Top 10 Security Alerts You Should Set Up In GAT

Show Flow

0

ወ Shield



31

D Unlock



Training Resources

Top 10 Security Alerts You Should Set Up in GAT

For Google Workspace Admins, security threats don't come with warning signs; they come as overlooked file shares, inactive accounts, suspicious downloads, or missed login events.

While Google Workspace offers a strong foundation, it doesn't always give you the realtime visibility or control needed to catch the subtle signs of insider threats, data leaks, or compromised accounts.

Some of the most common challenges we hear from Admins include:

- "I had no idea that file was shared publicly."
- "We didn't catch the mass download until it was too late."
- "There's no way to know who accessed the file and when."
- "Too many inactive accounts, but no time to monitor them."

That's why proactive alerting matters.

This guide walks you through the 10 most important alerts you should configure right away to improve your Google Workspace security posture.

Each alert below includes:

- The risk you're solving
- Where to find it in GAT
- How to configure it
- Best practices
- Related articles from our Knowledge Base with a full step-by-step guide

Let's get started.



1. Files Shared Externally Without Owner Awareness

The risk: Sensitive internal files are shared with outside parties without oversight.

Our tool offers an alternative solution to Google Admin Console alerting, which we refer to as Alert Rules.

In GAT+, alerts are available across multiple areas:

- Applications
- Emails
- Drive
- YouTube
- Mobile devices
- Users
- User Logins

Drive Alert Rules support a range of activities, including:

- Number of files downloaded per day
- Number of files shared out per day
- Pattern-matching alerts (regex) for newly shared out files (Google-native, PDFs, TXT)
- Alerts based on "share to" email address patterns

=	GAT+						Claire Mills
*	Files Files Content Search	Files Deleted Shared D	rives Events Folders	s tree Group Sharing	External Domains	Domain Connection G	raph External Users
**	Drive File Audit and	d Remediation					
.	1,114 Open to full p	ublic	2,155 Open to put	olic with link	149,28	5 Files 🗧	29,264 PDFs
	20,047 Open to spec	ific external users(s)	80,044 Open to spe	cific internal users(s)	7,574 C	Documents 💡	20 maps
	61,343 Shared Drives	s Files	1,836 Shared Driv	e file with extra share:	 63,528 30,286 	Spreadsheets	1,842 Videos 72,132 Folders
4	🔊 Unlock 🔻						
\searrow	Tiala	Dath	0	Oantributara	Miannan	Flores	Actions
Ē		/Sales	smith james	-	viewer	Shared in	Actions
	Brand Guidelines.r	Open in Google Drive 대	erningen de	-	-	Public with link	

03

How to set it up:

Navigate:

GAT+ > Configuration > Alert Rules

- Create new alert
- Type: Drive
- Trigger: File shared externally
- Scope: Select Org Units, Groups or domain-wide
- Enable notification to file owners



Best practice: Notify both the admin and file owner for better accountability.

Related Articles: Set Up Google Drive DLP Alerts for Shared Out Files



2. Alert Logins from Users outside your City or Country

The risk: Suspicious logins from new or unexpected locations could indicate credential compromise, VPN tunneling, or unauthorized access attempts.

Without visibility into login geolocation, these incidents often go unnoticed until it's too late.

How to set it up:

Navigate:

GAT+ > Configuration > Alert Rules

- Add a name to the new rule and enable it.
- Type: Select User Logins
- Select Scope
- Trigger:
 - A Failed login from a country or city not previously detected
 - Add a list of expected locations (e.g. countries) where login is permitted. If multiple boxes are selected it will trigger for any, so its best practice to have a separate alert rule for each trigger.
- Start alert execution

d / edit alert rule	
Name	Users Logins
Enabled	
Туре	Users Logins 👻
Scope	Org. Unit 👻
	[F*×]
	 The care use windows contracters ^a, writen will be interpreted as any number of characters (0 or more). Example of use: /^a - full domain (root OU and all sub OUs), / (restou)^a - all Ou shat last with <i>FestOU</i>, / (restou)^a - all sub OUS of <i>/FestOU</i>.
Recipients	@generalaudittool.com ×
Notify on negative logins	
Notify new IP adresses with negative logins are used	
Notify on login events	Cogin_failure ×
Notify on logins outside	Country Ireland X United Kingdom X Bulgaria X Spain X United States X
	type full country/city names in English, eg "London", "Dublin", "United Kingdom", "Ireland"
	Type of events



How to investigate user logins:

Navigate: (GAT+ > Audit & Management > Users Logins

Use the **Events tab** to apply the following filters:

- Country not equal to expected country
- Event equal to "OK" (successful login)

Logins filters		
Event Current	⊙ Recent P Saved	
Name	Unnamed	
Definition	AND V	+ Add rule • Add group
	Country not equal United States	×
	Event equal OK	×
	• Date fields (relative): previous days/months include full days (00:00 to 23:59) or months of month) in your GAT configured time zone Etc/UTC C	(1 to last day
vent O Scheduled	Note, filter results are not presorted on any particular field.	

Best practice: Always confirm with the user before taking action. Travel or legitimate remote work may explain the event.





3. Use of Risky Chrome Extensions

The risk: Chrome extensions can introduce major vulnerabilities if they require sensitive permissions or are not vetted.

Some may access private user data, change browser settings, or even exfiltrate files, all without the user's full awareness. In schools and enterprise environments, it's critical to monitor and assess these extensions proactively.

How to monitor extensions:

Navigate:

GAT Shield > Audit > Extensions

View data on every extension installed across your domain:

- Extension name and version
- Permission list and permission score (Low, Medium, High)
- Whether enabled or disabled
- When installed or removed
- Who installed it

Use filters to audit by risk level or scope, click the "details" icon on the right end side to review deeper permissions.

=	🧑 SHIELD								🔺 🔅 🎟 😣
÷	Back to the previous UI		Extensions						
ıh	Dashboard								
	My Domain	*	+ New view - Extensions	: ×					Schedule a report
Ê	Reporting	-	User • Shield UUID • 1	Name • Is	s enabled?	+ More		To Advanced	÷ ⊞ ± :: 5 C
0	Audit ()	*	User i		Name I	Version 1	Is enabled?	3 Used permissions :	Permission score
	Cookies		providencies participants	a1daeb15b	TIM - Online Meetings Timer	2.0.9	9	alarms +4	Low
	Downloads		bila pieceleste@decisp.pelate.com	:b12466ff7b	Anti-tracker Bitdefender	1.5.0.38	0	declarativeNetRequest +7	Low
	Extensions 2		bile piecelesis (bile inpopulate care	:b12466ff7b	Shield Enterprise	3.23.0	٢	activeTap +23	Medium
	Extensions Events		tala piecelula (piecela) pelate. (pri	:b12466ff7b	Vue.js devtools	7.7.6	۲	devtools +1 +	
	Chats		Ma pincel state (him in particles (1971	:b12466ff7b	Teacher Assist	36.0.0	0	activeTap +23	Medium
	User/Device Geo Reporting		formijeles inspecials, com	1ffb52b5fc8	GAT Shield	25.3.0	0	alarms +20	Medium
	Login Control Events		Manifesting in the private and	ob819e2b76e	TIM - Online Meetings Timer	2.0.9	9	alarms +4	Low
0	Site Access Control	*	strationistics as private and	ob819e2b76e	Google Docs Offline	1.91.1	0	alarms +3 +	Medium
0	Alerts	*	striptions inform in private and	ob819e2b76e	Tango – Document and Automate Your	8.1.0	0	activeTap +	Medium
10	Commands	-	terimini shipin te prista con	71f3ce00dcf	Google Docs Offline	1.92.1	0	alarms +3 +	Medium
ŝ	Configuration	-	terioristicalities to print out	71f3ce00dcf	Vue.js devtools	7.7.6	0	devtools +1 +	
	Delegated Auditors		4						



Risk Assessment:

Navigate: (GAT Shield > Extensions > Extensions Explorer

Permission scores are calculated based on Chrome's permission categories. A high score signals potentially risky behavior, like file system access, audio/video capture, or identity manipulation.

=	SHIELD									🔺 🔅 🏼 🙆 🔹
÷	Back to the previous UI		Extensio	Details				×		
th.	Dashboard			Marris						
₽	My Domain	*	+ Ne	Name				0		Schedule a report 🔹
Ê	Reporting	*	User		Jmine				To Advanced	≑ 皿 坐 ∷ ち で
0	Audit	^	11.00	7c4a9da2-a550-49c	8-acca-cbb819e2b76e_ghbmnnjooekpm	oecnnnilnnbdlolhkhi				
	Browsing		User						Used permissions :	Permission score :
	Cookies		pawe	Origin	Chrome Web Store	Version	1.91.1		alarms 👻	Low
	Downloads		julia.p	Is enabled?	Yes	Permission score	Medium		ativeNetRequest +7	Low
	Extensions		julia.p	Туре	Extension	Used permissions	alarms 👻		activeTap +23	Medium
	Extensions Events		julia.p	Install type	Sideload	Installed at	05/10/2024 11:45:03		devtools +1 +1	
	Searches		iulia e	User can disable	Yes	Removed at	-		activeTan -	Medium
	Chats		Juno.p						(+20)	
	User/Device Geo Reporting		luna@	User				^	alarms 👻	Medium
	Login Control Events		abiga	0001					alarms +	Low
0	Site Access Control	٣	abiga	User	abigail.lewis@dev.bp.gatlabs.com	Org. unit	/Students		alarms +3	Medium
0	Alerts	*	abiga						activeTab +7	Medium
70	Commands	*	bartic	Device				~	alarms +3	Medium
鐐	Configuration	*	bartic						devtools +1 +1	*
-	Delegated Auditors		4	Shield Extension				~	Records per page 25	▶ 1 - 25 of many < >
										-

Related Articles: Audit Chrome Extensions with GAT Shield



4. Privilege Misuse or Role Escalation

The risk: Admin privileges are among the most powerful tools in Google Workspace.

If a user is given elevated permissions by mistake or if an attacker gains access to a super admin account, the consequences can be severe.

How to monitor and audit admin roles:

Navigate:

GAT+ > Audit & Management > Roles & Privileges> Roles

- Review which users hold elevated roles (Super Admin, Groups Admin, User Management, etc.)
- View role metadata and assigned privileges
- Export the list of users per role

GAT+ gives you a more readable breakdown of privileges than the native Google Admin Console, so you can quickly understand each role's risk level.

🖲 GAT+ - 🧹 🧹	Roles Privileges						
🔺 timbyin 💡 🥄 🥐							17:1-
MANAGED ACCOUNTS	•					12 records T Tx	2
# Dashboard							
AUDIT AND MANAGEMENT	<u></u>	1. D	5.6		5 C		25 50 100
🛔 Üsers	Name *	Description :	Role ID :	Super Admin Role 😂	System Role :	Actions	
🚰 Groups	_DIRECTORY_SYNC_ADMIN_ROLE	Directory Sync Admin Role	61,348,308,102,152,200		Yes	A • =	2
📥 Org. Units	_GCDS_DIRECTORY_MANAGEMENT_R OLE	GCDS Directory Management Role	61,348,308,102,152,200		Yes	4 * =	
Target Audiences	_GROUPS_ADMIN_ROLE	Groups Administrator	61,348,308,102,152,190		Yes	4 • =	
Classroom	_GROUPS_EDITOR_ROLE	Groups Editor	61,348,308,102,152,190		Yes	4 * =	
Classroom Insights	_GROUPS_READER_ROLE	Groups Reader	61,348,308,102,152,190		Yes	4 • =	
Applications Devices	_HELP_DESK_ADMIN_ROLE	Help Desk Administrator	61,348,308,102,152,200		Yes	4 • =	
C Drive	_INVENTORY_REPORTING_ADMIN_RO	Admin for Inventory Reporting	61,348,308,102,152,210	-	Yes	4 • =	
Email	_MOBILE_ADMIN_ROLE	Mobile Administrator	61,348,308,102,152,200		Yes	4 • =	
Calendars	_SEED_ADMIN_ROLE	Google Workspace Administrator Seed Role	61,348,308,102,152,190	Ves	Tes	4 • =	
YouTube	_SERVICE_ADMIN_ROLE	Services Administrator	61,348,308,102,152,200	-	Yes	4 . =	
User Logins One Click Reports	_STORAGE_ADMIN_ROLE	Storage Admin Role	61,348,308,102,152,200	•	Yes	4 . =	
Google Workspace DLP	_USER_MANAGEMENT_ADMIN_ROLE	User Management Administrator	61,348,308,102,152,200		Tes	4 • =	
A Roles & Privileges							
Looker Studio							25 50 100

Best practice: Periodically review all user roles to eliminate dormant or unnecessary elevated permissions.

Related Articles:

User Roles and Privileges within Google Workspace Admin Console



5. Detect Deleted Drive Files and Who Deleted Them

The risk: Files deleted without approval, especially from Shared Drives, can disrupt workflows or indicate insider threats.

How to investigate Drive deletions:

Navigate:

GAT+ > Drive > Events

- Filter by Event = Delete
- Filter by File Owner = Shared Drive (for Shared Drive files)
- Use the Email column to identify who deleted the file

An Admin can combine the filters and search for Events equal to 'Delete' or 'Trash' to view all Deleted and Trashed files and who performed the Deletion.

🖨 Files File Co	ontent Search	Files (Trino) Files Deleted	Shared Drives Events Folders	Tree Groups Sharing	External Domains	Domain Connection Graph
Geo located IPs						
				'Unnamed' filter -	at least 26 records	T To Z-
« 1 2 » 2				3	and the	25 5
Email	Event	Date -	Title	"Unnamed' filter - at least 26 records T 3 25 50 File Owner IP Shared Out 07:16, are presented be ow (at least 26 records have be en found). Click here to refresh. py of Alex Invoice Mar generatauditioot.com - atomic 2021 xlsx Account interateuditioot.com - - atomic atomic atomic colspan="2">- - <		
	The search is	finished. Complete results, compute	d at Nov 17, 2021 18:07:16, are presented be	ow (at least 26 records have t	en found). Click here to	refresh.
system	delete	6 days ago	Copy of Alex Invoice Mar	generalaudittool.com		-
system	delete	7 days ago	Customer 2021 xlsx	Accounts	2a02:8084:82:a600	-1-1245 at
system	delete	10 days ago	Untitled document	IIIIII IIggeneralaudittool.com	-	+1.4
system	delete	12 days ago	settings.xml	generalaudittool.com		
system	delete	12 days ago	shield-ws-large-dmff.log	generalaudittool.com	-	
generalaudittool.com	delete	12 days ago	C Sub	generalaudittool.com	192.	
generalaudittool.com	delete	12 days ago	Sub2	generalaudittool.com	192.00.00.00.00.00.00.00.00.00.00.00.00.00	-
generalauditiool.com	delete	12 days ago	Broken Inheritance Report	generalaudittool.com	192.m2+01.2m3	
generalaudittool.com	delete	12 days ago	- Long Path Report	generalaudittool.com	192.	÷

Best practice: Combine this alert with a daily Drive activity report to spot suspicious behavior, especially around sensitive content.

Related Articles: How to Find Who Deleted a File in Google Drive



6. Detect and Remove Public or Public with Link File Shares

The risk: Public file sharing settings expose internal data to anyone with a link, or to everyone on the internet.

How to find and remove public links:

Navigate:

GAT+ > Drive > Files

- Apply filter:
 - Sharing Flags contains Public OR Public with link
- Use File Operations > Remove Permissions to:
 - Remove "everyone" or "everyone with link" permissions
 - Apply scheduled cleanup
 - Optionally notify file owners



Best practice: Enable Report Only first to audit before taking action. Then automate remediation with scheduled reports.

Related Articles: Remove Public and Public with Link Permissions from Google Drive Files



7. Force Sign Out Suspicious or Compromised Accounts

The risk: A user forgets to log out from a shared device, or a lost/stolen device remains logged into a corporate account, creating an open door to sensitive data.

How to force a logout of a user account:

Navigate: (GAT Fl

GAT Flow > Create Workflow

- Choose workflow type: Modify (for active users) or Offboard (for departing users)
- Select the user(s), group, or Org Unit
- Add the Force Sign Out action
- Submit for Security Officer approval
- Once approved, users will be signed out of all active sessions

≪ 🔊 GAT Flow ∽		Ø 🌲 🦷
Q. Search in menu		
MANAGERS	Create workflow	
V Create workflow	2	
Workflow Ø Ø Ø Ø Ø Ø Ø Ø Ø	Workflow type → H Search for a user	→ D Choose actions
Event workflow		
C Recurring workflow	Force sign out users 3	
Custom attributes Custom attributes Custom attributes	Enter workflow description	
It Preapproved access		
CONFIGURATION ~		0/1000
es settings		
	Modify 4 Conditional flow	Run immediately after approval
		5
		Next

Best practice: Combine with GAT+ login alerts to create a response workflow that auto-triggers a forced sign-out when suspicious login behavior is detected.

Related Articles: Force Sign Out Users in Google Workspace



8. Block Risky or Inappropriate Websites for Users

The risk: Students or staff may visit dangerous or inappropriate sites, whether by accident or intent. This opens the door to malware, phishing, and productivity loss.

How to block websites:

Navigate: (GAT Shield > Site Access Control

• Go to Rules > Allow/Block Websites

=	🔊 SHIELD 🛛 🚺	🔺 🐮 🖽 💼 🗧
←	Back to the previous UI	Rules 0
th	Dashboard	+ New Rule Test Rules
₽	My Domain	Check is the website of ORL is allowed / blocked for a user
Ê	Reporting	+ New view - Rules i X
0	Audit	
0	Site Access Control	Search rule by website • Kulle name • Active • Action • + More
	User Defined Categories	Rule name : Active : Action : Description : Category type : Category :
	Predefined Categories	
	Rules 3	
	Block Partial Content On Pages	C annual C a
	Events	
	Block Page Configuration	
0	Alerts	-
10	Commands	· · · · · · · · · · · · · · · · · · ·
\$	Configuration	
	Delegated Auditors	
	Admin Log	
0	Help & Support	
V: 1.1	1.0 API: 1.5.778 @ 2025 GAT Labs @	Records per page 25 💌 1 - 25 of many < >

- Choose Block and define the website(s)
- Optionally set a redirect URL (e.g., company homepage)
- Define the Scope: user, group, OU, or all users
- Click Block to activate



=	D SHIELD		A** = 💼 *
÷	Back to the previous UI	Rules @ Allow / Block Websites X	
$^{\rm th}$	Dashboard	+ Ne	os >
	My Domain 👻		ebsites or URLs for a user or group
Ê	Reporting -	+ Allow Selected websites will be blocked for the user(s).	
0	Audit 👻	You can customize the redirect URL.	The second s
0	Site Access Control	Redirect URL 2	T_0 Advanced \Rightarrow III C S C
	User Defined Categories		ry type : Category :
	Predefined Categories		
	Rules		the second second
	Events		and the second s
	Block Page Configuration	Scope • 3	and the second second
0	Alerts -	Scope type * X - Include sub. org. units	the second second
10	Commands ~		and the second s
\$	Configuration -	/Students × •	
-	Delegated Auditors		THE OWNER PROPERTY.
	Admin Log		and the second s
0	Help & Support	Website List Paste from clipboard	the second second
	Hear Manual FR		Records per page 25 × 1-25 of many < >
V: 1.1	1.0 API: 1.5.778 @ 2025 GAT Labs 12	Contraction of the second s	

Tip: You can batch paste website lists and apply rules by OU to support tiered browsing policies (e.g., students vs. staff).

Related Articles: Block Websites with Site Access Control in GAT Shield



9. Monitor Suspicious Gmail Forwarding and Calendar Events

The risk: Gmail forwarding rules are a classic method for data exfiltration.

Likewise, calendar invites with sensitive data or recurring access can expose internal information without oversight.

How to monitor Gmail alert activity:

Navigate: (GAT+ > Configuration > Alert Rules

- Create a new alert
- Type: Emails
- Scope: Choose user, group, or OU

🥵 GAT+ 🗸	<	AI	lert Rules		
A finingent	37	3			
MANAGED ACCOUNTS	-	+	Add rule		- X
🖨 Dashboard		-			
	- ÷.	• 1	Name	Emails	
		Name :	Enabled		
🕼 General		90	🚺 Туре	Emails •	
		50	Scope	Org. Unit	P
belegated Auditors		-		18	
		Drive			
Bcheduled reports				Check box here for the entire OU tree, otherwise see examples below	
Alert Rules 🥝		SELELAS Day		O You can use wildcard character *, which will be interpreted as any (0 or more) number of characters (all except slash). Example of use:	
	· ·	SF FI,45 DO		 /* - all first level OUs, /TestOU* - all first level OUs that start with /TestOU, 	
User Manual START HERE C	6			 /TestOU/* - all second level OUS of /TestOU. 	
💡 Guides 🗹		Emails excee	Alert Recipients	Start typing to search and add user or group	
O Video Guides 🕑			O An alarm will trigger when any condition is met		· .

- Enable one or more of the following alert types:
 - Alert on External email forwarding (when email forwarding is enabled)
 - Alert on Email delegation (when email delegation is set)
 - Alert on new Gmail filters (when a new Gmail filter is added)
 - Alert on new email Send as
 - Alert on number of external emails received (emails in a 24 hour period)
 - Alert on number of external emails sent (emails in a 24 hour period)
 - Alert on number of external emails sent (by number. of recipients) Note: It also includes the number of (external) members in groups
 - Alert on number of internal emails received
 - Alert on number of internal emails sent



How to investigate triggered alerts:

Navigate:

GAT+ > Dashboard> Alerts

- View the alert log by user and type
- Click into alert to trace timeline and related actions

	3		Alerts fe	eed 🕢		
Rule Name	Rule Type	User		Summary		Created
SG	EMAIL	Manage	ronalgiona produces	received external emails violat	ions: 1	22 minutes ago
SG	EMAIL	-	encodeling grandpare	received external emails violations: 1		
sa	EMAIL	Salary rain	establishing printighters	received external emails violat	ions: 1	3 hours ago
Storage exceeded 350 MB	USER	a state-right	rip gibbo an	storage alect - value 350.77 MI	B (threshold : 350 MB)	8 hours ago
Storage exceeded 350 MB	USER	materiality	a prista an	storage alert - value 350 63 Mt	B (threshold : 350 MB)	8 hours ago
Storage exceeded 350 MB	USER	and the game of	- pites set	storage alert - value 546.49 Mi	B (threshold : 350 MB)	8 hours ago
Storage exceeded 350 MB	USER	(And provide a second		storage alert - value 370.70 Mi	B (threshold : 350 MB)	8 hours ago
Storage exceeded 350 MB	USER	the Register of	ogilide on	storage alert - value 350 82 Mil	B (threshold : 350 MB)	8 hours ago
Storage exceeded 350 MB	USER	patysignevice	gallabs.com	storage alert - value 361.27 Mil	B (threshold : 350 MB)	8 hours ago
Contraction of the second			Course Second		In the second second	
Alerts in last 7 days	Email alerts	in last 7 days	Application alerts in last 7 days	Drive aierts in last 7 days	Youtube alerts in last 7 days	Mobile device alerts in days
100			0	00	0	
176	1	1		23		



Bonus: How to Audit Calendar Events in Parallel

Navigate: (

GAT+ > Calendars > Calendar Events

- Filter for future events or sensitive subjects
- Use Actions to remove attendees or cancel events

🔶 GAT+ 👻 <	🛗 Cale	endars	Calendar Events	Calendar R							
&	F		2					Contraction of the second	e		
A Dashboard	Quick links Pa	ast events	Future events			'FUTUR	E events' filter -	at least 26 records	x To 2	- 🗆	4
AUDIT AND MANAGEMENT											
🚨 Users	« 1 2	2								25 50	10
🚰 Groups	Summary 🖨	Start ¢	Duration	Period \$	Created \$	Updated	Creator ¢	Local External attendees	Status ¢	Action	s
Contacts	🛱 🖪 Rec		()								
Classroom	Call - Pa	in 10 days	30	Future	a year ago	10 months ago	jen	3 generalaudit	Cancelled	۲	
Classroom Insights	lest #1										3
Applications	Report" till	in a year	60	Future	2 years ago	5 days ago	iera	er na ere si	Confirmed	۲	-
ChromeOS Devices	Robert							Delete options			_
Mobile Devices	🗄 🕓 Acti	in 2 months	30	Future	a year ago	6 days ago	Aufferungen	Delete this particular event			
🔒 Drive	🗄 😉 Rec							Delete particular attendee o	nly from this pa	articular ev	ent
Email	Call - Paul	in 2 months	30	Future	a year ago	10 months ago	jen	Remove all recurring events	for this id	1.1	
A Classic Sites	CANCEL	in 2 months	120	Future	7 months ago	7 months ago	and an or	Change organizer	om all recurrin	g events	
Calendars 1											
Meet	CANCEL	in 3 months	47580	Future	9 months ago	9 months ago	rala		Cancelled	۲	
H YouTube	🗄 🕓 Acti 🔤 👘	in a year	30	Future	2 years ago	2 days ago	040	3 generalaudit	Confirmed	۲	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	status ca	and your			2 years ago	a sujo ugo	- yenn	- Berrer and a state	Committee		

Best practice: Combine Gmail forwarding alerts with calendar audits to catch coordinated misuse (e.g. external meetings with attachments + filter forwarding setup).

Related Articles:	 Set Up Gmail Alerts for Google Workspace Users with GAT+ Google Calendar Audit and Event Management with GAT+
--------------------------	--



10. Block Risky File Downloads in Google Chrome

The risk: Users downloading executable or compressed files (like .exe, .zip, .mp3) through Chrome can introduce malware, bypass data controls, or hoard internal assets.

How to configure download blocking:

Navigate: (GAT+ > Configuration > Alert Rules

- Click to create a new rule
- Rule Type: Select Downloads
- Scope: Apply to Org Unit, Group, or entire domain
- Trigger: Download of specific file extensions (e.g., .exe, .zip, .mp3, .apk)
- Select Actions:
 - Block the download in real time
 - Notify the user and/or IT admin
 - Optionally, auto-remove the downloaded file using post-alert actions

=	D SHIELD				and the second			🌲 🔅 🗉 🚳 -
4	Back to the previous UI		Alert R	ules 0	New Alert Rule	×		
th.	Dashboard		+ New	Alert Rule	Contraction of the second s	i		
	My Domain	-			Name & Type Scope Configuration Notifications Summa	y .		
	Reporting	-	+ N	ew view 👻	Manual Trans			B Schedule a report -
0	Audit	-	Nam	е тур	Name & Type		To Advanced	÷ = : : 5 C
0	Site Access Control				exe and png download X			1.1.1
0	Alerts			Name i	Type* Download	:Severity ;	↓ Modified ;	Modified by 1
	Rules			SF EDU DEN			06/19/2025 21:50:09	scottightes by participant
	Notifications			Bad Language	Selected rule type		06/19/2025 15:32:09	manifestinging and an ex-
10	Commands			Upload alert	 Receive a notification when a user downloads a file. You can customize file formats and sizes, and choose to which pages this alert applies to. 	cified	06/13/2025 18:16:27	month approximation or
\$	Configuration	-		Alert on stude			06/13/2025 11:46:16	NAMES OF TAXABLE
121	Delegated Auditors			Trying to dele	Action •		06/12/2025 16:54:01	promption to primit of
	Admin Log			Upload alert	Action * 5 × +	cified	05/30/2025 14:00:27	temperator
0	Help & Support	-		download	Warning message	cified	05/29/2025 18:22:09	NAMES OF TAXABLE PARTY.
	User Manual 🖄			SF US SSN I	Warring message *	cified	05/22/2025 18:48:35	scorpton to printerior
	Extension Deployment Guides 01			Trying to delk	The downloaded life stext: inggered the shame rule.	cified	05/20/2025 15:48:32	promptimes to permittence
	Video Guides @			block g down	Default Severity 0	cified	05/14/2025 21:25:15	COMPANY OF DESIGNATION.
	Contact Support			Search for po	Default Severity	cified	04/25/2025 15:21:39	ADVECTOR DE DEVELO DE
				Guns Alert	6	cified	04/24/2025 17:22:07	terralization for surfactor ray W
				and the	Continue	1000	Records per page 25 +	1-25 of many < >

Tip: You can also enable reporting-only mode first to observe behavior before enforcing blocks. Combine this rule with download thresholds or geolocation filters for additional context.

- **Related Articles:**
- Block .EXE File Downloads in Google Chrome
 Using GAT Shield
- Prevent MP3 and Other Risky File Downloads



Final Tips for Admins

Security alerts are most effective when they're tied to action, not just awareness. Here are some final tips to help you manage alerts more efficiently:

- Review alert rules quarterly to adapt to user, policy, or org structure changes
- Pair alerts with scheduled reports for ongoing visibility
- Use GAT Flow to trigger automatic actions based on alert conditions (like off boarding, password resets, or forced logouts)
- Keep a spreadsheet log of your current alert rules, scopes, and recipients to stay organized
- Use Report-Only mode to test rules before applying changes

If you're unsure where to start, begin with:

- Drive sharing alerts
- Gmail forwarding
- Login from new country

These are high-impact, low-effort wins.

From there, layer on Flow and Shield coverage as you grow.

Jusers	User/Device G	eo Report	ing
Devices			
🔛 Email			
A Drive			
		3 . 136	
S Classroom			
Alerts			
III Applications		-	
Applications			
YouTube		The an elithern	
	User I	Device OS 1	City I
CONFIGURATION	emma.carter@gat.com	Windows 11	Dublin
	ethan.ramirez@gat.com	Windows 11	Dublin
	maya.lee@gat.com	Mac OS 15.1.1	Madrid
	noan.johnson@gat.com	Linux 6.8.0	New York
	all de angelaffent arm	Linux 0.0.0	2110 diala



Want To Learn More?

VISIT OUR WEBSITE

VISIT OUR RESOURCES PAGE

TRAINING SESSIONS CALENDAR

