How-To Guide

Configuring Jamf Protect to Forward Logs with EventTracker

EventTracker v9.2x and above

Publication Date:

December 8, 2021

Abstract

This guide provides instructions to configure the **Jamf Protect API** to send its logs to EventTracker.

Scope

The configuration details in this guide are consistent with the EventTracker version v9.2x or above and Jamf Protect.

Audience

The Administrators who are assigned the task to monitor the Jamf Protect events using EventTracker.

Table of Contents

1. Overview

Jamf Protect is advanced software that protects Apple's macOS software. It is used to maintain endpoint compliance, anti-virus, and malware protection and focuses on remediating Mac-specific threats. Jamf Protect is integrated with EventTracker to send logs using the Jamf Protect API.

EventTracker provides insights about the Jamf Protect alerts and device activities. EventTracker reports Jamf Protect alerts and device activities which provide a detailed summary for various events like the USB devices insertions, prompts regarding user credentials before the process execute, etc.

EventTracker Alerts notify crucial events like suspicious activities, privilege escalation, defense evasion, and others.

2. Prerequisites

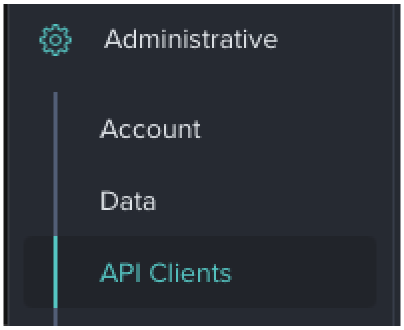
- **Admin** access to the **Jamf Protect** console.
- Windows PowerShell v5.0 and above should be installed**.**
- **EventTracker** Manager/Sensor should be installed and running.

3. Configuring Jamf Protect Logging

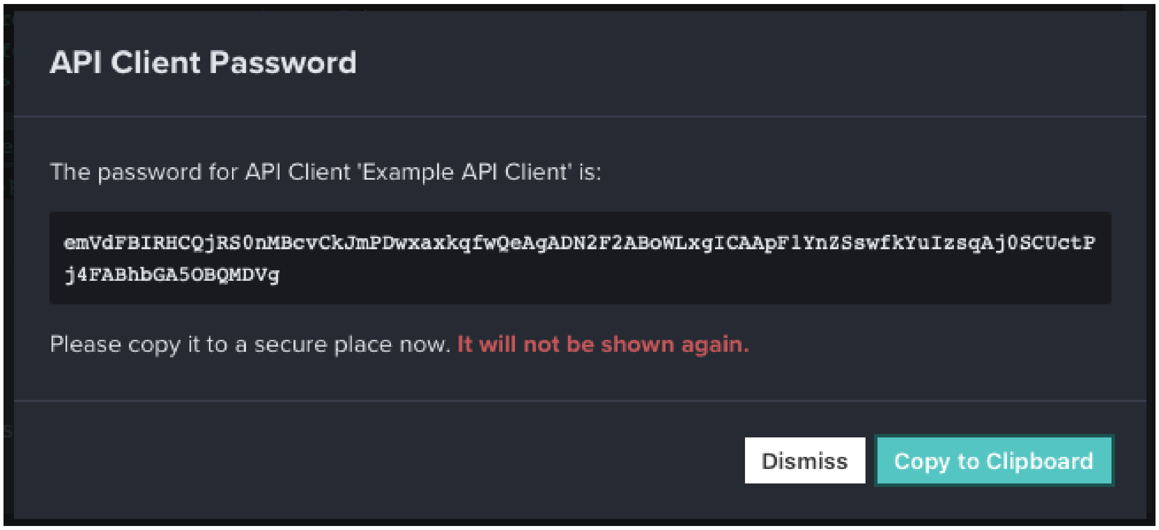
Refer to the following steps to configure the Jamf Protect API to send the logs to EventTracker.

3.1 Configuring Jamf Protect API

1. Login to the Jamf Protect console.
2. In the Jamf Protect, click **Administrative** > **API Clients.**



3. Click **Create API Client**.
4. Enter a name for your API client.
5. Copy the API client password for later use.

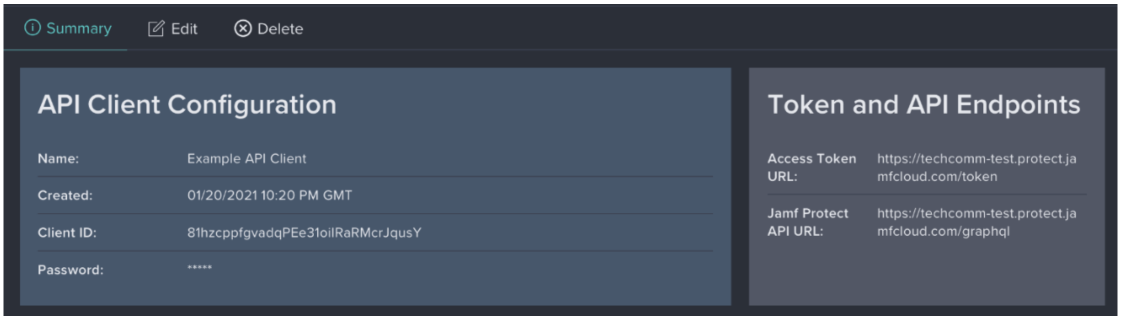


The password for API Client 'Example API Client' is:

```
emVdFBIRHCQjRS0nMBcvCkJmPDwxaxkqfwQeAgADN2F2ABoWLxgICAApFlYnZSswfkYuIzsqAj0SCUctP
j4FABhbGA5OBQMDVg
```

Please copy it to a secure place now. It will not be shown again.

Your API client configuration and endpoint information are displayed.



API Client Configuration

Name:	Example API Client
Created:	01/20/2021 10:20 PM GMT
Client ID:	81hzcppfgvadqPEe31oilRaRMcrJqusY
Password:	*****

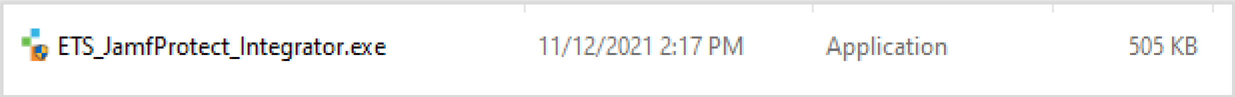
Token and API Endpoints

Access Token URL:	https://techcomm-test.protect.jamfcloud.com/token
Jamf Protect API URL:	https://techcomm-test.protect.jamfcloud.com/graphql

Note: Please capture the Client ID, Client Password, and tenant details for future use.

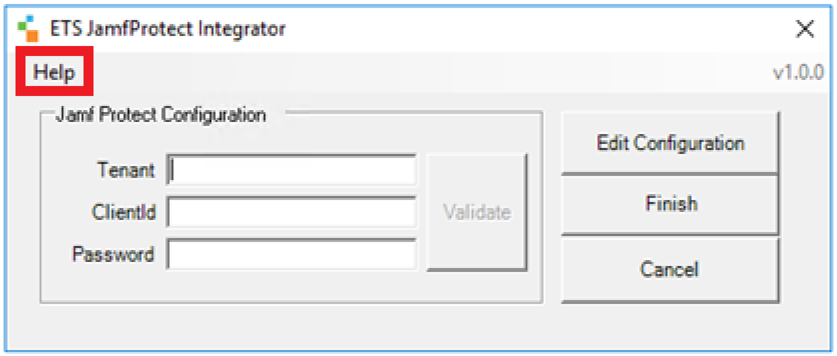
3.2 Configuring Jamf Protect Integrator

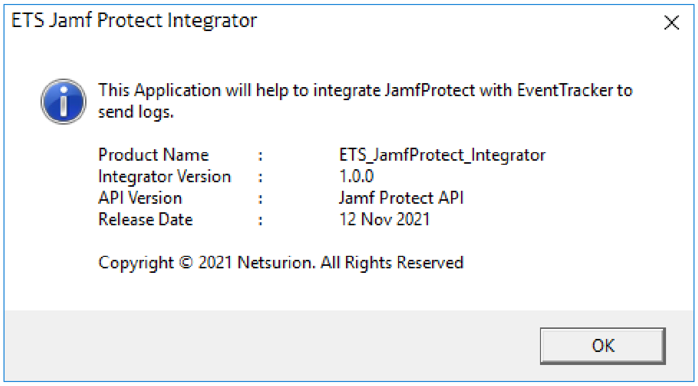
1. Please click here to download the Jamf Protect integrator files.
2. Run the **ETS_Jamf Protect_integrator.exe** file.



ETS_JamfProtect_Integrator.exe	11/12/2021 2:17 PM	Application	505 KB

3. Click **Help** >> **About** for checking the updated integrator version details.



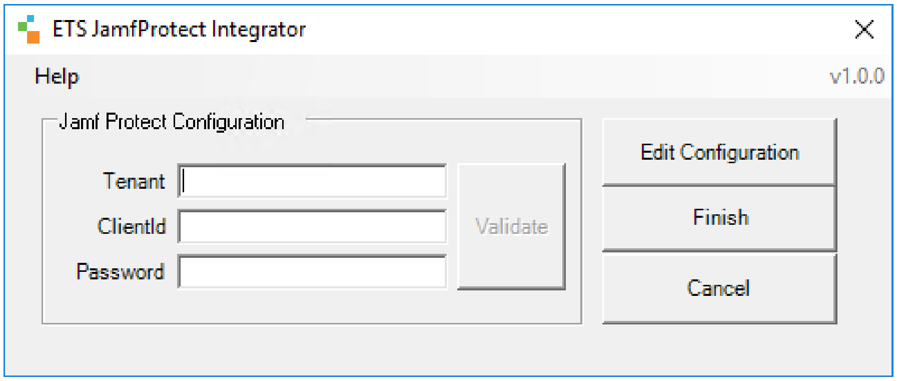

ETS Jamf Protect Integrator

This Application will help to integrate JamfProtect with EventTracker to send logs.

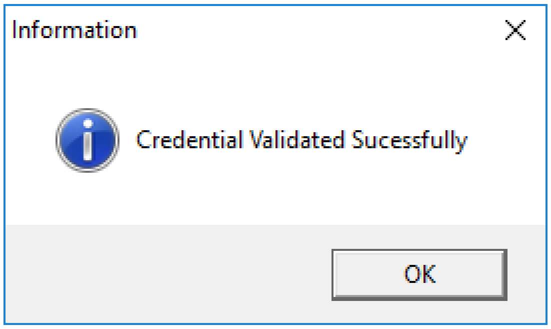
Product Name	:	ETS_JamfProtect_Integrator
Integrator Version	:	1.0.0
API Version	:	Jamf Protect API
Release Date	:	12 Nov 2021

Copyright © 2021 Netsurion. All Rights Reserved

4. Enter the necessary details into the Jamf Integrator and click **Validate**.

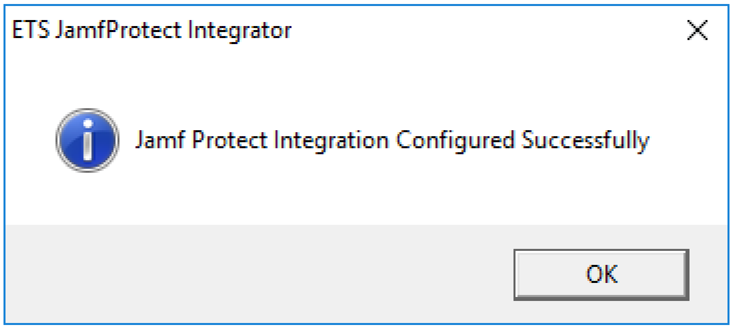


5. After credentials are validated successfully. Click **OK**.


Information

Credential Validated Sucessfully

6. Click the **Finish** button to integrate.
7. EventTracker displays a **Jamf Protect integration configured** success message. Click OK.



Jamf Protect Integration Configured Successfully

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, end 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