

## Handle user permission in attackers and targets dashboard

EventTracker Enterprise

Publication Date: Oct. 18, 2016

#### Update: ET82U16-029

**Abstract**: This update will help in handling the user group permission in Attacks and Targets dashboard.

#### Who should read this document?

Customers who use v8.1 Build 9 and v 8.2 Build 14.

#### Why to apply the Update ?

Google API key option provided in Manager Configuration to handle the issue of loading Attacks map. The update will also help in handling group level permission in Attacks & Targets Dashboard.

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
Frequently Asked Questions (FAQ's)	. 6



# Process to be followed after applying the Update

- Login to EventTracker web.
- Click the Admin dropdown and select Manager.

	og / VIRTUAL COLLECTIO	IN POINT DI	RECT LC	G ARCHIVER / NETFL	OW RECEIVER	AGENT SETTINGS	
AIL CONFIGURATION	STATUSTRACKER	COLLECTION M	ASTER P	ORTS NEWS			
ALERT EVENTS  ALERT EVENTS  Alenable alert notific  Alenable alert even  Purge events fror  Linable alert e-ma  Alert e-mail foote  CORRELATION RECEI	ation status II Enable remedi s cache for analyzing alerts n cache older than 7 If footer r	days	falerts [	Turn off filters Uppress duplicate Alert suppression i Maximum number Enable alert e-mail Alert e-mail subject	alerts 0 of alerts allowed subject prefix PNPLT	seconds 0 ESTING (99999-9999) USAGE DAT	<b>O</b>
Send results of all correl	ition rules to port	Collec	t cost savir	igs information		Collect u	sage data
CONFIGURATION							
Contact Ltd	http://kb.prismmicrosys.com	m/aantaat uu/		News Un	Diogog provide	nttracker.com/latest-news/ne	ws.
contact on	Disess and ide shares of	micontact-us/		EIVAS ON	Please provide	ETVAS UIL	0
ntopng Uri	Please provide htophg un.		0	ETIDS ON	Please provide	ETIDS UN	0
ETHoneynet Url	Please provide El Honeyne	et un	0	Google API Key			0
Check for knowledg	e base updates Show copyri	ight 🗹 Show help/a	bout menu	I Geolocation provider	Maximind Geo		
LOGON BANNER							
LOGON BANNER	xing D ice O Remote Indexing servic	ε		LOG SEARCH	Show graph		
LOGON BANNER	xing () ice O Remote Indexing servic	e		LOG SEARCH	☑ Show graph		SAVE O



- A new option has been provided 'Google API Key". Get the API key for loading the Google map for Attacks dashboard.
- To get the API key, click the Information icon 🛈 and it will redirect you to the Google Maps API page.
- Click the **Get a key** button.

🕅 Google Maps APIs	Home Documentation	Pricing and Plans	Q Search	≔ All Products SIGN IN	
Web > Maps JavaScript API	CE SAMPLES SUP	PORT		GET A KEY	VIEW PRICING AND PLANS
Get Started Authentication and Quota Get a Key Usage Limits Tutorials Adding a Map with a Marker Marker Clustering Importing Data into Maps Visualizing Data Mapping with Firebase Geolocation Concepts	Get a Key/Al All Google Maps JavaScr • Standard API users project of your choi • Premium Plan user authentication opti • Use an API ke purchased the or • Use your clier See the Google Map method.	uthentication ipt API applications requir : If you're using the API un ce. See more about API ke s: If you're using the API u ons: ay set up in the Google May a Premium Plan. at ID instead of an API key. os APIs Premium Plan sec	) re authentication. ader the <b>standard plan</b> , you m ays for the <b>standard API</b> . under the <b>Google Maps APIs F</b> ups APIs Premium Plan projec	ust use an <b>API key</b> set up in a <b>Premium Plan</b> you have two at created for you when you in choosing the best authentication	Contents Authentication for the standard API – API keys Get an API key Specify a key when loading the API Authentication for Google Maps APIs Premium Plan customers Using an API key Using a API key Using a API key Using a client ID Registering authorized URLs

Figure 2

- It will prompt you to enter your Google account credentials. Enter the credentials and click ٠ OK.
- Click **Get a Key** option.
- Enter the project name and click on 'Create and Enable API".

Enable Google Maps JavaScript API		×
Enter new project name EventTracker		
C	CANCEL	CREATE AND ENABLE API

Figure 3



Copy the API key to clipboard. •



Figure 4

In the Manager Configuration page, paste the API Key in the 'Google API key 'field. •

CONFIGURATION						
KB website http://kb.prismmicrosys.com		News Url	http://www.eventtracker.com/latest-news/news.			
Contact Url http://www.eventtracker.com/contact-us	i/	ETVAS Url	Please provide ETVAS url	(i)		
ntopng Url Please provide ntopng url	(j)	ETIDS Url	Please provide ETIDS url	(i)		
ETHoneynet Url Please provide ETHoneynet url	()	Google API Key	AlzaSyBZ_uuS_Ck9JpGkqXjWV9JJUyYczfhe8	(i)		
IP Reputation provider Borderware		IP Geolocation provider	MaxMind GeoLite			
Check for knowledge base updates 🗹 Show copyright 🗹 Show help/about menu						

Figure 5

• Save the changes and load the Attackers dashboard.



### Frequently Asked Questions (FAQ's)

1. For a Non-Admin user, how will be the Attackers Dashboard, after applying the update?

For non-admin users, the option 'Show only if paired with target" will be enabled by default.

2. What will happen if the non-admin user un-checks the 'Show only if paired with target" option?

The non-admin user will be able to view the IP's which are paired with other target machine, for which the user is not having permission.

3. What will happen, if a non-admin user performs a log search for an IP paired with a target machine, where the user does not have permission?

The user will not be getting any results as the user is not having permission t that machine.

