

How-To Guide

Configuring Ubiquiti Access Point to Forward Logs to EventTracker

EventTracker v9.x and above

Publication Date:

July 15, 2021

Abstract

This guide provides instructions to configure Ubiquiti UniFi controller to forward Ubiquiti access points logs via syslog.

Scope

The configuration details in this guide are consistent with EventTracker version v9.x or above and UAP/USW Firmware 3.7.x and above.

Audience

Administrators who are assigned the task to monitor Ubiquiti access points events using EventTracker.

Table of Contents

1. Overview.....	4
2. Prerequisites.....	4
3. Configuring UniFi Controller.....	4
3.1 Enabling Syslog/ Remote Logging.....	4
4. System Licensing.....	4
About Netsurion.....	5

1. Overview

Ubiquiti UniFi Access Points provide high-performance Wi-Fi. It is a scalable enterprise access point solution designed to be easily deployed and managed. Ubiquiti Access Points are well managed through Ubiquiti UniFi Controller, which is a wireless network management software solution.

EventTracker helps to monitor events from UniFi Access Point via syslog. EventTracker reports, alerts, and dashboards will help you to analyze the activity logs, such as MAC association, MAC disassociation, connection failed from unknown MAC, etc.

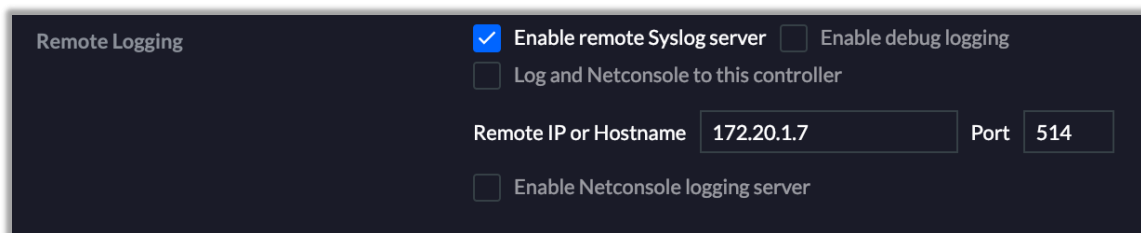
2. Prerequisites

- Admin access to UniFi Controller platform.
- EventTracker server IP address.
- EventTracker server port. E.g. 514.

3. Configuring UniFi Controller

3.1 Enabling Syslog/ Remote Logging.

1. Log in to the UniFi Controller's web interface.
2. Navigate to **Settings > Site**.
3. Navigate to the **Remote Logging** section.
4. Select the checkbox beside **Enable remote syslog server**. Leave the Enable debug logging box unchecked.
5. In the **Remote IP or Hostname**, enter the EventTracker server IP address.
6. In **Port** field, enter the syslog port for EventTracker server, e.g., 514.
7. Click **Apply** changes.



The screenshot shows the 'Remote Logging' configuration panel in the UniFi Controller. It features a dark background with white text. At the top left, the title 'Remote Logging' is displayed. To the right, there are two checkboxes: 'Enable remote Syslog server' (checked) and 'Enable debug logging' (unchecked). Below these, there is a checkbox for 'Log and Netconsole to this controller' which is unchecked. In the center, there are two input fields: 'Remote IP or Hostname' containing the value '172.20.1.7' and 'Port' containing the value '514'. At the bottom, there is a checkbox for 'Enable Netconsole logging server' which is unchecked.

4. System Licensing

Systems are created for as many access points reporting to UniFi controller. The system name format is as follow:

<AP-IP-address>-syslog. e.g., 172.16.12.113-syslog

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's [EventTracker](#) cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service.

Netsurion's [BranchSDO](#) delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations.

Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit [netsurion.com](https://www.netsurion.com) or follow us on [Twitter](#) or [LinkedIn](#). Netsurion is #19 among [MSSP Alert's 2020 Top 250 MSSPs](#).

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)

EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)

EventTracker Essentials SOC: 877-333-1433 (Option 4)

EventTracker Software Support: 877-333-1433 (Option 5)

<https://www.netsurion.com/eventtracker-support>