# v3.1.1 Release Notes for Forcepoint UEBA

Release Notes | Forcepoint UEBA | v3.1.1 | 22-Feb-2019

Use the Release Notes to find information about what's new and improved in Forcepoint UEBA version 3.1.1.

## Features

### Product renaming

At version 3.1.1, Forcepoint UEBA is renamed Forcepoint Behavioral Analytics. Product functionality is unchanged, continuing to deliver a solution that helps you understand and manage risks presented by an individual's behavior and intent.

While this change takes effect in this version, the new name will be reflected in the product UI and user documentation in the next release.

As part of the Human Point System, Forcepoint Behavioral Analytics version 3.1.1 is certified to work together with Forcepoint DLP v8.6.0 to deliver Dynamic Data Protection.

### Published Risk Score

- Previously, Forcepoint UEBA publisher would choose the highest risk score in a user's history as that user's published risk score, making it impossible to downgrade the risk score over time. The published risk score is now the most recently computed risk score for each user, regardless of the user's risk score history. (RPP-11839)

### Behaviors page displays without selecting an end date

- Prior to 3.1.1, when the Behaviors page was viewed without an end date selected, the end date would set as the current system time and the data displayed was incorrect. The end date now sets as the time of the last event in the dataset, which then displays the correct data. (RPP-12131)

## Behaviors page dataset time selector

- Previously, while on the Behaviors page, users could select hours from the date picker did not match the event dataset. This prevented scores from being properly updated and the entities appeared as having scores of “0”.

  The date picker now only loads dates and times that match the dataset, only allowing selection up to the first and last allowable hours for the given dates. (RPP-12095)

## Hourly Scores on the Entity Timeline

- Prior to v3.1.1, the Hourly Scores (formerly called Scenario Scores) shown on the Entity Timeline were normalized across all hours of the day and scaled by the 24 hour day score, rather than showing the normal score for events in the hour.

  The Hourly Scores have been updated to display as they do on the Behaviors page. They will now display normalized over the historical window and not rescaled. (RPP-12210)

## Entity Timeline shows events within an hour

- The entity timeline now calculates data matching the last hour and displays events that have occurred in that time frame. (RPP-12074)

## Publishing ingest metrics by mode

- With the removal of the convenience endpoints, event ingest metrics are bundled into “event”, “voice”, and “rfc822”. Public API metrics that are named after their type or mode can now be ingested and published by mode. (RPP-7812)

## Timezone field removed from public API model

- The public API model had a Timezone field that appeared to be completely disregarded. The correct way to submit timezone information with events is to include it in the timestamp. For example: `"timestamp": "2017-12-31T11:30:00-08:00". The Timezone field has been removed. (RPP-11307)

## Ingest processor to extract search terms from URL

- An ingest processor which operates on the string event attribute named "URL" has been added to extract the set of search terms using a regular expression. For example:

  ```
  \/search?.*?(q|s|b)=([^&]+)
  ```

  This appends the search terms into the beginning of the content field. (RPP-10351)

## Acknowledge zoned disclaimer text by default

- Zoned text is now excluded from feature analytics and from searches by default. This includes disclaimers and quoted text from email threads. (RPP-10550)

## Manually adjusting Risk Scores

- Users can now manually adjust risk level for a given entity for a set period of time. Navigating to the Risk Level tab of the Entity page, the Override Risk Level button allows an administrator to select a level and duration to override the given entity's calculated risk level. Adjustments are made based on external information the analytic platform cannot access. The manually adjusted risk level displays on the Top Entities list and on the Risk Level tab of the Entity page. The computed risk level displays as an offset circle to the adjusted risk level. The color of each circle matches the given risk level. All manual risk level adjustments are stored in the audit log. (RPP-11062, RPP-11058, RPP-11060, RPP-11588)

## Add stricter controls to Risk Level Attributes on Entity Profile

- Functions to edit, add, and delete attributes on the Details tab of an entity profile with the name Risk Level or Risk Level Override are disabled. A hover tooltip displays the following message: “This is a system-managed attribute and cannot be manually modified”. (RPP-11054)

## Move risk level export settings to appconfig

- The Risk Level attribute has been moved to AppConfig. It is no longer required as an analytic_display_attribute in the Analytics group of app config in order to see risk levels on the Analytic dashboard. If you are using the default settings for analytic_display_attribute, Risk Level will be removed for you. If you have a custom setting for analytic_display_attribute, remove Risk Level. (RPP-10069)

## User Management page

- The User Management page has been updated to include a User tab, a Groups tab, and a Permissions tab.

  From the Users tab of the User Management page, groups are now visible for each user within the users table. Hover over the groups number for each user to show which groups in which the user is a member.

  From the Groups tab, users can add, edit, and delete user groups. All groups that exist except for the All Users group are shown on the left pane and can be edited. Clicking the plus icon enables a user to create a new group and users can be added or removed from the listed groups by checking the appropriate checkbox.

  From the Permissions tab, administrators assign lexicons to be visible to specific user groups. A table with all lexicons and group names allows administrators to check boxes to assign a lexicon to one or more groups. By default, a lexicon is part of the All Users group, meaning it is visible to every user. Lexicons cannot be part of both the All Users group and a user defined group at the same time. (RPP-10428, RPP-10429, RPP-10431, RPP-10430)

## Add and manage Lexicon permissions on the Lexicons page

- Administrators can use a link on the Lexicons page to add and edit Lexicon permissions, including assigning lexicons to user groups. When this link is clicked the user will be taken to a modal where they can add or remove group access to existing lexicons. Once the changes are made, adminsitrators are required to review the desired changes before saving. It is possible to hide lexicons from yourself. The Review window warns against this. (RPP-10436, RPP-10433)

# Known Issues

A list of resolved and known issues in this release is available to Forcepoint UEBA customers here.

If you are not currently logged in to the Forcepoint support website, clicking the link brings up a My Account login prompt. Log in to view the list.