Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating Jamf Protect with EventTracker

EventTracker v9.2x and above

Publication Date:

December 8, 2021

© Copyright Netsurion. All Rights Reserved.

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.

© Copyright Netsurion. All Rights Reserved.

Table of Contents

© Copyright Netsurion. All Rights Reserved.

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

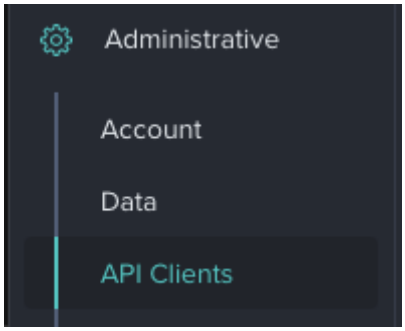
- **Admin** access to the **Jamf Protect** console.
- Windows PowerShell v5.0 and above should be installed**.**
- **EventTracker** Manager/Sensor should be installed and running.

3. Configuring Jamf Protect Logging

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

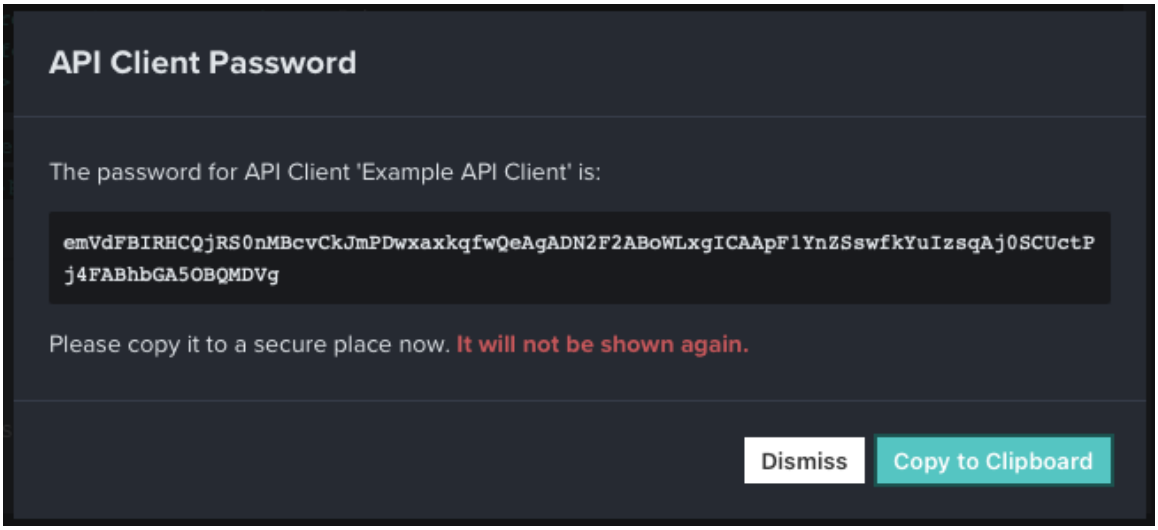
3.1 Configuring Jamf Protect API

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

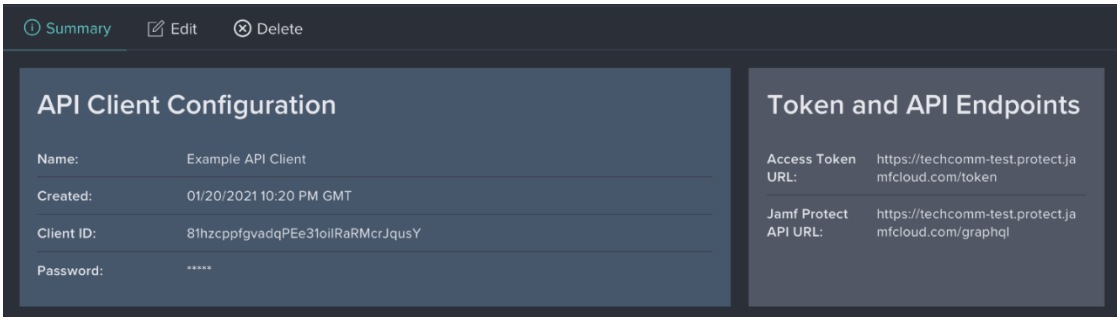


3. Click **Create API Client**.
4. Enter a name for your API client.
5. Copy the API client password for later use.

© Copyright Netsurion. All Rights Reserved.



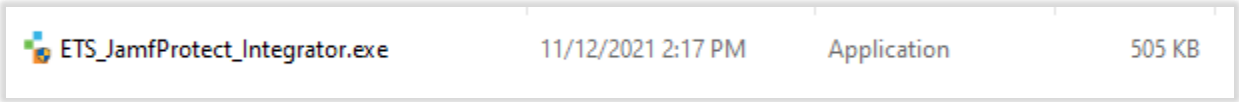
Your API client configuration and endpoint information are displayed.



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

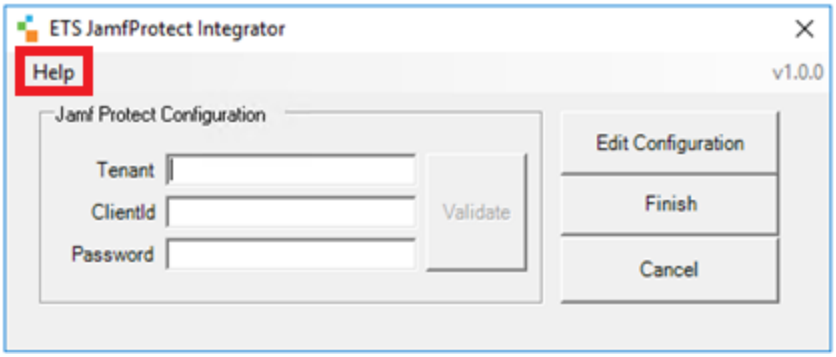
3.2 Configuring Jamf Protect Integrator

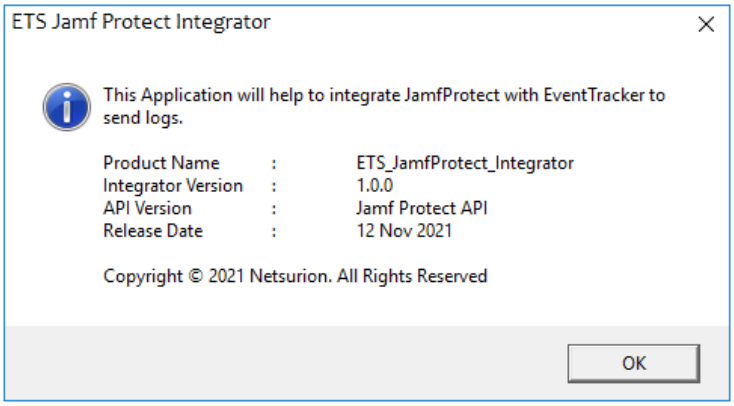
1. Please click here to download the Jamf Protect integrator files.
2. Run the **ETS_Jamf Protect_integrator.exe** file**.**



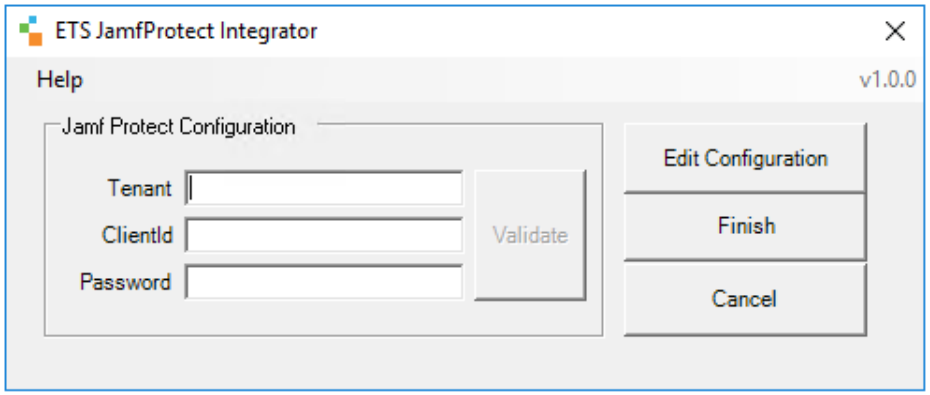
3. Click **Help** >> **About** to check the updated integrator version details.

© Copyright Netsurion. All Rights Reserved.

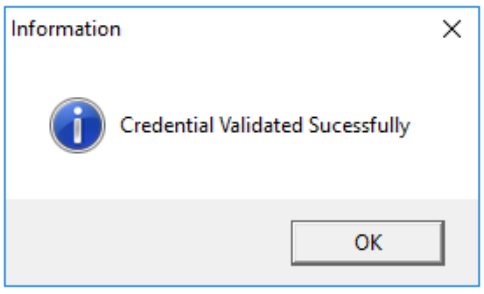




4. Enter the necessary details into the Jamf Integrator and click **Validate**.

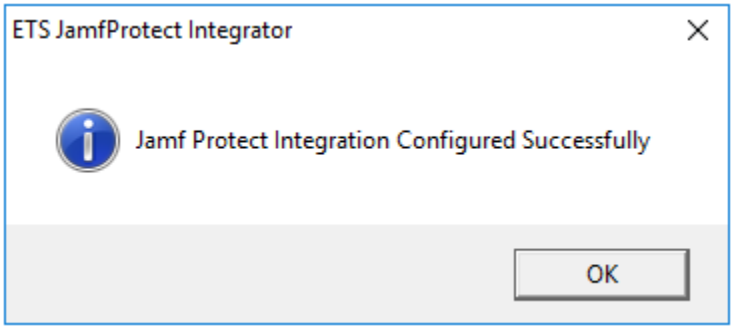


5. After the credentials are validated successfully. Click **OK**.



© Copyright Netsurion. All Rights Reserved.

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



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

© Copyright Netsurion. All Rights Reserved.

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.absolute.ctesservice.hdc.plist	"Persistence","MITREattack","LaunchDaemon"	Cannot find code onject on disk
11/16/2021 02:49:38 AM	Jamf Protect	ContosoWKS5344	192.168.100.232	maya	/Library/LaunchDaemons/com.absolute.ctesservice.hdc.plist	"Persistence","MITREattack","LaunchDaemon"	code object is not signed at all

Sample Logs


```
{"host":{"ips":["10.24.28.56"],"serial":"C02ZP0GFLVDNDJSWK","hostname":"WKSTS4738","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":"User 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":[],"version":1,"severity":0}],"actions":[],"context":[],"severity":0},"related":{"files":[],"users":[{"uid":0,"name":"root","uuid":"C02ZP0GSADAFLVDN0"},{"uid":503,"name":"awilson","uuid":"C02ZP0GADADSDFLVDN1f7"}],"groups":[{"gid":0,"name":"wheel","uuid":"C02ZP0SAAGFLVDN0"},{"gid":20,"name":"staff","uuid":"C02ZP0GFLVDN1ASD4"}],"binaries":[{"gid":0,"uid":0,"fsid":16777221,"mode":35273,"path":"/usr/security_authtrampoline","size":19120,"inode":1077942,"xattrs":[],"changed":1637073889,"created":1625982681,"sha1hex":"50af81aaa874dc8sd3432dsd8958e3164346762b983aa2604","accessed":1625982681,"modified":1625982681,"sha256hex":"1c8a5e54caea3455121adad3231r6721a5f9d0f6440e7f244eae26cfbad977310773892decd6028b1c8","isDownload":false,"isAppBundle":false,"isDirectory":false,gid":0,"uid":0,"fsid":1677243247221,"mode":33232461"eventType":"GPProcessEvent"}
```


- **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.

Sample Report

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 Logs

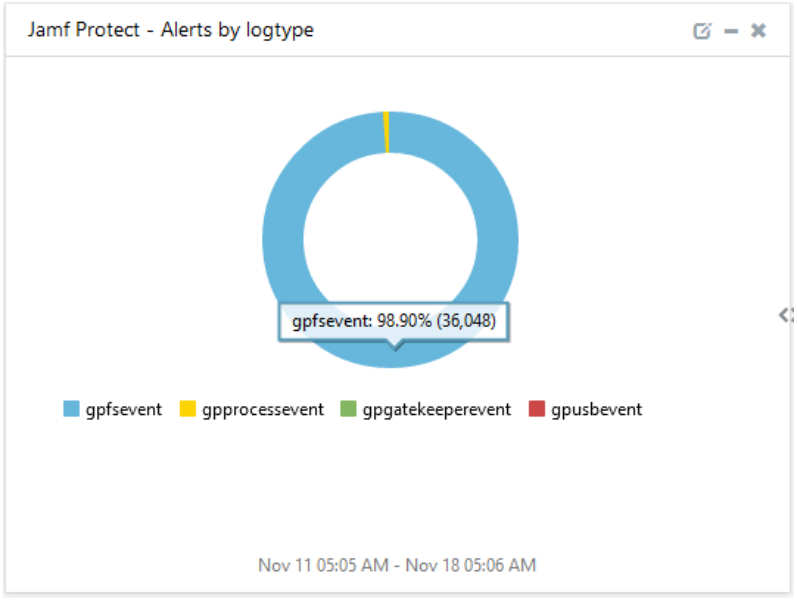

```
{"host":{"ips":["10.10.20.22"],"serial":"C02CDZSJDKFLADN","hostname":"WKSTSSER6434","provisioningUDID":"E1413283-A565-538B-948B-53129FDB3616"},"match":{"tags":["Visibility"],"uuid":"Aada6E6-5B6C-49D3-BD03-77202C403731","event":{"type":0,"uuid":"Aajdoiwq8-0E69-47BD-8EE2-4A92Cdaass","device":{"bsdName":"disk1","vendorId":5451,"writable":true,"productId":23127,"removable":true,"vendorName":"Kingston","deviceClass":0,"productName":"USB 3.0
FD","serialNumber":"070187E7F94F9A14","deviceSubClass":0},"usbPort":2,"timestamp":1.6369295646546469553127E9,"usbAddress":1},"facts":[{"name":"USBInser
```


© Copyright Netsurion. All Rights Reserved.

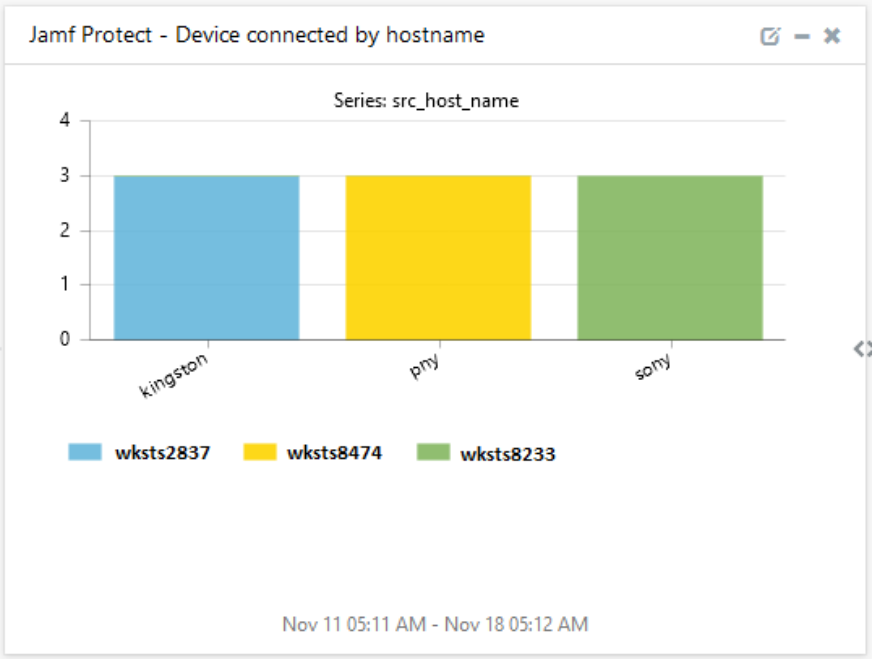
ted","tags":["Visibility"],"uuid":"B4FE77B3-F8D3-483D-BA29-EA2E1A5C44EA","human":"USB device was inserted.","actions":[{"name":"Report","parameters":{}}],"context":[],"version":1,"severity":0}],"actions":[],"context":[],"severity":0},"related":{"files":[],"users":[],"groups":[],"binaries":[],"processes":[]},"eventType":"GPUSBEvent"}

4.4 Dashboards

- **Jamf Protect - Alerts by log type**

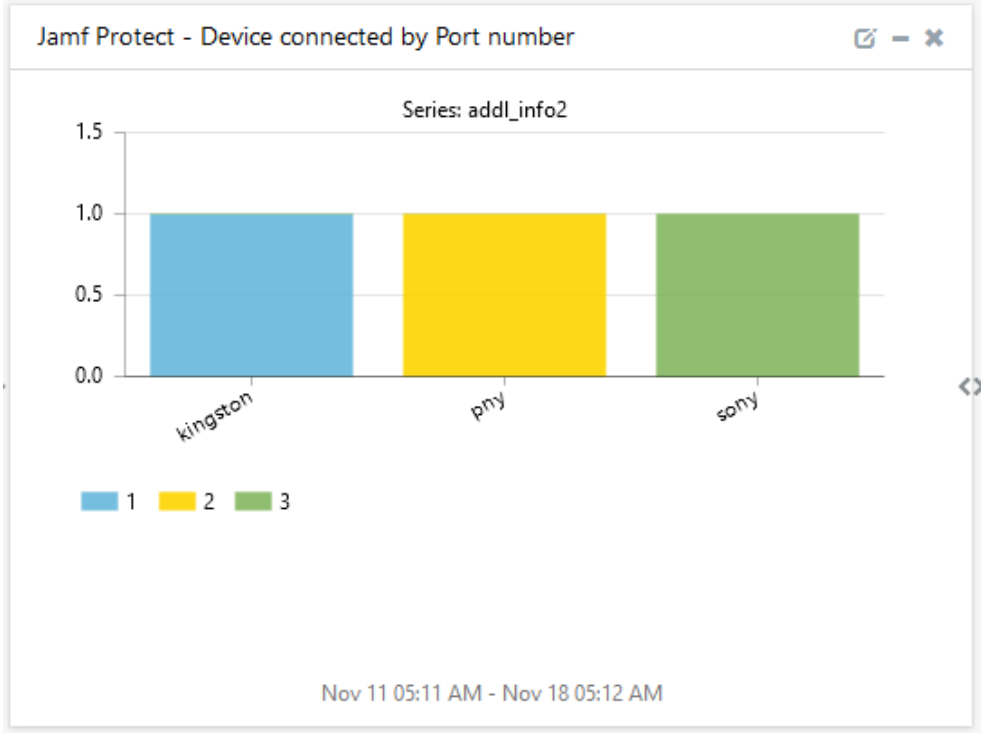


- **Jamf Protect - Device connected by the hostname**

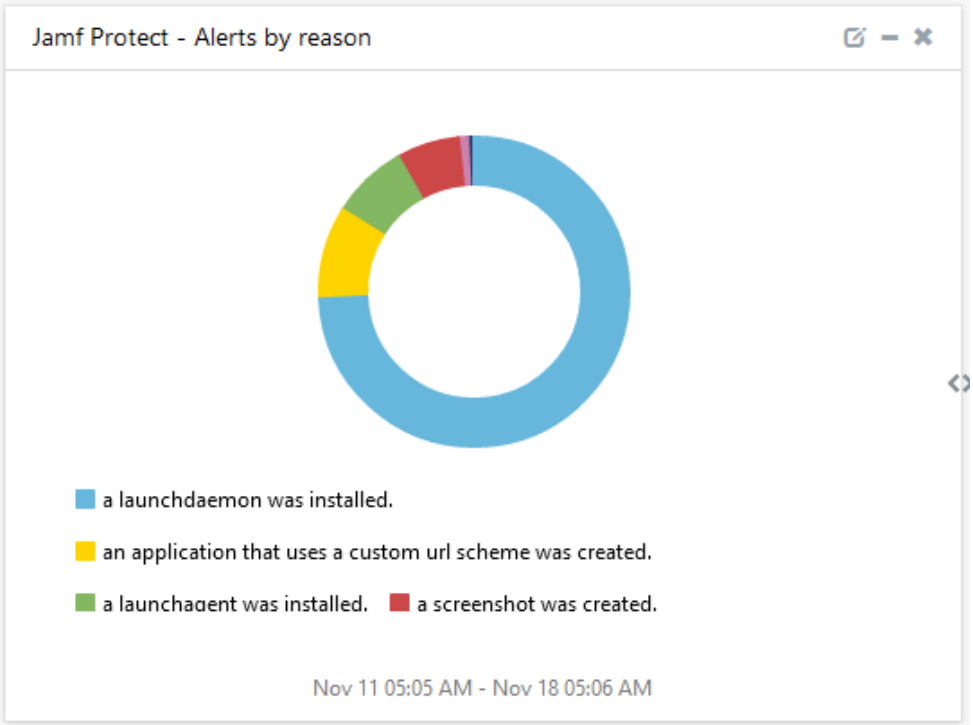


© Copyright Netsurion. All Rights Reserved.

- **Jamf Protect - Device connected by the Port number**

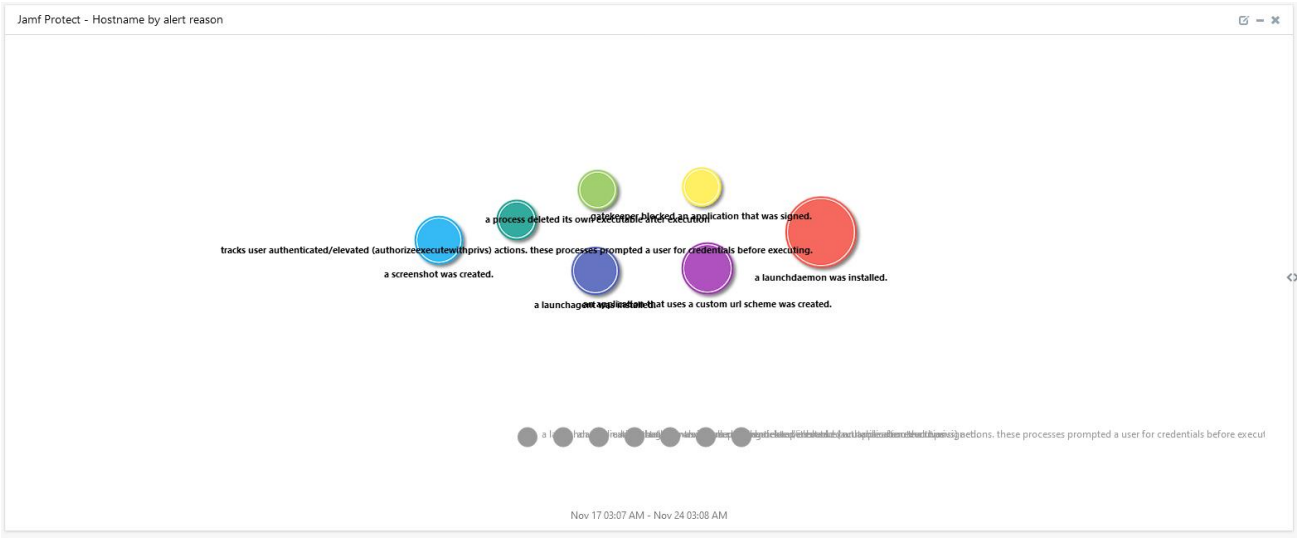


- **Jamf Protect - Alerts by reason**

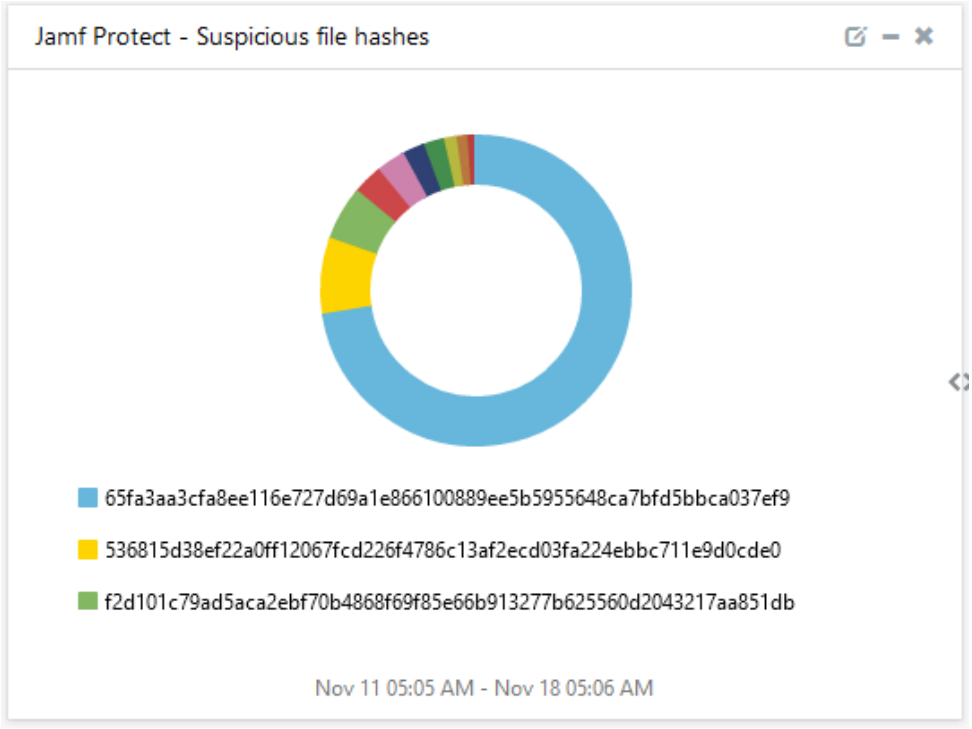


© Copyright Netsurion. All Rights Reserved.

- **Jamf Protect - Hostname by alert reason**



- **Jamf Protect - Suspicious file hashes**



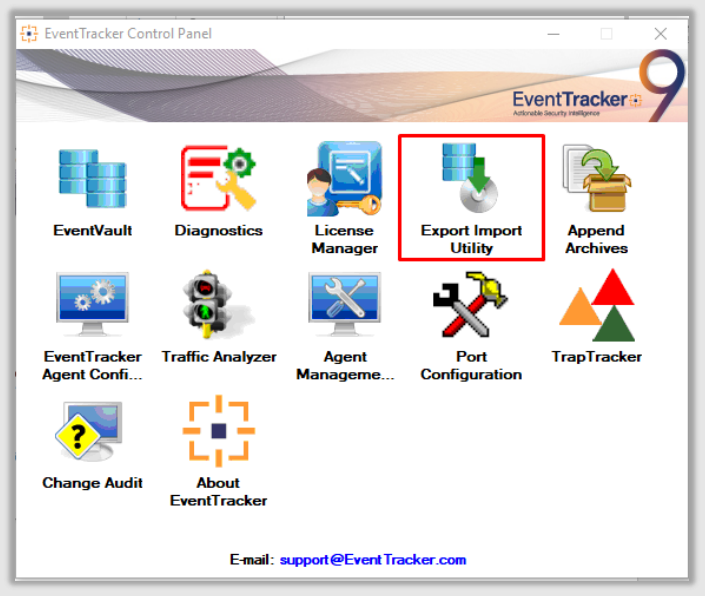
© Copyright Netsurion. All Rights Reserved.

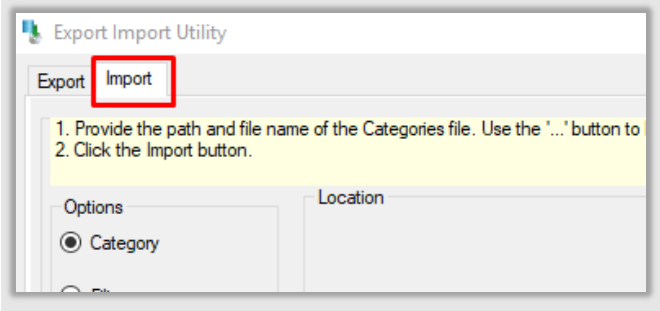
5. Importing Jamf Protect Knowledge Pack into EventTracker

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**.





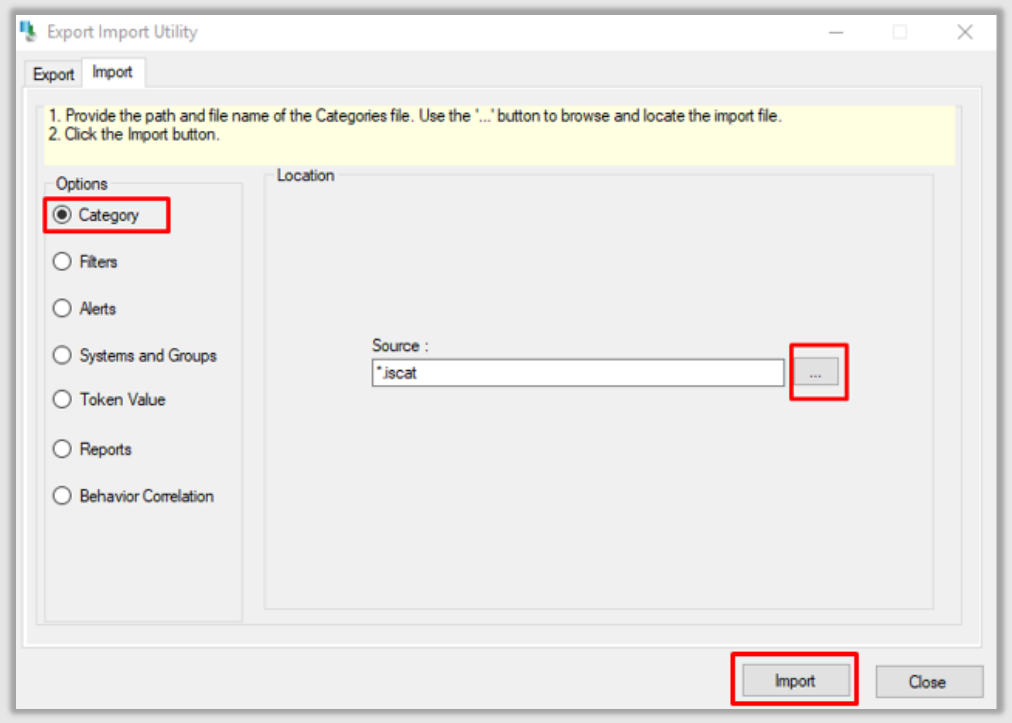
3. Click the **Import** tab.

5.1 Categories

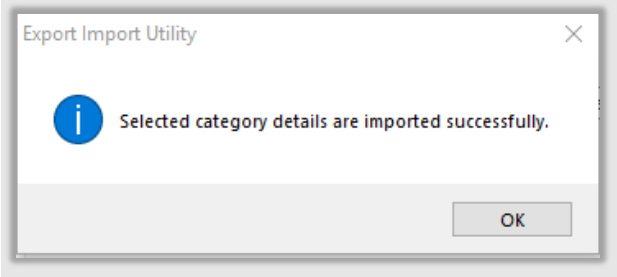
1. After opening the **Export-Import Utility** via the **EventTracker Control Panel**, click the **Category** option, and then click **Browse** ... .

© Copyright Netsurion. All Rights Reserved.

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.



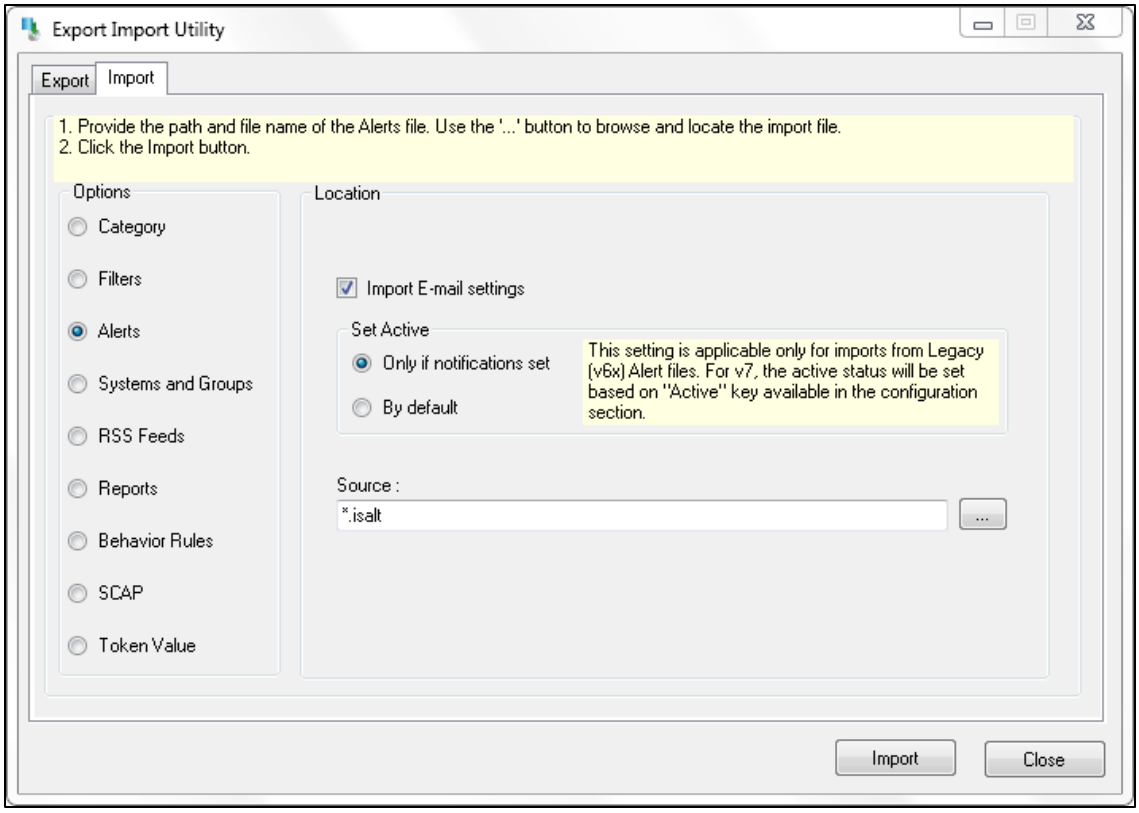
EventTracker displays a success message.



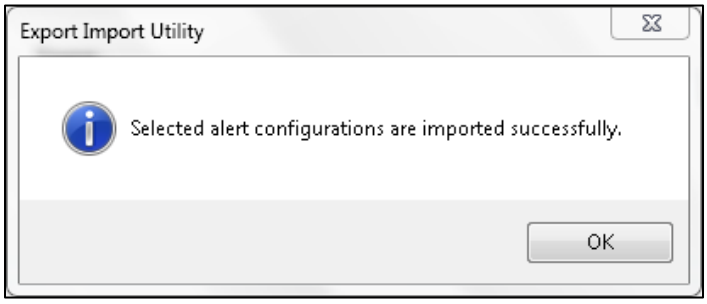
5.2 Alerts

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

© Copyright Netsurion. All Rights Reserved.



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.

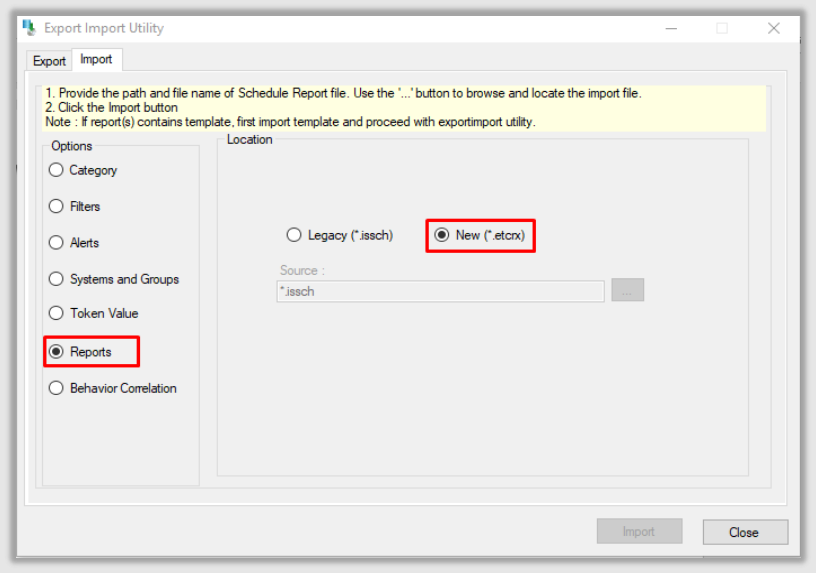


5. Click the **OK** button, and then click the **Close** button.

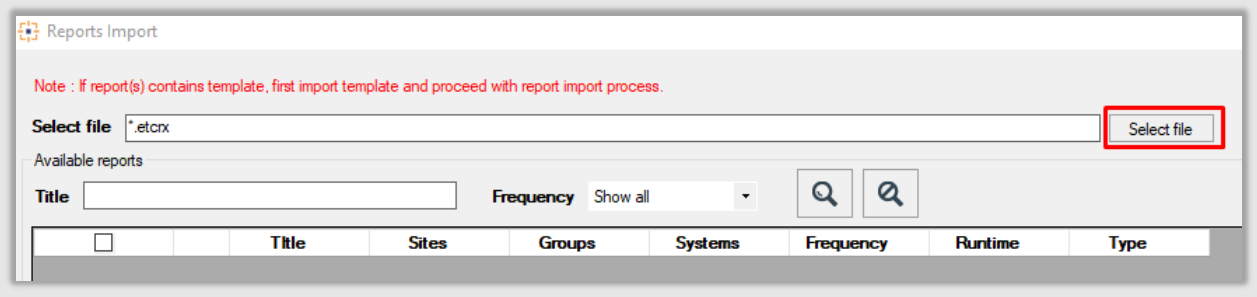
5.3 Reports

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

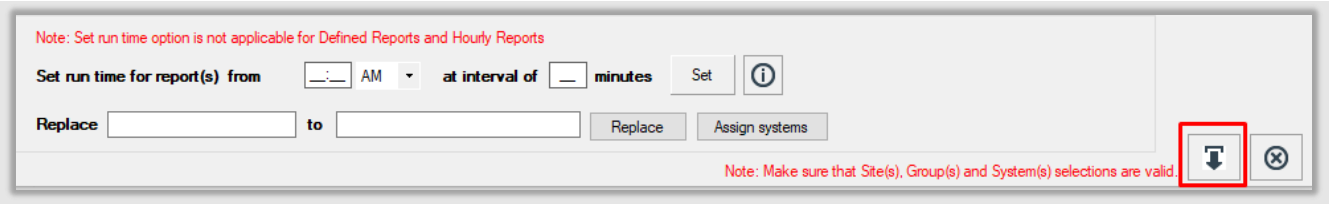
© Copyright Netsurion. All Rights Reserved.



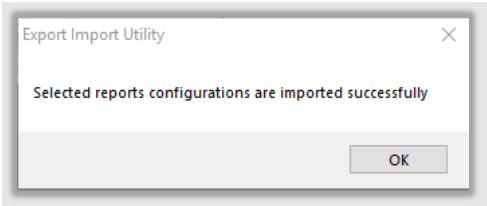
2. After selecting the **New (*.etcrx)** file, a new pop-up window appears. Click the **Select File** button and navigate to the file path with a file having the extension "**.etcrx", e.g., Reports_ Jamf Protect .etcrx.**



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



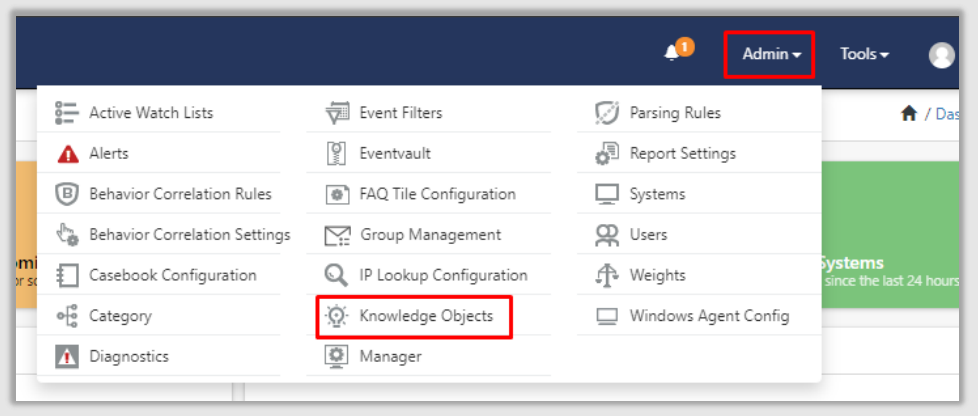
EventTracker displays a success message.



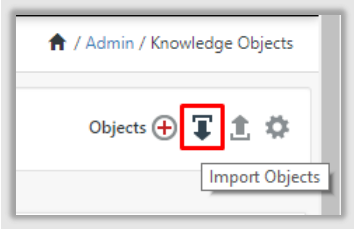
© Copyright Netsurion. All Rights Reserved.

5.4 Knowledge Objects

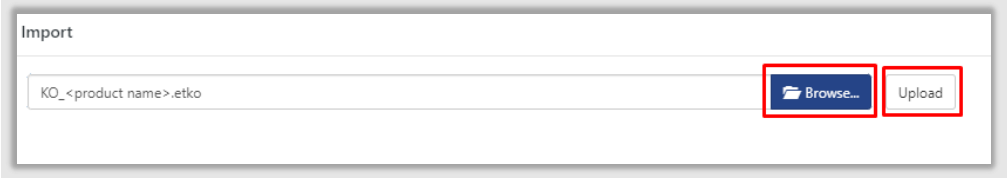
1. Click **Knowledge Objects** under the **Admin** option on the EventTracker page.



2. Click the **Import objects** icon.



3. 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**.

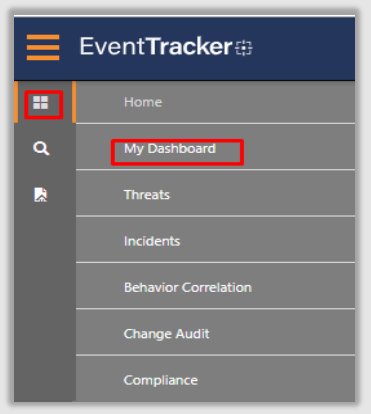


4. A list of available Knowledge Objects will appear. Select the relevant files and click the **Import** button.

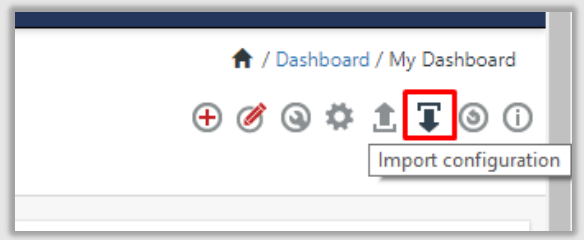
© Copyright Netsurion. All Rights Reserved.

5.5 Dashboards

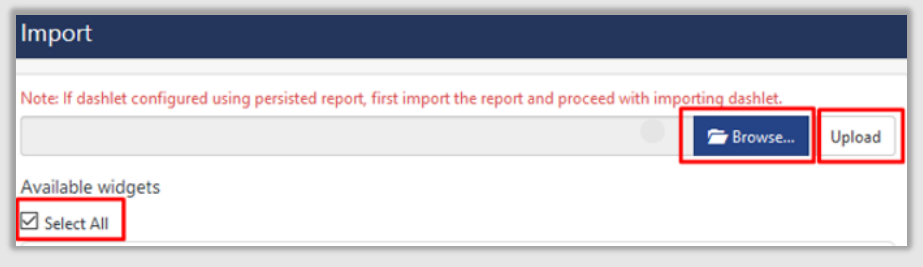
1. Login to **EventTracker**.
2. Navigate to **Dashboard → My Dashboard**.

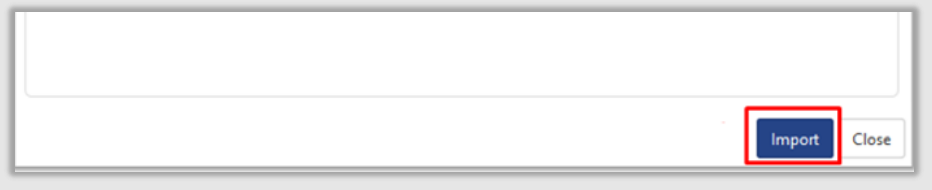


3. In **My Dashboard**, Click the **Import** button.



4. 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.



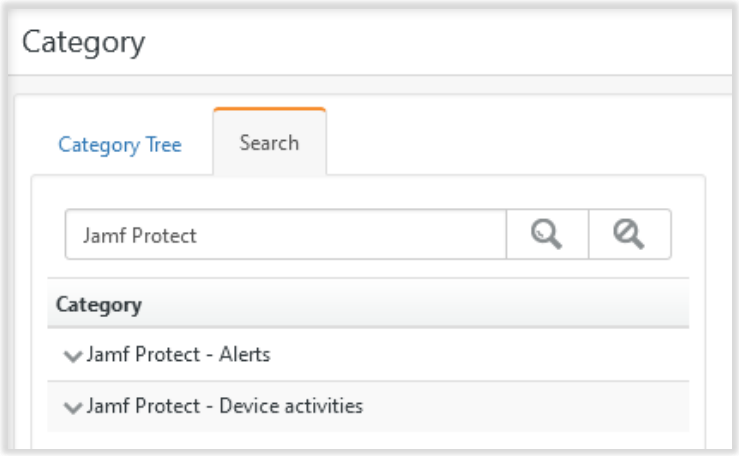


© Copyright Netsurion. All Rights Reserved.

6. Verifying Jamf Protect Knowledge Pack in EventTracker

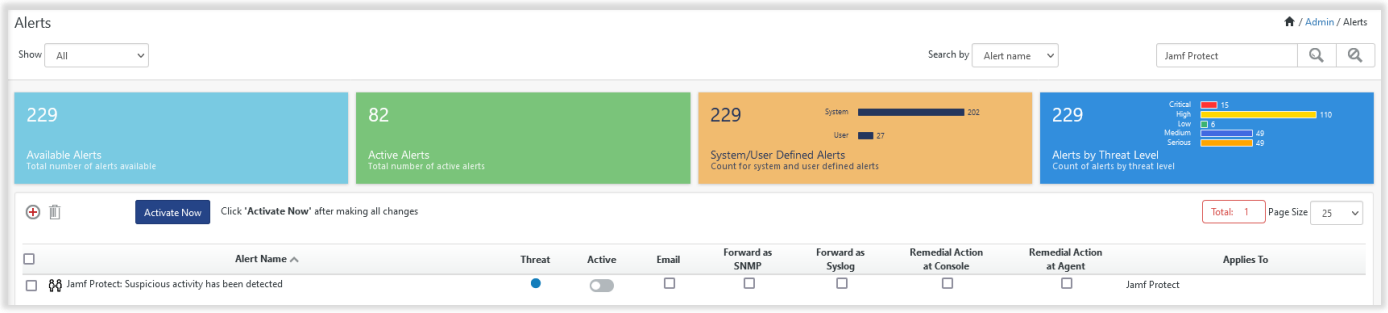
6.1 Categories

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.



6.2 Alerts

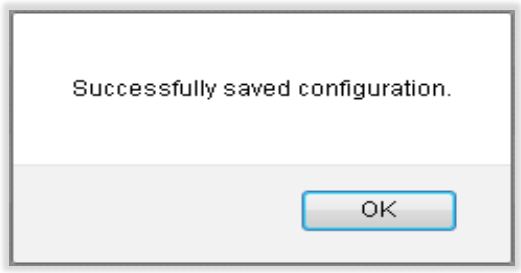
1. Login to **EventTracker**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In the **Search** box, type **Jamf Protect**, and then click the **Go** button.
   The **Alert Management** page will display all the imported alerts.



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

   EventTracker displays a success message.

© Copyright Netsurion. All Rights Reserved.

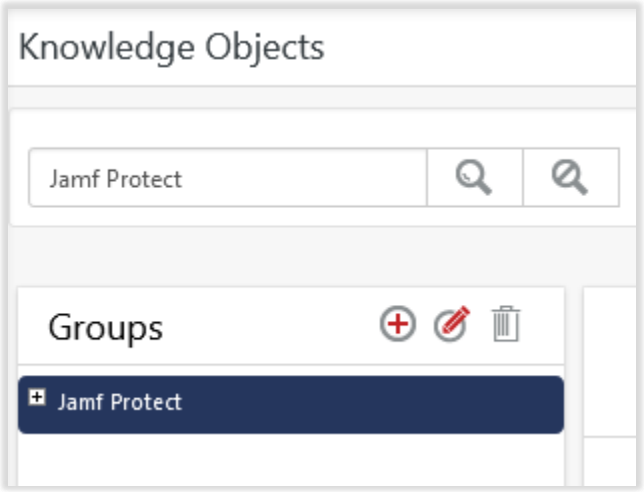


5. Click **OK**, and then click the **Activate Now** button.

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

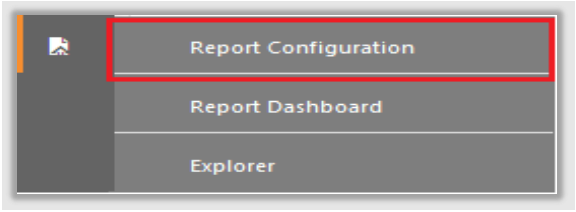
6.3 Knowledge Objects

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.



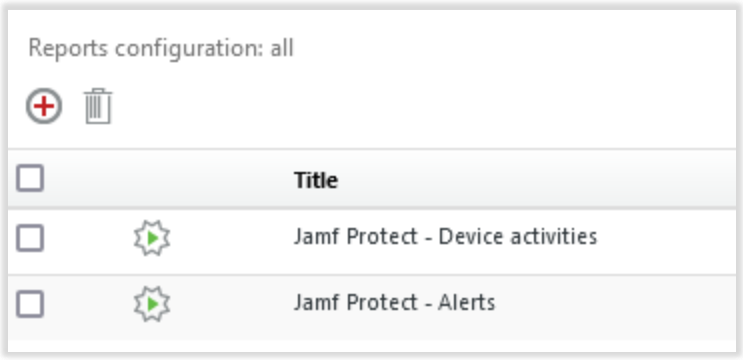
6.4 Reports

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



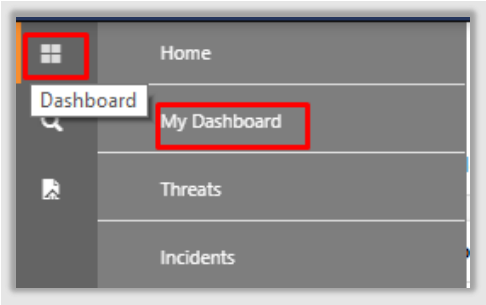
2. In the **Report Configuration** pane, select the **Defined** option.
3. Click the **Jamf Protect** group folder to view the imported reports.

© Copyright Netsurion. All Rights Reserved.

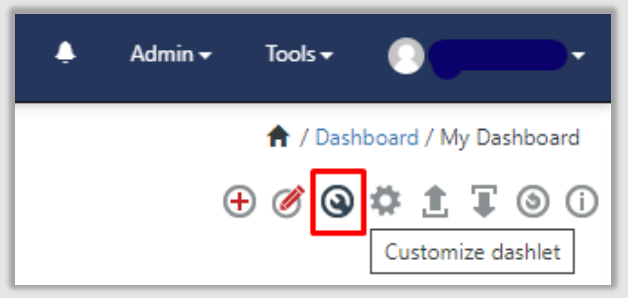


6.5 Dashboards

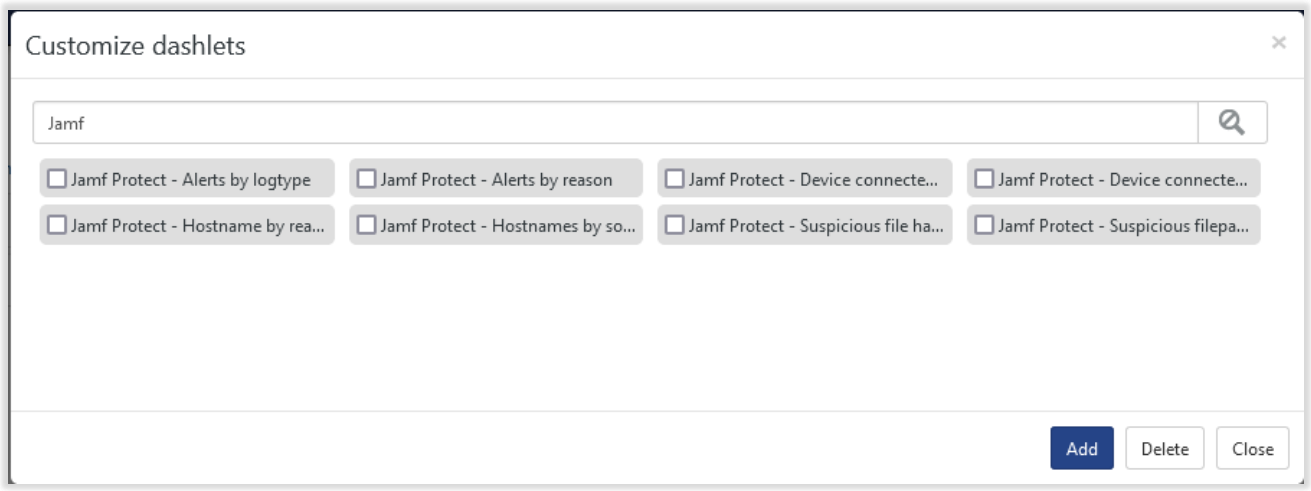
1. In the EventTracker web interface, click the **Home** Button and select **My Dashboard**.



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



© Copyright Netsurion. All Rights Reserved.



© Copyright Netsurion. All Rights Reserved.

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

© Copyright Netsurion. All Rights Reserved.