



# G-SUITE SECURITY BEST PRACTICES

---



# AGENDA

**Admin Account Security Practices.**

---

**Employee Account Security Practices.**

---

**Securing Access to DNS Zones.**

---

**Google Calendar.**

---

**Gmail.**

---

**Google Drive.**

---

# ADMIN ACCOUNT SECURITY PRACTICES

---

1

## REQUIRE 2-STEP VERIFICATION FOR ADMIN ACCOUNTS

Super admins control access to all business and employee data in the organization, it is especially important for their accounts to be protected by an additional authentication factor. Protect your business with 2-Step Verification.

- A compromised machine (having a keylogger installed or malware that sends input data), could send keystrokes to the attacker. Having a 2 step verification will prevent the worst-case scenario. Even if the attacker has the admin credentials they would need to verify their identity as an admin using extra layer authentication.
- Malicious insiders are those who maliciously and intentionally abuse legitimate credentials. Administrators prone to blackmail can sometimes pass on the credentials intentionally and can try to hold someone else accountable. Having a 2 step verification would hold the person in charge and provide accountability to whoever accesses the login.

2

## LIMIT THE USE OF AN ADMIN ACCOUNT ONLY FOR ADMIN ACTIVITIES

System Administrators must create a separate account for handling daily administrative tasks.

3

## CREATE MULTIPLE ADMIN ACCOUNTS

A business should have more than one super admin account, each managed by a separate person. If one account is lost or compromised, another super admin can perform critical tasks while the other account is recovered.

4

## ADMINS SHOULD ADD RECOVERY INFORMATION TO THEIR ACCOUNT

Having all the extra security can be a menace at times. The administrator can sometimes lose access to their extra protected password manager account / lose their passphrase to the 2FA Account, this can make it impossible to recover the account.

5

## WATCH OUT FOR ABNORMAL USAGE

For a G Suite admin, monitoring is especially important, as G Suite is used to manage massive amounts of personal financial information. Monitoring may help you prevent an incident before it occurs. Abnormal behaviour may include user's logging in and out too frequently and unusual high user activity. Monitoring abnormal usage will also help you detect suspicious activities in Google apps. Any data spike in Google Drive storage may mean the malicious actions of a third-party app.

# EMPLOYEE ACCOUNT SECURITY PRACTICES

1

## IMPLEMENT 2 FACTOR AUTHENTICATION

The benefit of 2FA is that if one of the factors is compromised, your account is usually still protected. It makes it much harder for an attacker to gain access.

Security > 2-Step Verification

### Security Settings

Organisational units

Search for organisational units

Groups

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

☐ 2 Step Password Forgetters

Showing settings for users in

### 2-step verification

**Authentication**  
Locally applied

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  Date

**New user enrolment period**  
Allows new users some time to enrol before enforcement is applied

None

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

Allow the user to trust the device

Set up 2FA for your Account [Now](#)

2

## MANAGE YOUR USER'S PASSWORD STRENGTH

Ensure to set a password of minimum 8 alphanumeric characters to make it difficult for attackers to attempt logging into your accounts.

### Security Settings

Organisational unit

Search for organisational units

Showing settings for users in

### Password management

**Password management**  
Locally applied

Configure password policies for your organisation

These policies don't apply in some cases, such as when users are authenticated by a third-party identity provider. [Learn more](#)

**Strength**  
Users are required to use strong passwords. [Learn more](#)

☒ Enforce strong password

**Length**  
Must be between 8 and 100 characters

Minimum length

Maximum length

8

–

100

**Strength and length enforcement**

# EMPLOYEE ACCOUNT SECURITY PRACTICES

3

## DISALLOW LOW SECURITY APPS FROM ACCESSING USER ACCOUNTS

Low-security apps can make it easier for hackers to get into your account, so blocking sign-ins from these apps will help in keeping your account safe. Low-security apps can make your account more vulnerable.

Security > Less secure apps

Security Settings

Users

Groups

Organisational units

Search for organisational units

Showing settings for users in

Less secure apps

Less secure apps

Applied at

Control user access to apps that use less secure sign-in technology and make accounts more vulnerable. [Learn more](#)

☒ Disable access to less secure apps (recommended)

☐ Allow users to manage their access to less secure apps

i

Most changes take effect within a few minutes. [Learn more](#)

You can view prior changes in the [audit log](#)

1 unsaved change CANCEL SAVE

Change the Settings [Now](#)

4

## ENSURE THAT UNINTENDED EXTERNAL REPLY WARNING IS ON

This feature gives your organisation protection against forged email messages and possible impersonation. Check the Settings [Now](#)

Gmail

Groups

Organisational units

Search for organisational units

POP and IMAP access

Enable IMAP access for all users: ON

Enable POP access for all users: ON

Google Workspace Sync

Enable Google Workspace Sync for Microsoft Outlook for my users: ON

Automatic forwarding

Allow users to forward incoming email automatically to another address: ON

Image URL proxy whitelist

Image URL patterns whitelist: ON

Allow per-user outbound gateways

Allow users to send email through an external SMTP server when configuring a 'from' address hosted outside your email domain: ON

Warn for external recipients


Highlight any external recipients in a conversation. Warn users before they reply to emails with external recipients who aren't in their contacts.: ON

# EMPLOYEE ACCOUNT SECURITY PRACTICES

5

## SECURE YOUR MOBILE DEVICES BY HAVING MANDATORY PIN

Devices > Mobile and endpoints > Universal settings > General

**Universal settings**

Organisational units ^  
Search for organisational units  
▼

Showing settings for users in

General ^

**Mobile Management**  
Applied at

Set the management option  
Unmanaged

**Password requirements**  
Applied at

Set for Android, iOS and Google Sync  
Off

Check the Settings [Now](#)

6

## OFFBOARD USERS IMMEDIATELY

7

## REGULARLY CHECK FOR SUSPICIOUS BEHAVIOUR

8

## SET UP ADMIN EMAIL ALERTS

# EMPLOYEE ACCOUNT SECURITY PRACTICES

9

## DISALLOW ROOT ACCESS DEVICES

Devices > Mobile and endpoints > Universal settings



Universal settings

organization data

Android devices.

ActiveSync.; Google Sync IP Whitelist (a list of IP addresses where user can access Google Sync);, Turned off: 'Automatically enable "Delete Email as Trash" setting on Google Sync devices.; +1 More.

iOS sync

Turned on: 'Allow work data to sync on iOS devices.'

Google Assistant

Turned on: 'Allow Google Assistant for iOS and Android.'

Applied at ''

Security

Turn on device security measures and approve devices.

Inactive company owned devices

Turned on: 'Send monthly report of inactive company owned devices to super administrators', Also Notify:

Camera

Turned on: 'Allow camera'

Device approvals

Turned off: 'Require admin approval'

Encryption

Turned off: 'Require device encryption.'

Compromised devices

Turned off: 'Block compromised Android devices.', Turned off: 'Block jailbroken iOS devices.'

Applied at ''

Make the changes in the Settings [Now](#)

# SECURE ACCESS TO YOUR DNS ZONES



**Cloud Identity and Google Workspace accounts are identified by a primary DNS domain name. When you create a new Cloud Identity or Google Workspace account, you must verify ownership of the DNS domain by creating a special DNS record in the corresponding DNS zone.**



- **Google Workspace relies on DNS MX records for routing emails. By modifying these MX records, an attacker might be able to route emails to a different server and gain access to sensitive information.**
- **If an attacker is able to add records to the DNS zone, they might then be able to reset the password of a super admin user and gain access to the account.**




# GOOGLE CALENDAR



## LIMIT EXTERNAL CALENDAR SHARING

Restrict external calendar sharing to free/busy information only. This reduces the risk of data leaks.

Apps > Google Workspace > Settings for Calendar > Sharing settings

 **Calendar**

Users

Groups

Organisational units

Search for organisational units

Showing settings for users in

Sharing settings

**Working location**

Allow users to set their daily working location. [Learn more](#)

ON

**External sharing options for primary calendars**

Outside - set user ability for primary calendars

Only free/busy information (hide event details)

**Internal sharing options for primary calendars**

Within - set default

Share all information

**Video conferencing**

Make Google Meet the default video conferencing provider when available [Learn more](#)

ON

# GMAIL

1

## **PREVENT SPOOFING, PHISHING, AND SPAM** Setup SPF for your Organisation

- Use Sender Policy Framework (SPF) to help protect your domain against spoofing, and help prevent your outgoing messages from being marked as spam. SPF specifies the mail servers that are allowed to send emails for your domain. Receiving mail servers use SPF to verify that incoming messages that appear to come from your domain were sent by servers authorized by you.
- Get the sign-in information for your domain provider and edit TXT Records according to your domain IP Addresses and servers.

2

## **INCREASE SECURITY FOR OUTGOING EMAIL WITH DKIM**

- Use the DomainKeys Identified Mail (DKIM) standard to help prevent spoofing on outgoing messages sent from your domain.
- Email spoofing is when email content is changed to make the message appear from someone or somewhere other than the actual source. Spoofing is a common unauthorized use of email, so some email servers require DKIM to prevent email spoofing.

# GMAIL

3

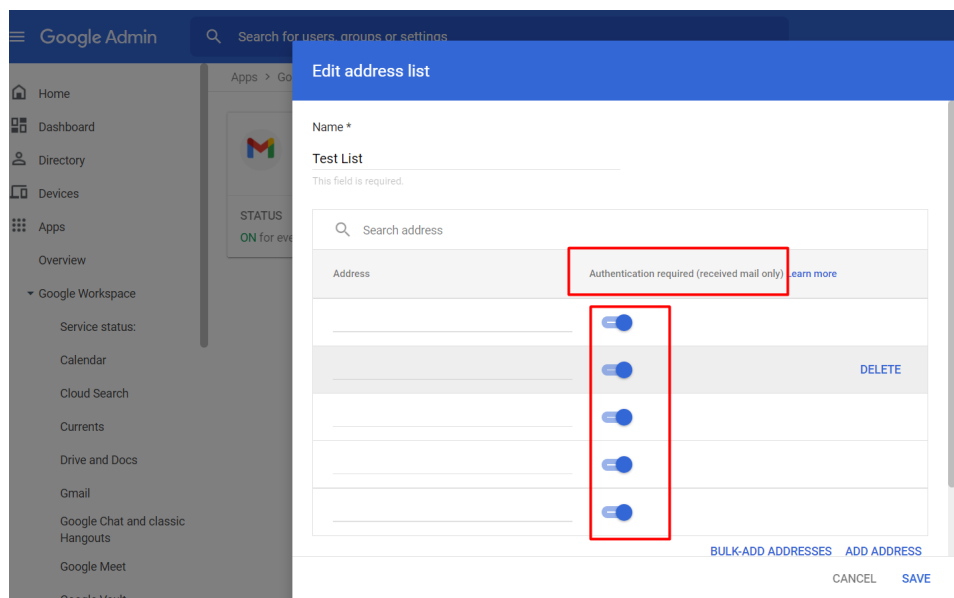
## SETUP DMARC RECORDS

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a standard email authentication method. DMARC helps mail administrators prevent hackers and other attackers from spoofing their organization and domain. Spoofing is a type of attack in which the "From" address of an email message is forged. A spoofed message appears to be from the impersonated organization or domain.

4

## REQUIRE SENDER AUTHENTICATION FOR ALL APPROVED SENDERS

When you create an address list of approved senders who can bypass spam classification, mandate sender authentication. When sender authentication is turned off, Gmail cannot verify that the message was actually sent by the person.



# GMAIL

5

## CONFIGURE MX RECORDS FOR CORRECT MAIL FLOW


Configure the MX records to point to Google's mail servers as the highest priority record to ensure correct mail flow to your Google Workspace domain users. This reduces the risk of data deletion (through lost email) and malware threats.

6

## DISABLE IMAP/POP ACCESS

IMAP and POP desktop clients let users access Gmail through third-party email clients. Disable POP and IMAP access for any users who don't explicitly need this access. This reduces data leak, data deletion, and data exfiltration risks.

Apps > Google Workspace > Settings for Gmail > End user access

 Gmail

Groups ▾

Organisational units ▲

Search for organisational units

Showing settings for users in

End user access ▲

POP and IMAP access

Applied at '

Enable IMAP access for all users: ON

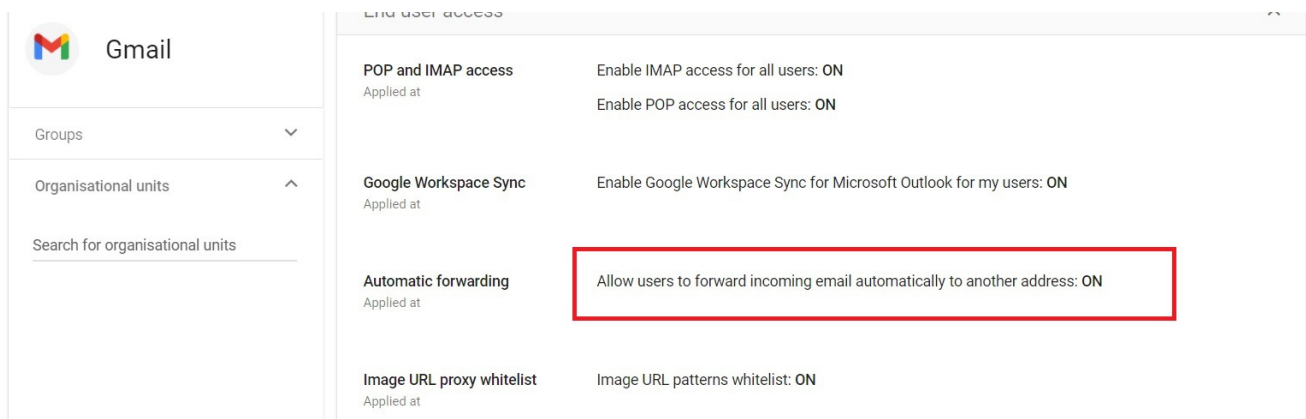
Enable POP access for all users: ON

# GMAIL

7

## DISABLE AUTOMATIC FORWARDING

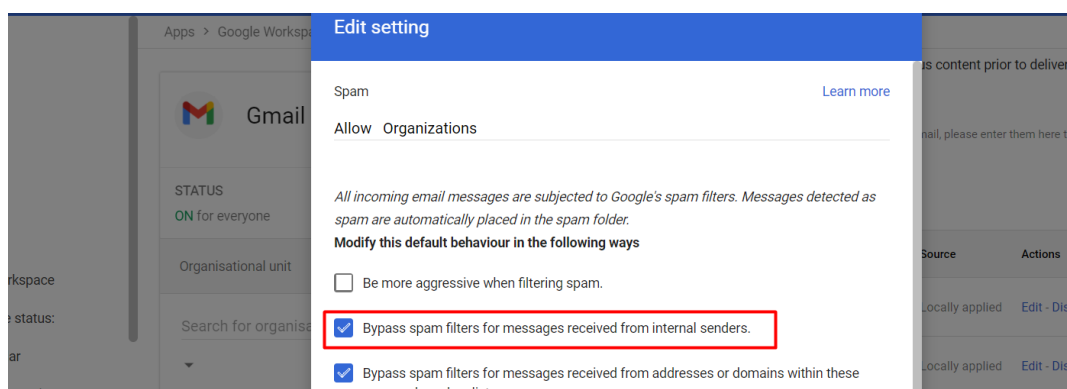
Prevent users from automatically forwarding incoming mail to another address. This reduces the risk of data exfiltration through email forwarding, which is a common technique employed by attackers.



8

## DO NOT BYPASS SPAM FILTERS FOR INTERNAL SENDERS

Turn off Bypass spam filters for internal senders, because any external addresses added to groups are treated as internal addresses. By turning off this setting, you can make sure all user email is filtered for spam, including mail from internal senders. This reduces the risk of spoofing and phishing/whaling.

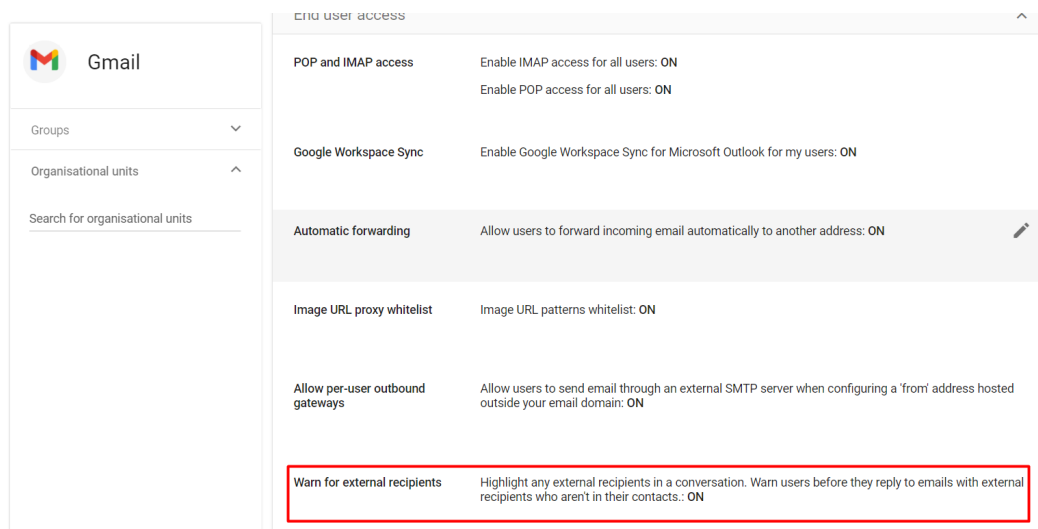


# GMAIL

9

## ENABLE EXTERNAL RECIPIENT WARNINGS

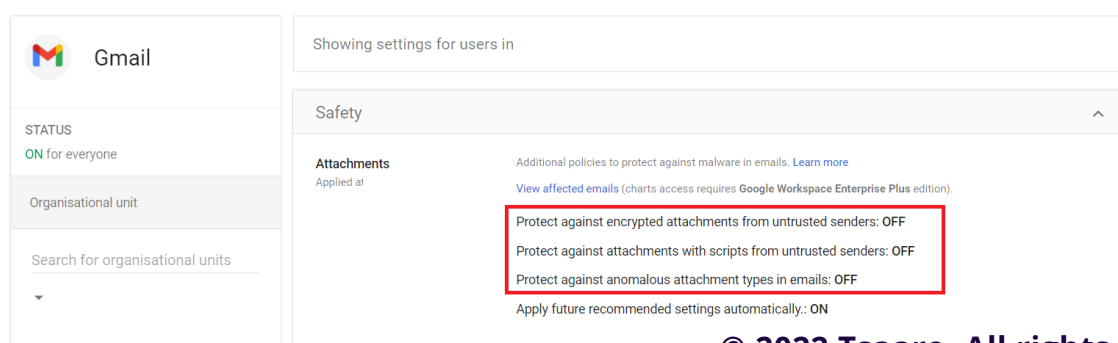
Gmail detects if an external recipient in an email response is not someone a user interacts with regularly or is not present in a user's Contacts. When you configure this setting, your users receive a warning and an option to dismiss.



10

## ENABLE ADDITIONAL ATTACHMENT PROTECTION

Google scans incoming messages to protect against malware, even if the additional malicious attachment protection settings aren't enabled. Turning on additional attachment protection can catch email that previously wasn't identified as malicious.




11

## DO NOT INCLUDE DOMAINS IN THE APPROVED SENDERS LIST

Excluding domains from the approved senders' list reduces the risk of spoofing and phishing/whaling.

Apps > Google Workspace > Settings for Gmail > Manage address list

**Gmail**

STATUS  
ON for everyone

**Manage address lists**

| Name      | Type         | Address count | Actions                                       |
|-----------|--------------|---------------|---|
| Test List | Address list | 5             | <a href="#">Edit</a> - <a href="#">Delete</a> |

[ADD ADDRESS LIST](#)

Most changes take effect within a few minutes. [Learn more](#)  
You can view prior changes in the [audit log](#)


[Navigate here](#)

12

## USE EARLY PHISHING DETECTION

You do not want your users getting phished for trouble. As a Gmail admin, you would want to add an extra layer of security to incoming emails—G Suite gives you 'Early Phishing Detection.' The moment Gmail detects suspicious content in an incoming email, it introduces a delivery delay and performs rigorous phishing analysis.

Apps > Google Workspace > Settings for Gmail > Spam, phishing and malware

**Gmail**

STATUS  
ON for everyone

Organisational unit

Search for organisational units

Showing settings for users in

**Spam, phishing and malware**

**Email whitelist**

An email whitelist is a list of IP addresses from which you want your users to receive emails. Mail sent from these IP addresses should not be marked as spam. In order to take full advantage of Gmail's spam filtering service and for best spam classification results, IP addresses of your mail servers that are forwarding email to Gmail should be added to the inbound gateway and not the IP whitelist. [Learn more](#)

Enter the IP addresses for your email whitelist: No IP address added yet

**Enhanced pre-delivery message scanning** [Learn more](#)  
Enables improved detection of suspicious content prior to delivery: ON


# GMAIL

13

## ENABLE ADDITIONAL LINK AND EXTERNAL CONTENT PROTECTION

Google scans incoming messages to protect against malware, even if the additional malicious link and content protections settings are not enabled. Turning on additional links and external images protection can catch email that previously was not identified as phishing.

Apps > Google Workspace > Settings for Gmail > Safety

 Gmail

STATUS  
ON for everyone

Organisational unit

Search for organisational units

Applied at

[View affected emails](#) (charts access requires Google Workspace Enterprise Plus edition).

Protect against encrypted attachments from untrusted senders: OFF

Protect against attachments with scripts from untrusted senders: OFF

Protect against anomalous attachment types in emails: OFF

Apply future recommended settings automatically: ON

IMAP view time protections  
Applied at

Additional settings to protect IMAP users as they interact with emails. [Learn more](#)

Enable IMAP link protection: OFF

Links and external images  
Applied at

Additional settings to prevent email phishing due to links and external images. [Learn more](#)

Identify links behind shortened URLs: ON

Scan linked images: ON

Show warning prompt for any click on links to untrusted domains: OFF

Apply future recommended settings automatically: ON



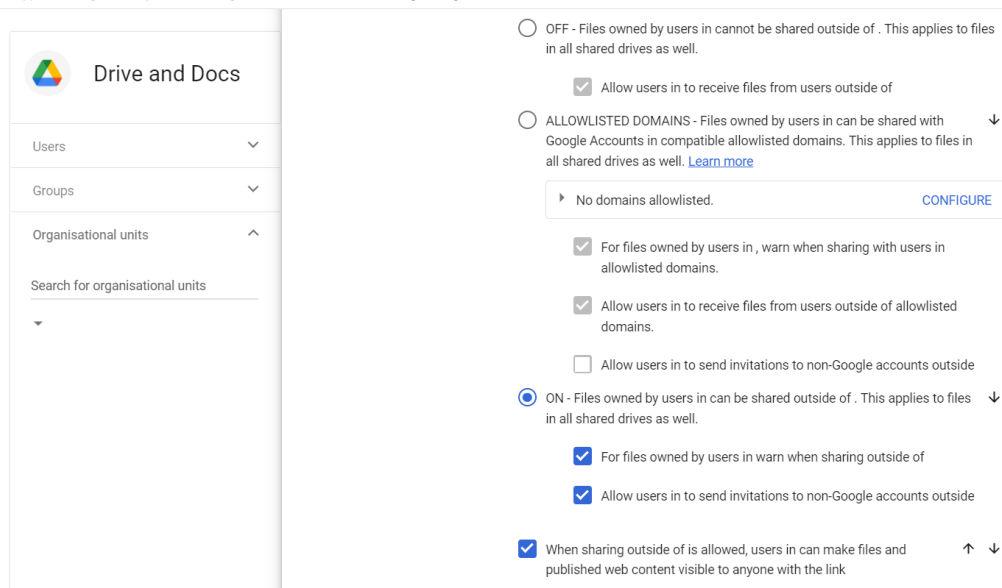
# GOOGLE DRIVE

1

## SET SHARING OPTIONS FOR YOUR DOMAIN

Confine file sharing within the boundary of your domains by turning off sharing options. This reduces data leak and data exfiltration risks. If sharing is required outside of a domain because of business needs, you can define how sharing is done for organizational units, or you can designate domains on your allow list.

Apps > Google Workspace > Settings for Drive and Docs > Sharing settings

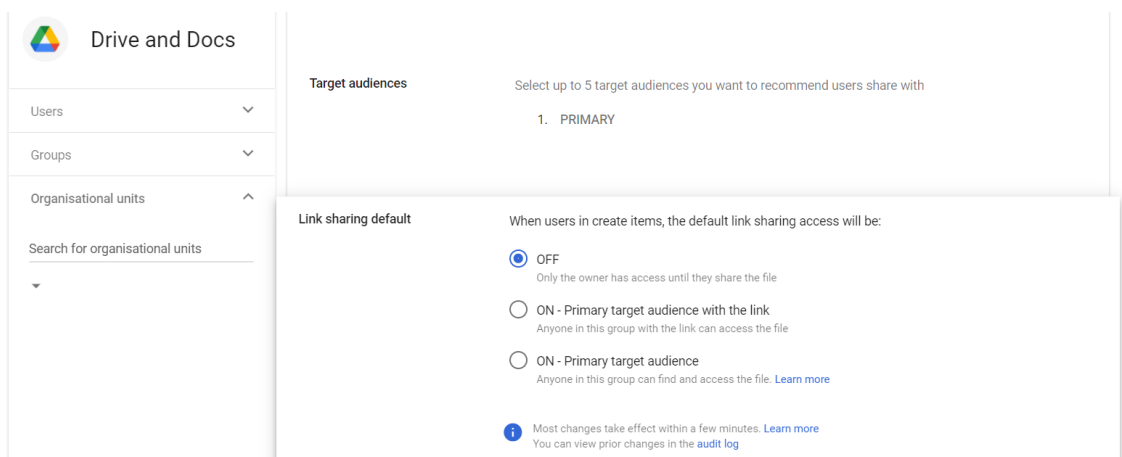


The screenshot shows the 'Sharing settings' page for Drive and Docs. On the left, there's a sidebar with 'Drive and Docs' and a search bar for 'organisational units'. The main content area has two sections: 'OFF - Files owned by users in cannot be shared outside of . This applies to files in all shared drives as well.' and 'ALLOWLISTED DOMAINS - Files owned by users in can be shared with Google Accounts in compatible allowlisted domains. This applies to files in all shared drives as well. [Learn more](#)'. Under 'OFF', there's a checkbox 'Allow users in to receive files from users outside of' which is checked. Under 'ALLOWLISTED DOMAINS', there's a dropdown menu showing 'No domains allowlisted.' with a 'CONFIGURE' button. Below this, there are checkboxes for 'For files owned by users in , warn when sharing with users in allowlisted domains.' (checked), 'Allow users in to receive files from users outside of allowlisted domains.' (checked), and 'Allow users in to send invitations to non-Google accounts outside' (unchecked). At the bottom, there's a section 'ON - Files owned by users in can be shared outside of . This applies to files in all shared drives as well.' with checkboxes for 'For files owned by users in warn when sharing outside of' (checked), 'Allow users in to send invitations to non-Google accounts outside' (checked), and 'When sharing outside of is allowed, users in can make files and published web content visible to anyone with the link' (checked).

2

## SET THE DEFAULT FOR LINK SHARING

Turn off link sharing for new files. Only the file owner should have access until they share the file.



The screenshot shows the 'Link sharing default' settings page for Drive and Docs. On the left, there's a sidebar with 'Drive and Docs' and a search bar for 'organisational units'. The main content area has two sections: 'Target audiences' and 'Link sharing default'. Under 'Target audiences', there's a text 'Select up to 5 target audiences you want to recommend users share with' and a list with '1. PRIMARY'. Under 'Link sharing default', there's a text 'When users in create items, the default link sharing access will be:' and three radio button options: 'OFF' (selected), 'ON - Primary target audience with the link', and 'ON - Primary target audience'. Below these options, there's a note 'Most changes take effect within a few minutes. [Learn more](#)' and 'You can view prior changes in the [audit log](#)'.

# GOOGLE DRIVE

3

## WARN USERS WHEN THEY SHARE A FILE OUTSIDE YOUR DOMAIN

If you allow users to share files outside your domain, turn on a warning when a user does so. This allows users to confirm whether this action is the intended one, and reduces the risk of data leaks.

The screenshot shows the 'Drive and Docs' settings page. On the left, there's a sidebar with 'Users', 'Groups', and 'Organisational units'. The main content area is titled 'Showing settings for users in' and 'Sharing settings'. Under 'Sharing options', the 'Sharing outside of' section is expanded. It shows three radio button options: 'OFF - Files owned by users in cannot be shared outside of . This applies to files in all shared drives as well.', 'ALLOWLISTED DOMAINS - Files owned by users in can be shared with Google Accounts in compatible allowlisted domains. This applies to files in all shared drives as well. [Learn more](#)', and 'No domains allowlisted.' (which is currently selected). Below these, there are two checked checkboxes: 'For files owned by users in , warn when sharing with users in allowlisted domains.' and 'Allow users in to receive files from users outside of allowlisted'.

4

## LIMIT FILE ACCESS TO RECIPIENTS ONLY

When a user shares a file via a Google product other than Docs or Drive (for example, by pasting a link in Gmail), Access Checker can check that the recipients can access the file. Set up Access Checker for Recipients only.

The screenshot shows the 'Drive and Docs' settings page, specifically the 'Access Checker' section. The breadcrumb trail at the top reads 'Apps > Google Workspace > Settings for Drive and Docs > Sharing settings'. The 'Access Checker' section has a description: 'When a user shares a file via a Google product other than Docs or Drive (e.g. by pasting a link in Gmail), Google can check that the recipients have access. If not, when possible, Google will ask the user to pick if they want to share the file to:'. There are three radio button options: 'Recipients only, suggested target audience, or public (no Google account required).', 'Recipients only, or suggested target audience.', and 'Recipients only.' (which is highlighted with a red box). Below this, the 'Distributing content outside of' section is expanded, showing three radio button options: 'Anyone', 'Only users in', and 'No one'. At the bottom, there's an information icon and text: 'Most changes take effect within a few minutes. [Learn more](#). You can view prior changes in the [audit log](#)'.

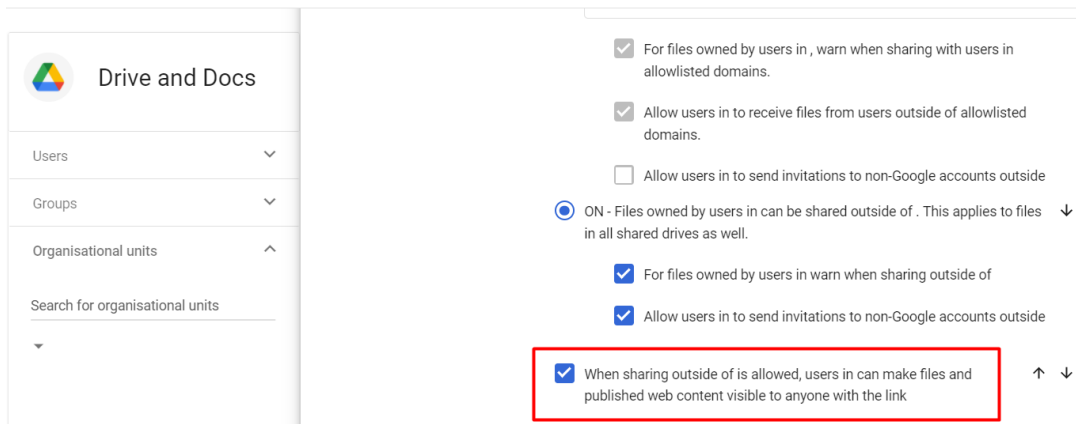
# GOOGLE DRIVE

5

## PREVENT USERS FROM PUBLISHING ON THE WEB

Disable file publishing on the web. This reduces the risk of data leaks.

Apps > Google Workspace > Settings for Drive and Docs > Sharing settings



Drive and Docs

Users ▾

Groups ▾

Organisational units ▲

Search for organisational units

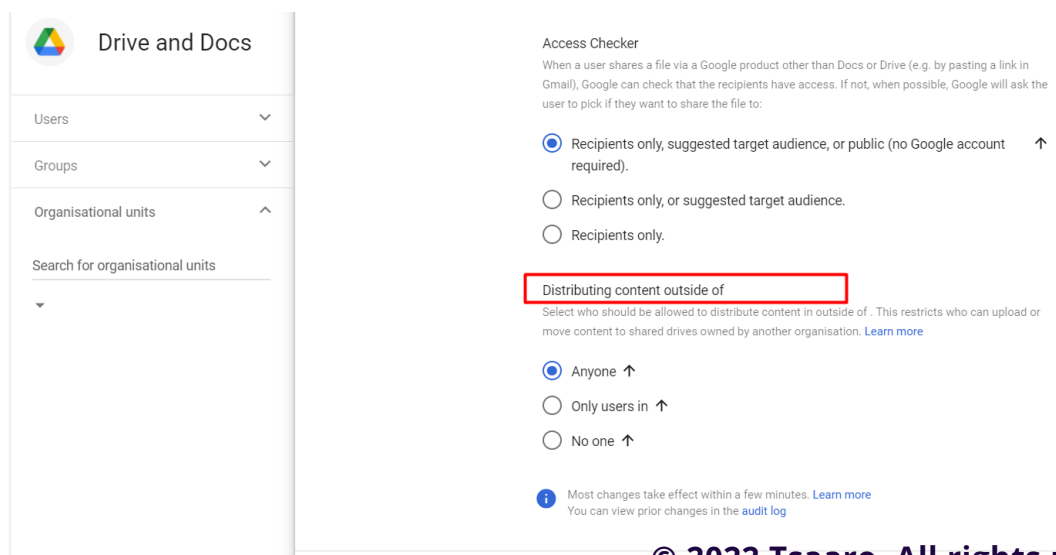
▼

- ☒ For files owned by users in , warn when sharing with users in allowlisted domains.
- ☒ Allow users in to receive files from users outside of allowlisted domains.
- ☐ Allow users in to send invitations to non-Google accounts outside
- ☒ ON - Files owned by users in can be shared outside of . This applies to files in all shared drives as well. ▾
- ☒ For files owned by users in warn when sharing outside of
- ☒ Allow users in to send invitations to non-Google accounts outside
- ☒ When sharing outside of is allowed, users in can make files and published web content visible to anyone with the link ↑ ▾

6

## LIMIT WHO CAN MOVE CONTENT FROM SHARED DRIVES

Allow only users in your organization to move files from their shared drives to a Drive location in a different organisation.



Drive and Docs

Users ▾

Groups ▾

Organisational units ▲

Search for organisational units

▼

Access Checker

When a user shares a file via a Google product other than Docs or Drive (e.g. by pasting a link in Gmail), Google can check that the recipients have access. If not, when possible, Google will ask the user to pick if they want to share the file to:

- ☒ Recipients only, suggested target audience, or public (no Google account required). ↑
- ☐ Recipients only, or suggested target audience.
- ☐ Recipients only.

**Distributing content outside of**

Select who should be allowed to distribute content in outside of . This restricts who can upload or move content to shared drives owned by another organisation. [Learn more](#)

- ☒ Anyone ↑
- ☐ Only users in ↑
- ☐ No one ↑

**i** Most changes take effect within a few minutes. [Learn more](#)  
You can view prior changes in the [audit log](#)


# GOOGLE DRIVE

7

## CONTROL CONTENT SHARING IN NEW SHARED DRIVES

Restrict who can create shared drives, access content, or change the settings for new shared drives.

Apps > Google Workspace > Settings for Drive and Docs > Sharing settings

**Drive and Docs**

Users

Groups

Organisational units

Search for organisational units

**Link sharing default**  
Applied at

When users in create items, the default link sharing access will be:  
OFF

**Shared drive creation**  
Applied at

☐ Prevent users in from creating new shared drives

When people in create shared drives, these are the default settings. The settings won't change if a shared drive is moved to a different organizational unit. To override individual shared drive settings, go to [Manage shared drives](#).

☒ Allow members with manager access to override the settings below

☒ Allow users outside to access files in shared drives  
This setting depends on Sharing outside of . [Learn more](#)

☒ Allow people who aren't shared drive members to be added to files


☒ Allow viewers and commenters to download, print, and copy files

8

## DO NOT ALLOW GOOGLE DOCS ADD-ONS

To reduce the risk of data leaks, consider not allowing users to install add-ons for Google Docs from the add-on store.

Apps > Google Workspace > Settings for Drive and Docs > Features and Applications

**Drive and Docs**

Users

Groups

Organisational units

Search for organisational units

**Google Drive for desktop**  
Applied at

Allow Google Drive for desktop in your organization  
ON

**Drive**  
Applied at

Allow users to download, install, and use Backup and Sync

**Drive SDK**  
Applied at

Allow users to access Google Drive with the Drive SDK API  
ON

**Add-Ons**  
Applied at

Allow users to install Google Docs add-ons from add-ons store.  
ON



## WHY TSAARO?

Tsaaro provides privacy and cybersecurity services to help organizations meet regulatory requirements while maintaining a robust security infrastructure.

Our industry-standard privacy services include Privacy compliance, DPO-as-a-service, Vulnerability Assessment & Penetration Testing, Cyber Strategy, DPIA to name a few, delivered by our expert privacy professionals recognized by IAPP.

### Our Team

**Akarsh Singh**  
(CEO & Co-Founder, Tsaaro)

Akarsh is a fellow in Information Privacy by IAPP, the highest certification in the field of privacy. His expertise lies in Data Privacy and Information Security Compliance.

**Krishna Srivastava**  
(Co-Founder & Head of Cyber Security, Tsaaro)

Krishna is a xKPMG data security consultant. He has vast experience in Information Security and Data Privacy Compliance.

## CONTACT US

You can assess risk with respect to personal data and strengthen your data security by contacting Tsaaro.

**Tsaaro Netherlands Office**

Regus Schiphol Rijk  
Beech Avenue 54-62,  
Het Poortgebouw,  
Amsterdam, 1119 PW,  
Netherlands  
P: +31-686053719

**Tsaaro India Office**

Manyata Embassy Business  
Park, Ground Floor, E1 Block,  
Beech Building, Outer  
RingRoad,  
Bangalore- 560045  
India  
P: +91-0522-3581

Email us

[info@tsaaro.com](mailto:info@tsaaro.com)