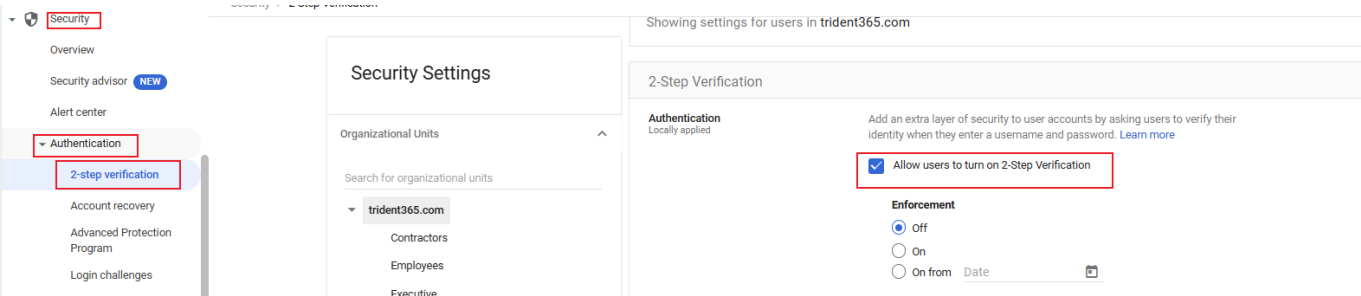


第3章 GWS安全

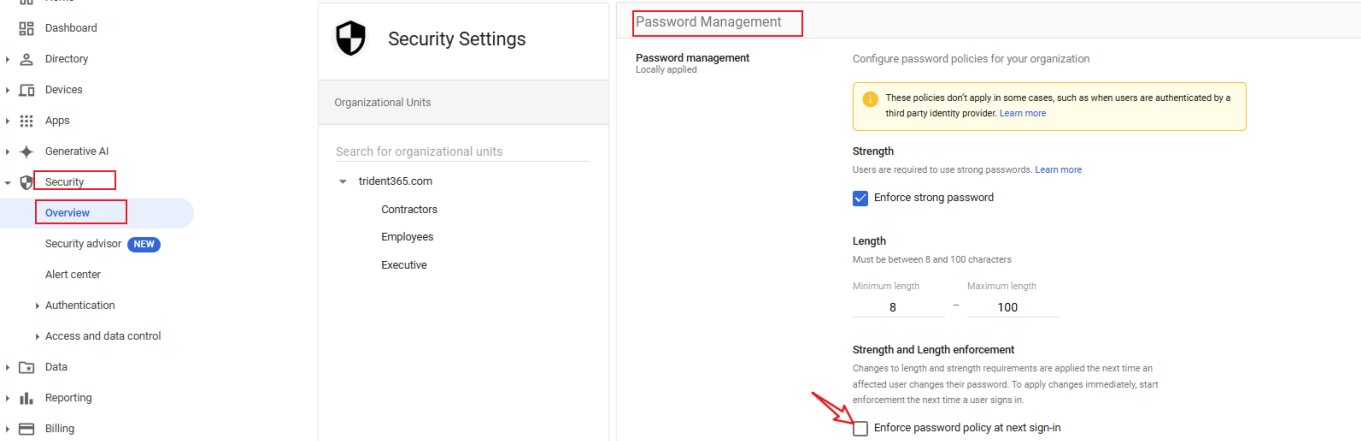
练习1

准备GWS域名，已经完成，略

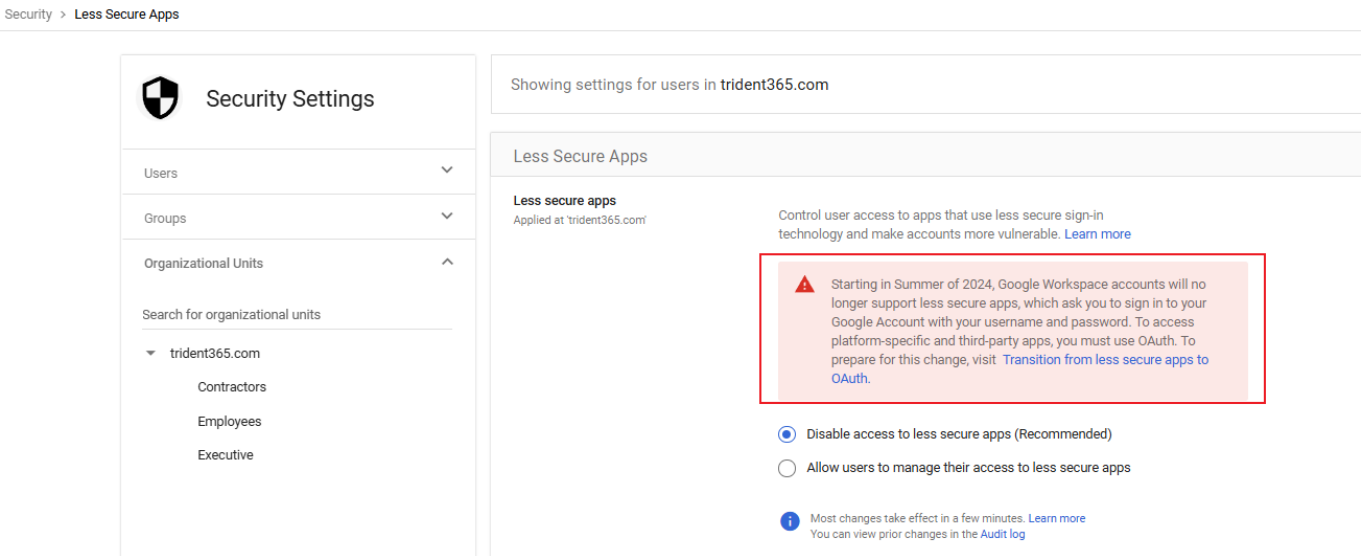
配置通用安全设定



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 > Account Recovery

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'

Allow super admins to recover their account

ON

User account recovery

Applied at 'trident365.com'

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'

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

Users > Alex Bell > Security

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

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

https://trident365.com/

Printed on 2025/04/21 19:26

| | |
|-------------------------------|---|
| Recovery information | <div>Email Add a recovery email</div> <div>Phone Add a recovery phone</div> <div>Recovery information is used to secure user accounts at sign-in and during account recovery.</div> |
| Require password change | <div>OFF</div> <div>This password won't need to be changed once Alex signs in.</div> |
| 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

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

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

https://trident365.com/

Printed on 2025/04/21 19:26



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

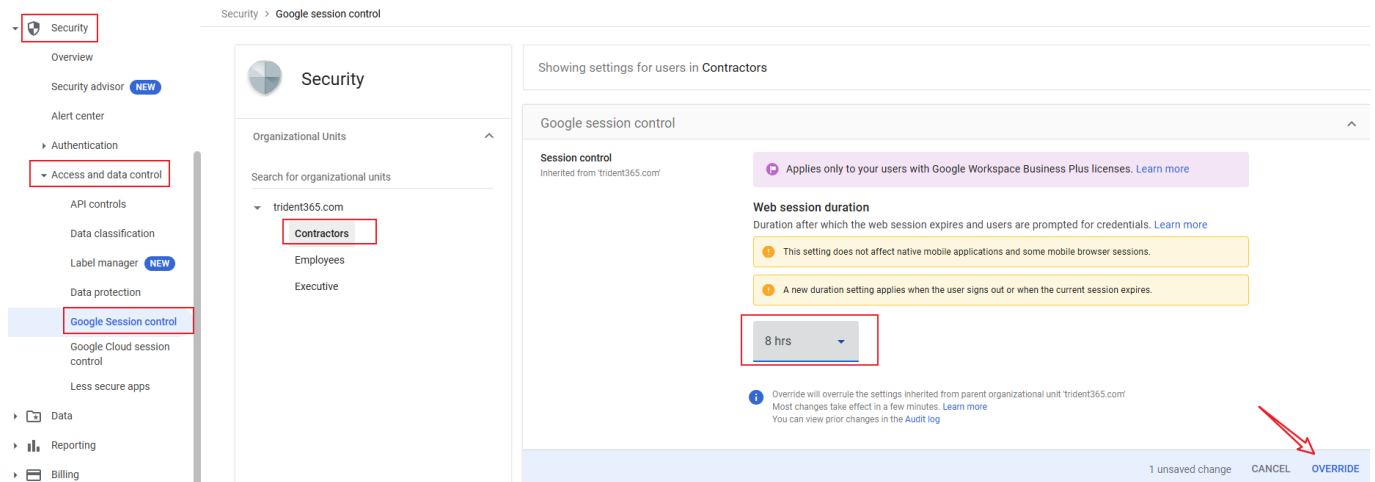
有4种方式

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

练习1

Security > SSO with Google as SAML IdP

Security Settings

Set up single sign-on (SSO) with Google as SAML Identity Provider (IdP)


Google Identity Provider details

To configure single sign-on (SSO) using SAML, follow your service provider's instructions. [Learn more](#)

SSO URL


Entity ID

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



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

15Five

Note: you can also 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/ldap?ldpid=C02jd4jr

Entity ID

https://accounts.google.com/o/saml2?ldpid=C02jd4jr

Certificate

Google_2030-1-21-223136_SAML2_0

Expires Jan 22, 2030

-----BEGIN CERTIFICATE-----
MIIDdCCAlvgAwIBAgIGAZSR2+6aMA0GCSqGSIb3DQEBwUAMHsxFDASBgNVBAoTC0d4b2dsZSBjbmMuMRwwFAYDVQQHEw1Nb3VudG9pbiBwaWV3MQ8wDQYDVQQDEwZhb29nbGluZGDAWBgNVBAAsTD0dvb2dsZSBGb3lgV29yazELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbmGimb3JuaWEwHicNMjUwMTZi

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 | 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HennggeOne所以GWS上的操作也可以免了。。

练习2

Security

Overview

Security advisor

Alert center

Authentication

2-step verification

Account recovery

Advanced Protection Program

Login challenges

Passwordless

Password management

SSO with SAML applications

SSO with third party IDP

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

BETA

System profile

ADD SAML 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

Apps

Overview

Google Workspace

Additional Google services

Web and mobile apps

Google Workspace Marketplace apps

LDAP

Generative AI

Security

Cloud icon

Your organization doesn't have any LDAP clients

ADD LDAP CLIENT

设置最高权限

×

Add LDAP client

✓ Client details

2 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.

✓ LDAPTest added

i 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 console interface. On the left, the 'API controls' link is highlighted in the 'Access and data control' section. The main content area shows 'API controls' with a description and an 'Overview' section. The 'Overview' section displays '0 restricted Google services' and '18 unrestricted Google services'. A red arrow points to the 'MANAGE GOOGLE SERVICES' link. Below this, the 'Settings' section is visible. In the foreground, a 'Change Access' dialog box is open, showing options to change access to Google Workspace Admin. The 'Restricted' option is selected, and a red arrow points to it. The dialog box has 'CANCEL' and 'CHANGE' buttons.

| Service | Access | Count |
|------------------------|--------------|-------|
| Service | Unrestricted | 0 |
| Drive | Unrestricted | 0 |
| Gmail | Unrestricted | 0 |
| Calendar | Unrestricted | 0 |
| Contacts | Unrestricted | 0 |
| Google Workspace Admin | Unrestricted | 0 |

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

Number of organizations using app: Not available

Client ID: 324281144739-p5q7g3a7ptrtkj5b3dia3ti7ca0sqffe.apps.googleusercontent.com

[View in Play Store](#)

Sync for iCloud Calendar



Android

Number of organizations using app: Not available

Client ID: com.granita.caldavsync

[View in Play Store](#)

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

Apps

Overview

Google Workspace

Additional Google services

Web and mobile apps

Google Workspace Marketplace apps

Apps list

Settings

LDAP

Generative AI

Security

Google Workspace Marketplace

All users in this account

Groups

Organizational Units

Search for organizational units

trident365.com

Contractors

Showing apps for users in all organizational units

Domain Installed Apps (0)

Allowlisted Apps

App Name

Distribution

Rows per page: 50

INSTALL APP

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 fo...
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 addon lets you pull Google Analytics™ 4 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 
-  Display and run third-party web content in prompts and sidebars inside Google applications 
-  Allow this application to run when you are not present 
-  View and manage your Google Analytics data 
-  See and download your Google Analytics data 
-  See your primary Google Account email address 
-  See your personal info, including any personal info you've made publicly available 


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

Page 1 of 1

然后设置，只允许用户安装白名单的APP

Google Workspace

Additional Google services

Web and mobile apps

Google Workspace Marketplace apps

Apps list

Settings

LDAP

Generative AI

Security

Data

Reporting

Billing

Account

Google Workspace Marketplace

Groups

Organizational Units

Search for organizational units

trident365.com

Contractors

Employees

Executive

Manage access to apps

Manage Google Workspace Marketplace allowlist access

Select which Marketplace apps users can run and install.

☐ Allow users to install and run any app from the Marketplace

☒ Allow users to install and run allowlisted apps from the Marketplace

☐ Allow exception for internal apps. Users can install and run any internal app, even if it's not allowlisted.

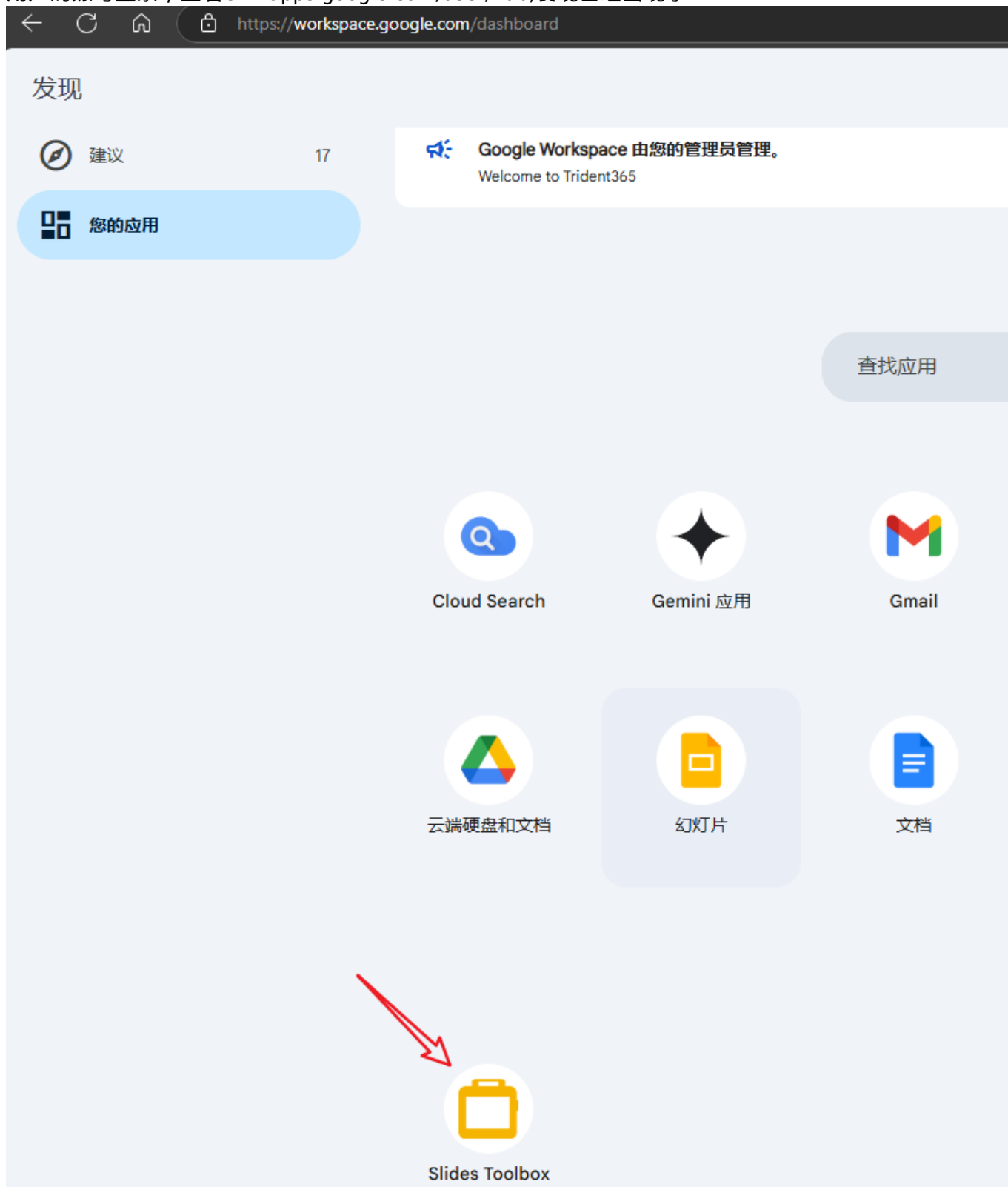
☐ Don't allow users to install and run apps from the Marketplace

1 unsaved change

CANCEL

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,发现已经出现了



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™

开发者: dialpad.com

应用详情更新日期: 2024年8月1日

管理员安装

单独安装



您的管理员不允许使用此应用。 [了解详情](#)

★★★★☆ 159 ⓘ ↓ 59万+

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

From:

<https://trident365.com/> - 三叉戟

Permanent link:

https://trident365.com/doku.php?id=resources:courses:gws_c3&rev=1737621334

Last update: **2025/01/23 17:35**

