Lacework getting started guide

Version 1.0

August 31, 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. Generate the Application Program Interface (API) Credentials; and
3. Configure the Lacework 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.

A. Create a user in Lacework for Expel or create an SSO user for Expel that has access to Lacework

Step 2 — Generate API credentials

In order to integrate the technology with Expel, we need to create secure credentials to the API. Depending on the permissions allowed in *Step 1* above, Expel may be able to generate API credentials. If you're unsure, please contact Expel at devicehealth@expel.io.

Lacework provides a combination of API Access keys and tokens to be used by clients and client applications to access the Lacework API. API access key IDs and secret access keys are created using the Lacework Console. Temporary access (bearer) tokens, which are used by clients, are created using the Lacework API

Only administrators can create API access keys with a limit of two per user. An API access key does not expire but can be disabled or deleted. After creation, administrators can download and securely store the secret key.

For more information about creating and using access (bearer) tokens for accounts in an Organization, see Role-Based API Authentication for Organizations.

A. To create an API key, navigate to **Settings > API Keys** and click **+ Create New**. Enter a name for the key and an optional description and click **Save**. To get the secret key, download the generated API key file and open it in an editor. Docs reference: https://support.lacework.com/hc/en-us/articles/360011403853-Generate-API-Access-Keys-and-Tokens

Step 3 — Configure the technology in Workbench

Now that we have all the correct access configured and have noted the credentials, we can integrate Lacework with Expel Workbench.

Register device in Expel Workbench

A. In a new browser tab, login to 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** (Figure 1)

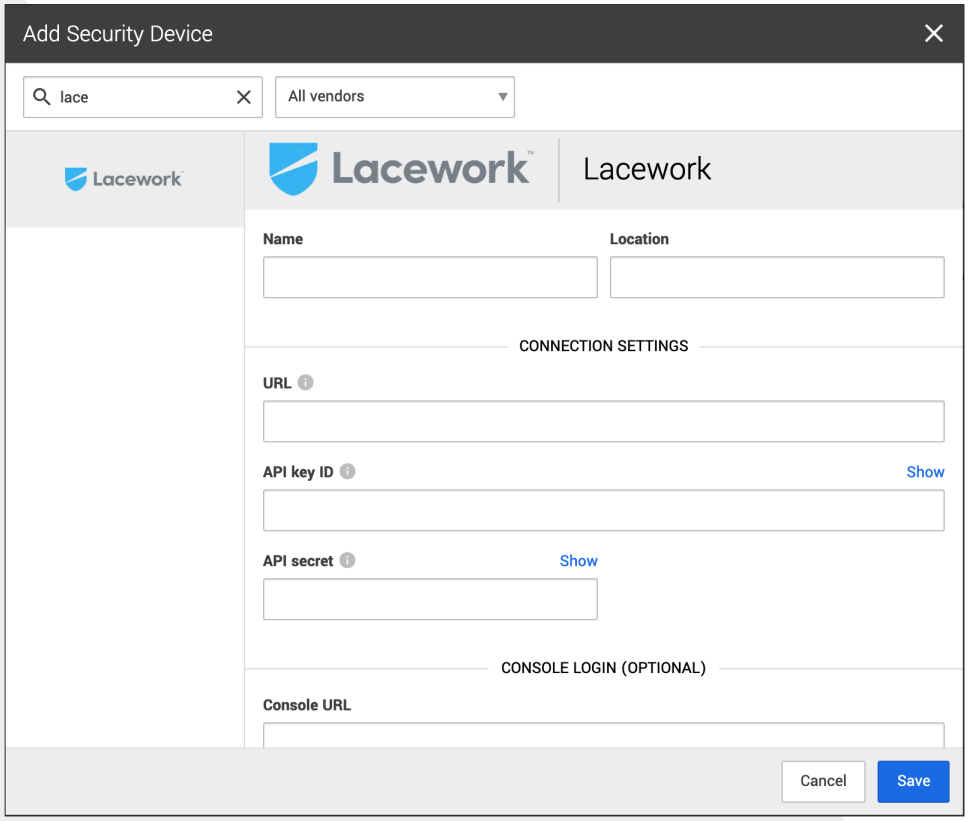

Figure 1

E. Search for and select your technology

F. Complete all fields using the credentials and information you collected in *Step 1* and *Step 2* above

G. For **Name** enter the hostname of the Lacework device

H. For **Location** enter the geographic location of the appliance

I. For **Server address** enter the hostname or IP address of the **Lacework management interface** (Device IP can be found in the Lacework console under Dashboard >> General Information >> MGT IP Address)

J. For **API key** enter the API generated in *Step 2*

K. Username and Password fields can be left blank, or can be filled in with the username and password created in *Step 1*

L. Select **Save**

M. 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

N. 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 Lacework 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.