Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring Thycotic Secret Server to Forward Logs to EventTracker

EventTracker v9.x and above

Publication Date:

May 24, 2021

Abstract

This guide provides instructions to configure/ retrieve Thycotic Secret Server logs via syslog.

Scope

The configuration details in this guide are consistent with EventTracker version v 9.x or above and Thycotic Secret Server (Cloud and On-Prem) version 10.9.

Audience

Administrators who are assigned the task to monitor Thycotic Secret Server events using EventTracker.

Table of Contents

Table of Contents 3
1. Overview 4
2. Prerequisites 4
3. Configuring Thycotic SS 4
   3.1 On Premise 4
   3.2 Cloud 5
4. Configuring EventTracker server to accept logs from Thycotic Secret Server 6
5. System Licensing 6
   About Netsurion 7

1. Overview

Thycotic Secret Server (SS) is an enterprise-grade, privileged access management solution that is quickly deployable and easily managed. With Thycotic SS, user can automatically discover and manage their privileged accounts through an intuitive interface, protecting against malicious activity, across the enterprise.

EventTracker helps to monitor events from Thycotic SS. EventTracker reports, alerts, and dashboards will help you to analyze the activity logs such as, user management, secret view/delete, heartbeat failure, etc.

2. Prerequisites

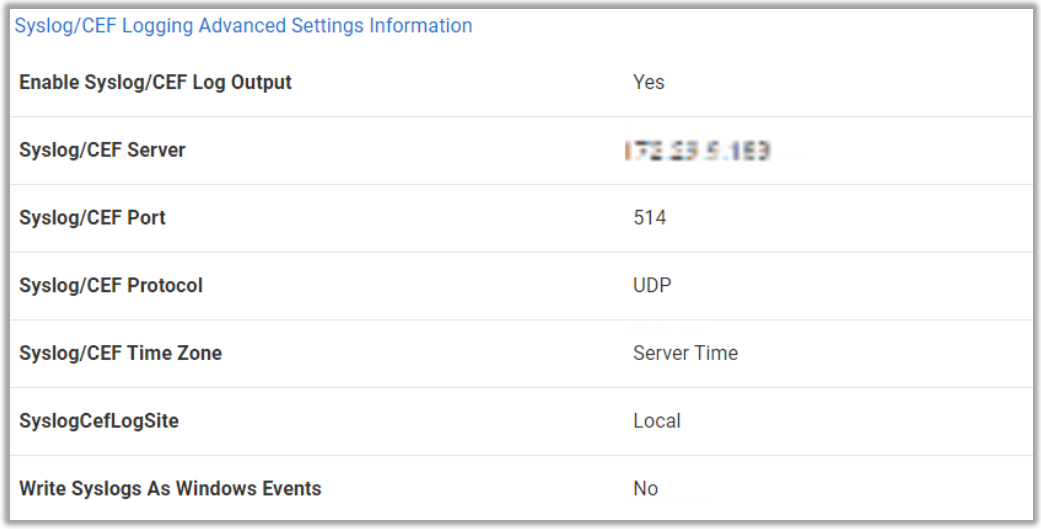
- Admin access to Thycotic Secret Server platform.
- EventTracker server IP address. (If Thycotic SS is cloud, the public IP is required.)
- EventTracker server port. E.g. 514 or 6514.
- Enable TLS on EventTracker Manager in case of syslog **TCP** connection.

3. Configuring Thycotic SS

3.1 On Premise

The steps provided below will help to configure Thycotic SS (On-prem) via syslog to help forward logs to EventTracker servers.

1. Login to your Thycotic SS platform.
2. Navigate to **Administration > Configuration**.
3. Select the **General** tab and click the **Edit** button.
4. Check the **Enable Syslog/CEF Logging** check box. Three additional textboxes or lists appear:
    a. **Syslog/CEF Server**: IP address or name of the EventTracker server.
    b. **Syslog/CEF Port**: Server port for sent events. E.g., 514.
    c. **Syslog/CEF Protocol**: Select UDP.
    d. **Syslog/CEF Time Zone: UTC Time** or **Server Time**, depending on your preference.
5. Complete or configure those controls.
6. Click **Save**.



Syslog/CEF Logging Advanced Settings Information	
Enable Syslog/CEF Log Output	Yes
Syslog/CEF Server	[redacted]
Syslog/CEF Port	514
Syslog/CEF Protocol	UDP
Syslog/CEF Time Zone	Server Time
SyslogCefLogSite	Local
Write Syslogs As Windows Events	No

3.2 Cloud

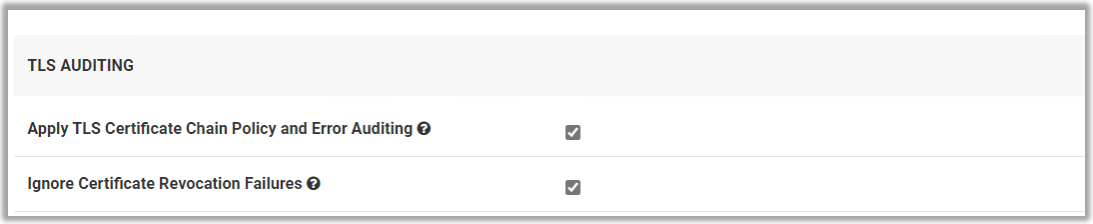
The steps provided below will help to configure Thycotic SS (On-prem) via syslog to help forward logs to EventTracker servers.

1. Login to your Thycotic SS platform.
2. Navigate to **Administration > Configuration**.
3. Select the **General** tab and click on the **Edit** button.
4. Check the **Enable Syslog/CEF Logging** check box. Three additional textboxes or lists appear:
    a. **Syslog/CEF Server**: IP address or name of the server. (Public IP address of syslog server)
    b. **Syslog/CEF Port**: Server port for sent events. E.g., 6514.
    c. **Syslog/CEF Protocol**: Either UDP or TCP.
    d. **Syslog/CEF Time Zone: UTC Time** or **Server Time**, depending on your preference.
5. Complete or configure those controls.
6. Click **Save.**

If **Secure TCP** is selected as protocol, perform below steps:

Note: Follow the below steps if you desire to encrypt the traffic. This also requires enabling the TLS in EventTracker manager as well.

1. Navigate to **Administration > Configuration**.
2. Select the **Security** tab and click the **Edit** button.
3. Go to **TLS Auditing** section and enable the option **Apply TLS Certificate Chain Policy and Error Auditing**.
4. Page will reload and display additional option to be configured.
5. Enable the checkbox for **Ignore Certificate Revocation Failures**.



4. Configuring EventTracker server to accept logs from Thycotic Secret Server

1. Login to your EventTracker server and connect with the SQL server management studio.
2. Import and Run the **Enable_logging.sql** from the Integration package.

5. System Licensing

For On-Prem, a single system will get created by the format of <HostName~syslog>.

For Cloud-based solution, multiple system with format <IPAddress~syslog> may get created.

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 #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
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