

# How to – Configure Symantec Endpoint Protection Cloud to forward logs to EventTracker

EventTracker v9.x and above

## Abstract

This guide helps you in configuring Symantec Endpoint Protection Cloud with EventTracker to receive 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 Symantec Endpoint Protection Cloud events 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.*

*© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

## Table of Contents

|  |   |
|--|---|
| Abstract .....   | 1 |
| Audience .....   | 1 |
| Overview.....  | 3 |
| Obtaining Symantec Endpoint Protection Cloud credential .....        | 3 |
| Integrating Symantec Endpoint Protection Cloud to EventTracker ..... | 5 |

## Overview

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

EventTracker KP for Symantec Endpoint Protection Cloud provides your insight about the Threat detection, Device Management, and other critical events.

## Obtaining Symantec Endpoint Protection Cloud credential

To obtain Symantec Endpoint Protection Cloud API credentials, follow the steps

1. Go to Settings.

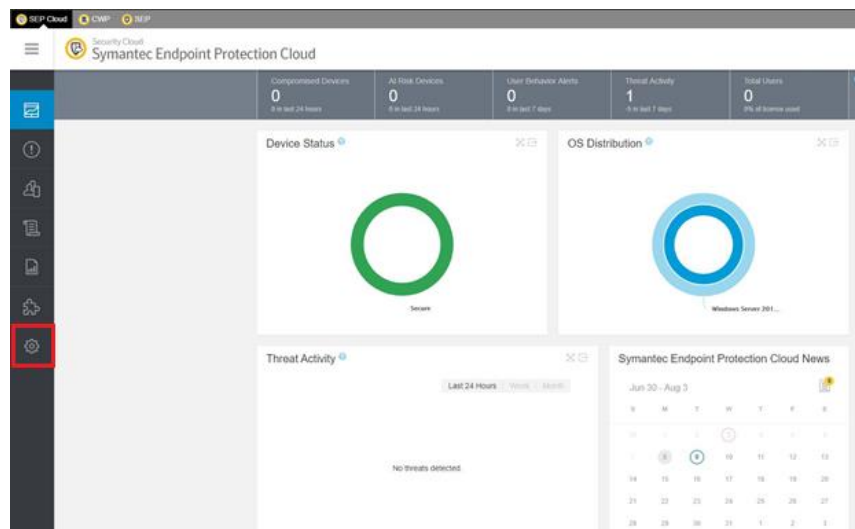


Figure 1

2. Select Client Application Management.

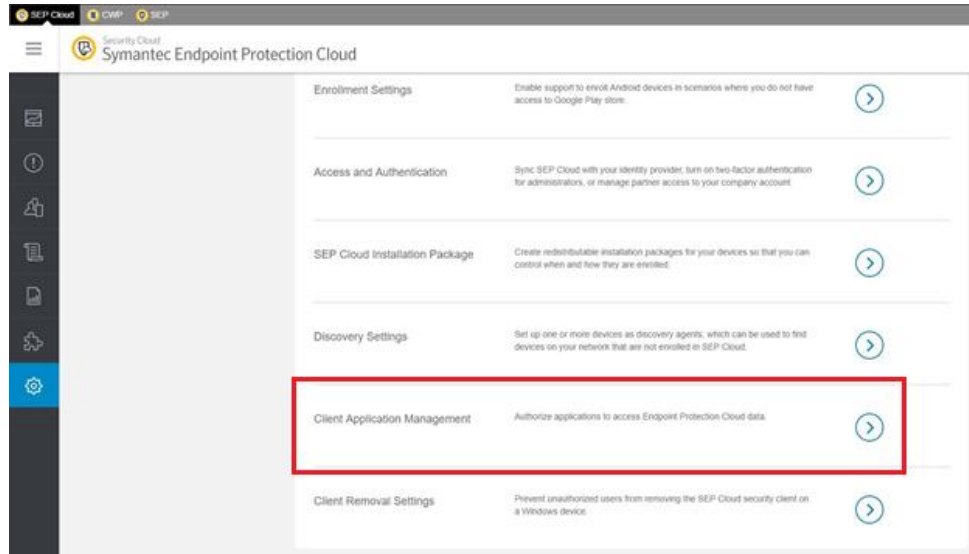


Figure 2

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

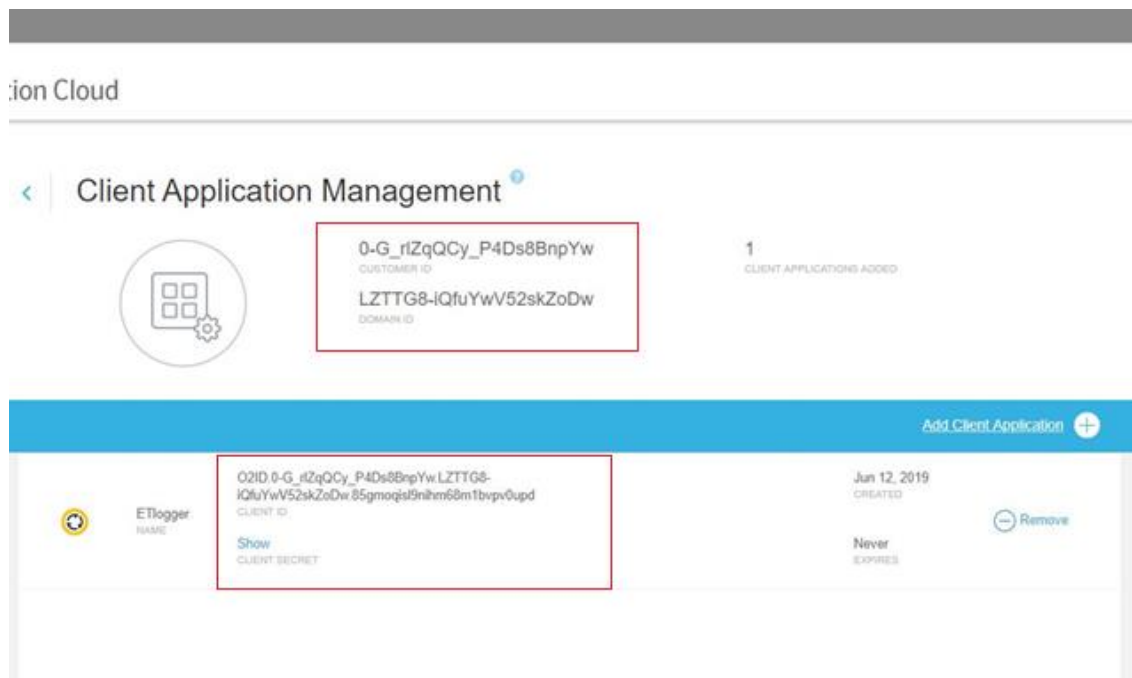


Figure 3

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

## Integrating Symantec Endpoint Protection Cloud to EventTracker

1. Download the [Integrator for Symantec Endpoint Protection Cloud](#).
2. Save .exe and run the executable file "SEPCIntegrator.exe".
3. This will launch the following window.

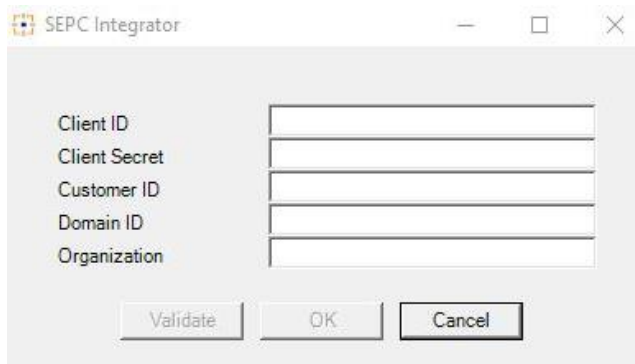


Figure 4

4. Enter the Details and click on validate, this will validate the keys and provide the below message if the credentials are successfully validated.



Figure 5

5. You will get a pop up suggesting the successful integration.

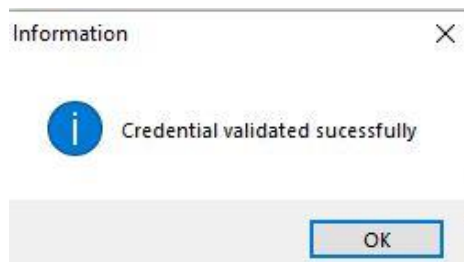


Figure 6