Cisco AMP Threat Grid Appliance Data Retention Notes

Version 2.2

Last Updated: 3/3/2017

Introduction

This document contains the Threat Grid Appliance data retention information:

FILE OR DATA TYPE	DAILY SIZE OCCUPATION LIMIT	RETENTION TIME	SPACE REQUIRED
Analysis	1.2GB	At least 1,000 days	1.3TB
Disk artifacts (“Blobs”)	31.5GB	At least 4.3 days	145GB
Network	3.6GB	At least 64 days	250.5GB
Processes	937.5MB	At least 64 days	63.3GB
Reports	1.5GB	At least 1,000 days	1.6TB
Samples	7.6GB	At least 64 days	522.1GB
Videos	2.3GB	At least 64 days	155.6GB

Additional 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.