



Real-time Personalized Security Awareness Program

# Zscaler SecurityAdvisor Integration Document

---

## Table of Contents

---

|   |   |
|---|---|
| Overview:                                       | 2 |
| Integrate Zscaler with SecurityAdvisor platform | 2 |
| Step 1: Acquire SecurityAdvisor License         | 3 |
| Step 2: Activate SecurityAdvisor Account        | 3 |
| Step 3: Send Zscaler logs to SecurityAdvisor    | 3 |
| Step 4: Test the Integration                    | 8 |
| Step 5: Manage User Engagement & Reporting      | 8 |

## Overview:

---

This document walks you through the steps to integrate the Zscaler log streaming service with SecurityAdvisor platform. To utilize the integration, you must have Administrator access to the Zscaler Nano log streaming service.

## Integrate Zscaler with SecurityAdvisor platform

---

To automate security awareness coaching using SecurityAdvisor platform, you can follow the 5 easy steps below:

### Acquire SecurityAdvisor License

Obtain SecurityAdvisor license

### Activate SecurityAdvisor Account

Activate your SecurityAdvisor account

### Send Zscaler logs to SecurityAdvisor

Configure your Zscaler log receiver and log formats

### Test the Integration

Verification & Testing

### Manage User Engagement & Reporting

Managing Teachable moments and messaging to your end-users and view various reports

## Step 1: Acquire SecurityAdvisor License

---

Visit <https://www.securityadvisor.io> to get started.

## Step 2: Activate SecurityAdvisor Account

---

Once you have successfully signed up, you will receive an activation email from SecurityAdvisor.

1. Activate your account and log on to the SecurityAdvisor management console (<https://www.securityadvisor.io/sabweb/login/>)
2. Log in to the platform using your username
3. Click on **Integrations** from the navigation menu and then select **Zscaler**. Follow the instructions in the setup guide there.
4. Note that your organization key (org\_key) is listed on the Zscaler activation page above or you can contact us at [support@securityadvisor.io](mailto:support@securityadvisor.io) to obtain the same.

## Step 3: Send Zscaler logs to SecurityAdvisor

---

Log on to your Zscaler Admin Portal and follow the screenshots below to configure your Zscaler log receiver, and update log formats.

1. Click on Administration > Nanolog Streaming Service
2. Click the pencil icon to update NSS feed with the following information:

**SIEM Destination Type: FQDN**

**SIEM TCP Port: 1468**

**SIEM FQDN: syslog.securityadvisor.io**

3. Feed output format (weblog only, do not send us your firewall log)

**User Obfuscation: Disabled**

**Timezone: GMT**

**Duplicate Logs: Disabled**

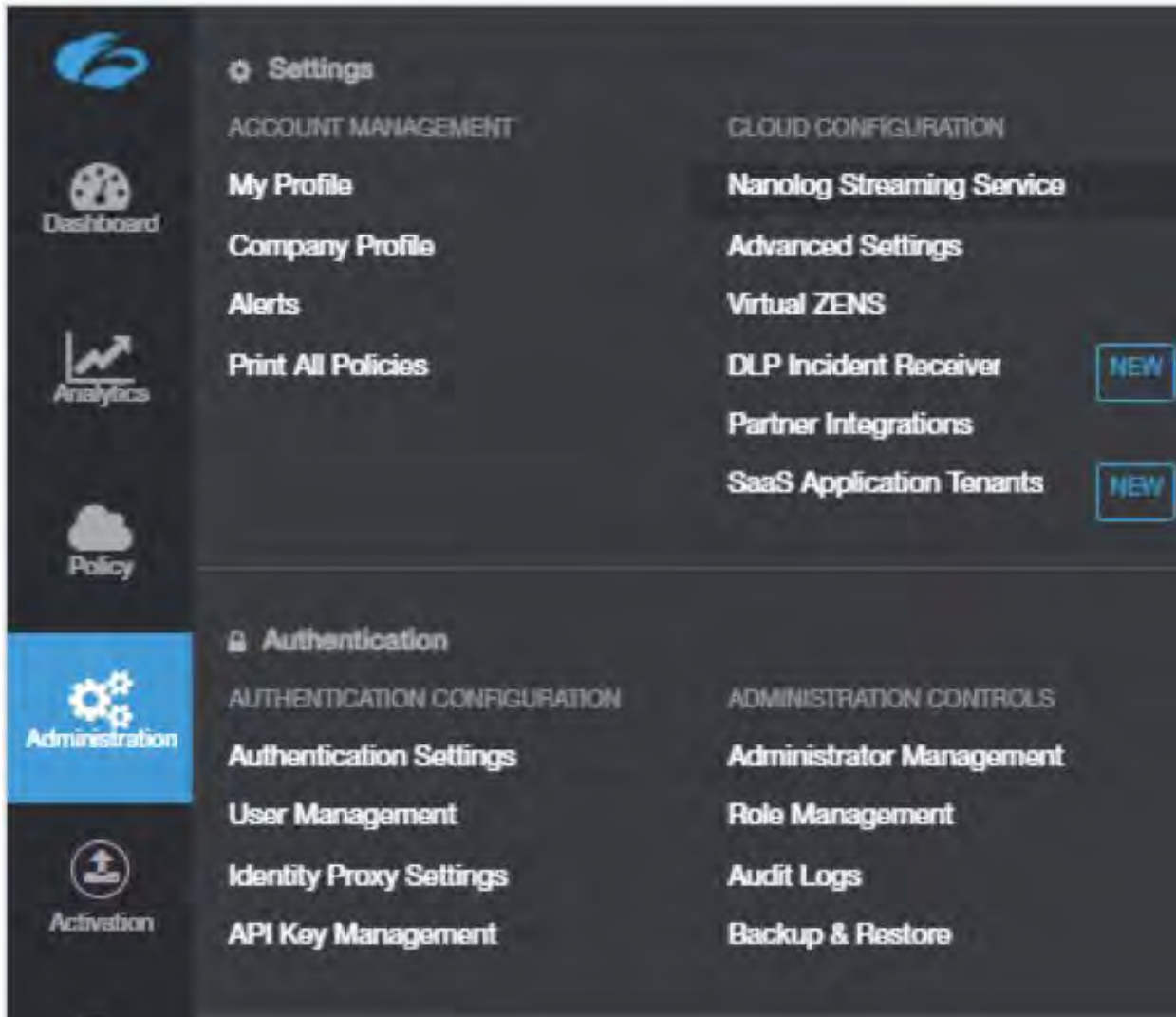
Here is the weblog format you should use:

zscaler-nss

```
CEF:0|Zscaler|NSS|4.1|NULL|NULL|NULL|org_key=XXXXXXX\tvendor_code_name=zscaler\tlog
_type=web\tcat=%s{action}\tdevTime=%s{mon} %02d{dd} %d{yy}
%02d{hh}:%02d{mm}:%02d{ss} %s{tz}\tdevTimeFormat=MMM dd yyyy
HH:mm:ssz\tsrc=%s{cip}\tdst=%s{sip}\tsrcPostNAT=%s{cintip}\trealm=%s{location}\tusrName=
%s{login}\tsrcBytes=%d{reqsize}\tdstBytes=%d{respsize}\trole=%s{dept}\tpolicy=%s{reason}\tr
ecordid=%d{recordid}\tbwthrottle=%s{bwthrottle}\tuseragent=%s{ua}\treferer=%s{ereferer}\th
ostname=%s{ehost}\tappproto=%s{proto}\turlcategory=%s{urlcat}\turlsupercategory=%s{urlsu
percat}\turlclass=%s{urlclass}\tappclass=%s{appclass}\tappname=%s{appname}\tmalwaretype=
%s{malwarecat}\tmalwareclass=%s{malwareclass}\tthreatname=%s{threatname}\triskscore=%d
{riskscore}\tdlpdict=%s{dlpdict}\tdlpeng=%s{dlpeng}\tfileclass=%s{fileclass}\tfiletype=%s{filetyp
e}\treqmethod=%s{reqmethod}\trespcode=%s{respcode}\t%s{bamd5}\turl=%s{eurl}\tdeviceho
stname=%s{devicehostname}\n
```

where XXXXXXX is your org\_key (organization key), which has the format like 305cd33aa1cc49ba945eb86844e9999c. Please replace this placeholder value (XXXXXXX) with your actual organization key.

**Note that your organization key (org\_key) is listed in your SecurityAdvisor console. Log In and go to Integrations > Zscaler.**



Nanolog Streaming Service

NSS SERVERS    NSS FEEDS

[Add NSS Feed](#)    [Add MCAS NSS Feed](#)   

| No. | Feed Overview  | Log Filter                             | Feed Output Format  | Feed Attributes   |
|-----|--|--|---|---|
| 16  | Feed Name<br>securityadvisor.io-FW<br>NSS Server<br>NSS_FW_2<br>Status<br>Enabled<br>Output Destination<br>syslog-dev.securityadvisor.io:1468<br>Log Type<br>Firewall Logs<br>Feed Type<br>Custom<br><a href="#">More...</a> | Firewall Log Type<br>Full Session Logs | zscaler-nss zscaler-nss CEF:0[Zscaler]NSS[4.1][NULL]<br>NULL[org_key=305cd33aa1cc49ba945eb86844e1683c vendor_code_name=zscaler log_type=firewall dateime=%s(time) user=%s(login) department=%s(dept) locationname=%s(location) cdpport=%d(cdport) csport=%d(csport) sdport=%d(sdport) sspport=%d(ssport) csip=%s(csip) cdpip=%s(cdpip) sspip=%s(sspip) sdip=%s(sdiip) tsip=%s(tsip) lunsport=%d(lunsport) luntype=%s(luntype) action=%s(action) drat=%s(drat) statelid=%s(statelid) aggregate=%s(aggregate) rwsvc=%s(rwsvc) rwapprvc=%s(rwapprvc) proto=%s(ppproto) ipcat=%s(ipcat) destcountry=%s(destcountry) avgduration=%d(avgduration) rulelabel=%s(rulelabel) inbytes=%d(inbytes) outbytes=%d(outbytes) duration=%d(duration) durationsms=%d(durationsms) numsessions=%d(numsessions) psrulelabel=%s(psrulelabel) threatcat=%s(threatcat) threatname=%s(threatname) deviceowner=%s(deviceowner) devicehostname=%s(devicehostname)\n   | Duplicate Logs<br>Disabled<br>User Obfuscation<br>Disabled<br>Timezone<br>GMT<br>SIEM Rate<br>Unlimited |
| 17  | Feed Name<br>securityadvisor.io-WEB<br>NSS Server<br>NSS_WEB_2<br>Status<br>Enabled<br>Output Destination<br>syslog-dev.securityadvisor.io:1468<br>Log Type<br>Web Log<br>Feed Type<br>Custom<br><a href="#">More...</a>     |  | zscaler-nss CEF:0[Zscaler]NSS[4.1][%s(reason)][NULL]<br>org_key=305cd33aa1cc49ba945eb86844e1683c vendor_code_name=zscaler log_type=web cat=%s(action) devTime=%s(mon)%02d(dd) %d(dy) %02d(hh):%02d(mm):%02d(ss) %s(tz) devTimeFormat=MMM dd yyyy HH:mm:ssz src=%s(cip) dst=%s(sip) srcPostNAT=%s(cintip) realm=%s(location) usrName=%s(login) srcBytes=%d(repsize) dstBytes=%d(repsize) role=%s(role) policy=%s(policy) recordid=%d(recordid) bwthrottle=%s(bwthrottle) useragent=%s(ua) referer=%s(referer) hostname=%s(ahost) appproto=%s(protocol) uriclass=%s(uriclass) urlsupercategory=%s(urlsupercategory) uriclass=%s(uriclass) appclass=%s(appclass) appname=%s(appname) malwaretype=%s(malwaretype) malwareclass=%s(malwareclass) threatname=%s(threatname) riskscore=%d(riskscore) dlpdict=%s(dlpdict) dipeng=%s(dipeng) fileclass=%s(fileclass) filetype=%s(filetype) reqmethod=%s(reqmethod) respcode=%s(respcode) %s(bamd5) url=%s(aur) devicehostname=%s(devicehostname)\n | Duplicate Logs<br>Disabled<br>User Obfuscation<br>Disabled<br>Timezone<br>GMT<br>SIEM Rate<br>Unlimited |

Edit NSS Feed
✕

---

**NSS FEED**

**Feed Name**  
securityadvisor.io-WEB

---

**NSS Server**  
NSS\_WEB\_2

---

**SIEM Destination Type**  
 IP Address  FQDN

---

**SIEM TCP Port**  
1468

---

**SIEM Rate**  
 Unlimited  Limited

---

**Log Type**  
 Web Log  Tunnel  Alert

---

**Feed Output Type**  
Custom

---

**Feed Output Format**  

```
zscaler-nss CEF:0|Zscaler|NSS|4.1|{%s[reason]}|NULL|org_key=305cd33aalcc49ba945eb86844e1683c vendor_code_name=zscaler log_type=web cat
={%s[action]} devTime={%s(mon)} %02d(dd) %d(yy) %02d(hh):%02d(mm):%02d(ss) %s(tz) devTimeFormat=%M dd yyyy H:mm:ssz src={%s(cip)} dst={%s(sip)}
srcPostNAI={%s(cintip)} realm={%s(location)} usrName={%s(login)} srcBytes={%d(reqsize)} dstBytes={%d(respsize)} role={%s(dept)} policy={%s(reason)}
recordid={%d(recordid)} bwthrottle={%s(bwthrottle)} useragent={%s(ua)} referer={%s(referrer)} hostname={%s(ehost)} appproto={%s(proto)} urlcategory
={%s(urlicat)} urlsupercategory={%s(urlsupercat)} urlclass={%s(urlclass)} appclass={%s(appclass)} appname={%s(appname)} malwaretype={%s(malwarecat)}
malwareclass={%s(malwareclass)} threatname={%s(threatname)} riskscore={%d(riskscore)} dlpdict={%s(dlpdict)} dlpeng={%s(dlpeng)} fileclass
={%s(fileclass)} filetype={%s(filetype)} reqmethod={%s(reqmethod)} respcode={%s(respcode)} %s(band5) url={%s(eurl)} devicehostname
```

---

**User Obfuscation**  
 Enabled  Disabled

---

**Duplicate Logs**  
Disabled

---

**NSS Type**  
 NSS for Web  NSS for Firewall

---

**Status**  
 Enabled  Disabled

---

**SIEM FQDN**  
syslog-dev.securityadvisor.io

---

**Feed Escape Character**

---

**Timezone**  
GMT

---

ACTION
WHO
FROM WHERE
TRANSACTION
TO WHERE
SECURITY
FILE TYPE
DLP

Save
Cancel
Delete

## Step 4: Test the Integration

---

You should start to receive log data in the SecurityAdvisor platform. If you have set up teachable moments, you should start to receive them. To create a Teachable Moment please navigate to **Automation and Analytics > Teachable Moments** in the SecurityAdvisor console.

## Step 5: Manage User Engagement & Reporting

---

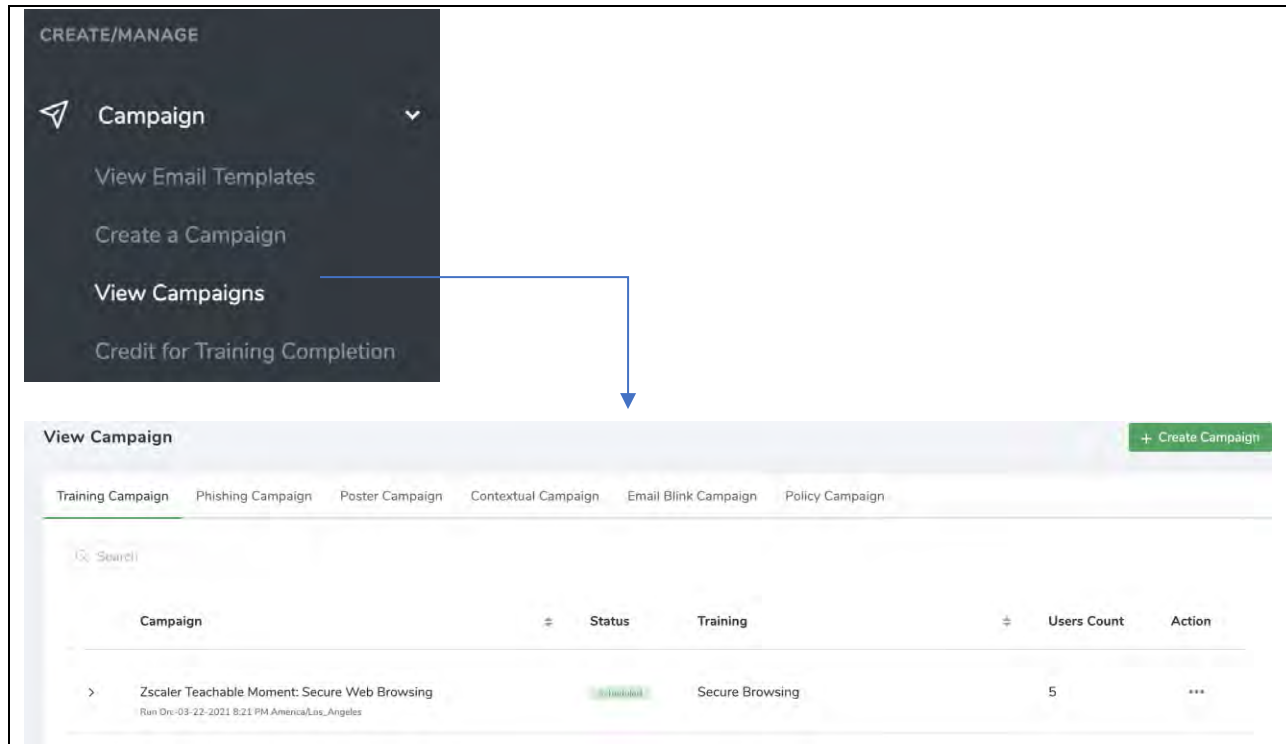
*Managing Teachable moments and messaging to your end-users and view various reports:*

You can create/customize campaigns through the SecurityAdvisor console by navigating to **Campaigns > View Campaigns**.

You can edit the campaigns and provide custom email templates, branding for your organization and pick different training from our awareness catalog.

Detailed reports are available under the campaign reporting.





The screenshot displays the SecurityAdvisor interface. On the left, a dark sidebar contains a 'CREATE/MANAGE' section with a 'Campaign' menu item. A blue arrow points from the 'View Campaigns' option in this menu to the 'View Campaign' page. The 'View Campaign' page features a header with a '+ Create Campaign' button and a navigation bar with tabs for 'Training Campaign', 'Phishing Campaign', 'Poster Campaign', 'Contextual Campaign', 'Email Blink Campaign', and 'Policy Campaign'. Below the navigation bar is a search bar and a table of campaigns.

| Campaign   | Status    | Training        | Users Count | Action |
|--|-----------|-----------------|-------------|--------|
| > Zscaler Teachable Moment: Secure Web Browsing<br><small>Run On: 03-22-2021 8:21 PM America/Los_Angeles</small> | Completed | Secure Browsing | 5           | ...    |