

How-To Guide

Configuring Cisco® Secure Endpoint to Forward Logs to EventTracker

Publication Date:

May 17, 2022

Abstract

This guide provides instructions to retrieve the **Cisco® Secure Endpoint** events via remote syslog. Once the logs start coming into EventTracker, then reports, dashboards, alerts, and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and **Cisco® Secure Endpoint**.

Audience

Administrators who are assigned the task to monitor the **Cisco® Secure Endpoint** events using EventTracker.

Table of Contents

Table of Contents3

1. Overview4

2. Prerequisites.....4

3. Integration of Cisco® Secure Endpoint events to EventTracker.....4

About Netsurion8

Contact Us.....8

1. Overview

Cisco® Secure Endpoint (formerly AMP for Endpoints) integrates prevention, detection, threat hunting, and response capabilities in a single solution, leveraging the power of cloud-based analytics. Secure Endpoint will protect your Windows, Mac, Linux, Android, and iOS devices through public or private cloud deployment.

EventTracker helps to monitor events from Cisco® Secure Endpoint. Its knowledge objects and flex reports will help you to analyse scanning details, threat detection and quarantine details, vulnerable application details, as well as suspicious and system activities.

2. Prerequisites

- **EventTracker v9.x or above** should be installed.
- A user with global administrator access of Cisco® Secure Endpoint.
- Administrative access on EventTracker.

3. Integration of Cisco® Secure Endpoint events to EventTracker

To configure the Cisco® Secure Endpoint integration.

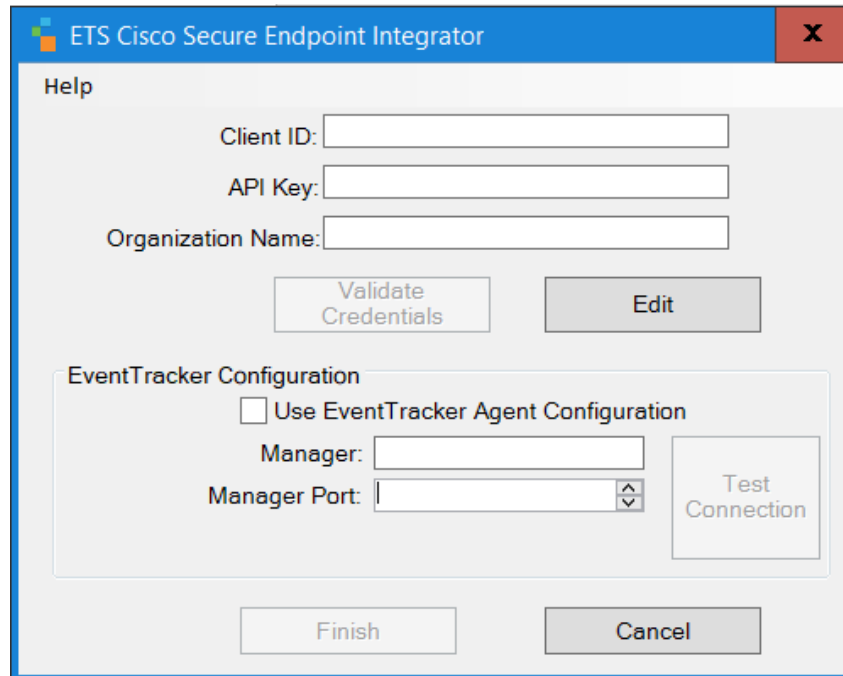
Generating Client ID and API Key:

1. Log into <https://console.amp.cisco.com/> (N.A.) or <https://console.eu.amp.cisco.com/> (E.U.)
2. Go to the **Business Page** from the **Accounts** dropdown menu.
3. Click the **Edit** button.
4. Under features, click the **Regenerate** button beside **3rd Party API Access** to generate the **Client ID** and **secure API Key**
5. Once you have the **API client ID** and **API key**, you can get the logs as follows:



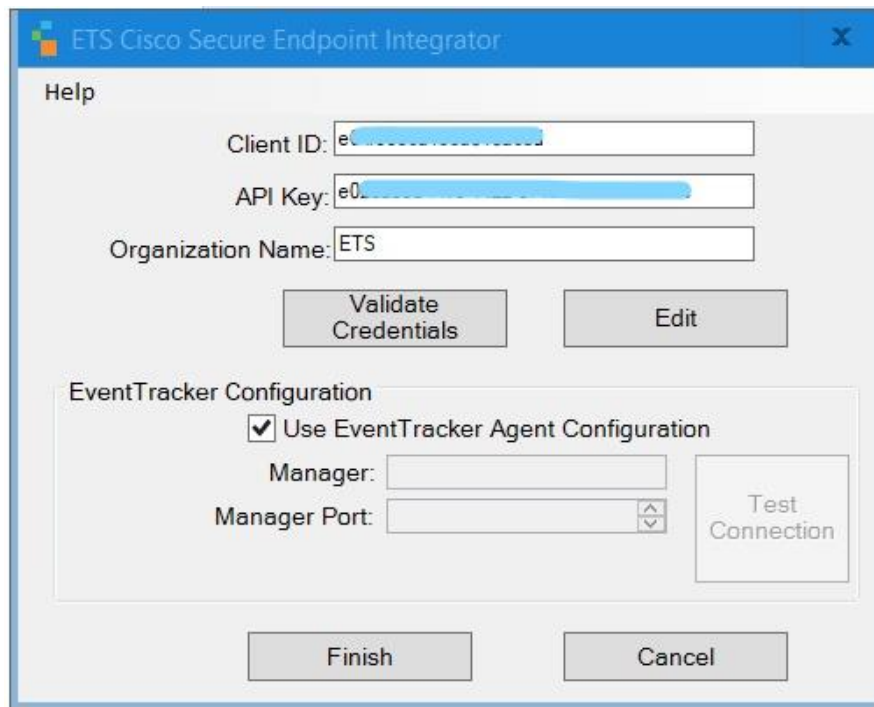
Following are the steps to integrate Cisco Secure Endpoint into EventTracker.

1. Get the **Cisco® Secure Endpoint** executable file:
https://downloads.eventtracker.com/kp-integrator/ETS_Cisco_Secure_Endpoint_Integrator.exe
2. Once the executable application is received, click the file **ETS_Cisco Secure Endpoint_Configure**.



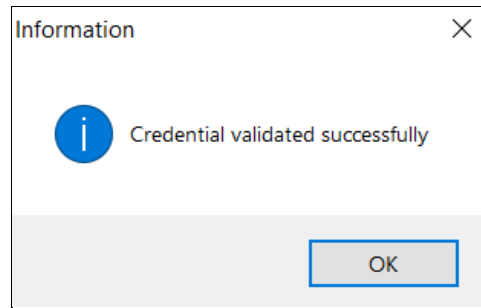
The image shows the 'ETS Cisco Secure Endpoint Integrator' window. It has a blue title bar with a close button. Below the title bar is a 'Help' link. The main area contains three text input fields: 'Client ID:', 'API Key:', and 'Organization Name:'. Below these fields are two buttons: 'Validate Credentials' and 'Edit'. Below these buttons is a section titled 'EventTracker Configuration'. Inside this section, there is a checkbox labeled 'Use EventTracker Agent Configuration'. Below the checkbox are two more text input fields: 'Manager:' and 'Manager Port:'. To the right of these fields is a button labeled 'Test Connection'. At the bottom of the window are two buttons: 'Finish' and 'Cancel'.

3. **Cisco® Secure Endpoint Integrator** window is displayed. Fill in the **Client ID**, and **API Key** as received from the web interface of Cisco® Secure Endpoint, and provide the **Organization Name**.

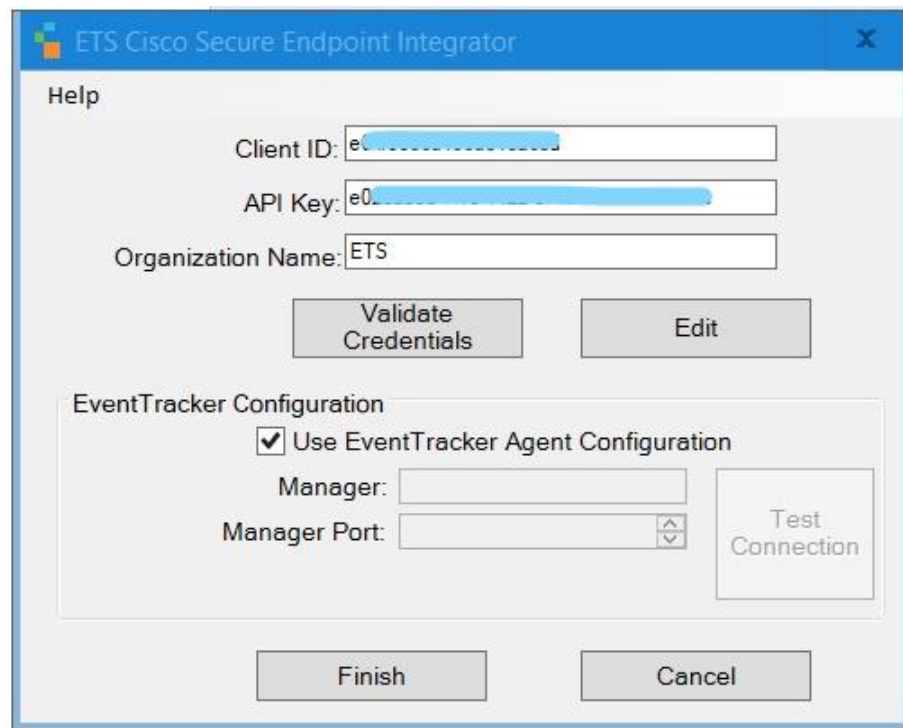


The image shows the 'ETS Cisco Secure Endpoint Integrator' window with the following fields filled out: 'Client ID:' contains 'e0...', 'API Key:' contains 'e0...', and 'Organization Name:' contains 'ETS'. The 'EventTracker Configuration' section has the checkbox 'Use EventTracker Agent Configuration' checked. The 'Manager:' and 'Manager Port:' fields are empty. The 'Test Connection' button is visible. The 'Finish' and 'Cancel' buttons are at the bottom.

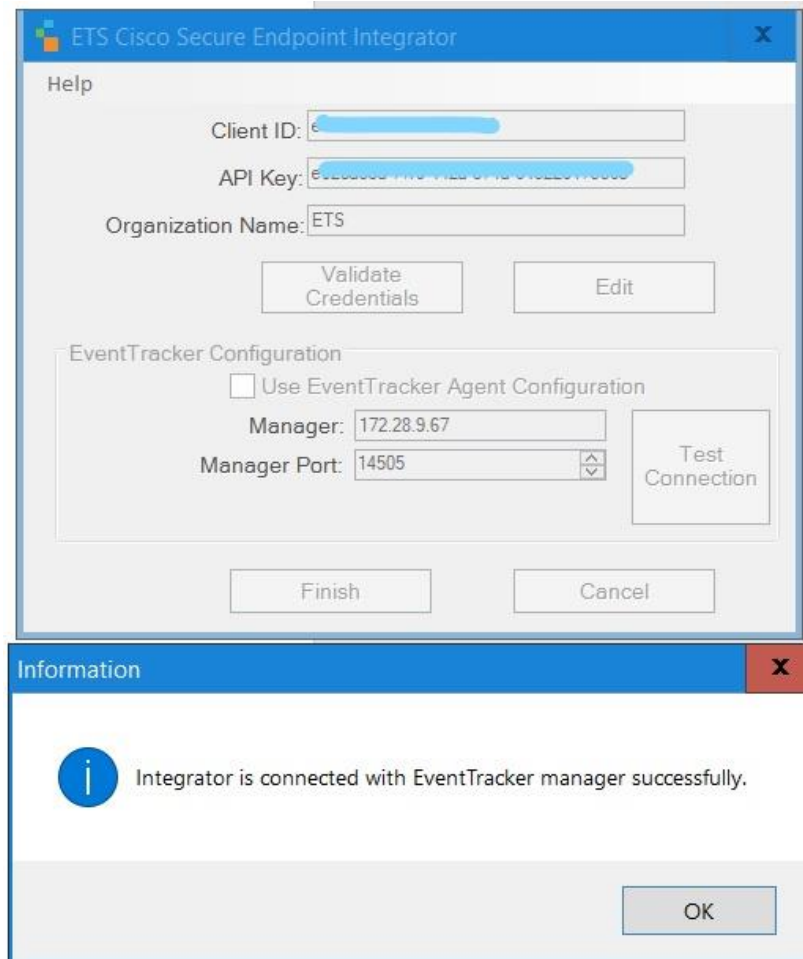
4. Once you have filled out the fields, click the **Validate** button to check if the credentials are correct and working properly.



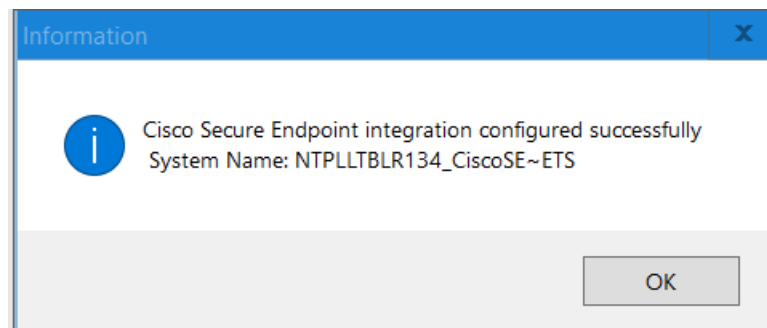
5. If the **Agent** is installed on the server where the program is launching, the **EventTracker Agent Configuration** check box is enabled to use the Agent machine **etaconfig.ini** file manager details to send the logs.



6. If the user wants to send the logs to specific EventTracker, then the user needs to mention EventTracker **Manager IP** and **Manager Port** to send the logs and click **Test Connection** to check the connectivity.



7. Once everything verified, click the **Finish** button to complete the Integration.



8. Run **ETS_Cisco Secure Endpoint_LogForwarder** exe to get the logs into EventTracker.

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>