

How to- Configure RWTD (Remote Workforce Threat Detection) Knowledge Packs EventTracker v9.3

Publication Date: August 7, 2020

Abstract

This guide provides instructions to configure RWTD knowledge packs. Once EventTracker is configured to collect and parse logs, dashboard and alerts can be configured for remote workforce threat detection.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3.

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	erviev	W	3
2.		Pre	requi	isites	3
3.	3.1	Imp L	ortin Knov	ng Knowledge Packs for Remote Workforce Threat Detection wledge Objects	3 3
	3.2	2	Dasł	hboard	5
	3.3	3	Aler	ts	8
		3.3.	1	Custom Alert	9
		3.3.	2	Importing RWTD alerts1	0
	3.4	1	Mac	chine Learning Jobs	.3
4.	4.1	RW	TD A Ann	lert/Dashboard Details	4
	4.2	2	Use	Cases	4
	4.3	3	Sam	ple Alerts1	.5
	4.4	1	Dasł	hboards1	7



1. Overview

Work from home or outside the office requires a remote connection to the organization's VPN. This increases the vulnerability risk of the organization's network. To combat the rapid increase in the remote workforce threat, EventTracker generates alerts using firewall devices descriptions. Alerts can be configured for remote workforce threat detection.

2. Prerequisites

- EventTracker v9.3 should be installed.
- **PowerShell 5.0** should be installed on the EventTracker Manager.
- Latest Knowledge Object files having version number 3.0.
- Latest golden image or ET93U20-8009.
- Following are the products which we support for RWTD Knowledge packs.

VPN	Cloud Suite	Authenticator
Cisco ASA Firewall	G Suite	OKTA SSO
FortiGate Firewall	Office 365	DUO Security
Palo Alto Firewall		Azure AD
Sophos XG Firewall		Windows
WatchGuard XTM		
Firewall		
SonicWall UTM Firewall		

3. Importing Knowledge Packs for Remote Workforce Threat Detection

3.1 Knowledge Objects

- 1. Click Knowledge objects under the Admin option in the EventTracker manager page.
- Locate the respective product folder in %et_install_path%\Knowledge Packs\ and locate file named KO_<Supported product name>.etko.

Note: If the folder name is not available, kindly install the update ET93U20-8009.



Import		×
KO_Office 365.etko	se Upload	
		Close

Figure 1

3. Now select all the checkbox and then click \blacksquare 'Import'.

Impo	rt		×
Sel	ect file	🚍 Br	rowse Upload
	Object name	Applies to	Group name
	Office365 Exchange Mail Traffic Details	Microsoft office365	Office 365
•	Office365 Exchange Message Trace Details	Microsoft office365	Office 365
	Office365 Unified Audit Logging	Microsoft office365	Office 365
1	Office365 Usage Statistics	Microsoft office365	Office 365
			Import Close



4. Knowledge objects are now imported successfully.



Figure 3



- 5. Please follow the above steps to download the KO's on other devices. RWTD package will contain KO for the supported devices.
- 6. Once KO's are imported for the required devices, check the KO version.

≡	Netsurion EventTrack								_	
=	Knowledge Objects				Edit object				×	
Q					Object name	Office365 Unified Audit Logging				
R	Search objects	Q Q	Ac	tivate Now	Applies to	Microsoft office365	Object version	3.0		
					Description					
	Groups	🕀 🗭 🗓	Object	name Office365 Unified Audit Logging	Select a group	Office 365	▼ Enabled			
	Accellion SFT	î.	Applie	s to Microsoft office365					- 1	
	Deep Instinct		Rules					Course of C		
	Duo Security			Title				Save	e	Eve
	EventTracker			Office365 Unified Audit Logging Message Signature:		UnifiedAudit	Office 365			323
	🖬 _{G suite}			Message Exception:						
	Microsoft Exchange			Expressions						
	Office 365			Expression type		Expression 1		Expres	ssion 2	
	Office365 Exchange Mail Traffic Details Office365 Exchange Message Trace D Office365 Unified Audit Logging Office365 Usage Statistics			Key Value Delimiter		-		/n		

Figure 4

7. Please do the source type mapping with respective system after importing the KO.

3.2 Dashboard

In EventTracker 9.3, we have added a new feature to import/export the dashlet. Following is the procedure.

1. Login into EventTracker Web console.



Figure 5



2. Go to My Dashboard option.

× Netsurion	. EventTr
Dashboard	
Home	
My Dashboard	
Threats	
Incidents	
Machine Learning	
MITRE ATT&CK™	
Change Audit	
Compliance	
Security Summary	



3. Click **Import** and select Dashboard_VPN.etwd file from %et_install_path%\Knowledge Packs\RWTD\Configuration.





h	mport	
	Note: If dashlet configured using persisted report, first import the report and proceed with imp dashlet.	ed report, first import the report and proceed with importing
	Dashboards_VPN.etwd 🗁 Browse	Upload
		Close

Figure 8

4. Click upload and select **Dashboard** you want to import.

nport											
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.											
Available widgets											
Select All											
VPN Login by User	VPN Login by Geolocation	VPN Login by IP address	VPN Login failed by user								
VPN Login failed by geolo	✓ VPN Login Success Trend	VPN Login failed Trend	VPN Login failed by IP Ad								
				Import Close							
				Close							



- 5. Click **Import** to upload all the selected dashboards.
- 6. Follow the above steps to import the required dashboards from the same path.



3.3 Alerts

Steps to import the alerts.

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



3. Click the Alert option, and then click Browse

💺 Export Import Utility		-		×
Export Import				
	me of the Alerts file. Use the '' button Location ☑ Import E-mail settings Set Active ④ Only if notifications set ○ By default Watchlist Configuration ☑ Import Watchlist configuration This setting is applicable only for Note: If this option is enabled th	on to browse and locate the import file. This setting is applicable only for imports from Legacy (Alert files. For v7, the active status will be set based or "Active" key available in the configuration section. on re user should make sure the watchlist configured. the user should make sure the watchlist groups are available	iv6x) 1	
Machine learning	Source : [*isalt	Import	 Clo	se

Figure 11

- 4. Locate the respective product folder in %et_install_path%\Knowledge Packs\ and locate file named Alert_<Supported product name>.isalt., and then click Open.
- 5. To import alerts, click **Import**.

EventTracker displays a success message.



Figure 12

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

Kindly follow the above steps to import the alerts on other devices.

3.3.1 Custom Alert

For custom alert, follow the instructions given below to add console side remedial action.

Note: The latest golden image or Update ET93U20-8009 should be installed.

- 1. Login to EventTracker manager console.
- 2. Go to Admin > Alert.
- 3. Search for Custom alert e.g. Sophos XG Firewall: VPN login failed.

Alerts										A.	/ Admin / Alerts
Show All 🗸							Search by Alert na	me 🖌	So	phos XG Firewall: VPN logi	Q Q
10	9				10	User 📗	10	10	Se	High1	2
Available Alerts Total number of alerts available	Active Alerts Total number of active alerts				System/User Det Count for system and	fined Alerts user defined alerts		Alerts by Th Count of alerts b	reat Level by threat level		
Activate Now Click 'Activate Now' after make	ing all changes									Total: 1 Page Si	ze 25 🗸
Alert Name 🔨	Ţ	Threat	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent		Applies To	
βδ Sophos XG Firewall: VPN login failed									VPN logs		



4. Edit the alert and go to Action tab > Console Remedial Action and in file section, and add the following location

"%et_install_path%\ScheduledActionScripts\Suspicious Login\SuspiciousLogin.exe"



Alerts							† /	Admin / Alerts /	Wizard
Configuration		Back	Event Details	Event Filter	Custom	<u>Systems</u>	Actions Next		\$
Alexandra (Theorem I and	*1	and a lateral						
Alert name	Inreat level		reshold level						
Sophos XG Firewall: VPN login failed	Serious	~	Low						~
Applies to	Alert version								
VPN logs	1.0								
Email SNMP Syslog Agent Remedial Action Console Remedial Action Remedial Action at Console Select a file to execute when an event occurs Select a file to execute when an event occurs The order of command line arguments to the file is as shown in the example given below Eg: Cimyfilebat Event Type, Log Type, Computer, Source, Category, Event Id, User, Description, Alert File "%et_install_path%jScheduledActionScripts/Suspicious Login/SuspiciousLogin.exe"	Name, Log Time, Alert Time, Incident Number, Domain, Group Name, System Description, Site Name								
								Finish C	ancel
	Figure 14								

3.3.2 Importing RWTD alerts

To import RWTD alerts

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



3. Click the Alert option, and then click Browse



🖞 Export Import Utility			-		×			
Export Import								
1. Provide the path and file na 2. Click the Import button.	me of the Alerts file. Use the '' but	on to browse and locate the import file.						
Ontions	Location							
Category	Import E-mail settings							
	Set Active							
 Filters 	Only if notifications set	Alert files. For v7, the active status will be set	Legacy (based on	v6x) 1				
Alerts	O By default	"Active" key available in the configuration se	ction.					
O Systems and Groups	Watchlist Configuration							
O Talva Vela	Import Watchlist configuration							
	This setting is applicable only f	or alerts which have Advanced watchlist config	ured.	hla				
◯ Reports	on the console where the alert	s are imported.	are avalia	Die				
	Source :			_				
	".isalt							
		Impo	rt.	Clau				
		Inpo		CIO	36			



Locate Alerts_RWTD.isalt file from

%et_install_path%\KnowledgePacks\RWTD\Configuration\Alerts_RWTD.isalt

- 4. Click **import** to complete the configuration.
- 5. Login to EventTracker manager console.
- 6. Go to Admin > Alert.

There are 4 new alerts are available in the alert management.

- Geographically improbable access detected
- Login activity from blacklisted location
- Suspicious multiple login attempts from same IP address
- Email with pandemic or corona subject
- 7. The default SuspiciousLogin.config is given in the update to parse username and IP address for the RWTD alerts. The below steps are given only for the custom alerts if want to extract the username and IP address from them.



- 8. Now, register the alert in SuspiciousLogin.config with its regex for parsing username and IP address.
- 9. In EventTracker manager, go to following location.

%et_install_path%\ScheduledActionScripts\Suspicious Login.

10. Open SuspiciousLogin.config file and add the section as show below.

```
<?xml version="1.0" encoding="utf-8" ?>
1
    <configuration>
2
3
        <AlertConfiguration>
4
           5
              <activities>
                  <Simult available="false"/>
6
                  <multiuser available='True'/>
7
8
                  9
              </activities>
              <regex>(?s)ClientIP\s=\s(?&lt;LoginIP&gt;[^\s]+).*?UserId\s=\s(?&lt;Username&gt;[^\s]+)</regex>
0
.1
           </alert>
           kalert Name='Sophos XG Firewall: VPN login failed'>
.2
3
           <activities>
             <Simult available='true'/>
.4
              <multiuser available='true'/>
5
            <blacklist available='true'/>
.6
.7
           </activities>
         ....<regex>(?s)ClientIP\s=\s(?&lt;LoginIP&gt;[^\s]+).*?UserId\s=\s(?&lt;Username&gt;[^\s]+)</regex>
.8
           </alert>
9
        </AlertConfiguration>
!0
11
        <Country>
!2
           <value>PK</value>
!3
           <value>CN</value>
14
        </Country>
!5
       <Speed>400</Speed>
!6
   </configuration>
```

Sample Configuration

```
<alert Name='Sophos XG Firewall: VPN login failed'>
        <activities>
            <Simult available='true'/>
            <multiuser available='true'/>
            <blacklist available='true'/>
            <blacklist available='true'/>
            </activities>
            <regex>(?s)ClientIP\s=\s(?&lt;LoginIP&gt;[^\s]+).*?UserId\s=\s(?&lt;User
name&gt;[^\s]+)</regex>
</alert>
```

11. If facing any issue with regex creation, kindly contact <u>Security Intelligence</u> team with sample Log.

3.4 Machine Learning Jobs

- 1. Launch the EventTracker control panel.
- 2. Click on Export import Utility > Import tab.

🐁 Export Import Utility		×
Export Import Utility Export Import Provide the path and file na Cick the Import button Options Category Filters Alerts Systems and Groups Token Value Benotts	ame of Machine learning file. Use the '' button to browse and locate the import file.	×
Machine learning	Import	8

Figure 17

3. Click on **Machine learning** and **Browse** for ML_RWTD.is rule file in following location %et_install_path%\Knowledge Packs\RWTD\Configuration.

Once Machine learning jobs are imported. It will display the follow message.

Export Import Utility	
Selected machine learning jobs are imported successful	ly.
ОК	



4. Click **OK** to complete the importing.

4. RWTD Alert/Dashboard Details

4.1 Applicable Log Sources

The alerts and dashboards are available for 3 types of log sources which are as below.

Cloud Suite	Authenticator
G Suite	OKTA SSO
Office 365	DUO Security
	Azure AD
	Windows
	Cloud Suite G Suite Office 365

4.2 Use Cases

By providing the alerts and dashboards, we are trying to solve the following use cases which the enterprises are on the lookout.

VPN Devices

- Successful Logins from rare/unexpected Countries
- Geographically improbable access (when the same account is logged into in a short time period from distant locations)
- Password Spraying (brute force attack)
- Too many failed VPN logins
- How many logins happened in a day?
- Which specific user is having too many login failures?

Cloud Suite

- Successful Logins from rare/unexpected Countries
- Geographically improbable access (when the same account is logged into in a short time period from distant locations)
- Password Spraying (brute force attack)
- Admin activities with changes to forwarding rules, permissions, admin account created
- Downloads from cloud shared drives

Authenticator

- Successful Logins from rare/unexpected Countries
- Geographically improbable access (when the same account is logged into in a short time period from distant locations)
- Password Spraying (brute force attack)
- Admin activities like adding new user, privilege escalation, adding user to a group etc.
- First login to an asset.

4.3 Sample Alerts

Alert Name	Login activity from blacklisted location
Event ID	11010
Source	EventTracker
Description	Login activity from blacklisted location.
	Source: Office 365 login activities
	IP Address: 14.1.104.10
	Country Code: PK
	Country Name: Pakistan
	Subdivision Name: Karchi
	City: Karchi
	Source Description:
	CreationTime = 2020-04-22T04:15:58 Id = 10c5a1a3-4413-4250-ac1a-
	f424be32bc17 Operation = UserLoggedIn OrganizationId = 0ac05f5c-4238-
	4951-89a8-2b5e518805f0 RecordType = 15 ResultStatus =
	Succeeded UserKey = <u>10032000549D77B7@eventtracker.com</u> UserType = 0
	Version = 1 Workload = AzureActiveDirectory ClientIP =
	14.1.104.10 ObjectId = 00000004-0000-0ff1-ce00-
	000000000000 UserId = <u>Mike@Contoso.com</u> AzureActiveDirectoryEventTyp
	e = 1 ExtendedProperties = [Name = UserAgent Value = Mozilla/5.0
	(Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
	Name = UserAuthenticationMethod Value = 9 Name = RequestType Value =
	OAuth2:Authorize Name = ResultStatusDetail Value = Redirect
] ModifiedProperties = [] Actor = [ID = 44a8954a-d1e4-4d0c-bd4a-
	d363352ed751 Type = 0 ID = <u>Sana.b@eventtracker.com</u> Type = 5 ID =
	10032000549D77B7 Type = 3] ActorContextId = 0ac05f5c-4238-4951-89a8-
	2b5e518805f0 ActorIpAddress = 182.74.234.198 InterSystemsId = 92f0269a-
	ebe4-48eb-9608-59958ce1dfee IntraSystemId = f527161c-0887-429a-9ba3-
	7ec2ea0d3e00 SupportTicketId = Target = [ID = 00000004-0000-0ff1-ce00-
	000000000000 Type = 0] TargetContextId = 0ac05f5c-4238-4951-89a8-
	2b5e518805f0 ApplicationId = e48d4214-364e-4731-b2b6-



	47dabf529218 RecordTypeName = AzureActiveDirectoryStsLogon UserType
	Name = Regular
Applicable to	VPN devices, O365, GSuite, OKTA SSO, DUO SSO, Windows, Azure AD

Alert Name	Suspicious multiple login attempts from same IP address
Event ID	11012
Source	EventTracker
Description	Multiple login attempts from same IP address.
	Source: Duo Security: Login activities
	IP Address: 14.1.104.10
	Accounts Logged In:
	Freddie Gallagher
	John
Applicable to	VPN devices, OKTA SSO, DUO SSO, Windows, Azure AD

Alert Name	Geographically improbable access detected
Event ID	11011
Source	EventTracker
Description	Geographically improbable access detected.
	Source: Duo Security: Login activities
	User: Freddie Gallagher
	Previous Login:
	Date Time: 2020-05-04 02:35:30
	IP Address: 199.188.93.188
	Country: United States
	Subdivision Name:
	City:
	Current Login:
	Date Time: 2020-05-04 02:36:00
	IP Address: 14.1.104.10
	Country: Pakistan
	Subdivision Name:
	City:
Applicable to	VPN devices, O365, GSuite, OKTA SSO, DUO SSO, Windows, Azure AD

Other existing alerts like login failure and anomalous login attempt will also be used as part of this offering.



4.4 Dashboards

• VPN Dashboard



Figure 19

• Cloud Suite Dashboard



Figure 20

Netsurion. EventTracker[®]



• Authenticator Dashboard

Figure 21

