Enhancement in EventTracker Receiver to support Alert Email Header

EventTracker Enterprise

Publication Date: Nov. 18, 2016

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Update: ET82U16-033

Abstract: This update will provide an option (Back to Top/Go to bottom) to navigate between Top/Bottom page and its details in Event Tracker application.

Who should read this document?

Customers who use v 8.2 Build 14.

Why to apply the Update?

- Multiple Selection of Reports (**Maximum: 5**) and download the Reports as zip file, from the Report Dashboard.
- Multiline header/footer allowed in Alert email configuration.

Other Enhancements:

- To avoid scrolling, an option (Back to Top/Go to bottom) has been provided, which will allow the user to navigate between Top/Bottom page and its details in Event Tracker application.
- Enhancement in remedial action scripts to generate new events like 10000,8012,8013,8014 & 8015 with the existing events 9998,9999,8009,8010 & 8012.

Table of Contents

Process to be followed after applying the Update

The Back to Top/Go to bottom option will be available in all the modules (**Except: Log Search**, **Parsing Rules** and **EventVault Explorer**) of EventTracker Application; where earlier the scrolling was required.

- Login to **EventTracker** web and click any module. For Example: **Incident->Tabular view**.

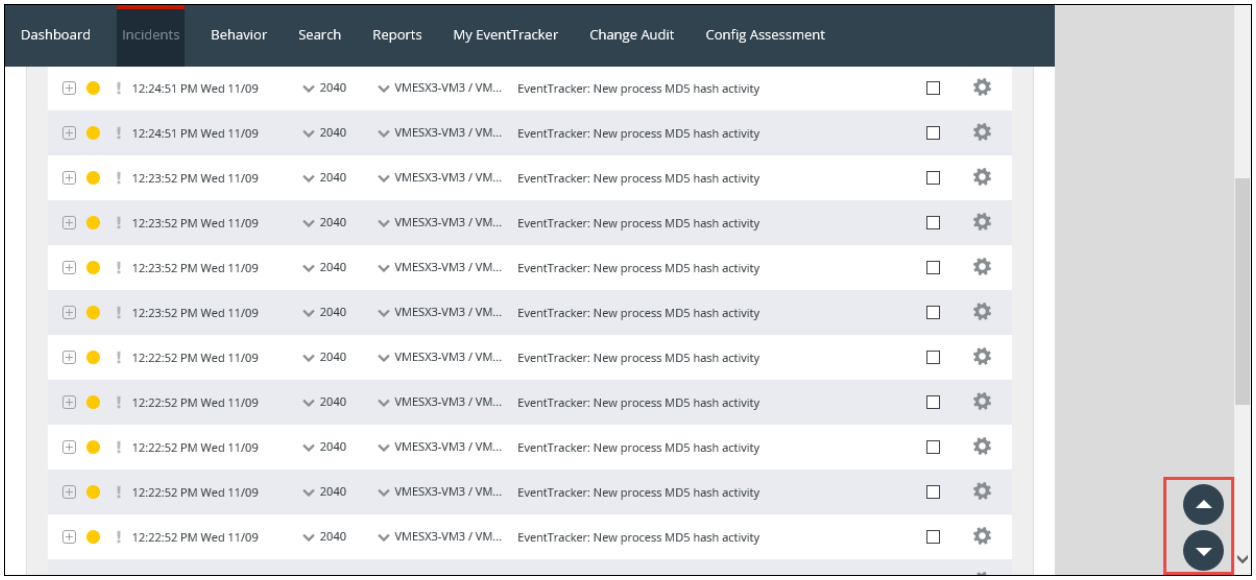

Figure 1

- Click the Top and Bottom arrows icon , as per navigation convenience.

Multiple Reports selection and download

This enhancement will be available in the modules: **Reports** and **My EventTracker Reports.**

- Select **Reports-> Dashboard**.
- Select Multiple Reports (Maximum**: 5**).
- Click the Download report(s) icon .

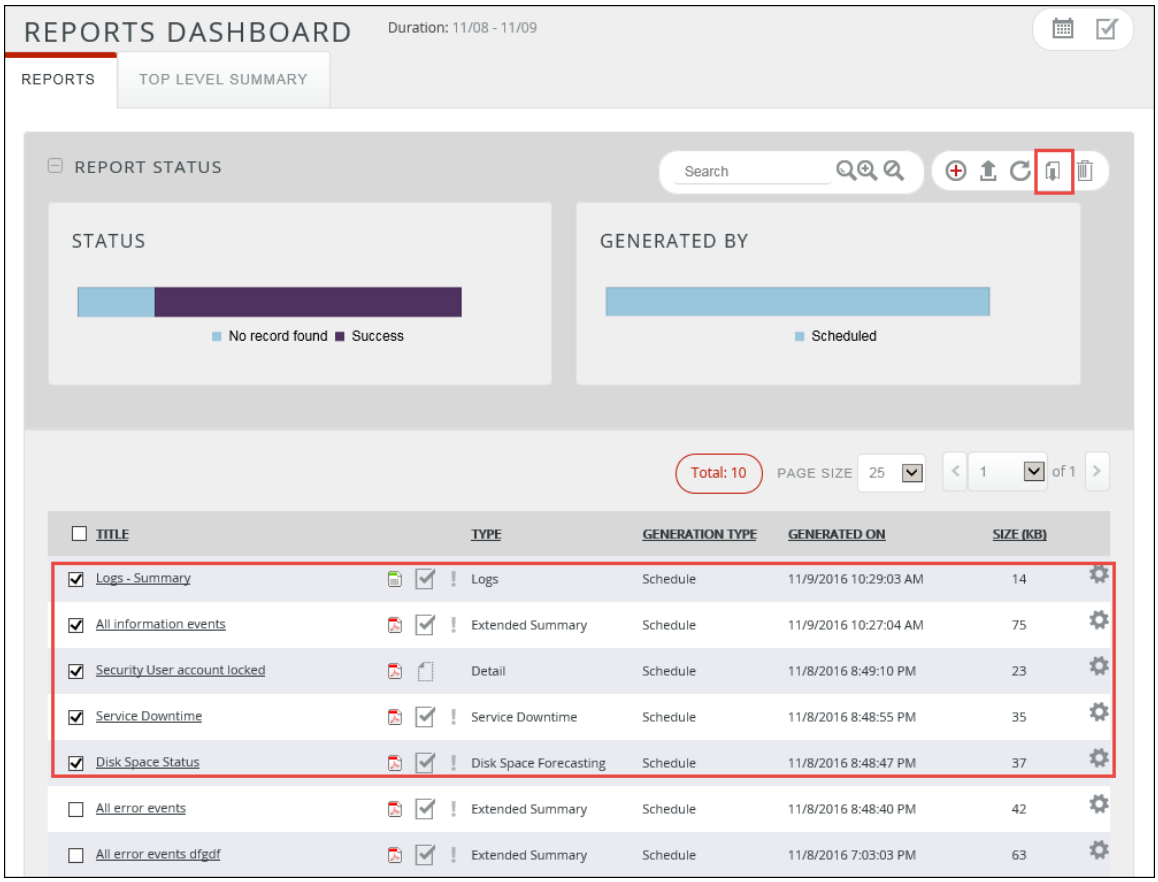

Figure 2

NOTE: If more than 5 reports are selected, it will display a warning message.

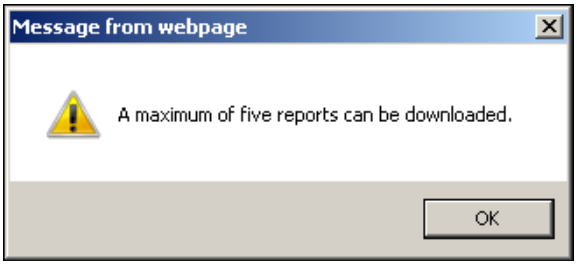

Figure 3

Multiline header/footer in Alert email configuration

In Manager Configuration

- From **Admin** dropdown, select **Manager**.
  Two new options will be available.

- To add the **Alert Header/Footer**, check the options and add the header/footer in the respective fields.

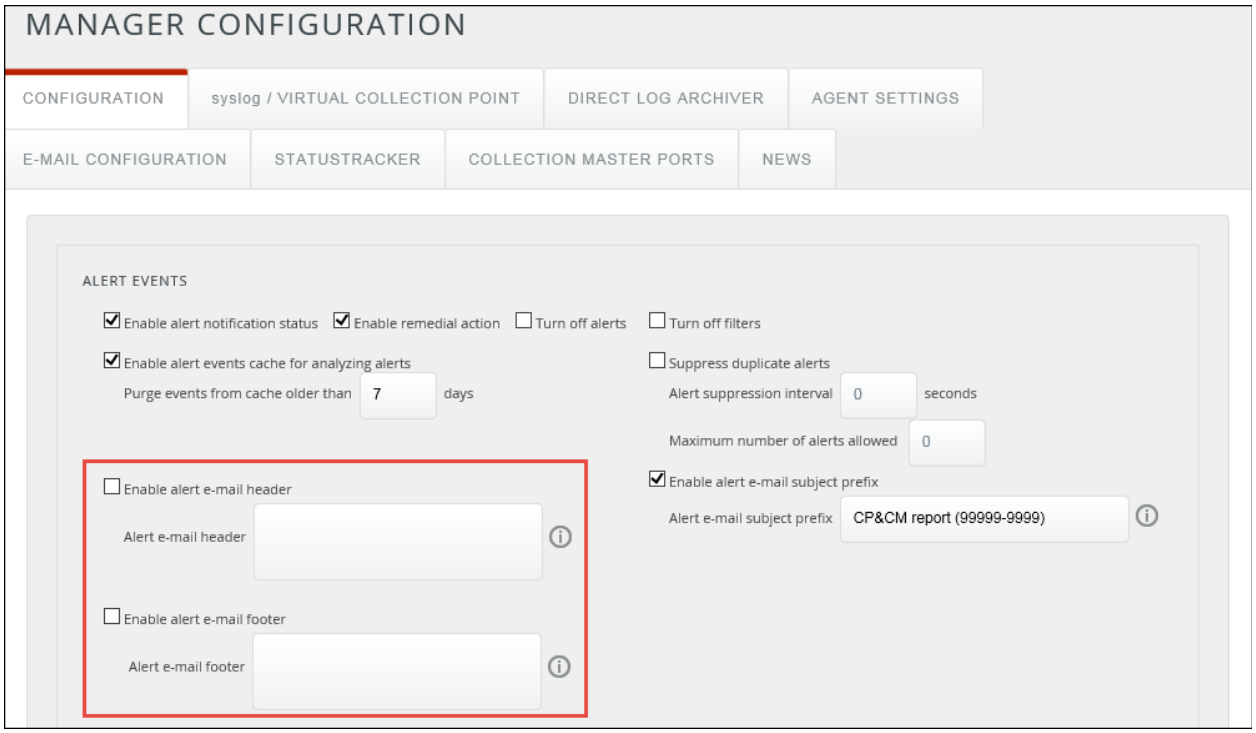

Figure 4

- **Save** the changes.

In Alert Configuration,

- Select **Admin** and click **Alerts** from the dropdown list.
- Select an alert and in the Alert configuration page, click '**Actions**".

In the e-mail configuration page, the user gets new option to add **Alert e-mail subject prefix**, **Alert Header/Footer**.

- Enter multiline header/footer, for configuring an email alert action.

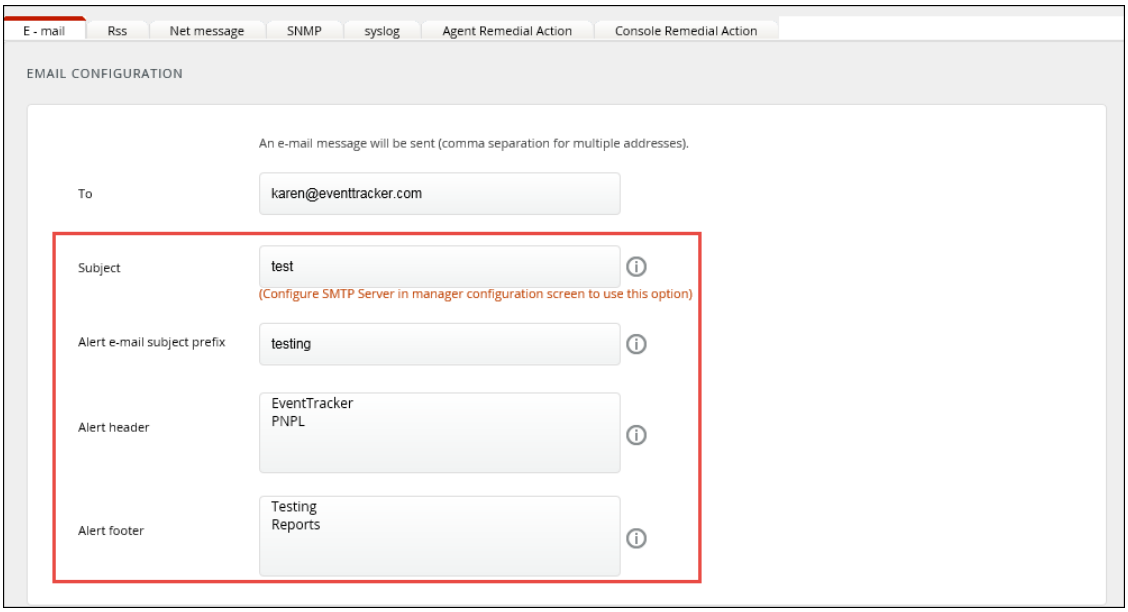

Figure 5

Alerts added for Breach Detection service

1. Critical Potential Breach :(Borderware) A new process connecting to low reputation IP address.
2. Critical Potential Breach :(Borderware) Unknown process connected to a bad reputed remote site across firewall.
3. Critical Potential Breach :(IPVOID) A new process connecting to low reputation IP address.
4. Critical Potential Breach :(IPVOID) Unknown process connected to a bad reputed remote site across firewall.
5. Critical Potential Breach :(IPVOID & Borderware) Unknown process connected to a bad reputed remote site across firewall.
6. Critical Potential Breach :(IPVOID & Borderware) A new process connecting to low reputation ip address.
7. EventTracker: Detected new bad reputation IP activity.

NOTE:

- The above mentioned alerts will get added/updated only if the user has all the existing alerts which are related to critical potential breach without any changes.
- The Breach detected service alerts are not applicable for syslog events.