Mandiant

DIGITAL THREAT MONITORING API LIMITS AND QUOTAS

The Digital Threat Monitoring (DTM) API has a number of limits in place to help ensure a secure and consistent experience for all users.

If you need increases to any configurable limits, you can work with your CSM.

API Rate Limits

Rate limits provide guardrails for the number of API calls a user and or organization can make in a given time frame.

Description	Duration	Limit	Scope	Configurable
All APIs: The total number of API requests allowed.	24 hours	50,000	Per user	Yes
Alert backfill: The number of backfills allowed during monitor creation. This applies to **POST** (https://docs.mandiant.com/home/digital-threat-monitoring-api#tag/Monitors/operation/post-monitor-backfill) and **PATCH** (https://docs.mandiant.com/home/digital-threat-monitoring-api#tag/Monitors/operation/patch-monitor-backfill) operations.	24 hours	50	Per user	Yes
Invalid requests: The total number of requests with a status code of 400 or greater.	1 hour	100	Per user	Yes
Bulk alert update: The number of **bulk alert changes** (https://docs.mandiant.com/home/digital-threat-monitoring-api#tag/Alerts/operation/post-alerts-bulk-apply) allowed. A bulk change applies when selecting more than 100 alerts and changing their status or tags.	1 hour	10	Per user	Yes

API Concurrency Limits

Concurrency limits provide limitations on the number of concurrent API requests that can be active at any given time.

Description	Concurrency Limit	Scope	Configurable
Document Search (https://docs.mandiant.com/home/digital-threat-monitoring-api#tag/Docs/operation/post-docs-search)	5	Per user	No
List alerts (https://docs.mandiant.com/home/digital-threat-monitoring-api#tag/Alerts/operation/get-alerts)	10	Per user	No

API Quotas

API quotas provide limitations that define the maximum number of resources a single organization can have.

Description	Quota	Scope	Configurable
Number of monitors	100	Per organization	Yes

Description	Quota	Scope	Configurable
Number of verified domains	15,000	Per organization	Yes

Monitor Limits

Limitations that define how many alerts a monitor can generate and how many resources those monitors can use while generating monitors.

Description	Quota	Scope	Configurable
Alert Limit: The alert limit is calculated as a running average starting from the moment the monitor is enabled; the rate is then projected out to twenty-four (24) hours. This means that if a recently-enabled monitor generates many alerts immediately, then the monitor can get disabled before hitting the maximum daily limit. This was done to prevent monitor misconfigurations from creating an overwhelming number of alerts.	10,000 alerts/day	Per monitor	No
Complexity Limit: The complexity limit is calculated by timing the average amount of CPU time a monitor consumes when searching documents. If the average time exceeds the threshold, the monitor is disabled.	2 seconds/document	Per monitor	No