

Integration Guide

Integrating Zscaler Internet Access Central Authority (CA) with EventTracker

EventTracker v9.2x and above

Publication Date:

October 28, 2021

Abstract

This guide provides instructions to configure the **Zscaler Internet Access CA** to send its syslog to EventTracker.

Scope

The configuration details in this guide are consistent with the EventTracker version v9.2x or above and the Zscaler Internet Access CA.

Audience

The Administrators who are assigned the task to monitor the Zscaler Internet Access CA events using the EventTracker.

Table of Contents

Table of Contents	3
1. Overview	4
2. Prerequisites.....	4
3. Configuring Zscaler Internet Access CA	4
3.1 To configure a feed for the Web Logs.....	4
3.2 To configure a feed for the Firewall Logs	6
3.3 To configure a feed for the DNS Logs	8
3.4 To configure a feed for the Alerts.....	9
3.5 To configure a feed for the Tunnel Logs.....	9
3.6 To configure a feed for the SaaS Security logs.....	10
4. EventTracker Knowledge Packs	11
4.1 Categories.....	11
4.2 Alerts.....	11
4.3 Reports	12
4.4 Dashboards.....	14
5. Importing Zscaler Internet Access CA Knowledge Pack into EventTracker.....	18
5.1 Categories.....	19
5.2 Alerts.....	19
5.3 Reports	20
5.4 Knowledge Objects.....	22
5.5 Dashboards.....	23
6. Verifying Zscaler Internet Access CA Knowledge Pack in the EventTracker	24
6.1 Categories.....	24
6.2 Alerts.....	24
6.3 Knowledge Objects.....	25
6.4 Reports	26
6.5 Dashboards.....	26
About Netsurion	28

1. Overview

The Zscaler Internet Access (ZIA) Central Authority (CA) is the vital system in the Zscaler cloud. It monitors the cloud and provides a central location for the software and database updates, policy and configuration settings, and threat intelligence.

The Nanolog Streaming Service (NSS) server can send the traffic logs to EventTracker. Using EventTracker, you can monitor the web traffic logs, firewall logs, tunnel logs, and alerts. You can easily track the malicious web activities, inbound and outbound traffic activities, and alerts even when the CPU memory is full, and the CPU utilization is high.

EventTracker can help organizations monitor the Zscaler Internet Access CA alerts triggered by the ZIA CA. EventTracker captures login and logout events into Zscaler Internet Access CA application and alerts the administrators in real-time.

2. Prerequisites

- **Admin** access to the Zscaler Internet Access CA console.

3. Configuring Zscaler Internet Access CA

The NSS feed specifies the data from the logs, which the NSS sends to EventTracker: Web logs, firewall logs, DNS logs, alerts, tunnel logs, SaaS security logs.

There are two reliable log delivery mechanisms in the NSS.

NSS to SIEM: The NSS buffers the logs in the Virtual Machine (VM) memory to increase its resilience to transit the network issues between the SIEM and the NSS. If the connection drops, the NSS replays the buffer logs, according to the Duplicate Logs setting.

Nanolog to SIEM: If the connectivity between Netsurion's cloud and the NSS is interrupted, the NSS will miss the logs that have arrived at the Nanolog cluster during the interruption, and the logs won't be delivered to the SIEM. Once the connection restores, the NSS one-hour recovery allows the Nanolog to replay the logs up to one hour back.

Note: Enable the TCP with port number 514 from the EventTracker to receive the Zscaler Internet Access CA logs.

3.1 To configure a feed for the Web Logs

1. Go to the **Administration > Nanolog Streaming Service**.
2. In the **NSS Feeds** tab, click **Add NSS Feed**.

The **Add NSS Feed** window appears.

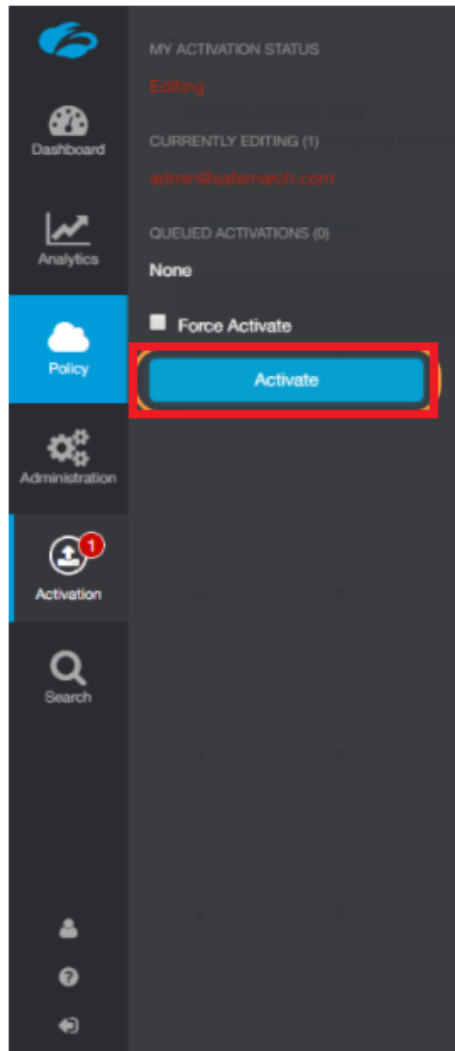
3. In the **Add NSS Feed** window, enter the following details.

- **Feed Name:** Enter the name as **Web logs**.
- **NSS Type:** Select **NSS for Web**.
- **NSS Server:** Choose the NSS from the list.
- **Status:** The NSS feed is **Enabled** by default.
- **SIEM Destination Type:** The type of destination.
 - **SIEM IP Address:** Enter the IP address of **EventTracker** to which the logs stream.
- **SIEM TCP Port:** Enter port number 514.
- **Log Type:** Choose **Web Log**.
- **SIEM Rate Limit (Events per Second):** Leave as unrestricted or unlimited.
- **Feed Output Type:** Select **Custom**.
- **Feed Output Format:** For the NSS feeds for web logs, copy and paste the pre-populated Feed Output format with the following.

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss-web CEF:0
|Zscaler|NSSWeblog|5.7|s{action}|s{reason}|3| act=s{action} re
ason=s{reason} app=s{proto} dhost=s{ehost} dst=s{sip} src=s{
cintip} sourceTranslatedAddress=s{cip} in=%d{respsize} out=%d{re
qsize} request=s{eurl} requestContext=s{ereferer} outcome=s{re
spcode} requestClientApplication=s{ua} requestMethod=s{reqmetho
d} suser=s{login} spriv=s{location} externalId=%d{recordid} fil
eType=s{filetype} destinationServiceName=s{apppname} cat=s{urloc
at} deviceDirection=1 cn1=%d{riskscore} cn1Label=riskscore cs1=s
{dept} cs1Label=dept cs2=s{urlocat} cs2Label=urlocat cs3=s{malwar
eclclass} cs3Label=malwareclass cs4=s{malwarecat} cs4Label=malware
cat cs5=s{threatname} cs5Label=threatname cs6=s{band5} cs6Label
```

```
=md5hash rulelabel=%s{rulelabel} ruletype=%s{ruletype} urlclass=%s{urlclass} devicemodel=%s{devicemodel} devicehostname=%s{devicehostname}\n
```

- **User Obfuscation:** Choose **Disable** to display the usernames.
 - **Timezone:** By default, this is set to the organization's time zone.
 - **Duplicate Logs:** Enter the number of 60 (minutes).
4. Click **Save** and activate the change.



3.2 To configure a feed for the Firewall Logs

1. Go to **Administration > Nanolog Streaming Service**.
2. In the **NSS Feeds** tab, click **Add NSS Feed**.
The **Add NSS Feed** window appears.
3. In the **Add NSS Feed** window, enter the following details.

Add NSS Feed

Feed Name

Firewall Log

NSS Server

NSS_Server1

SIEM Destination Type

☒ IP Address
☐ FQDN

SIEM TCP Port

514

SIEM Rate

☒ Unlimited
☐ Limited

Log Type

☒ Firewall Logs
☐ DNS Logs
☐ Alert

Firewall Log Type

☒ Full Session Logs
☐ Aggregate Logs
☐ Both Session and Aggregate Logs

Feed Output Type

Custom

Feed Output Format

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss-fw CEF:0|Zscaler|NSSFWlog|5.7|{%s(action)}|{%s(ruleLabel)}|3| act=%s{action}
suser=%s{login} src=%s{csip} spt=%d{csport} dst=%s{cdip} dpt=%d{cdport} deviceTranslatedAddress=%s{ssip} deviceTranslatedPort=%d{ssport}
destinationTranslatedAddress=%s{sdip} destinationTranslatedPort=%d{sdport} sourceTranslatedAddress=%s{tsip} sourceTranslatedPort=%d{tsport}
proto=%s{ipproto} tunnelType=%s{ttype} dur=%s{dnat} stateful=%s{stateful} spriv=%s{location} reason=%s{ruleLabel} in
=%d{inbytes} out=%d{outbytes} deviceDirection=1 cs1=%s{dept} cs1Label=dept cs2=%s{nswc} cs2Label=nwService cs3=%s{nuapp} cs3Label
=nuApp cs4=%s{aggregate} cs4Label=aggregated cs5=%s{threatcat} cs5Label=threatcat cs6=%s{threatname} cs6Label=threatname cs1
=%d{durations} cs1Label=durations cs2=%s{numSessions} cs2Label=numSessions cs3Label=ipCat cs3=%s{ipcat} cs5=%s{destCountry}
destCountry=%s{destCountry}
```

User Obfuscation

☐ Enabled
☒ Disabled

Timezone

GMT

Duplicate Logs

Disabled

ACTION

WHO

SOURCE

SERVER

SESSION

PROTOCOL CLASSIFICATION

SECURITY

FIREWALL FILTERS

Save

Cancel

- **Feed Name:** Enter or edit the name as **Firewall logs**.
- **NSS Type:** Select **NSS for Firewall**.
- **NSS Server:** Choose an NSS from the list.
- **Status:** It is **Enabled** by default.
- **SIEM Destination Type:** The type of destination.
 - **SIEM IP Address:** Enter the IP address of EventTracker.
- **SIEM TCP Port:** Enter port number 514.
- **Log Type:** Choose **Firewall Logs**.
- Choose the **Firewall Log Type:** Both Session and Aggregate Logs.
- **SIEM Rate Limit (Events per Second):** Leave as unrestricted or unlimited.
- **Feed Output Type:** Select **Custom**.
- **Feed Output Format:** **NSS Feeds** for firewall logs, copy and paste the pre-populated Feed Output format with the following:

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss-fw CEF
:0|Zscaler|NSSFWlog|5.7|{%s(action)}|{%s(ruleLabel)}|3| act=%s{act
ion} suser=%s{login} src=%s{csip} spt=%d{csport} dst=%s{cdip}
dpt=%d{cdport} deviceTranslatedAddress=%s{ssip} deviceTranslat
edPort=%d{ssport} destinationTranslatedAddress=%s{sdip} destin
```

```

ationTranslatedPort=%d{sdport} sourceTranslatedAddress=%s{tsip}
sourceTranslatedPort=%d{tsport} proto=%s{ipproto} tunnelType
=%s{ttype} dnat=%s{dnat} spriv=%s{location} reason=%s{rulelabel}
in=%ld{inbytes} out=%ld{outbytes} deviceDirection=1 cs1=%s{dept}
cs1Label=dept cs2=%s{nwsvc} cs2Label=nwService cs3=%s{nwapp}
cs3Label=nwApp cs4=%s{aggregate} cs4Label=aggregated cs5=%s{threatcat}
cs5Label=threatcat cs6=%s{threatname} cs6label=threatname cn1=%d{durationms}
cn1Label=durationms cn2=%d{numsessions} cn2Label=numsessions cs5Label=ipCat
cs5=%s{ipcat} destCountry=%s{destcountry} avgduration=%d{avgduration}\n

```

- **User Obfuscation:** Choose **Disable** to display the usernames.
 - **Time zone:** By default, this is set to the organization's time zone.
 - **Duplicate Logs:** Enter the number of 60 (in minutes).
4. Click **Save** and **Activate** the change.

3.3 To configure a feed for the DNS Logs

1. Go to **Administration > Nanolog Streaming Service**.
2. In the **NSS Feeds** tab, click **Add NSS Feed**.

The **Add NSS Feed** window appears.

3. In the **Add NSS Feed** window, enter the following details.

- **Feed Name:** Enter the name as **DNS logs**.
- **NSS Type:** Select **NSS for Firewall**.
- **NSS Server:** Choose an NSS from the list.
- **Status:** It is **Enabled** by default.
- **SIEM Destination Type:** The type of destination.
 - **SIEM IP Address:** Enter the IP address of EventTracker.
- **SIEM TCP Port:** Enter port number 514.
- **Log Type:** Choose **DNS Logs**.
- **Feed Output Type:** Select **Custom**.
- **Feed Output Format:** For **NSS Feeds** for Web logs, copy and paste the pre-populated Feed Output format with the following.

```

%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss-fw-dns
CEF:0|Zscaler|NSSFWlog|5.7| %s{action}| %s{rulelabel}|3| act=%s{
action} suser=%s{login} cip=%s{cip} cpt=%d{cport} spriv=%s{loc
ation} reason=%s{rulelabel} in=%ld{inbytes} out=%ld{outbytes}
deviceDirection=1 durationms=%d{durationms} ruleresponse=%s{re
srulelabel} responseaction=%s{resaction} suser=%s{login} serve
ripaddress=%s{sip} serverport=%d{sport} externalId=%d{recordid}
} FQDN=%s{req} Domaincategory=%s{domcat} requesttype=%s{reqtyp
e} encoded=%s{eedone} datacentername=%s{datacenter} detecenter
city=%s{datacentercity} datacentercountry=%s{datacentercountry}
}\n

```

- **User Obfuscation:** Choose **Disable** to display the usernames.

- **Time zone:** By default, this is set to the organization's time zone.
 - **Duplicate Logs:** Enter the number to 60 (in minutes).
4. Click **Save** and Activate the change.

3.4 To configure a feed for the Alerts

1. Go to **Administration > Nanolog Streaming Service**.
2. In the **NSS Feeds** tab, click **Add NSS Feed**.
The **Add NSS Feed** window appears.
3. In the **Add NSS Feed** window, enter the following details.
 - **Feed Name:** Enter the name as **Alerts**.
 - **NSS Type:** Select **NSS for Web**.
 - **NSS Server:** Choose an NSS from the list.
 - **Status:** The NSS feed is **Enabled** by default.
 - **SIEM Destination Type:** The type of destination.
 - **SIEM IP Address:** Enter the IP address of EventTracker.
 - **SIEM TCP Port:** Enter port number 514.
 - **Log Type:** Choose **Alerts**.
4. Select at which levels alerts will be sent: **Critical**.
5. Click **Save** and activate the change.

3.5 To configure a feed for the Tunnel Logs

1. Go to **Administration > Nanolog Streaming Service**.
2. From the **NSS Feeds** tab, click **Add NSS Feed**.
The **Add NSS Feed** window appears.
3. In the **Add NSS Feed** window, enter the following details.
 - **Feed Name:** Enter the name as **Tunnel logs**.
 - **NSS Type:** Select **NSS for Web**.
 - **NSS Server:** Choose an **NSS** from the list.
 - **Status:** The NSS feed is **Enabled** by default.
 - **SIEM Destination Type:** The type of destination.
 - **SIEM IP Address:** Enter the **IP** address of EventTracker.
 - **SIEM TCP Port:** Enter port number 514.
 - **SIEM Rate (Events per Second):** Leave as unrestricted or unlimited.
 - **Log Type:** Choose **Tunnel**.
 - **Record Type:** Specify the tunnel log record types to send in the single NSS Feed:
 - **Tunnel Event:** Status change events (applies to both GRE and IPSec)
 - **Feed Output Type:** Select **Custom**.
 - **Feed Output Format:** For **NSS Feeds** for Web logs, copy and paste the pre-populated **Feed Output Format** with the following.

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss-tunnel CE
F:0|Zscaler|NSSWeblog|5.7|s{action}|s{reason}|3| act=s{action}
```

```
reason=%s{reason} app=%s{proto} dhost=%s{ehost} dst=%s{sip} src=%s{cintip} sourceTranslatedAddress=%s{cip} in=%d{respsize} out=%d{reqsize} request=%s{eurl} requestContext=%s{ereferer} outcome=%s{respcode} requestClientApplication=%s{ua} requestMethod=%s{reqmethod} suser=%s{login} spriv=%s{location} externalId=%d{recordid} fileType=%s{filetype} destinationServiceName=%s{appname} cat=%s{urlcat} deviceDirection=1 cn1=%d{riskscore} cn1Label=riskscore cs1=%s{dept} cs1Label=dept cs2=%s{urlcat} cs2Label=urlcat cs3=%s{malwareclass} cs3Label=malwareclass cs4=%s{malwarecat} cs4Label=malwarecat cs5=%s{threatname} cs5Label=threatname cs6=%s{bamd5} cs6Label=md5hash rulelabel=%s{rulelabel} ruletype=%s{ruletype} urlclass=%s{urlclass} devicemodel=%s{devicemodel} devicehostname=%s{devicehostname}\n.
```

- **Timezone:** By default, this is set to the organization's time zone.
- **Duplicate Logs:** Enter the number of 60 (in minutes).

3. Click **Save** and activate the change.

3.6 To configure a feed for the SaaS Security logs

1. Go to **Administration > Nanolog Streaming Service**.
2. In the **NSS Feeds** tab, click **Add NSS Feed**.

The **Add NSS Feed** window appears.

3. In the **Add NSS Feed** window, enter the following details.

- **Feed Name:** Enter the name as **SaaS security logs**.
- **NSS Type:** Select **NSS for Web**.
- **NSS Server:** Choose an **NSS** from the list.
- **Status:** The NSS feed is **Enabled** by default.
- **SIEM Destination Type:** The type of **destination**.
 - **SIEM IP Address:** Enter the IP address of EventTracker.
- **SIEM TCP Port:** Enter port number 514.
- **Log Type:** Choose **SaaS Security API**.
- **SIEM Rate Limit (Events per Second):** Leave as unrestricted or unlimited.
- **Feed Output Type:** Select **Custom**.
- **Feed Output Format:** For **NSS Feeds** for Web logs, copy and paste the pre-populated Feed Output Format with the following.

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss-saas CEF:0|Zscaler|NSSWeblog|5.7|%s{action}|%s{reason}|3| act=%s{action} reason=%s{reason} app=%s{proto} dhost=%s{ehost} dst=%s{sip} src=%s{cintip} sourceTranslatedAddress=%s{cip} in=%d{respsize} out=%d{reqsize} request=%s{eurl} requestContext=%s{ereferer} outcome=%s{respcode} requestClientApplication=%s{ua} requestMethod=%s{reqmethod} suser=%s{login} spriv=%s{location} externalId=%d{recordid} fileType=%s{filetype} destinationServiceName=%s{appname} cat=%s{urlcat} deviceDirection=1 cn1=%d{riskscore} cn1Label=riskscore cs1=
```

```
s{dept} cs1Label=dept cs2=%s{urlcat} cs2Label=urlcat cs3=%s{malwareclass} cs3Label=malwareclass cs4=%s{malwarecat} cs4Label=malwarecat cs5=%s{threatname} cs5Label=threatname cs6=%s{bamd5} cs6Label=md5hash rulelabel=%s{rulelabel} ruletype=%s{ruletype} urlclass=%s{urlclass} devicemodel=%s{devicemodel} devicehostname=%s{devicehostname}\n
```

- **User Obfuscation:** Choose **Disable** to display the usernames.
- **Timezone:** By default, this is set to the organization's time zone.
- **Duplicate Logs:** Enter the number to 60 (in minutes).

4. Click **Save** and activate the change.

4. EventTracker Knowledge Packs

After the logs are received by EventTracker, the Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs are available in the EventTracker to support the **Zscaler Internet Access CA**.

4.1 Categories

- **Zscaler Internet Access CA: DNS activities** - This category provides information related to the domain name services events.
- **Zscaler Internet Access CA: Firewall activities** - This category provides information related to the firewall traffic events like allowed, denied, blocked traffic.
- **Zscaler Internet Access CA: SaaS security activities** - This category provides information related to the current state of the organization's security posture for the SaaS application events.
- **Zscaler Internet Access CA: Tunnel activities** - This category provides information related to tunnel traffic events.
- **Zscaler Internet Access CA: Web access activities** - This category provides information related to the web access details on your organization.

4.2 Alerts

- **Zscaler Internet Access CA: IPS traffic detected** - This alert generates whenever the Zscaler detects Intrusion prevention traffic.
- **Zscaler Internet Access CA: Malicious file has been detected** - This alert generates whenever the Zscaler detects a malicious file.

4.3 Reports

- **Zscaler Internet Access CA – Web access activities** – This report gives information about the web access details on your organization. It contains the field information like the username, source IP, destination IP, hostname, action, reason, URL address, a risk score of URL, total bytes in, total bytes out, etc.

Sample Report

LogTime	Computer	User Name	Reason	Action	Device Host Name	Source IP	Destination Host	Destination IP
10/06/2021 07:24:49 PM	ZSCALER-SYSLOG	kenneth	Not allowed to use this File Share site	denied	THINKPADkenneth	108.6.212.216	WKSETRWE24	17.247.135.233
10/06/2021 07:24:50 PM	ZSCALER-SYSLOG	maya	Not allowed to use this File Share site	denied	THINKPADmaya	108.6.212.215	WKSETRWE24	17.247.135.233

Sample Logs

```
Oct 22 11:26:13 10.10.110.63 Oct 22 10:24:30 zscaler-nss-web
CEF:0|Zscaler|NSSWeblog|5.7| Denied| Not allowed to use this File Share site|4|
act=denied reason=Not allowed to use this File Share site app=IPSEC
dhost=WKSETRWE24 dst=17.247.135.233 src=108.6.212.216
sourceTranslatedAddress=203.0.113.5, 192.168.2.200 in=101500 out=13010 request=
www.trythisencodeurl.com/index%1A%09 requestContext=ksjdjsyriwiojdj outcome=403
requestClientApplication=Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0;
rv:11.0) requestMethod=invalid suser=kenneth@contoso.com spriv=Headquarters
externalId=4745655 fileType=ZIP destinationServiceName=Dropbox cat=
deviceDirection=0 cn1=6 cn1Label=riskscore cs1= Sales cs1Label=dept cs2=
cs2Label=urlcat cs3=Win32.Rans0m.WannaCry cs3Label=malwareclass cs4=Adware
cs4Label=malwarecat cs5=tres.venim cs5Label=threatname
cs6=196a3d797bfee07fe4596b69f4ce1341 cs6Label=md5hash rulelabel= URL_Filtering_1
ruletype=Sandbox urlclass=PrivacyRisk devicemodel=20L8S7WC18
devicehostname=THINKPADkenneth
```

- **Zscaler Internet Access CA – SaaS security activities** – This report gives information about the current state of organization security posture for the SaaS application. It contains the field information like action, hostname, application, source IP address, destination IP address, threat name, URL address, etc.

Sample Report

LogTime	Computer	User Name	Device Host Name	Source IP	Destination Host	Destination IP	Requested URL	Total bytes in	Total Bytes Out
10/06/2021 07:24:49 PM	ZSCALER-SYSLOG	jdoe@safemarch.com	THINKPADJOE	108.6.211.216	WKSETRWE23	17.248.135.233	www.trythisencodeurl.com/index%1A%09	10500	1300
10/06/2021 07:24:50 PM	ZSCALER-SYSLOG	maxx@safemarch.com	THINKPADMAXX	108.6.211.217	WKSETRWE24	17.248.135.234	www.tryencodeurl.com/index%1A%09	10500	1300

Sample Logs

```
Oct 22 11:26:13 10.10.110.63 Oct 22 10:24:30 zscaler-nss-saas
CEF:0|Zscaler|NSSWeblog|5.7| Denied| Not allowed to use this File Share site|3|
act=denied reason=Not allowed to use this File Share site app=IPSEC
dhost=WKSETRWE24 dst=17.248.13.233 src=108.6.211.21
sourceTranslatedAddress=203.0.113.5, 192.168.2.200 in=10500 out=1300 request=
www.trythyfisencodeurl.com/index%1A%09 requestContext=ksjdjsyriwiojhyjdj
outcome=403 requestClientApplication=Mozilla/5.0 (Windows NT 6.1; WOW64;
Trident/7.0; rv:11.0) requestMethod=invalid suser=smith spriv=Headquarters
```

```
externalId=4754534655 fileType=ZIP destinationServiceName=Dropbox cat=
deviceDirection=1 cn1=6 cn1Label=riskscore cs1= Sales cs1Label=dept cs2=
cs2Label=urlcat cs3=Win32.Ransom.WannaCry cs3Label=malwareclass cs4=Adware
cs4Label=malwarecat cs5=trs.venum cs5Label=threatname
cs6=196a3d797bfee07fe4596b69f4ce11211 cs6Label=md5hash rulelabel=
URL_Filtering_1 ruletype=Sandbox urlclass=PrivacyRisk devicemodel=20L8S7WC08
devicehostname=THINKPADSMITH
```

- **Zscaler Internet Access CA – Tunnel activities** - This report gives information about the tunnel traffic. It contains the field information like the IP address, location, destination IP address, tunnel type, VPN name, etc.

Sample Report

LogTime	Computer	User Name	Action	Tunnel	Source IP	Source Port	Destination IP	Destination Port	Protocol	Source Location
10/06/2021 07:24:49 PM	ZSCALER-SYSLOG	joe	blocked	L2Tunnel	12.5.56.45	2526	198.51.100.54	22	TCP	Suboffice
10/06/2021 07:24:50 PM	ZSCALER-SYSLOG	kenneth	allowed	IPSEC	12.5.56.44	2527	198.51.100.23	22	TCP	Suboffice

Sample Logs

```
Oct 22 11:26:13 10.10.110.63 Oct 22 10:24:30 zscaler-nss-tunnel
CEF:0|Zscaler|NSSWeblog|5.7| Denied| Not allowed to use this File Share site|5|
act=denied reason=Not allowed to use this File Share site app=IPSEC
dhost=WKSETRWE28 dst=16.248.135.233 src=108.6.211.21
sourceTranslatedAddress=203.0.113.5, 192.168.2.200 in=10500 out=1300 request=
www.troythisencodeurl.com/index%1A%09 requestContext=ksjdjssyriwiojdj
outcome=403 requestClientApplication=Mozilla/5.0 (Windows NT 6.1; WOW64;
Trident/7.0; rv:11.0) requestMethod=invalid suser=joe@contoso.com
spriv=Headquarters externalId=475989655 fileType=ZIP
destinationServiceName=Dropbox cat= deviceDirection=1 cn1=5 cn1Label=riskscore
cs1= Sales cs1Label=dept cs2= cs2Label=urlcat cs3=Win32.Ransom.WannaCry
cs3Label=malwareclass cs4=Adware cs4Label=malwarecat cs5=trs.venim
cs5Label=threatname cs6=196a3d797bfee07fe4596b69f4ce1141 cs6Label=md5hash
rulelabel= URL_Filtering_1 ruletype=Sandbox urlclass=PrivacyRisk
devicemodel=20L8S7WC28 devicehostname=THINKPADjoe
```

- **Zscaler Internet Access CA – DNS activities** - This report gives information about the domain name service events. It contains the field information like the client IP address, server IP address, datacenter name, datacenter location, record type, username, response type, reason, action, etc.

Sample Report

LogTime	Computer	User Name	Action	Client IP	Source Location	Duration	Rule Response	Response Action	Server IP	Server Port
10/11/2021 07:42:25 PM	ZSCALER-SYSLOG	kenneth	REQ_ALLOW	10.20.1.13	Headquarters	456345	dns default request	allowed	192.168.2.200	4536
10/11/2021 07:42:25 PM	ZSCALER-SYSLOG	kenneth	REQ_BLOC	10.20.1.14	Headquarters	456345	dns spoc request	blocked	192.168.2.200	4536

Sample Logs

```
Oct 22 11:26:13 10.10.110.63 Oct 22 10:24:30 zscaler-nss-fw-dns
CEF:0|Zscaler|NSSFWlog|5.7|REQ_ALLOW|%s{rulelabel}|3| act=REQ_ALLOW
suser=kenneth cip=100.20.11.13 cport= spriv=Headquarters reason=dns_request in=
out= deviceDirection=1 durationms=456345 ruleresponse=dns default request
```

```
responseaction=allowed suser= serveripaddress=192.168.2.200 serverport=4536
externalId=2142342 FQDN=mail.safemarch.com Domaincategory=Professional Services
requesttype=A record encoded=faffawrjghkyrth datacentername=CA Client Node DC
detecentercity=Sa datacentercountry=US
```

- **Zscaler Internet Access CA – Firewall activities** - This report gives information about the firewall traffic events like allowed, denied, blocked traffic. It contains the field information like reason, action, source IP address, source port, destination IP address, destination port, total duration, total bytes in, total bytes out, protocol, etc.

Sample Report

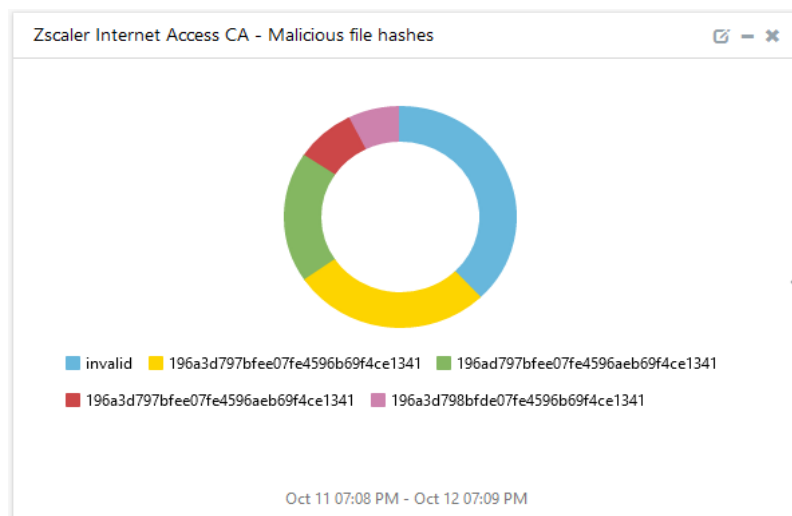
LogTime	Computer	User Name	Action	Source IP	Source Port	Destination IP	Destination Port	Protocol	Source Location
10/06/2021 07:24:49 PM	ZSCALER-SYSLOG	joe	blocked	12.5.56.45	2526	198.51.100.54	22	TCP	Suboffice
10/06/2021 07:24:50 PM	ZSCALER-SYSLOG	kenneth	allowed	12.5.56.44	2527	198.51.100.23	22	TCP	Suboffice
10/06/2021 07:24:51 PM	ZSCALER-SYSLOG	maya	blocked	12.5.56.55	45263	198.51.100.57	22	TCP	Suboffice

Sample Logs

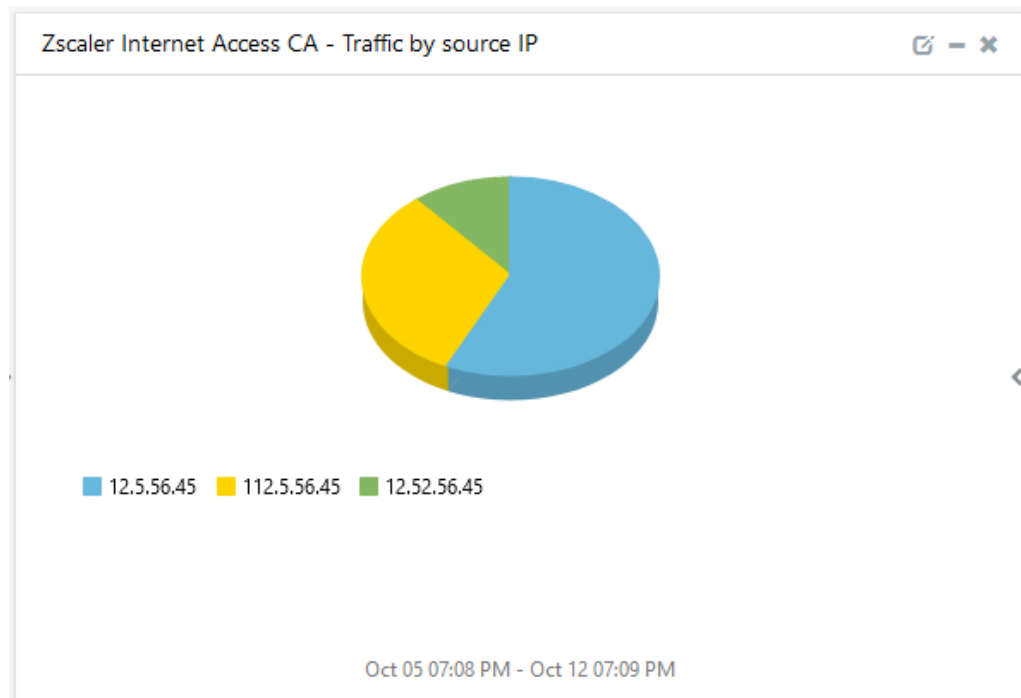
```
Oct 22 11:26:13 10.10.110.63 Oct 22 10:24:30 zscaler-nss-fw
CEF:0|Zscaler|NSSFWlog|5.7|allowed|Default firewall filtering rule|3|
act=allowed suser= maxx@safemarch.com src=12.52.56.45 spt=2526 dst=198.52.100.54
dpt=22 deviceTranslatedAddress=18.51.65.42 deviceTranslatedPort=22
destinationTranslatedAddress= destinationTranslatedPort= 192.0.2.100
sourceTranslatedAddress= 192.0.2.15 sourceTranslatedPort=22 proto=TCP
tunnelType=IPSEC dnat=yes spriv=Suboffice reason=Default firewall filtering rule
in=51556 out=6269665 deviceDirection=1 cs1=Development cs1Label=dept cs2=HTTP
cs2Label=nwService cs3=teams cs3Label=nwApp cs4=aggre cs4Label=aggregated
cs5=clean cs5Label=threatcat cs6=clean cs6label=threatname cn1=58555
cn1Label=durationms cn2=6 cn2Label=numsessions cs5Label=ipCat cs5=Finance
destCountry=USA avgduration= 600,000
```

4.4 Dashboards

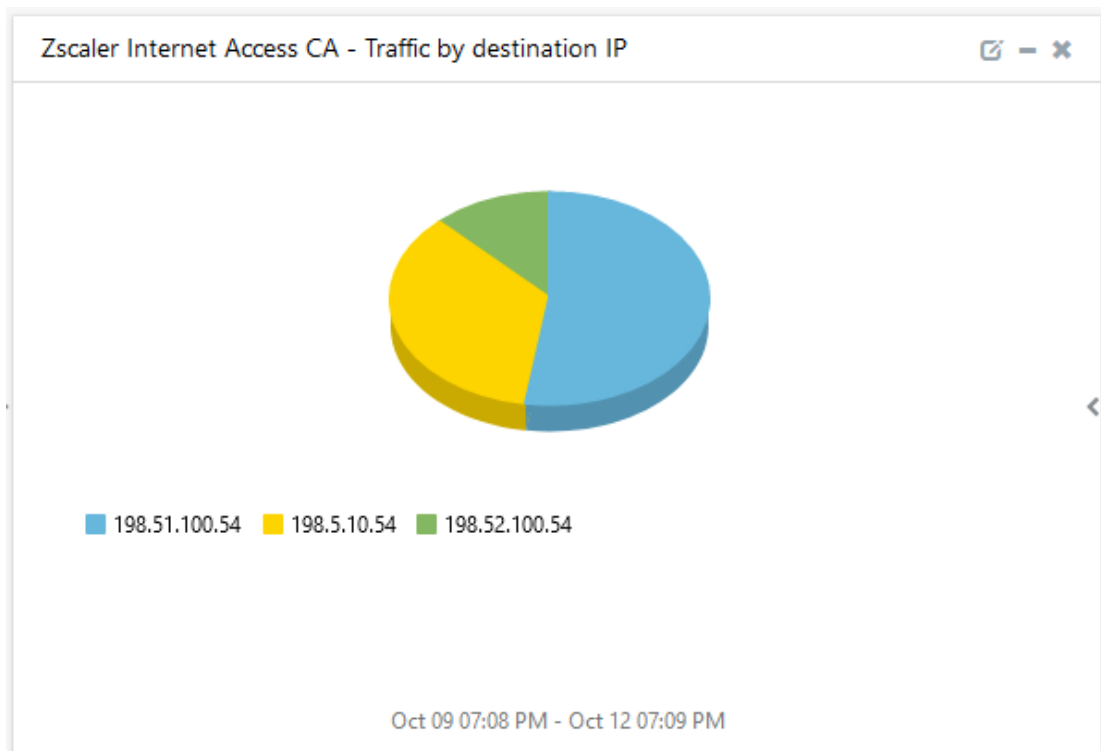
- **Zscaler Internet Access CA - Malicious file hashes**



- **Zscaler Internet Access CA - Traffic by the Source IP**



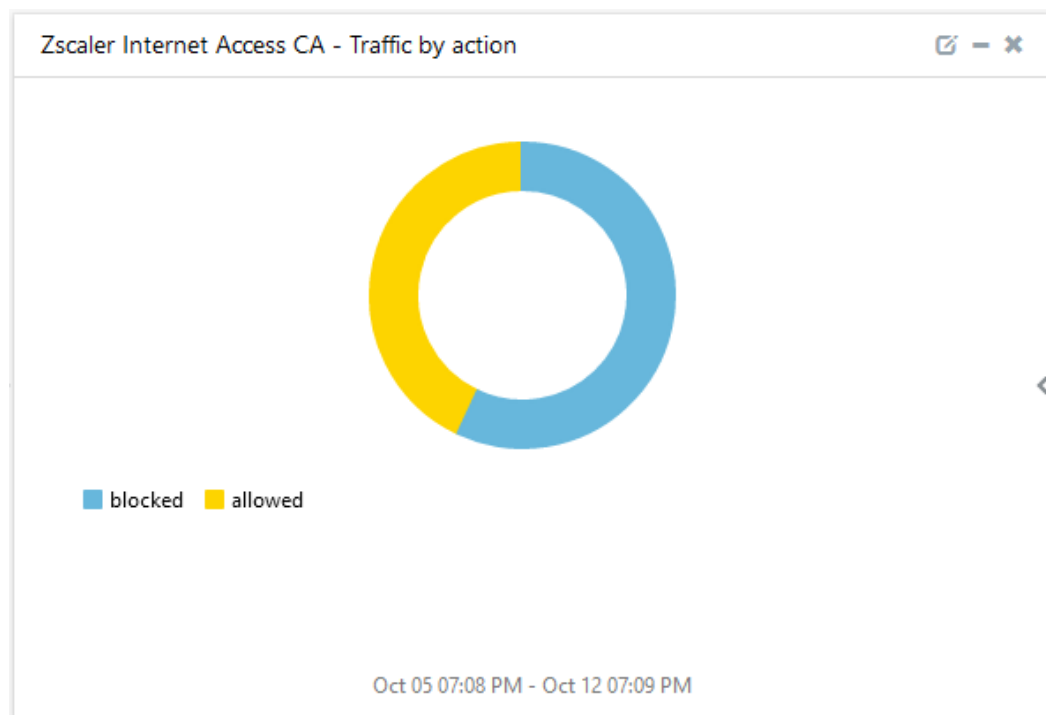
- **Zscaler Internet Access CA - Traffic by the destination IP**



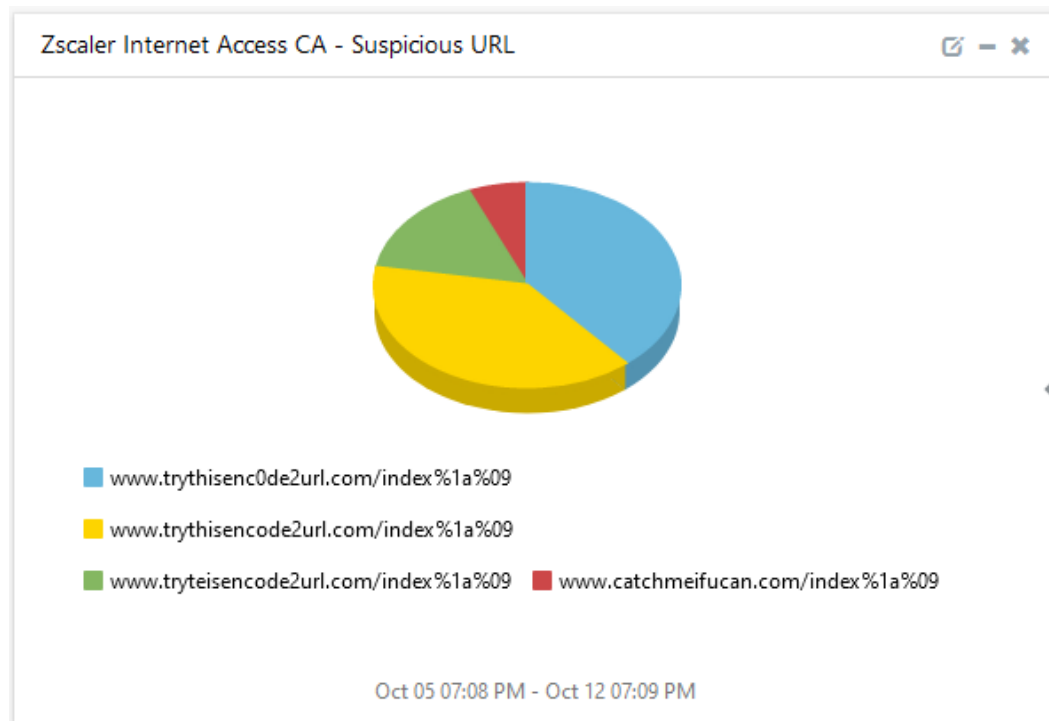
- **Zscaler Internet Access CA - Source IP traffic by the geo-location**



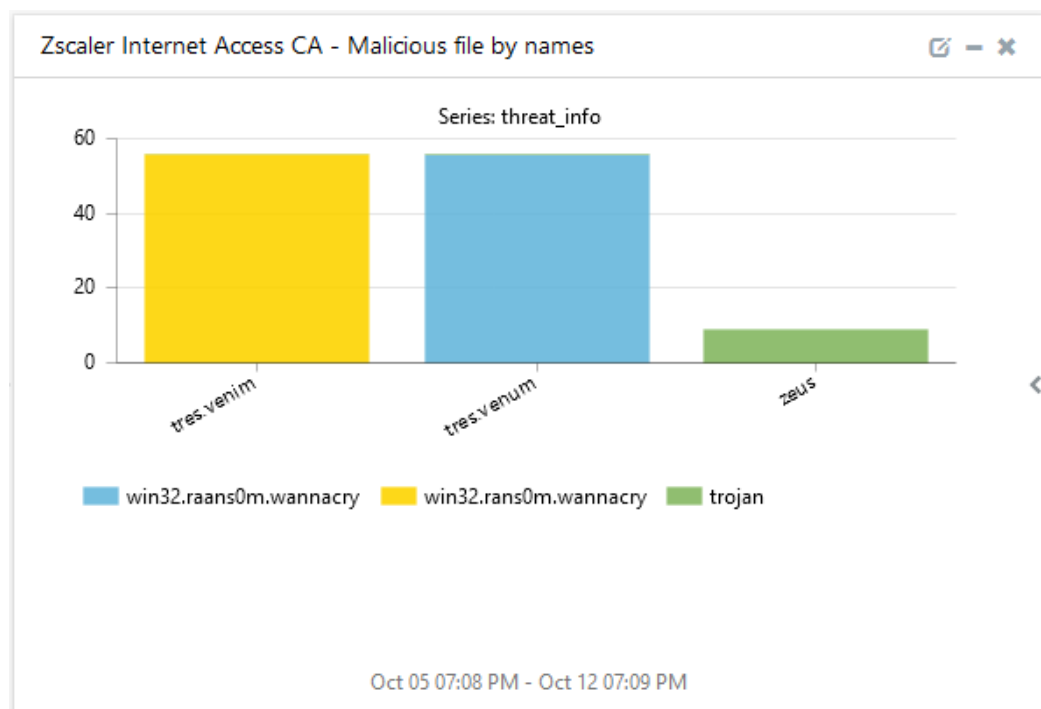
- **Zscaler Internet Access CA - Traffic by Action**



- Zscaler Internet Access CA - Suspicious URL



- Zscaler Internet Access CA - Malicious file by names

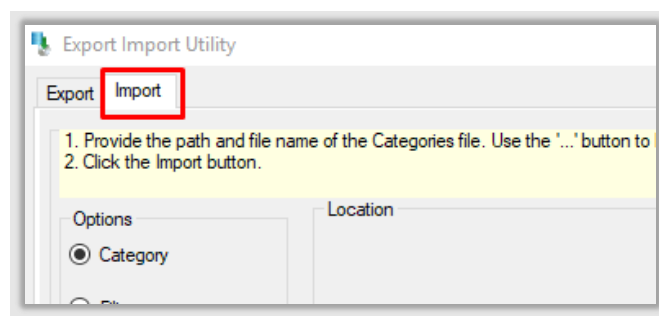
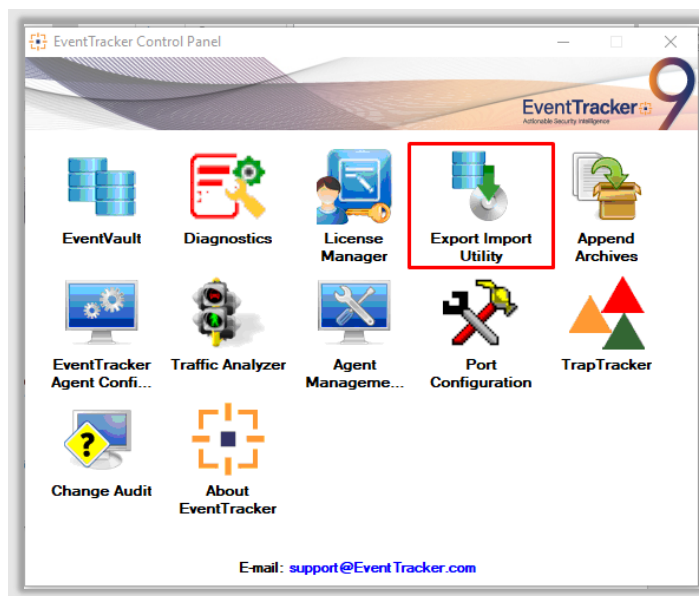


5. Importing Zscaler Internet Access CA Knowledge Pack into EventTracker

NOTE: Import the Knowledge Pack items in the following sequence:


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

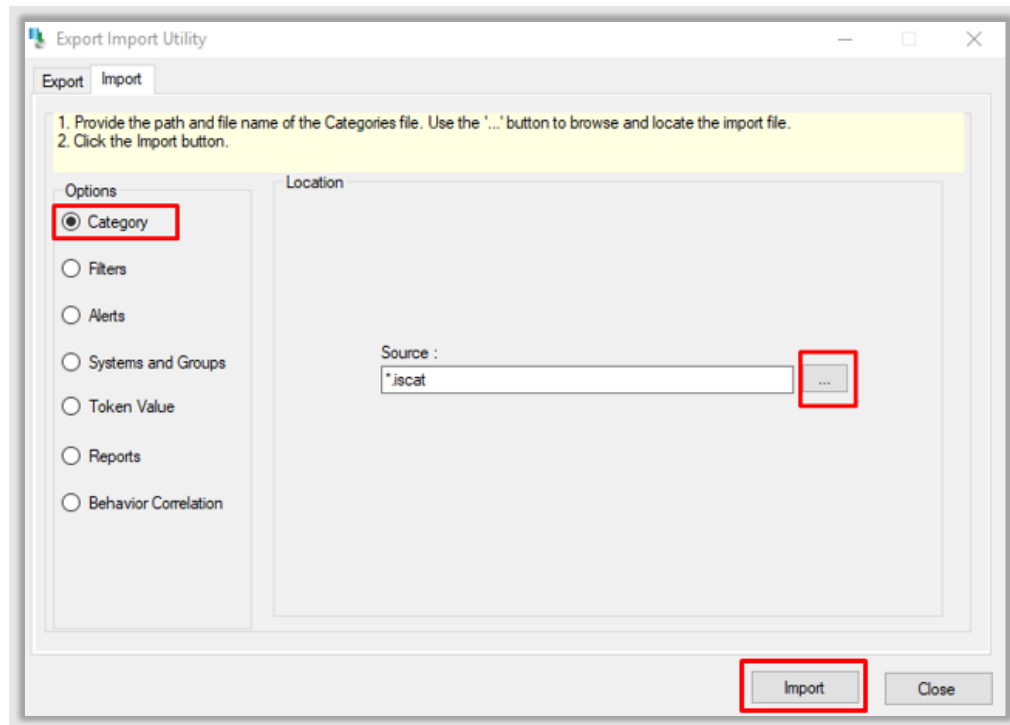
1. Launch the **EventTracker Control Panel**.
2. Double click **Export-Import Utility**.



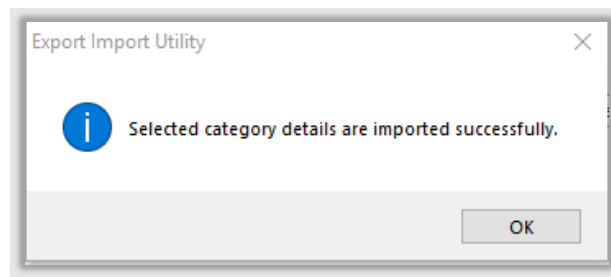
3. Click the **Import** tab.

5.1 Categories

1. After opening the **Export-Import Utility** via the **EventTracker Control Panel**, click the **Category** option, and then click Browse .
2. Navigate to the Knowledge Pack folder and select the file with the extension **".iscat"**, e.g., **"Categories_Zscaler Internet Access CA .iscat"** and click the **Import** button.

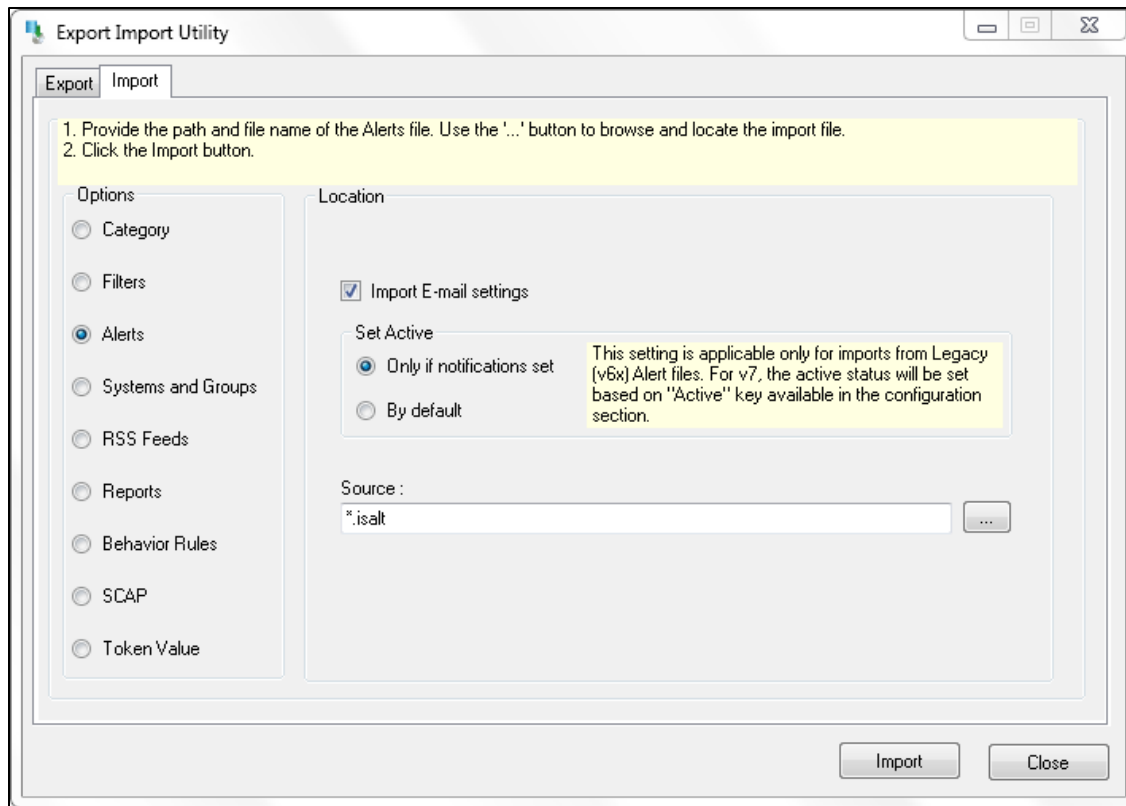


EventTracker displays a success message.

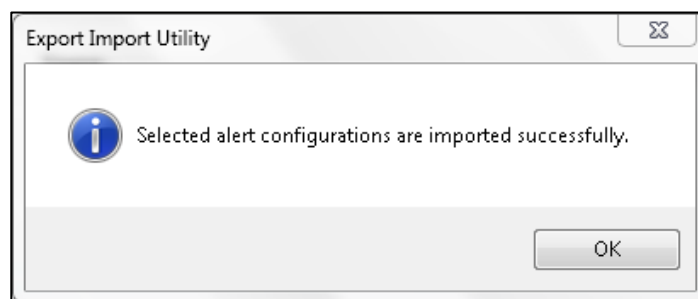


5.2 Alerts

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



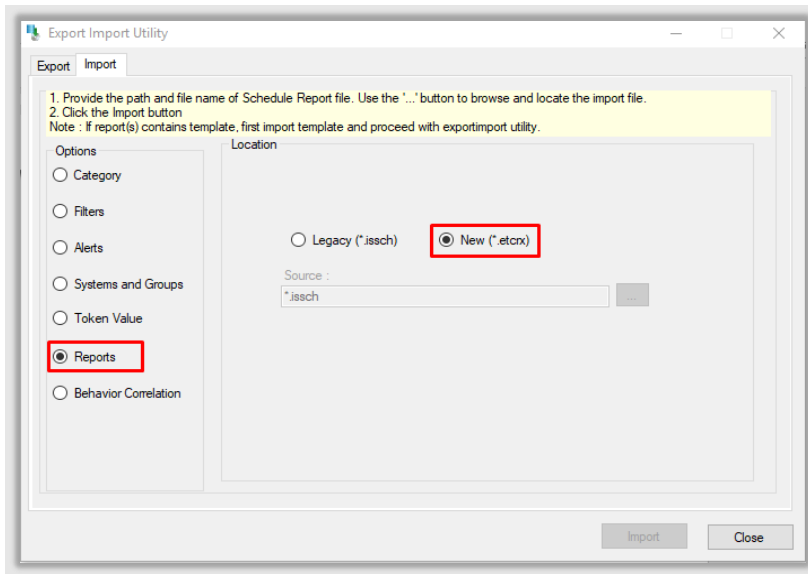
2. Locate the **Alerts_Zscaler Internet Access CA.isalt** file, and then click the **Open** button.
3. To import the alerts, click the **Import** button.
4. EventTracker displays a success message.



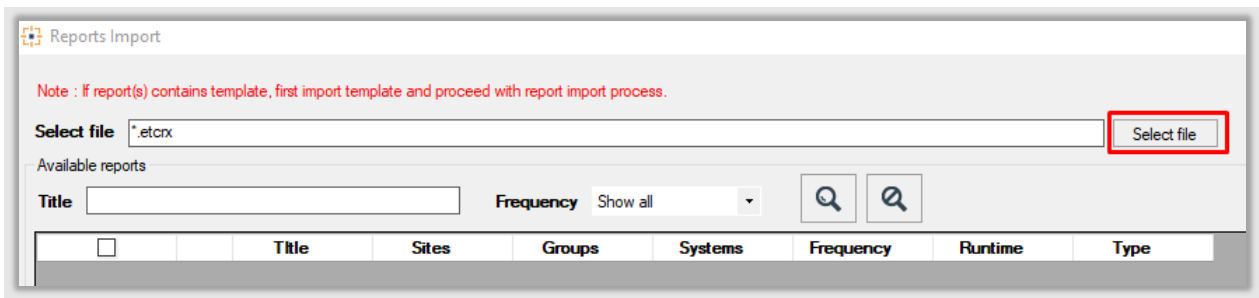
5. Click the **OK** button, and then click the **Close** button.

5.3 Reports

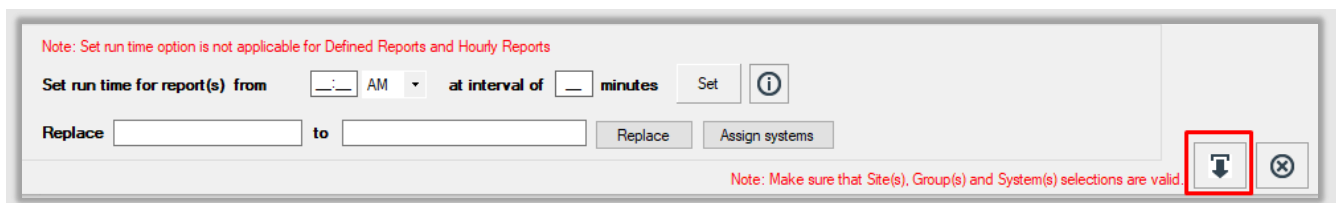
1. In the EventTracker Control Panel, select **Export/ Import utility** and select the **Import tab**. Then, click the **Reports** option, and choose **New (*.etcrx)**.



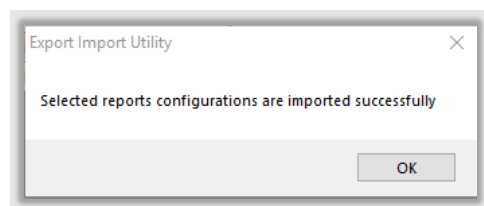
- After selecting the **New (*.etcrx)** file, a new pop-up window appears. Click the **Select File** button and navigate to the file path with a file having the extension **".etcrx"**, e.g., **Reports_ Zscaler Internet Access CA .etcrx**.



- Wait while the reports populate in the below tables. Now, select all the relevant reports and then click the **Import** button.

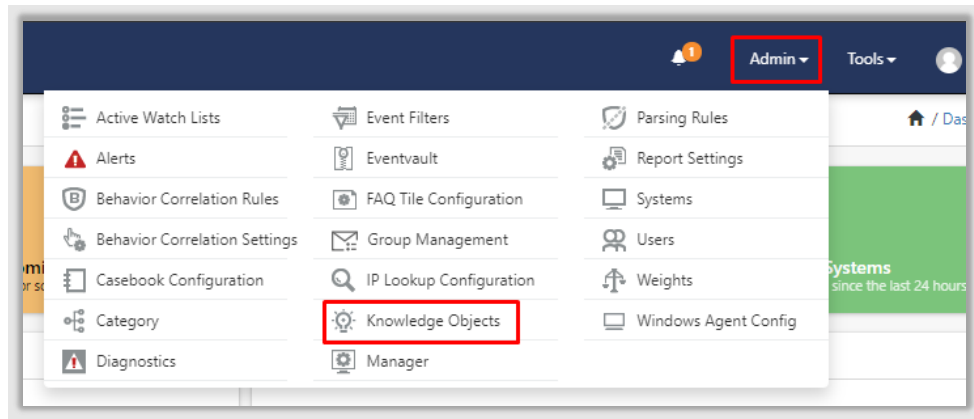


EventTracker displays a success message.

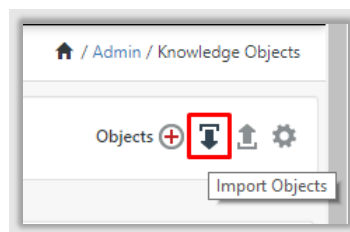


5.4 Knowledge Objects

1. Click **Knowledge Objects** under the **Admin** option on the EventTracker page.



2. Click the **import object** icon.



3. A pop-up box appears, click **Browse** and navigate to the Knowledge Packs folder (type `%et_install_path%\Knowledge Packs` in the navigation bar) with the extension `".etko"`, e.g., `KO_Zscaler Internet Access CA .etko`, and then click **Upload**.

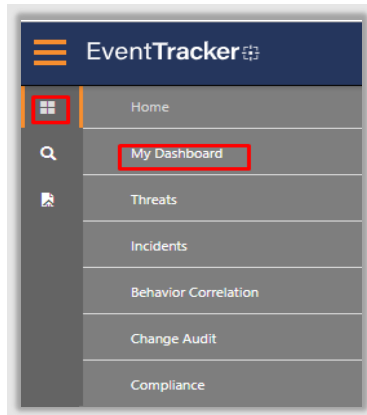


4. A list of available Knowledge Objects will appear. Select the relevant files and click the **Import** button.

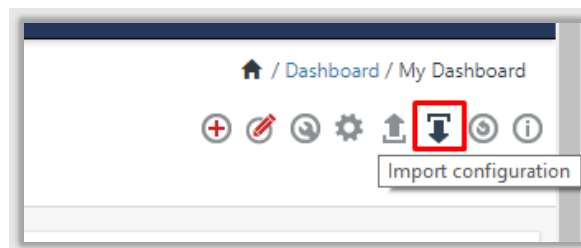


5.5 Dashboards

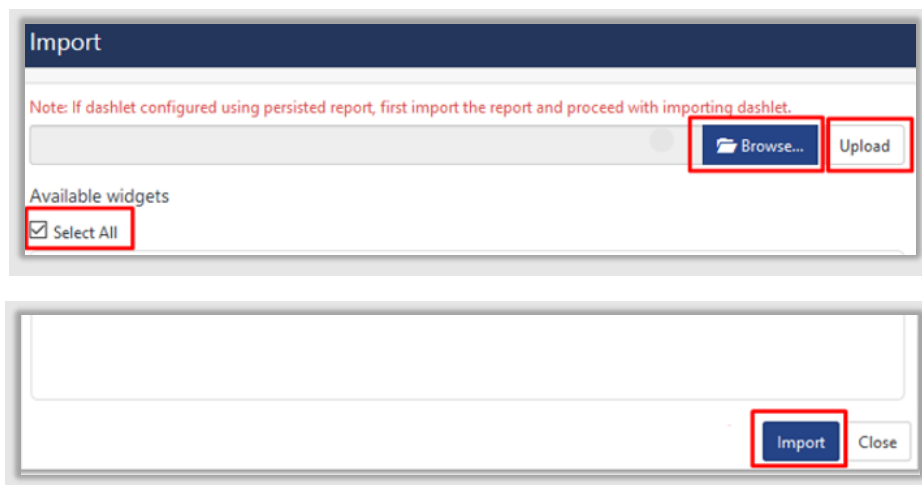
1. Login to **EventTracker**.
2. Navigate to **Dashboard** → **My Dashboard**.



3. In **My Dashboard**, Click the **Import** button.



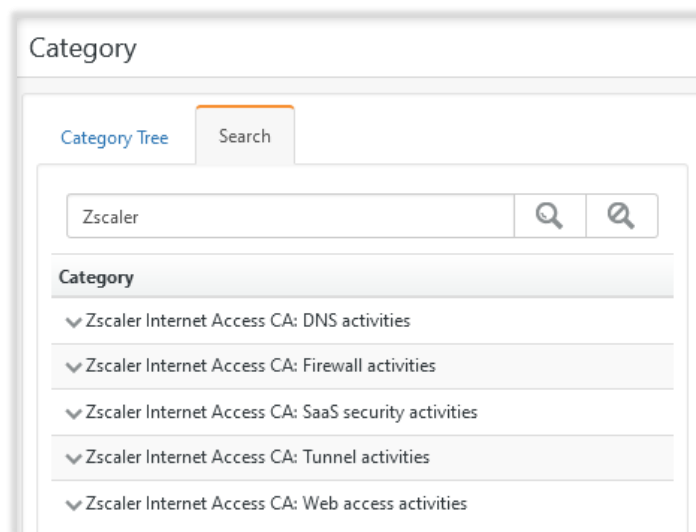
4. Select the **browse** button and navigate to the Knowledge Pack folder (type **%et_install_path%\Knowledge Packs** in the navigation bar) where the **.etwd** file is saved, e.g., **Dashboards_Zscaler Internet Access CA .etwd** and click **Upload**.
5. Wait while EventTracker populates all the available dashboards. Now, choose **Select All** and click the **Import** button.



6. Verifying Zscaler Internet Access CA Knowledge Pack in the EventTracker

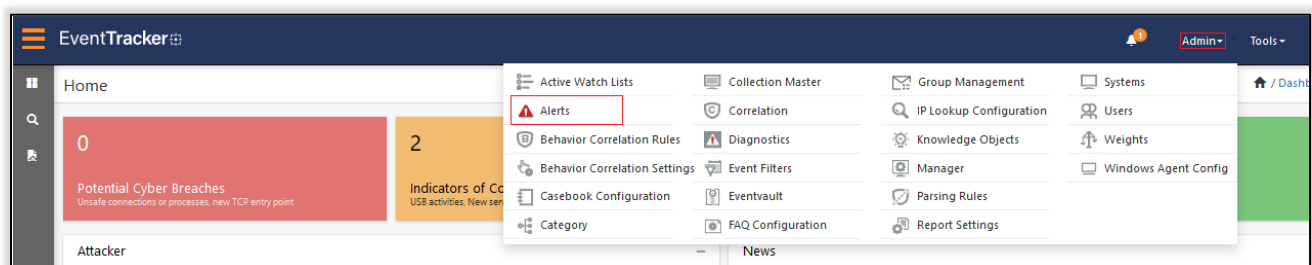
6.1 Categories

1. Login to **EventTracker**.
2. Click the **Admin** dropdown, and then click **Categories**.
3. In the **Category Tree** scroll down and expand the **Zscaler Internet Access CA** group folder to view the imported categories.



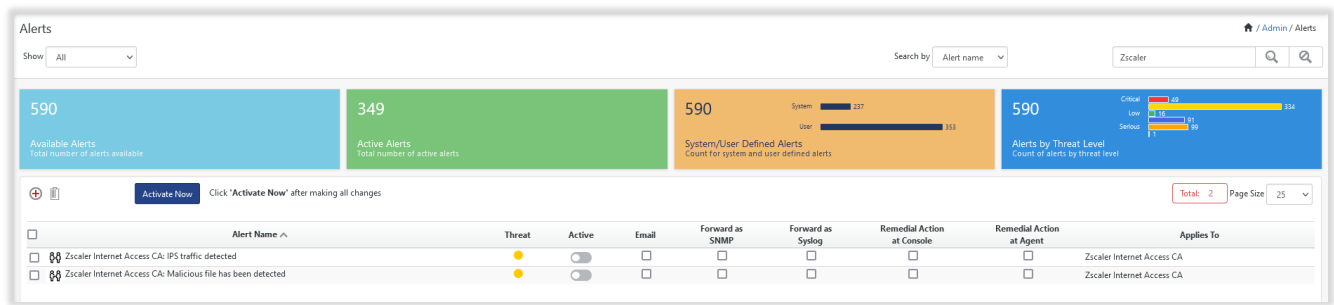
6.2 Alerts

1. Login to **EventTracker**.
2. Click the **Admin** menu, and then click **Alerts**.



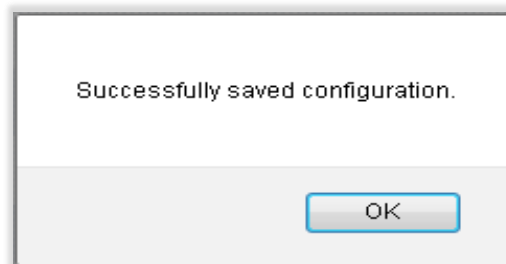
3. In the **Search** box, type **Zscaler Internet Access CA**, and then click the **Go** button.

The **Alert Management** page will display all the imported alerts.



- To activate the imported alerts, select the respective checkboxes in the **Active** column.

EventTracker displays a success message.

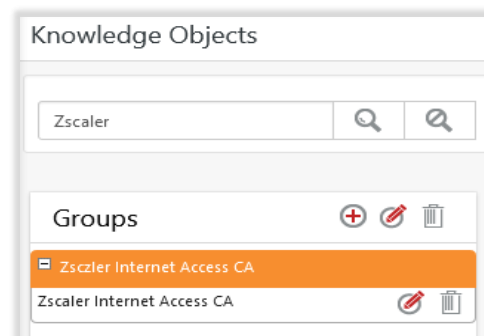


- Click **OK**, and then click the **Activate Now** button.

Note: Specify the appropriate **systems** in the **alert configuration** for better performance.

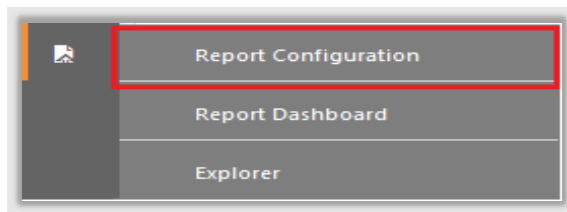
6.3 Knowledge Objects

- In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects**.
- In the **Knowledge Objects** tree, expand the **Zscaler Internet Access CA** group folder to view the imported Knowledge Objects.

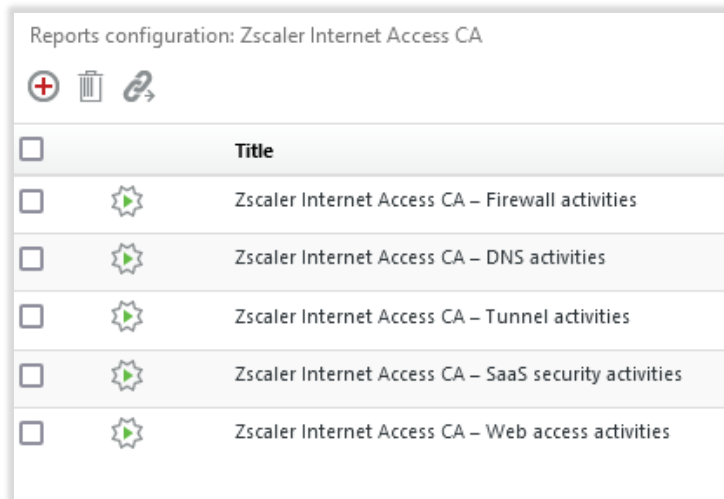


6.4 Reports

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

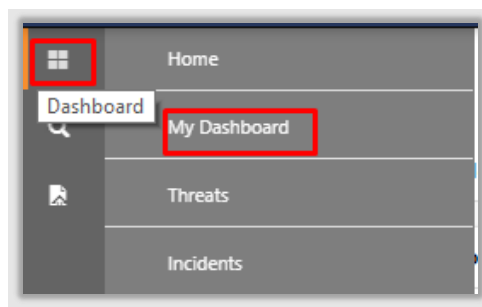


2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click the **Zscaler Internet Access CA** group folder to view the imported reports.

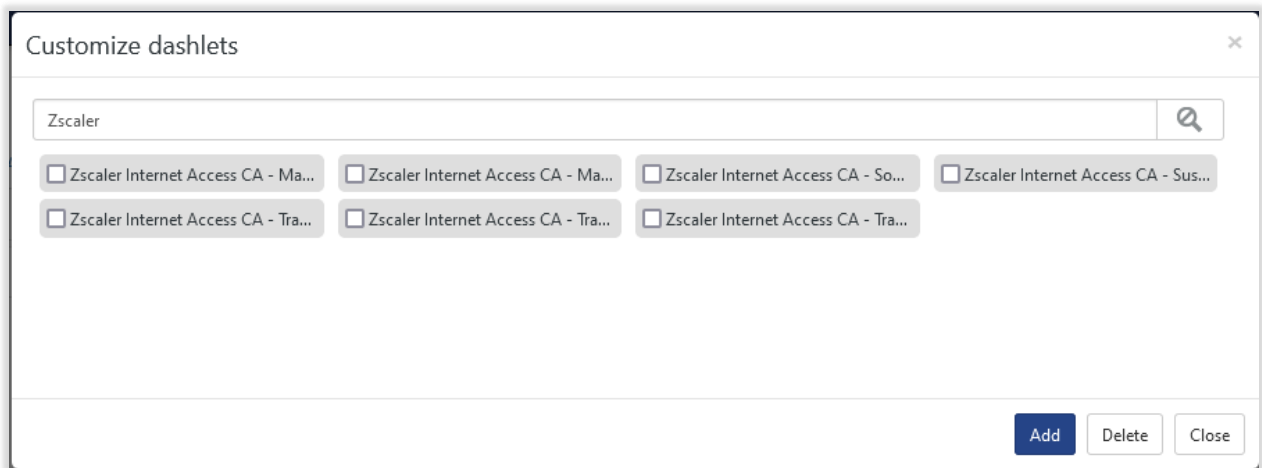
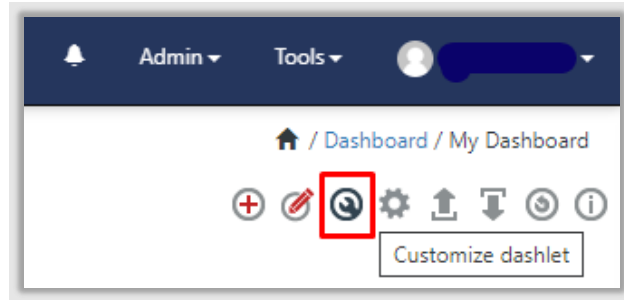


6.5 Dashboards

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



2. Select **Customize daslets**  and type **Zscaler Internet Access CA** in the search bar.



About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's [EventTracker](#) cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service.

Netsurion's [BranchSDO](#) delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations.

Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit [netsurion.com](https://www.netsurion.com) or follow us

on [Twitter](#) or [LinkedIn](#). Netsurion is #23 among [MSSP Alert's 2021 Top 250 MSSPs](#).

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)

EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)

EventTracker Essentials SOC: 877-333-1433 (Option 4)

EventTracker Software Support: 877-333-1433 (Option 5)

<https://www.netsurion.com/eventtracker-support>