expel®

Getting started with Expel

Version 2.7

www.expel.io

Welcome to Expel. We're excited to be working with you! We've put a lot of effort into making it as easy as possible to get going. There are three basic steps and this guide walks you through each of them.

- **Step one** is getting your account set up in the Expel Workbench™.
- **Step two** is downloading and installing the Expel Assembler. It's the only piece of software you need to install.
- **Step three** is connecting your security devices to Expel.

Three steps. That's it and you'll be ready to go. We're always looking to make things easier. If you see anything along the way that would make this process smoother don't be shy – let us know!

Things you'll need to get started

Before you get going there are four things you'll need for smooth sailing. We recommend you have all of these at your fingertips before you move forward.

1. A smartphone with the Google Authenticator app installed
2. Access to VMware ESXi version 4.1 or later to run the Expel Assembler with the following minimum resources available:
   - 4 virtual CPUs
   - 8 GB RAM
   - 100 GB disk space
3. The ability for the Assembler virtual machine to connect to the following:

Host	Ports
provisionvpn.ops.expel.io	TCP 443 or TCP 1194
servicevpn.ops.expel.io	

4. Appropriate access for the devices you'll be connecting to the Expel Assembler. Here's a quick list of what you'll need for each product we support. If you're trying to connect a product that's not in the list below just let your Expel engagement manager know.

Product Type	Prerequisite
Carbon Black	Access to Carbon Black Response Console as Administrator for the creation of an API Key
Palo Alto Networks	Access to the Palo Alto Networks Panorama or firewall for the creation of an API Key

Step 1: Set up your Expel Workbench account

The Expel Workbench is what you'll use to see everything Expel is doing for you. Here's how you get your account set up.

1. Check your inbox. You should have received a *Welcome to Expel* email. It includes a link to activate your Expel Workbench account. If you haven't received the email (or just can't find it) don't worry. Just let us know and we'll shoot another one over to you right away.
2. Click the **activation link** in your welcome email and follow the directions to configure your password and two-factor authentication using the Google Authenticator app on your smartphone.
3. **Protip:** Bookmark https://workbench.expel.io so you'll have quick access to the Expel Workbench in the future.

Step 2: Set up the Expel Assembler

The Expel Assembler is what enables you to create a secure VPN connection so that we can access your security devices. We've packaged it as a virtual machine. If you install VM images regularly this should be pretty straightforward. If not, now's your chance to phone a friend. Here's how you download it and get your applications connected:

- Download the Assembler image from the Expel Workbench
- Register the Assembler in the Expel Workbench
- Deploy the Assembler virtual machine in your network
- Activate the Assembler via the virtual machine console
- Authorize the Assembler in the Expel Workbench

If your network is segmented you may need to deploy multiple assemblers. If you have any questions about how many Assemblers to install let us know and we'll recommend the best approach for your environment. Follow these steps for each Assembler you will deploy.

Download the Assembler image

1. In the Expel Workbench, click on **Settings** in the top navigation bar.
2. Click the **Download Installer** button. Now's a good time to grab a cup of coffee because it'll take a few minutes to download.
3. After the download completes, verify that a hash of the file downloaded matches the data shown in the Expel Workbench. The table below shows how you can do this for the three main operating systems.

This is an important step because it will confirm that your download is complete and that no one has tampered with the image. If the hash doesn't match, download it again and re-check the hash. If the hash still doesn't match after the second time something's not right. In that case, please contact your Expel engagement manager.

Operating system	Hash to verify	Command

Windows	SHA256	Search for cmd, and select cmd.exe or "Command Prompt" from the results. Run these commands in the window that opens:
		`cd <your download folder>`
		`certutil -hashfile expel-assembler-vmware-<version>.ova sha256`

Mac OS	SHA1	In Spotlight Search, search for the Terminal program and run it. In the terminal window, run this command: `shasum ~/Downloads/expel-assembler-vmware-<version>.ova`
Linux	SHA256	In a terminal program, run: `sha256sum ~/Downloads/expel-assembler-vmware-<version>.ova`

Register the Assembler in the Expel Workbench

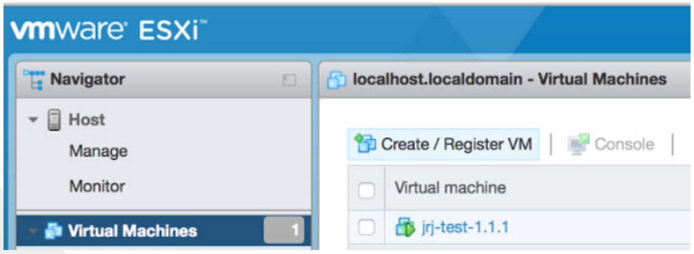
1. In the Expel Workbench, click on **Settings** in the top navigation bar.
2. You should see a box with the Assembler Name and Location fields—if not, click the **Add Assembler** button.
3. Enter the Assembler Name and Location for the Assembler. It's best to choose names that will be meaningful to both you and to Expel so you can easily identify the Assembler in the user interface (e.g. ACME HQ).
4. Click **Save**.
5. Note the **Install Code** for the newly registered Assembler. You will need this later to activate the Assembler.
6. If you want to add another Assembler, click the **Add Assembler** button and repeat the previous steps.

Deploy the Assembler virtual machine in your network

Import the file you downloaded from the Expel Workbench into your VMware environment using your VMware admin tools. The following instructions assume you are using the VMware ESXi web interface, but you're free to use another tool.

1. Select **Virtual Machines** in the Navigator panel on the left

2. Click the **Create / Register VM** button



3. Choose *"Deploy a Virtual Machine from an OVF or OVA file"*, then click **Next**.

4. Give the virtual machine a name, select the file you downloaded, then click **Next**.

5. Select the datastore to use for the virtual machine, then click **Next**. VMware will now extract the OVA file, which may take a minute or two.

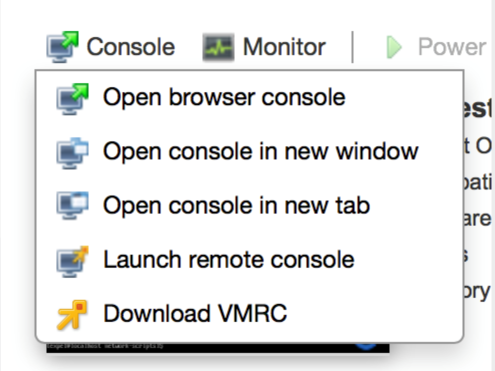
6. Choose your preferred network method and provisioning. Use the defaults unless you have a reason to change them. Click **Next**.

Review the settings, then click **Finish**. The OVA file will now upload to the ESXi server, which may take a few minutes.

Activate the Assembler via the virtual machine console

1. Select the newly imported Virtual Machine for the Assembler.

2. Click **Console** to access the console of the Assembler via one of the methods supported by VMware.



3. Log in with username **expel** and password **expel**.

4. Run the `passwd` command to set a unique and secure password on the "expel" account.

   You must first enter the existing password, then enter the new password twice.

   Remember the new password; you will need it to log in to the Assembler again.

   ```
   [expel@localhost ~]$ passwd
   (current) UNIX password: expel
   New password: <enter new password>
   Retype new password: <enter new password again>
   ```

5. Determine the network interface to use by running:

   ```
   sudo expelmanage --list-interfaces
   ```

6. The Assembler uses DHCP by default. If you wish to use DHCP, skip to the next step. If you wish to use a static network configuration, run:

   ```
   sudo expelmanage --net --interface <interface name> --type static --ip
   <IP address> --netmask <subnet mask> --gateway <gateway IP> --dns
   <nameserver IP>
   ```

   `<interface name>` is determined in the previous step.

   Get the IP address, subnet mask, gateway IP, and nameserver IP to input into the above command from your VMware administrator.

7. Activate the Assembler by supplying the 8-character install code created in Step 2: Register the Assembler above:

   ```
   sudo expelmanage --activate <eight-character install code>
   ```

   You should see output like this:

   ```
   [expel@hostname ~]$ sudo expelmanage --activate abcd1234
   Activation code set
   Regenerating SSH keys
   Activated
   [expel@hostname ~]$
   ```

Authorize the Assembler in the Expel Portal

Within 30 seconds of activating the Assembler with a matching install code, the Assembler you registered at https://workbench.expel.io/settings/assemblers will change status from *Not Yet Connected* to *Connected*, and an **Authorize** button will appear for the Assembler. Once this happens, click the Authorize button.

Expel will now automatically configure the Assembler. This process takes approximately 10 minutes but could take longer if you have a slow network connection. When complete, the status will change to *Active*.

Step 3: Register your security devices

Follow this procedure on https://workbench.expel.io for each security device you wish to connect to Expel.

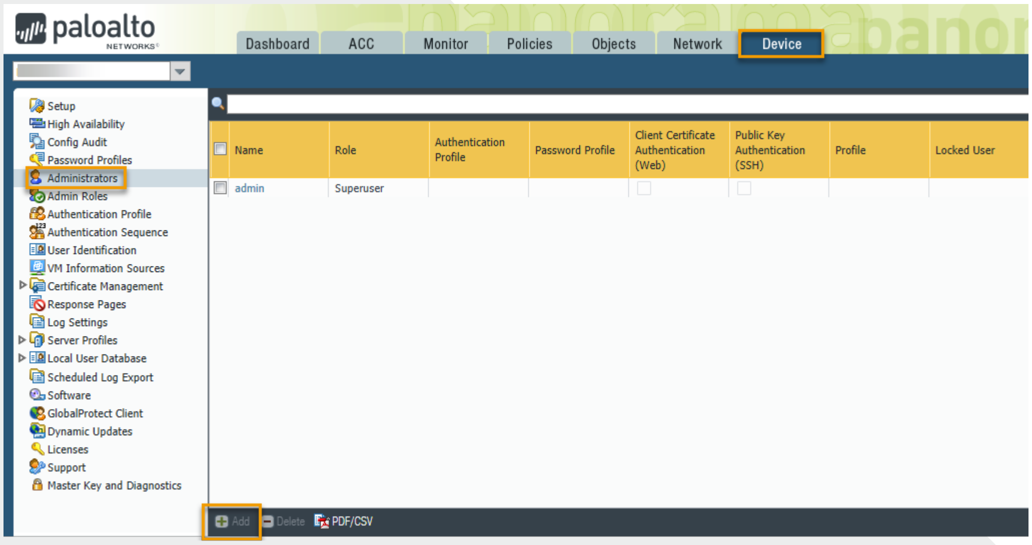
1. Click on **Settings** in the top navigation bar
2. Click **Security Devices** in the left panel
3. Click the **Add Security Device** button
4. Choose the Assembler that has network connectivity to the security device
5. Choose the type of security device you want to connect
6. Enter a Name and Location that will be meaningful to both you and to Expel
7. Enter additional information specific to the security device type (described below)
8. Click **Finish**

Registration steps for Palo Alto Networks

This procedure will create a user account for Expel to use that will keep Expel's activity separate from other activity on the Palo Alto console.

Step 1: Create an Administrator

1. Navigate to "Devices >> Administrators" and click the "Add" button at the bottom of the page.

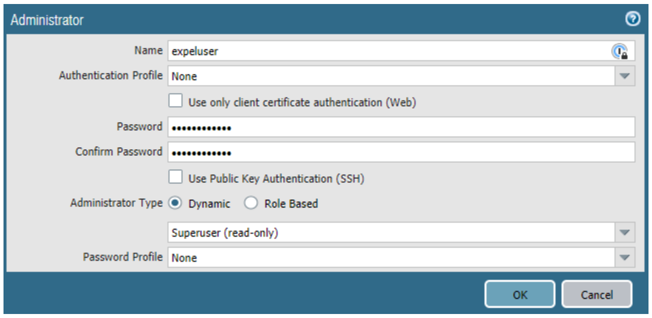


☐	Name	Role	Authentication Profile	Password Profile	Client Certificate Authentication (Web)	Public Key Authentication (SSH)	Profile	Locked User
☐	admin	Superuser			☐	☐		

Adding an Administrator

- Enter the desired admin name and password.
- Make sure the "Administrator Type" radio button is set to "Dynamic".

- Select “Superuser (read-only)” from the dropdown list.



Name: expeluser
Authentication Profile: None
□ Use only client certificate authentication (Web)
Password: ••••••••••••
Confirm Password: ••••••••••••
□ Use Public Key Authentication (SSH)
Administrator Type: ● Dynamic ○ Role Based
Superuser (read-only)
Password Profile: None

Selecting the appropriate Administrator Type

- Click OK.
- Commit the changes.

Step 3: Create the API Key

Note: SAML authenticated accounts on Palo Alto Networks cannot generate API keys.

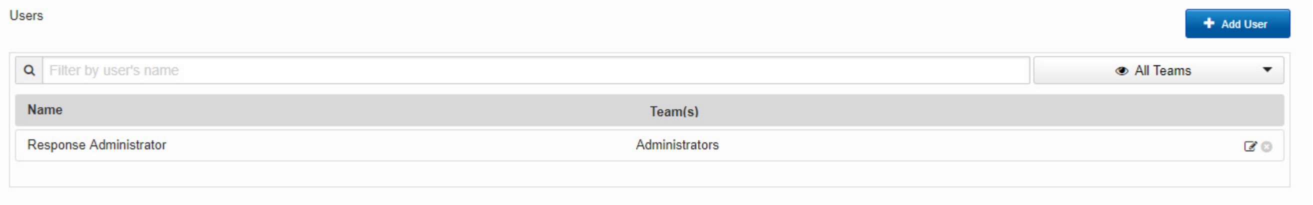
Supply the following additional information in the Palo Alto device screen on the Expel Workbench:

Field	Description
Apikey	Authentication token that allows the Expel Assembler to access the Palo Alto Networks Panorama or firewall. Create one by accessing the following URL in your browser, replacing `<hostname or IP address>`, `<username>`, and `<password>` with the appropriate values for your Panorama or the management interface of your Palo Alto Networks firewall: `https://<hostname or ip address>/api/?type=keygen&user=<username>&password=<password>`
Server	The IP address of the Palo Alto Networks Panorama or the firewall’s management network interface

Registration steps for Carbon Black hosted on premise

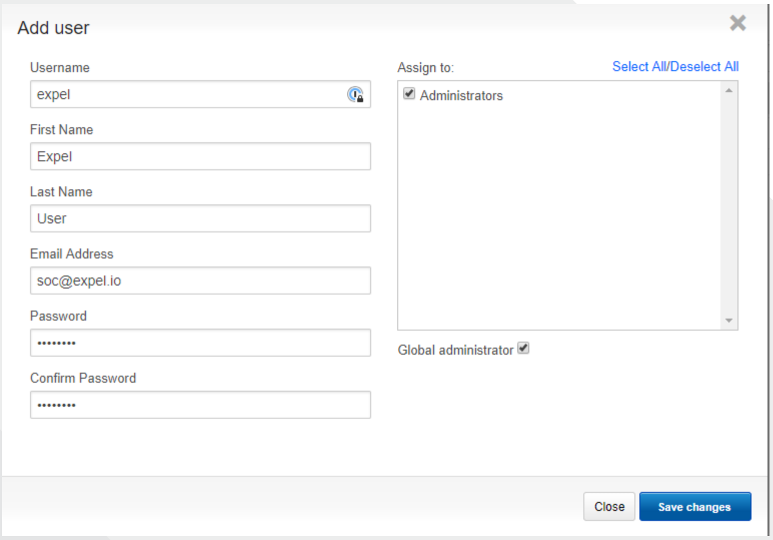
This procedure will create an Expel User Account for your Carbon Black Response Console hosted on premise.

1. Log in to your Carbon Black Response Console.
2. Click **Administration** then **Users** on the Carbon Black menu in the top-right of the screen.
3. Click **Add User**.



Name	Team(s)
Response Administrator	Administrators

4. Create the Expel User with the following properties as shown below:
   - Username: expel
   - First Name: Expel
   - Last Name: User
   - Email address: <something at your company>
   - Password: Use a complex password of your choice that you remember or store in a password manager
   - Assign to: Administrators
   - Check: Global administrator (global administrators is required to perform the necessary functions within Carbon Black Response for pulling process listings, etc.)



Username: expel

First Name: Expel

Last Name: User

Email Address: soc@expel.io

Password: ••••••••

Confirm Password: ••••••••

Assign to:

☑ Administrators

Global administrator ☑

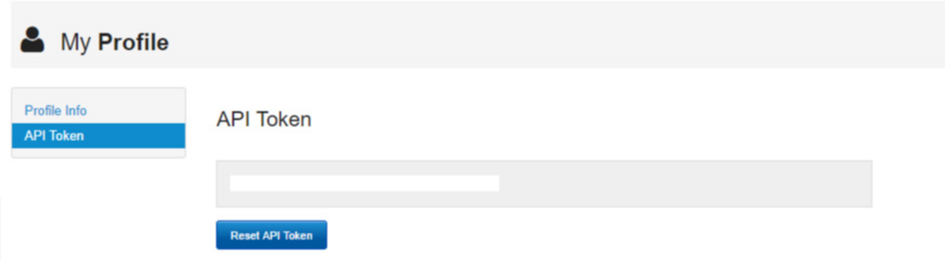
5. Log out of the Carbon Black Response Console

6. Log in to the Carbon Black Response Console, this time as the newly-created Expel User

7. Click **Expel User** in the top-right, then **My Profile**, then **API Token**

8. Copy the API token to the *Apikey* field in the Expel Workbench's Add Security Device form

9. Log out of the Carbon Black Response Console



10. Enter the URL of the Carbon Black server for the Server field in Expel Workbench. For example, https://10.0.0.10

    The last step is enabling live response so we can interact with your endpoints (pull process listings, etc.). To verify Carbon Black Live Response is enabled:

11. Go to the sensor tab on the left menu in the Cb console

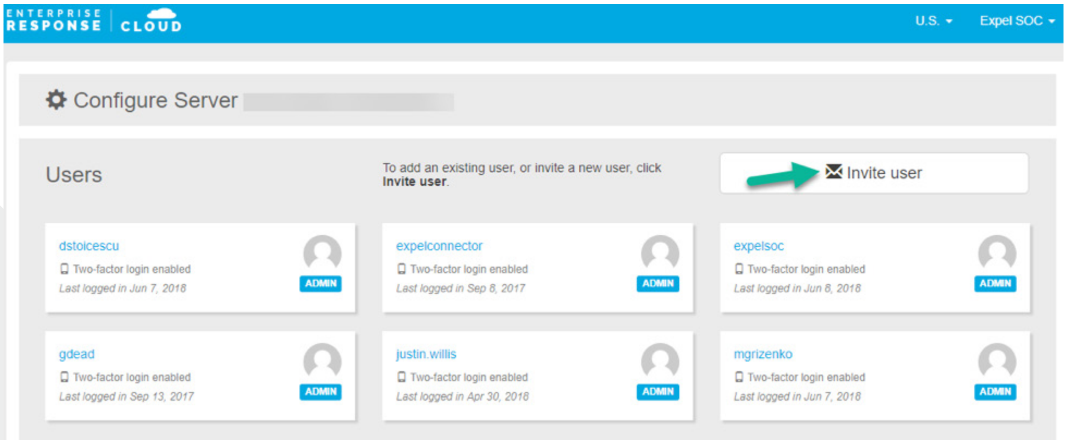
12. Click any host name

13. In the top-left corner, the button "Go Live" will be active if Carbon Black Live Response is enabled. If it is you are DONE.

Registration steps for Carbon Black Response (Cloud Hosted)

This procedure will create an Expel User Account for your Carbon Black Response Console hosted in the Cloud.

1. Log in to your Carbon Black Response Console.
2. Click on the **Users** icon listed on the toolbar, towards the left.
3. Select **Invite User**



To add an existing user, or invite a new user, click **Invite user**.

4. Create the Expel User with the following properties as shown below:
   - Email address: **soc@expel.io**
   - Privileges: **Administrator**
   - Select **Send Invite**

If Carbon Black Live Response is not enabled and hosted on prem:

1. SSH into the Cb appliance and perform the command “vi /etc/cb/cb.conf”
2. Search for “CbLREnabled=False” and change the value from False to True
3. Restart services for the change to take effect: “service cb-enterprise restart”

If Carbon Black Live Response is not enabled and hosted in their cloud:

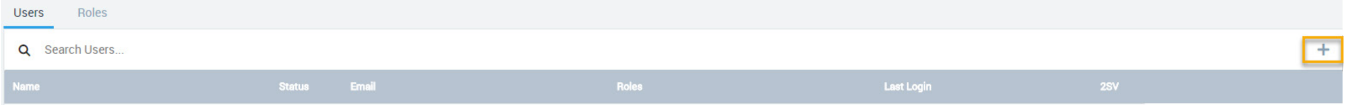
1. You will need to submit a request to the Carbon Black Cloud Support team requesting this feature be enabled. You can simply send the request with the following:

   “Please enable Live Response and VDI Behavior”

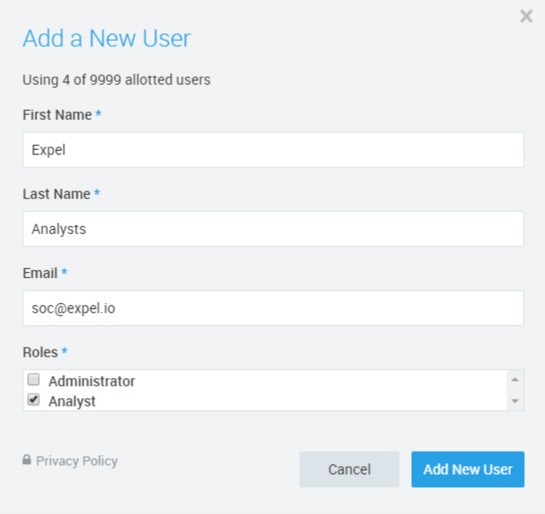
Registration steps for SumoLogic

This procedure will create a user account for Expel to use that will keep Expel's activity separate from other activity on your instance of SumoLogic.

1. Log in to your SumoLogic instance
2. Click "Administration" then select "Users and Roles"
3. In the "Users" menu, click on the + to add a new user



4. Create an Expel user with the following properties as shown:
   a. First Name: Expel
   b. Last Name: Analysts
   c. Email: soc@expel.io
   d. Roles: Analyst



Add a New User

Using 4 of 9999 allotted users

First Name *: Expel

Last Name *: Analysts

Email *: soc@expel.io

Roles *:
☐ Administrator
☑ Analyst

5. Click "Add New User"

I’m done setting it up. Now what?

Congratulations. Give yourself a high five. Expel will now verify that we have connectivity to your security products and understand the current state of your environment.

Once the data starts flowing we can begin gathering context about your environment, we will be working to identify things like your critical assets, admin accounts, vulnerability scanning services as just a start. As we continue to gain more context we can better integrate with your organization. Don’t worry, we will be reaching out to validate things as we find them, but it will never be a one-time thing. As things change we continue to learn, we also learn from our other customers and will pass those learnings over to you.