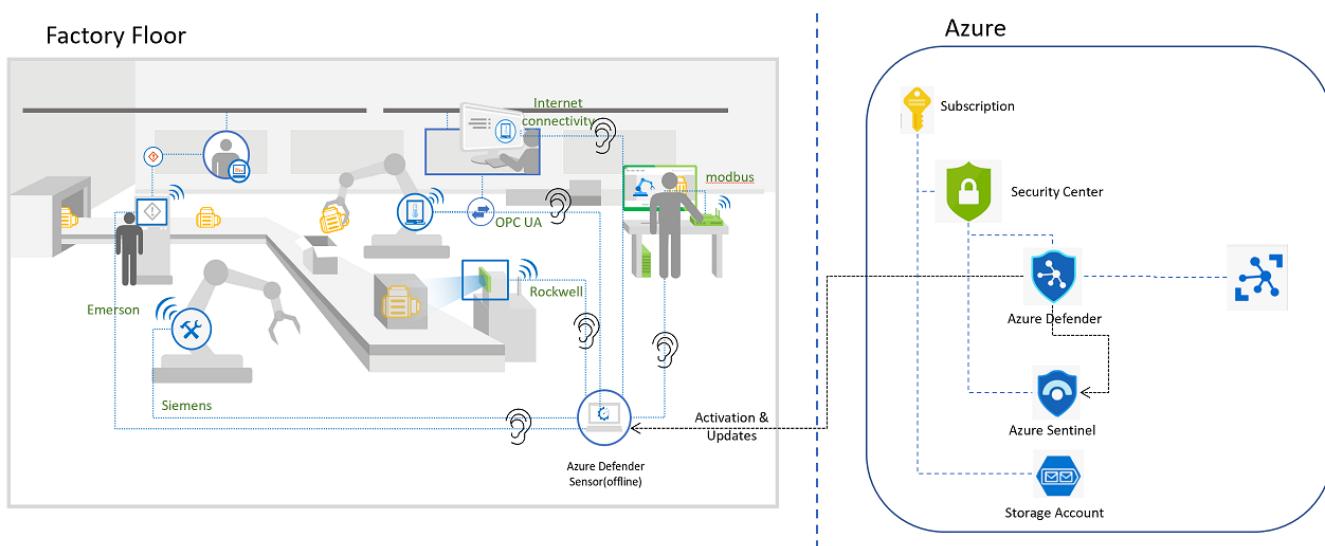


Internet of Things - Microsoft Defender for IoT HOL

Before starting this Lab make sure you completed the steps specified in the [prerequisites](#) file in this repository.

Architecture Diagram

During this workshop we will be focusing on setting up our Microsoft Defender for IoT sensors, for online alerts and also for offline scenarios. You will learn how to configure your environment, assess the results, and integrate with SIEM systems like Microsoft Sentinel. This Hands-on-Lab (HOL) will be focus on securing your facilities. It will cover brownfield and greenfield devices (currently not part of the HOL). The scenario below is one of many you would apply these lessons to, other scenarios are Oil, Gas, Utility, and Energy companies.



Content:

- Exercise #1: Enabling Defender
 - Task 1: Enabling Microsoft Defender for IoT
 - Task 2: Create an IoT Hub:
 - Task 3: Onboarding sensors
- Exercise #2: Setting up your offline sensor
 - Task 1: Set up your offline sensor
 - Task 2: Collect Information
- Exercise 3: Enabling system settings
 - Task 1: System Properties
 - Task 2: Pcap Files
- Exercise 4: Analyzing the Data
 - Task 1: Devices Map
 - Task 2: Alerts
 - Task 3: Device Inventory
 - Task 4: Event Timeline
 - Task 5: Data Mining
- Exercise 5: Online Sensor
 - Task 1: Reconfiguring sensor

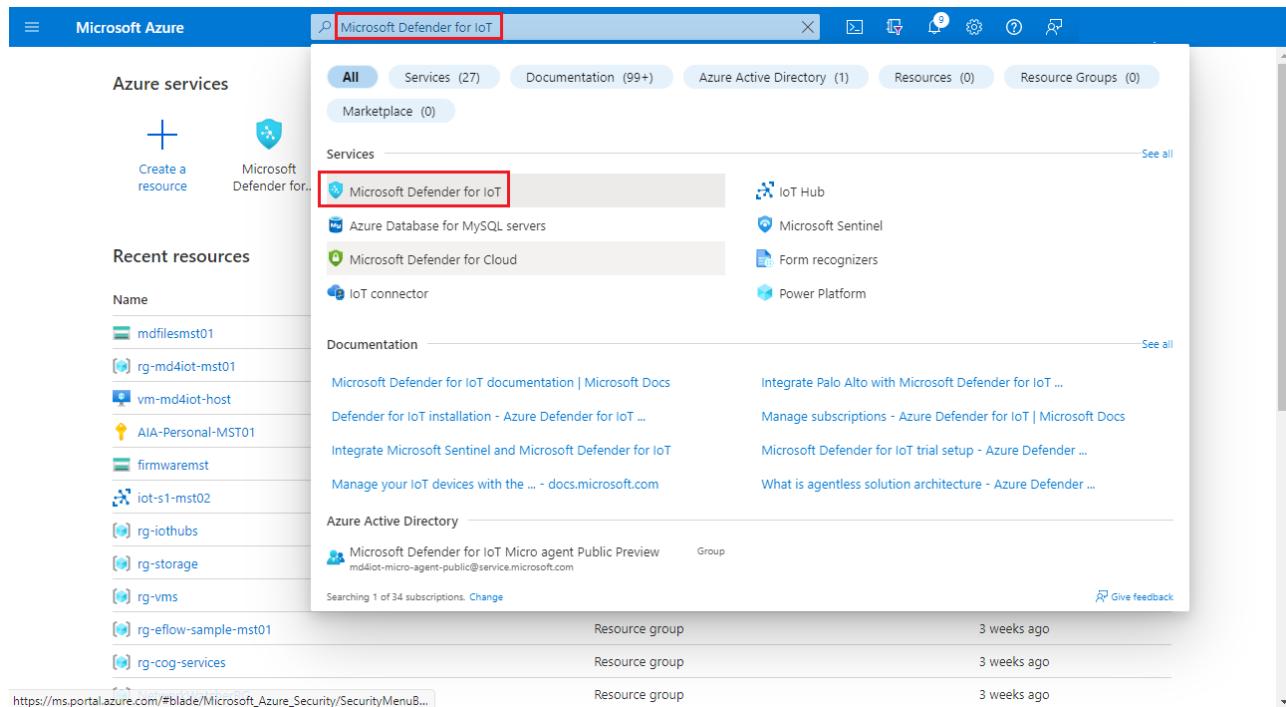
- Exercise 6: Integrate with Sentinel
 - Task 1: Enabling IoT to Integrate with Sentinel
 - Task 2: Connecting Data Connectors
 - Task 3: Acknowledge Alerts and Re-run PCAPs
 - Task 4: Sentinel interaction with IoT Incidents
 - Task 5: Kusto Query Language to Find Alert Details
- Exercise 7: Clean Up
 - Task 1: Delete resources
- Appendix 1: Troubleshooting

Exercise #1: Enabling Defender

Task 1: Enabling Microsoft Defender for IoT

You will execute this task on your physical machine, not on the Virtual Machine that you will use later in this HOL to host your Microsoft Defender for IoT sensors.

1. In the [Azure Portal](#), search for **Microsoft Defender for IoT**. Select **Microsoft Defender for IoT** in the popup window, to open the Microsoft Defender for IoT Page.



Microsoft Azure

Microsoft Defender for IoT

Azure services

Recent resources

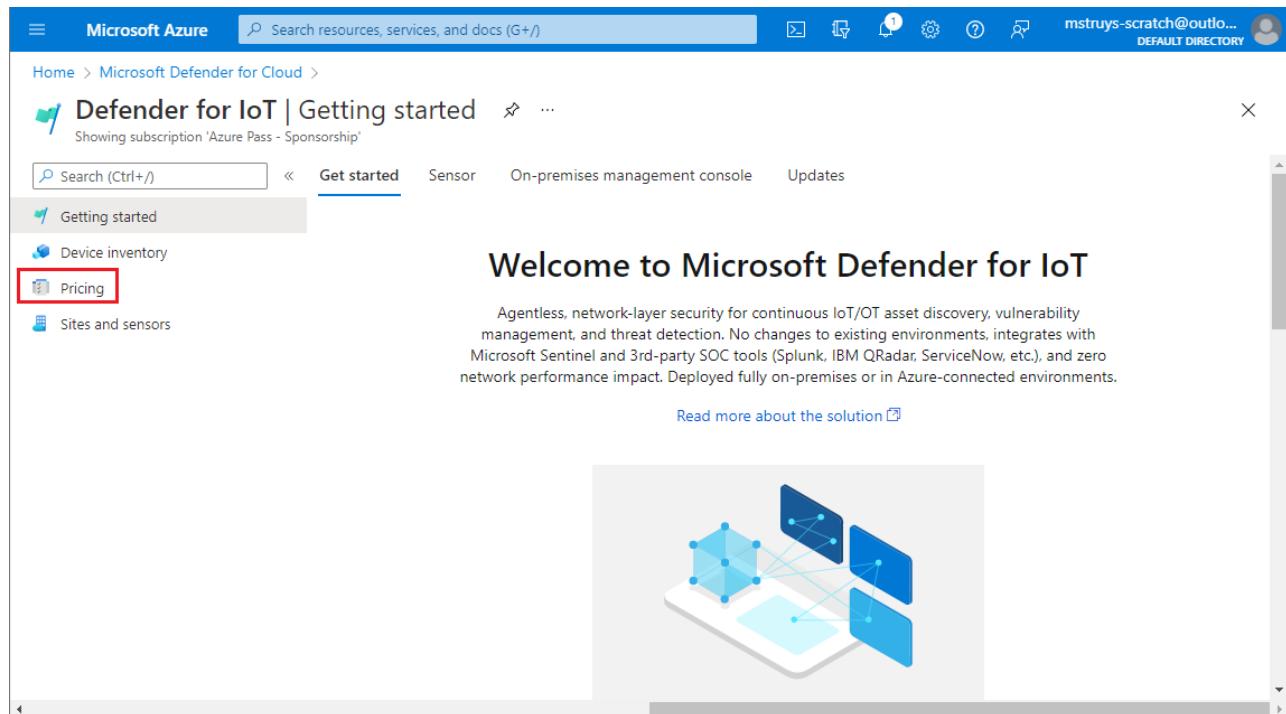
Documentation

Azure Active Directory

Give feedback

https://ms.portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade

2. On the Defender for IoT page, in the **Getting Started** section, select **pricing**.



Microsoft Azure Search resources, services, and docs (G+/)

Home > Microsoft Defender for Cloud > Defender for IoT | Getting started

Showing subscription 'Azure Pass - Sponsorship'

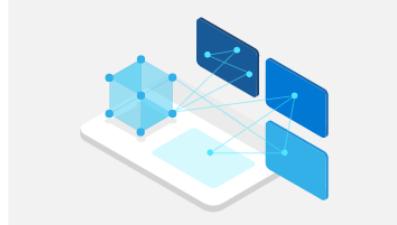
Get started Sensor On-premises management console Updates

Getting started Device inventory Pricing Sites and sensors

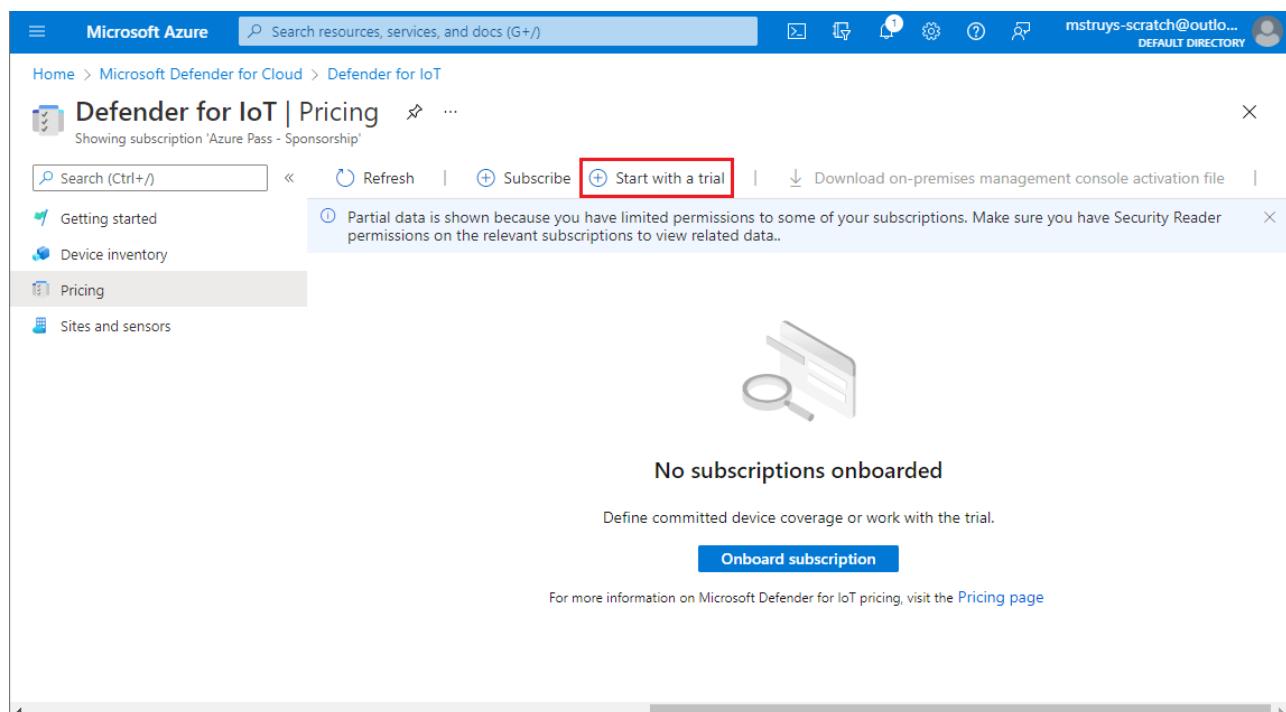
Welcome to Microsoft Defender for IoT

Agentless, network-layer security for continuous IoT/OT asset discovery, vulnerability management, and threat detection. No changes to existing environments, integrates with Microsoft Sentinel and 3rd-party SOC tools (Splunk, IBM QRadar, ServiceNow, etc.), and zero network performance impact. Deployed fully on-premises or in Azure-connected environments.

Read more about the solution



3. On the **Pricing** page, select **Start with a trial**.



Microsoft Azure Search resources, services, and docs (G+/)

Home > Microsoft Defender for Cloud > Defender for IoT

Showing subscription 'Azure Pass - Sponsorship'

Defender for IoT | Pricing

Getting started Device inventory Pricing Sites and sensors

Refresh Subscribe **+ Start with a trial** Download on-premises management console activation file

Partial data is shown because you have limited permissions to some of your subscriptions. Make sure you have Security Reader permissions on the relevant subscriptions to view related data.



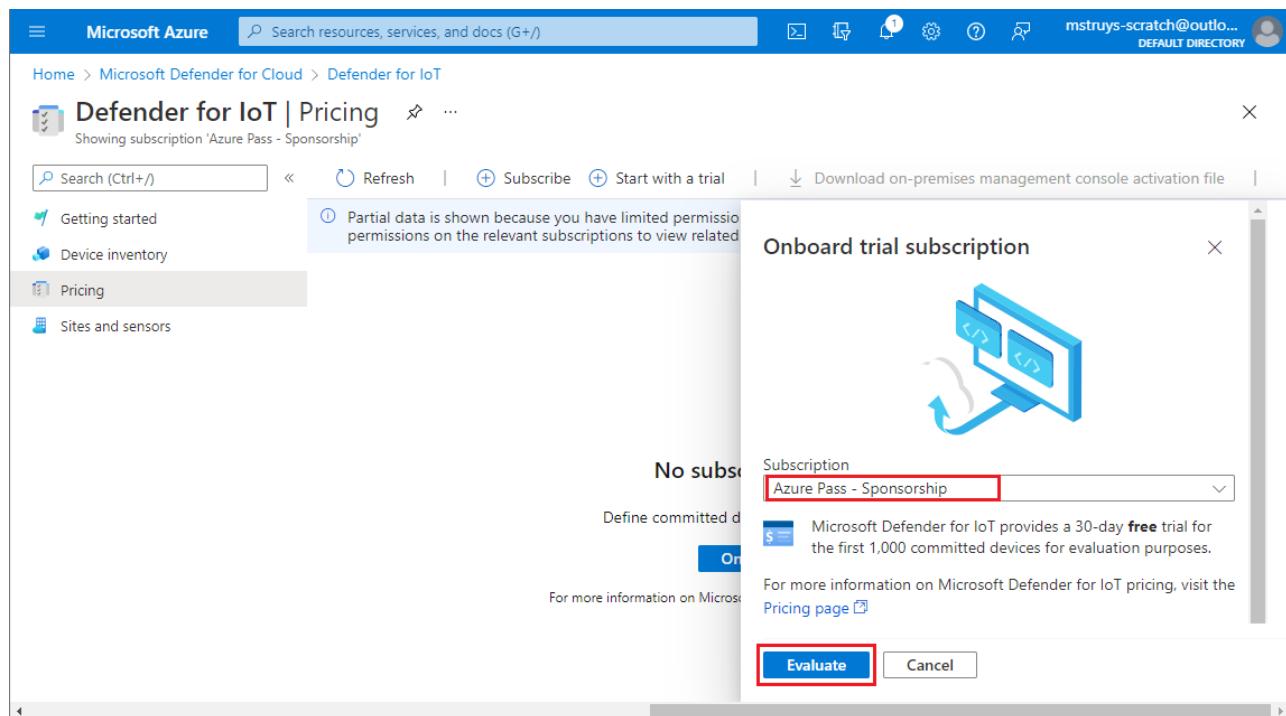
No subscriptions onboarded

Define committed device coverage or work with the trial.

Onboard subscription

For more information on Microsoft Defender for IoT pricing, visit the [Pricing page](#)

4. In the popup screen leave all defaults (make sure you are using the same subscription you have been using for this lab) and click **Evaluate**, followed by **Confirm**.



You now have a valid Microsoft Defender for IoT Trial with 1000 committed devices. These devices represent 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.

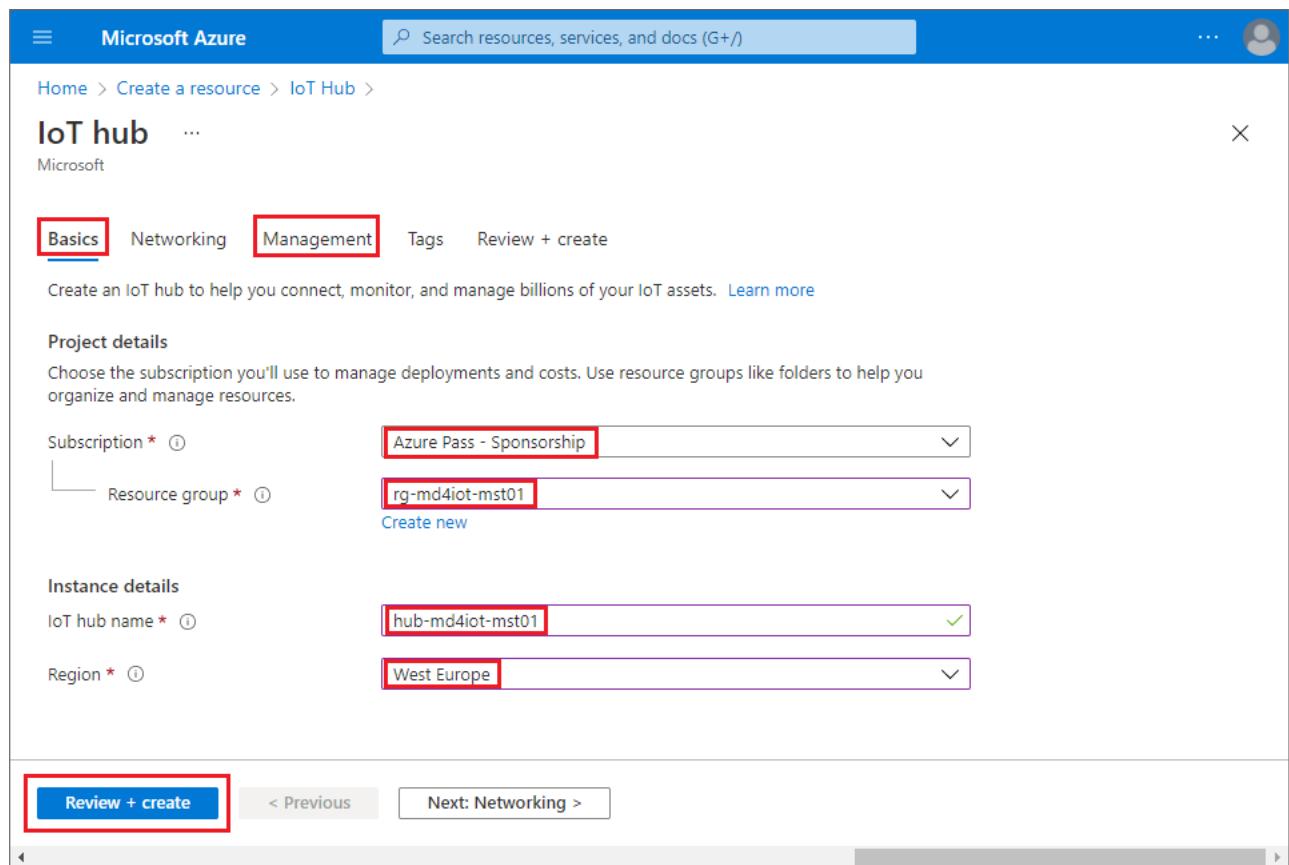
Task 2: Create an IoT Hub:

During this HOL you will work both with an online sensor and an offline sensor. The offline sensor can operate completely disconnected, but the online sensor needs to be connected to an Azure IoT Hub. Before onboarding your sensors you will create an IoT Hub for your online sensor to connect to. You will execute this task on your physical machine, not in the Virtual Machine that we will use later in this HOL to host your Microsoft Defender for IoT sensors.

1. Go to the resource group you created for this training. In the Overview panel, click on **+ Create** 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 working on.
- **Resource Group:** Should be the resource group created in previous step.
- **IoT Hub Name:** hub-md4iot+**SUFFIX**
- **Region:** A region close to your physical location (e.g. West Europe).



Microsoft Azure

Search resources, services, and docs (G+/-)

Home > Create a resource > IoT Hub >

IoT hub

Microsoft

Basics Networking Management Tags Review + create

Create an IoT hub to help you connect, monitor, and manage billions of your IoT assets. [Learn more](#)

Project details

Choose the subscription you'll use to manage deployments and costs. Use resource groups like folders to help you organize and manage resources.

Subscription * ⓘ Azure Pass - Sponsorship

Resource group * ⓘ rg-md4iot-mst01

Create new

Instance details

IoT hub name * ⓘ hub-md4iot-mst01

Region * ⓘ West Europe

Review + create < Previous Next: Networking >

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

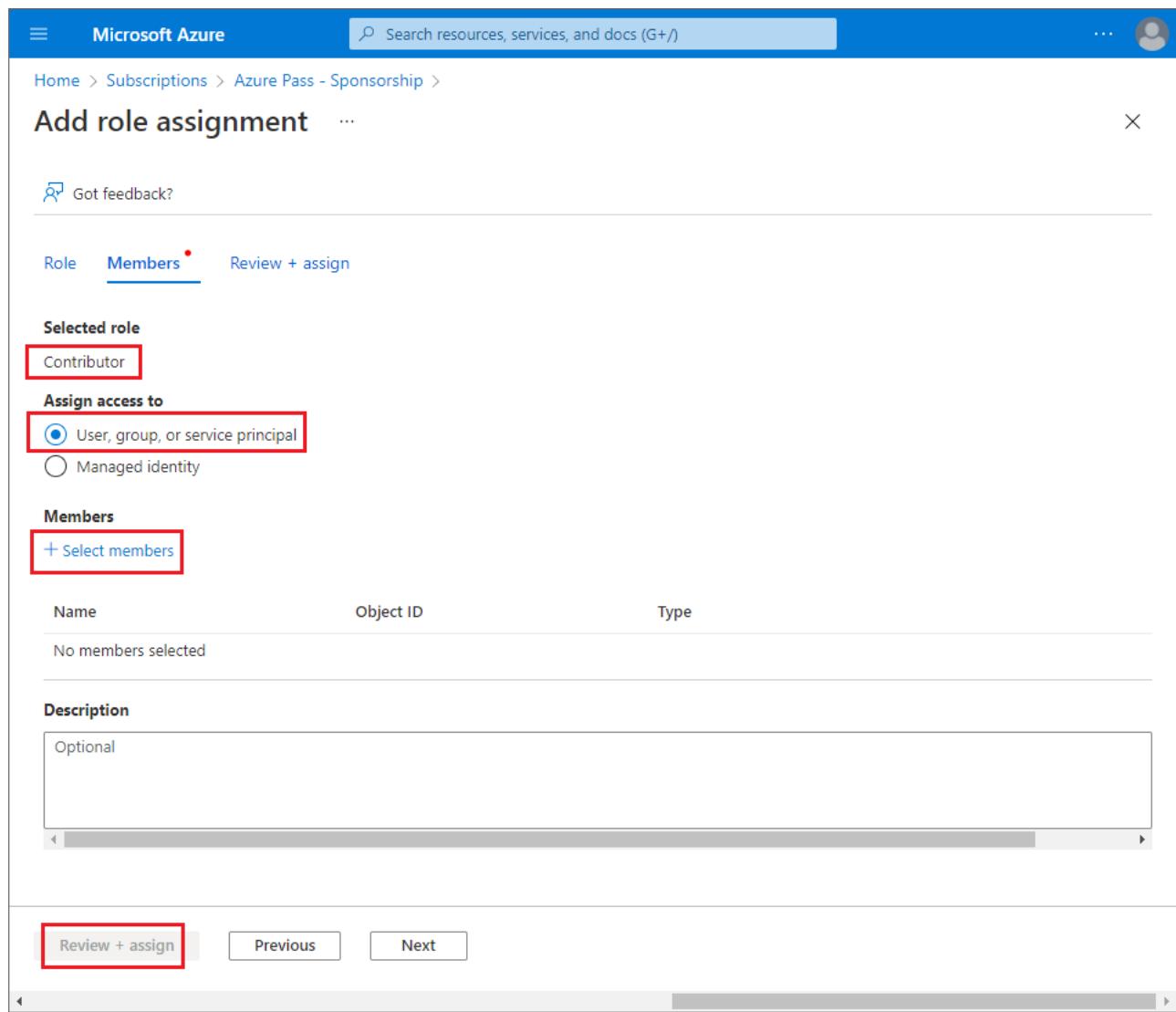
4. Finally, click **Review + create**, once validation is completed, click **Create**.

5. While the IoT Hub is creating , in the 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 members:** search for the email you are using in this subscription. Select that email and click **Select**.

6. Click **Review + assign** and again **Review + assign**.

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



The screenshot shows the 'Add role assignment' page in the Microsoft Azure portal. The 'Members' tab is selected. The 'Selected role' dropdown is set to 'Contributor'. The 'Assign access to' section has a radio button selected for 'User, group, or service principal'. The 'Members' section contains a button labeled '+ Select members'. At the bottom, the 'Review + assign' button is highlighted with a red box. Other buttons like 'Previous' and 'Next' are also visible.

Task 3: Onboarding sensors

For the hands-on lab we will work with two type of sensors, an offline sensor that does not need to be connected to the public Internet and an online sensor that is connected to Azure. In the next steps we will begin by onboarding the offline sensor. You will execute most of this task on your physical machine, not in the Virtual Machine that we will use later in this HOL to host your Microsoft Defender for IoT sensors.

1. Go back to Microsoft Defender for IoT to create the sensors. You can find it by searching for **Microsoft Defender for IoT** in the Azure Portal.
2. You can download the latest sensor iso image here (from the **Sensor** section). You **already did this step** as a prerequisite in the **Before HOL Section**. The ISO file is already available in your VM so you don't have to download it to your VM right now. However, you need to know where to find the ISO file. In the **Getting Started** section, select **Sensor**, then pick the **10.5.5 (Stable) and above - Recommended** version. To download it, you would click **Download**. This results in the ISO file being downloaded to your physical device.

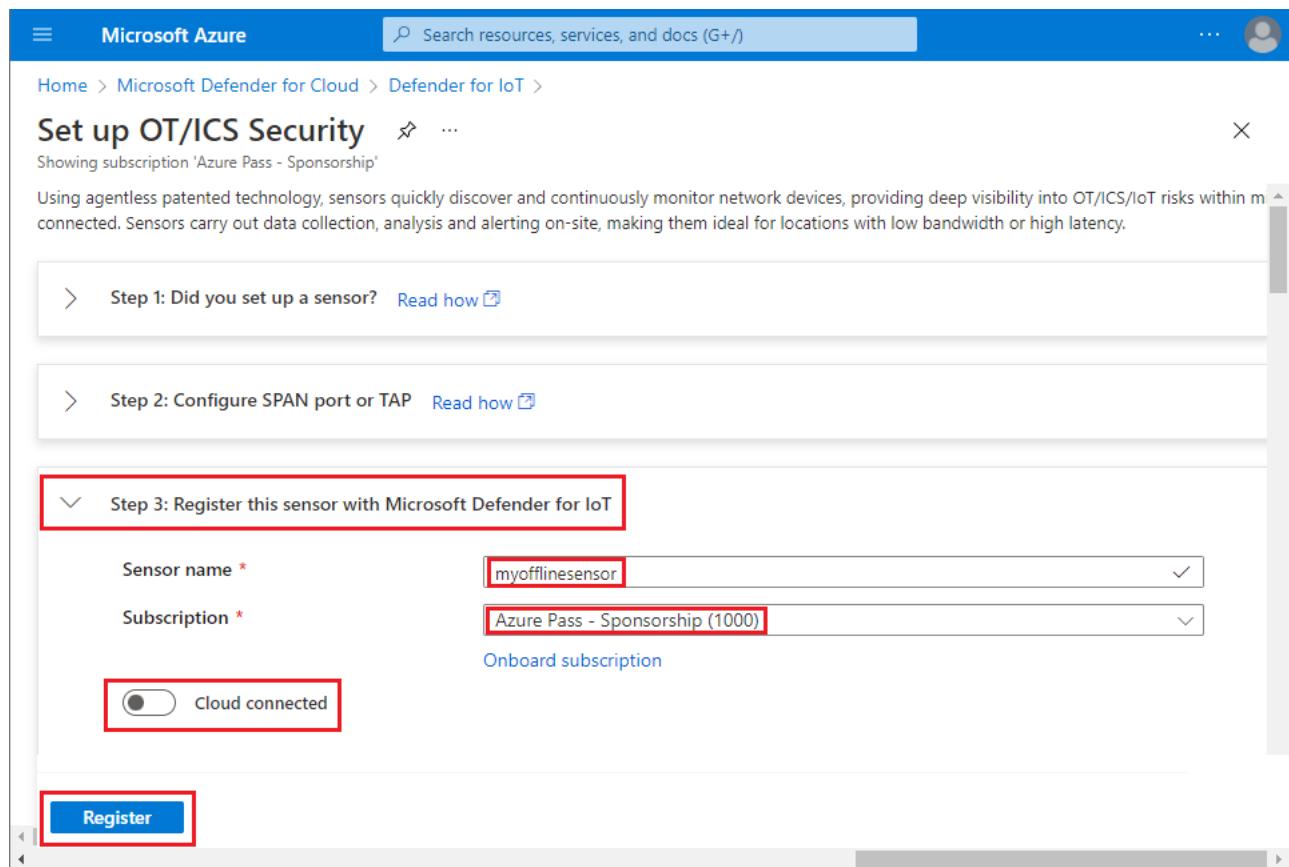
Did you already set up a sensor?
Proceed by onboarding your sensor with Microsoft Defender for IoT.
[Set up OT/ICS Security](#)

NOTE: At this moment, you might see a Window asking for contact details. You don't have to provide your contact details. Just go to the bottom of the windows and click on **Continue without submitting**.

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

There are no sensors to display

4. In the Setup OT/ICS Security screen, expand step 3 and set the following values: Sensor name = **myofflinesensor**, select your subscription and disable **Cloud Connected**. Click **Register**.



Microsoft Azure

Search resources, services, and docs (G+)

Home > Microsoft Defender for Cloud > Defender for IoT > Set up OT/ICS Security

Showing subscription 'Azure Pass - Sponsorship'

Using agentless patented technology, sensors quickly discover and continuously monitor network devices, providing deep visibility into OT/ICS/IoT risks within my network. Sensors are connected. Sensors carry out data collection, analysis and alerting on-site, making them ideal for locations with low bandwidth or high latency.

Step 1: Did you set up a sensor? [Read how](#)

Step 2: Configure SPAN port or TAP [Read how](#)

Step 3: Register this sensor with Microsoft Defender for IoT

Sensor name * myofflinesensor

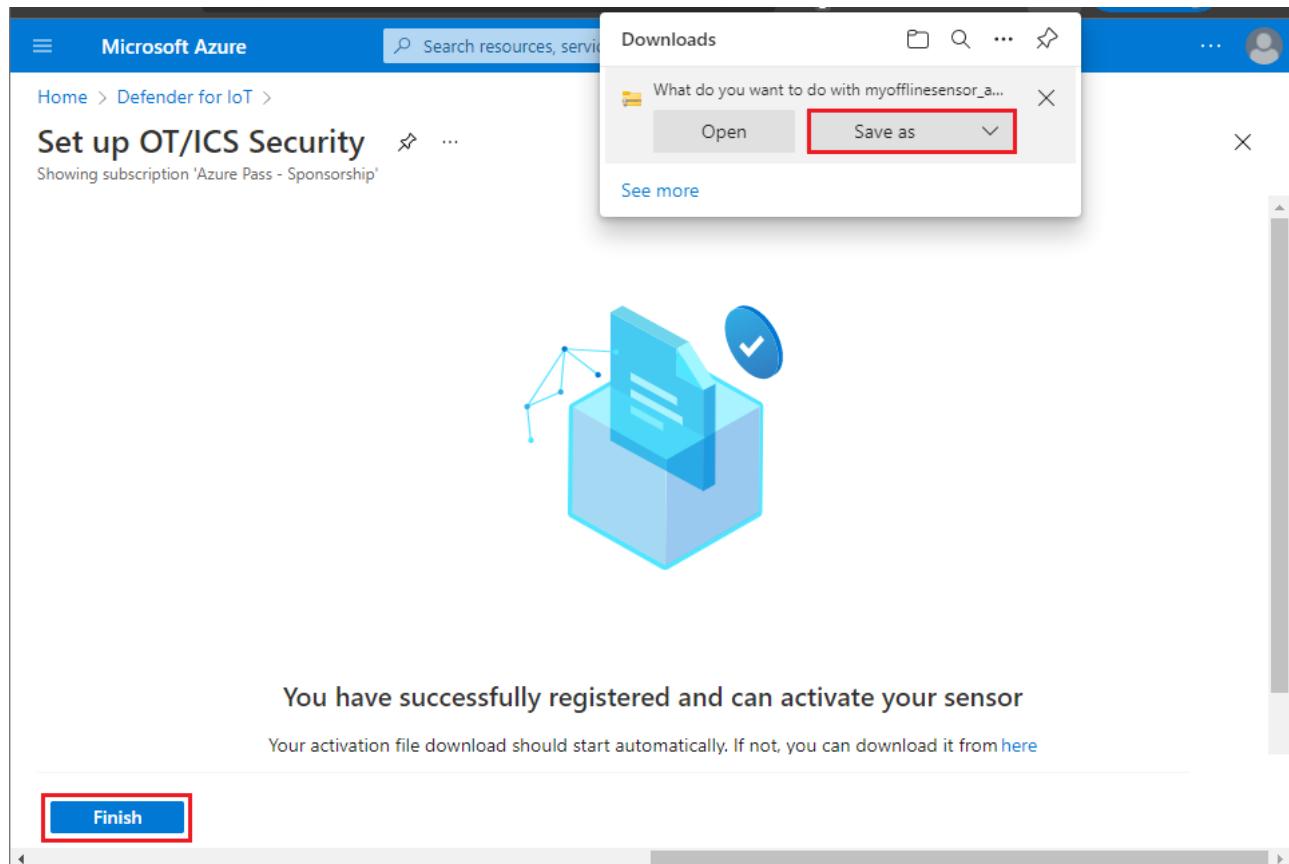
Subscription * Azure Pass - Sponsorship (1000)

Onboard subscription

Cloud connected

Register

5. In the next step, you will be prompted to save the sensor activation file. Save it with the default filename and click **Finish**.



Microsoft Azure

Search resources, services, and docs (G+)

Home > Defender for IoT > Set up OT/ICS Security

Showing subscription 'Azure Pass - Sponsorship'

Downloads

What do you want to do with myofflinesensor_a...

Open Save as

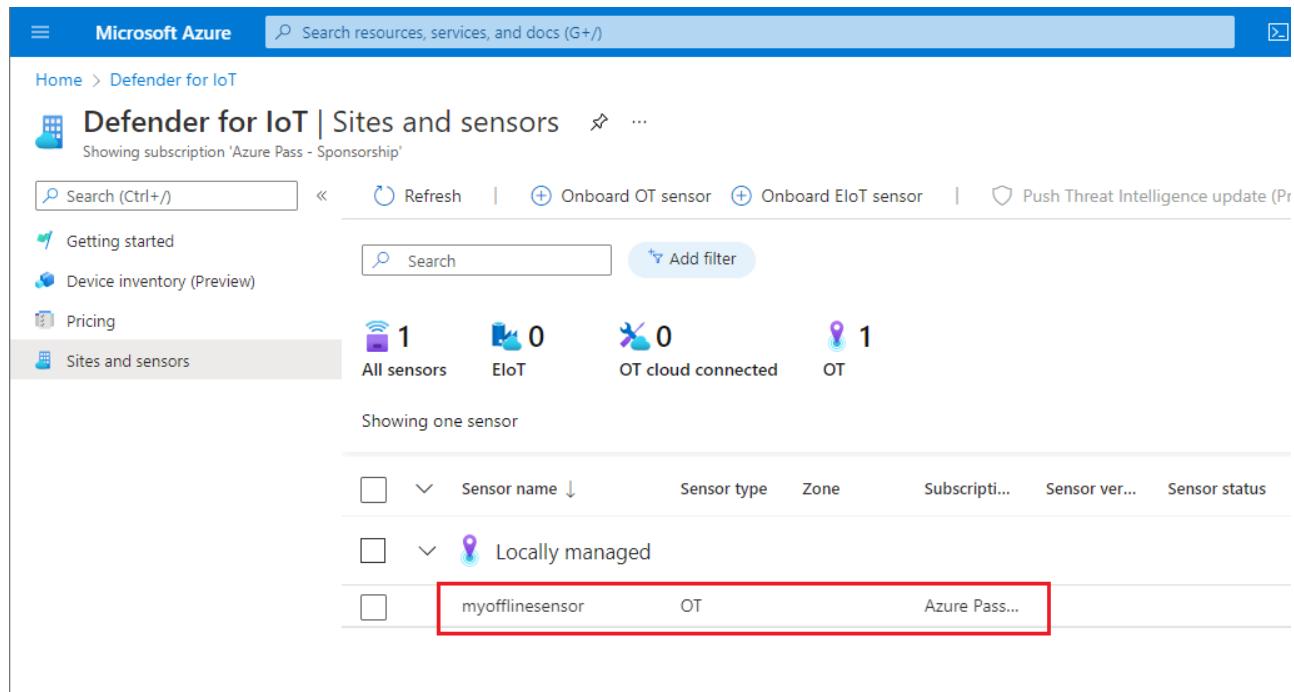
See more

You have successfully registered and can activate your sensor

Your activation file download should start automatically. If not, you can download it from [here](#)

Finish

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



Defender for IoT | Sites and sensors

Showing subscription 'Azure Pass - Sponsorship'

Search (Ctrl+ /) Refresh Onboard OT sensor Onboard EloT sensor Push Threat Intelligence update (Pr)

Getting started Device inventory (Preview) Add filter

Pricing

Sites and sensors

All sensors 1 EloT 0 OT cloud connected 0 OT 1

Showing one sensor

	Sensor name ↓	Sensor type	Zone	Subscription	Sensor ver...	Sensor status
Locally managed	myofflinesensor	OT	Azure Pass...			

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

- **Sensor name:** myonlinesensor
- **Subscription:** Select the subscription you are using for this lab.
- **Cloud Connected:** Enabled (= default).
- **Automatic Threat Intelligence Updates (Preview):** Enabled (= default).

Site Section

- **Hub:** Select the IoT Hub you created in the previous step.
- **Name:** MD4IoTHub. Usually this name will represent the site you will be analyzing, such as *Plant 1*.
- **Zone:** Default.

Set up OT/ICS Security

Showing subscription 'Azure Pass - Sponsorship'

Step 1: Did you set up a sensor? [Read how](#)

Step 2: Configure SPAN port or TAP [Read how](#)

Step 3: Register this sensor with Microsoft Defender for IoT

Sensor name * myonlinesensor

Subscription * Azure Pass - Sponsorship (1000)

Cloud connected

Automatic Threat Intelligence Updates

Site * Hub * hub-md4iot-mst01

Create IoT Hub for your site [Create](#)
It takes approximately 10 minutes for a new IoT Hub to be active and ready to use

Name * MD4IoTHub

Tags

Zone * default

Register

8. Click **Register**.

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

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

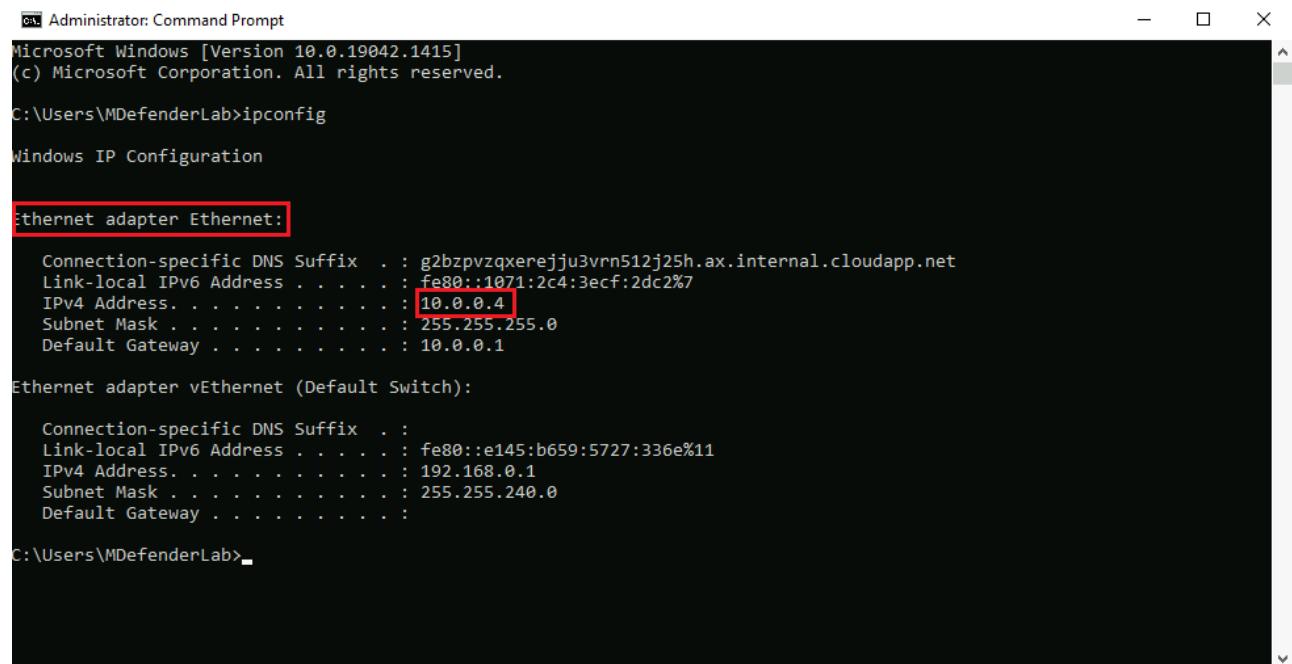
11. At this point you have 2 files downloaded locally (the activation files for your sensors). Since you are using RDP to connect to the Virtual Machine that will host your Microsoft Defender for IoT Sensor, you can simply copy the activation files and paste them in your VM using copy (ctrl-c) and paste (ctrl-v).

Exercise #2: Setting up your offline sensor

During this exercise you will create a new nested Virtual Machine inside the Virtual Machine that you created as part of the prerequisites.

Task 1: Set up your nested Virtual Machine

1. On the Windows 10 Virtual machine created previously, login with RDP if you have not done so before. Open a command prompt and run the command "ipconfig".



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.1415]
(c) Microsoft Corporation. All rights reserved.

C:\Users\MDefenderLab>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix  . : g2bzpvzxerejju3vrn512j25h.ax.internal.cloudapp.net
  Link-local IPv6 Address . . . . . : fe80::1071:2c4:3ecf:2dc2%7
  IPv4 Address. . . . . : 10.0.0.4
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.0.0.1

Ethernet adapter vEthernet (Default Switch):

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::e145:b659:5727:336e%11
  IPv4 Address. . . . . : 192.168.0.1
  Subnet Mask . . . . . : 255.255.240.0
  Default Gateway . . . . . :

C:\Users\MDefenderLab>
```

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 10.0.0.4, 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.

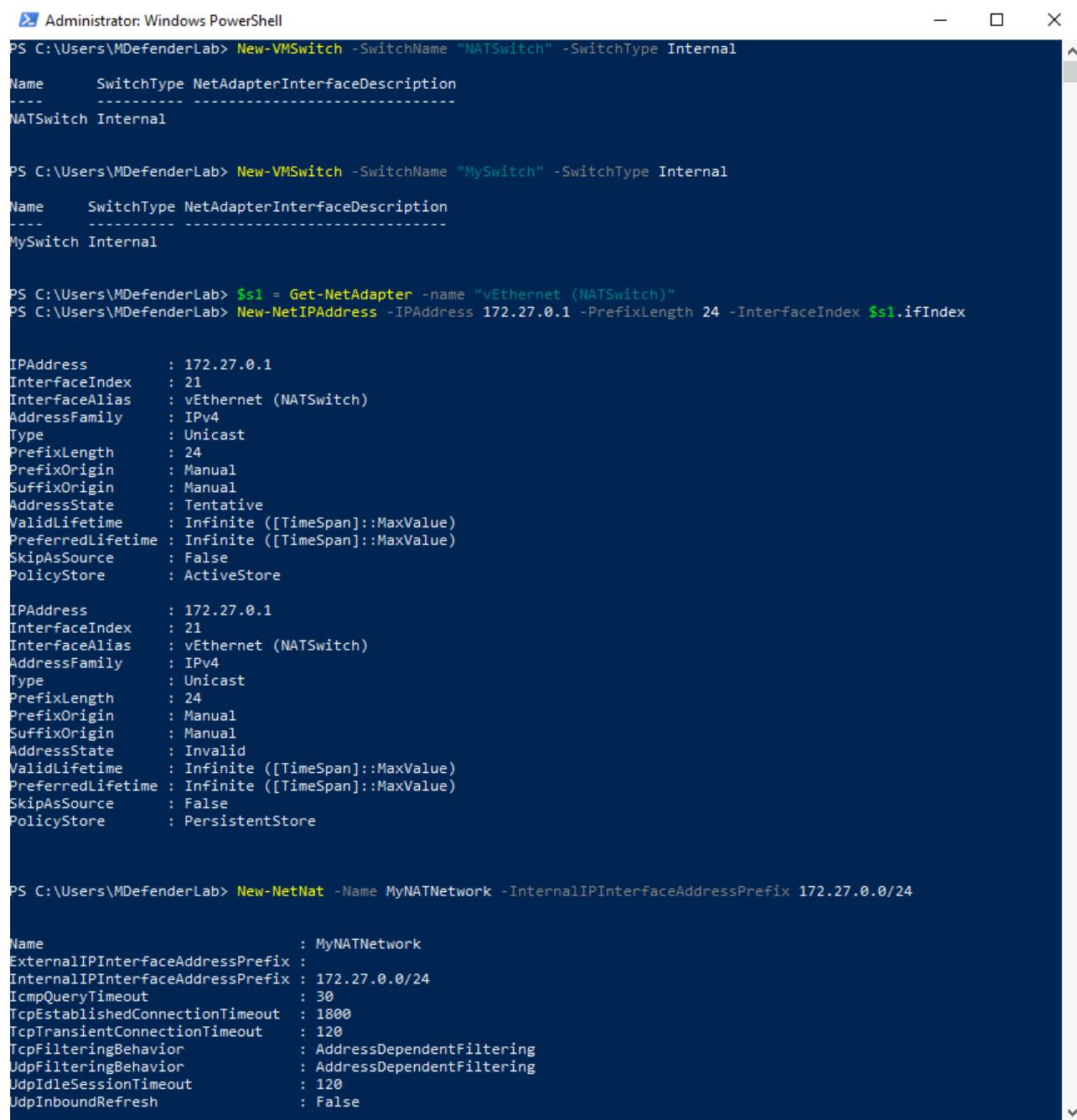
```
$s1 = Get-NetAdapter -name "vEthernet (NATswitch)"
```

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
```



The screenshot shows a Windows PowerShell window titled 'Administrator: Windows PowerShell' with the following command history:

```

PS C:\Users\MDefenderLab> New-VMswitch -SwitchName "NATSwitch" -SwitchType Internal
Name      SwitchType NetAdapterInterfaceDescription
----      ----- -----
NATSwitch Internal

PS C:\Users\MDefenderLab> New-VMswitch -SwitchName "MySwitch" -SwitchType Internal
Name      SwitchType NetAdapterInterfaceDescription
----      ----- -----
MySwitch Internal

PS C:\Users\MDefenderLab> $s1 = Get-NetAdapter -name "vEthernet (NATSwitch)"
PS C:\Users\MDefenderLab> New-NetIPAddress -IPAddress 172.27.0.1 -PrefixLength 24 -InterfaceIndex $s1.ifIndex

IPAddress      : 172.27.0.1
InterfaceIndex  : 21
InterfaceAlias  : vEthernet (NATSwitch)
AddressFamily   : IPv4
Type           : Unicast
PrefixLength   : 24
PrefixOrigin   : Manual
SuffixOrigin   : Manual
AddressState   : Tentative
ValidLifetime  : Infinite ([TimeSpan]::.MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::.MaxValue)
SkipAsSource   : False
PolicyStore    : ActiveStore

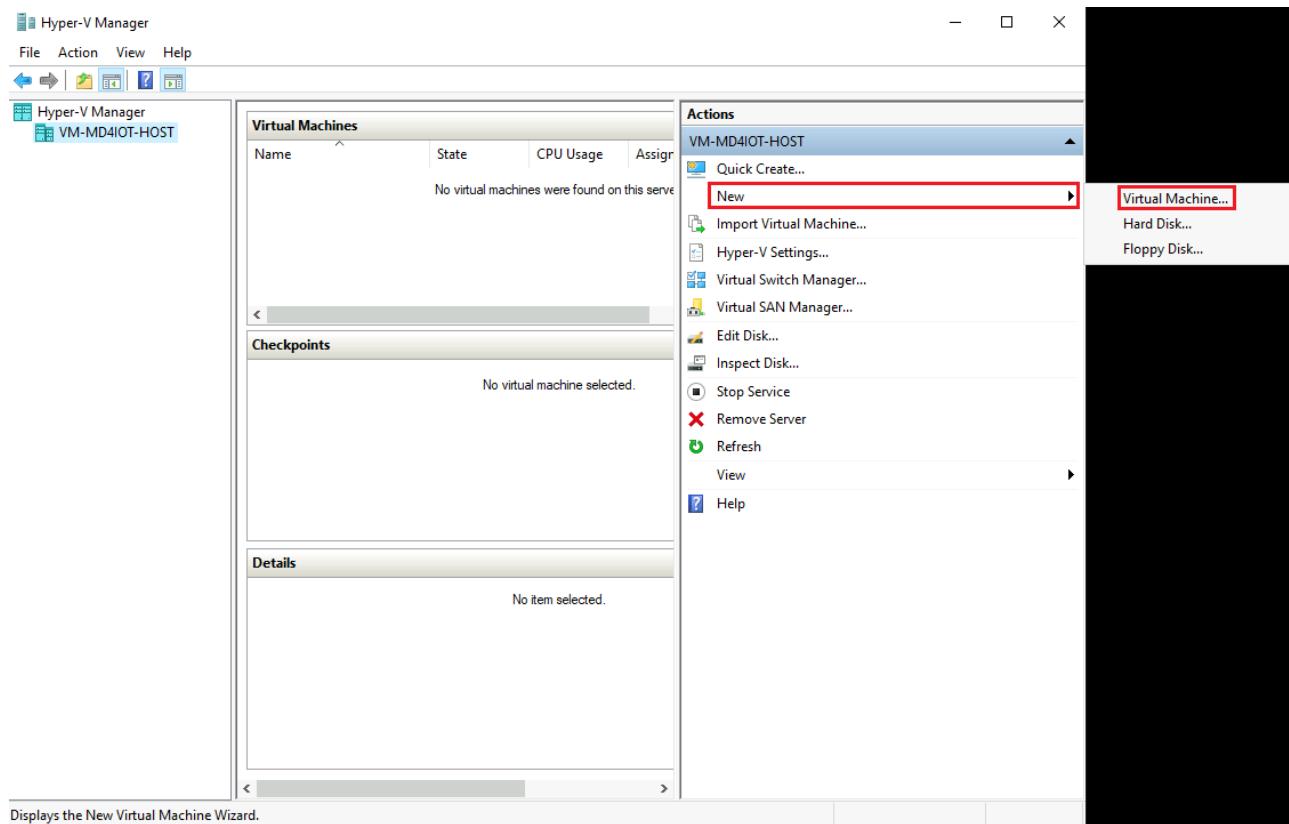
IPAddress      : 172.27.0.1
InterfaceIndex  : 21
InterfaceAlias  : vEthernet (NATSwitch)
AddressFamily   : IPv4
Type           : Unicast
PrefixLength   : 24
PrefixOrigin   : Manual
SuffixOrigin   : Manual
AddressState   : Invalid
ValidLifetime  : Infinite ([TimeSpan]::.MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::.MaxValue)
SkipAsSource   : False
PolicyStore    : PersistentStore

PS C:\Users\MDefenderLab> New-NetNat -Name MyNATNetwork -InternalIPInterfaceAddressPrefix 172.27.0.0/24

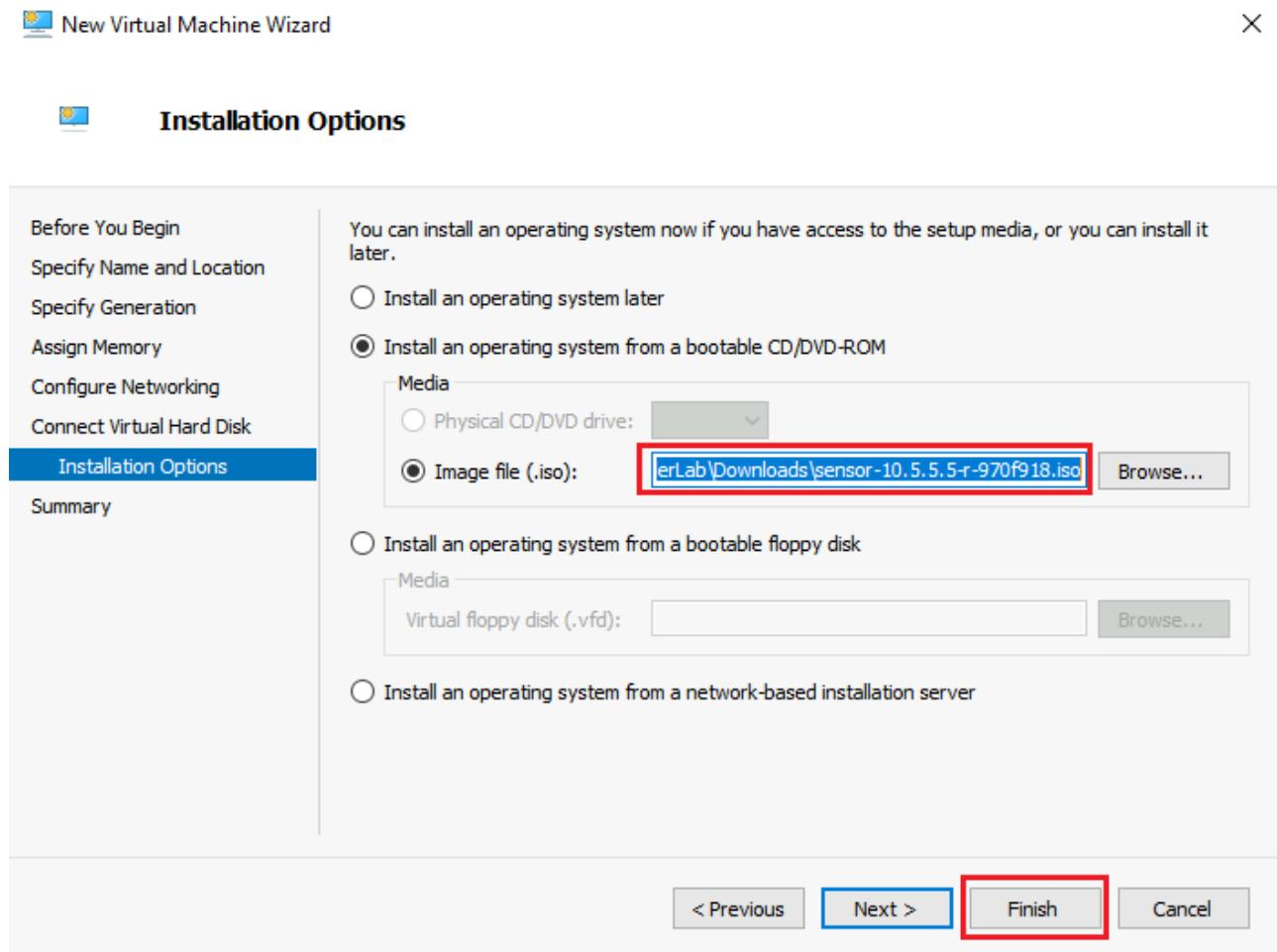
Name           : MyNATNetwork
ExternalIPInterfaceAddressPrefix :
InternalIPInterfaceAddressPrefix : 172.27.0.0/24
IcmpQueryTimeout      : 30
TcpEstablishedConnectionTimeout : 1800
TcpTransientConnectionTimeout : 120
TcpFilteringBehavior  : AddressDependentFiltering
UdpFilteringBehavior  : AddressDependentFiltering
UdpIdleSessionTimeout : 120
UdpInboundRefresh    : False

```

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



- In the first tab, assign the name **md4iotsensoroffline** to your VM, then click **Next**.
- **Specify Generation**, select **Generation 1**, click **Next** again.
- Change the memory to **8196MB**, click **Next**.
- **Configure Network** tab, select in **Connection**, **NATSwitch**, click **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 to the Azure defender .iso file that you downloaded in the prerequisites. Click **Finish**



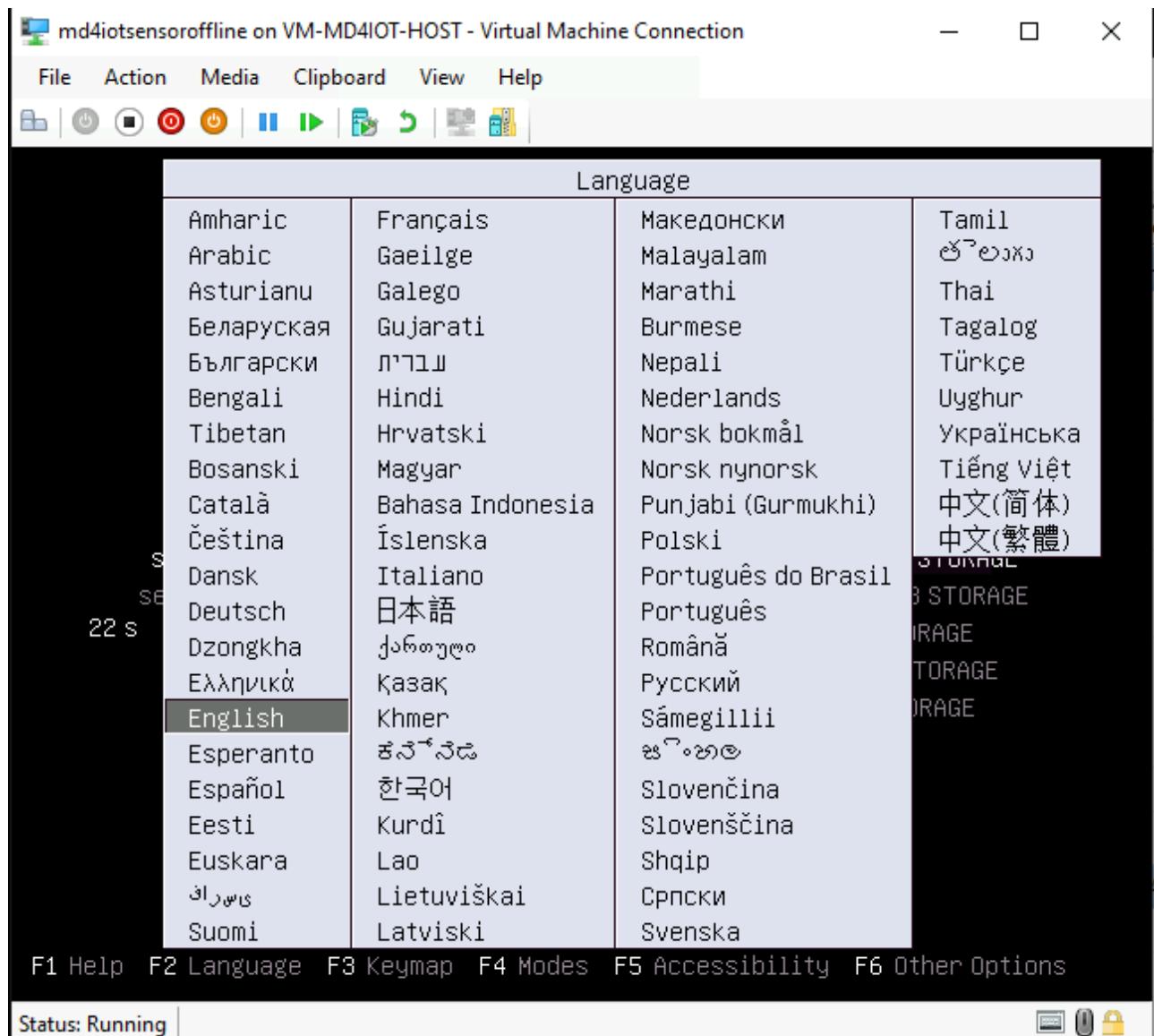
9. Right click on the Virtual machine that you just created, select **Settings** in the **Add Hardware** section and select **Network Adapter**, followed by clicking on **Add**. Now select the virtual switch created previously with the name **My Switch**, and click **Apply**. Increase the Processor number from **1** to **4** Virtual Processors, click **Apply** and click **Ok**.

Task 2: Configure a Microsoft Defender for IoT offline sensor

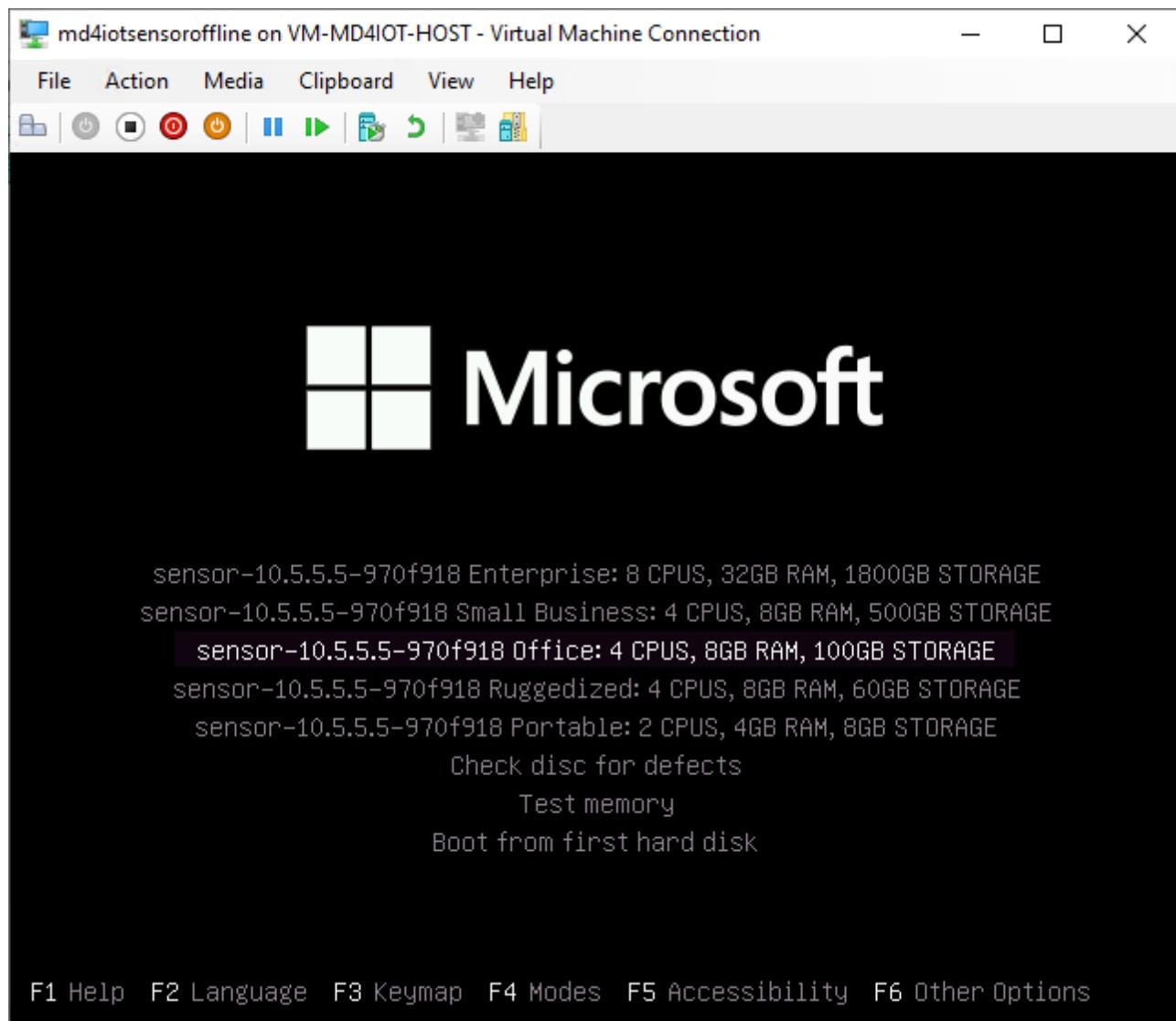
During this task we will configure Azure Defender based on the IPs highlighted before, this first configuration will be based on an offline sensor.

1. In the Hyper-V Manager, find the **Connect...** in the lower right hand of the screen and click on it, and in the newly opened VM connection window click **Start**.
2. When you connect to the Ubuntu VM you should see the following screen to start the configuration process.

Note!: If you don't see the 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. The timeout period is relatively short so make sure you connect immediately to the nested VM and select the language and the sensor type (in Task 2).



3. Press **Enter** for English.
4. Select the third option (*Office 4CPUs*) and press **Enter**.



At this moment, the offline sensor will be installed (including its operating system). This installation takes some time, expect it to run for approximately 15 minutes.

5. As part of the installation process, you will be asked to provide some parameters, it is **VERY IMPORTANT** you paid attention to the previous task because you will use the network information you captured before. This information 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 intentionally 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**.

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

```
configure hardware profile
- portable
- office
- enterprise
- ruggedized
- small business
- corporate
Please type hardware profile: office

configure management network interface
- docker0
- eth0
- eth1
- veth2138163
Please type management network interface: eth0

configure management network IP address
Please type management network IP address: 192.168.0.50

configure subnet mask
Please type subnet mask: 255.255.255.0

configure DNS
Please type DNS: 8.8.8.8

configure default gateway IP address
Please type default gateway IP address: 192.168.0.1
Or 192.168.0.2 for "Offline"

configure input interface(s)
- docker0
- eth1
- veth2138163
Please type your selected item(s) (separate with ","): eth1

configure bridge interface(s)
- docker0
- eth0
- eth1
- veth2138163
Please type your selected item(s) (separate with ","): _
```

Leave the Bridge blank

Now the installation will continue running for another 10-15 minutes.

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

```

md4iotsonline on VM-MD4IOT-HOST - Virtual Machine Connection
File Action Media Clipboard View Help
disabling Horizon Agent 2 component...
enabling Profiling Service component...
disabling Squid Proxy component...
restarting watchdog ...
watchdog started

Usage:
kill [options] <pid> [...]

Options:
<pid> [...]           send signal to every <pid> listed
--signal, -s, --signal <signal>      specify the <signal> to be sent
-l, --list=[<signal>]    list all signal names, or convert one to a name
-L, --table            list all signal names in a nice table

-h, --help             display this help and exit
-V, --version          output version information and exit

For more details see kill(1).
Command 'sudo kill -9' returned non-zero exit status 1.
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for rsyslog (8.32.0-1ubuntu4) ...
Processing triggers for fontconfig (2.12.6-0ubuntu2) ...
xsense debian installation returned the following exit code: 0
finished installing xsense debian
running cyberx-xsense-prepare-for-production-offline --automated --prompt-for-password --no-restart
starting to show prompt title: Credentials message:
-----Credentials-----
This is your generated login information
appliance ID: 6D7CA15F-1C9A-8944-BAC4-AE45656462A3
username: cyberx
password: :t^,lU@,gxr10erf

IMPORTANT - this is the only time this information will be displayed
please safely backup this information and press enter to continue
press Enter to continue...
Finished showing prompt
starting to show prompt title: Credentials message:
-----Credentials-----
This is your generated login information
appliance ID: 6D7CA15F-1C9A-8944-BAC4-AE45656462A3
username: support
password: qec28Ubrpmcial^I

IMPORTANT - this is the only time this information will be displayed
please safely backup this information and press enter to continue
press Enter to continue...
Status: Running

```

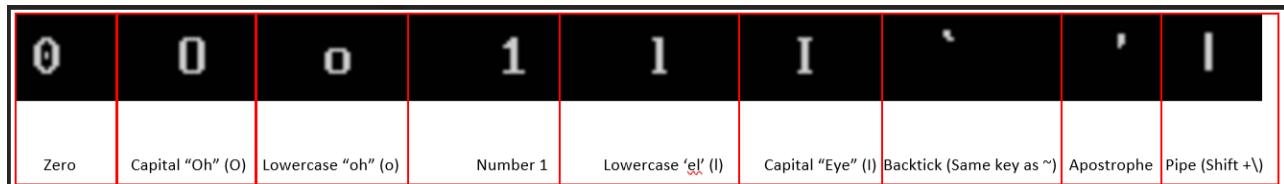
7. Once the installation finished you will ask to login, enter the credentials from previous step. In this screen you can also validate the IP, you will use that IP in your browser.

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 follow the troubleshooting guidance below.

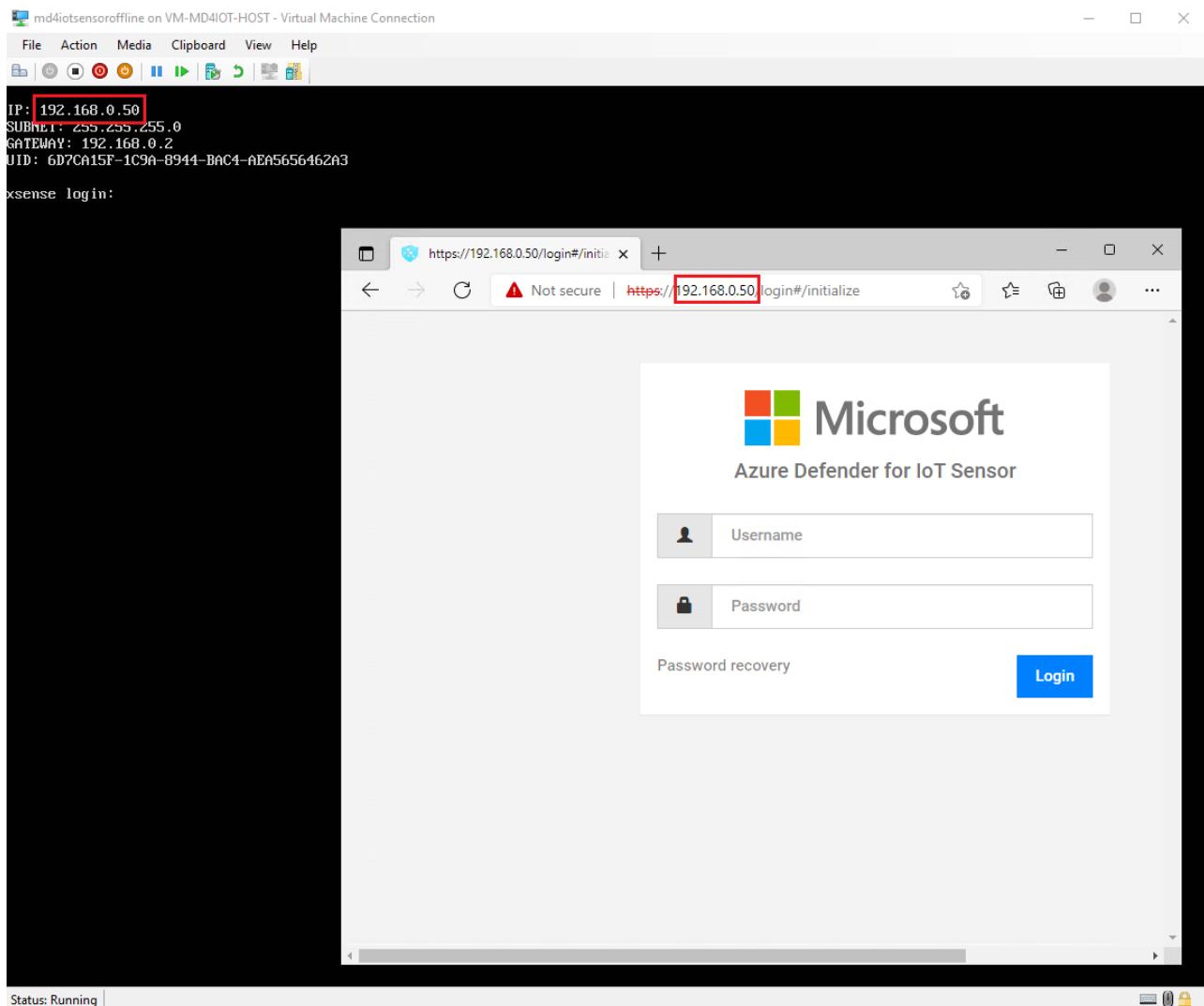
Troubleshooting Note: Once the installation is complete, you will be able to access Azure Defender Console. Check if you can open a cmd window, ping the IP Address you entered in the step 'Configure management network interface'. If the request times out, you will need to reconfigure this step again,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

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

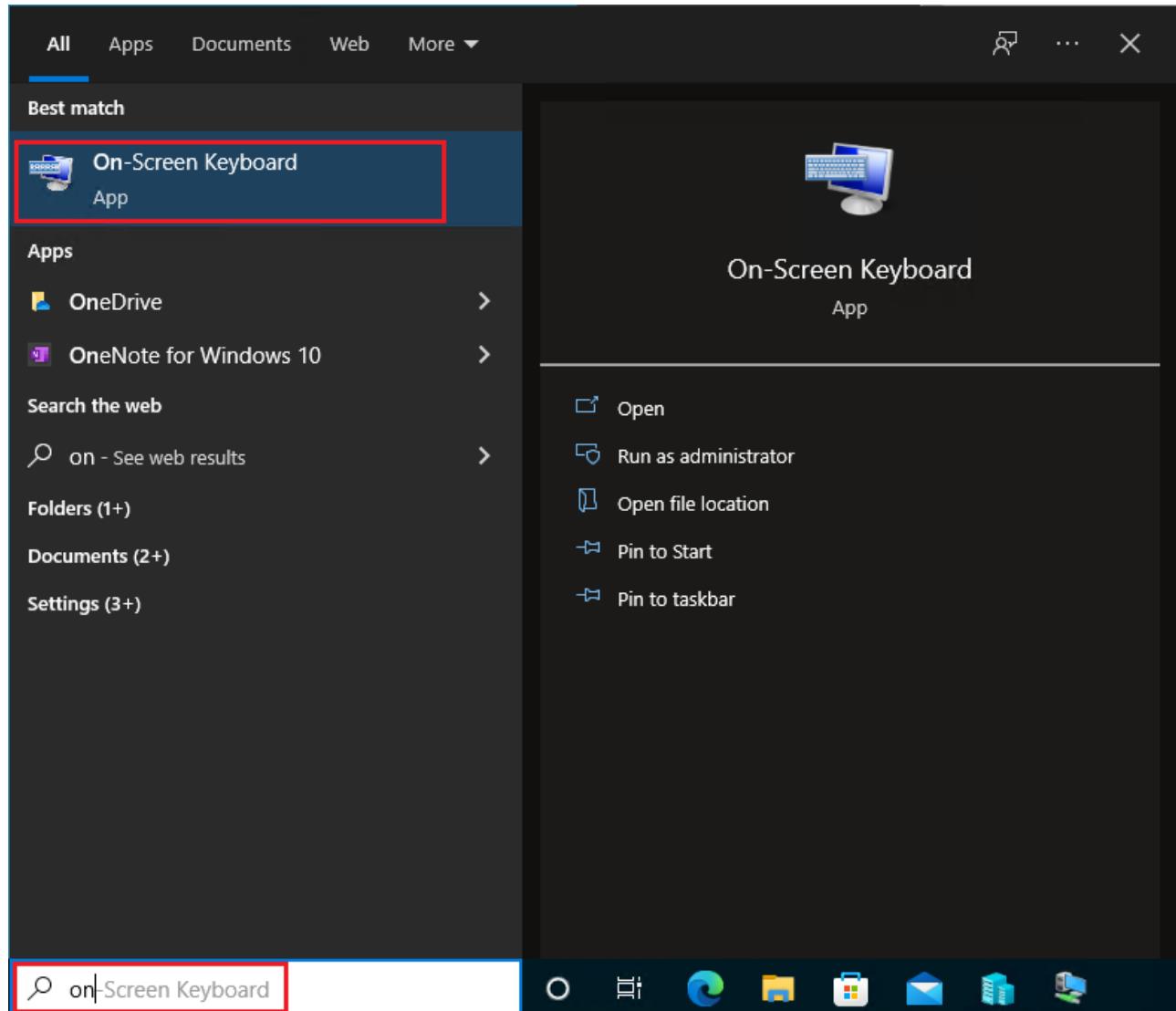
In the next steps you will be prompt to enter the password capture above, some characteres look alike but they are not, this image will help you to identify some of them.



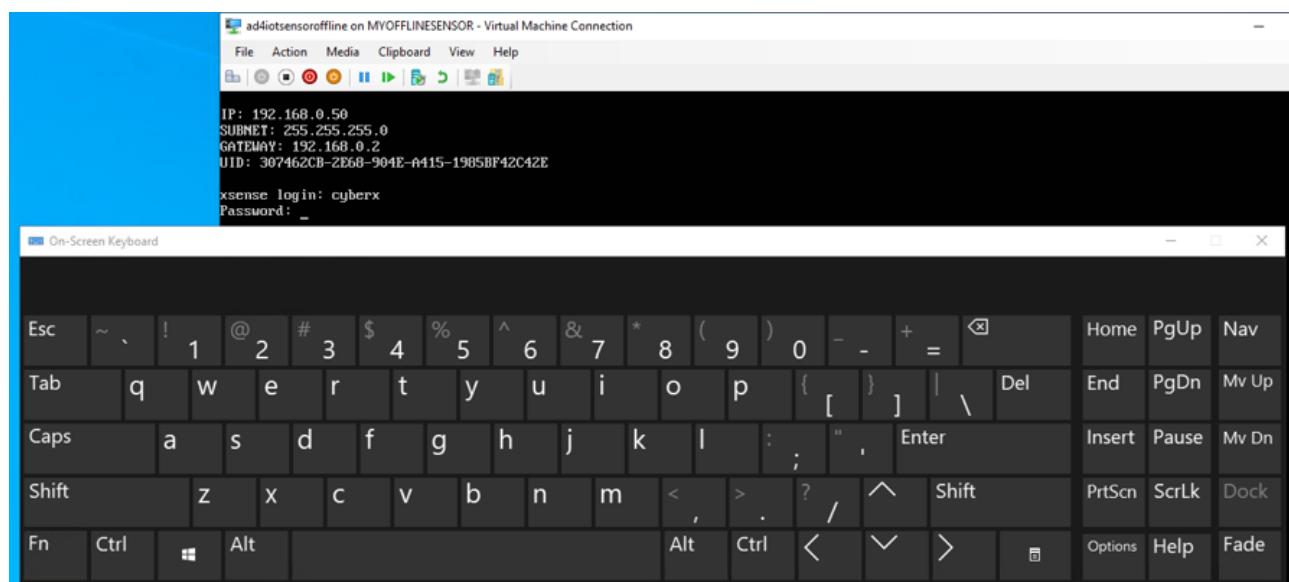
8. Login with the credentials provided in step 4.



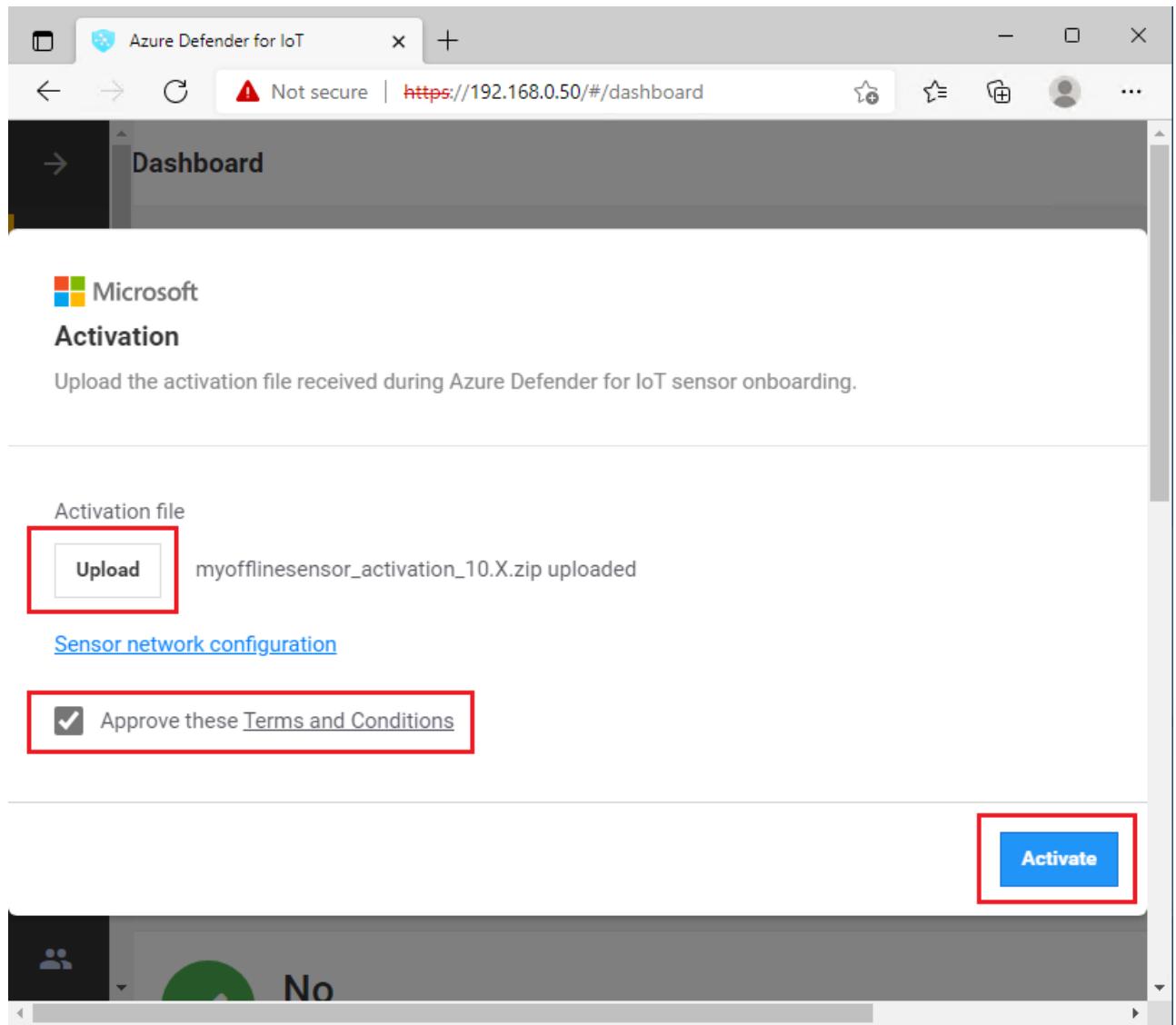
NOTE: the "md4iotsensoroffline" VM's keyboard layout is US by default, and it may not match the layout of your physical keyboard. To avoid issues when entering the password, you may use the windows 10 on-screen keyboard. To run it, type "osk" in the search box and click on "On-Screen Keyboard"...



...and use it to enter the credentials:

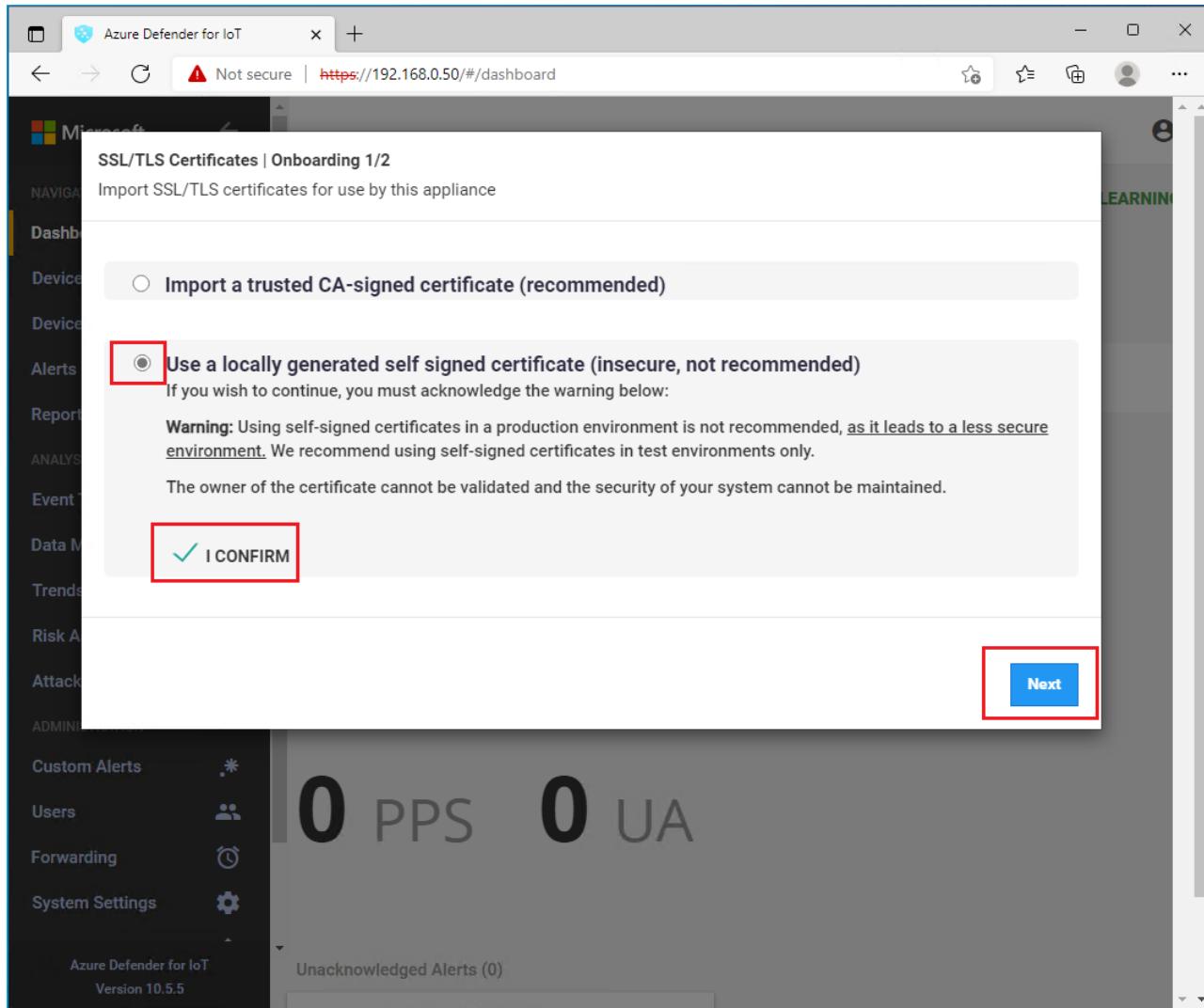


9. Next, you will be asked to activate the product, click **Upload**, then **Browse Files**, in your downloads folder select the file you downloaded from the Storage Explorer, in this example **myofflinesensor.zip**.



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

11. 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**.



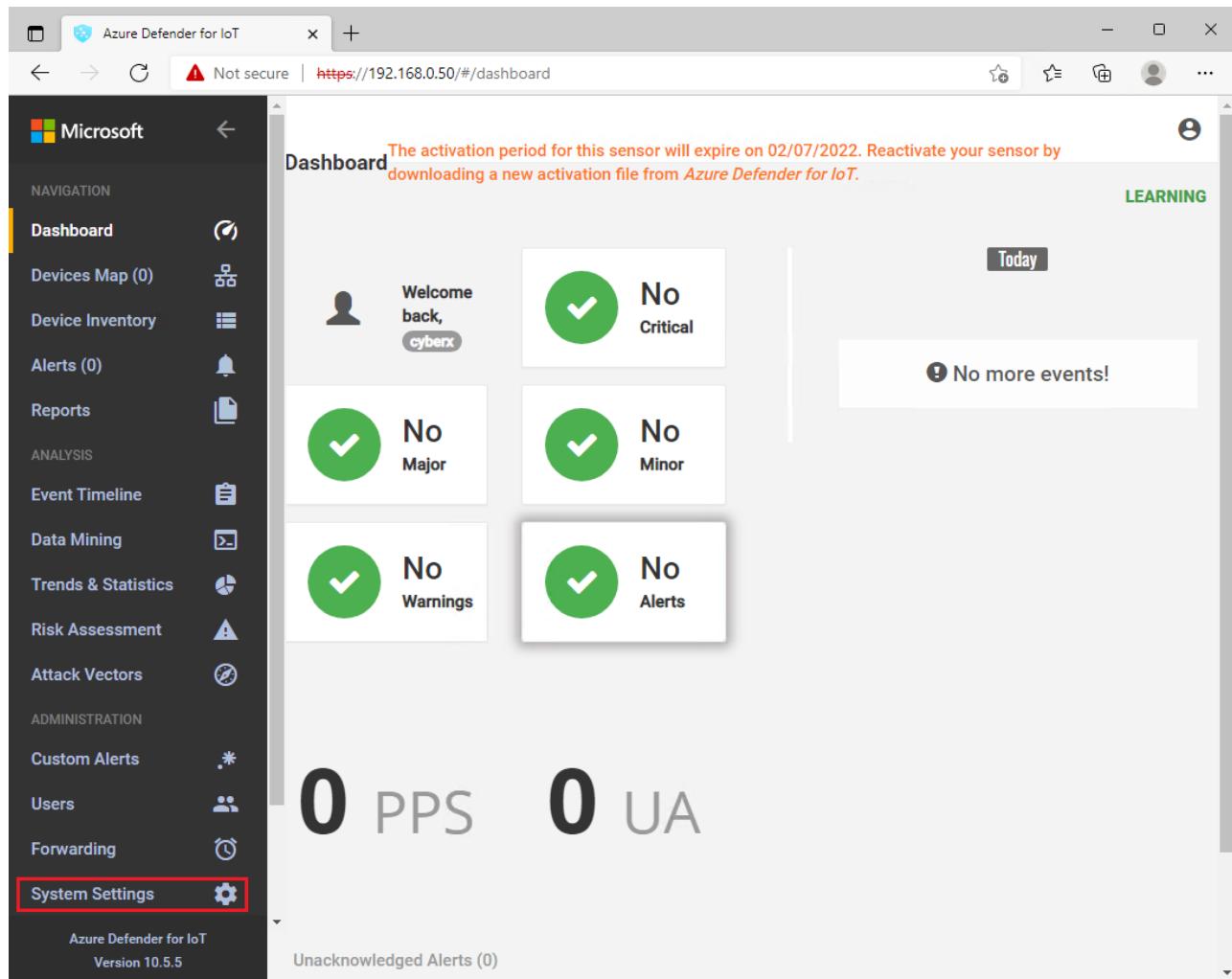
12. For this lab in the next step we will **Disable** the system wide validation. **Finish.**

13. 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.



The activation period for this sensor will expire on 02/07/2022. Reactivate your sensor by downloading a new activation file from Azure Defender for IoT.

Today

No more events!

0 PPS 0 UA

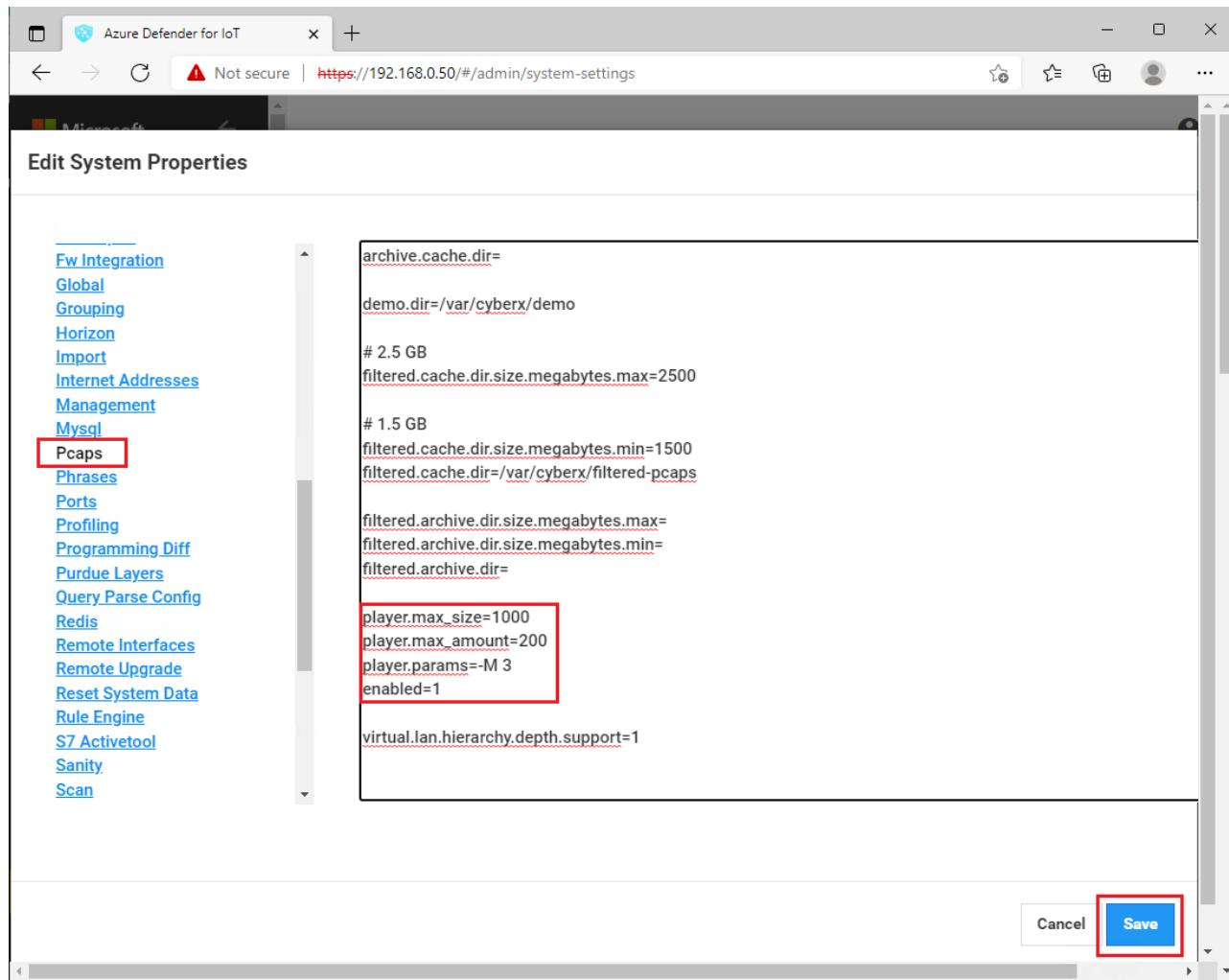
Unacknowledged Alerts (0)

2. Next, look for the icon **System Properties** on the right side. Click on the icon. You will see a pop up warning, click **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**

Amongst others, these settings enable the PCAP player and allow it to playback faster than real-time.



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

5. At this point you should see the Pcap Player available (you can close the **Edit System Properties** screen now by clicking the **Cancel** button):

Enabled engines - 5 of 5 available

PCAP Player
upload and replay PCAP files

Upload Play All Clear All

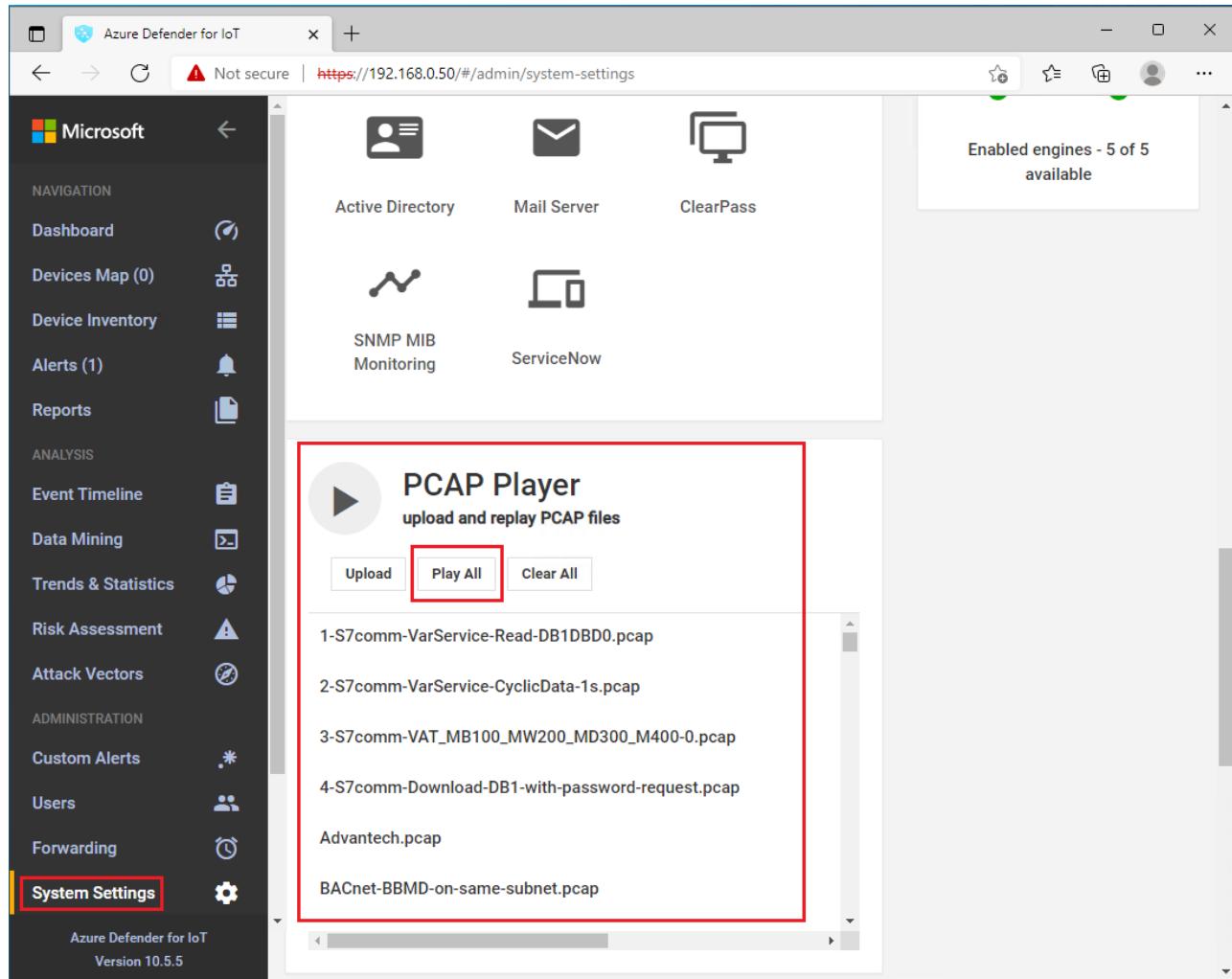
Engines
controlling engines

Protocol Violation
Enabled
Packet Structure or Field Values That Don't Comply with
Protocol Specification

Policy Violation
Enabled

Task 2: Pcap Files

1. In a previous step you already downloaded a **holpcaps.zip** file from the Storage account. It should be in your Azure Virtual Machine's **Downloads** folder.
2. Unzip **holpcaps.zip**
3. 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.
4. At this point you should see all the files uploaded.



The screenshot shows the Azure Defender for IoT interface. The left sidebar has a red box around the 'System Settings' option. The main content area has a red box around the 'PCAP Player' section. Inside the 'PCAP Player' section, the 'Play All' button is highlighted with a red box. The list of PCAP files is as follows:

- 1-S7comm-VarService-Read-DB1DBD0.pcap
- 2-S7comm-VarService-CyclicData-1s.pcap
- 3-S7comm-VAT_MB100_MW200_MD300_M400-0.pcap
- 4-S7comm-Download-DB1-with-password-request.pcap
- Advantech.pcap
- BACnet-BBMD-on-same-subnet.pcap

5. 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

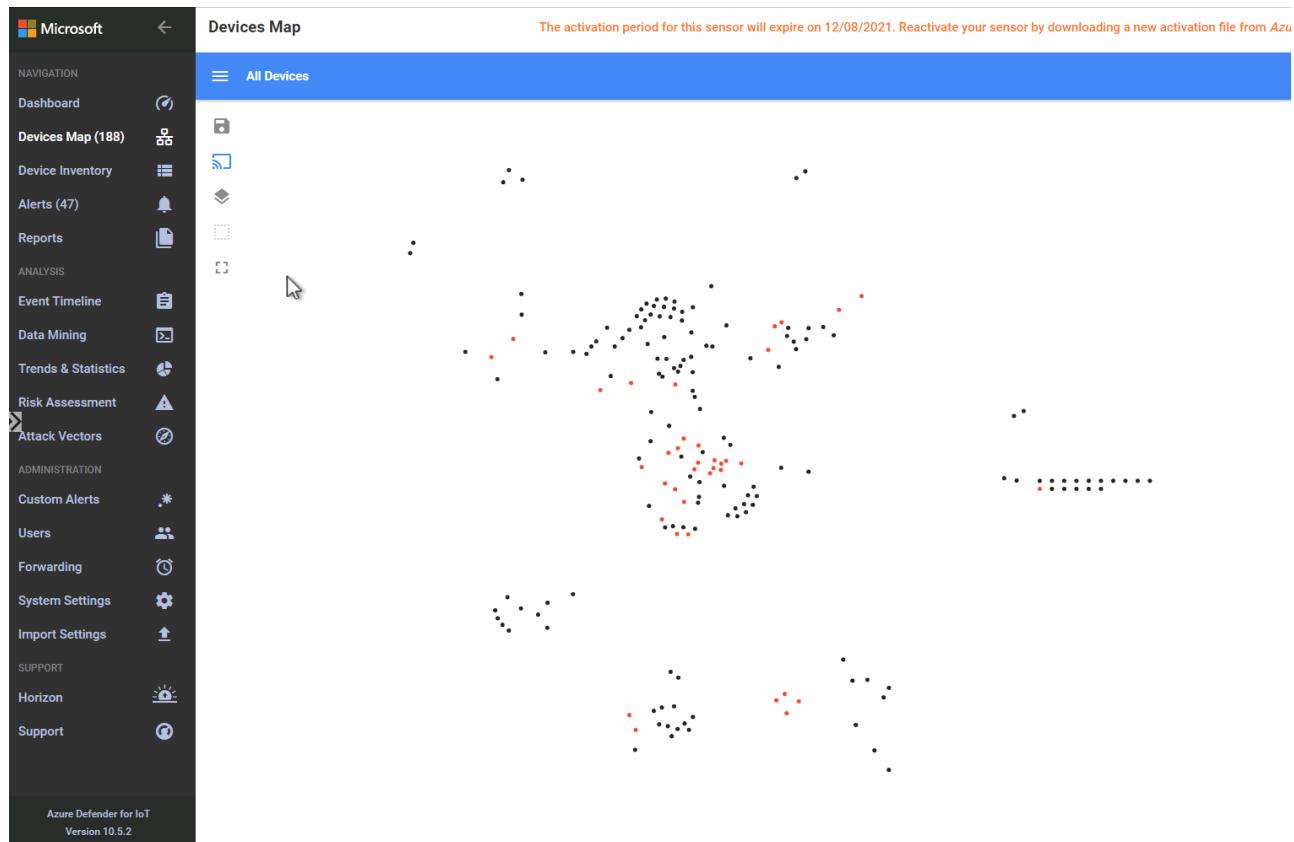
After Defender for Cloud learnt about your environment it will be able to share insights pretty fast.

Task 1: Devices Map

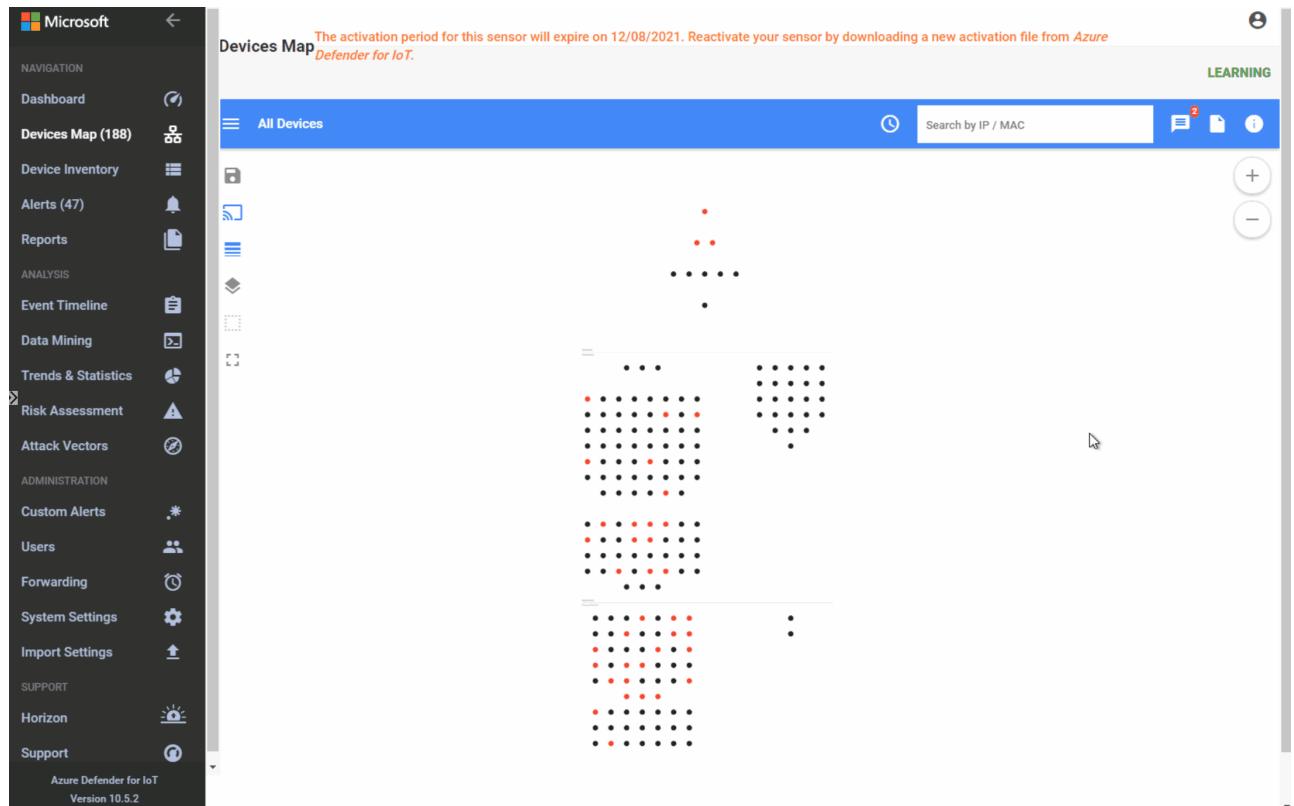
Your first interaction with Devices map you will see a similar map like the one below (details of what you actually see may vary):



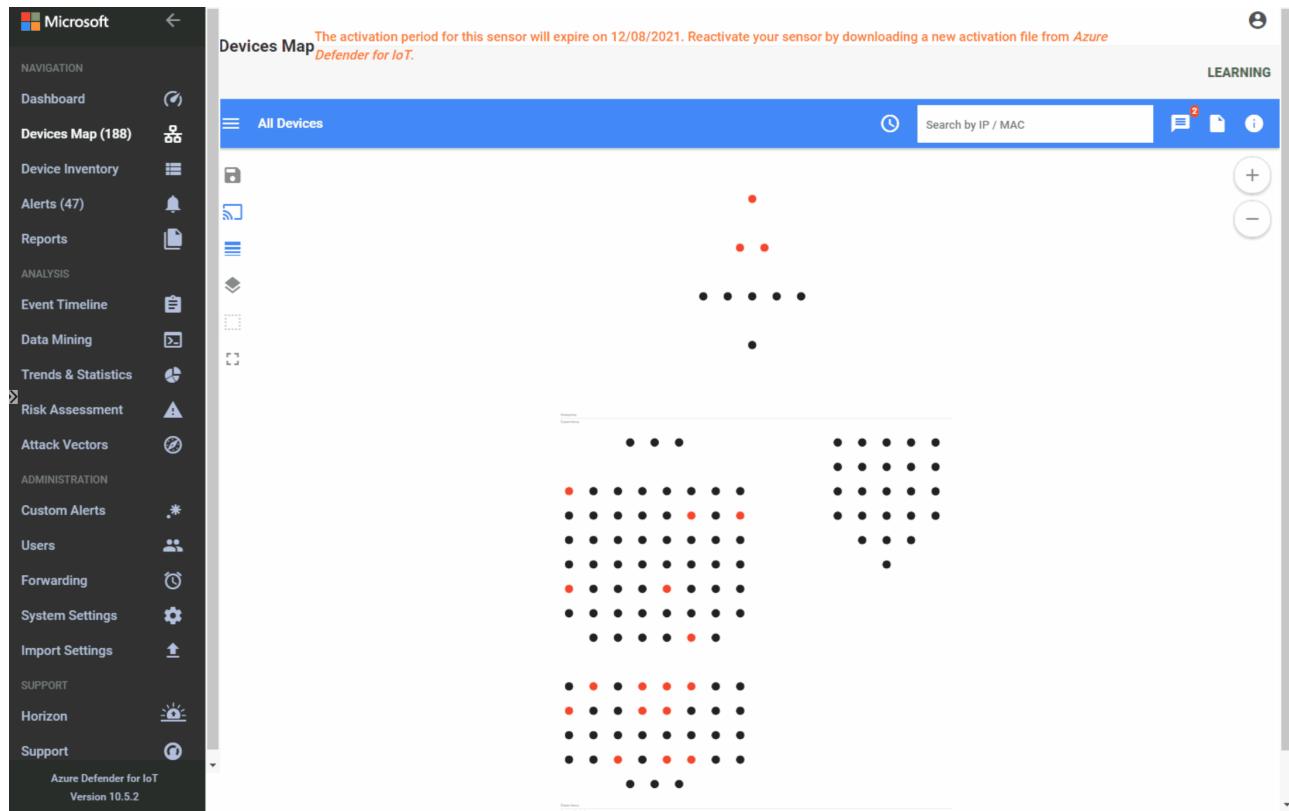
1. Use the four icon bar on the left to select **Layout by Purdue**. In this model you will see the different layers between Corporate IT and site operations.



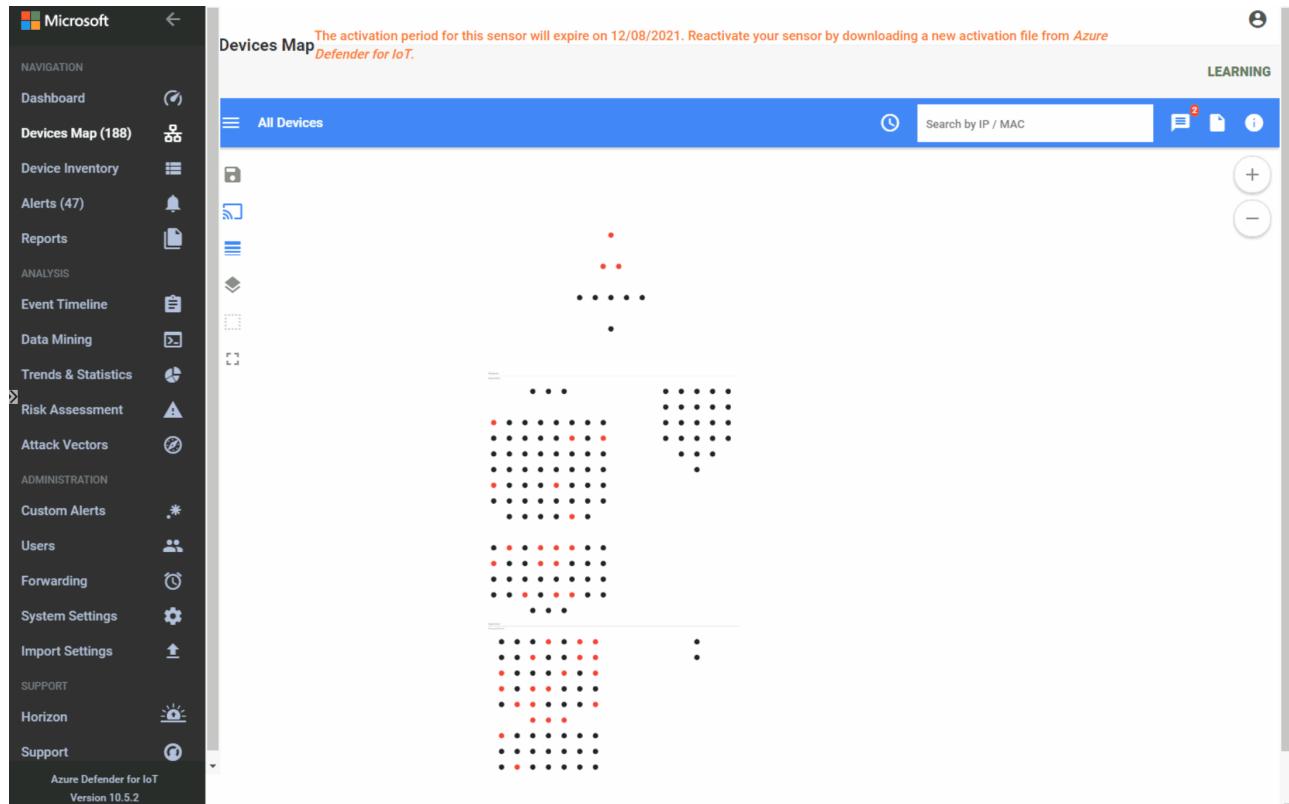
2. Check your notifications available and you can take action at this point.



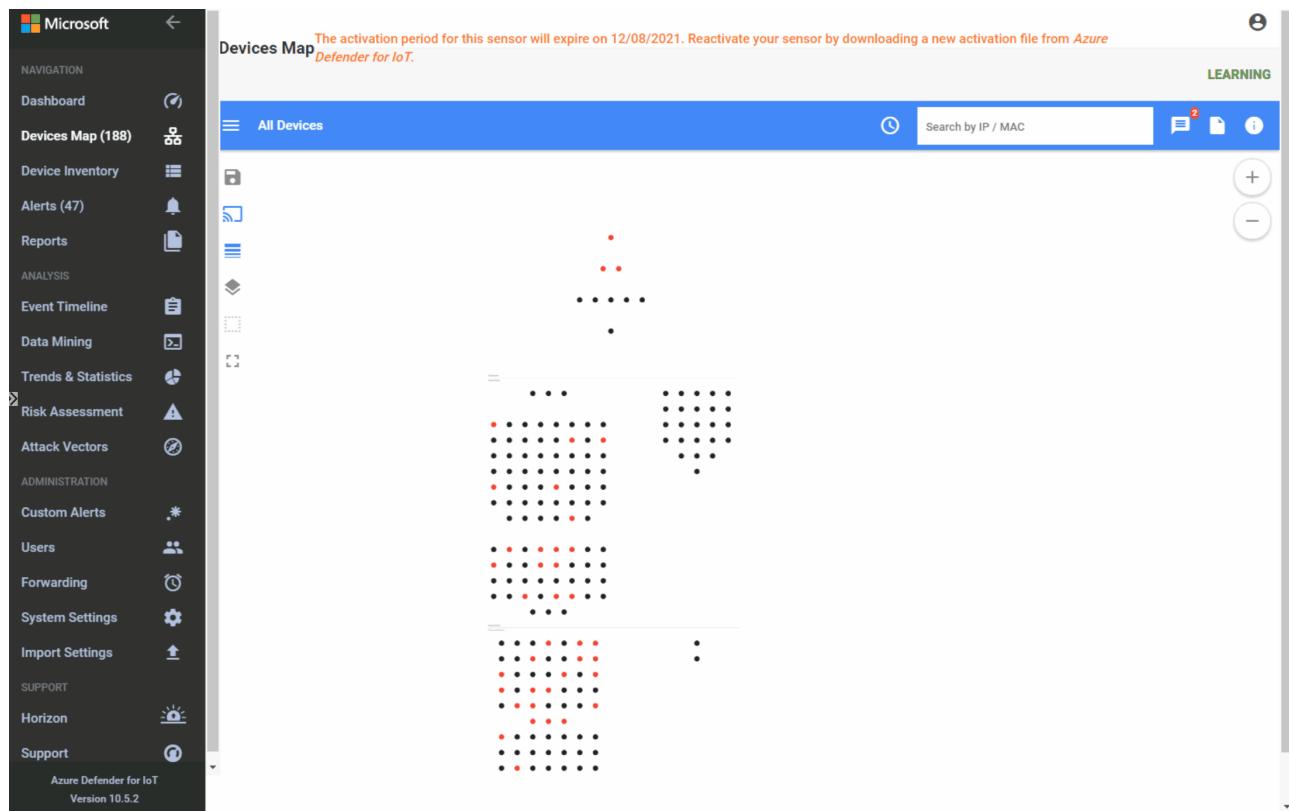
3. For each device right click to analyze properties, show events, reports and simulate attack vectors.



4. In the hamburger 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



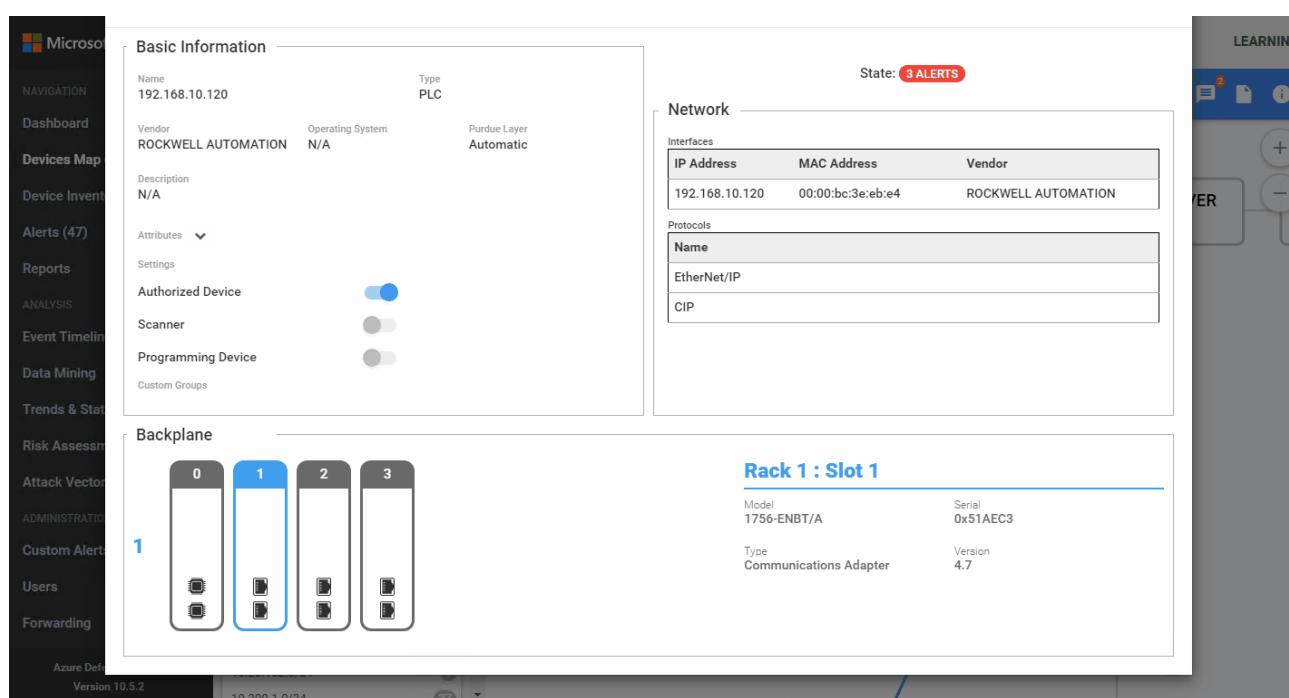
5. Then filter your devices by **CIP** OT Protocol, at the bottom of your map you will see a PLC, where the Vendor is Rockwell Automation, has already 3 alerts activated. Right click on the device, **View Properties**. In this view you will be able to analyze the Backbone of your PLCs, take actions and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



Task 2: Alerts

- 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**

The screenshot shows the Microsoft Defender for IoT interface. The left sidebar contains navigation links for Dashboard, Devices Map, Device Inventory, Alerts (47), Reports, Analysis, Event Timeline, Data Mining, Trends & Statistics, Risk Assessment, Attack Vectors, Administration, Custom Alerts, Users, Forwarding, System Settings, and Import Settings. The main content area is titled 'Alerts' and displays three sections: 'Important Alerts (3)', 'Pinned Alerts (0)', and 'Recent Alerts (3)'. The 'Important Alerts' section shows three alerts: 'EtherNet/IP CIP Service Request Failed' (Operational, 16 hours ago), 'Firmware Change Detected' (Policy Violation, 16 hours ago), and 'Controller Stop' (Operational, 16 hours ago). The 'Recent Alerts' section shows three alerts: 'Firmware Change Detected' (Policy Violation, Nov 9 15:53), 'EtherNet/IP CIP Service Request Failed' (Operational, Nov 9 15:52), and 'Controller Stop' (Operational, Nov 9 15:52). The bottom of the page shows the URL <https://192.168.0.50/#/asset-inventory>.

Task 3: Device Inventory

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

NOTE: if you don't see the column "Is Authorized", click on the "Device Inventory Settings" gear icon (upper-right corner) and add it to the view.

The screenshot shows the Microsoft Defender for IoT interface. The left sidebar contains navigation links for Dashboard, Devices Map, Device Inventory, Alerts (47), Reports, Analysis, Event Timeline, Data Mining, Trends & Statistics, Risk Assessment, Attack Vectors, Administration, Custom Alerts, Users, Forwarding, System Settings, and Import Settings. The main content area is titled 'Device Inventory' and displays a table of assets. The table columns are: IP Address, Name, Last Seen, Type, Protocols, MAC Address, Vendor, and Firmware Version. The table contains 20 rows of asset information. The bottom of the page shows the URL <https://192.168.0.50/#/asset-inventory>.

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 Filters**, filter the timeline by **CIP**, let's analyze the alert timeline.

IP Address	Name	Last Seen	Type	Protocols	MAC Address	Vendor	Firmware Version	Model
192.168.1.120	IAN	Jan 19, 2022 10:18:14 AM	Unknown	DHCP, HTTP, Netbios Name Service, Netbios Session Service, RPC Endpoint Mapper, SMB	00:a0:01:23:40:3f	INVENTEC CORPORATION		
192.168.1.117	LAW	Jan 19, 2022 10:18:14 AM	Workstation	Netbios Datagram Service, Netbios Name Service, RPC Endpoint Mapper, SMB	00:1c:23:fd:38:73	DELL INC.		
192.168.1.100	RNPB179FC	Jan 19, 2022 10:18:14 AM	PLC	BACNet, BACNet (NPDU), Netbios Datagram Service, Netbios Name Service, SMB	00:80:c8:38:6a:57	D-LINK SYSTEMS INC.		
192.168.1.104	BWW-D630	Jan 19, 2022 10:18:14 AM	Unknown	Netbios Name Service, Netbios Session Service	00:1c:23:54:8e:de	DELL INC.		
192.168.1.10	192.168.1.10	Jan 19, 2022 10:18:14 AM	Engineering Station	Siemens S7, Siemens S7 Plus	90:e6:ba:84:5e:41	ASUSTEK COMPUTER INC.		
192.168.1.113	192.168.1.113	Jan 19, 2022 10:18:14 AM	Unknown					
192.168.1.115	192.168.1.115	Jan 19, 2022 10:18:14 AM	Unknown					
192.168.1.5	192.168.1.5	Jan 19, 2022 10:18:14 AM	Unknown	DHCP	00:19:b9:cd:f8:05	DELL INC.		
192.168.1.121	192.168.1.121	Jan 19, 2022 10:18:14 AM	Unknown		00:a0:d1:2e:13:74	INVENTEC CORPORATION		
192.168.1.119	192.168.1.119	Jan 19, 2022 10:18:14 AM	Unknown		00:25:af:00:01:88	COMFILE TECHNOLOGY		
192.168.1.30	192.168.1.30	Jan 19, 2022 10:18:14 AM	Unknown		00:16:76:29:b5:2e	INTEL CORPORATE		
192.168.1.250	192.168.1.250	Jan 19, 2022 10:18:14 AM	PLC	BACNet, BACNet (NPDU), ICMP	00:1b:ae:00:02:ef	MICRO CONTROL SYSTEMS INC		
192.168.1.107	IANMITCHELL-PC	Jan 19, 2022 10:17:55 AM	Workstation	MDNS, Netbios Datagram Service, Netbios Name Service, SMB	00:22:5f:01:60:e9	LITEON TECHNOLOGY CORPORATION		
192.168.1.1	192.168.1.1	Jan 19, 2022 10:17:55 AM	HMI	BACNet, BACNet (NPDU)	00:16:b6:04:f0:ce	CISCO-LINKSYS LLC		
192.168.1.15	PROD-3	Jan 19, 2022 10:17:55 AM	Workstation	Netbios Datagram Service, Netbios Name Service, SMB	00:02:a5:94:08:4b	HEWLETT PACKARD		
192.168.1.37	192.168.1.37	Jan 19, 2022 10:17:55 AM	HMI	BACNet, BACNet (NPDU)	00:01:f0:80:43:12	TRIDIUM INC.		
192.168.1.108	CAG	Jan 19, 2022 10:17:55 AM	Workstation	Netbios Datagram Service, Netbios Name Service, SMB	00:1c:23:04:be:b9	DELL INC.		
192.168.1.7	FTP	Jan 19, 2022 10:17:55 AM	Workstation	Netbios Datagram Service, Netbios Name Service, SMB	00:02:a5:cb:42:a0	HEWLETT PACKARD		

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)**

The screenshot shows the 'Create new Report' dialog in the Azure Defender for IoT portal. The 'Data Mining' section in the navigation bar is highlighted. The report dialog has 'PLC Firmware Versions' as the name and a description 'This report shows the firmware versions for different PLCs'. The 'Firmware Version (GENERIC)' filter is selected in the 'Filters' section. The 'Save' button is highlighted.

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.

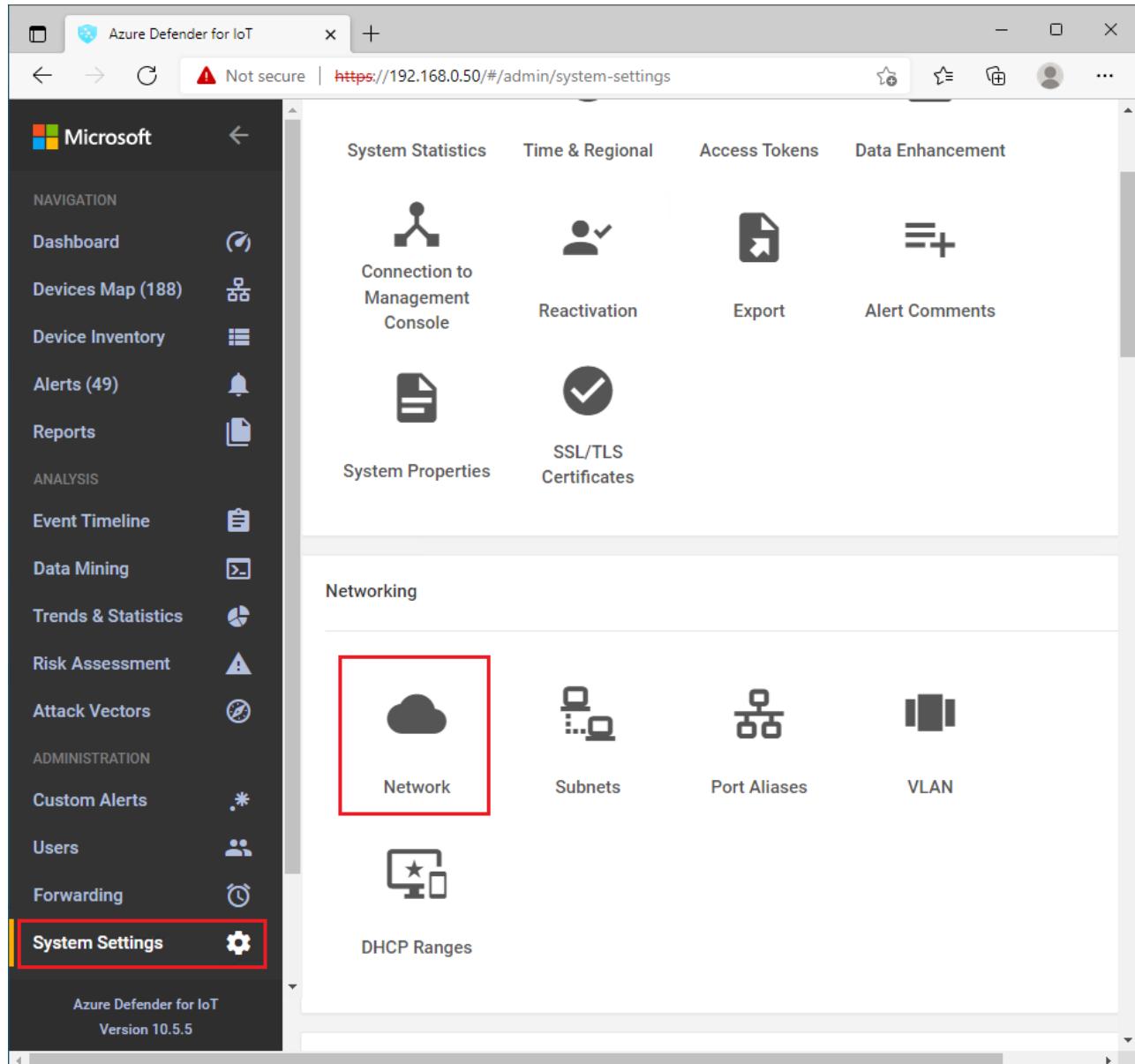
Exercise 5: Online Sensor

To modify our sensor to become an online sensor, we will use the same virtual machine that we used for the offline sensor, but we will reactivate the sensor using **System settings**. In a real scenario you probably would create a new sensor, running in its own virtual machine or physical appliance.

Task 1: Reconfiguring sensor

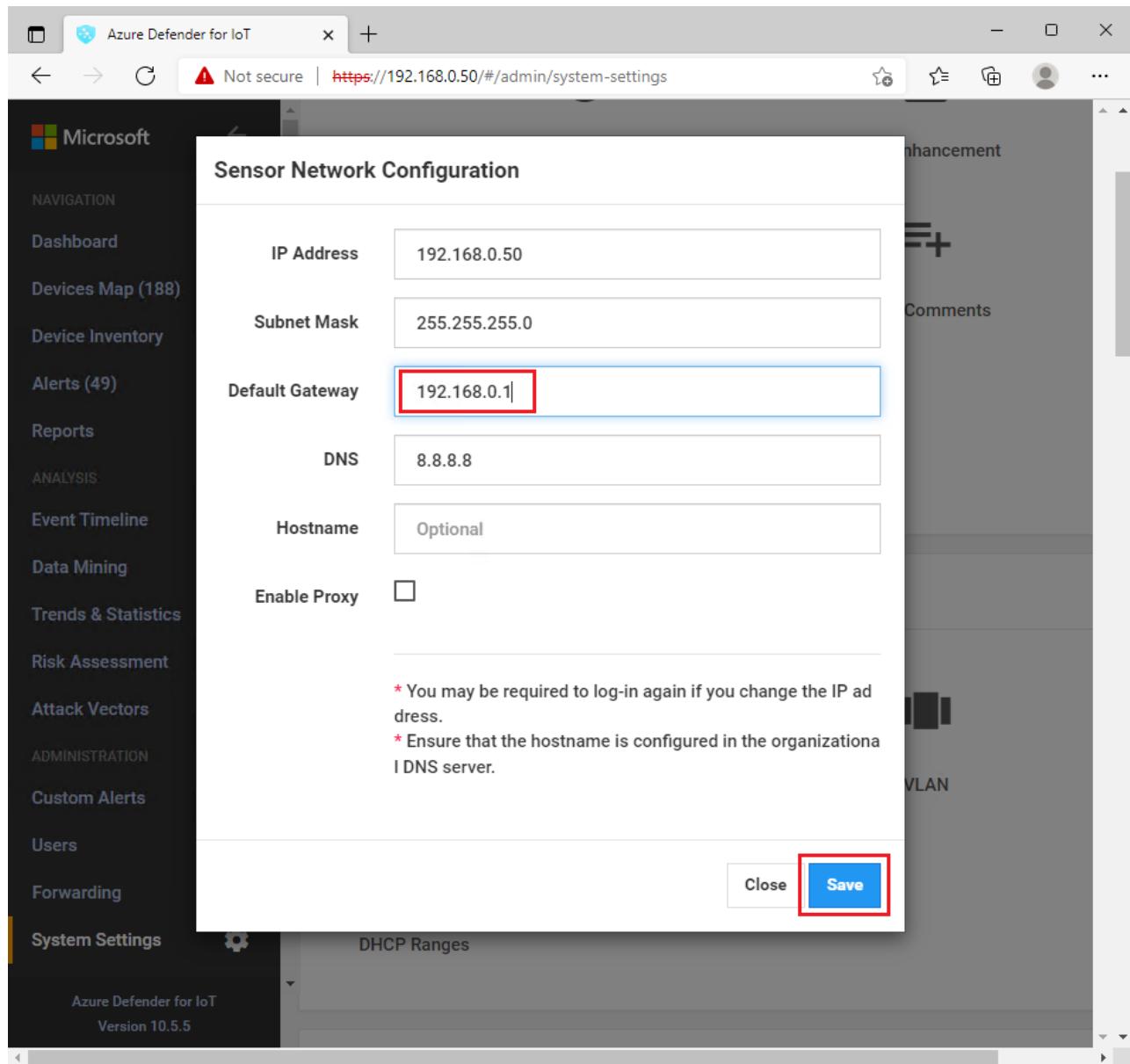
To modify your sensor to be connected with Azure, you will need to modify the network configuration.

1. In your sensor's Azure Defender for IoT Portal (in the Virtual Machine), select **System Settings** and **Network**.

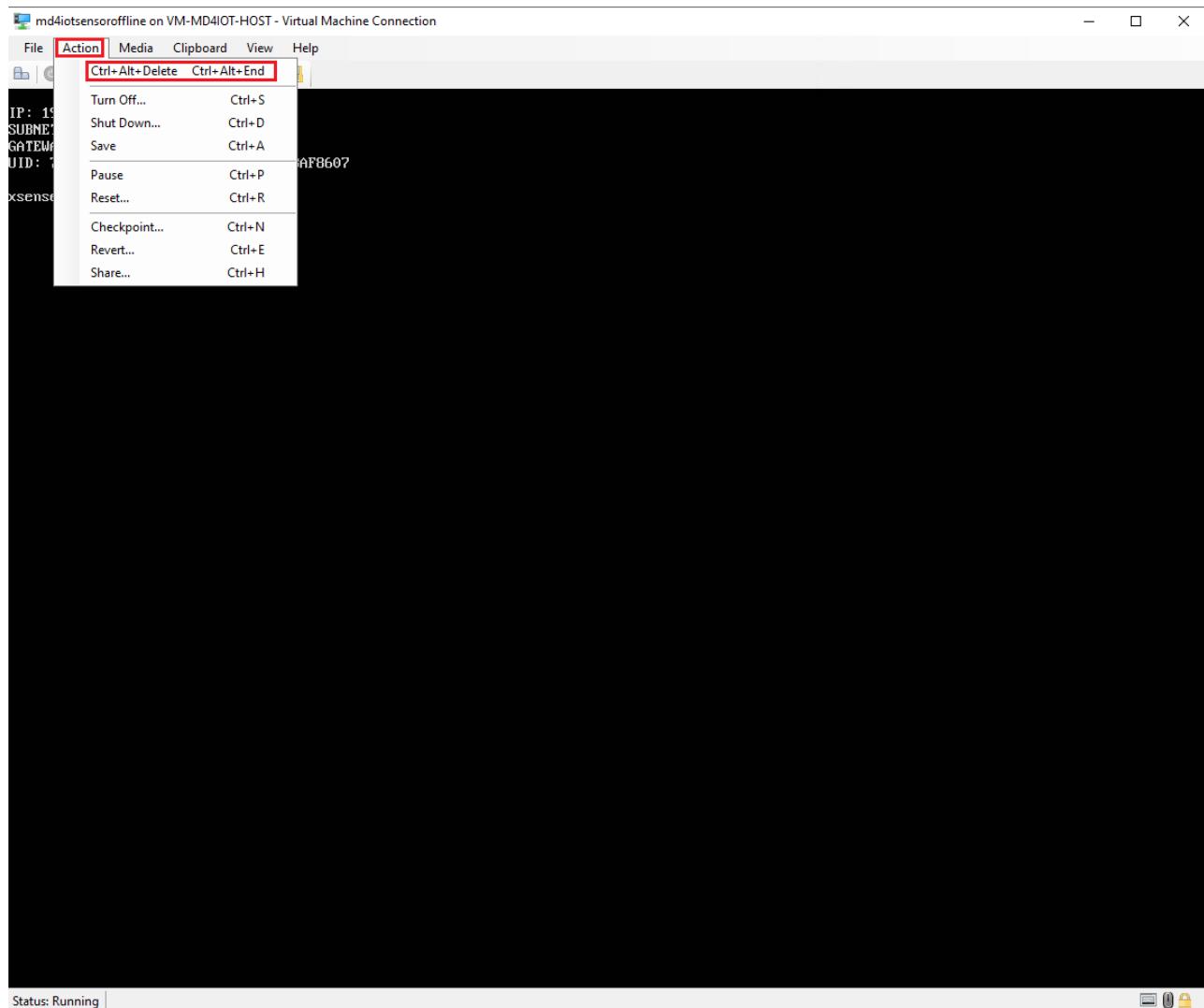


The screenshot shows the 'System Settings' page of the Azure Defender for IoT interface. The left sidebar lists various navigation options like Dashboard, Devices Map, and System Settings, with System Settings being the active tab. The main content area is titled 'System Statistics' and contains several management icons: 'Connection to Management Console', 'Reactivation', 'Export', 'Alert Comments', 'System Properties', and 'SSL/TLS Certificates'. Below this, a 'Networking' section is shown with icons for 'Network' (which is highlighted with a red box), 'Subnets', 'Port Aliases', and 'VLAN'. At the bottom of the page, it says 'Azure Defender for IoT Version 10.5.5'.

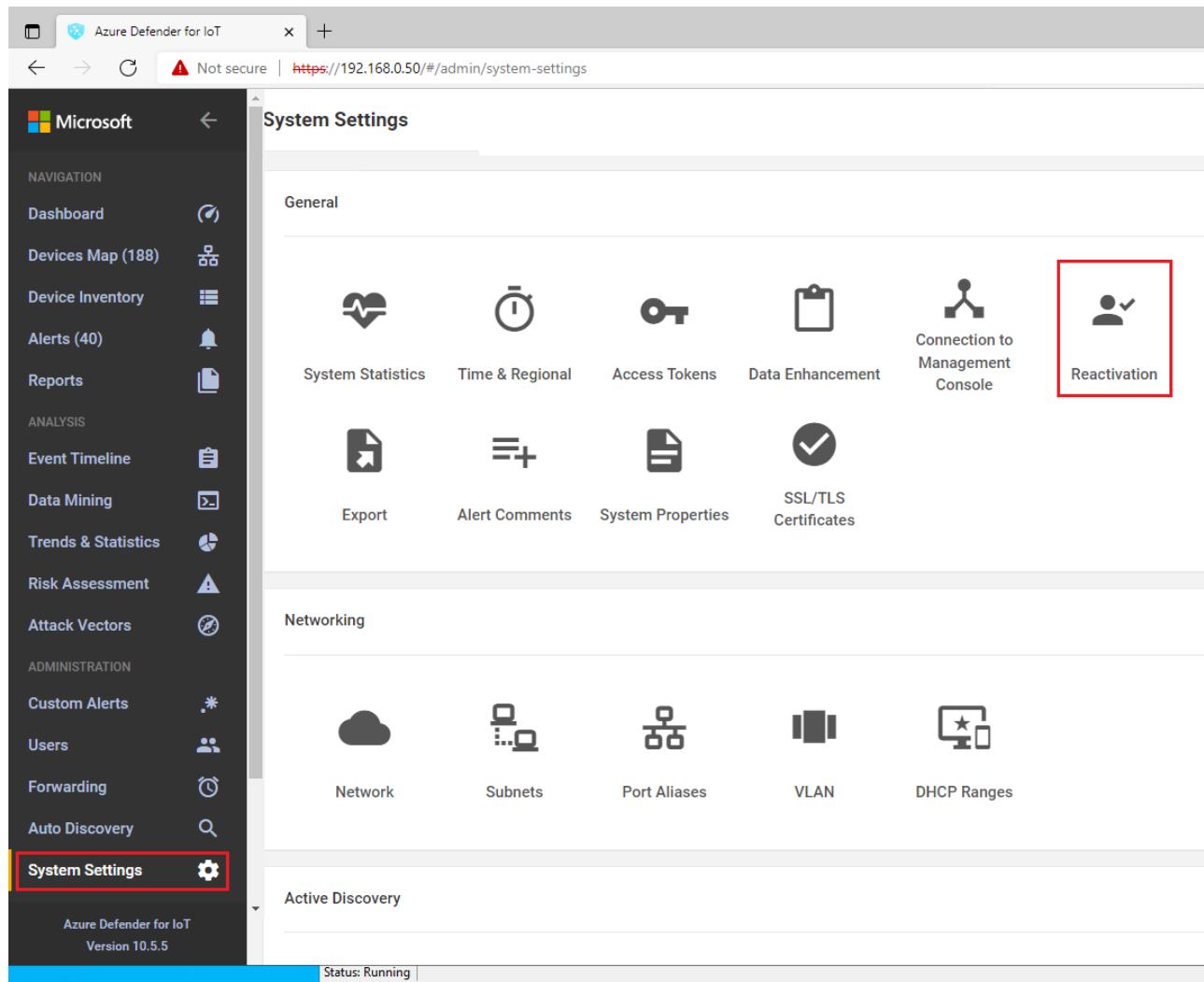
2. Change the IP Address of the Default Gateway to 192.168.0.1 or 172.27.0.1, depending on the settings you used earlier in the HOL.



3. On the "md4iotsensoroffline" Virtual Machine Connection, select **Action** and **Ctrl+Alt+Delete** to reboot the sensor.



4. Login to your sensor's Azure Defender for IoT Portal (in the Virtual Machine) again, select **System Settings** and then, **Reactivation**.
5. 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



The screenshot shows the 'System Settings' page of the Azure Defender for IoT interface. The left sidebar includes 'System Settings' (selected and highlighted with a red box) and 'Azure Defender for IoT Version 10.5.5'. The main content area is titled 'System Settings' and contains three sections: 'General', 'Networking', and 'Active Discovery'. The 'General' section includes icons for 'System Statistics', 'Time & Regional', 'Access Tokens', 'Data Enhancement', 'Connection to Management Console' (which is also highlighted with a red box), and 'Reactivation'. The 'Networking' section includes icons for 'Network', 'Subnets', 'Port Aliases', 'VLAN', and 'DHCP Ranges'. The 'Active Discovery' section is currently empty. The status bar at the bottom shows 'Status: Running'.

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

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

System Settings

Reactivation

Upload the activation file received from Azure Defender for IoT to reactivate this sensor

Activation Mode: Cloud Connected

Activation Period Status: Active

Tenant ID: 405128db-3471-44a4-9bc7-0b91ed773643

Subscription ID: 438ef167-082d-4eea-ba47-61537c8bd4b1

Expiration Date: N/A

Activation file

Upload

Close Activate

8. Run the Pcap files again in your console. In a few minutes you can verify if IoT Hub in Azure Portal on your physical machine is receiving messages from your sensor:

Microsoft Azure

hub-md4iot-mst01

IoT Hub

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Events
- Pricing and scale

Device management

- Devices
- IoT Edge
- Configurations
- Updates
- Queries

Hub settings

- Built-in endpoints
- Message routing
- File upload
- Failover
- Properties
- Locks

Security settings

- Identity

IoT Hub Usage

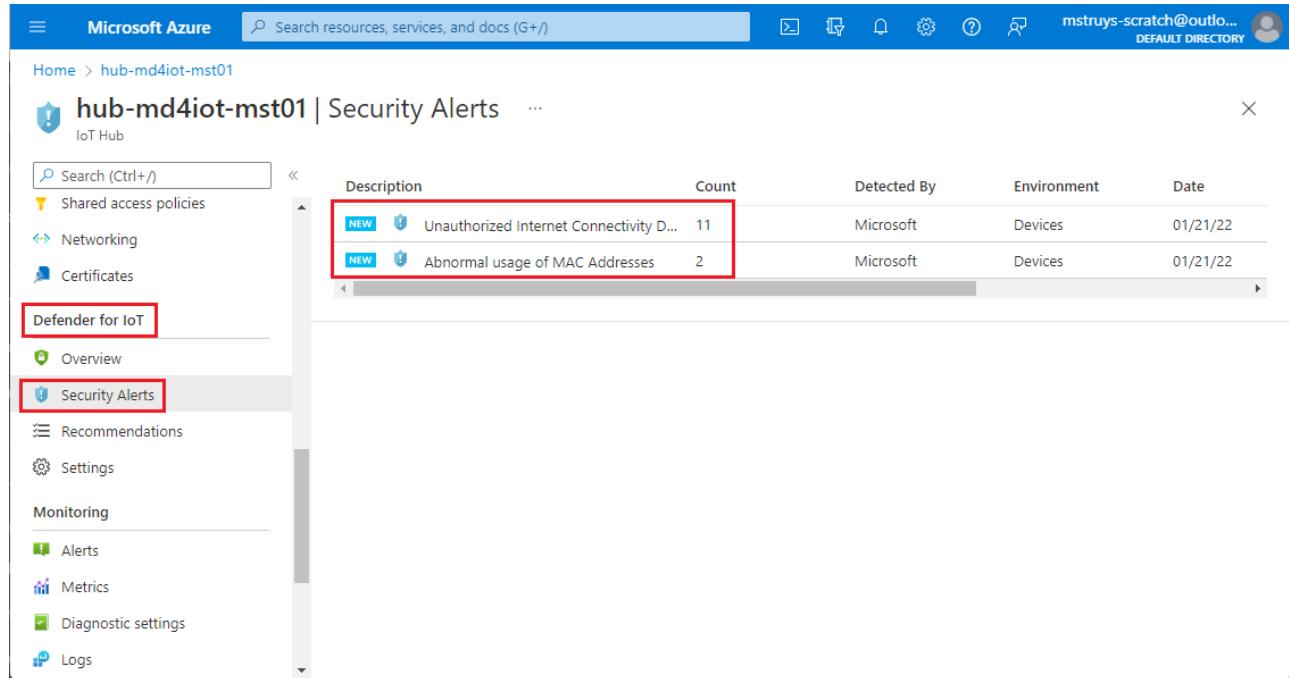
- Messages used today: 0
- Daily messages quota: 400000
- IoT Devices: 1

Number of messages used

Device to cloud messages

Connected Devices

9. In the same IoT Hub now you should see the alerts generated by Defender for IoT. Scroll down to **Defender for IoT**, select **Security Alerts**, on the right side you will see some alerts already available.



Description	Count	Detected By	Environment	Date
Unauthorized Internet Connectivity D...	11	Microsoft	Devices	01/21/22
Abnormal usage of MAC Addresses	2	Microsoft	Devices	01/21/22

Exercise 6: Integrate with Sentinel

You will execute most of this task on your physical machine, not in the Virtual Machine that hosts your your Microsoft Defender for IoT sensor.

Note: Please ensure you have completed Task 6 in the '['Before HOL'](#)' instructions prior to working through the following tasks.

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 > Defender for IoT > Settings > Data Collection

Microsoft Azure

Home > hub-md4iot-mst01

hub-md4iot-mst01 | Settings

IoT Hub

Search (Ctrl+/)

Locks

Security settings

- Identity
- Shared access policies
- Networking
- Certificates

Defender for IoT

- Overview
- Security Alerts
- Recommendations
- Settings

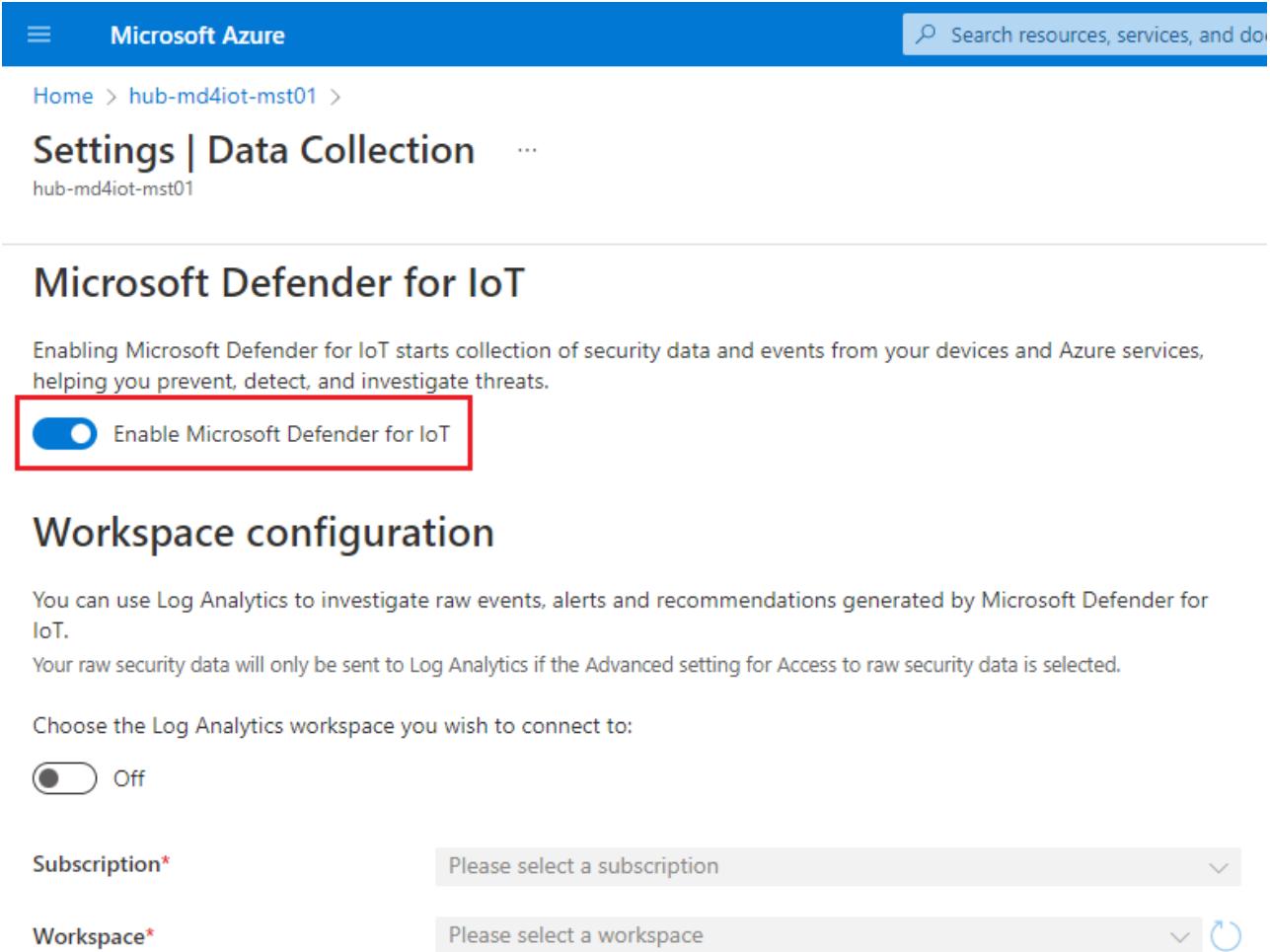
Monitoring

Settings Page

Set the desired configuration to maximize your security.

Name
Data Collection
Recommendations Configuration
Monitored Resources
Custom Alerts

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



Microsoft Azure

Home > hub-md4iot-mst01 >

Settings | Data Collection

Microsoft Defender for IoT

Enabling Microsoft Defender for IoT starts collection of security data and events from your devices and Azure services, helping you prevent, detect, and investigate threats.

Enable Microsoft Defender for IoT

Workspace configuration

You can use Log Analytics to investigate raw events, alerts and recommendations generated by Microsoft Defender for IoT.

Your raw security data will only be sent to Log Analytics if the Advanced setting for Access to raw security data is selected.

Choose the Log Analytics workspace you wish to connect to:

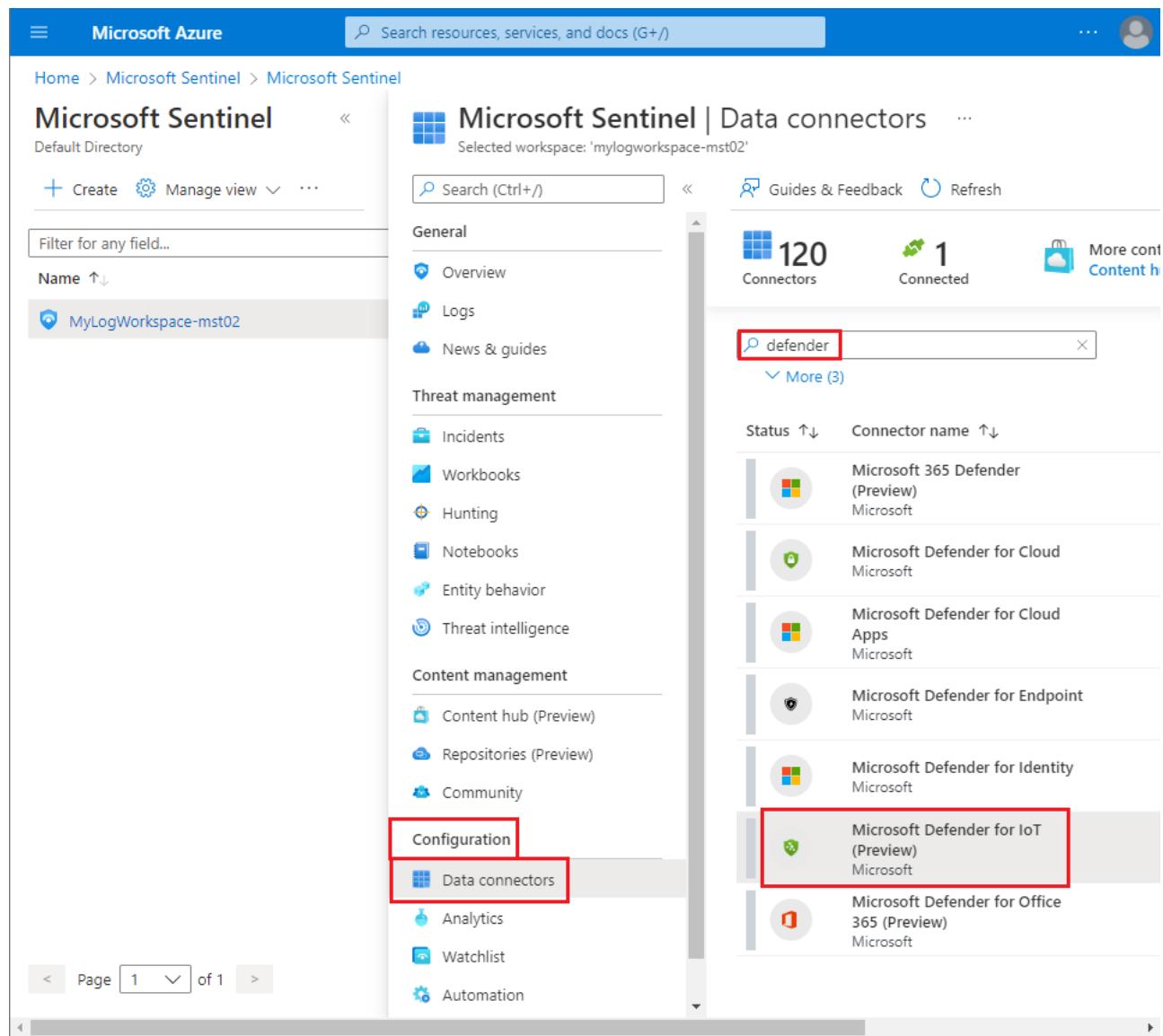
Off

Subscription* Please select a subscription

Workspace* Please select a workspace

Task 2: Connecting Data Connectors

1. With the *Microsoft Defender for IoT* switch enabled, go to **Microsoft Sentinel** > Configuration > Data Connectors > Search **Microsoft Defender for IoT** to connect Microsoft Defender for IoT to Microsoft Sentinel.



Microsoft Sentinel | Data connectors

Selected workspace: 'mylogworkspace-mst02'

120 Connectors | 1 Connected | More content

Search (Ctrl+ /) | Guides & Feedback | Refresh

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

Data connectors

Analytics

Watchlist

Automation

defender

More (3)

Status	Connector name
Connected	Microsoft 365 Defender (Preview) Microsoft
Connected	Microsoft Defender for Cloud Microsoft
Connected	Microsoft Defender for Cloud Apps Microsoft
Connected	Microsoft Defender for Endpoint Microsoft
Connected	Microsoft Defender for Identity Microsoft
Connected	Microsoft Defender for IoT (Preview) Microsoft
Connected	Microsoft Defender for Office 365 (Preview) Microsoft

2. Click the **Open Connector Page**

Microsoft Defender for IoT (Preview)

Not connected Status Microsoft Provider 2 Last Log Received --

Description

Gain insights into your IoT security by connecting Microsoft Defender for IoT alerts to Microsoft Sentinel. You can get out-of-the-box alert metrics and data, including alert trends, top alerts, and alert breakdown by severity. You can also get information about the recommendations provided for your IoT hubs including top recommendations and recommendations by severity.

Last data received --

Related content

1 Workbooks 2 Queries 1 Analytics rules templates

Data received

Go to log analytics

100

80

60

40

20

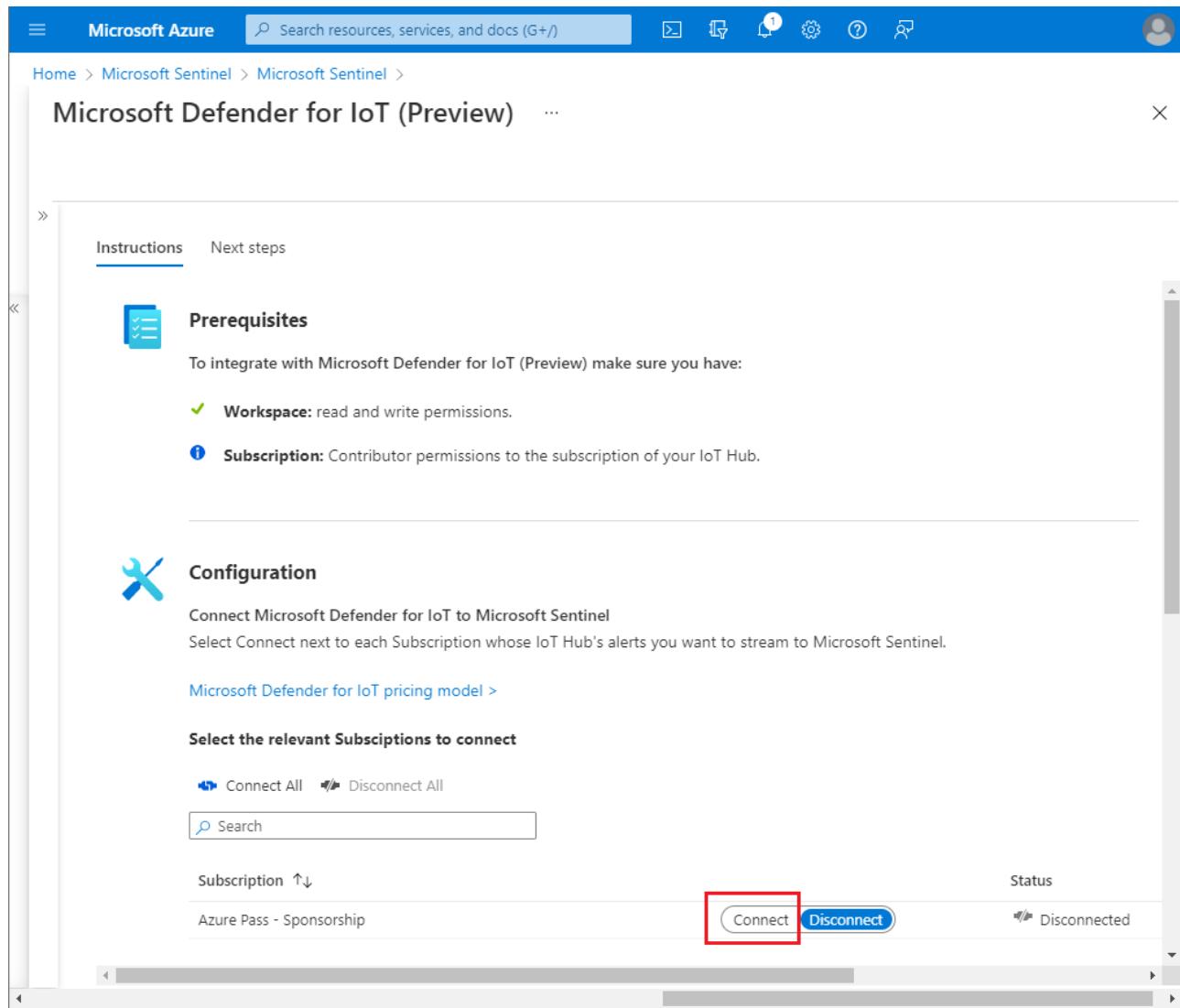
0

January 19 January 21 January 23

Total data received

Open connector page

3. Review the instructions and click the "Connect" button to connect Microsoft 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.



Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel > Microsoft Defender for IoT (Preview) ... X

Instructions Next steps

Prerequisites

To integrate with Microsoft Defender for IoT (Preview) make sure you have:

- ✓ **Workspace:** read and write permissions.
- ⓘ **Subscription:** Contributor permissions to the subscription of your IoT Hub.

Configuration

Connect Microsoft Defender for IoT to Microsoft Sentinel

Select Connect next to each Subscription whose IoT Hub's alerts you want to stream to Microsoft Sentinel.

[Microsoft Defender for IoT pricing model >](#)

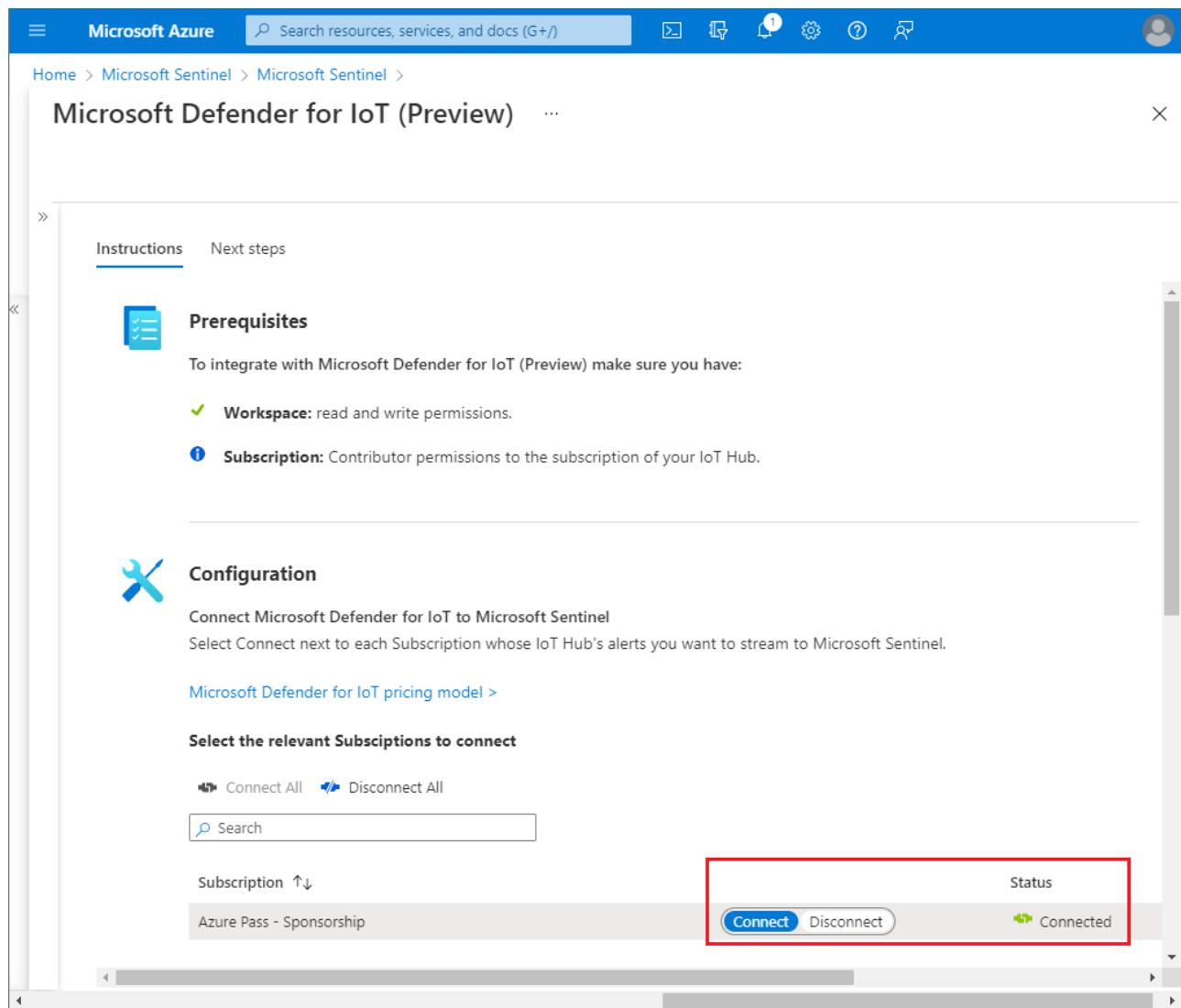
Select the relevant Subscriptions to connect

Connect All Disconnect All

Search

Subscription ↑↓	Status
Azure Pass - Sponsorship	<input type="button"/> Connect <input type="button"/> Disconnect

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



Home > Microsoft Sentinel > Microsoft Sentinel >

Microsoft Defender for IoT (Preview)

Instructions Next steps

Prerequisites

To integrate with Microsoft Defender for IoT (Preview) make sure you have:

- ✓ **Workspace:** read and write permissions.
- ℹ **Subscription:** Contributor permissions to the subscription of your IoT Hub.

Configuration

Connect Microsoft Defender for IoT to Microsoft Sentinel

Select Connect next to each Subscription whose IoT Hub's alerts you want to stream to Microsoft Sentinel.

[Microsoft Defender for IoT pricing model >](#)

Select the relevant Subscriptions to connect

Connect All Disconnect All

Search

Subscription	Status
Azure Pass - Sponsorship	Connected

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.

Microsoft Defender for IoT (Preview)

Instructions **Next steps**

Recommended workbooks (1)

Go to workbooks gallery >

Query samples (2)

All logs

SecurityAlert | where ProductName == "Azure Security Center for IoT"
| sort by TimeGenerated

Run

Summarize by severity

SecurityAlert | where ProductName == "Azure Security Center for IoT"
| summarize count() by AlertSeverity

Run

Relevant analytics templates (1)

Severity ↑↓ Name ↑↓ Rule type ↑↓ Data sources Tactics CREATE RULE

Severity ↑↓	Name ↑↓	Rule type ↑↓	Data sources	Tactics	CREATE RULE
High	Create incidents based on Azure Defender f...	Microsoft Secur...	Microsoft Defender ...		Create rule

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

Analytics rule wizard - Create new rule from template

Validation passed.

General Automated response **Review and create**

Analytics rule details

Name	MyNewRule
Description	Create incidents based on all alerts generated in Azure Defender for IOT
Status	Enabled

Analytics rule logic

Microsoft security service	Microsoft Defender for IoT
Filter by severity	Any
Include by alert name(s)	Any
Exclude by alert name(s)	Any

Automated response

Incident trigger (preview)	Not configured
----------------------------	----------------

Previous **Create**

7. Additionally, you can create the rule not only on the data connectors page but also on the Microsoft Sentinel “Analytics” blade. See an example below when you go to the “Rule Templates” tab and filter

data sources by "Microsoft Defender for IoT (Preview)".

The screenshot shows the Microsoft Sentinel Analytics interface. On the left, a navigation sidebar includes 'Analytics' (which is selected and highlighted in red). The main area displays a list of 'Active rules' (2) and 'Rule templates'. A specific rule template is highlighted with a red box, showing its details: 'TEARDROP memory-only dropper' (High severity, Scheduled, Microsoft 365 Defender (Preview), Initial Access, Persistence). The rule query is: `DeviceEvents | where ActionType has "Exploit" and "Signed" has "SignedBlocked" and InitiatingProcessName contains "svchost.exe" and Filename contains "NetSetupSvc.dll"`. The 'Create rule' button is also highlighted with a red box.

Task 3: Acknowledge Alerts and Re-run PCAPs

You will execute most of this task on the Virtual Machine that hosts your Microsoft Defender for IoT sensor.

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.

1. Navigate to the Alerts Page
2. Click the double check box
3. Click **Ok** to acknowledge the alerts

The screenshot shows the Microsoft Sentinel Alerts page. The left sidebar has 'Alerts (48)' selected and highlighted with a red box. The main area shows a list of 'Important Alerts (48)' under the 'POLICY VIOLATION' category. Each alert entry includes the alert name, timestamp, and a brief description. To the right of the list is an 'Acknowledge All' button, which is highlighted with a red box. The 'Acknowledge All' button has a checked checkbox icon.

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

The screenshot shows the Microsoft Defender for IoT console interface. On the left, a dark sidebar menu lists various features: Alerts (0), Reports, ANALYSIS (Event Timeline, Data Mining, Trends & Statistics), Risk Assessment, Attack Vectors, ADMINISTRATION (Custom Alerts, Users, Forwarding, Auto Discovery), and System Settings. The 'System Settings' item is highlighted with a red box. The main content area is titled 'PCAP Player' with the sub-instruction 'upload and replay PCAP files'. It features a play button icon, an 'Upload' button, a 'Play All' button (which is also highlighted with a red box), and a 'Clear All' button. Below these controls is a list of PCAP files: 1-S7comm-VarService-Read-DB1DBD0.pcap, 2-S7comm-VarService-CyclicData-1s.pcap, 3-S7comm-VAT_MB100_MW200_MD300_M400-0.pcap, 4-S7comm-Download-DB1-with-password-request.pcap, Advantech.pcap, and BACnet-BBMD-on-same-subnet.pcap. A horizontal scrollbar is visible at the bottom of this list.

Task 4: Sentinel interaction with IoT Incidents

You will execute most of this task on your physical machine, not in the Virtual Machine that hosts your Microsoft Defender for IoT sensor.

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**.

Microsoft Sentinel | Incidents

Selected workspace: 'mylogworkspace-mst02'

Search (Ctrl+ /) Refresh Last 24 hours Actions Security efficiency workbook Columns Guides & Feedback

General

Threat management

Incidents (16)

New incidents (16)

Active incidents (0)

Open incidents by severity

High (4) Medium (10) Low (2) Informational (0)

Search by ID, title, tags, owner or product Severity: All Status: 2 selected Product name: Microsoft Defender for IoT Owner: All

Auto-refresh incidents

Severity ↑	Incident ID ↑	Title ↑	Alerts	Product names	Created time ↑	Last update time ↑	Owner
High	16	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:42 PM	01/25/22, 04:42 PM	Unas...
High	15	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Low	14	Outstation Restarted	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	13	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	12	Firmware Change Detected	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Low	11	Controller Stop	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
High	10	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	9	EtherNet/IP CIP Service Requ...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	8	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
High	7	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	6	Unknown Object Sent to Out...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	5	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	4	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	3	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	2	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...

< Previous 1 - 16 Next >

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

Microsoft Sentinel | Incidents

Selected workspace: 'mylogworkspace-mst02'

Search (Ctrl+ /) Refresh Last 24 hours Actions Security efficiency workbook Columns Guides & Feedback

General

Threat management

Incidents (16)

New incidents (16)

Active incidents (0)

Open incidents by severity

High (4) Medium (10) Low (2) Informational (0)

Search by ID, title, tags, owner or product Severity: All Status: 2 selected Product name: Microsoft Defender for IoT Owner: All

Auto-refresh incidents

Severity ↑	Incident ID ↑	Title ↑	Alerts	Product names	Created time ↑	Last update time ↑	Owner
High	16	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:42 PM	01/25/22, 04:42 PM	Unas...
High	15	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Low	14	Outstation Restarted	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	13	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	12	Firmware Change Detected	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Low	11	Controller Stop	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
High	10	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	9	EtherNet/IP CIP Service Requ...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	8	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
High	7	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	6	Unknown Object Sent to Out...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	5	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	4	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	3	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	2	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...

< Previous 1 - 16 Next >

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.

4. By clicking the **Investigate** button, you can dig deeper in the cause of the incident and the relation to other incidents.

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"
```

Microsoft Sentinel | Logs

New Query 1*

Run

Time range: Last 24 hours

1 SecurityAlert
2 | where ProviderName contains "IoTSecurity"

Results

Completed. Showing results from the last 24 hours.

TimeGenerated [UTC]	DisplayName	AlertName	AlertSeverity	Description
1/25/2022, 3:41:27.651 PM	Unknown Object Sent to Outstation	Unknown Object Sent to Outstation	Medium	The destination device received an invalid request.
1/25/2022, 3:42:27.511 PM	Outstation Restarts Frequently	Outstation Restarts Frequently	Low	An excessive number of cold restarts were detected on a source device.
1/25/2022, 3:41:27.464 PM	Firmware Change Detected	Firmware Change Detected	Medium	Firmware was updated on a source device. This may be authentic or malicious.
1/25/2022, 3:42:27.361 PM	Port Scan Detected	Port Scan Detected	High	A source device was detected scanning network devices. This may be authentic or malicious.
1/25/2022, 3:44:27.356 PM	Port Scan Detected	Port Scan Detected	High	A source device was detected scanning network devices. This may be authentic or malicious.
1/25/2022, 3:43:27.373 PM	Unauthorized Internet Connectivity Det...	Unauthorized Internet Connectivity Det...	High	A source device defined as part of your network is communicating with an external network.
1/25/2022, 3:40:27.499 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server returned an error code. This indicates a server error.
1/25/2022, 3:42:27.473 PM	Outstation Restarted	Outstation Restarted	Low	A cold restart was detected on a source device. This means the device has been turned off and back on.
1/25/2022, 3:41:27.324 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server returned an error code. This indicates a server error.
1/25/2022, 3:41:27.443 PM	EtherNet/IP CIP Service Request Failed	EtherNet/IP CIP Service Request Failed	Medium	A server returned an error code. This indicates a server error.
1/25/2022, 3:41:27.407 PM	Controller Stop	Controller Stop	Low	The source device sent a stop command to a destination component.
1/25/2022, 3:41:27.384 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server returned an error code. This indicates a server error.

SecurityAlert | where CompromisedEntity == "hub-md4iot-mst01"

Run

Time range: Last 7 days

1 SecurityAlert
2 | where CompromisedEntity == "adt4iothub"

Results

Completed. Showing results from the last 7 days.

TimeGenerated [UTC]	DisplayName	AlertName	AlertSeverity	Description
10/1/2021, 4:00:04.420 PM	Unauthorized Internet Connectivity Det...	Unauthorized Internet Connectivity Det...	High	A source device defined as part of your network is communicating with an external network.
10/1/2021, 4:00:04.087 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server returned an error code. This indicates a server error.
10/1/2021, 4:00:07.358 PM	Controller Stop	Controller Stop	Low	The source device sent a stop command to a destination component.
10/1/2021, 4:00:07.445 PM	Port Scan Detected	Port Scan Detected	High	A source device was detected scanning network devices. This may be authentic or malicious.

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.

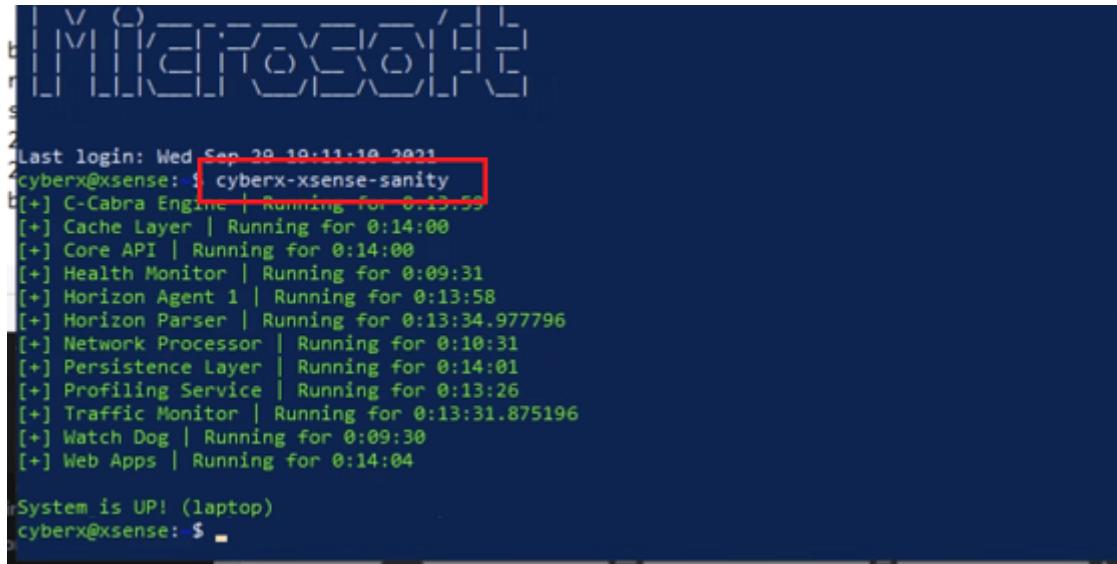
Enter your-resource-group-name for **TYPE THE RESOURCE GROUP NAME** and select Delete. This operation will take a few minutes.

After that is done go to Microsoft Defender for IoT and deactivate the subscription.

Appendix 1: 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
```

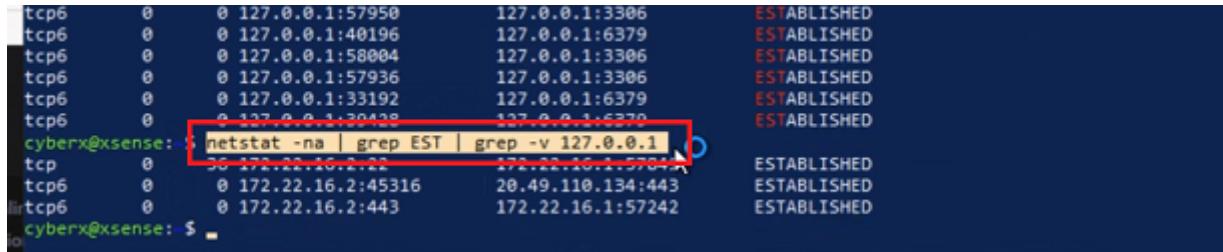


```
Last login: Wed Sep 29 19:11:10 2021
cyberx@xsense: $ cyberx-xsense-sanity
[+] C-Cabra Engine | Running for 0:13:59
[+] Cache Layer | Running for 0:14:00
[+] Core API | Running for 0:14:00
[+] Health Monitor | Running for 0:09:31
[+] Horizon Agent 1 | Running for 0:13:58
[+] Horizon Parser | Running for 0:13:34.977796
[+] Network Processor | Running for 0:10:31
[+] Persistence Layer | Running for 0:14:01
[+] Profiling Service | Running for 0:13:26
[+] Traffic Monitor | Running for 0:13:31.875196
[+] Watch Dog | Running for 0:09:30
[+] Web Apps | Running for 0:14:04

System is UP! (laptop)
cyberx@xsense: $
```

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
```



```
tcp6      0      0 127.0.0.1:57950      127.0.0.1:3306      ESTABLISHED
tcp6      0      0 127.0.0.1:40196      127.0.0.1:6379      ESTABLISHED
tcp6      0      0 127.0.0.1:58004      127.0.0.1:3306      ESTABLISHED
tcp6      0      0 127.0.0.1:57936      127.0.0.1:3306      ESTABLISHED
tcp6      0      0 127.0.0.1:33192      127.0.0.1:6379      ESTABLISHED
tcp6      0      0 127.0.0.1:30428      127.0.0.1:6379      ESTABLISHED
cyberx@xsense:~$ netstat -na | grep EST | grep -v 127.0.0.1
tcp      0      0 172.22.16.2:22      172.22.16.1:57815      ESTABLISHED
tcp6      0      0 172.22.16.2:45316      20.49.110.134:443    ESTABLISHED
tcp6      0      0 172.22.16.2:443      172.22.16.1:57242    ESTABLISHED
cyberx@xsense:~$
```

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

```
tcp6      0      0 127.0.0.1:40196      127.0.0.1:6379      ESTABLISHED
tcp6      0      0 127.0.0.1:58004      127.0.0.1:3306      ESTABLISHED
tcp6      0      0 127.0.0.1:57936      127.0.0.1:3306      ESTABLISHED
tcp6      0      0 127.0.0.1:33192      127.0.0.1:6379      ESTABLISHED
tcp6      0      0 127.0.0.1:39428      127.0.0.1:6379      ESTABLISHED
cyberx@xsense: $ netstat -na | grep EST | grep -v 127.0.0.1
tcp      0      36 172.22.16.2:22      172.22.16.1:57841      ESTABLISHED
tcp6      0      0 172.22.16.2:45316      20.49.110.134:443      ESTABLISHED
tcp6      0      0 172.22.16.2:443      172.22.16.1:57242      ESTABLISHED
cyberx@xsense: $ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=55 time=2.30 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=55 time=2.44 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 2.300/2.370/2.440/0.070 ms
cyberx@xsense: $ ping ad4iothol.azure-devices.net
PING ihsu-eastus-4.eastus.cloudapp.azure.com (20.49.110.134) 56(84) bytes of data.
^C
```