SecurityAdvisor

Real-time Personalized Security Awareness Program

Zscaler SecurityAdvisor Integration Document

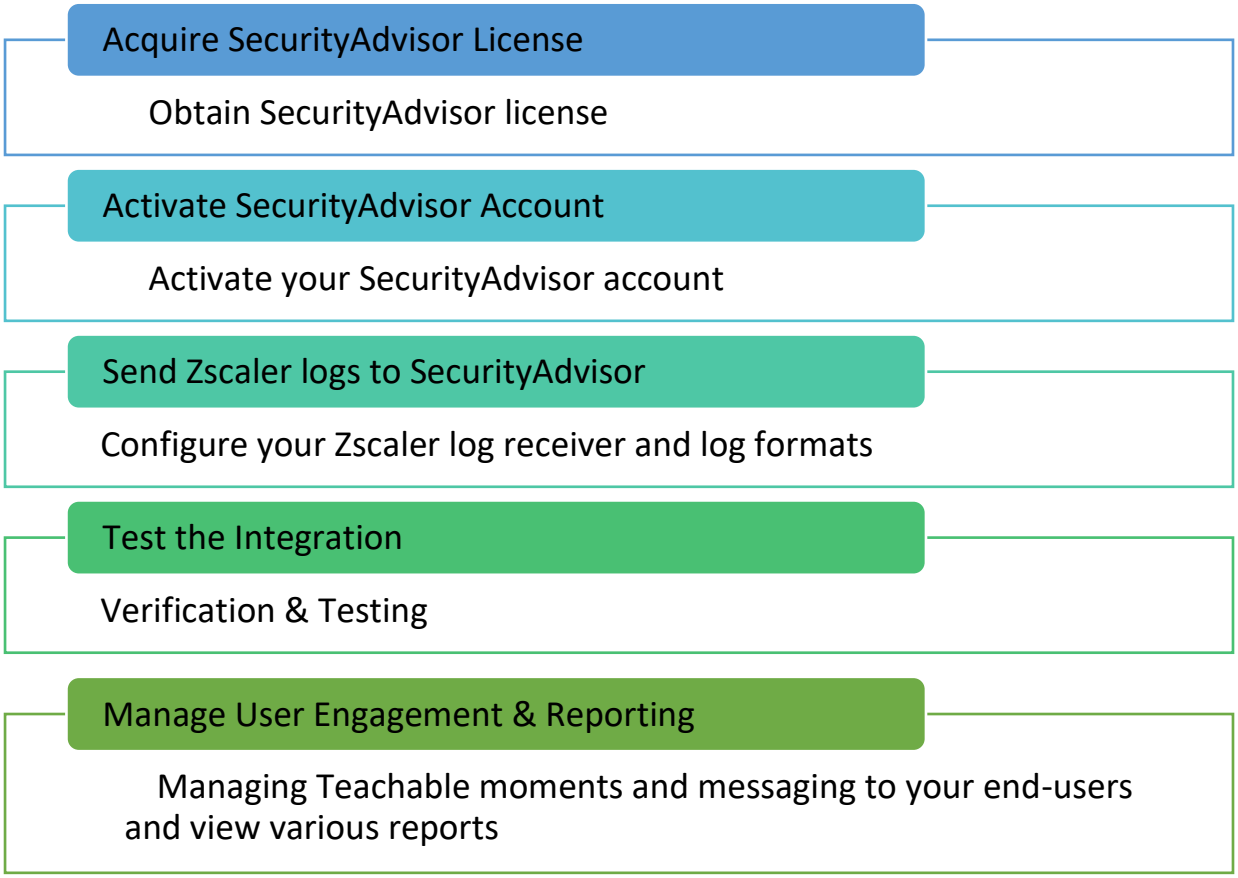
Table of Contents

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:



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 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)

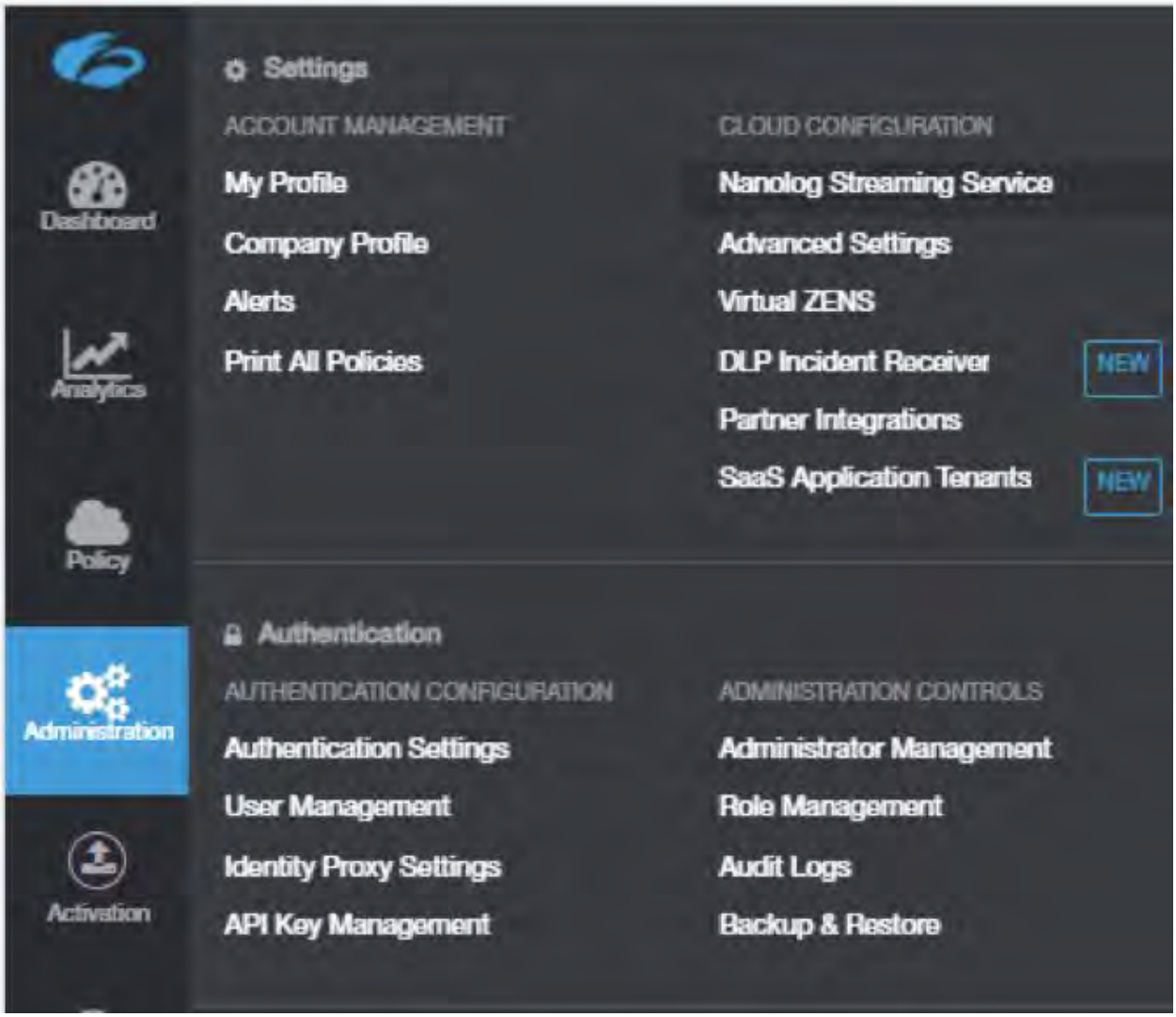
   User Obfuscation: Disabled
   Timezone: GMT
   Duplicate Logs: Disabled

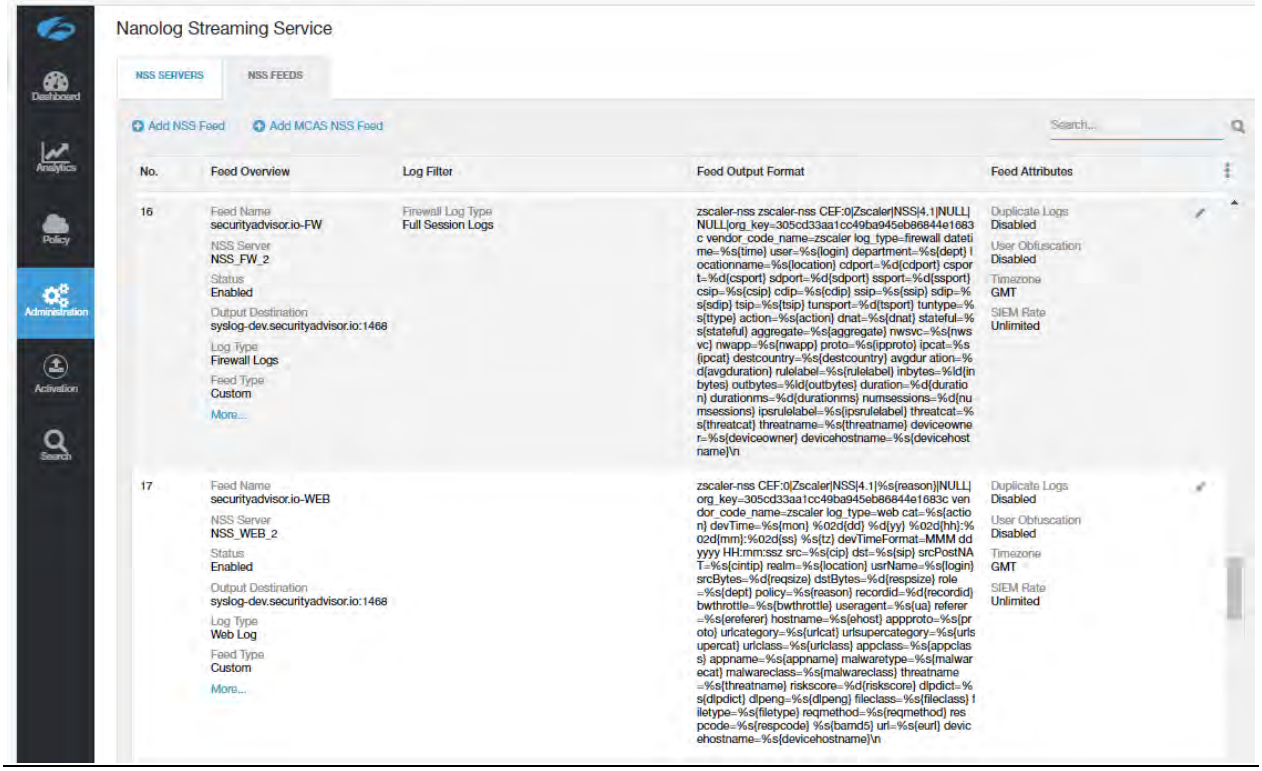
   Here is the weblog format you should use:

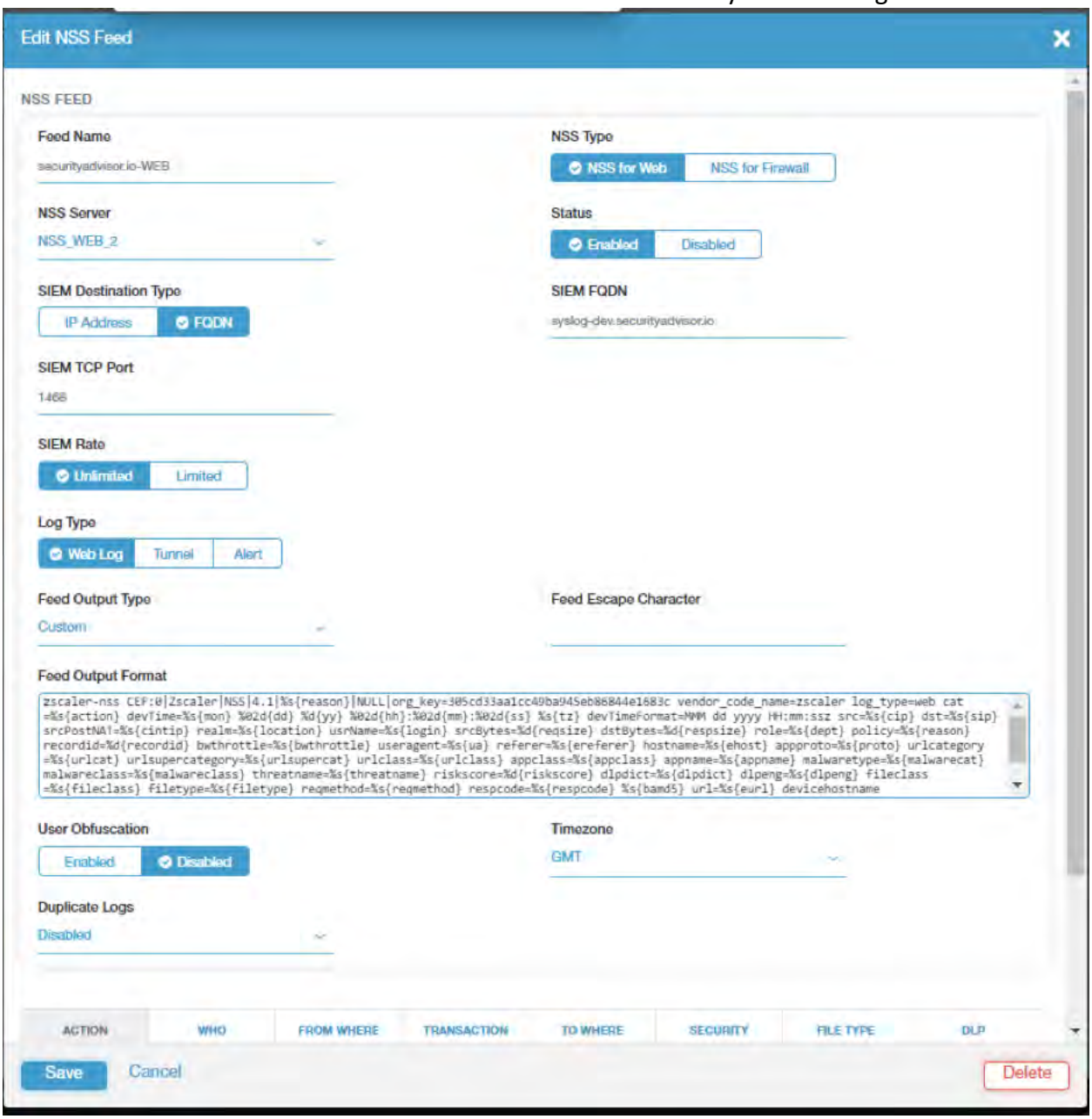
zscaler-nss
CEF:0|Zscaler|NSS|4.1|NULL|NULL|NULL|org_key=XXXXXXX\tvendor_code_name=zscaler\tlog_type=web\tcat=%s{action}\tdevTime=%s{mon} %02d{dd} %d{yy} %02d{hh}:%02d{mm}:%02d{ss} %s{tz}\tdevTimeFormat=MMM dd yyyy HH:mm:ssz\tsrc=%s{cip}\tdst=%s{sip}\tsrcPostNAT=%s{cintip}\trealm=%s{location}\tusrName=%s{login}\tsrcBytes=%d{reqsize}\tdstBytes=%d{respsize}\trole=%s{dept}\tpolicy=%s{reason}\trecordid=%d{recordid}\tbwthrottle=%s{bwthrottle}\tuseragent=%s{ua}\treferer=%s{ereferer}\thostname=%s{ehost}\tappproto=%s{proto}\turlcategory=%s{urlcat}\turlsupercategory=%s{urlsupercat}\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{filetype}\treqmethod=%s{reqmethod}\trespcode=%s{respcode}\t%s{bamd5}\turl=%s{eurl}\tdevicehostname=%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.







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.