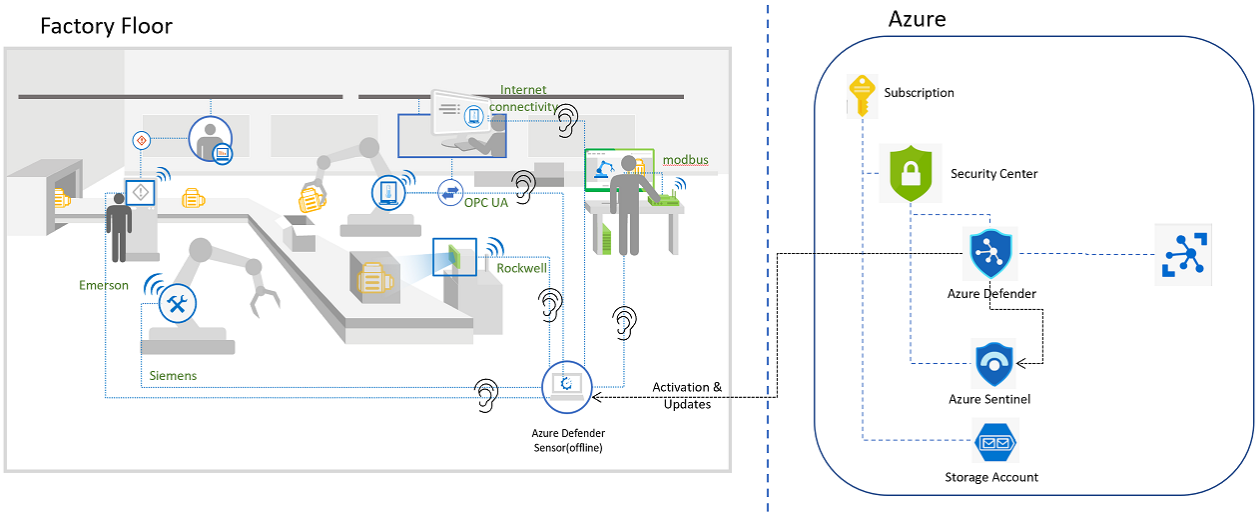
Internet of Things - Azure Defender for IoT HOL

Before starting this Lab make sure you completed the steps specified in **Azure Defender for IoT BHOL.md** File in this repository.

Architecture Diagram

During this workshop we will be focusing on setting up our Azure Defender sensors, for online alerts and also offline scenarios, you will learn how to configure your environment, assess the results, and integrate with SIEM systems like Azure Sentinel. This hands-on lab will be focus on Securing your facilities, this will cover brownfield and greenfield devices. The scenario below is one of many you would apply these lessons, other scenarios are Oil, Gas, Utility, and Energy companies.

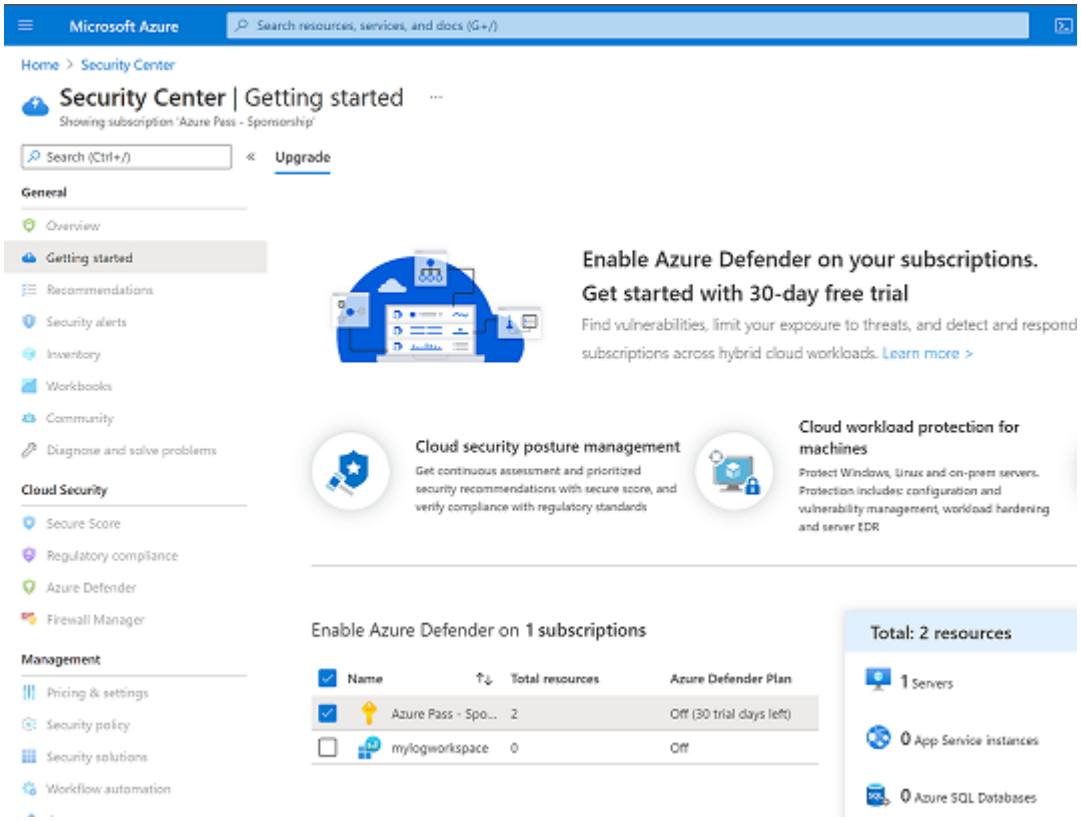


Content:

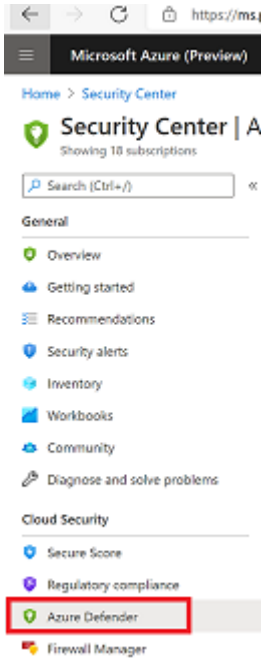
Exercise #1: Enabling Defender

Task 1: Enabling Azure Defender for IoT

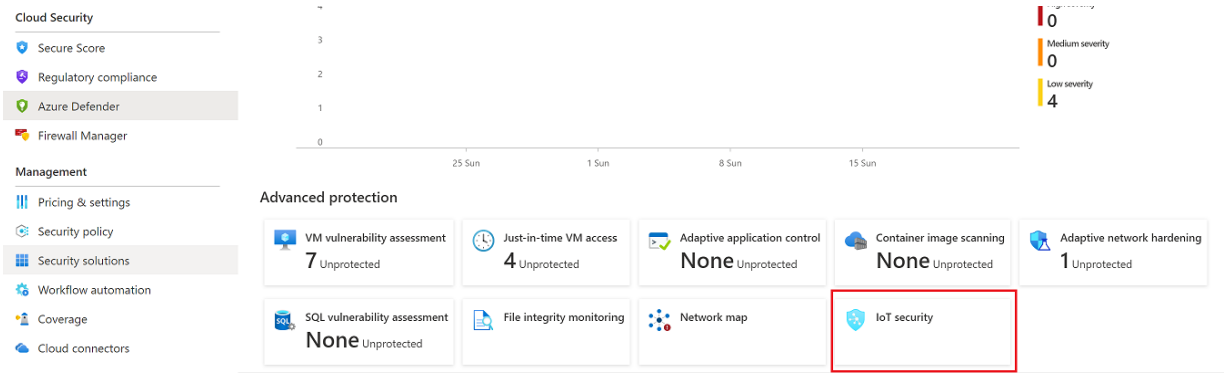
1. In Azure Portal open **Security Center**. The first opening Azure Security Center you will need to click on **Upgrade**, this buttom will appear at the bottom of the screen, scroll down.



2. Once enabled, on the left panel under **Cloud Security** select **Azure Defender**

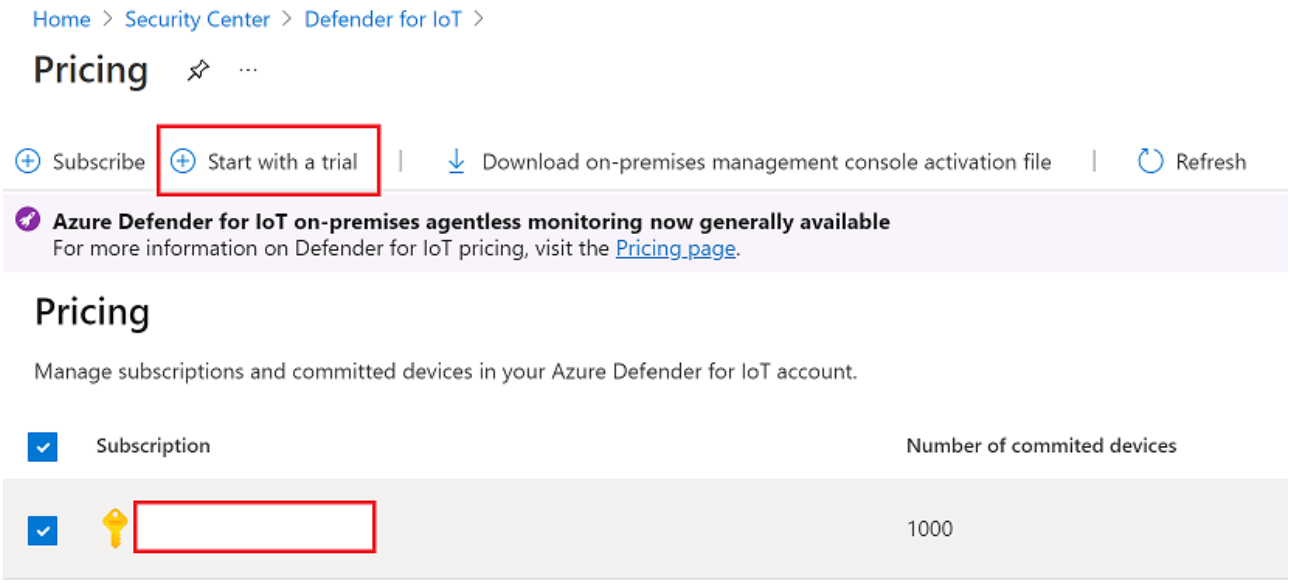


3. Next, select **IoT Security** under **Advanced Protection** section as shown below:



4. Next in the **Getting Started** section, select **Onboard Subscription**.

Before selecting your subscription make sure you select the option to + **Start with Trial** as shown below:



5. Then, select your subscription and keep the devices selection to 1000, that is the minimum amount of devices configuration. These devices represents all those equipments/sensors connected to your network in the facility you are analyzing. This configuration allows you for a 30 days trial for free. Select **Evaluate** to continue, last **Confirm**.

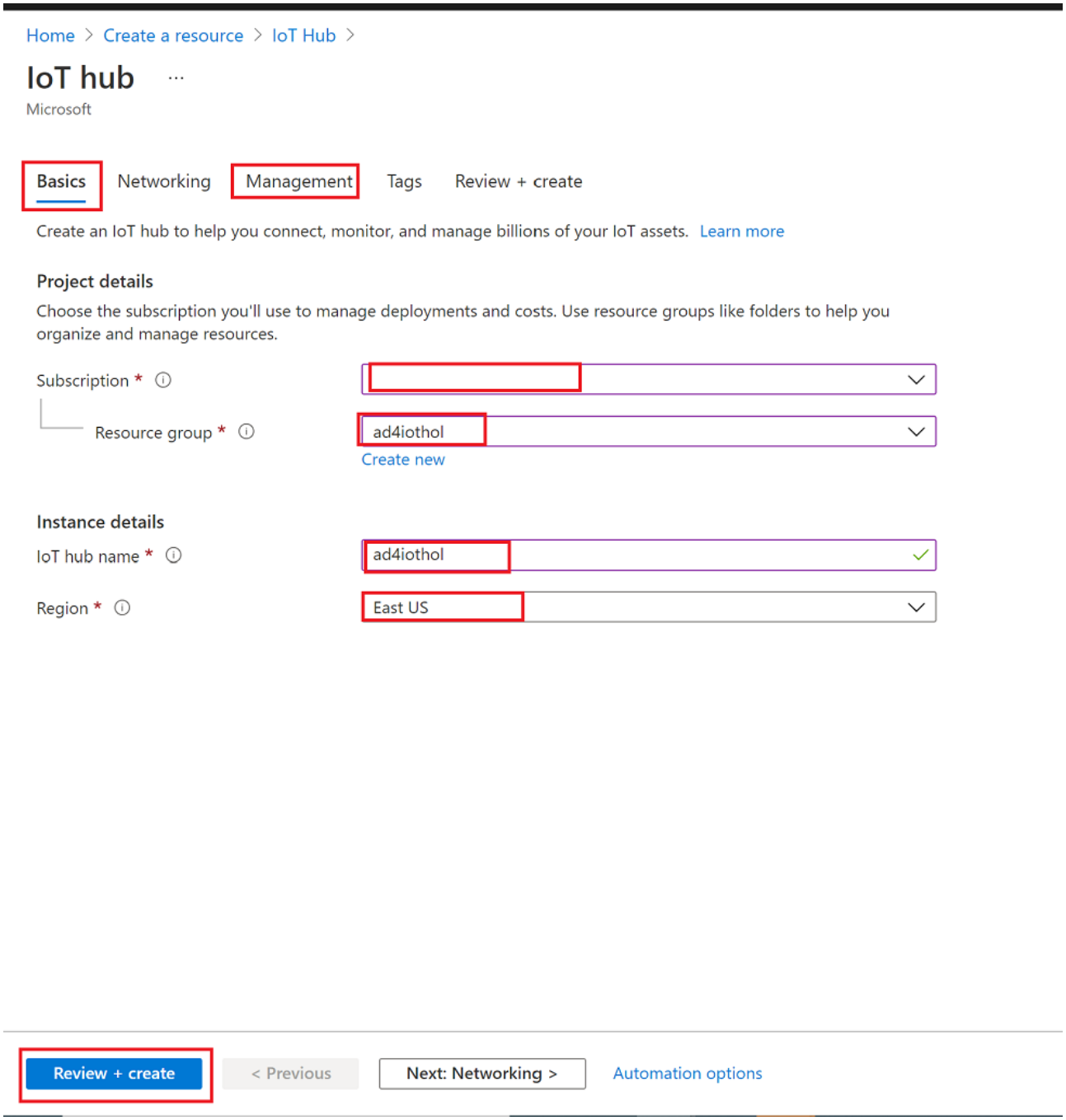
Task 2: Create an IoT Hub:

Before onboarding your sensors we will need to create an IoT Hub for your online sensor to connect to.

1. Go to the resource group you created for this training, in the Overview panel, you will see at the top + **Create**, click there and type **IoT Hub** in the search box, then click **Create**.

2. In the next screen you will ask to fill the **Basics** tab:

- **Subscription**: Select the Subscription you are woking on.
- **Resource Group**: Should be the resource group created in previous step.
- **IoT Hub Name**: adt4iothub+SUFFIX
- **Region**: East US.



3. Next, click on **Management** tab and make sure it is selected **S1:Standard Tier** in the **Pricing and scale tier** section.

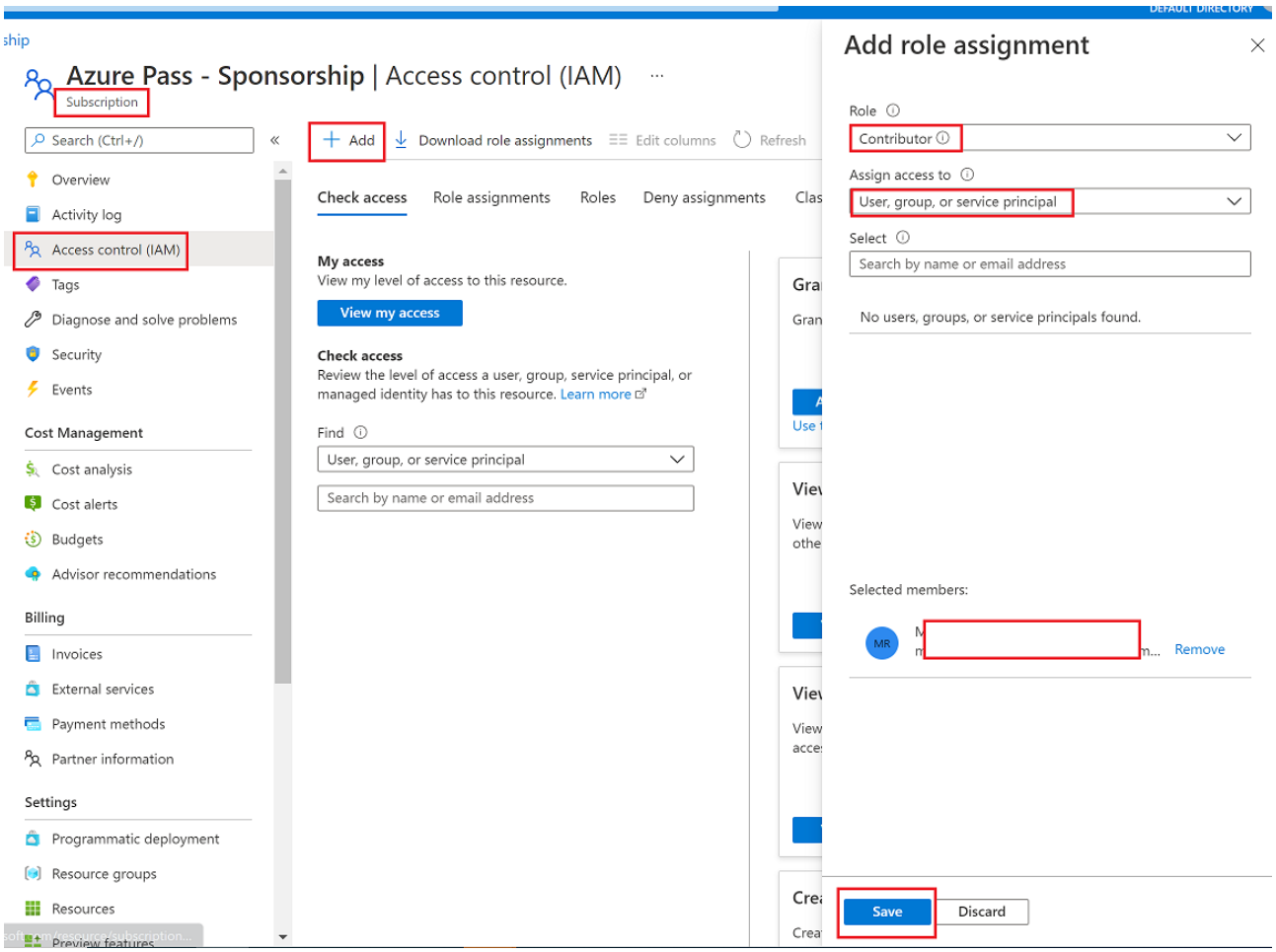
4. Last, click **Review + create**, once validation is completed, click **Create**.

5. While the IoT Hub is creating , in Azure Portal look for the Subscription, click on **Access Control(IAM)**, then select **+ Add**, a new window will open on your right, select the following:

    - **Role**: Contributor
    - **Assign access to**: User, group or service principal

- **Select**: search for the email you are using in this subscription. Select that email. Last, **Save**.

Azure Sentinel will need this access to collect the alerts in further exercises when your sensor is online.

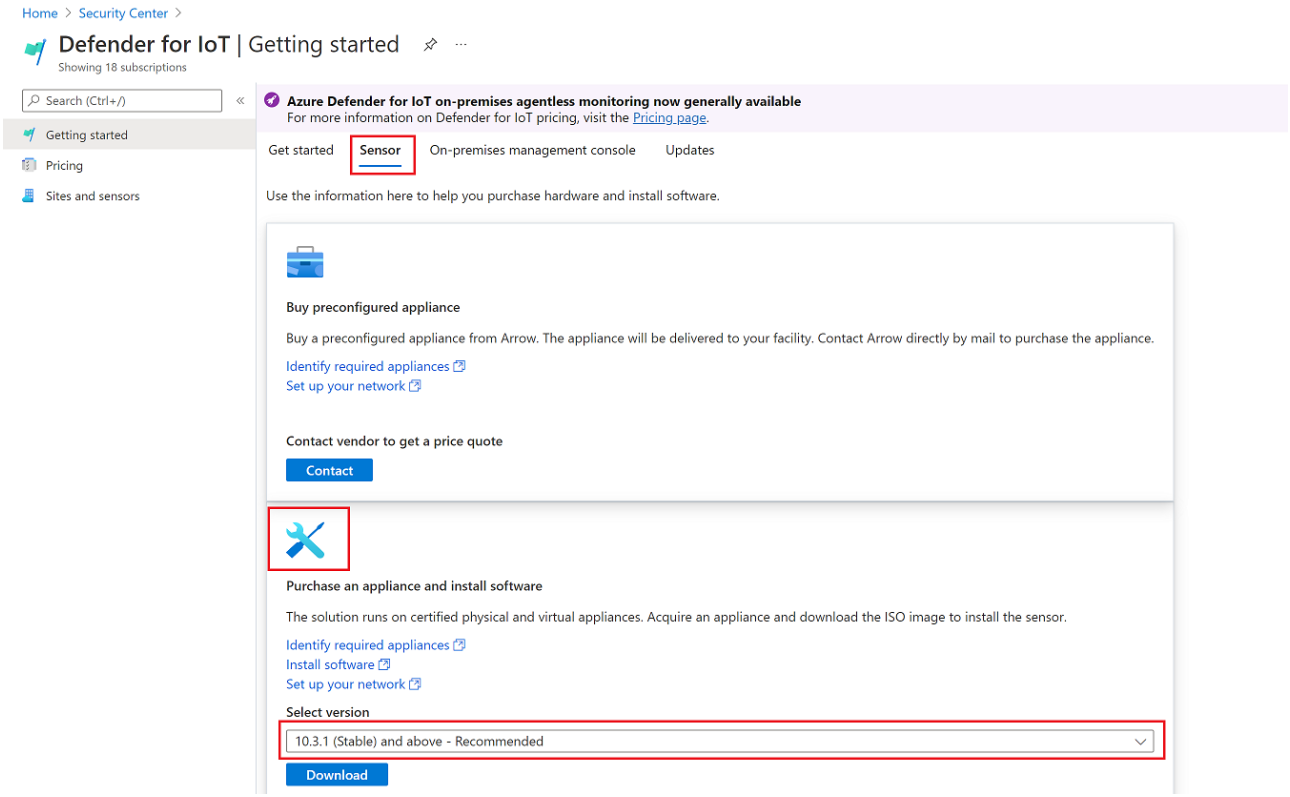


Task 3 - Onboarding sensors

For the hands-on lab we will work with two type of sensors, one offline and one online connectected to Azure. In the next steps we will onboard both, starting with the offline sensor.

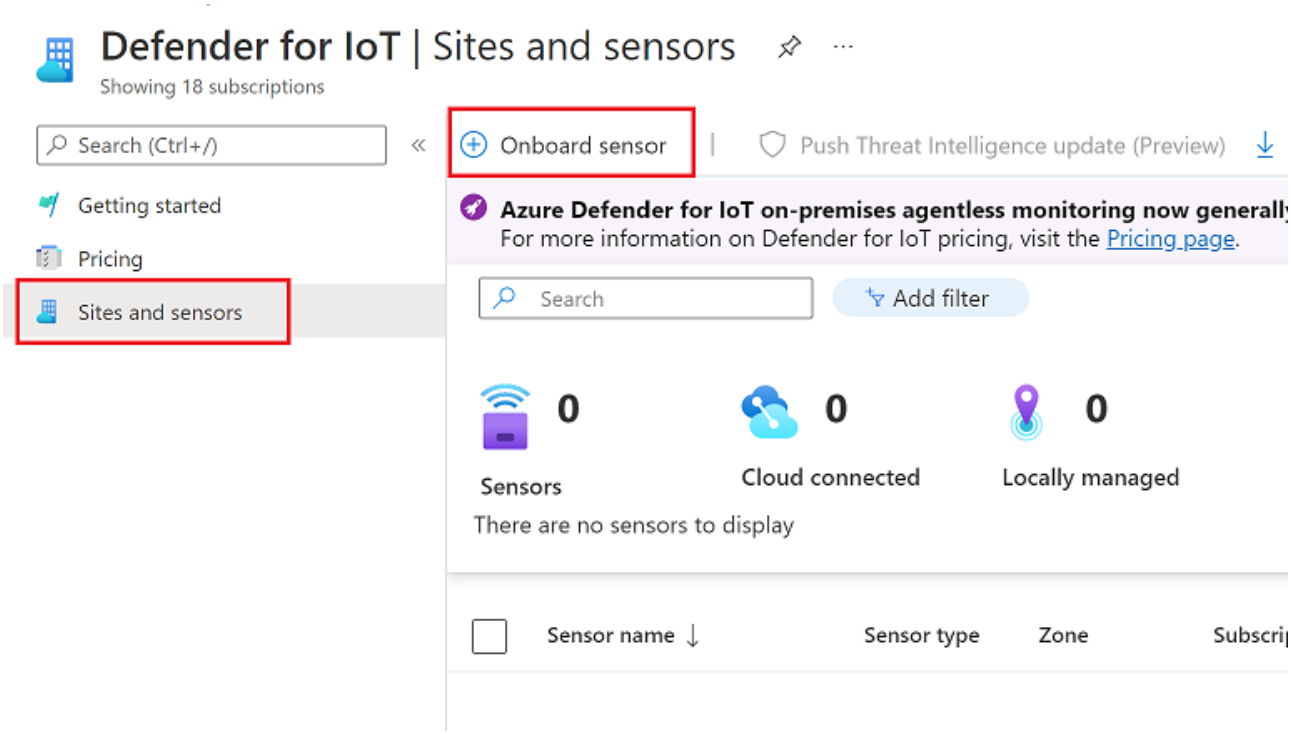
1. Go back to Azure Defender for IoT to create the sensors. You can go back through **Security Center**, **Cloud Security**, **Defender** then in the right side, under **Advanced Protection**, click on **IoT Security**.

2. **!NOTE:** You are dowunloading the iso image here, you ***alreadid did this step*** in the **Before HOL Section** the iso file is already in your VM so we don't have to wait BUT you need to learn where it is, so we are **SKIPING** this step. In the **Getting Started** section, select **Sensor**, then pick the **10.3.1 (Stable) and above - Recommended** version, and click **Download**.

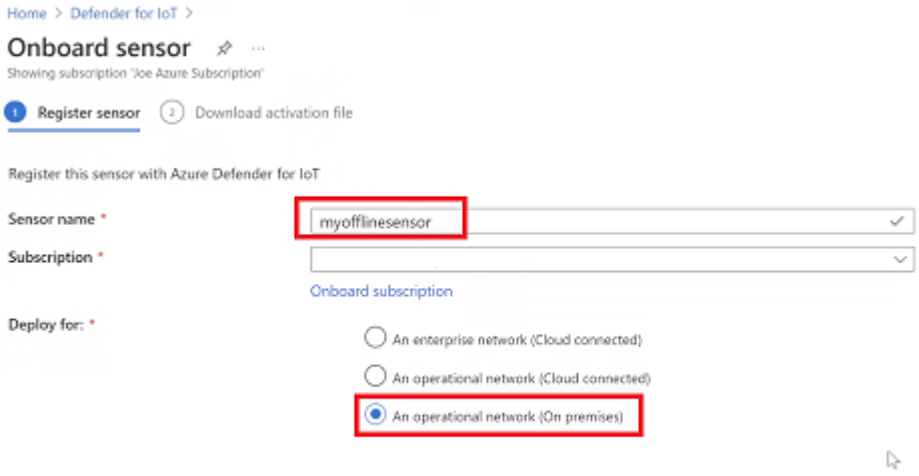


Fill the contact info window and then wait for a few minutes to complete the download.

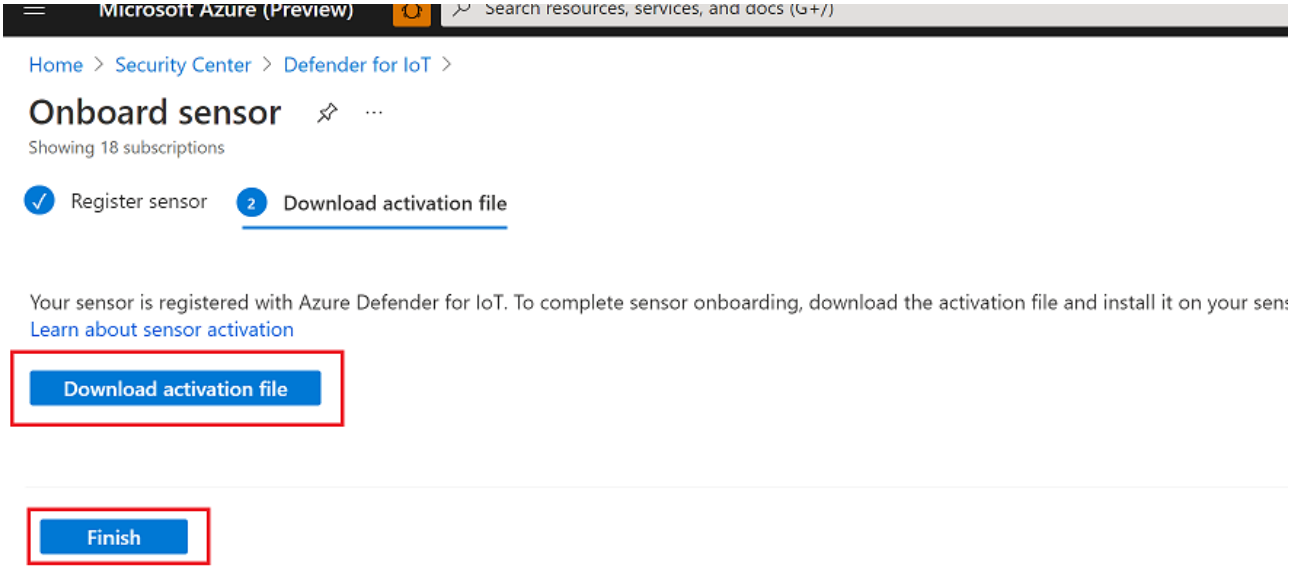
3. Next go to **Sites and Sensors** and click on **+ Onboard sensor**.



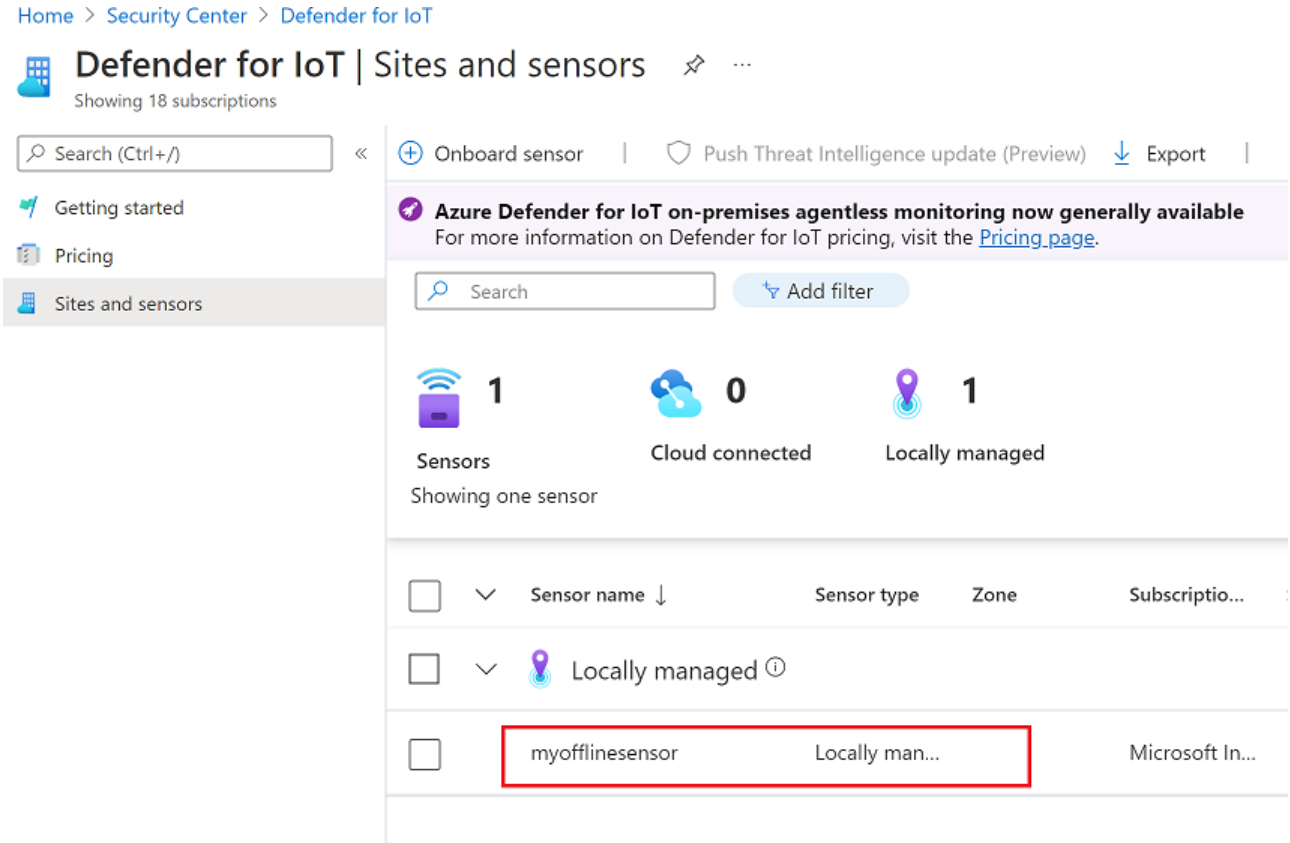
4. Assign a name to the sensor **myofflinesensor**, select your subscription and **An operational network(On premises)** or disable **Cloud Connected**. Click **Register**.



5. In the next step, click on **Download activation file** this will generate a zip file and click **Finish**.



6. You should see your new sensor onboarded, locally managed, in your list of sensors as shown below.



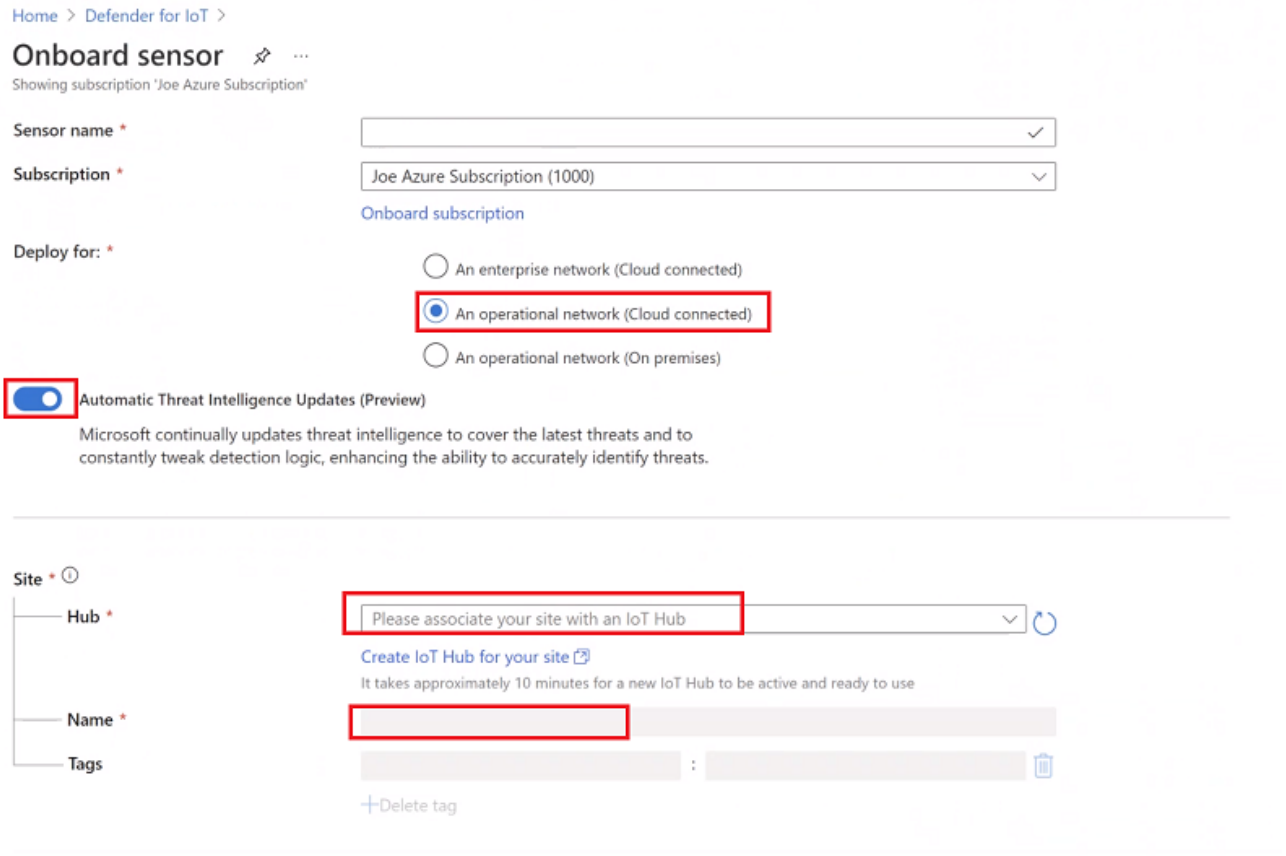
7. Now, we will create another sensor, in this case we will be the online sensor. Click on + **Onboard sensor**, in the next screen input the following information:

- **Sensor name**: myonlinesensor
- **Subscription**: Select the subscription you are using for this lab.
- **Cloud Connected**: keep it as Enabled

- **Automatic Threat Intelligence Updates (Preview)**: keep it as Enabled.
- **Deploy for**: An Operational network(Cloud Connected). this option might or not appear.

Site Section

- **Hub**: Select the IoT Hub created in previous step.
- **Display Name**: AD4IoTHub, usually this name will represent the site you will be analyze such as Plant I.
- **Zone**: Default.



8. Click **Register**.

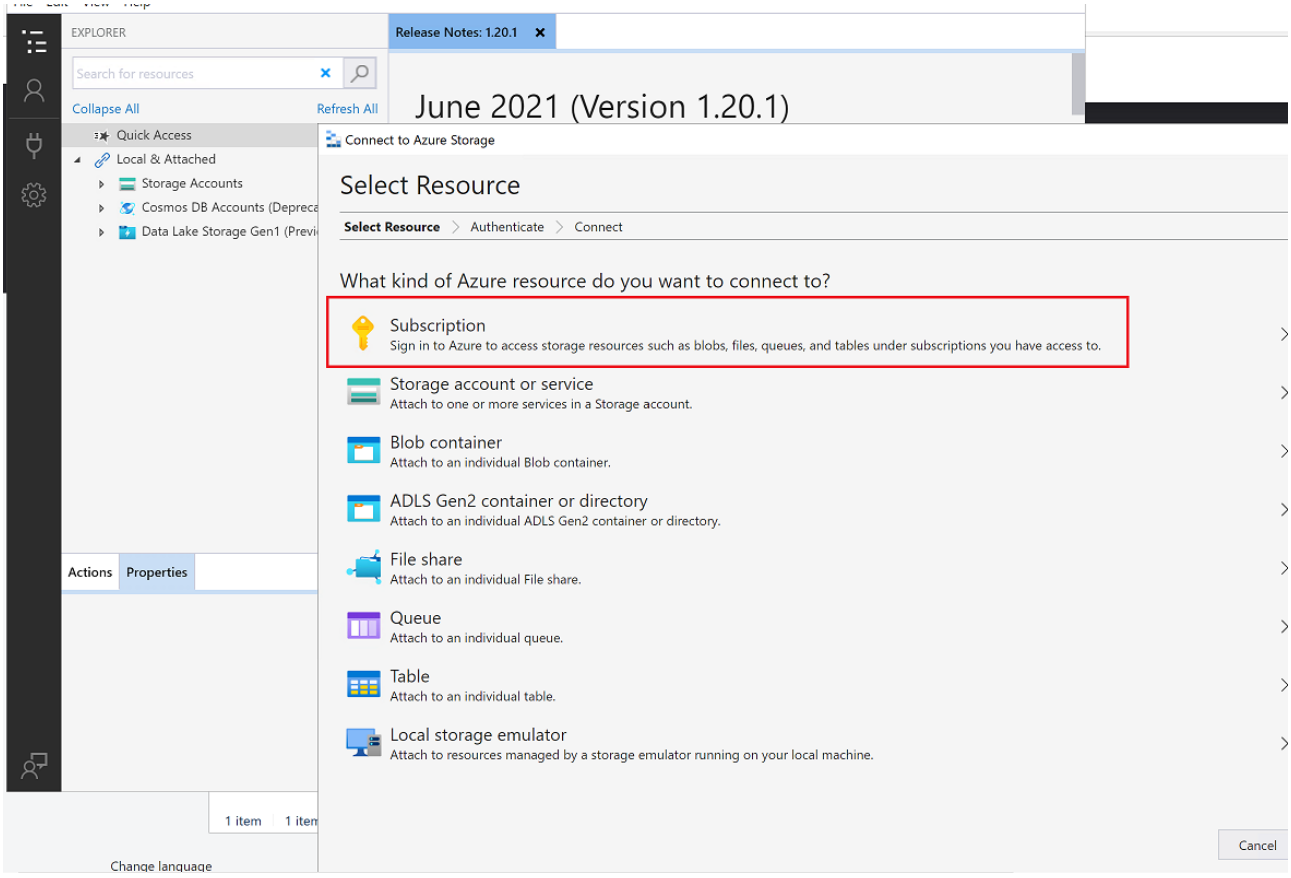
9. In the next step **Download activation file** and click **Finish**.

10. Check again your **Sites and sensors** section you should see both sensors onboarded.

11. At this point you have 3 files downloaded locally (two zips licenses sensors and the iso file) we will upload them to the Storage account created in the section **Azure Defender for IoT BHOL**, this way we will be able to make them available to download in the Virtual Machine. Another option could be to download the files directly in the Virtual Machine, if you are login in the Azure Portal inside the VM. However, sometimes you will have policies on place not allowing this, so the storage account route will make this feasible.

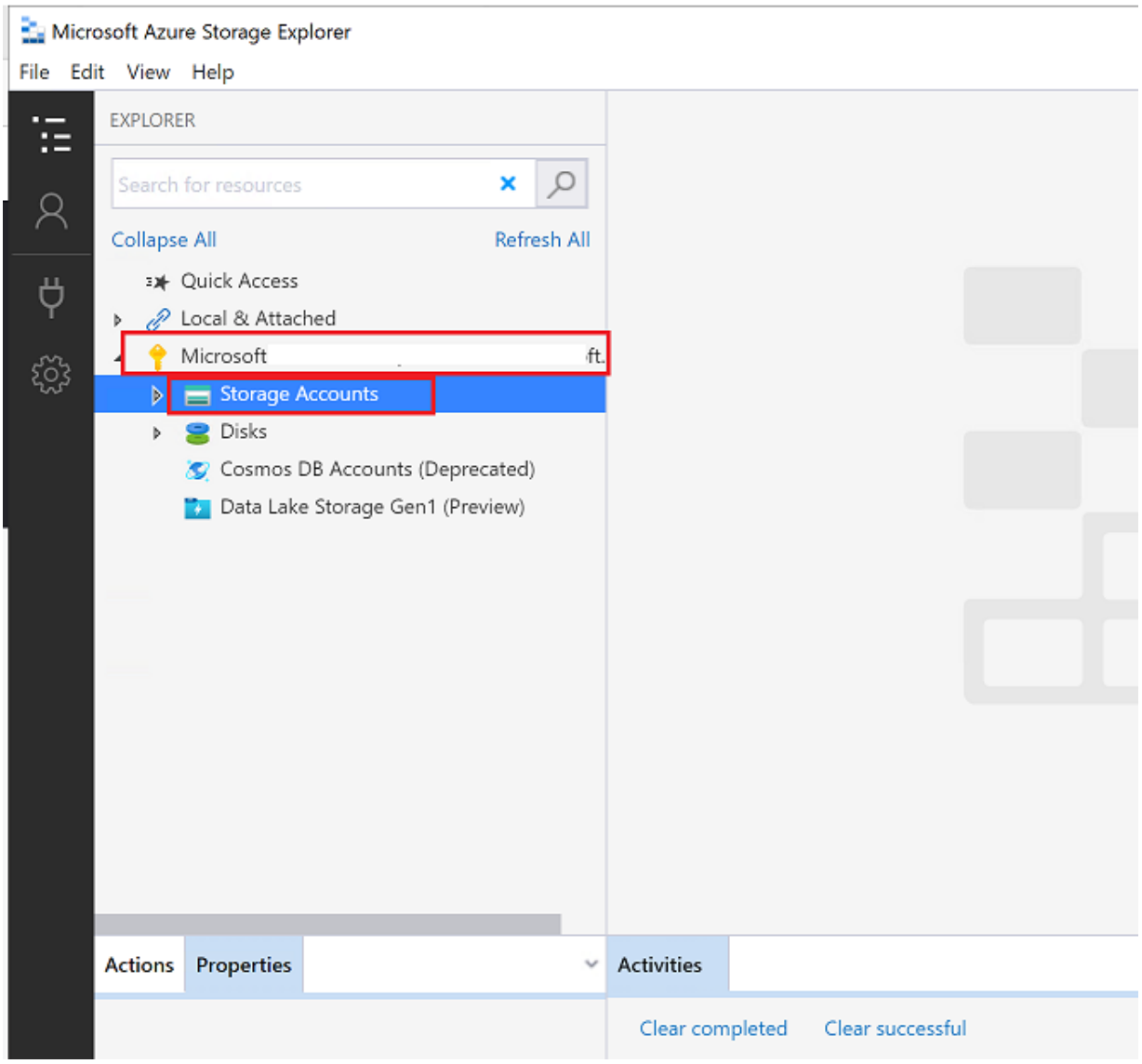
12. To Upload the Files, go to the Storage Account you created before in the Azure Portal. On the left panel select **Containers**, on the right side, click on **acitvationfiles**, next on the top menu click **Upload** browse to the location where you download the files, select all of them and click **Upload**.

13. Go back to the windows Virtual Machine, open **Storage Explorer**. You will be ask to login to your Azure account where you just upload the files. Then select **Subscription**.

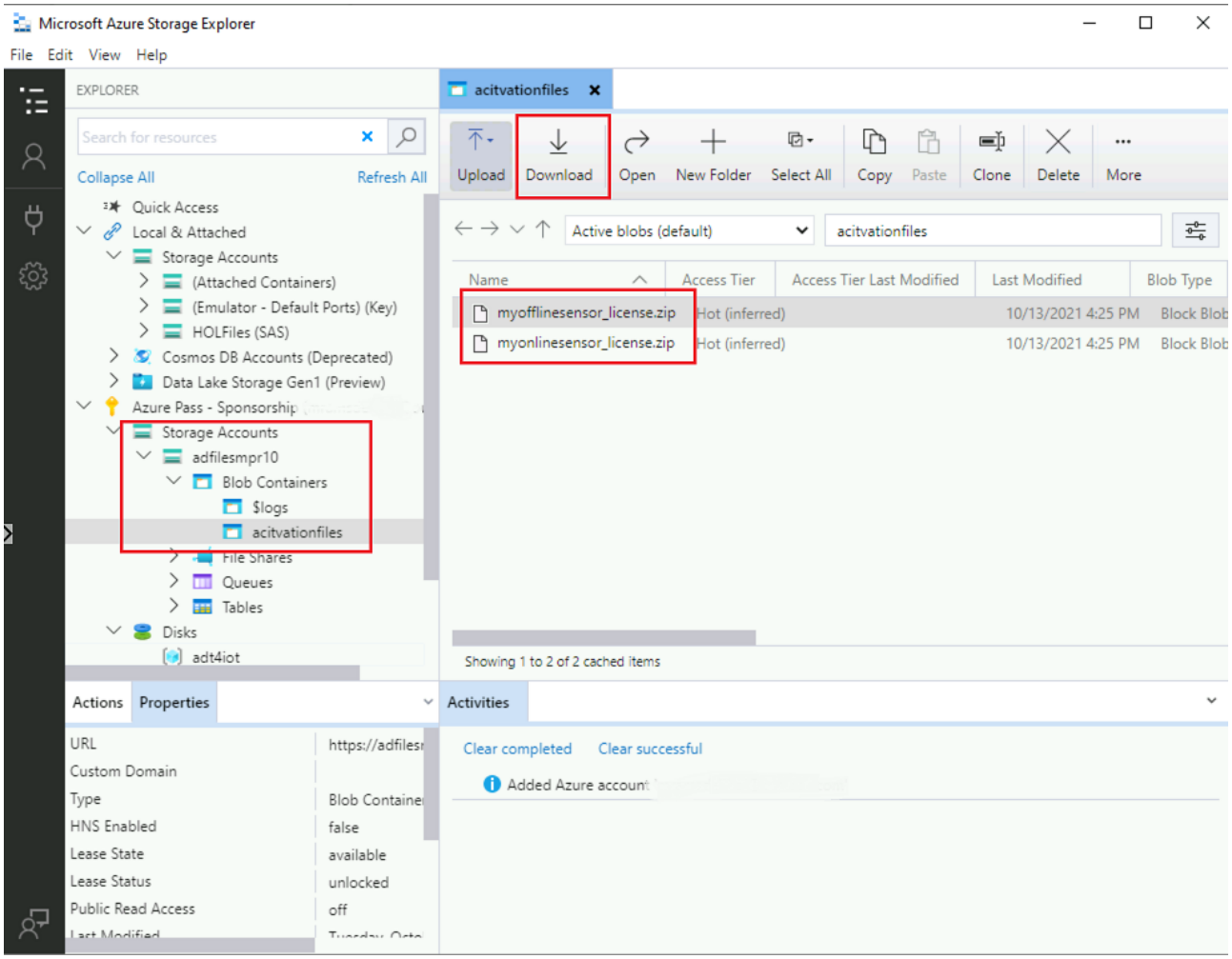


14. Next, click on **Azure**, **Next**. Now **Sign in** to Azure. Once you are signed in, close the browser, in the Storage explorer you you should see your subscription. You might need to select multiple directories, in the Account section to see your subscription. thne **Open Explorer** to see your storage accounts.

15. On the left panel, select **Storage Accounts** under your Subscription.



16. Once you selected the container on the right side you should see the files, just select the files and click **Download**

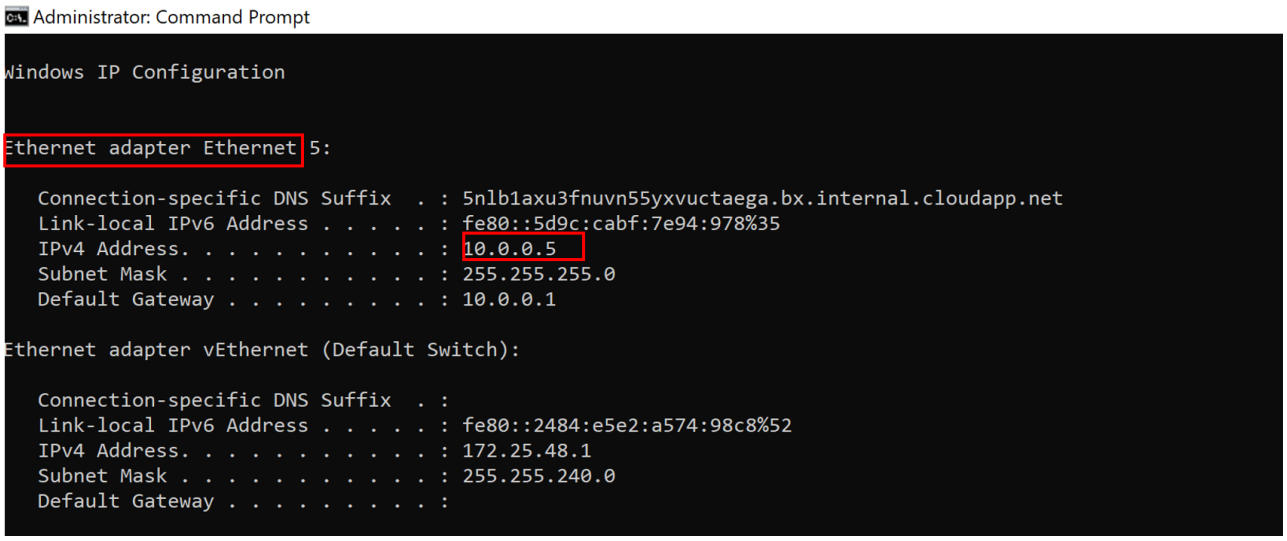


Exercise #2: Setting up your offline sensor

During this exercise we will set up the Virtual Machine created before with Azure Defender acting as a sensor offline.

Task 1: Set up your Virtual Machine

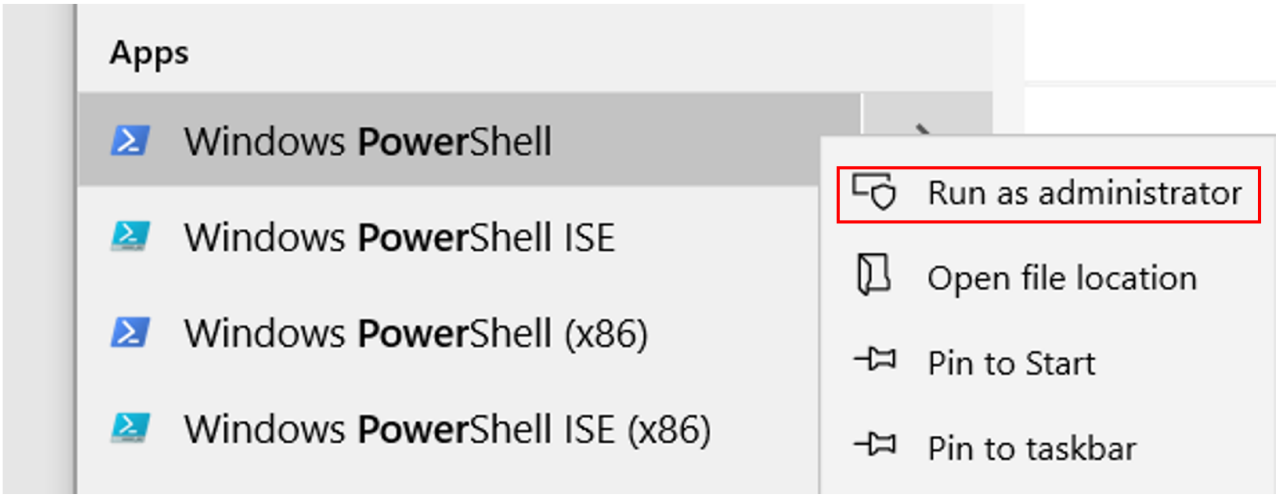
1. On the Windows 10 Virtual machine created previously, login with Bastion or RDP. Open a command prompt and run the command "ipconfig". **NOTE: Ignore the (Default Switch)**



2. Take note of the IP address used on your Windows 10 Host's Ethernet Adapter. **NOTE: Ignore the (Default Switch)**

NOTE: In this example, the Win10 host Ethernet Adapter is assigned an IP of 10.0.0.5, therefore we will use 192.168.0.0/24 as the network scope of the "NATSwitch". If your primary adapter is already using 192.168.x.x, then use 172.27.0.0/24 for your "NATSwitch".

3. Open a PowerShell prompt as an Administrator by searching for PowerShell and right-clicking to "Run as administrator".



4. Run the next two commands in the PowerShell window.

```
New-VMSwitch -SwitchName "NATSwitch" -SwitchType Internal
```

```
New-VMSwitch -SwitchName "MySwitch" -SwitchType Internal
```

5. Run the following command to store the network adapter information to a local variable.

```
$s1 = Get-NetAdapter -name "vEthernet (NATSwitch)"
```

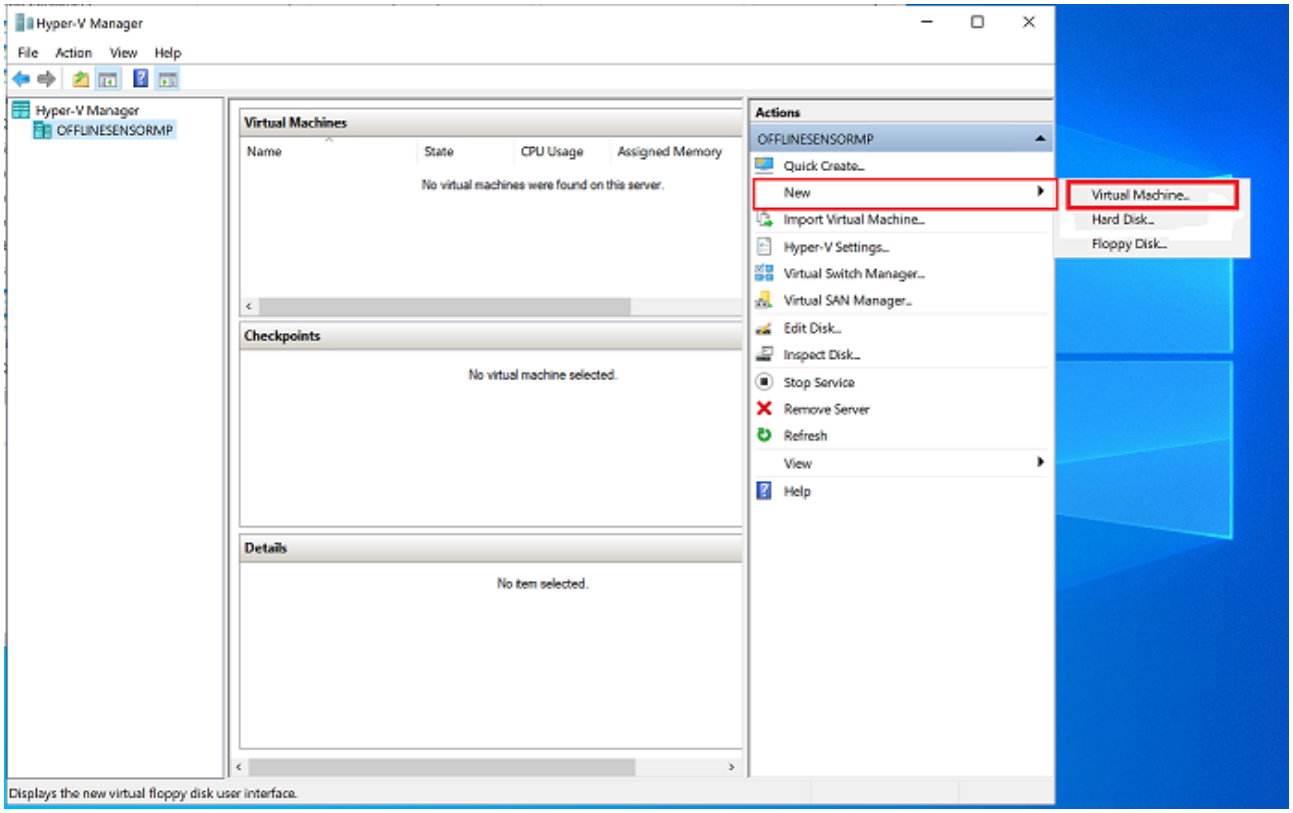
6. Assign an IP address to the NATSwitch (either 192.168.0.1 or 172.27.0.1) depending on your network address based on step 1.

```
New-NetIPAddress -IPAddress 192.168.0.1 -PrefixLength 24 -InterfaceIndex $s1.ifIndex
```

7. Create the new NAT network. Again, your IP address space will either be 192.168.0.0/24 or 172.27.0.0/24 depending on step 1.

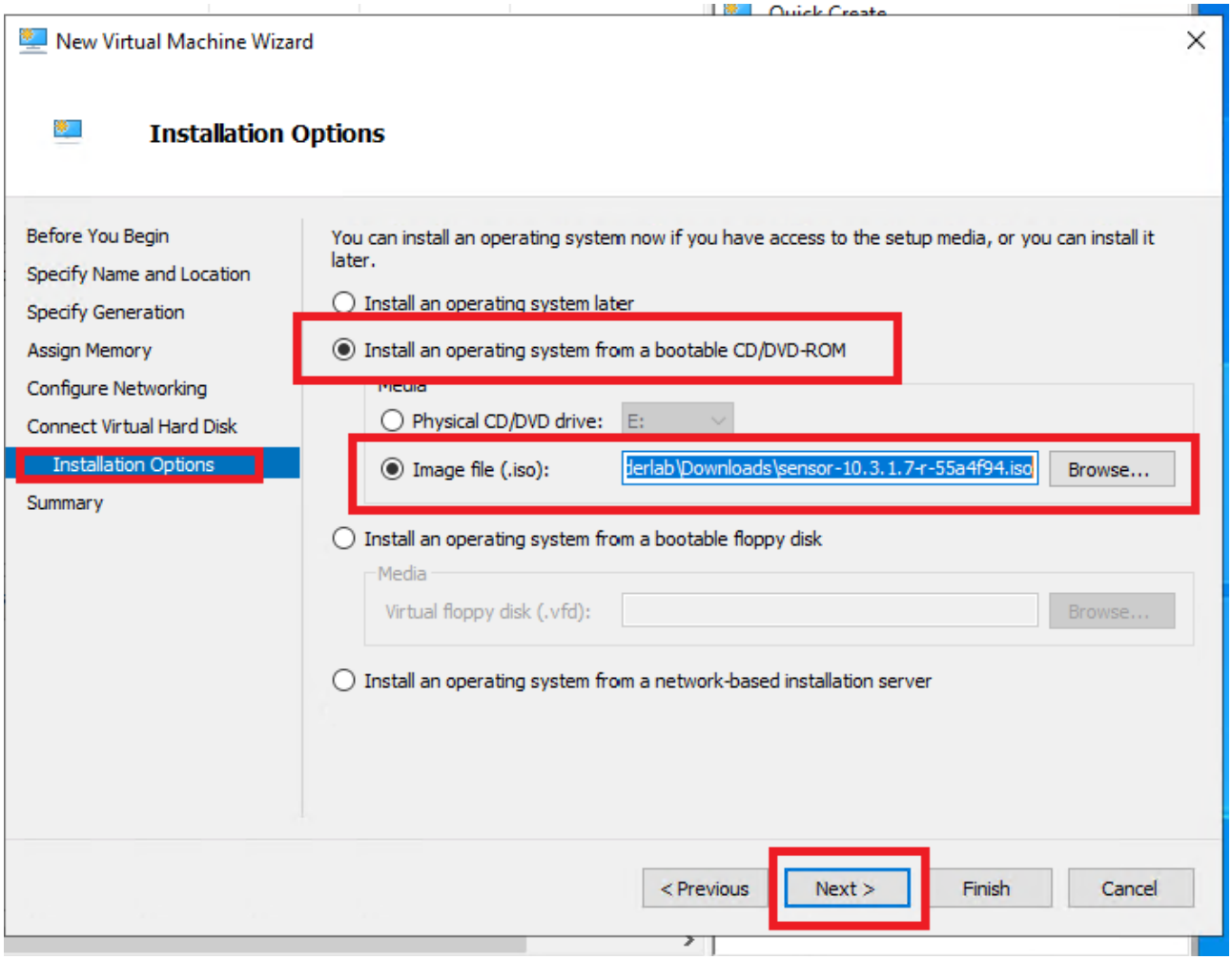
```
New-NetNat -Name MyNATnetwork -InternalIPInterfaceAddressPrefix 192.168.0.0/24
```

8. Once inside the VM in the windows search box, type **Hyper-V** and enter. This should open a new window with Hyper-V console. Select **New** on the left side will open multiple options, select **Virtual Machine**



- First tab, assign a name **ad4iotsensoroffline**, then click **Next**

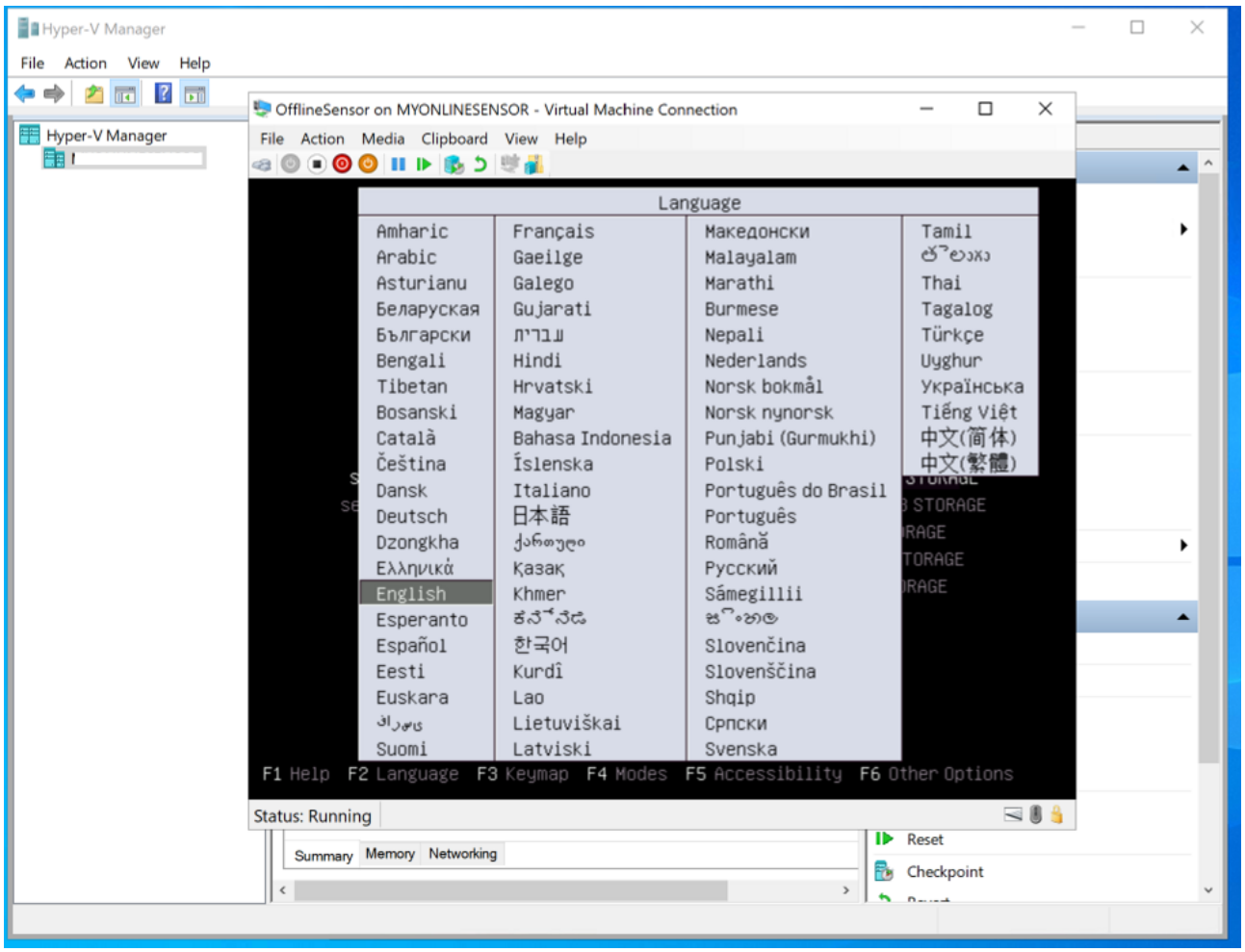
- **Specify Generation**, select **Generation 1**, click **Next** again.
- Change the memory to **8196MB**, **Next**.
- **Configure Network** tab, select in **Connection**, **NATSwitch**, **Next**.
- **Connect Virtual Hard Disk** tab, **Create a virtual hard disk** click **Next**.
- **Installation Options**, select **Install an operating system from a bootable CD/DVD-ROM** then select **Image file (.iso)** and browse the Azure defender .iso file downloaded in previous steps. Last **Finish**



7. Right click on your Virtual machine just created, select **Settings** in the **Add Hardware** section select **Network Adapter**, click on **Add**, select the virtual switch created previously **My Switch**, click **Apply**. Increase the Processor from **1** to **4** Virtual Processors, click **Apply** and click **Ok**.
8. Back to the Hyper-V, right click on the VM and select **Start**, then in the console click **Connect**.

9. When you connect to the Ubuntu VM you should see the following screen to start the configuration process.

Note!: If you don't see that screen below, your installation timed out or you pressed enter selecting a different configuration by mistake, delete the virtual machine and start this task over.

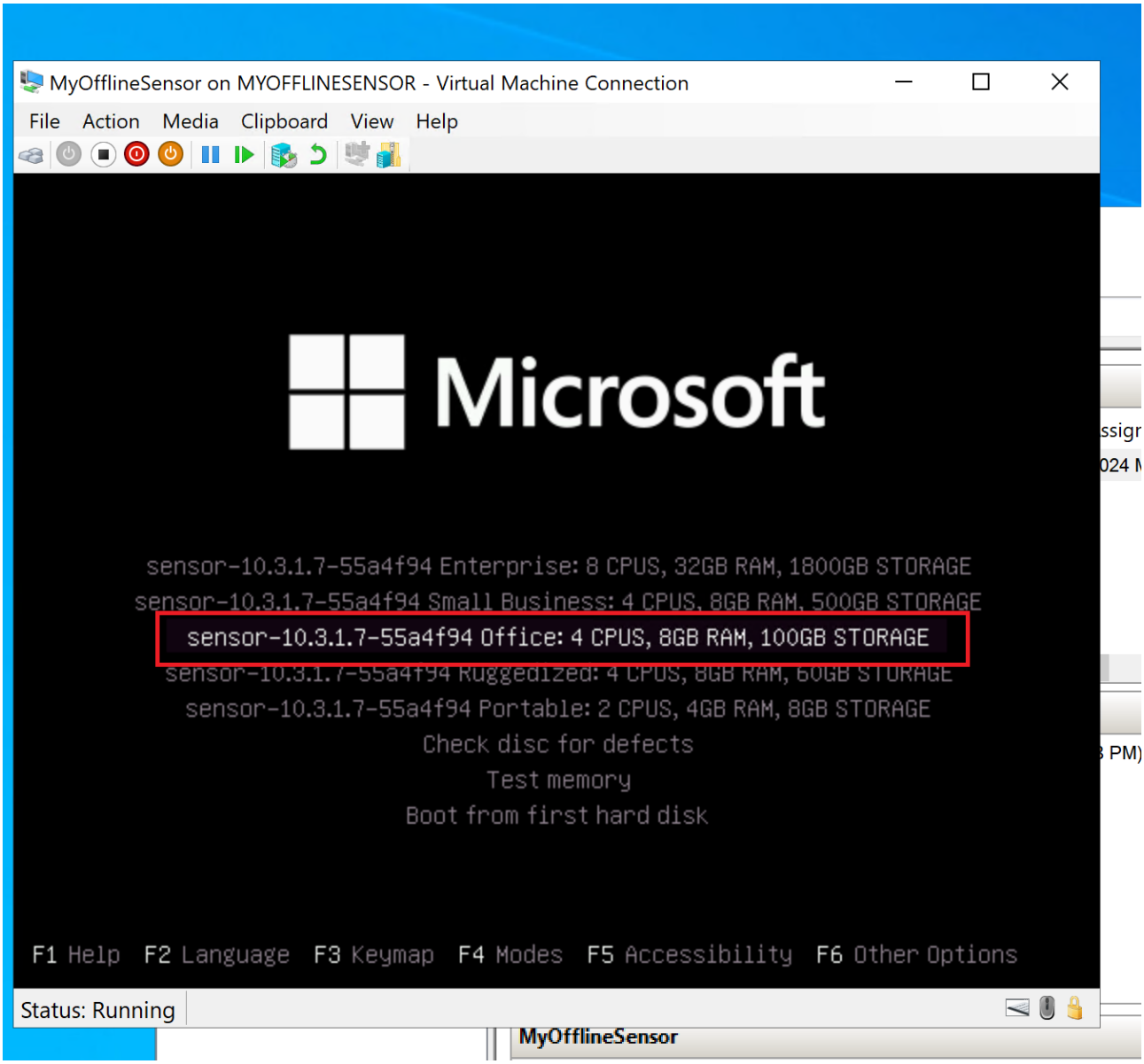


Task 2: Configure Azure Defender

During this task we will configure Azure Defender based on the IPs highlighted before, this first configuration will be based on an offline sensor.

1. Press **Enter** for English.

2. Select the third option (Office 4CPUs)and press **Enter**.



3. You will be ask to fulfill some parameters, it is ***VERY IMPORTANT*** you pay attention to the previous task because you will use the network information you captured before, this is unique to each Virtual Machine. So the following is an **EXAMPLE**.

- **configure hardware profile**: **office**, then press enter.
- **Configure network interface**, type **eth0**
- **Configure management network interface**: in this example we're using **192.168.0.50**, you will use one of the **Ipv4 Addresses** depending on your network scope from the previous task, either **192.168.0.50 or 172.27.0.50**. Click Enter to continue. ***Take a note of this IP you will need it later on***.
- **Subnets mask**: **255.255.255.0** this will be the SAME for everyone.
- **Configure DNS**: 8.8.8.8

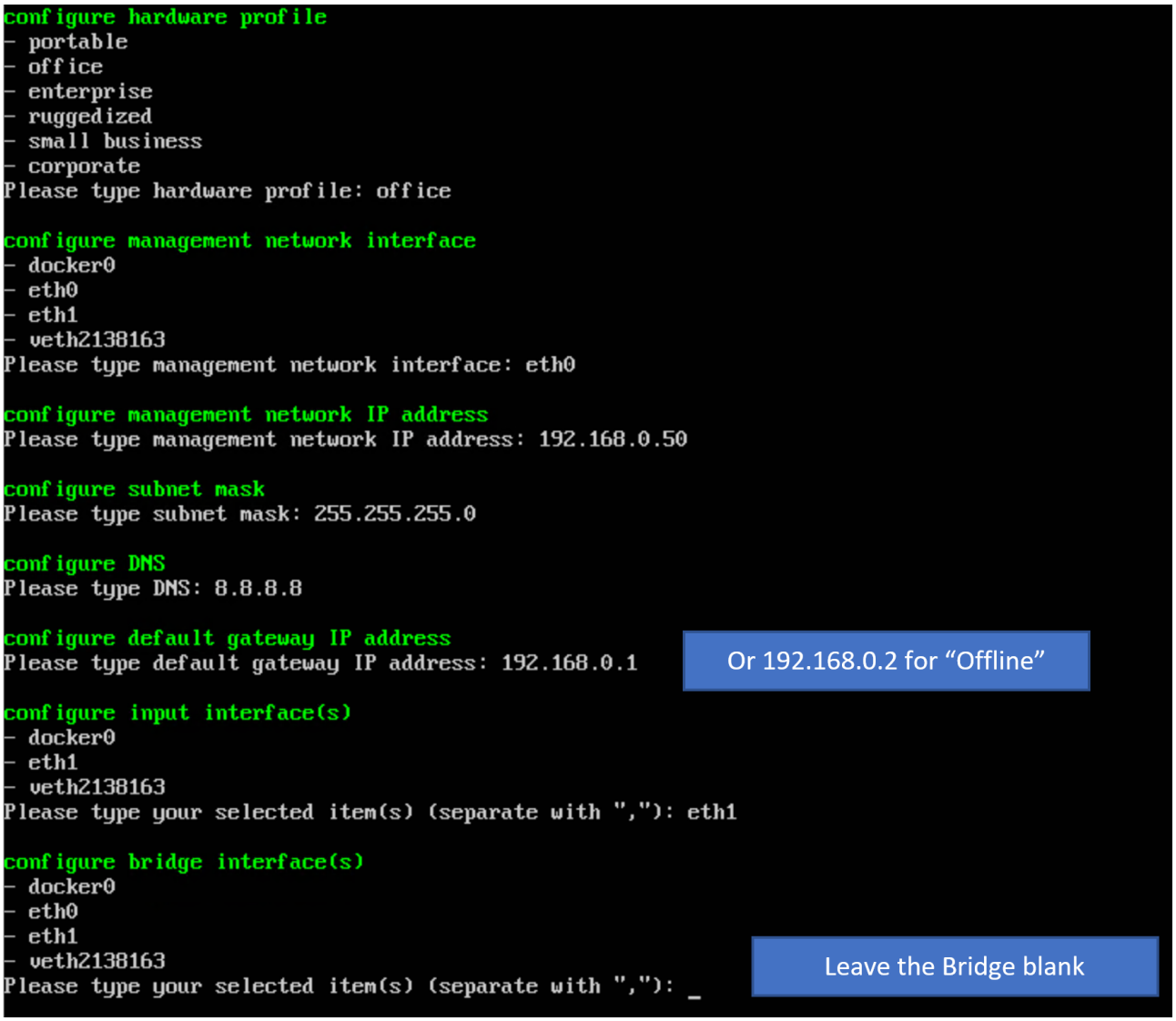
- **Configure default gateway IP Address**: We are intentionaly mis-configuring this value to force the sensor in **offline** mode. Use either 192.168.0.**2** or 172.27.0.**2**.
- **Configure input interface(s)**: **eth1**
- **Configure bridge interface**: Just press Enter
- Then type **Y** to apply the changes and click **Enter**.

Now the installation will run for 10-15 minutes.

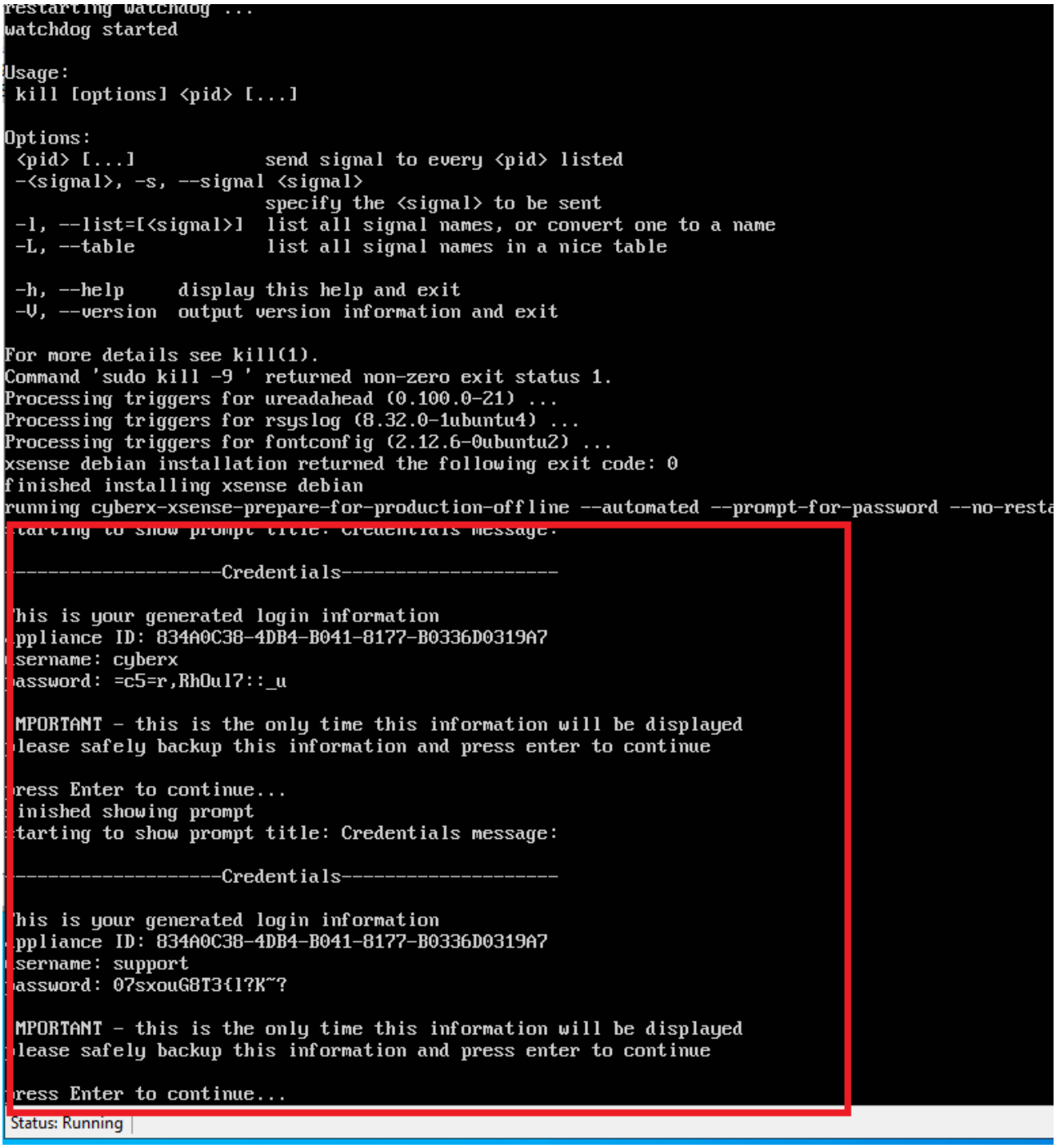
Troubleshooting Note: Once the installation is complete, you will be able to access Azure Defender Console, check if you can open a cmd window, ping the IP Address you enter in the step 'Configure management network interface' If the request times out, you will need to reconfigure this step again, for that review the IPs one more time and use the command below to start over:

```
sudo cyberx-xsense-network-reconfigure
```

Below, a ***sample*** screen, your parameters will be different.



4. ***IMPORTANT STEP!!!*** Once the installation is complete, you will have the login information availabe in the screen **TAKE THE PRTSCRN!!** before continuing, press **Enter**. Now you will have the support account, again **TAKE THE PRTSCRN!!** press **Enter** to continue. If you fail to capture the credentials, you will need to start over.

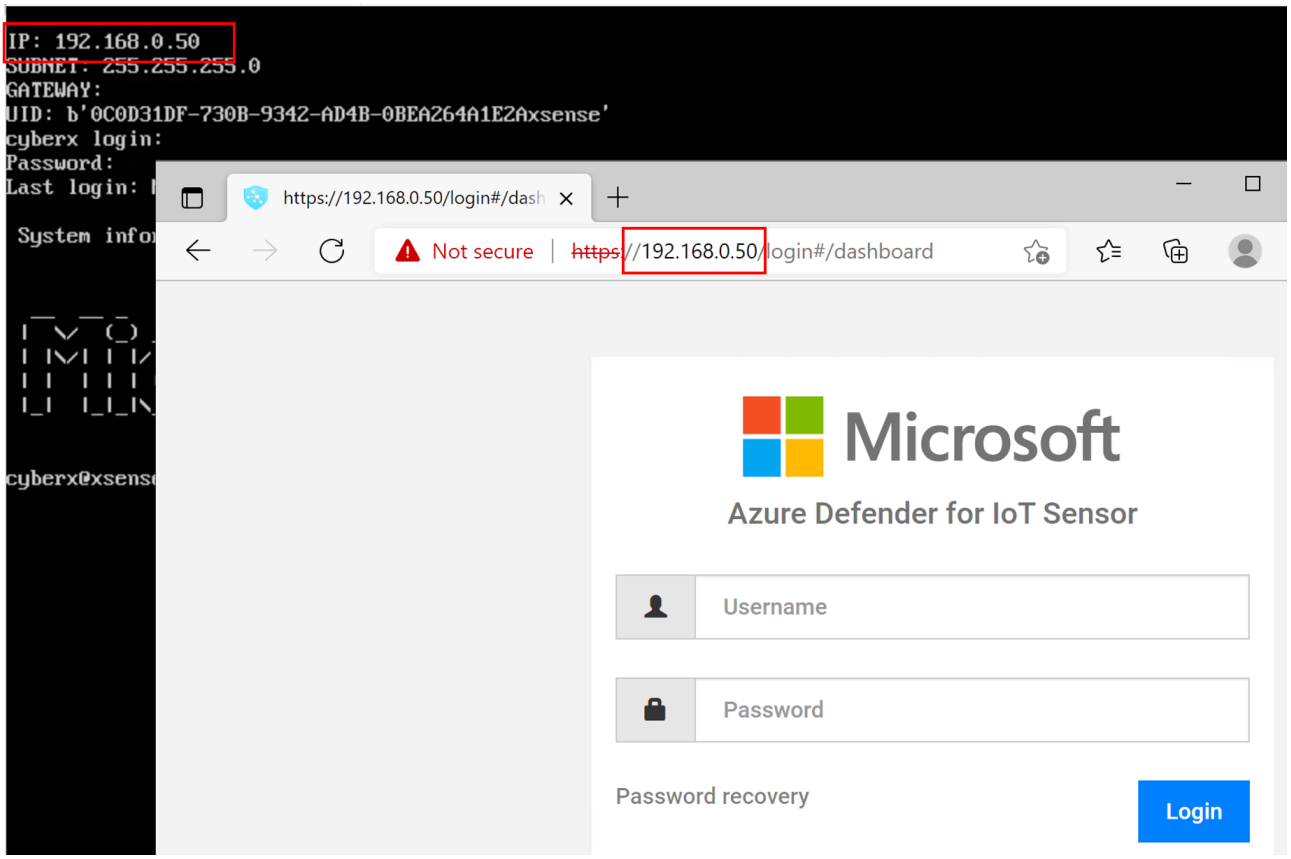


5. Once the installation finished you will ask to login, enter the credentials from previous step. In this screen you can also validate the IP, you will use that IP in your browser.

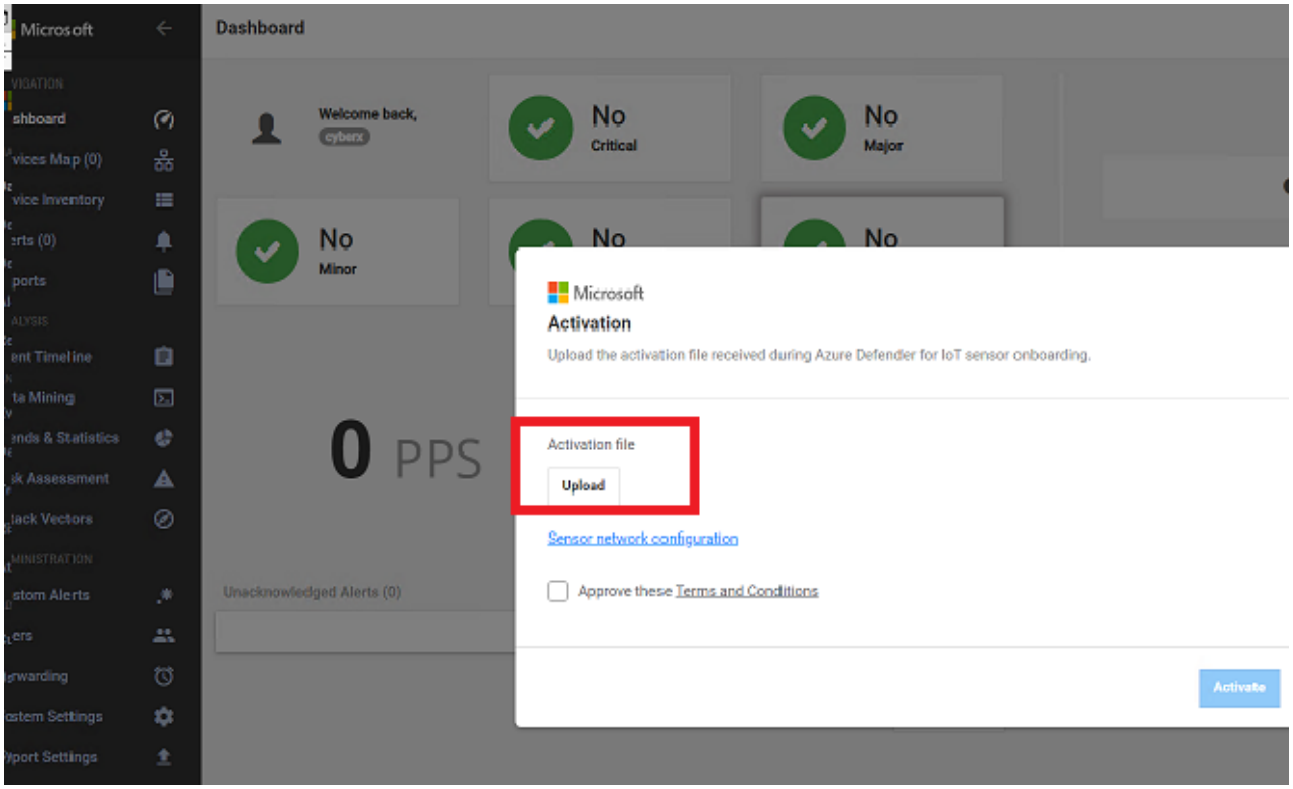
Note: At this stage your IPs should look similar to the example below, if you can't reach the portal validate the IPs. If you restarted your VM there is a chance your IPs changed so you will need to go back and reconfigure them, if that is the case use the command in step 3.

In the next steps you will be prompt to enter the password capture above, some characteres look alike but they are not, this image will help you to identify some of them.

6. Login with the credentials provided in step **4**.

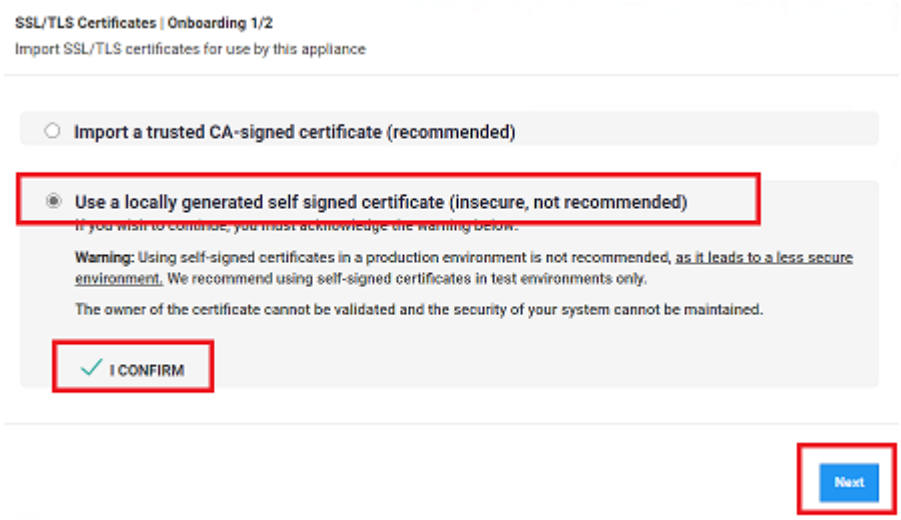


7. Next, you will be ask to activate the product, click **Upload**, then **Browse Files**, in your downloads folder select the file you downloaded from the Storage Explorer, in this example **myofflinesensor.zip**.



8. Click **Approve these terms and Conditions**, then **Activate**.

9. You will be prompted to select **SSL/TLS Certificates | Onboarding 1/2** for this lab will use the second option **Use a locally generated self signed certificate(..)**. Then click **I CONFIRM**, **Next**.



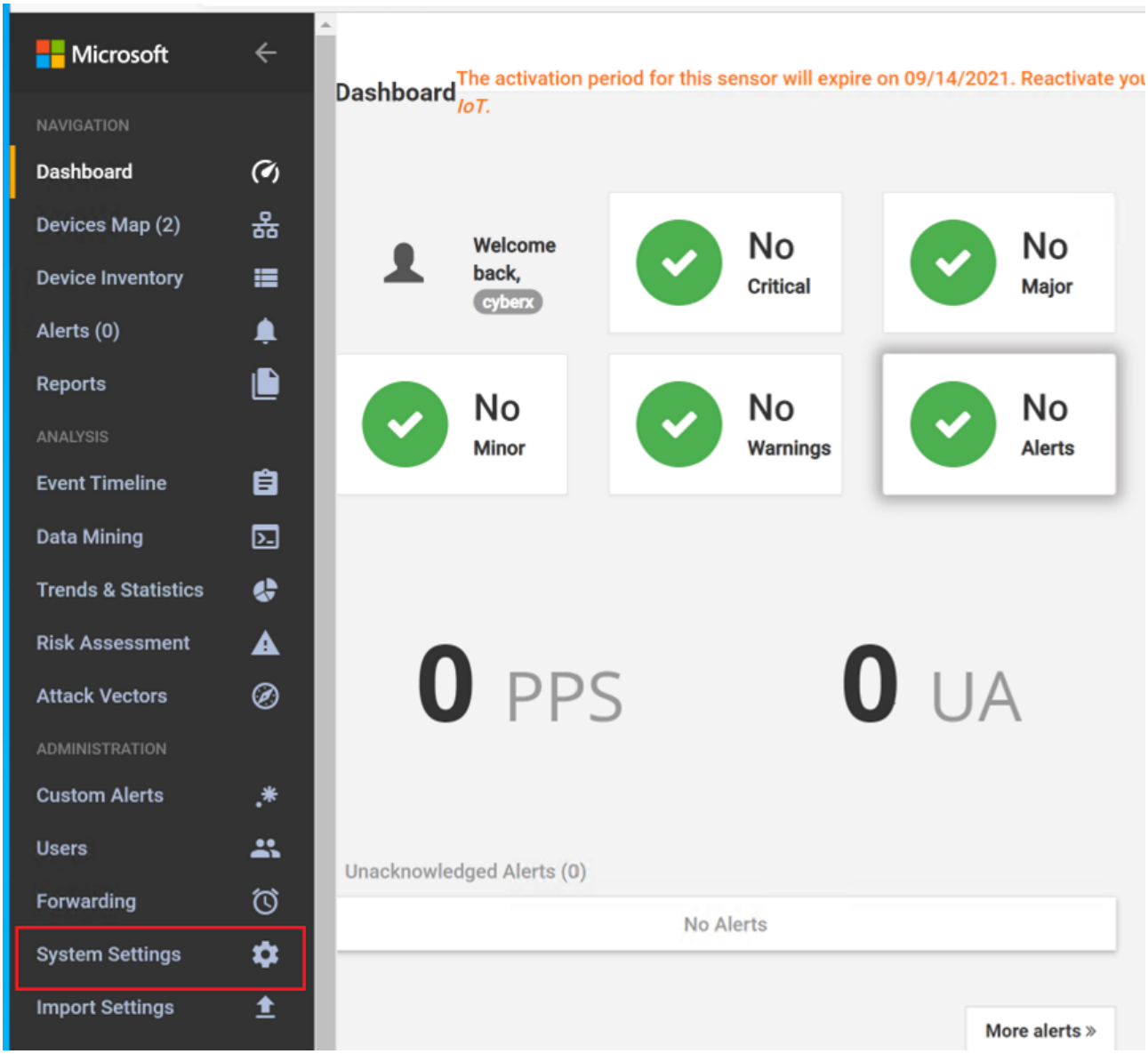
10. For this lab in the next step we will **Disable** the system wide validation. **Finish**.

11. Let's analyze together what information we already have available before moving forward.

Exercise 3: Enabling system settings

Task 1: System Properties

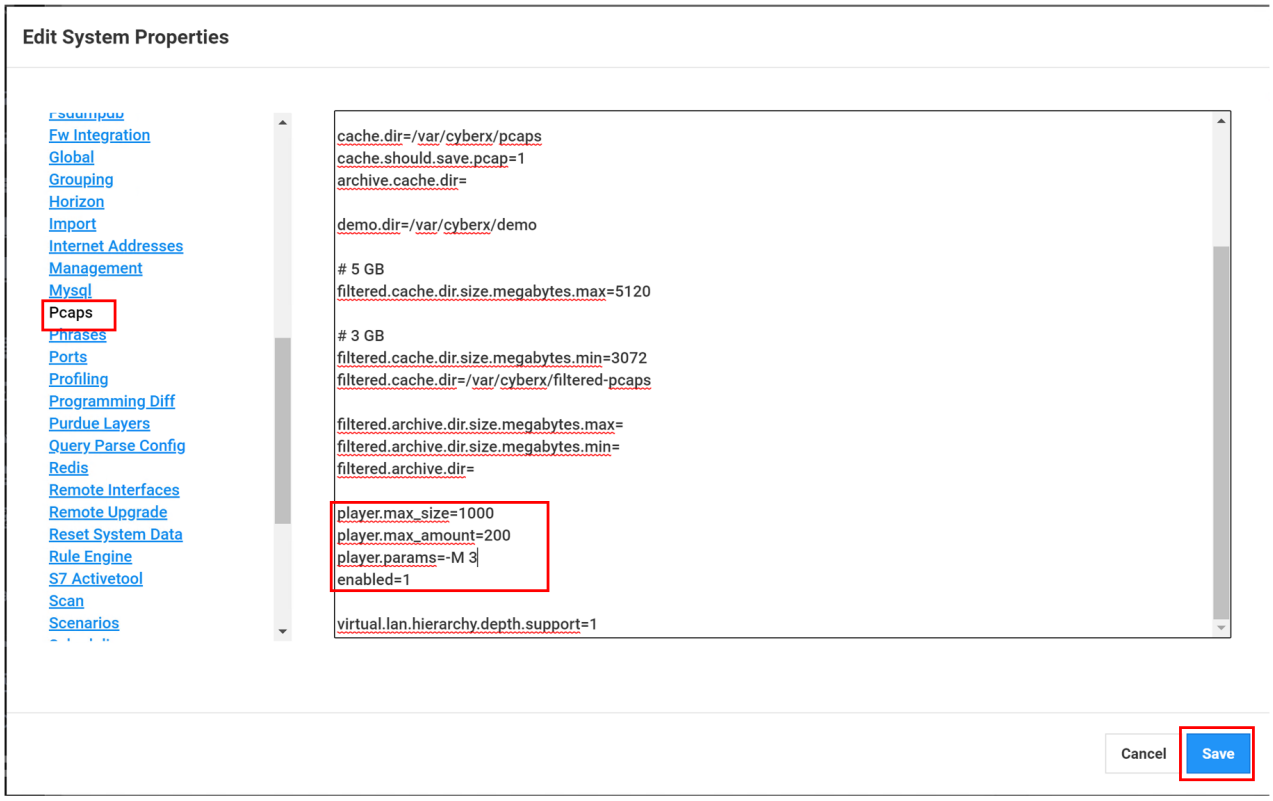
1. In your offline sensor you will find **System Settings** on the left side of the Azure Defender portal, click there as shown below.



2. Next, look for the icon **System Properties** on the right side. Click in the icon, you will see a pop up warning, select **Ok**.

3. In the new window on the left side, scroll down until you see **Pcaps**, click there. Now on the right side scroll all the way down and we will modify three parameters as shown below:

    - **player_max_amount=200**
    - **enabled=1**
    - **player.params=-M 3**



4. Click **Save** and then **Ok**.

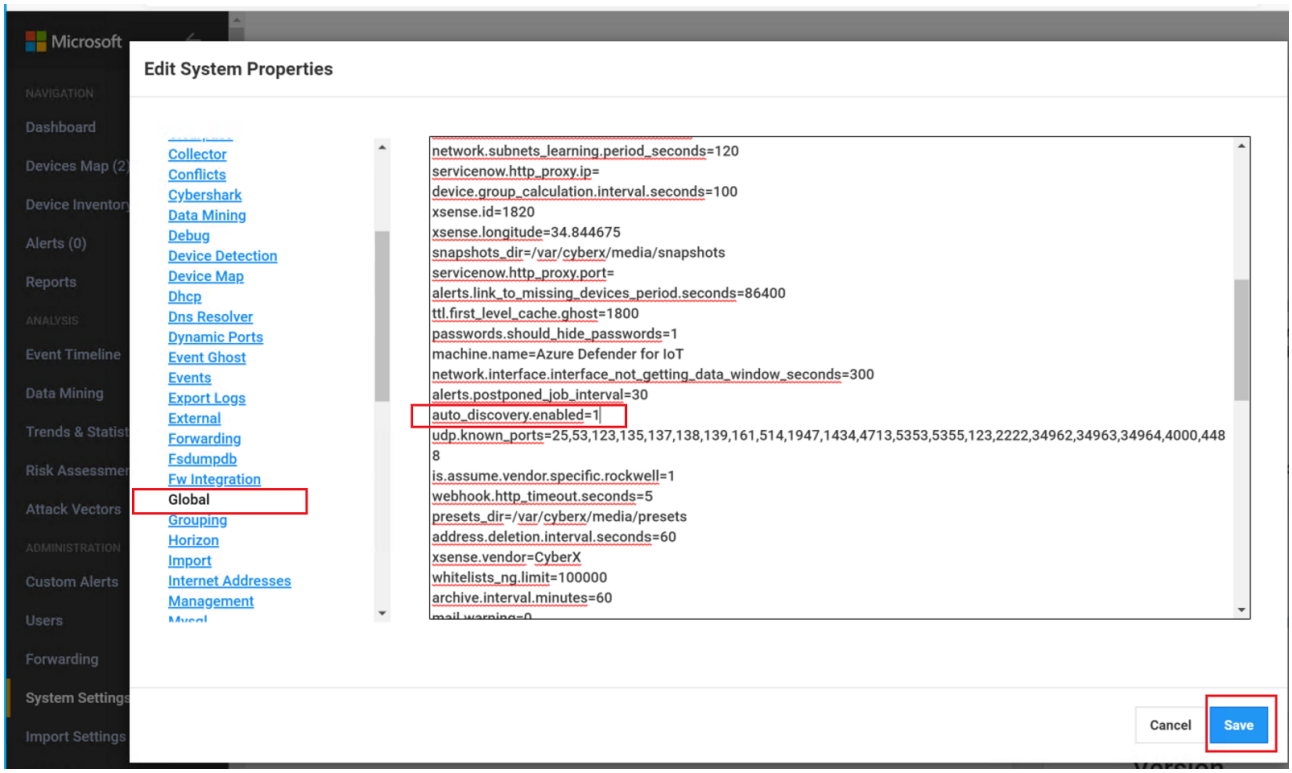
5. Continue in the System Properties window, scroll up and select **Horizon** on the left side select, scroll down and modify the following parameter:

    - **ui.enabled=true**

6. Click **Save** and then **Ok**.

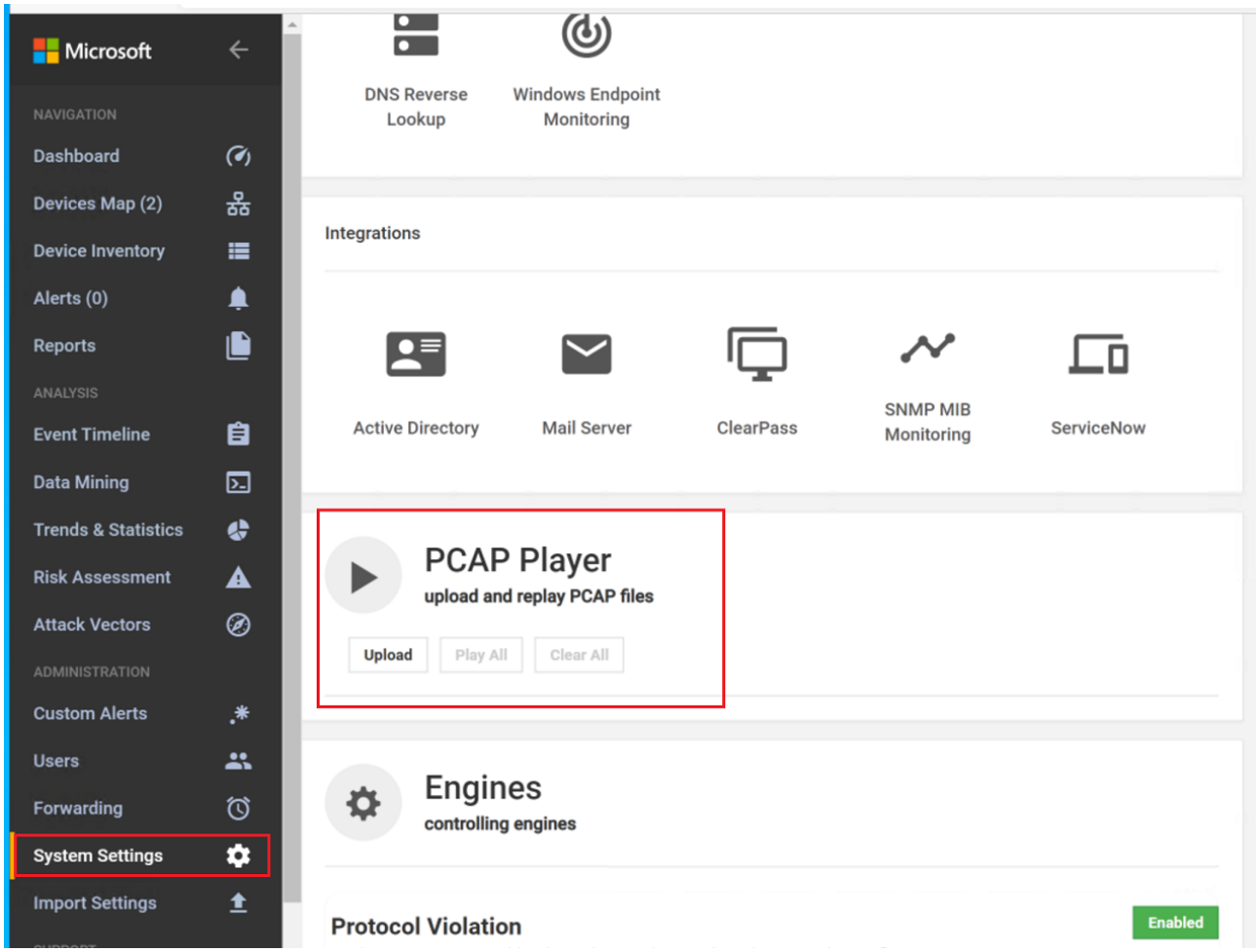
7. In System Properties, look for **Global** and modify the following parameter:

    - **auto_discovery.enabled=1**



8. Click on **Save** and then **OK**.

9. At this point you should see the Pcap Player available:

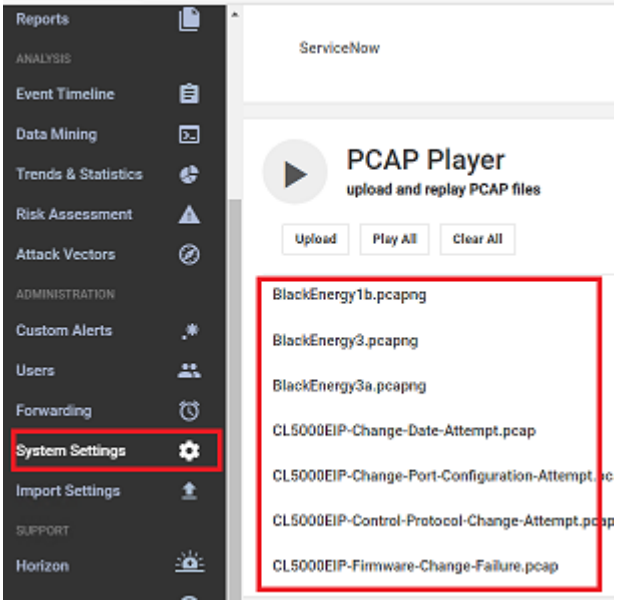


Task 2: Pcap Files

1. In previous steps you already downloaded a **holpcaps.zip** file from the Storage account. It should be in the Virtual Machine **Downloads** folder, unzip that file.

2. Go back to Azure Defender, Click on **System Settings**, then **PCAP Player** now select **Upload**, **Browse Files**, browse to the folder where you download the files in the previous step, select all the files and click **Open**. This operation will take a few minutes to upload all the files.

3. At this point you should see all the files uploaded.



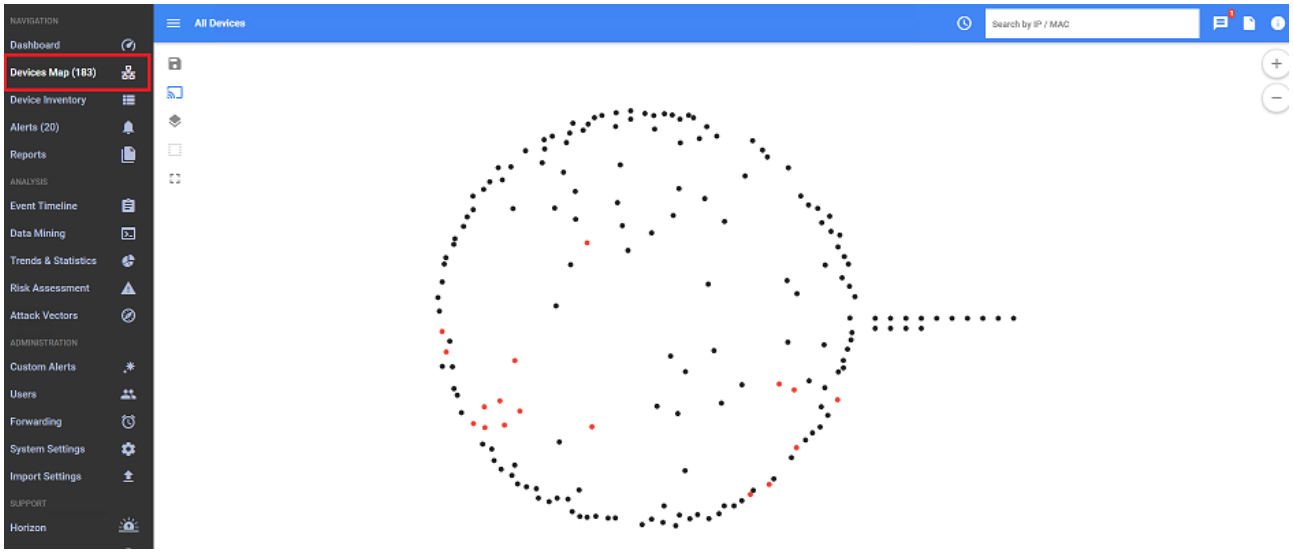
4. Click on **Play All**, in a few minutes you will receive a message saying all the files has been played.

Exercise 4: Analyzing the Data

After Azude Defender learnt about your environment it will be able to share insights pretty fast.

Task 1: Devices Map

Your first interaction with Devices map you will see a similar map like the below

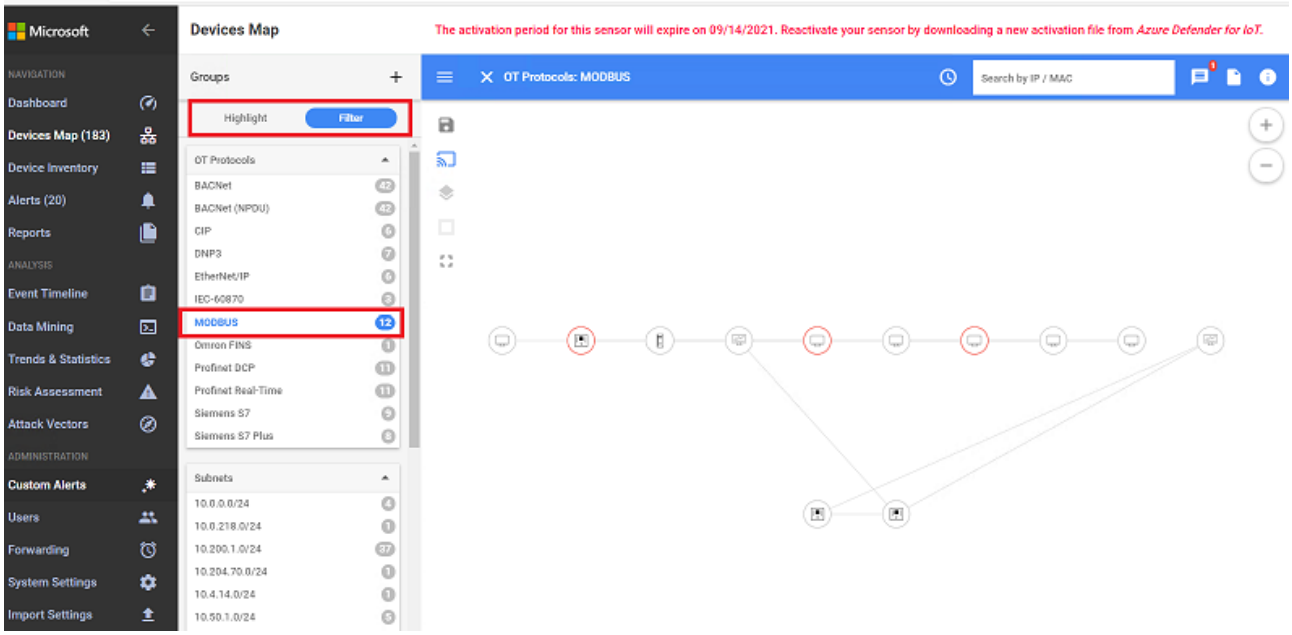


1. Use the four icon bar on the left to select **Layout by Purdue**. In this model you will see the different layers between Corporate IT and site operations.

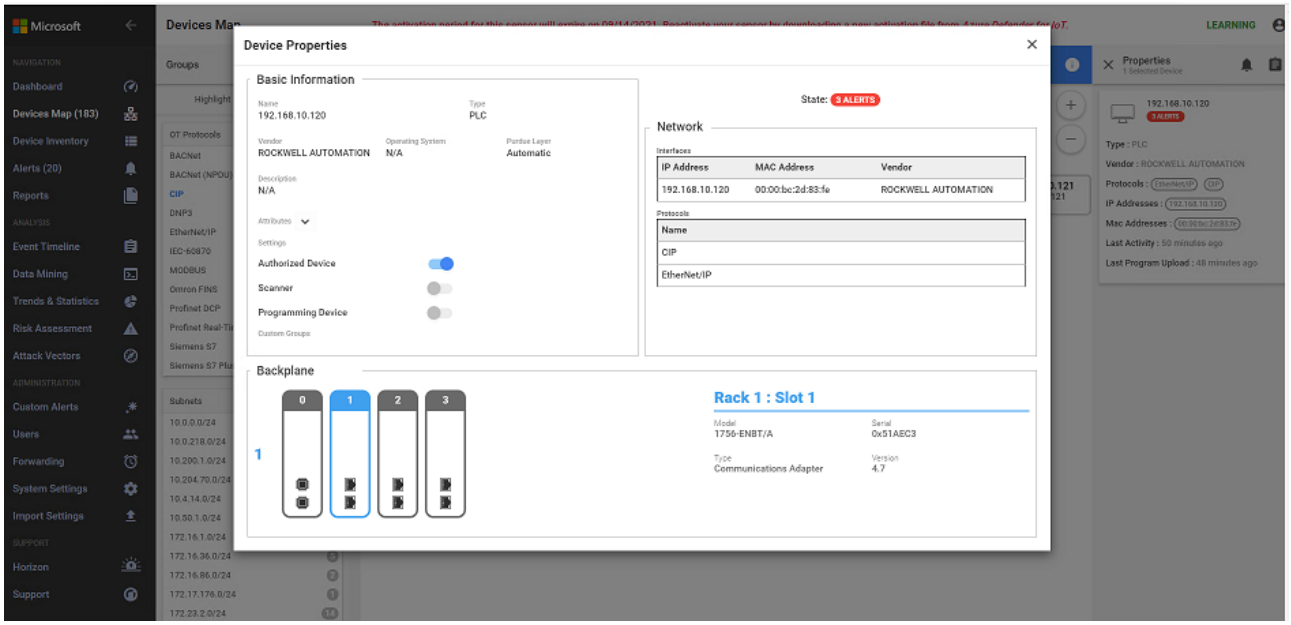
2. Check your notifications available and you can take action at this point.

3. For each device right click to analyze properties, show events, reports and simulate attack vectors.

4. In the hamburguer menu on the left, click the highlights and select one of the **OT Protocols** i.e. **MODBUS** and click on **Filter**. Now your map will show those devices only



5. Then filter your devices by **CIP** OT Protocol, at the bottom of your map you will see a PLC, where the Vendor is Rockwell Automation, has already 3 alerts activated. Right click on the device, **View Properties**. In this view you will be able to analyze the Backbone of your PLCs, take actions and analyze the Alerts.



Task 2: Alerts

1. Once you click Alerts in your PLC you will see a new window pop up showing three different types of alerts.
    - Operational(high Alert and lower alert)
    - Policy Violation

For each of these alerts you will be able to analyze the pcap file, export a report, analyze the timeline or mute the alert.

2. If we remove the device filter from the top of the screen, then click **Confirm** you will see 20 Alerts in process.

3. Apply **Custom Groups** to filter different scenarios, such as **Unclassified subnets** then **Confirm**

Task 3: Device Inventory

1. In this view, filter all your devices by **Is Authorized**, True or False are possible values.

2. Organize your devices based on filters.

3. Export the list to a csv files.

Task 4: Event Timeline

This view will allow you a Forensic analysis of your alerts.

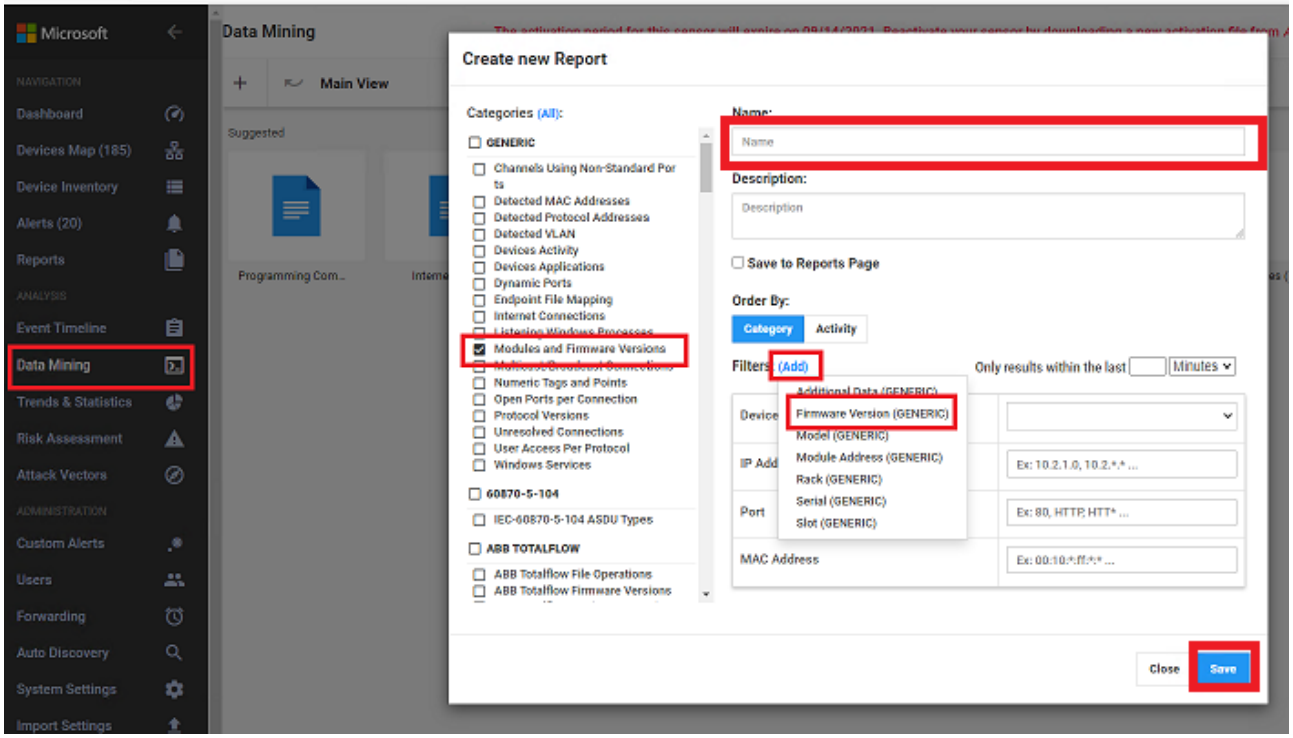
1. Choose **Advanced Filers**, filter the timeline by **CIP**, let's analyze the alert timeline.

Task 5: Data Mining

In this section you can create multiple custom reports. As an example we will create a Report based on firmware updates versions.

1. Go To +, **New report**, in the categories section select **Modules and Firmware update versions**

2. Assign a name to your report. Then go to Filters, **add** and select **Firmware version(generic)**



3. In the new field added **Firmware Version(GENERIC)** add **0.4.1**, then **Save**.

4. You can remove the filter to list all the firmware updates version in your list also.

5. Export you report(pdf, csv) for further actions.

Task 6: Risk Assessment

1. Go to the Risk assessment, run the assessment. During this task we will show you how to analyze the assessment.

IMPORTANT, after completing this workshop you will have a period of two weeks to run the risk assessment in your evironment and schedule an appointment with our Cybersecurity team to guide you through analysis, best practices, and vulnerabilities in your facilities.

Exercise 5: Online Sensor

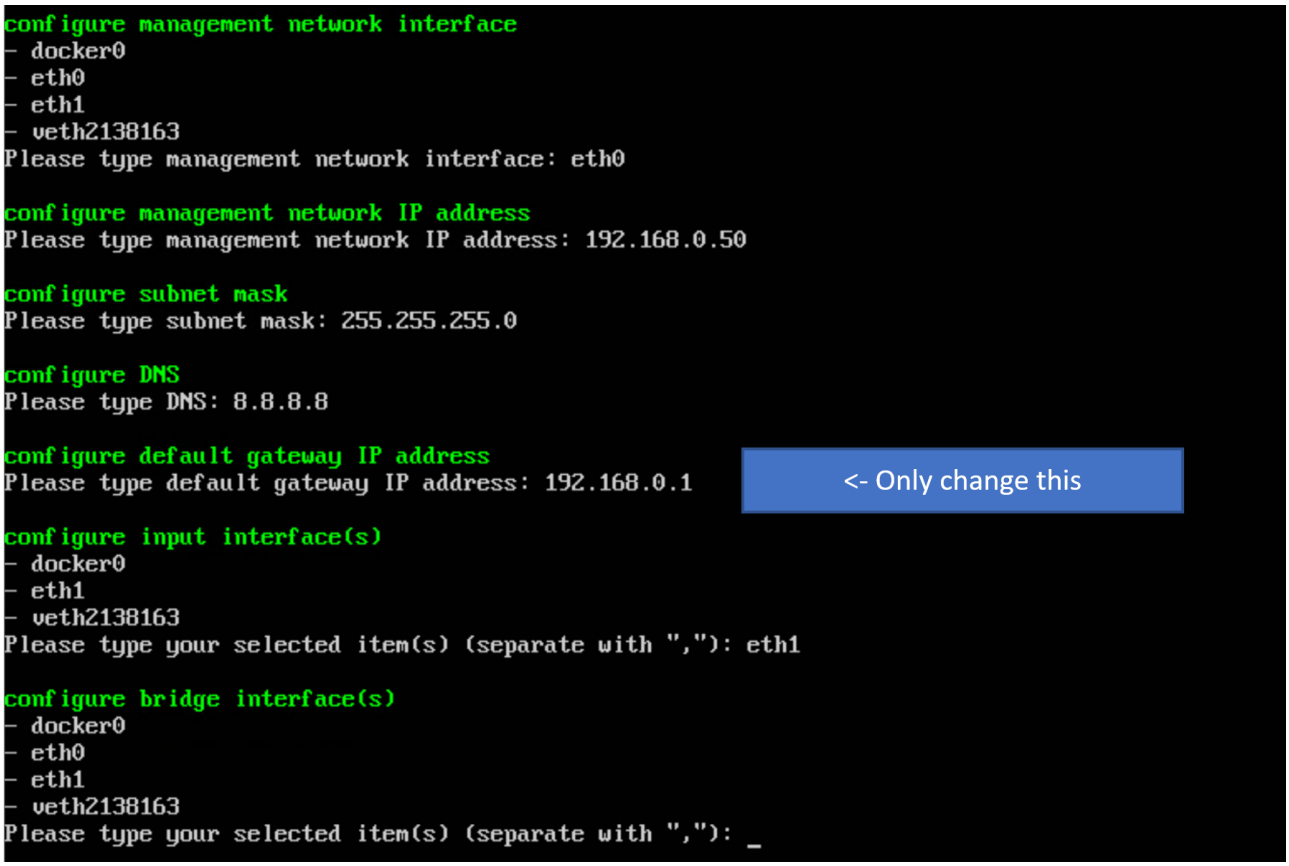
To modify our sensor to be an online sensor, we will use the same virtual machine but we will reactivate the sensor using **System settings**

Task 1: Reconfiguring sensor

1. To modify your sensor to be connected with Azure, we will need to modify the network configuration. If you test your sensor using:
    - **ping 8.8.8.8** google dns, you will receive a message as **network unreacheable** your sensor needs connectivity before changing the activation mode.
2. In the Ubuntu sensor we will need to reconfigure the gateway to bring it online and allow it to reach Azure IoT Hub, type the following:

```
sudo cyberx-xsense-network-reconfigure
```

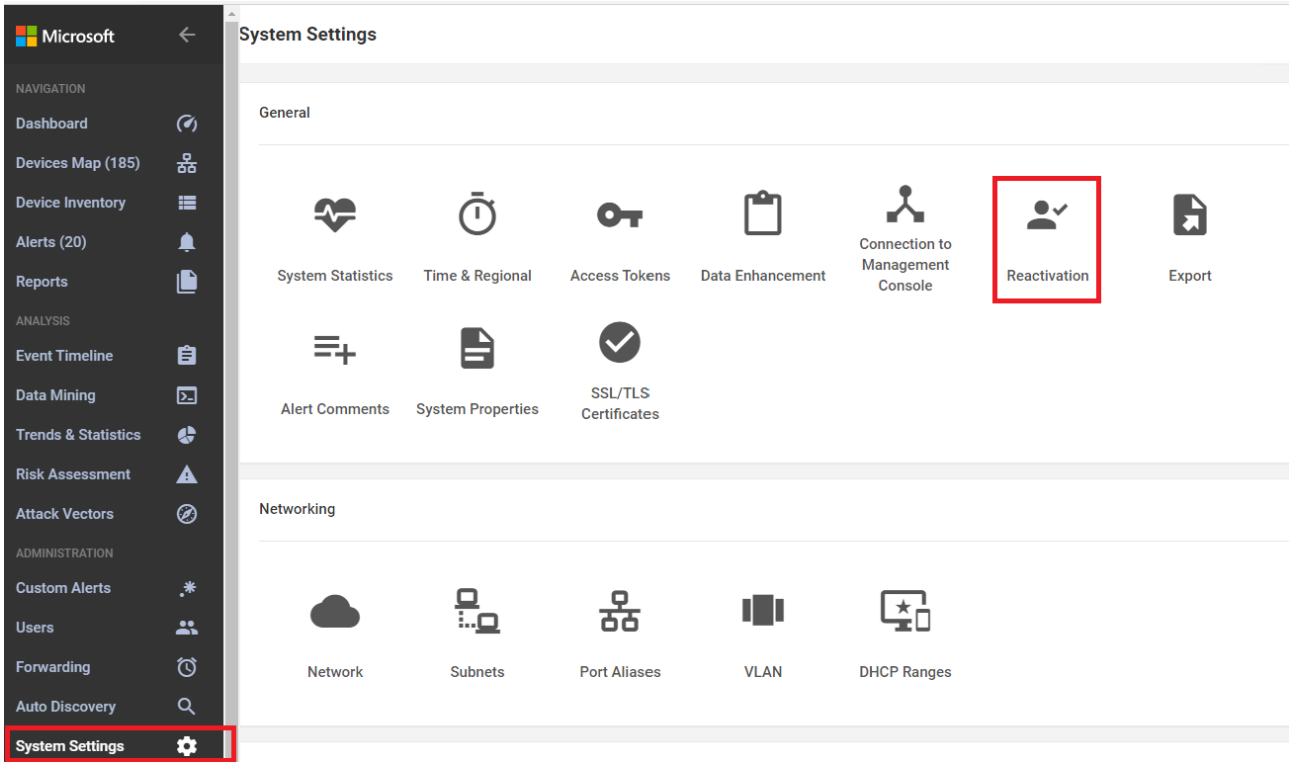
3. You will ask to login, then you can start to reconfigure the network settings, you will only change **one** value, **configure default gateway IP address** you will assign the IP Address of the NATSwitch value configured in previous steps, either 192.168.0.**1** or 172.27.0.**1**, you will keep all the other values as before.



4. Type **Y** at the end of the process to apply the change, it will run a reconfiguration and reboot.
5. After logging back in, test that you have external connectivity: **ping 8.8.8.8.8** in the Ubuntu sensor, you should now receive a different message containing "...icmp...". Note: hit Cntrl-C to stop the pinging.

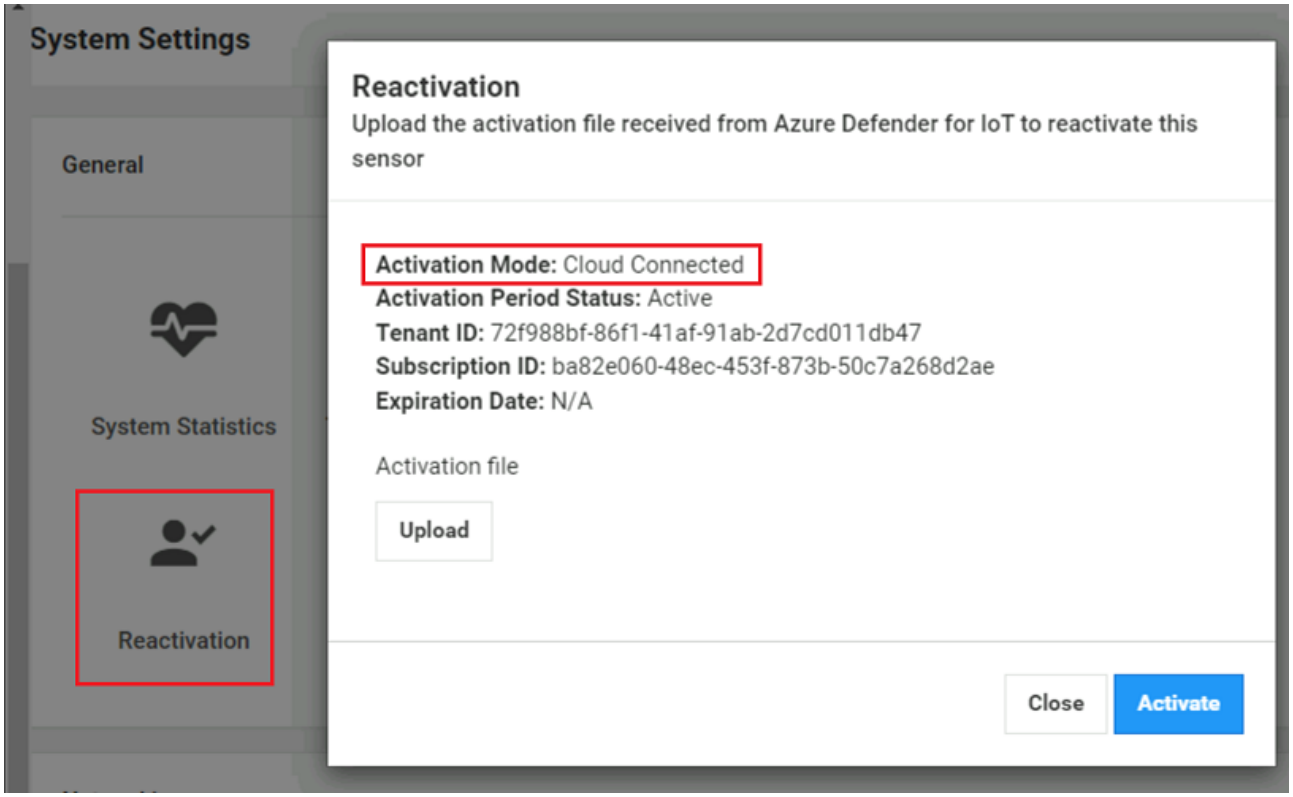
6. Now that your sensor has connectivity, go to the Azure Defender Portal, select **System Settings** and then, **Reactivation**.

7. In the new window, select **Upload**, **Browse File**, select the zip file you downloaded from the storage account in previous steps **myonlinesensor.zip**, then **Open** and **Activate**, **Ok** to the instructions

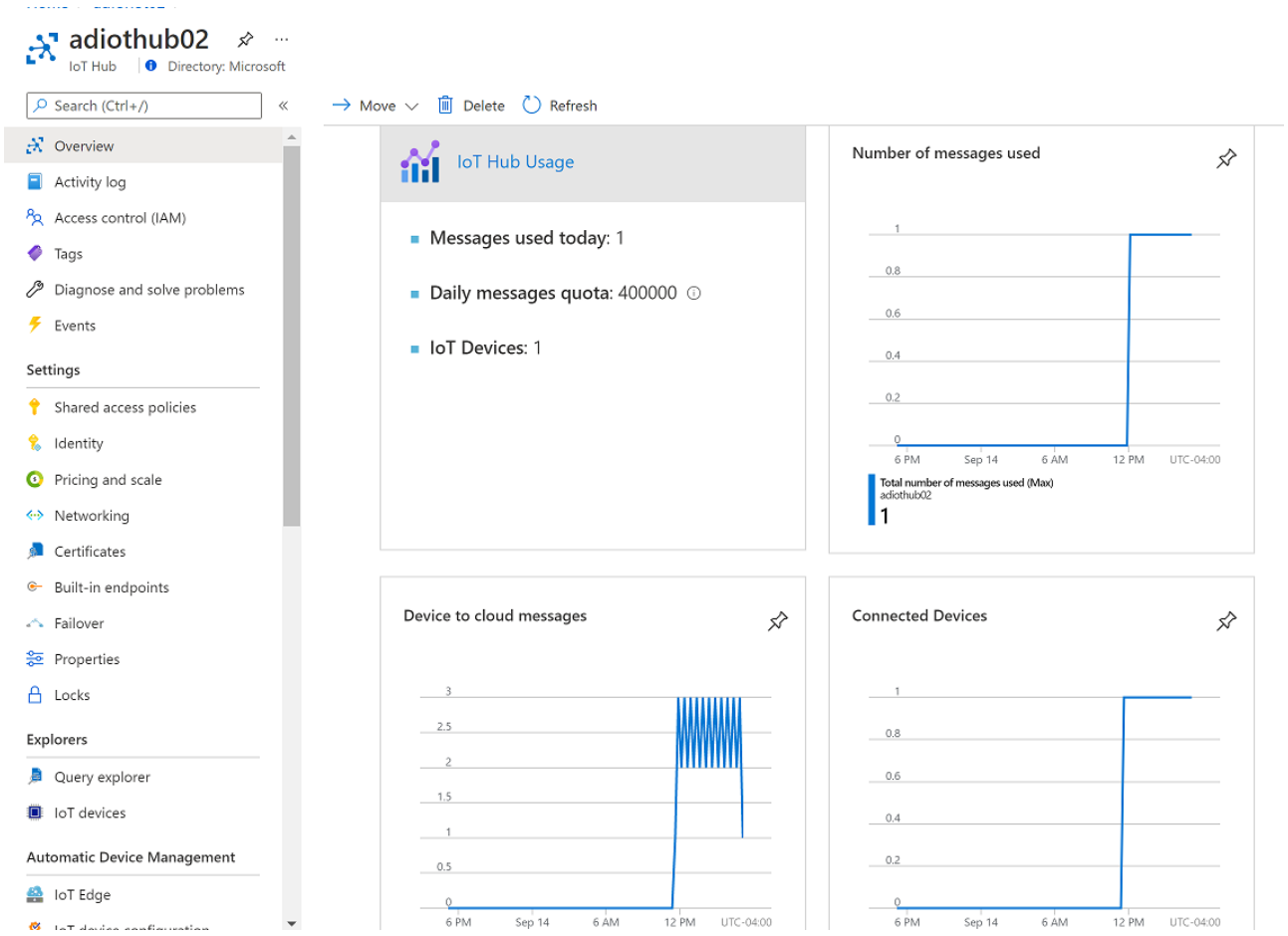


8. Last, you should receive a message showing your sensor modified to **Connected**.

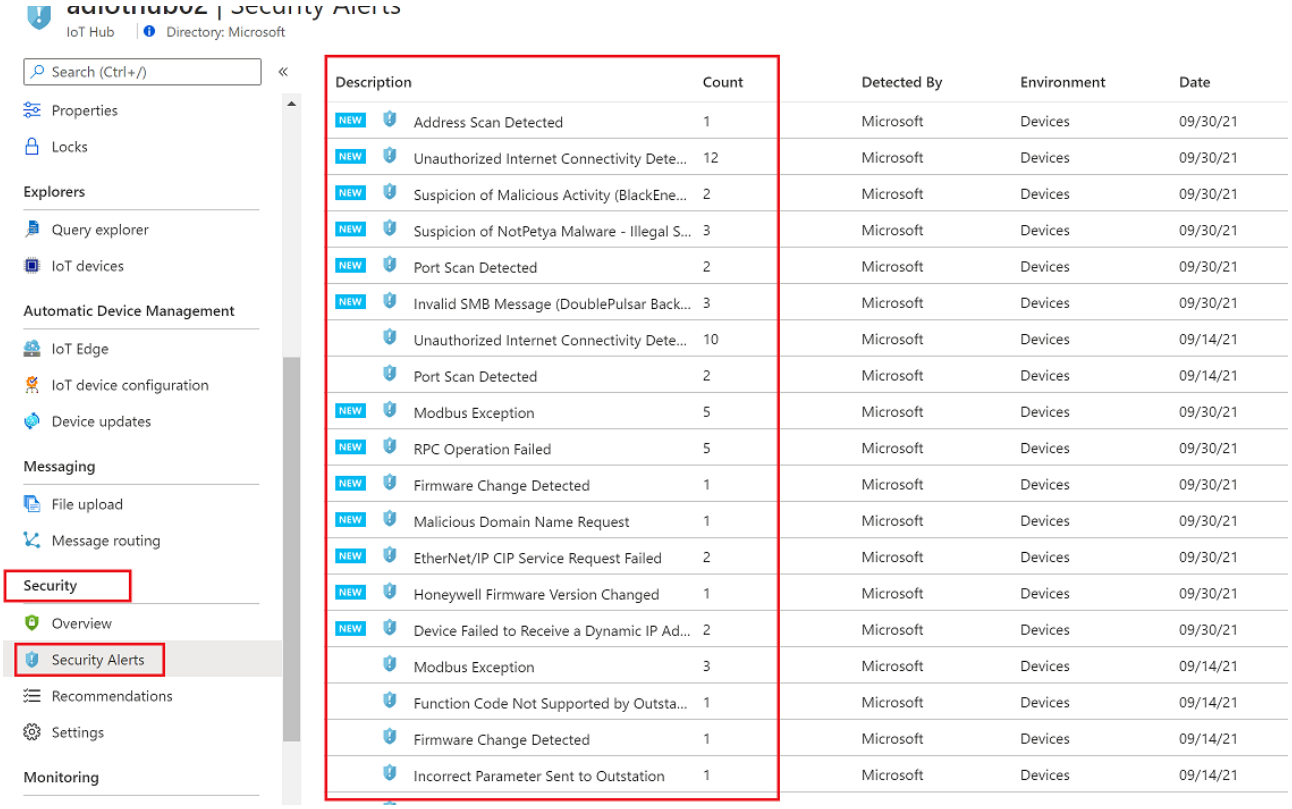
9. Close the screen, open again the **Reactivation** window and double check if your sensor is **Cloud Connected** as shown below:



10. Run the Pcap files again in your console, in a few minutes you can verify if IoT Hub in Azure Portal is receiving messages from your sensor:



11. In the same IoT Hub now you should see the alerts generated for Defender, scroll down to **Security**, select **Security Alerts**, on the right side you will see some alerts already available. (Note that this alert view will be deprecated soon and will be available in Azure's "Defender for IoT" Portal)

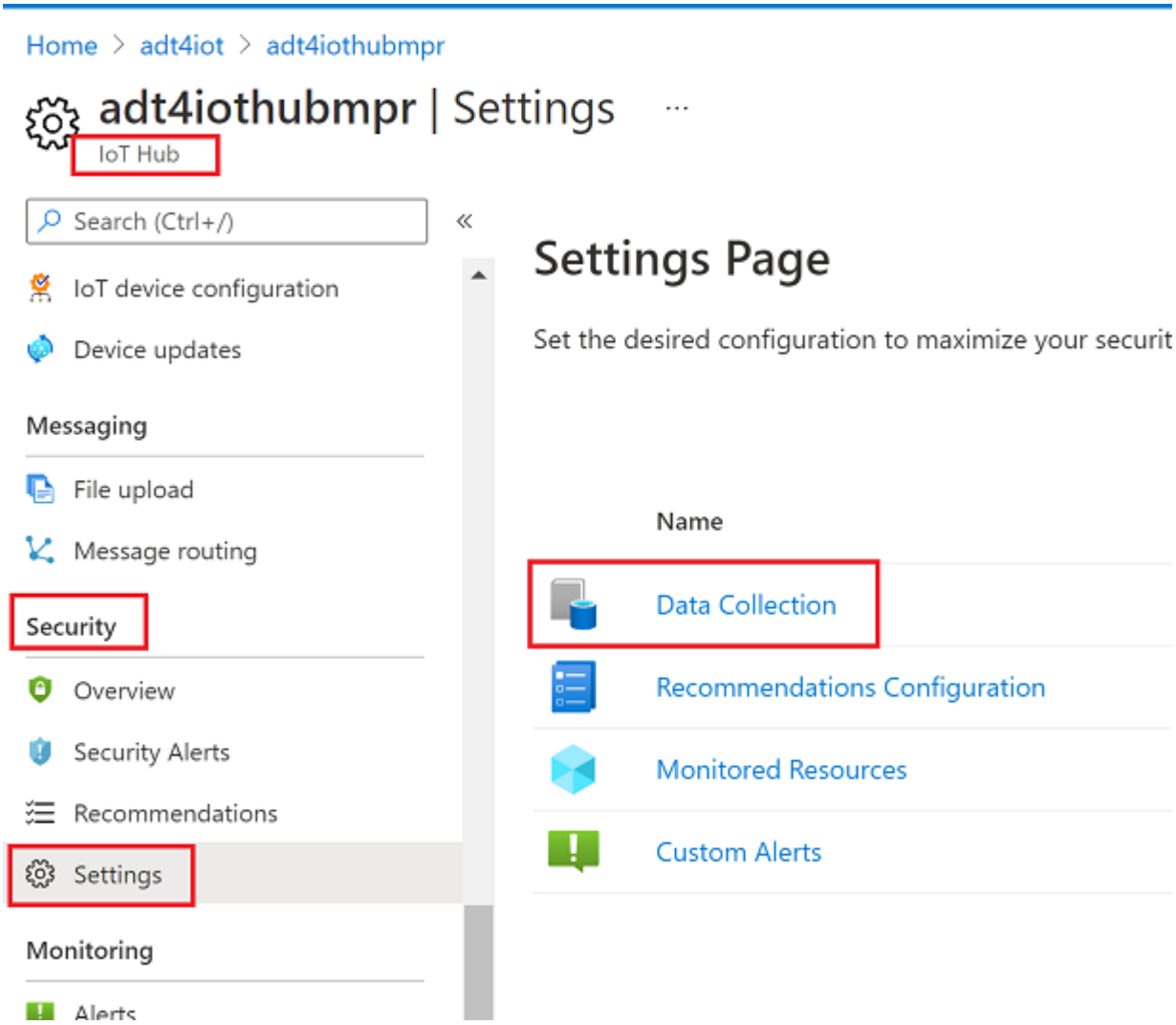


Exercise 6: Integrate with Sentinel

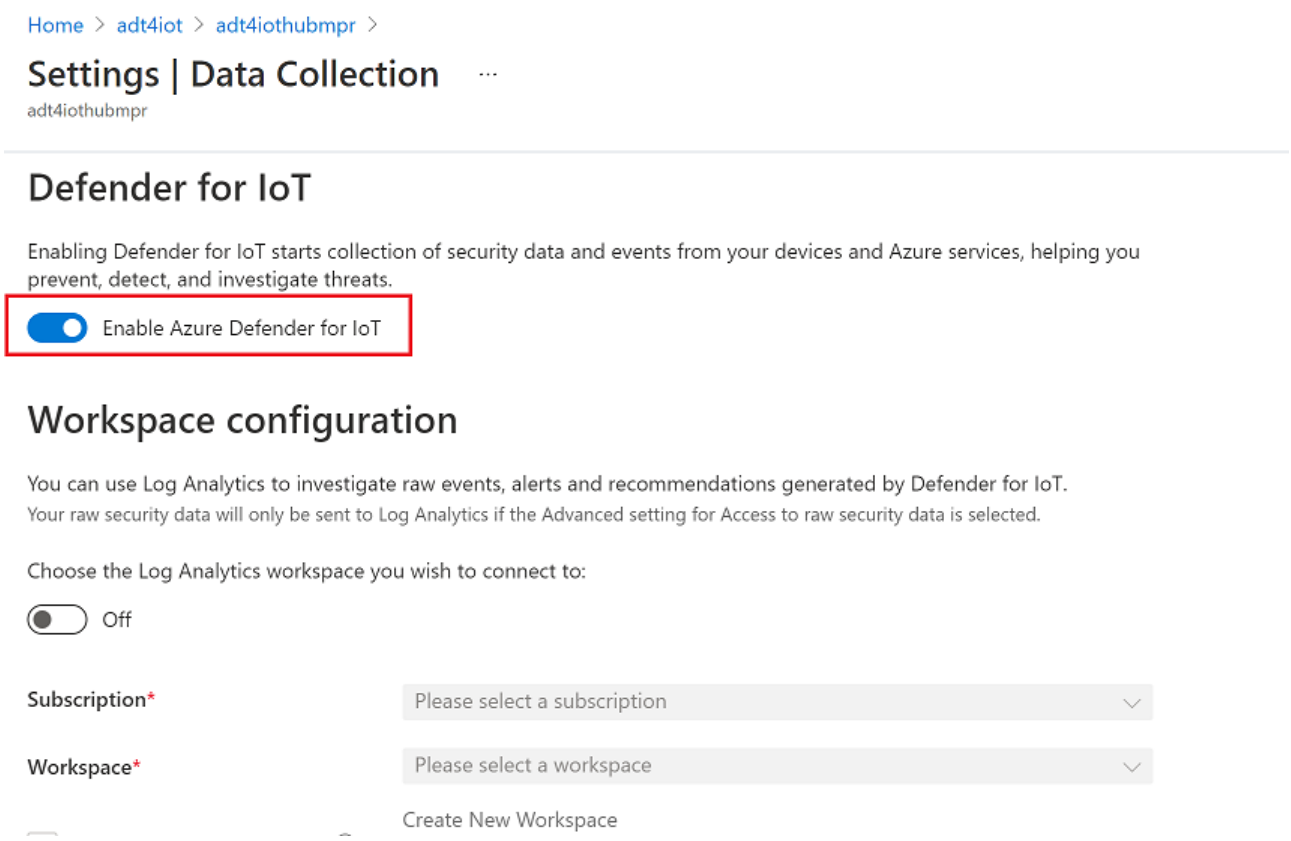
Note: Please ensure you have completed Task 6 in the 'Before HOL' prior to working through these instructions.

Task 1: Enabling IoT to Integrate with Sentinel

1. Ensure your IoT Hub is configured to send Security Alerts to Sentinel.
2. Navigate to your IoT Hub > Security > Settings > Data Collection

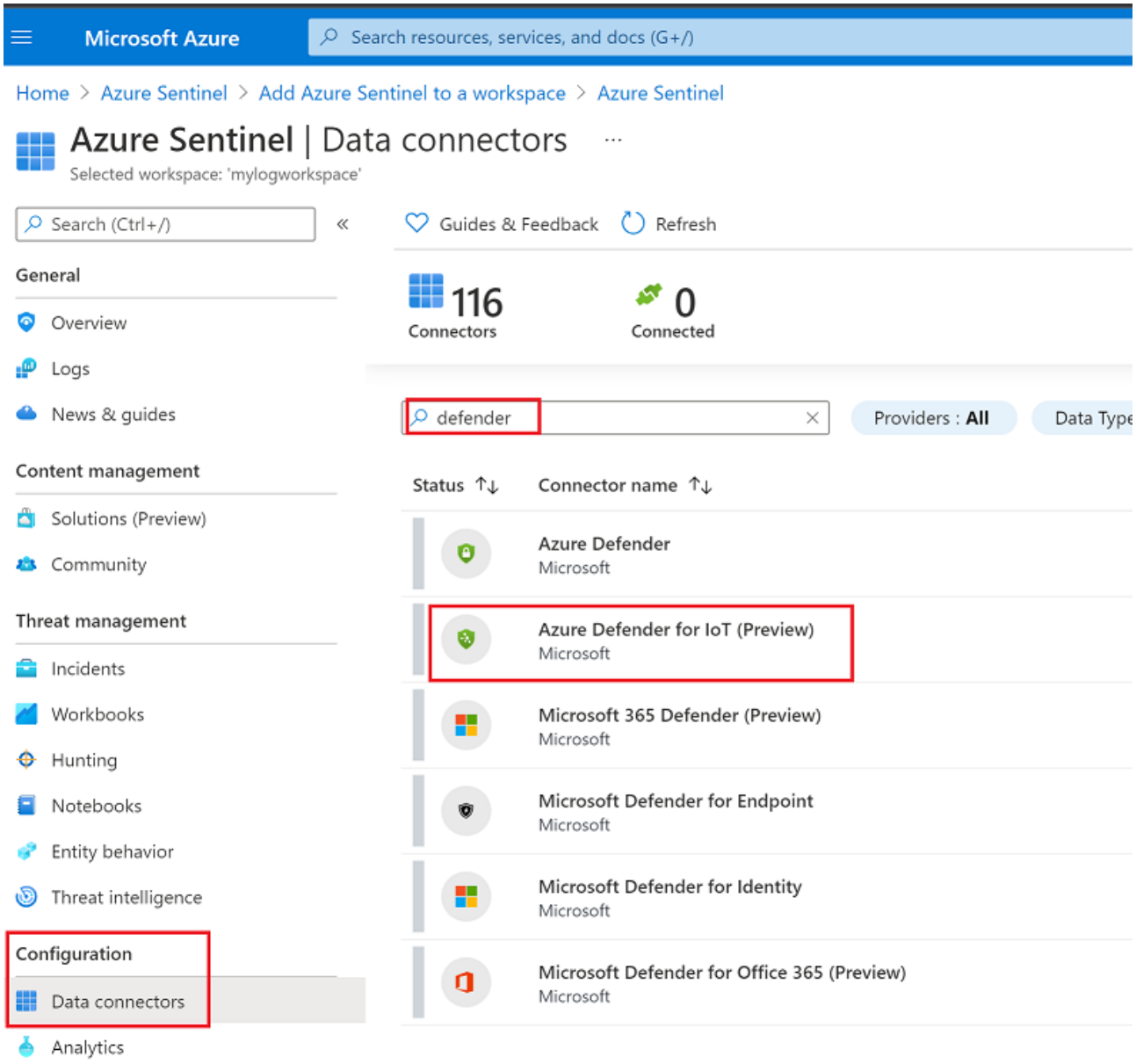


3. Double check that Data Collection blade, is enabled for **Enable Azure Defender for IoT**

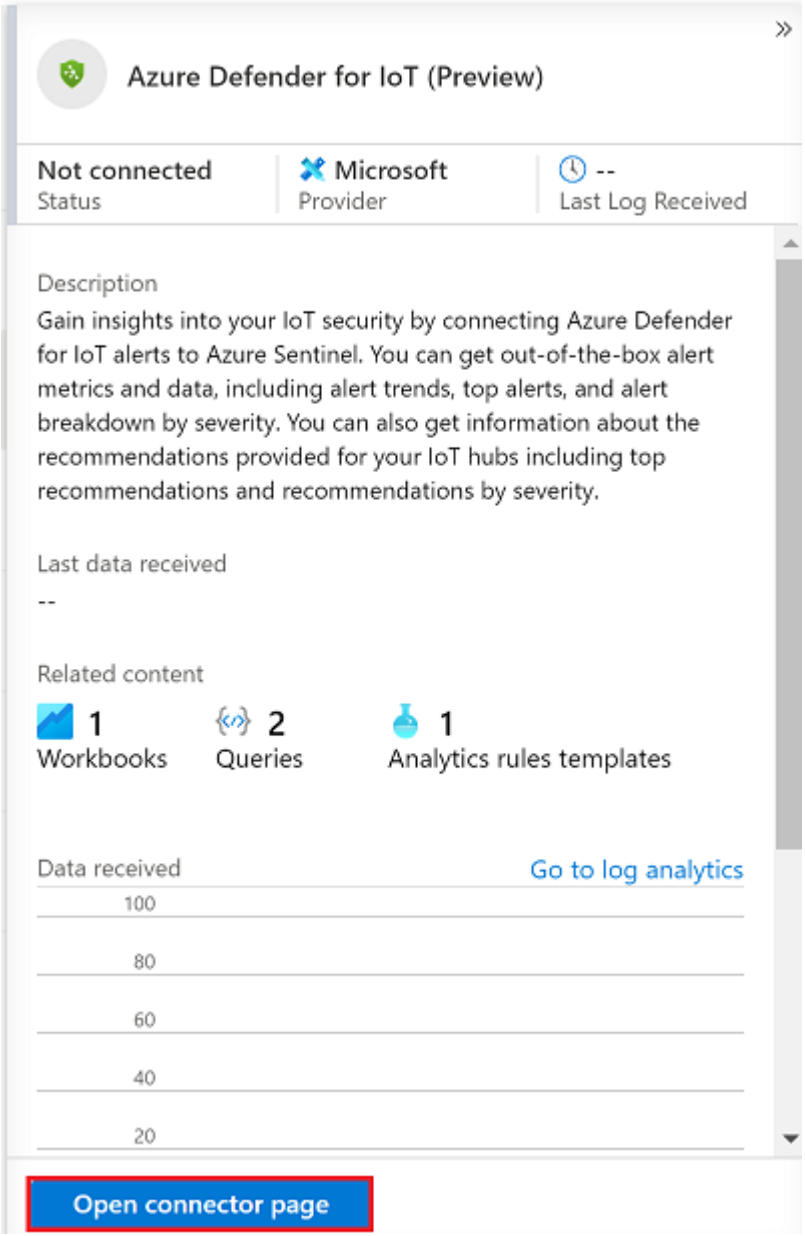


Task 2: Connecting Data Connectors

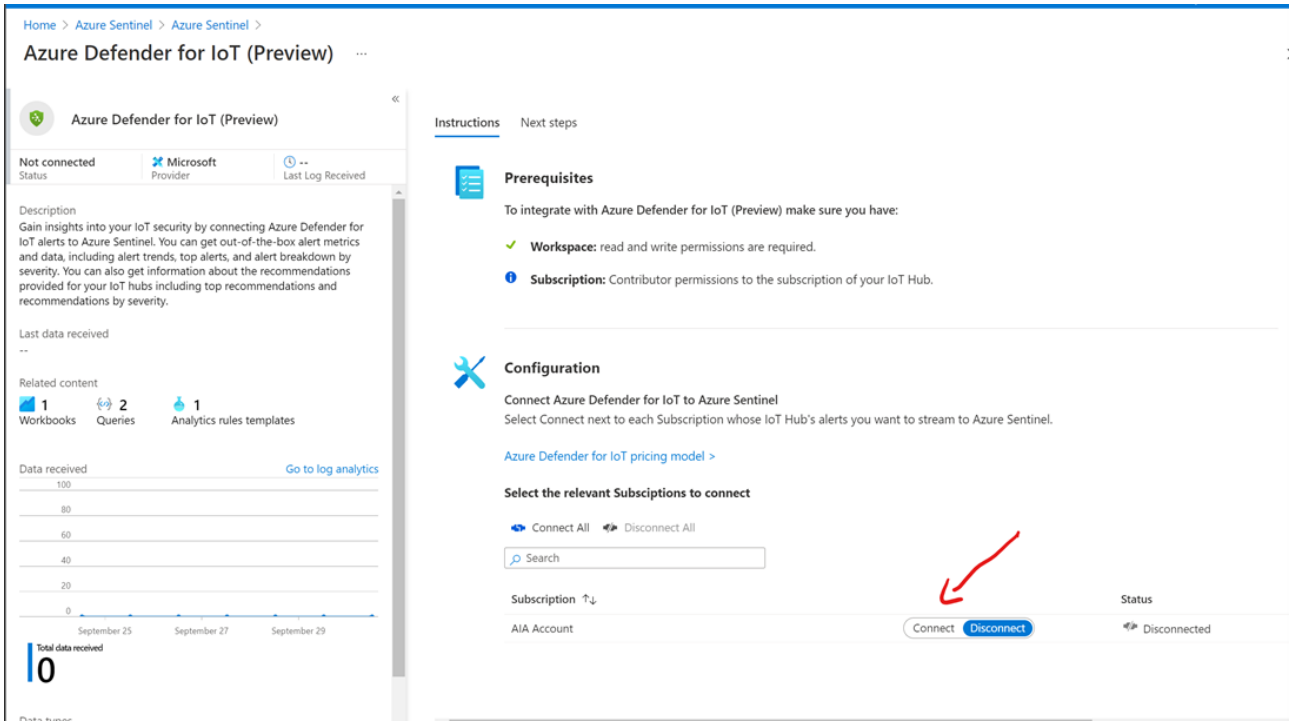
1. After all the flags are enabled, go to **Sentinel** > Configuration > Data Connectors > Search **Azure Defender for IoT** to connect IoT to Sentinel.



2. Click the **Open Connector Page**

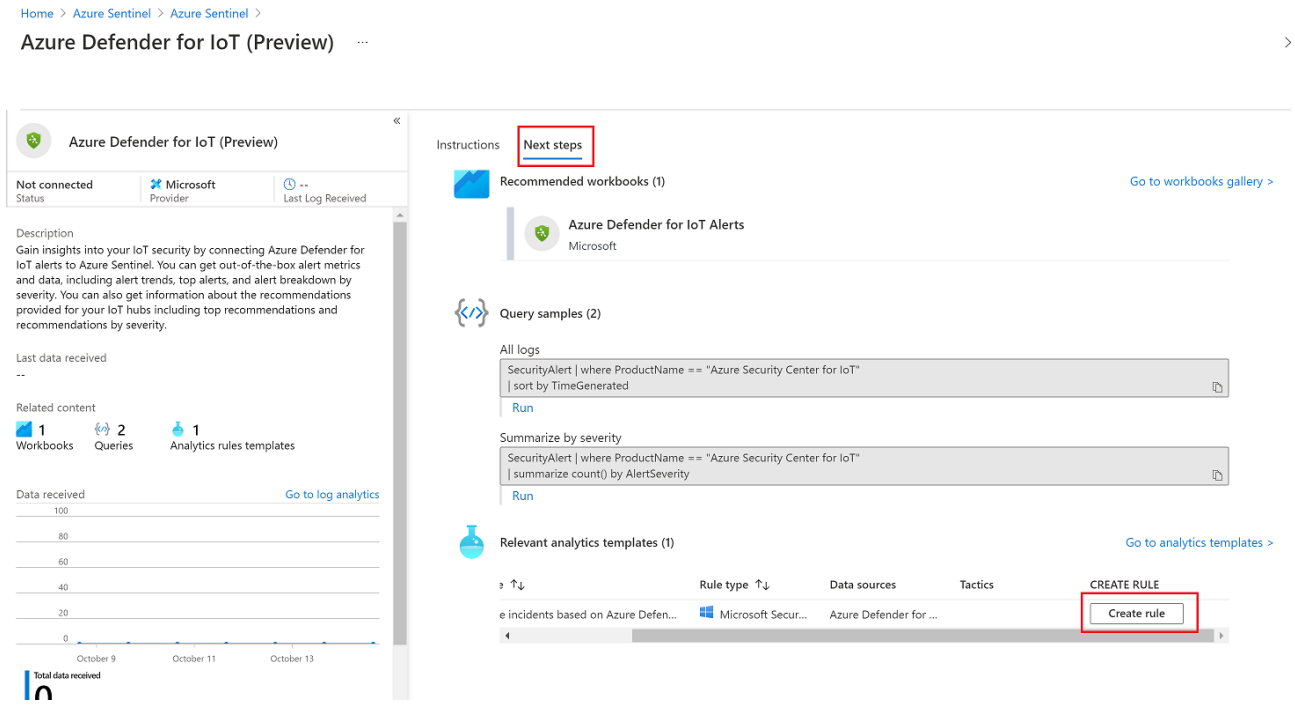


3. Review the instructions and click the “Connect” button to connect Azure Defender for IoT to Sentinel. If the connection continues to fail, this will most likely be due to the user not having the "Contributor" permissions and you may have missed the access step in the prerequisites.

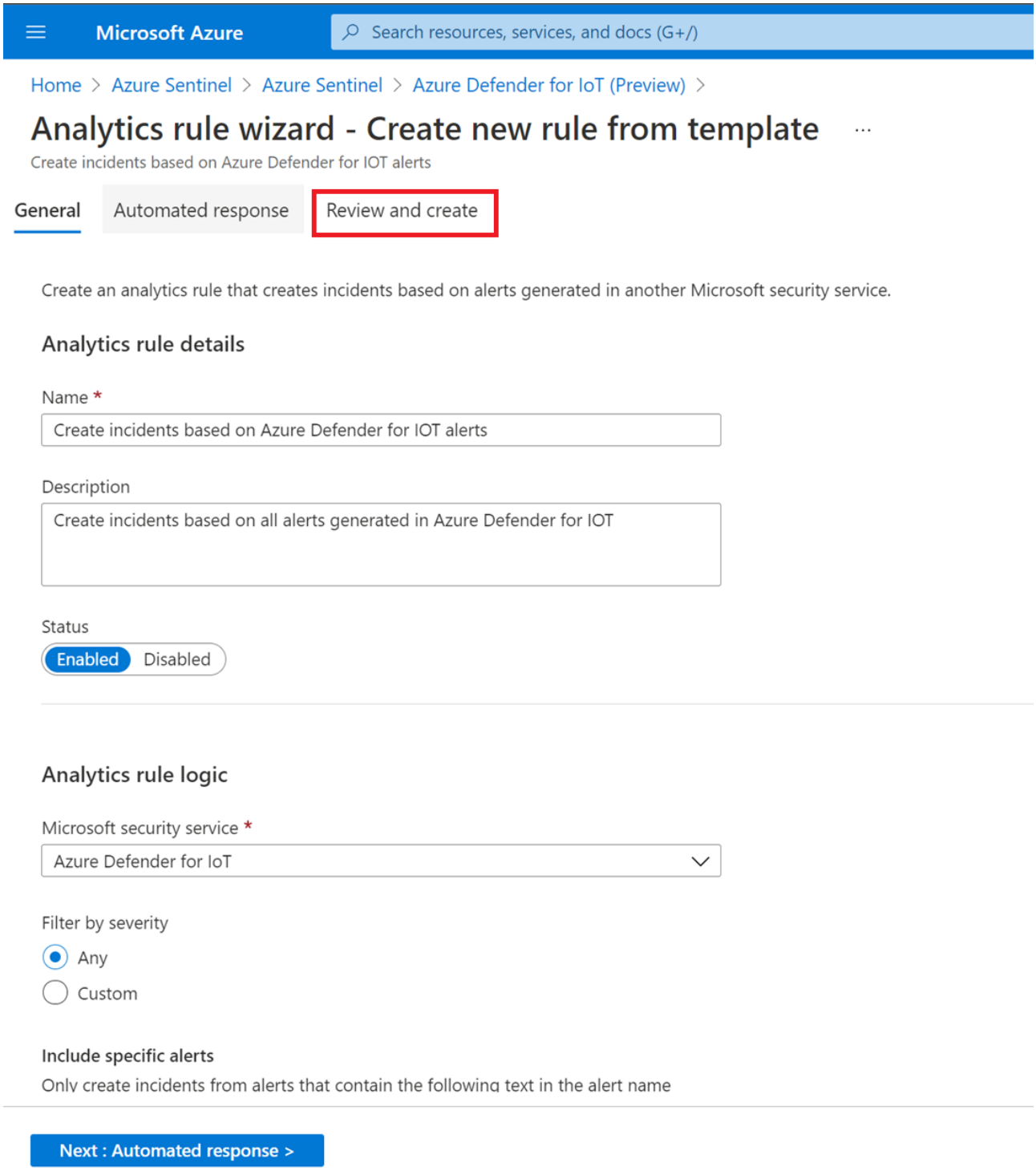


4. If connected correctly you should expect to see the Status change to “Connected” and the link light up green.

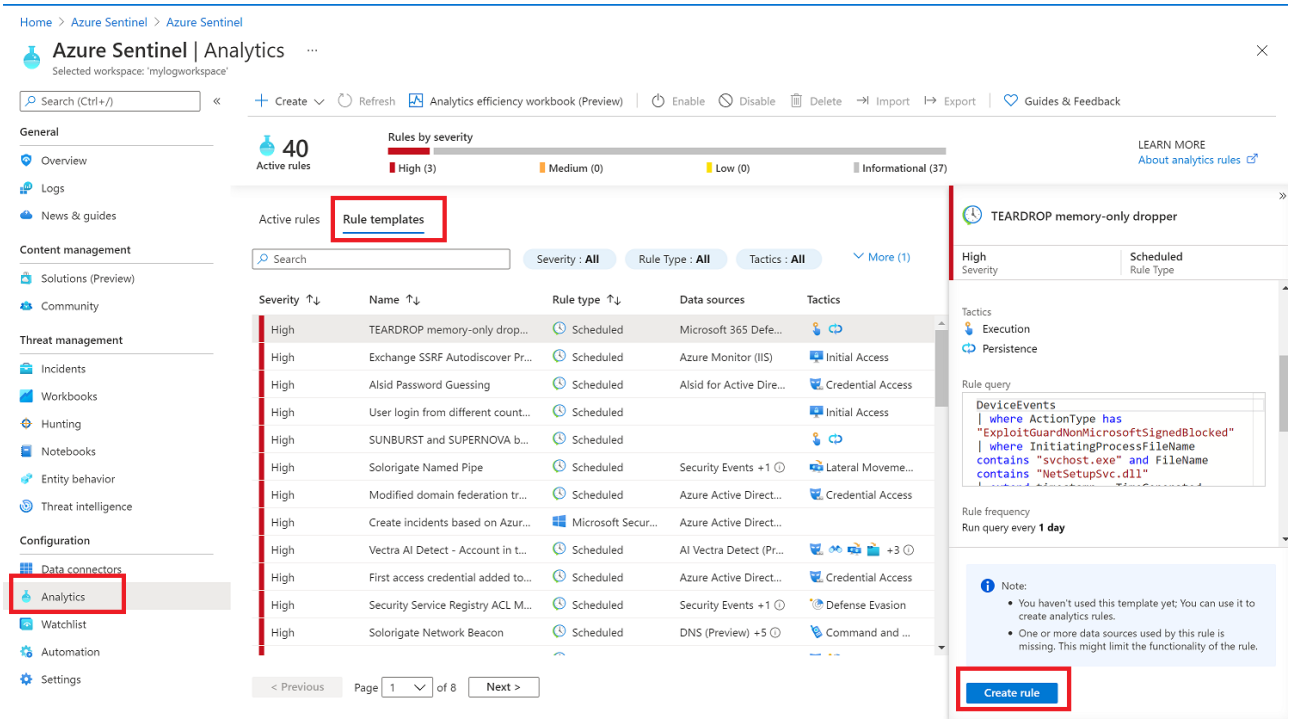
5. Use the next steps tab to enable Out of the Box alerts. For example, click the create rule and follow the instructions to turn on the rule.



6. Fill in the “Name” and click **Review and Create**. This is enabling incidents to be created based on the Azure Defender IoT alerts that are ingested into Sentinel.



7. Additionally, you can create the rule not only on the data connectors page but also on the “Analytics” blade. See an example below when you go to the “Rule Templates” tab and filter data sources by “Azure Defender for IoT (Preview)”.



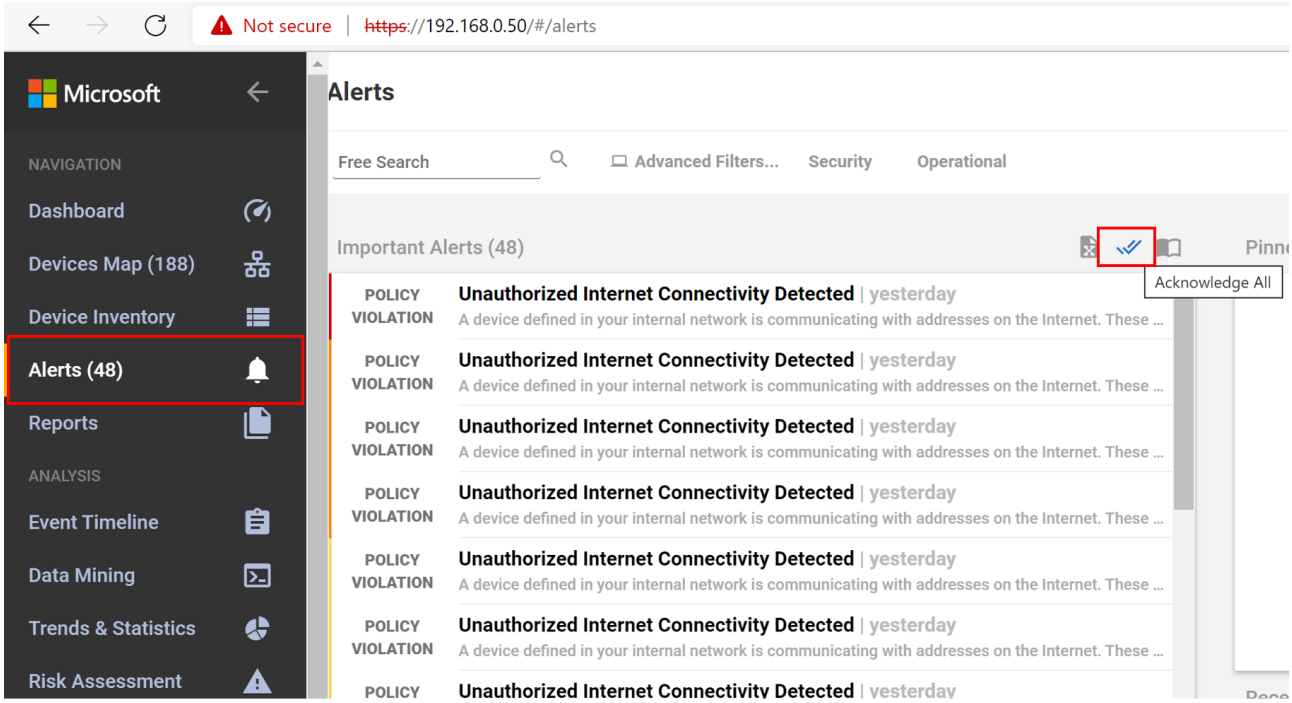
Task 3: Acknowledge Alerts and Re-run PCAPs

1. Go back to your browser interface and acknowledge all of the alerts. The reason we are doing this is so we can re-run the alerts to show how they are sent and analyzed by Sentinel.

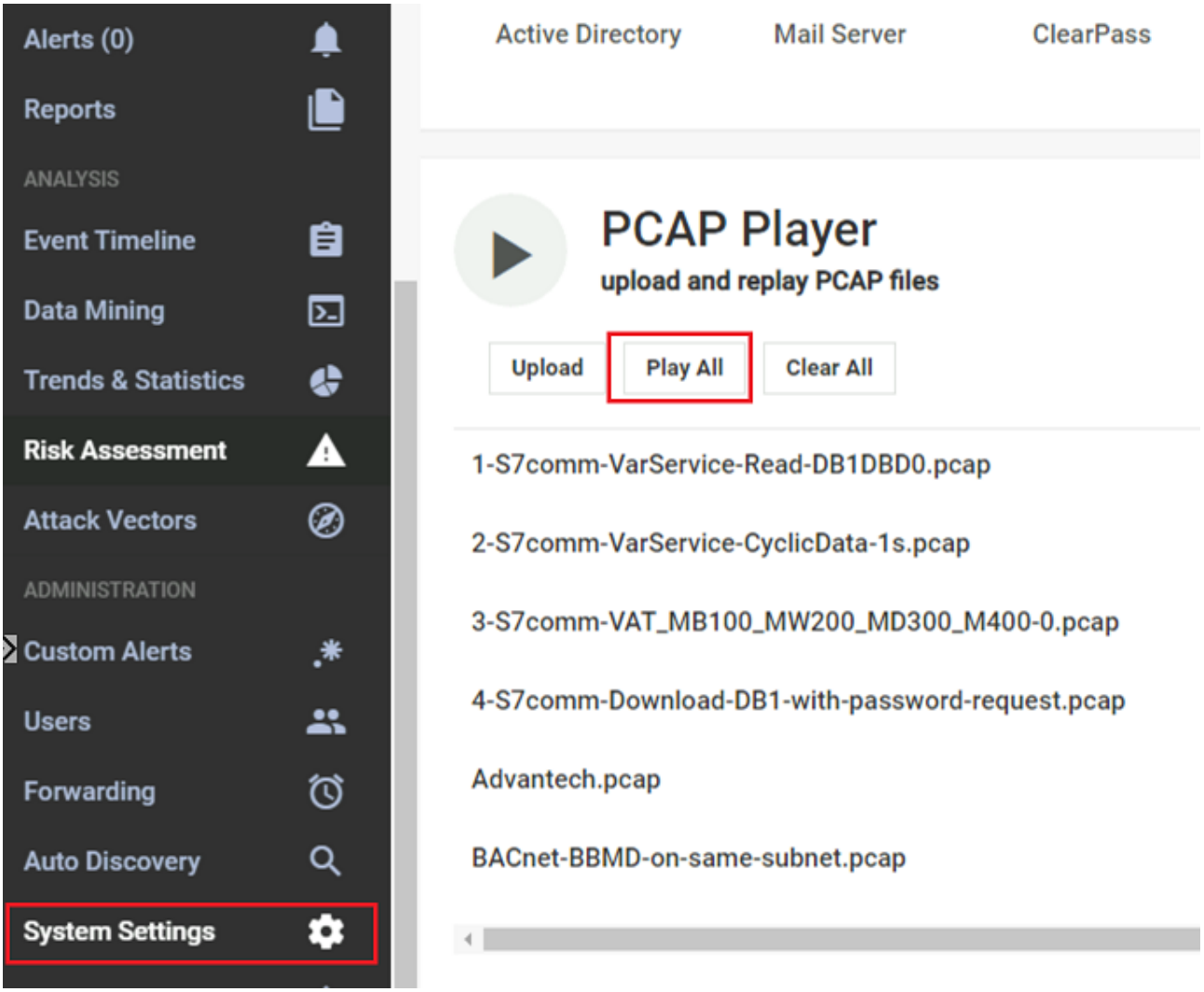
    i. Navigate to the Alerts Page

    ii. Click the double check box

    iii. Click **Ok** to acknowledge the alerts

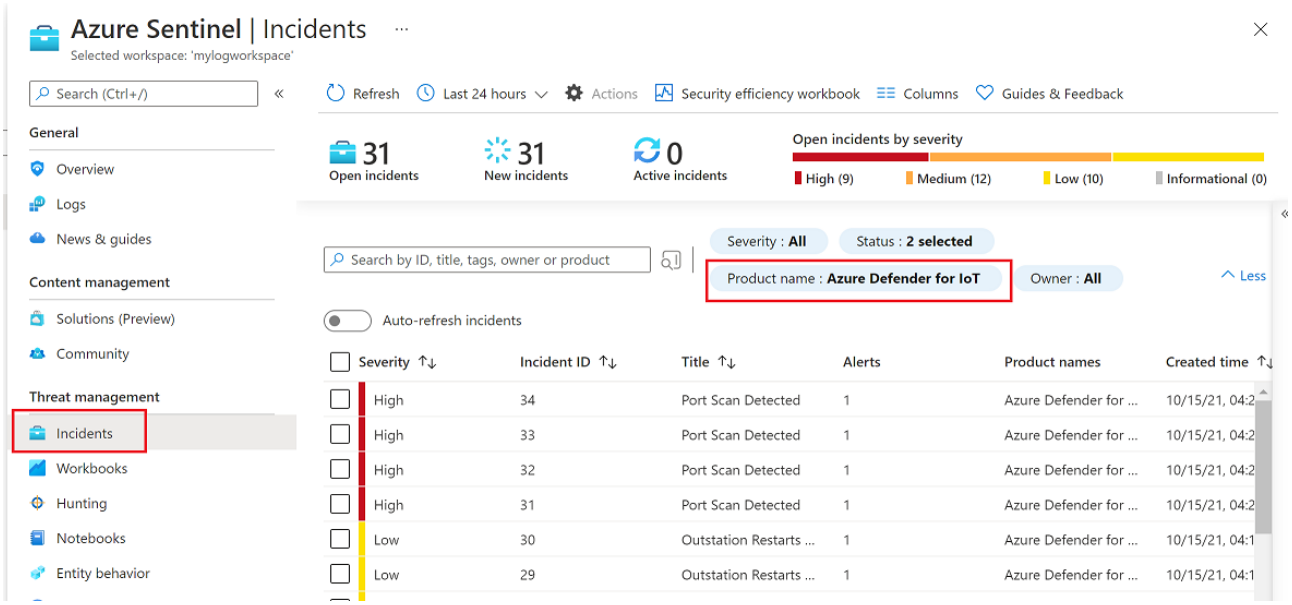


4. Now go to the System Setting tab.
5. Click the **Play All** on the PCAP Files to replay simulating the alerts.

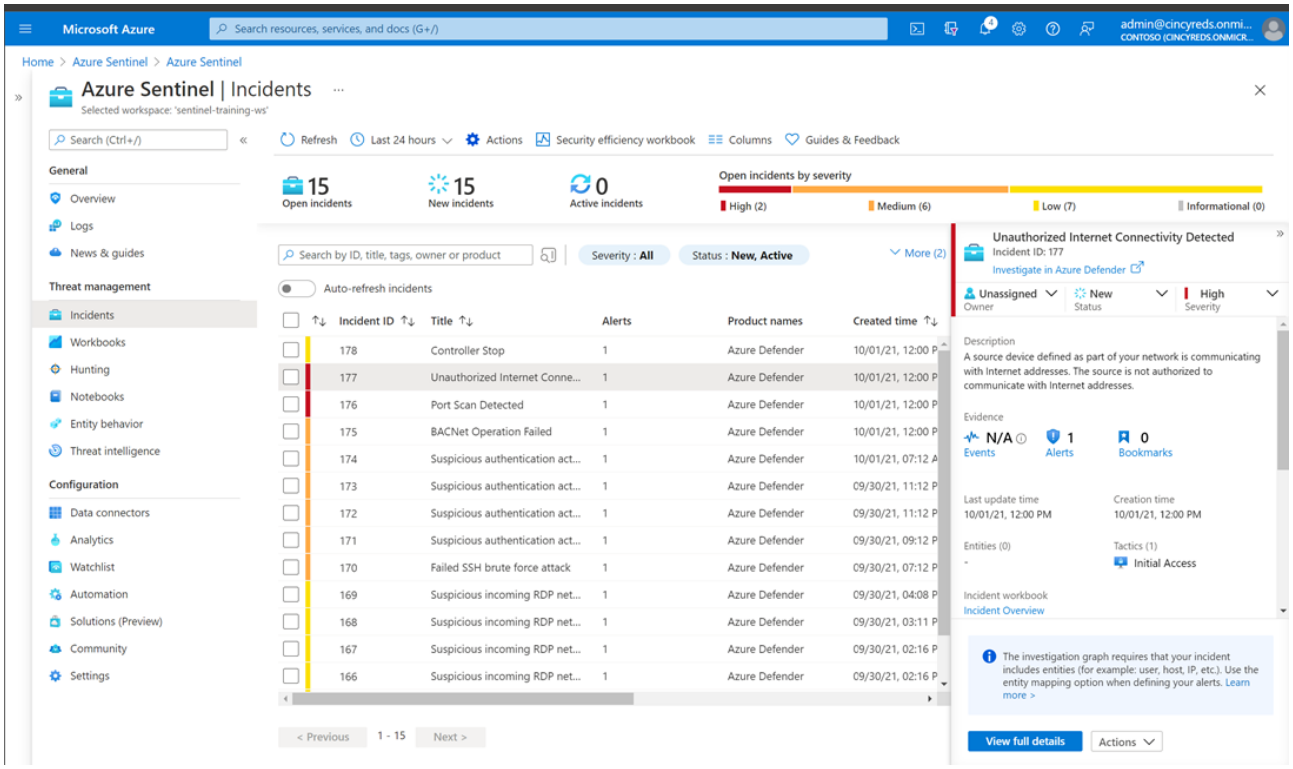


Task 4: Sentinel interaction with IoT Incidents

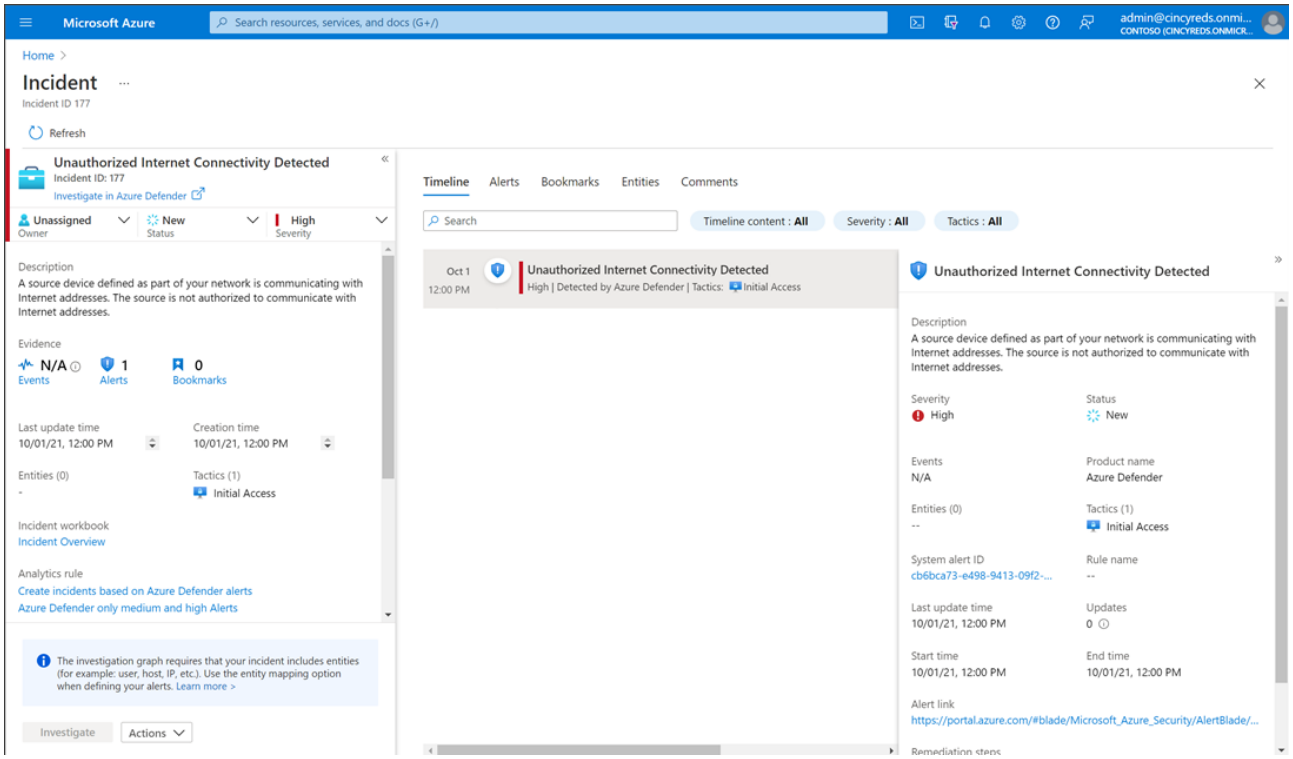
1. Go back to the Sentinel console and under the **Threat Management** section, select the **Incidents** tab. Filter by Product Name **Azure Defender for IoT**.



2. Select one of the alerts and click **View full details**



3. It will take you to this screen to get all the information relative to the incident. This allows analyst to get more details on the entity including what other alerts made up the incident, playbooks to enrich the context of the alert, and comments section to leave details on what the analyst discovered during review or how they came to the determination to dismiss the incident.

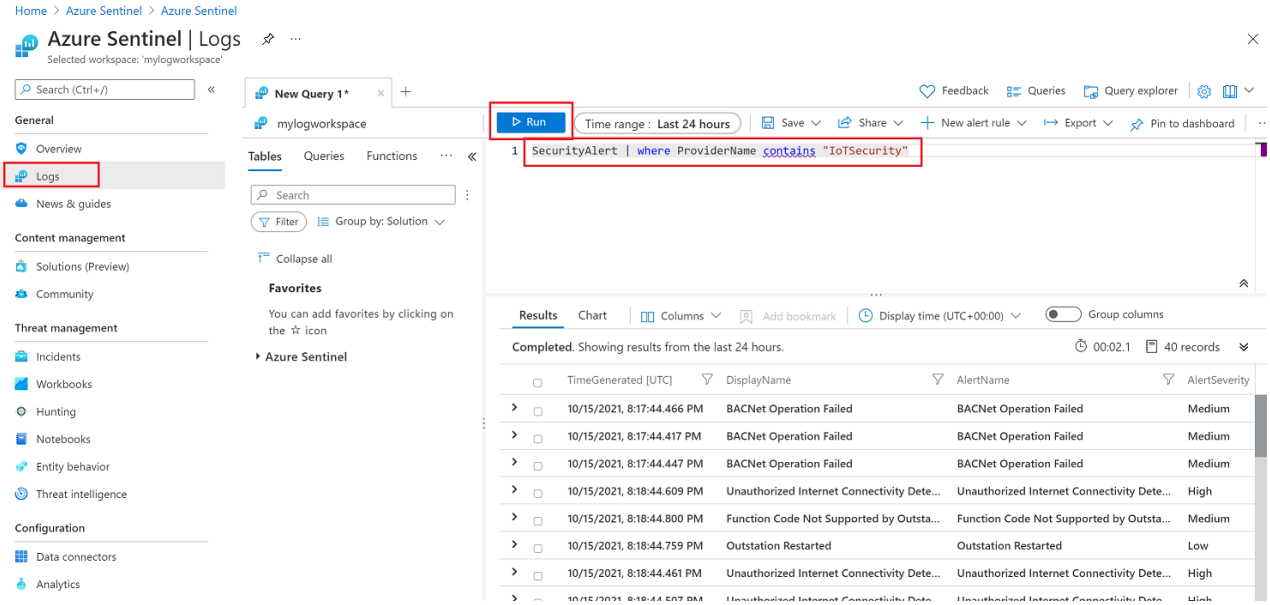


Task 5: Kusto Query Language to Find Alert Details

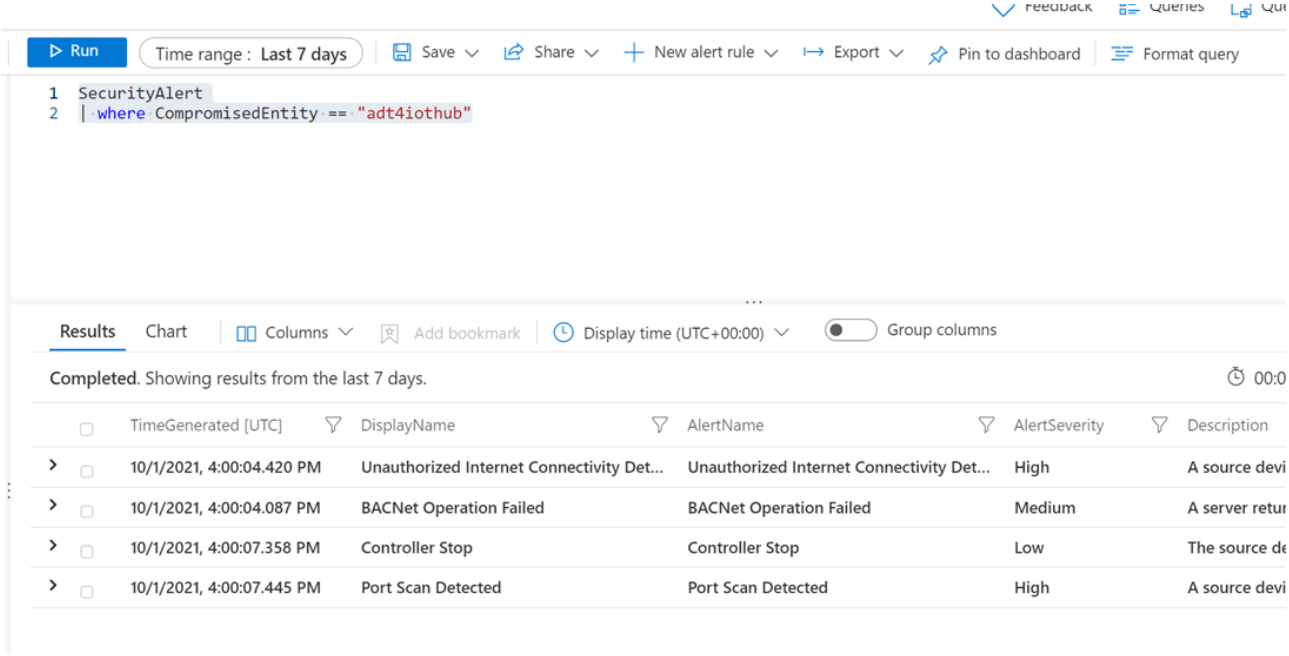
1. Navigate to the “Logs” tab and run this query. Querying the data will provide the ability to join tables and datasets to curate data from multiple sources. KQL is a similar language to SQL but will take some research and some dedicated time to become familiar with.

Here are two basic examples:

```
SecurityAlert | where ProviderName contains "IoTSecurity"
```




```
SecurityAlert | where CompromisedEntity == "adt4iothub"
```



Exercise 7: Clean Up

Task 1: Delete resources

The Azure Passes will allow you to run the services for 90 days for training purposes. Although it is a best practice to delete all your resources after the training.

Search for the Resource Group created for this training.

Select Delete resource group on the top right side.

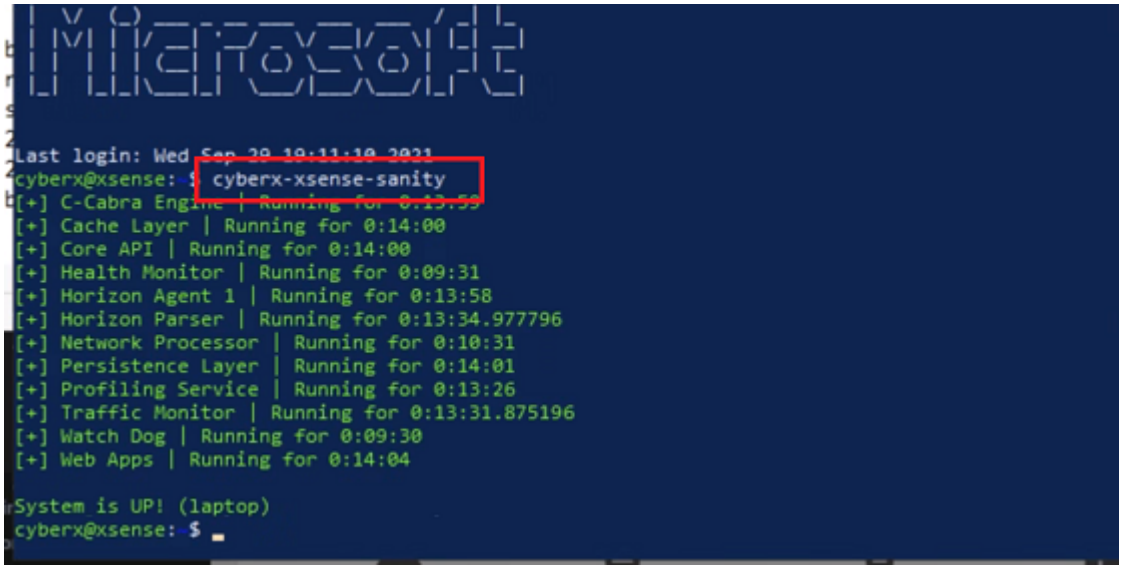
Enter your-resource-group-name for **TYPE THE RESOURCE GROUP NAME** and select Delete. This operation will take a few minutes.

After that is done go to Azure defender for IoT and deactivate the subscription.

Appendix: Troubleshooting

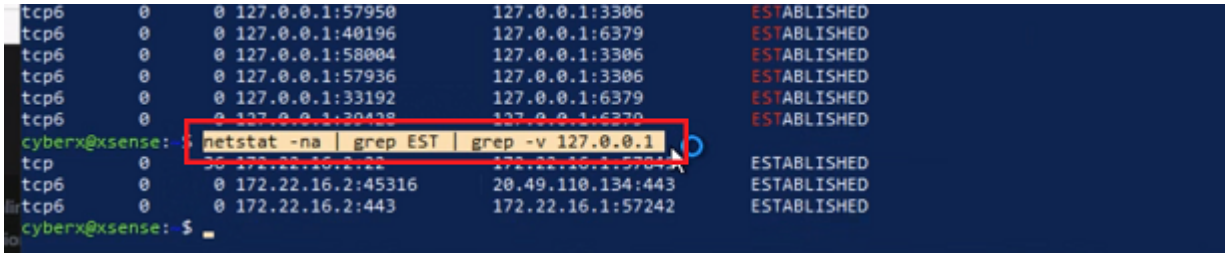
1. If your Defender portal is not working properly run the following command to validate if the components are running properly

```
cyberx-xsense-sanity
```



2. If your IoT hub is not receiving messages, check if ubuntu machine can reach IoT Hub, first run the following command to identify the IP of your IoT Hub:

```
netstat -na | grep EST | grep -v 127.0.0.1
```



Then, ping the IoT Hub using the connection string from the overview blade in Azure Portal.