Zscaler getting started guide

Version 2.1

April 15, 2020

What's in this guide?

Howdy! In this guide, you'll find instructions on how to:

1. Enable and configure console access for the Expel Security Operations Center (SOC);
2. Send Zscaler events to a SIEM; and
3. Configure Zscaler in Expel Workbench™.

Step 1 — Enable console access

Having read-only access to the interface of your technology allows Expel to dig deeper when performing incident investigations. Our device health team uses this access to investigate potential health issues with your tech.

By following these steps, you'll create a user account for Expel that will keep Expel's activity separate from other activity on the Zscaler console. Please make sure Expel.io is added as an authorized domain for Zscaler prior to implementing the following steps.

Create an admin account

A. Log into Zscaler

B. Navigate to **Administration > Administrators** and click the **Add Administrator** button (see Figure 1 for steps B-I)

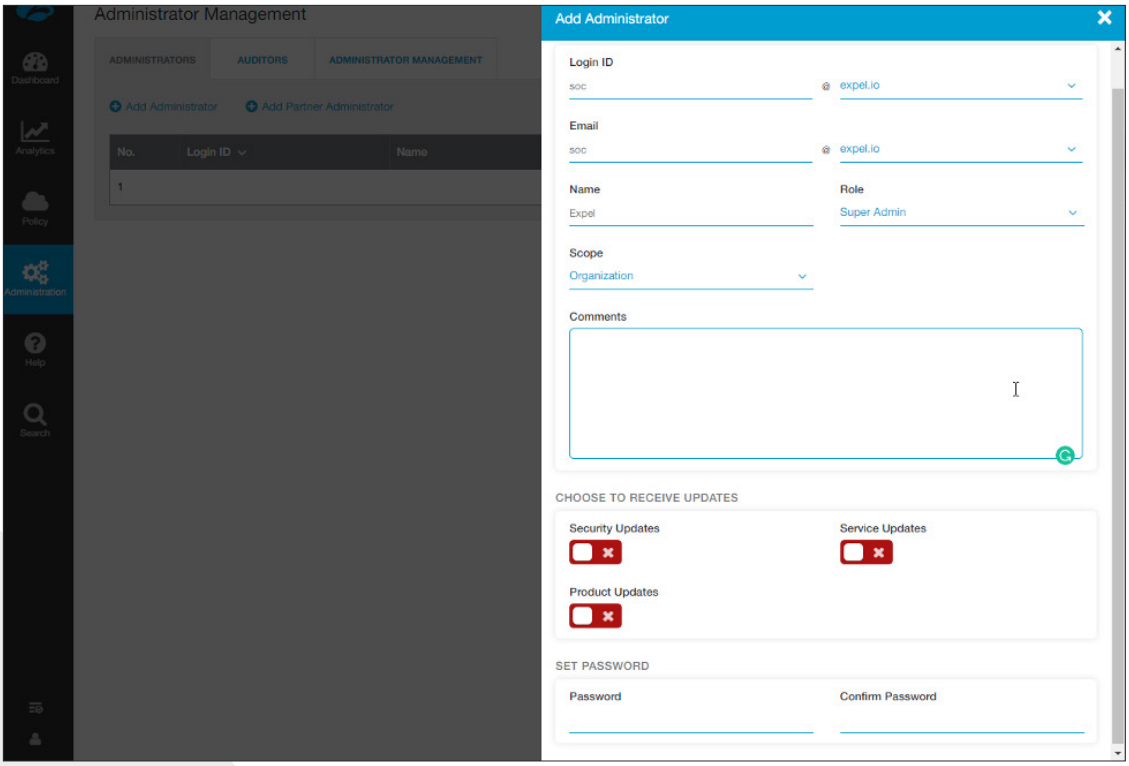

Figure 1

C. For **Login ID** enter soc and choose *expel.io* from the drop-down

D. For **Email** enter *soc* and choose *expel.io* from the drop-down

E. For **Name** enter *Expel*

F. For **Role** select *Super Admin*

G. For **Scope** select *Organization*

H. Enter the desired **Password**

I. Click **Save**

Step 2 — Send Zscaler events to a SIEM

The Nanolog Streaming Service (NSS) feed specifies the data from the logs that the NSS will send to the SIEM. Expel uses three NSS feeds to forward data to a SIEM (Figure 2).

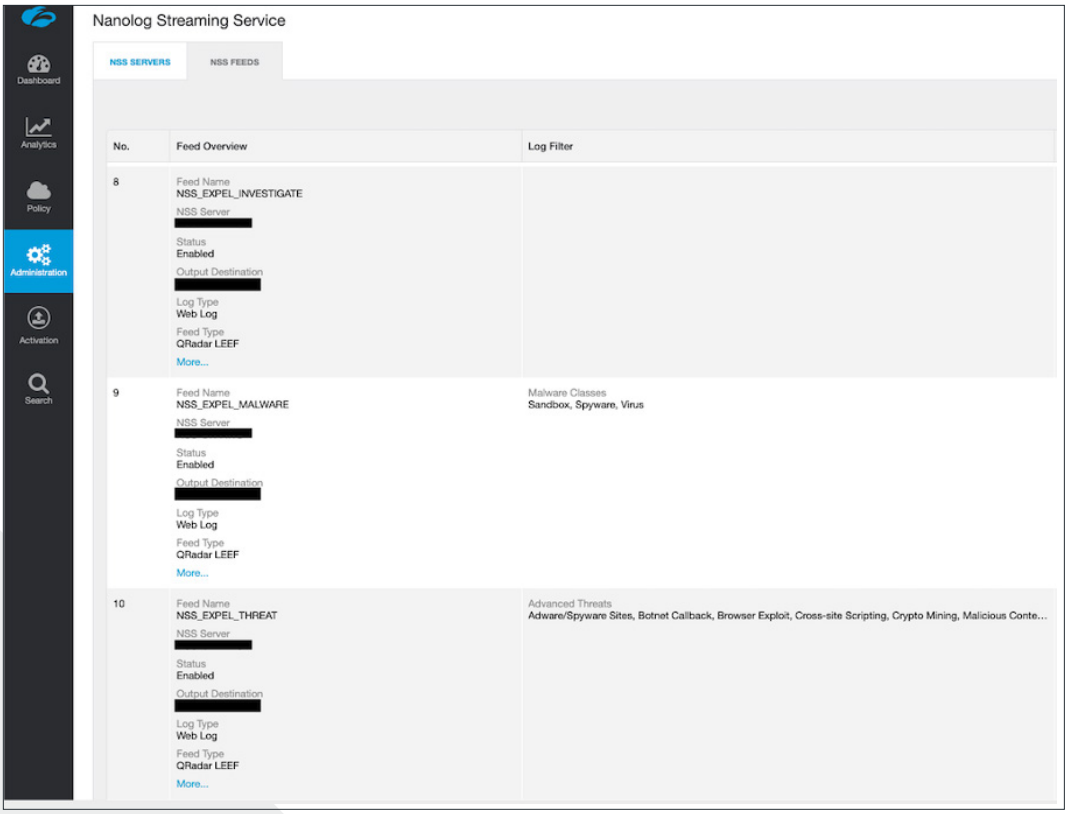

Figure 2

A. The EXPEL_MALWARE feed captures any malware class events (Figure 3)

   a. **Feed Output Type : QRadar LEEF**

   b. **Web Log Filters =** Security > Malware Classes : Sandbox, Spyware, Virus

   c. **Feed Output Format =** %s{mon} %02d{dd}

```
%02d{hh}:%02d{mm}:%02d{ss} zscaler-EXPEL_MALWARE: LEEF:1.0|Zscaler|NSS|4.1|fqdn=%s{host}\
turl=%s{url}\t method=%s{reqmethod}\tuser_agent=%s{ua}\turlclass=%s{ urlclass}\tcategory=%s{urlcat}\
treferrer=%s{referer}\ tresponse=%s{respcode}\tprotocol=%s{proto}\tduration_ ms=%d{ctime}\
tsrc=%s{cip}\tdst=%s{sip}\tbytes_rx=%d{r espsize}\tbytes_tx=%d{reqsize}\tappclass=%s{appclass} \
tappname=%s{appname}\tflow_id=%d{recordid}\torganiza tion=%s{dept}\tusername=%s{login}\
tvendor_version=%s{ productversion}\tname=%s{reason}\talert_at=%s{time}%s {tz}\
talertaction=%s{action}\tfile_hash=%s{bamd5}\tmi me_type=%s{filetype}\tfilename=%s{filename}\
tscore=%d {riskscore}\trealm=%s{location}\tnsssvcip=%s{nsssvcip }\tthreatname=%s{threatname}\
tmalwarecategory=%s{malw arecat}\tmalwareclass=%s{malwareclass}\t\n
```

Figure 3: Configuration

B. The EXPEL_THREAT feed surfaces any Advanced Threat events (Figure 4)

a. **Feed Output Type : QRadar LEEF**

b. **Web Log Filters =** Security > Advanced Threats : Adware/Spyware Sites, Botnet Callback, Browser Exploit, Cross-site Scripting, Cryptomining, Malicious Content, Other Threat, Peer-to-Peer, Phishing, Spyware Callback, Suspicious Content, Suspicious Destination, Unauthorized Communication, Web Spam

c. **Feed Output Format =** %s{mon} %02d{dd}

```
%02d{hh}:%02d{mm}:%02d{ss} zscaler-EXPEL_THREAT: LEEF:1.0|ZscalerlNSS|4.1|fqdn=%s{host}\
turl=%s{url}\t method=%s{reqmethod}\tuser_agent=%s{ua}\turlclass=%s{ urlclass}\tcategory=%s{urlcat}\
treferrer=%s{referer}\ tresponse=%s{respcode}\tprotocol=%s{proto}\tduration_ ms=%d{ctime}\
tsrc=%s{cip}\tdst=%s{sip}\tbytes_rx=%d{r espsize}\tbytes_tx=%d{reqsize}\tappclass=%s{appclass} \
tappname=%s{appname}\tflow_id=%d{recordid}\torganiza tion=%s{dept}\tusername=%s{login}\
tvendor_version=%s{productversion}\tname=%s{reason}\talert_at=%s{time}%s {tz}\
talertaction=%s{action}\tfile_hash=%s{bamd5}\tmi me_type=%s{filetype}\tfilename=%s{filename}\
tscore=%d {riskscore}\trealm=%s{location}\tnsssvcip=%s{nsssvcip }\tthreatname=%s{threatname}\
tmalwarecategory=%s{malw arecat}\tmalwareclass=%s{malwareclass}\t\n
```

Figure 4: Configuration

C. (OPTIONAL) An additional feed, EXPEL_INVESTIGATE, can be added to forward all web log data to Splunk. Expel analysts will use this information to understand, scope, and answer security questions related to threat behavior. Specifically, how it got there, what it is and what needs to be done to remediate (Figure 5)

a. **Feed Output Type : QRadar LEEF**

b. **Web Log Filters =** None

c. **Feed Output Format =** %s{mon} %02d{dd}

```
%02d{hh}:%02d{mm}:%02d{ss} zscaler-EXPEL_INVESTIGATE: LEEF:1.0|ZscalerlNSS|4.1|fqdn=%s{host}\
turl=%s{url}\tmetho d=%s{reqmethod}\tuser_agent=%s{ua}\turlclass=%s{urlclass}\ tcategory=%s{urlcat}\
treferrer=%s{referer}\tresponse=%s{re spcode}\tprotocol=%s{proto}\tduration_ms=%d{ctime}\
tsrc=%s {cip}\tdst=%s{sip}\tbytes_rx=%d{respsize}\tbytes_tx=%d{req size}\tappclass=%s{appclass}\
tappname=%s{appname}\tflow_id =%d{recordid}\torganization=%s{dept}\tusername=%s{login}\t
vendor_version=%s{productversion}\tname=%s{reason}\talert_ at=%s{time}%s{tz}\
talertaction=%s{action}\tfile_hash=%s{ba md5}\tmime_type=%s{filetype}\tfilename=%s{filename}\
tscore =%d{riskscore}\trealm=%s{location}\tnsssvcip=%s{nsssvcip}\ tthreatname=%s{threatname}\
tmalwarecategory=%s{malwarecat} \tmalwareclass=%s{malwareclass}\t\n
```

Figure 5: Configuration

Step 3 — Configure the technology in Workbench

Now that we have the correct access configured and events are being sent to a SIEM, we can integrate Zscaler with Expel.

Register Zscaler in Expel Workbench

A. In a new browser tab, log into https://workbench.expel.io

B. Enter the security code from Google Authenticator (two-factor authentication)

C. On the console page, navigate to **Settings** and click **Security Devices**

D. At the top right of the page, select **Add Security Device** (Figure 6)

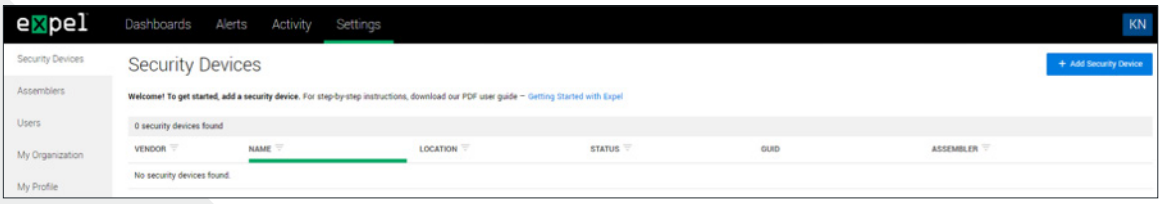

Figure 6

E. Search for and select Zscaler (Figure 7)

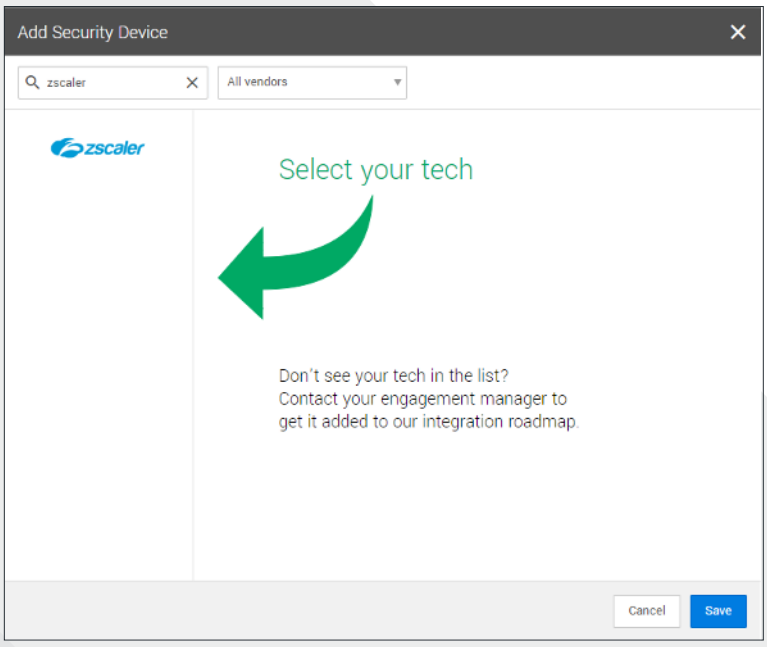

Figure 7

F. Complete all fields using the credentials and information you collected in *Step 1* and *Step 2* above (see Figure 8 for *Steps G-M*)

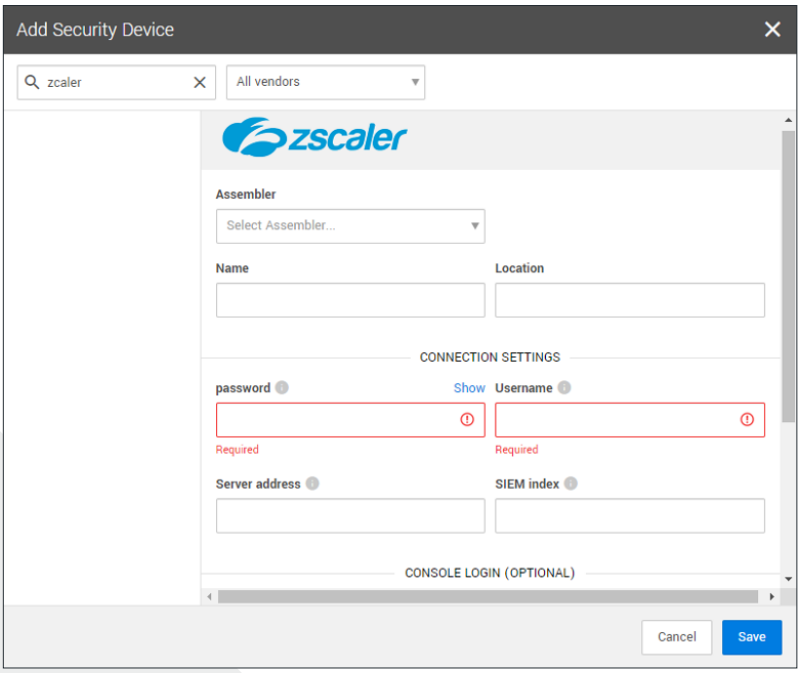

Figure 8

G. Select **Assembler** from the drop down (Choose the assembler you set up in *Step 2* of the Getting Started with Expel guide)

H. Enter assembler **Name** and **Location**

I. The **password** (access key) is from the Sumo Logic SIEM

J. The **Username** (access ID) is from the Sumo Logic SIEM

K. For **Server address**, use the server address from your SIEM; the default address is https://service.us2.sumologic.com

L. For **SIEM index**, enter the SIEM that is holding the data formatted by NSS

M. Select **Save**

N. Add Sumo Logic SIEM device to Workbench using the same steps (*Steps C-M*), and with the same information as above (Figure 9)

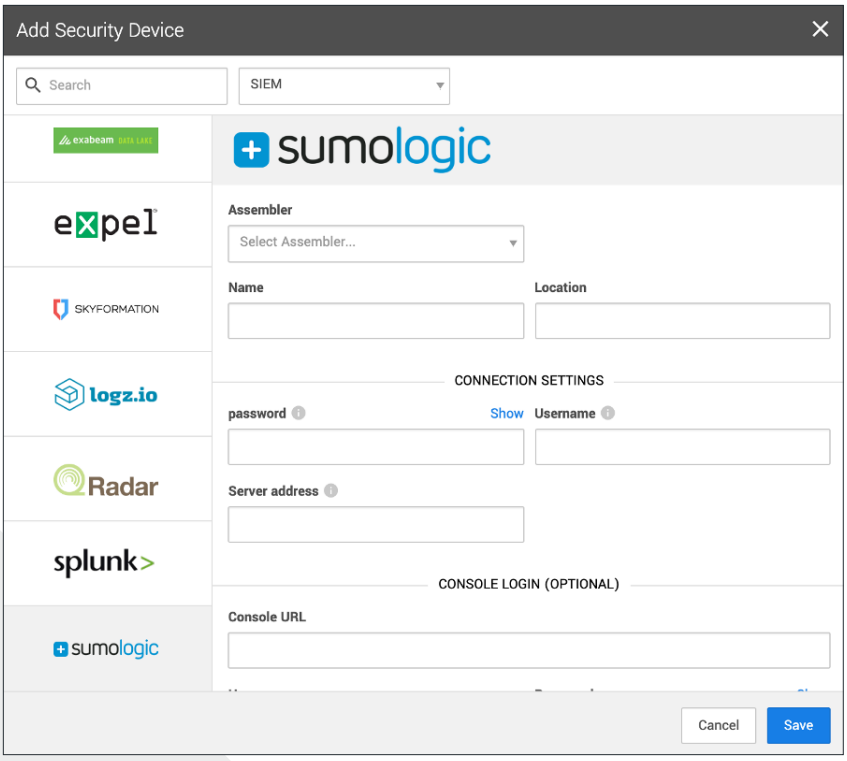

Figure 9

O. After a few minutes, refresh the **Security Devices** page and you should see your device status reporting as *Healthy*, or if there is an issue, it will provide more details of what the issue may be

P. To check and see if alerts are coming through, navigate to **Alerts** on the console page, then click the icon in the upper right to switch to grid view, then check the list for Zscaler alerts

That's it. Give yourself a pat on the back — you're done!

If you have any issues, concerns, questions or feedback,
please don't hesitate to contact Expel at devicehealth@expel.io.