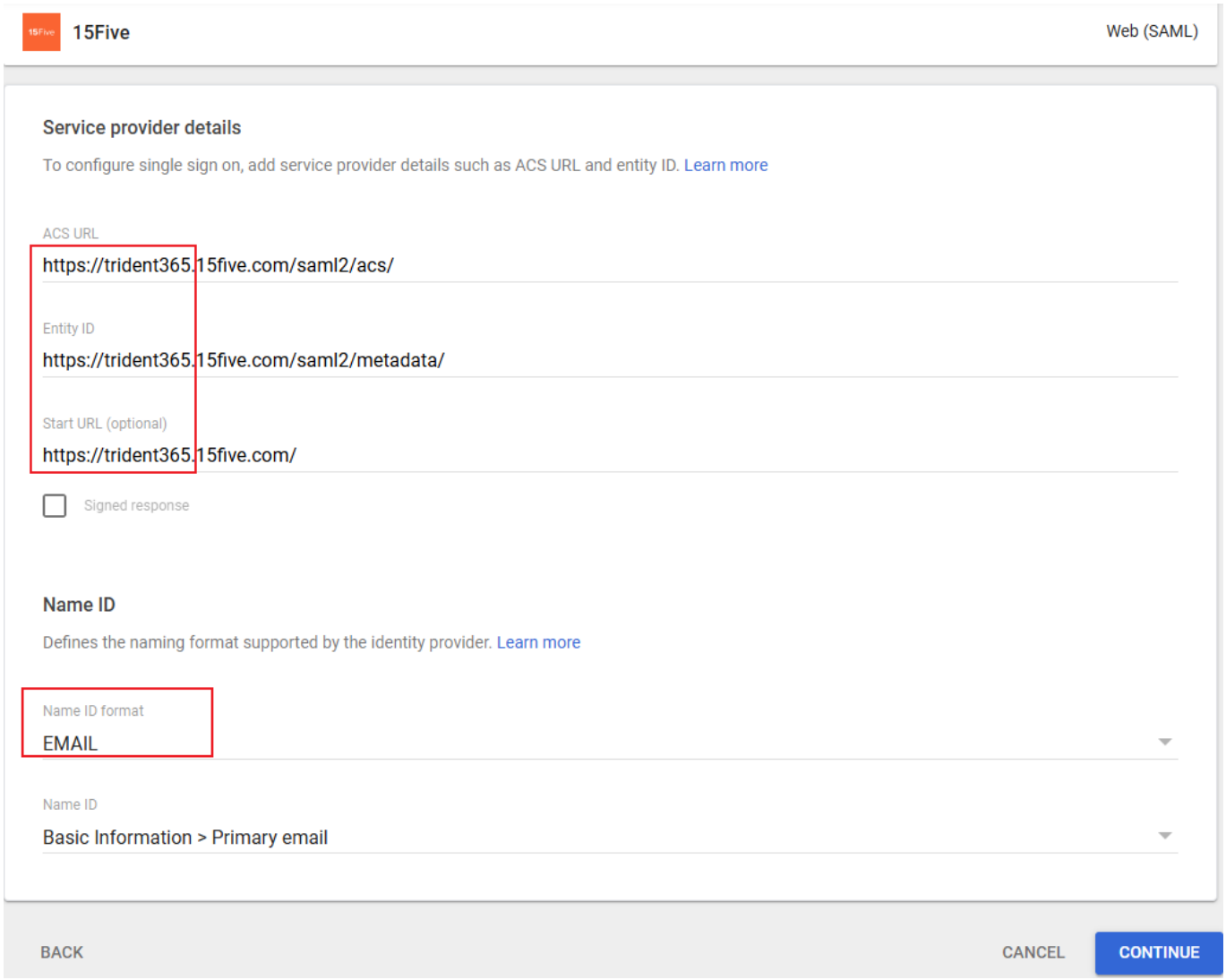
如果要使用SAML来实现SSO，则需要同第三方服务商确认SSO的URL和EntityID信息， App>Search for apps,根据练习要求，搜索15Five



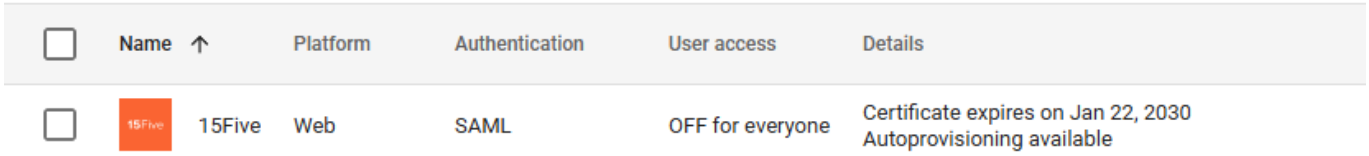
下载Metadata



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

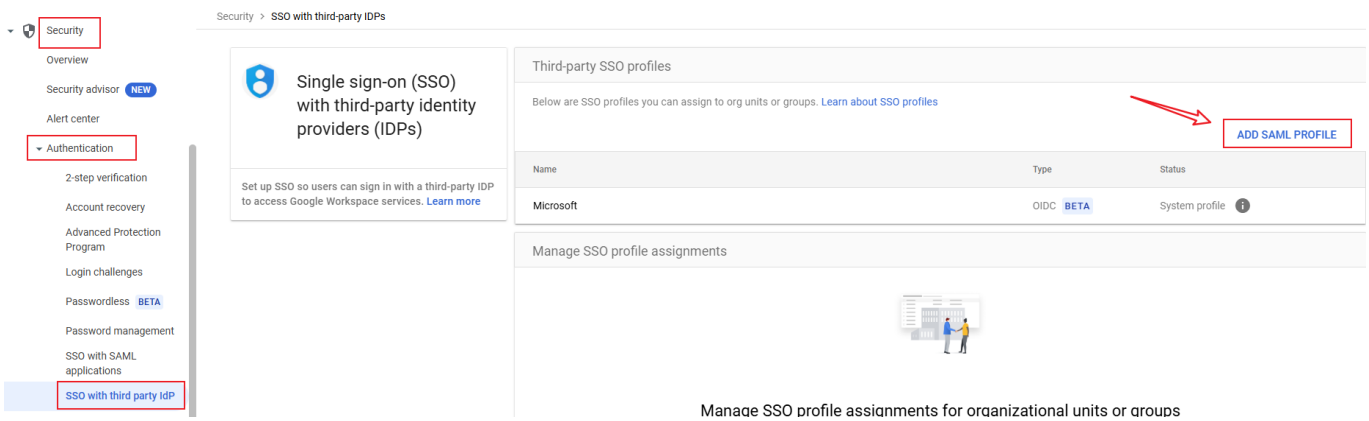


把域名补全，然后ID格式选择Email，继续



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

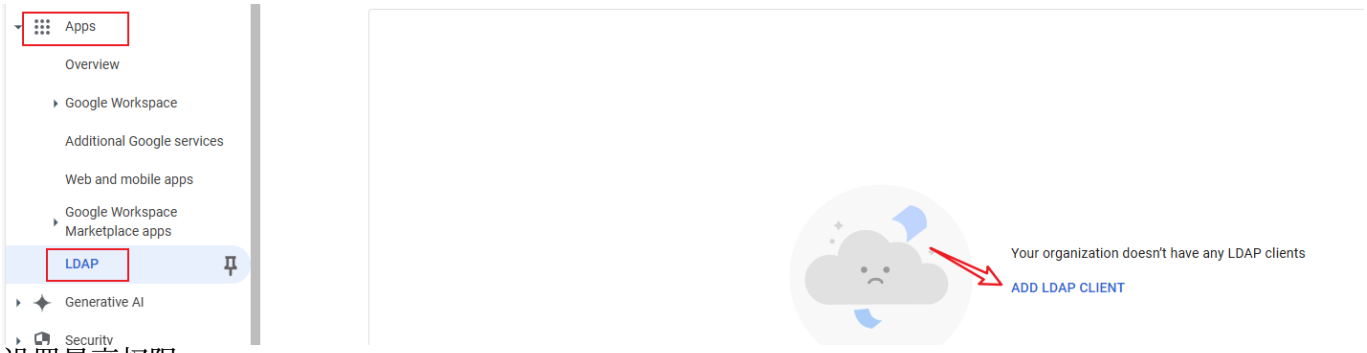
同时管理SaaS和传统程序，需要LDAP服务，除了微软的AD外，还有谷歌的Secure LDAP

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

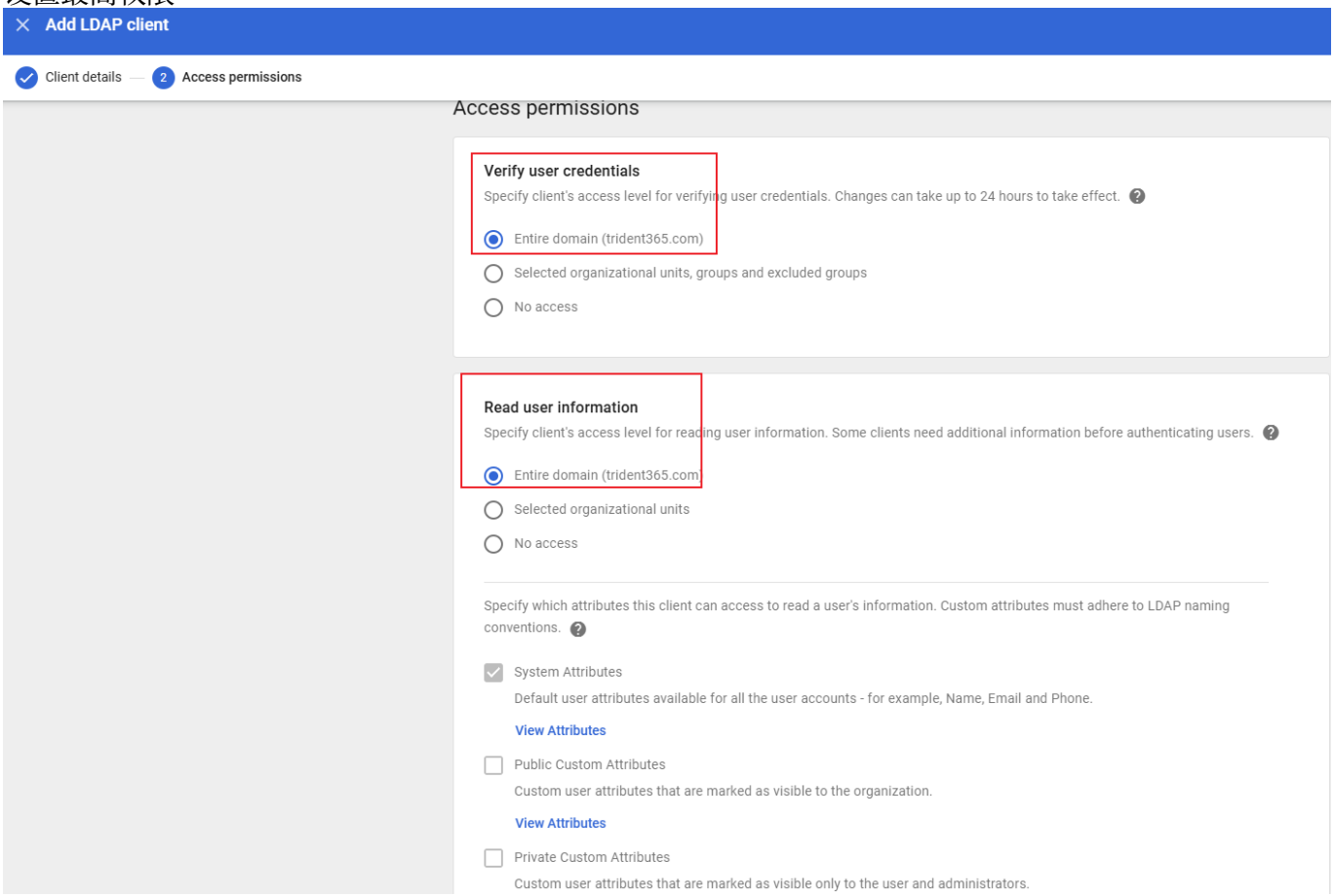
步骤

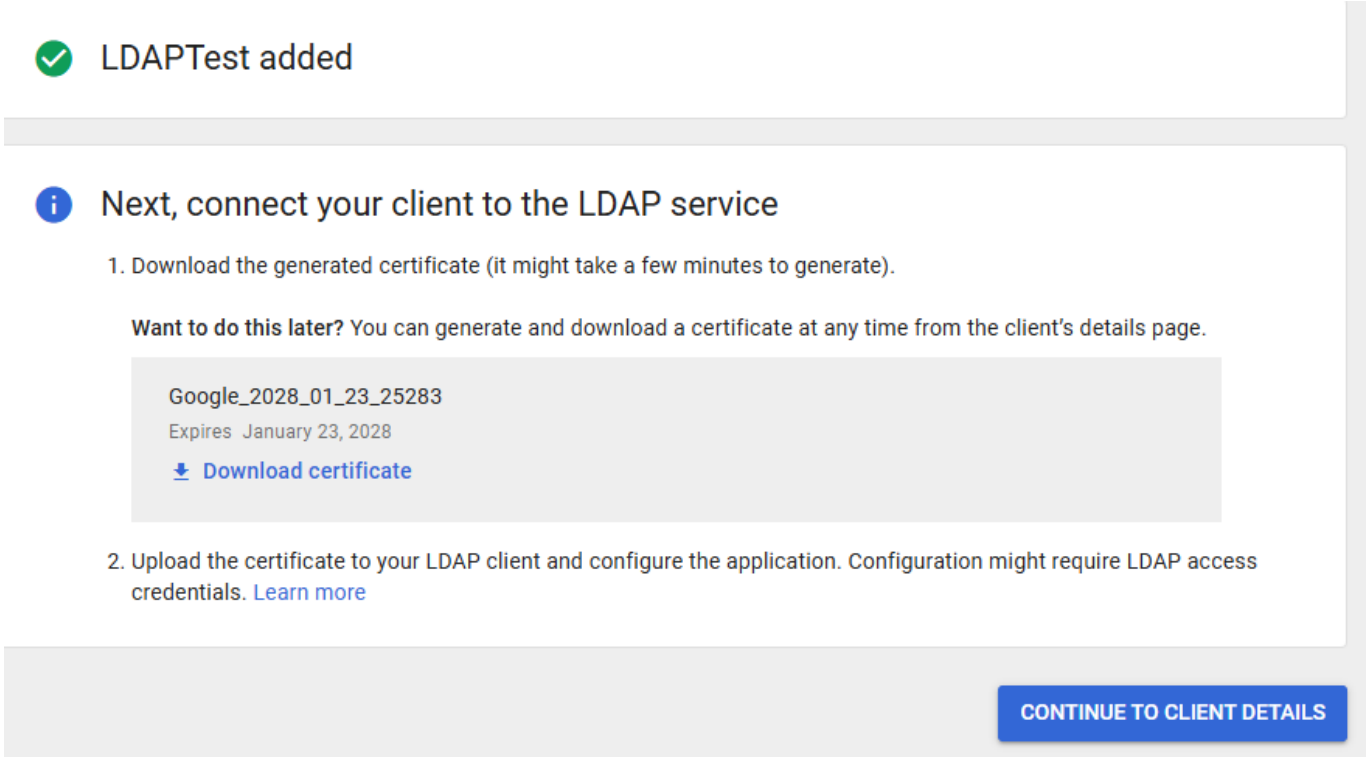
- Create LDAP client in the Admin console
- Configure your LDAP client to connect to the secure LDAP service

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

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

Permanent link:
https://trident365.com/doku.php?id=resources:courses:gws_c3&rev=1737616259

Last update: **2025/01/23 16:10**