

Exabeam Data Lake Release Notes

Exabeam Security Management Platform - Version SMP 2020.4 (I36)

Publication date April 29, 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

Disclaimer: Please ensure you are viewing the most up-to-date version of this guide by visiting the [Exabeam Community](#).

Copyright

All content in this document, including text, graphics, logos, icons, images, and video clips, is the exclusive property of Exabeam or its content suppliers and is protected by U.S. and international copyright laws. The compilation (meaning the collection, arrangement, and assembly) of all content in this document is the exclusive property of Exabeam and is also protected by U.S. and international copyright laws. The content in this document may be used as a resource. Any other use, including the reproduction, modification, distribution, transmission, republication, display, or performance, of the content in this document is strictly prohibited.

Copyright ©2021 Exabeam, Inc. All Rights Reserved.

Trademarks

Exabeam, the Exabeam logo, Threat Hunter, Smarter SIEM, Smart Timelines and Security Management Platform are service marks, trademarks or registered marks of Exabeam, Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. The marks and logos displayed in this document may not be used without the prior written consent of Exabeam or their respective owners.

Patents

Exabeam owns, and reserves all rights for, patents for Exabeam products and services, which may be protected under registered patents as well as patents pending.

Other Policies

For information regarding Exabeam's treatment of personally identifiable information, please review Exabeam's current privacy policy at www.exabeam.com/privacy.

Table of Contents

1. What's New	5
1.1. Update Security Content Over Cloud	5
1.2. Syslog Forwarding Rate Configuration	5
1.3. Exporting Large Volume Query Results	5
1.4. Improved Correlation Rules Monitoring	5
1.5. Improved Parser Management Controls	5
1.6. Exabeam Site Collector Egress Filtering	6
1.7. Smartctl Added To System Monitoring	6
2. Known Issues In Data Lake SMP 2021.1 DL-I36 General Availabilty	7
3. Fixed Issues In Data Lake SMP 2021.1 DL-I36 General Availability	8
4. Issues Fixed In Data Lake I36.7	9

1. What's New

This release of Data Lake arrives with some very powerful and handy use cases for the Security Analyst in addition to other system stability and maintainability improvements.

Data Lake I36 features include:

- [Security content package updates via cloud as well as management dashboard improvements](#)
- [Syslog forwarding rate is now configurable](#)
- [CSV and PDF exports supports large volume query results](#)
- [Improved correlation rules monitoring](#)
- [Improved parser management controls](#)
- [Egress log filtering at site collectors](#)
- [Improved system monitoring](#)

1.1. Update Security Content Over Cloud

Stay update with threat filters using Exabeam's security content parsers downloaded on a regular basis from the cloud. If you choose to, you can also upload your own customized security content parsers or remove obsolete ones. For more information, see [Manage Security Content in Exabeam Data Lake](#) .

1.2. Syslog Forwarding Rate Configuration

Manage syslog forwarding volumes from Data Lake to log recipients. Balance the output of Data Lake log forwarding with ingestion limits at destination endpoints. Configure maximum throughput between 3,000 to 55,000 events per second. For more information, see [Configure Log Forwarding Rate](#) .

1.3. Exporting Large Volume Query Results

Up to 10 million records can be exported to CSV files for each query. You can choose to chunk results into 10k, 50k, 100k, 250k, and 1M records per CSV file.

PDF exports are available for reports and dashboards with up to 5 monthly scheduled reports per time window and 20 nested objects.

1.4. Improved Correlation Rules Monitoring

In some cases, correlation rules trigger their suspension and require correction before resuming. You can verify the status of correlation rules by querying the Exabeam audit logs. For more information, see "How to Find Disabled or Erred Correlation Rules" in [How to Forward Alerts Using Correlation Rules in Exabeam Data Lake](#).

1.5. Improved Parser Management Controls

As custom parsers can wrack havoc on system performance, Exabeam continue to make improvements to allow you control and visibility to your parsers. You can select how host resources are allocated. Parsers performance will be weighted against your performance preference. Parsers that cross performance thresholds are suspended. You can review parser statistics and resume a suspended parser as you need to. For more information, see [Parser Management](#) .

1.6. Exabeam Site Collector Egress Filtering

Optimize logs ingested by the Exabeam Site Collector by applying additional filters before forwarding. Configure correlation rules to the site collector to focus your data and reduce the load for the log recipient. For more information, see [Filtering Outbound Logs in Exabeam Site Collector](#).

1.7. Smartctl Added to System Monitoring

`smartctl` is now part of Exabeam's tools to monitor cluster nodes. With `smartctl`, hard drive failures will be detected more readily.

2. Known Issues in Data Lake SMP 2021.1 DL-i36 General Availabilty

3. Fixed Issues in Data Lake SMP 2021.1 DL-i36 General Availability

DLA-3148	Exabeam Data Lake Collector beats upgrade failed due to compatibility mismatch.
PLT-11559	The Exabeam UI was unable to display when the browser was configured to the language "French (France)".

4. Issues Fixed in Data Lake i36.7

LMS-14433	Syslog port 515 allowed TLSv1.0 instead of only TLSv1.2+. The TLSv1.0 protocol is outdated and less secure than TLSv1.2+.
PLT-11381	After installing an SXB default package from Content over Cloud, the previously installed default package disappeared. Without the previous package, the customer could not roll back to it if needed.
LMS-14200	Table fields were not properly exported to CSV files. Fields in the CSV file did not always match the fields in the source table, and they were often displayed in a different order.
LMS-14099	When trying to export logs related to the <code>cef-carbonblack-network-connection-successful-2</code> parser, users encountered the following error: <code>Export CSV: Error 500 : undefined.</code>
DLA-3242	The backslash (\) escape character was not always recognized in correlation rules.