

Integrate Microsoft Azure

EventTracker v.9x and above

Publication Date: April 12, 2019

Abstract

This guide provides instructions to configure Azure to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Azure Activity, Azure Intune and Keyvault.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 9.x and later, and Microsoft Azure.

Audience

IT Admins, Azure administrators and EventTracker users who wish to forward logs to EventTracker Manager and monitor events using EventTracker Enterprise.

The information contained in this document represents the current view of Netsurion. on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

Abstract	1
Scope	1
Audience	1
Overview	3
Prerequisites	3
Configure Azure to forward logs to EventTracker Eventtracker Integrator for Azure	3 3
Register Application with your Azure Active Directory Tenant	8
Grant the Azure AD Application Reader Access to the Subscription	. 13
To Enable Auditing for Keyvault in the Azure portal	. 13
To find your Azure tenant ID in the Azure AD portal	. 16
Verify Azure Integration	. 17
EventTracker Knowledge Pack (KP) Reports	. 18 . 18
Sample Dashboards	. 21
Import Knowledge Pack into EventTracker Knowledge Objects	. 25 . 26
Flex Reports	. 27
Dashlets	. 29
Verify Knowledge Pack in EventTracker Knowledge Object	. 31 . 31
Flex Reports	. 32
Dashlets	. 32

Overview

EventTracker Knowledge pack for Microsoft Azure captures important and critical activities in Azure. Monitoring these activities is critical from a security aspect and is required for compliance and operational reasons. The dashboards, reports will help you in getting deeper insights to analyze various security use cases like azure resource and service activities and changes.

EventTracker helps you to monitor day to day activities of Azure resource activities, Intune and Keyvault audit activities.

Prerequisites

- EventTracker v9.x or above should be installed.
- PowerShell 5.0 should be installed on EventTracker Manager.
- App should be registered in Azure AD with Azure Management API and Microsoft graph API permission. Instructions are mentioned <u>here</u>.
- Please enable following URL, if there is any web filter or firewall in between:
 - https://graph.microsoft.com
 - https://login.windows.net
 - https://manage.office.com

Configure Azure to forward logs to EventTracker

- 1. To create "**Microsoft graph** and **Azure Management API**" enabled app in Azure AD, please follow the steps mentioned <u>here</u>.
- 2. After successful creation of user and application, run the Azure Integrator.

EventTracker Integrator for Azure

You need to follow these steps, if you want to create application.

- 1. Please contact EventTracker Support for Azure Integration package.
- 2. Run executable file "Azure Integrator.exe".

3	Azure Integrator
Actionable Security Intelligence	This will help to integrate Azure with EventTracker. Follow the following intructions: Click Browse button and navigate to location. Select the location. Click on Install button.
cker	Destination folder C:\Program Files (x86)\AzureIntegrator V Browse Installation progress
	Install Cancel



After launching integrator, it will check for PowerShell compatibility. If it is found compatible, integrator will allow you to configure Azure. Otherwise, update PowerShell on the EventTracker Manager machine.

3. Please follow the <u>Register Application section</u> and permission sections for application creation respectively. Fill the details in the Application.

🚯 Azure Integrator		201	\times
API Client Id	sdfgdgdfg -sdfssd-sdfsasd-afdsfasdfad		
API Key	********************************		
Redirect URL	http://localhost		
Tenant Id	bjdsfsdf-asfdgbg-asdfadf -asdfbbgfewrw		
Subcrition ID	785452a4sdf-454-454784-789asdfsdafdsf3		
Organisation Name	contoso.com		
Group Name	contos		
Select the Azure Products to	Monitor		
Azure Monitor			
T Azure Intune			
🗖 Azure Keyvault			
OK Canc	el		
			111

Figure 2

- 4. Fill the details of the app registered in Azure AD with Microsoft graph and Azure Management API permission. If user doesn't have app registered in Azure AD, please follow the instructions mentioned <u>here</u>.
- 5. Provide the tenant ID for the enterprise. Please follow the instruction mentioned <u>here</u>, if tenant ID is not known.
- 6. Once you have filled the appropriate fields in the forms, it will enable the **Select Azure Product** checkboxes.
- 7. Select the Check box which is required to monitor.
- 8. If Azure Intune has been selected, it will pop up the browser window to authorize the client. Login with Azure administrator account to authorize the application.



9. If the browser window is not popped-up, it will pop up a form with URL. Click "Copy URL to Clipboard" button.

🔁 Azure Integrator	—		\times
Authorization URL			
I%20DeviceManagement	ntApps.Rea	d.All&stat	e=12345
Copy URL to Clipboard			
Redirected Auth URL			
ОК			
			//

- 10. Once the link is copied, paste it in your web browser and login with azure administrator credentials.
- 11. If the application is authorized, the page will redirect to your localhost or redirect to the URL, which you are given.
- 12. Copy the redirected URL from the browser and paste it in **Redirected Auth URL** text box and click OK to proceed further.
- 13. If Azure Keyvault Auditing is enabled, please provide the azure Keyvault auditing storage account and storage account resource group.



🚹 Azure Integrator		1000	×
API Client Id	sdfgdgdfg -sdfssd-sdfsasd-afdsfasdfad		
API Key	***********		
Redirect URL	http://localhost		
Tenant Id	bjdsfsdf-asfdgbg-asdfadf -asdfbbgfewrw		
Subcrition ID	785452a4sdf-454-454784-789		
Organisation Name	contoso.com		
Group Name	contos		
Select the Azure Products to M	lonitor		
Azure Monitor			
Azure Intune			
🔽 Azure Keyvault			
Storage Account Name	audit_storage_keyvault		
Storage resource Group	Keyvault_resource_group		
OK Cancel	1		
L			

- 14. Once you provide all the details in Integrator "OK" button will be enabled.
- 15. Click on **OK** button to complete the Integration.

Register Application with your Azure Active Directory Tenant

If Application has not been registered in Azure AD, please follow the below procedure. This procedure should be carried out by a user having **Global Administrator** rights in Azure.

- 1. Sign in to the <u>Azure portal</u>.
- 2. If your account gives you access to more than one, click your account in the top right corner, and set your portal session to the desired Azure AD tenant.
- 3. In the left-hand navigation pane, click the **Azure Active Directory** service, click **App registrations**, and click **New application registration**.

Micro	osoft Azure developer - App registra	tions
≡	developer - App registrations Azure Active Directory	
+	Overview	+ New application registration 🗄 Endpoints 🗙 Troubleshoot
	Quick start	To view and manage your registrations for converged applications, please visit the Microsoft Application Console.
۲	MANAGE	Search by name or Appld
	R ^R Users and groups	DISPLAY NAME
3	Enterprise applications	AdminUterApp
٢	Devices (Preview)	
3	App registrations	We WebApp-OpeniDConnect-Dotiver
Q	Application proxy	ni mwapuau
	Licenses	
	Azure AD Connect	
	Domain names	
	Mobility (MDM and MAM)	
	Password reset	



- 4. When the Create page appears, enter your application's registration information:
 - Name: Enter an appropriate application name
 - Application type: Select Web app / API
 - Sign-On URL: Enter http://localhost





- 5. When finished, click Create. Azure AD assigns a unique Application ID to your application, and you are taken to your application's main registration page. Please note down the Application ID.
- 6. To add permission(s) to access resource APIs from your client,
 - Click the **Required Permissions** section on the **Settings** page. ٠
 - Click the Add button. .
 - Click Select an API to select the type of resources you want to pick from and then select . Microsoft Graph.





Figure 7

- 7. After selecting Microsoft Graph, add following application permissions:
 - Read all identity risky user information
 - Read all usage reports.
 - Read your organization security events.



Enable Access Microsoft Graph		
🔒 Save 🗴 Delete		
Read all access reviews	Yes	
 Read all identity risky user information 	🔮 Yes	
Read and create online meetings (preview)	🤣 Yes	
 Read all usage reports 	🥑 Yes	
Read all users' relevant people lists	🤣 Yes	
Flag chat messages for violating policy	🤣 Yes	
Read all chat messages	🤣 Yes	
Read all channel messages	🤣 Yes	
Flag channel messages for violating policy	🤣 Yes	
Read and write all applications	🤣 Yes	
Manage apps that this app creates or owns	🤣 Yes	
Read online meeting details (preview)	🤣 Yes	
Access media streams in a call as an app (preview)	🤣 Yes	
Join group calls and meetings as a guest (preview)	🤣 Yes	
Join group calls and meetings as an app (preview)	🤣 Yes	
Initiate outgoing group calls from the app (preview)	🤣 Yes	
Initiate outgoing 1:1 calls from the app (preview)	🤣 Yes	
Read all audit log data	🤣 Yes	
 Read your organization's security events 	🕑 Yes	
Read and update your organization's security events	📀 Yes	
Read and write items in all site collections (preview)	🤣 Yes	

Figure 8

Netsurion... EventTracker

8. Click Grant permissions after selecting Required permissions. For granting permissions, user(s) with "Global Administrator" privileges are required.

Settings	×	Required permissions			×
		🕂 Add 🏾 🗣 Grant Permissions			
GENERAL		API	APPLICATION PERMI	DELEGATED PERMIS	
Properties >		Microsoft Graph	1	0	-
Reply URLs		Windows Azure Active Directory (Microsoft Azure Act.	. 0	2	
🗳 Owners					
API ACCESS					
👗 Required permissions					

Figure 9

- 9. You are taken to the application's main registration page, which opens the **Settings** page for the application. To add a secret key for your web application's credentials:
 - Click the **Keys** section on the **Settings** page.
 - Add a description for your key.
 - Select Never from expires drop-down.
 - Click **Save**. The right-most column will contain the key value, after you save the configuration. Make note of value generated. This will be used in the integrator as **client secret**.

Micr	osoft Azure developer - App registration	s > NewApplication > Settings > Keys					P Search resources, services and doc
≡	NewApplication Registered app	* ×	Settings >	×	Keys		
+	🗘 Settings 🖌 Manifest 📋 Delete		,D. Alter settings		Save X Discard		
	Essentials A Display name New Application Application type Web app / API Home page https://focalhost	Application IO 8666u272-6006-4803-9060-7a84642c5f76 vogen ov e6455391-a835-4409-ar06-72699c90e414 Manage Application In local directory NewApplication Att settings →	D Hater pattings CONDUX, III Properties >> III Reply URLs >> III Owners >> APLACCESS APLACCESS APLACCESS >>		otscarrion GigCred V	EXPRES	VALUE V liabue will be displayed on save
0 8 4 1			* Keys > TROUBLES-COTING - SUPPORT * Troubleshoot * Troubleshoot * New support request				

Figure 10

10. Please note down the **Application ID** after completing app configuration.

Grant the Azure AD Application Reader Access to the Subscription

- 1. After creating the Azure application (which is similar to a service account), the application needs to be granted Security reader access to the subscription(s) via a service principal object.
- Select Subscriptions -> Your subscription -> Access control (IAM) -> Add -> select the Security Reader role -> type the name of your application registration from the previous step -> select the application when it appears in the results -> click the Save button.

+ Create a resource	Subscriptions 🖈 🗙	Pay-As-You-Go - Access co	ntrol (IAM)		
i∃ All services	+ Add	Search (Ctrl+/)	+ Add 🗈 Remove 🔹 Roles 🕐 Refresh ? Help		Role Ro
- * FAVORITES	Showing subscriptions in splunk. Don't see a subscription?	Overview	Name Ø Type Ø	Role 🛛	Assign access to a Azure AD user, group, or application
All resources	My role Status O	Access control (IAM)	Search by name or email All V	4 selected V	Select 0
C Recent	7 selected V 3 selected V	X Diagnose and solve problems	Role ~		azuremoni
🔕 App Services	Search to filter items	COST MANAGEMENT + BILLING	15 items (3 Users, 12 Service Principals) NAME TYPE	ROLE	AzureMonitor
Q Virtual machines (classi	SUBSCRIP 14 SUBSCRIPTION ID 14	Invoices			
Virtual machines	Pay-As-You	 Cost analysis 	API MANAGEMENT SERVICE CONTRIBUTOR		
👼 SQL databases		External services	· · · · · · · · · · · · · · · · · · ·	API Management Servix	
Cloud services (classic)		Payment methods	CONTRIBUTOR		
Subscriptions		Partner information	CONTRIBUTOR		
Azure Active Directory		SETTINGS	•	Contributor O	Colorial markets



To Enable Auditing for Keyvault in the Azure portal

Before you can enable this, you need a storage account. You can use your existing storage account or create a new storage account in resource group to store the logs.

- 1. Sign in to the <u>Azure portal</u>.
- 2. In the Microsoft Azure portal, click Keyvault.
- 3. Navigate to the **Diagnostic logs** under the **MONITORING.**





Figure 12

- 4. Click "Turn on diagnostics"
- 5. Enter the Name for the setting. Example (Keyvault_logger)



6. Select "Archive to Storage Account" and pick the storage account you have just created.

	Suco secon						
Save	X Discard	Delete					
0	You'll be char diagnostics to	irged normal data r to a storage accour	rates for stora st.	ge and trans	actions when	you send	
Name							~
Archiv	ve to a storage	account					
Storage	account						>
_ Stream	m to an event h	hub					
Stream	m to an event h to Log Analytic	nub					
] Stream	m to an event h to Log Analytic	nub					
Stream	n to an event h to Log Analytic AuditEvent	nub		Retention (d	əys) O		0
Stream	m to an event h to Log Analytic AuditEvent	nub Es		Retention (d	8y%) O		0
Stream	n to an event h to Log Analytic AuditEvent AllMetrics	nub IS		Retention (d	ays) O ays) O		0

Figure 13



Diagnostics settings	×
Save X Discard 📋 Delete	
You'll be charged normal data rates for sto diagnostics to a storage account.	rage and transactions when you send
* Name	
logging	~
Archive to a storage account	
Storage account	>
Stream to an event hub	
Send to Log Analytics	
LOS	
V AuditÉvent	Retention (days)
METRIC	
AllMetrics	Retention (days)
Retention only applies to storage account.	

Figure 14

- 7. Select the AuditEvent log and Retention days as required.
- 8. Click Save.

If you are enabling Azure Keyvault you have to enable addition role to the storage account for accessing Keyvault log.

- 9. Follow these steps to assign the **Reader** role so that a user can access blobs from the Azure portal. In this example, the assignment is scoped to the storage account:
- 10. In the Azure portal, navigate to your storage account.
- 11. Select **Access control (IAM)** to display the access control settings for the storage account. Select the **Role assignments** tab to see the list of role assignments.
- 12. In the Add role assignment window, select the Reader role.
- 13. From the Assign access to field, select Azure AD Application which we created.
- 14. Save the role assignment.
- 15. Repeat the same procedure to assign Storage Blob Data Reader to the application.

To find your Azure tenant ID in the Azure AD portal

1. Sign in to the <u>Azure portal</u>.



Netsurion EventTracker

- 2. In the Microsoft Azure portal, click Azure Active Directory.
- 3. Under Manage, click Properties. Make note of the value in Directory ID box. This will be used as Tenant ID in the integrator.

Enterprise applications	^	Rave X Discard	
Devices		* Name	
App registrations		Event Iracker Security LLC	
Application proxy		Country or region United States	
🔓 Licenses		Location	
Azure AD Connect		United States datacenters Notification language	
Custom domain names		English	~
Mobility (MDM and MAM)		Global admin can manage Azure Subscriptions	
Company branding		Yes No	
User settings			
Properties			
Notifications settings			

Figure 15

Verify Azure Integration

17

After providing details in Azure Integrator, please follow the steps to verify the Azure integration.

1. Check if the following task is created in Task Scheduler.

🕑 Task Scheduler)
File Action View Help					
🗢 🔿 🙍 🖬 👔 👘					
Task Scheduler (Loca) Task Scheduler Library Lenovo Smicrosoft Symantec Endpoint Pt TVT	Name © [AGIF1256-975F-4112-83CB-E010762D94E0] © Adobe Acrobat Update Task © AWS Logging © Azure Konitor © Azure Monitor © Brave Software Update Task Machine Core © Brave Software Update Task Machine LA	Status Ready Disabled Disabled Disabled Ready Ready Ready	Triggers When the task is created or modified Multiple triggers defined At 1147 AM every day At 7:10PM every day - After triggered, repeat every 1 hour indefinitely. Multiple triggers defined At 11:108 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	Next Run Time 04/06/2019 2:00:00 PM 04/06/2019 11:47:32 AM 04/05/2019 3:10:29 PM 04/06/2019 11:08:06 AM 04/05/2019 11:08:06 AM	Last Run Time 02/17/2017 3:32:25 08/27/2018 8:28:39 12/19/2018 11:47:3 11/30/1999 12:00:0 04/05/2019 12:06:4 04/05/2019 2:08:06
	Gisco AMP Gisco AMP GoventTracker-Attackers EventTracker-DShieldOrgBlockedIPList EventTracker-DshieldOrgBlockedIPList EventTracker-IblockIstBlueTackHigackedIPList EventTracker-IblockIstBlueTackHigackedIPList EventTracker-IblockIstBlueTackHigackedIPList EventTracker-IblockIstBlueTackFigsyWareList EventTracker-IblockIstBlueTackSpyWareList EventTracker-IblockIstBlueTackSpyWareList	Disabled Ready Ready Ready Ready Ready Ready Ready Ready	At 1:55 PM every day - After triggered, repeat every 1 hour indefinitely. At 5:12 PM every day At 5:12 PM on 03/18/2019 - After triggered, repeat every 15 minutes indefinitely.	04/05/2019 2:55:37 PM 04/05/2019 5:12:00 PM	07/11/2018 11:55:3 04/05/2019 10:30:0 04/05/2019 10:30:0 04/05/2019 10:30:0 04/05/2019 10:30:0 04/05/2019 10:30:0 04/05/2019 10:30:0 04/05/2019 2:42:00 >

EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; Reports, Knowledge Objects and Dashboards can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v9.x and later to support Azure monitoring:

Reports

• Azure – Intune Audit Events: This report will provide you information related to Azure Intune Audit Events.

Sample Report:

LogTime	Computer	Activity Date Time	Activity Type	Activity Result	Application Display Name	Category	Activity Operation Type	Log Type	Component Name	User Name	User Type
04/08/2019 06:52:20 PM	AZUREINTUEN_009	2019-03-07T15:50:34.3091045Z	Create MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Create	Create MobileAppAssignment	MobileApp	netadmin@contoso.local	tPro
04/08/2019 06:52:20 PM	AZUREINTUEN_009	2019-03-07T15:51:18.2210346Z	Delete MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Delete	Delete MobileAppAssignment	MobileApp	netadmin@contoso.local	tPro
04/08/2019 06:52:21 PM	AZUREINTUEN_009	2019-03-07T14:47:55.828692Z	Create MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Create	Create MobileAppAssignment	MobileApp	netadmin@contoso.local	tPro
04/08/2019 06:52:21 PM	AZUREINTUEN_009	2019-03-07T14:50:48.0748327Z	Create MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Create	Create MobileAppAssignment	MobileApp	netadmin@contoso.local	tPro
04/08/2019 06:52:21 PM	AZUREINTUEN_009	2019-03-07T14:50:48.0748327Z	Create MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Create	Create MobileAppAssignment	MobileApp	netadmin@contoso.local	tPro
04/08/2019 06:52:22 PM	AZUREINTUEN_009	2019-03-06T22:08:16.3036989Z	SyncWindowsAutopilotDevices WindowsAutopilotSettings	Success	Microsoft Intune portal extension	Enroliment	Action	Syncing Windows Autopilot Devices	Enrollment	netadmin@contoso.local	tPro
04/08/2019 06:52:22 PM	AZUREINTUEN_009	2019-03-07T14:47:55.828692Z	Create MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Create	Create MobileAppAssignment	MobileApp	netadmin@contoso.local	tPro
04/08/2019 06:52:23 PM	AZUREINTUEN_009	2019-03-06T16:32:15.1599439Z	Create MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Create	Create MobileAppAssignment	MobileApp	netadmin@contoso.local	tPro
04/08/2019 06:52:23 PM	AZUREINTUEN_009	2019-03-06T16:32:15.1599439Z	Create MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Create	Create MobileAppAssignment	MobileApp	netadmin@contoso.local	tPro
04/08/2019 06:52:23 PM	AZUREINTUEN_009	2019-03-06T22:08:16.3036989Z	SyncWindowsAutopilotDevices WindowsAutopilotSettings	Success	Microsoft Intune portal extension	Enroliment	Action	Syncing Windows Autopilot Devices	Enroliment	netadmin@contoso.local	tPro
04/08/2019 06:52:24 PM	AZUREINTUEN_009	2019-03-06T16:29:50.0340179Z	Delete MobileApp	Success	Microsoft Intune portal extension	Application	Delete	Delete application.	MobileApp	netadmin@contoso.local	ttPro
04/08/2019 06:52:25 PM	AZUREINTUEN_009	2019-03-06T16:29:50.0340179Z	Delete MobileApp	Success	Microsoft Intune portal extension	Application	Delete	Delete application.	MobileApp	netadmin@contoso.local	tPro
04/08/2019 06:52:25 PM	AZUREINTUEN_009	2019-03-06T16:29:42.6480499Z	Delete MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Delete	Delete MobileAppAssignment	MobileApp	netadmin@contoso.local	tPro
04/08/2019 06:52:26 PM	AZUREINTUEN_009	2019-03-06T16:29:42.6480499Z	Delete MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Delete	Delete MobileAppAssignment	MobileApp	netadmin@contoso.local	tPro
04/08/2019 06:52:26 PM	AZUREINTUEN_009	2019-03-06T16:29:42.6480499Z	Delete MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Delete	Delete MobileAppAssignment	MobileApp	netadmin@contoso.local	tPro
04/08/2019 06:52:27 PM	AZUREINTUEN_009	2019-03-06T16:29:42.6480499Z	Delete MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Delete	Delete MobileAppAssignment	MobileApp	netadmin@contoso.local	tPro
04/08/2019 06:52:27 PM	AZUREINTUEN_009	2019-03-05T22:36:46.2275035Z	Patch MobileApp	Success	Microsoft Intune portal extension	Application	Patch	Modify application.	MobileApp	netadmin@contoso.local	tPro
04/08/2019 06:52:27 PM	AZUREINTUEN_009	2019-03-05T22.36:46.2275035Z	Patch MobileApp	Success	Microsoft Intune portal extension	Application	Patch	Modify application.	MobileApp	netadmin@contoso.local	11Pro

Figure 17

Netsurion... EventTracker

Sample Log

event_category	+- 0
event_computer	+- azureintuen_009
event_datetime	+- 04/08/2019 7:49:13 PM
event_datetime_utc	+- 1554733153
event_description	id =
	displayName = Delete MobileAppAssignment
	componentName = MobileApp
	activity =
	activityDateTime = 2019-03-05T21:13:08.0171743Z
	activityType = Delete MobileAppAssignment
	activityOperationType = Delete
	activityResult = Success
	correlationId =
	category = Application
	actor =
	type = ItPro
	userPermissions =
	*
	applicationId =
	applicationDisplayName = Microsoft Intune portal extension
	userPrincipalName = contoso.admin@contososer.local
	servicePrincipalName =
	ipAddress =
	userld =
	resources =
	displayName = Microsoft Word
	type = MobileApp
	resourceId =
	modifiedProperties =

Figure 18

• Azure – Key vault Audit Events: This report will provide you information related to Azure Keyvault Audit Events.

Sample Log:

- Apr 08 11:06:44 PM	time = 2019-03-11T14:24:45.9785190Z category = AuditEvent operationName = VaultGet resultType = Success callerlpAddress
event_log_type	+- Application
event_type	+- Information
event_id	+- 3230
event_source	+- azure_keyvault
event_user_domain	+- N/A
event_computer	+- azurekey_009
event_user_name	+- N/A
event_description	time = 2019-03-11T14:24:45.9785190Z
	category = AuditEvent
	operationName = VaultGet
	resultType = Success
	callerIpAddress =
	identity =
	claim =
	http://schemas.microsoft.com/identity/claims/objectidentifier =
	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn = john@contoso.org
	appid =
	properties =



Sample Dashboards

1. Azure – Azure Intune Audit Activities by Category





2. Azure Intune Audit Activities by Type





3. Azure Intune Audit Activities by User





4. Azure Intune Audit Activities by Status



Figure 23



- Azure Intune Audit Activities by Component
- 5. Azure Intune Audit Activities by Component

6. Azure Keyvault Audit Activities by Type







7. Azure Keyvault Audit Activities By user



8. Azure Keyvault Audit Activities By Geo Location





9. Azure Keyvault Audit Activities by Status



Import Knowledge Pack into EventTracker

- 1. Launch EventTracker Control Panel.
- 2. Double click Export/Import Utility, and then click the Import tab.



Figure 29

3. Import Tokens/Flex Reports as given below.



Knowledge Objects

- 1. Click Knowledge objects under Admin option in the EventTracker manager page.
- 2. Locate the file named KO_Azure.etko.

Import	×
KO_Azure.etko 🗁 Browse Upload	
	Close



- 3. Now select all the check box and then click on \mathbb{T} '**Import**' option.
- 4. Knowledge objects are now imported successfully.

File imported su	iccessfully.
	ОК

Figure 31



Flex Reports

1. Click **Reports** option and select new (.etcrx) from the option.

ote : If report(s) contains temp Options O Category	plate, first imp Location	ort template and proceed	with exportimport utility.		
) Filters					
○ Alerts		C Legacy (*.issch)	New (*.etcrx)		
O Systems and Groups		Source :			
O RSS Feeds		JISSCH			
Reports					
O Behavior Rules					
⊖ SCAP					
O Token Value					

Figure 32

2. Locate the file named Flex Reports_Azure.etcrx and select all the check box.

🔁 Repor	ts Import				×
Note : If	report(s) contains template, first import template	and proceed with report import process			
Select	File D: Vinture final/Eley, Peperte Agure eteru	and proceed with report import process.		Calast Ca	
- Available	e reports			Select file	
Title		Frequency Show all	- Q Q		
	Title	Sites	Groups	Systems	Frequency
	DIT Azure - Key vault Audit Events	NTPLDTBLR47			Undefined
	DIT Azure Intune Audit Activities	NTPLDTBLR47			Undefined
<				_	>
Note	Set run time option is not applicable for Dofined	Reports and Hourly Reports			
NU(e)	Sector time option is not applicable for Defined	nepoits and nouny nepoits			
Set n	un time for report(s) from	M ▼ at interval of minute	s Set		
Repla	ace to	Repla	ace Assign systems		
			Note: Make sure that Site(s),	Group(s) and System(s) selections are v	alid. I 🛞



3. Click the Import button to import the reports. EventTracker displays success message.

Export Import Utility	\times
Selected reports configurations are imported successfully.	
ОК	





Dashlets

In EventTracker 9.0, we have added a new feature which will help to import/export the dashlet. Following is the procedure to do that:

1. Login into EventTracker Enterprise Web console.

	EventTracker 😛					
1	Username					
	Password					
	Login					
log	8,333,946 logs processed since install on Dec 30, 2017					
35,002 logs processed today						
Col	ontact Us FAQ Help					

Figure 35

2. Go to My Dashboard option.



Figure 36



3. Click on import button and select .etwd File.



Figure 37

4. Browse to the file path.

Import	^
Note: If dashlet configured using persisted report, first import the report and procee importing dashlet.	d with
Dashboard_Azure_Intune.etwd 🗁 Browse	Upload
	•

Figure 38

5. Click Upload and select the Dashboards which you want to import.



Import							
		1					
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.							
	🗁 Browse	Upload					
Available widgets							
Select All							
Azure Intune Audit Activi Azure Intune Audit Activi							
🖉 Azure Intune Audit Activi 🗹 Azure Intune Audit Activi							
🖉 Azure Intune Audit Activi 🗹 Azure Intune Audit Activi							

Figure 39

- 6. Click on Import button. It will upload all the selected dashboards.
- 7. Repeat the same procedure to import **Dashboard_Keyvault.etwd** for Keyvault Dashboards.

Verify Knowledge Pack in EventTracker

Knowledge Object

- 1. Logon to EventTracker Enterprise.
- 2. Click the Admin menu, and then click Knowledge Object.
- 3. In **Knowledge Object Group Tree** to view imported knowledge object, scroll down and click **Azure** group folder.

Knowledge Object are displayed in the pane.

Netsurion... EventTracker

Knowledge Objects										🔒 / Adm	in / Knowledge Objects
Search objects	objects							Obje	acts 🕂 🖡 🏌 🏟		
Groups	+ 🖉	Û	Object	name Azure Int	une Audit Activities						🕂 🏦 🕀
Applies to Azure Intune											
Aruba AirWave			Rules								
Aruba OS				Title		Log type	Event source	Event id	Event type		
- Arriva			+	Azure Intune A	udit Activities		Azure_intune	3230		1	Ê <i>0</i> ,
Azure Intune Audit Activities	<i>d</i> i i	Message Sig			Message Signature:						
Azure Keyvault Audit Activities	8	Ë.	Message Exception:								
Azure Intune	Expressions										
Azure Kewault		=		Expression type	Expression 1					Expression I	Format
Azure Stack	Acure Stack Regular (f)jidu/l=v+(?4D>*7)diiplayName\v+\=\v+(?4Diiplay_Name>*7)componentName\v+\=\v+(?4Domponent_Name>*7)activity Expression							Ī			
Bitdefender GravityZone	Are GravityZone Regular (t)sactivityAsteTime(s+=)s+(? <activity_datetime(s+=)s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s< td=""><td>tivityResult\s+\=\s+</td><td></td><td>Î</td></activity_datetime(s+=)s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+(?<activity_type(s+)=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s+()=(s<>						tivityResult\s+\=\s+		Î		
Bluecoat Content Analysis	Print Regular (?s)actor(s+)=?%pe(s+)=(?c)pe(s-)?")userPermission():+]=(x+)?(CUser_Permission.?")application():y=(x+)?(Application_jd>.?")application());pe(s)pe(s)pe(s)pe(s)pe(s)pe(s)pe(s)pe(s)					+		I Î			
Cisco AMP			Expression (? <application_display_name>*7)usePrincipalName>+*(><=><?<UserPrincipalName>*7)servicePrincipalName>+?>=>+(?<serviceprincipalname>*7)igAddress>+?userdS++=>+(?<userprincipalname>+7)igAddress>+?userdS++=>+(?<userprincipalname>+7)igAddress>+?userdS++=>+(?<userprincipalname>+7)igAddress>+?userdS++=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+7)igAddress>+?userdS+=>+(?<userprincipalname>+>+(?<userprincipalname>++>+(?<userprincipalname>++>+(?<userprincipalname>++>+(?<userprincipalname>++>++>+(?<userprincipalname>++>++>++>+(?<userprincipalname>++>++>++>+(?<userprincipalname>++>+>+>++></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></userprincipalname></serviceprincipalname></application_display_name>								
Cisco ASA Firewall	SA Firewall										

Figure 40

Flex Reports

- 1. Logon to EventTracker Enterprise.
- 2. Click the Reports menu, and then Configuration.
- 3. Select **Defined** in report type.
- 4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click **Azure** group folder.

Reports are displayed in the Reports configuration pane.

Report Configuration								
O Scheduled O Queued 🖲 Defined					Search			
Report Groups		()	🕀 🇱 Reports configuration: Azure					
Active sync		~						
🔁 All Compliance Repor		0						
Apache Web Server		0		Title	Created on			
Aruba AirWave				Azure – Key vault Audit Events	Apr 05 04:41:40 PM			
ArubaOS		<u> </u>		Azure Intune Audit Activities	Mar 11 04:13:40 PM			
🕞 Azure		0						
🕞 Bitdefender GravityZ		0						
🔁 🛛 Bluecoat Content Ana		0						
Cisco AMP		0						
Cisco ASA		0						

Figure 41

Dashlets

1. Logon to EventTracker Enterprise.

Integrate Microsoft Azure

2. Click the **Dashboard** menu, and then **My Dashboard**.

Customize dashlets			×					
Azure			Q					
Azure Intune Audit Activities by								
Azure Intune Audit Activities by	Azure Intune Audit Activities Ti	Azure Keyvault Audit Activities	Azure Keyvault Audit Activities					
Azure Keyvault Audit Activities	Azure Keyvault Audit Activities	Azure Keyvault Audit Activities						
			Add Delete Close					
Figure 42								

- 3. Then click on **Customize Dashlet** button (a) and search for **"Azure"**.
- 4. Click on Add, for adding the dashlets to the My Dashboard.

