

Enhancement in EventTracker Receiver to support Alert Email Header

EventTracker Enterprise

Enhancement in EventTracker Receiver to support Alert Email Header

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.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Process to be followed after applying the Update	3
Multiple Reports selection and download	3
Multiline header/footer in Alert email configuration	4
Alerts added for Breach Detection service	6

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**.

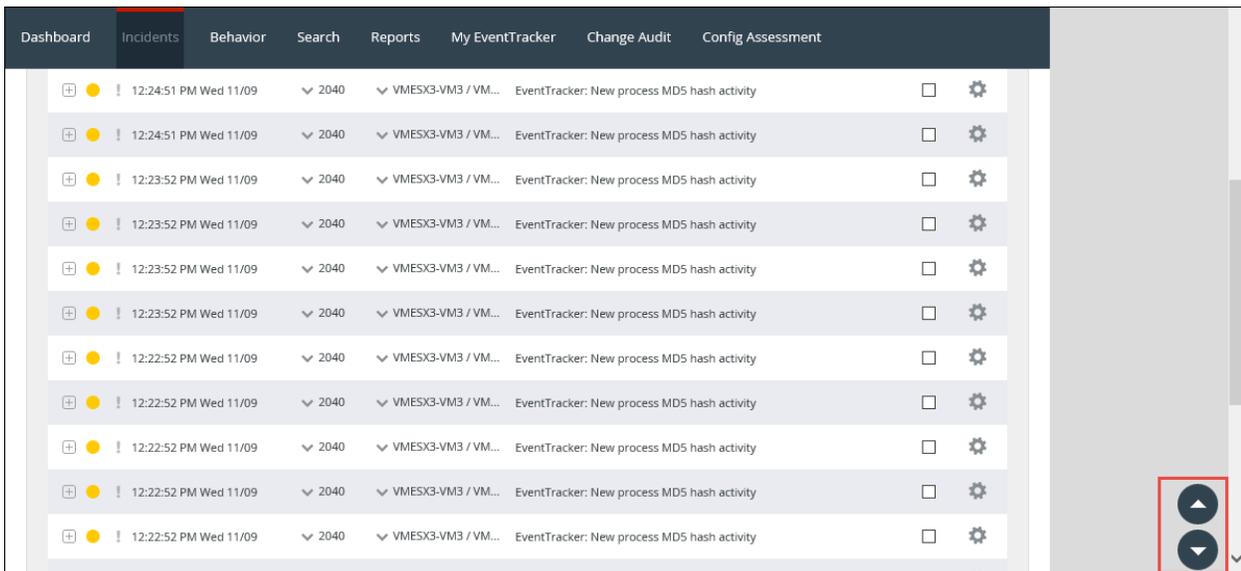


Figure 1

- 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 .

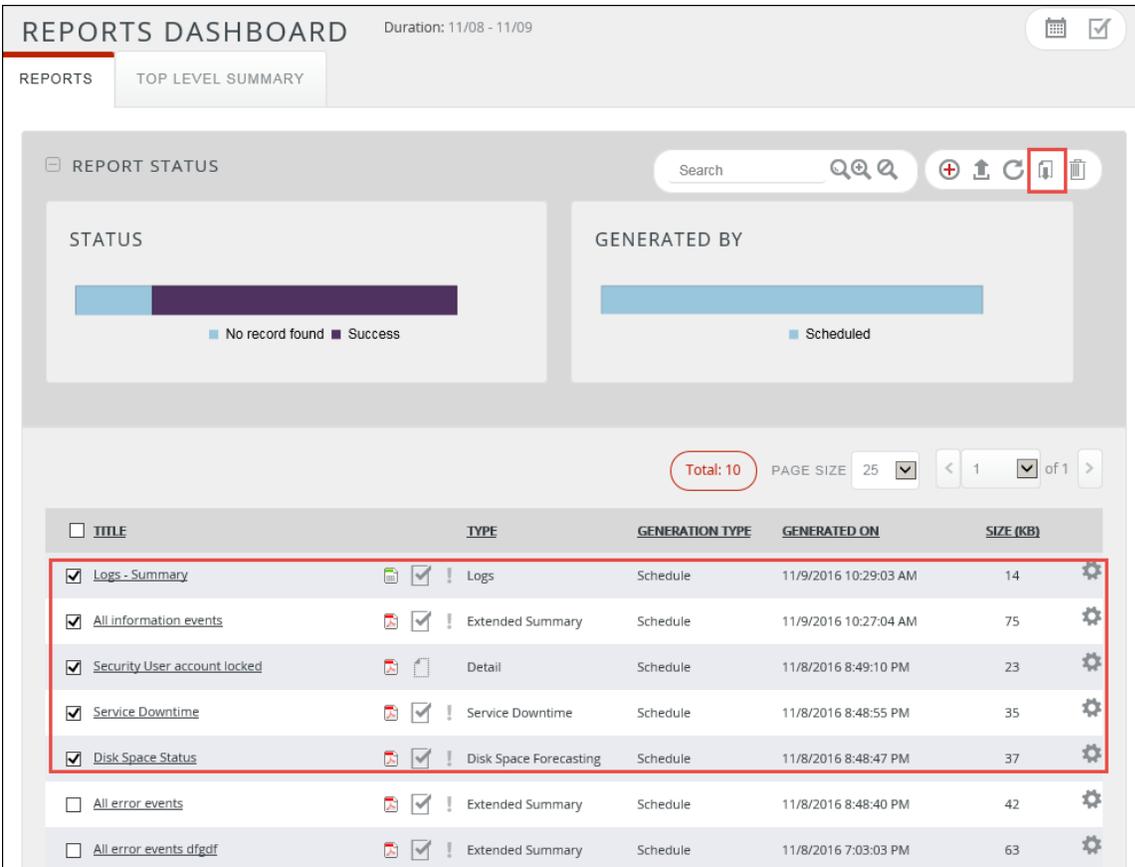


Figure 2

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

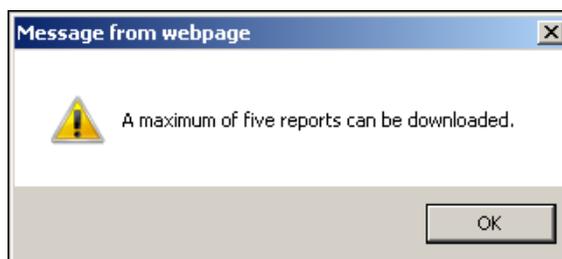


Figure 3

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.

Enhancement in EventTracker Receiver to support Alert Email Header

MANAGER CONFIGURATION

CONFIGURATION syslog / VIRTUAL COLLECTION POINT DIRECT LOG ARCHIVER AGENT SETTINGS

E-MAIL CONFIGURATION STATUSTRACKER COLLECTION MASTER PORTS NEWS

ALERT EVENTS

Enable alert notification status Enable remedial action Turn off alerts Turn off filters

Enable alert events cache for analyzing alerts Suppress duplicate alerts

Purge events from cache older than days Alert suppression interval seconds

Maximum number of alerts allowed

Enable alert e-mail header Enable alert e-mail subject prefix

Alert e-mail header Alert e-mail subject prefix

Enable alert e-mail footer

Alert e-mail footer

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.

The screenshot shows the 'EMAIL CONFIGURATION' interface. At the top, there are tabs for 'E-mail', 'Rss', 'Net message', 'SNMP', 'syslog', 'Agent Remedial Action', and 'Console Remedial Action'. Below the tabs, the 'EMAIL CONFIGURATION' section is displayed. A note states: 'An e-mail message will be sent (comma separation for multiple addresses)'. The 'To' field contains 'karen@eventtracker.com'. The 'Subject' field contains 'test' and is highlighted with a red box. Below the 'Subject' field, a red note reads: '(Configure SMTP Server in manager configuration screen to use this option)'. The 'Alert e-mail subject prefix' field contains 'testing'. The 'Alert header' field contains 'EventTracker PNPL'. The 'Alert footer' field contains 'Testing Reports'. Each field has an information icon (i) to its right.

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.