EventTracker
Actionable Security Intelligence

Integrate Untangle

EventTracker v8.x and above

Publication Date: April 13, 2018

Abstract

This guide provides instructions to configure Untangle to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Untangle.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version v8.x or above and Untangle.

Audience

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

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

This document is for informational purposes only. EventTracker 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 EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker 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 EventTracker, 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.

Table of Contents

Overview

Untangle, a network software and appliance company, provides the most complete multi-function firewall and Internet management application suite available today.

EventTracker helps to monitor events from Untangle. It’s knowledge object and flex reports will help you to analyze critical activities and to monitor login events.

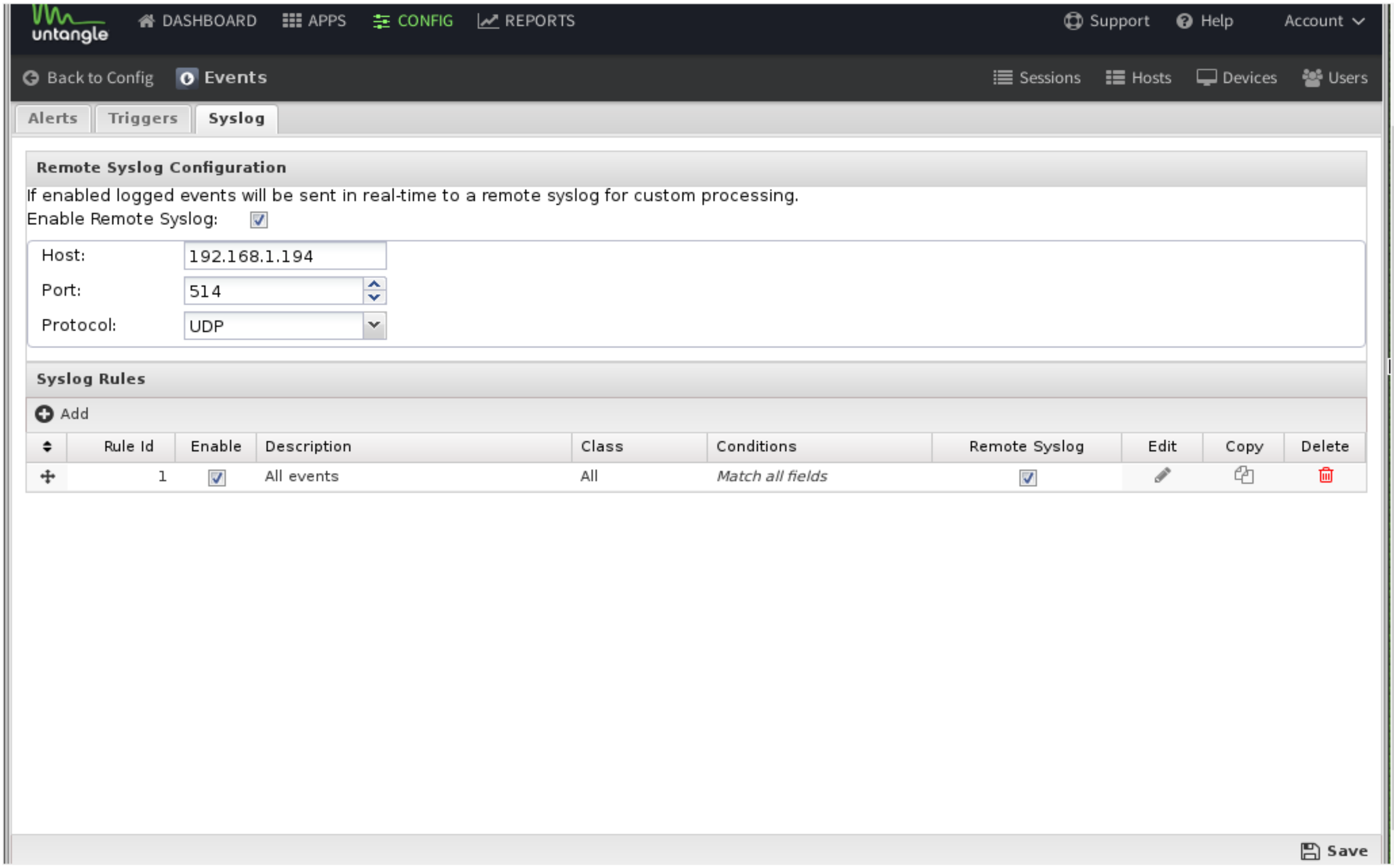
Prerequisites

- EventTracker agent should be installed.
- Untangle should be configured for forwarding logs.
- Please add exception for port 514 in firewall if exists in between Untangle and EventTracker Manager.

Configure Untangle to forward logs to EventTracker

To configure the Untangle to forward logs to a syslog server,

1. Log on to the Untangle Management Console as an Administrator.
2. From Web GUI choose **CONFIG**.
3. Go to **Events > Syslog** to display the configuration page**.**
4. Under the **Remote Syslog Configuration**.
5. Check the ‘**Enable Remote Syslog’** box to enable the remote logging.
6. For **Host,** type the IP address of **EventTracker Manager**.
7. For **Port,** type **514** for default syslog server port.
8. For **Protocol,** dropdown and select **UDP**.
9. Under the **Syslog Rules**.
10. Check the ‘**Enable’** and ‘**Remote Syslog’** box to set the rules.
11. Click the **Save** option to save the configurations.



Remote Syslog Configuration

If enabled logged events will be sent in real-time to a remote syslog for custom processing.

Enable Remote Syslog: ☑

Host: 192.168.1.194

Port: 514

Protocol: UDP

Syslog Rules

Rule Id	Enable	Description	Class	Conditions	Remote Syslog	Edit	Copy	Delete
1	☑	All events	All	*Match all fields*	☑			

Figure 1

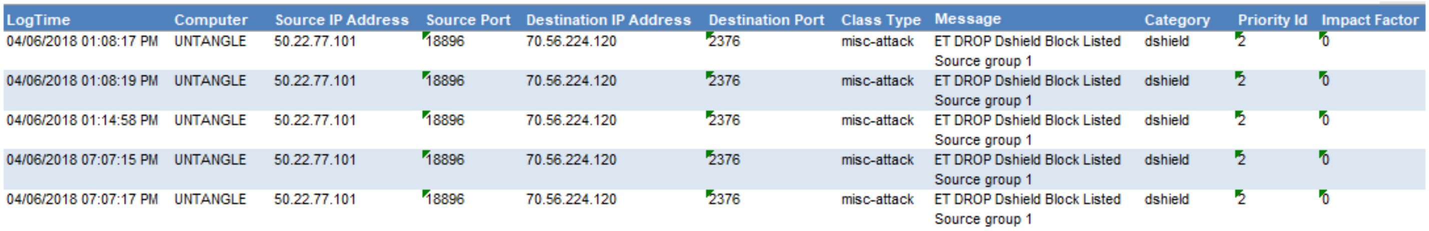
EventTracker Knowledge Pack

Once logs are received by EventTracker manager, Knowledge Packs can be configured into EventTracker.

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

Flex Reports

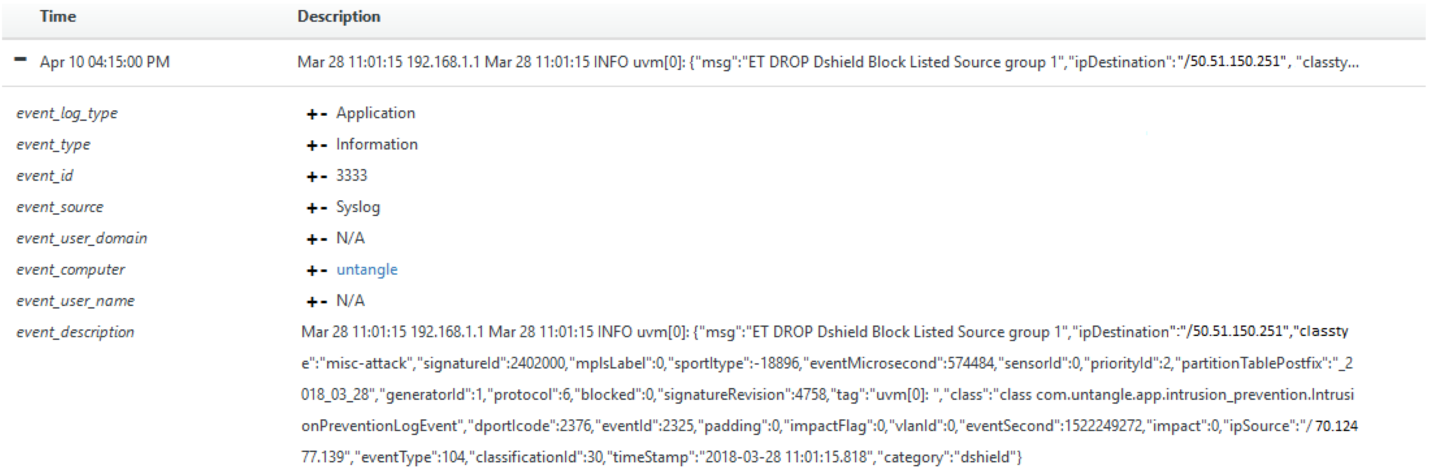
- **Untangle - Threat detection -** This report gives the information about all the threats that are detected by Untangle firewall.



LogTime	Computer	Source IP Address	Source Port	Destination IP Address	Destination Port	Class Type	Message	Category	Priority Id	Impact Factor
04/06/2018 01:08:17 PM	UNTANGLE	50.22.77.101	18896	70.56.224.120	2376	misc-attack	ET DROP Dshield Block Listed Source group 1	dshield	2	0
04/06/2018 01:08:19 PM	UNTANGLE	50.22.77.101	18896	70.56.224.120	2376	misc-attack	ET DROP Dshield Block Listed Source group 1	dshield	2	0
04/06/2018 01:14:58 PM	UNTANGLE	50.22.77.101	18896	70.56.224.120	2376	misc-attack	ET DROP Dshield Block Listed Source group 1	dshield	2	0
04/06/2018 07:07:15 PM	UNTANGLE	50.22.77.101	18896	70.56.224.120	2376	misc-attack	ET DROP Dshield Block Listed Source group 1	dshield	2	0
04/06/2018 07:07:17 PM	UNTANGLE	50.22.77.101	18896	70.56.224.120	2376	misc-attack	ET DROP Dshield Block Listed Source group 1	dshield	2	0

Figure 2

Sample logs:

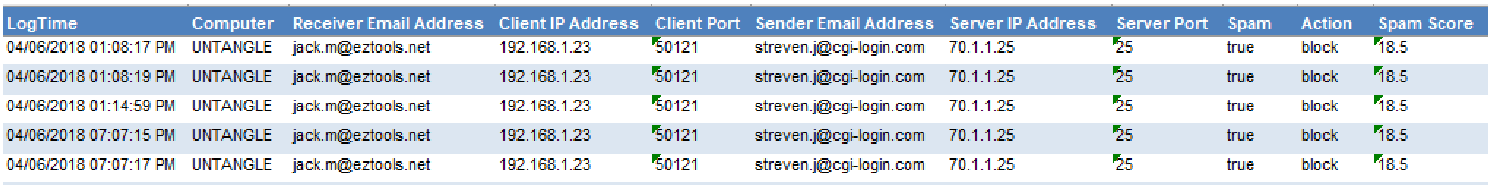


```
Time                   Description
− Apr 10 04:15:00 PM   Mar 28 11:01:15 192.168.1.1 Mar 28 11:01:15 INFO uvm[0]: {"msg":"ET DROP Dshield Block Listed Source group 1","ipDestination":"/50.51.150.251", "classty...

event_log_type         +- Application
event_type             +- Information
event_id               +- 3333
event_source           +- Syslog
event_user_domain      +- N/A
event_computer         +- untangle
event_user_name        +- N/A
event_description      Mar 28 11:01:15 192.168.1.1 Mar 28 11:01:15 INFO uvm[0]: {"msg":"ET DROP Dshield Block Listed Source group 1","ipDestination":"/50.51.150.251","classty
                       e":"misc-attack","signatureId":2402000,"mplsLabel":0,"sportItype":-18896,"eventMicrosecond":574484,"sensorId":0,"priorityId":2,"partitionTablePostfix":"_2
                       018_03_28","generatorId":1,"protocol":6,"blocked":0,"signatureRevision":4758,"tag":"uvm[0]: ","class":"class com.untangle.app.intrusion_prevention.Intrusi
                       onPreventionLogEvent","dportIcode":2376,"eventId":2325,"padding":0,"impactFlag":0,"vlanId":0,"eventSecond":1522249272,"impact":0,"ipSource":"/ 70.124
                       77.139","eventType":104,"classificationId":30,"timeStamp":"2018-03-28 11:01:15.818","category":"dshield"}
```

Figure 3

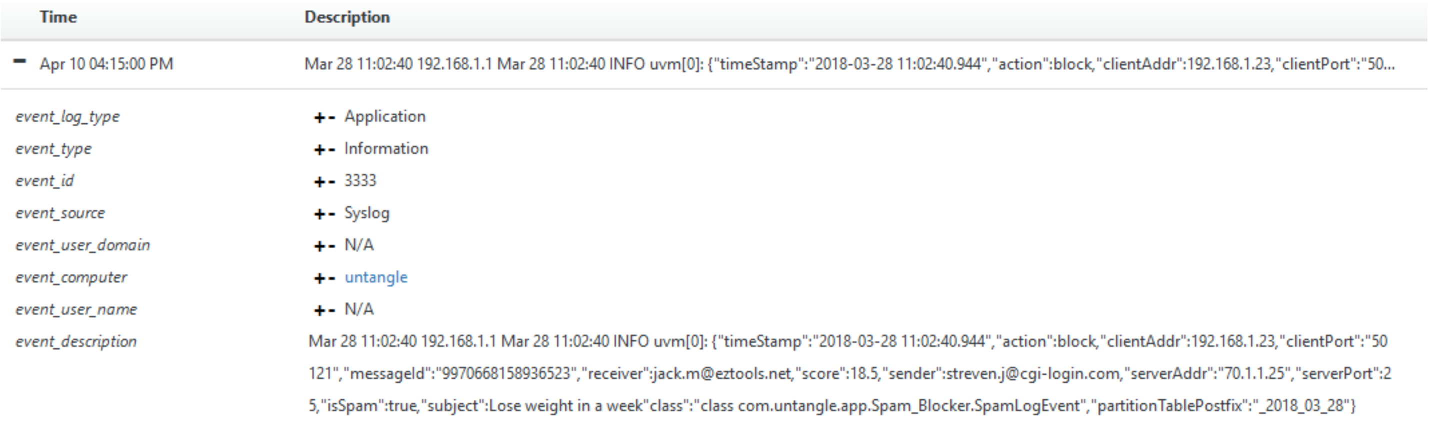
- **Untangle - Spam emails -** This report gives the information about all the spam emails which are blocked or allowed.



LogTime	Computer	Receiver Email Address	Client IP Address	Client Port	Sender Email Address	Server IP Address	Server Port	Spam	Action	Spam Score
04/06/2018 01:08:17 PM	UNTANGLE	jack.m@eztools.net	192.168.1.23	50121	streven.j@cgi-login.com	70.1.1.25	25	true	block	18.5
04/06/2018 01:08:19 PM	UNTANGLE	jack.m@eztools.net	192.168.1.23	50121	streven.j@cgi-login.com	70.1.1.25	25	true	block	18.5
04/06/2018 01:14:59 PM	UNTANGLE	jack.m@eztools.net	192.168.1.23	50121	streven.j@cgi-login.com	70.1.1.25	25	true	block	18.5
04/06/2018 07:07:15 PM	UNTANGLE	jack.m@eztools.net	192.168.1.23	50121	streven.j@cgi-login.com	70.1.1.25	25	true	block	18.5
04/06/2018 07:07:17 PM	UNTANGLE	jack.m@eztools.net	192.168.1.23	50121	streven.j@cgi-login.com	70.1.1.25	25	true	block	18.5

Figure 4

Sample logs:

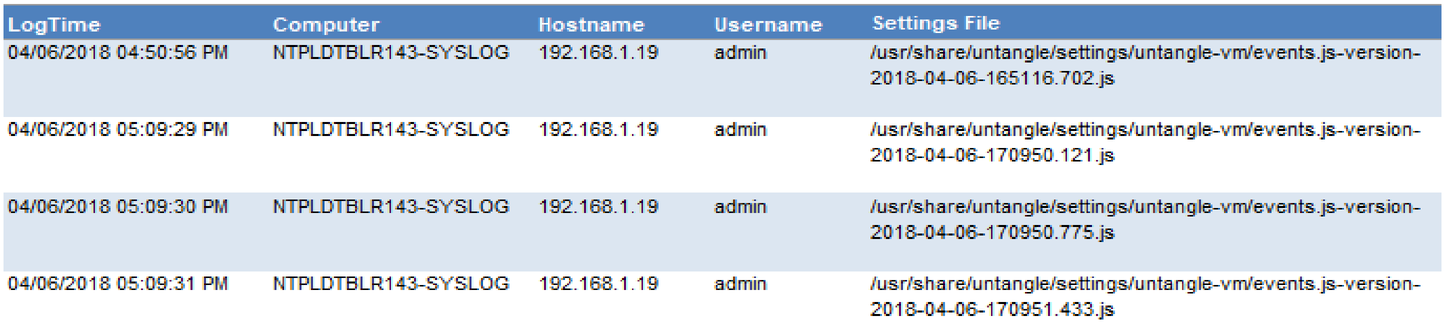


```
Time                   Description
− Apr 10 04:15:00 PM   Mar 28 11:02:40 192.168.1.1 Mar 28 11:02:40 INFO uvm[0]: {"timeStamp":"2018-03-28 11:02:40.944","action":block,"clientAddr":192.168.1.23,"clientPort":"50...

event_log_type         +- Application
event_type             +- Information
event_id               +- 3333
event_source           +- Syslog
event_user_domain      +- N/A
event_computer         +- untangle
event_user_name        +- N/A
event_description      Mar 28 11:02:40 192.168.1.1 Mar 28 11:02:40 INFO uvm[0]: {"timeStamp":"2018-03-28 11:02:40.944","action":block,"clientAddr":192.168.1.23,"clientPort":"50
                       121","messageId":"9970668158936523","receiver":jack.m@eztools.net,"score":18.5,"sender":streven.j@cgi-login.com,"serverAddr":"70.1.1.25","serverPort":2
                       5,"isSpam":true,"subject":Lose weight in a week"class":"class com.untangle.app.Spam_Blocker.SpamLogEvent","partitionTablePostfix":"_2018_03_28"}
```

Figure 5

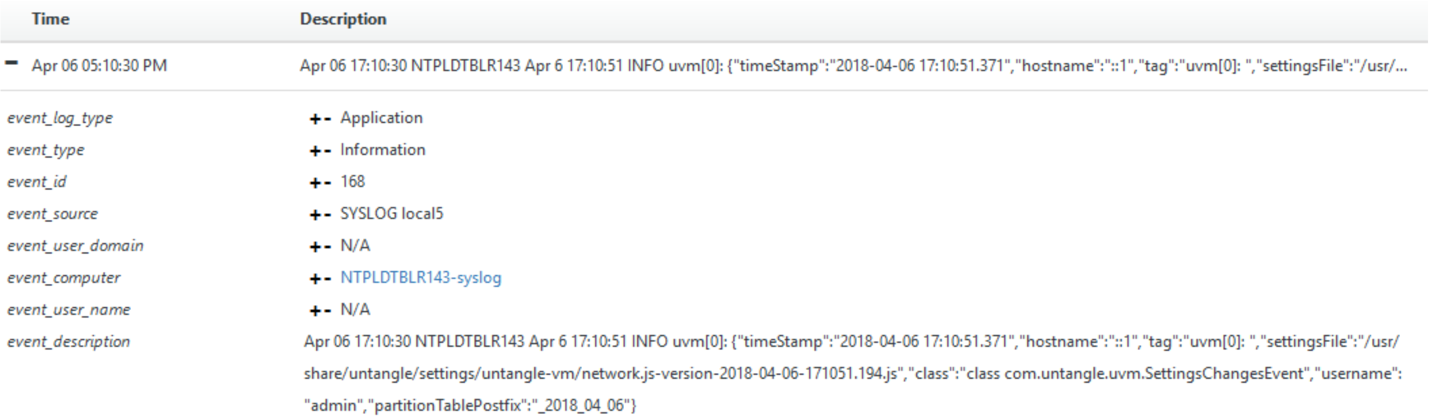
- **Untangle - Settings changes -** This report gives information about device settings changes.



LogTime	Computer	Hostname	Username	Settings File
04/06/2018 04:50:56 PM	NTPLDTBLR143-SYSLOG	192.168.1.19	admin	/usr/share/untangle/settings/untangle-vm/events.js-version-2018-04-06-165116.702.js
04/06/2018 05:09:29 PM	NTPLDTBLR143-SYSLOG	192.168.1.19	admin	/usr/share/untangle/settings/untangle-vm/events.js-version-2018-04-06-170950.121.js
04/06/2018 05:09:30 PM	NTPLDTBLR143-SYSLOG	192.168.1.19	admin	/usr/share/untangle/settings/untangle-vm/events.js-version-2018-04-06-170950.775.js
04/06/2018 05:09:31 PM	NTPLDTBLR143-SYSLOG	192.168.1.19	admin	/usr/share/untangle/settings/untangle-vm/events.js-version-2018-04-06-170951.433.js

Figure 6

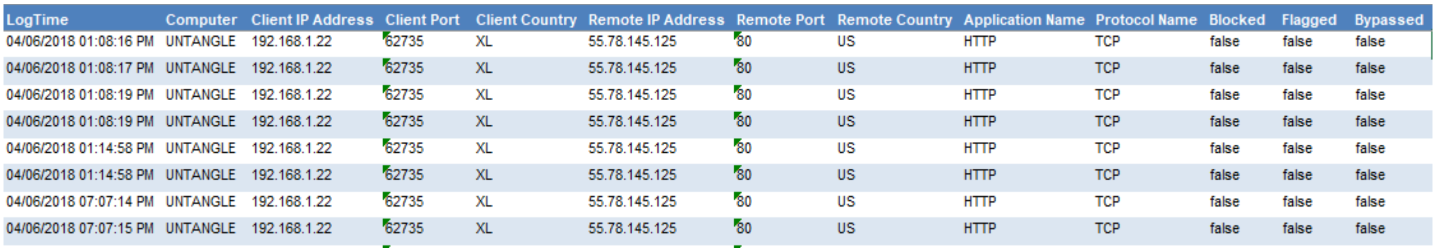
Sample logs:



Time	Description
− Apr 06 05:10:30 PM	Apr 06 17:10:30 NTPLDTBLR143 Apr 6 17:10:51 INFO uvm[0]: {"timeStamp":"2018-04-06 17:10:51.371","hostname":"::1","tag":"uvm[0]: ","settingsFile":"/usr/...
event_log_type	+- Application
event_type	+- Information
event_id	+- 168
event_source	+- SYSLOG local5
event_user_domain	+- N/A
event_computer	+- NTPLDTBLR143-syslog
event_user_name	+- N/A
event_description	Apr 06 17:10:30 NTPLDTBLR143 Apr 6 17:10:51 INFO uvm[0]: {"timeStamp":"2018-04-06 17:10:51.371","hostname":"::1","tag":"uvm[0]: ","settingsFile":"/usr/share/untangle/settings/untangle-vm/network.js-version-2018-04-06-171051.194.js","class":"class com.untangle.uvm.SettingsChangesEvent","username":"admin","partitionTablePostfix":"_2018_04_06"}

Figure 7

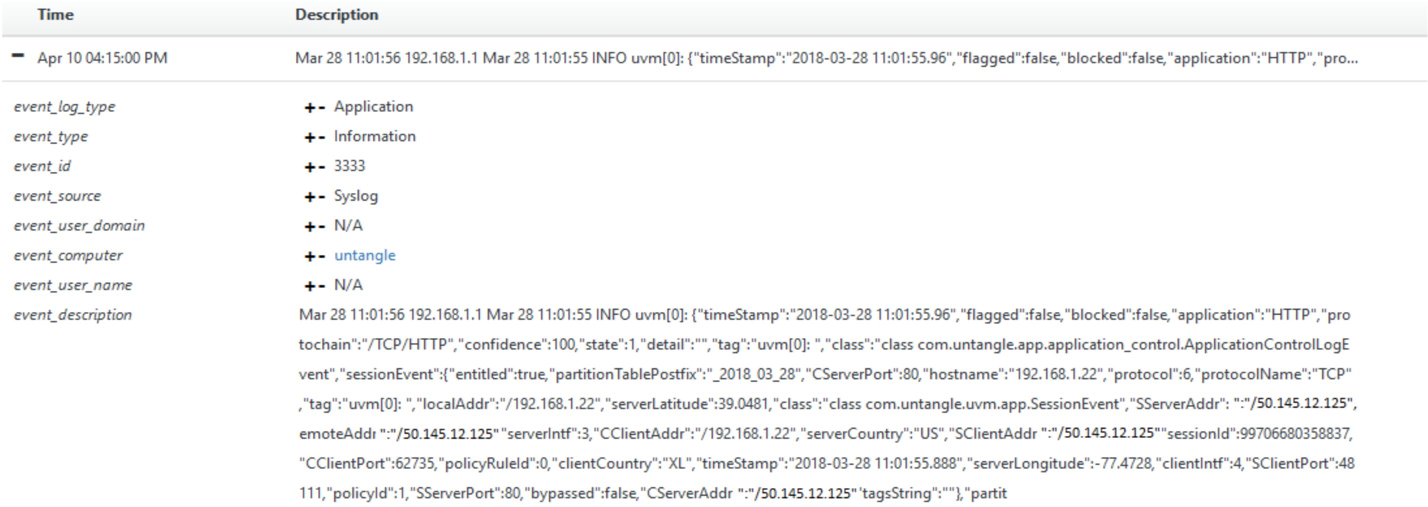
- **Untangle - Application control -** This report gives information about all the applications which are blocked or allowed.



LogTime	Computer	Client IP Address	Client Port	Client Country	Remote IP Address	Remote Port	Remote Country	Application Name	Protocol Name	Blocked	Flagged	Bypassed
04/06/2018 01:08:16 PM	UNTANGLE	192.168.1.22	62735	XL	55.78.145.125	80	US	HTTP	TCP	false	false	false
04/06/2018 01:08:17 PM	UNTANGLE	192.168.1.22	62735	XL	55.78.145.125	80	US	HTTP	TCP	false	false	false
04/06/2018 01:08:19 PM	UNTANGLE	192.168.1.22	62735	XL	55.78.145.125	80	US	HTTP	TCP	false	false	false
04/06/2018 01:08:19 PM	UNTANGLE	192.168.1.22	62735	XL	55.78.145.125	80	US	HTTP	TCP	false	false	false
04/06/2018 01:14:58 PM	UNTANGLE	192.168.1.22	62735	XL	55.78.145.125	80	US	HTTP	TCP	false	false	false
04/06/2018 01:14:58 PM	UNTANGLE	192.168.1.22	62735	XL	55.78.145.125	80	US	HTTP	TCP	false	false	false
04/06/2018 07:07:14 PM	UNTANGLE	192.168.1.22	62735	XL	55.78.145.125	80	US	HTTP	TCP	false	false	false
04/06/2018 07:07:15 PM	UNTANGLE	192.168.1.22	62735	XL	55.78.145.125	80	US	HTTP	TCP	false	false	false

Figure 8

Sample logs:

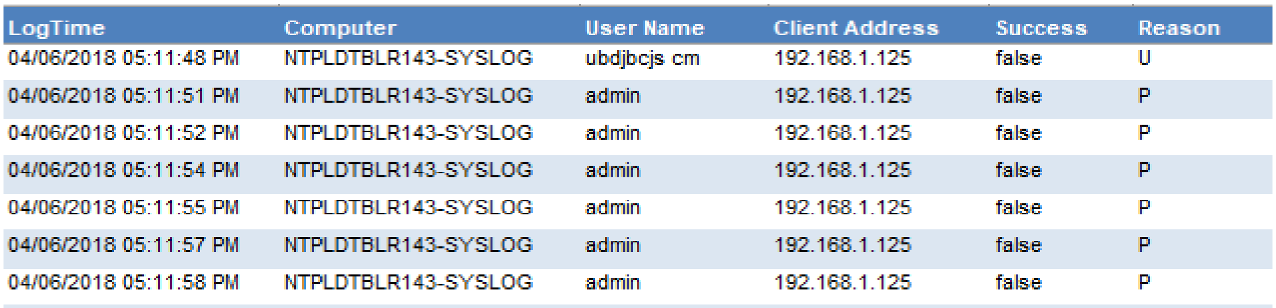


```
Time                    Description
−  Apr 10 04:15:00 PM   Mar 28 11:01:56 192.168.1.1 Mar 28 11:01:55 INFO uvm[0]: {"timeStamp":"2018-03-28 11:01:55.96","flagged":false,"blocked":false,"application":"HTTP","pro...

event_log_type          +- Application
event_type              +- Information
event_id                +- 3333
event_source            +- Syslog
event_user_domain       +- N/A
event_computer          +- untangle
event_user_name         +- N/A
event_description       Mar 28 11:01:56 192.168.1.1 Mar 28 11:01:55 INFO uvm[0]: {"timeStamp":"2018-03-28 11:01:55.96","flagged":false,"blocked":false,"application":"HTTP","pro
                        tochain":"/TCP/HTTP","confidence":100,"state":1,"detail":"","tag":"uvm[0]: ","class":"class com.untangle.app.application_control.ApplicationControlLogE
                        vent","sessionEvent":{"entitled":true,"partitionTablePostfix":"_2018_03_28","CServerPort":80,"hostname":"192.168.1.22","protocol":6,"protocolName":"TCP"
                        ,"tag":"uvm[0]: ","localAddr":"/192.168.1.22","serverLatitude":39.0481,"class":"class com.untangle.uvm.app.SessionEvent","SServerAddr": ":"/50.145.12.125",
                        emoteAddı ":"/50.145.12.125" "serverIntf":3,"CClientAddr":"/192.168.1.22","serverCountry":"US","SClientAddr ":"/50.145.12.125""sessionId":99706680358837,
                        "CClientPort":62735,"policyRuleId":0,"clientCountry":"XL","timeStamp":"2018-03-28 11:01:55.888","serverLongitude":-77.4728,"clientIntf":4,"SClientPort":48
                        111,"policyId":1,"SServerPort":80,"bypassed":false,"CServerAddr ":"/50.145.12.125" 'tagsString":""},"partit
```

Figure 9

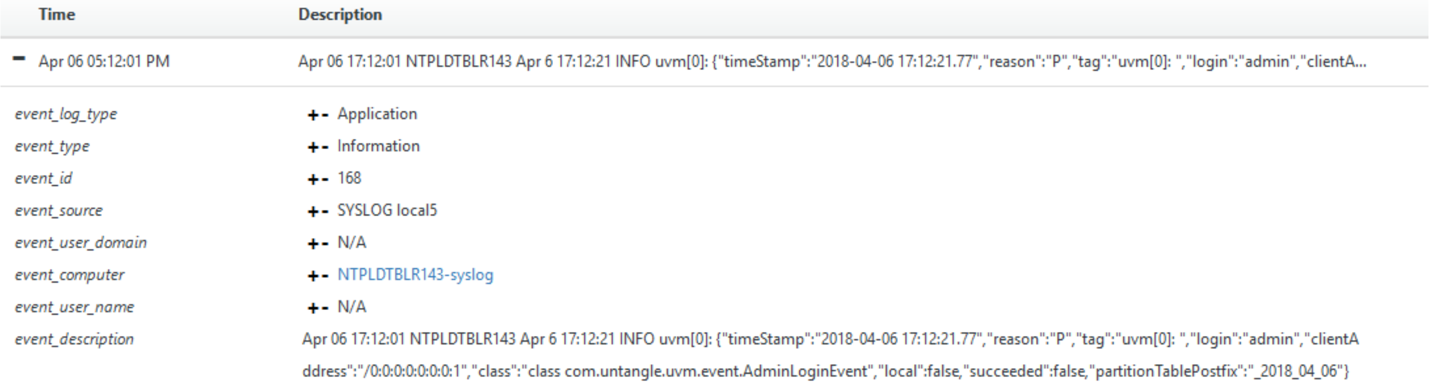
- **Untangle - Login failure -** This report gives information about user login failures.



LogTime	Computer	User Name	Client Address	Success	Reason
04/06/2018 05:11:48 PM	NTPLDTBLR143-SYSLOG	ubdjbcjs cm	192.168.1.125	false	U
04/06/2018 05:11:51 PM	NTPLDTBLR143-SYSLOG	admin	192.168.1.125	false	P
04/06/2018 05:11:52 PM	NTPLDTBLR143-SYSLOG	admin	192.168.1.125	false	P
04/06/2018 05:11:54 PM	NTPLDTBLR143-SYSLOG	admin	192.168.1.125	false	P
04/06/2018 05:11:55 PM	NTPLDTBLR143-SYSLOG	admin	192.168.1.125	false	P
04/06/2018 05:11:57 PM	NTPLDTBLR143-SYSLOG	admin	192.168.1.125	false	P
04/06/2018 05:11:58 PM	NTPLDTBLR143-SYSLOG	admin	192.168.1.125	false	P

Figure 10

Sample logs:

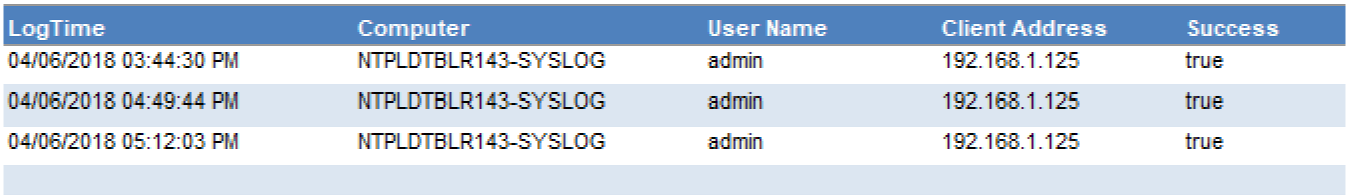


```
Time                    Description
−  Apr 06 05:12:01 PM   Apr 06 17:12:01 NTPLDTBLR143 Apr 6 17:12:21 INFO uvm[0]: {"timeStamp":"2018-04-06 17:12:21.77","reason":"P","tag":"uvm[0]: ","login":"admin","clientA...

event_log_type          +- Application
event_type              +- Information
event_id                +- 168
event_source            +- SYSLOG local5
event_user_domain       +- N/A
event_computer          +- NTPLDTBLR143-syslog
event_user_name         +- N/A
event_description       Apr 06 17:12:01 NTPLDTBLR143 Apr 6 17:12:21 INFO uvm[0]: {"timeStamp":"2018-04-06 17:12:21.77","reason":"P","tag":"uvm[0]: ","login":"admin","clientA
                        ddress":"/0:0:0:0:0:0:0:1","class":"class com.untangle.uvm.event.AdminLoginEvent","local":false,"succeeded":false,"partitionTablePostfix":"_2018_04_06"}
```

Figure 11

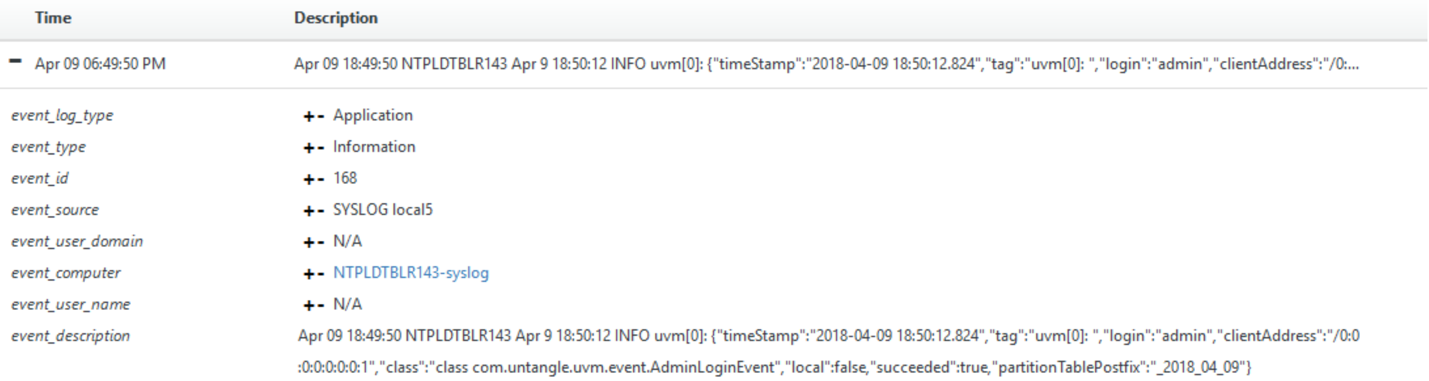
- **Untangle - Login success -** This report gives information about successful user logins.



LogTime	Computer	User Name	Client Address	Success
04/06/2018 03:44:30 PM	NTPLDTBLR143-SYSLOG	admin	192.168.1.125	true
04/06/2018 04:49:44 PM	NTPLDTBLR143-SYSLOG	admin	192.168.1.125	true
04/06/2018 05:12:03 PM	NTPLDTBLR143-SYSLOG	admin	192.168.1.125	true

Figure 12

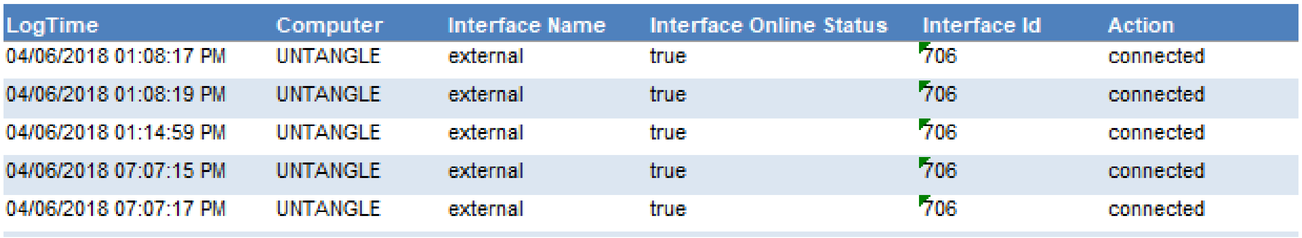
Sample logs:



Time	Description
− Apr 09 06:49:50 PM	Apr 09 18:49:50 NTPLDTBLR143 Apr 9 18:50:12 INFO uvm[0]: {"timeStamp":"2018-04-09 18:50:12.824","tag":"uvm[0]: ","login":"admin","clientAddress":"/0:...
event_log_type	+- Application
event_type	+- Information
event_id	+- 168
event_source	+- SYSLOG local5
event_user_domain	+- N/A
event_computer	+- NTPLDTBLR143-syslog
event_user_name	+- N/A
event_description	Apr 09 18:49:50 NTPLDTBLR143 Apr 9 18:50:12 INFO uvm[0]: {"timeStamp":"2018-04-09 18:50:12.824","tag":"uvm[0]: ","login":"admin","clientAddress":"/0:0:0:0:0:0:0:1","class":"class com.untangle.uvm.event.AdminLoginEvent","local":false,"succeeded":true,"partitionTablePostfix":"_2018_04_09"}

Figure 13

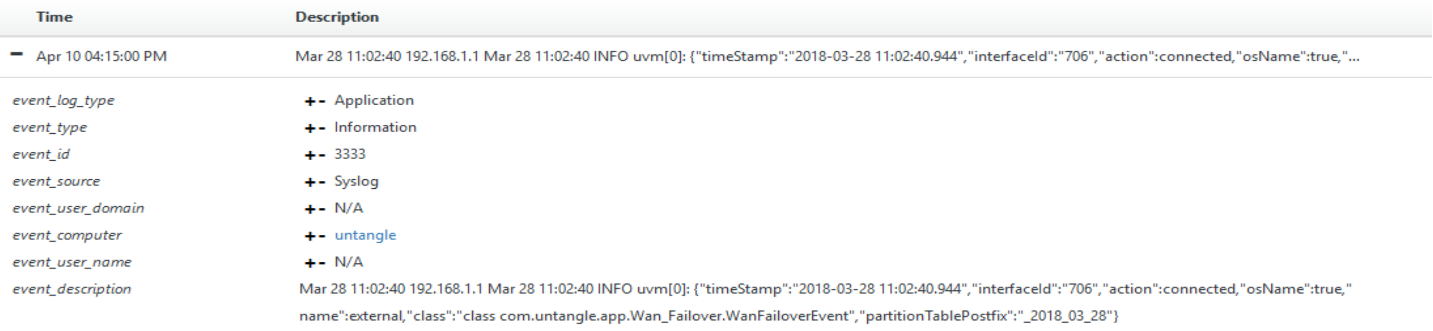
- **Untangle - WAN failover -** This report gives information about all the successful and failed WAN connections.



LogTime	Computer	Interface Name	Interface Online Status	Interface Id	Action
04/06/2018 01:08:17 PM	UNTANGLE	external	true	706	connected
04/06/2018 01:08:19 PM	UNTANGLE	external	true	706	connected
04/06/2018 01:14:59 PM	UNTANGLE	external	true	706	connected
04/06/2018 07:07:15 PM	UNTANGLE	external	true	706	connected
04/06/2018 07:07:17 PM	UNTANGLE	external	true	706	connected

Figure 14

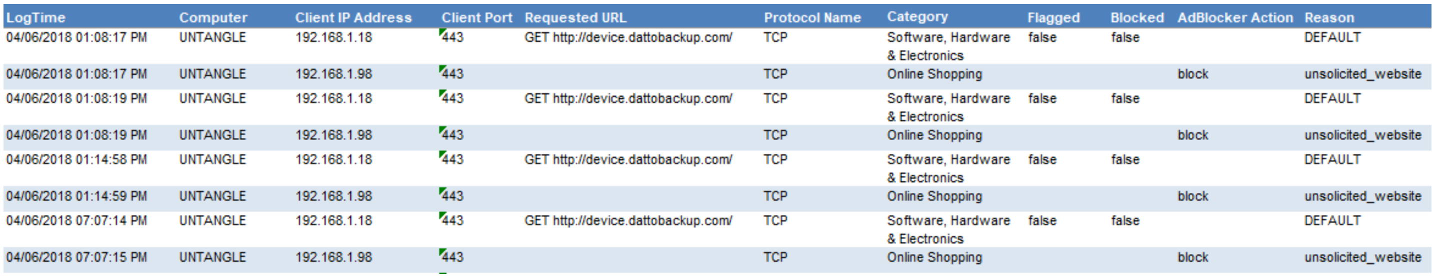
Sample logs:



Time	Description
− Apr 10 04:15:00 PM	Mar 28 11:02:40 192.168.1.1 Mar 28 11:02:40 INFO uvm[0]: {"timeStamp":"2018-03-28 11:02:40.944","interfaceId":"706","action":connected,"osName":true,"...
event_log_type	+- Application
event_type	+- Information
event_id	+- 3333
event_source	+- Syslog
event_user_domain	+- N/A
event_computer	+- untangle
event_user_name	+- N/A
event_description	Mar 28 11:02:40 192.168.1.1 Mar 28 11:02:40 INFO uvm[0]: {"timeStamp":"2018-03-28 11:02:40.944","interfaceId":"706","action":connected,"osName":true,"name":external,"class":"class com.untangle.app.Wan_Failover.WanFailoverEvent","partitionTablePostfix":"_2018_03_28"}

Figure 15

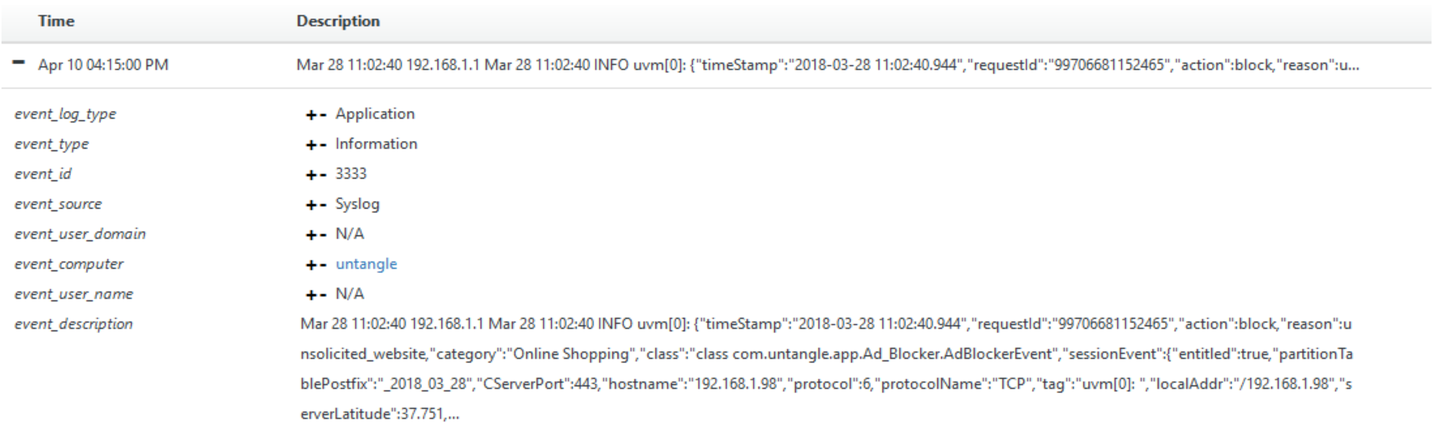
- **Untangle - Web filter -** This report gives information about all the URL filtering that is done.



LogTime	Computer	Client IP Address	Client Port	Requested URL	Protocol Name	Category	Flagged	Blocked	AdBlocker Action	Reason
04/06/2018 01:08:17 PM	UNTANGLE	192.168.1.18	443	GET http://device.dattobackup.com/	TCP	Software, Hardware & Electronics	false	false		DEFAULT
04/06/2018 01:08:17 PM	UNTANGLE	192.168.1.98	443		TCP	Online Shopping			block	unsolicited_website
04/06/2018 01:08:19 PM	UNTANGLE	192.168.1.18	443	GET http://device.dattobackup.com/	TCP	Software, Hardware & Electronics	false	false		DEFAULT
04/06/2018 01:08:19 PM	UNTANGLE	192.168.1.98	443		TCP	Online Shopping			block	unsolicited_website
04/06/2018 01:14:58 PM	UNTANGLE	192.168.1.18	443	GET http://device.dattobackup.com/	TCP	Software, Hardware & Electronics	false	false		DEFAULT
04/06/2018 01:14:59 PM	UNTANGLE	192.168.1.98	443		TCP	Online Shopping			block	unsolicited_website
04/06/2018 07:07:14 PM	UNTANGLE	192.168.1.18	443	GET http://device.dattobackup.com/	TCP	Software, Hardware & Electronics	false	false		DEFAULT
04/06/2018 07:07:15 PM	UNTANGLE	192.168.1.98	443		TCP	Online Shopping			block	unsolicited_website

Figure 16

Sample logs:



```
Time                      Description
− Apr 10 04:15:00 PM      Mar 28 11:02:40 192.168.1.1 Mar 28 11:02:40 INFO uvm[0]: {"timeStamp":"2018-03-28 11:02:40.944","requestId":"99706681152465","action":block,"reason":u...

event_log_type            +- Application
event_type                +- Information
event_id                  +- 3333
event_source              +- Syslog
event_user_domain         +- N/A
event_computer            +- untangle
event_user_name           +- N/A
event_description         Mar 28 11:02:40 192.168.1.1 Mar 28 11:02:40 INFO uvm[0]: {"timeStamp":"2018-03-28 11:02:40.944","requestId":"99706681152465","action":block,"reason":u
                          nsolicited_website,"category":"Online Shopping","class":"class com.untangle.app.Ad_Blocker.AdBlockerEvent","sessionEvent":{"entitled":true,"partitionTa
                          blePostfix":"_2018_03_28","CServerPort":443,"hostname":"192.168.1.98","protocol":6,"protocolName":"TCP","tag":"uvm[0]: ","localAddr":"/192.168.1.98","s
                          erverLatitude":37.751,...
```

Figure 17

Alerts

- **Untangle: Login failure -** This alert will be generated when the user login failure attempted.
- **Untangle: Spam emails -** This alert will be generated when a spam email is blocked.
- **Untangle: Threat detection -** This alert will be generated when a threat is detected by Untangle.

Categories

- **Untangle - Application control -** This category based report provides information related to applications which are blocked or allowed.
- **Untangle - Login failure -** This category based report provides information related to user login failures.
- **Untangle - Login success -** This category based report provides information related to successful user logins.
- **Untangle - Settings changes -** This category based report provides information related to device settings changes.
- **Untangle - Spam emails -** This category based report provides information related to all the spam emails which are blocked or allowed.

- **Untangle - Threat detection -** This category based report provides information related to all the threats that are detected by Untangle firewall.
- **Untangle - WAN failover -** This category based report provides information related to all the successful and failed WAN connections.
- **Untangle - Web filter -** This category based report provides information related to all the URL filtering that is done.
- **Untangle - System statistics -** This category based report provides information related to system statistics.

Knowledge Objects

- **Untangle - Application control -** This knowledge object helps to analyze logs related to applications which are blocked or allowed.
- **Untangle - Login failure -** This knowledge object helps to analyze logs related to user login failures.
- **Untangle - Login success -** This knowledge object helps to analyze logs related to successful user logins.
- **Untangle - Settings changes -** This knowledge object helps to analyze logs related to device settings changes.
- **Untangle - Spam emails -** This knowledge object helps to analyze logs related to all the spam emails which are blocked or allowed.
- **Untangle - Threat detection -** This knowledge object helps to analyze logs related to all the threats that are detected by Untangle firewall.
- **Untangle - WAN failover -** This knowledge object helps to analyze logs related to all the successful and failed WAN connections.
- **Untangle - Web filter -** This knowledge object helps to analyze logs related to all the URL filtering that is done.
- **Untangle - System statistics -** This knowledge object helps to analyze logs related to system statistics.

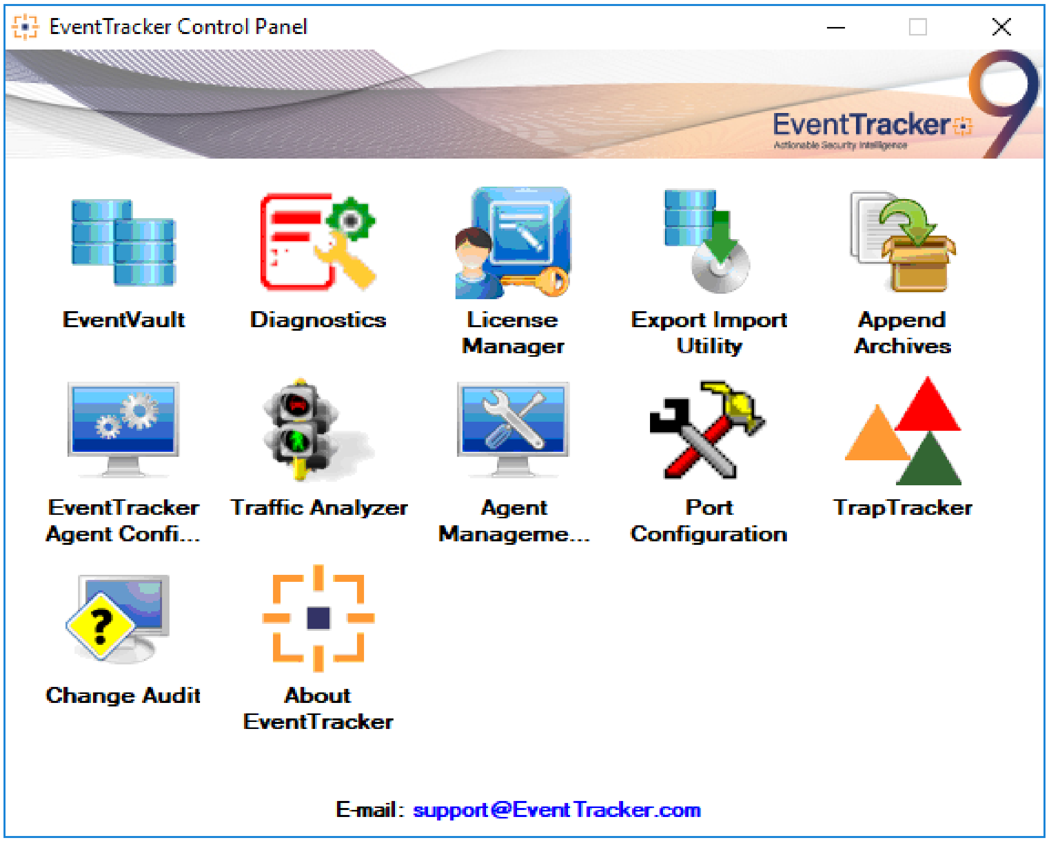
Import Untangle knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

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

1. Launch **EventTracker Control Panel**.

2. Double click **Export Import Utility**.



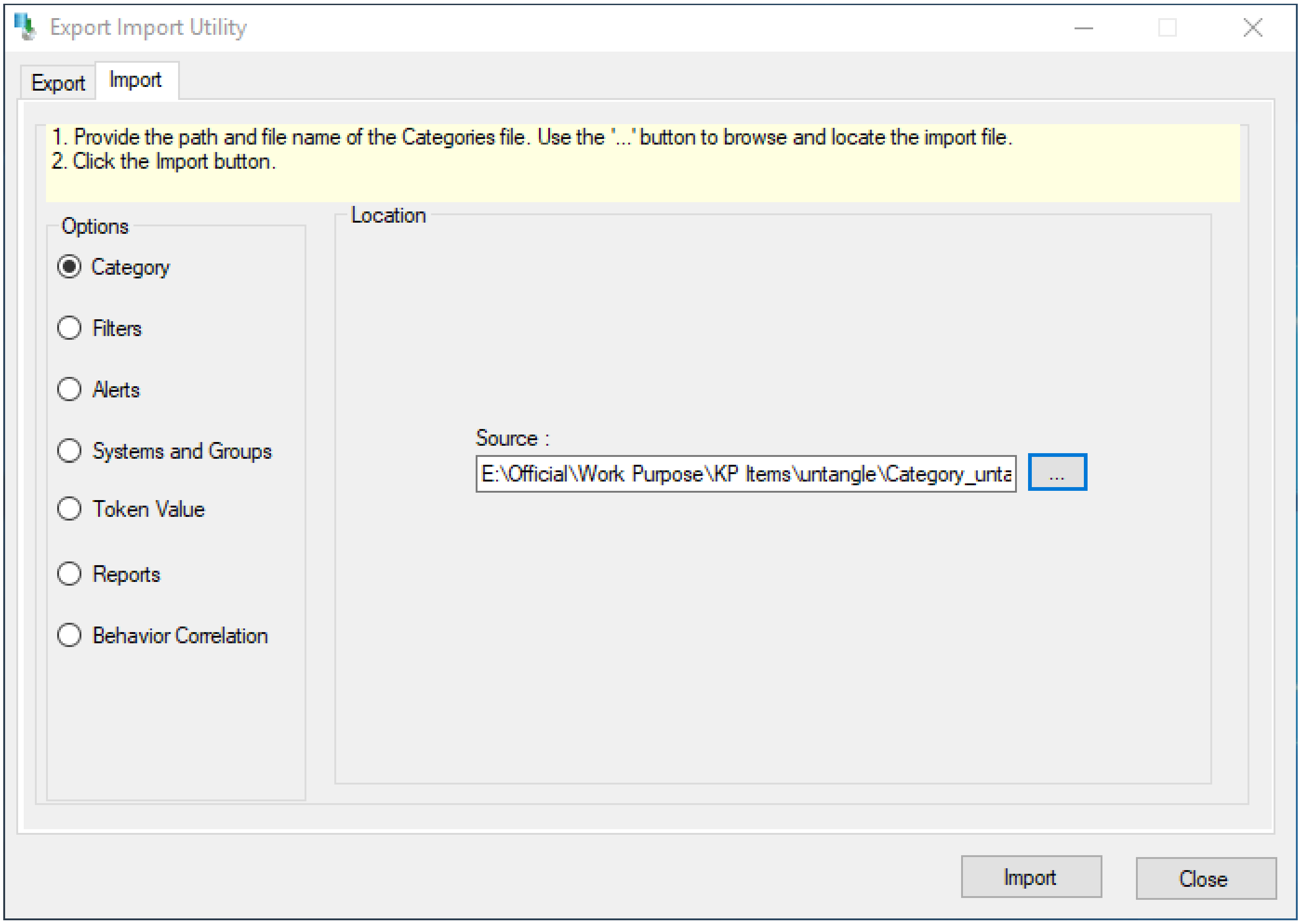
E-mail: support@EventTracker.com

Figure 18

3. Click the **Import** tab.

Category

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



1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

● Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

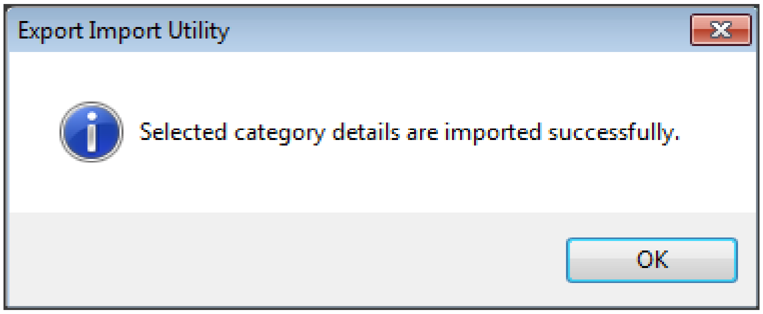
Source : E:\Official\Work Purpose\KP Items\untangle\Category_unta

Figure 19

2. Locate **Category_untangle.iscat** file, and then click the **Open** button.

3. To import categories, click the **Import** button.

   EventTracker displays success message.



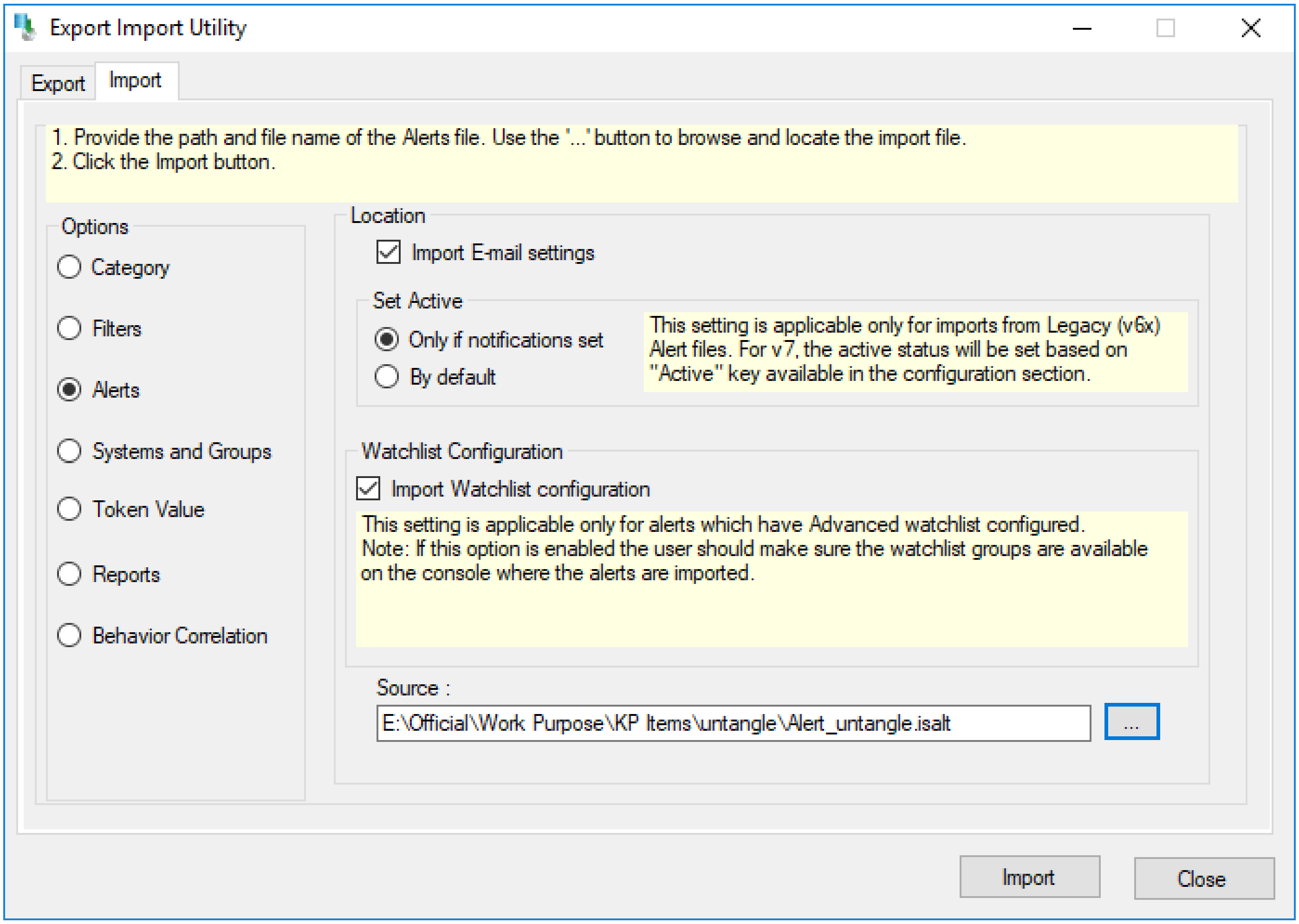
Selected category details are imported successfully.

Figure 20

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

Alerts

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



1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options
○ Category
○ Filters
● Alerts
○ Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

Location
☑ Import E-mail settings

Set Active
● Only if notifications set
○ By default

This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Watchlist Configuration
☑ Import Watchlist configuration

This setting is applicable only for alerts which have Advanced watchlist configured.
Note: If this option is enabled the user should make sure the watchlist groups are available on the console where the alerts are imported.

Source : E:\Official\Work Purpose\KP Items\untangle\Alert_untangle.isalt

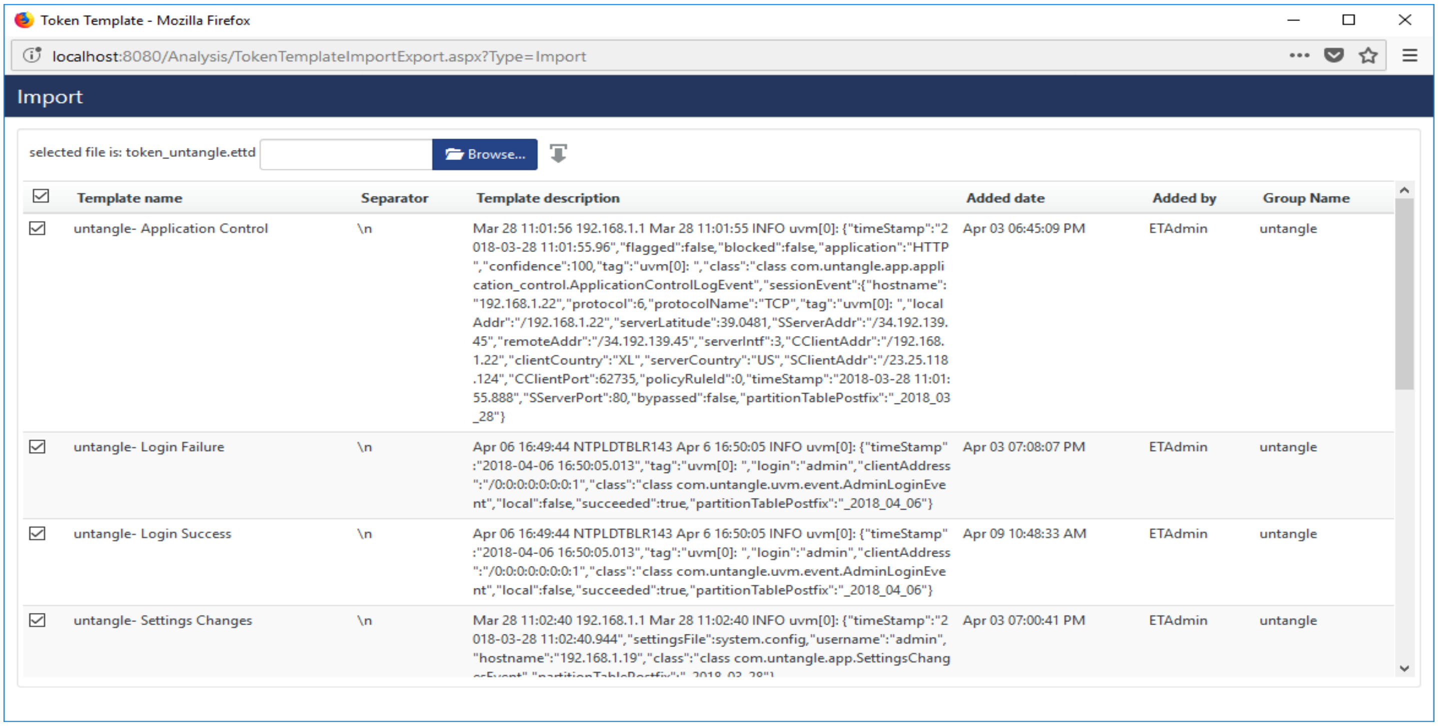
Figure 21

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

Token Templates

1. Click **Parsing rules** under **Admin** option in the EventTracker manager page.
2. Move to **Template** and click on import configuration icon on the top right corner.
3. In the popup window browse the file named **Token Template_ Untangle.ettd**.

4. Now select all the check box and then click on ⤓ Import option.


Token Template - Mozilla Firefox
localhost:8080/Analysis/TokenTemplateImportExport.aspx?Type=Import
Import
Browse...

selected file is: token_untangle.ettd

☑	Template name	Separator	Template description	Added date	Added by	Group Name
☑	untangle- Application Control	\n	Mar 28 11:01:56 192.168.1.1 Mar 28 11:01:55 INFO uvm[0]: {"timeStamp":"2018-03-28 11:01:55.96","flagged":false,"blocked":false,"application":"HTTP","confidence":100,"tag":"uvm[0]: ","class":"class com.untangle.app.application_control.ApplicationControlLogEvent","sessionEvent":{"hostname":"192.168.1.22","protocol":6,"protocolName":"TCP","tag":"uvm[0]: ","localAddr":"/192.168.1.22","serverLatitude":39.0481,"SServerAddr":"/34.192.139.45","remoteAddr":"/34.192.139.45","serverIntf":3,"CClientAddr":"/192.168.1.22","clientCountry":"XL","serverCountry":"US","SClientAddr":"/23.25.118.124","CClientPort":62735,"policyRuleId":0,"timeStamp":"2018-03-28 11:01:55.888","SServerPort":80,"bypassed":false,"partitionTablePostfix":"_2018_03_28"}	Apr 03 06:45:09 PM	ETAdmin	untangle
☑	untangle- Login Failure	\n	Apr 06 16:49:44 NTPLDTBLR143 Apr 6 16:50:05 INFO uvm[0]: {"timeStamp":"2018-04-06 16:50:05.013","tag":"uvm[0]: ","login":"admin","clientAddress":"/0:0:0:0:0:0:0:1","class":"class com.untangle.uvm.event.AdminLoginEvent","local":false,"succeeded":true,"partitionTablePostfix":"_2018_04_06"}	Apr 03 07:08:07 PM	ETAdmin	untangle
☑	untangle- Login Success	\n	Apr 06 16:49:44 NTPLDTBLR143 Apr 6 16:50:05 INFO uvm[0]: {"timeStamp":"2018-04-06 16:50:05.013","tag":"uvm[0]: ","login":"admin","clientAddress":"/0:0:0:0:0:0:0:1","class":"class com.untangle.uvm.event.AdminLoginEvent","local":false,"succeeded":true,"partitionTablePostfix":"_2018_04_06"}	Apr 09 10:48:33 AM	ETAdmin	untangle
☑	untangle- Settings Changes	\n	Mar 28 11:02:40 192.168.1.1 Mar 28 11:02:40 INFO uvm[0]: {"timeStamp":"2018-03-28 11:02:40.944","settingsFile":system.config,"username":"admin","hostname":"192.168.1.19","class":"class com.untangle.app.SettingsChangesEvent","partitionTablePostfix":"_2018_03_28"}	Apr 03 07:00:41 PM	ETAdmin	untangle

Figure 22

Knowledge Objects

1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.
2. Locate the **KO_Untangle.etko** file.

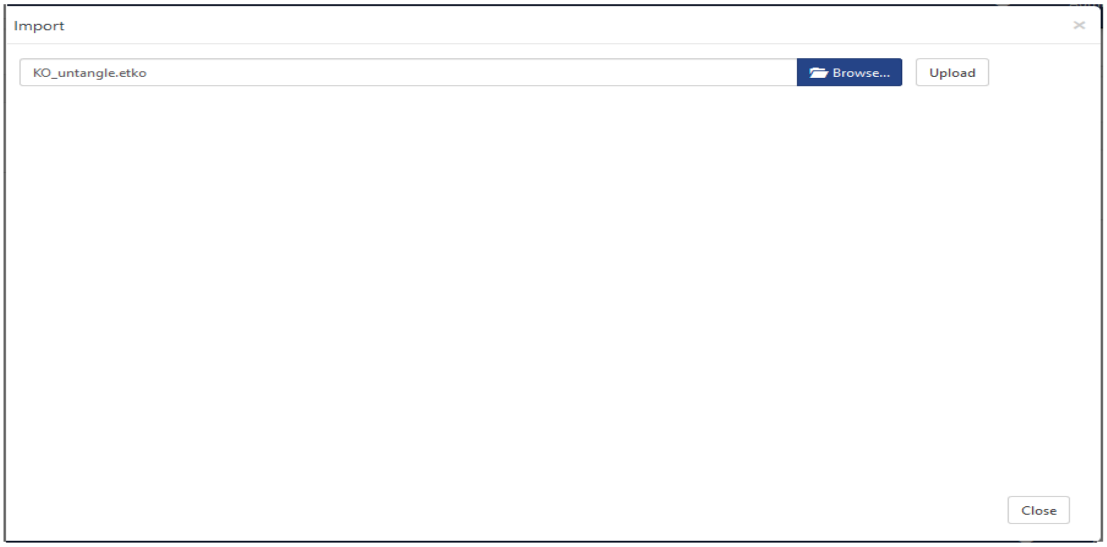
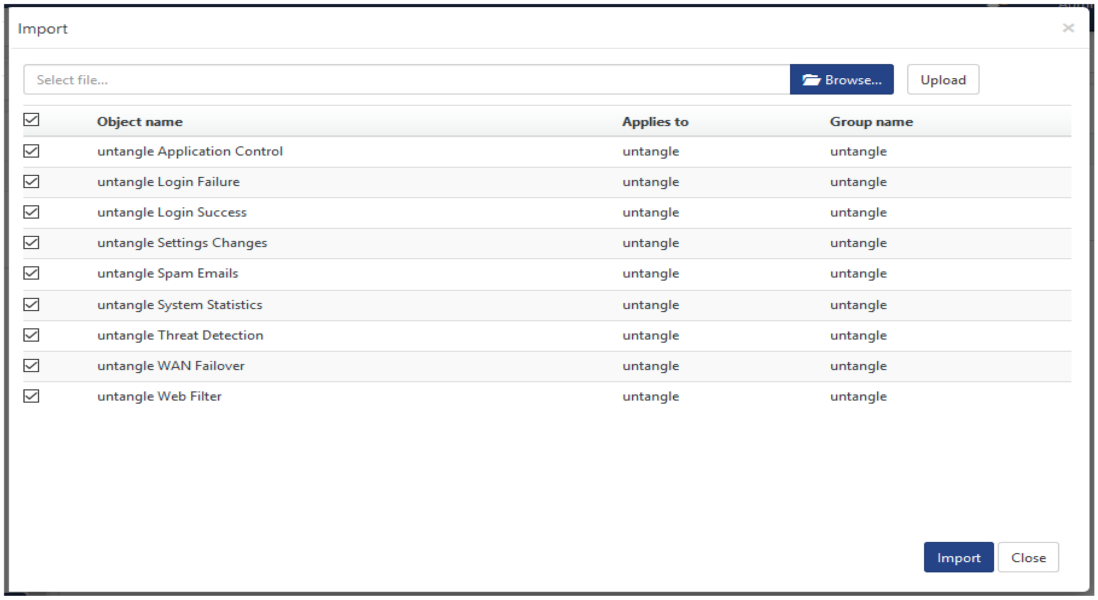


Figure 23

3. Click the '**Upload'** option.
4. Now select all the check box and then click on '**Import**' option.



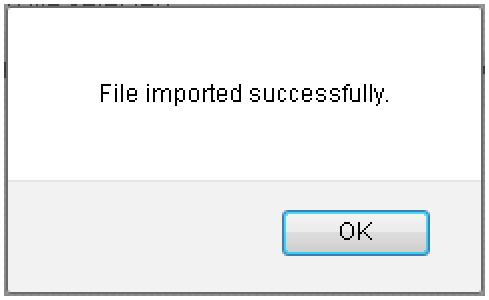
Import

Select file... | Browse... | Upload

☑	Object name	Applies to	Group name
☑	untangle Application Control	untangle	untangle
☑	untangle Login Failure	untangle	untangle
☑	untangle Login Success	untangle	untangle
☑	untangle Settings Changes	untangle	untangle
☑	untangle Spam Emails	untangle	untangle
☑	untangle System Statistics	untangle	untangle
☑	untangle Threat Detection	untangle	untangle
☑	untangle WAN Failover	untangle	untangle
☑	untangle Web Filter	untangle	untangle

Figure 24

5. Knowledge objects are now imported successfully.



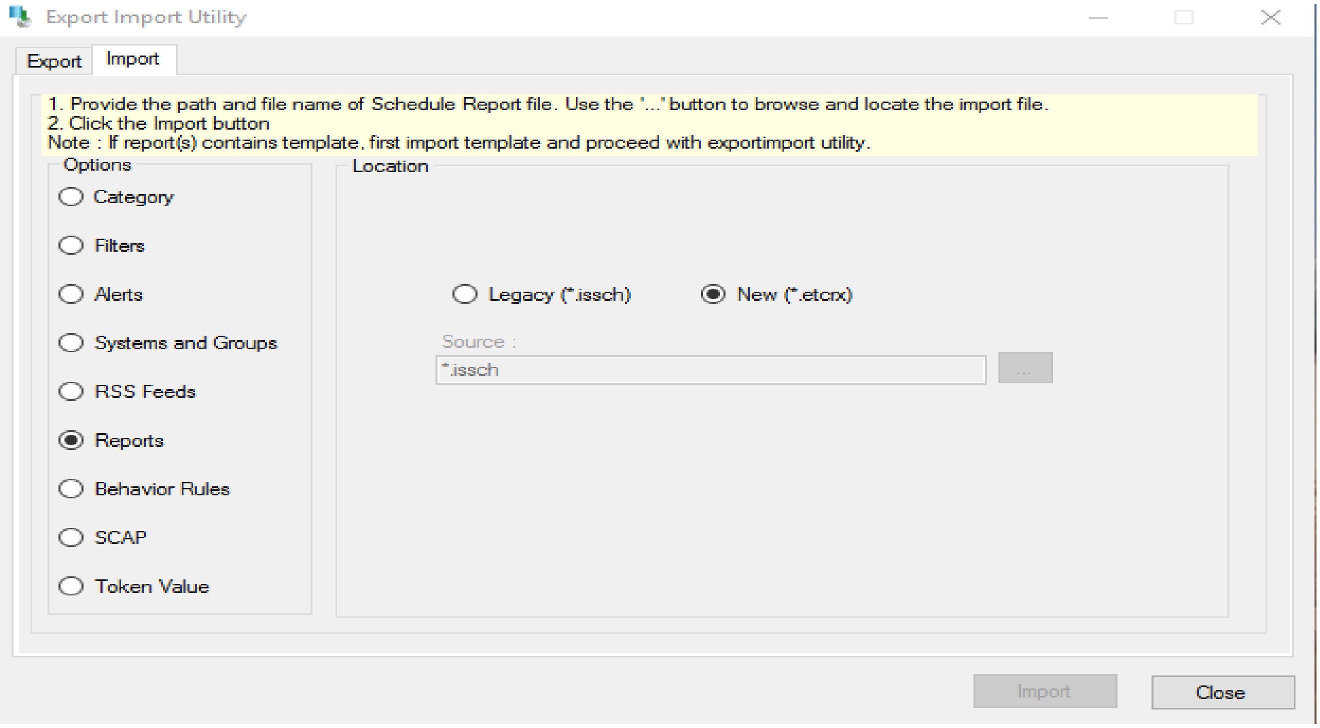
File imported successfully.

Figure 25

Flex Reports

On EventTracker Control Panel,

1. Click **Reports** option, and select **new (*.etcrx)** from the option.



1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Options

○ Category
○ Filters
○ Alerts
○ Systems and Groups
○ RSS Feeds
● Reports
○ Behavior Rules
○ SCAP
○ Token Value

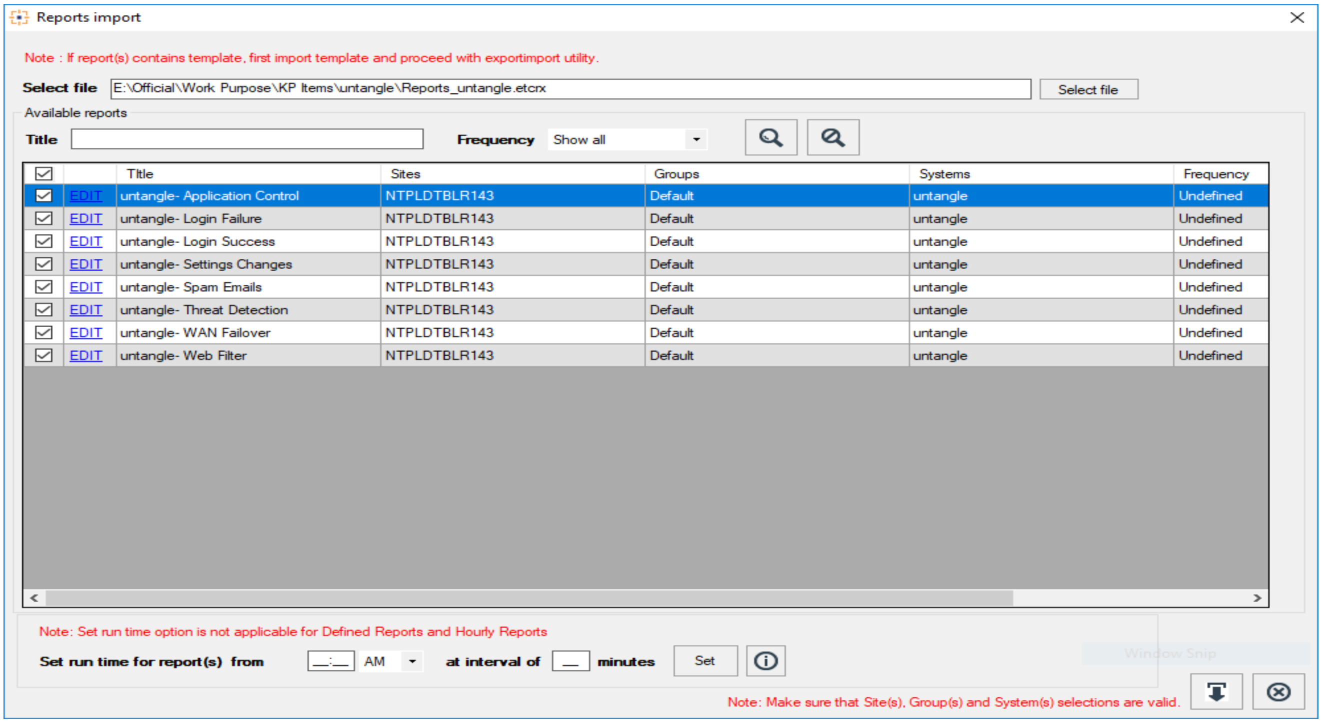
Location

○ Legacy (*.issch) ● New (*.etcrx)

Source : *.issch

Figure 26

2. Locate the **Reports_Untangle.etcrx** file, and select all the check box.



Note : If report(s) contains template, first import template and proceed with exportimport utility.

Select file E:\Official\Work Purpose\KP Items\untangle\Reports_untangle.etcrx

Available reports

Title

Frequency Show all

☑		Title	Sites	Groups	Systems	Frequency
☑	EDIT	untangle- Application Control	NTPLDTBLR143	Default	untangle	Undefined
☑	EDIT	untangle- Login Failure	NTPLDTBLR143	Default	untangle	Undefined
☑	EDIT	untangle- Login Success	NTPLDTBLR143	Default	untangle	Undefined
☑	EDIT	untangle- Settings Changes	NTPLDTBLR143	Default	untangle	Undefined
☑	EDIT	untangle- Spam Emails	NTPLDTBLR143	Default	untangle	Undefined
☑	EDIT	untangle- Threat Detection	NTPLDTBLR143	Default	untangle	Undefined
☑	EDIT	untangle- WAN Failover	NTPLDTBLR143	Default	untangle	Undefined
☑	EDIT	untangle- Web Filter	NTPLDTBLR143	Default	untangle	Undefined

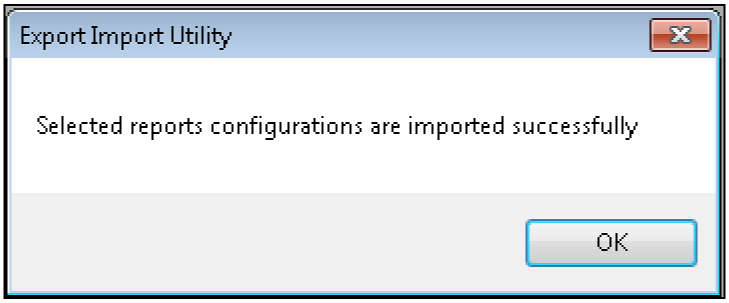
Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Set run time for report(s) from __:__ AM **at interval of** __ **minutes**

Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

Figure 27

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



Export Import Utility

Selected reports configurations are imported successfully

Figure 28

Dashboards

Note: If you have EventTracker Enterprise version **v9.0**, you can import dashboards.

1. Open **EventTracker Enterprise**.

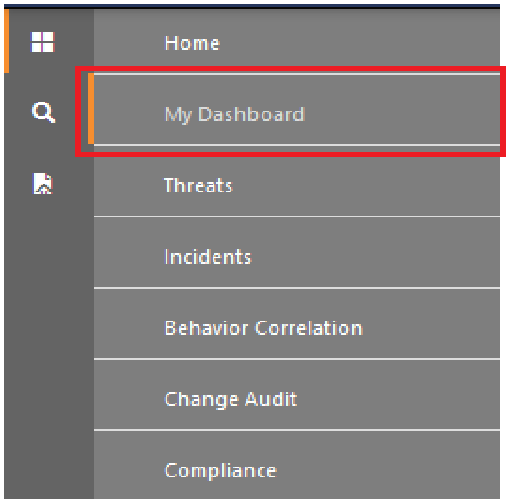
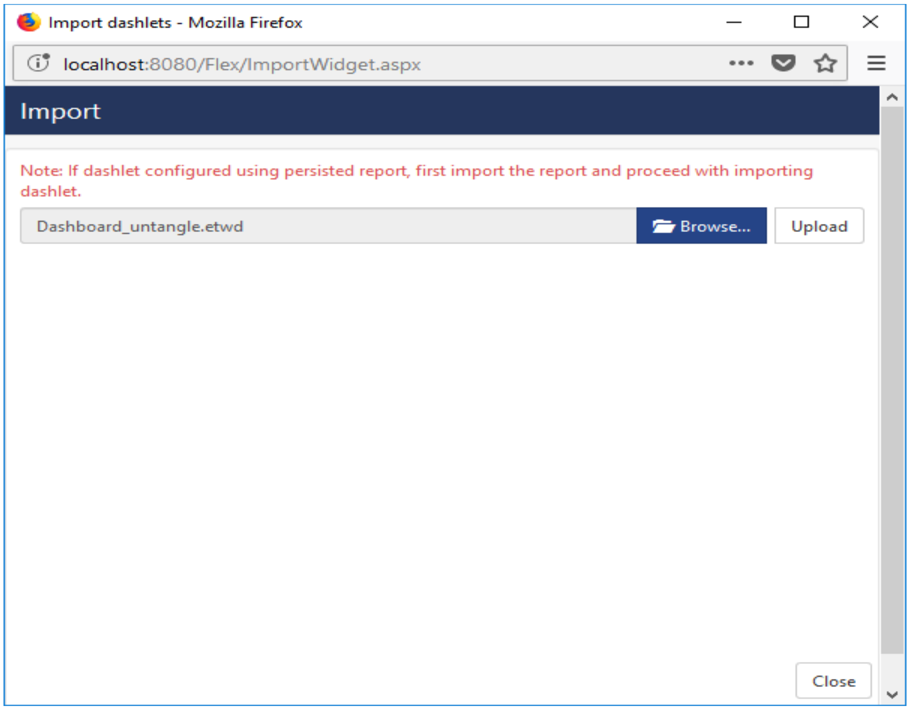


Figure 29

2. Navigate to **Dashboard>My Dashboard**.
   My Dashboard pane is shown.

3. Click the **'Import'** ⤓ button to import the dashlets.

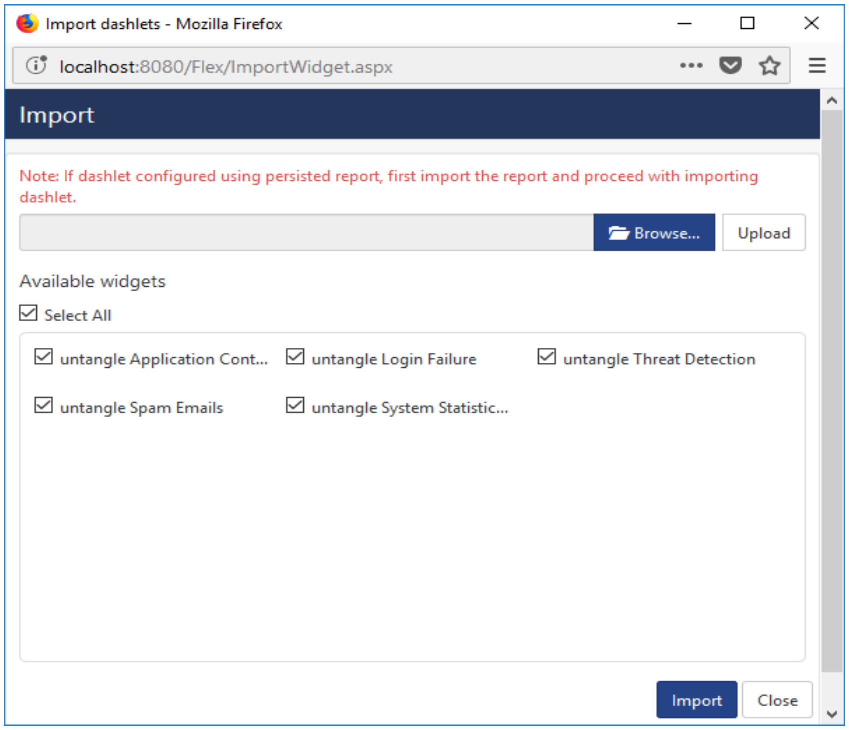

Import dashlets - Mozilla Firefox
localhost:8080/Flex/ImportWidget.aspx
Import

Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.

Dashboard_untangle.etwd

Figure 30

4. Locate the Dashboard_Untangle**.etwd** file.
5. Click the '**Upload'** option.


Import dashlets - Mozilla Firefox
localhost:8080/Flex/ImportWidget.aspx
Import

Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.

Available widgets

☑ Select All

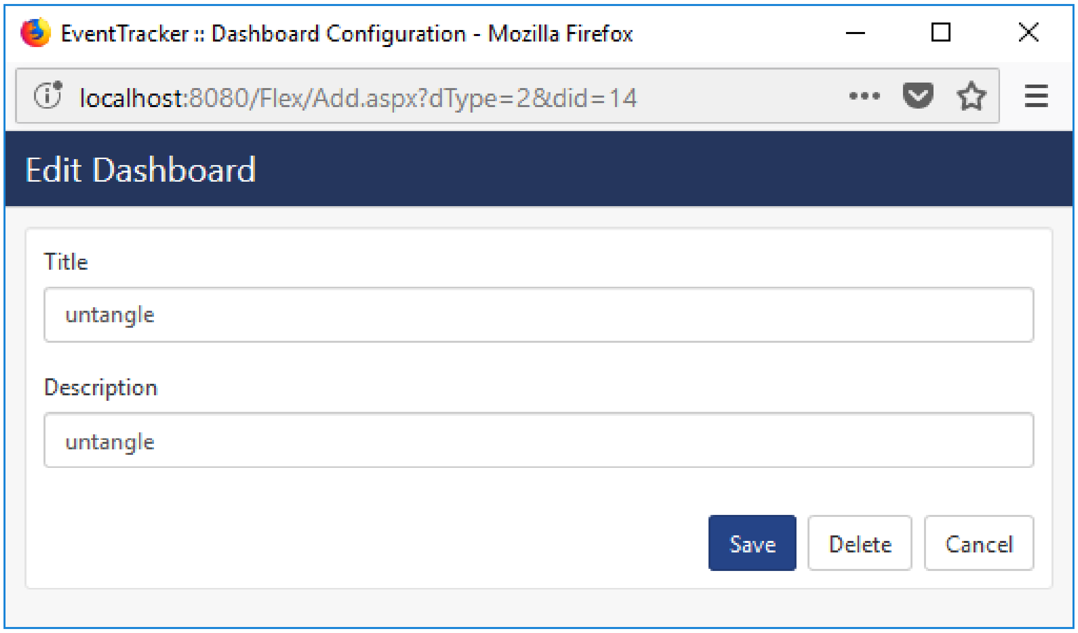
☑ untangle Application Cont... ☑ untangle Login Failure ☑ untangle Threat Detection

☑ untangle Spam Emails ☑ untangle System Statistic...

Figure 31

6. Now select all the check box and then click on ‘**Import**’ option.
   Dashlets are now imported successfully.

7. Click the ‘**Add’** ⊕ button to create a new dashlets.


EventTracker :: Dashboard Configuration - Mozilla Firefox

localhost:8080/Flex/Add.aspx?dType=2&did=14

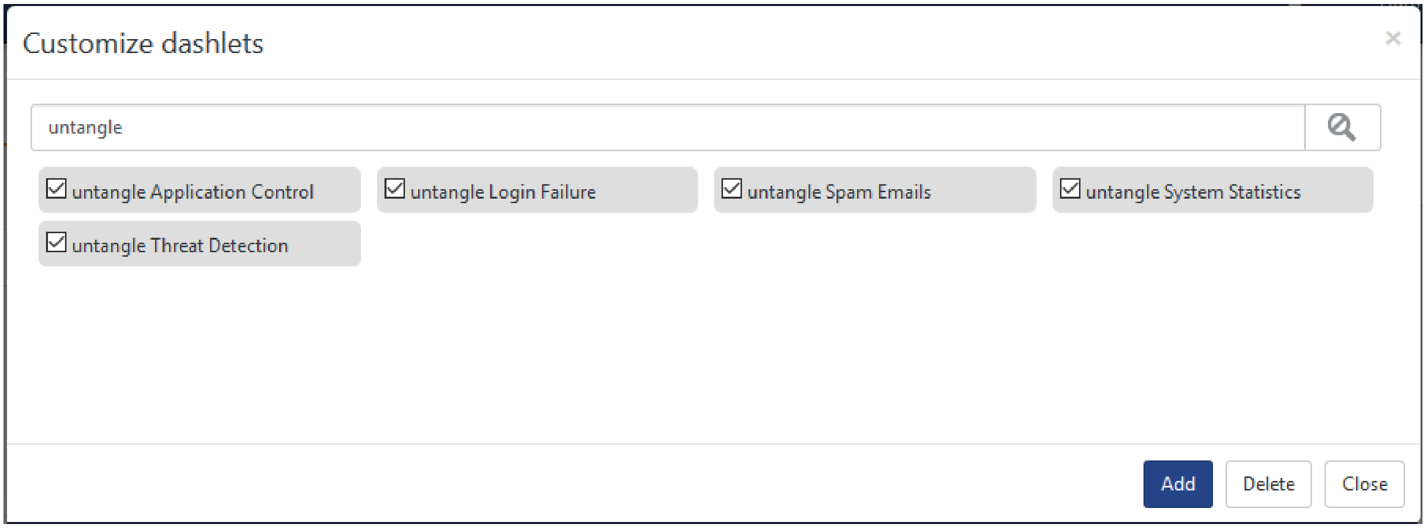
Edit Dashboard

Title: untangle

Description: untangle

Figure 32

8. Fill suitable Title and Description and click **Save** button.


Customize dashlets

untangle

☑ untangle Application Control
☑ untangle Login Failure
☑ untangle Spam Emails
☑ untangle System Statistics
☑ untangle Threat Detection

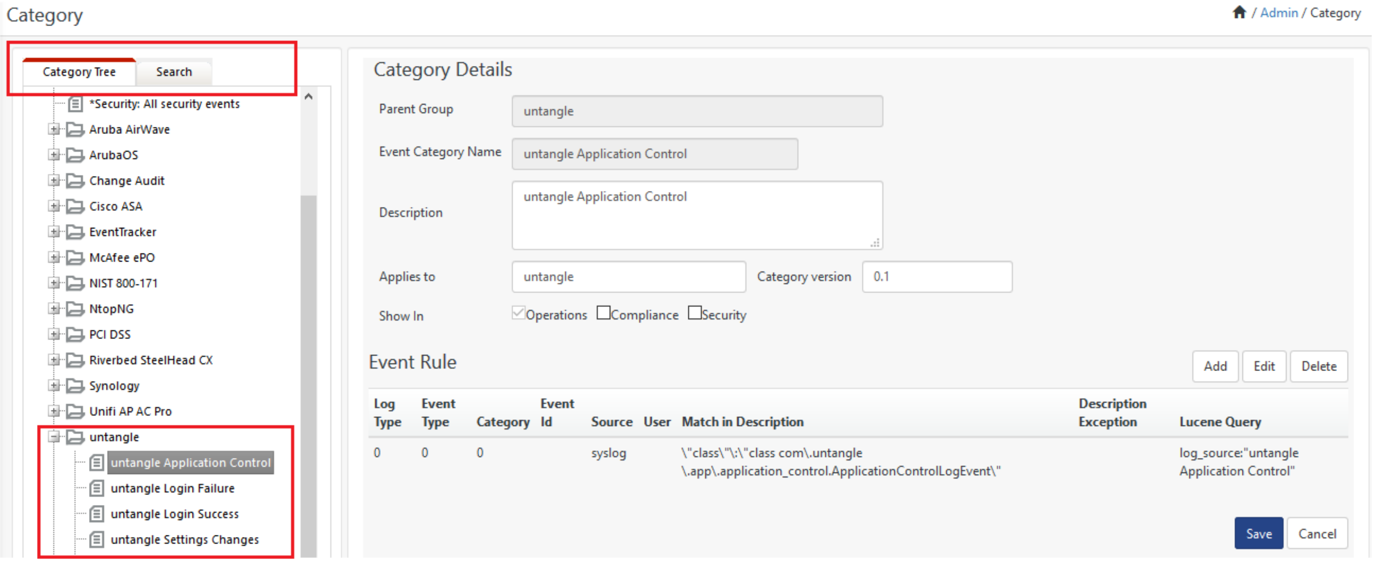
Figure 33

9. Click **‘Customize’** to locate and choose all created dashlets.
10. Click ‘**Add’** dashlet to create dashboard.

Verify Untangle knowledge pack in EventTracker

Categories

1. Logon to **EventTracker Enterprise**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **Untangle** group folder to view the imported categories.



Category Details

Parent Group: untangle

Event Category Name: untangle Application Control

Description: untangle Application Control

Applies to: untangle

Category version: 0.1

Show In: ☑Operations □Compliance □Security

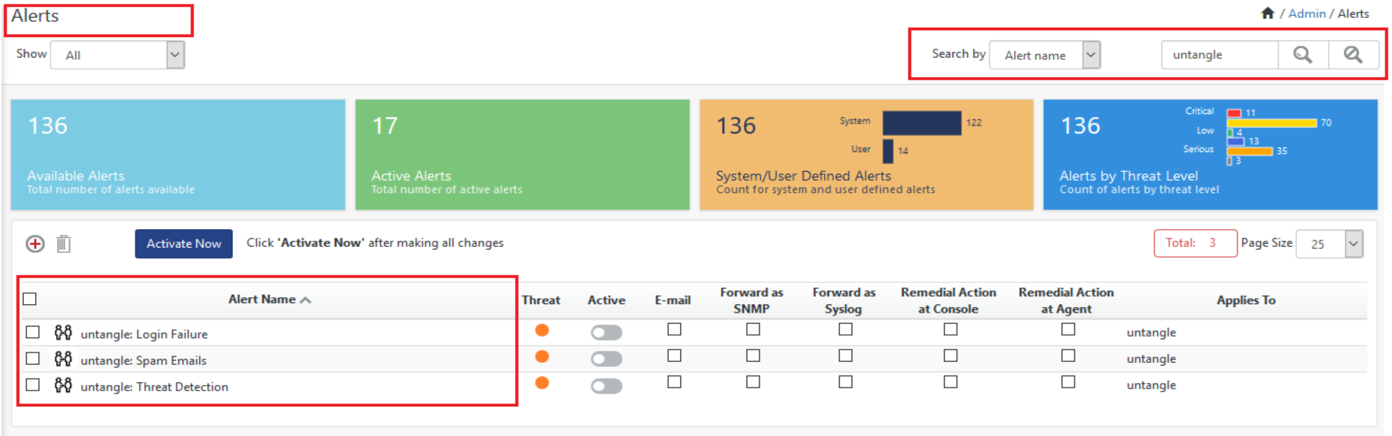
Event Rule

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception	Lucene Query
0	0	0		syslog		\"class\"\:\"class com\.untangle \.app\.application_control.ApplicationControlLogEvent\"		log_source:"untangle Application Control"

Figure 34

Alerts

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Alerts.**
2. In search box, enter **Untangle** and then click the **Search** button.
   EventTracker displays alert of **Untangle.**

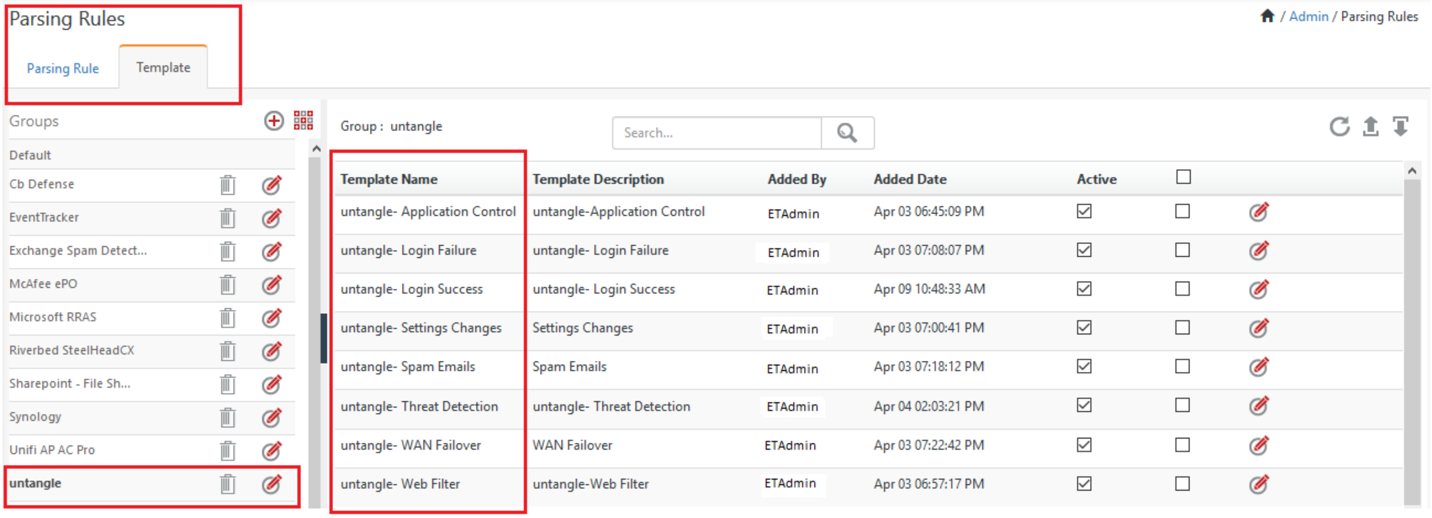

Alerts
🏠 / Admin / Alerts
Show All
Search by Alert name
untangle
136
Available Alerts
Total number of alerts available
17
Active Alerts
Total number of active alerts
136
System 122
User 14
System/User Defined Alerts
Count for system and user defined alerts
136
Critical 11
70
Low 4
13
Serious 35
3
Alerts by Threat Level
Count of alerts by threat level
Activate Now
Click 'Activate Now' after making all changes
Total: 3
Page Size 25

□	Alert Name	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□	untangle: Login Failure	●		□	□	□	□	□	untangle
□	untangle: Spam Emails	●		□	□	□	□	□	untangle
□	untangle: Threat Detection	●		□	□	□	□	□	untangle

Figure 35

Token Templates

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Parsing rules.**
2. On **Template** tab, click on the **Untangle** group folder to view the imported Token Values.



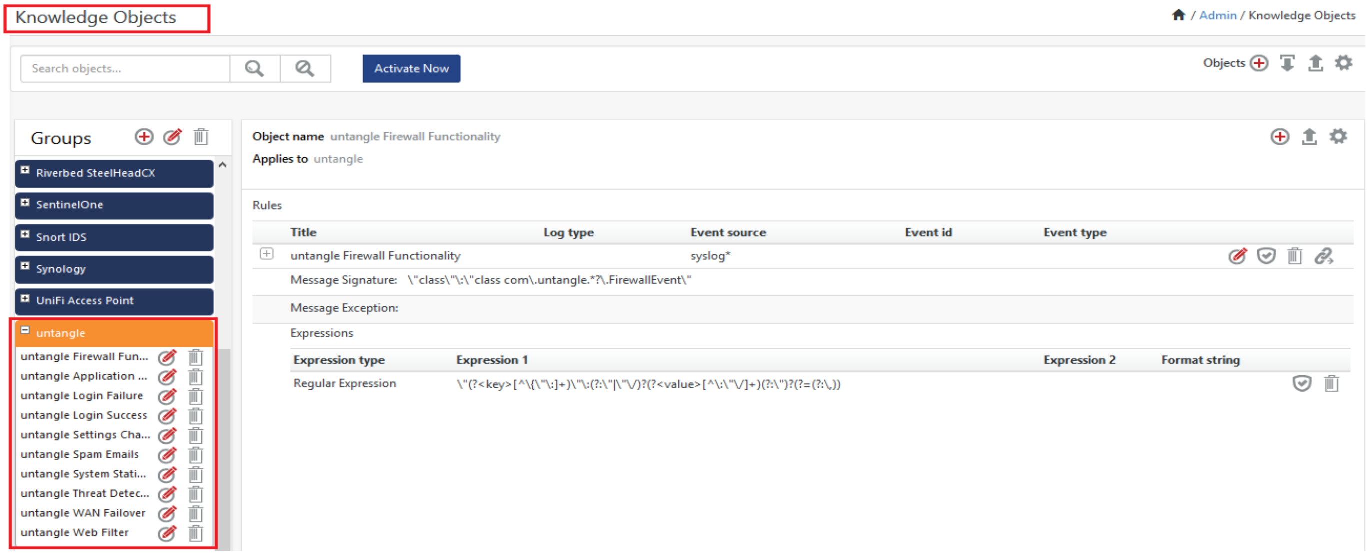
Template Name	Template Description	Added By	Added Date	Active	□
untangle- Application Control	untangle-Application Control	ETAdmin	Apr 03 06:45:09 PM	☑	□
untangle- Login Failure	untangle- Login Failure	ETAdmin	Apr 03 07:08:07 PM	☑	□
untangle- Login Success	untangle- Login Success	ETAdmin	Apr 09 10:48:33 AM	☑	□
untangle- Settings Changes	Settings Changes	ETAdmin	Apr 03 07:00:41 PM	☑	□
untangle- Spam Emails	Spam Emails	ETAdmin	Apr 03 07:18:12 PM	☑	□
untangle- Threat Detection	untangle- Threat Detection	ETAdmin	Apr 04 02:03:21 PM	☑	□
untangle- WAN Failover	WAN Failover	ETAdmin	Apr 03 07:22:42 PM	☑	□
untangle- Web Filter	untangle-Web Filter	ETAdmin	Apr 03 06:57:17 PM	☑	□

Figure 36

Knowledge Objects

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

2. In the **Knowledge Object** tree, expand **Untangle** group folder to view the imported Knowledge objects.



Object name untangle Firewall Functionality

Applies to untangle

Rules

Title	Log type	Event source	Event id	Event type
untangle Firewall Functionality		syslog*		

Message Signature: \"class\"\:\"class com\.untangle.*?\.FirewallEvent\"

Message Exception:

Expressions

Expression type	Expression 1	Expression 2	Format string
Regular Expression	\"(?<key>[^\{\"\:]+)\"\:(?:\"|\"\/)?(?<value>[^\:\"\/]+)(?:\")?(?=(?:\,))		

Figure 37

Flex Reports

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

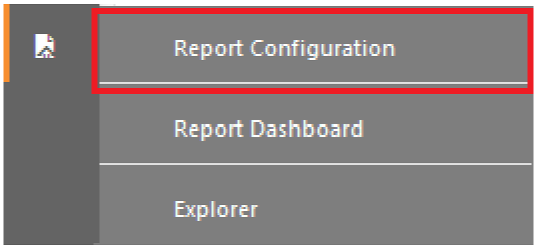
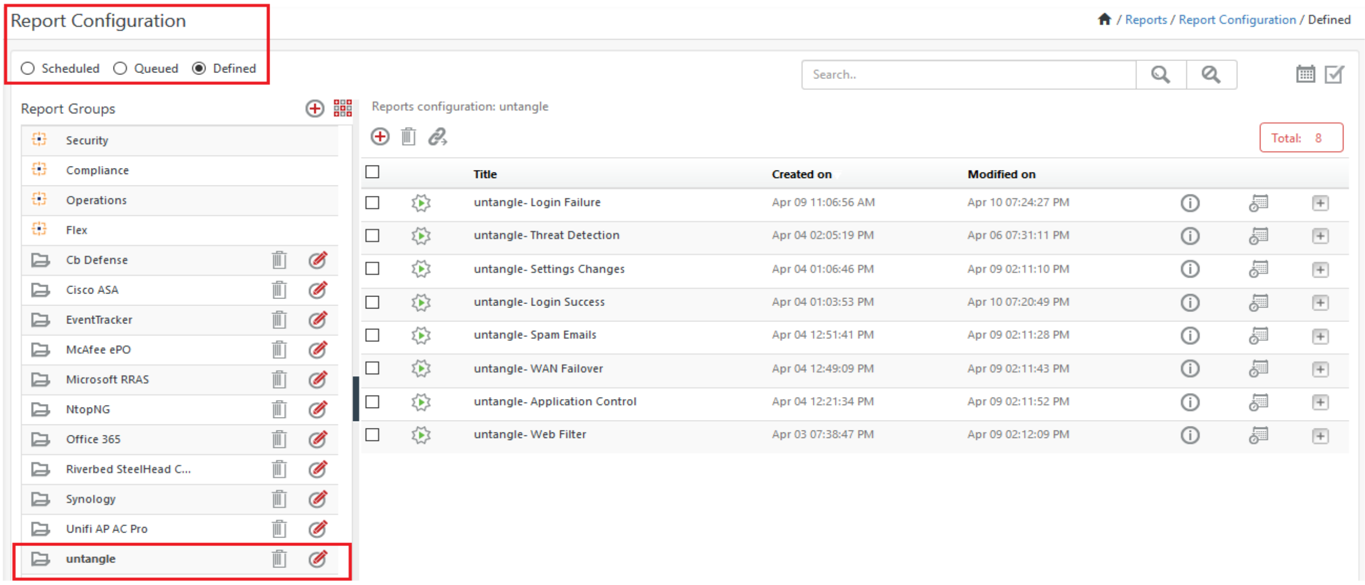


Figure 38

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



Report Configuration

○ Scheduled ○ Queued ● Defined

/ Reports / Report Configuration / Defined

Report Groups

- Security
- Compliance
- Operations
- Flex
- Cb Defense
- Cisco ASA
- EventTracker
- McAfee ePO
- Microsoft RRAS
- NtopNG
- Office 365
- Riverbed SteelHead C...
- Synology
- Unifi AP AC Pro
- untangle

Reports configuration: untangle

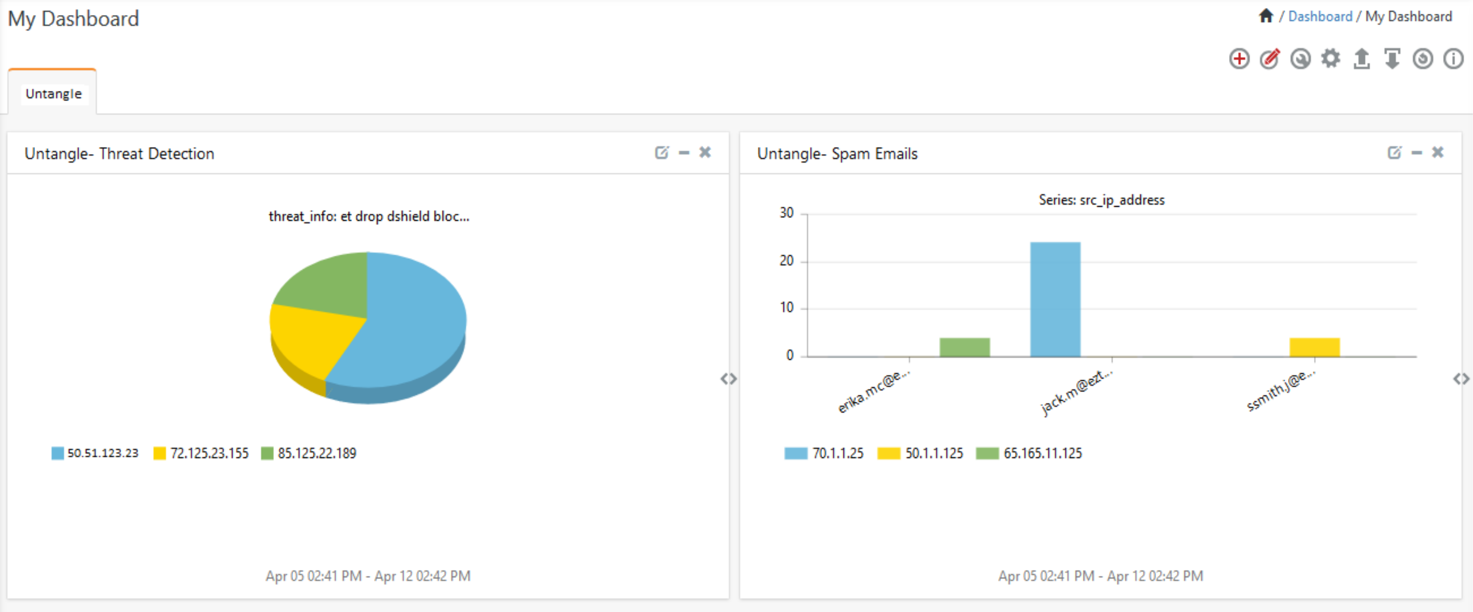
Total: 8

	Title	Created on	Modified on
□	untangle- Login Failure	Apr 09 11:06:56 AM	Apr 10 07:24:27 PM
□	untangle- Threat Detection	Apr 04 02:05:19 PM	Apr 06 07:31:11 PM
□	untangle- Settings Changes	Apr 04 01:06:46 PM	Apr 09 02:11:10 PM
□	untangle- Login Success	Apr 04 01:03:53 PM	Apr 10 07:20:49 PM
□	untangle- Spam Emails	Apr 04 12:51:41 PM	Apr 09 02:11:28 PM
□	untangle- WAN Failover	Apr 04 12:49:09 PM	Apr 09 02:11:43 PM
□	untangle- Application Control	Apr 04 12:21:34 PM	Apr 09 02:11:52 PM
□	untangle- Web Filter	Apr 03 07:38:47 PM	Apr 09 02:12:09 PM

Figure 39

Dashboards

1. Open **EventTracker Enterprise** in browser and logon.
2. Navigate to **Dashboard>My Dashboard**.
   My Dashboard pane is shown.



My Dashboard

/ Dashboard / My Dashboard

Untangle

Untangle- Threat Detection

threat_info: et drop dshield bloc...
50.51.123.23
72.125.23.155
85.125.22.189
Apr 05 02:41 PM - Apr 12 02:42 PM

Untangle- Spam Emails

Figure 40

Create Dashlets

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

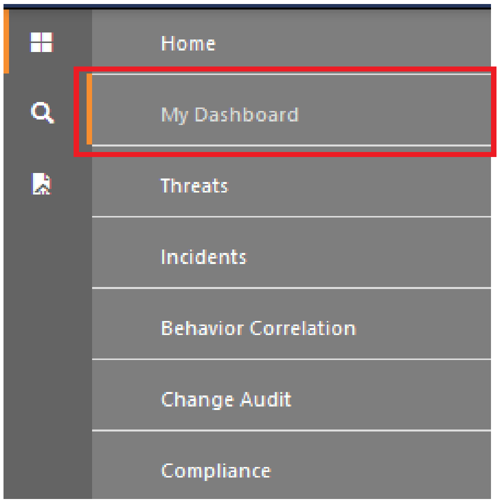
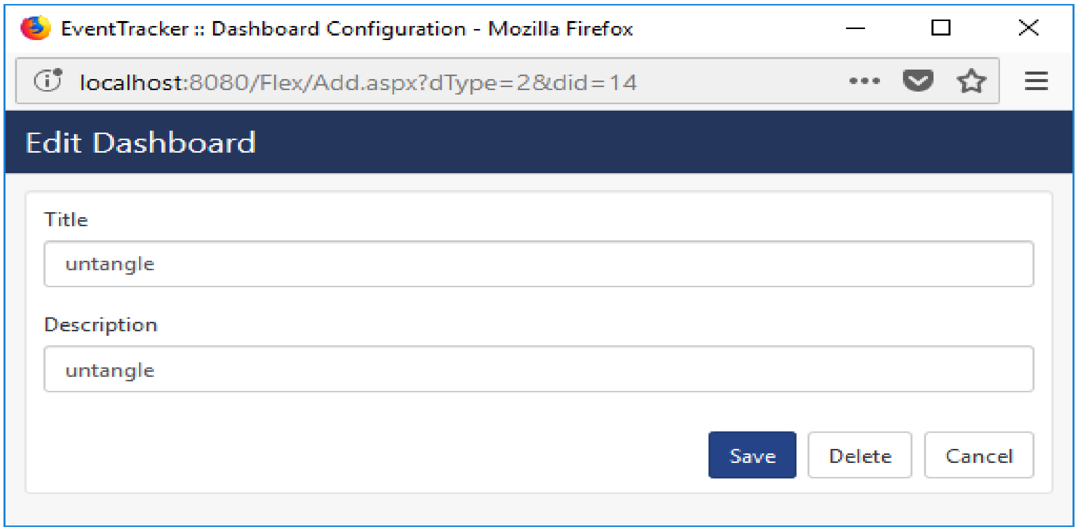


Figure 41

2. Navigate to **Dashboard>My Dashboard**.
   My Dashboard pane is shown.

3. Click the '**Add**' ⊕ button to create a new dashlet.

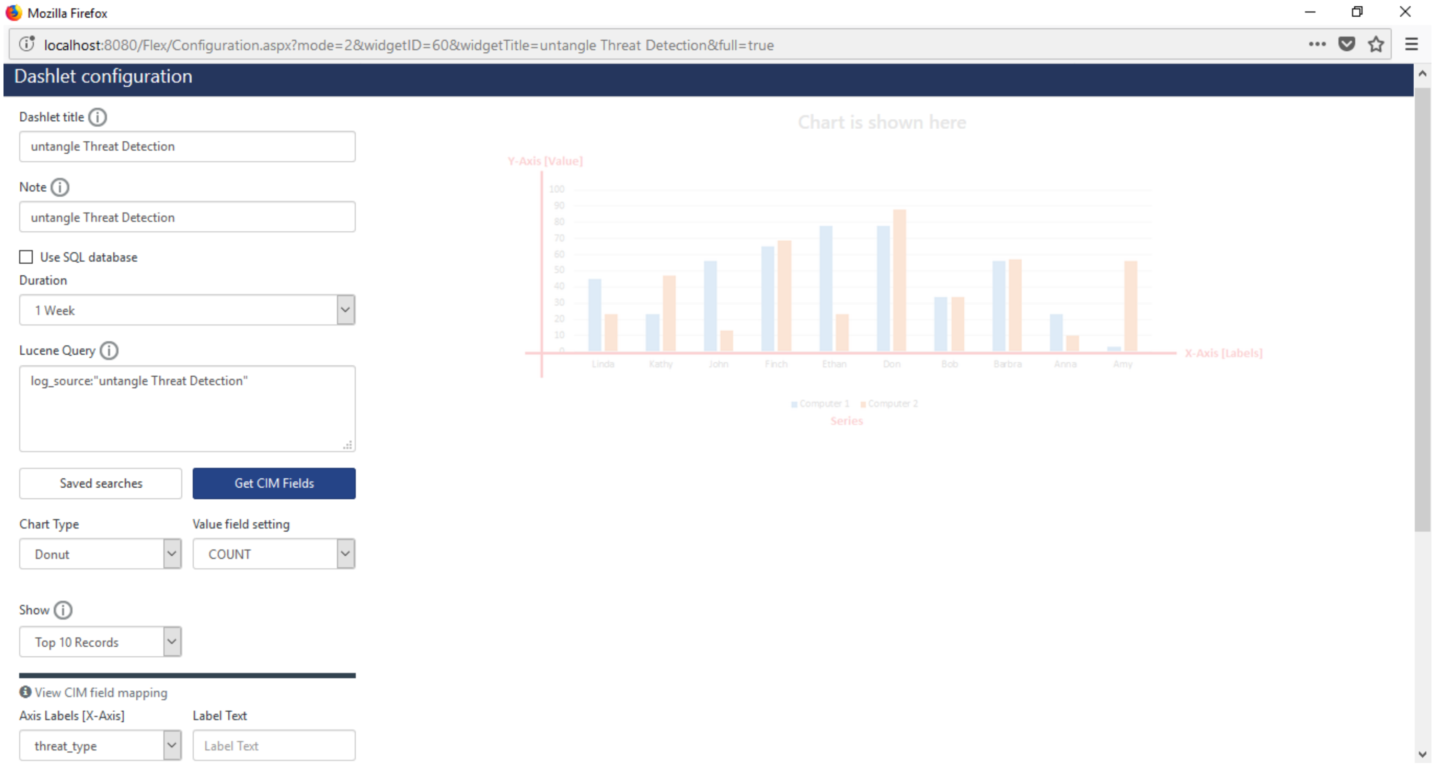

EventTracker :: Dashboard Configuration - Mozilla Firefox
localhost:8080/Flex/Add.aspx?dType=2&did=14
Edit Dashboard
Save
Delete
Cancel

Title: untangle

Description: untangle

Figure 42

4. Fill suitable Title and Description and click **Save** button.
5. Click ⚙ to **configure** a new dashlet. Widget configuration pane is shown.



Dashlet title: untangle Threat Detection

Note: untangle Threat Detection

□ Use SQL database

Duration: 1 Week

Lucene Query: log_source:"untangle Threat Detection"

Chart Type: Donut

Value field setting: COUNT

Show: Top 10 Records

Axis Labels [X-Axis]: threat_type

Label Text: Label Text

Figure 43

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

Evaluated chart is shown.

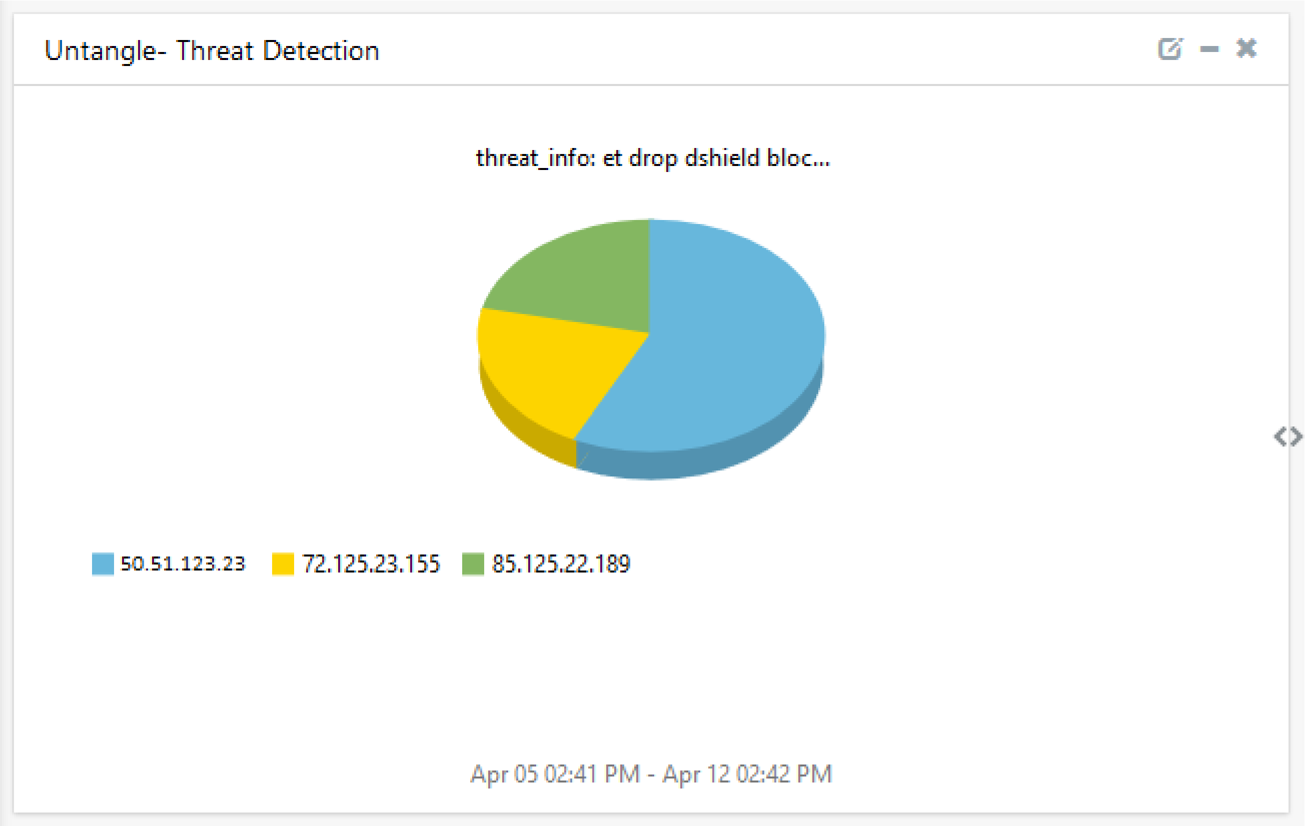
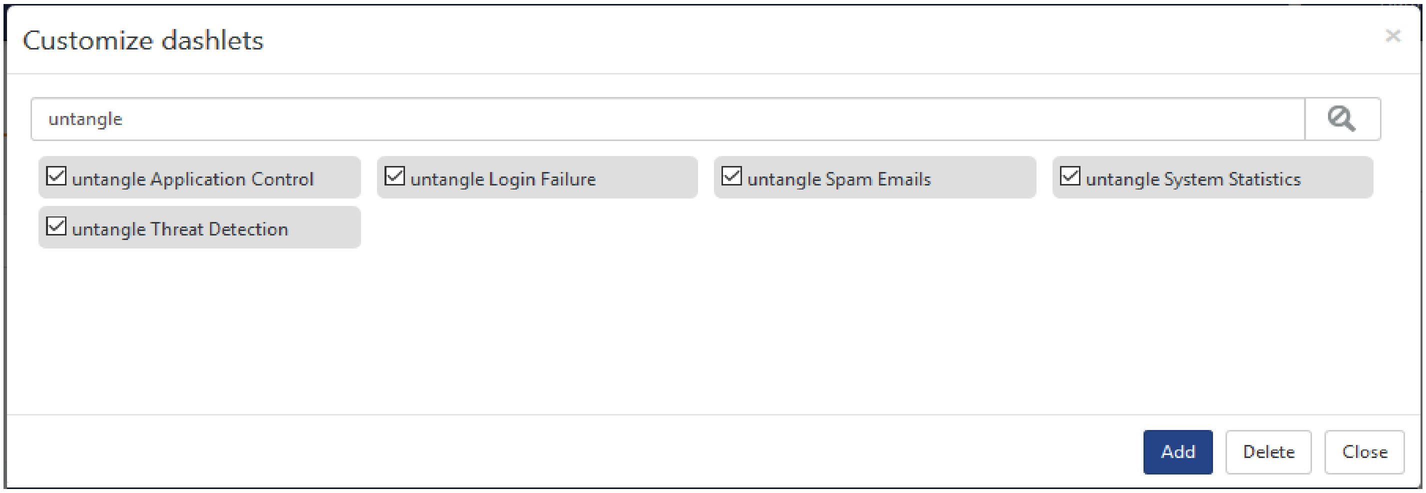


Figure 44

15. If satisfied, click **Configure** button.



Customize dashlets

untangle

☑ untangle Application Control ☑ untangle Login Failure ☑ untangle Spam Emails ☑ untangle System Statistics

☑ untangle Threat Detection

Figure 45

16. Click **'Customize'** to locate and choose created dashlet.
17. Click '**Add'** dashlet to earlier created dashboard.

Sample Flex Dashboards

For below dashboard:

WIDGET TITLE: Untangle- Threat Detection
DATA SOURCE: Untangle Threat Detection
CHART TYPE: Pie
AXIS LABELS [X-AXIS]: Src_ip_address
LEGEND[SERIES]: Threat_info

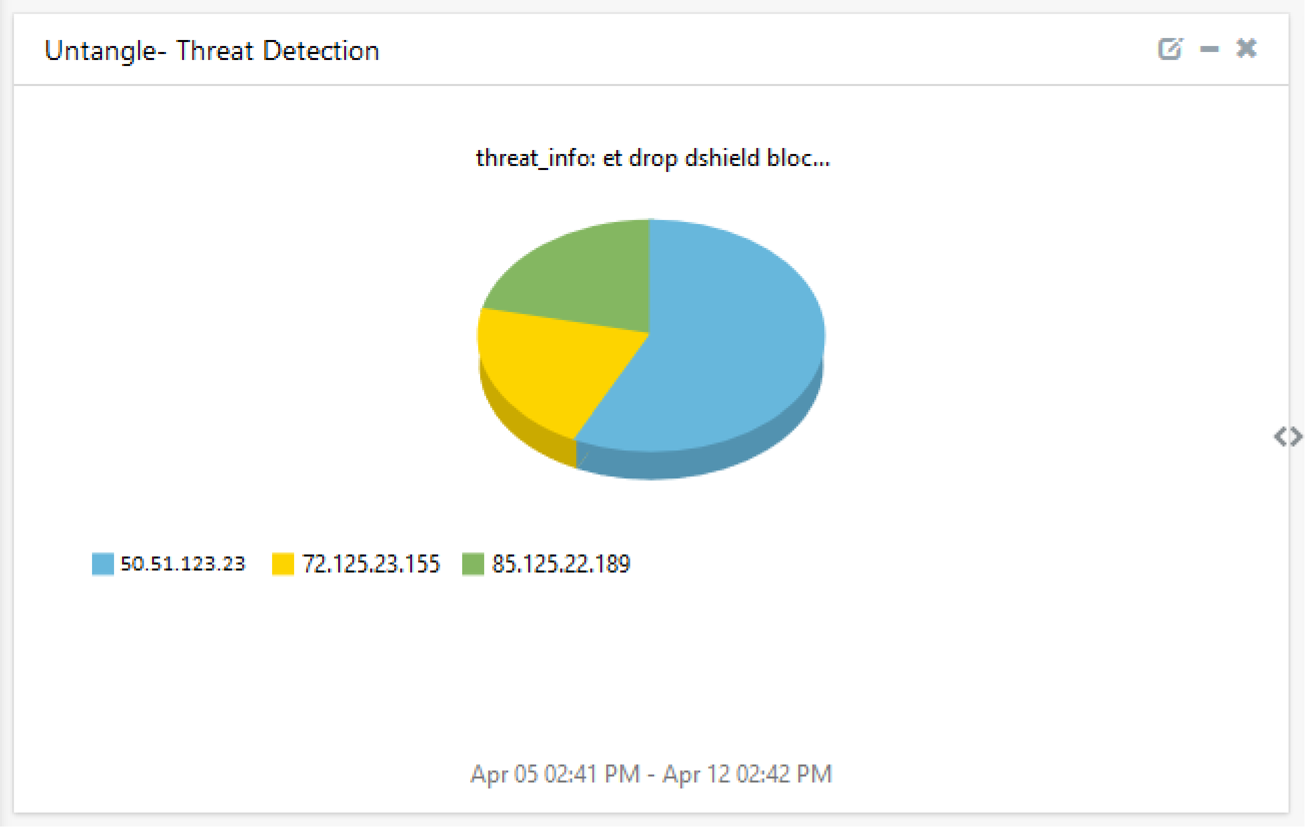

Untangle- Threat Detection
threat_info: et drop dshield bloc...
🟦 50.51.123.23
🟨 72.125.23.155
🟩 85.125.22.189
Apr 05 02:41 PM - Apr 12 02:42 PM

Figure 46

For below dashboard:

WIDGET TITLE: Untangle- Spam Emails
DATA SOURCE: Untangle Spam Emails
CHART TYPE: Column
AXIS LABELS [X-AXIS]: Recipient_address
LEGEND[SERIES]: Src_ip_address

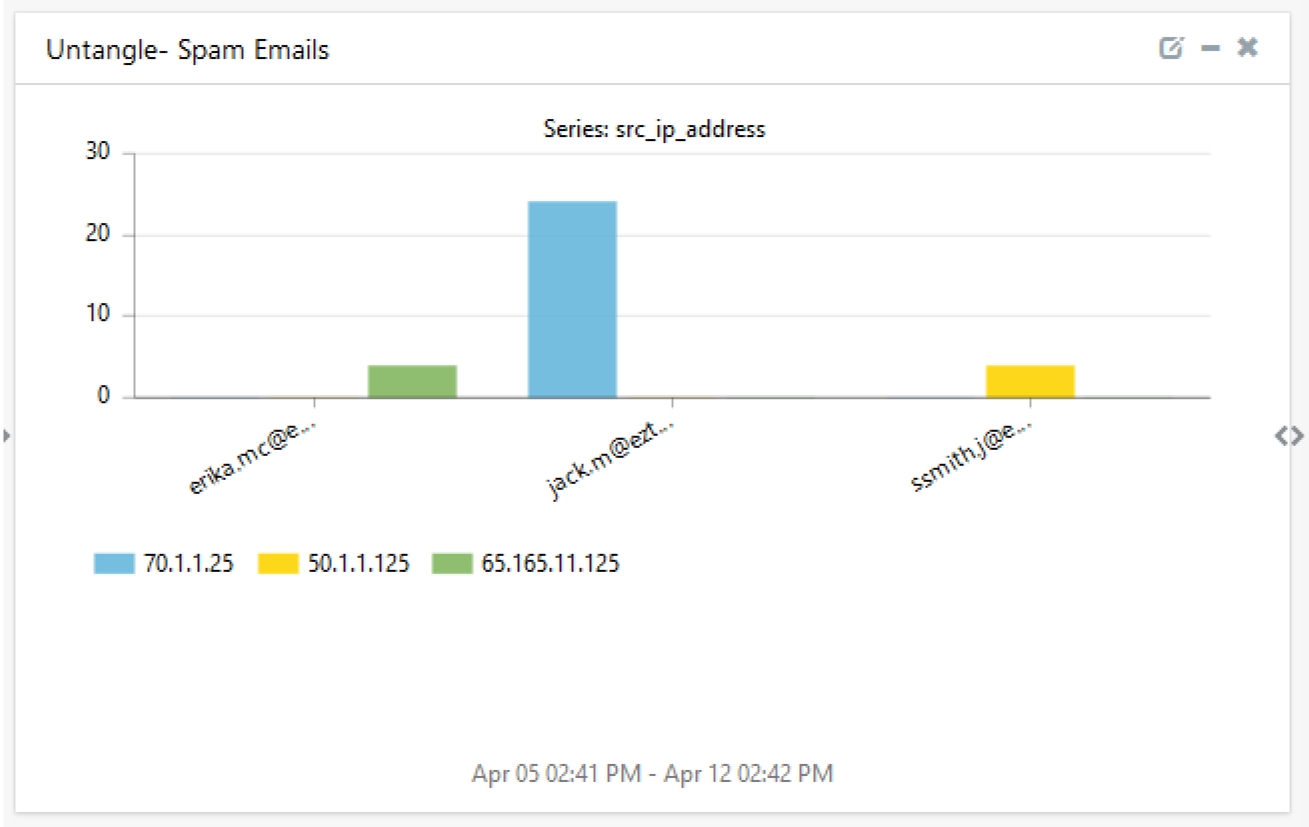


Figure 47