EventTracker

Actionable Security Intelligence

Integrate Trend Micro Vulnerability Protection

EventTracker v8.x and above

Publication Date: January 8, 2018

Abstract

This guide provides instructions to configure **Trend Micro Vulnerability Protection** to send crucial events to EventTracker Enterprise by means of syslog.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise version 8.x and later**, and **Trend Micro Vulnerability Protection version up to 2.x.**

Audience

Trend Micro Vulnerability Protection users, who wish to forward its events to EventTracker Manager and monitor them using EventTracker Enterprise.

Table of Contents

Overview

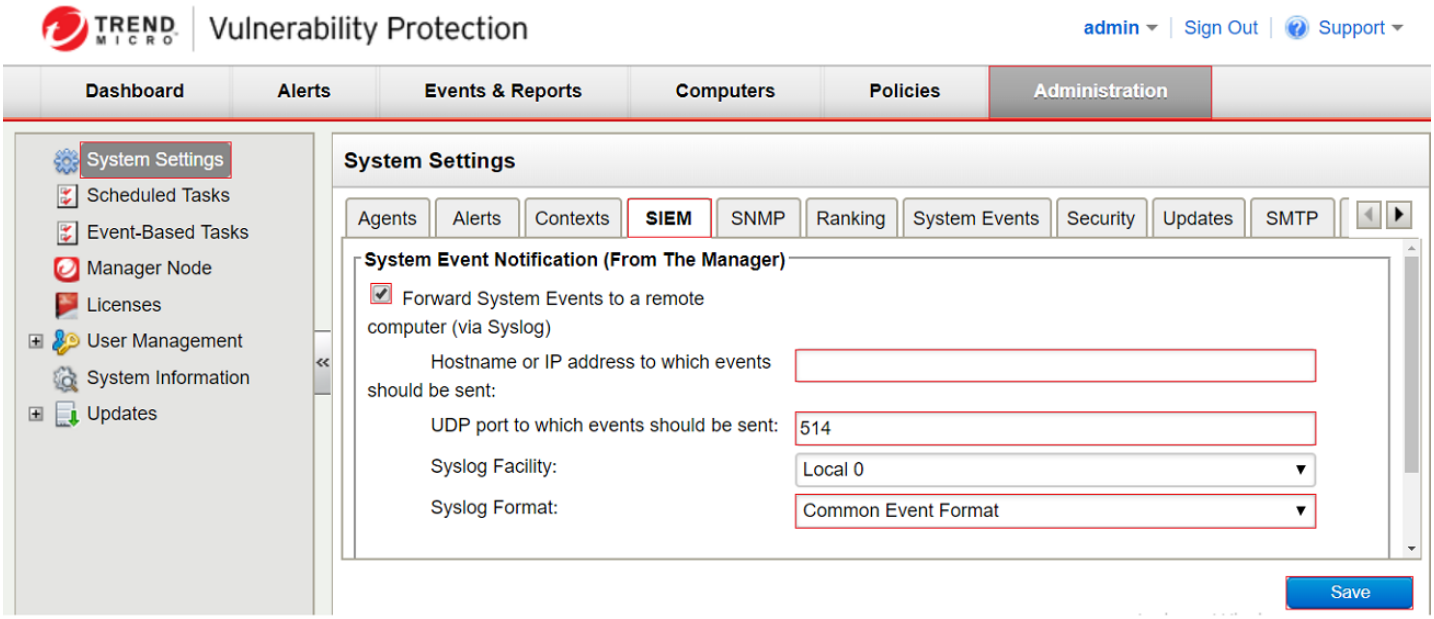
Trend Micro Vulnerability Protection provides earlier, stronger endpoint protection by supplementing desktop anti-malware and threat security with proactive virtual patching. A high-performance engine monitors traffic for new specific vulnerabilities using host based intrusion prevention system (IPS) filters as well as zero-day attack monitoring. So, you can detect network protocol deviations, or suspicious content that signals an attack, or security policy violations.

Prerequisites

- **EventTracker** should be installed.
- **Trend Micro Vulnerability Protection** version **upto 2.x** should be installed.

Enable Syslog Forwarding in Trend Micro Vulnerability Protection

1. Go to the **Administration** > **System Settings** > **SIEM** tab.
2. In the **System Event Notification** (from the **Manager**) area, set the **Forward System Events to a remote computer** (via Syslog) option.
3. In the **hostname** or the **IP address** field, type in the **EventTracker Manager IP Address**.



4. Enter which **UDP port** to use (**514**).

5. Select which **Syslog Facility** to use (Local 0)
6. Select which **Syslog Format** to use. (**Common Event Format**)

EventTracker Knowledge Pack

Once logs are received into EventTracker, Categories and reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Windows.

Categories

- **Trend Micro VP- User activities-** This category based report provides information related to all user activities.
- **Trend Micro VP- User login and logout-** This category based report provides information related to all the user login and logout activity.
- **Trend Micro VP- User login failures-** This category based report provides information related to all the user login failures that is done.
- **Trend Micro VP- Computer activities-** This category based report provides information related to all the different Trend Micro agent activities that is added in the Trend Micro manager.
- **Trend Micro VP- System events-** This category based report provides information related to all the system activities that is done.
- **Trend Micro VP- Rules and policy changes-** This category based report provides information related to all the firewall/IPS rules and policy changes that are done.
- **Trend Micro VP- Firewall allowed traffic-** This category based report provides information related to all the traffic that are allowed by the Trend Micro Vulnerability Protection.
- **Trend Micro VP- Firewall denied traffic-** This category based report provides information related to all the traffic that are denied by the Trend Micro Vulnerability Protection.
- **Trend Micro VP- IPS activities-** This category based report provides information related to all the IPS attack that is detected by the Trend Micro Vulnerability Protection.

Alerts

- **Trend Micro VP: User activities:** This alert is generated when a critical user activity is detected by Trend Micro Vulnerability Protection.
- **Trend Micro VP: User login failures:** This alert is generated when any user login failure is attempted.
- **Trend Micro VP: System events:** This alert is generated when any critical system event is triggered by Trend Micro Vulnerability Protection.
- **Trend Micro VP: IPS activities:** This alert is generated when any IPS attack is detected by the Trend Micro Vulnerability Protection.

Flex Reports

- **Trend Micro VP- User activities-** This report provides information related to all user activities that is done.

LogTime	Manager Machine Name	Source User Name	Target Entity	Action
12/29/2017 01:25:40 PM	Contoso-TMV	admin	Jiren	User Viewed Firewall Event
12/29/2017 01:25:40 PM	Contoso-TMV	admin	Jiren	User Viewed Intrusion Prevention Event
12/29/2017 01:25:40 PM	Contoso-TMV	Jeremy	stacy	User Viewed admin Event
12/29/2017 01:25:40 PM	Contoso-TMV	admin	alberto	User Created
12/29/2017 01:25:40 PM	Contoso-TMV	stacy	greg	User Deleted
12/29/2017 01:25:40 PM	Contoso-TMV	admin	gilbert	User Updated
12/29/2017 01:25:40 PM	Contoso-TMV	admin	Jiren	User Password Set

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
1/3/2018 4:27:41 PM	3333	NTPLDTBLR38 / ntpldt...	N/A	N/A	Syslog

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Dec 29 11:57:32 Contoso-TMV Dec 29 11:57:31 Contoso-TMV CEF:0|Trend Micro|Vulnerability Protection Manager|2.0.8367|651|User Deleted|3|suser= stacy target=greg msg=Description Omitted

- **Trend Micro VP- User login and logout-** This report provides information related to all the user login and logout activity.

LogTime	Manager Device Name	Source IP Address	Source User Name	Target Entity	Action	Message
12/29/2017 01:25:40 PM	Contoso-TMV	172.16.54.97	admin	admin	User Signed In	User signed in from 172.16.54.97
12/29/2017 01:25:40 PM	Contoso-TMV		System	admin	User Signed Out	Description Omitted

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
1/3/2018 4:27:42 PM	3333	NTPLDTBLR38 / ntpldt...	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Description: Dec 29 11:58:27 Contoso-TMV Dec 29 11:58:27 Contoso-TMV CEF:0|Trend Micro|Vulnerability Protection Manager|2.0.8367|601|User Signed Out|3|suser=System target=edward msg=Description Omitted				
1/3/2018 4:27:42 PM	3333	NTPLDTBLR38 / ntpldt...	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Description: Dec 29 11:58:27 Contoso-TMV Dec 29 11:58:27 Contoso-TMV CEF:0|Trend Micro|Vulnerability Protection Manager|2.0.8367|601|User Signed In|3|suser=System target=katy msg=Description Omitted				

- **Trend Micro VP- User login failures-** This provides information related to all the user logon failures that is attempted.

LogTime	Manager Machine Name	Source IP Address	Source User Name	Target Entity	Action	Message
12/29/2017 01:25:40 PM	Contoso-TMV		admin	Katie	User Locked Out	Description Omitted
12/29/2017 01:25:40 PM	Contoso-TMV		victor	Katie	User Timed Out	Description Omitted
12/29/2017 01:25:40 PM	Contoso-TMV		victor	Katie	User Unlocked	Description Omitted
12/29/2017 01:25:40 PM	Contoso-TMV	172.16.54.97	victor	admin	Authentication Failed	User password incorrect for username admin on an attempt to sign in from 172.16.54.97

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
1/3/2018 4:27:42 PM	3333	NTPLDTBLR38 / ntpldt...	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Description: Dec 29 11:58:22 Contoso-TMV Dec 29 11:58:19 Contoso-TMV CEF:0|Trend Micro|Vulnerability Protection Manager|2.0.8367|603|User Locked Out|3|suser=admin target=Katie msg=Description Omitted				
1/3/2018 4:27:42 PM	3333	NTPLDTBLR38 / ntpldt...	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Description: Dec 29 12:44:38 Contoso-TMV Dec 29 12:44:34 Contoso-TMV CEF:0|Trend Micro|Vulnerability Protection Manager|2.0.8367|160|Authentication Failed|3|suser=victor target=admin msg=User password incorrect for username admin on an attempt to sign in from 172.16.54.97				

- **Trend Micro VP- Computer activities-** This report provides information related to all the different Trend Micro agent activities that is added in the Trend Micro manager.

LogTime	Manager Machine Name	Source User Name	Target Entity	Action
12/29/2017 03:09:24 PM	Contoso-T11	admin	192.163.11.47	Scan for Open Ports
12/29/2017 03:09:24 PM	Contoso-T11	victor	172.154.16.49	Computer Deleted
12/29/2017 03:09:24 PM	Contoso-T11	pedro	174.25.18.93	Scan for Open Ports Failed
12/29/2017 03:09:24 PM	Contoso-T11	christian	192.168.12.147	Deactivation Requested
12/29/2017 03:09:24 PM	Contoso-T11	john	203.154.28.79	Unlocked
12/29/2017 03:09:24 PM	Contoso-T11	admin	192.163.11.47	Computer Created
12/29/2017 03:09:24 PM	Contoso-T11	katie	192.160.14.22	Activation Requested
12/29/2017 03:09:24 PM	Contoso-T11	admin	192.163.11.47	Computer Moved

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
1/3/2018 6:00:17 PM	3333	NTPLDTBLR38 / ntpldt...	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Description: Dec 29 11:35:56 Contoso-T11 Dec 29 11:35:54 Contoso-T11 CEF:0|Trend Micro|Vulnerability Protection Manager|2.0.8367|251|Computer Deleted|3|suser=victor target=192.163.11.47 msg=Description Omitted				
1/3/2018 6:00:17 PM	3333	NTPLDTBLR38 / ntpldt...	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Description: Dec 29 11:55:55 Contoso-T11 Dec 29 11:55:53 Contoso-T11 CEF:0|Trend Micro|Vulnerability Protection Manager|2.0.8367|250|Computer Created|3|suser=admin target=174.25.18.93 msg=Description Omitted				

- **Trend Micro VP- System events-** This report provides information related to all the system activities that is done.

LogTime	Manager Machine Name	Source User Name	Target Entity	Action
01/02/2018 12:38:39 PM	Contoso-T17	admin	172.154.12.160	Script Executed
01/02/2018 12:38:39 PM	Contoso-T17	jeremy	110.25.96.41	Script Execution Failed
01/02/2018 12:38:39 PM	Contoso-T17	tony	154.92.44.112	Software Deleted
01/02/2018 12:38:39 PM	Contoso-T17	admin	172.154.12.160	Firewall Events Exported
01/02/2018 12:38:39 PM	Contoso-T17	admin	113.15.34.210	Manager Available Disk Space Too Low
01/02/2018 12:38:39 PM	Contoso-T17	admin	172.154.12.160	Vulnerability Protection Manager Shutdown
01/02/2018 12:38:39 PM	Contoso-T17	kim	110.25.96.41	Heartbeat Server Failed
01/02/2018 12:38:39 PM	Contoso-T17	admin	172.154.12.160	Credential Generation

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
1/3/2018 4:27:41 PM	3333	NTPLDTBLR38 / ntpldt...	N/A	N/A	Syslog

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Dec 29 11:35:56 Contoso-T17 Dec 29 11:35:54 Contoso-T17 CEF:0|Trend Micro|Vulnerability Protection Manager|2.0.8367|120|Heartbeat Server Failed|3|suser=kim target=110.25.96.41 msg=Description Omitted

- **Trend Micro VP- Rules and policy changes-** This report provides information related to all the firewall/IPS rules and policy changes that are done.

LogTime	Manager Machine Name	Source User Name	Target Entity	Action
01/02/2018 11:16:00 AM	Contoso-T11	katie	172.168.45.12	Send Policy Failed
01/02/2018 11:16:00 AM	Contoso-T11	admin	192.161.15.131	Policy Sent
01/02/2018 11:15:59 AM	Contoso-T11	admin	192.161.15.131	Policy Deleted
01/02/2018 11:16:00 AM	Contoso-T11	admin	192.161.15.131	Intrusion Prevention Rules Require Configuration
01/02/2018 11:16:00 AM	Contoso-T11	fisher	145.92.15.47	Scheduled Rule Update Downloaded and Applied
01/02/2018 11:16:00 AM	Contoso-T11	Nell	174.15.94.65	Firewall Rule Deleted
01/02/2018 11:16:00 AM	Contoso-T11	admin	192.161.15.131	Intrusion Prevention Rule Exported
01/02/2018 11:16:00 AM	Contoso-T11	admin	172.54.88.147	Intrusion Prevention Rule Updated
01/02/2018 11:16:00 AM	Contoso-T11	vincent	54.168.10.132	Intrusion Prevention Rule Deleted

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
1/3/2018 4:27:41 PM	3333	NTPLDTBLR38 / ntpldt...	N/A	N/A	Syslog

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Dec 29 11:55:55 Contoso-T11 Dec 29 11:55:53 Contoso-T11 CEF:0|Trend Micro|Vulnerability Protection Manager|2.0.8367|106|Scheduled Rule Update Downloaded and Applied|3|suser=fisher target=145.92.15.47 msg=Description Omitted

- **Trend Micro VP- Firewall allowed and denied traffic-** This report provides information related to all the traffic that are allowed and denied by the Trend Micro Vulnerability Protection.

LogTime	Manager Machine Name	Source IP Address	Source Port	Destination IP Address	Destination Port	Device Host Name	Source Mac Address	Destination Mac Address	Frame Type	Event Name	Action	Protocol	Bytes In	Bytes Out	Count
01/02/2018 03:50:02 PM	Contoso-11	192.168.126.10	49617	72.14.204.147	80	127.10.25.194	00:0C:29:EB:35:DE	00:50:56:F5:7F:47	IP	Log for TCP Port 80	Log	TCP	1589	1019	1
01/02/2018 03:50:02 PM	Contoso-11	fe80:0:0:0:8810:33cc:ba4c:665	55899	ff02:0:0:0:0:0:1:3	5355	192.154.21.52	D4:3D:7E:12:5E:92	33:33:00:01:00:03	IPv6	Out Of Allowed Policy	Deny	UDP	91	256	6

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
1/3/2018 5:24:58 PM	3333	NTPLDTBLR38 / ntpldt...	N/A	N/A	Syslog

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Dec 28 15:43:20 Contoso-11 Dec 28 15:08:58 Contoso-11 CEF:0|Trend Micro|Vulnerability Protection Agent|2.0.8367|123|Out Of Allowed Policy|5|cn1=3 cn1Label=Host ID dvc=192.154.21.52 act=Deny dmac=33:33:00:01:00:03 smac=D4:3D:7E:12:5E:92 TrendMicroDsFrameType=IPv6 src=fe80:0:0:0:8810:33cc:ba4c:665 dst=ff02:0:0:0:0:0:1:3 in=91 out=256 cs3= cs3Label=Fragmentation Bits proto=UDP spt=55899 dpt=5355 cnt=1

- **Trend Micro VP- IPS activities-** This report provides information related to all the IPS attack that is detected by the Trend Micro Vulnerability Protection.

LogTime	Manager Machine Name	Source IP Address	Source Port	Destination IP Address	Destination Port	Device Host Name	Source Mac Address	Destination Mac Address	Event Name	Action	Bytes In	Bytes Out	Count
01/02/2018 04:29:06 PM	Contoso-13	172.15.164.15	1548	72.14.204.105	45	Contoso-11	00:0C:29:EB:35:DE	00:50:56:F5:7F:47	Region Too Big	Reset	96321	1093	2
01/02/2018 04:29:06 PM	Contoso-13	154.23.59.19	49786	110.45.93.101	152	54.80.48.73	b2:11:4c:ee:f5:c7	a6:11:4c:ee:f5:c3	Insufficient Memory	IDS:Block	1252	256	3
01/02/2018 04:29:06 PM	Contoso-13	172.15.164.15	189	72.14.204.105	96	Contoso-13	c4:be:45:e1:f5:d8	a6:19:3c:aa:f5:c3	Runtime Error	Reset		4953	1
01/02/2018 04:29:06 PM	Contoso-13	78.42.154.22	7845	19.56.19.78	46	172.203.15.49	a6:11:4c:ee:f5:c3	d8:f5:e1:44:eb:4c	Error Generating Master Key(s)	Block	4561	9524	1

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
1/3/2018 4:27:40 PM	3333	NTPLDTBLR38 / ntpldt...	N/A	N/A	Syslog

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Dec 28 15:43:20 Contoso-13 Dec 28 15:08:57 Contoso-13 CEF:0|Trend Micro|Vulnerability Protection Agent|2.0|500|URI Path Depth Exceeded|3|cn1=1 cn1Label=Host ID dvchost=Contoso-19 dmac=12:7d:4f:ae:b4:69 smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP src=45.12.96.78 dst=103.25.78.46 out=1123 cs3=DF MF cs3Label=Fragmentation Bits proto=TCP spt=6521 dpt=213 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=61 act=IDS:Reset cn3=10 cn3Label=Intrusion Prevention Packet Position cs5=10 cs5Label=Intrusion Prevention Stream Position cs6=8 cs6Label=Intrusion Prevention Flags TrendMicroDsPacketData=R0VUlC9zP3

Import Trend Micro Vulnerability Protection Knowledge Pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Knowledge Objects
- Alerts
- Token Templates
- Flex Reports

NOTE: Export knowledge pack items in the following sequence:

- Categories
- Knowledge Objects
- Alerts
- Token Templates
- Flex Reports

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

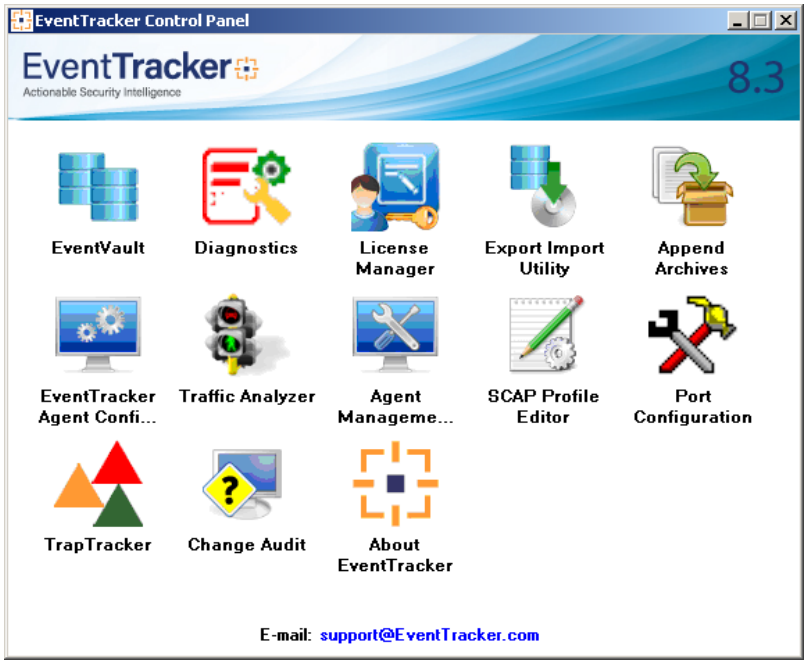


Figure 1

Import Category

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

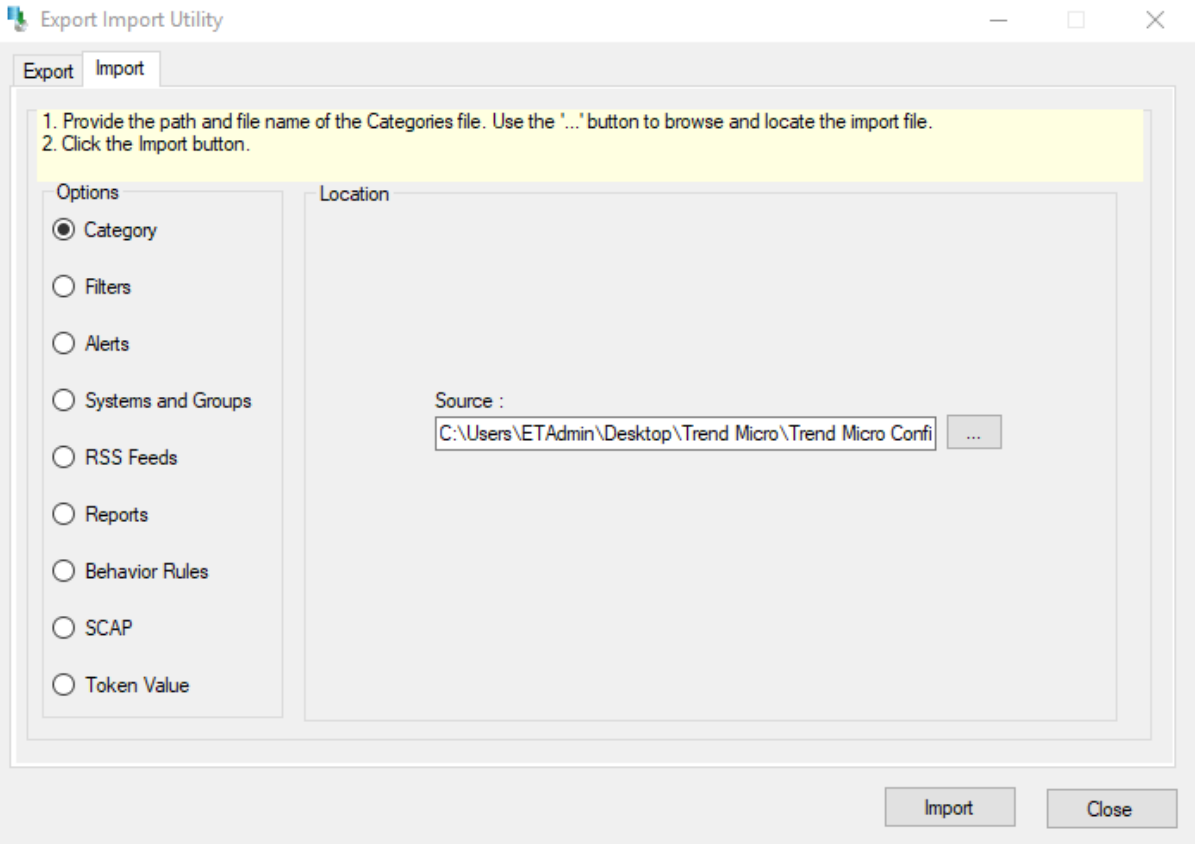


Figure 2

2. Locate **Trend Micro VP categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.
   EventTracker displays success message.

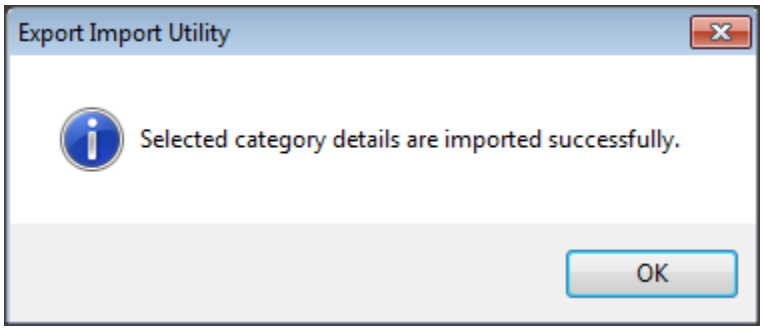


Figure 3

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

Import Alerts

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

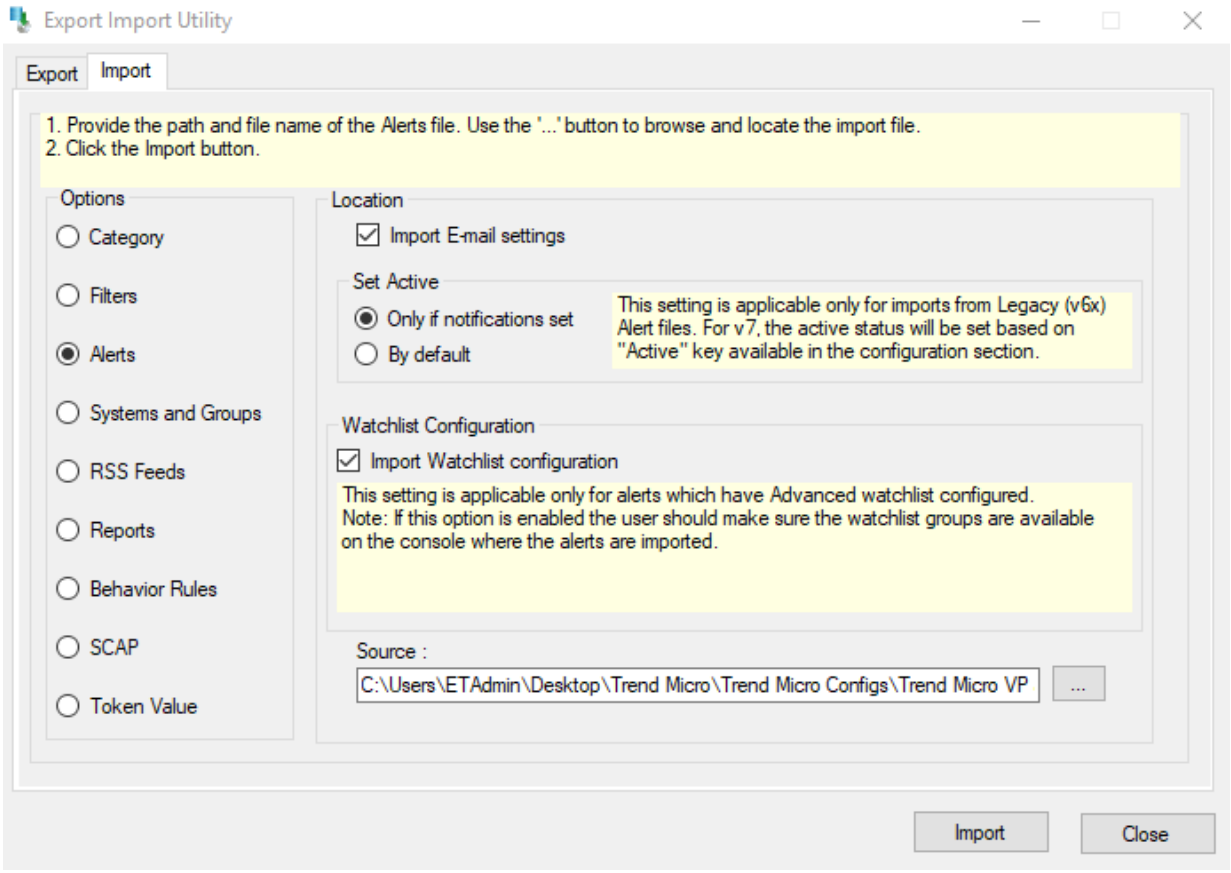


Figure 4

2. Locate **Trend Micro VP alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
   EventTracker displays success message.

Figure 5

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

Import Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on ‘**Import**’ option.

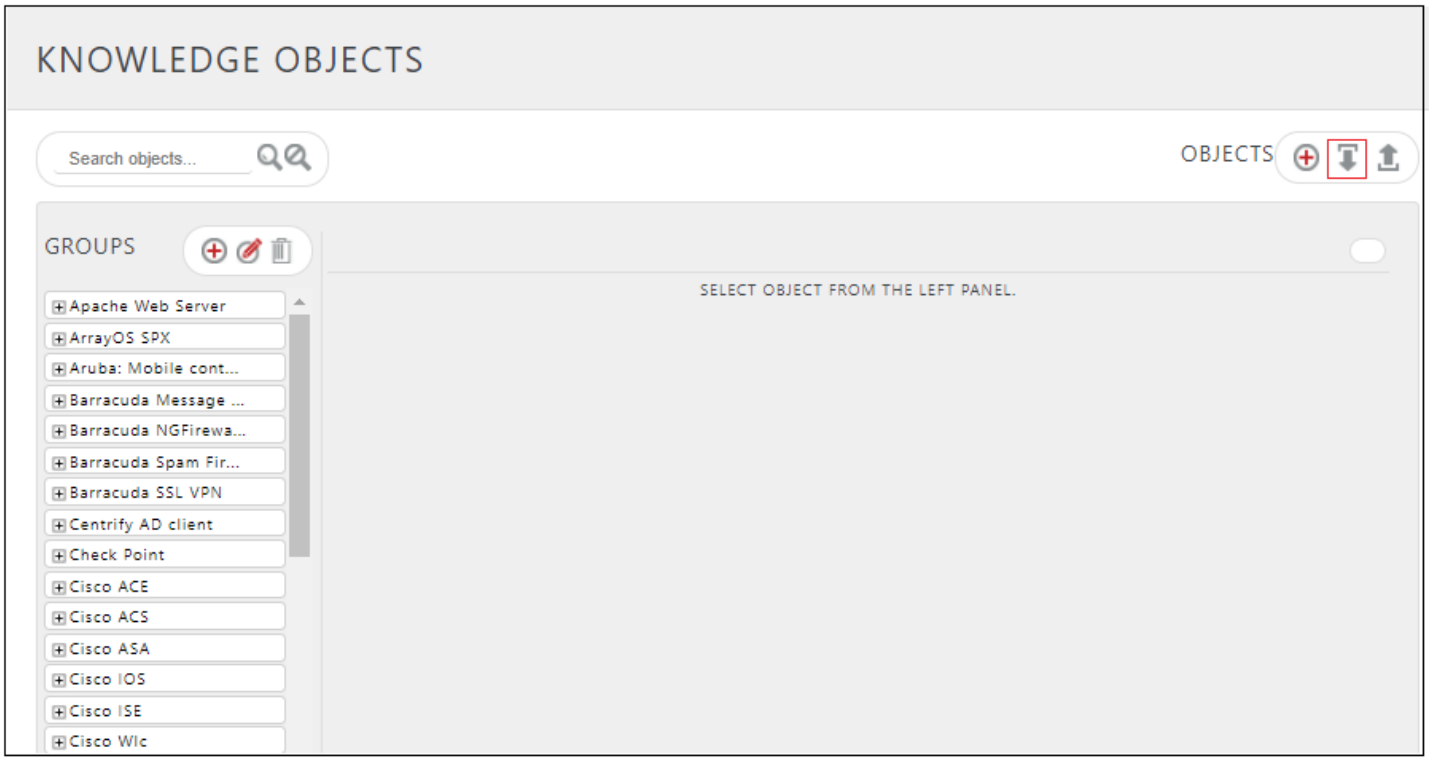


Figure 6

3. In **IMPORT** pane click on **Browse** button.

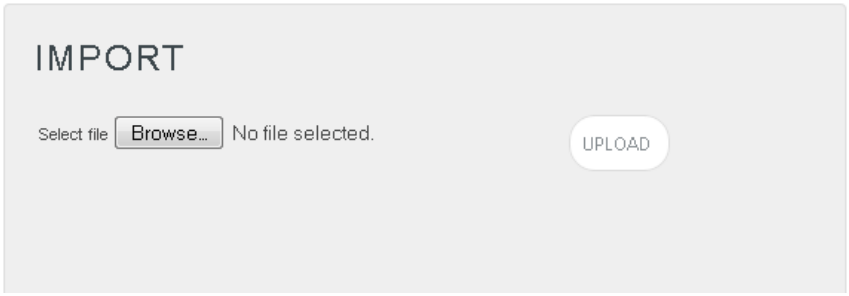


Figure 7

4. Locate **KO_Trend Micro VP.etko** file, and then click the **UPLOAD** button.

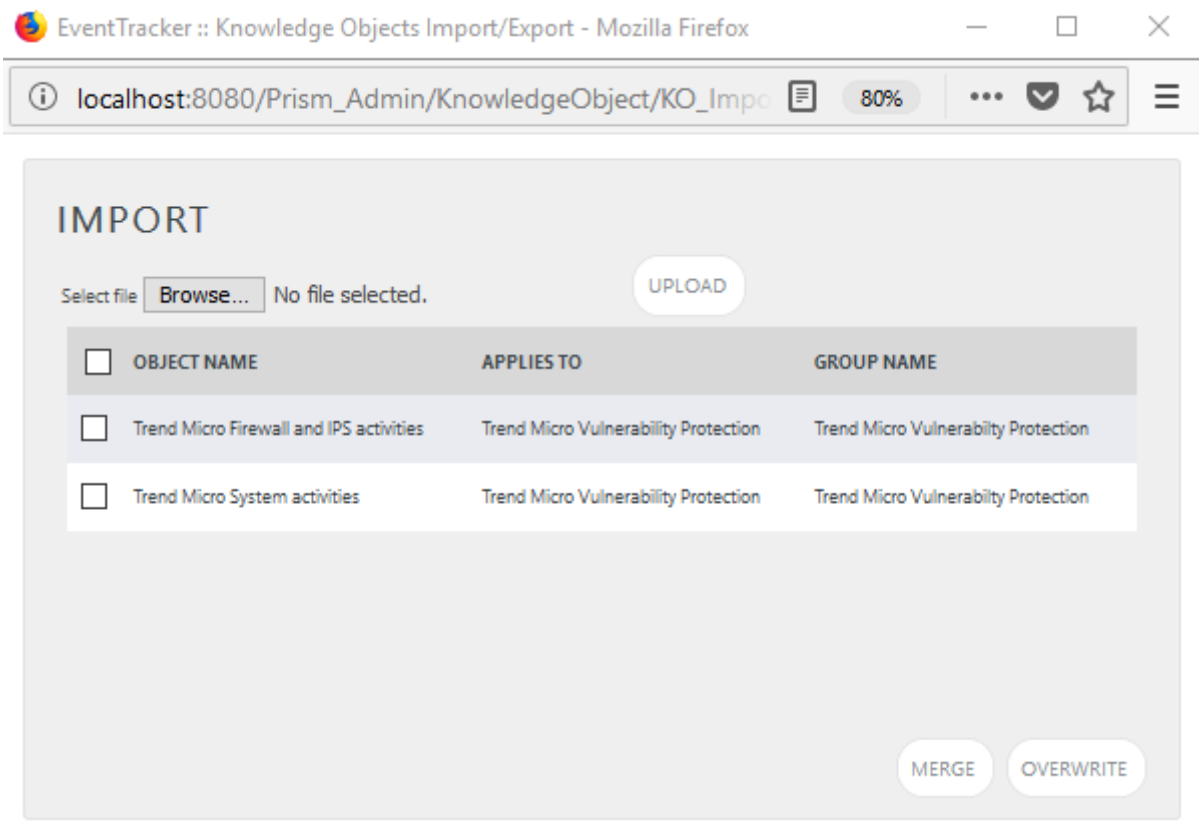


Figure 8

5. Now select the check box and then click on '**OVERWRITE**' option. EventTracker displays success message.

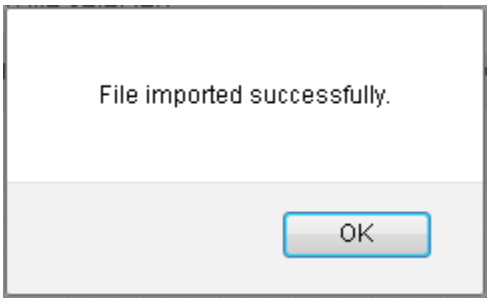


Figure 9

6. Click on **OK** button.

Token Template

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on '**Import**' option.
3. Click on **Browse** button.

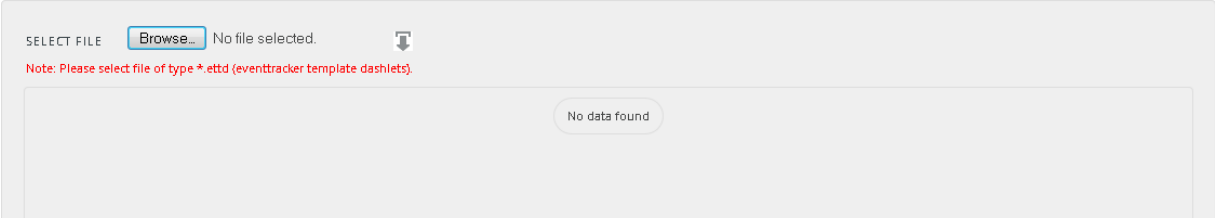


Figure 10

4. Locate **Trend Micro VP templates.ettd** file, and then click the **Open** button.

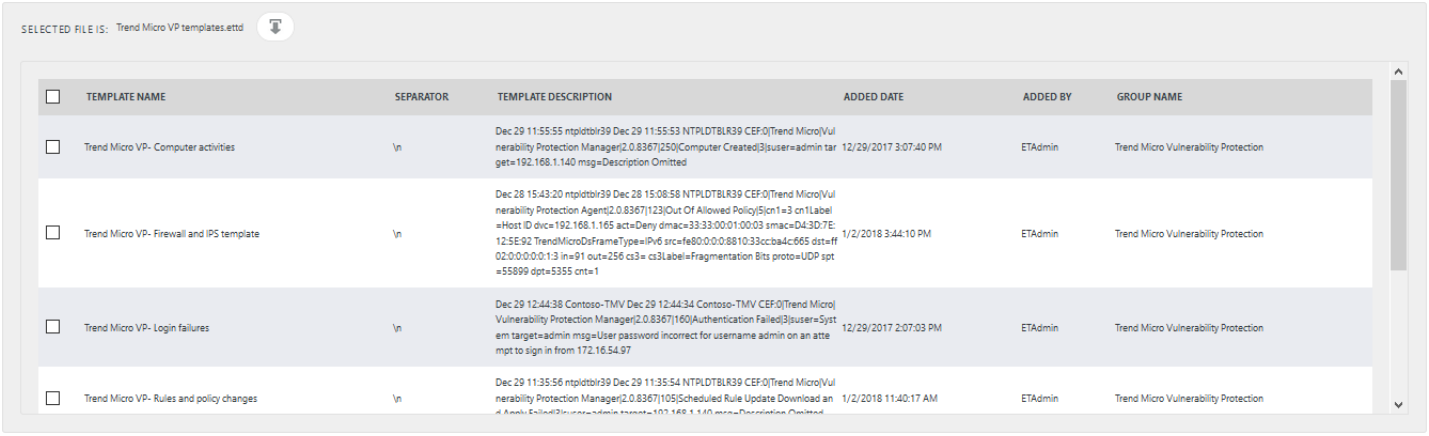


Figure 11

5. Now select the check box and then click on '**Import**' option.
   EventTracker displays success message.

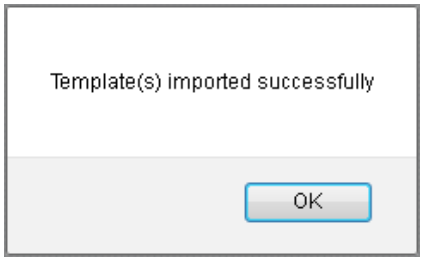


Figure 12

6. Click on **OK** button.

Import Flex Reports

1. Click **Reports** option, and then click the '**browse**' button.
2. Locate applicable **Trend Micro VP Reports.etcrx** file, and then click the **Open** button.

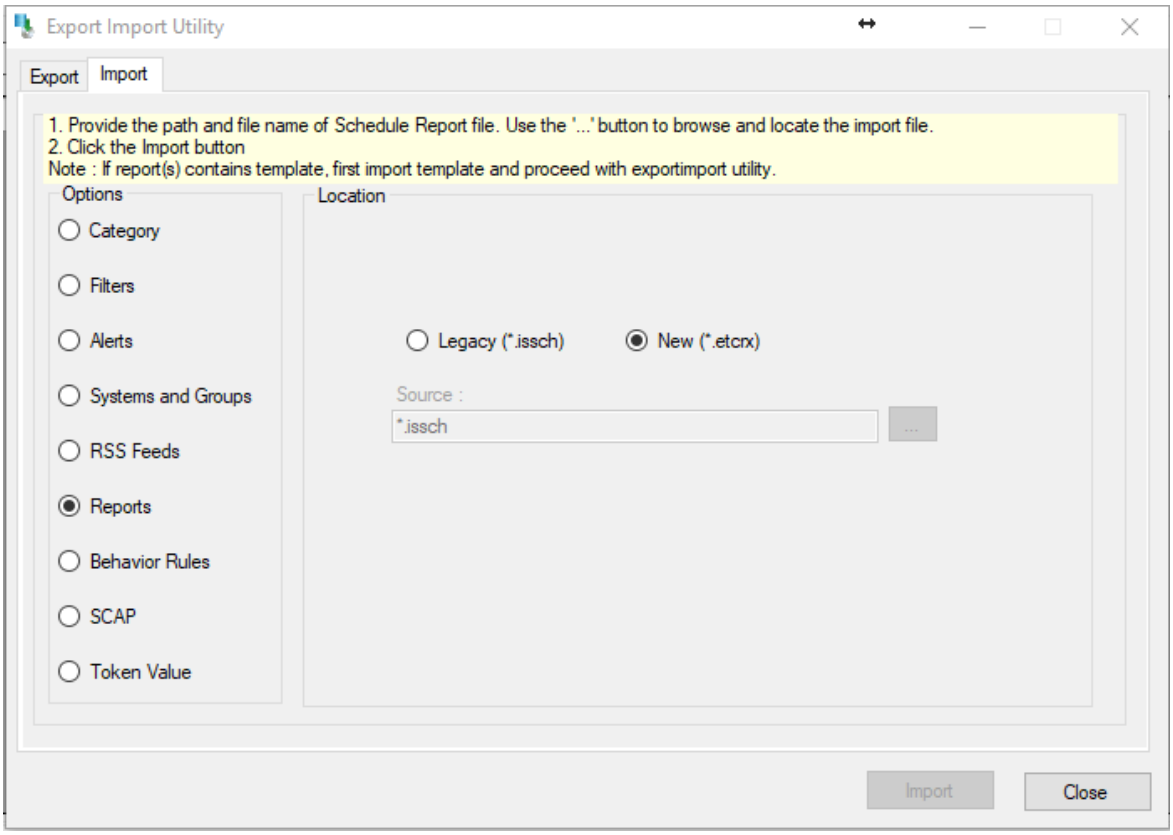


Figure 13

3. To import scheduled reports, click the **Import** button.

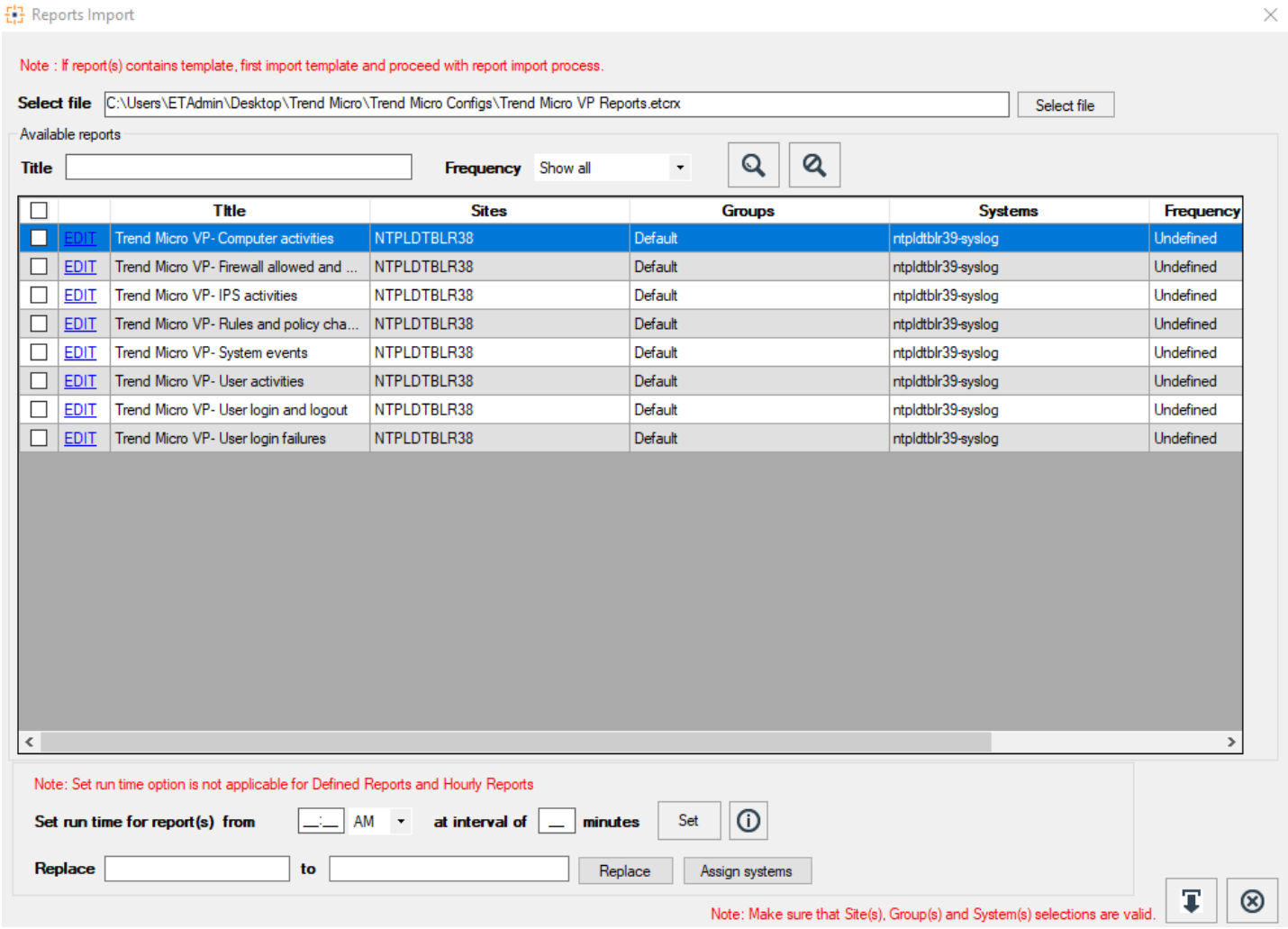


Figure 14

4. EventTracker displays success message.

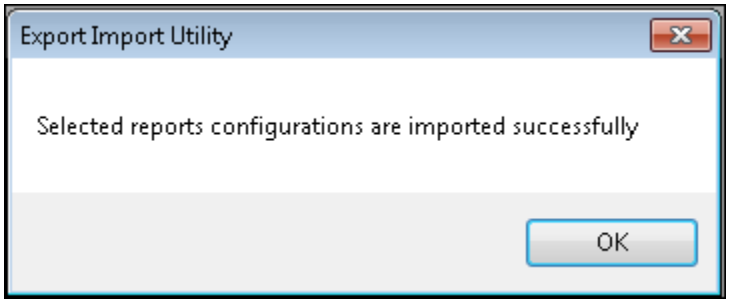


Figure 15

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

Verify Trend Micro Vulnerability Protection Knowledge Pack

Verify Categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Category**.
3. In **Category Tree** to view imported categories, scroll down and expand **'Trend Micro Vulnerability Protection'** group folder to view the imported categories.

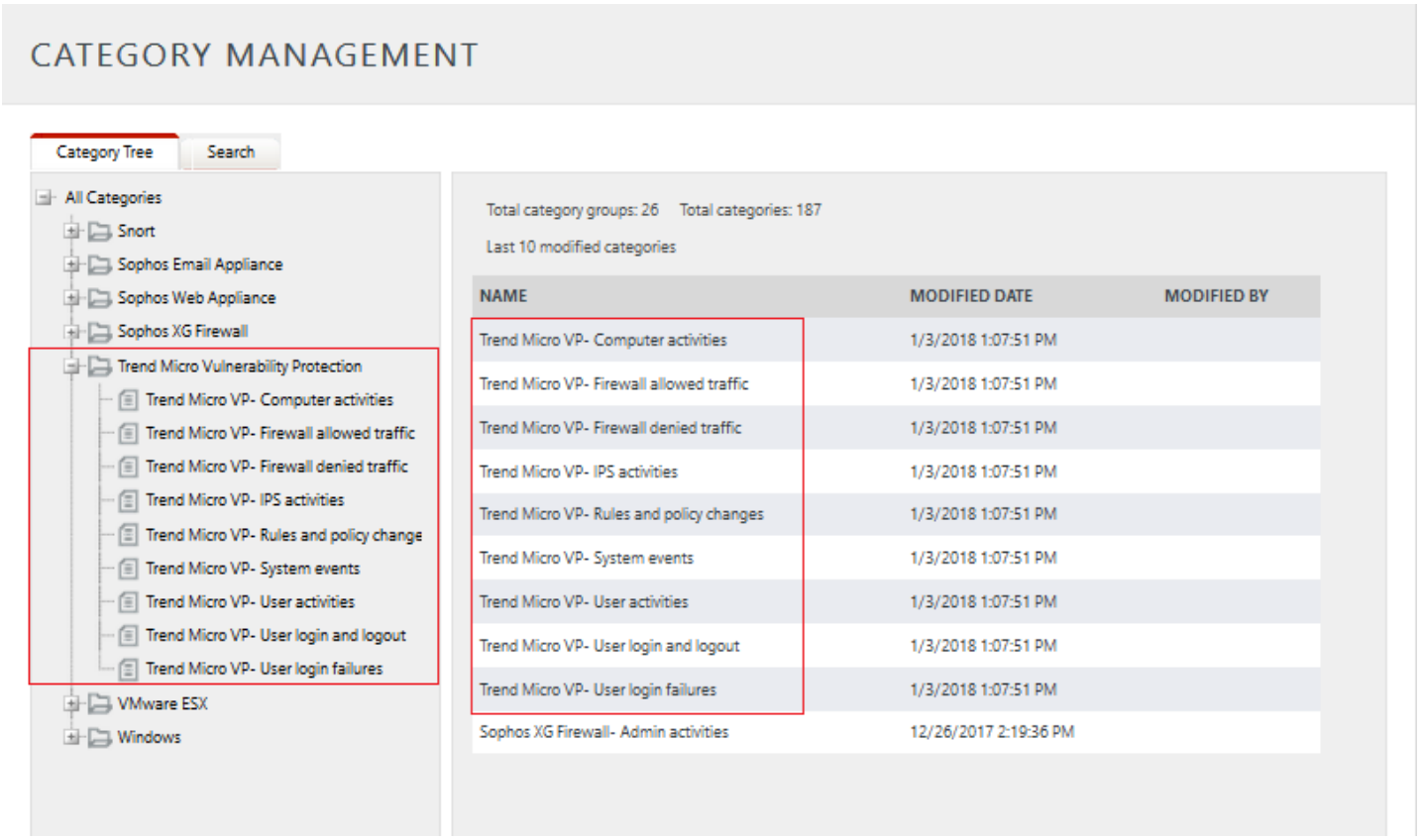


Figure 16

Verify Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In the **Search** box, type **'Trend Micro Vulnerability Protection'**, and then click the **Go** button. Alert Management page will display all the imported alerts.

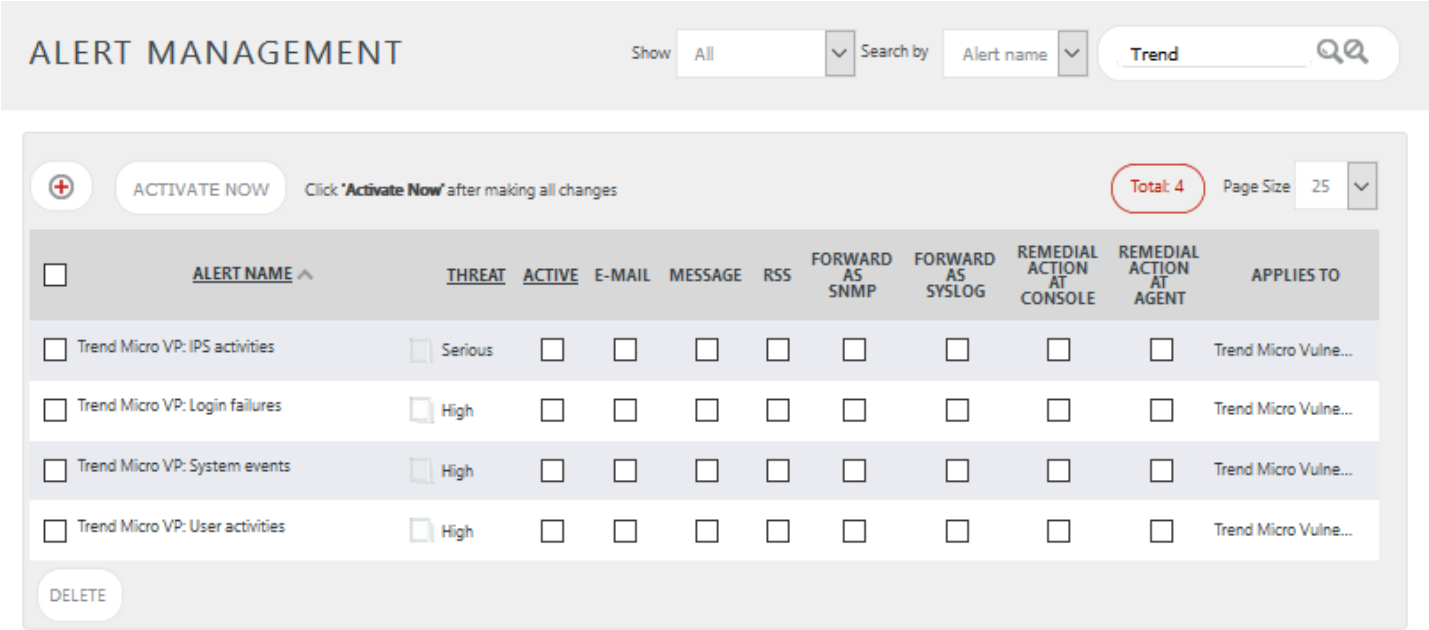


Figure 17

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays message box.

Figure 18

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

NOTE: Please specify appropriate **systems** in **alert configuration** for better performance.

Verify Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**
2. Scroll down and select **Trend Micro Vulnerability Protection** in **Objects** pane.
   Imported Trend Micro Vulnerability Protection details are shown.

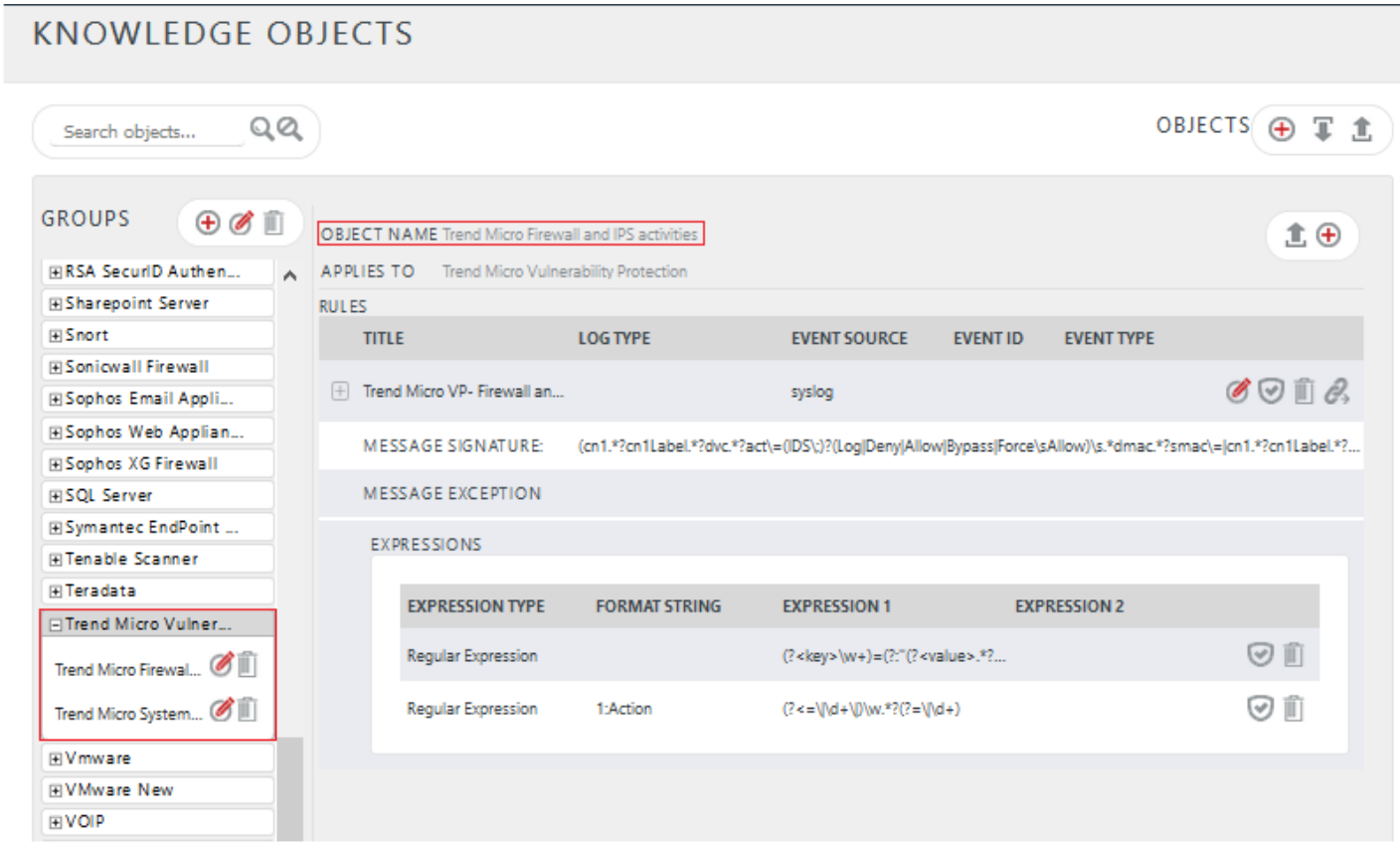


Figure 19

Token Template

1. Logon to **EventTracker Enterprise** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules** and click **Template**.
3. Click on **Trend Micro Vulnerability Protection** group option.

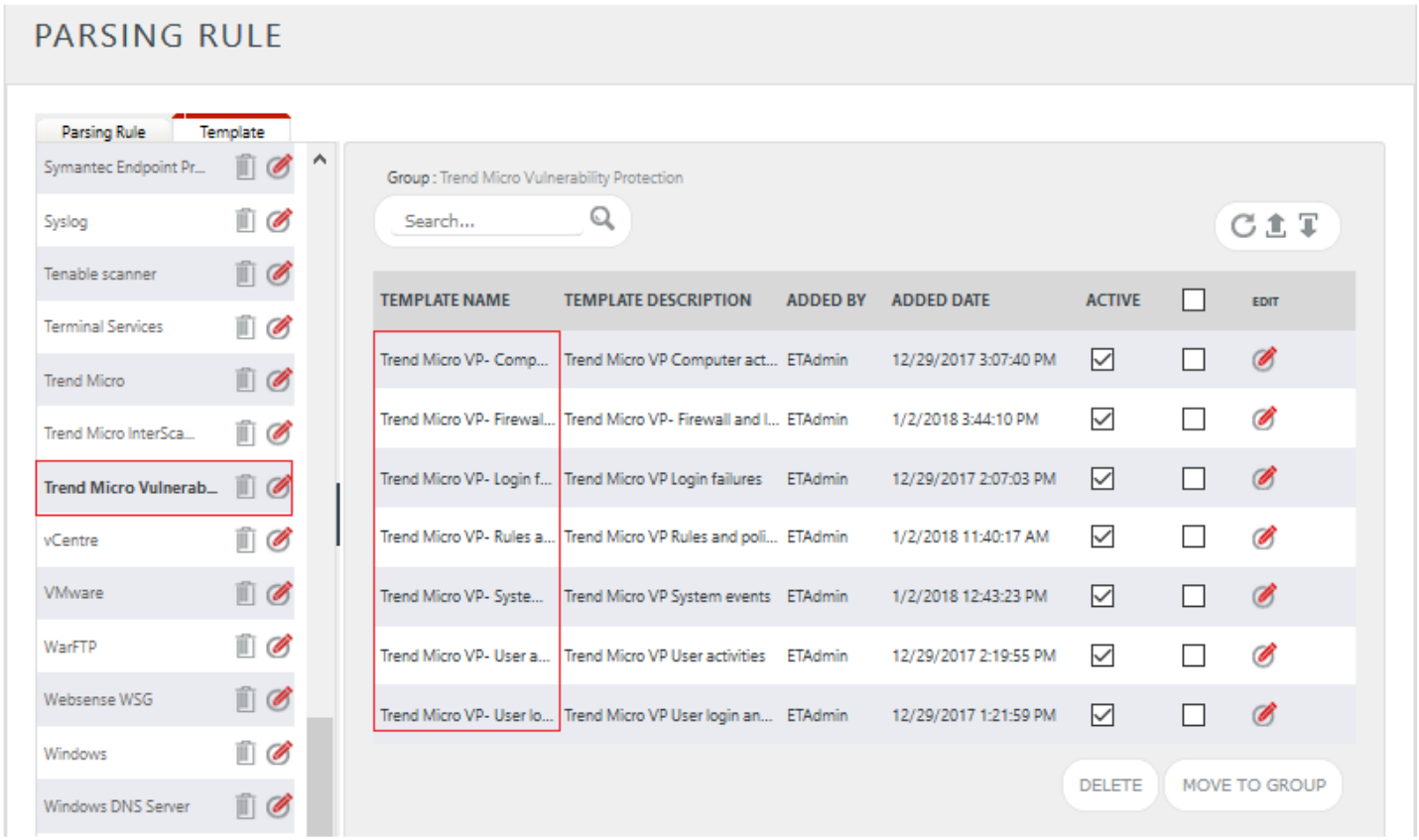


Figure 20

Verify Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then **Configuration**.
3. Select **Defined** in report type.
4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click **Trend Micro Vulnerability Protection** group folder.

   Scheduled Reports are displayed in the Reports configuration pane.

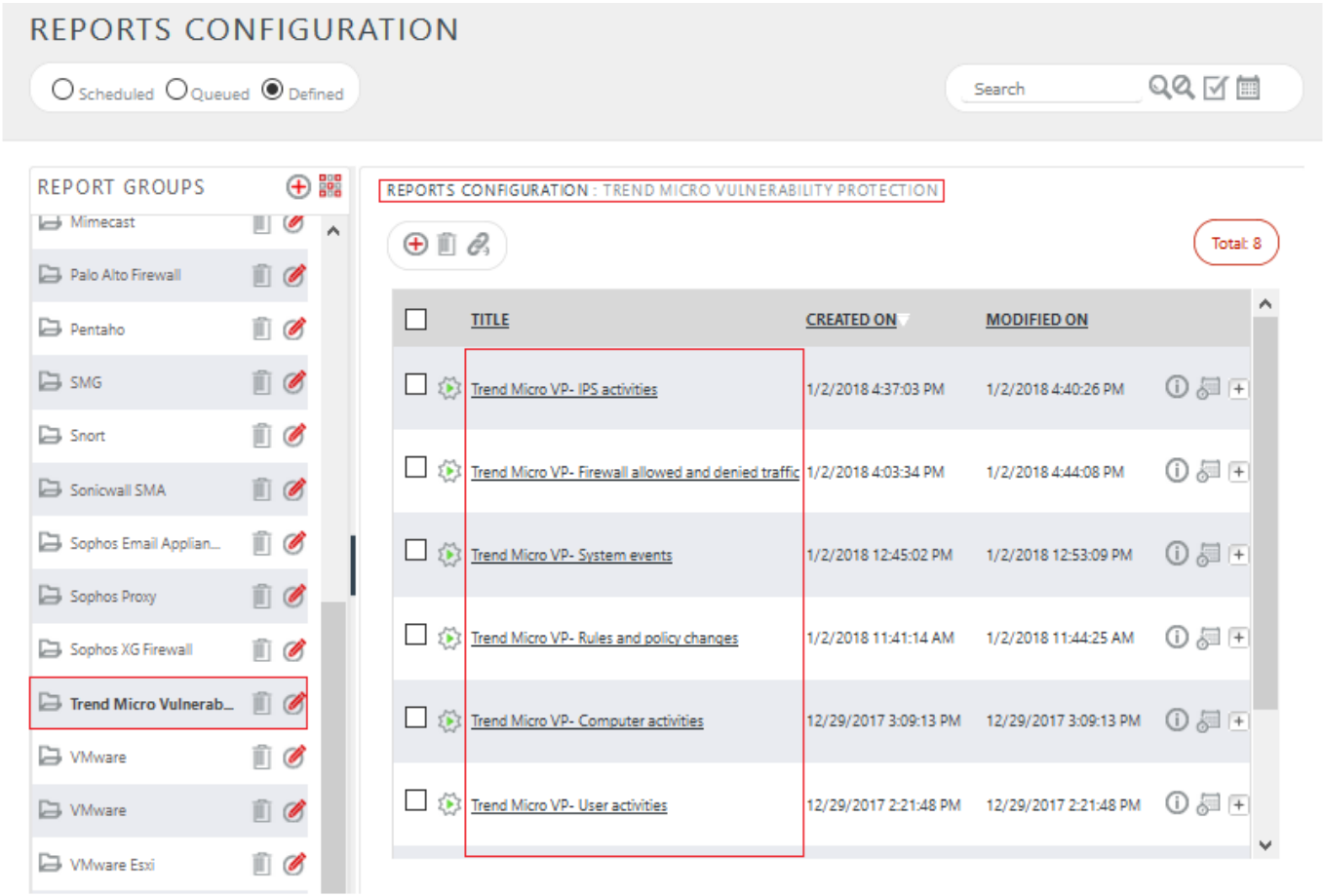


Figure 21

NOTE: Please specify appropriate **systems** in **report wizard** for better performance.

Create Dashboards in EventTracker

Schedule Reports

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

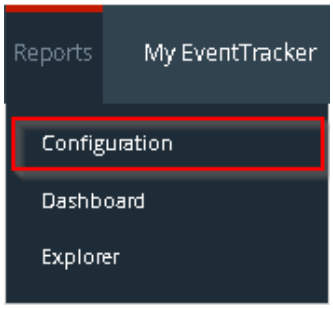


Figure 22

2. Navigate to **Reports>Configuration**.

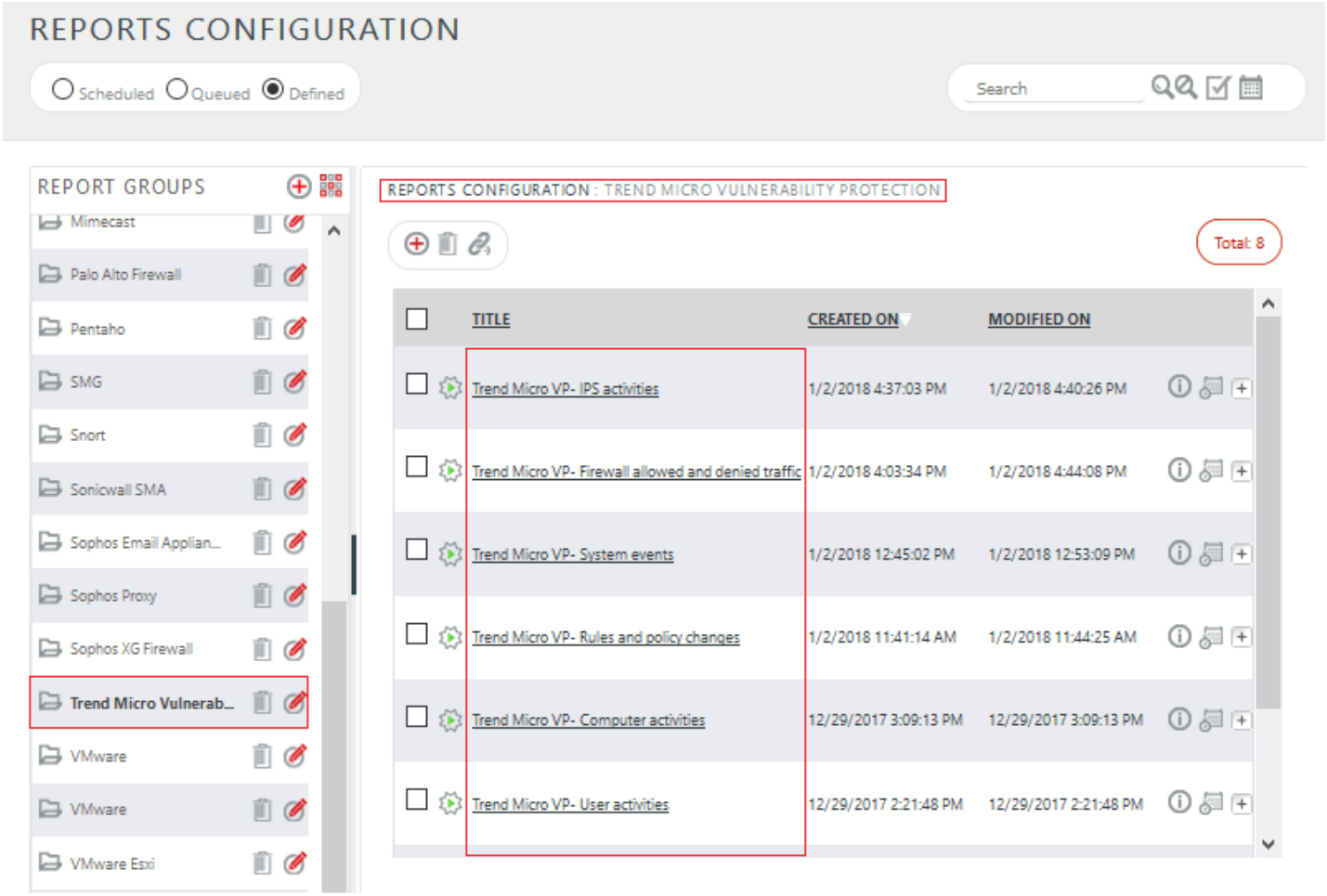


Figure 23

3. Select **Trend Micro Vulnerability Protection** in report groups. Check **defined** dialog box.
4. Click on '**schedule**'  to plan a report for later execution.

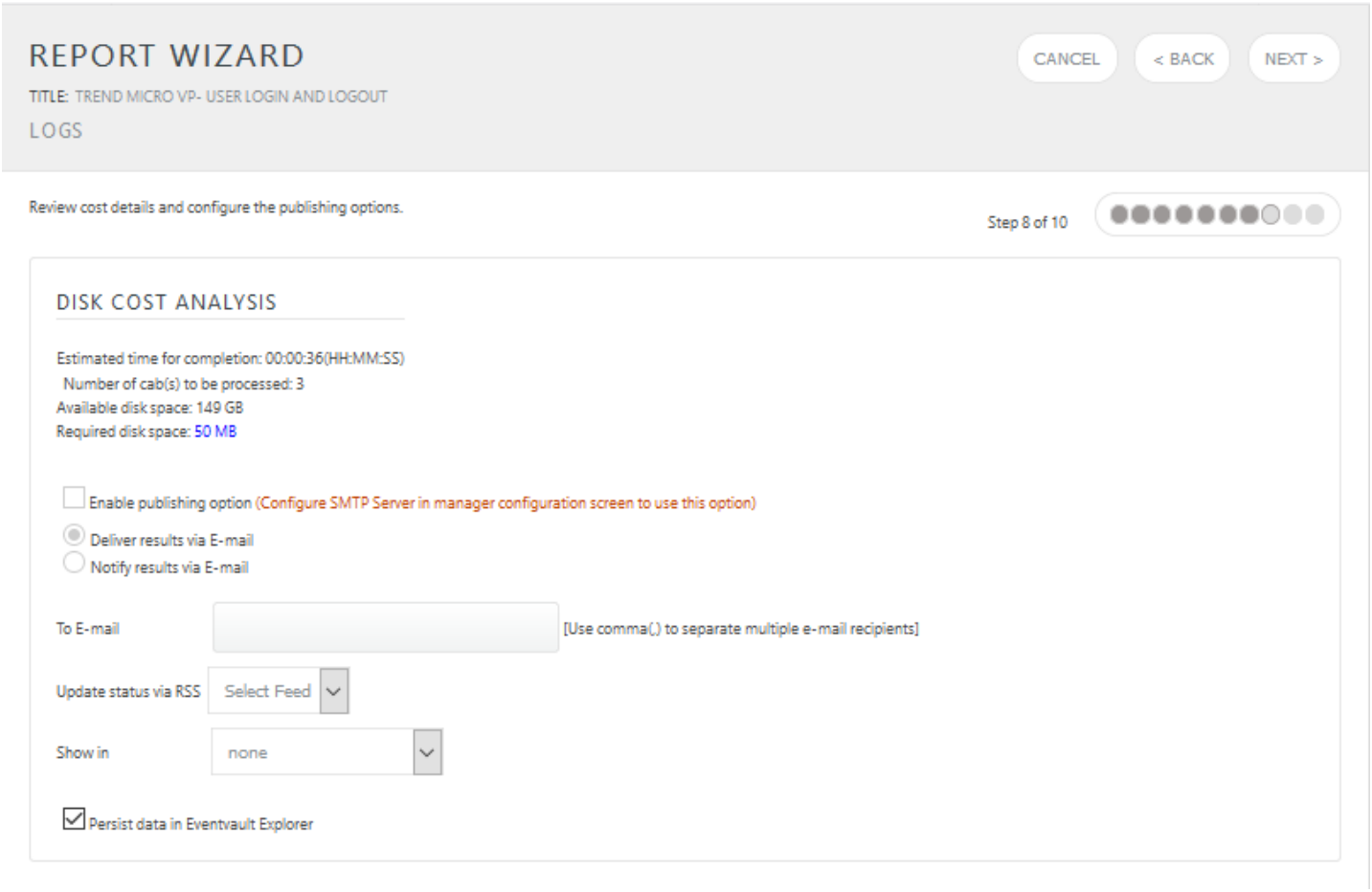


Figure 24

5. Choose appropriate time for report execution and in **Step 8** check **Persist data in Eventvault explorer** box.

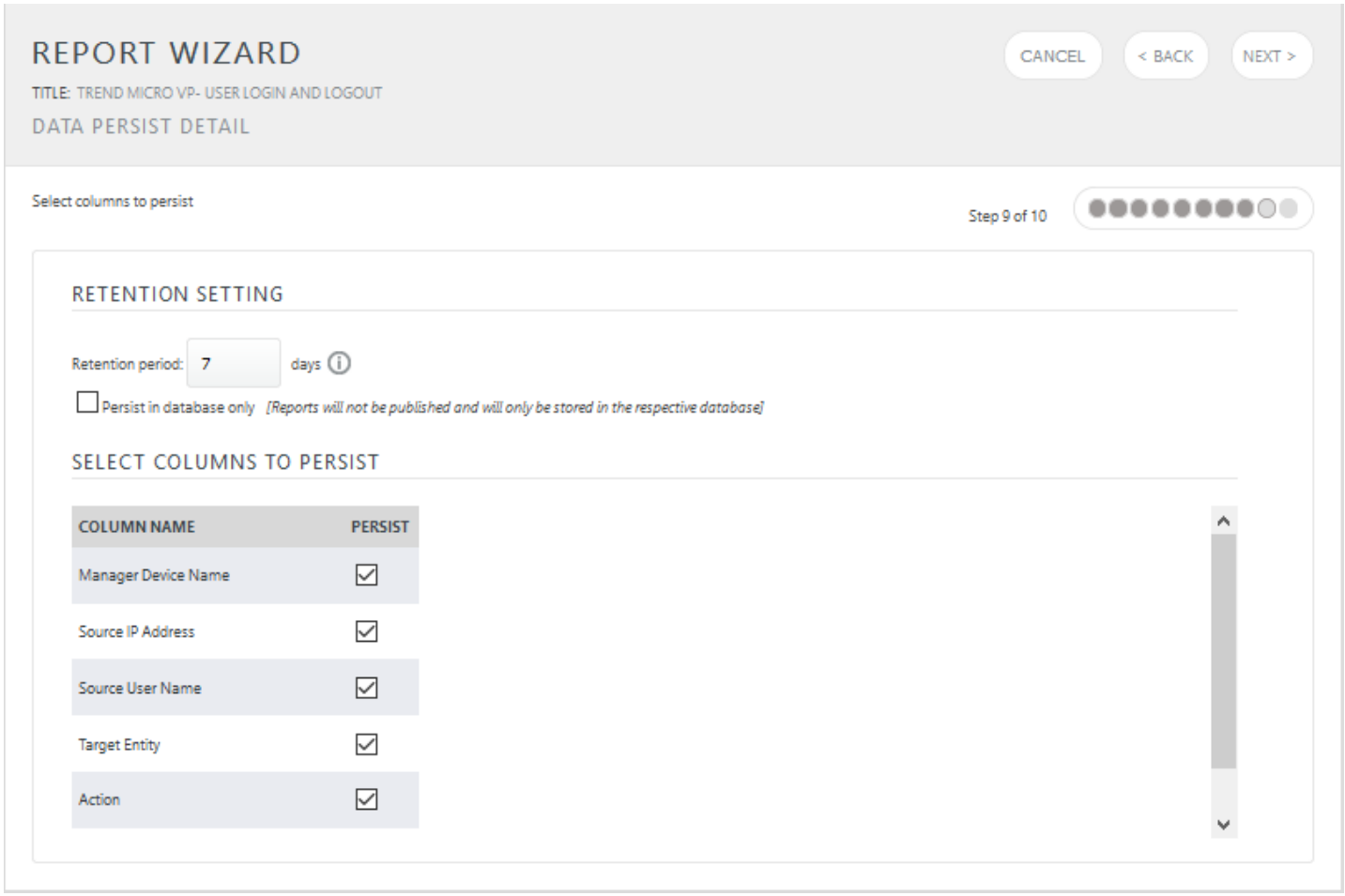


Figure 25

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
7. Proceed to next step and click **Schedule** button.
8. Wait for scheduled time or generate report manually.

Create Dashlets

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.

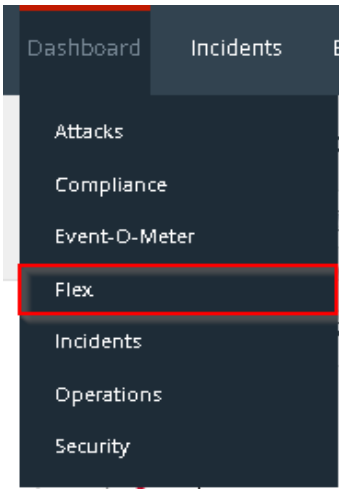


Figure 26

3. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

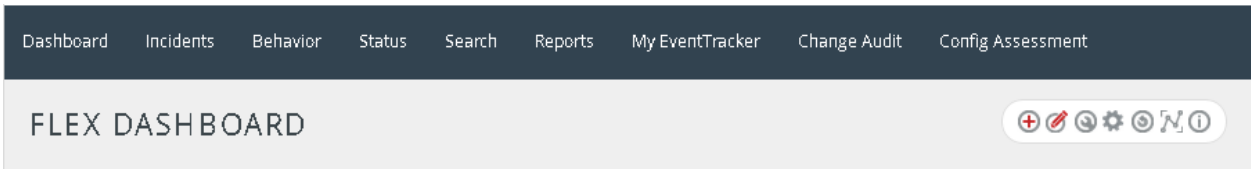


Figure 27

4. Click ⊕ to add a new dashboard.
   Flex Dashboard configuration pane is shown.

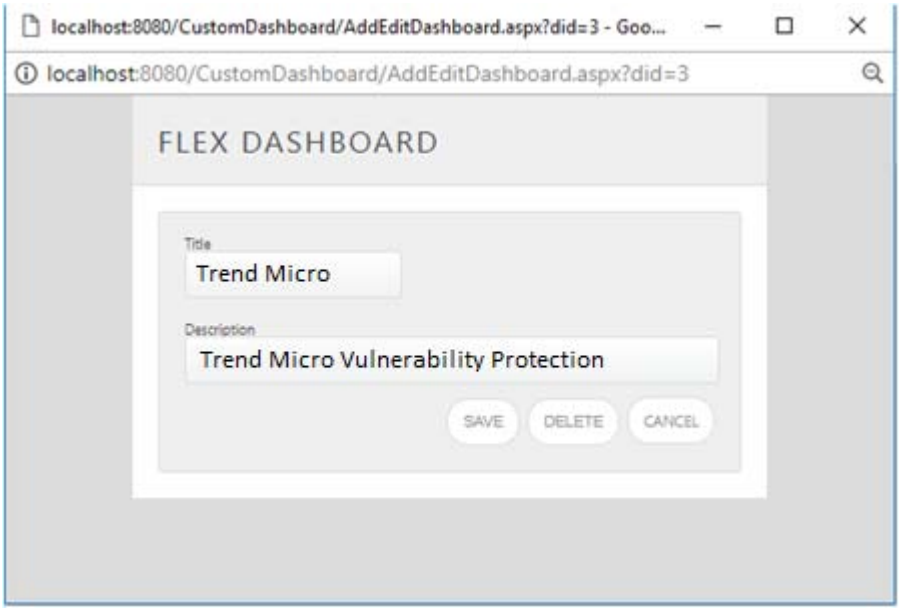


Figure 28

5. Fill fitting title and description and click **Save** button.
6. Click ⚙ to configure a new flex dashlet.
   Widget configuration pane is shown.

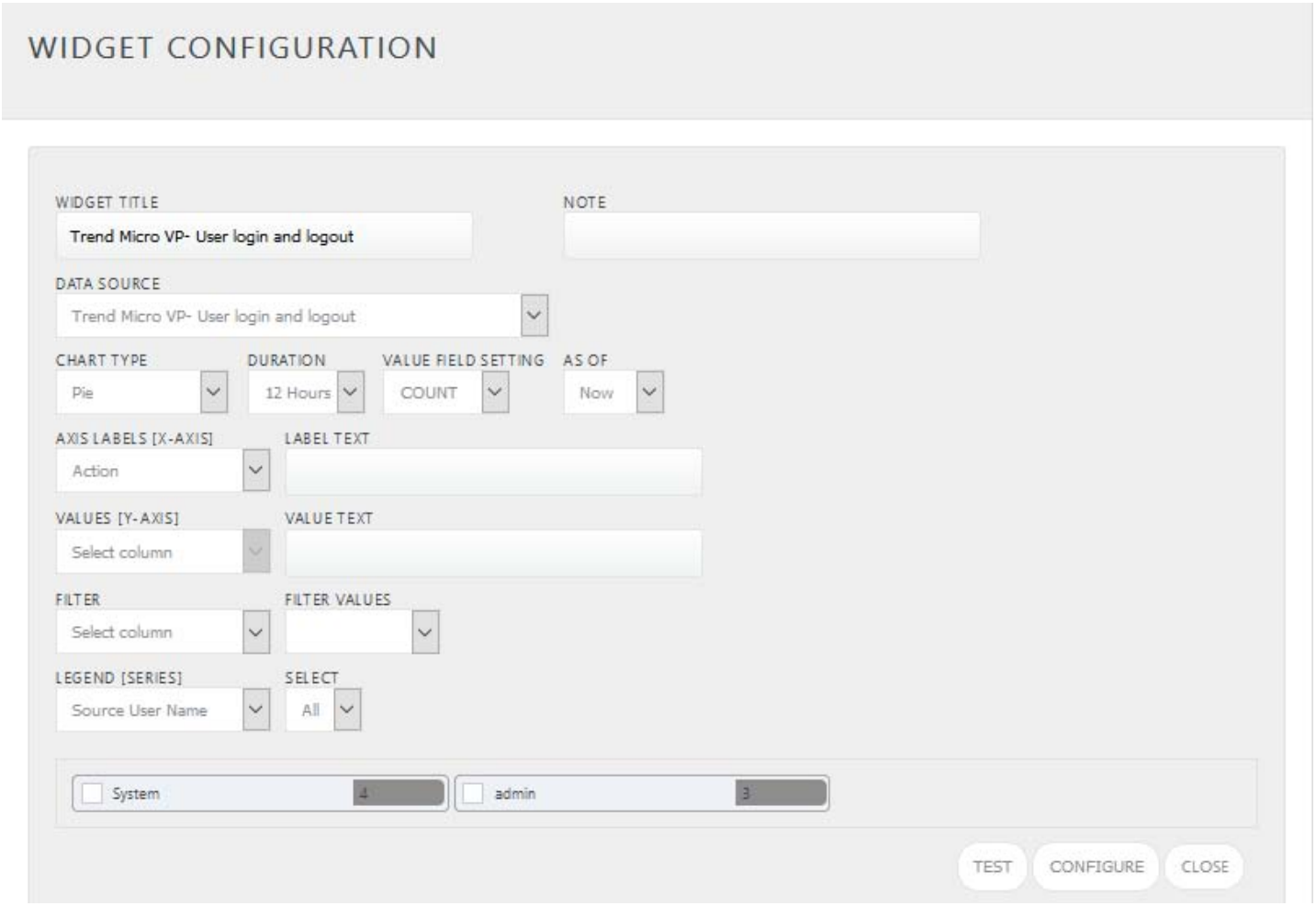


Figure 29

7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from dropdown.
9. Select extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X Axis** with suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Test** button to evaluate.
    Evaluated chart is shown.

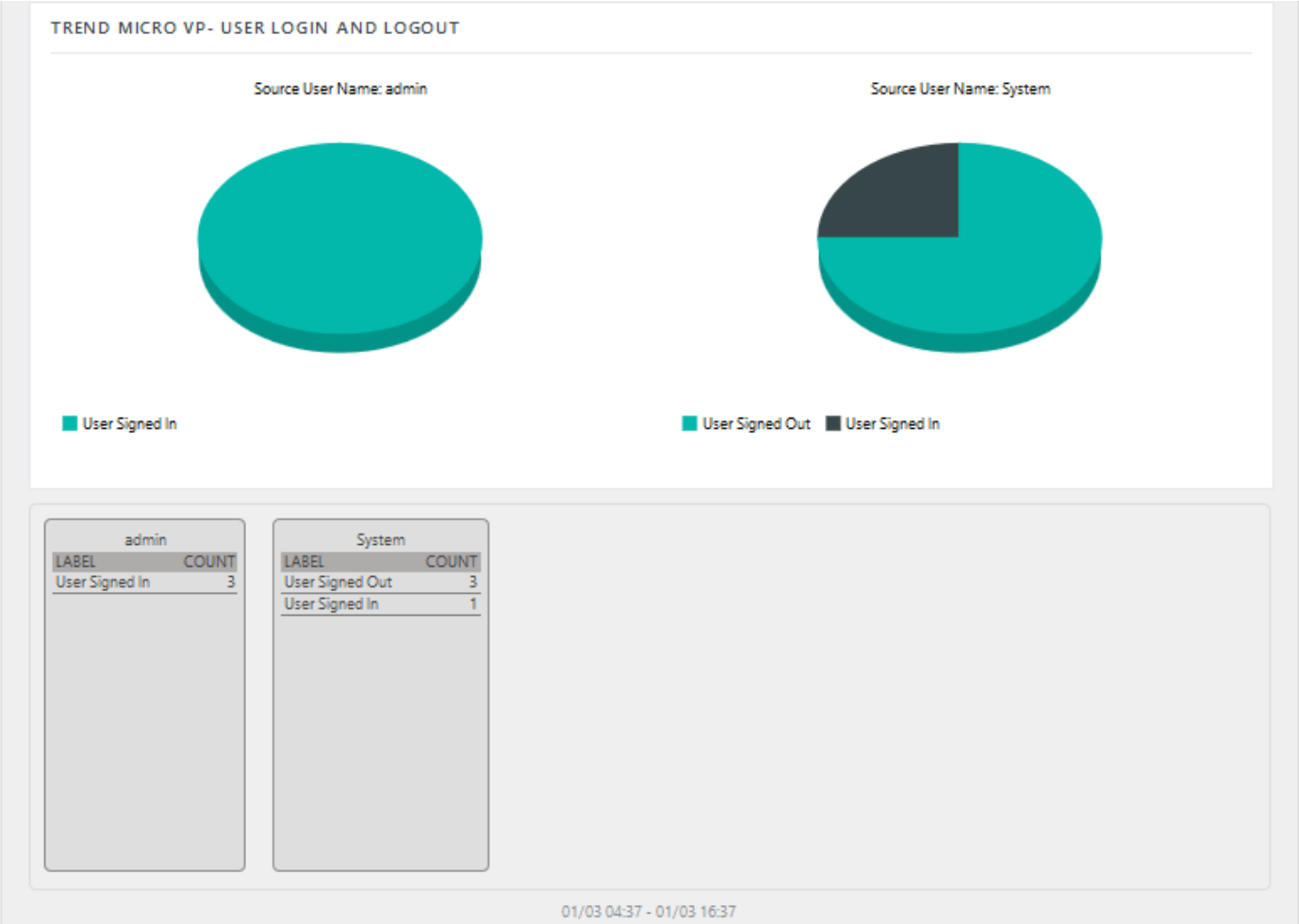
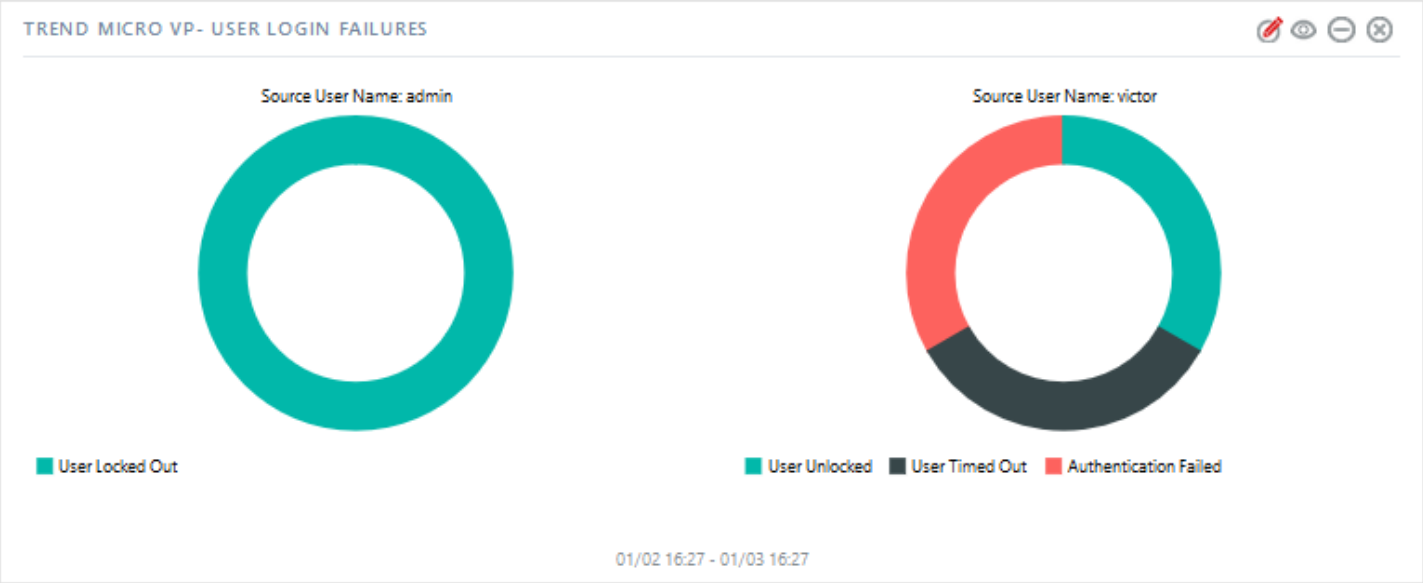


Figure 30

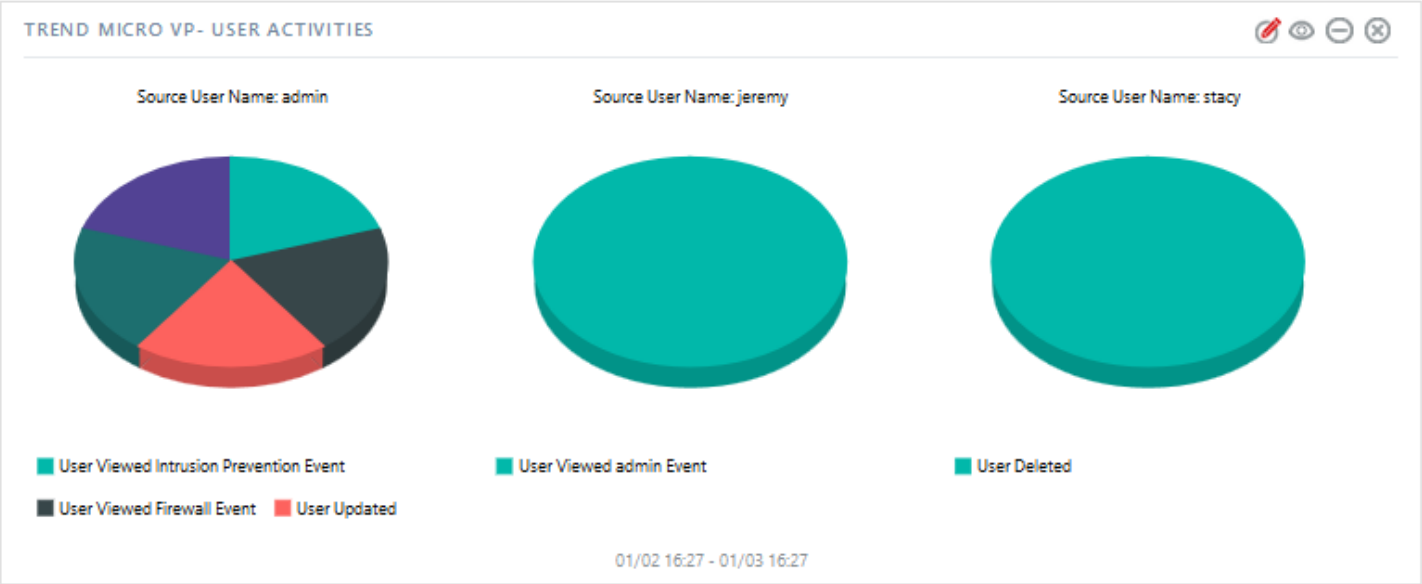
16. If satisfied, Click **Configure** button.
17. Click 'customize' to locate and choose created dashlet.
18. Click to add dashlet to earlier created dashboard.

Sample Dashboards

- **REPORT: Trend Micro Vulnerability Protection- User login failures**
  WIDGET TITLE: Trend Micro Vulnerability Protection- User login failures
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: Action
  LEGEND [SERIES]: Source IP Address

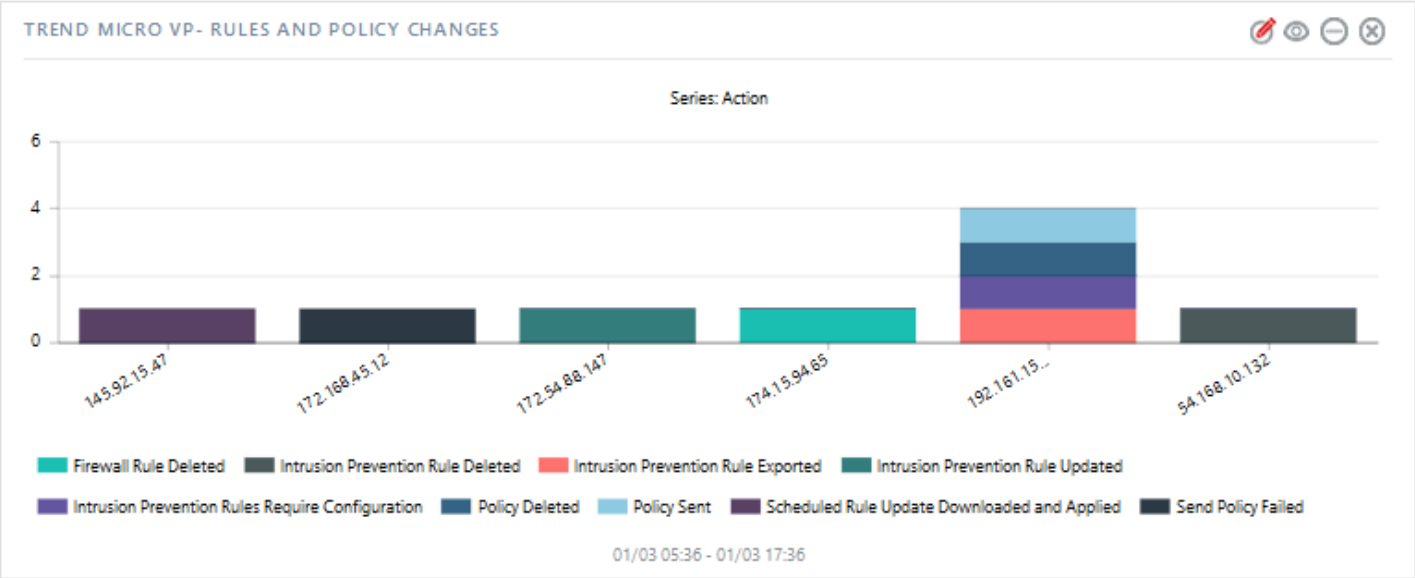


- **REPORT: Trend Micro Vulnerability Protection- User activities**
  WIDGET TITLE: Trend Micro Vulnerability Protection- User activities
  CHART TYPE: Pie
  AXIS LABELS [X-AXIS]: Event Name
  LEGEND [SERIES]: Source User Name

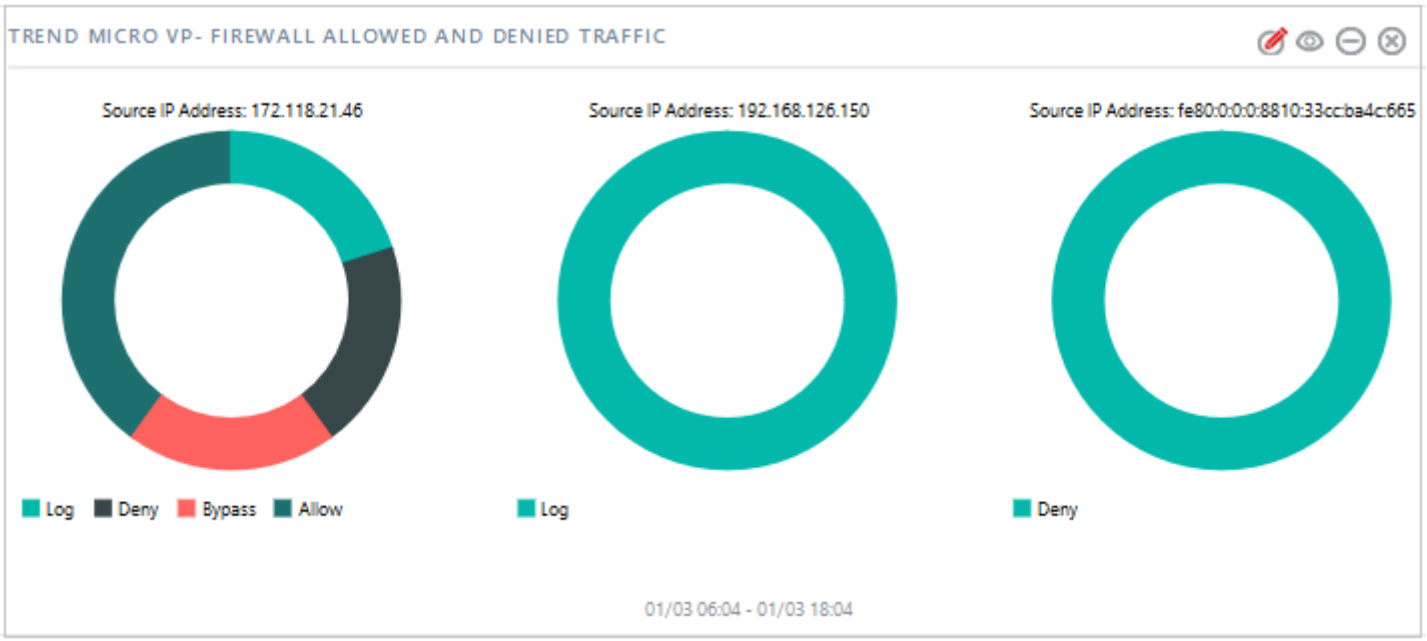


- **REPORT: Trend Micro Vulnerability Protection- System activities**
  WIDGET TITLE: Trend Micro Vulnerability Protection- System activities
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: Action
  LEGEND [SERIES]: Target Entity

- **REPORT: Trend Micro Vulnerability Protection- Rules and policy changes**
  WIDGET TITLE: Trend Micro Vulnerability Protection- Rules and policy changes
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Action
  LEGEND [SERIES]: Target Entity



- **REPORT: Trend Micro Vulnerability Protection- Firewall allowed and denied traffic**
  WIDGET TITLE: Trend Micro Vulnerability Protection- Firewall allowed and denied traffic
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: Action
  LEGEND [SERIES]: Source IP Address



- **REPORT: Trend Micro Vulnerability Protection- IPS activities**
  WIDGET TITLE: Trend Micro Vulnerability Protection- IPS activities
  CHART TYPE: Pie
  AXIS LABELS [X-AXIS]: Source IP Address
  LEGEND [SERIES]: Event Name

- **REPORT: Trend Micro Vulnerability Protection- Computer activities**
  WIDGET TITLE: Trend Micro Vulnerability Protection- Computer activities
  CHART TYPE: Pie
  AXIS LABELS [X-AXIS]: Action
  LEGEND [SERIES]: Target Entity