Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring Duo Security to Forward Logs to EventTracker

Publication Date:

October 14, 2021

Abstract

This guide helps you in configuring the **Duo Security** with the EventTracker to receive the **Duo Security** events.

Scope

The configuration details in this guide are consistent with the EventTracker version 9.3 or above and the **Duo Security.**

Audience

Administrators who are assigned the task to monitor and manage the **Duo Security** events using the **EventTracker.**

Table of Contents

1. Overview

The Duo Security verifies the identity of users and protects against breaches due to phishing and other password attacks. It comes with an easy-to-use two-factor authentication (2FA) solution that adds another layer of security to their logins.

The EventTracker helps to monitor events from the Duo Security. Its dashboard, alerts and reports will help you to monitor the Duo login activities by the client based on user, the geolocation, username, and the login attributes which helps you to find the compromised user login. EventTracker will trigger alert if any fraudulent user is trying to login. It monitors the audit activities, the user management, group management, the access management activities, the policy changes, and other changes happening on the Duo Security.

2. Prerequisites

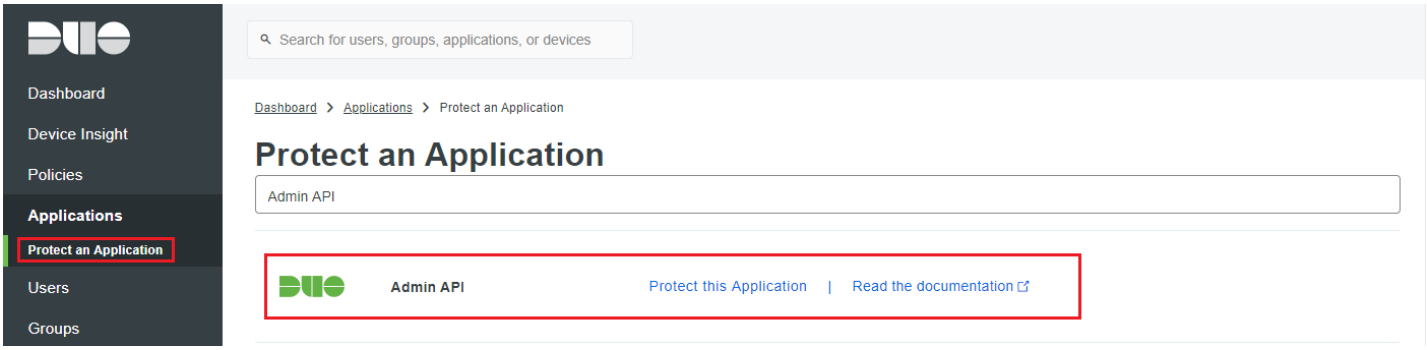
- Host machine should have installed the EventTracker Sensor.
- Administrator privilege for the Duo Security web interface.
- PowerShell 5.0 and later should be installed on the Duo integrator host machine.

3. Integrating the Duo Security events with the EventTracker

To configure the Duo Security application and generate reports, enable the Admin API.

The following steps helps you to enable the Admin API.

1. Logon to the Web interface of the Duo Security.
2. Click the **Application** tab and click the **Protect an Application** option as shown in the following image.



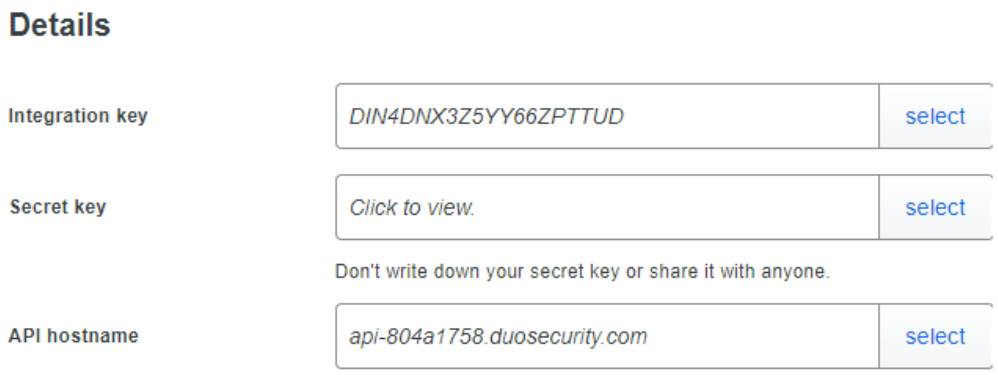
3. Click the option **Protect this Application** under the **Admin API** header.

Note: If the Admin API does not exist please contact Duo Security support for enabling the Admin API. Kindly find the mail id for contacting Duo Security Support.

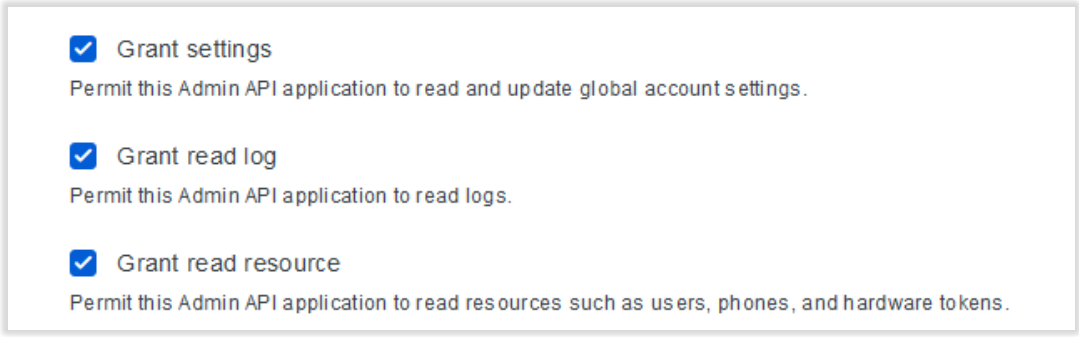
4. After completed, you will get the required credentials for integration of the Duo Security with the EventTracker.
   - Integration Key
   - Secret Key

- API hostname

5. Click **Select** to copy the keys and save them for future use.



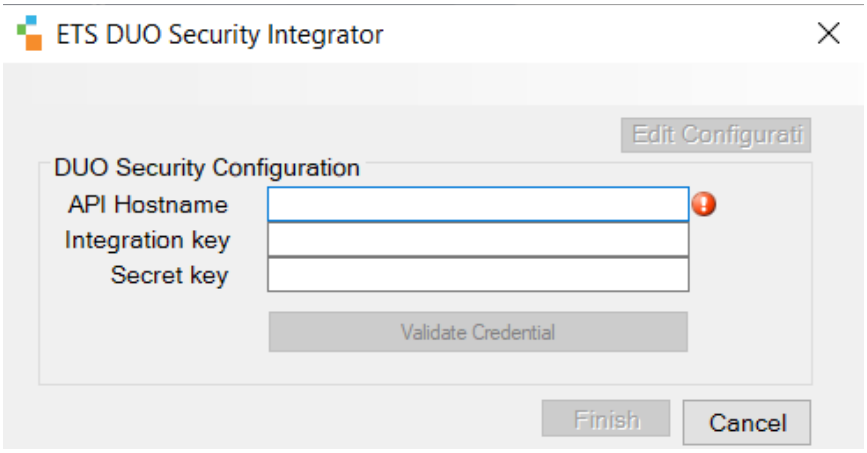
6. Select all the below permissions from the **Permissions** section and click **Save Changes**.



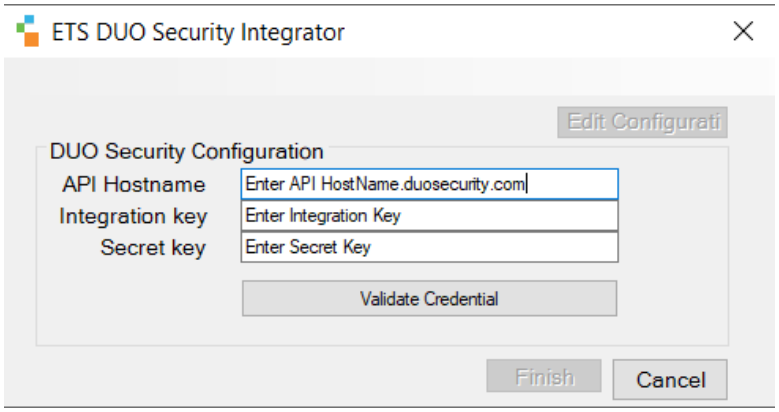
Following are the steps to integrate the Duo Security with the EventTracker.

1. Get the **Duo Security Integrator** executable file.
   https://downloads.eventtracker.com/kp-integrator/ETS_DuoSecurity_Integrator.exe

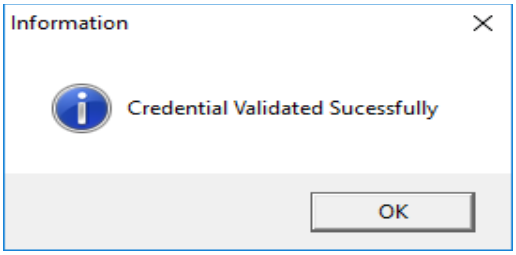
2. After the executable application is received, click the file.



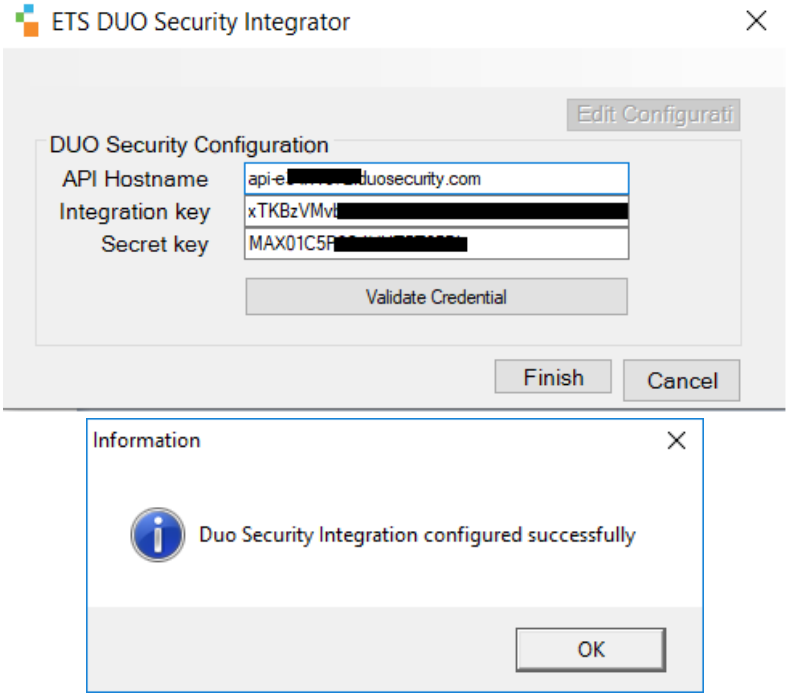
3. The **Duo Integrator** window display. Fill in the **Integration Key**, **Secret Key**, and **API HostName** as received from the web interface of the Duo Security.



4. Click the **Validate Credential** button to check if the credentials are correct and are working properly.



5. Click **OK** to close the **Validation** window and click **Finish** to complete the integration process.



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 or follow us on Twitter or LinkedIn. Netsurion is #23 among MSSP Alert's 2021 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