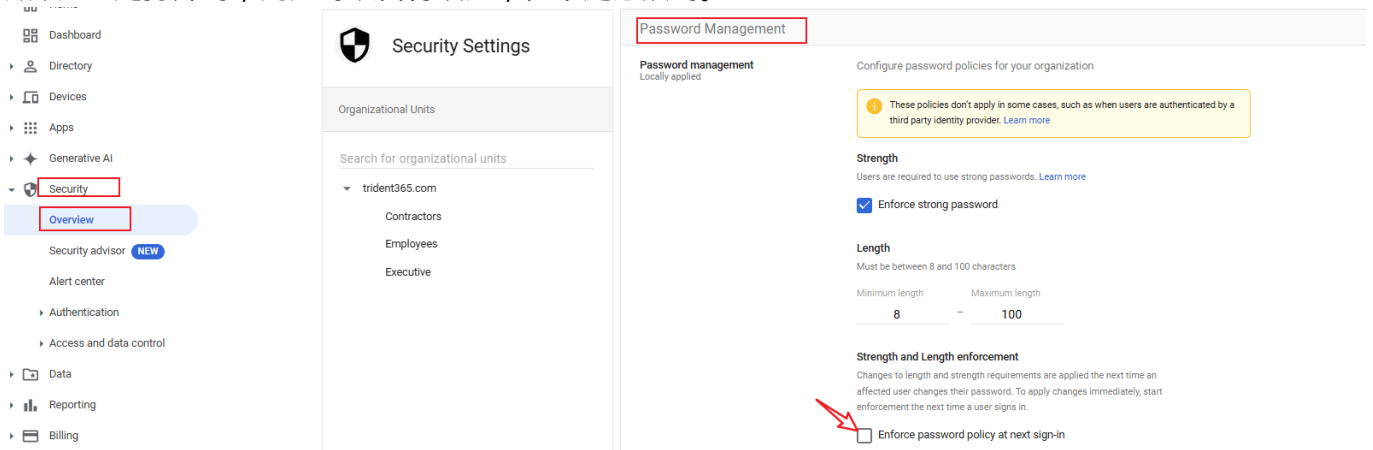
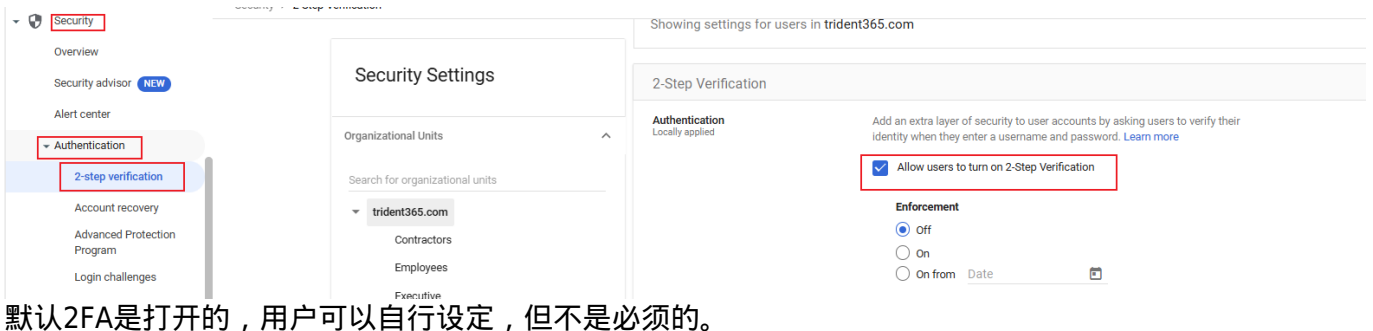


# 第3章 GWS安全

## 练习1

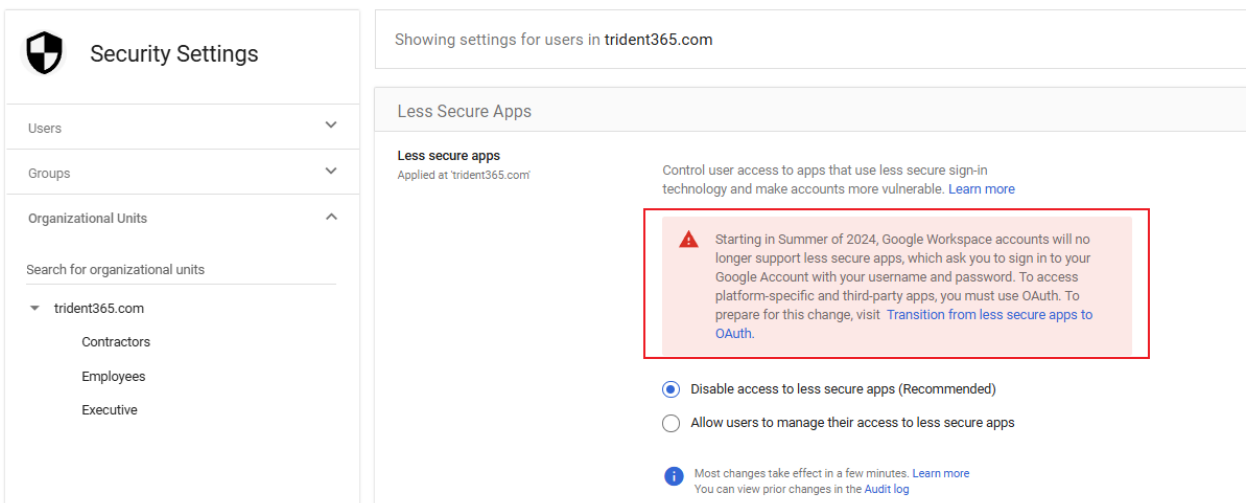
准备GWS域名，已经完成，略

## 配置通用安全设定



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。

Security > Less Secure Apps



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，在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

**Security**

- Users
- Groups
- Organizational Units

Search for organizational units

- trident365.com
  - Contractors
  - Employees
  - Executive

Showing settings for users in trident365.com

### Account Recovery

**Super admin account recovery**  
Applied at 'trident365.com'

Super admins can recover their own accounts if they forget their password. [Learn more](#)

Allow super admins to recover their account  
**ON**

**User account recovery**  
Applied at 'trident365.com'

Users and non-super admins can recover their own account if they forget their password. [Learn more](#)

**OFF**

This setting doesn't apply if you're using single sign-on (SSO) with a third-party identity provider or Password Sync. [Learn more](#)

**Recovery information**  
Applied at 'trident365.com'

Recovery information is used in user security anomalies and user account recovery. [Learn more](#)

**ON**

This setting doesn't apply if you're using single sign-on (SSO) with a third-party identity provider or Password Sync. Ensure that you are legally allowed to collect end-user phone and recovery email information. [Learn more](#)

If recovery info options are turned off, user accounts are less secure.

Allow admins and users to add recovery email information to their account.  
**ON**

Allow admins and users to add recovery phone information to their account.  
**ON**

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

## 练习2

### 查看用户安全设置

**ADMIN**

**Alex Bell**  
alex.bell@trident365.com

**Active**  
Last sign in: Hasn't signed in  
Created: Jan 19, 2025

Organizational unit  
trident365.com > **Executive**

- RESET PASSWORD
- UPDATE USER
- ADD ALTERNATE EMAILS
- ADD TO GROUPS
- EMAIL
- SUSPEND USER
- RESTORE DATA
- DELETE USER

User details **Security** Groups Investigate

### Security

**Password settings**

**Password** [Reset Alex's password.](#)

**Security keys** [Alex has no security keys. Learn more](#)

**Advanced Protection** **OFF**

Once you turn off Advanced Protection enrollment, only the user can re-enroll. [Learn more](#)

Trouble signing in  
Use a backup code for users who are unable to use their security key to sign in. Get a backup code from the 2-Step Verification card.

**2-step verification** **OFF** | Not enforced across your organization

The ability for users to sign in with an additional authentication factor, in addition to using their username and password (e.g. a verification code). [Change security settings](#)  
Only the user can turn on 2-step verification. [Learn more](#)

Recovery information

Email  
*Add a recovery email*

Phone  
*Add a recovery phone*


Recovery information is used to secure user accounts at sign-in and during account recovery.

Require password change

OFF  
This password won't need to be changed once Alex signs in.

Login challenge

Turn off identity questions for 10 minutes after a suspicious attempt to sign in. [Learn more](#)



Sign in cookies

Resets the user's sign-in cookies, which also signs them out of their account across all devices and browsers.

Application integrations

Application-specific password

0 application-specific passwords. [Learn more](#)

Connected applications

0 applications connected to this user. [Learn more](#)

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

/ > 2-Step Verification

## Security Settings

Organizational Units

Search for organizational units

trident365.com

Contractors

Employees

Executive

Groups

Customize settings for a group within an organizational unit. One group per organizational unit. [Learn more](#)

Search for a group

## 2-Step Verification

### Authentication

Inherited

Add an extra layer of security to user accounts by asking users to verify their identity when they enter a username and password. [Learn more](#)

Allow users to turn on 2-Step Verification

#### Enforcement

Off

On

On from Feb 13, 2025

设定2~3周的对应时间

#### New user enrollment period

Allows new users some time to enroll before enforcement is applied

None

#### Frequency

Users can avoid repeated 2-Step Verification at login on their trusted devices. [Learn more](#)

Allow user to trust the device

#### Methods

Select the method to enforce. [Learn more](#)

Any

Any except verification codes via text, phone call

Only security key

#### 2-Step Verification policy suspension grace period

Let users temporarily sign in with verification codes in addition to their security keys. The user's exception period starts when you generate verification codes.

1 day

然后找一个高管的邮箱，比如Alex登录后，会出现提示



## 避免您无法访问自己的账号



您所在的网域即将强制实行两步验证政策，以便提升账号安全性。

此政策将于 2025年2月13日起强制实行，届时系统将会在您登录账号时要求您输入动态密码。

**为了避免您无法访问自己的账号，请立即注册两步验证。**

[详细了解两步验证。](#)

注册

以后再说



对于已经使用SSO登录的公司来说，不需要设置

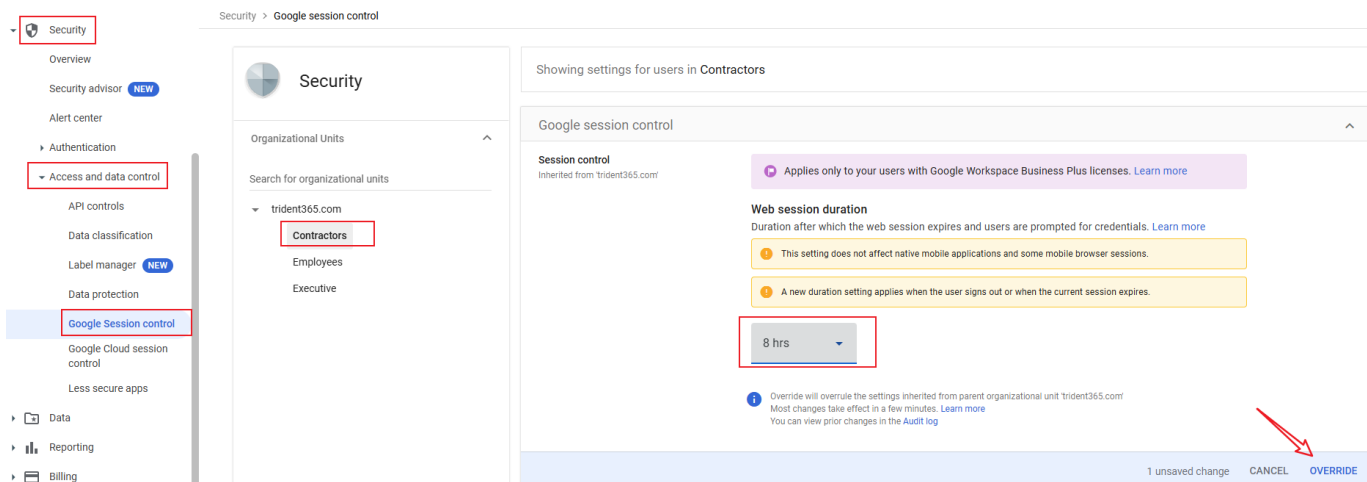
有4种方式

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 in 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

From:

<https://www.trident365.com/> - 三叉戟

Permanent link:

[https://www.trident365.com/doku.php?id=resources:courses:gws\\_c3&rev=1737613795](https://www.trident365.com/doku.php?id=resources:courses:gws_c3&rev=1737613795)

Last update: **2025/01/23 15:29**

