Advanced Analytics i63 Release Notes

Exabeam Security Operations Platform - Cloud-Delivered

October 10, 2024

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

Disclaimer: Ensure that you are viewing the most up-to-date version of this guide by visiting the Exabeam Documentation Portal.

Table of Contents

About Advanced Analytics i63 Releases

Advanced Analytics releases enable you to stay up-to-date with features and bug fixes. Some releases may introduce internal bug fixes or features for other Exabeam products such as Case Manager and Incident Responder. In those cases, Advanced Analytics may have a new revision that does not have any customer-facing updates.

Some updates are managed by Exabeam and are communicated in advance so that you can initiate upgrade planning activities. Some updates are your responsibility and you must schedule the installation and upgrade of the cloud-delivered software and related security content packages.

Security Content Updates

In addition to new features and enhancements, each Advanced Analytics release includes updates to security content. These updates can include changes to supported data sources and uses cases, as well as to rules, parsers, and models. In Advanced Analytics i63 and later releases, updates can also include changes to correlation rule templates and changes to content supported by the common information model, such as product categories, platforms, and landscapes.

For detailed updates, refer to the Release Notes for the security content that corresponds to your Advanced Analytics release:

- Advanced Analytics i63 and later releases, see the New-Scale Content Library based on the common information model 2.0.
- Advanced Analytics i62 and earlier releases see the Content Library.

Features Introduced in Advanced Analytics i63

The following features were introduced in Advanced Analytics i63 releases:

Advanced Analytics i63.7

Feature	Description
Advanced Analytics Engine Restart Improvements	The Advanced Analytics engine can now restart from the beginning of the current day thus ensuring reprocessing completes more quickly. Previously, a restart could require reprocessing from a full day prior which could take longer to complete.

Advanced Analytics i63.6

There are no new features in this release.

Advanced Analytics i63.5

There are no new features in this release.

Advanced Analytics i63.3

There are no new features in this release.

Advanced Analytics i63.2

There are no new features in this release.

Advanced Analytics i63.1

There are no new features in this release.

Advanced Analytics i63.0

The following features were introduced in Advanced Analytics i63.0:

Feature	Description
Log Feed Migration	The functions and features previously under **Log Feeds** have been removed from Advanced Analytics i63. They are now managed through the Site Collectors and Cloud Collectors. For more information, see Collectors.
Rule Delivery Change	To give you more control, new Exabeam rules now ship to Advanced Analytics in a disabled state. To enable these rules, you must manually update their status on the Exabeam Rules page. See Disable or Enable a Rule.
Dashboard Support	The Dashboards app in the Exabeam Security Operations Platform which provides data visualization capabilities is now supported with Advanced Analytics. The Dashboard includes a pre-built dashboard for anomalies, which you can use as is or you can duplicate and customize it. For more information, see Anomalies Dashboard.
Search Support	The Search app in the Exabeam Security Operations Platform which enables you to perform advanced queries is now available with Advanced Analytics. Search receives enriched data from Advanced Analytics on events that have been identified as anomalous. For more information, see Anomaly Search.

Retention Policy Notice

Feature	Description
Retention Policy Information	While Exabeam has not introduced any product or entitlement change in Advanced Analytics, we are taking steps to clarify the data retention policy in regard to Advanced Analytics. The retention policy defines how long logs, events, and session data are stored in Advanced Analytics. The data retention periods are defined when you purchase a license from Exabeam. For an explanation of data retention for logs, events, and sessions, see Data Retention in the Advanced Analytics Administration Guide. To view retention period information specific to your license, see the Product Entitlement page on the Community site.

Known Issues in Advanced Analytics i63

Issue ID	Description
LMS-16790	Due to an issue with browser cookies, when you continue investigation in Advanced Analytics using the `Go to page` link for an incident, Data Lake displays an empty Data Lake page or query lacking the incident details. To view the incident details in Data Lake you must refresh the page in Data Lake.

Addressed Issues in Advanced Analytics i63

Advanced Analytics i63.7

Issue ID	Summary
UIPAA-671	Fixed an issue where Alert Triage pushed excessive alerts causing unnecessary strain on the system. With this fix, you can now dynamically disable Alert Triage or have it automatically pause when alert volumes exceed configured thresholds, allowing the system to maintain stability during spikes in activity.
PLT-14349	Fixed a synchronization issue for deployments with Unified Login enabled, where if a user was deleted, Advanced Analytics did not implement the change in real-time. With this fix, you can now ensure seamless user deletion synchronization between Advanced Analytics and the Exabeam Security Operations Platform.
PLT-14187	Fixed a logout synchronization issue for deployments with Unified Login enabled, where logging out of cloud-delivered Advanced Analytics did not automatically log you out of other Exabeam applications. With this fix, you can now enjoy seamless single logout support ensuring a unified experience across all applications.
EXA-39107	Fixed an issue related to custom asset groups where the NTLM-mismatch rule triggered incorrectly. With this fix, the rule now will be able to identify a mismatch with new hosts that arrive without any asset groups populated.
EXA-38875	Fixed an issue with user label assignment where Advanced Analytics looked at historical labels and ignored current labels. With this fix, you can now see the correct and up-to-date labels associated with your accounts in Exabeam.
EXA-38518	Advanced Analytics now provides additional visibility to help you understand why a dynamic peer group wasn't assigned to a user. Now, additional statistics in the log explain the reason for this behavior, such as when users' relation coefficient doesn't meet the minimum threshold.
Also see:	• Incident Responder Release Notes • Alert Triage Release Notes

Advanced Analytics i63.6

Issue ID	Description
UIPAA-421	Fixed an issue to address lengthy processing times for events that lack user definitions. Now, Advanced Analytics allows automatic partitioning in a number of scenarios to prevent overloading processors.
PLT-14061	Fixed an issue with IDP sessions in Advanced Analytics which caused the web interface to restart.
PLT-13813	Fixed an issue that prevented context data from being pulled from domains with dash characters (-) in their filenames.
PLT-13571	Fixed an issue that prevented context tables from populating when data in the first column of context records began with a # character. To correct this issue, parsing support for the data starting with # character has been added.
PLT-13492	Fixed a license processing issue that caused delays in navigating from the Exabeam Cloud Platform to Data Lake and Advanced Analytics.
EXA-38287	The Exabeam home icon in the upper left corner of Advanced Analytics left-navigation menu now opens the home page for the Exabeam Security Operations Platform.
EXA-37890	Fixed an issue with Risk Score sorting in various session and activity details in Threat Hunter, which caused the results to display out of order.

Issue ID	Description
EXA-37847	Fixed an issue with the Dynamic Peer Group logic where the calculation was triggered before the slave (worker) nodes had time to complete training for some models. When this occurred, the Dynamic Peer Groups were partially populated in Advanced Analytics.
EXA-37800	Fixed a calculation issue where Advanced Analytics displayed a different number of incidents on the homepage (folder icon) and on the View all Incidents page for some Users & Assets. With this fix, the calculation is consistent across the homepage and the View all Incidents page. Additionally the View all Incidents page now filters incidents by entity instead of keyword.
EXA-36199	Fixed an issue where the First access of admin share on asset (A-SA-AsU-F) rule was triggered on an asset but did not show up in the asset timeline.
Also see:	Incident Responder Release Notes

Advanced Analytics i63.5

The following issues were addressed in Advanced Analytics i63.5:

Issue ID	Description
CONT-17429	To reduce false positive alerts and provide more accurate threat detection, the scoring system for IP addresses collected from threat detection services has been modified. The default score for IP addresses, as assigned in the `is_ip_threat` field, has been reduced to a score of 1. For a list of the rule score changes, see Scoring Updates for IP Threat Rules in the Security Content Release Notes.
EXA-31707	Fixed an issue encountered during threat hunting where the Data Upload size was mislabeled as MB instead of MiB. The UI label is now corrected.
EXA-35817	Fixed an issue with model calculations that affected up to 320 rules. The model threshold calculation incorrectly evaluated event counts as anomalous based on outdated model snapshot data, causing rules to be either over or under triggered. With this fix, the percentile threshold count is now always calculated based on the latest model snapshot data instead of cached snapshots. This fix does not change the underlying calculation logic for the percentile threshold count.
EXA-36685	Fixed an issue on asset timeline pages where setting a date/time ahead of the current time resulted in an error that required the page to be reloaded. With this fix, a **No more data** message is displayed to indicate that data for future dates does not yet exist.
EXA-36703	Fixed a processing issue where Alert Triage did not raise alerts from some third-party vendors.
EXA-36988	Fixed an issue on the Exabeam Rules page where the Action drop-down menu was not fully visible on the last rule in the search list.
EXA-37190	On the System Activity page, the text color has been changed to make it visible in Day Mode.
EXA-37376	Fixed an issue where asset timelines could not load domain controller timelines. When this occurred the timeline would appear to hang without loading data. This was due to an error with the logic for defining asset IDs by IP address or hostname.
EXA-37380	Fixed an issue on the Timeline pages where the screen would hang and Timeline buttons would become disabled.
EXA-37441	Fixed an issue where Data Insights and Rule Definitions were not available for some processes when `peerGroupInfo` and `groupInfo` could not be determined.
EXA-37559	Introduced an enhancement to improve performance related to reprocessing time after Advanced Analytics restarts. With this enhancement, the time required to analyze logs during the downtime is now significantly decreased.

Issue ID	Description
EXA-37788	Fixed an issue with worker nodes that caused processing delays when an empty event list was encountered. With this fix, worker nodes can now proceed with processing to avoid any additional delays and provide additional helpful details in the log.
NGPM-1425	Fixed a link on the Exabeam Engine page for initiating UIP Log Reprocessing through Customer Support.
PLT-13600	Fixed an issue that caused excessive delays with audit log ingestion times and anomaly notifications.

Advanced Analytics i63.4

The following issues were addressed in Advanced Analytics i63.4:

Issue ID	Description
EXA-37324	Fixed an issue where alerts from Advanced Analytics to Alert Triage were delayed excessively.

Advanced Analytics i63.3

The following issues were addressed in Advanced Analytics i63.3:

Issue ID	Description
SRE-1891	Fixed an issue where logs for login events did not contain the correct source IP address.

Advanced Analytics i63.2

This release does not include bug fixes for Advanced Analytics.

Advanced Analytics i63.1

This release does not include bug fixes for Advanced Analytics.

Advanced Analytics i63.0

The following issues were addressed in Advanced Analytics i63:

Issue ID	Description
PLT-13458	Fixed a license processing issue that caused delays in navigating from the Exabeam Security Operations Platform to SaaS Data Lake and Advanced Analytics.