Getting started with Expel

Version 2.10

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 three 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 your preferred app installed to generate TOTP tokens, like the Google Authenticator app.

2. A place to run the Expel Assembler virtual machine. We work with VMware or Hyper-V for on-prem environments and AWS or Microsoft Azure for cloud environments. You'll need 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:

    a. Our VPN servers.

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

    b. The security devices you'll be connecting to the Expel Assembler. Reach out to your engagement manager for documentation on each security device.

    c. Your DHCP server (unless you choose to assign a static IP to the Assembler).

    d. Your DNS server.

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** button 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 virtual machine 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.

3. Select your preferred virtualization technology.

4. Click the **Download** button. Now's a good time to grab a cup of coffee because it'll take a few minutes to download.

5. 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	SHA256	In Spotlight Search, search for the Terminal program and run it. In the terminal window, run this command: `shasum -a 256 ~/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 virtual infrastructure environment using your admin tools. Click the appropriate link below for instructions on deploying the Assembler virtual machine in your network:

- [Deploying the Assembler on VMware](#).

- [Deploying the Assembler on Hyper-V](#).

- [Deploying the Assembler on Microsoft Azure](#).

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.

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.

   Note: Your password must be at least 8 characters and not a word found in the dictionary.

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

5. **AZURE USERS ONLY:** Delete the users you had to create during VM creation by running:

   ```
   sudo userdel temp
   ```

6. Determine the network interface to use by running:

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

7. 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.

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

8. 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 ~]$
```

9. Run **exit** to log out of the console.

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**

For additional information for registering your specific security devices, contact your engagement manager.

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.