EventTracker
Actionable Security Intelligence

Integrate Trend Micro Control Manager

EventTracker v8.x and above

Publication Date: May 24, 2018

Abstract

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

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version v8.x or above and Trend Micro Control Manager 7.0.

Audience

Administrators who are assigned the task to monitor and manage Trend Micro CM events using EventTracker.

Table of Contents

Introduction

Centralized security management will help you improve visibility and protection, reduces complexity, and eliminates redundant and repetitive tasks in security administration - all of which make your organization more secure and your life easier. It can manage multiple OfficeScan servers for endpoint security solution.

With EventTracker, you can monitor Trend Micro CM 7.0 events from a single view. EventTracker can generate flex reports; trigger alerts for web and email violation, policy changes, service changes and threat detection.

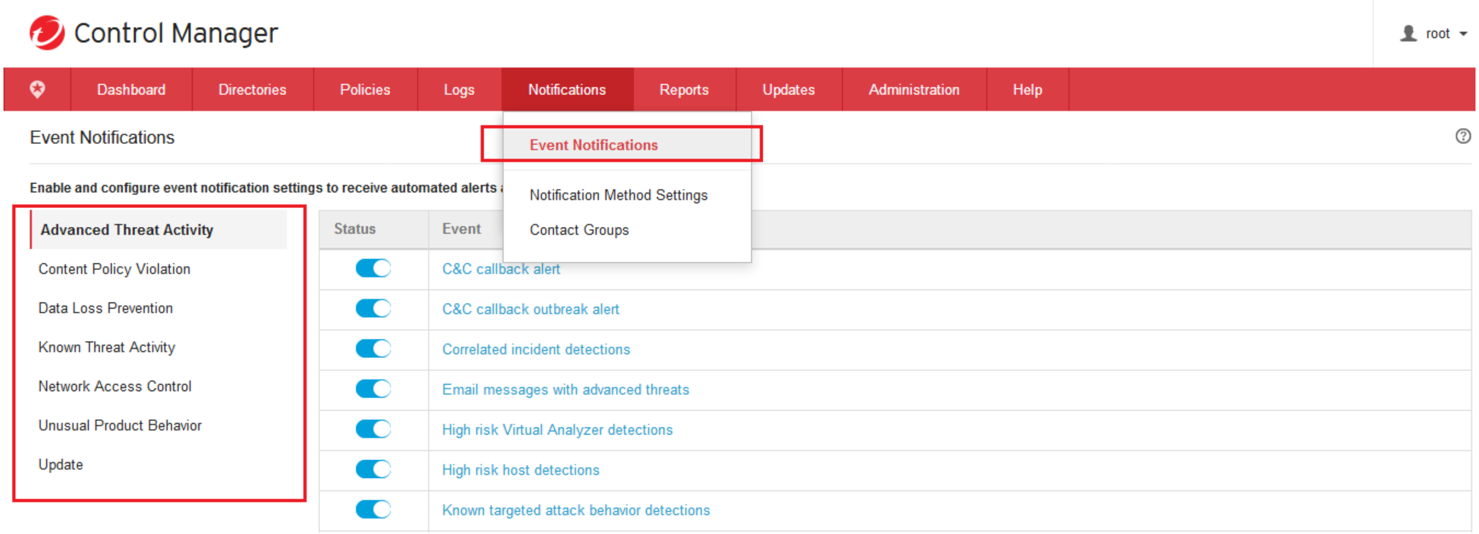
Prerequisites

- Trend Micro CM 7.0 should be installed on Microsoft Windows Server 2008 R2 and later.
- EventTracker Agent should be installed on the respective server.

Configure Trend Micro CM to forward logs to EventTracker

Trend Micro CM configuration

1. Log in to the Trend Micro Control Manager web console.
2. Select **Notification > Event Notification**.

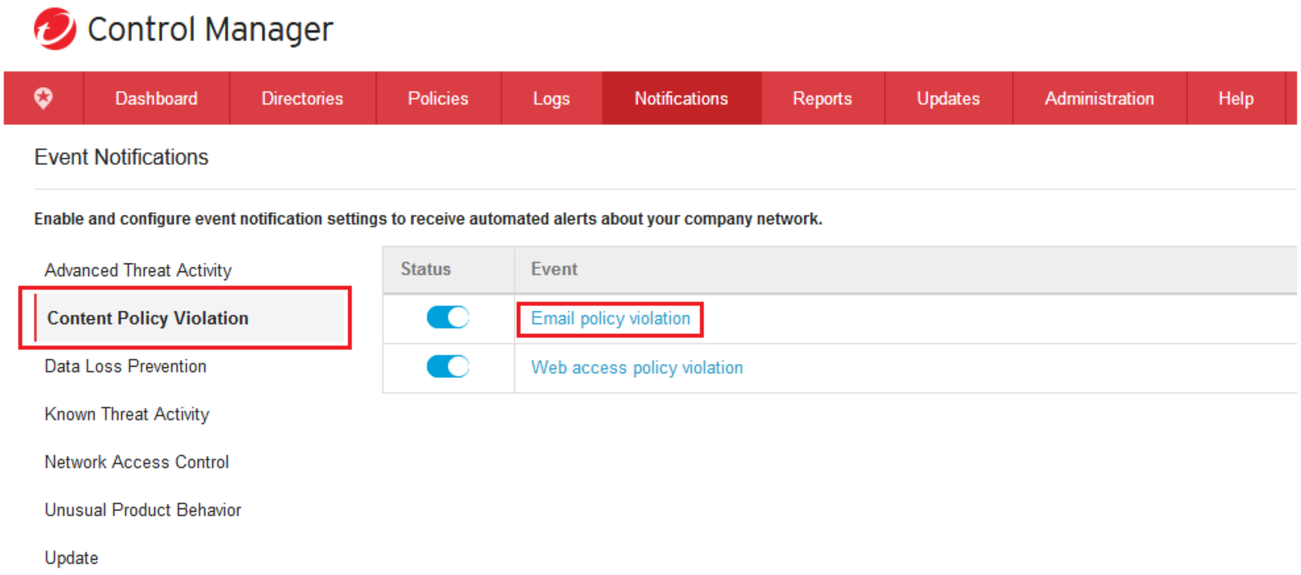


Enable and configure event notification settings to receive automated alerts

Status	Event
●	C&C callback alert
●	C&C callback outbreak alert
●	Correlated incident detections
●	Email messages with advanced threats
●	High risk Virtual Analyzer detections
●	High risk host detections
●	Known targeted attack behavior detections

Figure 1

3. In **Event Notification**, enable events under each event type.



Event Notifications

Enable and configure event notification settings to receive automated alerts about your company network.

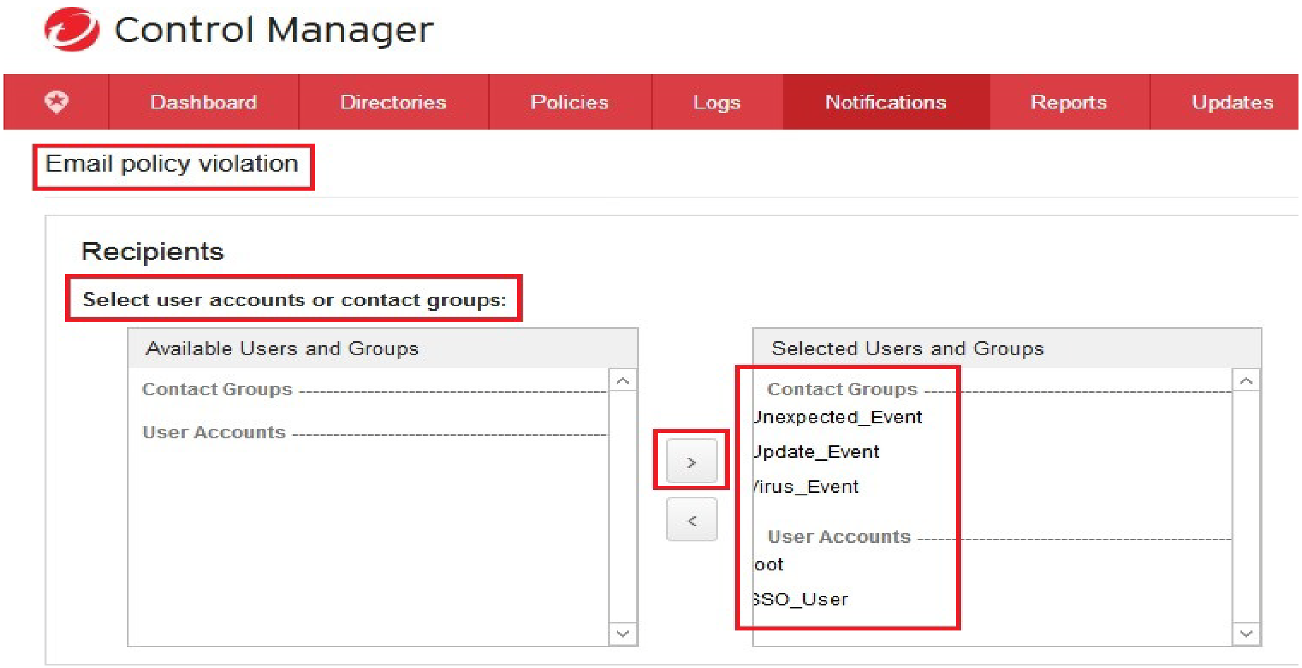
- Advanced Threat Activity
- Content Policy Violation
- Data Loss Prevention
- Known Threat Activity
- Network Access Control
- Unusual Product Behavior
- Update

Status	Event
On	Email policy violation
On	Web access policy violation

Figure 2

4. Click on each event to configure.

5. In **Recipients** section of selected event, select all **Available Users and Groups** and press > to move them to **Selected Users and Groups** box.



Email policy violation

Recipients

Select user accounts or contact groups:

Available Users and Groups

Contact Groups

User Accounts

Selected Users and Groups

Contact Groups

Jnexpected_Event

Jpdate_Event

/irus_Event

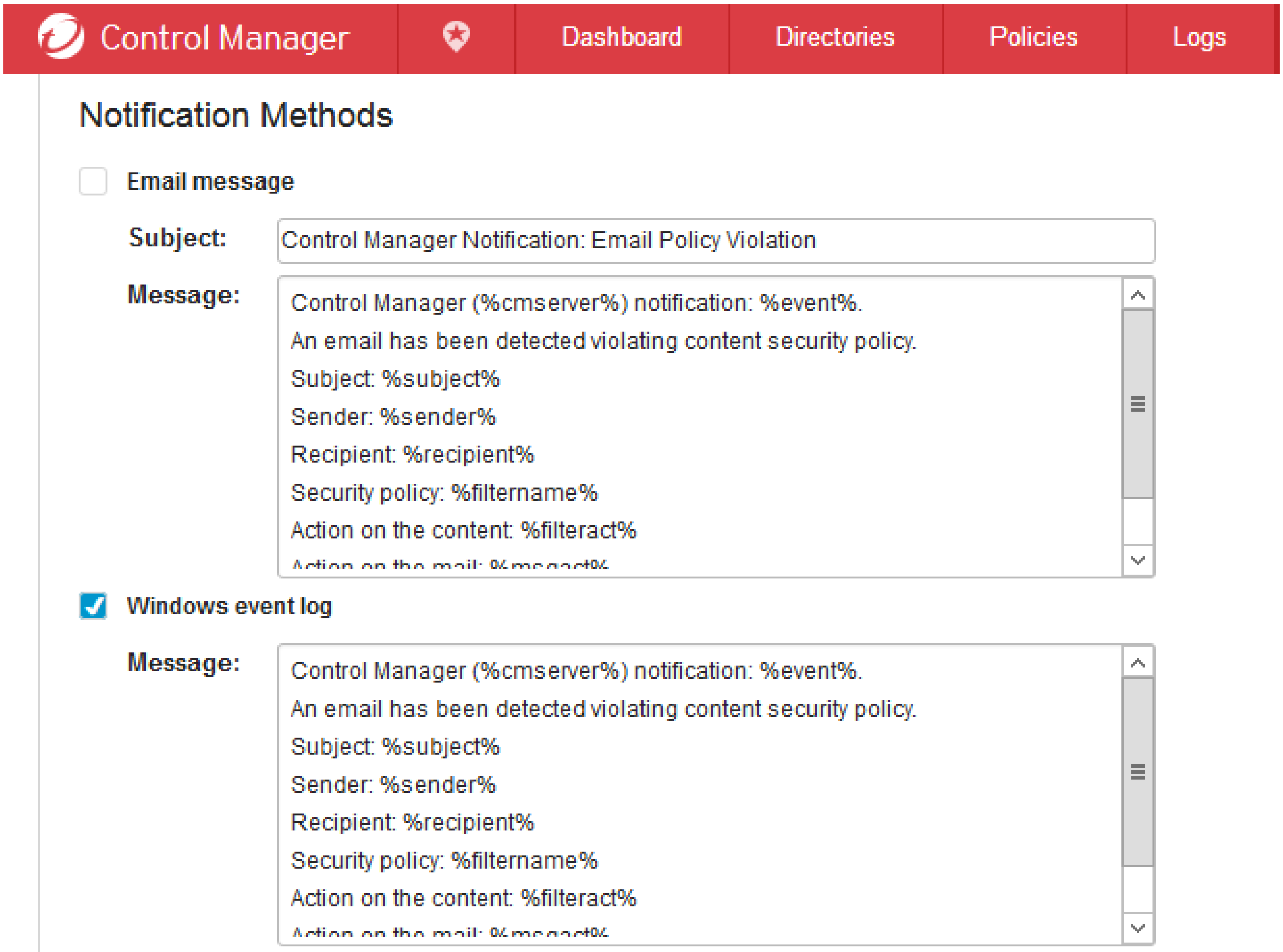
User Accounts

oot

SSO_User

Figure 3

6. In **Notification methods** section of selected event, select **Windows event log** option.



Notification Methods

☐ Email message

Subject: Control Manager Notification: Email Policy Violation

Message:

```
Control Manager (%cmserver%) notification: %event%.
An email has been detected violating content security policy.
Subject: %subject%
Sender: %sender%
Recipient: %recipient%
Security policy: %filtername%
Action on the content: %filteract%
Action on the mail: %msgact%
```

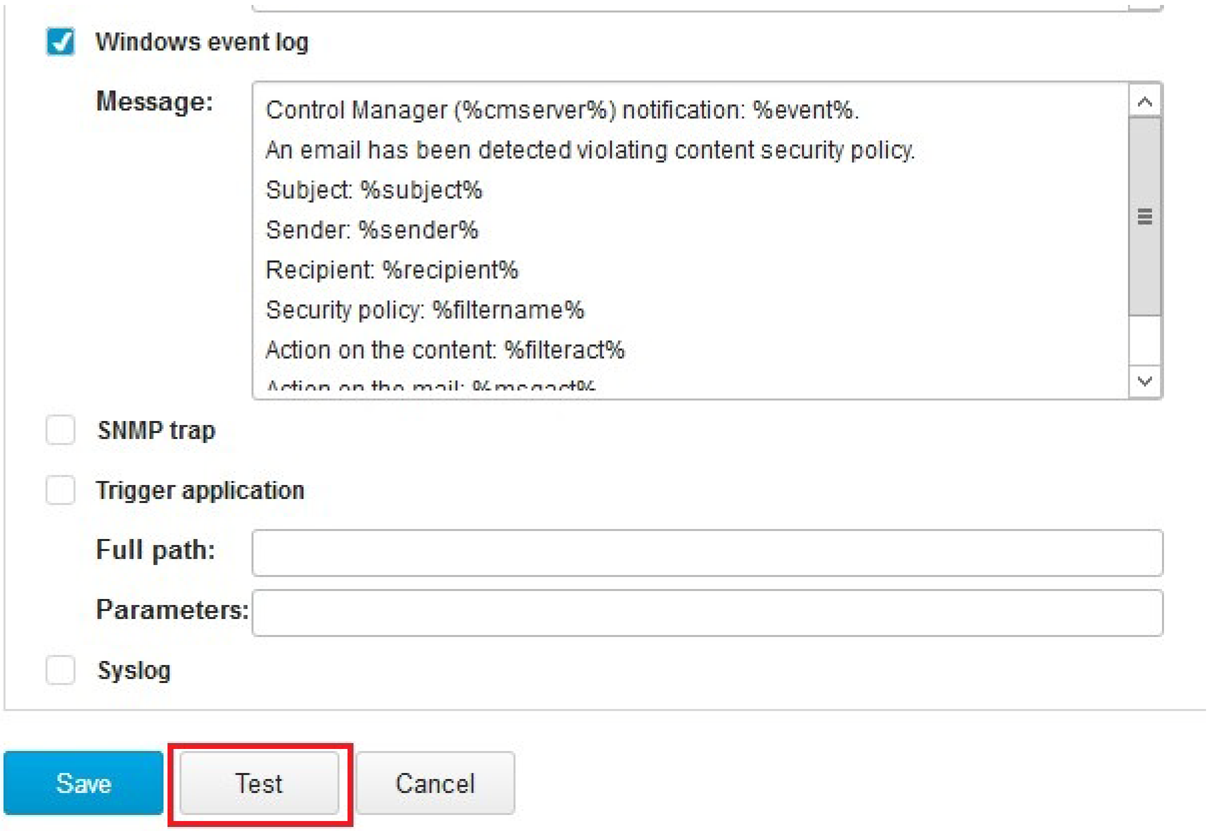
☑ Windows event log

Message:

```
Control Manager (%cmserver%) notification: %event%.
An email has been detected violating content security policy.
Subject: %subject%
Sender: %sender%
Recipient: %recipient%
Security policy: %filtername%
Action on the content: %filteract%
Action on the mail: %msgact%
```

Figure 4

7. Click the **Test** button to send the text messages to **Event Viewer**.



☑ Windows event log

Message:

```
Control Manager (%cmserver%) notification: %event%.
An email has been detected violating content security policy.
Subject: %subject%
Sender: %sender%
Recipient: %recipient%
Security policy: %filtername%
Action on the content: %filteract%
Action on the mail: %msgact%
```

□ SNMP trap

□ Trigger application

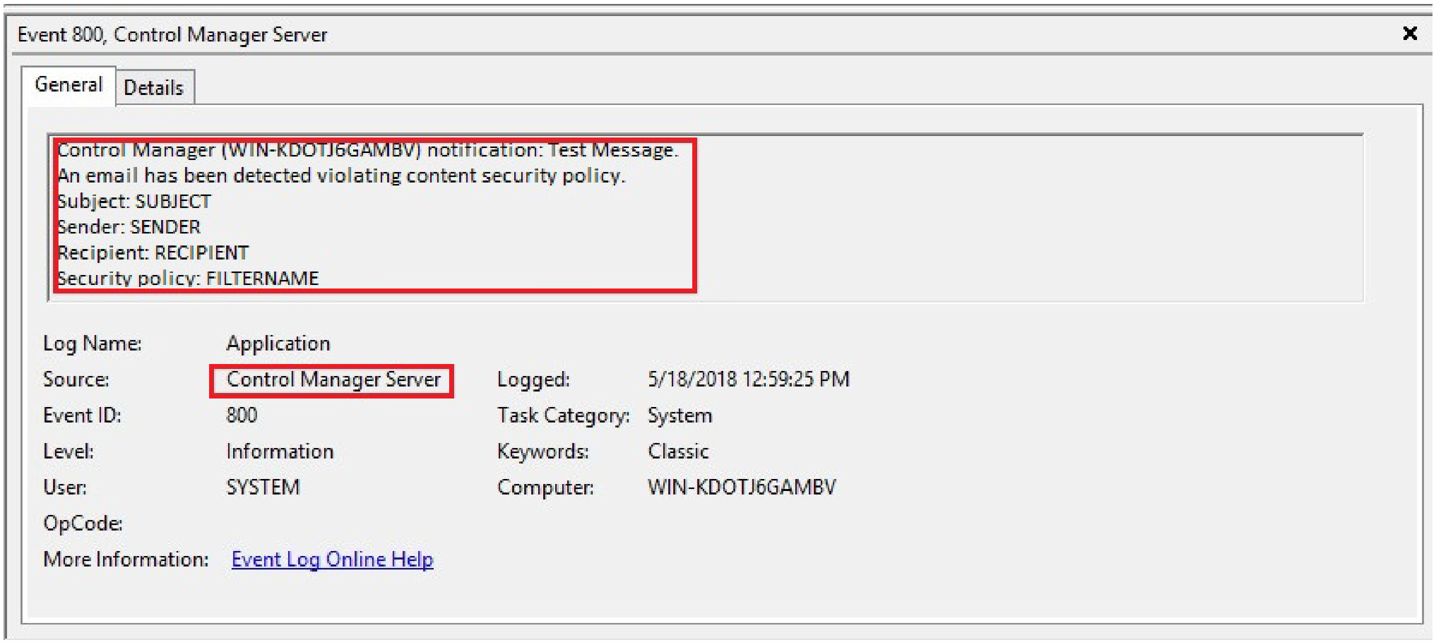
Full path:

Parameters:

□ Syslog

Figure 5

Test event can be observed in **Event Viewer**.



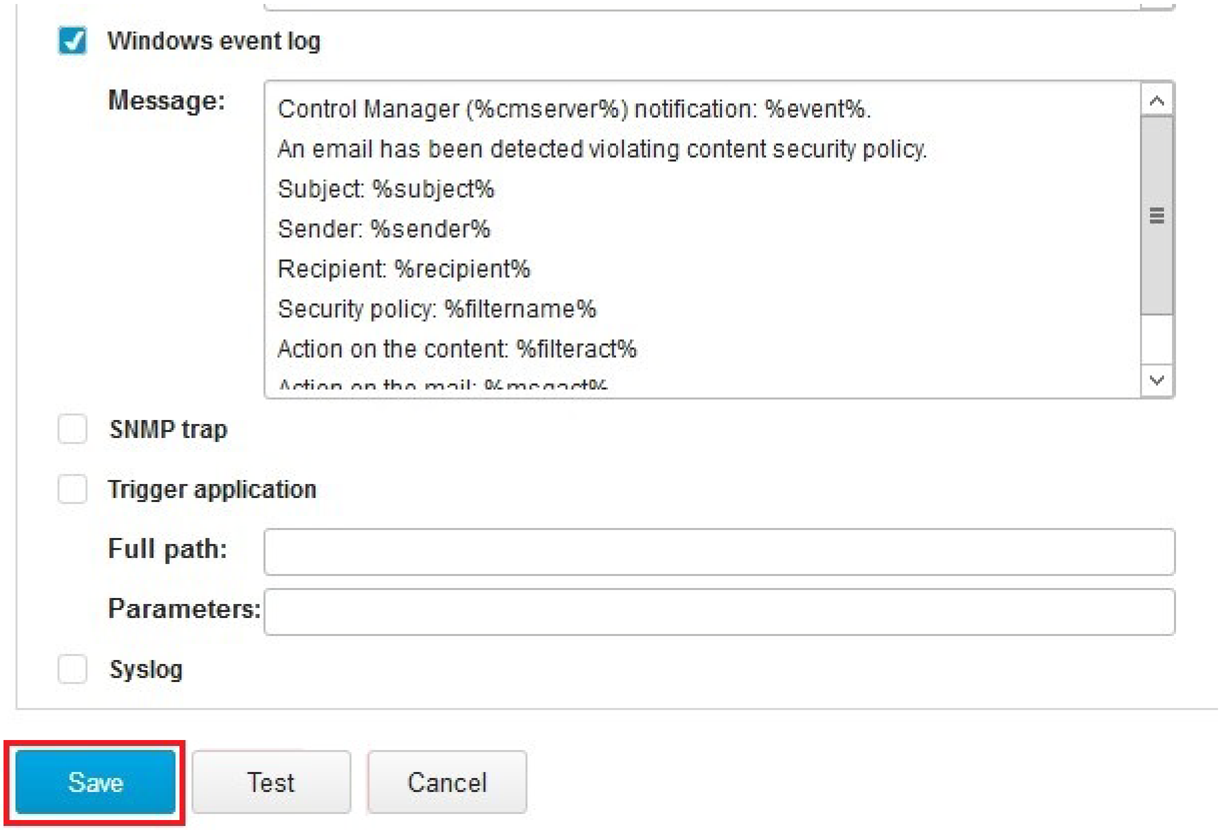
Event 800, Control Manager Server

```
Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message.
An email has been detected violating content security policy.
Subject: SUBJECT
Sender: SENDER
Recipient: RECIPIENT
Security policy: FILTERNAME
```

Log Name:	Application		
Source:	Control Manager Server	Logged:	5/18/2018 12:59:25 PM
Event ID:	800	Task Category:	System
Level:	Information	Keywords:	Classic
User:	SYSTEM	Computer:	WIN-KDOTJ6GAMBV
OpCode:			
More Information:	Event Log Online Help		

Figure 6

8. Click the **Save** button to save the changes.



☑ Windows event log

Message:

```
Control Manager (%cmserver%) notification: %event%.
An email has been detected violating content security policy.
Subject: %subject%
Sender: %sender%
Recipient: %recipient%
Security policy: %filtername%
Action on the content: %filteract%
Action on the mail: %msgact%
```

☐ SNMP trap

☐ Trigger application

Full path:

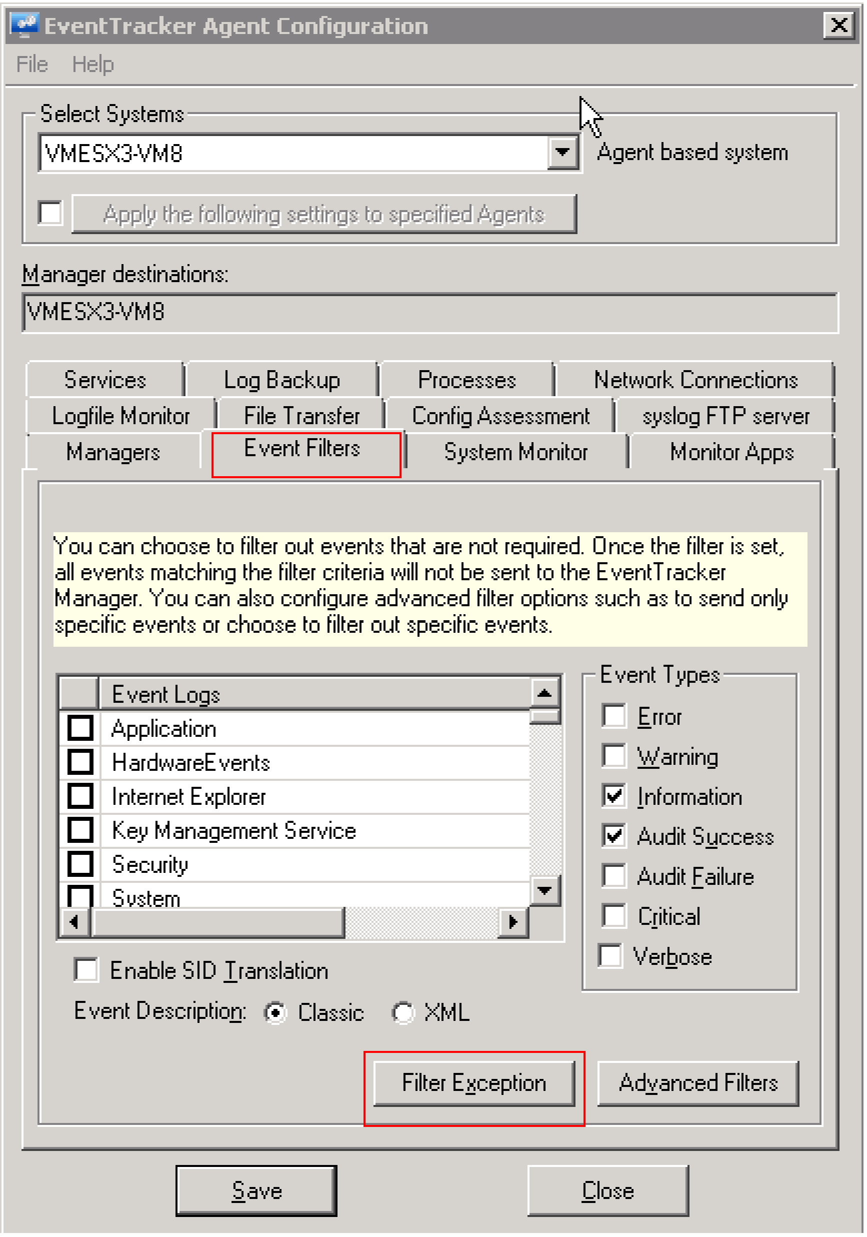
Parameters:

☐ Syslog

Figure 7

Create Filter Exception on EventTracker

1. Go to the EventTracker agent installation file path and search for **‘etaconfig’** application.
2. Then right click on the application and **Run as Administrator**.
3. Select **Event Filters** tab.
4. Select **Event Filters** tab, and then select the **Filter Exception** button.



You can choose to filter out events that are not required. Once the filter is set, all events matching the filter criteria will not be sent to the EventTracker Manager. You can also configure advanced filter options such as to send only specific events or choose to filter out specific events.

	Event Logs
□	Application
□	HardwareEvents
□	Internet Explorer
□	Key Management Service
□	Security
□	System

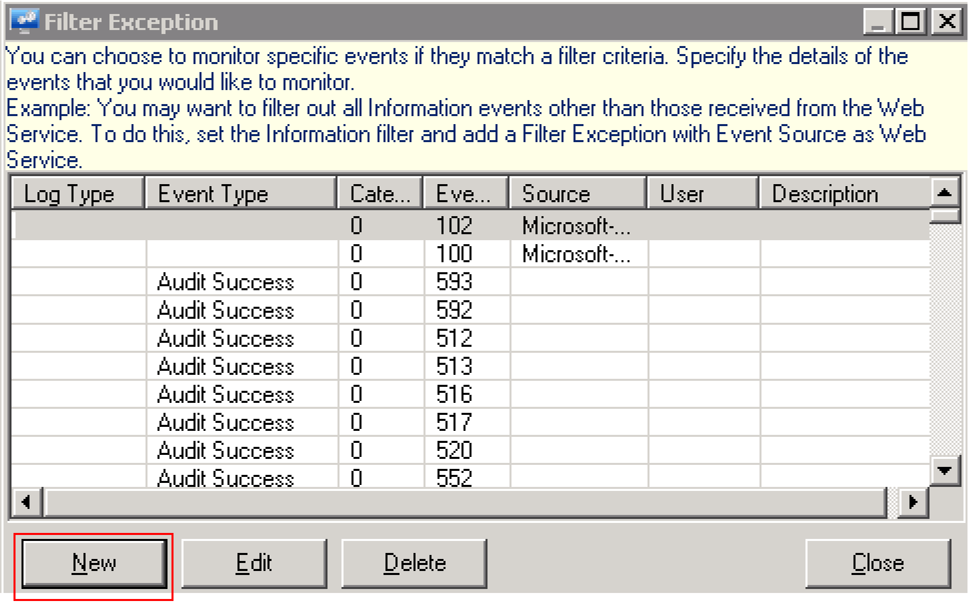
Event Types: □ Error □ Warning ☑ Information ☑ Audit Success □ Audit Failure □ Critical □ Verbose

□ Enable SID Translation

Event Description: ● Classic ○ XML

Figure 8

5. Click the **New** button.

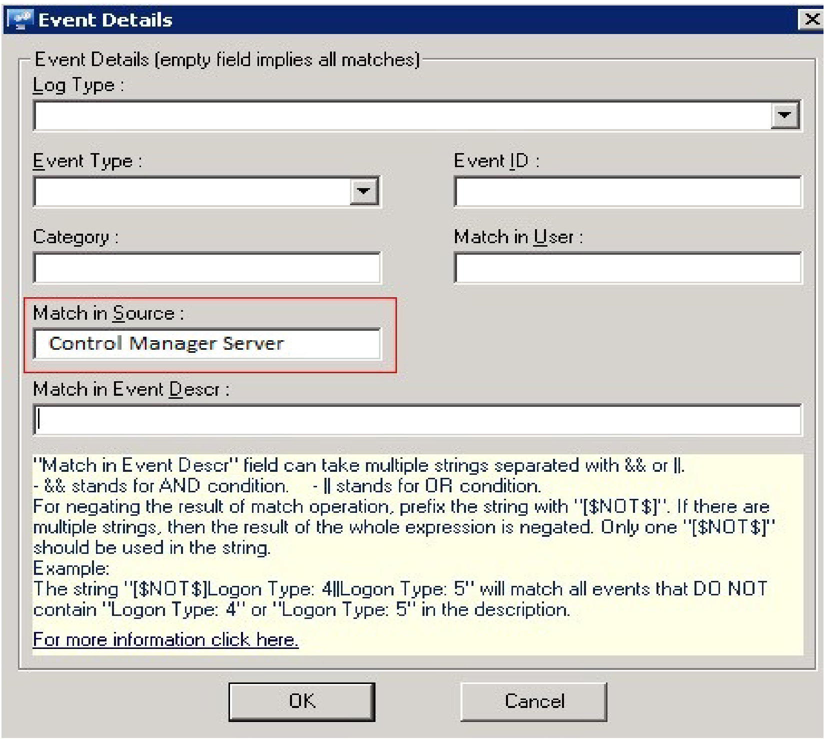


You can choose to monitor specific events if they match a filter criteria. Specify the details of the events that you would like to monitor.
Example: You may want to filter out all Information events other than those received from the Web Service. To do this, set the Information filter and add a Filter Exception with Event Source as Web Service.

Log Type	Event Type	Cate...	Eve...	Source	User	Description
		0	102	Microsoft-...		
		0	100	Microsoft-...		
	Audit Success	0	593			
	Audit Success	0	592			
	Audit Success	0	512			
	Audit Success	0	513			
	Audit Success	0	516			
	Audit Success	0	517			
	Audit Success	0	520			
	Audit Success	0	552			

Figure 9

6. In **Match in Source:** box, enter “**Control Manager Server** “.



Event Details (empty field implies all matches)

Log Type :

Event Type :

Event ID :

Category :

Match in User :

Match in Source : Control Manager Server

Match in Event Descr :

"Match in Event Descr" field can take multiple strings separated with && or ||.
- && stands for AND condition. - || stands for OR condition.
For negating the result of match operation, prefix the string with "[NOT]". If there are multiple strings, then the result of the whole expression is negated. Only one "[NOT]" should be used in the string.
Example:
The string "[NOT]Logon Type: 4||Logon Type: 5" will match all events that DO NOT contain "Logon Type: 4" or "Logon Type: 5" in the description.
For more information click here.

Figure 10

7. Click the **OK** and Save to apply changes.

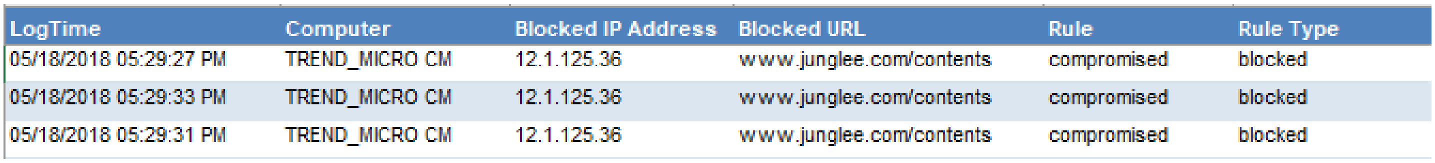
EventTracker Knowledge Pack

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 Trend Micro CM.

Flex Reports

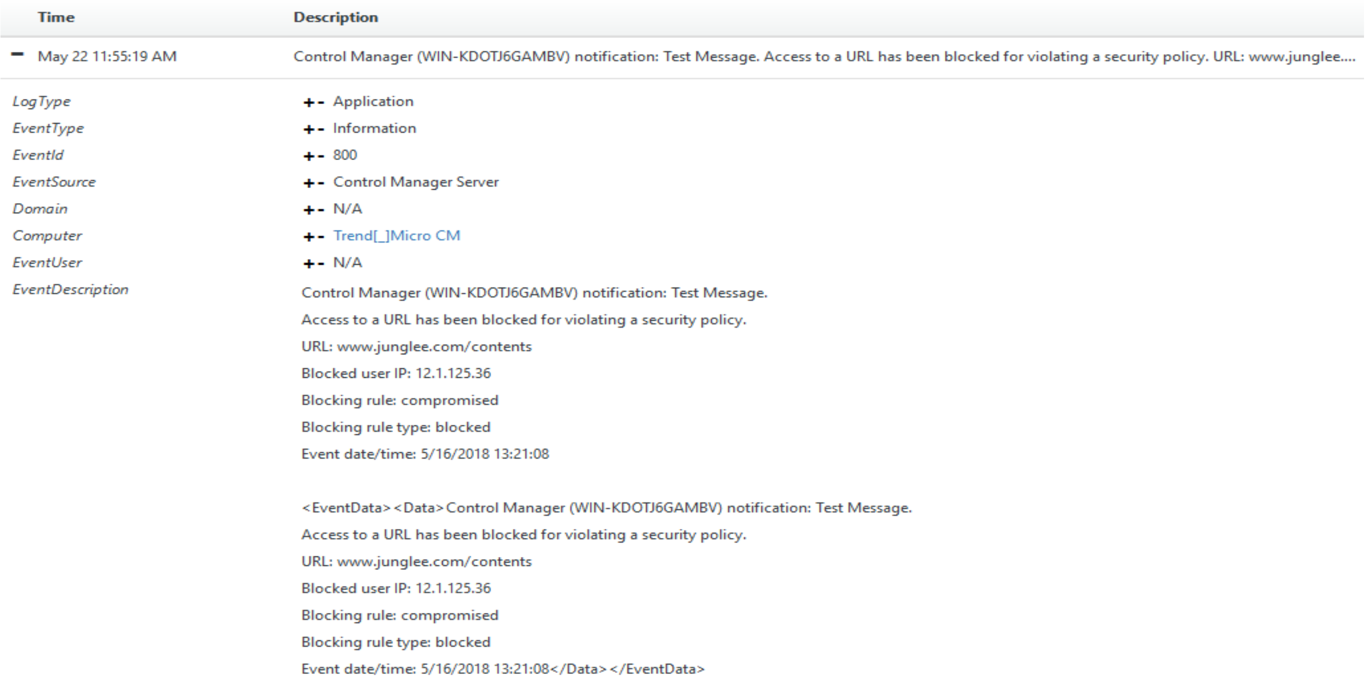
- **Trend Micro CM- Web Access Violation -** This report gives the information about URLs blocked by Trend Micro.



LogTime	Computer	Blocked IP Address	Blocked URL	Rule	Rule Type
05/18/2018 05:29:27 PM	TREND_MICRO CM	12.1.125.36	www.junglee.com/contents	compromised	blocked
05/18/2018 05:29:33 PM	TREND_MICRO CM	12.1.125.36	www.junglee.com/contents	compromised	blocked
05/18/2018 05:29:31 PM	TREND_MICRO CM	12.1.125.36	www.junglee.com/contents	compromised	blocked

Figure 11

Sample logs:



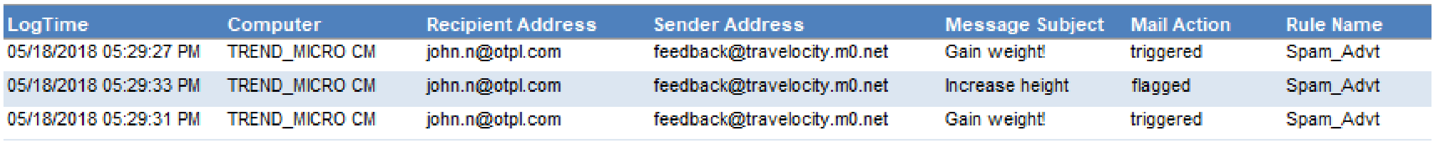
Time	Description
May 22 11:55:19 AM	Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message. Access to a URL has been blocked for violating a security policy. URL: www.junglee....

```
LogType            Application
EventType          Information
EventId            800
EventSource        Control Manager Server
Domain             N/A
Computer           Trend[_]Micro CM
EventUser          N/A
EventDescription   Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message.
                   Access to a URL has been blocked for violating a security policy.
                   URL: www.junglee.com/contents
                   Blocked user IP: 12.1.125.36
                   Blocking rule: compromised
                   Blocking rule type: blocked
                   Event date/time: 5/16/2018 13:21:08

                   <EventData><Data>Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message.
                   Access to a URL has been blocked for violating a security policy.
                   URL: www.junglee.com/contents
                   Blocked user IP: 12.1.125.36
                   Blocking rule: compromised
                   Blocking rule type: blocked
                   Event date/time: 5/16/2018 13:21:08</Data></EventData>
```

Figure 12

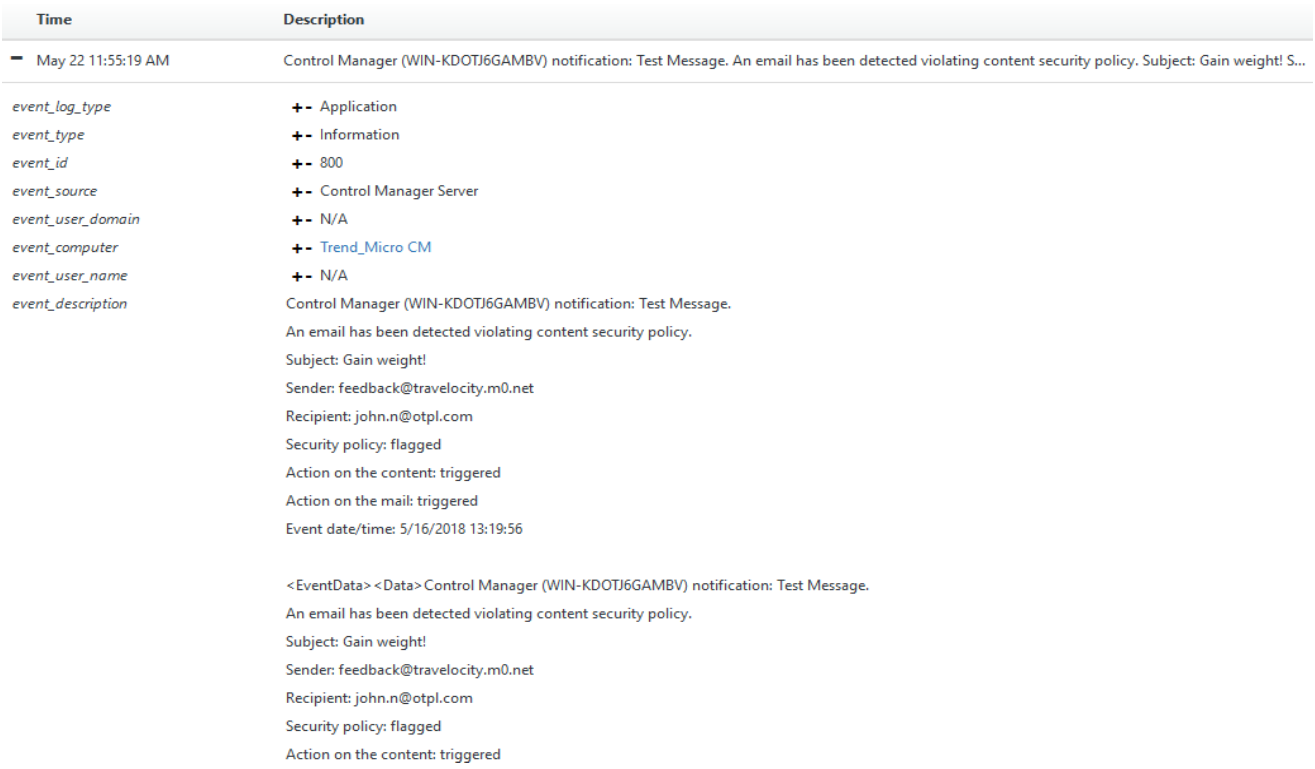
- **Trend Micro CM- Email Violation -** This report gives the information about suspicious emails detected by Trend Micro.



LogTime	Computer	Recipient Address	Sender Address	Message Subject	Mail Action	Rule Name
05/18/2018 05:29:27 PM	TREND_MICRO CM	john.n@otpl.com	feedback@travelocity.m0.net	Gain weight!	triggered	Spam_Advt
05/18/2018 05:29:33 PM	TREND_MICRO CM	john.n@otpl.com	feedback@travelocity.m0.net	Increase height	flagged	Spam_Advt
05/18/2018 05:29:31 PM	TREND_MICRO CM	john.n@otpl.com	feedback@travelocity.m0.net	Gain weight!	triggered	Spam_Advt

Figure 13

Sample logs:



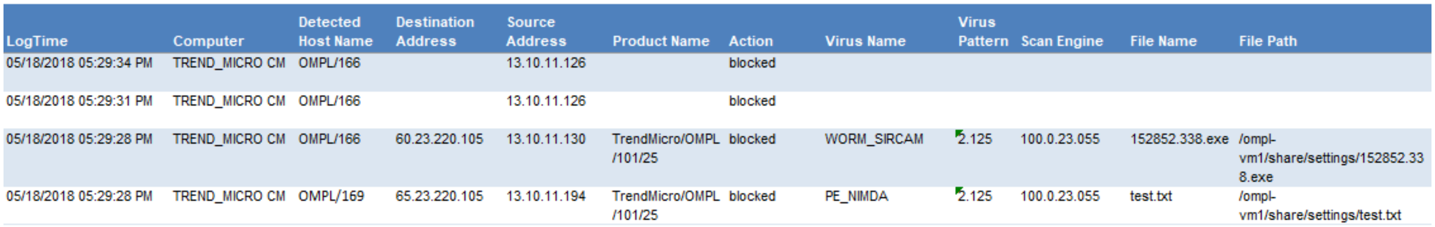
```
Time                Description
−  May 22 11:55:19 AM   Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message. An email has been detected violating content security policy. Subject: Gain weight! S...

event_log_type      +- Application
event_type          +- Information
event_id            +- 800
event_source        +- Control Manager Server
event_user_domain   +- N/A
event_computer      +- Trend_Micro CM
event_user_name     +- N/A
event_description   Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message.
                    An email has been detected violating content security policy.
                    Subject: Gain weight!
                    Sender: feedback@travelocity.m0.net
                    Recipient: john.n@otpl.com
                    Security policy: flagged
                    Action on the content: triggered
                    Action on the mail: triggered
                    Event date/time: 5/16/2018 13:19:56

                    <EventData><Data>Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message.
                    An email has been detected violating content security policy.
                    Subject: Gain weight!
                    Sender: feedback@travelocity.m0.net
                    Recipient: john.n@otpl.com
                    Security policy: flagged
                    Action on the content: triggered
```

Figure 14

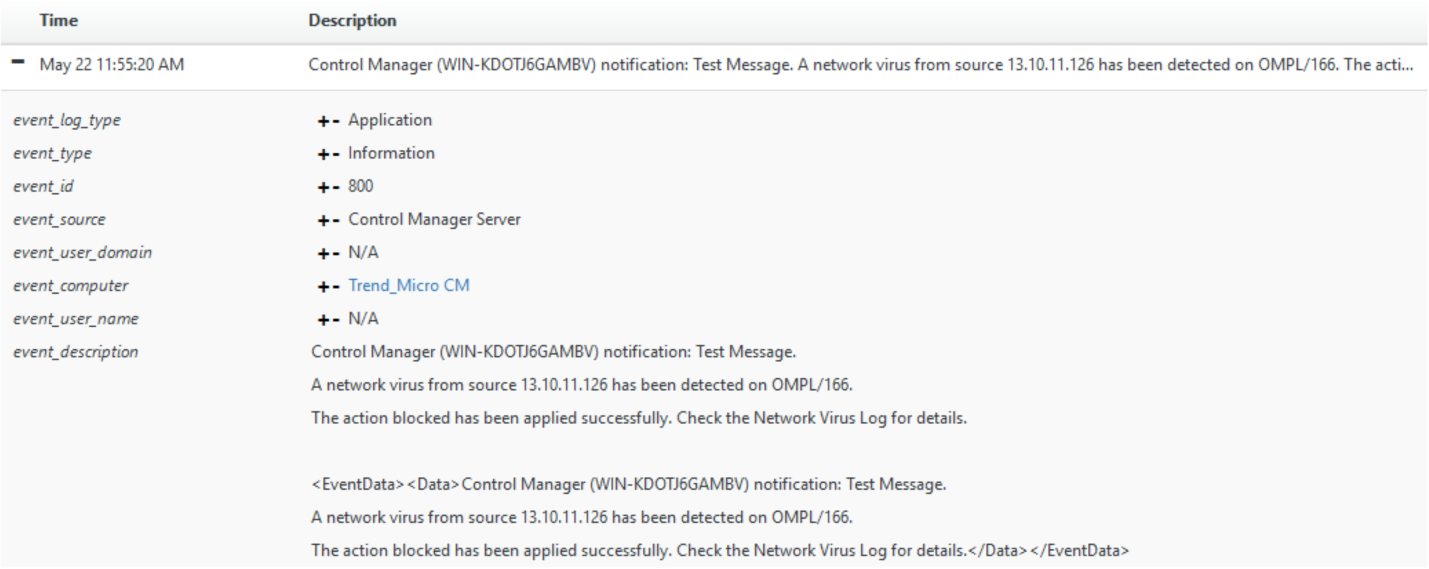
- **Trend Micro CM- Threat Activity -** This report gives the information about threats detected by Trend Micro.



LogTime	Computer	Detected Host Name	Destination Address	Source Address	Product Name	Action	Virus Name	Virus Pattern	Scan Engine	File Name	File Path
05/18/2018 05:29:34 PM	TREND_MICRO CM	OMPL/166		13.10.11.126		blocked					
05/18/2018 05:29:31 PM	TREND_MICRO CM	OMPL/166		13.10.11.126		blocked					
05/18/2018 05:29:28 PM	TREND_MICRO CM	OMPL/166	60.23.220.105	13.10.11.130	TrendMicro/OMPL /101/25	blocked	WORM_SIRCAM	2.125	100.0.23.055	152852.338.exe	/ompl-vm1/share/settings/152852.338.exe
05/18/2018 05:29:28 PM	TREND_MICRO CM	OMPL/169	65.23.220.105	13.10.11.194	TrendMicro/OMPL /101/25	blocked	PE_NIMDA	2.125	100.0.23.055	test.txt	/ompl-vm1/share/settings/test.txt

Figure 15

Sample logs:



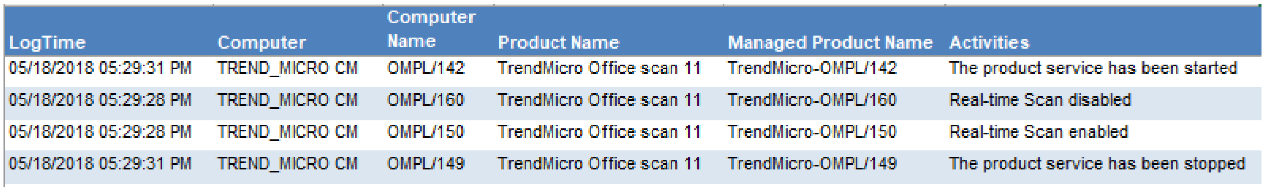
```
Time                    Description
−  May 22 11:55:20 AM   Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message. A network virus from source 13.10.11.126 has been detected on OMPL/166. The acti...

event_log_type          +- Application
event_type              +- Information
event_id                +- 800
event_source            +- Control Manager Server
event_user_domain       +- N/A
event_computer          +- Trend_Micro CM
event_user_name         +- N/A
event_description       Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message.
                        A network virus from source 13.10.11.126 has been detected on OMPL/166.
                        The action blocked has been applied successfully. Check the Network Virus Log for details.

                        <EventData><Data>Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message.
                        A network virus from source 13.10.11.126 has been detected on OMPL/166.
                        The action blocked has been applied successfully. Check the Network Virus Log for details.</Data></EventData>
```

Figure 16

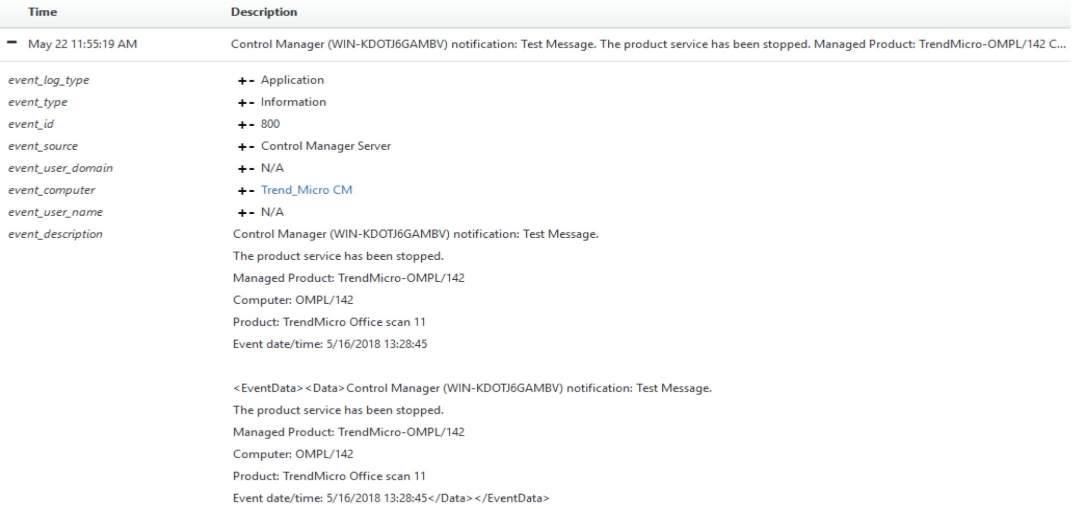
- **Trend Micro CM- Service Changes -** This report gives the information about Trend Micro system activities.



LogTime	Computer	Computer Name	Product Name	Managed Product Name	Activities
05/18/2018 05:29:31 PM	TREND_MICRO CM	OMPL/142	TrendMicro Office scan 11	TrendMicro-OMPL/142	The product service has been started
05/18/2018 05:29:28 PM	TREND_MICRO CM	OMPL/160	TrendMicro Office scan 11	TrendMicro-OMPL/160	Real-time Scan disabled
05/18/2018 05:29:28 PM	TREND_MICRO CM	OMPL/150	TrendMicro Office scan 11	TrendMicro-OMPL/150	Real-time Scan enabled
05/18/2018 05:29:31 PM	TREND_MICRO CM	OMPL/149	TrendMicro Office scan 11	TrendMicro-OMPL/149	The product service has been stopped

Figure 17

Sample logs:



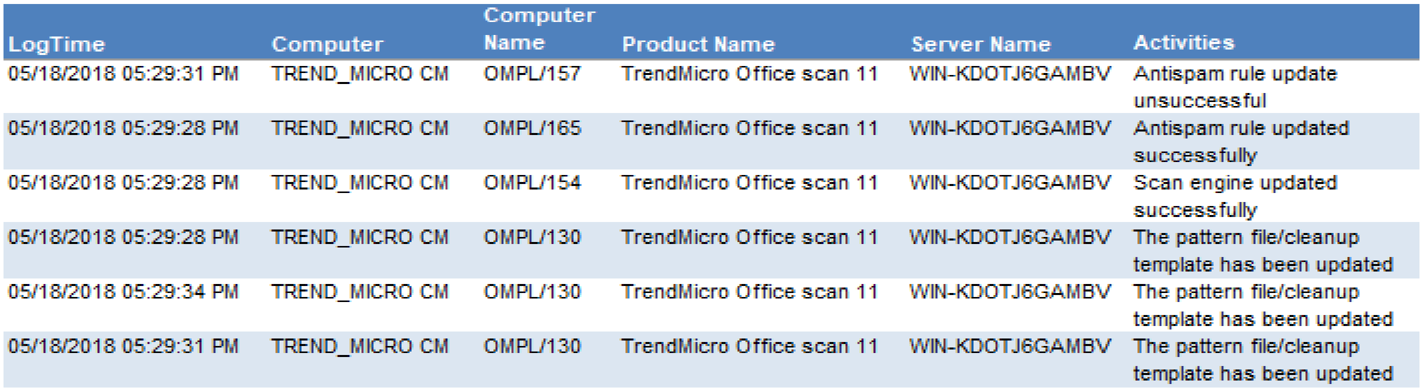
```
Time                    Description
−  May 22 11:55:19 AM   Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message. The product service has been stopped. Managed Product: TrendMicro-OMPL/142 C...

event_log_type          +- Application
event_type              +- Information
event_id                +- 800
event_source            +- Control Manager Server
event_user_domain       +- N/A
event_computer          +- Trend_Micro CM
event_user_name         +- N/A
event_description       Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message.
                        The product service has been stopped.
                        Managed Product: TrendMicro-OMPL/142
                        Computer: OMPL/142
                        Product: TrendMicro Office scan 11
                        Event date/time: 5/16/2018 13:28:45

                        <EventData><Data>Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message.
                        The product service has been stopped.
                        Managed Product: TrendMicro-OMPL/142
                        Computer: OMPL/142
                        Product: TrendMicro Office scan 11
                        Event date/time: 5/16/2018 13:28:45</Data></EventData>
```

Figure 18

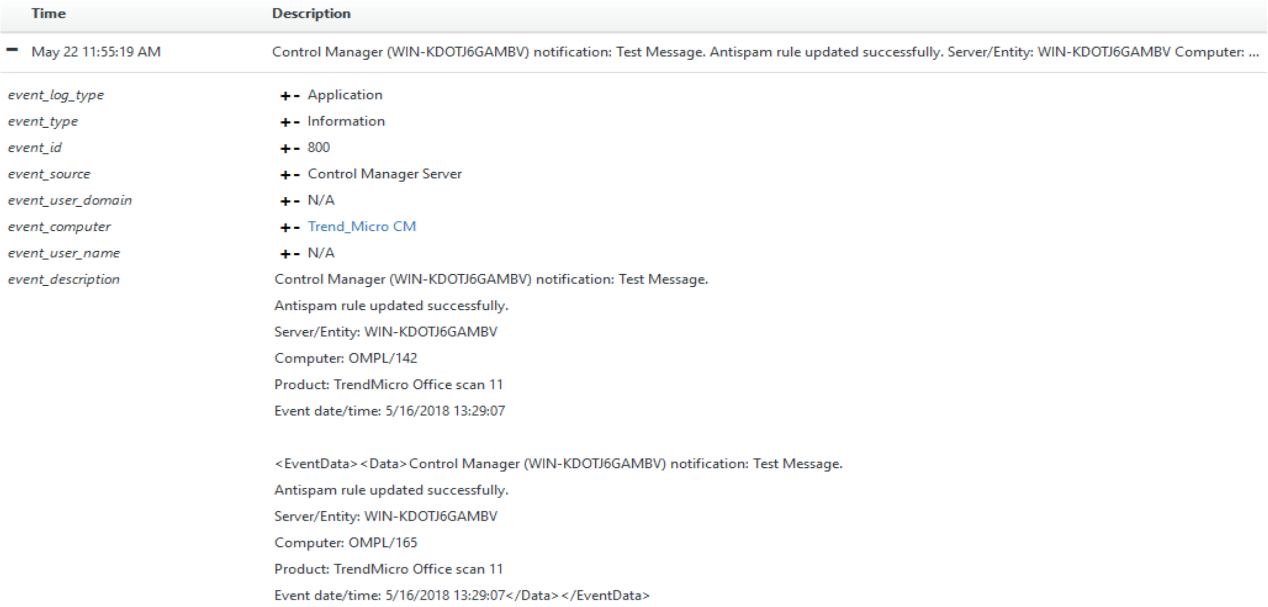
- **Trend Micro CM- Policy Changes -** This report gives the information about policy changes on Trend Micro.



LogTime	Computer	Computer Name	Product Name	Server Name	Activities
05/18/2018 05:29:31 PM	TREND_MICRO CM	OMPL/157	TrendMicro Office scan 11	WIN-KDOTJ6GAMBV	Antispam rule update unsuccessful
05/18/2018 05:29:28 PM	TREND_MICRO CM	OMPL/165	TrendMicro Office scan 11	WIN-KDOTJ6GAMBV	Antispam rule updated successfully
05/18/2018 05:29:28 PM	TREND_MICRO CM	OMPL/154	TrendMicro Office scan 11	WIN-KDOTJ6GAMBV	Scan engine updated successfully
05/18/2018 05:29:28 PM	TREND_MICRO CM	OMPL/130	TrendMicro Office scan 11	WIN-KDOTJ6GAMBV	The pattern file/cleanup template has been updated
05/18/2018 05:29:34 PM	TREND_MICRO CM	OMPL/130	TrendMicro Office scan 11	WIN-KDOTJ6GAMBV	The pattern file/cleanup template has been updated
05/18/2018 05:29:31 PM	TREND_MICRO CM	OMPL/130	TrendMicro Office scan 11	WIN-KDOTJ6GAMBV	The pattern file/cleanup template has been updated

Figure 19

Sample logs:



```
Time                    Description
− May 22 11:55:19 AM    Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message. Antispam rule updated successfully. Server/Entity: WIN-KDOTJ6GAMBV Computer: ...

event_log_type          +- Application
event_type              +- Information
event_id                +- 800
event_source            +- Control Manager Server
event_user_domain       +- N/A
event_computer          +- Trend_Micro CM
event_user_name         +- N/A
event_description       Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message.
                        Antispam rule updated successfully.
                        Server/Entity: WIN-KDOTJ6GAMBV
                        Computer: OMPL/142
                        Product: TrendMicro Office scan 11
                        Event date/time: 5/16/2018 13:29:07

                        <EventData><Data>Control Manager (WIN-KDOTJ6GAMBV) notification: Test Message.
                        Antispam rule updated successfully.
                        Server/Entity: WIN-KDOTJ6GAMBV
                        Computer: OMPL/165
                        Product: TrendMicro Office scan 11
                        Event date/time: 5/16/2018 13:29:07</Data></EventData>
```

Figure 20

Alerts

- **Trend Micro CM: Policy Changed -** This alert will be generated when a policy is changed on Trend Micro.
- **Trend Micro CM: Service Changed -** This alert will be generated when a service status is changed on Trend Micro.
- **Trend Micro CM: Threat Detected -** This alert will be generated when a threat is detected by Trend Micro.

Categories

- **Trend Micro CM Web Access Violation -** This category provides information related to web access violations.
- **Trend Micro CM Email Violation -** This category provides information related to email violations.
- **Trend Micro CM Threat Activity -** This category provides information related to threats detected.
- **Trend Micro CM Service Changes -** This category provides information related to service status changes.
- **Trend Micro CM policy Changes -** This category provides information related to policy changes.

Knowledge Objects

- **Trend Micro CM Web Access Violation -** This knowledge object helps to analyze logs related to web access violations.
- **Trend Micro CM Email Violation -** This knowledge object helps to analyze logs related to email violations.
- **Trend Micro CM Threat Activity -** This knowledge object helps to analyze logs related to threats that are detected.
- **Trend Micro CM Service Changes -** This knowledge object helps to analyze logs related to service changes.
- **Trend Micro CM policy Changes -** This knowledge object helps to analyze logs related to policy changes.

Import Trend Micro CM knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Parsing Rules
- Knowledge Objects
- Flex Reports
- Dashboards

1. Launch **EventTracker Control Panel**.

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

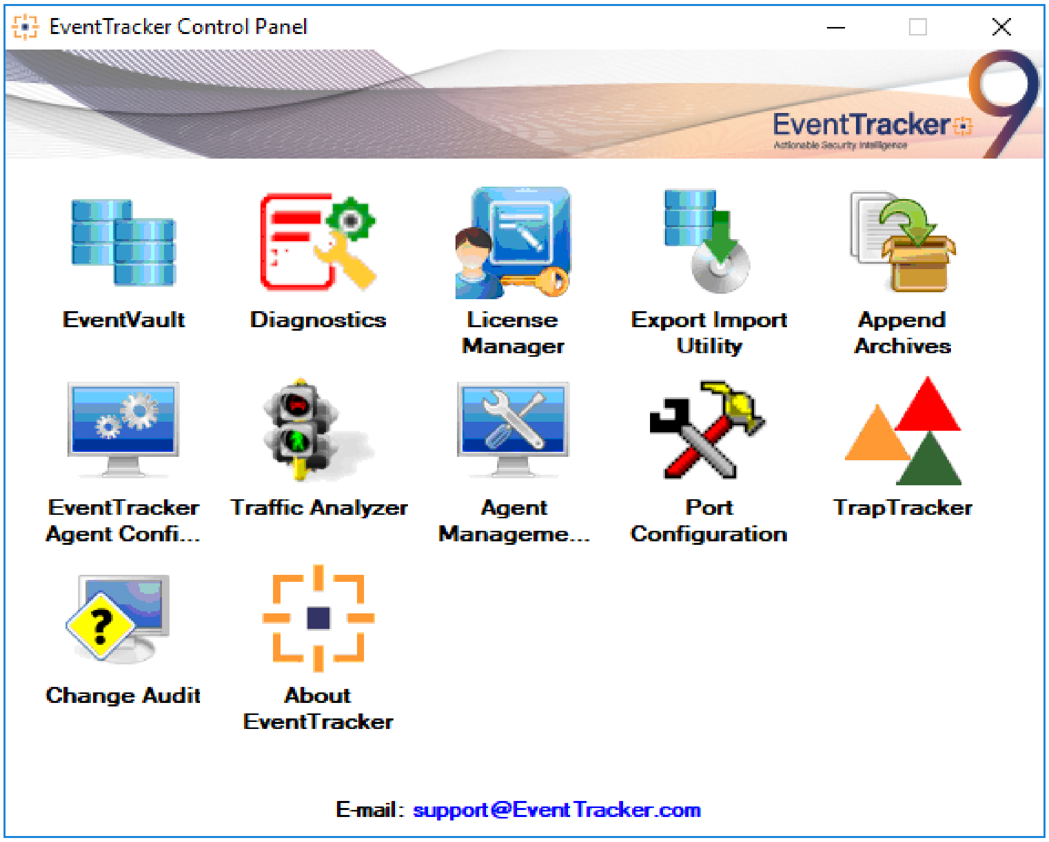
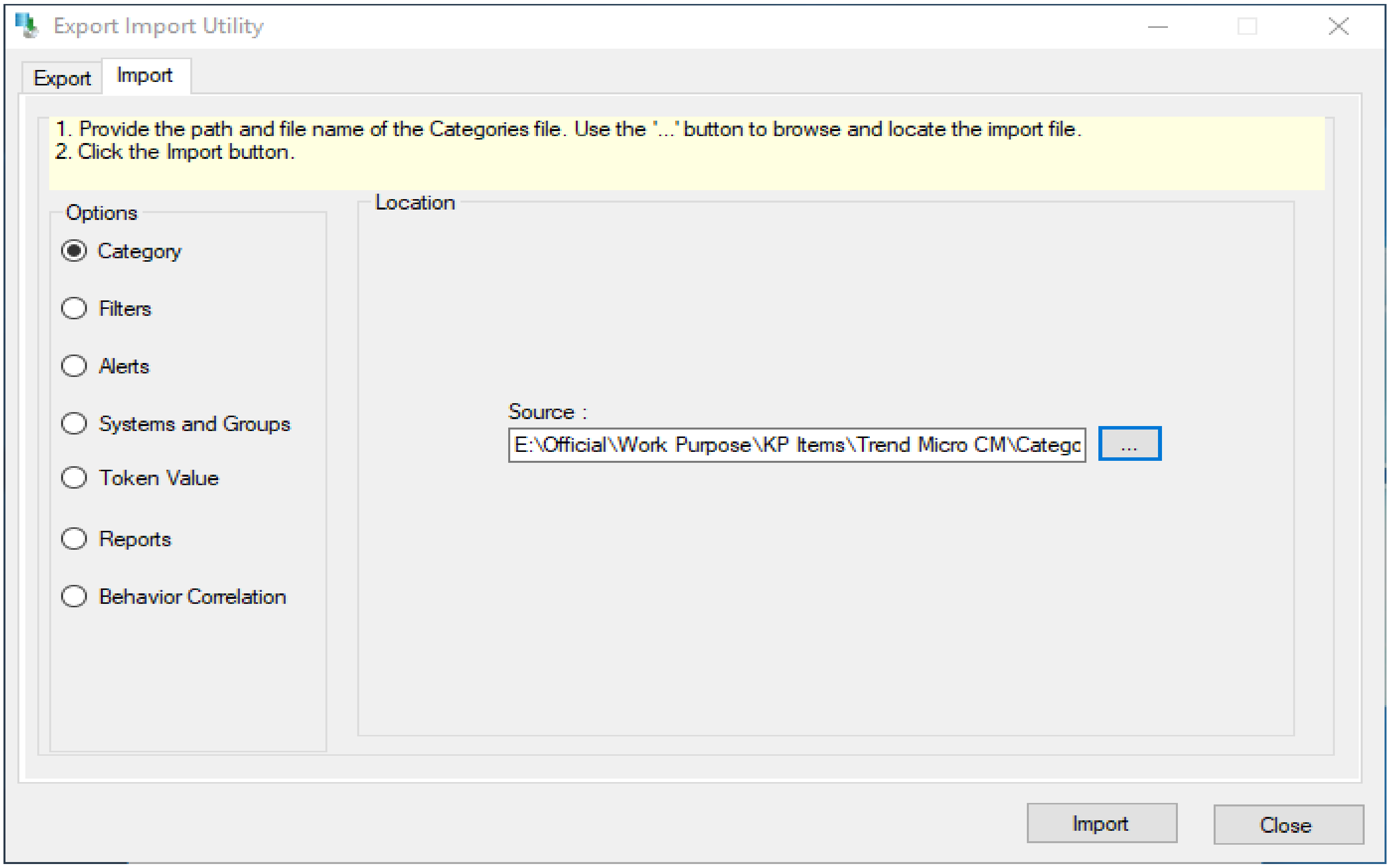


Figure 21

3. **Click** the Import tab**.**

Category

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



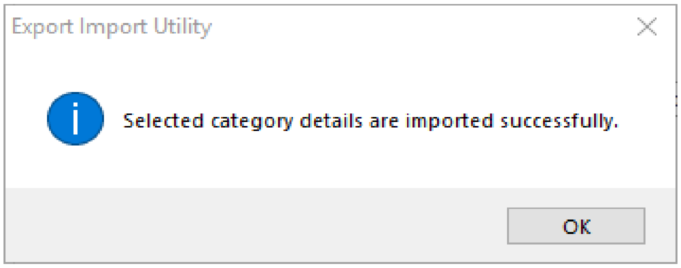
1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

● Category

Source : E:\Official\Work Purpose\KP Items\Trend Micro CM\Catego

Figure 22

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



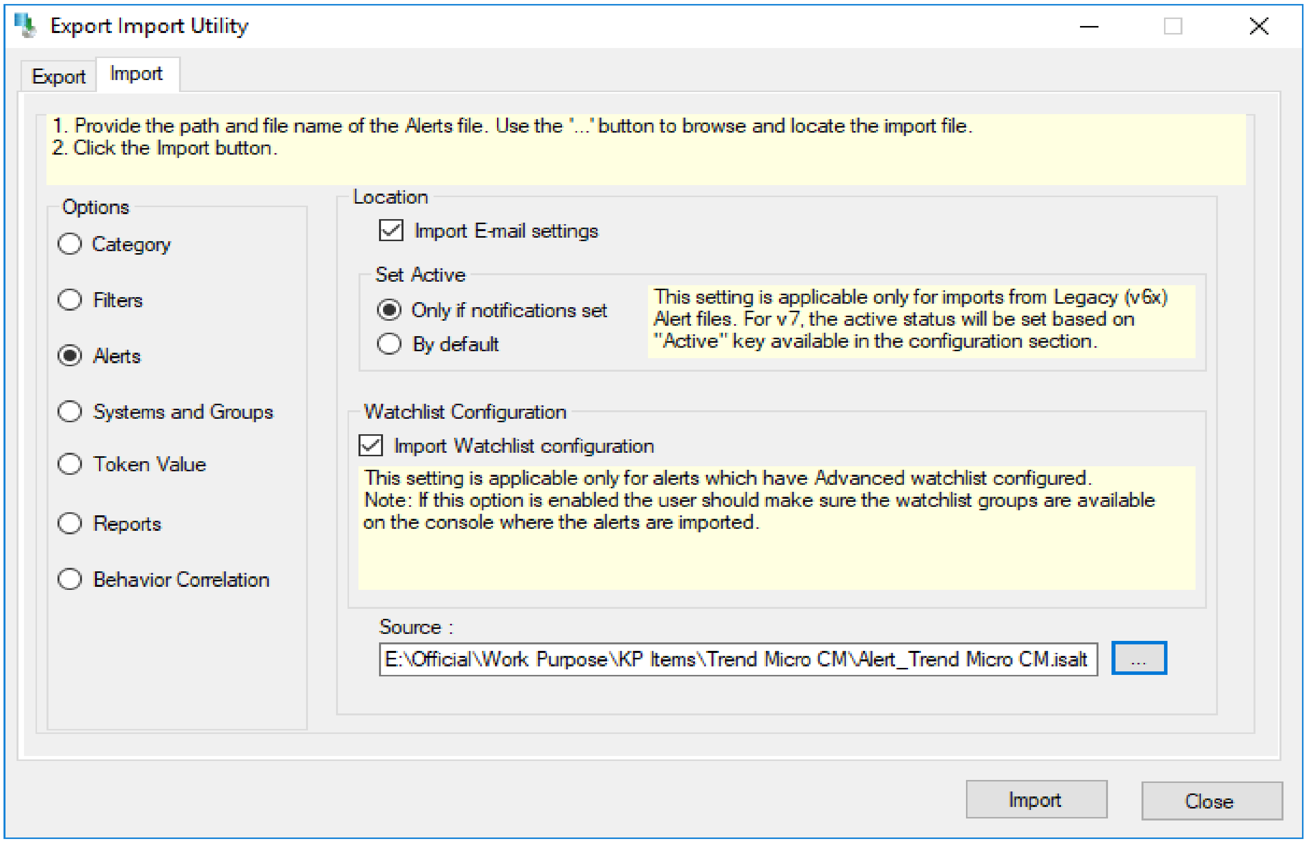
Selected category details are imported successfully.

Figure 23

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.

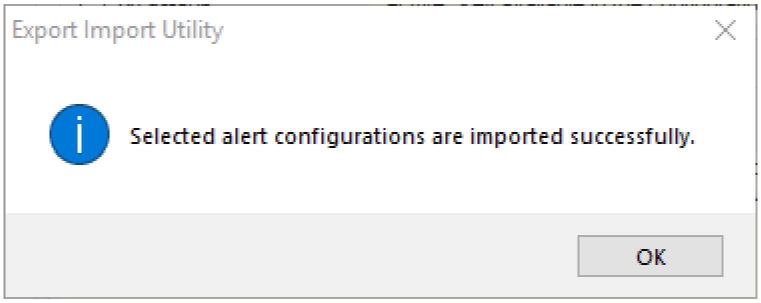
Watchlist Configuration
☑ Import Watchlist configuration

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\Trend Micro CM\Alert_Trend Micro CM.isalt

Figure 24

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



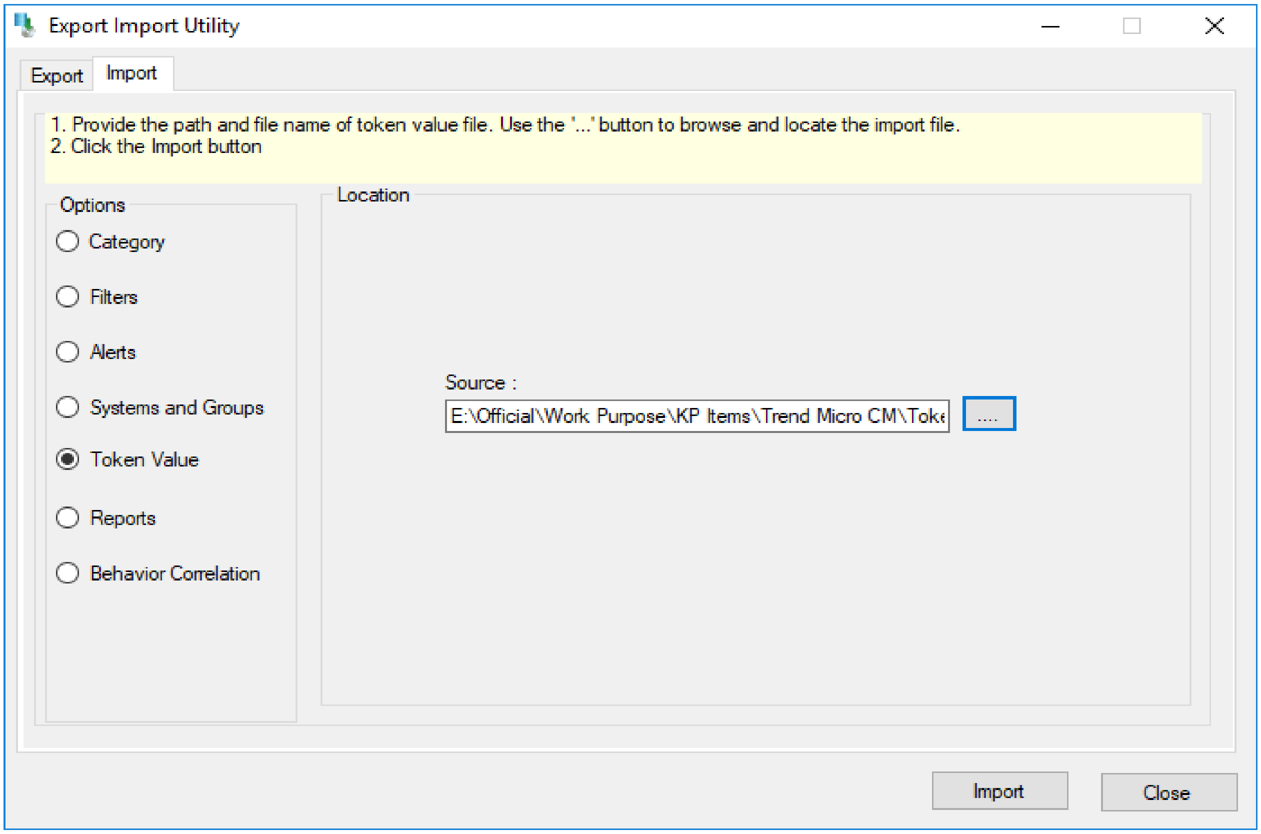
Selected alert configurations are imported successfully.

Figure 25

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

Parsing Rules

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



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

Source : E:\Official\Work Purpose\KP Items\Trend Micro CM\Toke

Figure 26

2. Locate **Token Value_Trend Micro CM.istoken** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

Knowledge Objects

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

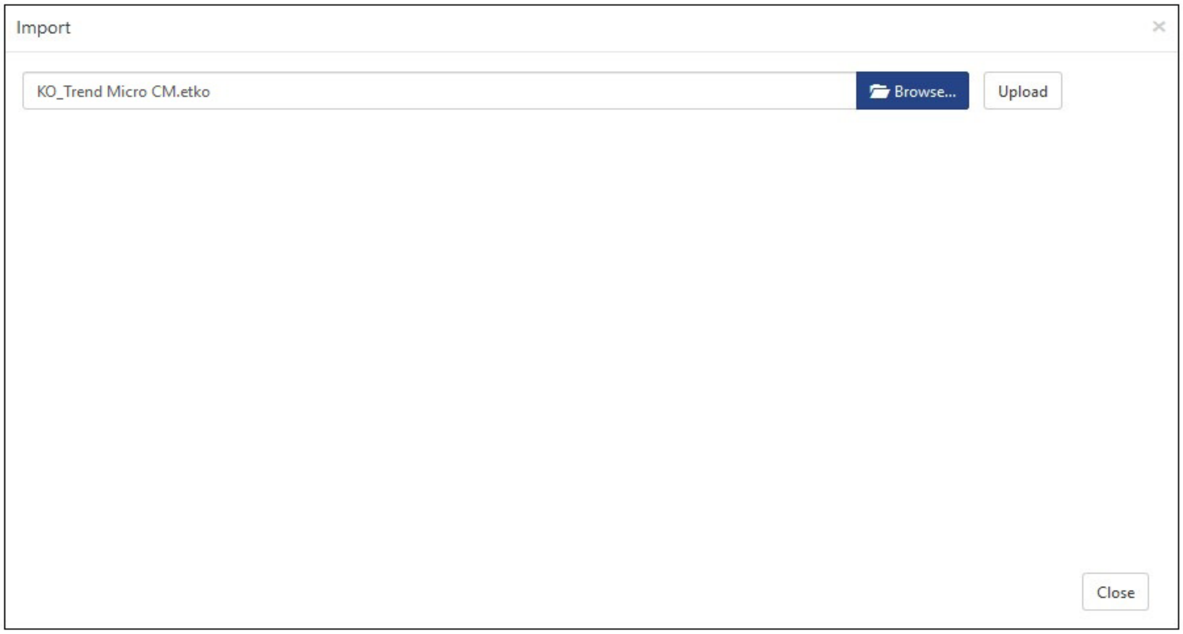
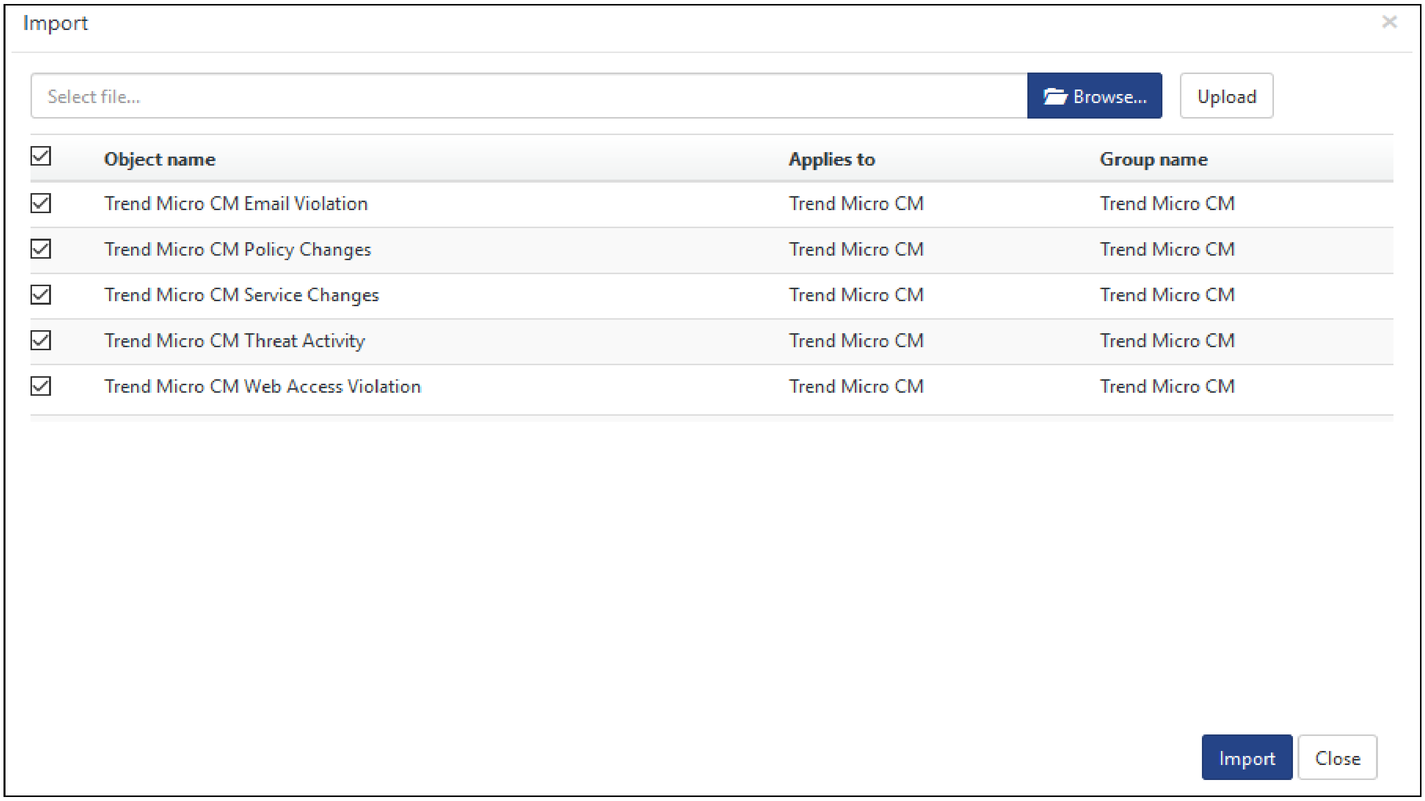


Figure 27

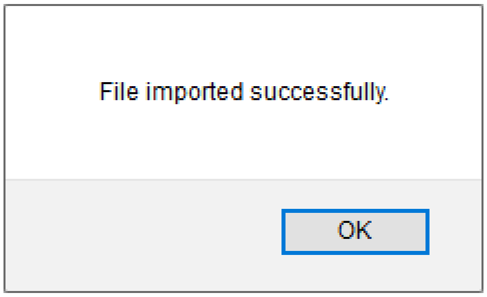
3. Click the ‘**Upload’** option.
4. Now select all the check box and then click on ‘**Import**’ option.



☑	Object name	Applies to	Group name
☑	Trend Micro CM Email Violation	Trend Micro CM	Trend Micro CM
☑	Trend Micro CM Policy Changes	Trend Micro CM	Trend Micro CM
☑	Trend Micro CM Service Changes	Trend Micro CM	Trend Micro CM
☑	Trend Micro CM Threat Activity	Trend Micro CM	Trend Micro CM
☑	Trend Micro CM Web Access Violation	Trend Micro CM	Trend Micro CM

Figure 28

5. Knowledge objects are now imported successfully.



File imported successfully.

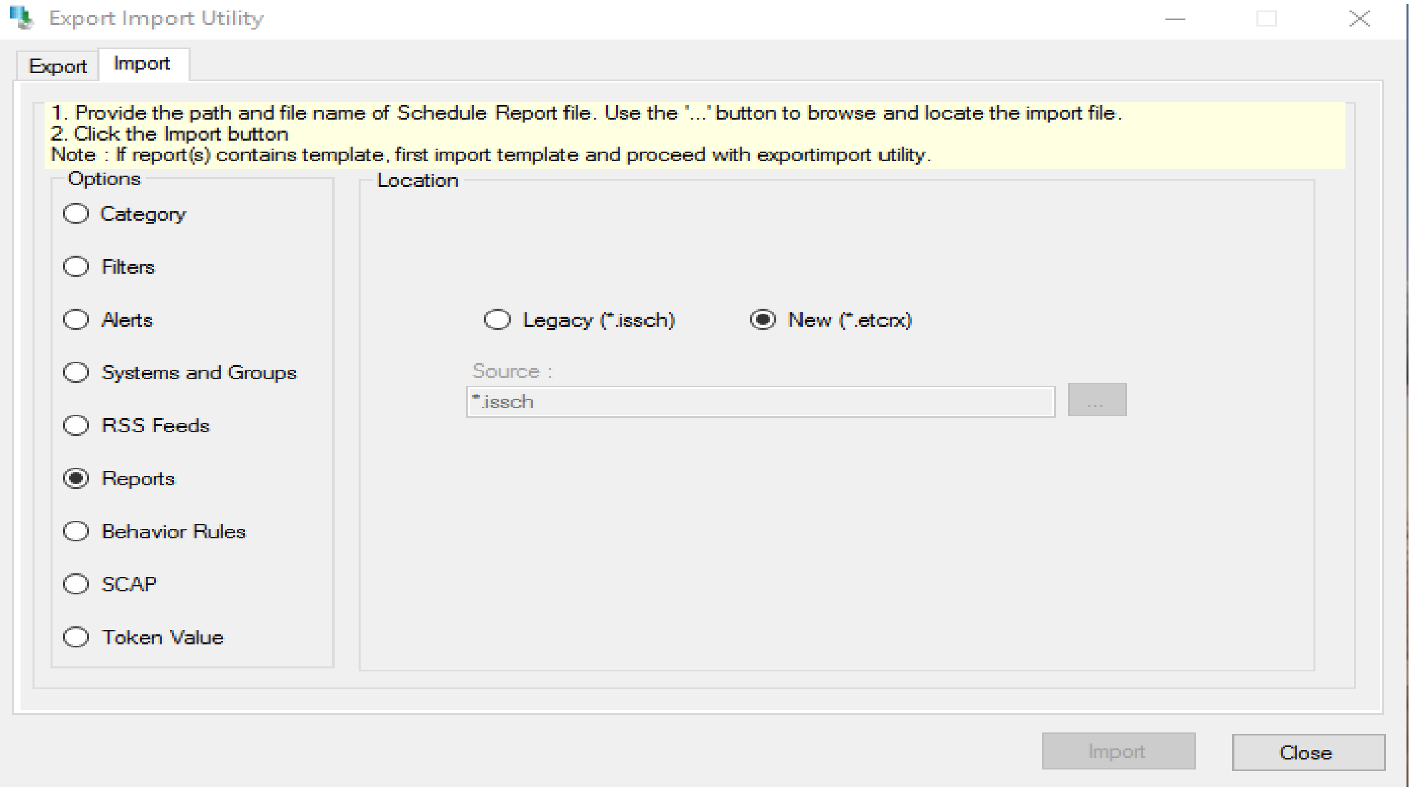
Figure 29

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

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

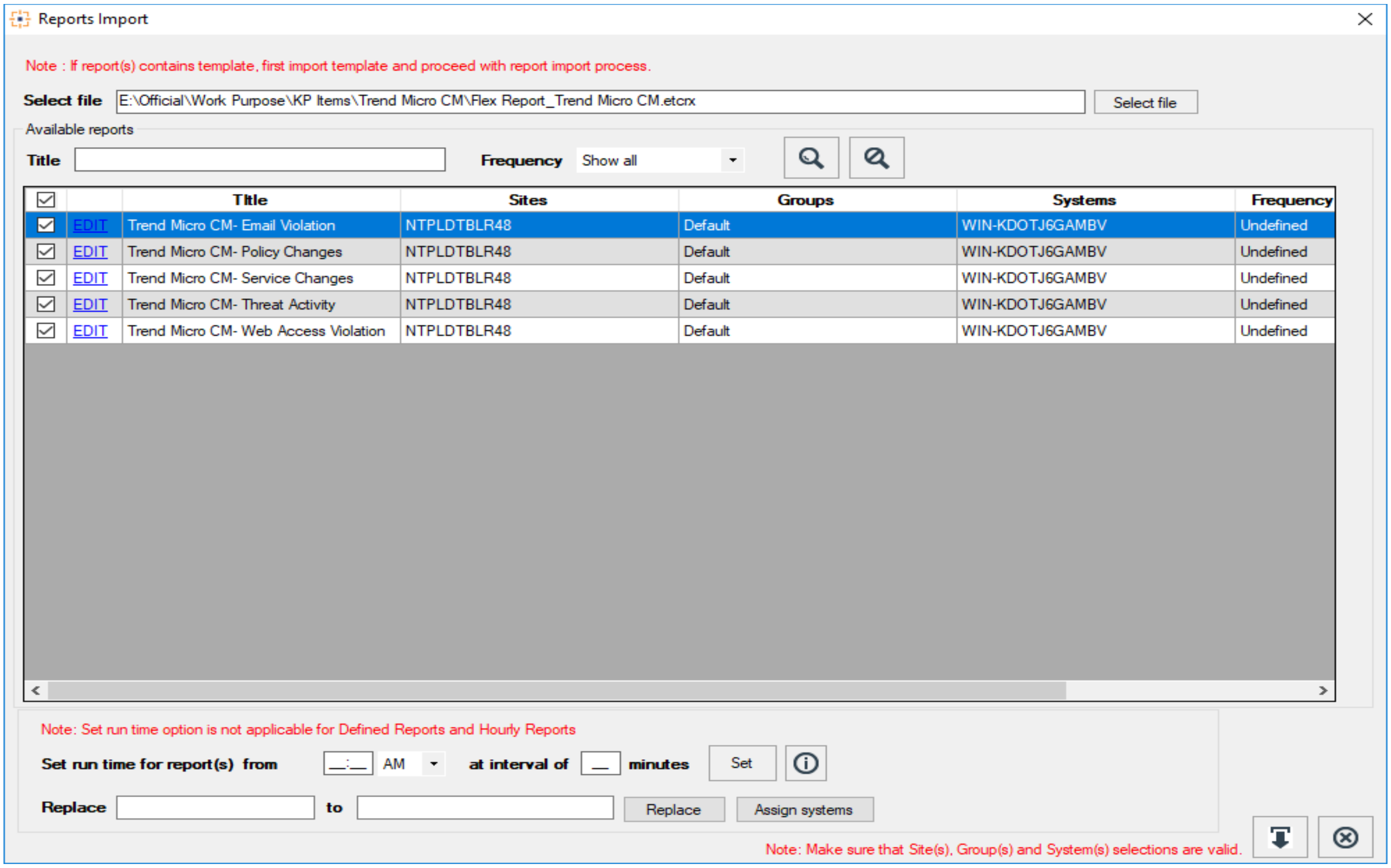
Location

○ Legacy (*.issch) ● New (*.etcrx)

Source : *.issch

Figure 30

2. Locate the **Flex Reports_Trend Micro CM.etcrx** file, and select all the check box.



Reports Import

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

Select file E:\Official\Work Purpose\KP Items\Trend Micro CM\Flex Report_Trend Micro CM.etcrx

Available reports

Title Frequency Show all

☑		Title	Sites	Groups	Systems	Frequency
☑	EDIT	Trend Micro CM- Email Violation	NTPLDTBLR48	Default	WIN-KDOTJ6GAMBV	Undefined
☑	EDIT	Trend Micro CM- Policy Changes	NTPLDTBLR48	Default	WIN-KDOTJ6GAMBV	Undefined
☑	EDIT	Trend Micro CM- Service Changes	NTPLDTBLR48	Default	WIN-KDOTJ6GAMBV	Undefined
☑	EDIT	Trend Micro CM- Threat Activity	NTPLDTBLR48	Default	WIN-KDOTJ6GAMBV	Undefined
☑	EDIT	Trend Micro CM- Web Access Violation	NTPLDTBLR48	Default	WIN-KDOTJ6GAMBV	Undefined

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

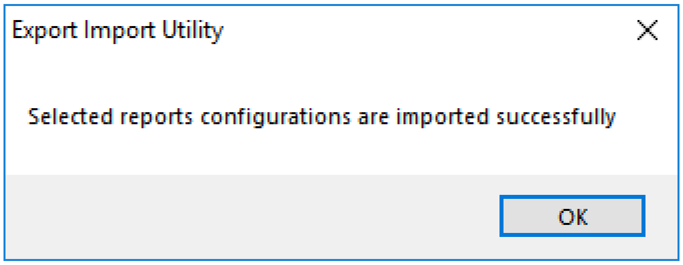
Set run time for report(s) from __:__ AM at interval of __ minutes

Replace to

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

Figure 31

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



Export Import Utility

Selected reports configurations are imported successfully

Figure 32

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

Dashboards

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

1. Open **EventTracker Enterprise**.

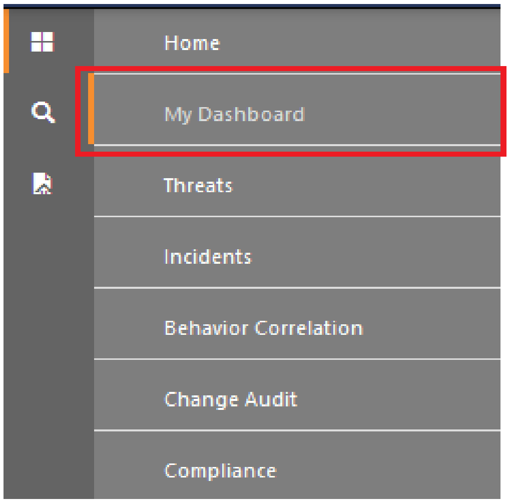
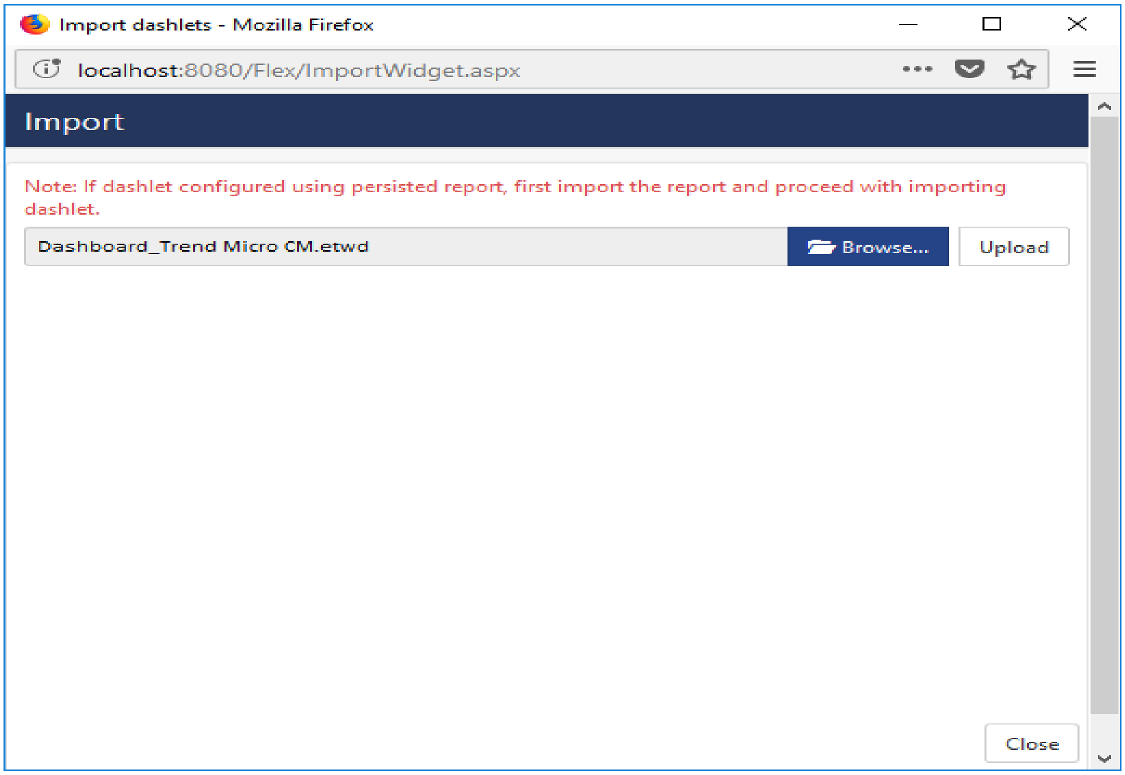


Figure 33

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

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

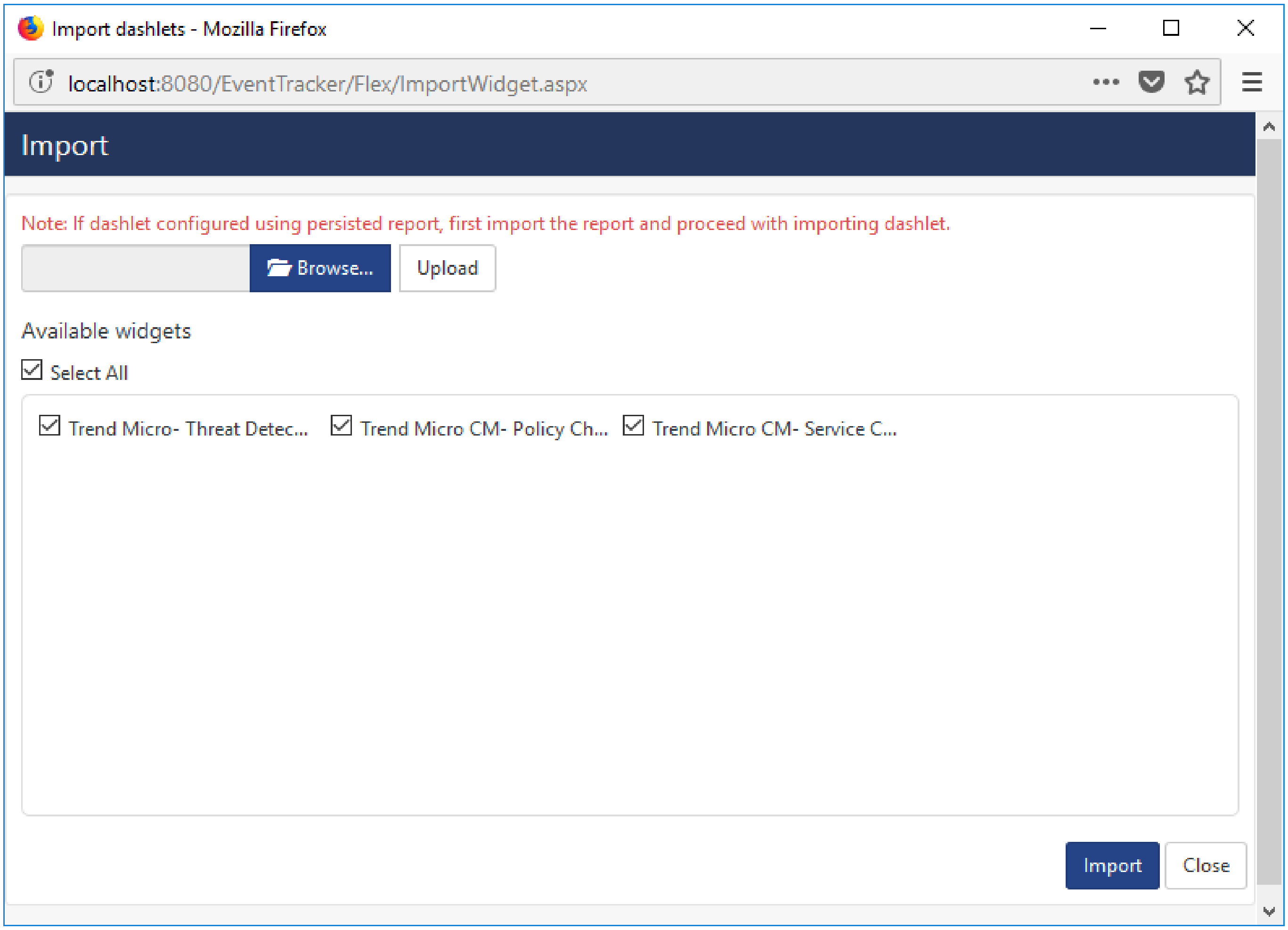

Import dashlets - Mozilla Firefox
localhost:8080/Flex/ImportWidget.aspx
Import

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

Dashboard_Trend Micro CM.etwd

Figure 34

4. Locate the **Dashboard_Trend Micro CM.etwd** file.
5. Click the **'Upload'** option.


Import dashlets - Mozilla Firefox
localhost:8080/EventTracker/Flex/ImportWidget.aspx
Import
Browse...
Upload
Import
Close

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

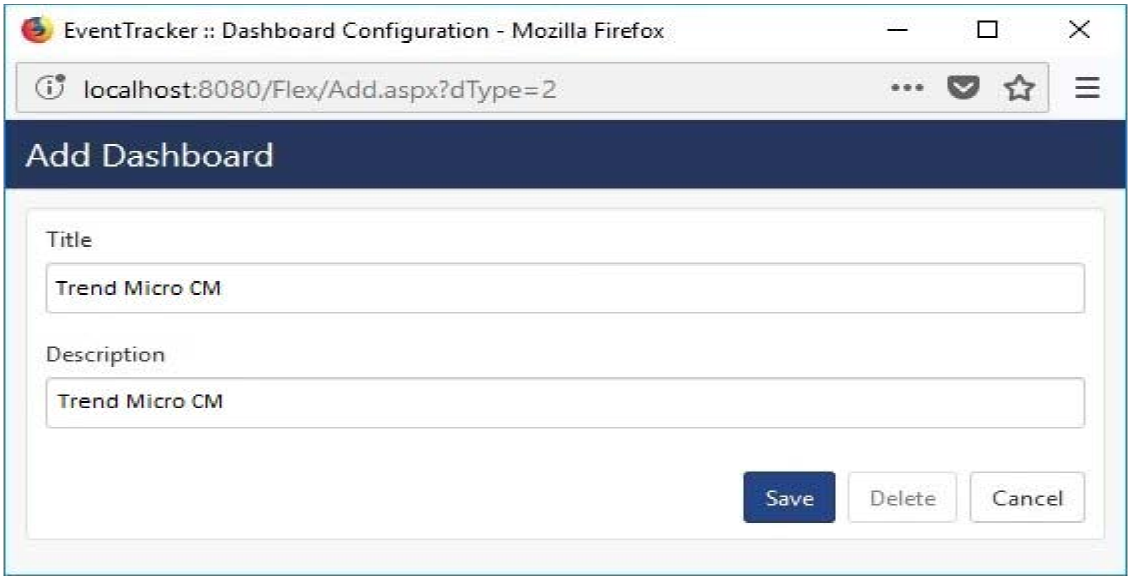
Available widgets

☑ Select All

☑ Trend Micro- Threat Detec... ☑ Trend Micro CM- Policy Ch... ☑ Trend Micro CM- Service C...

Figure 35

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 dashlet.



EventTracker :: Dashboard Configuration - Mozilla Firefox

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

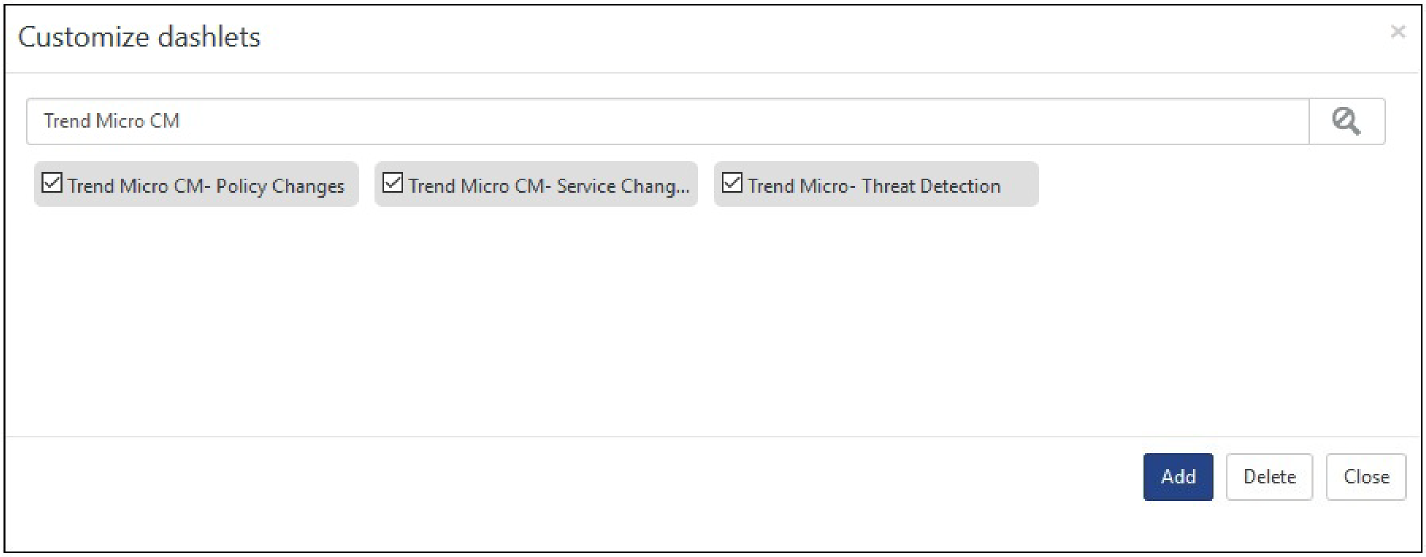
Add Dashboard

Title: Trend Micro CM

Description: Trend Micro CM

Figure 36

8. Fill suitable Title and Description and click **Save** button.
9. Click **'Customize'** to locate **Trend Micro CM** dashlets and choose all created dashlets for **Trend Micro CM** and choose all created dashlets.



Customize dashlets

Trend Micro CM

☑ Trend Micro CM- Policy Changes
☑ Trend Micro CM- Service Chang...
☑ Trend Micro- Threat Detection

Figure 37

10. Click **'Add'** dashlet to create dashboard.

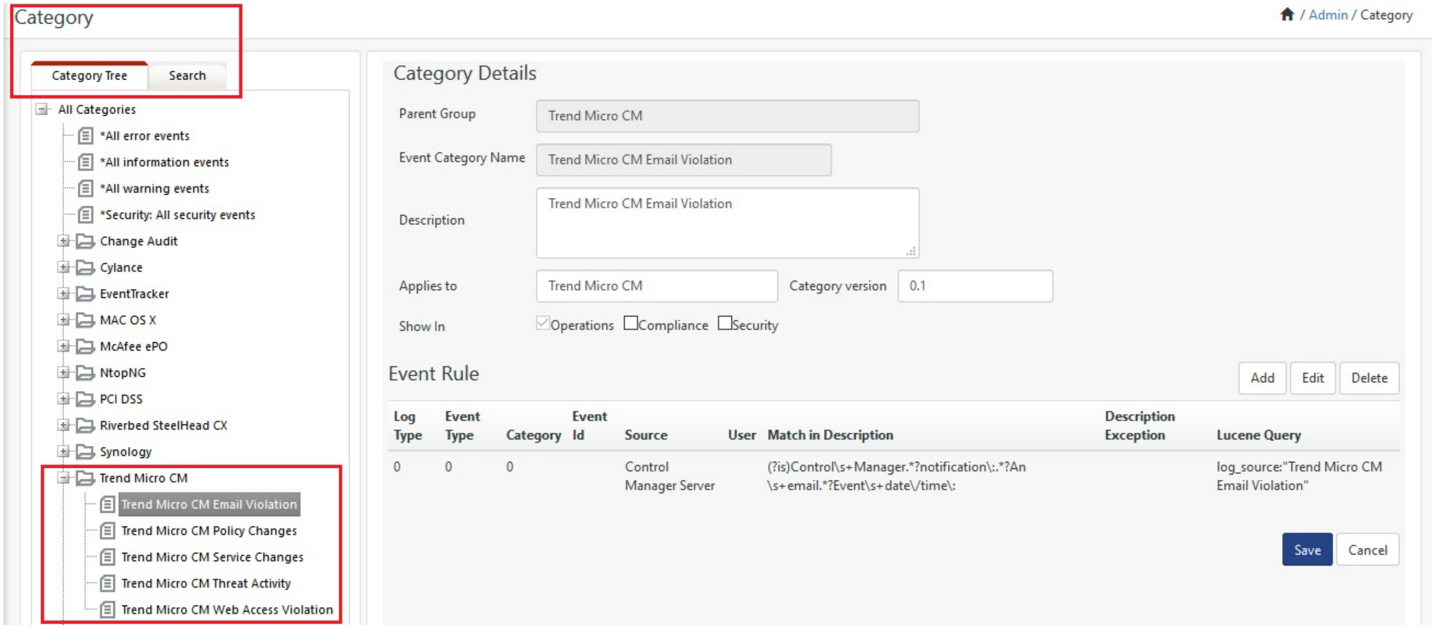
Verify Trend Micro CM knowledge pack in EventTracker

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 **Trend Micro CM** group folder to view the imported categories.



Category Details

Parent Group: Trend Micro CM

Event Category Name: Trend Micro CM Email Violation

Description: Trend Micro CM Email Violation

Applies to: Trend Micro CM

Category version: 0.1

Show In: ☑ Operations ☐ Compliance ☐ Security

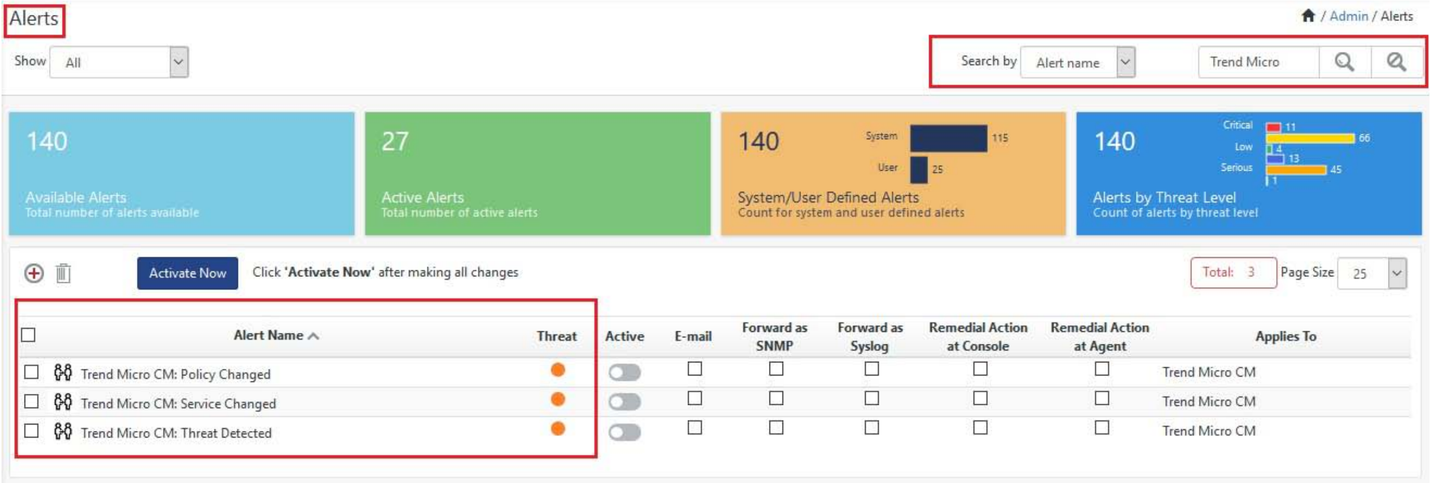
Event Rule

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception	Lucene Query
0	0	0		Control Manager Server		(?is)Control\s+Manager.*?notification\:.*?An \s+email.*?Event\s+date\/time\:		log_source:"Trend Micro CM Email Violation"

Figure 38

Alerts

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

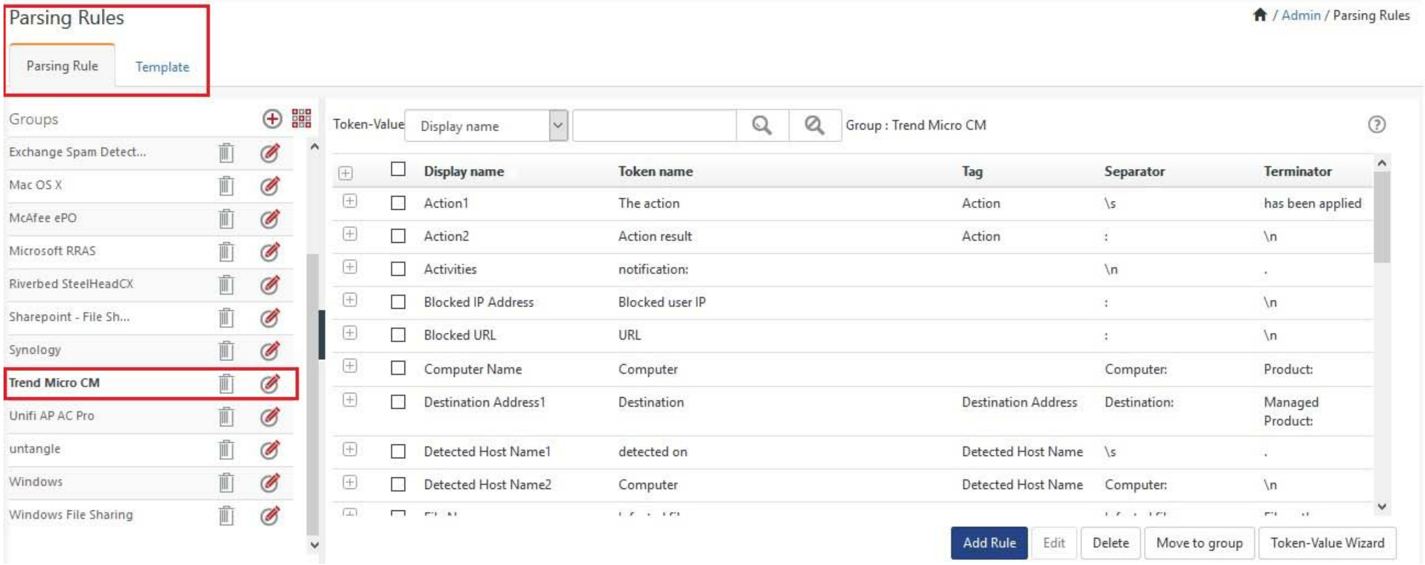

Alerts
/ Admin / Alerts
Show All
Search by Alert name
Trend Micro
140
Available Alerts
Total number of alerts available
27
Active Alerts
Total number of active alerts
140
System 115
User 25
System/User Defined Alerts
Count for system and user defined alerts
140
Critical 11
66
Low 4
13
Serious 45
1
Alerts 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
□	Trend Micro CM: Policy Changed	●		□	□	□	□	□	Trend Micro CM
□	Trend Micro CM: Service Changed	●		□	□	□	□	□	Trend Micro CM
□	Trend Micro CM: Threat Detected	●		□	□	□	□	□	Trend Micro CM

Figure 39

Parsing Rules

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

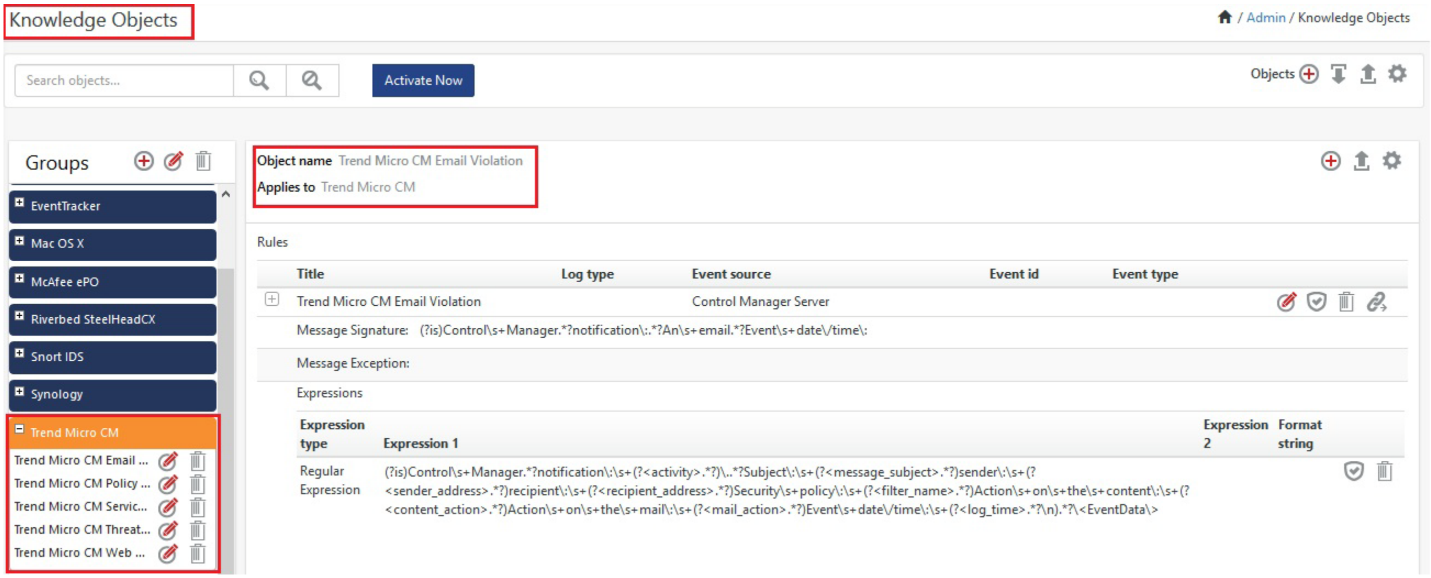


□	Display name	Token name	Tag	Separator	Terminator
□	Action1	The action	Action	\s	has been applied
□	Action2	Action result	Action	:	\n
□	Activities	notification:		\n	.
□	Blocked IP Address	Blocked user IP		:	\n
□	Blocked URL	URL		:	\n
□	Computer Name	Computer		Computer:	Product:
□	Destination Address1	Destination	Destination Address	Destination:	Managed Product:
□	Detected Host Name1	detected on	Detected Host Name	\s	.
□	Detected Host Name2	Computer	Detected Host Name	Computer:	\n

Figure 40

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 **Trend Micro CM** group folder to view the imported Knowledge objects.



Knowledge Objects

/ Admin / Knowledge Objects

Search objects...

Activate Now

Objects

Groups

- EventTracker
- Mac OS X
- McAfee ePO
- Riverbed SteelHeadCX
- Snort IDS
- Synology
- Trend Micro CM
  - Trend Micro CM Email ...
  - Trend Micro CM Policy ...
  - Trend Micro CM Servic...
  - Trend Micro CM Threat...
  - Trend Micro CM Web ...

Object name Trend Micro CM Email Violation

Applies to Trend Micro CM

Rules

Title	Log type	Event source	Event id	Event type
Trend Micro CM Email Violation		Control Manager Server		

Message Signature: (?is)Control\s+Manager.*?notification\:.*?An\s+email.*?Event\s+date\/time\:

Message Exception:

Expressions

Expression type	Expression 1	Expression 2	Format string
Regular Expression	(?is)Control\s+Manager.*?notification\:\s+(?<activity>.*?)\..*?Subject\:\s+(?<message_subject>.*?)sender\:\s+(?<sender_address>.*?)recipient\:\s+(?<recipient_address>.*?)Security\s+policy\:\s+(?<filter_name>.*?)Action\s+on\s+the\s+content\:\s+(?<content_action>.*?)Action\s+on\s+the\s+mail\:\s+(?<mail_action>.*?)Event\s+date\/time\:\s+(?<log_time>.*?\n).*?\<EventData\>		

Figure 41

Flex Reports

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

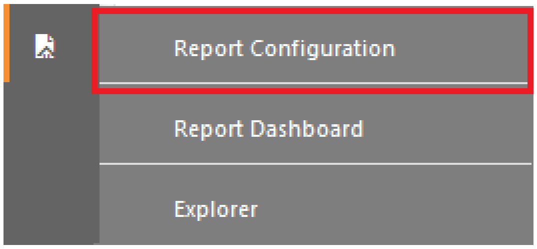
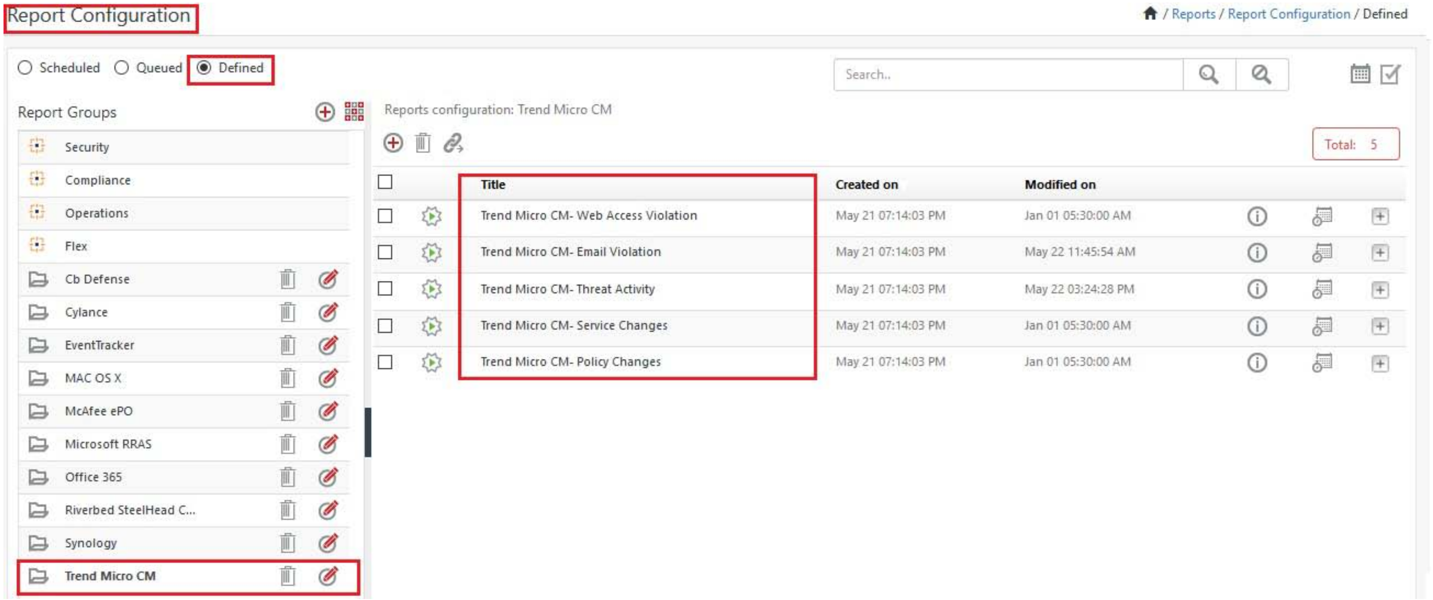


Figure 42

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



Report Configuration

/ Reports / Report Configuration / Defined

○ Scheduled ○ Queued ● Defined

Search..

Report Groups

- Security
- Compliance
- Operations
- Flex
- Cb Defense
- Cylance
- EventTracker
- MAC OS X
- McAfee ePO
- Microsoft RRAS
- Office 365
- Riverbed SteelHead C...
- Synology
- Trend Micro CM

Reports configuration: Trend Micro CM

Total: 5

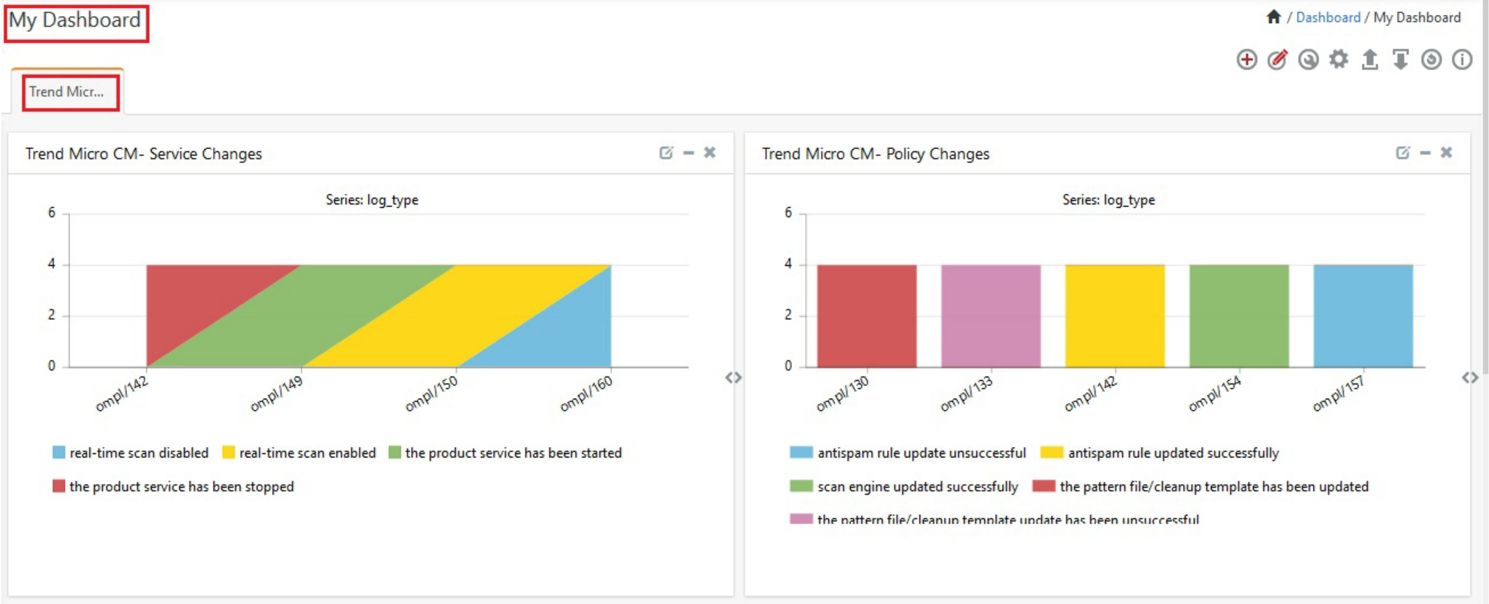
□		Title	Created on	Modified on
□		Trend Micro CM- Web Access Violation	May 21 07:14:03 PM	Jan 01 05:30:00 AM
□		Trend Micro CM- Email Violation	May 21 07:14:03 PM	May 22 11:45:54 AM
□		Trend Micro CM- Threat Activity	May 21 07:14:03 PM	May 22 03:24:28 PM
□		Trend Micro CM- Service Changes	May 21 07:14:03 PM	Jan 01 05:30:00 AM
□		Trend Micro CM- Policy Changes	May 21 07:14:03 PM	Jan 01 05:30:00 AM

Figure 43

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

Trend Micr...

Trend Micro CM- Service Changes

Series: log_type
6
4
2
0
ompl/142
ompl/149
ompl/150
ompl/160
🟦 real-time scan disabled
🟨 real-time scan enabled
🟩 the product service has been started
🟥 the product service has been stopped

Trend Micro CM- Policy Changes

Series: log_type
6
4
2
0
ompl/130
ompl/133
ompl/142
ompl/154
ompl/157
🟦 antispam rule update unsuccessful
🟨 antispam rule updated successfully
🟩 scan engine updated successfully
🟥 the pattern file/cleanup template has been updated
🟪 the pattern file/cleanup template update has been unsuccessful

Figure 44

Sample Flex Dashboards

1. **Trend Micro CM- Threat detection**: This dashboard provides information related to threats detected on systems.

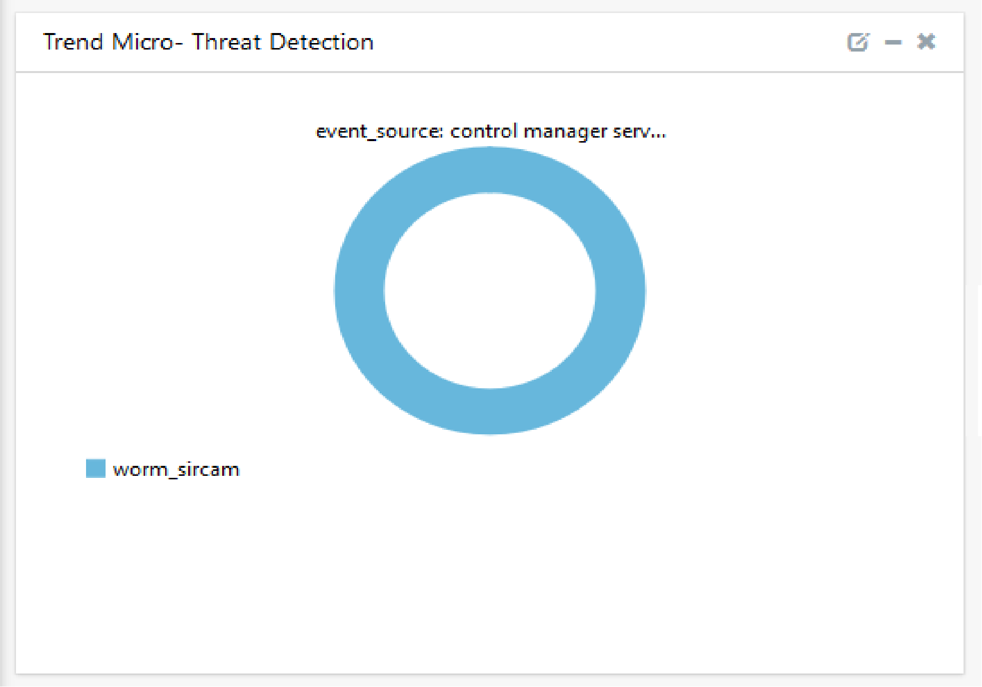

Trend Micro- Threat Detection
event_source: control manager serv...
worm_sircam

Figure 45

2. **Trend Micro CM- Policy Changes**: This dashboard provides information related to policy changes.

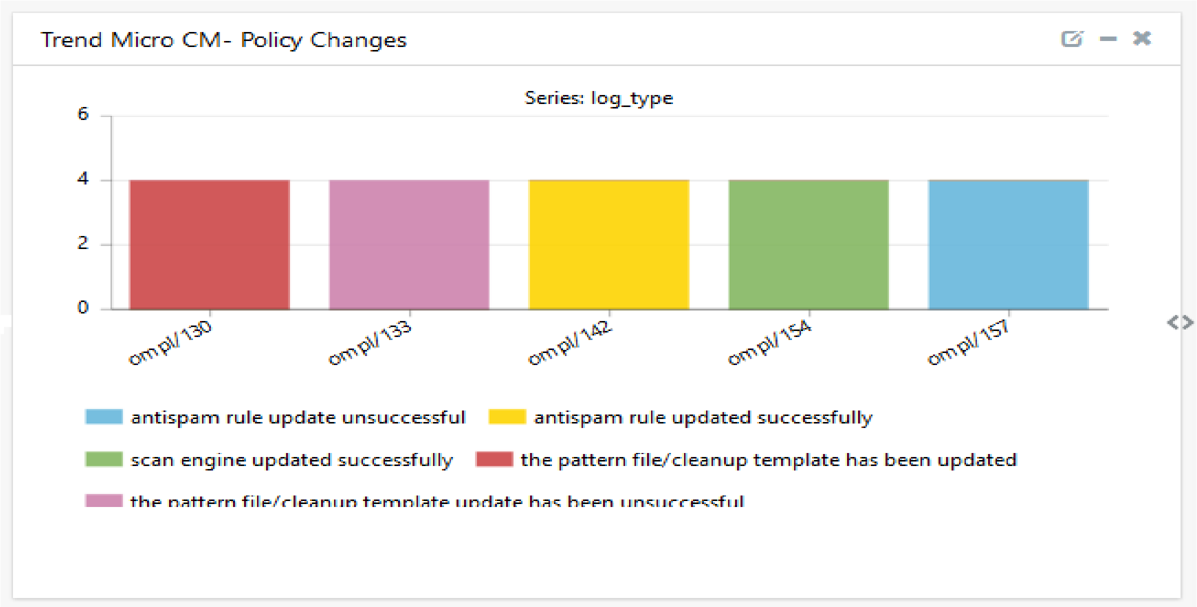

Trend Micro CM- Policy Changes
Series: log_type
6
4
2
0
om pl/130
om pl/133
om pl/142
om pl/154
om pl/157
antispam rule update unsuccessful
antispam rule updated successfully
scan engine updated successfully
the pattern file/cleanup template has been updated
the pattern file/cleanup template update has been unsuccessful

Figure 46

3. **Trend Micro CM- Service Changes**: This dashboard provides information related to service changes.

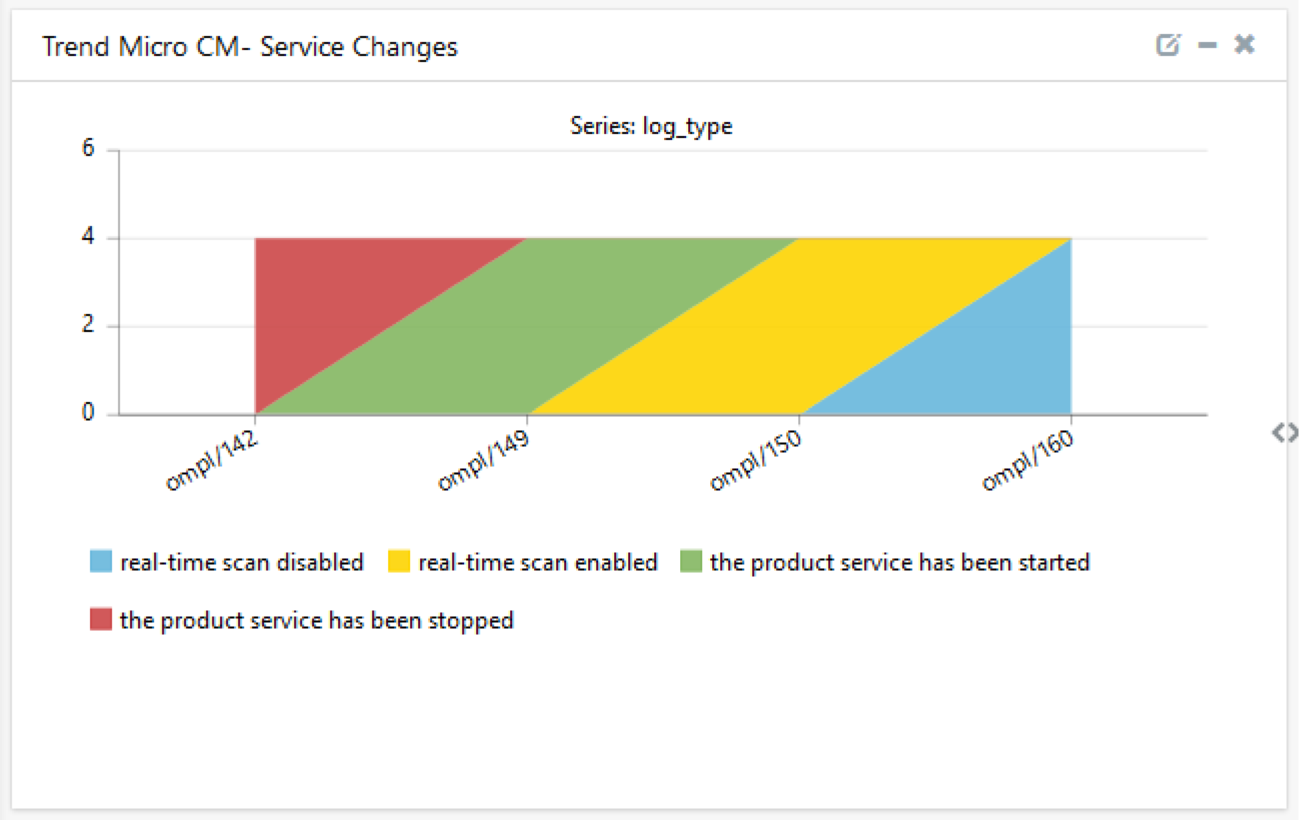

Trend Micro CM- Service Changes
Series: log_type
6
4
2
0
ompl/142
ompl/149
ompl/150
ompl/160
real-time scan disabled
real-time scan enabled
the product service has been started
the product service has been stopped

Figure 47