v3.0.1 Release Notes for Forcepoint UEBA

Release Notes | Forcepoint UEBA | v3.0.1 | 10-Jul-2018

Use the Release Notes to find information about what's new and improved in Forcepoint UEBA version 3.0.1.

Features

Search for current Entity Attribute values

Users can now search for a specific entity attribute based on the current time. For example, users can search for the attribute time interval that overlaps with the current instant (null start/end indicate that the attribute is unbounded in that direction). (RPP-9858)

Rose installed on anonymized and non-anonymized environments

Upgrades are supported from v2.60, 2.61, and 2.70. Pseudonyms are preserved and transferred from refdata to rose. (RPP-9430)

ER Keys migrating to pseudonym

ER Keys are now using pseudonym column header. ER keys stored in ES are migrating to the new format so they can be pulled down and be in the correct format. (RPP-9544)

Risk Level added to the Top 50 Entities of Interest card

Risk Level has been added to the Top 50 Entities of Interest card on the Analytic Dashboard. There are now two columns on the card:

- Risk Level

  The Risk Level column contains the Risk Level for the assigned entity corresponding to the end date of the current view on the analytics dashboard.

  The dashboard shows a 7 day view, and the risk level displayed represents the most recent risk level, or the risk level on the end date. (RPP-9830)

  Note that the risk level entity attribute now has a start and end date. If either is unpopulated, it means that value unbounded, or continues on indefinitely in whichever direction is null. The UI needs to process the dated entity attributes to find which corresponds with the end date currently being displayed on the analytic dashboard.

- Risk Score

  Nothing changes here except that we've changed the column from Score to Risk Score.

Filter by Entity Risk Level

From the analytic dashboard, users can filter their dashboard by each entity's risk level, numbered 1-5. This allows analysts in the RAP space to quickly triage risky users and filter lower risk level users. This also helps keep those recently risky (high risk level) though not currently risky (risk score) in view for longer. (RPP-9831)

All filters are selected by default. To remove a Risk Level filter, click the number filter to be removed, then click **Apply**.

Specify start and end times in Feature Configuration

The UI for configuring features to apply to data ingested in the future has been updated to allow specific start and end times to be selected.

Active start and end date times can be specified in both the Create Feature and Update Feature modal. Deselecting the checkboxes disables date/time.

When a user creates a new feature, the active start date time defaults to the current date/time rounded up to the next minute. The active end date and time defaults to none.

Both start and end active date time can be either in the past or in the future. (RPP-8195)

✓ **Note**

Start and end date time will be in UTC, since that is what is implemented in MDS.

Identifiable information for browser-based event log entries

For browser-based event log entries that refer to Event ID, additional information is now included to make the event identifiable and retrievable from archives outside of Forcepoint UEBA, similar to the audit log entries. This includes the event mode and compound key information available: (RPP-7548)

- Event ID (already included)
- Type
- Roles
- Event timestamp
- Subject

Stop timeline from computing analytic data in intervals

An analytics configuration option has been added that, when activated, stops the entity timeline from computing analytic data in intervals. To enable this configuration, set "disable_timeline_compute" to “true”.

```
curl -k -XPUT https://&lt;mds-url&gt;:&lt;port&gt;/
reference/config/analytics -d'{"disable_timeline_compute":
true}'
```

✓ **Note**

When using this option and viewing entity timeline data for uncomputed intervals, it results in an error.

The recommended workflow for this configuration is:

- Compute timeline data regularly (daily, hourly, etc.)
- Only visit the timeline for data that is already computed.

Pre-computing the timeline will results in a much faster entity timeline with this option configured. (RPP-9616)

Generating pseudonyms automatically for ER Keys

A new query parameter has been added to `/resolution_key/upload`, `pseudonymStrategy`, that determines how new pseudonyms are to be generated. (RPP-9634)

There are four possible values:

- NONE: Does not generate new pseudonyms.
- STRICT: Generates new pseudonyms only if the key does not have a pseudonym column.

> ✓ **Note**
>
> Using STRICT for a resolution key with a pseudonym column results in an error.

- WITHOUT: Generates new pseudonyms only for entries without existing pseudonyms.
- OVERWRITE: Generates a new pseudonym for every entry, overwriting any existing pseudonyms.

Known Issues

A list of resolved and known issues in this release is available 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.