

Integration Guide

Integrating Jamf Protect 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

Τa	able of	f Contents	3							
1.	Ove	Overview4								
2.	Pre	Prerequisites4								
3.	Cor	nfiguring Jamf Protect Logging	4							
	3.1	Configuring Jamf Protect API	4							
	3.2	Configuring Jamf Protect Integrator	5							
4.	Eve	entTracker Knowledge Packs	7							
	4.1	Categories	7							
	4.2	Alerts	7							
	4.3	Reports	7							
	4.4	Dashboards	9							
5.	Imp	porting Jamf Protect Knowledge Pack into EventTracker	12							
	5.1	Categories	12							
	5.2	Alerts	13							
	5.3	Reports	14							
	5.4	Knowledge Objects	16							
	5.5	Dashboards	17							
6.	Ver	rifying Jamf Protect Knowledge Pack in EventTracker								
	6.1	Categories								
	6.2	Alerts								
	6.3	Knowledge Objects	19							
	6.4	Reports	19							
	6.5	Dashboards	20							
	Abou	It Netsurion	22							

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.



API Client Password
The password for API Client 'Example API Client' is:
emVdFBIRHCQjRS0nMBcvCkJmPDwxaxkqfwQeAgADN2F2ABoWLxgICAApF1YnZSswfkYuIzsqAj0SCUctP j4FABhbGA50BQMDVg
Please copy it to a secure place now. It will not be shown again.
Dismiss Copy to Clipboard

Your API client configuration and endpoint information are displayed.

(i) Summary	🗹 Edit 🛛 🛞 Delete		
API Clie	nt Configuration	Token a	nd API Endpoints
Name:	Example API Client	Access Token URL:	https://techcomm-test.protect.ja mfcloud.com/token
Created:	01/20/2021 10:20 PM GMT	lamf Brotoct	https://tachcomm.tact.protoct.ia
Client ID:	81hzcppfgvadqPEe31oilRaRMcrJqusY	API URL:	mfcloud.com/graphql
Password:			

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

3.2 Configuring Jamf Protect Integrator

- 1. Please <u>click here</u> to download the Jamf Protect integrator files.
- 2. Run the ETS_Jamf Protect_integrator.exe file.

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

3. Click **Help** >> **About** to check the updated integrator version details.



肯 ETS JamfPi	rotect Integrator				×	
Help					v1.0.0	
Jamf Prote	ct Configuration			Edit Configuration	1	
Tenar Client	Tenant ClientId		Validate	Finish	1	
Passwor	d			Cancel		
ETS Jam	Protect Integrate	or		;	<	
1	This Application will help to integrate JamfProtect with EventTracker to send logs.					
	Product Name Integrator Version API Version Release Date	:	ETS_JamfProtect_h 1.0.0 Jamf Protect API 12 Nov 2021	ntegrator		
	Copyright © 2021 N	Netsurion. A	All Rights Reserved			
				ОК		

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

ETS JamfProtect Integrator	×
Help	v1.0.0
Jamf Protect Configuration	Edit Configuration
ClientId Validate	Finish
Password	Cancel

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

Information	×
Credential Validated Sucessfully	
ОК]



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

ETS JamfProtect Integrator	×
Jamf Protect Integration Configured Successfully	
ОК]

4. EventTracker Knowledge Packs

After the logs are received by EventTracker, the Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support Jamf Protect.

4.1 Categories

- Jamf Protect Alerts This category provides information related to Jamf Protect suspicious activities on their hosts.
- Jamf Protect Device activities This category provides information related to the device's connectivity on their hosts.

4.2 Alerts

- Jamf Protect: Defense Evasion has been detected This alert generates whenever a running process deletes its executable after executing into the host.
- Jamf Protect: Privilege Escalation has been detected This alert generates whenever the processes prompt a user for credentials before executing.
- Jamf Protect: The signed application has been blocked This alert generates whenever the Gatekeeper blocks an application that was signed.
- Jamf Protect: Suspicious activity has been detected This alert generates whenever suspicious activities are detected on their hosts.

4.3 Reports

Jamf Protect – Alerts - This report gives information about the alerts triggered by Jamf Protect. It contains field information like the source IP address, hostname, username, file path, detected tags, and status.

Sample Report



LogTime	Computer	HostName	Source IP	User Name	File Path	Detected Tags	Status
11/16/2021 02:49:38 AM	Jamf Protect	ContosoWKS5344	192.168.100.232	kenneth	/Library/LaunchDaemons/com.abs olute.ctesservice.hdc.plist	"Persistence","MITREattack","Laun chDaemon"	Cannot find code onject on disk
11/16/2021 02:49:38 AM	Jamf Protect	ContosoWKS5344	192.168.100.232	maya	/Library/LaunchDaemons/com.abs olute.ctesservice.hdc.plist	"Persistence","MITREattack","Laun chDaemon"	code object is not signed at all

Sample Logs

{"host":{"ips":["10.24.28.56"],"serial":"C02ZP0GFLVDNDJSWK","hostname":"WKST S4738", "provisioningUDID": "4EKN899328-0016-5E90-BD7E-53F206E04DD3"}, "match": {"tags": ["PrivilegeEscalation", "MITREattack"], "uuid": "4DAJBHB602E-E247-4FB7-B42C-9ED57469B565", "event": { "pid": 4014, "type": 1, "uuid": "13C23973-871C-4612-965F-19BA6BA56B4B", "subType":23, "timestamp":16370783534939}, "facts": [{"name":"Use r Elevated Action", "tags": ["MITREattack", "PrivilegeEscalation"], "uuid": "DB4564865-99C2-416C-9F06-E7740D9E8A20", "human": "Tracks user authenticated/elevated (AuthorizeExecuteWithPrivs) actions. These processes prompted a user for credentials before executing.", "actions": [{"name": "Report", "parameters": {}}], "context": [], "vers ion":1,"severity":0}],"actions":[],"context":[],"severity":0},"related":{"fi les":[],"users":[{"uid":0,"name":"root","uuid":"C02ZP0GSADAFLVDN0"},{"uid":5 03, "name": "awilson", "uuid": "C02ZP0GADADSDFLVDN1f7"}], "groups": [{"gid":0, "nam e":"wheel","uuid":"C02ZP0SAAGFLVDN0"}, {"gid":20,"name":"staff","uuid":"C02ZP OGFLVDN1ASD4"}],"binaries":[{"gid":0,"uid":0,"fsid":16777221,"mode":35273,"p ath":"/usr/security authtrampoline","size":19120,"inode":1077942,"xattrs":[] "changed":1637073889,"created":1625982681,"shalhex":"50af81aaa874dc8sd3432d sd8958e3164346762b983aa2604", "accessed":1625982681, "modified":1625982681, "sh a256hex":"1c8a5e54caea3455121adad3231r6721a5f9d0f6440e7f244eae26cfbad9773107 73892decd6028b1c8", "isDownload": false, "isAppBundle": false, "isDirectory": fals e,gid":0,"uid":0,"fsid":1677243247221,"mode":33232461"eventType":"GPProcessE vent"}

 Jamf Protect - Device activities - This report gives information about the devices connected to their hosts. It contains fields information like the hostname, device name, vendor name, BSD name, device connected port, etc.

LogTime	Computer	HostName	Source IP	BSD Name	Device Name	Device Connected Port	Vendor Name	Reason
11/14/2021 02:37:50 PM	JAMFPROTECT	WKSTSSRV543	10.10.20.24	disk2	USB 3.0 FD	2	Kingston	USB device was inserted.
11/14/2021 02:37:50 PM	JAMFPROTECT	WKSTSSRV545	10.10.20.28	disk2	USB 3.0 FD	3	PNY	USB device was inserted.

Sample Report

Sample Logs

{"host":{"ips":["10.10.20.22"],"serial":"C02CDZSJDKFLADN","hostname":"WKSTSS
ER6434","provisioningUDID":"E1413283-A565-538B-948B-

```
53129FDB3616"},"match":{"tags":["Visibility"],"uuid":"Aada6E6-5B6C-49D3-
BD03-77202C403731","event":{"type":0,"uuid":"Aajdoiwq8-0E69-47BD-8EE2-
4A92Cdaass","device":{"bsdName":"disk1","vendorId":5451,"writable":true,"pro
ductId":23127,"removable":true,"vendorName":"Kingston","deviceClass":0,"prod
uctName":"USB 3.0
```

FD", "serialNumber": "070187E7F94F9A14", "deviceSubClass": 0}, "usbPort": 2, "times tamp": 1.63692956465464469553127E9, "usbAddress": 1}, "facts": [{"name": "USBInser

```
ted","tags":["Visibility"],"uuid":"B4FE77B3-F8D3-483D-BA29-
EA2E1A5C44EA","human":"USB device was
inserted.","actions":[{"name":"Report","parameters":{}}],"context":[],"versi
on":1,"severity":0}],"actions":[],"context":[],"severity":0},"related":{"fil
es":[],"users":[],"groups":[],"binaries":[],"processes":[]},"eventType":"GPU
SBEvent"}
```

4.4 Dashboards

Jamf Protect - Alerts by log type



Jamf Protect - Device connected by the hostname



Netstrion

Jamf Protect - Device connected by the Port number



 Jamf Protect - Alerts by reason
 Image: Comparison of the second seco

Jamf Protect - Alerts by reason

Jamf Protect - Hostname by alert reason



Jamf Protect - Suspicious file hashes





5. Importing Jamf Protect Knowledge Pack into EventTracker

NOTE: Import the Knowledge Pack items in the following sequence:

- Categories
- Alerts
- Knowledge Objects
- Flex Reports
- Dashboards
- 1. Launch the EventTracker Control Panel.
- 2. Double click **Export-Import Utility**.

EventTracker Con	trol Panel		Eve	- ×				
EventVault	Diagnostics	License Manager	Export Import	Append Archives				
EventTracker	Fraffic Analyzer	Agent	Port	TrapTracker				
Agent Confi	53	Manageme	Configuration					
Change Audit	About EventTracker							
	E-mail: support@Event Tracker.com							

🐁 Export Import Utility	
Export Import	
1. Provide the path and file n. 2. Click the Import button.	ame of the Categories file. Use the '' button to
Options	Location
 Category 	

3. Click the **Import** tab.

5.1 Categories

1. After opening the **Export-Import Utility** via the **EventTracker Control Panel**, click the **Category** option, and then click **Browse** .



2. Navigate to the Knowledge Pack folder and select the file with the extension ".iscat", e.g., "Categories_Jamf Protect.iscat" and click the Import button.

Export Import Utility		—		×
Export Import				
 Provide the path and file n Click the Import button. 	ame of the Categories file. Use the '' button to browse and locate the import file.			
Options Category Filters	Location			
Alerts	Source :	_		
 Systems and Groups Token Value 	*iscat			
⊖ Reports				
O Behavior Correlation				
	Impr	ort	Clos	e

EventTracker displays a success message.

Export Imp	Export Import Utility	
1	Selected category details are imported successfully.	
	ОК	

5.2 Alerts

1. Click the **Alert** option, and then click the **Browse** button.

Netsurion

2. Click the Import button. Options		
Category		
Filters	Import E-mail settings	
Alerts	Set Active	This settion is set in the sub-facing state from the second
Systems and Groups	 Only if notifications set Bu default 	(v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration
RSS Feeds	0 0, 0.0	section.
Reports	Source :	
Behavior Rules	*.isalt	
SCAP		
💿 Token Value		

- 2. Locate the Alerts_Jamf Protect.isalt file, and then click the Open button.
- 3. To import the alerts, click the **Import** button.
- 4. EventTracker displays a success message.



5. Click the **OK** button, and then click the **Close** button.

5.3 Reports

1. In the EventTracker Control Panel, select **Export/Import utility** and select the **Import tab**. Then, click the **Reports** option, and choose **New (*.etcrx)**.



2. Click the Import button	inte of Schould report life. See the Subtrine Showae and locate the import life.	
Options Category	Location	
O Filters		
O Alerts	C Legacy (*issch) New (*.etcnx)	
O Systems and Groups	Source : *issch	
◯ Token Value		
Reports		
O Behavior Correlation		

2. After selecting the **New (*.etcrx)** file, a new pop-up window appears. Click the **Select File** button and navigate to the file path with a file having the extension ".etcrx", e.g., Reports_Jamf Protect .etcrx.

🛟 Reports Im	nport							
Note : If repor	t(s) contains ter	mplate, first import tem	plate and proceed	with report import proces	s.			
Select file	*.etcrx							Select file
Available repo	orts							
Title				Frequency Show all	•	QQ		
		Title	Sites	Groups	Systems	Frequency	Runtime	Туре
					-,	,		

3. Wait while the reports populate in the below tables. Now, select all the relevant reports and then click the **Import T** button.

Note: Set run time option is not applicabl	e for Defined Reports and Hourly Reports	
Set run time for report(s) from	AM • at interval of _ minutes	Set ()
Replace	to Replace	e Assign systems
		Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

EventTracker displays a success message.

Export Import Utility	×
Selected reports configurations are impo	orted successfully
	ОК



5.4 Knowledge Objects

1. Click Knowledge Objects under the Admin option on the EventTracker page.

			🔎 Admin 🗸	Tools 👻 📀
Π.	Active Watch Lists	Event Filters	😥 Parsing Rules	🔒 / Das
н.	Alerts	Ventvault	Report Settings	
	Behavior Correlation Rules	FAQ Tile Configuration	Systems	
	🗞 Behavior Correlation Settings	Group Management	🗙 Users	
o mi prisc	Casebook Configuration	Q IP Lookup Configuration	🕀 Weights	since the last 24 hours
	● Category	·☆ Knowledge Objects	Windows Agent Config	
	1 Diagnostics	Dianager 🖉		

2. Click the Import objects icon.

↑ Admin / Knowledge Objects
Objects 🕀 ፒ 🏦 🌣
Import Objects

A pop-up box appears, click Browse and navigate to the Knowledge Packs folder (type %et_install_path%\Knowledge Packs in the navigation bar) with the extension ".etko", e.g., KO_Jamf Protect.etko, and then click Upload.

Import		
KO_ <product name="">.etko</product>	🚔 Browse	Upload

4. A list of available Knowledge Objects will appear. Select the relevant files and click the **Import** button.





5.5 Dashboards

- 1. Login to EventTracker.
- 2. Navigate to **Dashboard** \rightarrow **My Dashboard**.



3. In **My Dashboard**, Click the **Import** button.



- Select the Browse button and navigate to the Knowledge Pack folder (type %et_install_path%\Knowledge Packs in the navigation bar) where the .etwd file is saved, e.g., Dashboards_Jamf Protect .etwd and click Upload.
- 5. Wait while EventTracker populates all the available dashboards. Now, choose **Select All** and click the **Import** button.

Import	
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.	
Available widgets	
Import	•



6. Verifying Jamf Protect Knowledge Pack in EventTracker

6.1 Categories

- 1. Login to EventTracker.
- 2. Click the Admin dropdown, and then click Categories.
- 3. In the **Category Tree** scroll down and expand the **Jamf Protect** group folder to view the imported categories.

Category
Category Tree Search
Jamf Protect Q Q
Category
✓ Jamf Protect - Alerts
✓ Jamf Protect - Device activities

6.2 Alerts

- 1. Login to EventTracker.
- 2. Click the Admin menu, and then click Alerts.
- 3. In the **Search** box, type **Jamf Protect**, and then click the **Go** button. The **Alert Management** page will display all the imported alerts.

Alerts							🕈 / Admin / Alerts
Show All 🗸					Search by Alert name	: ~	Jamf Protect Q Q
229	82		229	System	202	229	Critical 15 High 6 10 Medium 49
Available Alerts Total number of alerts available	Active Alerts Total number of active alerts		System/User Def Count for system an	ined Alerts d user defined alerts		Alerts by Thre Count of alerts	eat Level by threat level
Activate Now Click 'Activate Now' after making all changes Total: 1 Page Size 25						Total: 1 Page Size 25 V	
Alert Name A	Threat	Active Email	Forward as SNMP	Forward as Syslog	Remedial Action I at Console	Remedial Action at Agent	Applies To
βδ Jamf Protect: Suspicious activity has been detected	•						Jamf Protect

4. To activate the imported alerts, select the respective checkboxes in the **Active** column.

EventTracker displays a success message.



Successfully saved configuration.	
ок	

5. Click **OK**, and then click the **Activate Now** button.

Note: Specify the appropriate systems in the Alert configuration for better performance.

6.3 Knowledge Objects

- 1. In the EventTracker web interface, click the Admin dropdown, and then click Knowledge Objects.
- 2. In the **Knowledge Objects** tree, expand the **Jamf Protect** group folder to view the imported Knowledge Objects.

Knowledge Objects	
Jamf Protect	Q Q
Groups	🕂 🏈 🗓
■ Jamf Protect	

6.4 Reports

1. In the EventTracker web interface, click the Reports menu, and then select Report Configuration.



- 2. In the Report Configuration pane, select the Defined option.
- 3. Click the Jamf Protect group folder to view the imported reports.



Reports configuration: all				
Ð				
		Title		
	200	Jamf Protect - Device activities		
	200	Jamf Protect - Alerts		

6.5 Dashboards

1. In the EventTracker web interface, click the **Home** Button and select **My Dashboard**.

	Home
Dashb	My Dashboard
R	Threats
	Incidents

2. Select **Customize dashlets** (and type **Jamf Protect** in the search bar.



Netsurion®

0	ustomize dashlets				×
[Jamf			Q	
	Jamf Protect - Alerts by logtype	Jamf Protect - Alerts by reason	Jamf Protect - Device connecte	Jamf Protect - Device connecte	
	Jamf Protect - Hostname by rea	Jamf Protect - Hostnames by so	Jamf Protect - Suspicious file ha	Jamf Protect - Suspicious filepa	
				Add Delete Close	e



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 <u>EventTracker</u> 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 <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation 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 <u>netsurion.com</u> 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