How-To Guide

Configuring Zscaler Internet Access Central Authority (CA) to Forward Logs to EventTracker

EventTracker v9.2x and above

Publication Date:

October 28, 2021

Abstract

This guide provides instructions to configure Zscaler Internet Access Central Authority (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 Zscaler Internet Access CA.

Audience

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

Table of Contents

1. Overview

The Zscaler Internet Access (ZIA) Central Authority (CA) is a 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 the 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 NSS.

NSS to SIEM: The NSS buffers the logs in the Virtual Machine (VM) memory to increase its resilience to transient 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.

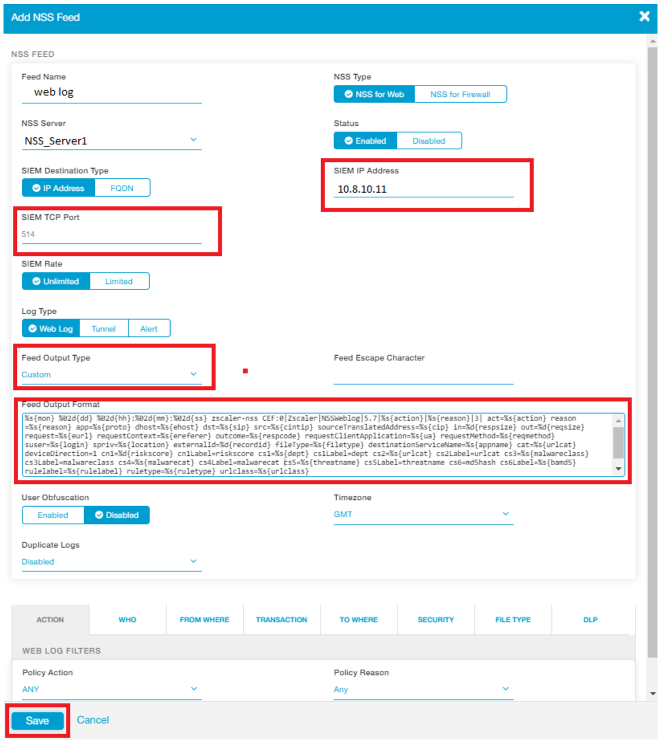
Note: Enable the TCP with port number 514 from EventTracker to receive the Zscaler Internet Access CA logs.

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.



Add NSS Feed

NSS FEED

Feed Name: web log

NSS Type: ● NSS for Web ○ NSS for Firewall

NSS Server: NSS_Server1

Status: ● Enabled ○ Disabled

SIEM Destination Type: ● IP Address ○ FQDN

SIEM IP Address: 10.8.10.11

SIEM TCP Port: 514

SIEM Rate: ● Unlimited ○ Limited

Log Type: ● Web Log ○ Tunnel ○ Alert

Feed Output Type: Custom

Feed Escape Character:

Feed Output Format:

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss 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=md5hash cs6Label=%s{bamd5}
rulelabel=%s{rulelabel} ruletype=%s{ruletype} urlclass=%s{urlclass}
```

User Obfuscation: ○ Enabled ● Disabled

Timezone: GMT

Duplicate Logs: Disabled

WEB LOG FILTERS

Policy Action: ANY

Policy Reason: Any

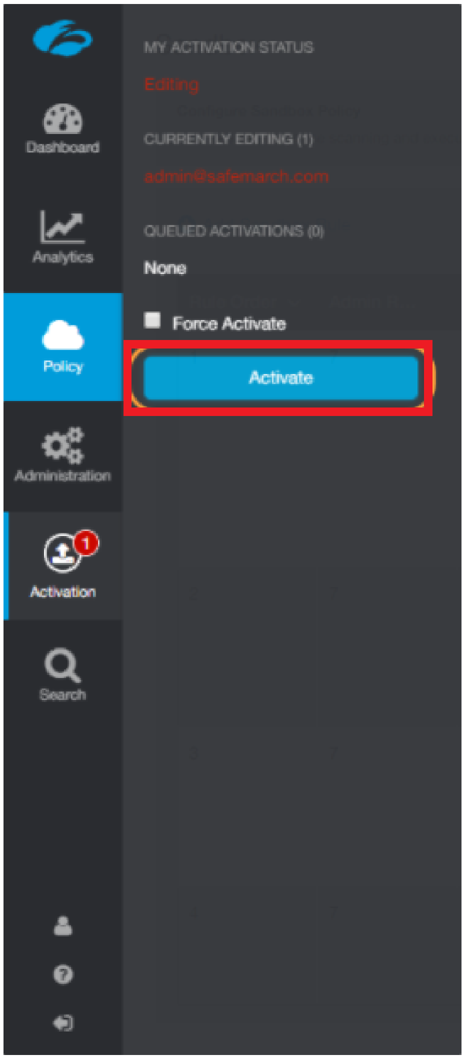
- **Feed Name:** Enter the name as **Web logs**.
- **NSS Type**: Select **NSS for Web**.
- **NSS Server**: Choose the NSS from the list.
- **Status:** The NSS feed is **Enabled** by default.
- **SIEM Destination Type**: The type of destination.
    - **SIEM IP Address**: Enter the IP address of **EventTracker** 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{malwar
eclass} cs3Label=malwareclass cs4=%s{malwarecat} cs4Label=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).

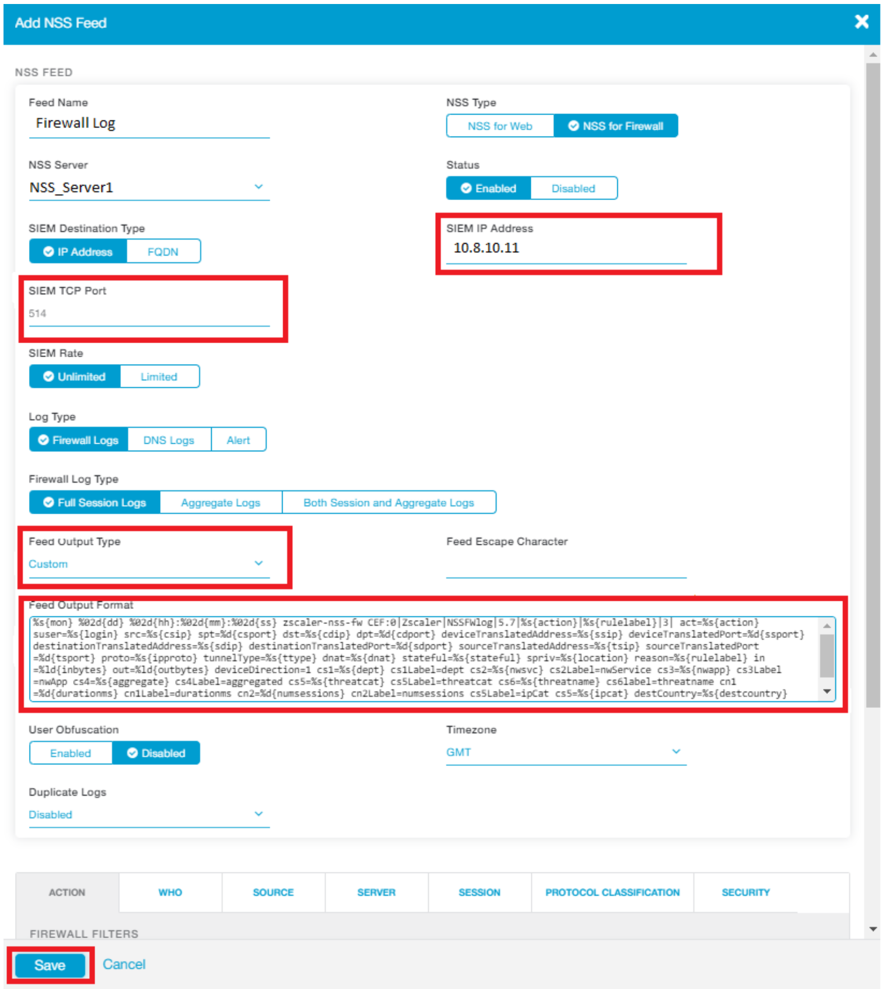
4. Click **Save** and activate the change.



3.2 To configure a feed for the Firewall Logs

1. 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

NSS FEED

Feed Name: Firewall Log

NSS Type: NSS for Web | ● NSS for Firewall

NSS Server: NSS_Server1

Status: ● Enabled | Disabled

SIEM Destination Type: ● IP Address | FQDN

SIEM IP Address: 10.8.10.11

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 Escape Character:

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} dnat=%s{dnat} stateful=%s{stateful} 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}
```

User Obfuscation: Enabled | ● Disabled

Timezone: GMT

Duplicate Logs: Disabled

- **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 to 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 the 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 of 60 (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{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 to 60 (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 of 60 (in minutes).

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

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, end 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 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