Exabeam Advanced Analytics getting started guide

Version 2.0

March 19, 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. Configure Exabeam Advanced Analytics 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.

The Exabeam Security Management Platform uniquely combines a data lake for unlimited data collection, machine learning for advanced analytics, and automated incident response into an integrated set of products. The Expel SOC requires a dedicated User Account, which will allow our analysts to respond to security alerts and leverage the data available in Exabeam.

Create a user account

A. At the top right from drop down menu, navigate to **Settings** (Figure 1)

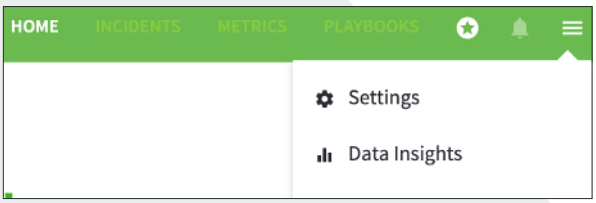

Figure 1

B. Under the **Exabeam User Management** section select **Users** (Figure 3)

C. Select **Add User**

D. Enter the following information for the requested fields (see Figures 2 and 3):

Field Name	What to put in it
User Type	Local
Username	expel
Full Name	Expel SOC
Email	This optional field can be left blank
Password	Enter a password. **Save the password to enter later in Workbench**

Figure 2

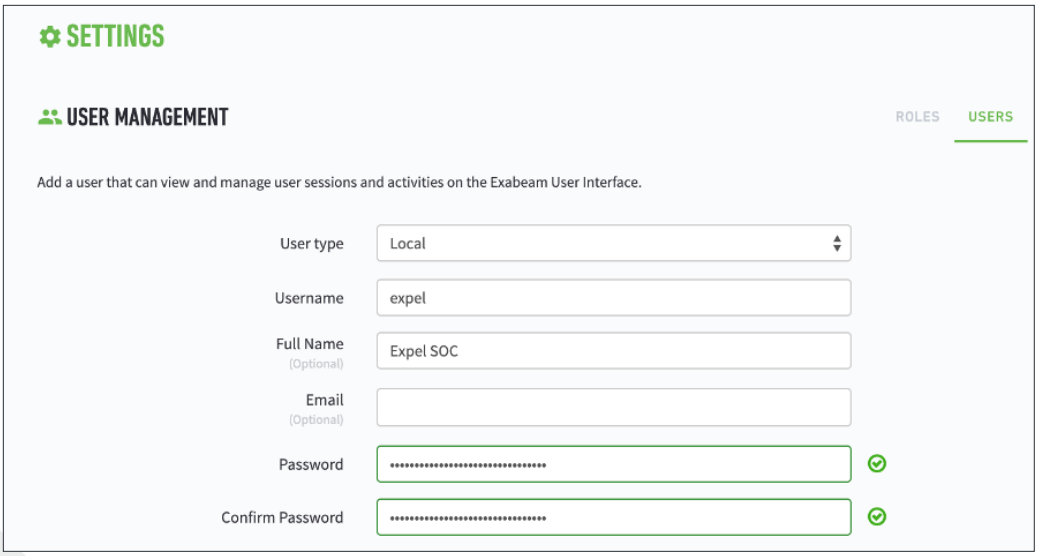

Figure 3

E. For Role, select **Tier 3 Analyst**. See Figure 4 (If a custom role is preferred, please complete *Steps F and G* below. Please note the permission requirements. If a custom role is not needed, please skip to *Step 2* below)

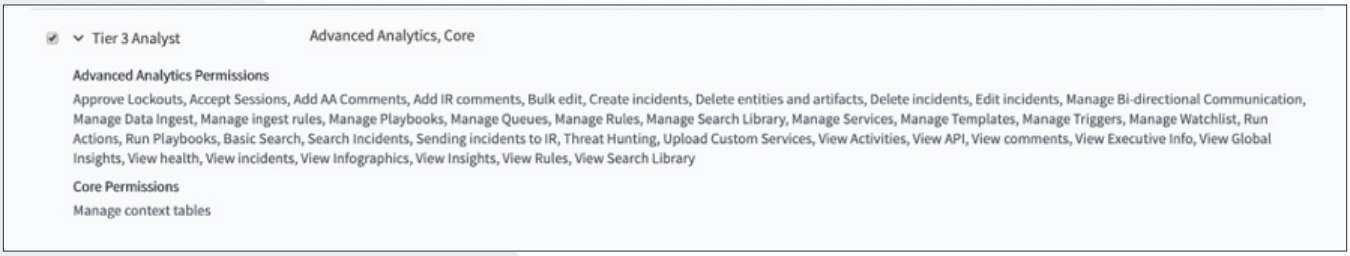

Figure 4

F. For a **custom role**, enter **Expel** for Role Name and **Expel Custom Role** for Description

G. Select **Advanced Analytics**, and choose the following permissions (see Figure 5):

View	
View Activities	Required
View Executive Info	Required
View Global Insights	Required
View Infographics	Required
View Insights	Required
View Rules	Required
Edit & Approve	
Approve Lockouts	Optional but recommended
Accept Sessions	Optional but recommended
Manage Rules	Optional but recommended
Manage Watchlist	Optional but recommended
Search	
Manage Search Library	Optional but recommended
Basic Search	Required
Threat Hunting	Required
View Search Library	Required

Figure 5

Step 2 — Configure the technology in Workbench

Now that we have all the correct access configured, we can integrate Exabeam with Expel.

Register device in Expel Workbench

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

B. Enter 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** (See Figure 6)

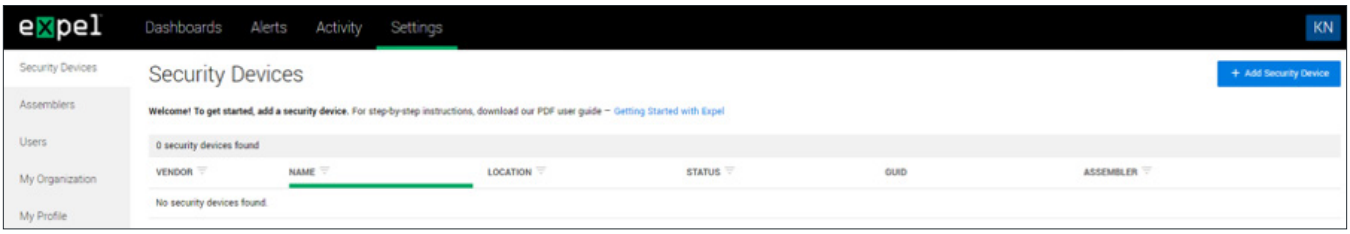

Figure 6

E. Search for and select **Exabeam Advanced Analytics** from the list of support technologies

F. Complete all fields using the credentials and information you collected in *Step 1* above (see Figure 7)

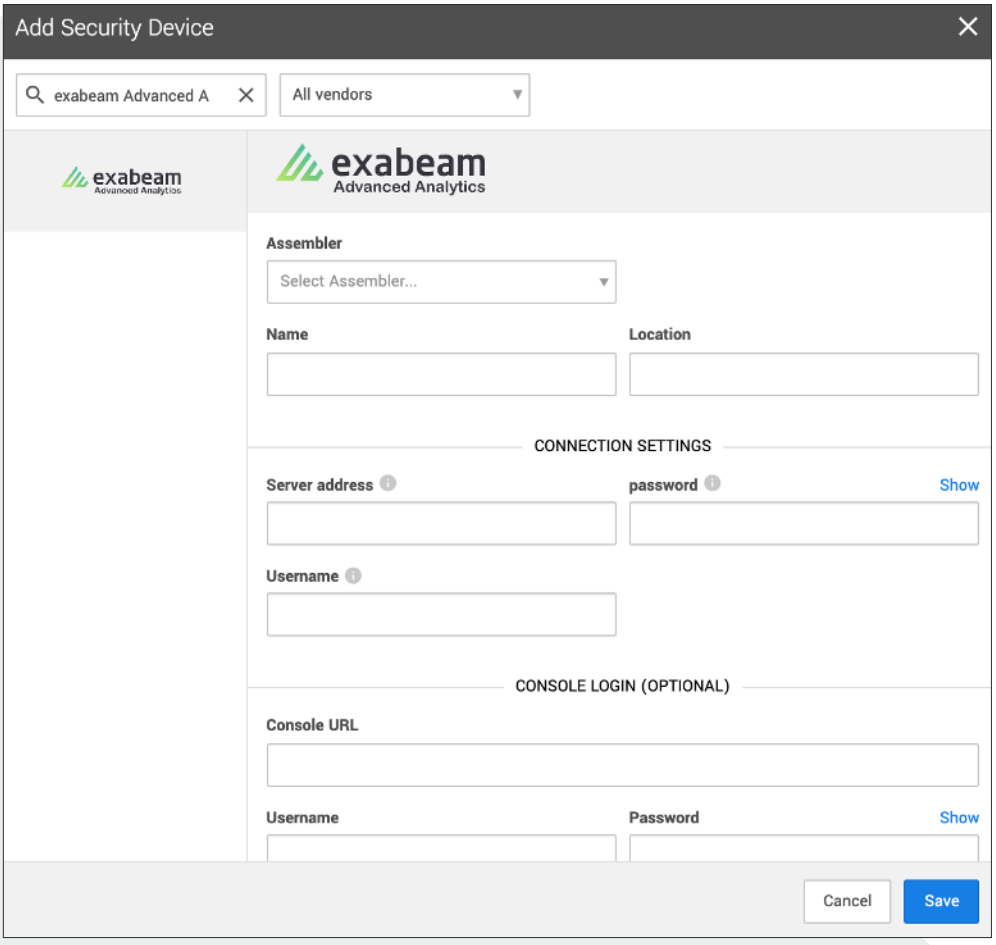

Figure 7

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

H. Enter **Name** (give your Exabeam a name)

I. Enter city or site where your Exabeam is located for **Location**

J. Enter **Server Address** (IP address for Exabeam)

K. For **Password** enter the password you entered in *Step 1, letter D*

L. Enter **Username** enter the username you entered in *Step 1, letter D*

M. Select **Save**

N. After a few minutes (1–10 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

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