exabeam

Exabeam Advanced Analytics Release Notes

Exabeam Security Management Platform - Version SMP 2021.1 (I55)

Publication date April 17, 2021

Exabeam
1051 E. Hillsdale Blvd., 4th Floor
Foster City, CA 94404

650.209.8599

Have feedback on this guide? We'd love to hear from you!
Email us at docs@exabeam.com

Table of Contents

1. What's New

1.1. An Easier Navigating Experience for Smart Timelines™

It's easier than ever to investigate an event using Smart Timelines, even when you have thousands of events, with an improved navigation experience.

Never lose track of which session you're looking at. The session summary information is now always visible at the top of the page. Refer to it to immediately know which session an event belongs to.

There's a faster way to jump to the end of a Smart Timeline. Previously, clicking the down arrow loaded more events in the same session; to reach the end of the Smart Timeline, you clicked the arrow repeatedly or scrolled endlessly. Now when you click the down arrow while you're on the latest session, you're sent straight to the end of the Smart Timeline.

For asset Smart Timelines, you can now navigate to a sequence on a specific date. Use the calendar to view high risk days at a glance, then jump to the session on that day.

1.2. Protect Log Ingestion and Messaging Engine (LIME) when Ingesting with Syslog

If you use Syslog to ingest logs, a new watchdog utility keeps Log Ingestion and Messaging Engine (LIME) running when it's overwhelmed.

If LIME accumulates a backlog of data that's too large to process, it may run out of disk space and stop working correctly. A new watchdog utility ensures that your disk doesn't get full and actively monitors how much disk space you're using.

When the disk has 25 percent capacity remaining, a health alert notifies you that you're running low on disk space. In the rare case that your disk has 15 percent capacity remaining, the utility deletes files, starting with the largest one, as a last resort to keep your system running. Expect this to happen rarely, if at all.

To avoid this situation, consider tuning your system so it ingests less logs or ingests logs more slowly. If you ingest logs from Data Lake, consider setting a lower log forwarding rate.

Exabeam Documentation: Configure Log Forwarding Rate

Exabeam Documentation: System Health Alerts for Low Disk Space

1.3. Better Storage, Better Models

We optimized how we stored data so your models work better than ever.

With access to more asset data, your models more accurately detect anomalies and aggregate event statistics. This doesn't affect other aspects of your system.

2. Known Issues

EXA-33364	After you upgrade to i55, the post-upgrade check fails because the Analytics Engine can't start. The cloud service that delivers security content to Advanced Analytics settings takes a few minutes to start after your upgrade, and the Analytics Engine can't start without it.
	
	To solve this issue, restart the Analytics Engine three minutes after you complete your upgrade:
	
	`exabeam-analytics-stop`
	`exabeam-analytics-start`

VMPT-51	Previously, API authentication mechanisms accepted parameters passed through GET or POST request methods. Now, API authentication mechanisms enforce POST only. If you have custom scripts that authenticate using GET, you must update these scripts to use POST. If you have questions, contact an Exabeam technical representative.

3. Issues Fixed in Advanced Analytics i55.5 (General Availability)

The i55.5 release does not include fixed issues for Advanced Analytics.