Quotas & Limits   📝

To maintain the stability, availability, and performance of Wiz infrastructure, some features are subject to quotas and/or limits.

You can review the general [feature limits](#), or jump to a specific section:

- [Cloud service limits](#)
- [Connector limits](#)
- [Data scanning limits](#)
- [Forensics package limits](#)
- [Host Configuration Rule limits](#)
- [Report result limits](#)
- [SBOM limits](#)
- [Runtime Execution Data (RED) report limits](#)
- [Wiz API limits](#)

> ⓘ   In some cases, it may be possible to <u>request limit increases</u>.

Feature limits

Some feature limits are applied on a per user or per service account basis; others are applied on a per tenant basis.

For features that are limited both per user or service account and per tenant, all limits apply simultaneously. For instance, 5 service accounts could each make 7 API calls per second (35 calls per second total), but if 20 service accounts attempted to make 7 API calls per second (140 calls per second total), the per tenant limit would be exceeded.

Feature	Limits
[AI policies](#)	- 5 per user or service account per minute - 200 per minute per tenant - 3,000 per day per tenant
[AI remediation](#)	- 5 per user or service account per min

English ▲

Feature	Limits
	• 200 per minute per tenant • 1,000 per day per tenant
AI security graph	• 5 per user or service account per minute • 200 per minute per tenant • 3,000 per day per tenant
Automation Rule running an Action	• For Issues and Controls, 300 Actions per Automation Rule per day per tenant • For some cloud events[1], 20 Actions per Automation Rule per second[2] • For audit logs, 100 Actions per Automation Rule per second
Automation Rules saved	—
Cloud services	Varies by CSP and service. See below
Compliance	• Custom compliance frameworks: up to 200 200 categories and 200 sub-categories per category • Host configuration assessment frameworks: one enabled built-in framework from each target platform host • Enabled compliance frameworks: up to 100 (built-in cloud assessment frameworks + custom frameworks)
Custom Cloud Configuration Rules	• 1,000 custom CCRs per tenant • 1,000 custom or built-in CCRs that generate Issues per tenant • 50,000 characters per Rego matcher
Custom file detection	• 20,000 total hashes per tenant • 10 MB per CSV of hashes • 1 GB per hash file • 20 CSV uploads per day; additional uploads will be calculated after the following day's scan
Custom tag enrichment	• 10 tags per cloud asset • 10,000 total tags every 48 hours
Custom user roles	• 20 custom user roles per tenant • 150 scopes per custom user role

English ▲

Feature	Limits
Data scanning	Varies by data store. See below.
Excessive Access Findings	For groups - only for groups that don't exceed the limit. See below
Export Issue evidence as part of an Action	Maximum of 10 rows for the attached evidence.
Forensics packages	40 downloads per user per day - Each package is stored for 3 days - Package size and contents varies. See below.
Host Configuration Rules	1,000 custom HCRs per tenant - Rule assessment varies by type. See below.
Ignore Rules	150 Ignore Rules per tenant 20 Polices per Ignore Rule 20 resources per Ignore Rules 1400 characters for the name and description fields
Issues	10,000 per Control
Issue notes	1,400 characters per note - Plaintext only
Malware Detection	10,000 malware instances per workload - Maximum 100 MB per archive file (.zip, .jar, .war, .par)
Manually run an Action on multiple Issues	400 Issues
Okta Connector	2,000 user accounts per Okta group
Policy tags	- Supported Policy types: Controls, Cloud Configuration Rules, and Ignore Rules - Maximum of 10 tags per Policy (not including "wiz" keys) - Keys cannot begin with "wiz" - Keys must be unique per Policy and can have only one value - Key length: minimum 1, maximum 200 UTF-8 characters - Value length: minimum 0, maximum 200 UTF-8 characters

English ▲

Feature	Limits
	- Allowed characters for keys: English letters, numbers, and - - Allowed characters for values: English letters, numbers, spaces representable in UTF-8, ., :, =, +, -, and @ - Keys and values are case sensitive
[Projects](#)	50 Project assignments per user - Only Projects can be associated with cloud resources - Only Project Folders can contain Projects 5,000 child Projects per Project Folder 5 hierarchical levels of Project Folders and Projects 10,000 Projects or Project Folders per tenant - Project and Project Folder names must be unique
Projects scoped to a Remediation and Response deployment	500 Projects
[Run an Action on (or update) multiple Issues](#)	400 Issues per request
[Run a report](#)	5 reports running concurrently per tenant 50 reports queued per tenant 20 scheduled reports per tenant - Reports are retained for 7 days - Report result limits vary by type and export method. [See below](#).
Runtime Execution Data (RED) report	[See below](#).
[SAML role mappings](#)	250 per SAML integration
[SAML role mapping](#) group names	2,048 characters per SSO identity provider
Scanning cloud services	Varies by CSP and service. [See below](#).
Secrets scanning	300 KB per file for VCS, Wiz CLI, and IDE scans
Software bill of materials (SBOM)	Varies by Wiz license. [See below](#).

English ▲

Feature	Limits
[Threat Detection Rules](#)	100 custom Threat Detection Rules per tenant
User-initiated rescans of [application endpoints](#)	1 per ten minutes per tenant 5 per 12 hours per tenant 30 per month per tenant
User-initiated rescans of [Connectors](#)	1 per ten minutes per tenant 5 per day per tenant 30 per month per tenant
User-initiated rescans of [individual resources](#) (VMs, buckets, serverless, databases, and database servers)	1 per ten minutes per tenant 5 per day per tenant 30 per month per tenant
User-initiated rescans of [Subscriptions](#)	1 per ten minutes per tenant 5 per day per tenant 30 per month per tenant
[Wiz API](#)	10 calls per second per user or service account 100 calls per second per tenant 2 minutes per query timeout

① Cloud events that are sent to one of the following destinations may have additional limits:
`AWS_SNS`, `AZURE_LOGIC_APPS`, `AZURE_SENTINEL`, `AZURE_SERVICE_BUS`, `CISCO_WEBEX`, `AWS_EVENT_BRIDGE`, `GOOGLE_CHAT`, `GCP_PUB_SUB`, `MICROSOFT_TEAMS`, `SLACK_BOT`, `SPLUNK`, `WEBHOOK`, `SUMO_LOGIC`, `HUNTERS`.

② There is, however, no Action limit per day per tenant

Cloud service limits

The services listed below are cloud provider native types, which may be [normalized](#) to other terms in Wiz.

CSP	Service	Limit(s)
AWS	Accounts	AWS Account tags and creation times are fetched only for Organization connectors due to permission limitations.

English ▲

CSP	Service	Limit(s)
		Wiz attempts to set the value of `providerID` using [DescribeAccount](#): • For accounts scanned via an organizational Connector, the call succeeds • For accounts scanned via an account-level Connector, the call fails, so `providerID` it is set to empty
AWS	Athena Workgroups	• 10 data usage alerts per workgroup • Only Workgroups on regions with recent queries are scanned
AWS	Bedrock Agent	Only the latest agent version is fetched
AWS	Certificate Manager	10,000 per account
AWS	CloudWatch Log Group	10,000 per account
AWS	DynamoDB Table	1,000 per region per account
AWS	Elastic Block Store (EBS)	100 public snapshots per account 100,000 total snapshots per account
AWS	Elastic Container Registry (ECR)	1,000 container images per ECR repository
AWS	EMR Serverless Applications	200 per account and region
AWS	IAM Policies	IAM Policies are not fetched with tags
AWS	Identity Center (SSO)	20,000 users per SSO instance
AWS	Identity Center (SSO)	10,000 group members per SSO group
AWS	Lambda Layer	• Only versions with attached resource policy • 1,000 maximum versions per layer
AWS	Launch Template	Only the default version and versions used by autoscaling groups are fetched
AWS	RDS	100 cluster or database instances public snapshots per account
AWS	SageMaker	Disks are not scanned

English ▲

CSP	Service	Limit(s)
AWS	Simple Email Service (SES)	1000 verified identities per region per account
AWS	Simple Notification Service (SNS)	10,000 SNS topics per Account - SNS Topic subscriptions are not fetched
AWS	Simple Queue Service (SQS)	10,000 SQS queues per Account
AWS	Simple Storage Service (S3)	10,000 S3 buckets per Account
AWS	Workspaces	Disks are not scanned
Azure	Microsoft Entra ID (AAD)	10,000 group members per Microsoft Entra ID (AAD) group
Azure	Blob Storage	10,000 Blob containers per Storage Account
Azure	Service Bus Queues	10,000 queues per Account
Azure	Container Registry (ACR)	1,000 container images per ACR repository
Azure	Key Vault	1,000 secrets, keys, and/or certificates per Key Vault
Azure	OpenAI	Training datasets are scanned in the [same region as your Wiz data center](#)
Azure	Synapse Analytics	Disks are not scanned
GCP	Cloud Storage Buckets	10,000 storage buckets per GCP Project
GCP	Compute Snapshot	Only snapshots encrypted with Google keys are scanned
GCP	Container Registry	1,000 container images per Container Registry
GCP	DNS Records	100,000 DNS records per DNS zone
GCP	DNS Zone	1,000 DNS Zones per GCP Project
GCP	Google Workspace	2,000 group members per Google Workspace group
GCP	Organization policies	Organization connector is needed to view all of the inherited policies
OCI	ManagedCompartmentForPaaS	Not scanned due to an OCI lim

English ▲

Connector limits

The table below lists the maximum number of Connectors you can create per tenant. If you exceed this limit, the Connector creation will fail.

Type	Limits
AWS, Azure, and GCP	300
AKS, EKS, GKE, and self-managed Kubernetes	500
Alibaba Cloud, CrowdStrike, GitHub, Jfrog, HashiCorp Terraform, Linode, OCI, OKE, Okta, OpenAI, OpenShift, VMware vSphere, and Snowflake	100

> ℹ️ We are in the process of adding limits to all Registry Connectors.

Data scanning limits

Data scanning is limited in multiple ways: sampling, file type, and file size.

Data sampling

Wiz samples data stores to identify potential PII, PHI, PCI, secrets, etc. subject to the following limits:

Scan Parameter	Limits
Total data per data store	Buckets—200 MB Disk—Unlimited SQL Server—300 MB BigQuery–1000 lines per table DynamoDB—300 MB per database, or 1000 items (whichever limit is reached first)
Folder levels	Buckets—10 levels Disk—Unlimited SQL Server—N/A DynamoDB—N/A Azure Storage Accounts with over 500 containers are skipped as these are auto-generated containers with little or no data
Subfolders within a folder	Buckets—50 subfolders per folder Disk—Unlimited SQL Server—N/A DynamoDB—N/A

English ▲

Scan Parameter	Limits
Sampled files per folder	Buckets—100 files Disk—Unlimited SQL Server—N/A DynamoDB—N/A
Data per file	Buckets—50 MB Disk—N/A SQL Server—N/A DynamoDB—400 KB
`ListObject` API calls performed per folder	Buckets—1 call per folder, each call returns up to 1000 objects Disk—N/A SQL Server—N/A DynamoDB—N/A
Tables per region	Bucket files—N/A Disk—N/A SQL Server—N/A DynamoDB—1000 tables
(DynamoDB only) Scan API calls per table	50 RCU/sec (read capacity limit) up to 1000 items (request size, actual number depends on the object size)
(SQL only) Bytes per column	4 KB Columns containing more data are truncated. Blob columns are filtered.
(SQL and Snowflake only) Rows to sample	1000 rows

File type

Some file types are subject to data scanning limitations:

File type	Limits
JSON	Only the last two levels of the JSON file (i.e. levels `n` and `n-1`)
ZIP	• Only ZIP files in buckets • Only the first level of the ZIP file (i.e. archived formats inside the ZIP are not scanned (ZIP, docx, parquet) • Since ZIP files can be huge, Wiz scans only a sample of its content (according to the same limitations applied to bucket scanning)

File size

When a file exceeds the maximum allowed size for analysis, Wiz either performs partial analysis or skips it altogether:

File type	Limits
Files supporting streaming (i.e. CSV, TSV, Parquet, or JSON)	Wiz samples the file partially up to the maximum allowed limit
Files that do not support streaming (i.e. XLSX or Zip)	Wiz skips the analysis

Forensics package limits

Forensics packages are subject to the following limits:

Object	Limit
Single file size	15 MB
All files in the collection path	30 MB
File count in the collection path	1000 files
ZIP file	200 MB
Minimum file size	200 bytes

> ℹ️ Data is omitted from files that exceed these limits.

Host Configuration Rule limits

The assessment of each Host Configuration Rule is subject to the following host engine limitations:

Type	Description	Limit
General	Timeout for host engine running Host rule	5 minutes
File metadata test	Max traversals (recursion iterations)	1,000
File metadata test	Maximum results	1,000
Registry test	Maximum results	1,000
File content test	Maximum results	1,000
File content test	Max file size that can be checked	0.5

English ▲

> ℹ An `Error` result is returned when a Host Configuration Rule violates any of these limits.

Report result limits

> ℹ Results beyond these limits are omitted.

Different types of reports have different result limits depending upon how they are generated:

Report type	Exported via UI	Exported via API	Saved Reports
Issues	5,000 (simple) 30,000 (detailed)	N/A	50,000 (non-incremental) 500,000 (incremental)
Graph Search	10,000 (simple) 30,000 (detailed)	10,000	50,000
Vulnerabilities	N/A	N/A	—
Compliance Executive Summary	N/A	N/A	—
Host Configuration	N/A	10,000	—
Cloud Configuration	8,000	10,000	—
CI/CD Scans	N/A	N/A	N/A
Network Exposure	5,000	10,000	—
Projects	10,000	10,000	N/A
System Activity Log	5,000	10,000	100,000
Audit Log	1,000	10,000	100,000
Cloud Resources	—	—	100,000
Compliance Detailed Report	N/A	N/A	—

English ▲

Runtime Execution Data (RED) report limits

Scope	Limits
Single report	- Up to 10GB daily per tenant - Up to 10MB of data per Runtime Sensor
Entire tenant	- Up to 10GB daily per tenant - Up to 50MB of data per Runtime Sensor These limits are included with all other report limits per tenant.

RED reports scheduled hourly can only be exported to a data storage.

SBOM limits

SBOM generation and export capabilities vary by [Wiz license](#):

Wiz License	Limits
Essential	- Generate SBOM for a single resource only. - Export SBOM reports for maximum 20 resources a day.
Standard or Advanced	- Generate SBOM for single or multiple resources. - Export SBOM reports for maximum 10,000 resources a day.

Wiz API limits

> ℹ These limits do not apply to service accounts of type Sensor or Complete K8s Deployment. In these cases, a single service account can be used to cover your entire production environment

To avoid excessive impact on its backend, Wiz implements the following rate limits and timeout:

Limit	Description
10 API calls per second for queries	This limit is applied for each user and service account, so 5 service accounts on the same tenant could each make 10 calls per second, or 50 calls per second total
2 calls per second for mutations	This limit is applied for each user and service account, so 5 service accounts on the same tenant could each make 2 calls per second, or 10 calls per second total

English ▲

Limit	Description
100 API calls per second	This limit is applied across all users and service accounts on a tenant, so 10 service accounts could each make 10 calls per second or 20 service accounts could make 5 calls per second, but 11 service accounts attempting 10 calls per second would trigger throttling
2 minute timeout	API calls have a timeout of 2 minutes per query

If you have an environment with large concurrency requirements for remote access to Wiz (e.g. CI/CD pipelines with dozens of Wiz CLI scans per second, which is quite rare), then:

- Consider using different service accounts for each, or
- Embed a retry on throttle error mechanism in your scripts

In case you are encountering a timeout, consider optimizing the query by following our optimizing queries guide.

Request limit increases

Some feature limits can be increased for especially large tenants or for well-defined (but unusual) use cases.

Contact Wiz Support if you would like to explore limit increases.

Updated 1 day ago

Did this page help you?   👍 **Yes**   👎 **No**

English ▲