Integrate Duo Security with EventTracker

EventTracker v9.0 and above

Publication Date: December 18, 2019
Abstract

This guide will facilitate a Duo Security user to send logs to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker 9.x or later and Duo Security.

Audience

Administrators who want to monitor the Duo Security 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.

© 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

1. Introduction ........................................................................................................................................... 3  
   1.1 Pre-requisites ..................................................................................................................................... 3  
   1.2 Integration of Duo Security events to EventTracker ........................................................................... 3  
2. EventTracker Knowledge Pack .............................................................................................................. 6  
   2.1 Categories .......................................................................................................................................... 6  
   2.2 Alerts ................................................................................................................................................. 7  
   2.3 Report ............................................................................................................................................... 7  
   2.4 Dashboards ......................................................................................................................................... 10  
3. Importing knowledge pack into EventTracker ...................................................................................... 14  
   3.1 Categories .......................................................................................................................................... 15  
   3.2 Alerts ............................................................................................................................................... 16  
   3.3 Parsing Rule ....................................................................................................................................... 17  
   3.4 Flex Reports ...................................................................................................................................... 18  
   3.5 Knowledge Objects ........................................................................................................................... 20  
   3.6 Dashboards ........................................................................................................................................ 21  
4. Verifying knowledge pack in EventTracker ............................................................................................ 22  
   4.1 Categories .......................................................................................................................................... 22  
   4.2 Alerts ............................................................................................................................................... 23  
   4.3 Parsing Rules ..................................................................................................................................... 23  
   4.4 Flex Reports ..................................................................................................................................... 24  
   4.5 Knowledge Objects ........................................................................................................................... 24  
   4.6 Dashboards ........................................................................................................................................ 25
1. Introduction

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 solution that adds another layer of security to their logins.

EventTracker can be integrated with Duo Security using its API. It helps you to visualize the Duo login activities happening by client based on user geolocation, username and login attributes which helps you to find the compromised user login.

EventTracker also alerts you if any fraud user is trying to login. It also monitors the audit activities of Duo and helps you to visualize the user management, group management, access management activities, policy changes and other changes which are happening on Duo Security.

EventTracker can also generate schedule report for user management activities, changes happening in Duo Security (policy changes, user & group changes, enrollment of devices & application in Duo).

1.1 Pre-requisites

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

1.2 Integration of Duo Security events to EventTracker

In order to configure the Duo Security application and generate reports, you need to first enable the admin API.

The below steps shows to enable the Admin API.

1. Logon to the Web interface of Duo Security.
2. Click on the Application tab and click on the Protect an application option as shown in the below image.

![Figure 1](image-url)
3. Click on the option **Protect this application** under the Admin API header.

Note: If Admin API does not exist please contact Duo Security support for enabling the Admin API. Please find below the mail id for contacting **Duo Security Support**.

4. Once that is done, you will get the credentials that are required for integration of Duo Security with EventTracker.
   - Integration Key
   - Secret Key
   - API hostname

5. Click on “**select**” to copy the key and save it for future use.

![Figure 2](image2.png)

6. Please select the permission “**Grant read log**” from the “**Permissions**” section and click on “**Save Changes**”.

![Figure 3](image3.png)

**Following are the steps to integrate Duo Security to EventTracker:**

1. Please contact the **EventTracker support team** for obtaining the Duo Security Integrator pack.
2. Once the executable application is received, right-click on the file and select “Run as Administrator”.
3. “Duo Integrator” window is displayed. Fill in the “Integration Key”, “Secret Key”, and “API HostName” as received from the web interface of Duo Security.

![Duo Security Integrator](image)

**Figure 4**

4. Once you have filled out the fields, click on the “Validate” button to check if credentials are correct and working properly.

![Information](image)

**Figure 5**

5. Click on the “OK” button to close the Validation window and then finally click on the “Submit” button to complete the integration process.

![Duo Security Integrator](image)

**Figure 6**
Integrate Duo Security with EventTracker

Figure 7

2. EventTracker Knowledge Pack

Once Duo Security events are received in EventTracker, Alerts, and Reports can be configured in EventTracker. The following Knowledge Packs are available in EventTracker to support the Duo Security monitoring.

2.1 Categories

**Duo Security: Admin self-activation** – This category provides information when the admin activates Duo Security account by himself.

**Duo Security: Login success**- This category provides information related to Duo Security web console login success.

**Duo Security: API management** – This category provides information related to API key created, deleted and viewed.

**Duo Security: Authentication failure** – This category provides information related to 2Factor authentication failed while logging into the Duo Security console.

**Duo Security: Authentication success** - This category provides information related to 2Factor authentication success while logging into the Duo Security console.

**Duo Security: Authentication success by mobile** - This category provides information related to Duo Security console login access allowed from registered mobile numbers for Duo Security users.

**Duo Security: Bypass key management**- This category provides information related to bypass key created, bypass key updated, bypass key deleted for users.

**Duo Security: Directory management**- This category provides information related to the directory created, directory deleted, and directory updated.

**Duo Security: Group management**- This category provides information related to a group created, group deleted, and group updated.
Integrate Duo Security with EventTracker

**Duo Security: Login failed** - This category provides information relates to failed login to Duo Security web console.

**Duo Security: Policy management** - This category provides information related to the policy created, policy updated, and policy deleted.

**Duo Security: User management** - This category provides information related to user-created, user updated, user deleted, and user permanently deleted.

### 2.2 Alerts

**Duo Security: Authentication failed** – This alert is triggered when the user tries to login from anonymous IP, call timed out, denied by policy, invalid passcode, etc.

**Duo Security: Fraud user detected** – This alert is triggered when the user is marked as fraud 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 issue completing primary password or SAML authentication, issue completing secondary authentication.

**Duo Security: User deleted** - This alert is triggered when the user is deleted from the Duo Security web console.

### 2.3 Report

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

Log Considered

access_device : @{browser=; browser_version=; flash_version=; java_version=; os=; os_version=}
device : +91 60051 22291
factor : Duo Push
integration : Microsoft RDP
ip : 172.27.100.14
location : @{city=; country=; state=}
new_enrollment : False
reason : User mistake
result : FAILURE
timestamp : 1575973838
username : etadmin

Sample Report

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Reason</th>
<th>Device Ip address</th>
<th>Application</th>
<th>New enrollment</th>
<th>Admin Name</th>
<th>Authentication type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/16/2019 11:17:05 AM</td>
<td>User mistake</td>
<td>172.27.100.14</td>
<td>Microsoft RDP</td>
<td>False</td>
<td>etadmin</td>
<td>Duo Push</td>
<td>FAILURE</td>
</tr>
</tbody>
</table>
Duo Security – Login failed: This report provides information when the user enters the primary password authentication or have issue completing the 2F authentication.

Log Considered

action : admin_login
description : {"factor": "push", "ip_address": "182.74.234.198", "primary_auth_method": "Password", "device": "600-512-2291"}
object :
timestamp : 1576153566
username : maxx

Sample Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Action</th>
<th>Reason</th>
<th>2Factor Authentication Type</th>
<th>Email</th>
<th>IP Address</th>
<th>Admin Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/09/2019 04:33:39 PM</td>
<td>admin_2fa_error</td>
<td>Login timed out</td>
<td>push</td>
<td><a href="mailto:MAXX@contoso.com">MAXX@contoso.com</a></td>
<td>182.74.234.198</td>
<td>Maxx</td>
</tr>
</tbody>
</table>

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

Log Considered

action : policy_create
description : {"endpoint_security_agents": [], "pretty_trusted_devices": "", "name": "Auth_New_2fA", "webauthn_policies_allowed_authenticator Enums": [], "endpoint_health_policy": null, "auth_status": "No action", "endpoint_security_agent remediation message": null, "endpoint_password": null, "software_policies": {}, "endpoint_encryption": null, "endpoint_firewall": null, "admin_email": "maxx@erp.com"}
object : Auth_New_2fA
timestamp : 1576155512
username : maxx

Sample Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Action</th>
<th>Authentication Status</th>
<th>Enroll Policy</th>
<th>Admin Email ID</th>
<th>Name</th>
<th>Admin Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/13/2019 11:43:52 AM</td>
<td>policy_create</td>
<td>Allow access without 2F</td>
<td>Require Enrollment</td>
<td><a href="mailto:maxx@contoso.com">maxx@contoso.com</a></td>
<td>Policy for bypass</td>
<td>maxx</td>
</tr>
<tr>
<td>12/13/2019 11:43:52 AM</td>
<td>policy_delete</td>
<td>No action</td>
<td>allow</td>
<td><a href="mailto:maxx@contoso.com">maxx@contoso.com</a></td>
<td>Auth_New_2fA</td>
<td>maxx</td>
</tr>
<tr>
<td>12/13/2019 11:43:52 AM</td>
<td>policy_update</td>
<td>Require Enrollment</td>
<td></td>
<td><a href="mailto:maxx@contoso.com">maxx@contoso.com</a></td>
<td>Auth_New_2fA</td>
<td>maxx</td>
</tr>
</tbody>
</table>

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

Log Considered

action : user_create
description : {"status": "Active", "notes": "", "email": "", "uname": "etadmin", "alias1": "", "realname": "", "alias2": "", "alias3": "", "alias4": ""}
Integrate Duo Security with EventTracker

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

Sample Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Action</th>
<th>Name</th>
<th>User Account Status</th>
<th>Admin Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/09/2019 06:57:19 PM</td>
<td>DUO_SECURITY</td>
<td>user_create</td>
<td>John</td>
<td>Active</td>
<td>maxx</td>
</tr>
<tr>
<td>12/09/2019 06:57:20 PM</td>
<td>DUO_SECURITY</td>
<td>user_delete</td>
<td>Mary</td>
<td>Disabled</td>
<td>System</td>
</tr>
<tr>
<td>12/09/2019 07:10:44 PM</td>
<td>DUO_SECURITY</td>
<td>user_delete</td>
<td>John</td>
<td>Disabled</td>
<td>System</td>
</tr>
<tr>
<td>12/09/2019 07:10:44 PM</td>
<td>DUO_SECURITY</td>
<td>user_pending_delete</td>
<td>John</td>
<td>Pending Deletion</td>
<td>maxx</td>
</tr>
</tbody>
</table>

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

Log Considered

- access_device : @{browser=; browser_version=; flash_version=; java_version=; os=; os_version=}
- device : +91 60051 22291
- factor : Duo Push
- integration : Microsoft RDP
- ip : 172.27.100.14
- location : @{city=; country=; state=}
- new_enrollment : False
- reason : User approved
- result : SUCCESS
- timestamp : 1575973761
- username : etadmin

**Duo Security – Offline enrollment:** This report provides information related to device enrollments, user agent detail, 2Factor authentication, user name, etc.

Sample Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>User Name</th>
<th>Reason</th>
<th>IP Address</th>
<th>Integration Name</th>
<th>Authentication type</th>
<th>Web Agent</th>
<th>Web Agent Version</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/10/2019 04:05:28 PM</td>
<td>etadmin</td>
<td>User approved</td>
<td>162.74.234.196</td>
<td>portal</td>
<td>n/a</td>
<td>Chrome</td>
<td>78.0.3904.108</td>
<td>Windows</td>
</tr>
<tr>
<td>12/10/2019 04:05:28 PM</td>
<td>etadmin</td>
<td>User approved</td>
<td>172.27.100.14</td>
<td>Microsoft RDP</td>
<td>Duo Push</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Duo Security – Login success: This report provides information related to the user entering the primary password authentication and completes 2F authentication.

Duo Security – Authentication by mobile: This report provides information related to a mobile device allowed access, mobile number, credits used for allowing access, etc.

Log Considered

context: administrator login  
credits: 1  
phone: +16005122291  
timestamp: 1575963392  
type: sms

Sample Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Mobile Credits Used</th>
<th>Mobile Number</th>
<th>Authentication Via</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/09/2019</td>
<td>Duo_SECURITY</td>
<td>1</td>
<td>+16005122291</td>
<td>sms</td>
</tr>
</tbody>
</table>

2.4 Dashboards

Duo Security – Login success: This dashboard shows login success user names into the Duo Security web console.

Figure 8

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

**Duo Security – Login failed**: This dashboard shows information about failed user login for Duo Security web console and user name.

**Duo Security – Authentication failed**: This dashboard shows information about users trying to login Duo Security web console and failed 2Factor authentication.
Integrate Duo Security with EventTracker

Duo Security – Authentication success: This dashboard shows information about users trying to login Duo Security web console and succeeds 2Factor authentication.

Duo Security – Registered mobile numbers: This dashboard shows information about user registered mobile numbers with Duo Security.
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 policy management and policy names.
3. Importing knowledge pack into EventTracker

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

- Categories
- Alerts
- Token Template/ Parsing Rules
- Flex Reports
- Knowledge Objects
- Dashboards

1. Launch the EventTracker Control Panel.
2. Double click Export-Import Utility.
3. Click the **Import** tab.

### 3.1 Categories

1. Once you have opened “**Export-Import Utility**” via “**EventTracker Control Panel**”, click the **Category** option, and then click the browse ... button.
2. Navigate to the knowledge pack folder and select the file with the extension “.iscat”, like “Categories_Duo Security. iscat” and then click on the “**Import**” button:
Integrate Duo Security with EventTracker

Figure 18

EventTracker displays a success message:

Figure 19

3.2 Alerts

1. Once you have opened “Export-Import Utility” via “EventTracker Control Panel”, click Alert option, and then click the browse button.
2. Navigate to the knowledge pack folder and select the file with the extension “.isalt”, e.g. “Alerts_Duo Security.isalt” and then click on the “Import” button:
Integrate Duo Security with EventTracker

EventTracker displays a success message:

3.3 Parsing Rule

1. Once you have opened “Export-Import Utility” via “EventTracker Control Panel”, click the Token Value option, and then click the browse button.

2. Navigate to the knowledge pack folder and select the file with the extension “.iscat”, like “Parsing Rule_Duo Security. istoken” and then click on the “Import” button:
3.4 Flex Reports

1. In the EventTracker control panel, select “Export/ Import utility” and select the “Import tab”. Then, click Reports option, and choose “New (*.etcrx)”: 
2. Once you have selected “New (*.etcrx)”, a new pop-up window will appear. Click the “Select File” button and navigate to the knowledge pack folder and select file with the extension “.etcrx”, e.g. “Reports_Duo Security.etcrx”.

3. Wait while reports are being populated in the below tables. Now, select all the relevant reports and then click the **Import** button.
Integrate Duo Security with EventTracker

EventTracker displays a success message:

3.5 Knowledge Objects

1. Click **Knowledge objects** under the **Admin** option in the EventTracker web interface.

2. Next, click the “import object” icon:
3. A pop-up box will appear, click “Browse” in that and navigate to the knowledge packs folder (type “C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs” in the navigation bar) with the extension “.etko”, e.g. “KO_Duo Security.etko” and then click the “Upload” button.

![Figure 30](Image)

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones and click on the “Import” button:

![Figure 31](Image)

### 3.6 Dashboards

1. Login to the EventTracker web interface.
2. Navigate to Dashboard → My Dashboard.
3. In “My Dashboard”, Click Import Button:

![Figure 32](Image)
4. Select the browse button and navigate to the knowledge pack folder (type “C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs” in the navigation bar) where “.etwd”, e.g. “Dashboard_Duo Security.etwd” is saved and click on “Upload” button.

5. Wait while EventTracker populates all the available dashboards. Now, choose “Select All” and click on “Import” Button.

4. Verifying knowledge pack in EventTracker

4.1 Categories

1. Login to the EventTracker web interface.
2. Click Admin dropdown, and then click Categories.
3. In **Category Tree** to view imported categories, please click on “Search” and search with the “Duo Security”. You will see the below results:

![Category Tree](image)

Figure 36

### 4.2 Alerts

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In search box enter “**Duo Security**” and then click the **Search** button.

EventTracker displays an alert related to Duo Security:

![Alerts](image)

Figure 37

### 4.3 Parsing Rules

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Parsing Rule**.
2. In the **Parsing Rule** tab, click on the “**Duo Security**” group folder to view the imported Token Values.
4.4 Flex Reports

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

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

4.5 Knowledge Objects

1. In the EventTracker web interface, click the Admin dropdown, and then click Knowledge Objects.
2. In the Knowledge Object tree, expand the “Duo Security” group folder to view the imported Knowledge objects.
4.6 Dashboards

1. In the EventTracker web interface, Click on Home Button and select “My Dashboard”.

2. In “Duo Security” dashboard you should be now able to see something like this: