

Integration Guide

Integrating Duo Security with EventTracker

Publication Date:

October 14, 2021

© Copyright Netsurion. All Rights Reserved.



Abstract

This guide helps you in configuring the **Duo Security** with the EventTracker to receive the **Duo Security** events. In this guide, you will find the detailed procedures required for monitoring the **Duo Security**.

Scope

The configuration details in this guide are consistent with the EventTracker version 9.3 or above and the **Duo** Security.

Audience

Administrators who are assigned the task to monitor and manage the **Duo Security** events using the **EventTracker.**



Table of Contents

Та	able c	of Contents	.3
1.	0	verview	.4
2.	Pr	rerequisites	.4
3.	In	itegrating the Duo Security events with the EventTracker	.4
4.	Εv	ventTracker Knowledge Pack	.7
	4.1	Category	.7
	4.2	Alerts	.7
	4.3	Reports	.8
	4.4	Dashboards	.9
5.	In	nporting the Duo Security Knowledge Pack into the EventTracker	2
	5.1	Category1	13
	5.2	Alerts1	4
	5.3	Knowledge Objects (KO)	15
	5.4	Reports1	17
	5.5	Dashboards1	8
6.	Ve	erifying the Duo Security Knowledge Pack in the EventTracker	21
	6.1	Category	21
	6.2	Alerts	21
	6.3	Knowledge Objects	22
	6.4	Reports	23
	6.5	Dashboards	24
	Abo	ut Netsurion	25
	Cont	tact Us	25

1. Overview

The Duo Security verifies the identity of users and protects against breaches due to phishing and other password attacks. It comes with an easy-to-use two-factor authentication (2FA) solution that adds another layer of security to their logins.

The EventTracker helps to monitor events from the Duo Security. Its dashboard, alerts and reports will help you to monitor the Duo login activities by the client based on user, the geolocation, username, and the login attributes which helps you to find the compromised user login. EventTracker will trigger alert if any fraudulent user is trying to login. It monitors the audit activities, the user management, group management, the access management activities, the policy changes, and other changes happening on the Duo Security.

2. Prerequisites

- Host machine should have installed the EventTracker Sensor.
- Administrator privilege for the Duo Security web interface.
- PowerShell 5.0 and later should be installed on the Duo integrator host machine.

3. Integrating the Duo Security events with the EventTracker

To configure the Duo Security application and generate reports, enable the Admin API.

The following steps helps you to enable the Admin API.

- 1. Logon to the <u>Web interface</u> of the Duo Security.
- 2. Click the Application tab and click the Protect an Application option as shown in the following image.

	A Search for users, groups, applications, or devices
Dashboard	Dashboard > Applications > Protect an Application
Device Insight	Protect an Application
Policies	
Applications	Adulti API
Protect an Application	
Users	Admin API Protect this Application Read the documentation C
Groups	

3. Click the option **Protect this Application** under the **Admin API** header.

Note: If the Admin API does not exist please contact Duo Security support for enabling the Admin API. Kindly find the mail id for contacting <u>Duo Security Support</u>.

- 4. After completed, you will get the required credentials for integration of the Duo Security with the EventTracker.
 - Integration Key
 - Secret Key



- API hostname
- 5. Click **Select** to copy the keys and save them for future use.

Details		
Integration key	DIN4DNX3Z5YY66ZPTTUD	select
Secret key	Click to view.	select
	Don't write down your secret key or share it with anyone.	
API hostname	api-804a1758.duosecurity.com	select

6. Select all the below permissions from the **Permissions** section and click **Save Changes**.

Grant settings Permit this Admin API application to read and update global account settings.	
Grant read log Permit this Admin API application to read logs.	
Grant read resource Permit this Admin API application to read resources such as users, phones, and hardware tokens.	

Following are the steps to integrate the Duo Security with the EventTracker.

- 1. Get the **Duo Security Integrator** executable file. <u>https://downloads.eventtracker.com/kp-integrator/ETS_DuoSecurity_Integrator.exe</u>
- 2. After the executable application is received, click the file.

ETS DUO Security Int	egrator	\times
	Edit Configurati	
DUO Security Configu	ration	
API Hostname	0	
Integration key		
Secret key		
	Validate Credential	
	Finish Cancel	



3. The **Duo Integrator** window display. Fill in the **Integration Key**, **Secret Key**, and **API HostName** as received from the web interface of the Duo Security.

늘 ETS DUO Security	Integrator		\times
		Edit Configurati	
DUO Security Conf	figuration		
API Hostname	Enter API HostName.duosecurity.com		
Integration key	Enter Integration Key		
Secret key	Enter Secret Key		
	Validate Credential		
	Fin	ish Cancel	

4. Click the Validate Credential button to check if the credentials are correct and are working properly.

Information	\times
Credential Validated Sucessfully	
ОК	

5. Click **OK** to close the **Validation** window and click **Finish** to complete the integration process.

5	ETS DUO Security	/ Integrator		X	
			Edit C	onfigurati	
	DUO Security Con	figuration			
	API Hostname	api-ei	om		
	Integration key	xTKBzVMvł			
	Secret key	MAX01C5P			
		Validate Cred	dential		
			Finish	Cancel	
	Information			×	
	() Duc	Security Integration cont	figured successfully		
			ОК		

4. EventTracker Knowledge Pack

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

The following Knowledge Packs are available in the EventTracker to support the Duo Security.

4.1 Category

- Duo Security Admin self-activation This category provides information when admins activate the Duo Security account by themselves.
- Duo Security Login success- This category provides information related to the Duo Security web console login success.
- Duo Security API management This category provides information related to the API key created, deleted, and viewed.
- **Duo Security Authentication failure** This category provides information related to the Two-Factor Authentication (2FA) failed while logging into the Duo Security console.
- **Duo Security Authentication success -** This category provides information related to the Two-Factor Authentication success while logging into the Duo Security console.
- Duo Security Authentication success by mobile This category provides information related to the Duo Security console login access allowed from the registered mobile numbers for the Duo Security users.
- **Duo Security Bypass key management-** This category provides information related to the bypass key created, bypass key updated, and bypass key deleted for the users.
- **Duo Security Directory management-** This category provides information related to the directory created, the directory deleted, and the directory updated.
- **Duo Security Group management-** This category provides information related to a group created, a group deleted, and a group updated.
- **Duo Security Login failed-** This category provides information related to the failed login to the Duo Security web console.
- **Duo Security Policy management-** This category provides information related to the policy created, the policy updated, and the policy deleted.
- **Duo Security User management** This category provides information related to the user created, the user updated, the user deleted, and the user permanently deleted.

4.2 Alerts

- **Duo Security: Authentication failed** This alert is triggered when the user tries to login from an anonymous IP address, a call timed out, is denied by policy, has an invalid passcode, etc.
- **Duo Security: Fraud user detected** This alert is triggered when the user is marked as fraud ulent, and the same user tries to login to the Duo Security web UI portal.
- **Duo Security: Login failed** This alert is generated when there is an issue completing primary password or SAML authentication, or an issue completing secondary authentication.
- **Duo Security**: **User deleted** This alert is triggered when the user is deleted from the Duo Security web console.

4.3 Reports

• **Duo Security – Authentication failed:** This report provides information related to authentication fails for a user, reason of failure, 2FA details, device name, username, and IP address.

		Device Ip		New	Admin	Authentication	
LogTime	Reason	address	Application	enrollment	Name	type	Result
12/16/2019 11:17:05 AM	User mistake	172.27.100.14	Microsoft RDP	False	etadmin	Duo Push	FAILURE

• **Duo Security – Login failed:** This report provides information when the user enters the primary password authentication or has an issue completing the 2FA.

			2Factor Authentication			
LogTime	Action	Reason	Туре	Email	IP Address	Admin Name
12/09/2019 04:33:39 PM	admin_2fa_error	Login timed out.	push	MAXX@contoso.com	182.74.234.198	Махх

• **Duo Security – Policy management:** This report provides information related to the policy created, policy updated, policy deleted, policy name, username, etc.

LogTime	Action	Authentication Status	Enroll Policy	Admin Email ID	Name	Admin Name
12/13/2019 11:43:52 AM	policy_create	Allow access without 2FA	Require Enrollment	maxx@contoso.com	Policy for bypass	maxx
12/13/2019 11:43:52 AM	policy_delete	No action	allow	maxx@contosorev.com	Auth_New_2fA	maxx
12/13/2019 11:43:52 AM	policy_update		Require Enrollment	maxx@contoso.com	Auth_New_2fA	maxx

• **Duo Security – User management:** This report provides information related to user-created, user-updated, user-deleted, username, and admin name.

	LogTime	Computer	Action	Name	User Account Status	Admin Name
	12/09/2019 06:57:19 PM	DUO_SECURITY	user_create	john	Active	maxx
	12/09/2019 06:57:20 PM	DUO_SECURITY	user_delete	mary	Disabled	System
	12/09/2019 07:10:44 PM	DUO_SECURITY	user_delete	john	Disabled	System
Ĩ	12/09/2019 07:10:44 PM	DUO_SECURITY	user_pending_delete	john	Pending Deletion	maxx

• **Duo Security – Admin self-activation:** This report provides information related to the Duo Security admin account trying to activate alone.

Sample Report

]	LogTime	Computer	Action	Name	Role	Admin Name	Phone Number
	12/09/2019 04:33:39 PM	DUO_SECURITY	admin_self_activate	maxx	Owner	maxx	+16005122291

 Duo Security – Authentication success: This report provides information related to authentication success allowed by policy, bypass username, remembered device, trusted location, trusted network, approved by the user, etc.



	User				Authentication		Web Agent	Operating
LogTime	Name	Reason	IP Address	Integration Name	type	Web Agent	Version	System
12/10/2019 04:05:2	8 PM etadmin		182.74.234.198	portal	n/a	Chrome	78.0.3904.108	Windows
12/10/2019 04:05:2	8 PM etadmin	User approved	172.27.100.14	Microsoft RDP	Duo Push			

- Duo Security Offline enrollment: This report provides information related to the device enrollments, user agent detail, the 2FA, username, etc.
- **Duo Security Login success:** This report provides information related to user entering the primary password authentication and completing the 2FA.
- Duo Security Authentication by mobile: This report provides information related to a mobile device allowed access, mobile number, credits used for allowing access, etc.

4.4 Dashboards

• **Duo Security – Login success:** This dashboard shows login success usernames into the Duo Security web console.



• **Duo Security – Authentication by mobile:** This dashboard shows information about the user who tries to login to the Duo Security web console by using the configured mobile numbers.





• **Duo Security – Login failed:** This dashboard shows information about failed user logins for the Duo Security web console and username.



• **Duo Security – Authentication failure:** This dashboard shows information about users trying to login to the Duo Security web console and the failed 2FA attempts.



• **Duo Security – Authentication success:** This dashboard shows information about users trying to login to the Duo Security web console and succeeds the 2FA attempts.





• **Duo Security – Registered mobile numbers:** This dashboard shows information about user-registered mobile numbers with the Duo Security.

Duo Security - Registered mobile numbers	© - ×
	O
+917382275451 +16005122291	
Dec 09 11:18 AM - Dec 16 11:19 AM	

• **Duo Security – Bypass key status by user:** This dashboard shows information about the Duo Security bypass key status based on the user.





 Duo Security – Policy management: This dashboard shows the information on the policy management and the policy names.



5. Importing the Duo Security Knowledge Pack into the EventTracker

NOTE: Import the EventTracker Knowledge Pack items in the following sequence:

- Category
- Alerts



- Knowledge Object
- Reports
- Dashboard
- 1. Launch the EventTracker Control Panel.
- 2. Double click Export Import Utility.



3. Click the **Import** tab.

5.1 Category

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

-1) 	Export Import Utility	-		x
Export Import	Export Import Utility ne of the Categories file. Use the '' button to browse and locate the import file. Location Source :			×
 Systems and Groups Token Value Reports Behavior Correlation 	Source :			
	Import		Close	



- 2. Locate the **Categories_Duo Security.iscat** file, and then click the **Open** button.
- 3. To import the categories, click the **Import** button.

EventTracker displays a success message.



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

5.2 Alerts

1. Click the **Alert** option, and then click the **Browse** button.

4	Export Ir	nport Utility	-		x
Export Import 1. Provide the path and file	name of the Alerts file. Use the '' butt	on to browse and locate the import file.			
2. Click the Import button. Options Category Filters	Location Import E-mail settings Set Active Only if notifications set By default	This setting is applicable only for imports from Legac Alert files. For v7, the active status will be set based "Active" key available in the configuration section.	y (v6x) on		
 Systems and Groups Token Value Reports Behavior Correlation 	Watchlist Configuration Import Watchlist configuration This setting is applicable only f Note: If this option is enabled t on the console where the alert Source : *isalt	on or alerts which have Advanced watchlist configured. he user should make sure the watchlist groups are ava s are imported.	ilable]	
L		Import		Clos	se

- 2. Locate the Alerts_Duo Security.isalt file, and then click the Open button.
- 3. To import the alerts, click the **Import** button. EventTracker displays a success message.



Export Import Utility
Selected alert configurations are imported successfully.
ОК

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

5.3 Knowledge Objects (KO)

1. Click Knowledge Objects under the Admin option in the EventTracker Manager page.

≡	Event Tracker ⊕					Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٩		_	Alerts	© Correlation	🔍 IP Lookup Configuration	Q Users	
	0	1	Behavior Correlation Rules	Diagnostics	😥 Knowledge Objects	🕀 Weights	
k			🇞 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. Click the **Import** \mathbb{T} button as highlighted in the below image.

	Knowledge Obj	jects		🕈 / Admin / Knowledge Objects
Q R	Search objects	Q	Q Activate Now	Objects 🕀 ፒ 🏦 🌣
	Groups	🕀 🖉 🗓		1.
	• Cylance			
	• EventTracker			

3. Click the **Browse** button.



Import		×
Select file	🖆 Browse Upload	
		Close

- 4. Locate the file named **KO_Duo Security.etko**.
- 5. Select the check box and then click the \mathbb{T} Import option.

Select	file		🖆 Browse Upload	
)	Object name	Applies to	Group name	
	Duo Security	Duo Security	Duo Security	
			Import Clo	ose

6. The Knowledge Objects are now imported successfully.



5.4 Reports

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

		Export Import Utility
Aport Imp 1. Provide 2. Click th Note : If n Options Categ Filten Alerts Syste Toke Repo Beha	oot e the path and file nar e the import button eport(s) contains temp gory s ems and Groups en Value orts	ne of Schedule Report file. Use the '' button to browse and locate the import file. Idate, first import template and proceed with exportimport utility. Location Legacy (* issch) Source : *issch
		Import Close

2. Locate the file named **Reports_ Duo Security.etcrx** and select all the check box.

alable re				Selectine	
le	pons	Frequency Show all	- Q Q		
3	Title	Sites	Groups	Systems	Frequency
EDI	Duo Security- Administrator activities		Default		Undefined
EDI	I Duo Security- Authentication failures		Default		Undefined
EDI	I Duo Security- Authentication success		Default		Undefined
EDI	Duo Security- Device authentication d		Default		Undefined
EDI	Duo Security- Device authentication ty		Default		Undefined
					*



3. Click the **Import** \blacksquare button to import the report. EventTracker displays a success message.



5.5 Dashboards

NOTE: Below steps given are specific to the EventTracker9 and later.

1. Open the **EventTracker** in a browser and logon.

11	Home		
۹	My Dashboard		
R	Threats	1	
	Incidents	Indicators of Compromise USB activities, New services or software install	
	Behavior Correlation		-
	Change Audit		-
	Compliance	Contraction of the	

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

Event Tracker ⊕	, 0	Admin -	Tools •	💽 ETAdmin 🔹
My Dashboard		A	/ Dashboard	d / My Dashboard
		÷	o 🖉 🎯	1 3 0

- 4. Import the dashboard file Dashboards_Duo Security.etwd and select the Select All checkbox.
- 5. Click the **Import** button as shown below.



Import							
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.							
🗁 Browse Upload							
Available widgets Select All							
Duo Security - Login succ Duo Security - Authentica							
Duo Security - login fail Duo Security - Authentica							
Duo Security - Authentica Duo Security - Registered							
Duo Security - Bypass key Duo Security - Policy man							
Import Close							

6. The Import is successfully completed.

Selected dashlets impo	rted successfully.
	ОК

7. In the **My Dashboard** page select ^① to add the dashboard.



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



Add Dashboard	
Title	
Duo Security	
Description	
Duo Security	
	Save Delete Cancel

9. In the **My Dashboard** page select $^{\textcircled{O}}$ to add the dashlets.

My Dashboa	rd
Duo Security	Ρ

10. Select the imported dashlets and click **Add**.

duo security			Q
Duo Security - Authentication b	Duo Security - Authentication f	Duo Security - Authentication s	Duo Security - Bypass key statu
Duo Security - Login activitiy by	Duo Security - login failed	Duo Security - Login success	Duo Security - Policy managem
Duo Security - Registered mobil			

Netsurion®

6. Verifying the Duo Security Knowledge Pack in the EventTracker

6.1 Category

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

≡	Event Tracker ⊕					🐥 🛛 Admin 🗸	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٩		_	Alerts	Correlation	🔍 IP Lookup Configuration	QQ Users	
	0	1	Behavior Correlation Rules	A Diagnostics	·⊙ Knowledge Objects	A 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		
		-	oloocoloocoloocoloocoloocoloocoloocolo	FAQ Configuration	Report Settings		
	Attacker			- News			

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

Category	
Category Tree Search	
 Duo Security Duo Security: Admin self activation Duo Security: Administrative Logon Duo Security: API management Duo Security: Authentication Failure Duo Security: Authentication Success Duo Security: Authentication success by mobile Duo Security: Bypass key management Duo Security: Directory management Duo Security: Group management Duo Security: Login failed 	^
(Duo Security: Policy management	

6.2 Alerts

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

Netsurion

	Event Tracker ⊕					🔎 🛛 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dash
a			Alerts	Correlation	Q IP Lookup Configuration	🛱 Users	
	0	2	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 Cc USB activities, New sen	Casebook Configuration	Seventvault	🧭 Parsing Rules		
			o [o Category	FAQ Configuration	Report Settings		
	Attacker			- News			

In the Search box, type Duo Security, and then click the Go button.
 Alerts Management page will display the imported alert.

Alerts Show All	v		
197			89
Available Alerts Total number of al			Active Alerts Total number of active alert
⊕ <u>∭</u>	Activate Now	Click 'Activate Now' after making	all changes
		Alert Name 🔨	
🗌 နိုဂ္ဂိ Duo Sec	urity: Fraud user detected		
🗌 ဇိုဂို Duo See	urity: User deleted		
🗌 ဇိုဂို Duo See	urity:Authentication failu	e	
🗌 နို့ရှိ Duo Secu	urity:Authentication success		

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

EventTracker displays a message box.



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

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

6.3 Knowledge Objects

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



≡	Event Tracker ⊕					🐥 🛛 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
Q		_	Alerts	Correlation	Q IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	A Diagnostics	Knowledge Objects	T Weights	
~			🗞 Behavior Correlation Settings	🖼 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	P Eventvault	🧭 Parsing Rules		
		_	o-∰ Category	FAQ Configuration	Report Settings		
	Attacker			- News			

2. In the Knowledge Objects tree, expand the **Duo Security** group folder to view the imported Knowledge Objects.

Knowledge Objects	
Duo	Q Q
Groups	+ Ø i
Duo Security	

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

6.4 Reports

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

	Event Tracker ⊕				
	Home				
¢ ₿	Report Configuration		1		
	Report Dashboard	ntry point	Indicators of Compromise USB activities. New services or software install		
	Explorer Attacker			-	

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

Netsurion®

Reports configuration: Duo Security

(Ū 2,	
		Title
	2	Duo security - User management
	£¥3	Duo Security - Login failed
	£\$5	Duo Security - Admin self activation
	£ <u>₹</u> }	Duo Security - Authentication failed
	٤¥	Duo Security - Policy management
	₹ £ 5	Duo Security - Authentication success
	£¥5	Duo Security - Login success
	₹ £ 3	Duo Security - Authentication by mobile
	£ 5 3	Duo Security - User enrollment

6.5 Dashboards

1. In the EventTracker web interface, click the **Home** Button and select **My Dashboard**.

	Home
Dashb	My Dashboard
	Threats
	Incidents

2. In the **Duo Security** dashboard you will see the following screen.



About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's <u>EventTracker</u> cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #23 among <u>MSSP Alert's 2021 Top 250 MSSPs</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 MSP's 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