

Integration Guide

Integrate Azure Active Directory with EventTracker

Publication Date:

August 09, 2022

Abstract

This guide provides instructions to configure the Knowledge Packs in EventTracker to receive the logs from Azure Active Directory. The Knowledge Pack contains alerts, reports, dashboards, categories, and knowledge objects.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or later and Azure Active Directory.

Audience

This guide is for the administrators responsible for configuring the Knowledge Packs in EventTracker.



Table of Contents

1	Ove	erview4	
2	Pre	requisite4	
3	Eve	ntTracker Knowledge Packs4	
	3.1	Category	
	3.2	Alerts	
	3.3	Reports	
	3.4	Dashboard	I
4	Imp	oorting Azure Active Directory Knowledge Packs into EventTracker9	I
	4.1	Category10	I
	4.2	Alerts	
	4.3	Reports	
	4.4	Knowledge Objects (KO)	,
	4.5	Dashboard15	
5	Ver	ifying Azure Active Directory Knowledge Packs in EventTracker17	
	5.1	Category17	
	5.2	Alerts	,
	5.3	Reports19	ı
	5.4	Knowledge Objects (KO)	ł
	5.5	Dashboard	

1 Overview

Azure Active Directory (Azure AD), an aspect of Microsoft Entra, is an enterprise identity service that offers single sign-on, multifactor authentication, and conditional access to help protect against cybersecurity threats. Azure AD uses strong authentication and risk-based adaptive access policies to help protect access to resources and data.

Netsurion facilitates monitoring events from the Azure Active Directory. The dashboard, categories, alerts, and reports interface in Netsurion's threat protection platform, EventTracker, benefits in tracking azure active directory activities and changes to detect any suspicious activities performed on the Azure Active Directory.

2 Prerequisite

- EventTracker version 9.3 or later must be installed and configured to receive logs.
- Configure Azure Active Directory to forward logs to EventTracker.

Note

Refer to <u>How-To</u> guide to configure Azure Active Directory to forward logs to EventTracker.

3 EventTracker Knowledge Packs

After the logs are received by the EventTracker Manager, configure the Knowledge Packs into EventTracker.

The following Knowledge Packs (KPs) are available in EventTracker.

3.1 Category

Azure Active Directory – Audit operations: This category of the saved search will allow the users to parse the events that are specific to the audit level operations such as updating and deleting of the users in the Azure Active Directory.

Azure Active Directory – Sign in activities: This category of the saved search will allow the users to parse the events that are specific to the sign in operations in the Azure Active Directory.

3.2 Alerts

Azure Active Directory - Sign in failure: This alert indicates that an attempt was made to sign in without proper credentials.

Azure Active Directory - Sign in blocked: This alert indicates that an attempt was made to sign in from a malicious IP or is not trusted by the Azure Active Directory devices.



Azure Active Directory - User risk detection: This alert indicates that the user attempted a risky event in the Azure Active Directory.

Azure Active Directory – Audit operations failure: This alert provides the details of the failed attempts made to any update operations in the Azure Active Directory.

3.3 Reports

Azure Active Directory – Audit Operations: This report provides a detailed summary of the audit and performance activities in Azure Active Directory. It includes Tenant ID, User Mail ID, Activity Type and their Result, Activity Time, Caller IP.

LogTime	Activity Time	Caller IP	Activity Type	Result	Tenant ID	User Mail ID
07-15-2022 11:18:18 AM	2022-07-15T11:18:17.5894027+00:00	127.0.0.1	Update device	success	0ac05f5c-4238-4951-89a8-2b5e518805f0	
07-15-2022 12:25:53 PM	2022-07-15T12:25:52.9164149+00:00	127.0.0.1	Update device	success	0ac05f5c-4238-4951-89a8-2b5e518805f0	
07-15-2022 10:16:37 PM	2022-07-15T22:16:37.0842489+00:00		Change user password	success	0ac05f5c-4238-4951-89a8-2b5e518805f0	abcdef@eventtracker.onmicrosoft.co m
07-15-2022 10:16:37 PM	2022-07-15T22:16:37.0842489+00:00		Update StsRefreshTokenValidFron Timestamp	n success	0ac05f5c-4238-4951-89a8-2b5e518805f0	abcef@eventtracker.onmicrosoft.com
07-15-2022 10:36:27 PM	2022-07-15T22:36:27.351443+00:00		Update user	success	0ac05f5c-4238-4951-89a8-2b5e518805f0	nsdfgh@eventtracker.com

Azure Active Directory – Sign in Failures: This report provides a detailed summary of the sign in failure activities in Azure Active Directory. It includes Source IP, Tenant ID, User Mail ID, Authentication Type, etc.

LogTime	Source IP	Operating System	i Tenant ID	User Name	User Mail ID	System Name	Authentication Type	Failure Reason	Trusted By	Sign In Category
07-13-2022 11:26:25 A	M 211.12.12.112	Windows 10	0ac05f5c-4238-4951-89a8-2bdsfdg530	contoso	contoso@eventtracker.com	NTETSYSNAME1	singleFactorAuthentication	Other	Azure AD registered	NonInteractive UserSignInLogs
07-13-2022 11:26:26 A	V 127.0.0.1	Windows 10	034rf5c-4238-4951-89a8-2b5e518805f0	john	john@eventtracker.com	SYSNAME2	singleFactorAuthentication	Other	Azure AD registered	NonInteractive User SignInLogs
07-13-2022 11:26:29 A	M 234.12.12.45	Windows 10	0ac05f5c-4238-4951-89a8-2b5e518805f0	smith	smith@eventtracker.com	SYSNAME3	singleFactorAuthentication	Other	Azure AD registered	NonInteractive UserSignInLogs
07-13-2022 11:26:30 A	M 234.45.23.323	Windows 10	0ac05f5c-4238-4951-89a8-2b5e5dsff4f0	samanta	samanta@eventtracker.com	SYSNAME4	${\it singleFactorAuthentication}$	Other	Azure AD registered	NonInteractive User SignInLogs
07-13-2022 11:26:30 A	M 211.12.12.123	Windows 10	0ac05f5c-4238-4951-89a8-2bdst5g05f0	nayana tara	nayana@eventtracker.com	SYSNAME5	singleFactorAuthentication	Other	Azure AD registered	NonInteractiveUserSignInLogs

Azure Active Directory – Sign in Success: This report provides a detailed summary of the sign-in success activities in the Azure Active Directory. It includes Source IP, Tenant ID, User Mail ID, Authentication Type, etc.

LogTime	Authentication Type	Application	Source IP	Operating System	Activity Type	Tenant ID	Trusted By
08-05-2022 11:42:44 AM	multiFactorAuthentication	Rich Client 4.42.1.0	172.12.21.21	Windows10	Sign-in activity	0ac05f5c-4238-4951-89a8- 2b5f0	Azure AD registered
08-05-2022 11:43:50 AM	singleFactorAuthentication	Edge 18.19044	172.12.21.22	Windows 10	Sign-in activity	0ac05f5c-4238-4951-89a8- 2b5f1	Azure AD registered
08-05-2022 11:43:51 AM	multiFactorAuthentication	Edge 18.19044	172.12.21.23	Windows 10	Sign-in activity	0ac05f5c-4238-4951-89a8- 2b5f2	Azure AD registered
08-05-2022 11:43:51 AM	multiFactorAuthentication	Edge 18.19044	172.12.21.24	Windows 10	Sign-in activity	0ac05f5c-4238-4951-89a8- 2b5f3	Azure AD registered
08-05-2022 11:43:52 AM	multiFactorAuthentication	Edge 18.19044	172.12.21.25	Windows 10	Sign-in activity	0ac05f5c-4238-4951-89a8-	Azure AD registered



3.4 Dashboard



Azure Active Directory - Sign in failures by source IP

Azure Active Directory - Noninteractive sign in failures by user









Azure Active Directory - Sign in failures by error codes



Netsurion®



Azure Active Directory - Activity overview by operations

Azure Active Directory – Sign in by application





4 Importing Azure Active Directory Knowledge Packs into EventTracker

Import the Knowledge Pack items in the following sequence.

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



4.1 Category

1. In the **Import** tab, click **Category**, and then click the **Browse** button to locate the file.

<u>в</u>			Ехро	rt Impo	rt Utility				-		x
Export	nport										
1. Prov 2. Click	de the path and file name the Import button.	e of the Categori	ies file. Use ti	he '' butto	on to brows	e and locate	the import fi	le.			
Option	s	Location									
⊙ Ca	tegory										
⊖ Filt	ers										
O Ale	rts										
⊖ Sy	stems and Groups		Source :								
0 To	ken Value										
O Re	ports										
O Be	havior Correlation										
											_
								Import		Clos	e

- 2. In the Browse window, locate the Categories_Azure Active Directory.iscat file and click Open.
- **3.** To import the category, click **Import**.
- 4. EventTracker displays a success message on successfully importing the selected file in **Category**.



5. Click **OK** or the **Close** button to complete the process.



4.2 Alerts

1. In the Import tab, click Alerts, and then click the Browse button to locate the file.

<u>ц</u>	Export In	nport Utility	- 🗆 X
Export Import			
1. Provide the path and file name 2. Click the Import button.	e of the Alerts file. Use the '' butto	on to browse and locate the import file.	
Options O Category	Location Import E-mail settings		
⊖ Filters	 Set Active Only if notifications set 	This setting is applicable only for imports from Lega Alert files. For v7, the active status will be set base	acy (v6x) ed on
Alerts	 By default 	"Active" key available in the configuration section	
 Systems and Groups 	Watchlist Configuration		
O Token Value	Import Watchlist configuration This setting is applicable only for Nature 16 this setting is applicable only for	on or alerts which have Advanced watchlist configured	
⊖ Reports	on the console where the alerts	are imported.	Valiable
O Behavior Correlation			
	Source :		
	*.isalt		
L		Import	Close

- 2. In the Browse window, locate the Alerts_ Azure Active Directory.isalt file, and then click Open.
- **3.** To import the alerts, click **Import**.
- 4. EventTracker displays a success message on successfully importing the selected file in Alerts.



5. Click **OK** or the **Close** button to complete the process.

4.3 Reports

1. In the Import tab, click Reports and then click New (*.etcrx).

1	Export Import Utility	_	- x
Export Import 1. Provide the path and file name. 2. Click the Import button Note : If report(s) contains temple Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation 	of Schedule Report file. Use the '' button to browse and locate the import file. ite, first import template and proceed with exportimport utility. Location C Legacy (* issch) Source : *issch *issch		
	Import		Close

2. In the **Reports Import** window, click **Select file** to locate the **Reports_Azure Active Directory.etcrx** file.

		pois_neare nuive preux	ory erox					Select file	
able rep	orts	Frequency	Show all	-	Q	Q			
	Title	Sites			Groups		System	ms	Frequenc
EDIT	Azure Active Directory - Audit Operations	Versionserver		Default			A TRANSPORT		Undefined
EDIT	Azure Active Directory - Sign in Failures	DUCHMAL-OUDF CRV		Default			-Vertesch0-000500	la 4200 4301 000m	Undefined



- 3. Select the check box of all the files and click the **Import** \mathbb{T} button to import the selected files.
- 4. EventTracker displays a success message on successful importing of the selected file in **Reports**.

Export Import Utility	x
Selected reports configurations are imported successfully	
ОК	

5. Click **OK** or the **Close** button to complete the process.

4.4 Knowledge Objects (KO)

1. In the EventTracker Manager console, hover over the Admin menu and click Knowledge Objects.

≡	Event Tracker ⊕					🐥 🛛 Admin•	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
۵		_	Alerts	Correlation	Q IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	1 Diagnostics	💮 Knowledge Objects	r Weights	
			🗞 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		
				FAQ Configuration	Report Settings		
	Attacker			- News			

2. In the Knowledge Objects interface, click the Import \mathbb{T} button to import the KO files.





3. In the Import window, click Browse and locate the KO_ Azure Active Directory.etko file.



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

Import			×
Select	file		Deproved Upload
~	Object name	Applies to	Group name
	Azure Active Directory	Azure Active Directory	Microsoft Azure
			Import Close

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



6. Click **OK** or the **Close** button to complete the process.

4.5 Dashboard

1. Log in to the **EventTracker** web interface and go to **Dashboard** > **My Dashboard**.

	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. In the My Dashboard interface, click the Import I button to import the dashlet files.

Event Tracker ⊕	4	Admin -	Tools -	💽 ETAdmin •
My Dashboard		A	/ Dashboard	i / My Dashboard
		•	g 🕲 🌣	1 3 0

3. In the Import window, click Browse to locate the Dashboards_ Azure Active Directory.etwd file and then click Upload.



4. Click the **Select All** checkbox to select all the dashlet files and click **Import** to import the selected dashlet files.

nport		
Note: If dashlet configured using dashlet.	persisted report, first import the report and proceed with	importing
	🗁 Browse	Upload
Available widgets Select All		
Azure Active Directory	Azure Active Directory	
Azure Active Directory	Azure Active Directory	
Azure Active Directory	Azure Active Directory	
	Impo	rt Close

5. The EventTracker displays the success message on successfully importing the dashlet files.



6. Then, in the My Dashboard interface, click the Add 🕀 button to add the dashboard.

My Dashboard					♠ /	' Dasł	nboar	d / M	y Das	shboai				
CheckPoint Trer	nd Micr	Microsoft						Ð	Ø	9	\$	1	Ŧ	3



7. In the Add Dashboard interface, specify the Title and Description and click Save.

Title	
Azure Active Directory	
Description	
Azure Active Directory	
	Save Delete Cancel

- From the newly created dashboard interface (for example, Azure Active Directory), click the Configuration Sutton to add the Azure Active Directory dashlets.
- 9. Search and select the newly imported dashlets and click Add.

Customize dashlets			×
Azure Active			Q
Azure Active Directory - Activity	Azure Active Directory - Nonint	Azure Active Directory - Sign in	Azure Active Directory - Sign in
$\hfill\square$ Azure Active Directory - Sign in	Azure Active Directory - Sign in		
			Add Delete Close

5 Verifying Azure Active Directory Knowledge Packs in EventTracker

5.1 Category

1. In the EventTracker web interface, hover over the Admin menu and click Category.

Ξ	Event Tracker ⊕					🐥 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashi
a			Alerts	Correlation	Q IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	1 Weights	
			🗞 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 **Category** interface, under the **Category Tree** tab, click the **Microsoft Azure** group folder to expand and see the imported categories.

Category	
Category Tree	Search
All Categories Microsoft	Azure e Active Directory - Audit operations e Active Directory - Sign-in activities

5.2 Alerts

1. In the EventTracker web interface, hover over the Admin menu and click Alerts.

≡	Event Tracker ⊕					🔎 🗚 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	📌 / Dasht
٩			Alerts	Correlation	Q IP Lookup Configuration	QQ Users	
	0	2	Behavior Correlation Rules	Diagnostics	💮 Knowledge Objects		
~			🇞 Behavior Correlation Settings	😴 Event Filters	Manager	🔲 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
		_	● Category	FAQ Configuration	Report Settings		
	Attacker			- News			

- 2. In the Alerts interface, type Azure Active Directory in the search field, and click the Search soutton.
- 3. The Alerts interface will display all the imported Azure Active Directory alerts.

Ð	Click 'Activate Now' after making all changes		
	Alert Name 🔨	Threat	Active
	နူနို Azure Active Directory - Audit operation failure	•	
	နူဂ္ဂို Azure Active Directory - Sign in blocked	•	
	နိုဂ္ဂို Azure Active Directory - Sign in failure	•	
	နိုဂ္ဂိ Azure Active Directory - User risk detection	•	

4. To activate the imported alerts, click **Active**, which is available next to the respective alert name.

5. EventTracker displays a success message on successfully configuring the alerts.



6. Click **OK** and click **Activate now** to activate the alerts after making the required changes.

Note

You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

Note

In the Alert Configuration interface, specify the appropriate System for better performance.

5.3 Reports

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

	Event Tracker 🕀			
	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, click **Defined**.
- 3. In the search field, type Microsoft Azure and click Search to search for the Azure Active Directory files.

4. EventTracker displays the reports for Azure Active Directory.



5.4 Knowledge Objects (KO)

1. In the EventTracker web interface, hover over the Admin menu and click Knowledge Objects.

	Event Tracker ⊕					.▲ Admin•	Tools •
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
Q		_	Alerts	© Correlation	🔍 IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	Diagnostics	· 🔆 Knowledge Objects	(Weights	
.			🗞 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	P Eventvault	Parsing Rules		
				FAQ Configuration	Report Settings		
	Attacker			- News			

2. In the Knowledge Object interface, under Groups tree, click the Microsoft Azure group to expand and view the imported Knowledge objects.

Knowledge Obje	ects	
Search objects	Q Q	Activate Now
Groups	🕀 🧭 🗓	
Microsoft Azure		
Azure Active Directory	0	

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



5.5 Dashboard

In the EventTracker web interface, go to Home > My Dashboard, and click the Customize dashlets
 button.



- 2. In the **Customize dashlets** interface, search for **Azure Active Directory** in the search field.
- **3.** The following Azure Active Directory dashlet files will get displayed.

Customize dashlets ×				
(Azure Active			Q
	Azure Active Directory - Activity	Azure Active Directory - Nonint	Azure Active Directory - Sign in	Azure Active Directory - Sign in
	Azure Active Directory - Sign in	Azure Active Directory - Sign in		
				Add Delete Close



About Netsurion

Netsurion[®] delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at <u>netsurion.com</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