How to - Guide

How to – Configure McAfee ePolicy Orchestrator to forward logs to EventTracker

EventTracker v9.2 and later

Author: SI Team

June 1, 2021

Abstract

This guide provides instructions to configure McAfee ePolicy Orchestrator to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor McAfee ePolicy Orchestrator.

Scope

The configuration details in this guide are consistent with EventTracker version v8.x or above and McAfee ePolicy Orchestrator.

Audience

Administrators who are assigned the task to monitor McAfee ePolicy Orchestrator events using EventTracker.

Table of Contents

1. Overview

The McAfee ePolicy Orchestrator (McAfee ePO) platform enables centralized policy management and enforcement for your endpoints and enterprise security products.

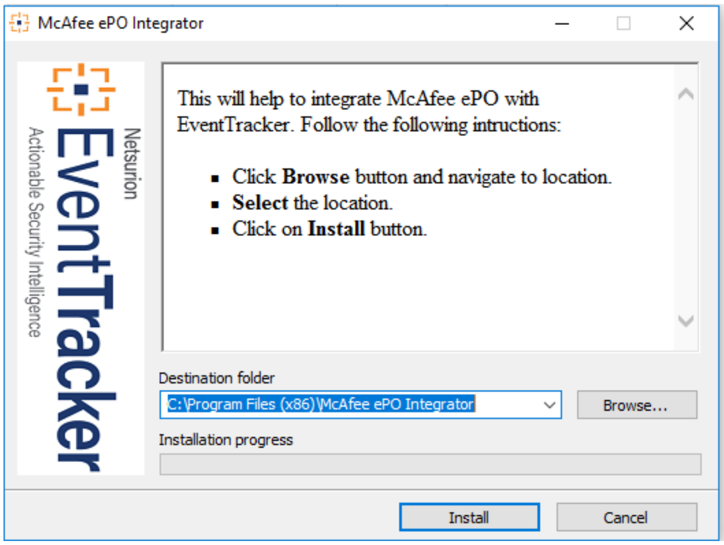
EventTracker helps to monitor events from McAfee ePolicy Orchestrator. Its knowledge object and flex reports help you to analyze critical activities (e.g., Threat Management) and to monitor login/logoff events.

2. Prerequisites

- EventTracker agent should be installed in McAfee ePO Server.
- PowerShell 5.0 and above should be installed on McAfee ePO server.
- User should have **global administrative privilege** on McAfee ePO server.

3. Configuring McAfee ePolicy Orchestrator to forward logs to EventTracker

1. Contact EventTracker support for McAfee ePO Integrator.
2. Download and run executable file **McAfeeePOIntegrator.exe**.

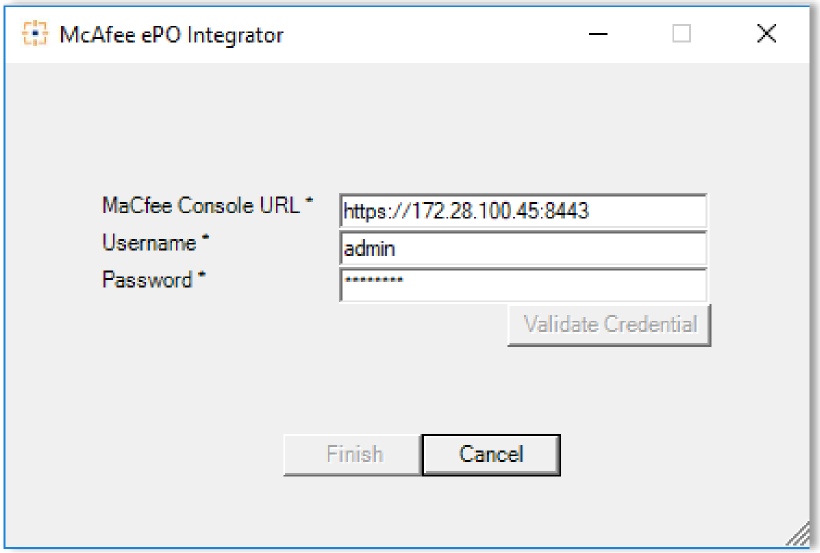


This will help to integrate McAfee ePO with EventTracker. Follow the following intructions:

- Click **Browse** button and navigate to location.
- **Select** the location.
- Click on **Install** button.

Destination folder: C:\Program Files (x86)\McAfee ePO Integrator

3. Select the path to install Integrator and then click **Install** to proceed.
4. Enter McAfee console URL, **global admin** username and password.



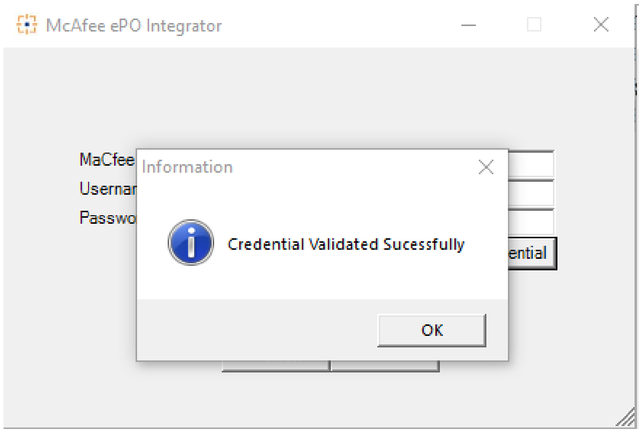
McAfee ePO Integrator

MaCfee Console URL * https://172.28.100.45:8443

Username * admin

Password * ********

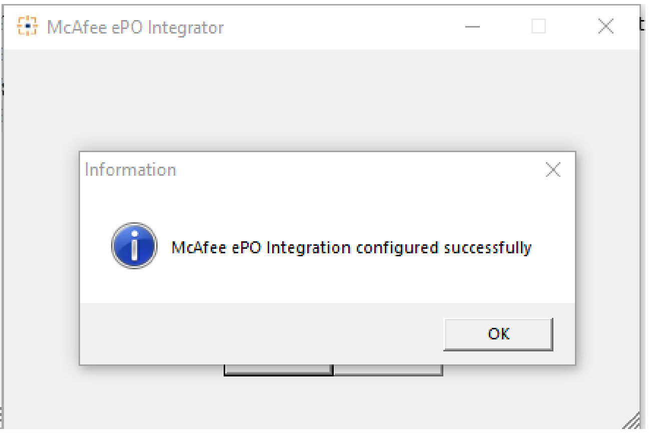
5. Click **Validate Credential** to confirm if the entered credentials are correct.
6. Click **Finish** to complete the process.



McAfee ePO Integrator

Information

Credential Validated Sucessfully



McAfee ePO Integrator

Information

McAfee ePO Integration configured successfully

Note: MacAfee ePO integration user should have **global admin privileges**. So, that it will work without any issues.

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

713-929-0200

https://www.netsurion.com/company/contact-us