Cisco Threat Grid Appliance Data Retention Notes

First Published: 2017-03-03

Last Modified: 2020-06-23

Data Retention Information

Data Retention by File and Data Type

File/Data Type	Number per Day	Daily Size Occupation Limit	Retention Time	Space Required
Analysis	10,000	429.7 MB	At least 1,000 days	464.1 GB
Disk artifacts (Blobs)	150,000	16.6 GB	At least 4.3 days	76.5 GB
Contents	10,000	39.1 MB	At least 64 days	2.6 GB
Networks	10,000	4.5 GB	At least 64 days	311.1 GB
Processes	10,000	1.0 GB	At least 64 days	71.2 GB
Reports	10,000	1.3 GB	At least 1,000 days	1.4 TB
Samples	10,000	7.6 GB	At least 64 days	524.7 GB
Sandcastle-Workers	10,000	39.1 MB	At least 64 days	2.6 GB
Screenshots	10,000	468.8 MB	At least 4 days	2.0 GB
Statuses	10,000	39.1 MB	At least 4 days	168.8 MB
Timelines	10,000	351.6 MB	At least 4 days	1.5 GB
USB Contents	10,000	39.1 MB	At least 64 days	2.6 GB
Videos	10,000	5.0 GB	At least 64 days	345.5 GB
Directories	10,300	37.3 GB/day in 270,000 files	--	3.1 TB

Additional Data Retention Information

- The retention times assume a sample rate of 10k per day.
- Analysis reports are retained for a minimum of two years on an as-yet unreleased 10k-sample appliance; twice that on TG5500s/TG5504s; and a factor of >3x longer than that (i.e., >3x longer than the TG5500

retention period) on TG5000s/TG5500s. In other words, >6x longer than the unreleased 10k-sample-appliance retention period.

- The same retention rule applies to analysis data.
- Other content will be retained for less time, depending on disk availability.
- If you run a system below capacity, more content will be retained for longer periods of time.
- Disk artifacts (blobs) originating from when a system was on 1.x will be included in the 2.2 migration.
- Blobs are only retained for a short period of time after the 2.2 migration.
- Because a sample can have multiple blobs, the sample rate of 150,000 blobs/day represents an average value. If your rate differs, it may have an impact on the retention period.

Strictly Enforcing Retention Period Limits

A tgsh configuration option was made available with the 2.6 release that allows you to strictly enforce the retention period limit, by not storing artifacts from analysis for more than fifteen (15) days. When set, files will be deleted during the first nightly pruning on which they are more than 15 days old.

Note: the time period of 15 days cannot be configured or changed.

Artifacts refers to the samples themselves and other things generated from them. Artifacts do not include the analysis report HTML, which is subject to its original limits as otherwise documented. Artifacts also do not include database entries and search indexes.

The tgsh option is **strict_retention** and it is disabled (false) by default.

To enable the hard-pruning of artifacts after 15 days, in tgsh set the option to true: configure set **strict_retention true**.