# Integrate Trend Micro Web Security with EventTracker

## EventTracker v9.2 and later

Publication Date: February 3, 2021

# Abstract

This guide provides instructions to retrieve the **Trend Micro Web Security (cloud) via syslog logging**. Once the logs start coming-in into EventTracker, reports, dashboards, alerts and saved searches can be configured.

# Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Trend Micro Web Security (cloud).**

# Audience

Administrators who are assigned the task to monitor **Trend Micro Web Security (cloud)** events using EventTracker.

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

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

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

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

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

# Table of Contents

# 1. Overview

Trend Micro Web Security (TMWS) provides users with forward-looking threat protection on web threats, URL filtering, and application control, etc. It uses cross-generational defenses to detect known and unknown threats while providing visibility and access control. The deployment model provides flexibility to deploy gateways on-premises, in the cloud or both - protecting users. It also provides a single cloud-based management console which allows to customize policy, manage users, and access reports through a single panel.

Trend Micro Web Security integrates with EventTracker SIEM application to give security analytics, with deep data context so that organizations can be confident in their data security strategy. Benefits include, scheduled reports, Integrated TMWS dashboards and alerts for streamlined investigation.

Reports are the best to view the historical data (depending on the timeline defined). Some of the reports provided by EventTracker for TMWS are audit activities summary such as, user or group management, or login and logout, gateway related activities summary, such as dropping or discarding or analyzing a traffic.

Dashboards are the graphical representations of activities occurring in TMWS. These dashboards can be a pie chart, a bar diagram, or even a map. This allows user to view the key highlights of TMWS events. Some of the dashboards includes, audit events timeline, UI login activities, dropped traffic by country code, etc.

Alerts such as, suspicious URL/Domains have been Identified, are included in the knowledge packs. These alerts can be configured to forward emails to users/admin of TMWS as soon as any suspicious events are detected.

# 2. Prerequisites

- EventTracker v9.2 and above should be installed.
- Administrative/root access to Trend Micro Web Security management UI.

# 3. Integrating TMWS with EventTracker

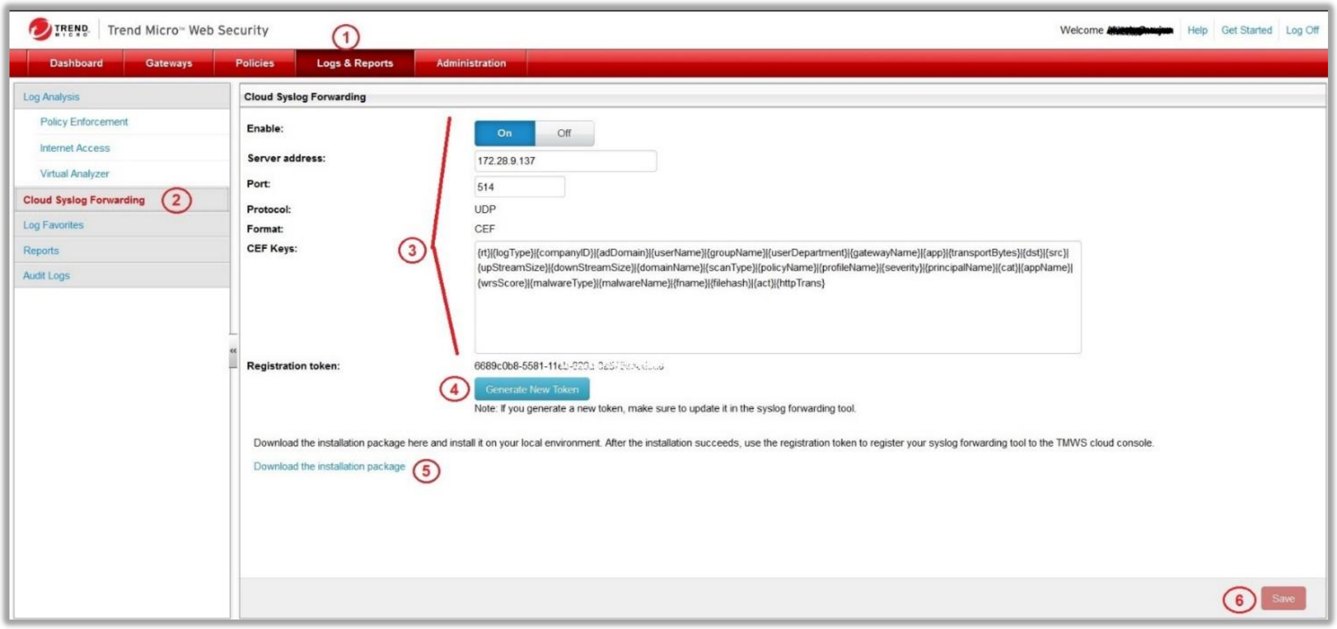
TMWS allows administrators to configure a syslog server and install a syslog forwarding tool to push access logs and audit logs in the TMWS cloud to syslog server.

## 3.1 Configuring Syslog forwarding

Login to your Trend Micro Web Security admin console.

1. Navigate to **Logs & Reports**.

2. From the left side panel, select **Cloud Syslog Forwarding**.
3. Specify the following parameters:
    a. Click **On** to enable syslog forwarding.
    b. **Server address**: IP address or FQDN of the EventTracker syslog server.
    c. **Port**: Port number of the syslog server. E.g. port 514.
    d. **Protocol**: Protocol to be used to transport logs to the syslog server. UDP is default.
    e. **Format**: Format in which event logs are sent to the syslog server. CEF is default.
    f. **CEF keys**: CEF keys you want to add in syslog messages. Let the default format be as it is.
4. **Registration token**: Generate a new token and save it. This is required in the syslog forwarding tool.
5. **Next,** Download the syslog forwarding tool.
6. Click on **Save**.



Cloud Syslog Forwarding

Enable: ● On ○ Off

Server address: 172.28.9.137

Port: 514

Protocol: UDP

Format: CEF

CEF Keys: {rt}|{logType}|{companyID}|{adDomain}|{userName}|{groupName}|{userDepartment}|{gatewayName}|{app}|{transportBytes}|{dst}|{src}|{upStreamSize}|{downStreamSize}|{domainName}|{scanType}|{policyName}|{profileName}|{severity}|{principalName}|{cat}|{appName}|{wrsScore}|{malwareType}|{malwareName}|{fname}|{filehash}|{act}|{httpTrans}

Registration token: 6689c0b8-5581-11e[redacted]

Generate New Token

Note: If you generate a new token, make sure to update it in the syslog forwarding tool.

Download the installation package here and install it on your local environment. After the installation succeeds, use the registration token to register your syslog forwarding tool to the TMWS cloud console.

Download the installation package

Save

Figure 1

## 3.2 Installing the Syslog forwarding Tool

Pre-requisites for installing syslog forwarding tool:

- TMWS supports the following environments for the syslog forwarding tool: VMware 6.5 and 6.7.
- Minimum system requirements:
    - **CPU**: 2 cores, 2 threads
    - **RAM**: 4 GB
    - **Disk size**: 50 GB (for installation)

1. Install the ISO file we downloaded from the TMWS management console, and upload it to the ESXi server you use to create a VM for the installation.
2. Follow the guide to install a new virtual machine.
3. You have created a new virtual machine, power on the machine and on the **TMWS Syslog Tool Installation Menu** screen, select Install **TMWS Syslog Forwarding Tool (EN)**.
4. View the disk information to use for the installation and click **Continue**.
5. On the **Hardware Profile** screen that appears, view the hardware settings for the syslog forwarding tool and click **Continue**.
6. On the **Repartition Disks** warning screen, click **Continue**.
7. Wait a few minutes until the installation is completed. (The system will reboot automatically.)
8. Log in to the machine as the **root** user through the command console, and press **Enter** to set a password.
9. Run the following command after you first log in: **clish**
10. Run the following command to enter the privileged mode: **enable**
11. Run the following command to configure basic network settings: **configure network basic**
    a. **Host name**: The host name of the VM.
    b. **Data interface**: The NIC used by the syslog forwarding tool to transmit data. The default value is eth0.
    c. **Method**: Whether to use static or dynamic IP address assignment. Continue to configure the following based on the method you select.
        i. **static**: IPv4 address, IPv4 subnet mask, IPv4 gateway, preferred DNS, and alternate DNS (optional)
        ii. **dhcp**: Preferred DNS and alternate DNS (optional).
12. Type **Y** or **y** to confirm the settings and restart the machine.
13. Log in to the machine through the command console as the root user.
14. Run the following command: **/usr/logsvc/logoffloadClient/switch.py –t <token>**

    **Note:** <token> is the registration token that you can get on the management console.

# 4. EventTracker Knowledge Packs

## 4.1 Saved Searches

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

- **TMWS - Audit Logs** – This category of saved searches allow user to extract the events that are specific to admin or operational activities in TMWS web console. Such as, login logout, user create/ delete, gateway add/remove, etc.

- **TMWS - Gateway Logs** – This category of saved searches allow user to extract the events that are specific to web traffic within the gateways that are configured in TMWS. Such as, allowed traffic, denied traffic, analyze traffic, etc.

## 4.2 Alerts

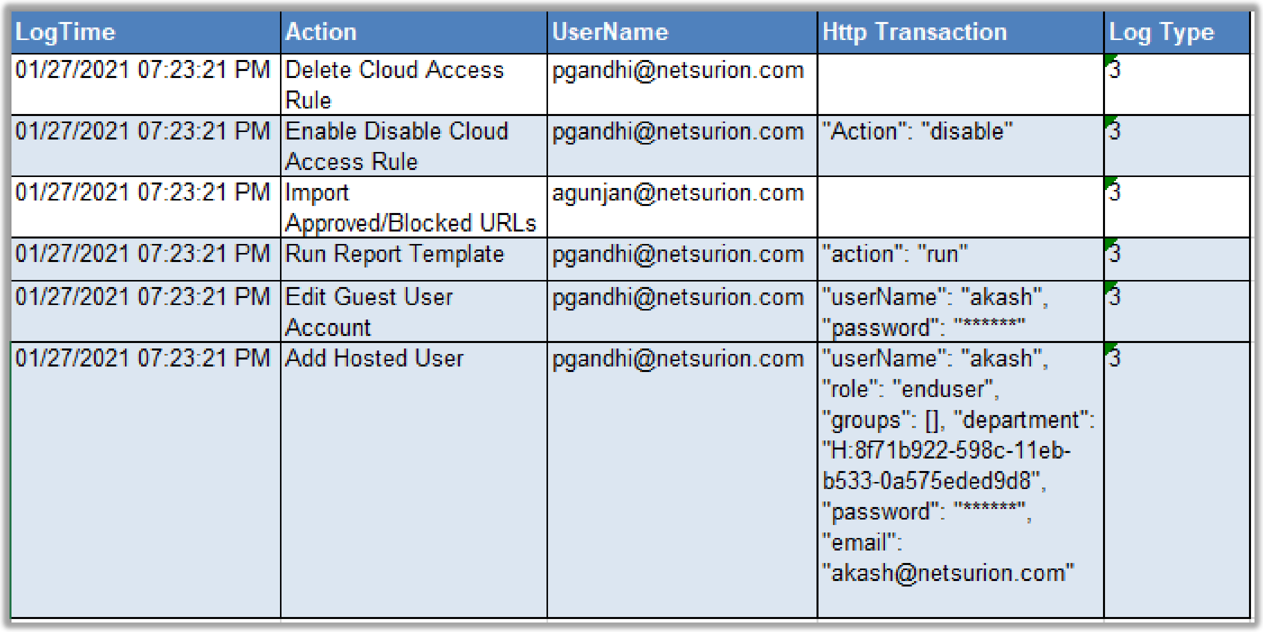
Alerts are triggered when an event received is identified as critical and requires immediate notification. Such as,

- **TMWS: Suspicious URL/Domains have been Identified** – This alert is triggered by EventTracker as it receives events that are either associated with gateway traffic labelled as drop, analyze, or warn**.**

## 4.3 Reports

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

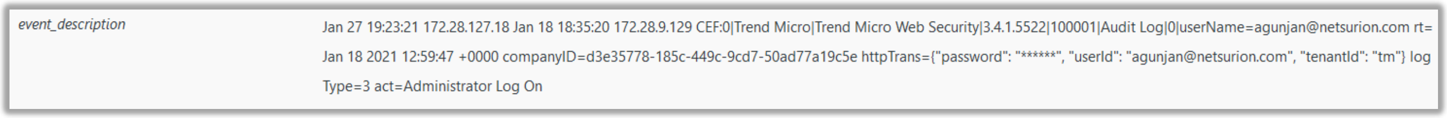
- **TMWS - Audit activities** - This report allows user to extract the detailed summary of events that are specific to admin or operational activities in TMWS web console. Such as, login logout, user create/ delete, gateway add/remove, etc. It contains, username, action type, log datetime, etc.



| LogTime | Action | UserName | Http Transaction | Log Type |
|---|---|---|---|---|
| 01/27/2021 07:23:21 PM | Delete Cloud Access Rule | pgandhi@netsurion.com | | 3 |
| 01/27/2021 07:23:21 PM | Enable Disable Cloud Access Rule | pgandhi@netsurion.com | "Action": "disable" | 3 |
| 01/27/2021 07:23:21 PM | Import Approved/Blocked URLs | agunjan@netsurion.com | | 3 |
| 01/27/2021 07:23:21 PM | Run Report Template | pgandhi@netsurion.com | "action": "run" | 3 |
| 01/27/2021 07:23:21 PM | Edit Guest User Account | pgandhi@netsurion.com | "userName": "akash", "password": "******" | 3 |
| 01/27/2021 07:23:21 PM | Add Hosted User | pgandhi@netsurion.com | "userName": "akash", "role": "enduser", "groups": [], "department": "H:8f71b922-598c-11eb-b533-0a575eded9d8", "password": "******", "email": "akash@netsurion.com" | 3 |

Figure 2

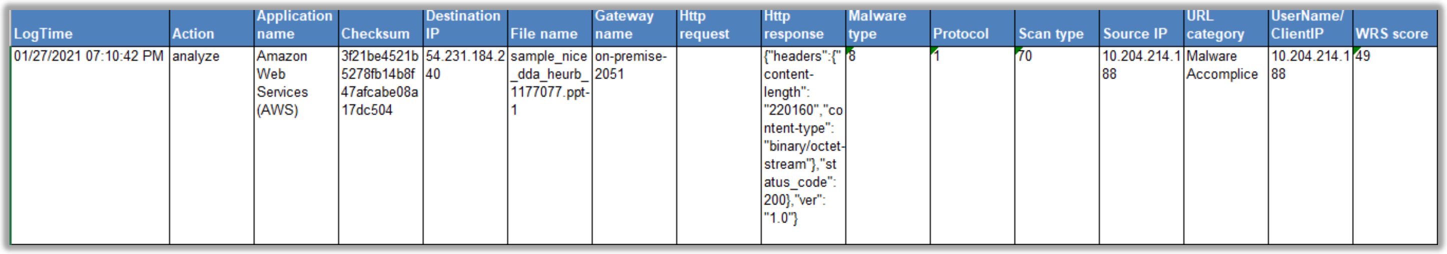
**Logs considered**:



```
event_description    Jan 27 19:23:21 172.28.127.18 Jan 18 18:35:20 172.28.9.129 CEF:0|Trend Micro|Trend Micro Web Security|3.4.1.5522|100001|Audit Log|0|userName=agunjan@netsurion.com rt=
                     Jan 18 2021 12:59:47 +0000 companyID=d3e35778-185c-449c-9cd7-50ad77a19c5e httpTrans={"password": "******", "userId": "agunjan@netsurion.com", "tenantId": "tm"} log
                     Type=3 act=Administrator Log On
```

Figure 3

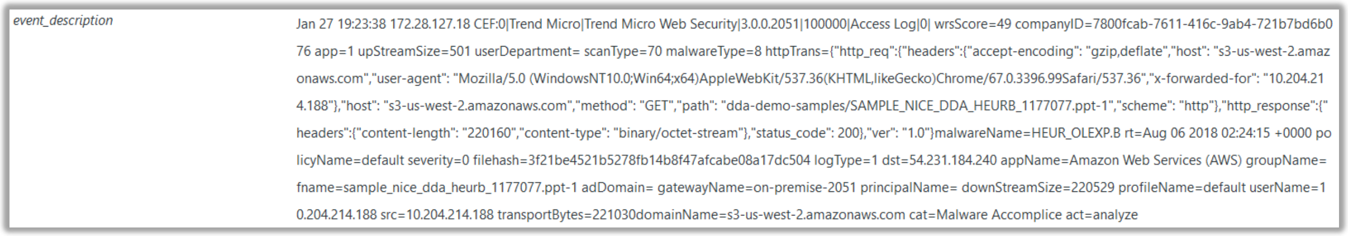
- **TMWS - Gateway Activities** - This report allows user to extract the detailed summary of events that are specific to web traffic within the gateways that are configured in TMWS. Such as, allowed traffic, denied traffic, analyze traffic, etc. It contains, action type, http request, http response, protocol type, log datetime, WRS score, etc.



| LogTime | Action | Application name | Checksum | Destination IP | File name | Gateway name | Http request | Http response | Malware type | Protocol | Scan type | Source IP | URL category | UserName/ ClientIP | WRS score |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01/27/2021 07:10:42 PM | analyze | Amazon Web Services (AWS) | 3f21be4521b5278fb14b8f47afcabe08a17dc504 | 54.231.184.240 | sample_nice_dda_heurb_1177077.ppt-1 | on-premise-2051 | | {"headers":{"content-length": "220160","content-type": "binary/octet-stream"},"status_code": 200},"ver": "1.0"} | 8 | 1 | 70 | 10.204.214.188 | Malware Accomplice | 10.204.214.188 | 49 |

Figure 4

**Logs considered**:



```
event_description    Jan 27 19:23:38 172.28.127.18 CEF:0|Trend Micro|Trend Micro Web Security|3.0.0.2051|100000|Access Log|0| wrsScore=49 companyID=7800fcab-7611-416c-9ab4-721b7bd6b0
                     76 app=1 upStreamSize=501 userDepartment= scanType=70 malwareType=8 httpTrans={"http_req":{"headers":{"accept-encoding": "gzip,deflate","host": "s3-us-west-2.amaz
                     onaws.com","user-agent": "Mozilla/5.0 (WindowsNT10.0;Win64;x64)AppleWebKit/537.36(KHTML,likeGecko)Chrome/67.0.3396.99Safari/537.36","x-forwarded-for": "10.204.21
                     4.188"},"host": "s3-us-west-2.amazonaws.com","method": "GET","path": "dda-demo-samples/SAMPLE_NICE_DDA_HEURB_1177077.ppt-1","scheme": "http"},"http_response":{"
                     headers":{"content-length": "220160","content-type": "binary/octet-stream"},"status_code": 200},"ver": "1.0"}malwareName=HEUR_OLEXP.B rt=Aug 06 2018 02:24:15 +0000 po
                     licyName=default severity=0 filehash=3f21be4521b5278fb14b8f47afcabe08a17dc504 logType=1 dst=54.231.184.240 appName=Amazon Web Services (AWS) groupName=
                     fname=sample_nice_dda_heurb_1177077.ppt-1 adDomain= gatewayName=on-premise-2051 principalName= downStreamSize=220529 profileName=default userName=1
                     0.204.214.188 src=10.204.214.188 transportBytes=221030domainName=s3-us-west-2.amazonaws.com cat=Malware Accomplice act=analyze
```

Figure 5

## 4.4 Dashboards

- **TMWS - Log Types (by log count)**

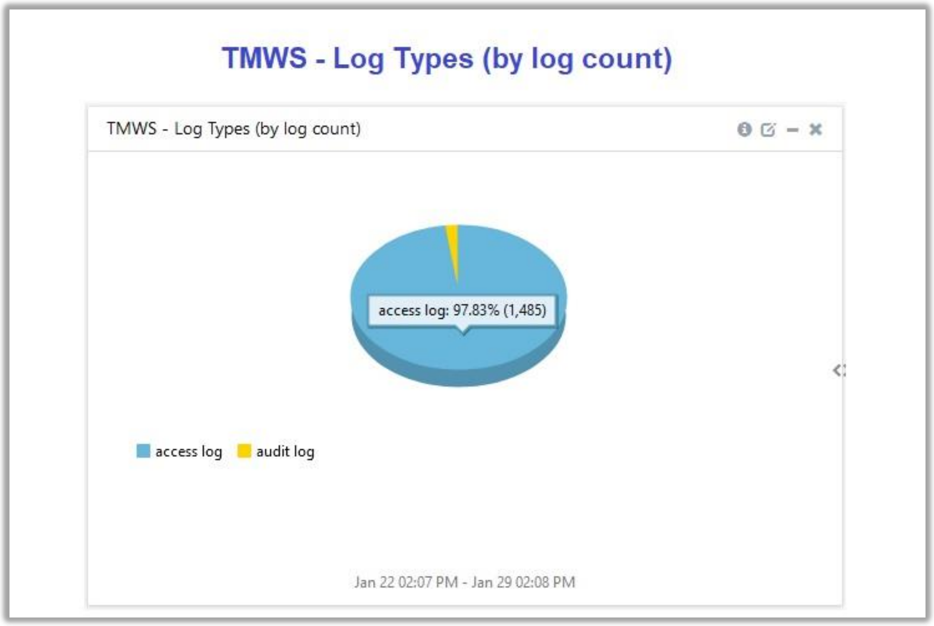

TMWS - Log Types (by log count)
TMWS - Log Types (by log count)
access log: 97.83% (1,485)
🟦 access log
🟨 audit log
Jan 22 02:07 PM - Jan 29 02:08 PM

Figure 6

- **TMWS - Top audit logs**

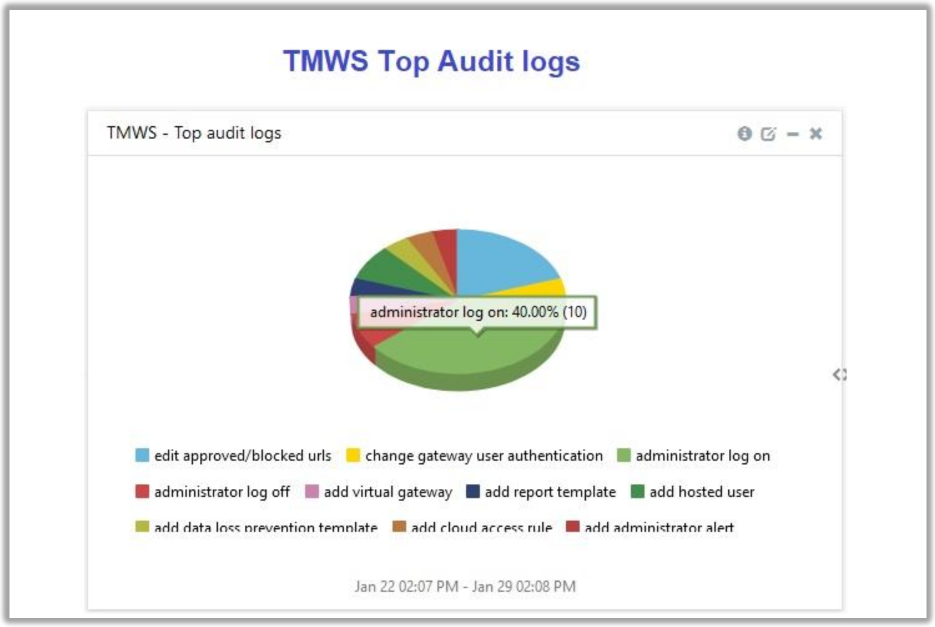


Figure 7

- **TMWS - Top access logs**

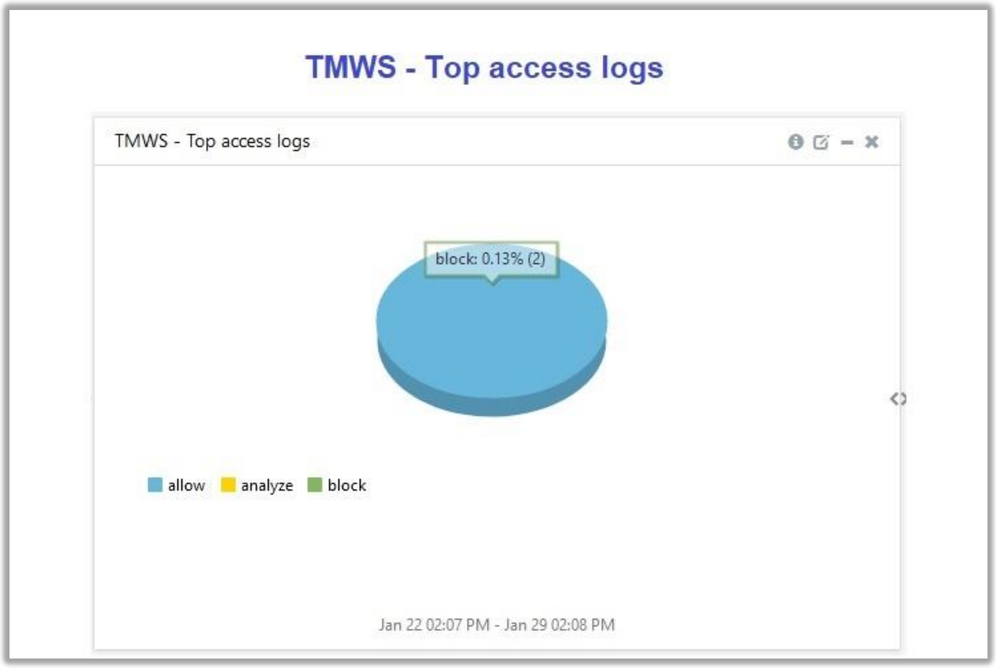


Figure 8

- **TMWS - Top audit activities by UserNames**

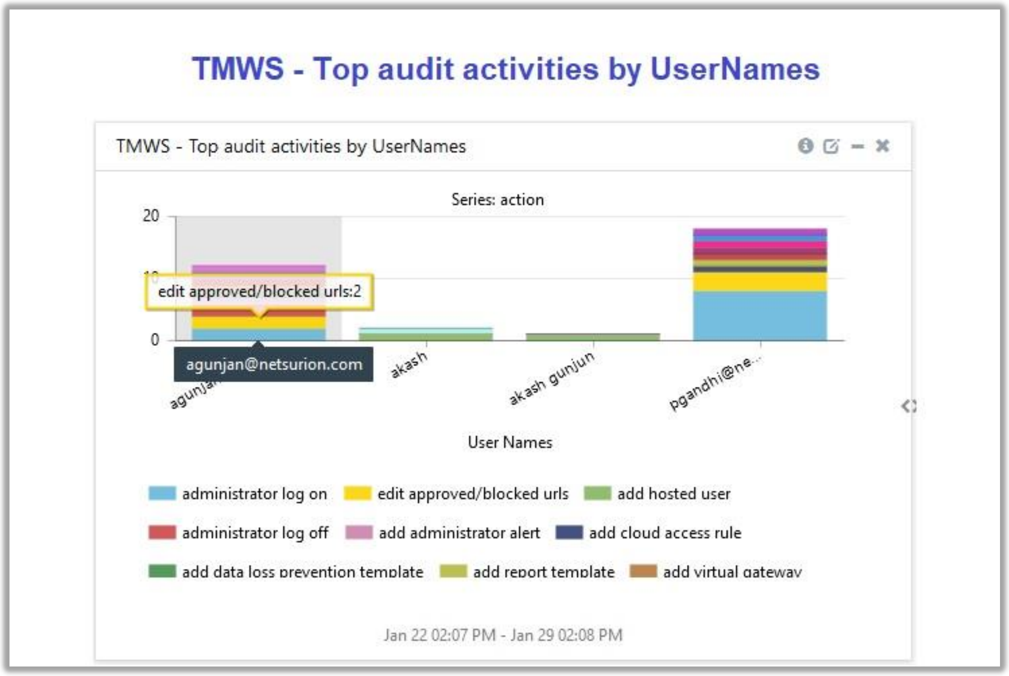


Figure 9

- **TMWS - Top gateway activities by UserNames/ IP Addresses**

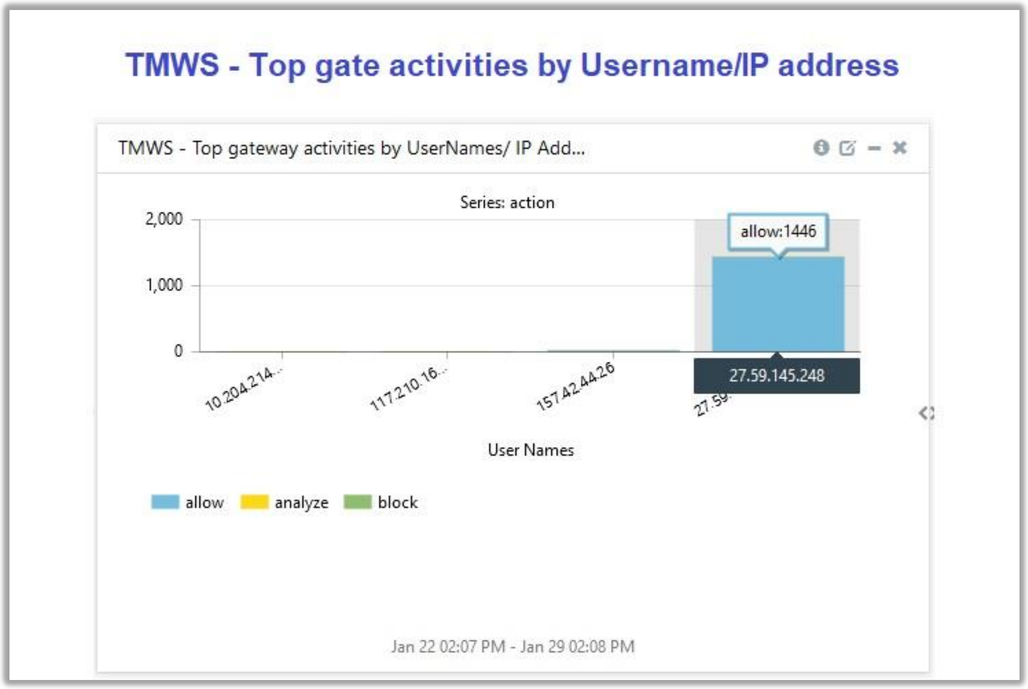

TMWS - Top gate activities by Username/IP address
TMWS - Top gateway activities by UserNames/ IP Add...
Series: action
2,000
1,000
0
allow:1446
10.204.214...
117.210.16...
157.42.44.26
27.59...
27.59.145.248
User Names
allow
analyze
block
Jan 22 02:07 PM - Jan 29 02:08 PM

Figure 10

- **TMWS - Audit log timeline**

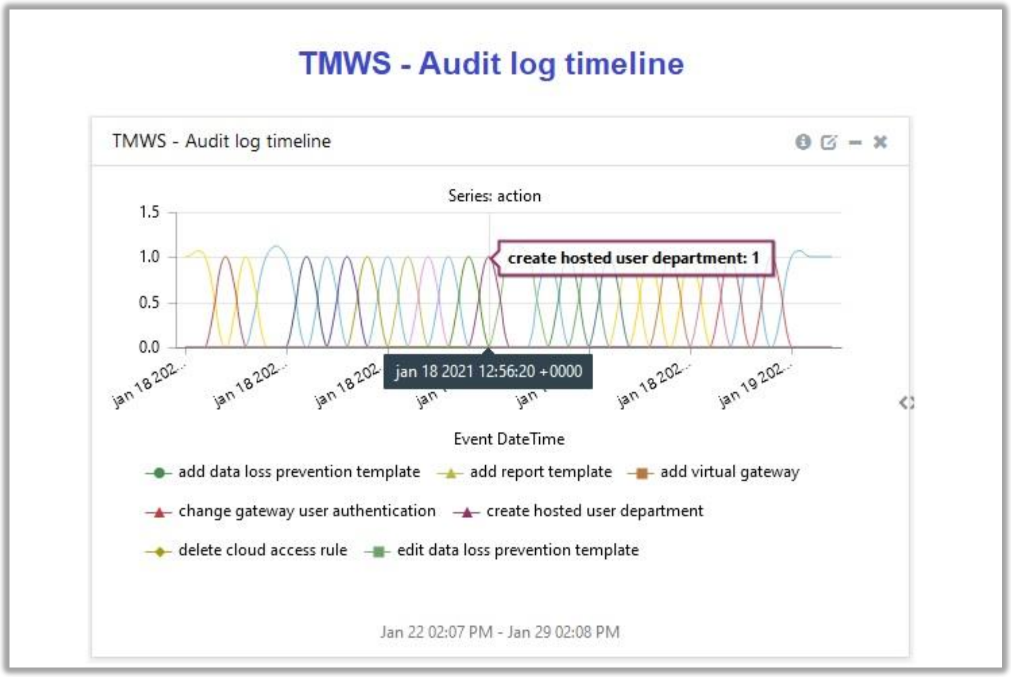

TMWS - Audit log timeline
TMWS - Audit log timeline
Series: action
1.5
1.0
0.5
0.0
create hosted user department: 1
jan 18 202...
jan 18 202...
jan 18 202...
jan 18 2021 12:56:20 +0000
jan
jan
jan 18 202...
jan 19 202...
Event DateTime
add data loss prevention template
add report template
add virtual gateway
change gateway user authentication
create hosted user department
delete cloud access rule
edit data loss prevention template
Jan 22 02:07 PM - Jan 29 02:08 PM

Figure 11

- **TMWS - Access log timeline**

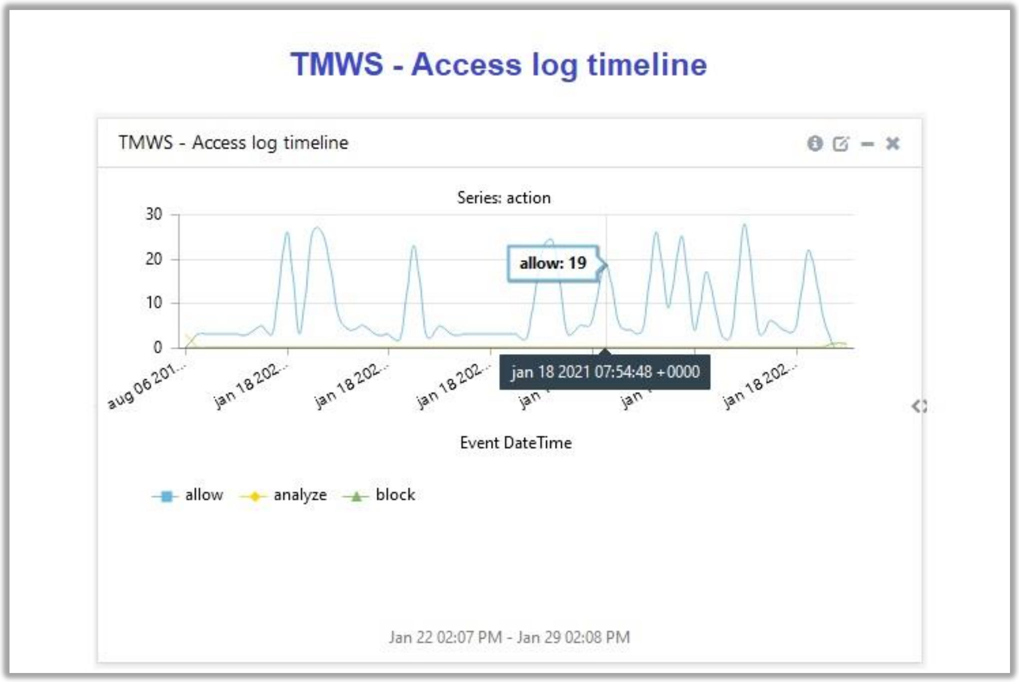


Figure 12

- **TMWS - Top user agents**

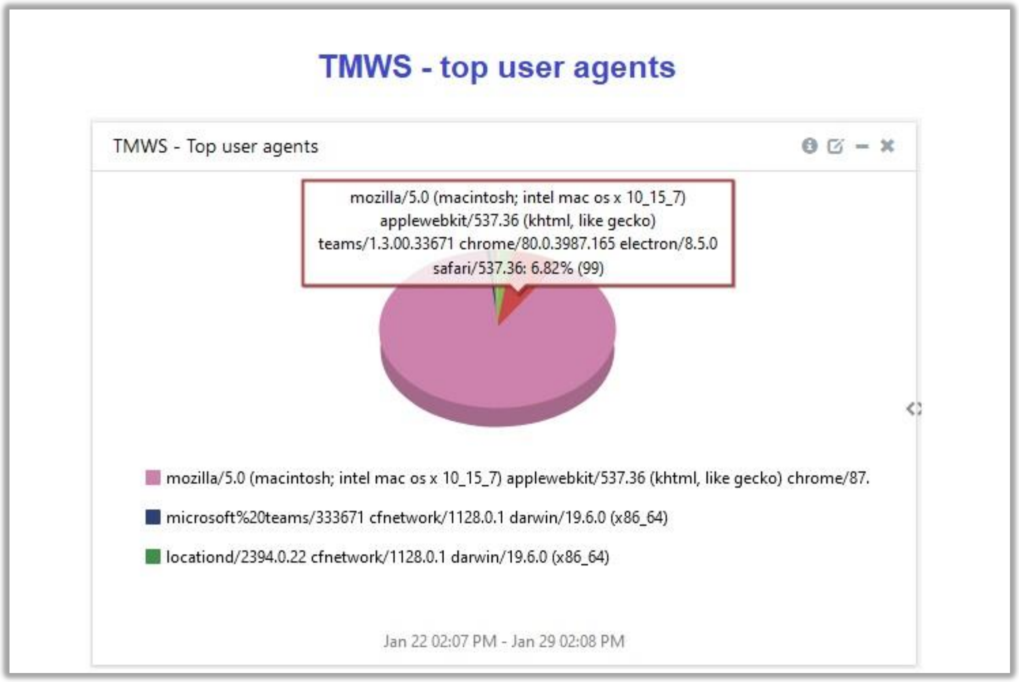

TMWS - top user agents
TMWS - Top user agents
mozilla/5.0 (macintosh; intel mac os x 10_15_7) applewebkit/537.36 (khtml, like gecko) teams/1.3.00.33671 chrome/80.0.3987.165 electron/8.5.0 safari/537.36: 6.82% (99)
mozilla/5.0 (macintosh; intel mac os x 10_15_7) applewebkit/537.36 (khtml, like gecko) chrome/87.
microsoft%20teams/333671 cfnetwork/1128.0.1 darwin/19.6.0 (x86_64)
locationd/2394.0.22 cfnetwork/1128.0.1 darwin/19.6.0 (x86_64)
Jan 22 02:07 PM - Jan 29 02:08 PM

Figure 13

- **TMWS - Top URL/Domains accessed by Gateway**

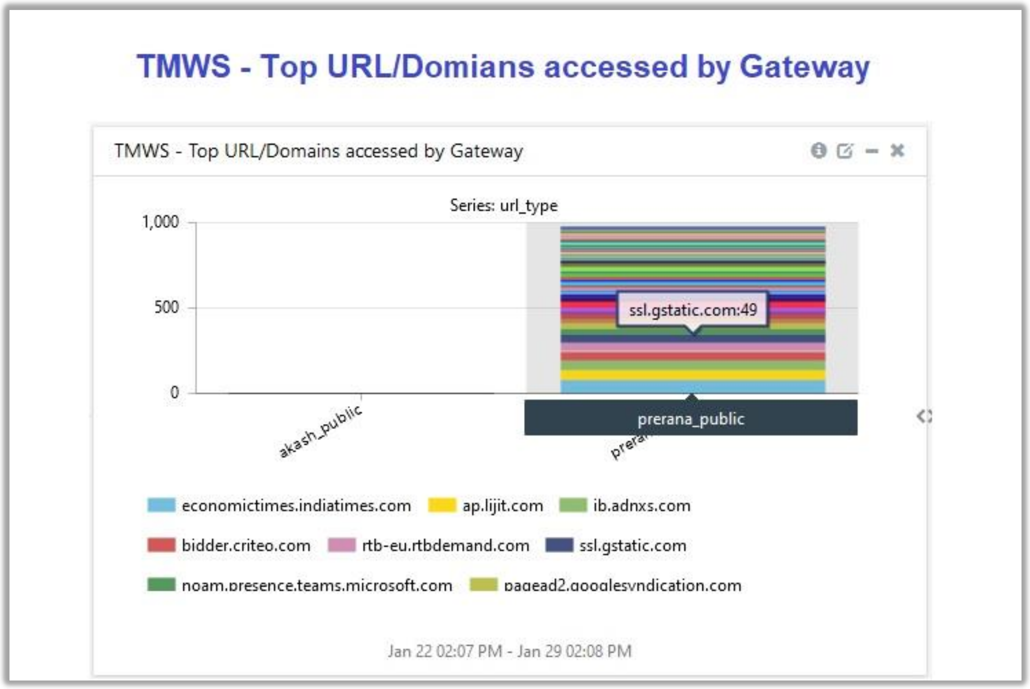

TMWS - Top URL/Domians accessed by Gateway
TMWS - Top URL/Domains accessed by Gateway
Series: url_type
1,000
500
0
ssl.gstatic.com:49
akash_public
prerana_public
prera
economictimes.indiatimes.com
ap.lijit.com
ib.adnxs.com
bidder.criteo.com
rtb-eu.rtbdemand.com
ssl.gstatic.com
noam.presence.teams.microsoft.com
pagead2.googlesyndication.com
Jan 22 02:07 PM - Jan 29 02:08 PM

Figure 14

- **TMWS - Blocked URL/Domains by source IP**

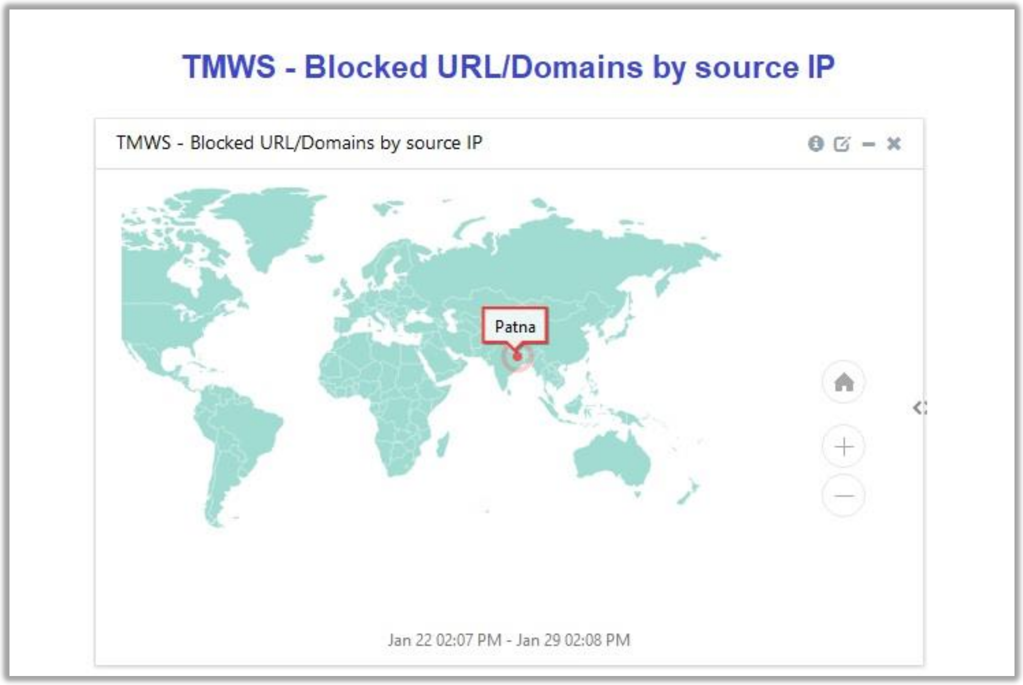
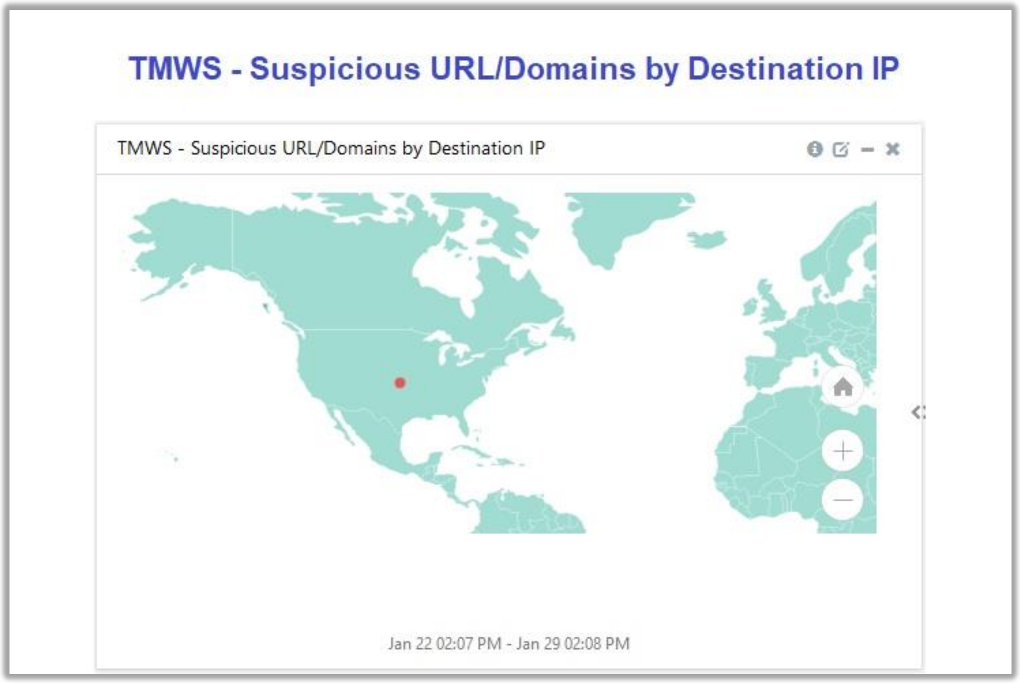

TMWS - Blocked URL/Domains by source IP
TMWS - Blocked URL/Domains by source IP
Patna
Jan 22 02:07 PM - Jan 29 02:08 PM

Figure 15

- **TMWS - Suspicious URL/Domains by Destination IP**



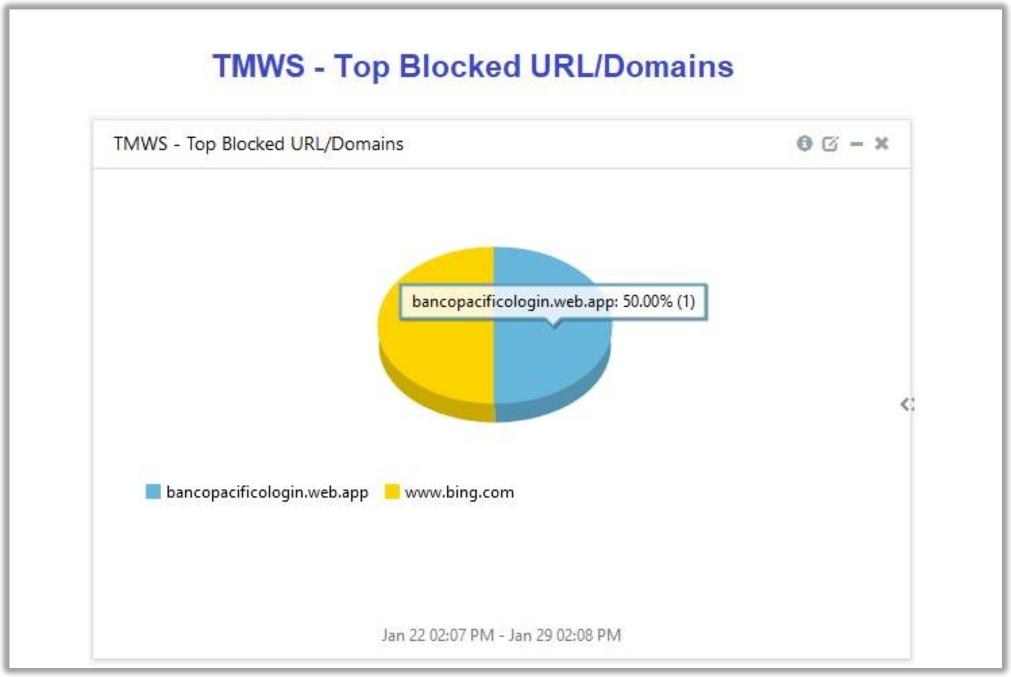
TMWS - Suspicious URL/Domains by Destination IP

TMWS - Suspicious URL/Domains by Destination IP

Jan 22 02:07 PM - Jan 29 02:08 PM

Figure 16

- **TMWS - Top Blocked URL/Domains**



TMWS - Top Blocked URL/Domains

TMWS - Top Blocked URL/Domains

bancopacificologin.web.app: 50.00% (1)
🟦 bancopacificologin.web.app
🟨 www.bing.com

Jan 22 02:07 PM - Jan 29 02:08 PM

Figure 17

- **TMWS - Access log by Event Category**

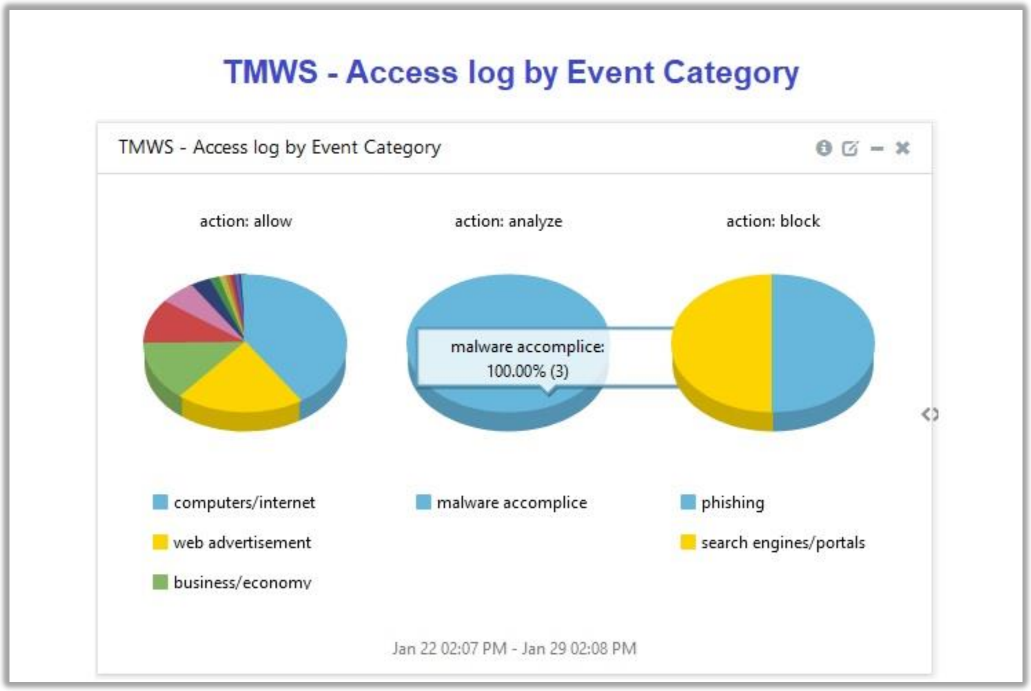
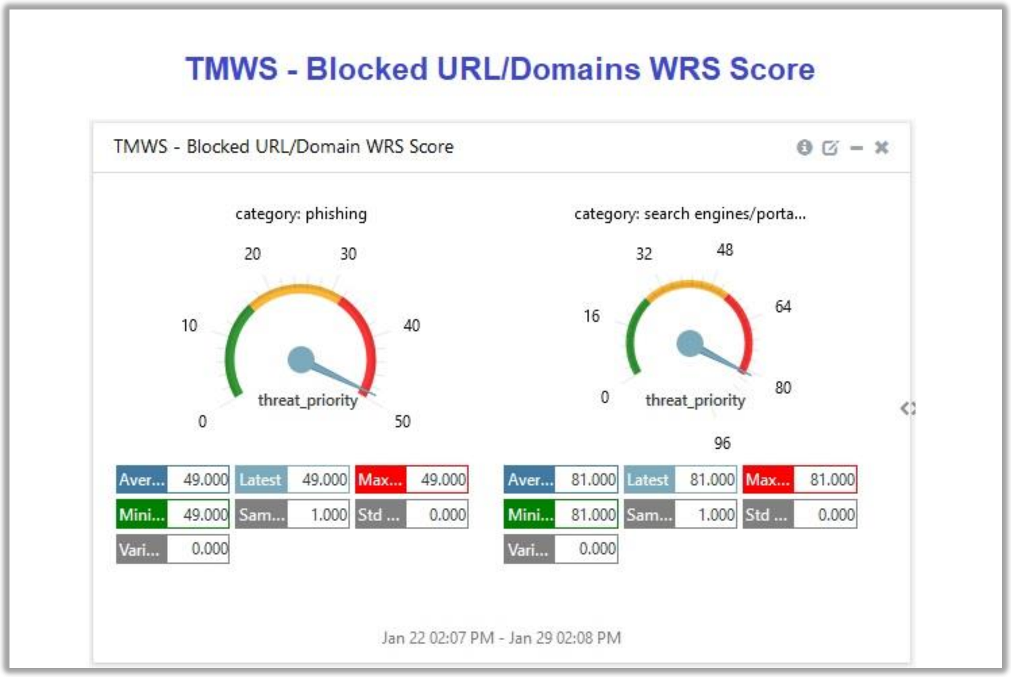


Figure 18

- **TMWS - Blocked URL/Domain WRS Score**

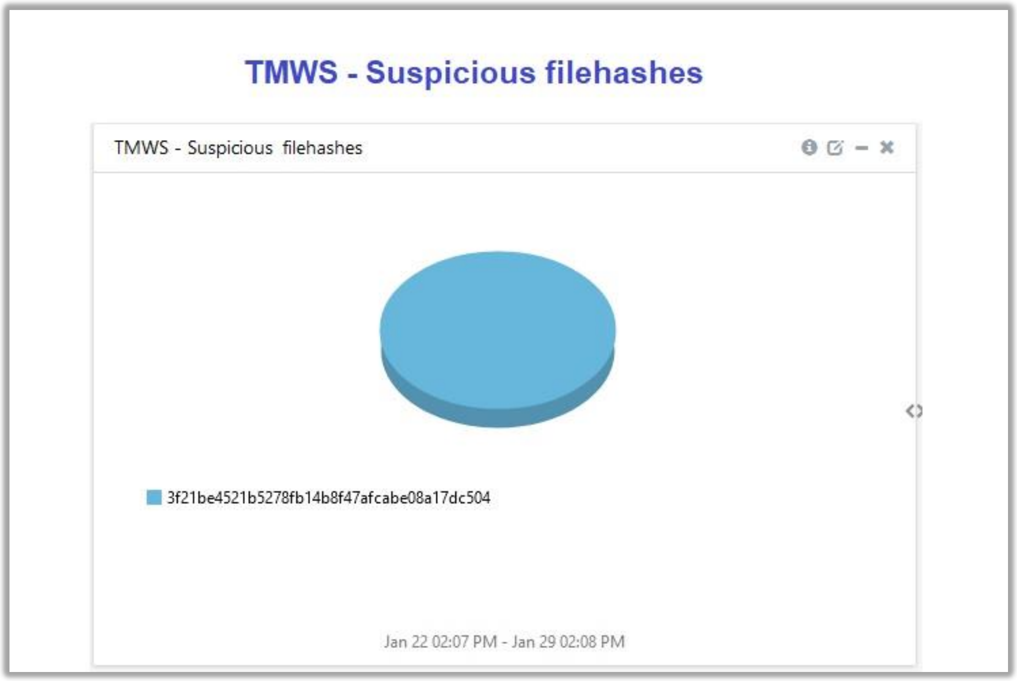

TMWS - Blocked URL/Domains WRS Score
TMWS - Blocked URL/Domain WRS Score
category: phishing
0
10
20
30
40
50
threat_priority
category: search engines/porta...
0
16
32
48
64
80
96
threat_priority
Jan 22 02:07 PM - Jan 29 02:08 PM

| | | | | | |
|---|---|---|---|---|---|
| Aver... | 49.000 | Latest | 49.000 | Max... | 49.000 |
| Mini... | 49.000 | Sam... | 1.000 | Std ... | 0.000 |
| Vari... | 0.000 | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Aver... | 81.000 | Latest | 81.000 | Max... | 81.000 |
| Mini... | 81.000 | Sam... | 1.000 | Std ... | 0.000 |
| Vari... | 0.000 | | | | |

Figure 19

- **TMWS - Suspicious filehashes**



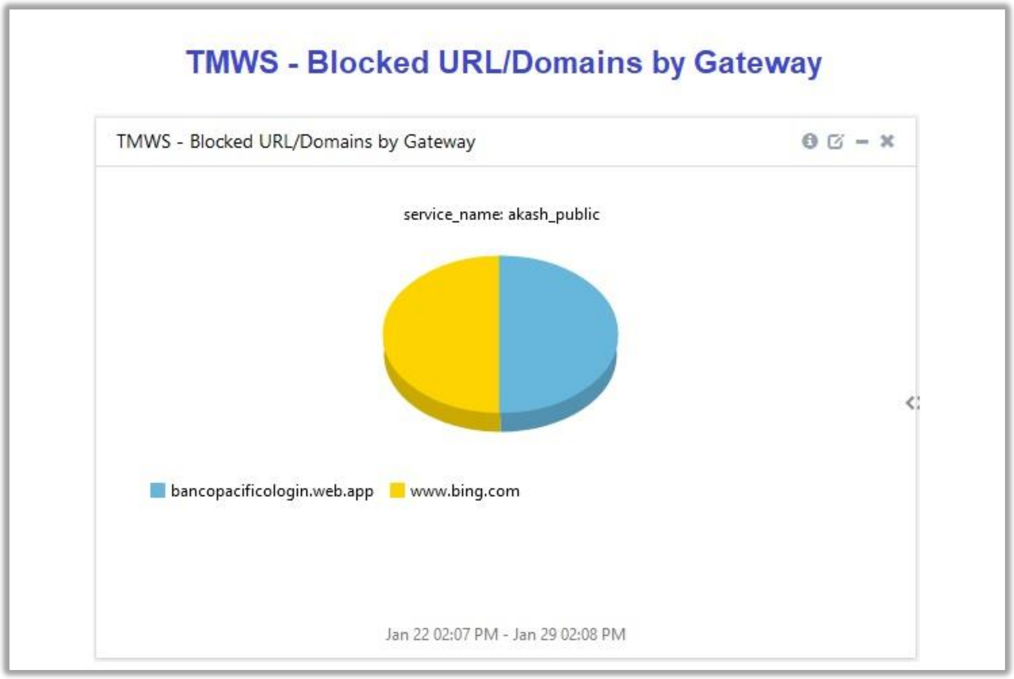
TMWS - Suspicious filehashes

TMWS - Suspicious filehashes

Jan 22 02:07 PM - Jan 29 02:08 PM

Figure 20

- **TMWS - Blocked URL/Domains by Gateway**



TMWS - Blocked URL/Domains by Gateway

TMWS - Blocked URL/Domains by Gateway

Jan 22 02:07 PM - Jan 29 02:08 PM

Figure 21

- **TMWS - Malware Discovered**

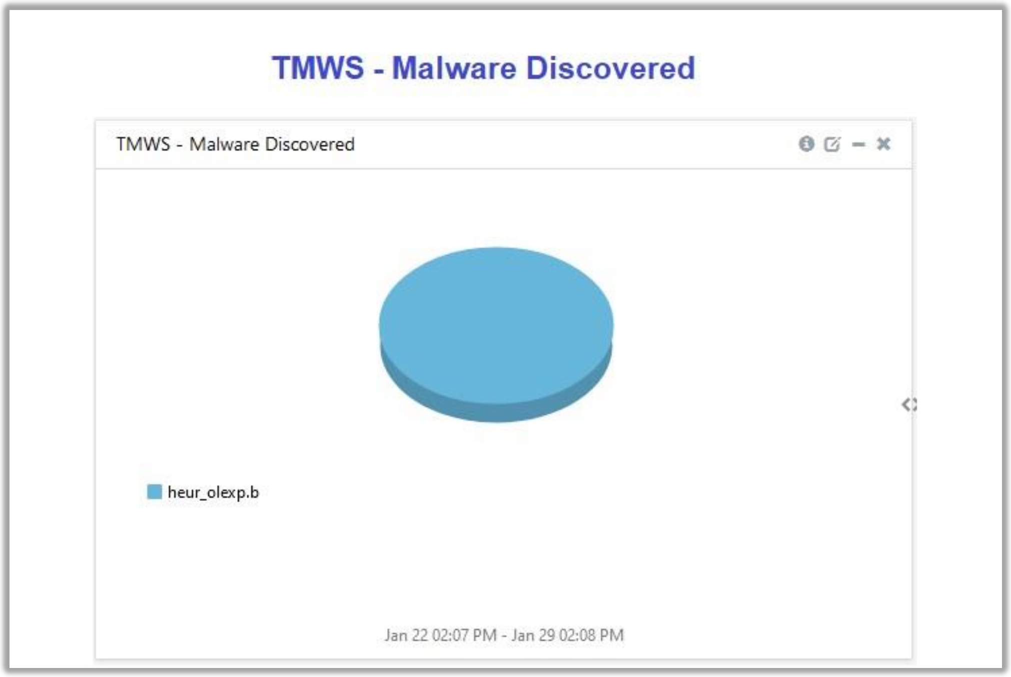

TMWS - Malware Discovered
TMWS - Malware Discovered
heur_olexp.b
Jan 22 02:07 PM - Jan 29 02:08 PM

Figure 22

# 5. Importing knowledge pack into EventTracker

## Getting Knowledge Packs

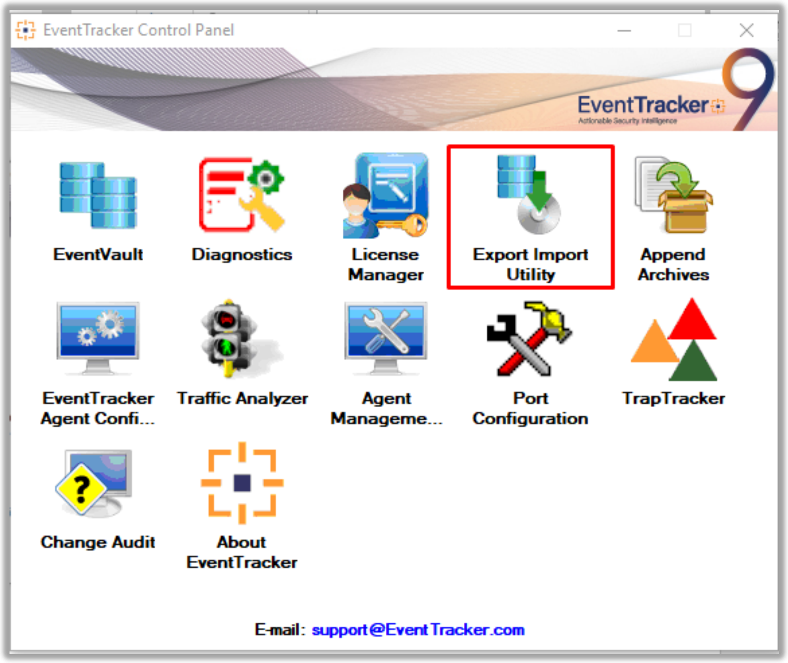
To get the knowledge packs, locate the knowledge pack folder. Follow the below steps:

1. Press ⊞ + R.
2. Type **%et_install_path%\Knowledge Packs** and press **Enter**.
   **Note** – If, not able to locate the file path as mentioned above, please contact EventTracker support to get the assistance.

**NOTE**: Import knowledge pack items in the following sequence:

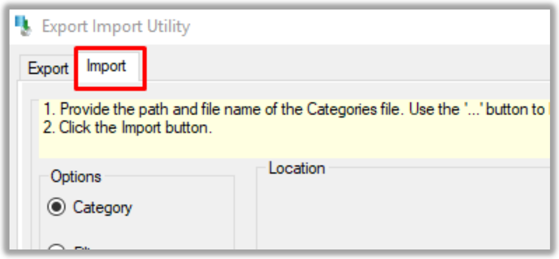
- Categories
- Alerts
- Token Template
- Reports
- Knowledge Objects
- Dashboards

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



E-mail: support@EventTracker.com

Figure 23



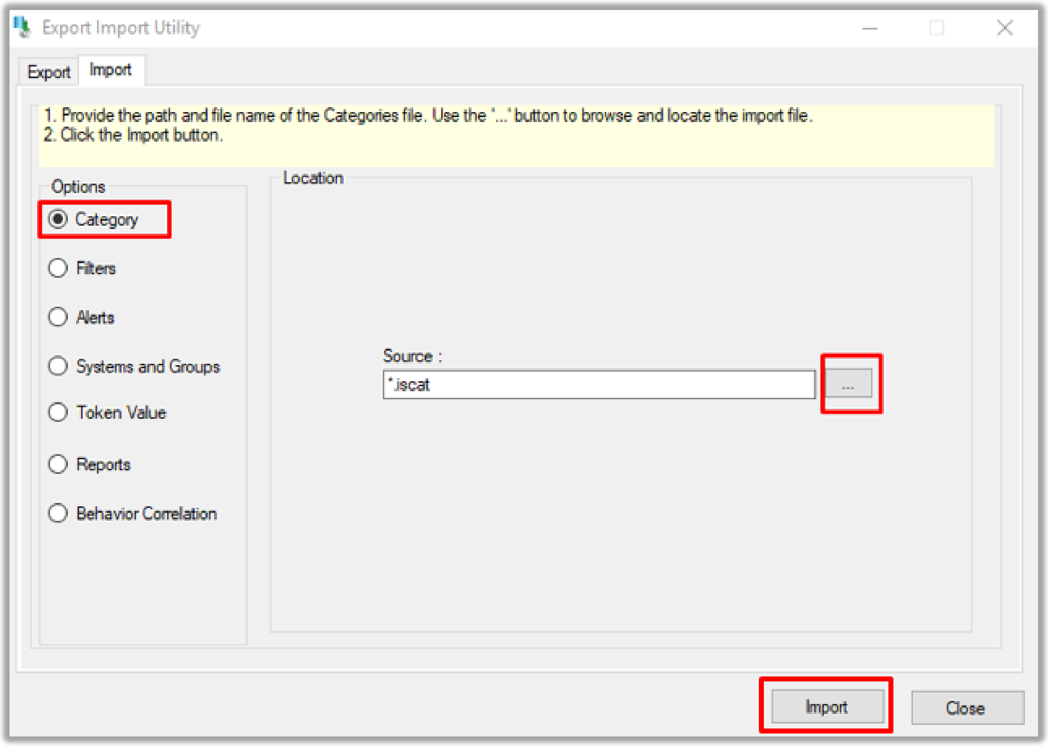
1. Provide the path and file name of the Categories file. Use the '...' button to
2. Click the Import button.

Figure 24

3. Click the **Import** tab.

## 5.1 Saved Searches

1. Once you have opened **Export Import Utility** via **EventTracker Control Panel**, click the **Category** option, and then click the browse ... .
2. Navigate to the knowledge pack folder and select the file with extension **".iscat", e.g. "Categories_TMWS.iscat"** and then click on the **Import** 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.

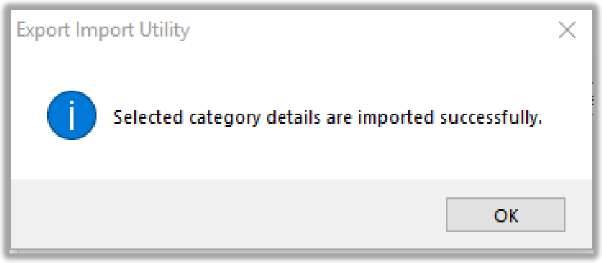
Options
- ● Category
- ○ Filters
- ○ Alerts
- ○ Systems and Groups
- ○ Token Value
- ○ Reports
- ○ Behavior Correlation

Location

Source : *.iscat

Figure 25

EventTracker displays a success message:

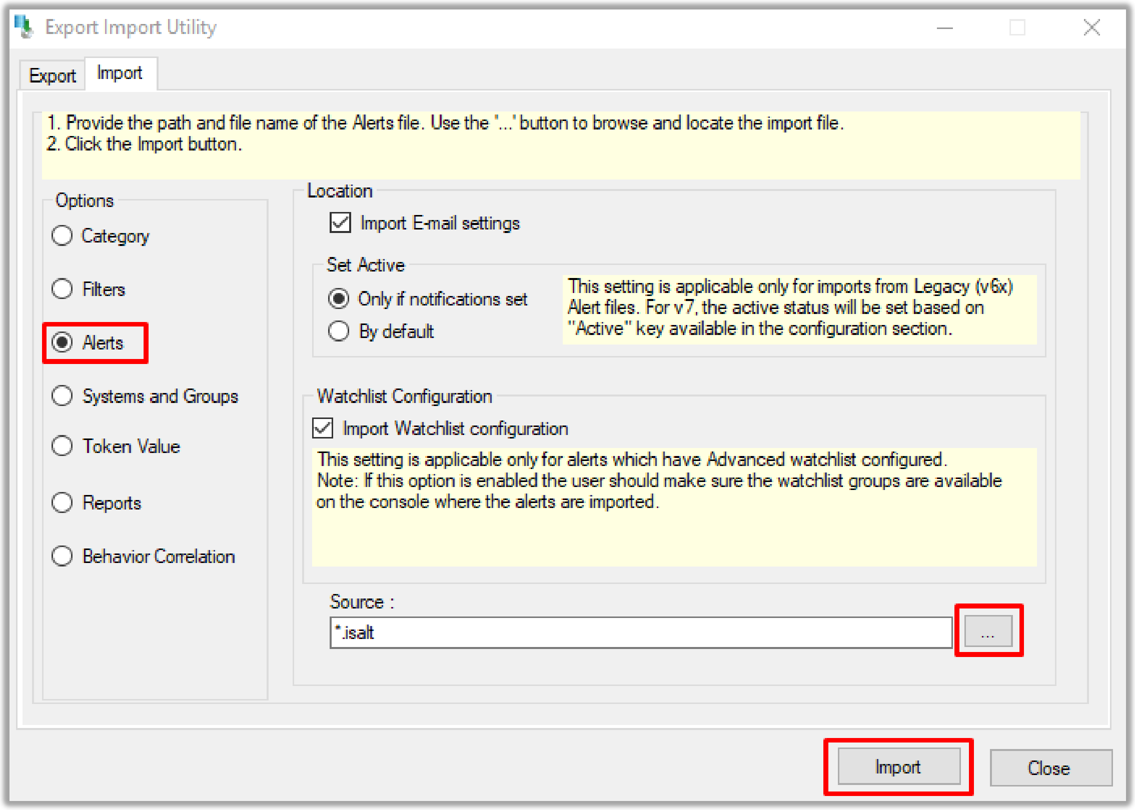


Selected category details are imported successfully.

Figure 26

## 5.2 Alerts

1. Once you have opened **Export Import Utility** via **EventTracker Control Panel**, click **Alert** option, and then click the browse button. ...
2. Navigate to the knowledge pack folder and select the file with extension **.isalt**, **e.g. Alerts_ TMWS.isalt** and then click on the "**Import**" 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.

☑ Import E-mail settings

● 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.

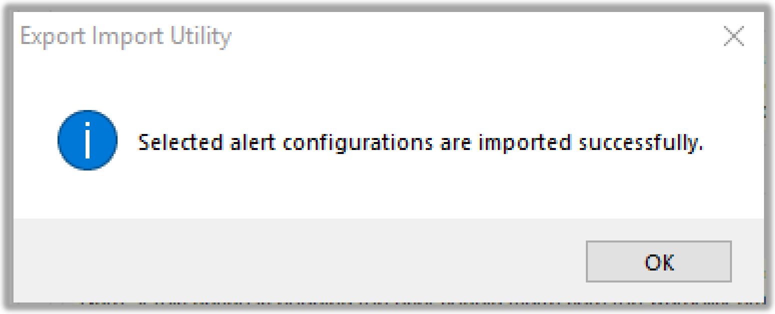
☑ Import Watchlist configuration

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 : *.isalt

Figure 27

EventTracker displays a success message:



Selected alert configurations are imported successfully.

Figure 28

## 5.3 Token Template

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

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

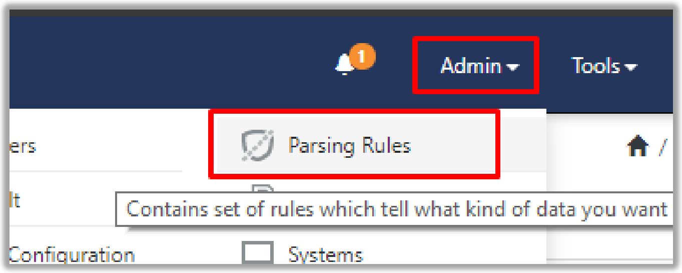


Figure 29

2. Click the **Template** tab and then click the **Import Configuration** button.

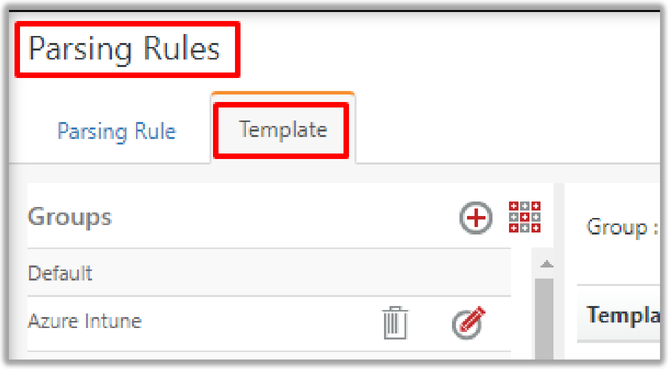


Figure 30

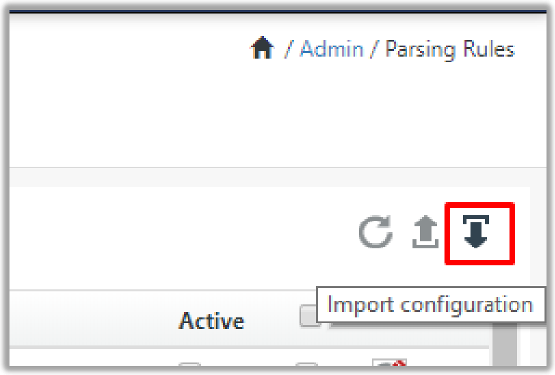
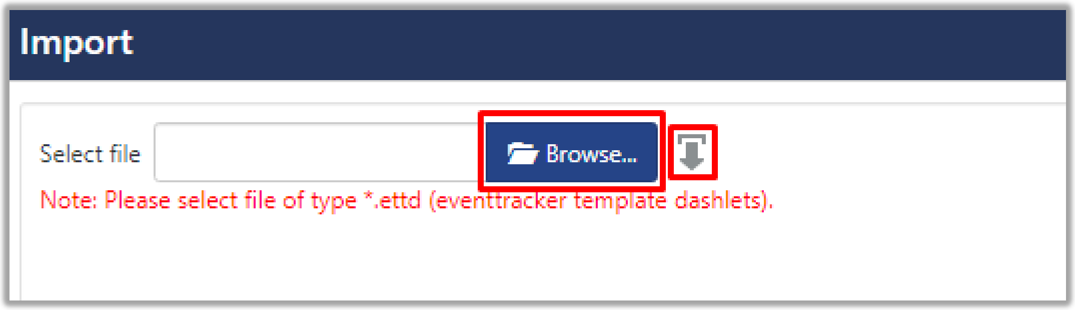


Figure 31

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



Import

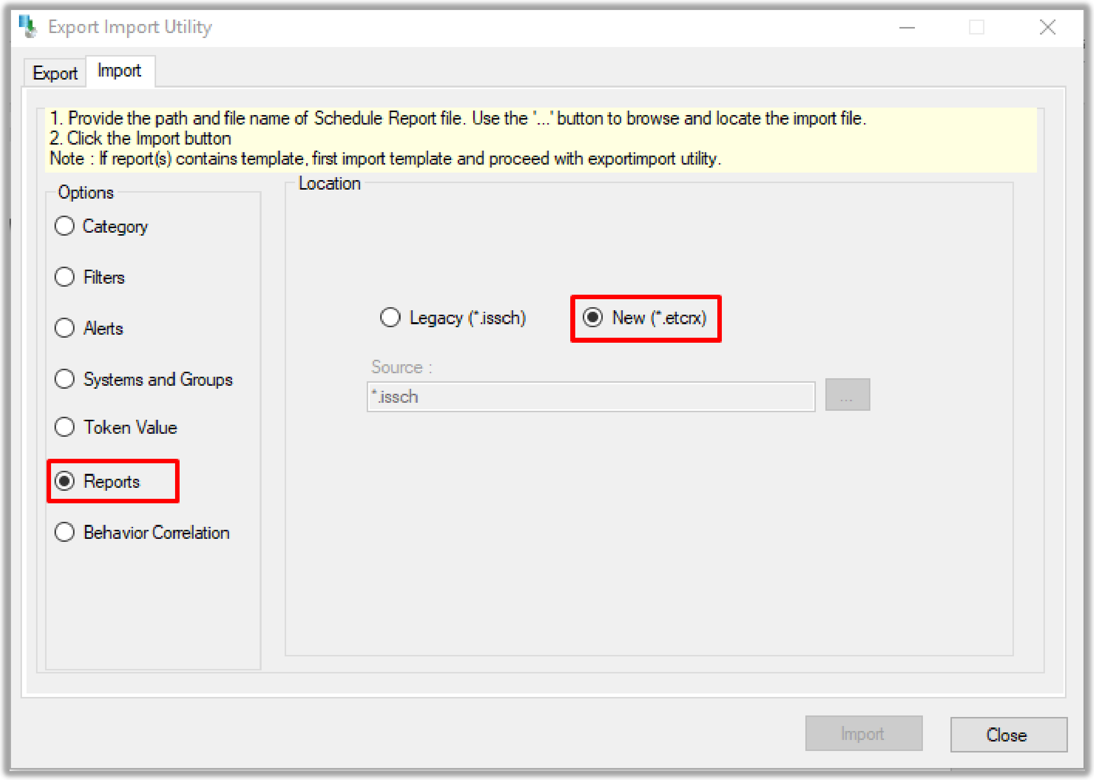
Select file

Note: Please select file of type *.ettd (eventtracker template dashlets).

Figure 32

## 5.4 Reports

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



Export Import Utility

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
○ Token Value
● Reports
○ Behavior Correlation

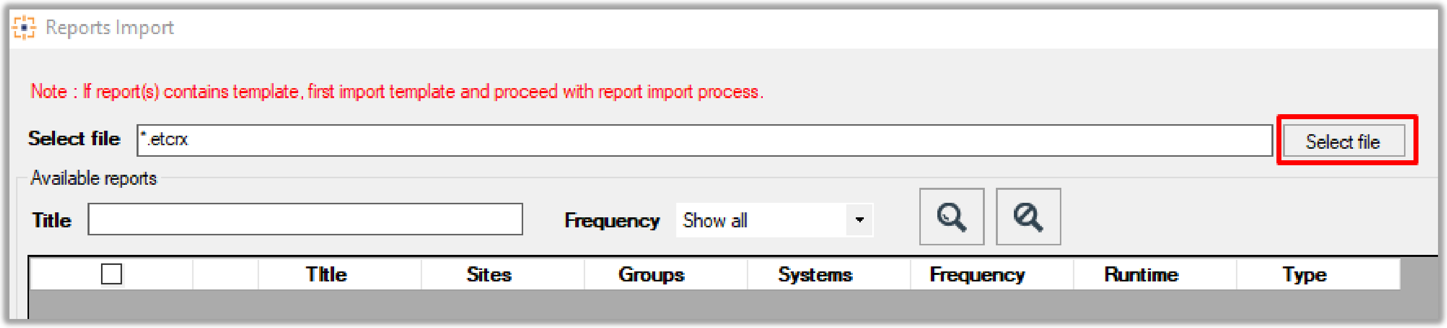
Location

○ Legacy (*.issch) ● New (*.etcrx)

Source : *.issch

Figure 33

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



Reports Import

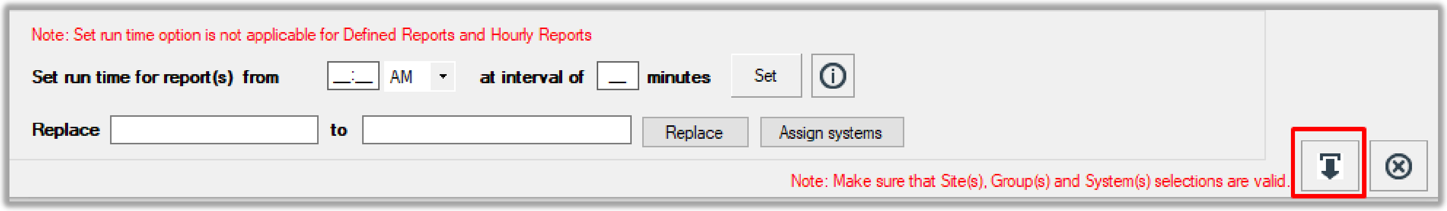
Note : If report(s) contains template, first import template and proceed with report import process.

Select file *.etcrx

| □ | | Title | Sites | Groups | Systems | Frequency | Runtime | Type |
|---|---|---|---|---|---|---|---|---|

Figure 34

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

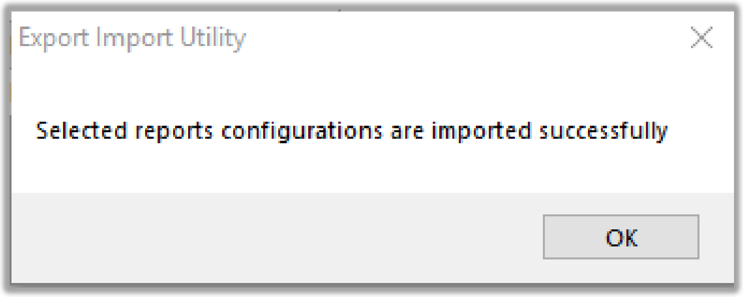


Note: Set run time option is not applicable for Defined Reports and Hourly Reports

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

Figure 35

EventTracker displays a success message:



Export Import Utility

Selected reports configurations are imported successfully

Figure 36

## 5.5 Knowledge Objects

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

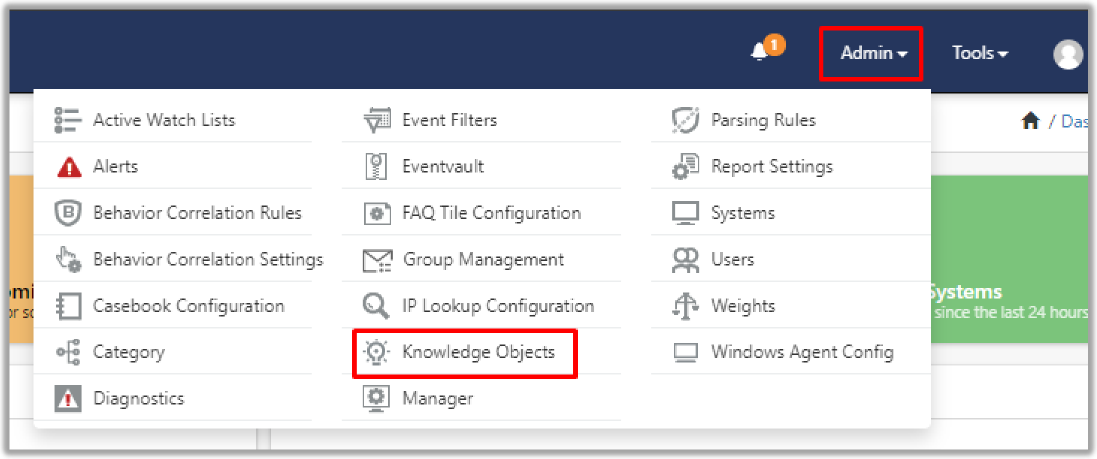


Figure 37

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

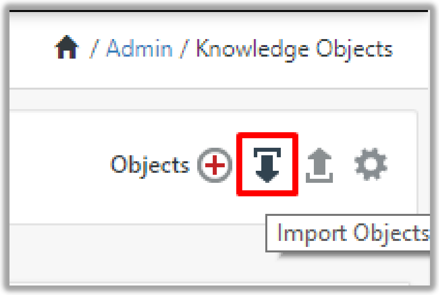


Figure 38

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

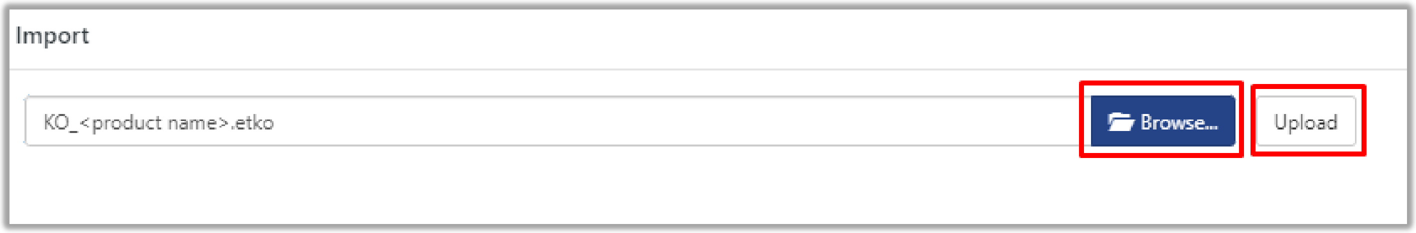


Figure 39

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

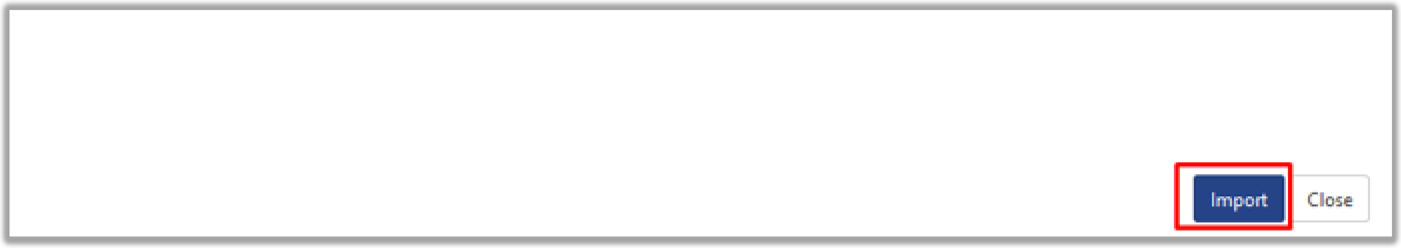


Figure 40

## 5.6 Dashboards

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

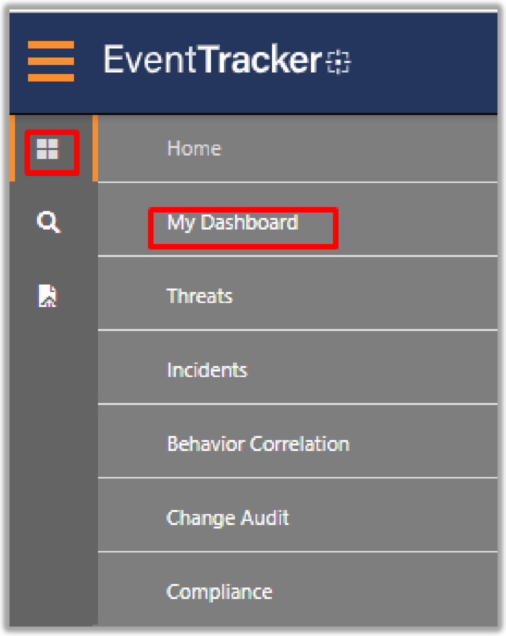


Figure 41

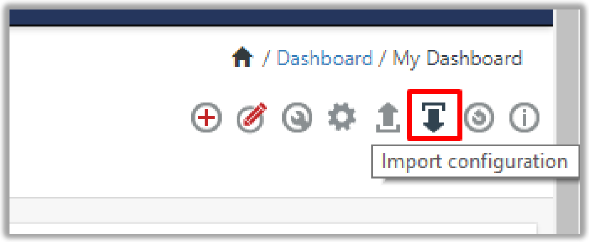
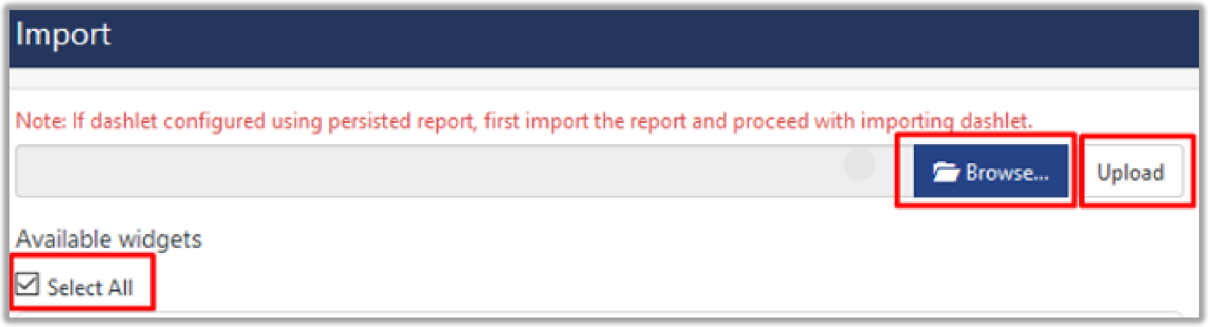


Figure 42

4. Select the **browse** button and navigate to knowledge pack folder (type **%et_install_path%\Knowledge Packs** in navigation bar) where **.etwd**, **e.g. Dashboards_ TMWS.etwd** is saved and click on **Upload** button.
5. Wait while EventTracker populates all the available dashboards. Now, choose **Select All** and click on **Import** Button.


Import

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

Figure 43

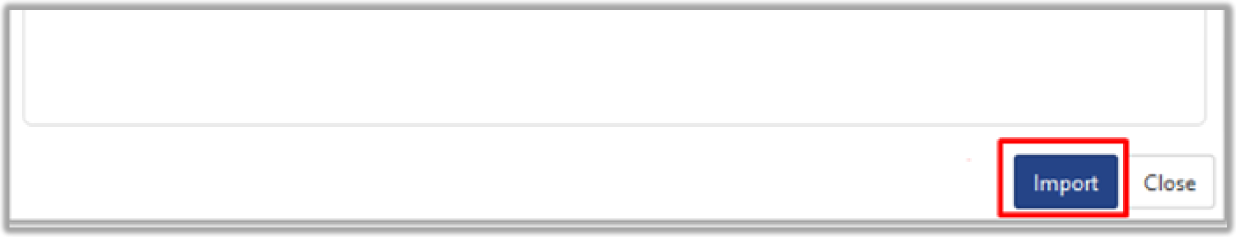
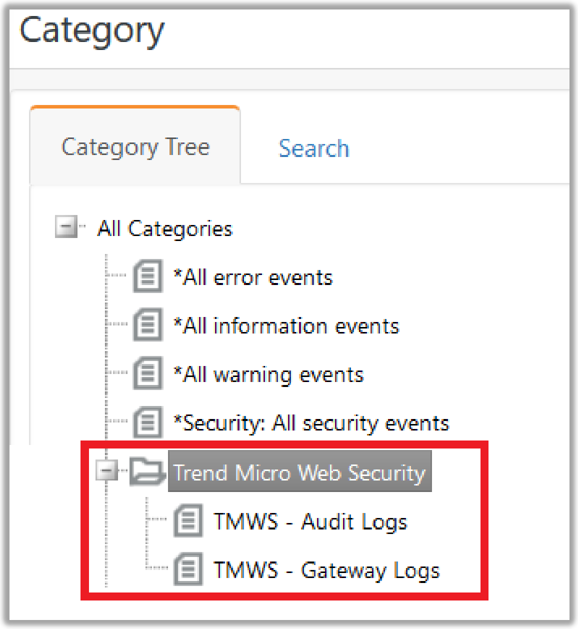


Figure 44

# 6. Verifying knowledge pack in EventTracker

## 6.1 Saved Searches

1. Login to **EventTracker manager web interface**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **Trend Micro Web Security** group folder to view the imported categories:



Category

Category Tree | Search

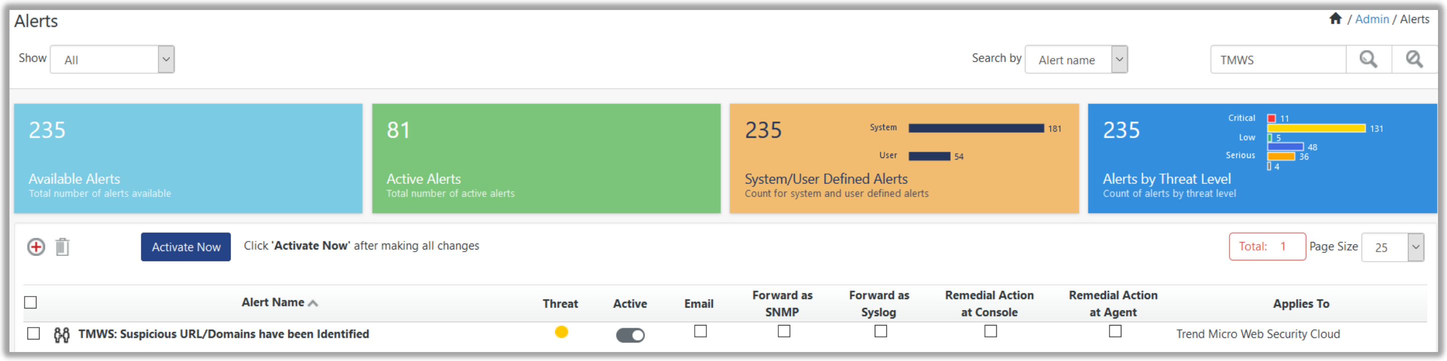
- All Categories
  - *All error events
  - *All information events
  - *All warning events
  - *Security: All security events
  - Trend Micro Web Security
    - TMWS - Audit Logs
    - TMWS - Gateway Logs

Figure 45

## 6.2 Alerts

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

   EventTracker displays an alert related to **TMWS:**



Alerts

/ Admin / Alerts

Show: All

Search by: Alert name — TMWS

235 Available Alerts — Total number of alerts available

81 Active Alerts — Total number of active alerts

235 System/User Defined Alerts — Count for system and user defined alerts (System 181, User 54)

235 Alerts by Threat Level — Count of alerts by threat level (Critical 11, 131, Low 5, 48, Serious 36, 4)

Click '**Activate Now**' after making all changes

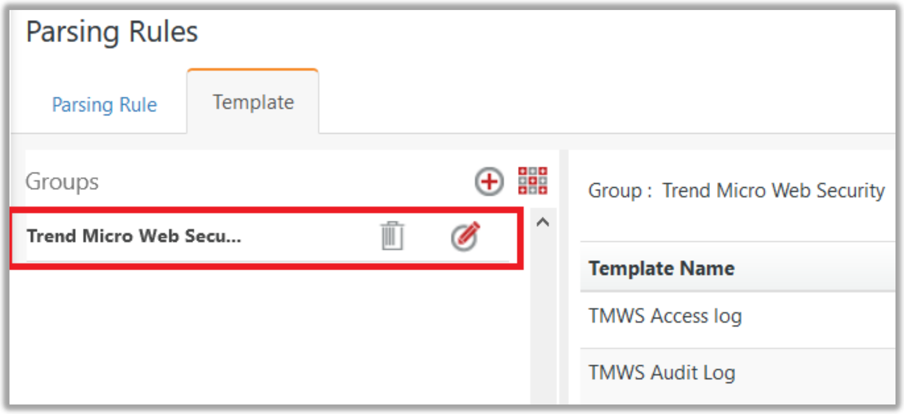
Total: 1 — Page Size: 25

| □ | Alert Name | Threat | Active | Email | Forward as SNMP | Forward as Syslog | Remedial Action at Console | Remedial Action at Agent | Applies To |
|---|---|---|---|---|---|---|---|---|---|
| □ | TMWS: Suspicious URL/Domains have been Identified | ● | ● | □ | □ | □ | □ | □ | Trend Micro Web Security Cloud |

Figure 46

## 6.3 Token Template

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Parsing Rules.**
2. In the **Template** tab, click on the **Trend Micro Web Security** group folder to view the imported Templates.



Parsing Rules

Trend Micro Web Secu...

Group : Trend Micro Web Security

| Template Name |
|---|
| TMWS Access log |
| TMWS Audit Log |

Figure 47

## 6.4 Reports

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

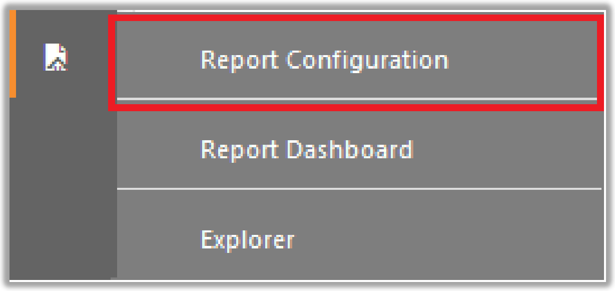
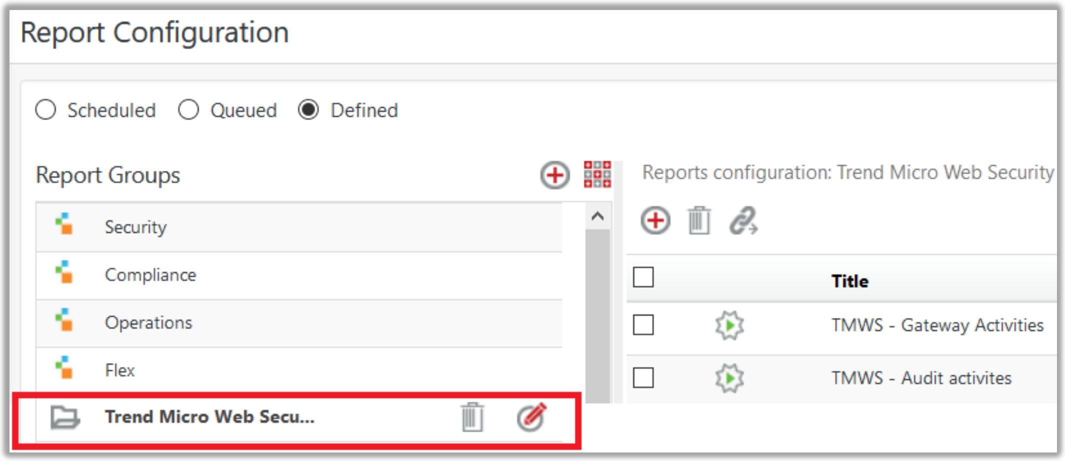


Figure 48

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



Report Configuration

○ Scheduled ○ Queued ● Defined

Reports configuration: Trend Micro Web Security

| □ | | Title |
|---|---|---|
| □ | | TMWS - Gateway Activities |
| □ | | TMWS - Audit activites |

Figure 49

## 6.5 Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects.**
2. In the **Knowledge Object** tree, expand the **Trend Micro Web Security** group folder to view the imported Knowledge objects.

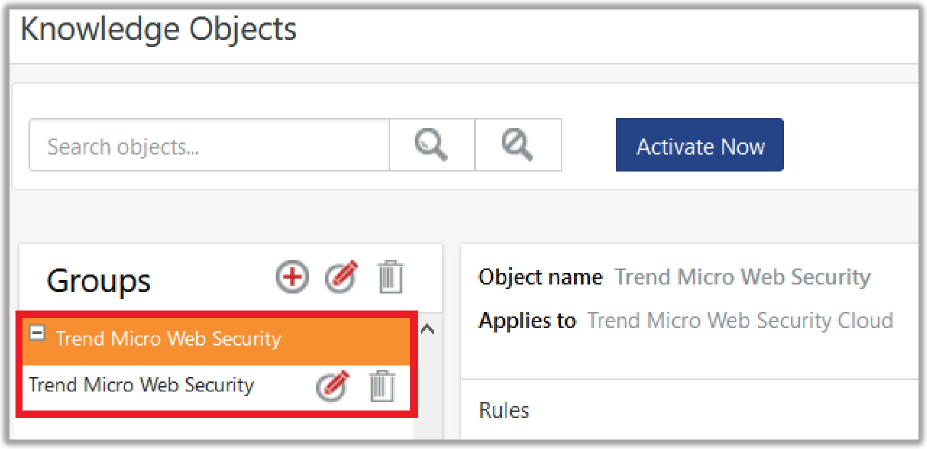


Figure 50

## 6.6 Dashboards

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

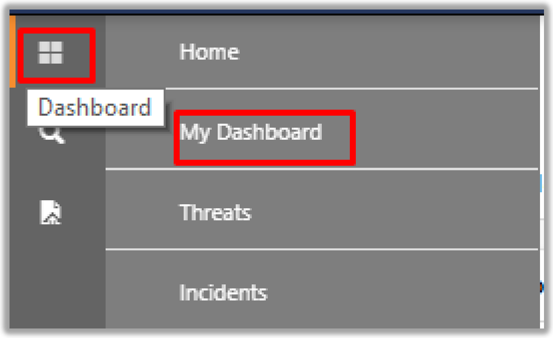


Figure 51

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

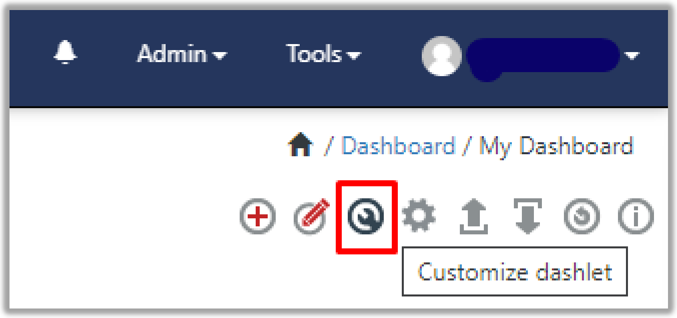
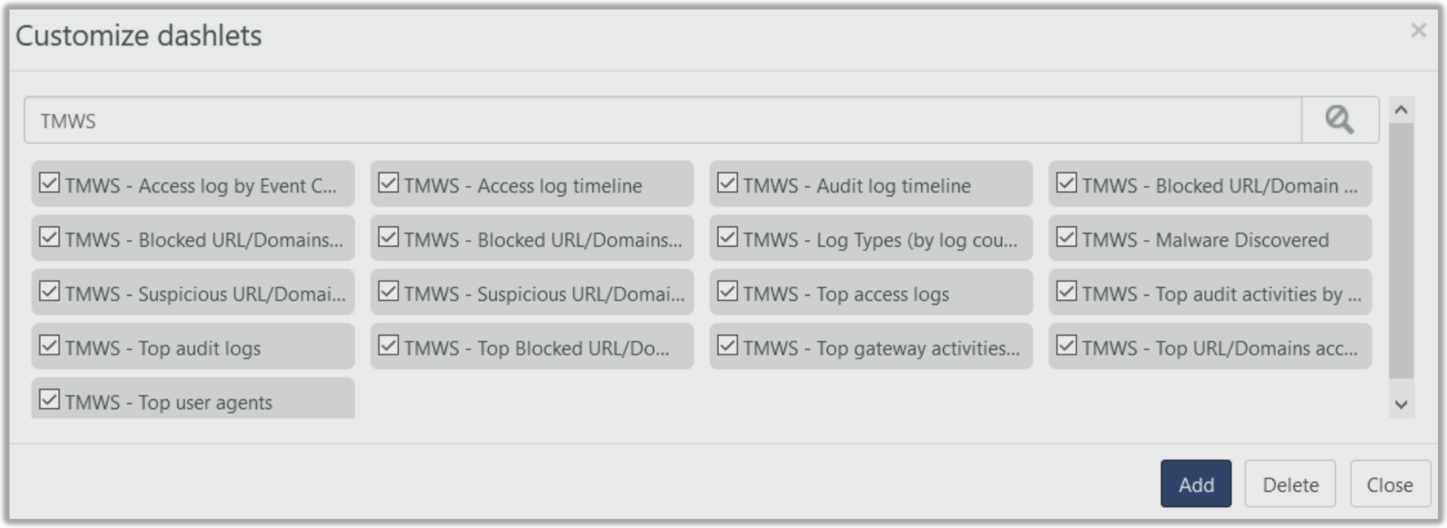


Figure 52



TMWS

☑ TMWS - Access log by Event C...
☑ TMWS - Access log timeline
☑ TMWS - Audit log timeline
☑ TMWS - Blocked URL/Domain ...
☑ TMWS - Blocked URL/Domains...
☑ TMWS - Blocked URL/Domains...
☑ TMWS - Log Types (by log cou...
☑ TMWS - Malware Discovered
☑ TMWS - Suspicious URL/Domai...
☑ TMWS - Suspicious URL/Domai...
☑ TMWS - Top access logs
☑ TMWS - Top audit activities by ...
☑ TMWS - Top audit logs
☑ TMWS - Top Blocked URL/Do...
☑ TMWS - Top gateway activities...
☑ TMWS - Top URL/Domains acc...
☑ TMWS - Top user agents

Figure 53