How to - Configure Barracuda Essentials to forward logs to EventTracker

EventTracker v9.0 and above

Publication Date: January 22, 2020

Abstract

This guide will facilitate a **Barracuda Essentials** user to send logs to **EventTracker.**

Scope

The configurations detailed in this guide are consistent with **EventTracker 9.x or later and Barracuda Essentials.**

Audience

Administrators who want to monitor the **Barracuda Essentials** using **EventTracker**.

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

This document is for informational purposes only. Netsurion 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 Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

Table of Contents

1. Introduction

Barracuda Essentials provides critical multi-layer security, archiving, and backup for Office 365, Microsoft Exchange, and G Suite.

The Barracuda Essentials service basically consists of:

- **Barracuda Email Security**
- **Barracuda Cloud Archiving Service**
- **Barracuda Cloud Backup**

Barracuda Essentials event is integrated with EventTracker via syslog. It helps to monitor both inbound and outbound emails against the latest spams, viruses, worms, and phishing.

Reports provide a detailed information about the email traffic allowed and email traffic blocked.

Reports provide insight into the security statistics like suspicious email such as spam links and suspicious attachments. One can analyze suspicious emails using the dashboards, we can view the top sender and recipient. Dashboards show emails with spam links, suspicious attachments along with action taken like blocked, quarantined and deferred with reason. Alerts are generated if emails have spam links, malicious attachments, and those that are getting blocked.

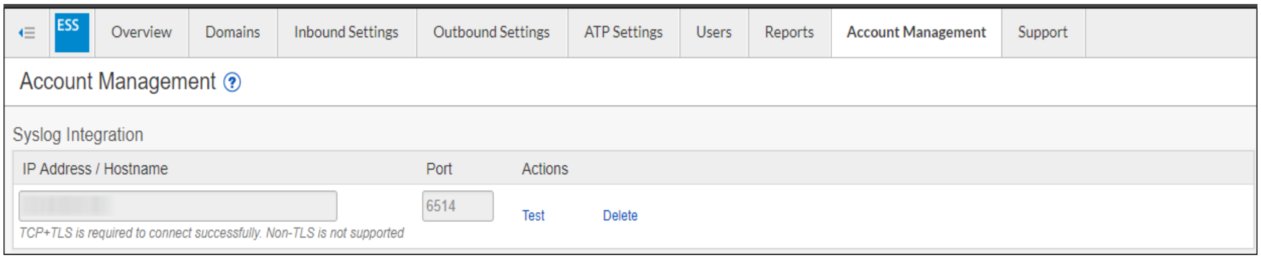
1.1 Pre-requisites

- The host machine should have installed the **EventTracker agent**.
- Administrator privilege for **Barracuda Essentials web interface**.
- Please use a new port that should support TCP+TLS certificate enabled in Eventtracker for receiving Barracuda Essentials syslog messages.
- EventTracker manager IP address and TCP+TLS certificate enabled port should be publically reachable.

Note: Please enable EventTracker bad syslog receiving to receive Barracuda Essentials syslog messages.

1.2 Integration of Barracuda Essentials events to EventTracker via syslog

1. Log into Barracuda Essentials web console (In Barracuda Cloud Control, in the left panel, click Barracuda Email Security Service) and navigate to the **Account Management** tab.



Account Management

Syslog Integration

IP Address / Hostname	Port	Actions
[redacted]	6514	Test Delete

TCP+TLS is required to connect successfully. Non-TLS is not supported

Figure 1

2. Open any firewall ports needed for communication with EventTracker.
3. Enter the **IP Address/Hostname** and **Port** for EventTracker Manager syslog port.
   - **IP Address/Hostname**: Please enter EventTracker Public IP address.
   - **Port**: Please enter the TCP+TLS certificate enabled port number.
4. Click **Test** to ensure that the Barracuda Essentials can connect with EventTracker.

Note: If the test works, your message log data begins transferring to EventTracker.