

Forcepoint Behavioral Analytics

KNOWN ISSUES FOR VERSION 3.4.1

Publish Date: September 20, 2021

Copyright © 2021

F23-06-02-09172021

Legal Notice

No part of this document shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the company. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this document, the authors and the company assume no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalized. The company cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or completeness is implied. The provided information is on an "as is" basis. The authors and the company shall have neither liability nor responsibility for any loss or damages arising from the information contained in this document. Printed in the United States of America.

This document contains proprietary information and is furnished for evaluation purposes only, and, except with written permission of the vendor, such information shall not be published, or disclosed to others, or used for any other purpose, or duplicated in whole or in part.

Attributions

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalized. The company cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Improvements and Bug Fixes

PST PARSER PARSES SUBJECT AS RECIPIENT

An issue was found with the PST parser where the email subject would sometimes be parsed as a recipient. The issue has been fixed.

Known Issues

LYNC CHATS WITH UNICODE CHARACTERS ARE DUPLICATED DURING INGESTION

When Lync chats that have unicode characters in them are split into events, two events are created for each chat entry. One of the events appears to correctly interpret the unicode characters and the other has diamond characters for the unicode. Altering the `type_detection_regex` seems to have no impact on the problem. **RPP-15128**

EVENT COUNT MISMATCH ON THE ENTITY TIMELINE

There is an event count mismatch between the Event Viewer and the Event shorthand block. **RPP-15092**

MDS ENDPOINT THAT CONVERTS RQL TO ES QUERY DOES NOT PRODUCE VALID QUERY

The MDS Endpoint `/reference/query/es/rql` (designed to convert an RQL query to an equivalent ES query) does not produce a valid query in the returned response. In particular, it returns two additional fields (ranges and indices) that are not valid for an ES query. **RPP-15117**

SOME ITEMS ARE UNREACHABLE IN LONG LISTS ON THE GROUP TAB

When adding users to a group, if the user suggestion list is too long to fit on the screen, a scroll bar is supposed to appear in the suggested user list. Instead, the list just keeps growing until it can no longer fit on the screen, leaving some entries unreachable unless the zoom of the browser is reduced enough that the entire list is displayed. **RPP-14634**

FEATURE SEARCHES CAN SOMETIMES RETURN TOO MANY RESULTS

Feature searches that are designed to return less than three recipients can sometimes return events with three or more recipients. **RPP-14496**