Netsurion®

Powering Secure and Agile Networks

How-To Guide

Configuring Symantec Endpoint Protection Cloud to Forward Logs to EventTracker

Publication Date:
October 28, 2021

Abstract

This guide helps you configure the Symantec Endpoint Protection Cloud (SEPC) with EventTracker to receive the Symantec Endpoint Protection Cloud events. In this guide, you will find the detailed procedures required for monitoring the Symantec Endpoint Protection Cloud.

Audience

Administrators who are assigned the task to monitor and manage the Symantec Endpoint Protection Cloud events using EventTracker.

Table of Contents

1. Overview

The Symantec Endpoint Protection Cloud is a cloud-based security solution tailored for small and medium-sized businesses.

The EventTracker Knowledge Pack (KP) for the Symantec Endpoint Protection Cloud provides insight into Threat Detection, Device Management, and other critical events.

2. Prerequisite

- EventTracker 9.0 and later should be installed.
- Install the integrator on the machine where the EventTracker Agent/Manager is installed.
- The users should have the administrative credentials for the Symantec Endpoint Protection Cloud console.
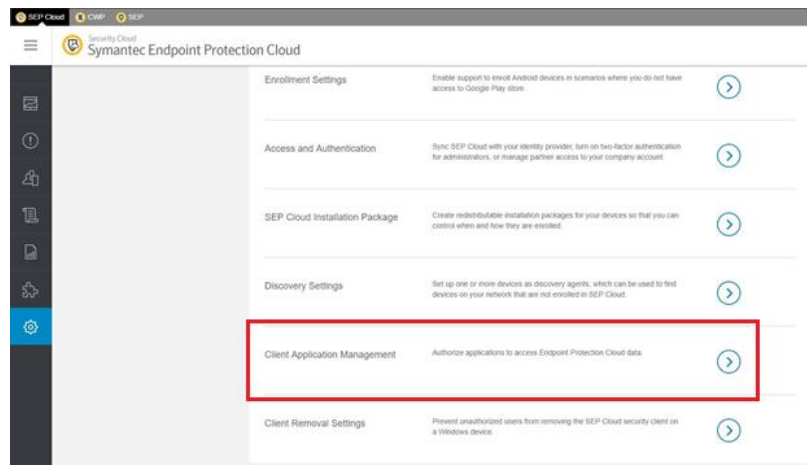
3. Obtaining Symantec Endpoint Protection Cloud Credentials

To obtain the **Symantec Endpoint Protection Cloud** API credentials, follow the steps.
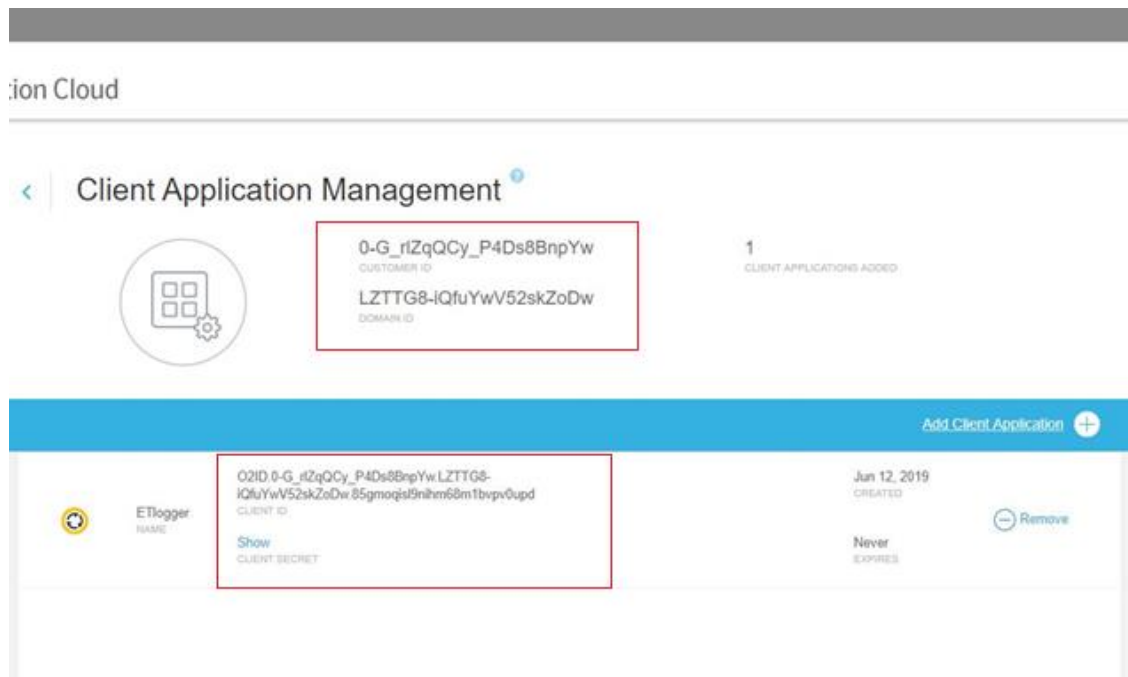
1. Go to the **Settings**.
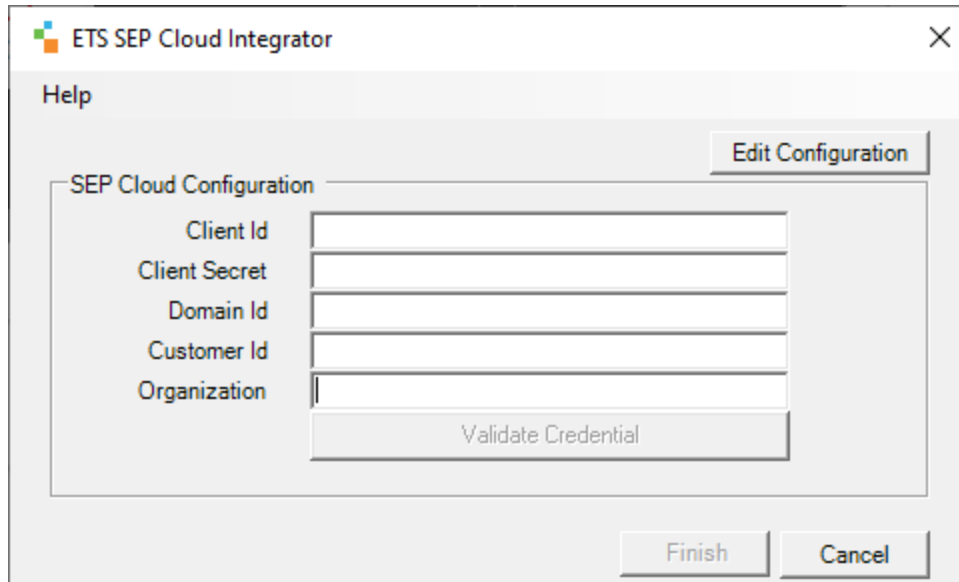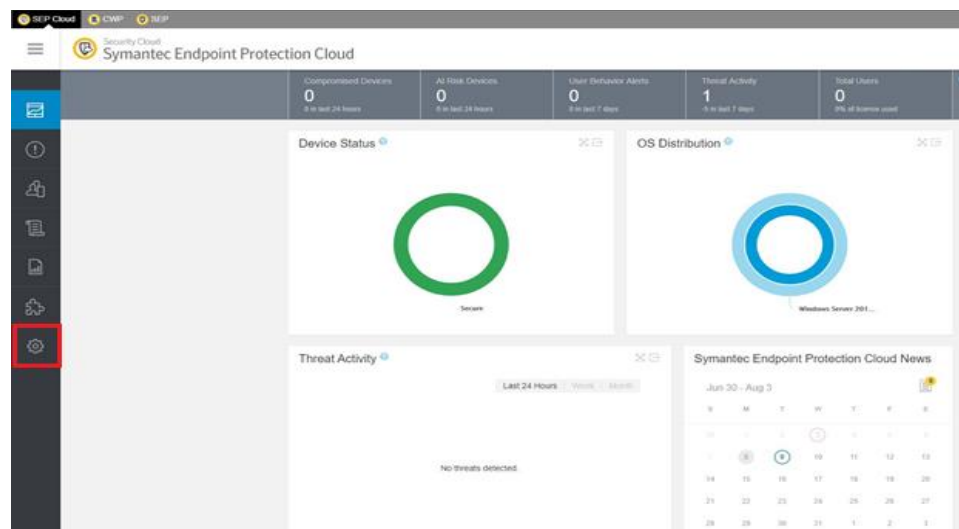

2. Select **Client Application Management**.

3. Click the **Add Client Application** and create the **API** keys.

4. Copy the **Client ID, Client Secret, Customer ID,** and the **Domain ID**.

4. Integrating Symantec Endpoint Protection Cloud to EventTracker

1. Download the Integrator for the Symantec Endpoint Protection Cloud.
2. Save the **.exe** file and run the executable file **ETS_SEP_Integrator.exe**. This will launch the **ETS SEP Cloud Integrator** window.
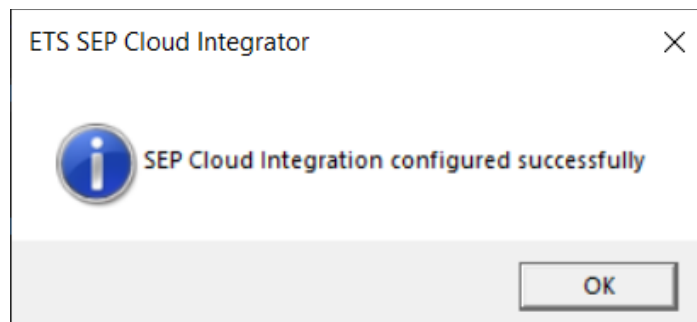3. Enter the **Details** and click the **Validate Credential** button.

It will validate the credentials the following message appears if the credentials are successfully validated and also enables the **Finish** button.
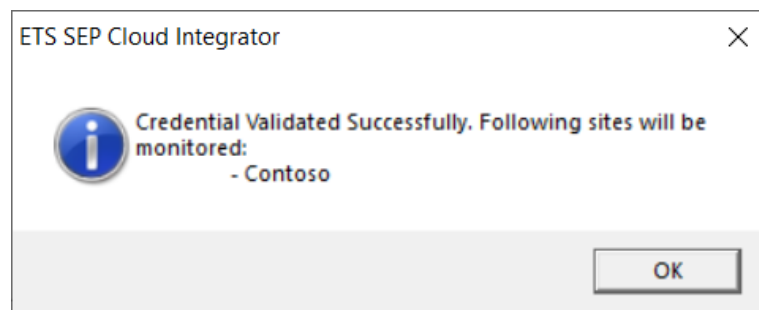
4. Click the **Finish** button to complete the integration.
   You will get a success message.

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