

# **Integrate Azure MFA On-Premise**

# EventTracker v9.x and above

Publication Date: May 18, 2020

### Abstract

This guide provides instructions to configure Microsoft Azure Multi-Factor Authentication (MFA) to send logs to EventTracker.

### Scope

The configuration details in this guide are consistent with EventTracker version v9.x or above and **Azure MFA On-Premise** 

### Audience

Administrators who are assigned the task to monitor Azure MFA On-Premise events using EventTracker.

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.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



# Table of Contents

1.	Ove	erview	. 3
2.	Pre	requisites	. 3
3.	Inte 3.1	egration of Azure MFA On-Premise with EventTracker Integrating via syslog configuration	.3 .3
4.	Eve 4.1	entTracker Knowledge Pack Category	.5 .5
	4.2	Alert	. 5
	4.3	Report	. 5
	4.4	Dashboards	. 6
5.	۱mp 5.1	oorting Azure MFA On-Premise knowledge pack into EventTracker Category	.9 .9
	5.2	Alert	10
	5.3	Token template	11
	5.4	Knowledge Object	13
	5.5	Report	15
	5.6	Dashboards	16
6.	Ver 6.1	ifying Azure MFA On-Premise knowledge pack in EventTracker Category	19 19
	6.2	Alert	20
	6.3	Token templates	21
	6.4	Knowledge Object	21
	6.5	Report	22
	6.6	Dashboards	23

Netsurion. EventTracker

## 1. Overview

Microsoft Azure Multi-Factor Authentication (MFA) prompts the users during the sign-in process for an additional form of identification, such as to enter a code on cellphone or to provide a fingerprint scan.

EventTracker helps to monitor events from **Azure MFA On-Premise**. Its dashboard and reports will help you to detect authentication activities.

EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a disastrous failure occurs.

## 2. Prerequisites

- Admin privileges for Azure MFA and should be installed.
- EventTracker agent should be installed in the system.

# 3. Integration of Azure MFA On-Premise with EventTracker

### 3.1 Integrating via syslog configuration

Follow the below steps to configure syslog.

- 1. Log on to the server running the Multi-Factor Authentication Server with administrative privileges.
- 2. Open the Multi-Factor Authentication Server Management console by searching for it on the Start Screen.
- 3. In the left pane, click Logging-> syslog tab.



Eile View Iools Help	Hala
Status Users	
Image: Construction of the system of the	
Image: Construction of the state of the	
LDAP Windows Authentication Authentication	
AD FS Company Settings	
Email Directory Integration	
User Portal Web Service SDK	
Mobile App Logging	



- 4. Check the "Enable logging to syslog server" box.
- 5. Enter the EventTracker Manager IP in the syslog server field.

Integration is complete, EventTrackser will receive Azure MFA logs.



# 4. EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support Azure MFA.

## 4.1 Category

- Azure MFA: Authentication Success This category provides information related to successful authentication.
- Azure MFA: Authentication Failure This category provides information related to all authentication failure.

### 4.2 Alert

• Azure MFA: Authentication Failure - This alert is generated when any authentication failure is detected by Azure MFA.

### 4.3 Report

 Azure MFA – Authentication Failure - This report gives information about all the authentication failure detected by Azure MFA. Report contains username, source IP, guide, call status along with other useful information for further analysis.

LogTime	Computer	Call Status	Guid	IP Address	Message	Username	EventDescription
05/07/2020 12:09:16 PM	172.xx.xx.xx-SYSLOG	FAILED_PHONE_BUSY	080dc30d-9b6d-419f-8378-46d762944486		Auth Already in Progress	ericschm	May 07 12:09:16 172:27.100.13 Apr 30 18:47:20 RAMADFS02 Apr 30 18:47:20 ramadfs02 pfsvc: infsvci080dc30d.966d.419f.8378_
05/07/2020 12:09:16 PM	172.xx.xx.xx-SYSLOG	FAILED_PHONE_APP_NO_RESPON SE	b345747c-09d3-4b26-94e7-58045fa8f1aa		Mobile App No Response	ericschm	May 07 12:09:16 172.27.100.13 Apr 30 18:49:49 RAMADFS02 Apr 30 18:49:49 ramadfs02 pfsvc: infsvch345747c-09d3-4b26-94e7-
05/07/2020 12:09:16 PM	172.xx.xx.xx-SYSLOG	FAILED_PHONE_APP_NO_RESPON SE	e0fec917-a60a-4743-92dd-9039bd20b93e		Mobile App No Response	ericschm	May 07 12:09:16 172.27.100.13 Apr 30 18:48:26 RAMADFS02 Apr 30 18:48:26 ramadfs02 pfsvc:



• Azure MFA – Authentication Success - This report gives information about all the successful authentication detected by Azure MFA. Report contains username, source IP, guide, call status along with other useful information for further analysis.

LogTime	Computer	Call Status	Guid	IP Address	Message	Username	EventDescription
05/07/2020 12:09:23 PM	172.xx.xx.xx-SYSLOG	SUCCESS_PHONE_APP_AUTHENT CATED	76bae747-3fb2-4c8e-a312- 3dcadfd7c997	172.xx.xx.xx	Mobile App Authenticated	joshmcde@connexusenergy.com	May 07 12:09:23 172.xx.xx.xx Apr 30 06:59:07 RAMMFA01 Apr 30 06:59:07 rammfa01 pfsvc:
05/07/2020 12:09:23 PM	172.xx.xx.xx-SYSLOG	SUCCESS_PHONE_APP_AUTHENT CATED	2ddadce3-ebc6-4c72-b3e9- 6ebaf8b2c962		Mobile App Authenticated	joshmcde	May 07 12:09:23 172:xx:xx: Apr 30 06:59:27 RAMADFS02 Apr 30 06:59:27 ramadfs02 pfsvc: ipfsvcl2ddadce3-ebc6-4c72-b3e9-
05/07/2020 12:09:23 PM	172.xx.xx.xx-SYSLOG	SUCCESS_PHONE_APP_AUTHENT CATED	2f7d1d88-2ab7-49a4-935f- c143d38ec20c		Mobile App Authenticated	mattclay	May 07 12:09:23 172 xxxxx Apr 30 07:11:20 RAMADFS02 Apr 30 07:11:20 ramadfs02 pfsvc:

Figure 3



### • Logs Considered

action	+- succeeded
event_category	+- 0
event_computer	+- 172.27.100.13-syslog
event_datetime	+- 5/7/2020 5:16:17 PM
event_datetime_utc	+- 1588851977
event_description	May 07 17:16:17 172.27.100.13 Apr 29 06:47:28 RAMADFS02 Apr 29 06:47:28 ramadfs02 pfsvc: i pfsvc 7c819
	succeeded for user 'davejohn'. Call status: SUCCESS_PHONE_APP_AUTHENTICATED - "Mobile App Authentic
event_group_name	+- Default
event_id	+- 128
event_log_type	+- Application
event_source	+- SYSLOG local0
event_type	+- Error
event_user_domain	+- N/A
event_user_name	+- N/A
log_source	+- Azure MFA
log_type	+- SUCCESS_PHONE_APP_AUTHENTICATED
object_id	+ - 7c8195d4-b738-45fa-9b4d-8d16dfa842d1
reason	+ - Mobile App Authenticated
source_type	+- Azure MFA
src_user_name	+- davejohn
tags	+ - Authentication Success
tags	+- Authentication Activities

### Figure 4

## 4.4 Dashboards

• Azure MFA: Authentication Success



Figure 5





### • Azure MFA: Authentication Failure

Figure 6

• Azure MFA: User Location



Figure 7









### • Azure MFA: Authentication Request Mode



Figure 9

Netsurion. EventTracker°

# 5. Importing Azure MFA On-Premise knowledge pack into EventTracker

**NOTE**: Import knowledge pack items in the following sequence.

- Category
- Alert
- Token template
- Knowledge Object
- Report
- Dashboard
- 1. Launch EventTracker Control Panel.
- 2. Double click Export Import Utility.

<b>8</b>	Event	tTracker Contro	l Panel	- 🗆 X
			Ev	entTracker
EventVault	Diagnostics	License Manager	Export Import Utility	Append Archives
EventTracker	Traffic Analyzer	Agent	Port	TrapTracker
Agent Confi	53	Manageme	Configuration	
Change Audit	About EventTracker			
	E-mail: s	support@EventTra	cker.com	

Figure 10

3. Click the **Import** tab.

### 5.1 Category

1. Click **Category** option, and then click **Browse** .



-9-	Export Import Utility	. 🗆 X
Export       Import         1. Provide the path and file nam         2. Click the Import button.         Options            • Category             • Filters             • Alerts             • Systems and Groups             • Token Value             • Reports             • Behavior Correlation	Export Import Utility e of the Categories file. Use the '' button to browse and locate the import file. Location Source :	
	Import	Close

Figure 11

- 2. Locate Categories\_Azure MFA.iscat file, and then click Open.
- 3. To import categories, click Import.

EventTracker displays success message.



Figure 12

4. Click **OK**, and then click **Close**.

### 5.2 Alert

1. Click Alert option, and then click Browse

1 Export Import Utility							
Export Import	Export In the of the Alerts file. Use the '' butto Location Import E-mail settings Set Active Only if notifications set By default Watchlist Configuration Import Watchlist configuration Import Watchlist configuration Set Configuration Source : [*isalt]	nport Utility on to browse and locate the import file. This setting is applicable only for imports from Alert files. For v7, the active status will be set I "Active" key available in the configuration sec on or alerts which have Advanced watchlist configu e user should make sure the watchlist groups a s are imported.	Legacy (v6x) based on tion. red. re available		X		
		Impor	t	Clos	e		

Figure 13

- 2. Locate Alerts\_Azure MFA.isalt file, and then click Open.
- 3. To import alerts, click **Import**.

EventTracker displays success message.



Figure 14

4. Click **OK**, and then click **Close**.

### 5.3 Token template

1. Click **Parsing rule** under **Admin** option in the EventTracker manager page.



		💭 Admin <del>-</del>
Active Watch Lists	FAQ Tile Configuration	🧭 Parsing Rules
Alerts	Group Management	Report Settings
Casebook Configuration	🔍 IP Lookup Configuration	Systems
● Category	- 🔆 Knowledge Objects	Q Users
Diagnostics	M Machine Learning Jobs	∰ Weights
Event Filters	🗞 Machine Learning Settings	
Ventvault	Manager	



2. Click Template.

Parsing Rule	S	
Parsing Rule	Template	
Groups		<b>(</b> )
A		A



3. To import token template, click Import.



Figure 17

4. Locate the **Templates\_Azure MFA.ettd** type file by clicking **Browse**, enable all the templates and click **import**.

nport	
elect file Note: Please select	file of type *.ettd (eventtracker template dashlets).

Figure 18

5. Click **OK**.

### 5.4 Knowledge Object

1. Click **Knowledge objects** under Admin option in the EventTracker manager page.

≡	Event <b>Tracker</b> ⊕					🐥 🛛 Admin 🕶	Tools <del>-</del>
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
Q		_	Alerts	Correlation	Q IP Lookup Configuration	Q Users	
	0	1	Behavior Correlation Rules	Diagnostics	😥 Knowledge Objects	∰ Weights	
Å			🏷 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		
			el <sup>®</sup> Category	FAQ Configuration	Report Settings		
	Attacker			- News			



2. Click Import  $\mathbb{T}$  as highlighted in the below image:



Figure 20

3. Click Browse.

Import		×
Select file	🗁 Browse Upload	
	с	iose

Figure 21

- 4. Locate the file named **KO\_Azure MFA.etko**.
- 5. Now select the check box and then click  $\blacksquare$  Import.

Import			×
Select	: file		🗁 Browse Upload
	Object name	Applies to	Group name
Ø	Azure MFA	MS Azure MFA	MS Azure MFA
			Import Close

Figure 22

6. Knowledge objects are now imported successfully.



Figure 23



### 5.5 Report

1. Click **Reports** option and select **New (\*.etcrx)** option.

Provide the path and file nan     Click the Import button     Note: If report(s) contains temp     Options     Category     Filters     Alerts     Systems and Groups     Token Value     Reports     Behavior Correlation	ne of Schedule Report file. Use the '' button to browse and locate the import file. late, first import template and proceed with exportimport utility. Location Legacy (* issch) Source : *.issch
--	--

Figure 24

2. Locate the file named **Reports\_ Azure MFA.etcrx** and select the check box.

t file		and the second state and second	Heports_Azure MFA.etcrx	Select file	
able repo	rts				
		Frequency Show a	- Q Q		
	Title	Sites	Groups	Systems	Frequenc
EDIT	Azure MFA - Authentication Failed	R1S5-VM30			Undefined
<u>EDIT</u>	Azure MFA - Authentication Success	R1S5-VM30			Undefined
e: Set n	In time option is not applicable for Defined	Reports and Hourly Reports			
e: Set n	In time option is not applicable for Defined	Reports and Hourly Reports	minutes Set		
e: Set n t run tit	In time option is not applicable for Defined ne for report(s) from	Reports and Hourly Reports	minutes Set		Activat

Figure 25



3. Click Import I to import the report. EventTracker displays success message.





## 5.6 Dashboards

NOTE- Below steps given are specific to EventTracker 9 and later.

1. Open EventTracker in browser and logon.





- 2. Navigate to My Dashboard option as shown above.
- 3. Click **Import** as show below:







- 4. Import dashboard file Dashboard\_Azure MFA.etwd and select Select All checkbox.
- 5. Click **Import** as shown below.

Import		
Note: If dashlet configured using persisted report, first import the dashlet.	report and proceed with im	porting
	🗁 Browse	Upload
Available widgets  Select All		
Azure MFA: Authentication 🗹 Azure MFA: Authentication	haar	
Azure MFA: Authentication 🗹 Azure MFA: Authentication	laas	
Azure MFA: User location		
	Import	Close

Figure 29

6. Import is now completed successfully.





7. In **My Dashboard** page select ⊕ to add dashboard.





8. Choose appropriate name for Title and Description. Click Save.



Title Azure MFA Description	Title Azure MFA Description Microsoft Azure MFA	dit Dashboard		
Azure MFA Description	Azure MFA Description Microsoft Azure MFA	Title		
Description	Description Microsoft Azure MFA	Azure MFA		
	Microsoft Azure MFA	Description		
Microsoft Azure MFA		Microsoft Azure MFA		

Figure 32

9. In **My Dashboard** page select (a) to add dashlets.



Figure 33

10. Select imported dashlets and click Add.

Customize dashlets				×
Azure MFA				Q
Azure MFA: Authentication Faile	Azure MFA: Authentication Failu	Azure MFA: Authentication Req	Azure MFA: Authentication	Succ
Azure MFA: User location				
			Add Delete	Close

Figure 34



# 6. Verifying Azure MFA On-Premise knowledge pack in EventTracker

### 6.1 Category

- 1. Logon to EventTracker.
- 2. Click Admin dropdown, and then click Category.

≡	Event <b>Tracker</b> ⊕					🐥 🛛 Admin 🗸	Tools <del>-</del>
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
q		_	Alerts	Correlation	🔍 IP Lookup Configuration	Q Users	
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	r 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 Cc USB activities, New sen	Casebook Configuration	P Eventvault	🧭 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			



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

Category	
Category Tree	Search
- All Categories	
🗐 *All em	or events
🗐 *All info	ormation events
🗐 *All wa	rning events
🗐 *Securi	ty: All security events
Accellic	on SFT
🗐 🔁 Aruba (	Clearpass
Azure N	MFA.
- E Azı	ure MFA: Authentication Failure
E Azu	ure MFA: Authentication Success

Figure 36

### 6.2 Alert

- 1. Logon to EventTracker.
- 2. Click the Admin menu, and then click Alerts.

≡	EventTracker					🔎 🛛 🗚 🗛 🖊	Tools <del>-</del>
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
٩		_	Alerts	Correlation	Q IP Lookup Configuration	🛱 Users	_
	0	2	Behavior Correlation Rules	Diagnostics	Knowledge Objects	The 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	Eventvault	Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			

### Figure 37

 In the Search box, type 'Azure MFA', and then click Go. Alert Management page will display the imported alert.

Alert Name A	Threat	Active	Email
Azure MFA: Authentication Failure	۰		

#### Figure 38

4. To activate the imported alert, toggle the Active switch.

EventTracker displays message box.



Figure 39

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

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



## 6.3 Token templates

1. In the EventTracker web interface, click the Admin dropdown, and then click Parsing rules.

≡	EventTracker @					🐥 🛛 Admin-	Tools <del>+</del>
	Home		Active Watch Lists	Collection Master	🖙 Group Management	Systems	🕈 / Dashb
٩		_	Alerts	© Correlation	🔍 IP Lookup Configuration	QQ Users	
	0	1	Behavior Correlation Rules	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			

Figure 40

2. On Template tab, click on the Azure MFA group folder to view the imported token values.

Parsing Rule	S					
Parsing Rule	Template					
Groups			Đ	Group : Azure MFA		Search
Default						
Accellion SFT			Ø	Template Name	Template [	Description
Azure MFA		Ē	1	Azure MFA	Microsoft A	Azure MFA
				Figure 41		

### 6.4 Knowledge Object

1. In the EventTracker web interface, click the Admin dropdown, and then select Knowledge Objects.

≡	Event <b>Tracker</b> ⊕					🐥 🛛 Admin-	Tools <del>+</del>
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a			Alerts	Correlation	Q IP Lookup Configuration	Q Users	_
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	∰ Weights	
<u>~</u>			🗞 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 Knowledge Object tree, expand **Azure MFA** group folder to view the imported knowledge object.



Knowledge Objects			
Search objects	Q	Q Acti	vate Now
Groups 🕂 🔗 🔟	Objec Appli	ct name Azure MFA les to MS Azure MFA	
Duo Security	Rules		
EventTracker		Title	Event source
	Ŧ	Azure MFA	syslog
+ G suite		Message Signature	: (?i)pfsvc\:\s(.\ (pfAuth pfsvc)\  pfauth)
Malwarebytes Antivirus		Message Exception	Î.
MS Azure MFA		Expressions	
Azure MFA		Expression type	Expression 1

Figure 43

3. Click Activate Now to apply imported knowledge objects.

### 6.5 Report

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

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



- 2. In **Reports Configuration** pane, select **Defined** option.
- 3. Click on the Azure MFA group folder to view the imported reports.



Repo	rt Configuration				
Scl	heduled 🔘 Queued 💿 Defined				
Repoi	rt Groups 🕢 🤂		Rep	orts confi	guration: Azure MFA
<b>S</b>	Security	*	•	İ 2,	
٩.	Compliance				Title
4	Operations				Azure MFA - Authentication Failed
<b>S</b> .	Flex			1	Azure MFA - Authentication Success
	Accellion SFT			14	
	Aruba ClearPass 📋 🧭				
	Azure MFA 📋 🧭				

Figure 45

## 6.6 Dashboards

1. In the EventTracker web interface, Click Home and select "My Dashboard".





2. In the "Azure MFA" dashboard you should be now able to see something like this.



Figure 47

