

Integration Guide

Integrating Zscaler Internet Access Central Authority (CA) with EventTracker

EventTracker v9.2x and above

Publication Date:

October 28, 2021

© Copyright Netsurion. All Rights Reserved.



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

Та	ble of	Contents
1.	Ove	erview4
2.	Prei	requisites4
3.	Con	figuring Zscaler Internet Access CA4
	3.1	To configure a feed for the Web Logs4
	3.2	To configure a feed for the Firewall Logs6
	3.3	To configure a feed for the DNS Logs8
	3.4	To configure a feed for the Alerts9
	3.5	To configure a feed for the Tunnel Logs9
	3.6	To configure a feed for the SaaS Security logs10
4.	Eve	ntTracker Knowledge Packs11
	4.1	Categories11
	4.2	Alerts11
	4.3	Reports12
	4.4	Dashboards14
5.	Imp	orting Zscaler Internet Access CA Knowledge Pack into EventTracker18
	5.1	Categories19
	5.2	Alerts19
	5.3	Reports
	5.4	Knowledge Objects
	5.5	Dashboards23
6.	Ver	ifying Zscaler Internet Access CA Knowledge Pack in the EventTracker
	6.1	Categories24
	6.2	Alerts
	6.3	Knowledge Objects25
	6.4	Reports
	6.5	Dashboards
	About	Netsurion

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.

d NSS Feed							
S FEED							
Feed Name				NSS Type			
web log				NSS for We	NSS for Fire	wall	
ISS Server				Status			
NSS_Server1		<u> </u>		Enabled	Disabled		
IEM Destination Typ	e			SIEM IP Address	5		
IP Address	FQDN			10.8.10.11			
IEM TCP Port							
14							
IEM Rate	United						
O Onininited	Cimited						
og Type	and Alast	Ъ					
	Alerc	_					
eed Output Type		~		Feed Escape Ch	aracter		
10010111							
%s(mon) %02d(dd) %& =%s(reason) app=%s; request=%s(aur1) re suser=%s(login) spr deviceDirection=1 o cs3Label=malwarecla rulelabel=%s(rulela	22d{hh}:%02d{m (proto} dhost=0 equestContext=0 riv=%s{locatior rn1=%d{riskscor ass cs4=%s{malw abel} ruletype	n):%02d{ss} zscale is{ehost} dst=%s{s is{ereferer} outco n} externalId=%d{rr re} cnLabel=risks warecat} cs4Label== %s(ruletype) urlc;	r-nss CEF:0 Zscaler ip} src=%s(cintip) me=%s{respcode} req ecordid} fileType=% core cs1=%s{dept} c malwarecat is5=%s{t lass=%s{urlclass}	NSSWeblog 5.7 %s{a sourceTranslatedAd westClientApplicati s[filetype] destina slLabel=dept cs2=%s hreatname} csSLabel	ction} %s{reason} fress=%s{cip} in=%d ion=%s{ua} requestM tionServiceName=%s :{urlcat} cs2Label= _=threatname cs6=md	3 act=%s{action) (respsize) out=%d ethod=%s{reqmetho (appname) cat=%s{ urlcat cs3=%s{ma] Shash cs6Label=%s	<pre>{reason {reqsize} d} urlcat} wareclass} {band5} </pre>
lser Obfuscation				Timezone			
Enabled	Disabled			GMT		~	
Juplicate Logs							
		~					
Disabled							
Disabled							
ACTION	WHO	FROM WHERE	TRANSACTION	TO WHERE	SECURITY	FILE TYPE	DLP
	WHO	FROM WHERE	TRANSACTION	TO WHERE	SECURITY	FILE TYPE	DLP
ACTION VEB LOG FILTERS	WHO	FROM WHERE	TRANSACTION	TO WHERE Policy Reason	SECURITY	FILE TYPE	DLP

- 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{appname} cat=%s{urlc
at} deviceDirection=1 cn1=%d{riskscore} cn1Label=riskscore cs1=%s
{dept} cs1Label=dept cs2=%s{urlcat} cs2Label=urlcat cs3=%s{malware
cat cs5=%s{threatname} cs5Label=threatname cs6=%s{bamd5} cs6Label
```



```
=md5hash rulelabel=%s{rulelabel} ruletype=%s{ruletype} urlclass=%
s{urlclass} devicemodel=%s{devicemodel} devicehostname=%s{deviceh
ostname}\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. Goto 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.

Netsurion®

d NSS Feed						
FEED						
eed Name Firewall Log				NSS Type NSS for Wel	b ONSS for Firewall	
SS Server ISS_Server1		~		Status	Disabled	
IEM Destination Type				SIEM IP Addres	S]
IEM TCP Port						
IEM Rate	ited					
og Type ♥ Firewall Logs	S Logs Ale	ert				
ewall Log Type	Aggregate I	.ogs Both	Session and Aggre	gate Logs		
eed Output Type ustom		~		Feed Escape Cl	haracter	
eed Output Format is{mon} %02d{dd} %02d{ user=%s{login} src=%s lestinationTranslatedA %dftsport} proto=%s{i %ld{inbytes} out=%ld ;muApp cs4=%s{aggregat %d{durationms} cnllab	hh]:%02d{mm}:% {csip} spt=%d{ ddress=%s{sdip pproto} tunnel outbytes} devi e} cs4Label=ag el=durationms	82d{ss} zscaler csport} dst=%s{d } destinationTra Type=%s{ttype} c ceDirection=1 cs gregated cs5=%s cn2=%d{numsession	nss-fw CEF:0 Zsca dip} dpt=%d(cdpor unslatedPort=%d(sd inat=%s(dnat) stat i=%s(dept) csllab threatcat) cs5lab uns} cn2Label=nums	ler NSSFWlog 5.7 % } deviceTranslate port) sourceTransl eful=%s{stateful} el=dept cs2=%s{mss el=threatcat cs6=% essions cs5Label=i	s{action} %s{rulelabel} 3] act dAddress-%s{sip} deviceTrans] actAddress-%s{sips ourceTra spriv#s{location} reason*s{c vc} cslabeleneService csl=%s s{threatname} csSlabel=threatn pCat csS=%s{ipcat} destCountry	=%s{action} atedPort=%d(ssport} ulelabel} in nmappl cs3label ame cn1 =%s{destcountry}
ser Obfuscation				Timezone		
Enabled 🛛 😔 Disa	abled			GMT	~	
uplicate Logs isabled		<u> </u>				
	WHO	SOURCE	SERVER	SESSION	PROTOCOL CLASSIFICATION	SECURITY
ACTION						

- 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{rulelabe
l} in=%ld{inbytes} out=%ld{outbytes} deviceDirection=1 cs1=%s{
dept} cs1Label=dept cs2=%s{nwsvc} cs2Label=nwService cs3=%s{nw
app} cs3Label=nwApp cs4=%s{aggregate} cs4Label=aggregated cs5=
%s{threatcat} cs5Label=threatcat cs6=%s{threatname} cs6label=t
hreatname cn1=%d{durationms} cn1Label=durationms cn2=%d{numses
sions} cn2Label=numsessions cs5Label=ipCat cs5=%s{ipcat} destC
ountry=%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} = 02ddd = 02dh: 02dh: 02ddm: 02dds = zscaler-nss-tunnel CE F: 0|Zscaler|NSSWeblog|5.7|s_{action} = 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{reqmet
hod} suser=%s{login} spriv=%s{location} externalId=%d{recordid} f
ileType=%s{filetype} destinationServiceName=%s{appname} cat=%s{ur
lcat} deviceDirection=1 cn1=%d{riskscore} cn1Label=riskscore cs1=
%s{dept} cs1Label=dept cs2=%s{urlcat} cs2Label=urlcat cs3=%s{malw
areclass} cs3Label=malwareclass cs4=%s{malwarecat} cs4Label=malwa
recat cs5=%s{threatname} cs5Label=threatname cs6=%s{bamd5} cs6Lab
el=md5hash rulelabel=%s{rulelabel} ruletype=%s{ruletype} urlclass
=%s{urlclass} devicemodel=%s{devicemodel} devicehostname=%s{devic
ehostname}\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} r
eason=%s{reason} app=%s{proto} dhost=%s{ehost} dst=%s{sip} src=%s
{cintip} sourceTranslatedAddress=%s{cip} in=%d{respsize} out=%d{r
eqsize} request=%s{eurl} requestContext=%s{ereferer} outcome=%s{r
espcode} requestClientApplication=%s{ua} requestMethod=%s{reqmeth
od} suser=%s{login} spriv=%s{location} externalId=%d{recordid} fi
leType=%s{filetype} destinationServiceName=%s{appname} cat=%s{url
cat} deviceDirection=1 cn1=%d{riskscore} cn1Label=riskscore cs1=%
```



```
s{dept} cs1Label=dept cs2=%s{urlcat} cs2Label=urlcat cs3=%s{malwa
reclass} cs3Label=malwareclass cs4=%s{malwarecat} cs4Label=malwar
ecat cs5=%s{threatname} cs5Label=threatname cs6=%s{bamd5} cs6Labe
l=md5hash rulelabel=%s{rulelabel} ruletype=%s{ruletype} urlclass=
%s{urlclass} devicemodel=%s{devicemodel} devicehostname=%s{device
hostname}\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.trythisencode2url.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

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

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.Ransum.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	Respose 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	blockced	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	тср	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 cs1Labe1=dept cs2=HTTP cs2Labe1=nwService cs3=teams cs3Labe1=nwApp cs4=aggre cs4Labe1=aggregated cs5=clean cs5Labe1=threatcat cs6=clean cs6labe1=threatname cn1=58555 cn1Labe1=durationms cn2=6 cn2Labe1=numsessions cs5Labe1=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.

Export Import Utility	_		>
xport Import			
1. Provide the path and file na 2. Click the Import button.	ame of the Categories file. Use the '' button to browse and locate the import file.		
Options Category Filters	Location		
Alerts Systems and Groups	Source :		
O Token Value	*iscat		
⊖ Reports			
Behavior Correlation			
	Import	Clos	е

EventTracker displays a success message.



5.2 Alerts

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



Provide the path and file na Click the Import button.	ime of the Alerts file. Use the '' buttor	n to browse and locate the import file.
Options	Location	
Category		
Filters	✓ Import E-mail settings	
Alerts	Set Active	
Systems and Groups	 Only if notifications set Bu 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
RSS Feeds	0 0, 0.00	section.
Reports	Source :	
Behavior Rules	*.isalt	
SCAP		
💿 Token Value		

- 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)**.

2. Click the import button Note : If report(s) contains ten	nplate first import template and proceed with exportimport utility		
Options Category	Location		
O Filters			
O Alerts	O Legacy (*.issch) New (*.etcnx)		
 Systems and Groups 	Source :		
O Token Value	JSSCN		
Reports			
Behavior Correlation			
0			

2. 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.

Reports Impor	t						
Note : If report(s) o	contains template, first import tem	plate and proceed wit	th report import proces	IS.			
Select file *.etc	רוכ						Select file
Available reports							
Title		Fr	equency Show all	•	Q Q		
	Title	Sites	Groups	Systems	Frequency	Runtime	Туре
	Title	Fr Sites	equency Show all Groups	• Systems	Q Q Frequency	Runtime	Туре

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

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 Set				
Replace	to Replace Assign systems				
	Note: Make sure that Site(s), Group(s) and System(s) selections are valid.				

EventTracker displays a success message.

Export Import Utility	×
Selected reports configurations a	are imported successfully
	ОК



5.4 Knowledge Objects

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

		🔑 🛛 Admin 🗸	Tools 👻 📀
Active Watch Lists	Event Filters	🧭 Parsing Rules	🏫 / Da
Alerts	Eventvault	Report Settings	
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	Q Users	
ni sc 🚺 Casebook Configuration	🔍 IP Lookup Configuration	🕀 Weights	Systems since the last 24 hour
● Category	·☆ Knowledge Objects	Windows Agent Config	
1 Diagnostics	Manager		

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

Admin / Knowledge Objects						
Objects 🕀 丁 🏦 🌣						
Import Objects						

 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.

Import	
KO_ <product name="">.etko</product>	🗲 Browse 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** \rightarrow **My Dashboard**.



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

🟫 / Dashboard / My Dashboard
+ 🖉 Q 🌣 İ 丁 O O
Import configuration

- 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.

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



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.

ategory			
Category Tree Search			
Zscaler		Q	Q
Category			
VZscaler Internet Access CA: DNS activities			
VZscaler Internet Access CA: Firewall activities			
✓Zscaler Internet Access CA: SaaS security activiti	es		
VZscaler Internet Access CA: Tunnel activities			
VZscaler Internet Access CA: Web access activitie	s		

6.2 Alerts

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

≡	Event Tracker ⊕					🔎 🛛 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
٩			Alerts	C Correlation	🔍 IP Lookup Configuration	Q Users	
	0	2	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	The Weights	
~			🇞 Behavior Correlation Settings	冠 Event Filters	Manager	🛄 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	😥 Parsing Rules		
			• Category	FAQ Configuration	Report Settings		_
	Attacker			- News			

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

Netsurion

The Alert Management page will display all the imported alerts.

Alerts Show All Y						Search by Alert name	~	↑ / Admin / Alets Zscaler Q Q
590 Available Alerts Total number et alrrit available	349 Active Alerts Total number of active alerts			590 System/User Defini Count for system and t	System 22 User ed Alerts user defined alerts	37	590 Alerts by Three Count of alerts b	Crical and a second state of the second state
Click 'Activate Now' after making	all changes							Total: 2 Page Size 25 V
Alert Name A	Thre	at Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□ §§ Zscaler Internet Access CA: IPS traffic detected	•							Zscaler Internet Access CA
βδ Zscaler Internet Access CA: Malicious file has been detected	•							Zscaler Internet Access CA

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

EventTracker displays a success message.

Successfully saved configuration.
ОК

5. 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

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

Knowledge Objects	
Zscaler	Q Q
Groups	🕀 🗭 🗓
Zsczler Internet Access CA	
Zscaler Internet Access CA	ø 1



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.

Reports configuration: Zscaler Internet Access CA					
		Title			
	£\$3	Zscaler Internet Access CA – Firewall activities			
	£\$3	Zscaler Internet Access CA – DNS activities			
	£\$3	Zscaler Internet Access CA – Tunnel activities			
	2.23	Zscaler Internet Access CA – SaaS security activities			
	₹ \$ \$	Zscaler Internet Access CA – Web access activities			

6.5 Dashboards

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



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





Customize dashlets			×
Zscaler			Q
Zscaler Internet Access CA - Ma	Zscaler Internet Access CA - Ma	Zscaler Internet Access CA - So	Zscaler Internet Access CA - Sus
Zscaler Internet Access CA - Tra	Zscaler Internet Access CA - Tra	Zscaler Internet Access CA - Tra	
			Add Delete Close



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 <u>EventTracker</u> cyber threat protection platform provides SIEM, end protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation 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 <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #23 among <u>MSSP Alert's 2021 Top 250 MSSPs</u>.

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