

Integrate Varonis

EventTracker v9.2 and later

Abstract

This guide provides instructions to retrieve the **Varonis** events via syslog. Once the logs start coming into EventTracker, reports, dashboards, alerts and saved searches can be configured.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.2 or above and **Varonis 6.3.190 and above**.

Audience

Administrators who are assigned the task to monitor **Varonis** events using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

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

Table of Contents

1. Overview.....	3
2. Prerequisites.....	3
3. Integrating Varonis with EventTracker.....	3
3.1 Configuring syslog message forwarding	3
3.2 Configuring syslog format.....	4
3.3 Configuring alerts for single or multiple rules	6
4. EventTracker knowledge packs	8
4.1 Saved searches.....	8
4.2 Alerts.....	9
4.3 Flex reports	9
4.4 Dashboards	11
5. Importing knowledge pack into EventTracker	14
5.1 Saved searches.....	15
5.2 Alerts.....	16
5.3 Token template.....	17
5.4 Flex reports	18
5.5 Knowledge objects.....	20
5.6 Dashboards	21
6. Verifying knowledge pack in EventTracker	23
6.1 Saved searches.....	23
6.2 Alerts.....	23
6.3 Token template.....	24
6.4 Flex reports	24
6.5 Knowledge objects.....	25
6.6 Dashboards	26

1. Overview

Varonis is a Data Security Platform that detects insider threats and cyberattacks by analyzing data, account activity and user behavior. It prevents and limits disaster by locking sensitive, and stale data and efficiently sustains a secure state with automation.

Varonis integrates with EventTracker SIEM application to provide security analytics with deep data context, so that organizations can be confident in their data security strategy. Benefits include scheduled reports, integrated Varonis dashboards and alerts for streamlined investigation.

Reports contain a detailed summary of events associated with exchange server activity, CIFS and NFS activity, share-point activity, and active directory activity.

Alerts are triggered as soon as critical events are received by EventTracker for Varonis, such as file permission change, file/folder deletion, password change or update, user lockout etc.

Dashboard is a graphical representation of all the activities happening in Varonis. These include event categories with cumulative log counts or percentage or by timeline.

These attributes or configurations of EventTracker allows administrators to quickly take appropriate actions against any threat/adversaries trying to jeopardize an organizations normal operation.

2. Prerequisites

- EventTracker v9.2 and above should be installed.
- Administrative/root access to Varonis UI.
- Syslog port (e.g. 514) should be allowed in firewall.
- EventTracker Manager public IP address (if Varonis is cloud based).

3. Integrating Varonis with EventTracker

3.1 Configuring syslog message forwarding

User can configure the syslog server address in DatAlert so that alerts are sent to EventTracker.

1. Login into your Varonis UI using admin credentials.
2. In DatAdvantage, select **Tools > DatAlert**. (DatAlert is displayed)
3. From the left menu, select **Configuration**.
4. In **syslog message forwarding**, do as follows.

- **Syslog server IP address** - The IP address of the EventTracker server on which you plan to setup a UDP listener.
 - **Port** - The port on which the EventTracker server will be listening
5. In the top-right corner, click **Syslog Settings**.

The screenshot shows the 'DatAlert' application window with the 'Configuration' tab selected. The left sidebar contains 'Rules', 'Configuration', 'Alert Templates', and 'Predefined Scopes'. The main area is titled 'Configuration' and includes a 'Restore Default Settings' button. Below this are three sections: 'Mail Settings', 'Syslog Message Forwarding', and 'SNMP Trap'.

Mail Settings:

- Aggregate similar events over: 5 minutes into a single message
- Threshold for suppressing messages: 20 messages within 5 minutes
- Select header image: Varonis DataAlert logo

Syslog Message Forwarding:

- Syslog server IP address: 10.10.34.40
- Port: 514
- Facility name: 1 - user-level messages
- Identity: Varonis - DatAlert
- Buttons: Add Additional Syslog Server, Test Message

SNMP Trap:

- SNMP server IP address: (empty)
- Port: 162
- Community name: public
- OID: (empty)
- Buttons: Add Additional SNMP Server, Test Message

At the bottom right are buttons for 'OK', 'Cancel', and 'Apply'.

Figure 1

6. Click OK.

3.2 Configuring syslog format

1. In **DatAlert**, from the left menu, click **Alert Templates**.

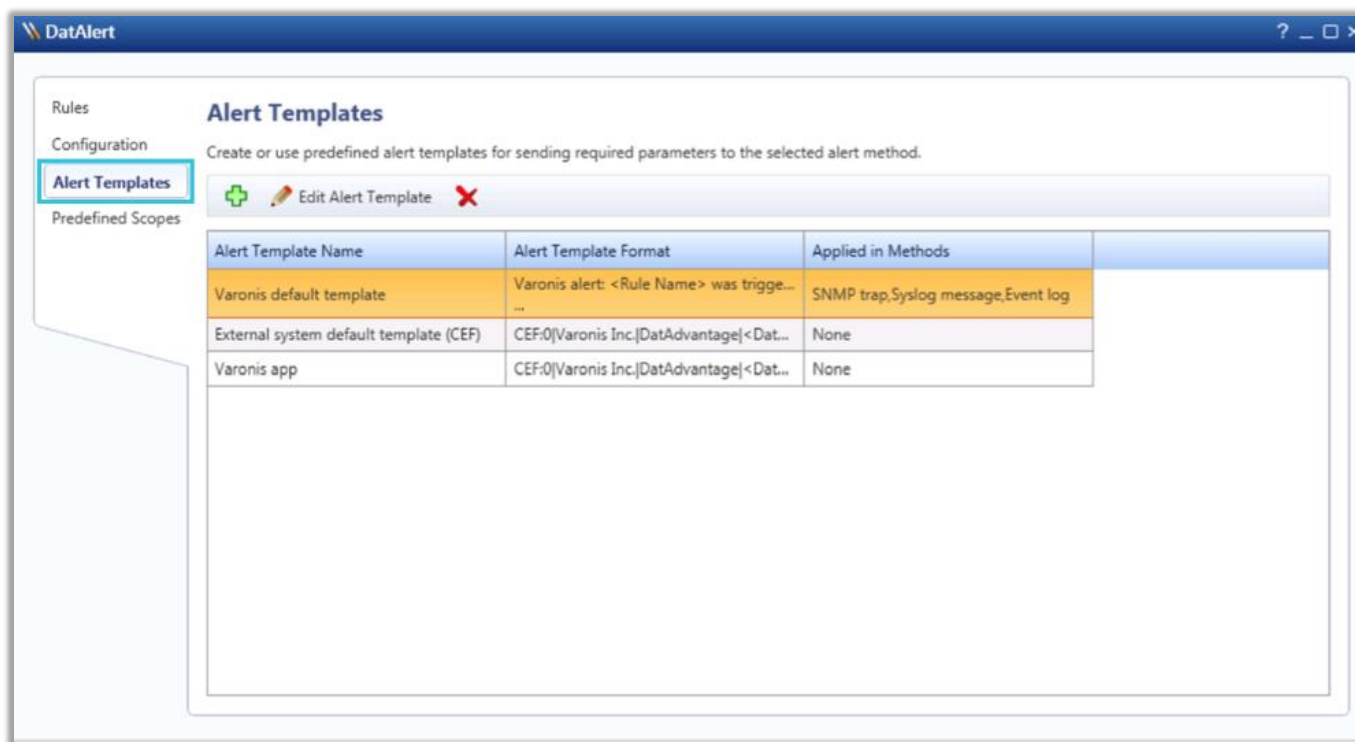


Figure 2

2. Click the green plus sign to add a new alert template:
 - Enter a **template name**. e.g. EventTracker syslog (CEF)
 - Open the **Apply to alert methods** dropdown list and select **Syslog message**.
 - Create a new **Alert Template Format** using the example templates below:
 - Manually edit the cs4 section, where DLS_IP_ADDRESS is the IP address or host name of the server running the Varonis Web UI.

```
CEF:0|Varonis Inc.|DatAdvantage|<DatAdvantage version>|<Event Op Code>|<Event
Type>|<Severity>|rt=<Alert Time> cat=Alert cs2=<Rule Name> cs2Label=RuleName cn1=<Rule
ID> cn1Label=RuleID end=<Event Time> duser=<Acting Object> dhost=<File Server/Domain>
filePath=<Access Path> fname=<Affected Object> act=<Event Type> dvchost=<Device Name>
dvc=<Device IP Address> outcome=<Event Status> msg=<Additional Data> cs3=<Attachment
Name> cs3Label=AttachmentName cs4=
http://<DLS_IP_ADDRESS>/DatAdvantage/#/app/analytics/entity/Alert/<Alert ID>
cs4Label=ClientAccessType deviceCustomDate1=<Mail Date> fileType=<Mail Item Type>
cs1=<Mail Recipients> cs1Label=MailRecipient suser=<Mail Source> cs5=<Mailbox Access
Type> cs5Label=MailboxAccessType cnt=<Threshold> cs6=<Changed Permissions>
cs6Label=ChangedPermissions oldFilePermission=<Permissions Before Change>
filePermission=<Permissions After Change> dpriv=<Trustee> start=<First Event Time>
```

e.g.

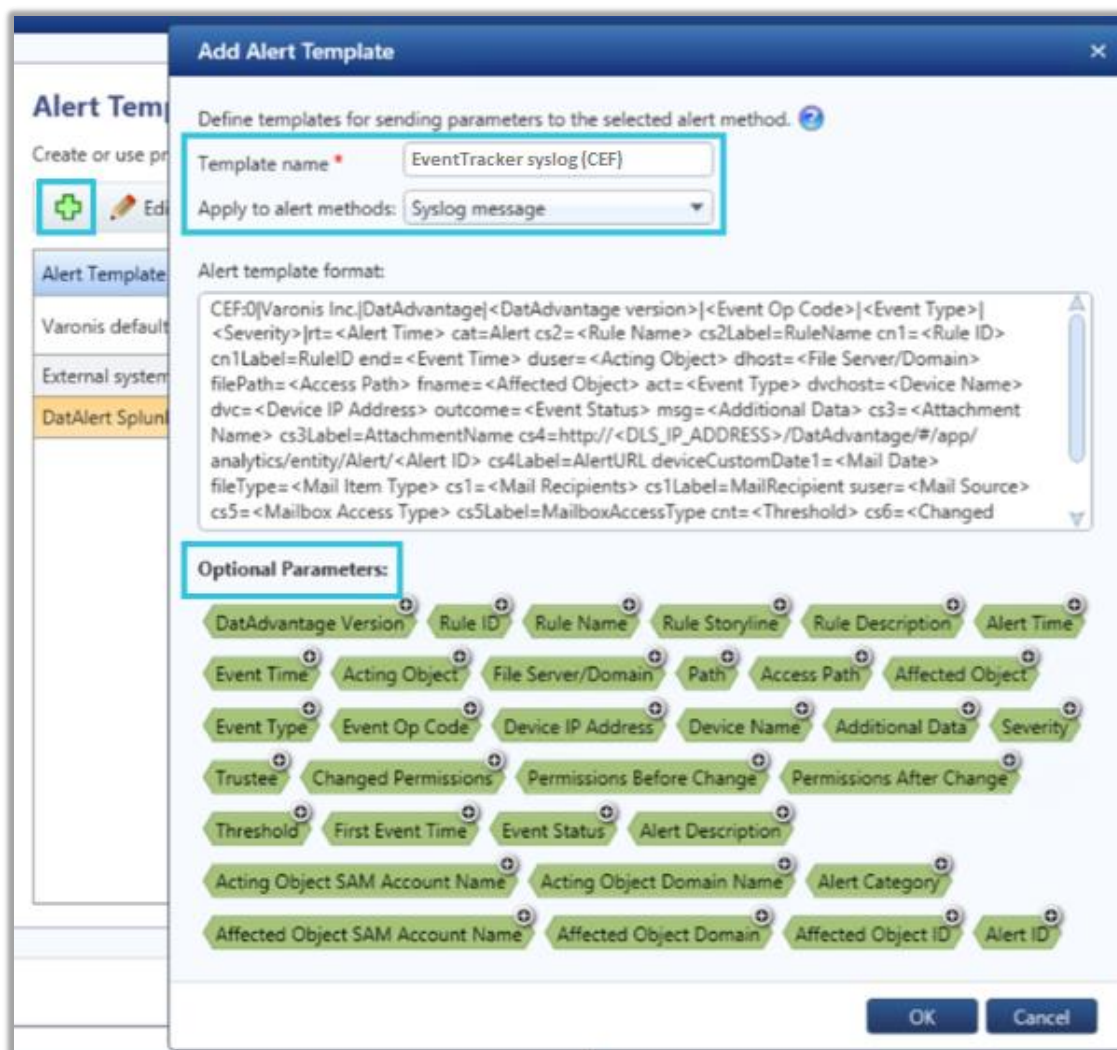


Figure 3

3. Click **OK** and verify that the new template appears in the “**Alert Templates**” table.
4. Click **OK**.

3.3 Configuring alerts for single or multiple rules

To send the events triggered by the rules to EventTracker, the alert must be forwarded by creating a syslog message.

To select the syslog alert method for a single rule.

1. From the DatAlert rules table, select the rule, then click **Edit Rule**. The rule editing menu appears.
2. From the left menu, select **Alerts Method**. The “Alert Method” window appears.

3. Select **syslog message**.
4. Click **OK**.

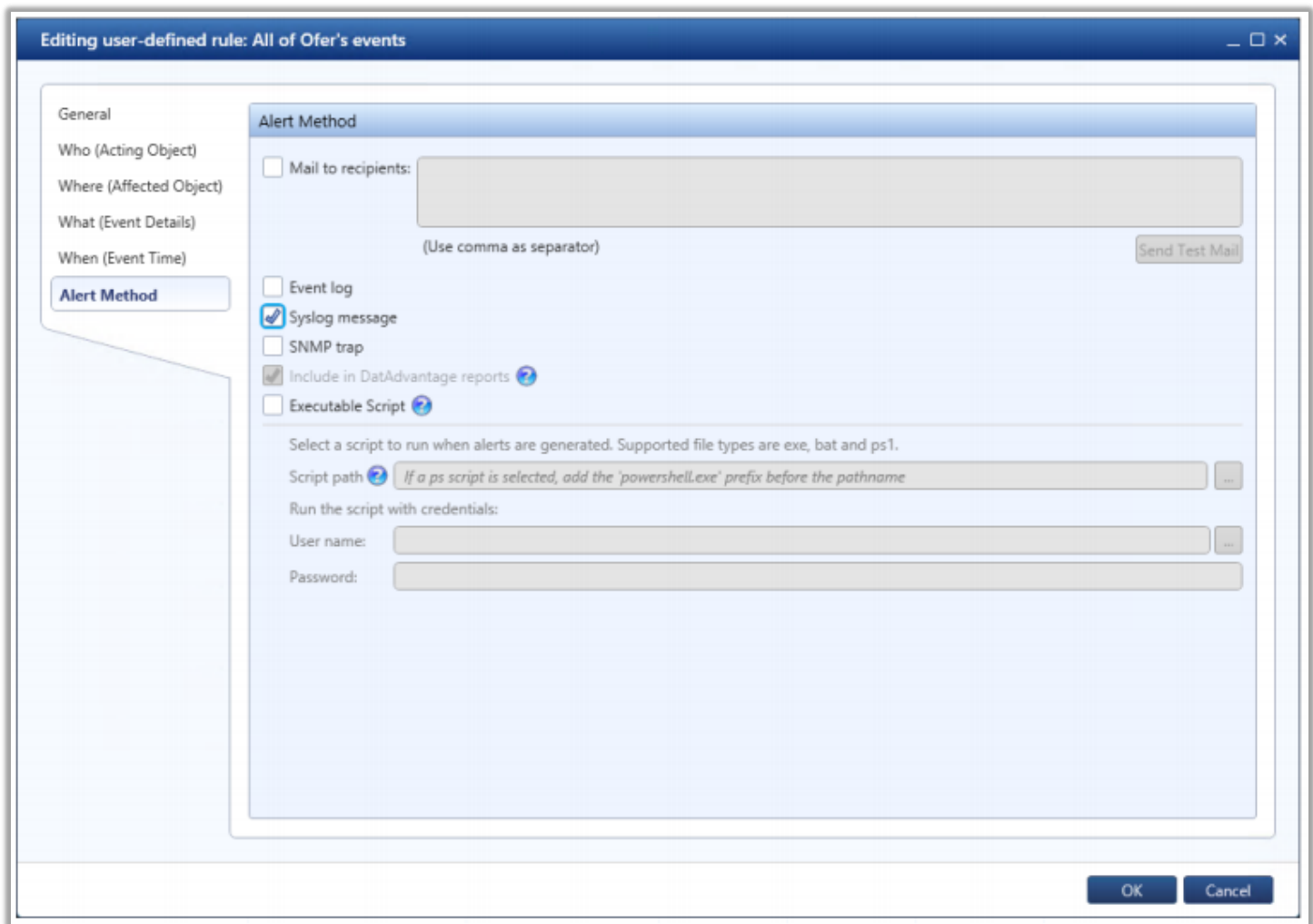



Figure 4

To select the syslog alert method for multiple rules:

1. From the DataAlert rules table, select the rules, then click **Edit Rule**. The rule editing menu appears.
2. From the left menu, select **Alerts Method**. Note that the window's contents are disabled for selection.
3. To enable **syslog message** for selection, click the edit  icon and select the checkbox.
4. Click **OK**.

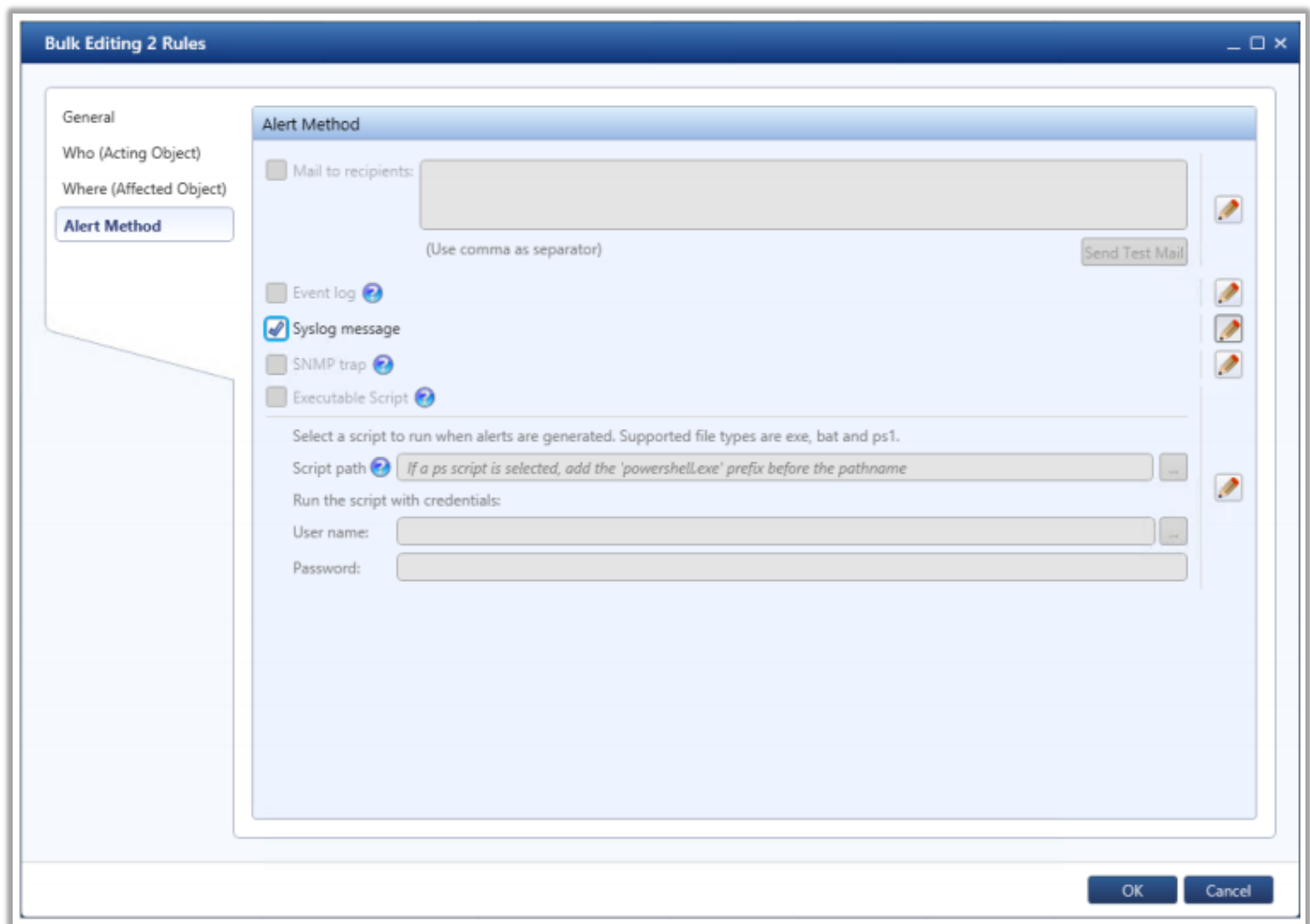


Figure 5

4. EventTracker knowledge packs

4.1 Saved searches

Saved searches are designed to quickly parse/filter logs and allow user to see only specific events related to:

- **Varonis - Domain service activities** - This category of saved searches allows users to quickly parse and display events associated with active directory domain service activities such as, DS object added, DS object modified, etc.

- **Varonis - Exchange folder activities** - This category of saved searches allows users to quickly parse and display events associated with exchange server folder activities, such as folder opened, folder, created, etc.
- **Varonis - File permissions** - This category of saved searches allows users to quickly parse and display events associated with file system permissions, such as file permission added, removed, etc.
- **Varonis - Mailbox permissions** – This category of saved searches allows users to quickly parse and display events associated with exchange server mailbox permissions, such as permissions added, removed, etc.
- **Varonis - User account status** – This category of saved searches allows users to quickly parse and display events associated with active directory user account lock out and unlock.

4.2 Alerts

Alerts are triggered when an event received is identified as critical and requires immediate notification. Such as,

- **Varonis: A user has been locked out** – This alert is triggered as soon as EventTracker receives an event specifying locking out of any user.

4.3 Flex reports

Reports are a detailed overview of any event occurring in Varonis, represented in column-value format.

- **Varonis - AD domain service and user status activities** – This report outlines a detailed overview of events related to active directory activities, such as creation and deletion of all objects, Lock/unlock accounts, etc. This will include event datetime, action taken, affected object name, etc.

LogTime	Action	Affected object	Event Category	Event ID	File Path	File Server/Domain	Rule ID	Rule Name	Source device name	Source user	Status
08/26/2020 08:50:48 PM	User unlocked	Chris Brown	Alert	5012	contoso.com\Domain Users/Users/SLC/ReDirection-USB/Chris Brown	DirectoryServices	160	Monitor All AD Changes to Users and Groups		contoso.com\ Admin	Success
08/26/2020 08:50:48 PM	User unlocked	Paul Bryan	Alert	5012	contoso.com\Domain Users/Users/SLC/ReDirection-USB/Paul Bryan	DirectoryServices	160	Monitor All AD Changes to Users and Groups	GC3321HQ	contoso.com\ Admin	Success

Figure 6

Logs considered:

```
event_description Aug 26 20:57:49 NTPLDTLR48 Aug 14 09:03:36 prd-slc-var00 Aug 14 09:03:36 PRD-SLC-VAR00 CEF:0|Varonis Inc.|DatAdvantage|7.5.21|5012|User unlock
ed|5|rt=Aug 14 2020 09:03:31 cat=Alert cs2=Monitor All AD Changes to Users and Groups cs2Label=RuleName cn1=160 cn1Label=RuleID end=Aug 14
2020 09:03:14 duser=primeis.com\Josh Eades Admin dhost=DirectoryServices filePath=primeis.com/Domain Users/Users/SLC/ReDirection-USB/Jodie Pi
dgeon fname=Jodie Pidgeon act=User unlocked dvchost=UTLTJENEWHQ outcome=Success msg= cs3= cs3Label=AttachmentName cs4= cs4Label=Cli
entAccessType deviceCustomDate1= fileType= cs1= cs1Label=MailRecipient suser= cs5= cs5Label=MailboxAccessType cnt= cs6= cs6Label=ChangedPe
rmissions oldFilePermission= filePermission= dpriv= start=
```

Figure 7

- **Varonis - File permissions activities** – This report outlines a detailed overview of events related to file system events, such as, file set permissions, file modify, file create, etc. This will include event datetime, action taken, file permission change, file/server domain, etc.

LogTime	Action	Affected object	Changed permissions	Event Category	Event ID	Event Threshold	File Path	File permissions	File Server/Domain	Message	Old File permissions	Rule ID	Rule Name
08/26/2020 08:50:48 PM	File permissions added	CAB_AL_AZ_AR_CT_C.xlsx	Full Control	Alert	6001		D:\userdrv\Pau\Desktop\CAB_AL_AZ_AR_CT_C.xlsx	Full Control	GCH3365Q	Full Control permissions for This object only (not inherited) was added to user CONTOSO\PauM on D:\userdrv\Pau\Desktop\CAB_AL_AZ_AR_CT_C.xlsx	None	138	Permissions granted directly to user in windows file system
08/26/2020 08:50:48 PM	File permissions added	DTP-Relocation.pdf	Full Control	Alert	6001	100	D:\dept\Production\IDTP-Relocation.pdf	Full Control	GCH3368Q	Full Control permissions for This object only (inherited) was added to group CONTOSO\Production on D:\dept\Production\IDTP-Relocation.pdf	None	164	File Permissions

Figure 8

Logs considered:

```
event_description Aug 26 20:57:49 NTPLDTLR48 Aug 14 09:14:13 prd-slc-var00 Aug 14 09:14:13 PRD-SLC-VAR00 CEF:0|Varonis Inc.|DatAdvantage|7.5.21|6001|File perm
issions added|6|rt=Aug 14 2020 09:14:09 cat=Alert cs2=File Permissions cs2Label=RuleName cn1=164 cn1Label=RuleID end=Aug 14 2020 09:13:15 duser
=primeis.com\Steven Ogella dhost=UTFS100HQ filePath=D:\depts\Producer Services\Labor Law Posters\Florida County - Pinellas.pdf fname=Florid
a County - Pinellas.pdf act=File permissions added dvchost=UTXENAPP22HQ outcome=Success msg=Full Control permissions for This object only (inhe
rited) was added to group PRIMEIS\Producer Services on D:\depts\Producer Services\Labor Law Posters\Florida County - Pinellas.pdf cs3= cs3Label
=AttachmentName cs4= cs4Label=ClientAccessType deviceCustomDate1= fileType= cs1= cs1Label=MailRecipient suser= cs5= cs5Label=MailboxAcces
sType cnt=100 cs6= Full Control cs6Label=ChangedPermissions oldFilePermission= None filePermission= Full Control dpriv=PRIMEIS\Producer Services s
tart=Aug 14 2020 09:10:19
```

Figure 9

- **Varonis - Exchange mailbox and folder activities** – This report will outline the detailed summary of events related to exchange server activities, such as, change folder permissions, create message, message received, etc. This will include event datetime, action taken, affected object name, rule name, etc.

LogTime	Action	Affected object	Event Category	Event ID	File Path	File Server/Domain	File Type	Mailbox access type	Message
08/26/2020 08:50:48 PM	Mailbox permission removed	prod@contoso.com	Alert	3075	Mailbox Store\prod@contoso.com	ExchOnline	Other	Non Owner	Administrative Deny 'FullAccess, MailboxFlag' permission(s) with an inheritance type of All was removed from account NAMPODGC12\AmyL for mailbox Mailbox Store\prod@contoso.com
08/26/2020 08:50:48 PM	Mailbox permission added	prod@contoso.com	Alert	3074	Mailbox Store\prod@contoso.com	ExchOnline	Other	Non Owner	Administrative 'FullAccess, MailboxFlag' permission(s) with an inheritance type of All was added to account NAMPODGC12\AmyL for mailbox Mailbox Store\prod@contoso.com
08/26/2020 08:50:48 PM	Exchange folder opened	Mailbox Store\Brenden@contoso.com\Inbox	Alert	2049		ExchOnline		Non Owner	

Figure 10

Logs considered:

```
event_description      Aug 26 20:57:49 NTPDLTBLR48 Aug 14 10:57:39 prd-slc-var00 Aug 14 10:57:39 PRD-SLC-VAR00 CEF:0[Varonis Inc.]DatAdvantage[7.5.21][3074]Mailbox per
mission added[3]rt=Aug 14 2020 10:57:37 cat=Alert cs2=Activity performed by Admin user from a non-corporate IP address cs2Label=RuleName cn1=1
57 cn1Label=RuleID end=Aug 14 2020 10:56:01 duser=ExchOnline\\Dale Lowder dhost=ExchOnline filePath=Mailbox Store\\rjl@primeis.com fname=rjl
@primeis.com act=Mailbox permission added dvchost= outcome=Success msg=Administrative 'FullAccess, MailboxFlag' permission(s) with an inheritan
ce type of All was added to account NAMPR16A002\\dalel54225146083668 for mailbox Mailbox Store\\rjl@primeis.com cs3= cs3Label=AttachmentNa
me cs4= cs4Label=ClientAccessType deviceCustomDate1= fileType=Other cs1= cs1Label=MailRecipient suser= cs5=Non Owner cs5Label=MailboxAcce
ssType cnt= cs6= cs6Label=ChangedPermissions oldFilePermission= filePermission= dpriv=NAMPR16A002\\dalel54225146083668 start=
```

Figure 11

4.4 Dashboards

- Varonis - Top actions performed

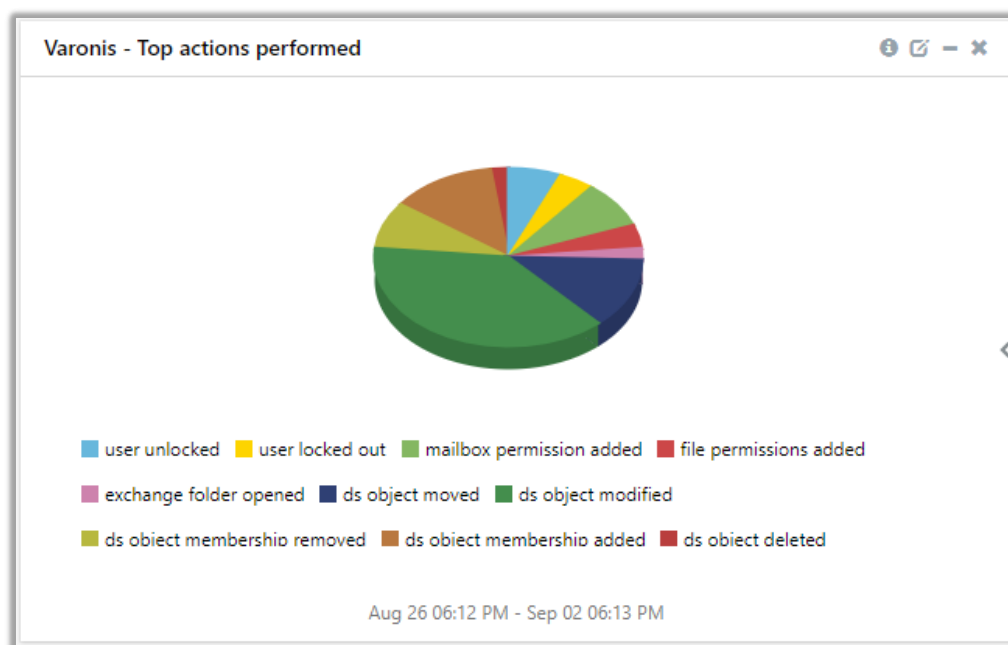


Figure 12

- Varonis - Top alerted rules

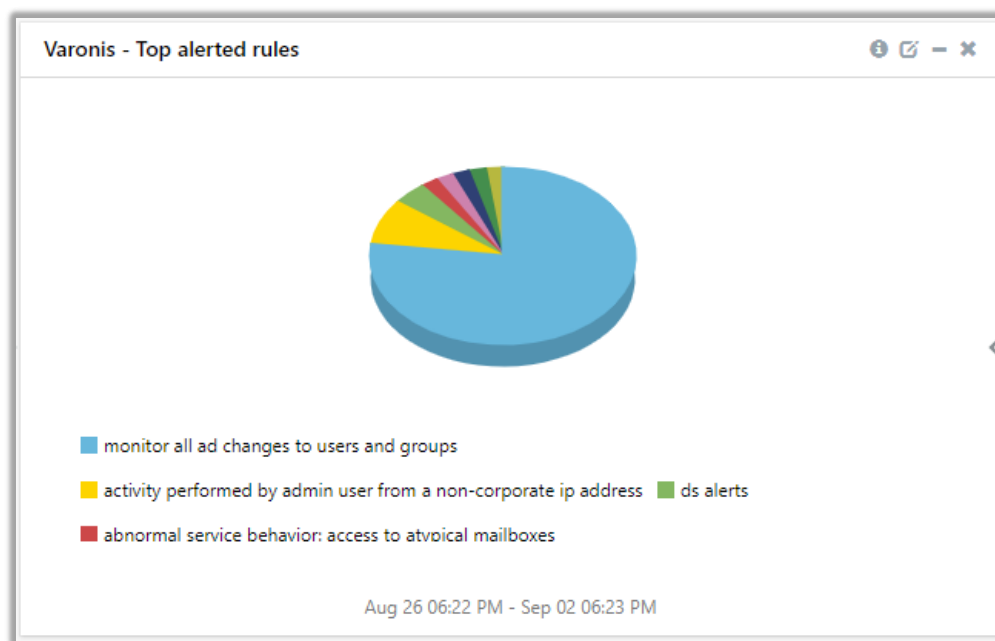


Figure 13

- Varonis - Top alerted users

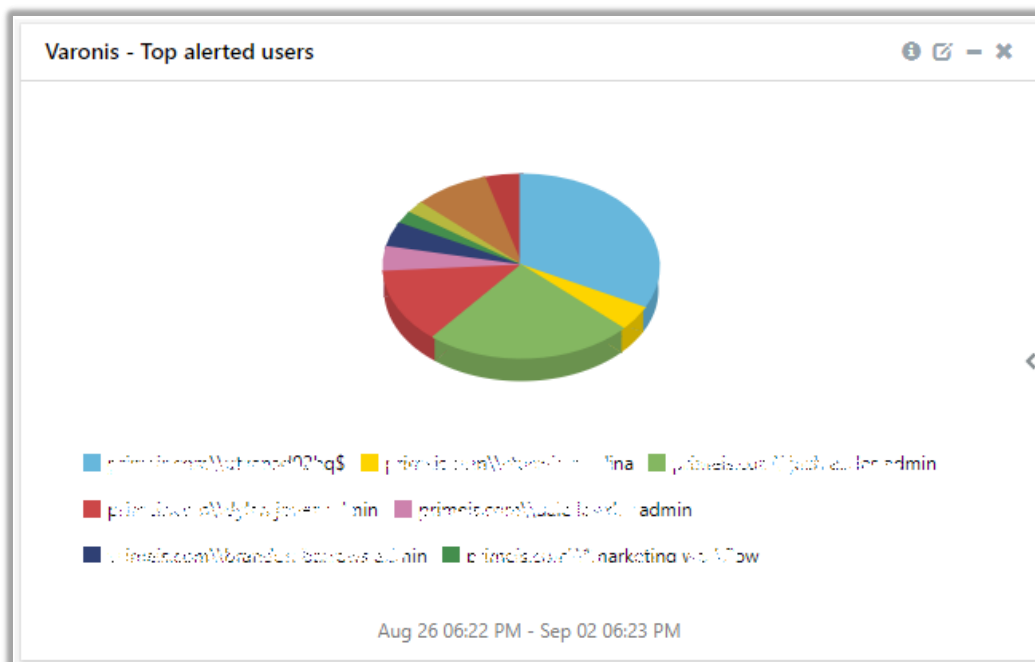


Figure 14

- **Varonis - Top alerted resources**

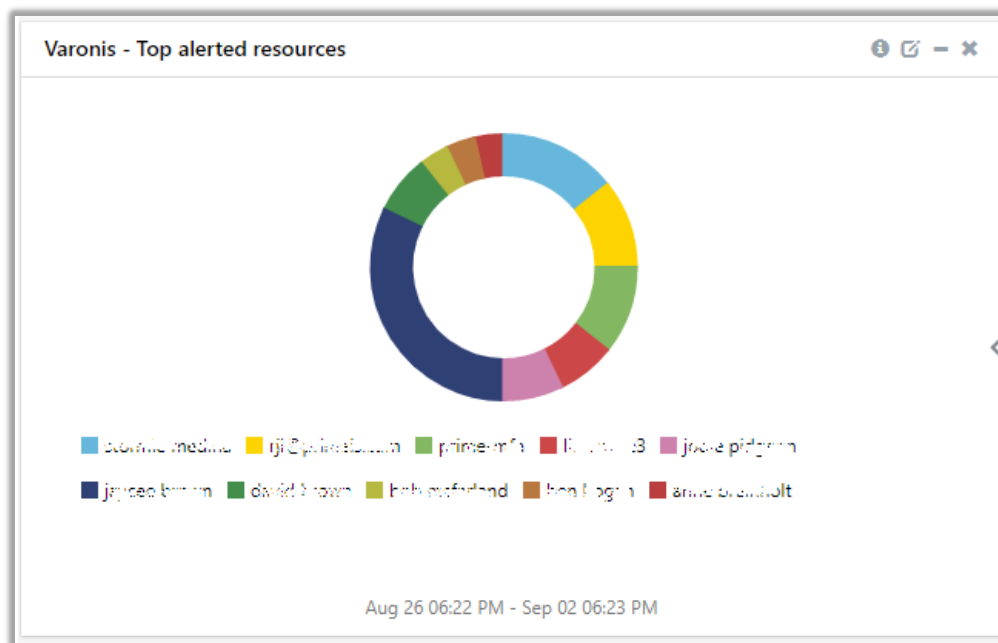


Figure 15

- **Varonis - Event Categories**

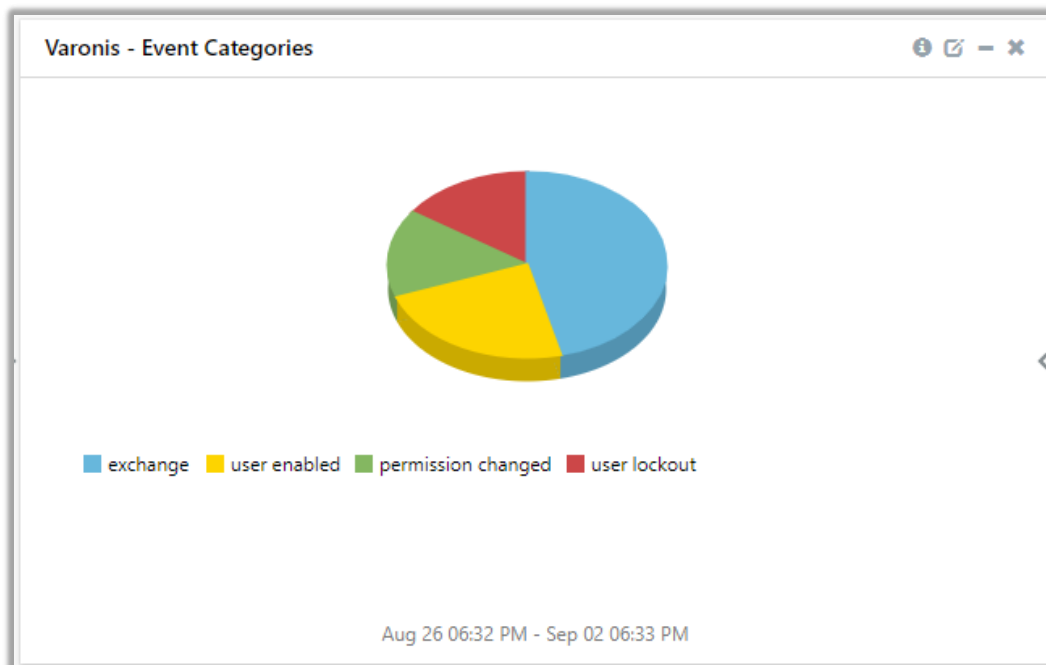


Figure 16

5. Importing knowledge pack into EventTracker

Getting Knowledge Packs

To get the knowledge packs, locate the knowledge pack folder. Follow the below steps.

1. Press “**Windows** + R”.
 2. Now, type “**%et_install_path%\Knowledge Packs**” and press “**Enter**”.
- (**Note** – If, not able to locate the file path as mentioned above, please contact [EventTracker support](#) to get the assistance).

NOTE: Import knowledge pack items in the following sequence:

- Categories
 - Alerts
 - Token Template
 - Flex Reports
 - Knowledge Objects
 - Dashboards
1. Launch the **EventTracker Control Panel**.
 2. Double click **Export-Import Utility**.

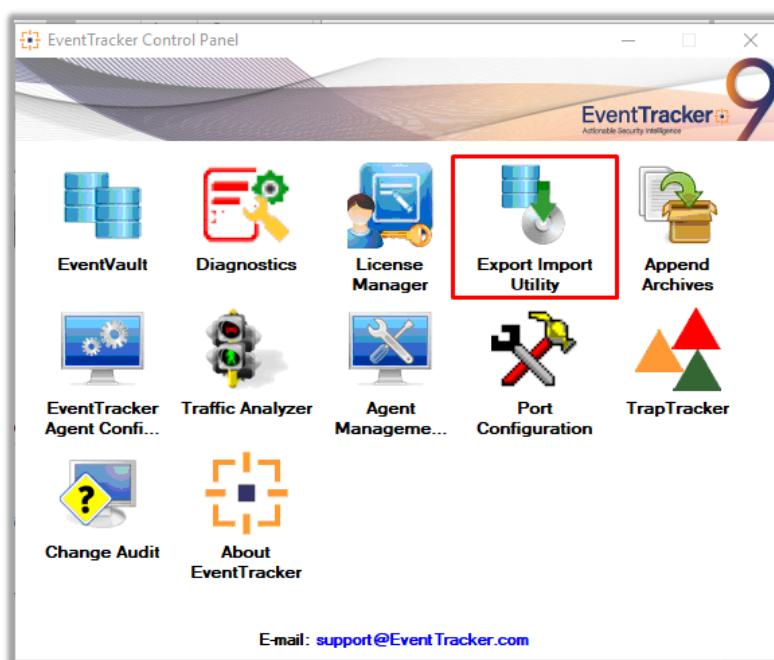


Figure 17

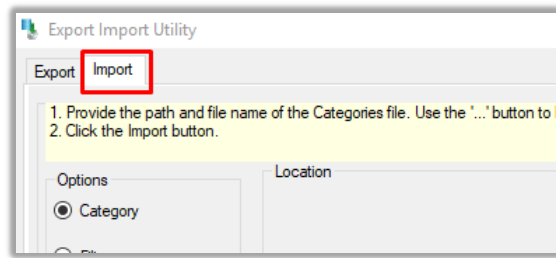


Figure 18

3. Click the **Import** tab.

5.1 Saved searches

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 extension “.iscat”, e.g. “**Categories_Varonis.iscat**” and then click on the “**Import**” button.

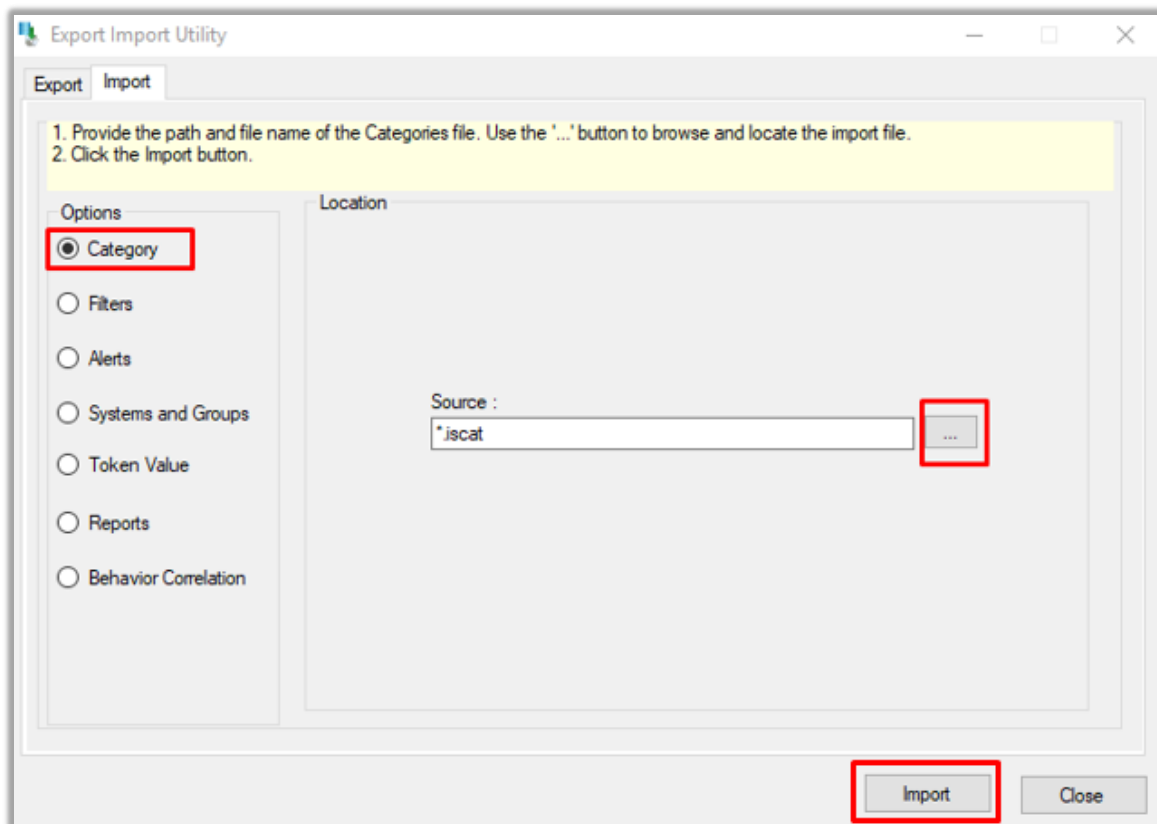


Figure 19

EventTracker displays a success message:

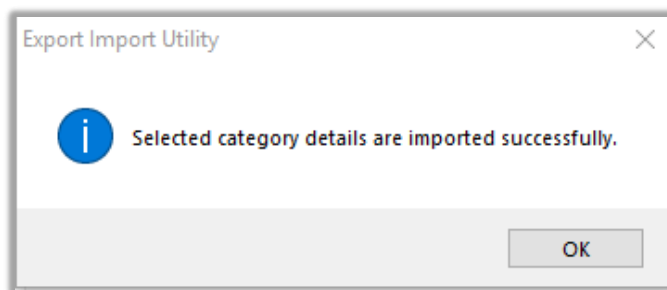



Figure 20

5.2 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 extension “.isalt”, e.g. “**Alerts_Varonis.isalt**” and then click on the “**Import**” button:

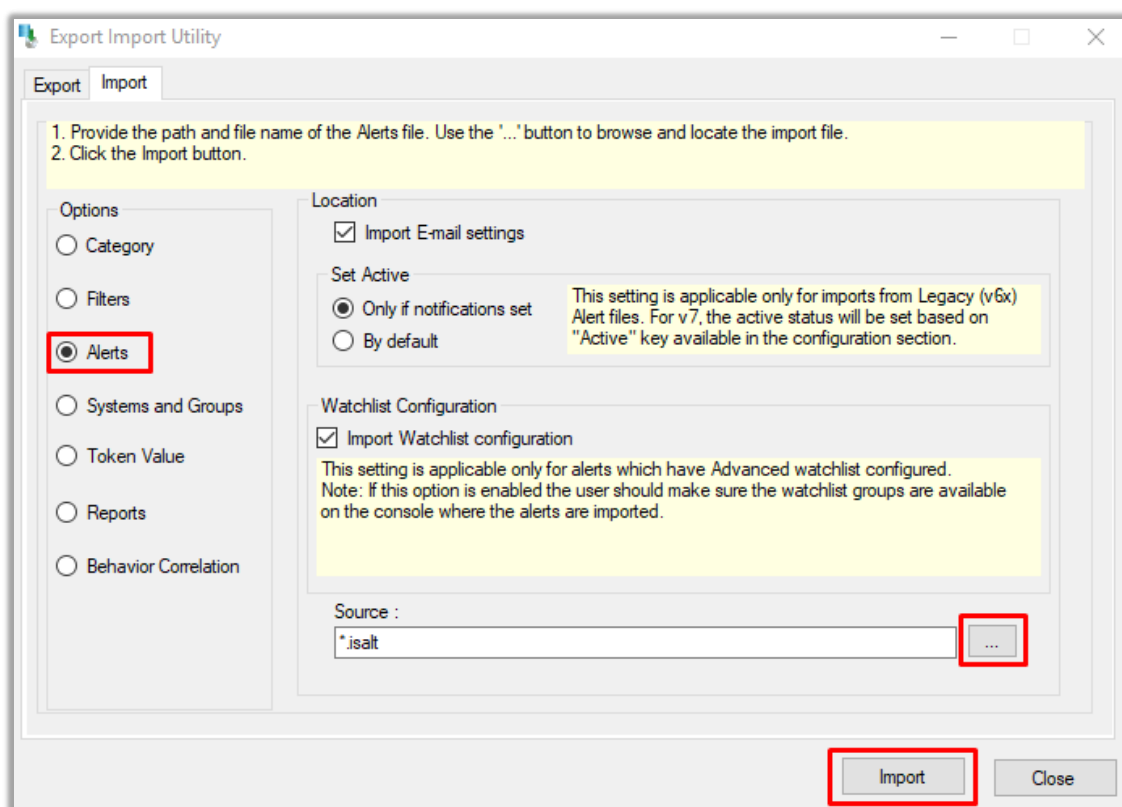


Figure 21

EventTracker displays a success message:

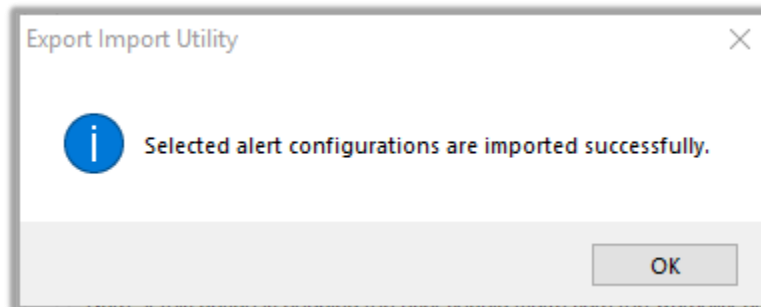


Figure 22

5.3 Token template

For importing “**Token Template**”, please navigate to **EventTracker manager** web interface.

1. Click **Parsing Rules** under the **Admin** option in the EventTracker manager web interface.

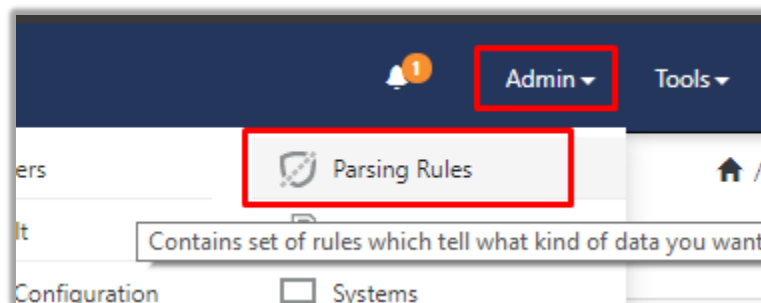


Figure 23

2. Next, click the “**Template**” tab and then click the “**Import Configuration**” button.

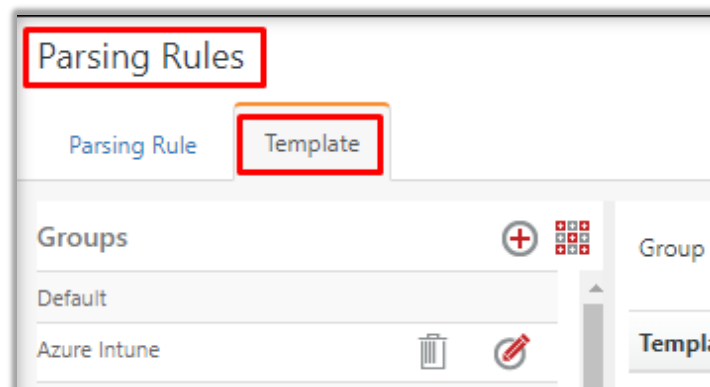


Figure 24

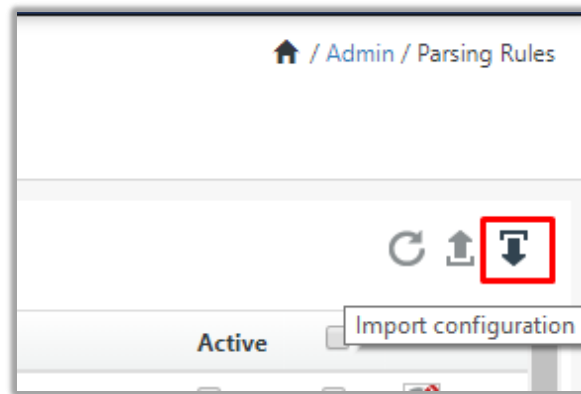


Figure 25

- Now, click **"Browse"** button and navigate to the knowledge packs folder (type **"%et_install_path%\Knowledge Packs"** in navigation bar) where **".ettd"**, e.g. **"Templates_Varonis.ettd"** file is located. Wait for few seconds, as templates will be loaded. Once you see the templates, click desired templates and click **"Import"** button:

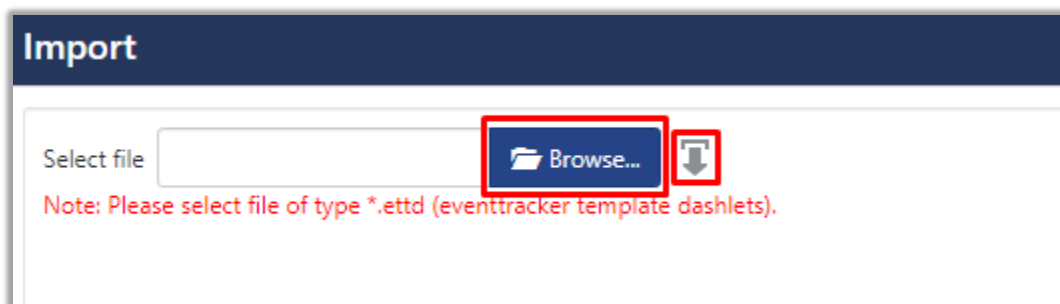


Figure 26

5.4 Flex reports

- In EventTracker control panel, select **"Export/ Import utility"** and select the **"Import tab"**. Then, click **Reports** option, and choose **"New (*.etcrx)"**:

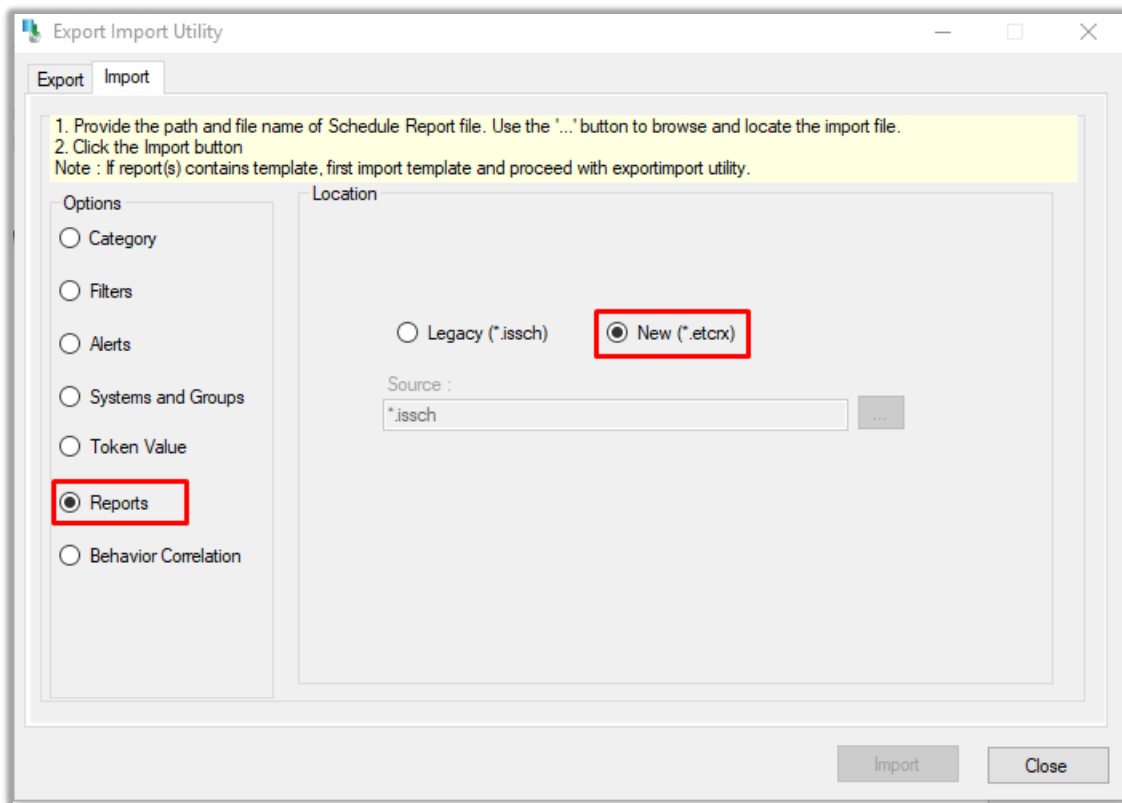


Figure 27

2. Once you have selected “**New (*.etcrx)**”, a new pop-up window will appear. Click “**Select File**” button and navigate to knowledge pack folder and select file with extension “**.etcrx**”, e.g. “**Reports_Varonis.etcrx**”.

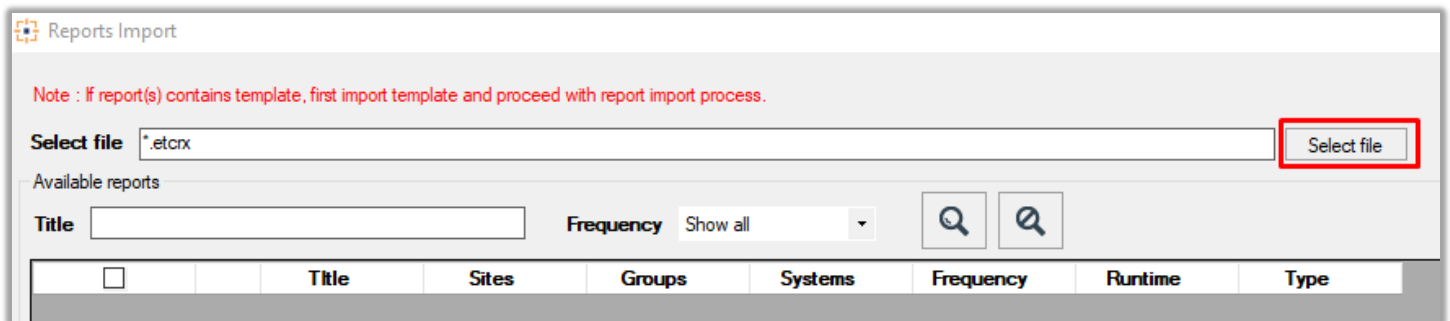



Figure 28

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

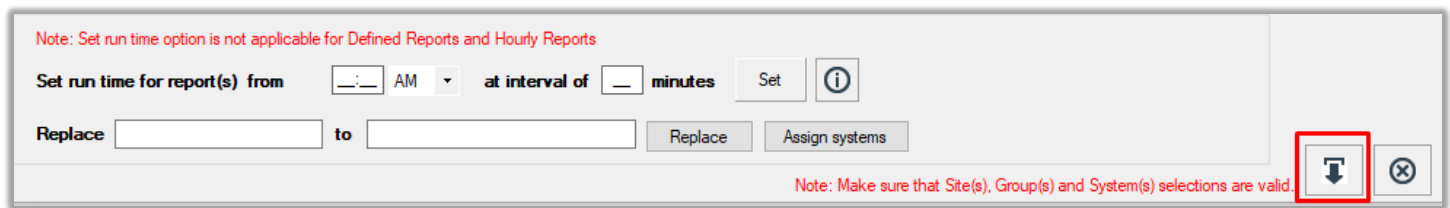


Figure 29

EventTracker displays a success message:

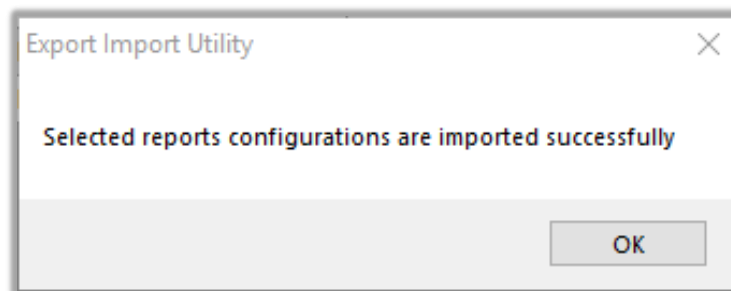


Figure 30

5.5 Knowledge objects

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

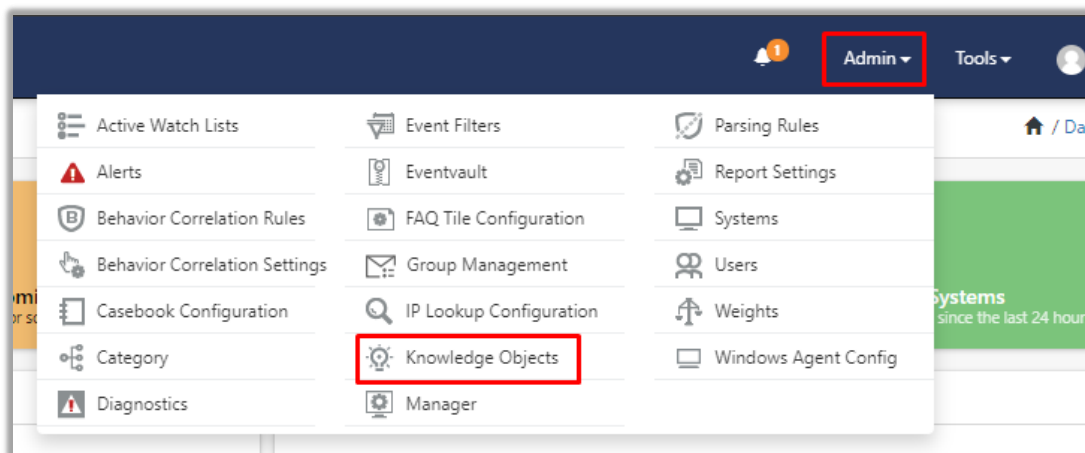


Figure 31

2. Next, click the **"import object"** icon.

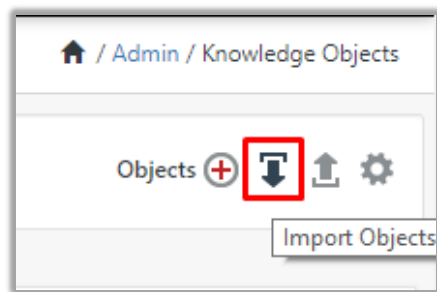


Figure 32

3. A pop-up box will appear, click "**Browse**" in that and navigate to knowledge packs folder (type "`%et_install_path%\Knowledge Packs`" in navigation bar) with the extension **".etko"**, e.g. **"KO_Varonis.etko"** and then click **"Upload"** button.

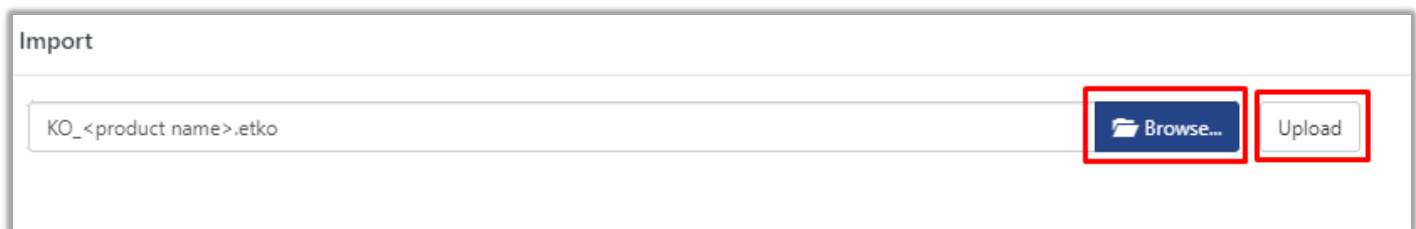


Figure 33

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



Figure 34

5.6 Dashboards

1. Login to **EventTracker manager web interface**.
2. Navigate to **Dashboard → My Dashboard**.
3. In "My Dashboard", Click **Import Button**.

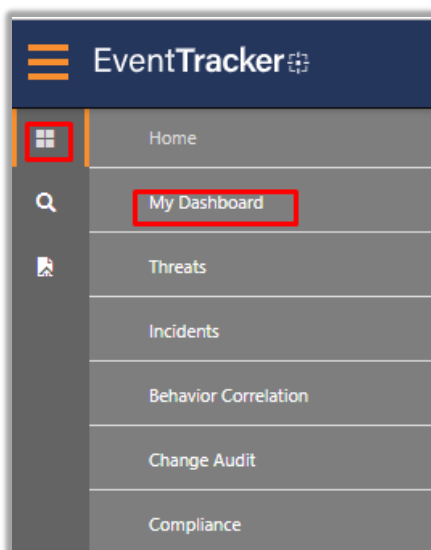


Figure 35

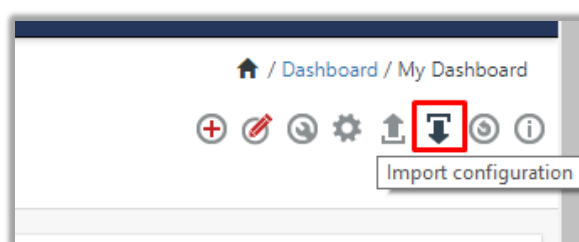


Figure 36

4. Select the **browse** button and navigate to knowledge pack folder (type “%et_install_path%\Knowledge Packs” in navigation bar) where “.etwd”, e.g. “Dashboards_ Varonis.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.

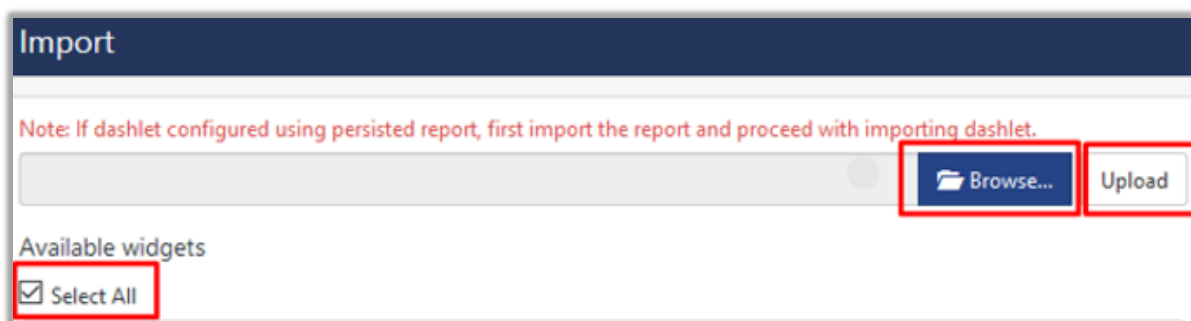


Figure 37



Figure 38

6. Verifying knowledge pack in EventTracker

6.1 Saved searches

1. Login to **EventTracker manager web interface**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand “**Varonis**” group folder to view the imported categories.

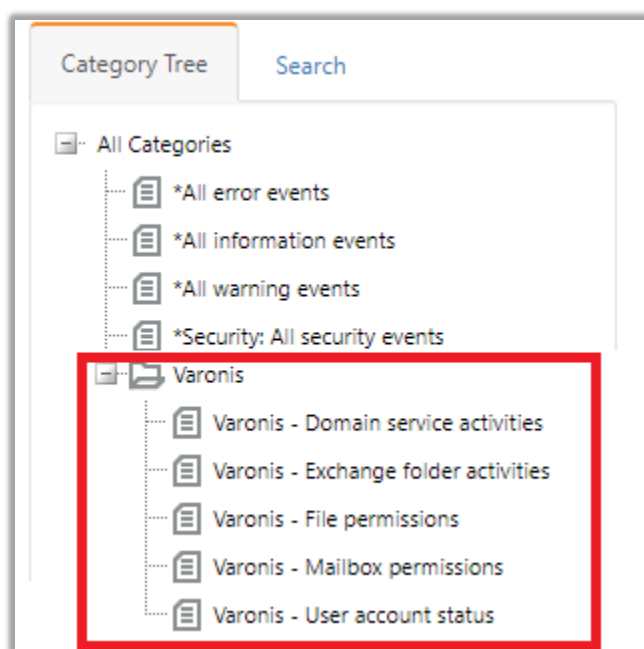


Figure 39

6.2 Alerts

1. In the **EventTracker manager** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In search box enter “<search criteria> e.g. “**Varonis**” and then click on the **Search** button.

EventTracker displays an alert related to “Varonis”.

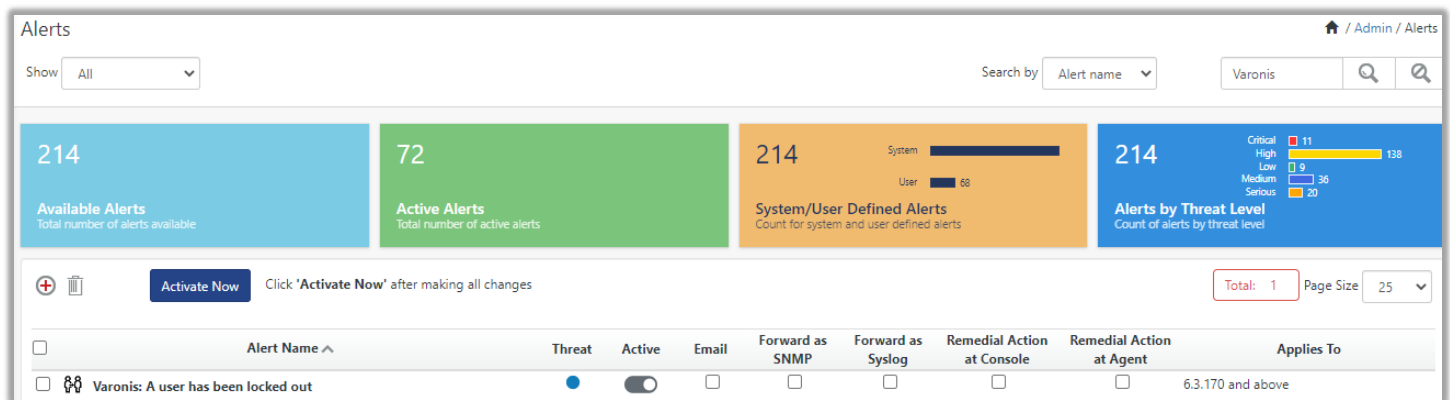


Figure 40

6.3 Token template

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Parsing Rules**.
2. In the **Template** tab, click on the “<product name/ report group name>” e.g. “**Varonis**” group folder to view the imported templates.

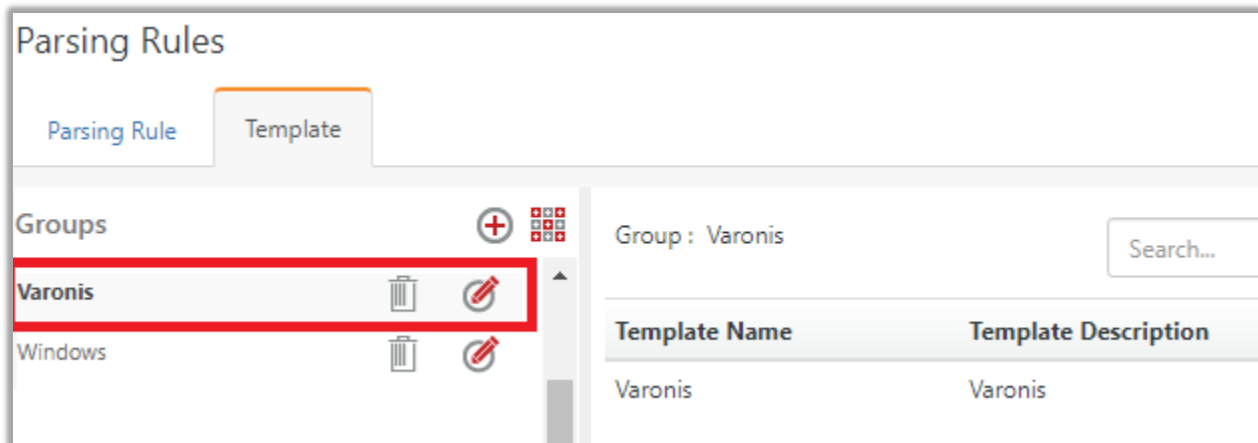


Figure 41

6.4 Flex reports

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

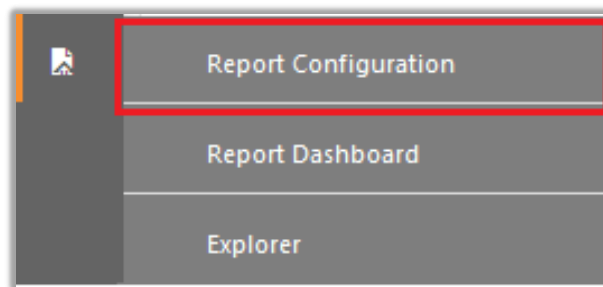


Figure 42

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

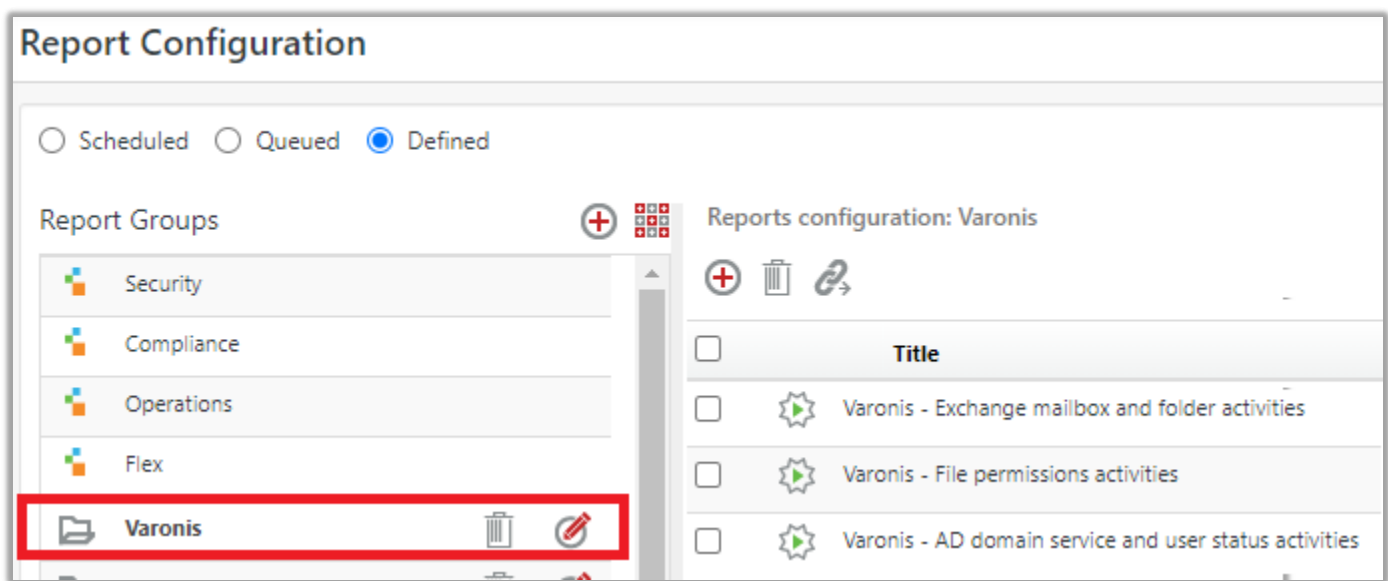


Figure 43

6.5 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 “**Varonis**” group folder to view the imported Knowledge objects.

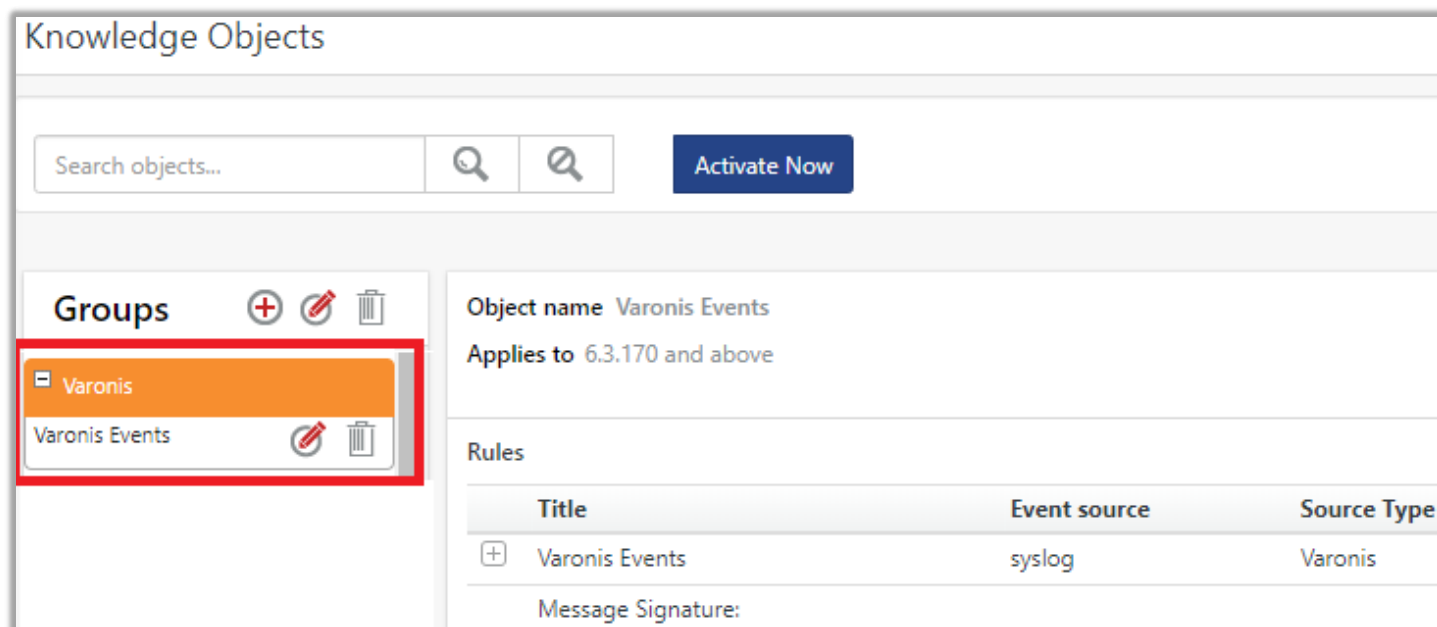


Figure 44

6.6 Dashboards

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

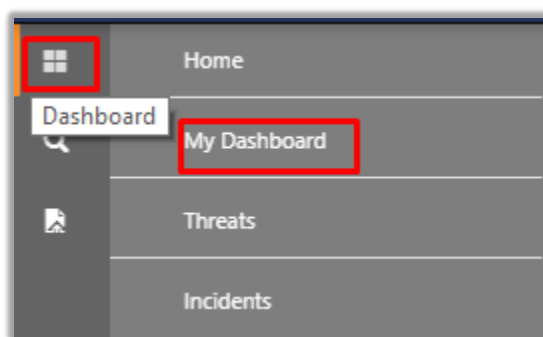


Figure 45

2. Select **"Customize daslets"**  button and type **"Varonis"** in the search bar.

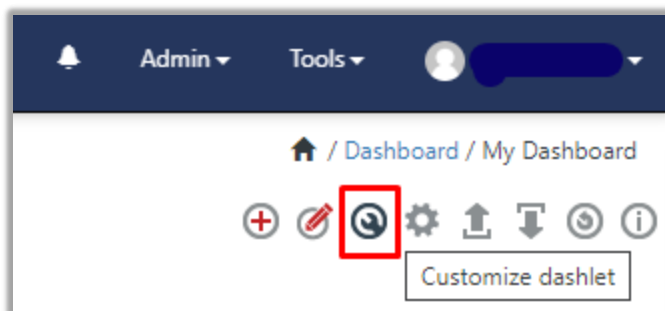


Figure 46

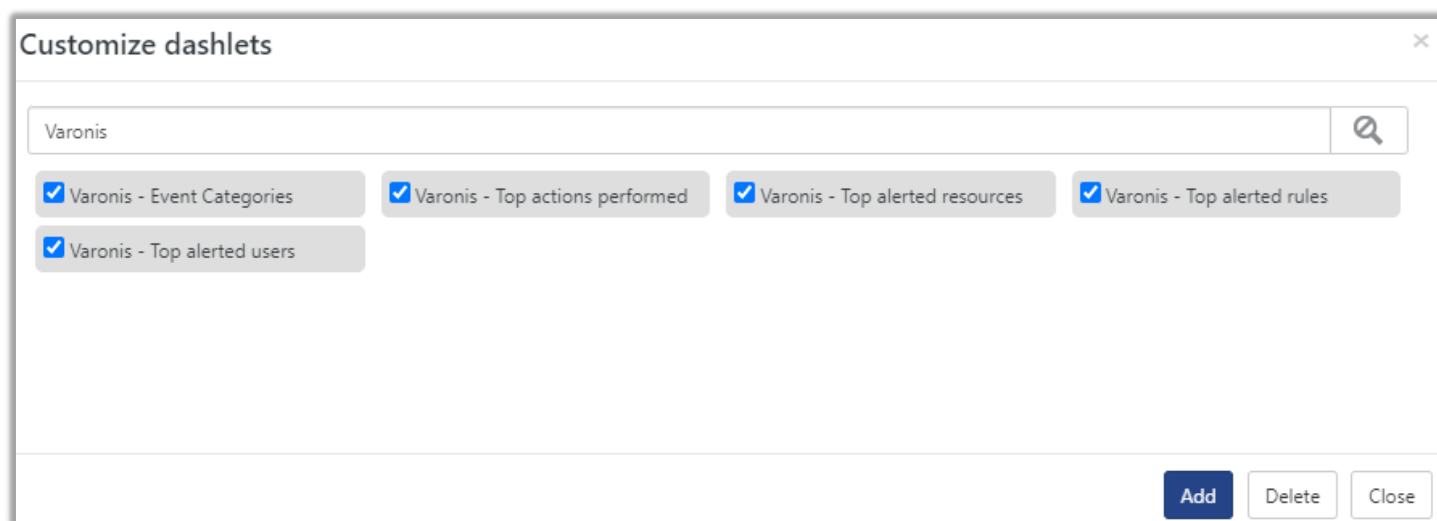


Figure 47