



AWS GuardDuty getting started guide (IAM role)

Version 2.0

April 2, 2020

What's in this guide?

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

1. Create an AWS IAM Policy;
2. Create an AWS IAM Role; and
3. Configure AWS GuardDuty in Expel Workbench™.

Prerequisite

An AWS account with permissions to create and modify IAM roles.

Step 1 — Create an AWS IAM policy

In this step, we're going to create a permissions policy that will be assigned to the IAM Role.

- A. Log into the AWS console and navigate to the **IAM service** (Figure 1)

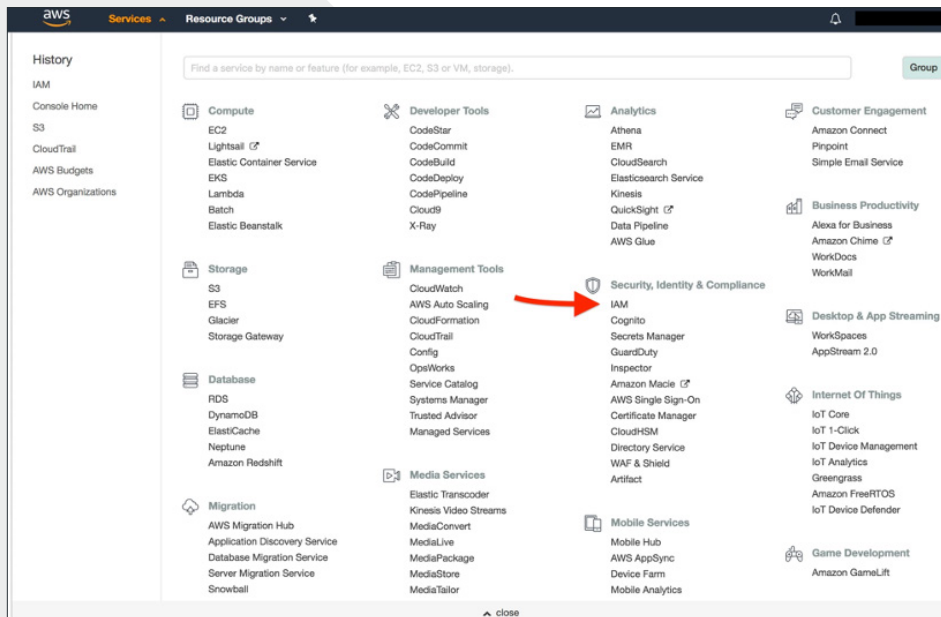


Figure 1

B. Go to **Policies** and click on **Create Policy** (Figure 2)

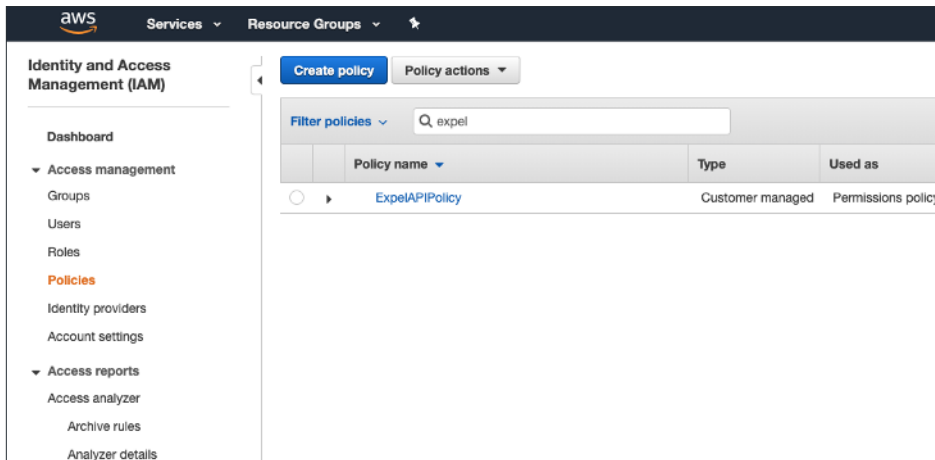


Figure 2

C. Add the following permissions using the JSON tab (Figure 3)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "guardduty:GetFindings",
        "guardduty:ListDetectors",
        "ec2:DescribeRegions",
        "guardduty:ListFindings",
        "guardduty:GetDetector"
      ],
      "Resource": "*"
    }
  ]
}
```

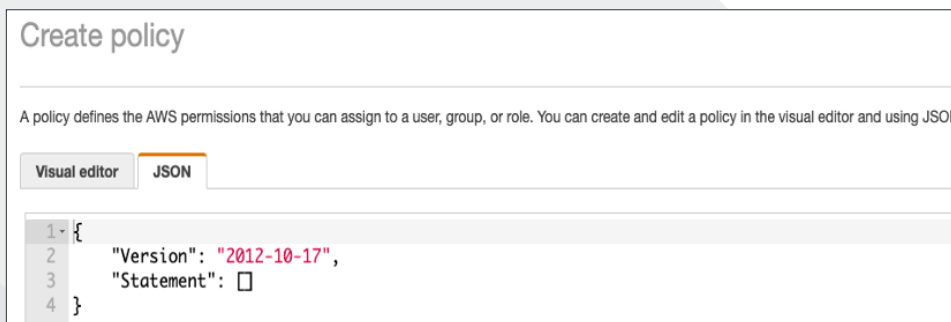


Figure 3

D. **Review** and **name** the policy (Figure 4)

Service	Access level	Resource	Request condition
Allow (2 of 216 services) Show remaining 214			
EC2	Limited: List	All resources	None
GuardDuty	Limited: List, Read	All resources	None

Figure 4

Step 2 — Create an IAM role

Create an IAM role to connect to your GuardDuty Service.

A. From within the IAM service, Navigate to **Roles** and press **Create Role** (Figure 5)

Figure 5

B. Select **Another AWS account** and fill out the required fields (Figure 6)

- a. **Account ID: 012205512454** (Expel’s AWS account ID)
- b. **External ID:** Choose a unique value. We recommend generating a long, unique passphrase

Create role 1 2 3 4

Select type of trusted entity

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID* ⓘ

Options Require external ID (Best practice when a third party will assume this role)

You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. [Learn more](#)

External ID

;

Important: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. [Learn more](#)

Require MFA ⓘ

Figure 6

C. Attach The **IAM policy** from *Step 1* to the Role (Figure 7)

Create role 1 2 3 4

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Filter policies ▾ Showing 2 results

	Policy name ▾	Used as
<input type="checkbox"/>	ExpelAPIPolicy	Permissions policy (4)
<input checked="" type="checkbox"/>	ExpelGuardDutyConnector	Permissions policy (1)

Figure 7

D. Give the Role a **name** and press **Create Role** (Figure 8)

Figure 8

E. Navigate to the role you just created and copy the following information for onboarding in Workbench (Figure 9)

- a. **Role ARN**
- b. **External ID Value** under the **Trust relationships** tab

Trusted entities	Conditions						
The account 012205512454	<table border="1"> <thead> <tr> <th>Condition</th> <th>Key</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>StringEquals</td> <td>sts:Externalid</td> <td>45f</td> </tr> </tbody> </table>	Condition	Key	Value	StringEquals	sts:Externalid	45f
Condition	Key	Value					
StringEquals	sts:Externalid	45f					

Figure 9

Step 3 – Onboard AWS GuardDuty in Workbench

Register device in Expel Workbench for IAM Role

- A. In a new browser tab, login to <https://workbench.expel.io>
- D. 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 10)

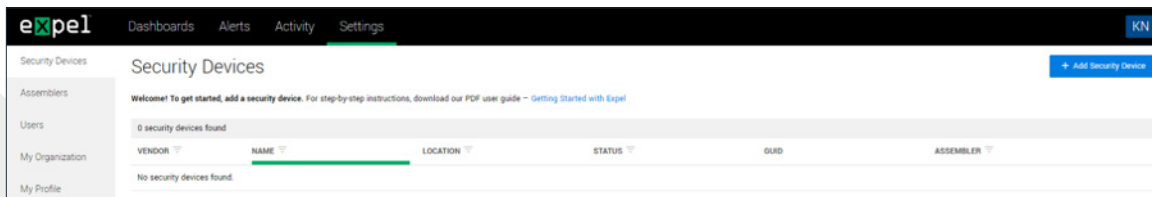


Figure 10

- E. Search for and select AWS Guard Duty (Figure 11)

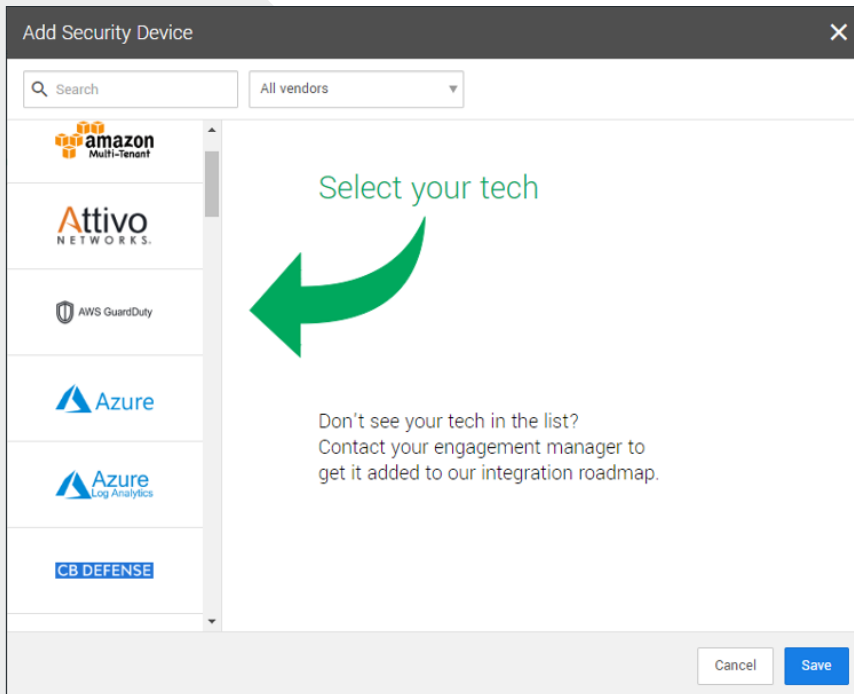


Figure 11

- F. See Figure 12 for Steps G-H

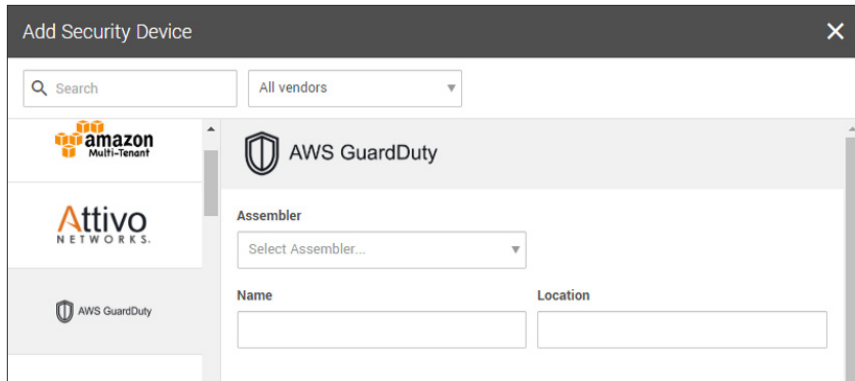
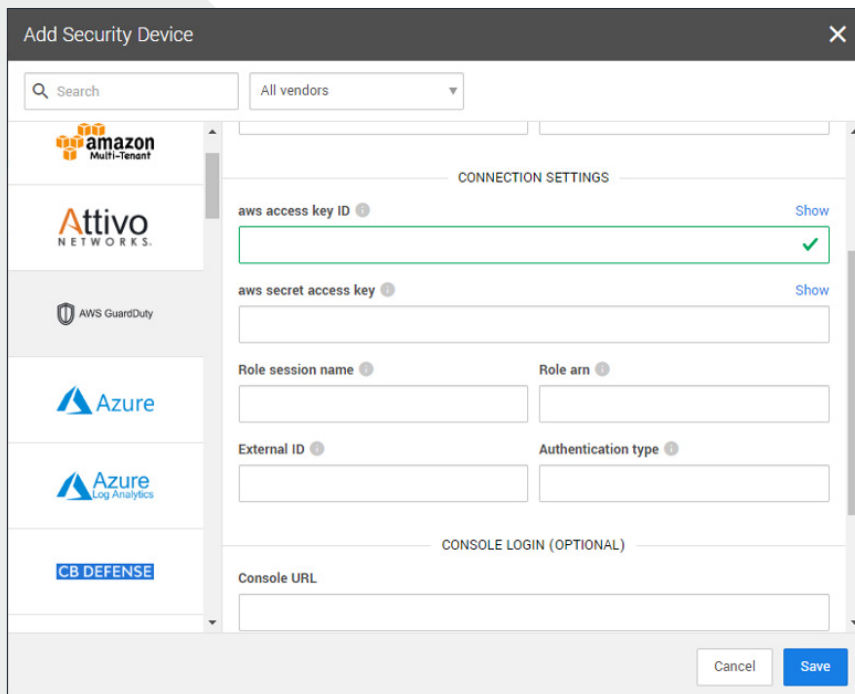


Figure 12

- G. For **Name** enter the hostname of the AWS GuardDuty device
- H. For **Location** enter the geographic location of the appliance
- I. See Figure 13 for Steps J-O

Figure 13



- J. **Role ARN:** Enter the Role ARN from Step 2, Letter E
- K. **External ID:** Enter the External ID from Step 2, Letter E
- L. **Role session name:** Use a unique name to identify the use of the role

- M. **Authentication type:** Enter **STSASSUMEROLE**
- N. Other fields can be left blank
- O. Select **Save**
- P. 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
- Q. 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 AWS GuardDuty 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.