Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating Duo Security with EventTracker

Publication Date:

October 14, 2021

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

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

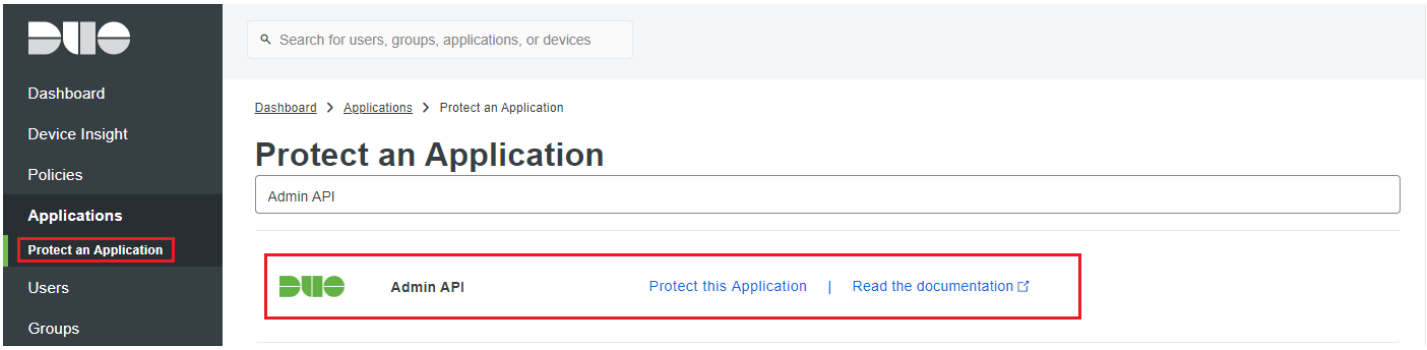
- Host machine should have installed the EventTracker Sensor.
- Administrator privilege for the Duo Security web interface.
- PowerShell 5.0 and later should be installed on the Duo integrator host machine.

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 Web interface of the Duo Security.
2. Click the **Application** tab and click the **Protect an Application** option as shown in the following image.



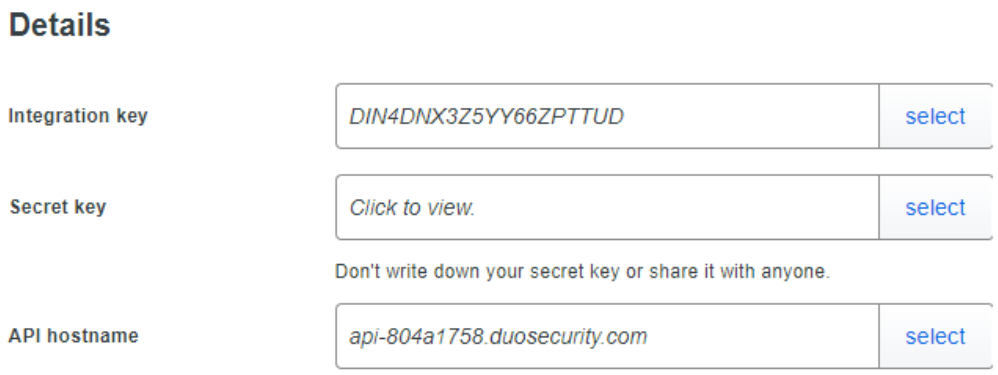
3. Click the option **Protect this Application** under the **Admin API** header.

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 Duo Security Support.

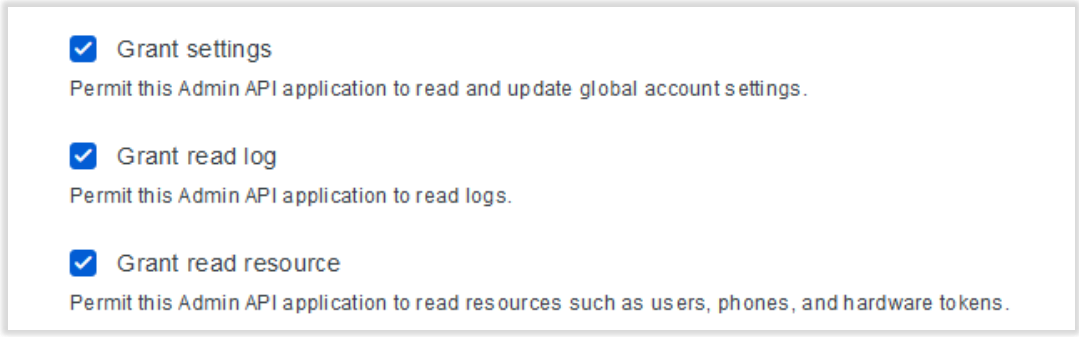
4. After completed, you will get the required credentials for integration of the Duo Security with the EventTracker.
   - Integration Key
   - Secret Key

- API hostname

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



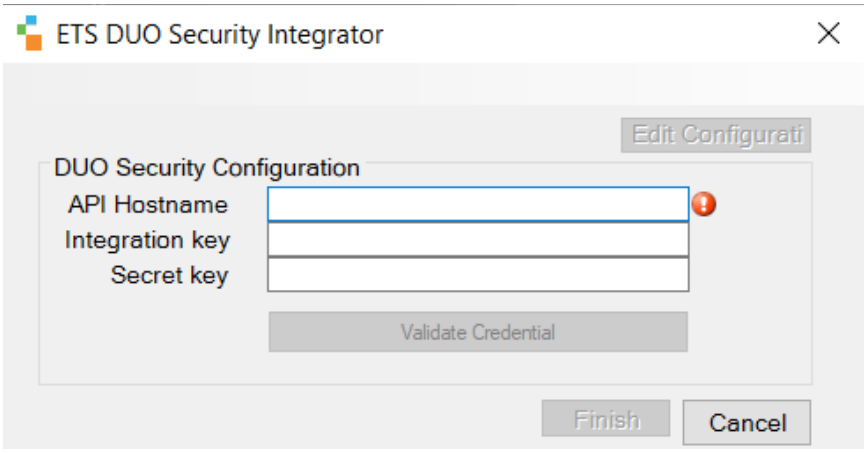
6. Select all the below permissions from the **Permissions** section and click **Save Changes**.



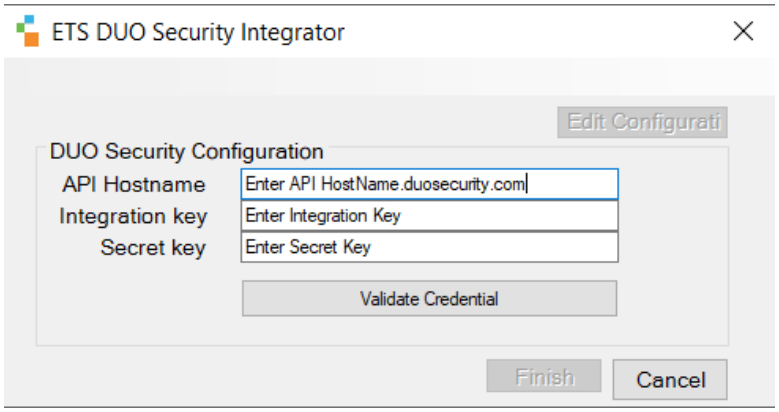
Following are the steps to integrate the Duo Security with the EventTracker.

1. Get the **Duo Security Integrator** executable file.
   https://downloads.eventtracker.com/kp-integrator/ETS_DuoSecurity_Integrator.exe

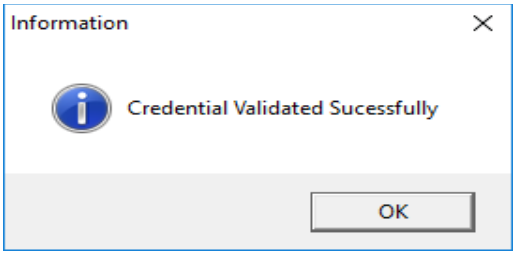
2. After the executable application is received, click the file.



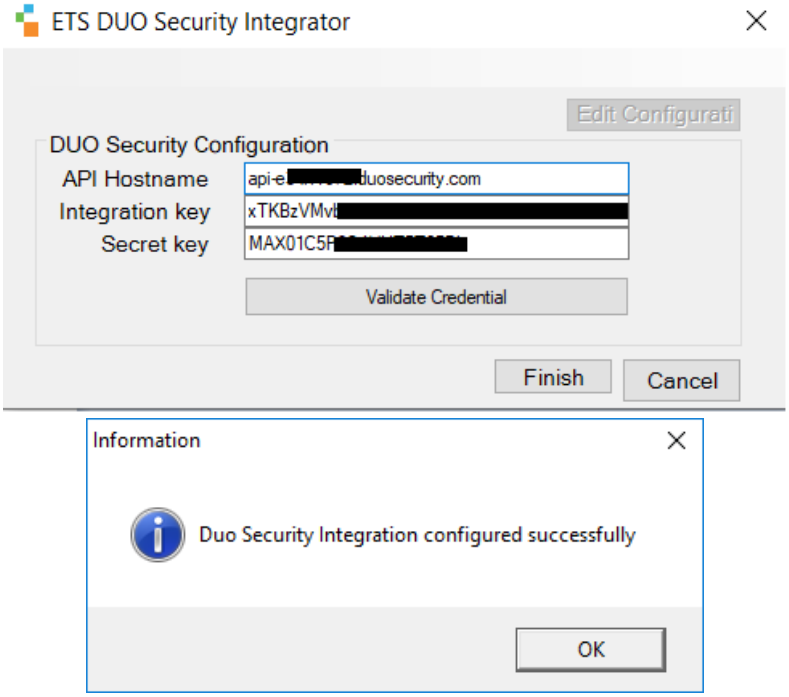
3. The **Duo Integrator** window display. Fill in the **Integration Key**, **Secret Key**, and **API HostName** as received from the web interface of the Duo Security.



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



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



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 fraudulent, 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.

LogTime	Reason	Device Ip address	Application	New enrollment	Admin Name	Authentication 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.

LogTime	Action	Reason	2Factor Authentication Type	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	Maxx

- **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
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

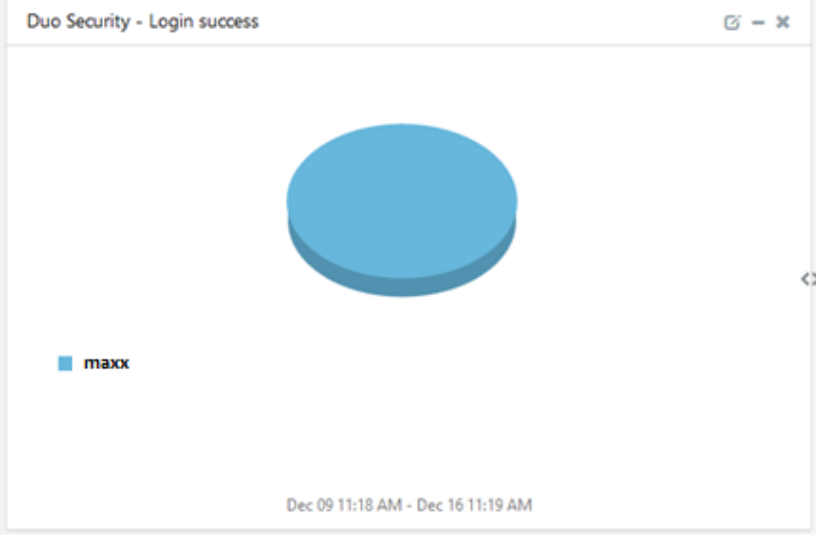
- **Duo Security – Authentication success:** This report provides information related to authentication success allowed by policy, bypass username, remembered device, trusted location, trusted network, approved by the user, etc.

LogTime	User Name	Reason	IP Address	Integration Name	Authentication type	Web Agent	Web Agent Version	Operating System
12/10/2019 04:05:28 PM	etadmin		182.74.234.198	portal	n/a	Chrome	78.0.3904.108	Windows
12/10/2019 04:05:28 PM	etadmin	User approved	172.27.100.14	Microsoft RDP	Duo Push			

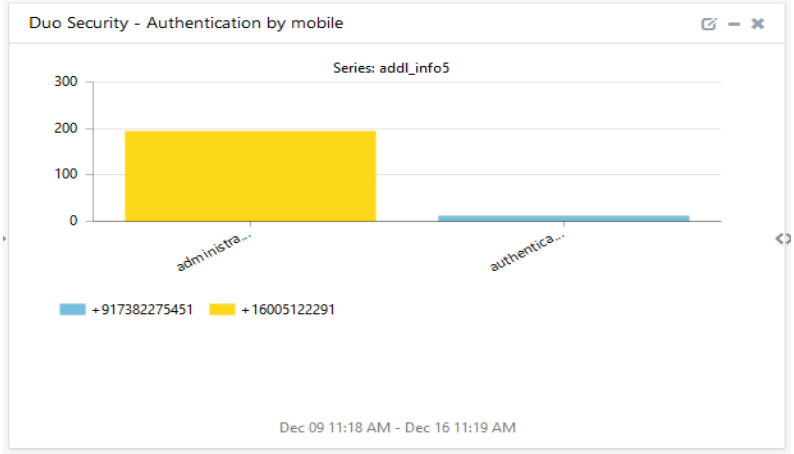
- **Duo Security – Offline enrollment:** This report provides information related to the device enrollments, user agent detail, the 2FA, username, etc.
- **Duo Security – Login success:** This report provides information related to user entering the primary password authentication and completing the 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

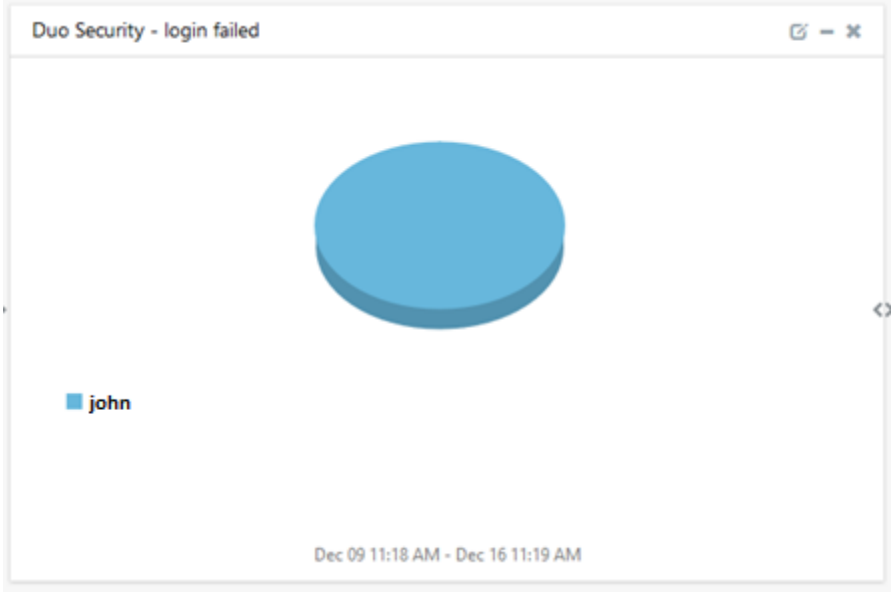
- **Duo Security – Login success:** This dashboard shows login success usernames into the Duo Security web console.



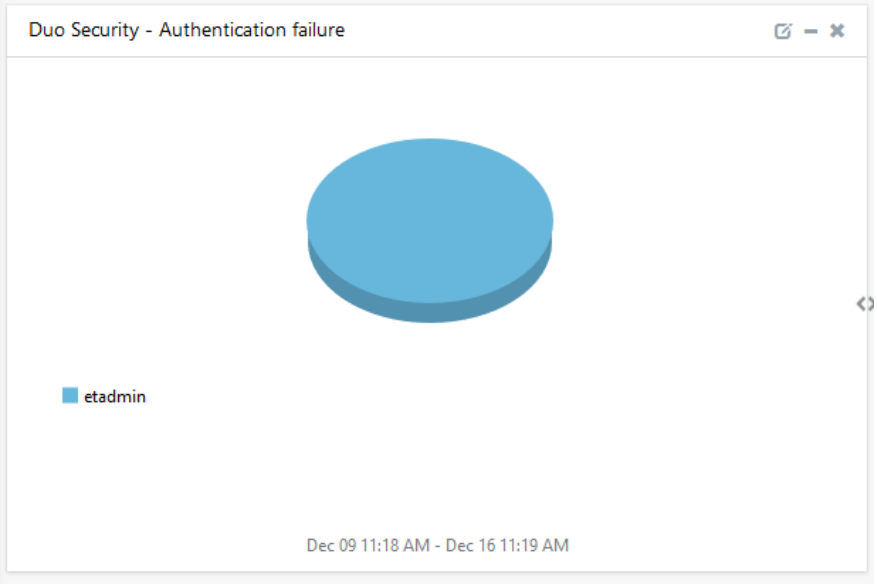
- **Duo Security – Authentication by mobile:** This dashboard shows information about the user who tries to login to the Duo Security web console by using the configured mobile numbers.



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

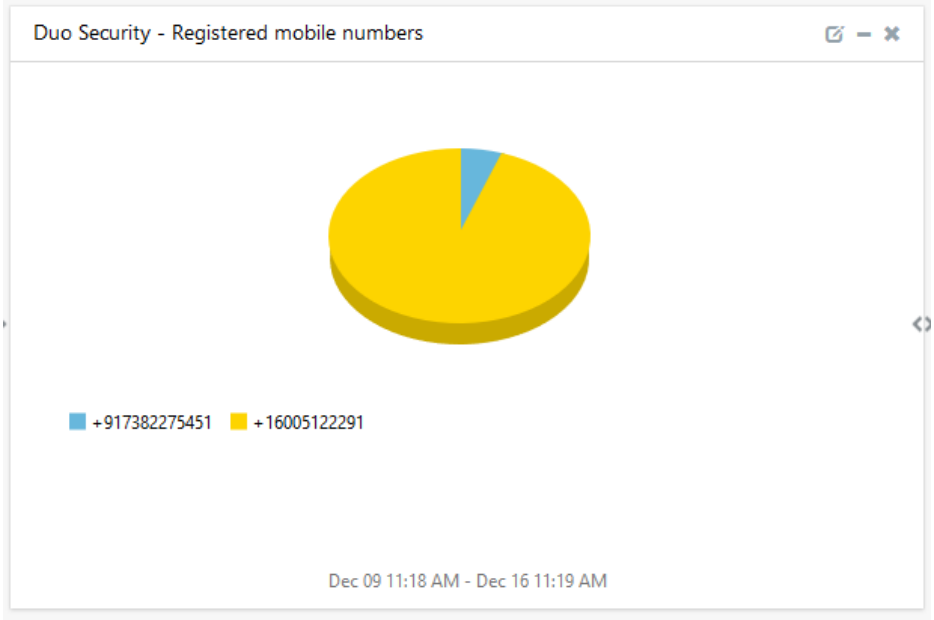


- **Duo Security – Authentication failure:** This dashboard shows information about users trying to login to the Duo Security web console and the failed 2FA attempts.

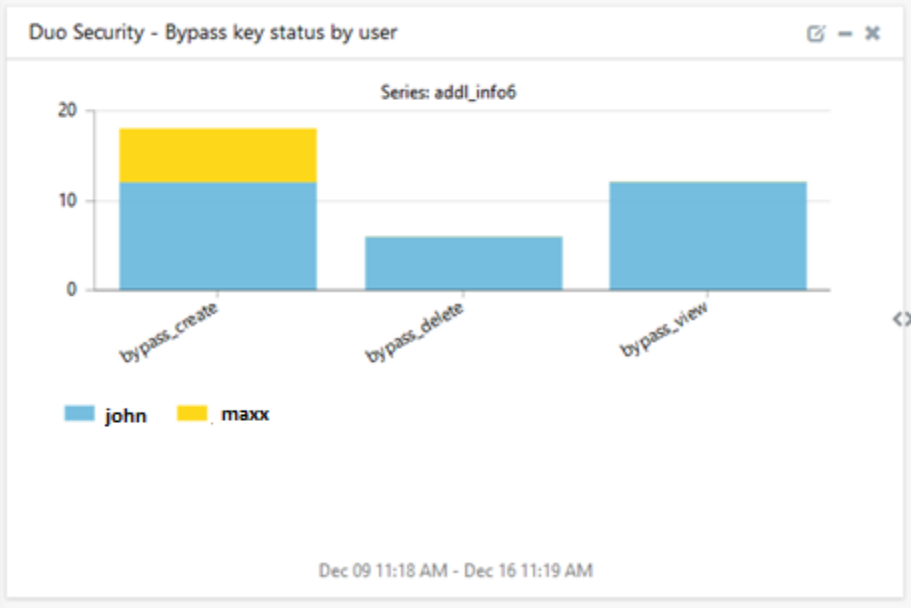


- **Duo Security – Authentication success:** This dashboard shows information about users trying to login to the Duo Security web console and succeeds the 2FA attempts.

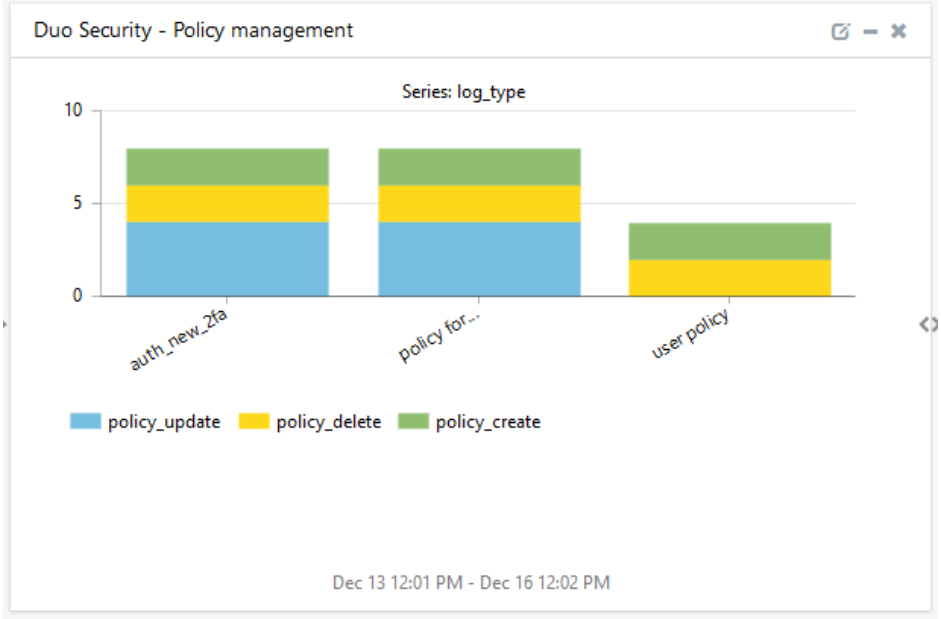
- **Duo Security – Registered mobile numbers:** This dashboard shows information about user-registered mobile numbers with the Duo Security.



- **Duo Security – 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

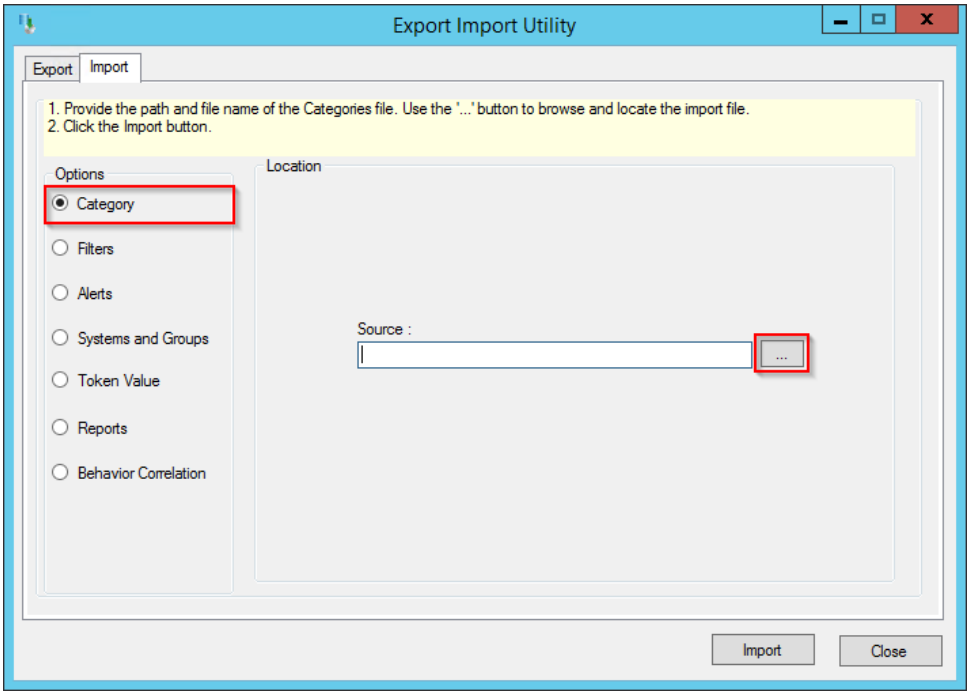
- Knowledge Object
- Reports
- Dashboard

1. Launch the **EventTracker Control Panel**.
2. Double click **Export Import Utility**.

3. Click the **Import** tab.

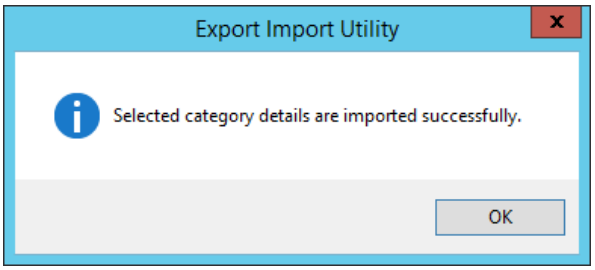
5.1 Category

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



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

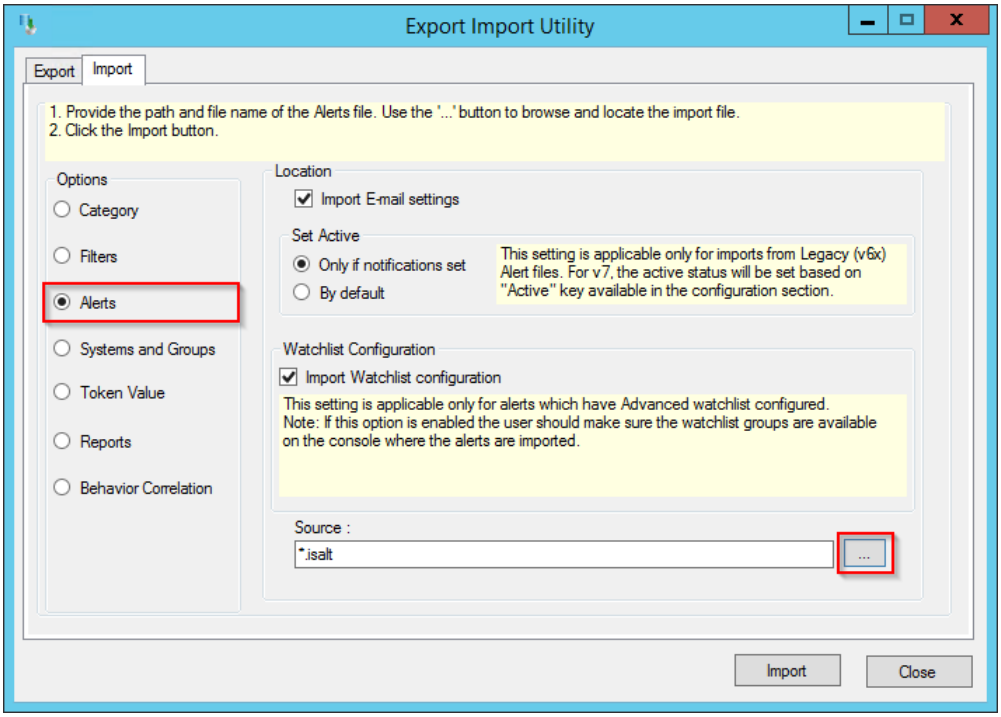
   EventTracker displays a success message.



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

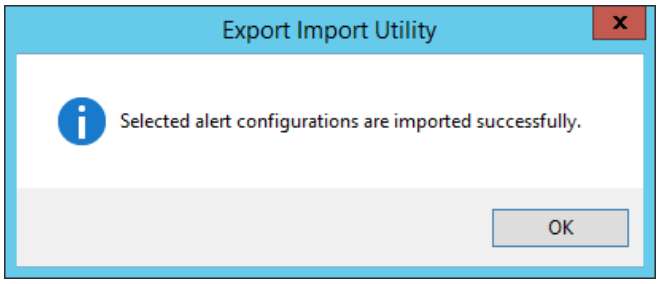
5.2 Alerts

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



2. Locate the **Alerts_Duo Security.isalt** file, and then click the **Open** button.
3. To import the alerts, click the **Import** button.

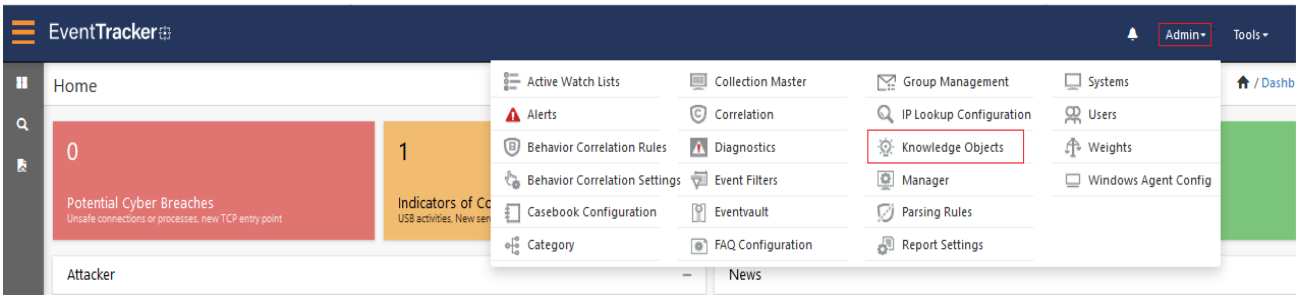
   EventTracker displays a success message.



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

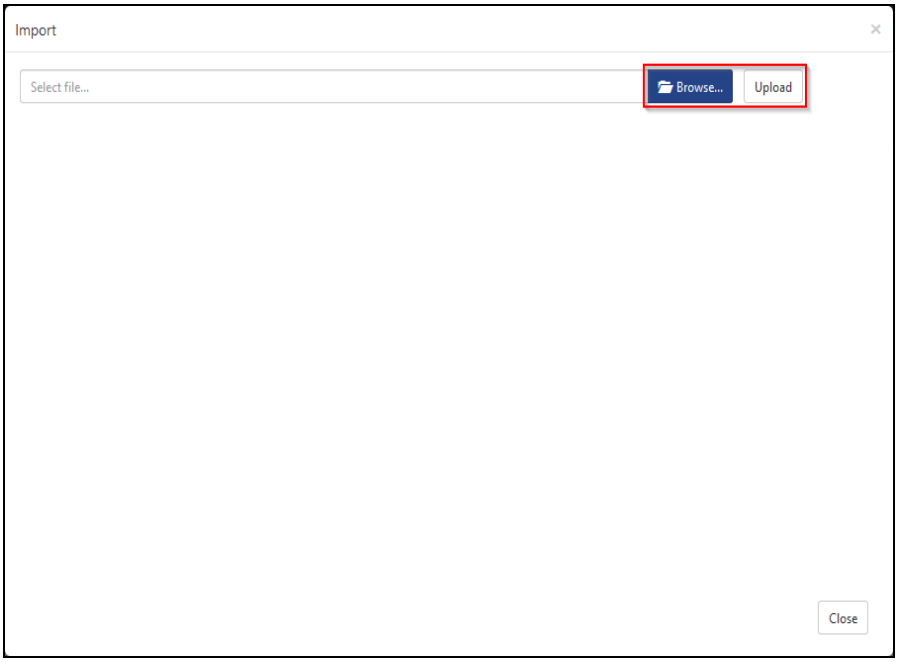
5.3 Knowledge Objects (KO)

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

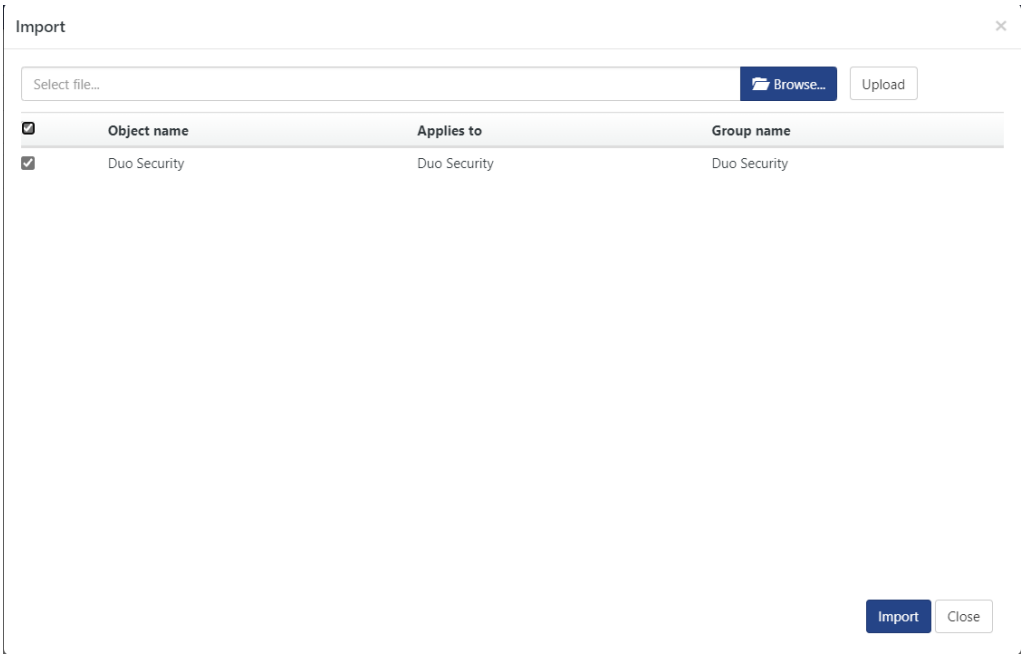


2. Click the **Import** button as highlighted in the below image.

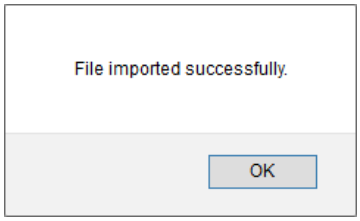
3. Click the **Browse** button.



4. Locate the file named **KO_Duo Security.etko**.
5. Select the check box and then click the **Import** option.

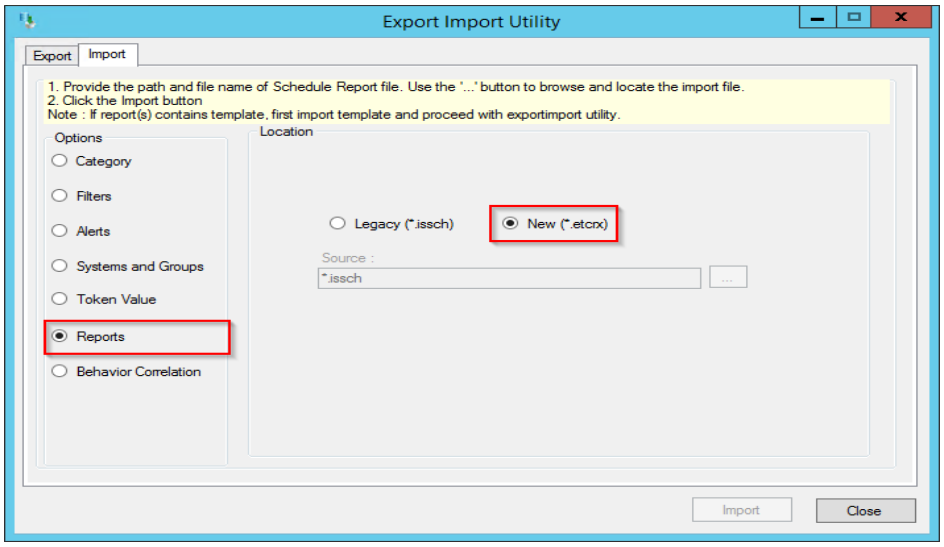


6. The Knowledge Objects are now imported successfully.

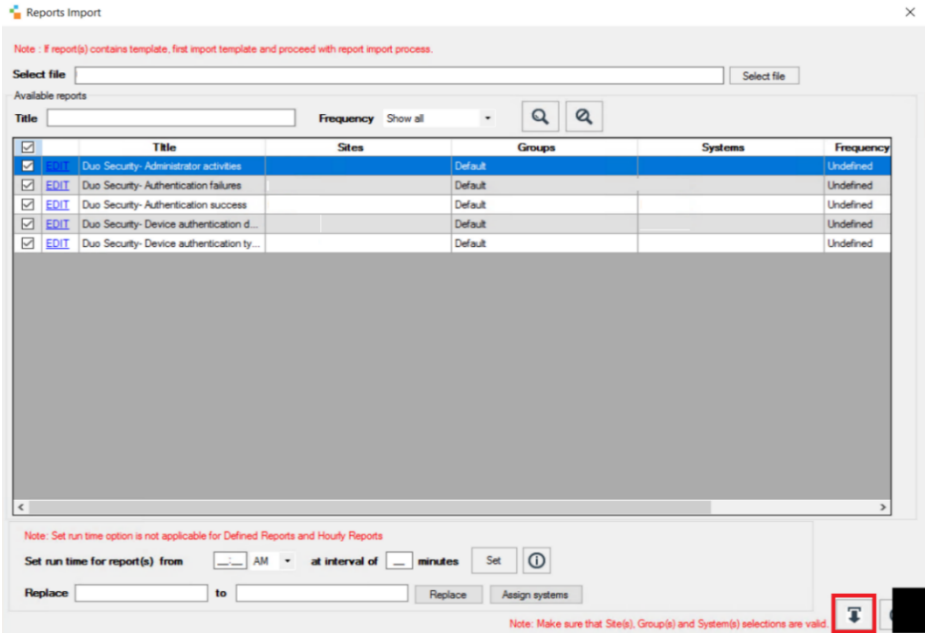


5.4 Reports

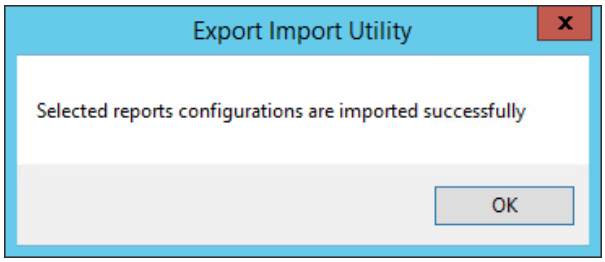
1. Click the **Reports** option and select the **New (*.etcrx)** option.



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



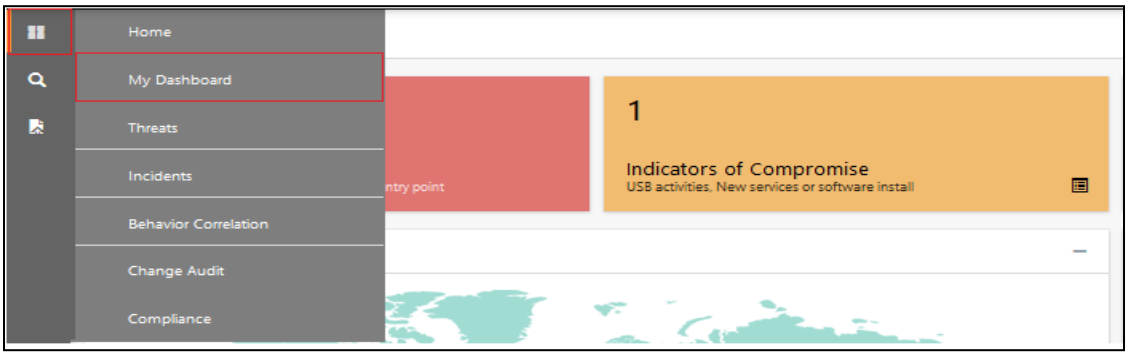
3. Click the **Import** button to import the report. EventTracker displays a success message.



5.5 Dashboards

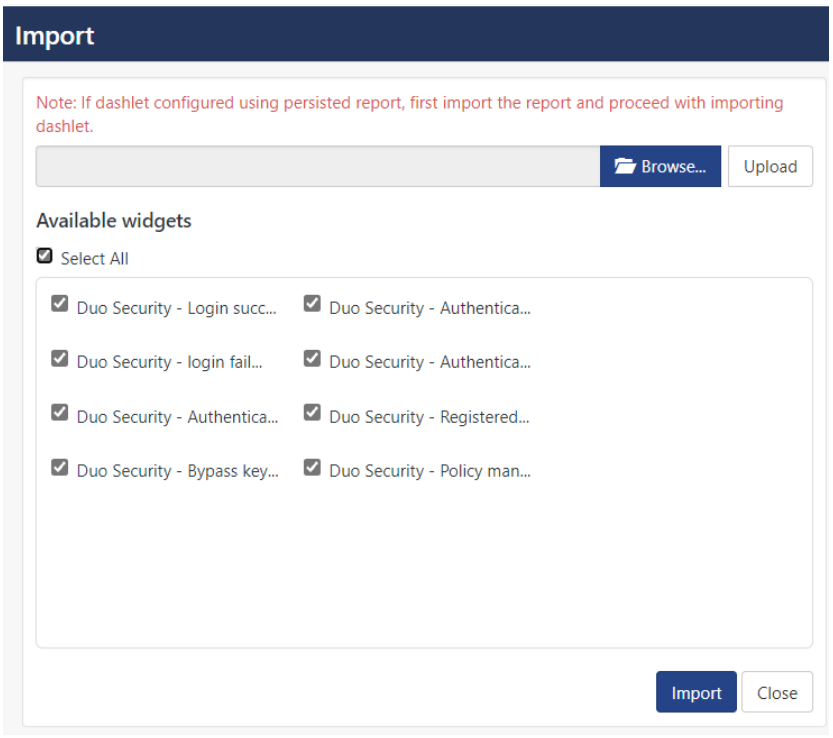
NOTE: Below steps given are specific to the EventTracker 9 and later.

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

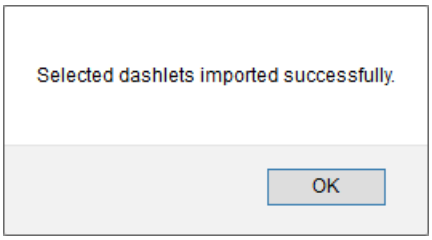


2. Navigate to the **My Dashboard** option as shown above.
3. Click the **Import** button as show below.

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

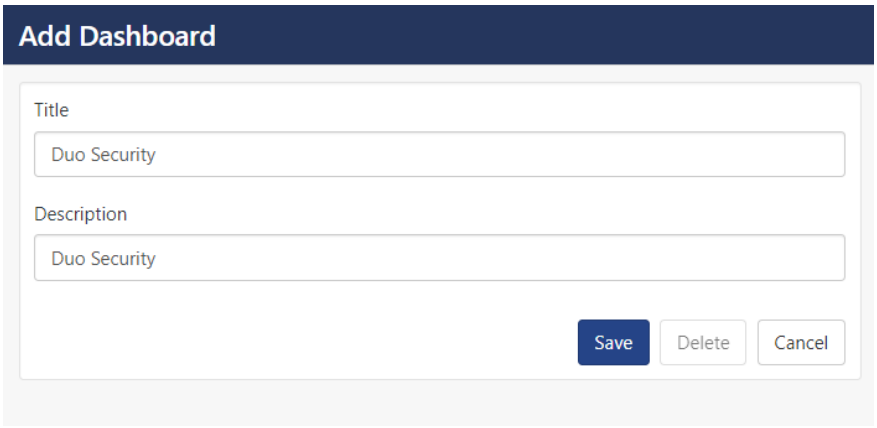


6. The Import is successfully completed.

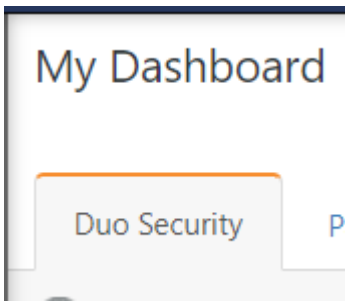


7. In the **My Dashboard** page select ⊕ to add the dashboard.

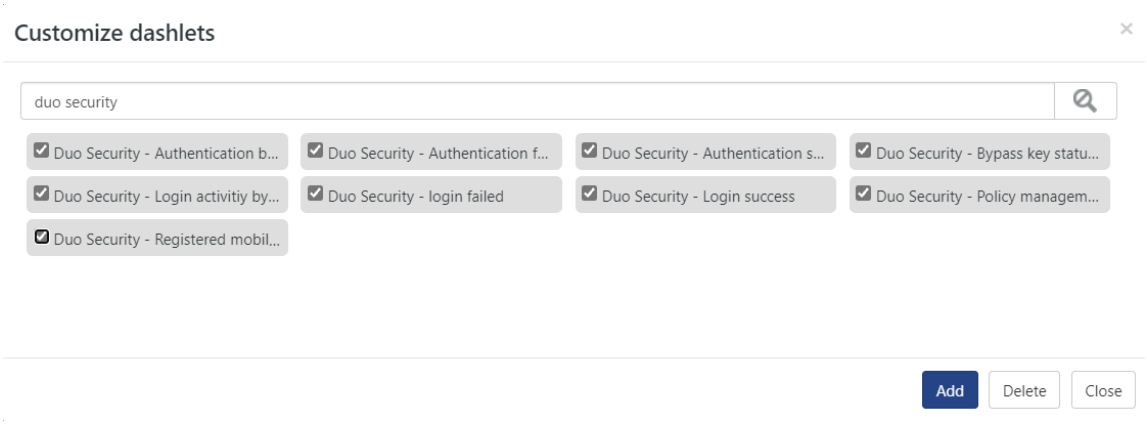
8. Choose the appropriate name for the **Title** and **Description**. Click **Save**.



9. In the **My Dashboard** page select to add the dashlets.



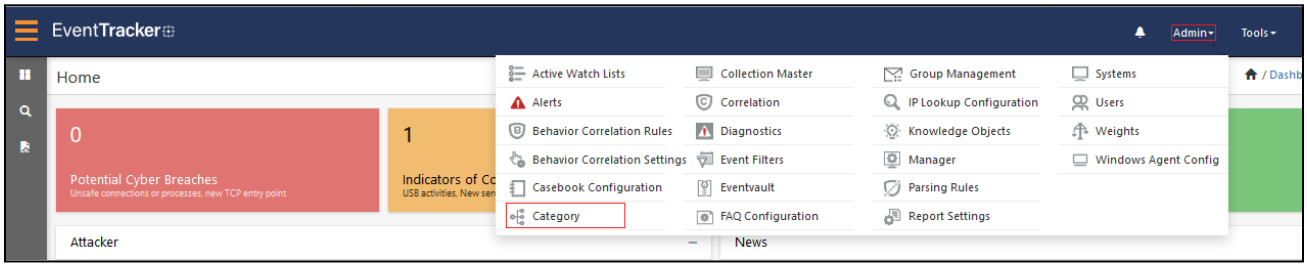
10. Select the imported dashlets and click **Add**.



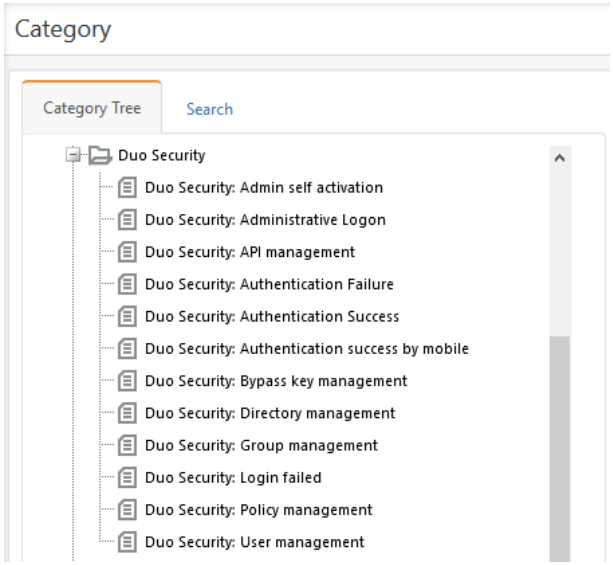
6. Verifying the Duo Security Knowledge Pack in the EventTracker

6.1 Category

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

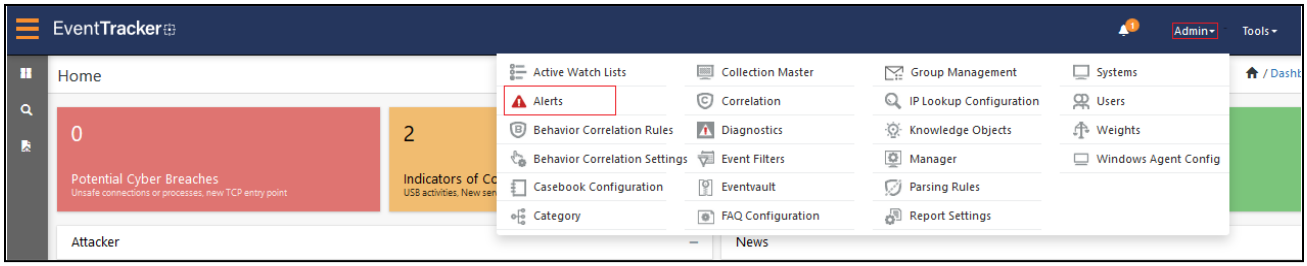


3. In the **Category Tree** to view the imported category, scroll down and expand the **Duo Security** group folder to view the imported category.

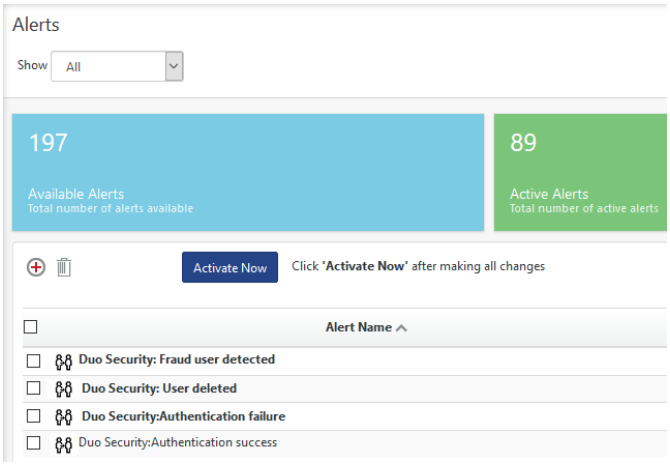


6.2 Alerts

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

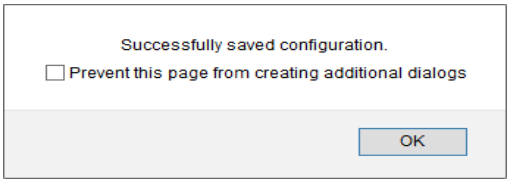


3. In the **Search** box, type **Duo Security**, and then click the **Go** button.
   Alerts Management page will display the imported alert.



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

   EventTracker displays a message box.

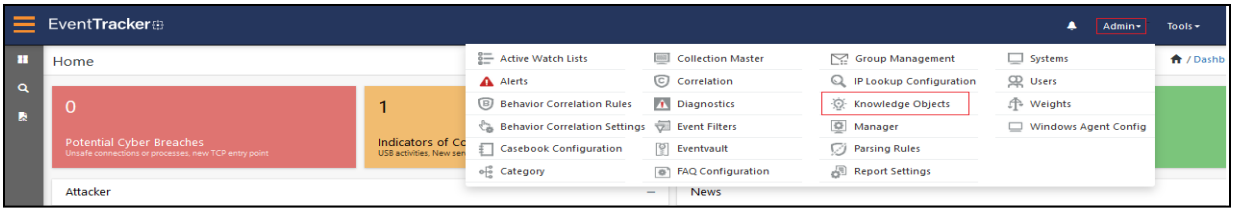


5. Click **OK**, and then click the **Activate Now** button.

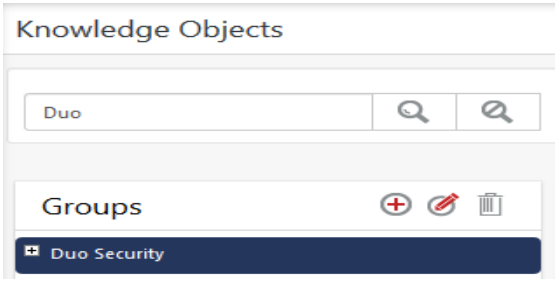
NOTE**:** Specify the appropriate **system** in the **alert configuration** for better performance.

6.3 Knowledge Objects

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



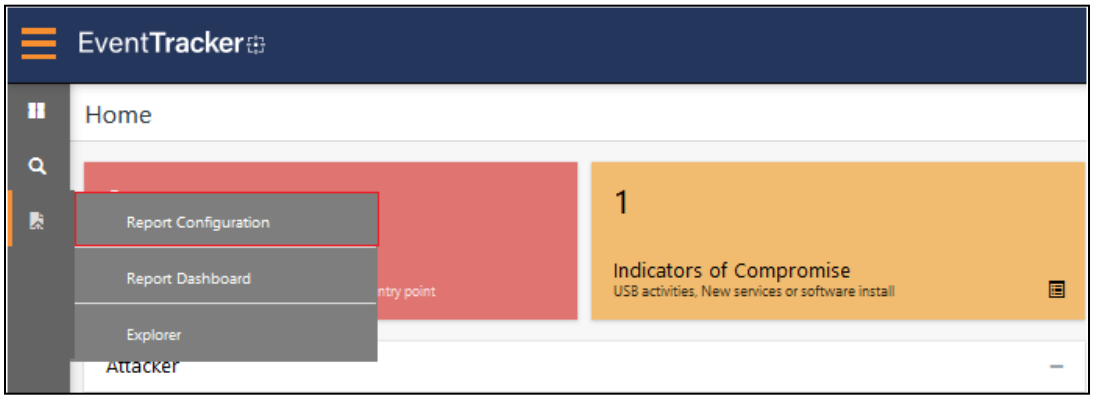
2. In the Knowledge Objects tree, expand the **Duo Security** group folder to view the imported Knowledge Objects.



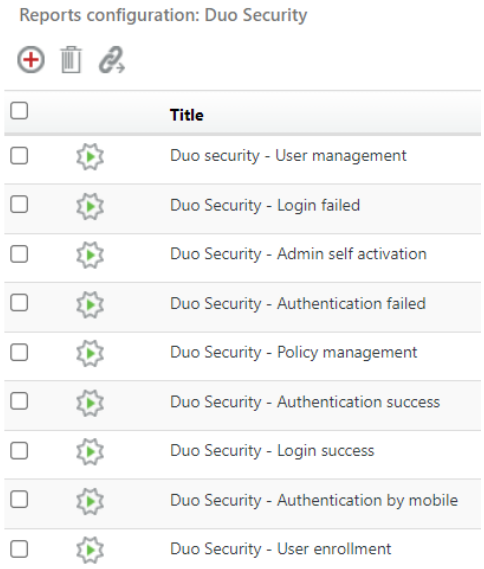
3. Click **Activate Now** to apply the imported Knowledge Objects.

6.4 Reports

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

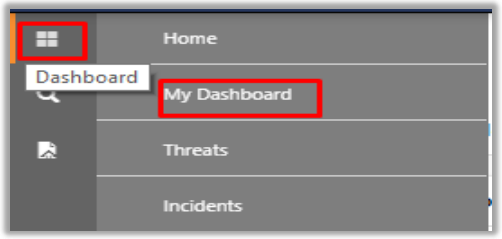


2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click the **Duo Security** group folder to view the imported reports.

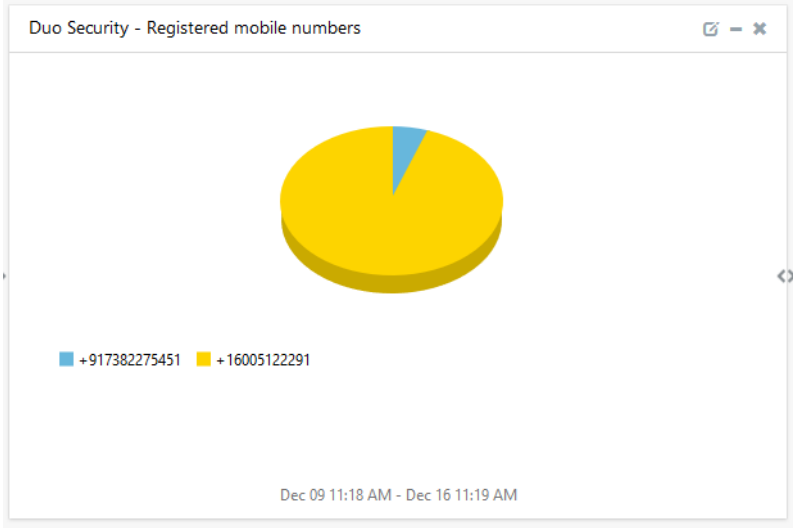


6.5 Dashboards

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



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 EventTracker 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 BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location 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 netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #23 among MSSP Alert's 2021 Top 250 MSSPs.

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