

**Integration Guide** 

# Integrating Microsoft Intune with EventTracker

**Publication Date:** 

June 02, 2022

# Abstract

This guide provides instructions to configure the Knowledge Pack in EventTracker to receive the logs from the Microsoft Intune service. The Knowledge Pack contains the reports, dashboard, alerts, and saved searches.

# Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or later and Microsoft Intune.

# Audience

This guide is for the Administrators responsible to configure the Knowledge Packs to EventTracker.



# Table of Contents

1	Ove	erview	4
2	Pre	erequisite	4
3	Eve	entTracker Knowledge Packs	4
	3.1	Alerts	4
	3.2	Categories	4
	3.3	Reports	5
	3.4	Dashboard	5
4	Imp	porting Microsoft Intune Knowledge Packs into EventTracker	8
	4.1	Categories	9
	4.2	Alerts	10
	4.3	Knowledge Objects (KO)	11
	4.4	Reports	13
	4.5	Dashboard	14
5	Ver	rifying Microsoft Intune Knowledge Packs in EventTracker	17
	5.1	Categories	17
	5.2	Alerts	17
	5.3	Knowledge Objects	19
	5.4	Reports	19
	5.5	Dashboard	20

## 1 Overview

Microsoft Intune is a cloud-based service that aims to provide unified endpoint management. It focuses on controlling both organization and personally owned mobile devices and mobile applications to protect corporate data. This service also configures specific policies to manage applications.

EventTracker facilitates monitoring events from the Microsoft Intune. Its dashboard and reports interface benefits you to track user activities, configurational changes, and device data to detect compliance, managed, and registered devices in Microsoft Intune. In this way, you will be able to recognize the device's criticality and take the necessary measure.

# 2 Prerequisite

Refer to <u>How-To Guide</u> to see the process of configuring Microsoft Intune to forward logs to EventTracker.

# 3 EventTracker Knowledge Packs

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

The following Knowledge Packs (KPs) are available in EventTracker to support the Microsoft Intune.

## 3.1 Alerts

**Microsoft Intune: Configuration modified:** This alert indicates the activity performed on Intune configuration or the user activity when configuring the devices in Microsoft Intune.

**Microsoft Intune: Failed audit action:** This alert indicates a failed action detected in Microsoft Intune.

**Microsoft Intune: Non-compliance/un-registered/un-managed device detected:** This alert indicates the detection of non-compliance, unregistered, and unmanaged devices in Microsoft Intune.

## 3.2 Categories

**Microsoft Intune - Intune activities:** This category of the saved search will allow the users to parse the events that are specific to the Intune activities in Microsoft Intune.

## 3.3 Reports

**Microsoft Intune - Audit activities:** This report provides a detailed summary of audit activities in Microsoft Intune. It includes source IP address, operation name, operation type, result, correlation ID, and more.

		Source IP					Result
LogTime	Computer	Address	Correlation ID	Operation	Operation Type	Result status	Reason
05-18-2022 03:37:44 AM	INTUNE	10.81.51.202	2256fb3a-b124-4902- 84fc-14bdb214fce5	Update device	Update	Failure	
05-18-2022 03:37:46 AM	INTUNE	10.1.12.202	25cefa-58e9-473d-96bf- e884b2561f2c	Update device	Update	success	

**Microsoft Intune - Device details**: This report provides a detailed summary of devices onboarded in Microsoft Intune. It provides the details of the compliance state, managed state, device name, tenant ID, username, owner type, MAC address, IMEI and more.

LogTime	Compute r	Compliance State	User Name	User Email	MAC address	UPN		Device state	jail broken	Device join type	Managed by	Device Name	Device ID	IMEI	Owner Type	Tenant ID	Device Serial
05-18-2022 03:37:55 AM	INTUNE	Not Evaluated	john s	john.s@cont oso.com		john.s @cont oso.co m	Androi d (Device )	RetireP ending	true	Azure AD registered	Intune	john.s_Andr oid_9/21/202 1_9:27 PM	dd2c50a47d- 9b3c-44e9- 960c- 2254030d57 84		Unknown	d958a902- 5c5d-4c4a- 8f1b- dbe0d31245 362	102d2a09da b49958
05-18-2022 03:37:56 AM	INTUNE	Noncompliant	franz r	franz.r@cont oso.com		franz.r @cont oso.co m	Androi d (Device )	RetireP ending	true	Azure AD registered	Intune	granz.s_And roid_5/16/20 21_8:52 PM	0e762526- 983c-44e9- 8852- ae84e91253 65		Unknown	d958a902- 5c5d-4c4a- 8f1b- dbe0d31245 362	458d2a09da 20314
05-18-2022 03:37:57 AM	INTUNE	Compliant	daniles m	daniles.m@c ontoso.com	4a6d0aa 5c823	danile s.m@ contos o.com	iOS/iP adOS	Manage d	False	Azure AD registered	Intune	ABT iPhone11- daniles	ae84e925- 17c8-4d30- b913- afdd2c50a47 d	35289 81172 24312	Personal	d958a902- 5c5d-4c4a- 8f1b- dbe0d31245 362	H54NCX17V 2NY6

## 3.4 Dashboard

#### **Microsoft Intune - Activities by categories**







#### Microsoft Intune - Audit activities by geo location

Microsoft Intune - Devices by compliance state



#### **Microsoft Intune - Devices details**

Microsof	t Intune - Device	es details						0 🖸 -	×	
action	shanga infa	Below are	the reference fo	r the table. actio	on = Registration state; log_action	n = Device state	; src_user_info	= Owne	rship; t	hreat_info = Is Jail:
action	change_into		log_action	log_status	src_os_name	src_user_into	threat_into	Count		
registered	2021-05-11 21:18:	53.0000000	retirepending	noncompliant	android (device administrator)	unknown	true	2		
registered	2021-07-30 21:33:	40.0000000	retirepending	not evaluated	android (device administrator)	unknown	true	2		
registered	2022-05-07 18:46:	05.9125002	managed	compliant	ios/ipados	personal	false	1		
registered	2022-05-07 18:57:	05.0371192	managed	compliant	ios/ipados	personal	false	1		
registered	2022-05-07 20:10:	56.9757844	managed	compliant	ios/ipados	personal	false	1		
registered	2022-05-07 20:14:	01.5576362	managed	compliant	ios/ipados	personal	false	1		>
registered	2022-05-07 20:32:	55.9807802	managed	compliant	ios/ipados	personal	false	1		
registered	2022-05-07 23:50:	02.7256229	managed	compliant	ios/ipados	personal	false	1		
registered	2022-05-07 23:50:	24.3582387	managed	compliant	ios/ipados	personal	false	1		
registered	2022-05-07 23:52:	04.0608936	managed	compliant	ios/ipados	personal	false	1		
2.6	2022 05 00 00 52	00 6400450		19 - A	1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -	1	10 A	*	•	
			M	ay 17 03:40 AM	- May 18 03:41 AM					

#### Microsoft Intune - Audit activities by result





# 4 Importing Microsoft Intune Knowledge Packs into EventTracker

Import the Knowledge Pack items in the following sequence.

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



3. In the Export Import Utility window, click on the Import tab.



## 4.1 Categories

**1.** In the **Import** tab, choose the **Category** option and click on the **Browse** button from the **Source** field.

			Export Import Utility		-		2
xport	t Import						
1. P 2. C	Provide the path and file na Click the Import button.	me of the Catego	es file. Use the '' button to browse and locate th	ie import file.			
-00	otions	Location					
۲	Category						
0	Filters						
0	Alerts						
0	Systems and Groups		Source :				
0	Token Value		<u>c</u>				
0	Reports						
0	Behavior Correlation						
				Import		Class	_

- 2. In the Browse window, locate the Categories\_Microsoft Intune.iscat file and click on the Open button.
- **3.** To import the categories, click on the **Import** button.
- 4. EventTracker displays a successful message on successfully importing the selected file in Categories.



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



#### 4.2 Alerts

1. In the **Import** tab, choose the **Alerts** option and click on the **Browse** button from the **Source** field.

<b>B</b>	Export In	nport Utility	-		x
Export Import					
1. Provide the path and file nar 2. Click the Import button.	me of the Alerts file. Use the '' butt	on to browse and locate the import file.			
Options	Location				
<ul> <li>Category</li> </ul>	Import E-mail settings				
O Filters	Set Active <ul> <li>Only if notifications set</li> </ul>	This setting is applicable only for imports from Leg Alert files. For v7, the active status will be set bas	acy (v6x) ed on		
<ul> <li>Alerts</li> </ul>	<ul> <li>By default</li> </ul>	"Active" key available in the configuration section	Ι.		
<ul> <li>Systems and Groups</li> </ul>	Watchlist Configuration				
O Token Value	✓ Import Watchlist configurati	on			
O Reports	This setting is applicable only for Note: If this option is enabled the on the console where the alerts	or alerts which have Advanced watchlist configured ne user should make sure the watchlist groups are a s are imported.	vailable		
O Behavior Correlation					
	Source :				
	*.isalt				
		Import		Clos	e

- 2. In the Browse window, locate the Alerts\_ Microsoft Intune.isalt file, and then click on the Open button.
- **3.** To import the alerts, click on the **Import** button.
- 4. EventTracker displays a successful message on successfully importing the selected file in Alerts.



5. Click OK, and then click Close.

## 4.3 Knowledge Objects (KO)

1. In the EventTracker Manager console, navigate to the Admin drop-down menu and click Knowledge Objects.

Ξ	Event <b>Tracker</b> ⊕					.▲ Admin•	Tools <del>-</del>
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٥			Alerts	Correlation	🔍 IP Lookup Configuration	QQ Users	
	0	1	Behavior Correlation Rules	Diagnostics	🔅 Knowledge Objects	r Weights	
k			🇞 Behavior Correlation Settings	🔛 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Co USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
			• Category	FAQ Configuration	Report Settings		
	Attacker			- News			

2. In the Knowledge Objects interface, click on the Import I button as shown in the below image.

11	Knowledge Obj	jects		🕈 / Admin / Knowledge Objects
Q 	Search objects	Q	Q. Activate Now	Objects 🕀 📳 🏦 🌣
	Groups	<b>⊕ ∅</b> Î		<u>۴</u>
	E Cylance			
	EventTracker			

3. In the Import window, click Browse and locate the file named KO\_ Microsoft Intune.etko.





4. Select the check box next to the browsed file and then click on the  $\mathbb{T}$  Import button.

Import			×
Select	file		Frowse Upload
	Object name	Applies to	Group name
	Microsoft Intune	Microsoft Intune	Microsoft Azure
			Import Close

5. EventTracker displays a successful message on successfully importing the selected file in Knowledge Objects.





### 4.4 Reports

1. In the Import tab, choose the Reports option and select New (\*.etcrx).

\$	Export Import Utility	x
Export Import		
Provide the path and file name Click the Import button Note : If report(s) contains temp Options	ne of Schedule Report file. Use the '' button to browse and locate the import file. slate, first import template and proceed with exportimport utility. Location	
Category Filters Alerts	Legacy (*issch)     New (*.etcnx)	
<ul> <li>Systems and Groups</li> <li>Token Value</li> </ul>	Source : *issch	
Reports     Behavior Correlation		
	Import	

2. In the Source field, click Browse and locate the file named Reports\_ Microsoft Intune.etcrx and select all the check boxes.

lable reports					
e	F	requency Show all	· Q Q	-	
Title		Sites	Groups	Systems	Frequen
EDIT Microsoft Intune - Addit activitie	ile ile				Undefined



- 3. Then, click on the Import  $\mathbb{T}$  button to import the selected files in report.
- 4. EventTracker displays a success message on successful importing of the selected file in **Reports**.



### 4.5 Dashboard

The following steps are specific to EventTracker 9.3 and later.

1. Open EventTracker in a browser and login.

88	Home			
٩	My Dashboard			
R	Threats		1	
	Incidents	ntry point	Indicators of Compromise USB activities, New services or software install	
	Behavior Correlation			
	Change Audit			_
	Compliance		Contraction of	

- 2. From the Home panel, navigate to My Dashboard.
- 3. In the My Dashboard interface, click on the Import  $\mathbb{T}$  button as shown below.

Event <b>Tracker</b> ⊕	4	Admin <del>-</del>	Tools <del>-</del>	💽 ETAdmin *
My Dashboard		A	/ Dashboard	i / My Dashboard
		+	g @ 🌣	1 3 0

4. In the Import window, browse and import the dashboard file Dashboards\_ Microsoft Intune.etwd and select the Select All checkbox.



5. Then, click Import as shown below.

Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.
🖆 Browse Upload
Available widgets
Select All
Microsoft Intune - Activi Microsoft Intune - Audit
Microsoft Intune - Device Microsoft Intune - Device
Microsoft Intune - Audit
Import Close

6. The EventTracker displays the success message on successful import of the dashlet files.

Selected dashlets impo	rted successfully.
	ОК

7. Then, in the **My Dashboard** interface click on the Add ⊕ button to add dashboard.





8. Choose the appropriate name for the Title and Description and click Save.

Add Dashboard		
Title		
Microsoft Intune		
Description		
Microsoft Intune		
	Save	Delete Cancel

9. In the My Dashboard interface click (a) to add dashlets.

My Dashboa	rd
Microsoft I	,

**10.** Search and select the newly imported dashlets and click **Add**.

Customize dashlets				×
Microsoft intune			Q	
Microsoft Intune - Activities by	Microsoft Intune - Audit activiti	Microsoft Intune - Audit activiti	Microsoft Intune - Devices by c	
Microsoft Intune - Devices details				
			Add Delete Close	:



# 5 Verifying Microsoft Intune Knowledge Packs in EventTracker

### 5.1 Categories

- 1. Log in to the EventTracker console.
- 2. Navigate to the Admin drop-down menu and click Category.

≡	Event <b>Tracker</b> ⊕					🐥 🛛 Admin 🗸	Tools <del>-</del>
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dash
q			Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	T Weights	
<b>•</b>			🗞 Behavior Correlation Settings	Event Filters	😟 Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Co USB activities, New ser	Casebook Configuration	Eventvault	🧭 Parsing Rules		
			etegory €	FAQ Configuration	Report Settings		
	Attacker			- News			

3. In the Category Tree, scroll down and expand the Microsoft Azure group folder to view the imported category.



#### 5.2 Alerts

1. Login to EventTracker and navigate to the Admin drop-down menu, and then click Alerts.

≡	Event <b>Tracker</b> ⊕					🔎 Admin-	Tools <del>+</del>
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashi
a		_	Alerts	© Correlation	🔍 IP Lookup Configuration	Q Users	
	0	2	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	T Weights	
<b>•</b>			🇞 Behavior Correlation Settings	🐨 Event Filters	O Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Co USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
			e <sup>®</sup> Category	FAQ Configuration	Report Settings		
	Attacker			- News			

2. In the Alerts interface, navigate to the **Search** field and type **Microsoft Intune** and then click on the **Go** button.

**3.** The Alerts Management interface will display all the imported alerts.



- **4.** To activate the imported alert, toggle the **Active** switch.
- **5.** EventTracker displays success message box.

Successfully saved configuration.  Prevent this page from creating additional dialogs	
ОК	

6. Click OK, and then click on the Activate Now button.

NOTE: Specify the appropriate system in alert configuration for better performance.

## 5.3 Knowledge Objects

1. In the EventTracker web interface, navigate to the Admin drop-down menu and click Knowledge Objects.

≡	Event <b>Tracker</b> ⊕					🐥 🛛 Admin-	Tools <del>-</del>
	Home		Street Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a			Alerts	Correlation	🔍 IP Lookup Configuration	QQ Users	
	0	1	Behavior Correlation Rules	A Diagnostics	Knowledge Objects	T Weights	
×.			🗞 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	USB activities, New sen	Casebook Configuration	C Eventvault	🧭 Parsing Rules		
			o[ <sup>®</sup> Category	FAQ Configuration	Report Settings		
	Attacker			<ul> <li>News</li> </ul>			

2. In the Knowledge Object tree, expand the Microsoft Azure group folder to view the imported Knowledge Objects.

Groups	🕂 🧭 🗓
Microsoft Azure	
Azure App Service	Ø 🗓

3. Click Activate Now to apply the imported Knowledge Objects.

#### 5.4 Reports

1. In the EventTracker web interface, navigate to the Reports menu in the left panel and click Report Configuration.

≡	Event <b>Tracker</b> #			
**	Home			
Q 	Report Configuration		1	
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install	
	Explorer AttacKer			-

2. In the **Reports Configuration** interface, select the **Defined** option.

3. Click the **Microsoft Azure** group folder to view the imported reports.



#### 5.5 Dashboard

1. In the EventTracker console, navigate to the Home button in the left panel and click My Dashboard.

	Home
Dashb	My Dashboard
	Threats
	Incidents

**2.** In the **Customize dashlets** window, type **Microsoft Intune** in the Search field and click **Search**. You will see the following screen.

Customize dashlets			×
Microsoft intune			Q
Microsoft Intune - Activities by	Microsoft Intune - Audit activiti	Microsoft Intune - Audit activiti	Microsoft Intune - Devices by c
Microsoft Intune - Devices details			
			Add Delete Close



#### **About Netsurion**

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion <u>Managed Threat Protection</u> combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion <u>Secure Edge Networking</u> delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all 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 <u>Twitter</u> or <u>LinkedIn</u>.

#### **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 MSPs 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