

# 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

Showing settings for users in trident365.com

**Security Settings**

**2-Step Verification**

**Authentication**

**Allow users to turn on 2-Step Verification**

**Enforcement**

Off

默认2FA是打开的，用户可以自行设定，但不是必须的。

**Security Settings**

**Overview**

**Password Management**

**Strength**

**Enforce strong password**

**Length**

8 - 100

**Strength and Length enforcement**

**Enforce password policy at next sign-in**

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

**Security Settings**

**Less Secure Apps**

**Less secure apps**

**Starting in Summer of 2024, Google Workspace accounts will no longer support less secure apps, which ask you to sign in to your Google Account with your username and password. To access platform-specific and third-party apps, you must use OAuth.**

**Disable access to less secure apps (Recommended)**

**Allow users to manage their access to less secure apps**

**Most changes take effect in a few minutes.**

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

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](#)

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

Allow users and non-super admins to recover their account  
**OFF**

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

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

! 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**  
[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	<p>Email <a href="#">Add a recovery email</a></p> <p>Phone <a href="#">Add a recovery phone</a></p>
Recovery information is used to secure user accounts at sign-in and during account recovery.	
Require password change	<p>OFF</p> <p>This password won't need to be changed once Alex signs in.</p>
Login challenge	<p>Turn off identity questions for 10 minutes after a suspicious attempt to sign in. <a href="#">Learn more</a></p> 
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. <a href="#">Learn more</a>
Connected applications	0 applications connected to this user. <a href="#">Learn more</a>

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

rganizational Units

search for organizational units

trident365.com

Contractors

Employees

**Executive**

roups

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

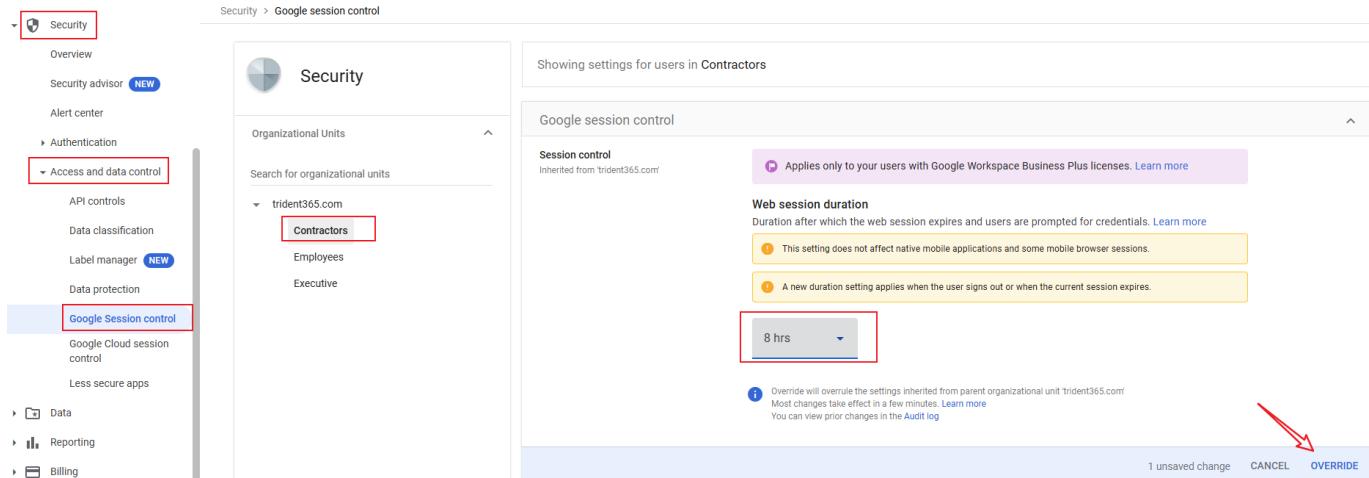
有4种方式

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。



Showing settings for users in **Contractors**

**Google session control**

**Session control**  
Inherited from 'trident365.com'

**Web session duration**  
Duration after which the web session expires and users are prompted for credentials. [Learn more](#)

This setting does not affect native mobile applications and some mobile browser sessions.

A new duration setting applies when the user signs out or when the current session expires.

8 hrs

Override will override the settings inherited from parent organizational unit 'trident365.com'. Most changes take effect in a few minutes. [Learn more](#)  
You can view prior changes in the [Audit log](#)

1 unsaved change [CANCEL](#) **OVERRIDE**

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**
- We wouldn't have to manage individual user IDs and passwords for each user
- 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**
- 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?

- 1. 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
- 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

Security > SSO with Google as SAML IdP

The screenshot shows the 'Security Settings' page for 'SSO with Google as SAML IdP'. The 'Google Identity Provider details' section is visible, containing fields for 'SSO URL' and 'Entity ID', both of which are set to 'https://accounts.google.com/o/saml2/idp?idpid=C02jd4j4r'. The 'SSO URL' field has a red border, indicating it is the current focus or a required field.

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

**Search apps**  
Search SAML enabled apps, Android apps in Google Play, and iOS apps in App Store

**i** iOS apps can't be configured because an Apple push certificate isn't set up. [?](#)

# 15Five

Note: you can also enter iOS App Store URLs [?](#)

App	Platform
	15Five Web (SAML)

## 下载Metadata

**Add '15Five'**

1 Google Identity Provider details — 2 Service provider details — 3 Attribute mapping

Option 1: Download IdP metadata  
[DOWNLOAD METADATA](#)

OR

Option 2: Copy the SSO URL, entity ID, and certificate

SSO URL  
<https://accounts.google.com/o/saml2/idp?idpid=C02jd4j4r>

Entity ID  
<https://accounts.google.com/o/saml2?idpid=C02jd4j4r>

Certificate  
[Google\\_2030-1-21-223136\\_SAML2\\_0](#)  
Expires Jan 22, 2030  
-----BEGIN CERTIFICATE-----  
MIID0dCCAYgAwIBAgjGAZSR2+6aMA0GCSqGSIb3DQEBCwUAMhsxFDASBgNVBAoTC0dvb2dsZSBJ  
bmMuMRYwFAYDVQQHEw1Nb3VudGFpbWV3MQ8wDQYDVQQDEwZhb29nbGUxGDAWBgNVBAstD0dv  
b2dsZSBgb3lgV29yazELMAkGA1UEBhMCVVMxEzARBgNVBghGImb3JuaWEwHhcNMjUwMTIz  
-----END CERTIFICATE-----

SHA-256 fingerprint  
[3B:81:DB:3E:1B:5D:20:D2:92:F1:F5:65:95:0C:BC:A2:52:FC:57:77:F7:92:F6:D1:B3:44:33:B1:34:C5:B3:31](#)

[CANCEL](#) [CONTINUE](#)

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

15Five Web (SAML)

**Service provider details**

To configure single sign on, add service provider details such as ACS URL and entity ID. [Learn more](#)

ACS URL  
https://trident365.15five.com/saml2/acs/

Entity ID  
https://trident365.15five.com/saml2/metadata/

Start URL (optional)  
https://trident365.15five.com/

Signed response

**Name ID**

Defines the naming format supported by the identity provider. [Learn more](#)

Name ID format  
EMAIL

Name ID  
Basic Information > Primary email

BACK

CANCEL

CONTINUE

把域名补全，然后ID格式选择Email继续

<input type="checkbox"/>	Name	Platform	Authentication	User access	Details
<input type="checkbox"/>	15Five	Web	SAML	OFF for everyone	Certificate expires on Jan 22, 2030 Autoprovisioning available

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

## 练习2

Security > SSO with third-party IDPs

**Single sign-on (SSO) with third-party identity providers (IDPs)**

Set up SSO so users can sign in with a third-party IDP to access Google Workspace services. [Learn more](#)

**Third-party SSO profiles**

Below are SSO profiles you can assign to org units or groups. [Learn about SSO profiles](#)

Name	Type	Status
Microsoft	OIDC <b>BETA</b>	System profile

**Manage SSO profile assignments**

Manage SSO profile assignments for organizational units or groups

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

**Add LDAP client**

Client details — Access permissions

Access permissions

**Verify user credentials**  
Specify client's access level for verifying user credentials. Changes can take up to 24 hours to take effect. [?](#)

Entire domain (trident365.com)

Selected organizational units, groups and excluded groups

No access

**Read user information**  
Specify client's access level for reading user information. Some clients need additional information before authenticating users. [?](#)

Entire domain (trident365.com)

Selected organizational units

No access

Specify which attributes this client can access to read a user's information. Custom attributes must adhere to LDAP naming conventions. [?](#)

System Attributes  
Default user attributes available for all the user accounts - for example, Name, Email and Phone.  
[View Attributes](#)

Public Custom Attributes  
Custom user attributes that are marked as visible to the organization.  
[View Attributes](#)

Private Custom Attributes  
Custom user attributes that are marked as visible only to the user and administrators.

Your organization doesn't have any LDAP clients

**ADD LDAP CLIENT**

✓ LDAPTest added

ⓘ Next, connect your client to the LDAP service

1. Download the generated certificate (it might take a few minutes to generate).

Want to do this later? You can generate and download a certificate at any time from the client's details page.

Google\_2028\_01\_23\_25283

Expires January 23, 2028

[Download certificate](#)

2. Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access credentials. [Learn more](#)

[CONTINUE TO CLIENT DETAILS](#)

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

The screenshot shows the Google Workspace Admin interface under the 'Security' section. The 'API controls' page is displayed, with the 'Access and data control' and 'API controls' buttons highlighted with red boxes. A modal window titled 'Change Access' is open over the list of Google services. The modal asks 'Change access to Google Workspace Admin:' and provides two options: 'Unrestricted: Any user-approved app can access a service' (radio button is empty) and 'Restricted: Only trusted apps can access a service' (radio button is selected). A red arrow points to the 'Restricted' radio button. The 'CHANGE' button at the bottom right of the modal is also highlighted with a red box. The list of services on the left includes 'Service', 'Drive', 'Gmail', 'Calendar', 'Contacts', and 'Google Workspace Admin', with 'Google Workspace Admin' also highlighted with a red box.

## 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。

Showing settings for users in trident365.com

**Settings**

**Custom user message** Off  
Applied at 'trident365.com'

**Unconfigured third-party apps** Allow users to access any third-party apps  
Applied at 'trident365.com'

**Internal apps**  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.  
Applied at 'trident365.com'

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](#)

Search: 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-p5q7g3a7ptrkj5b3dla3lj7ca0sqffe.apps.googleusercontent.com

 **Sync for iCloud Calendar**  **Android**

[View in Play Store](#)

Number of organizations using app: Not available

Client ID: com.granita.cal dav sync

Selected application  Sync for iCloud Calendar 

Access to Google Data Choose an access type to specify which data this app can request from users signing in with their Google Account.  
[Learn more about app access to Google data](#)

Trusted This app can request access to user data in any Google service via OAuth 2.0 scopes.  
[What to expect with trusted access](#)

Limited This app can request access to user data in any Google service marked unrestricted under Google services.  
[What to expect with limited access](#)

Specific Google data This app can only request access to user data from the Google services specified below. Note, you must include the Google Sign-in scope below to allow users to sign in with their Google Account.

 Google Sign-in 3 scopes

[Update Google services or scopes](#)

Blocked Users can't sign into this app with their Google Account, and the app can't request access to user data in any Google service.

Back

Cancel

Continue

## 最后点FINISH，然后再把它限制

Access to Google Data Select what type of access this app has to Google data for users in the selected org unit.  
[Learn more about app access](#)

Trusted App can request access to all Google data

Limited App can request access to unrestricted Google data

Specific Google data This app can only request access to user data from the Google services specified below. Note, you must include the Google Sign-in scope below to allow users to sign in with their Google Account.

 Google Sign-in 3 scopes

[Update Google services or scopes](#)

Blocked App can't request access to any Google data

BACK

CANCEL

NEXT

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

Showing apps for users in all organizational units

Domain Installed Apps (0) Allowlisted Apps

App Name Distribution

Rows per page: 50

Google Workspace Marketplace

All users in this account

Groups

Organizational Units

Search for organizational units

trident365.com

Contractors

Apps list

Google Analytics

All filters Works with Price Internal apps

Search results for Google Analytics

Google doesn't verify reviews or ratings. [Learn more about reviews and results](#)

**Worklytics**  
People Analytics for Google Apps

Worklytics - Analytics for... [www.worklytics.co](http://www.worklytics.co)  
Worklytics provides advanced analytics Google Workspace. Analyze collaboration and wor...

★ 4.7 615K+

**Google Analytics™ into Google Sheets™**

Google Analytics (GA4) ... SyncWith Inc.  
This GA4 Google Sheets add-on lets you pull Google Analytics™ data into Google Sheets™, to...

★ 4.8 113K+

**GA4 Reports Builder for... Google**  
Google Analytics users can use this add-on to create and run reports for GA4 properties...

★ 1.8 248K+

安装GA4



### GA4 Reports Builder ...

Google Analytics users can use this add-on to create and run reports for GA4 properties using Google Sheets™.

By: [Google](#)

Listing updated: April 26, 2024

[Admin install](#)

[Individual install](#)

-  View and manage spreadsheets that this application has been installed in (i)
-  Display and run third-party web content in prompts and sidebars inside Google applications (i)
-  Allow this application to run when you are not present (i)
-  View and manage your Google Analytics data (i)
-  See and download your Google Analytics data (i)
-  See your primary Google Account email address (i)
-  See your personal info, including any personal info you've made publicly available (i)

Install the app automatically for the following users

- Everyone at your organization
- Certain groups or organizational units  
Select users in the next step

I agree to the application's [Terms of Service](#), [Privacy Policy](#), and Google Workspace Marketplace's [Terms of Service](#)

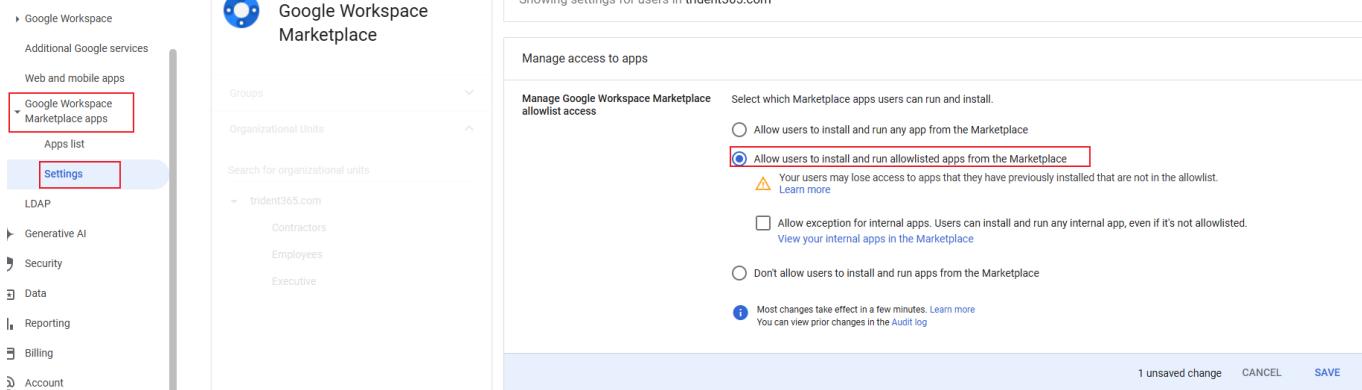
[CANCEL](#)

[FINISH](#)

[查看结果](#)

Domain Installed Apps (1)		Allowlisted Apps	Excluded Apps
App Name		Distribution	Details
 GA4 Reports Builder for Google Analytics™		ON	Sheet Add-on
Rows per page: 50 <span style="float: right;">Page 1 of 1</span>			

然后设置，只允许用户安装白名单的APP



The screenshot shows the Google Workspace Marketplace settings page. On the left, there's a sidebar with various Google services like Google Workspace, Additional Google services, and Google Workspace Marketplace apps. The 'Google Workspace Marketplace apps' section is highlighted with a red box. Below it, the 'Settings' section is also highlighted with a red box. The main content area is titled 'Manage access to apps' and shows the 'Allow users to install and run allowlisted apps from the Marketplace' option selected. This option is highlighted with a red box. A note below it says 'Your users may lose access to apps that they have previously installed that are not in the allowlist.' At the bottom right of the main content area, there are buttons for '1 unsaved change', 'CANCEL', and 'SAVE'.

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](https://workspace.google.com/user/hub),发现已经出现了

The screenshot shows the Google Workspace dashboard at the URL <https://workspace.google.com/user/hub>. The dashboard has a light gray background with a dark header bar at the top. In the header bar, there are icons for back, forward, and refresh, followed by a lock icon and the URL. The main content area is titled '发现' (Discover) in a light blue header. Below this, there are several sections: '建议' (Suggestions) with a count of 17, a 'Google Workspace 由您的管理员管理' (Google Workspace managed by your administrator) message with a 'Welcome to Trident365' sub-message, and a '您的应用' (Your Apps) section. A blue button labeled '查找应用' (Find App) is located on the right. The main application grid contains icons for Cloud Search, Gemini 应用, Gmail, 云端硬盘和文档, 幻灯片, 文档, and Slides Toolbox. A red arrow points to the Slides Toolbox icon, which is a yellow briefcase.

再打开Market，任意安装一个APP，会跳出提示



## Dialpad

One Beautiful Workspace for calling, messaging, meetings and contact center integrated with Google Workspace™

管理员安装

单独安装

开发者: [dialpad.com](https://dialpad.com)

应用详情更新日期: 2024年8月1日

⚠ 您的管理员不允许使用此应用。 [了解详情](#)

★★★★☆ 159 [i](#) ↓ 59万+

From:

<https://trident365.com/> - 三叉戟

Permanent link:

[https://trident365.com/doku.php?id=resources:courses:gws\\_c3&rev=1737620729](https://trident365.com/doku.php?id=resources:courses:gws_c3&rev=1737620729)

Last update: **2025/01/23 17:25**

