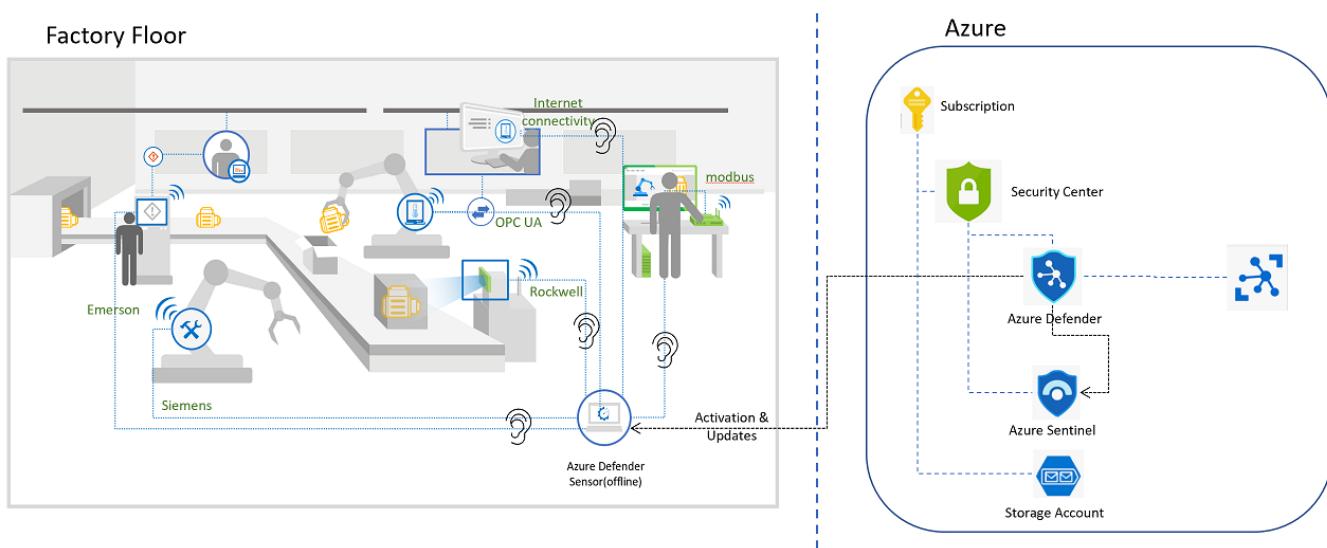


Internet of Things - Microsoft Defender for IoT HOL

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

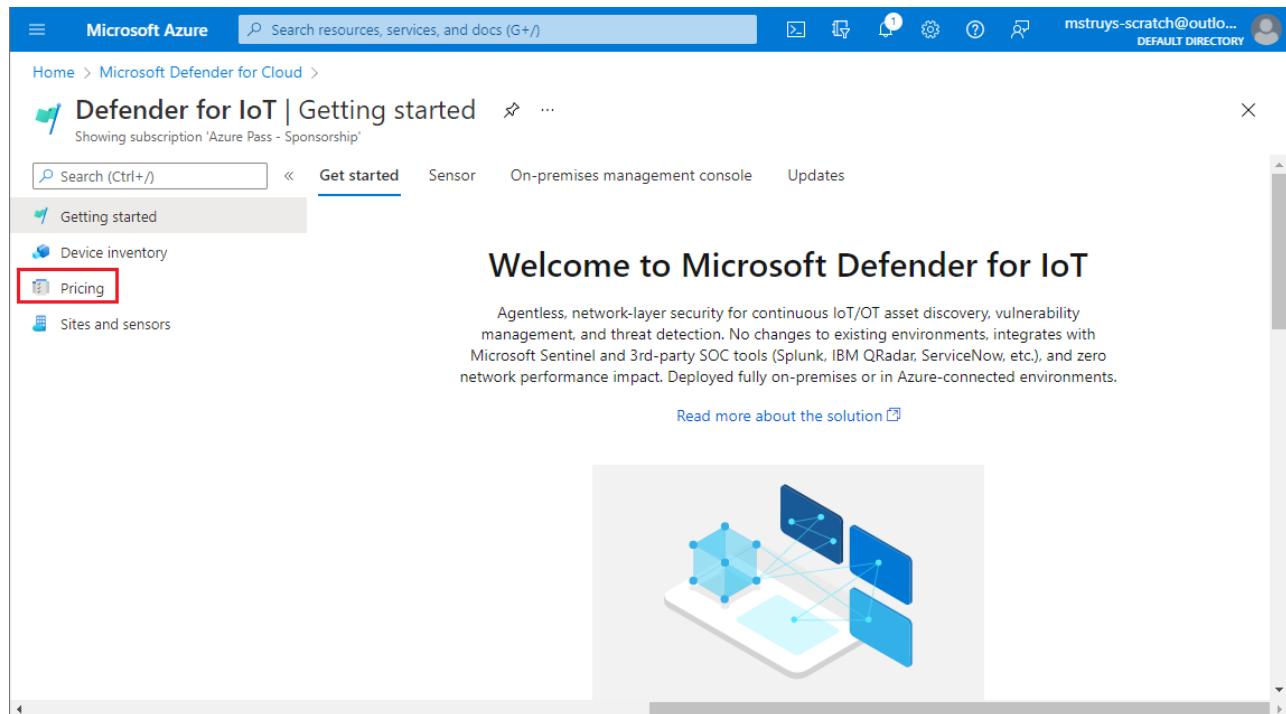
Task 1: Enabling Microsoft Defender for IoT

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.

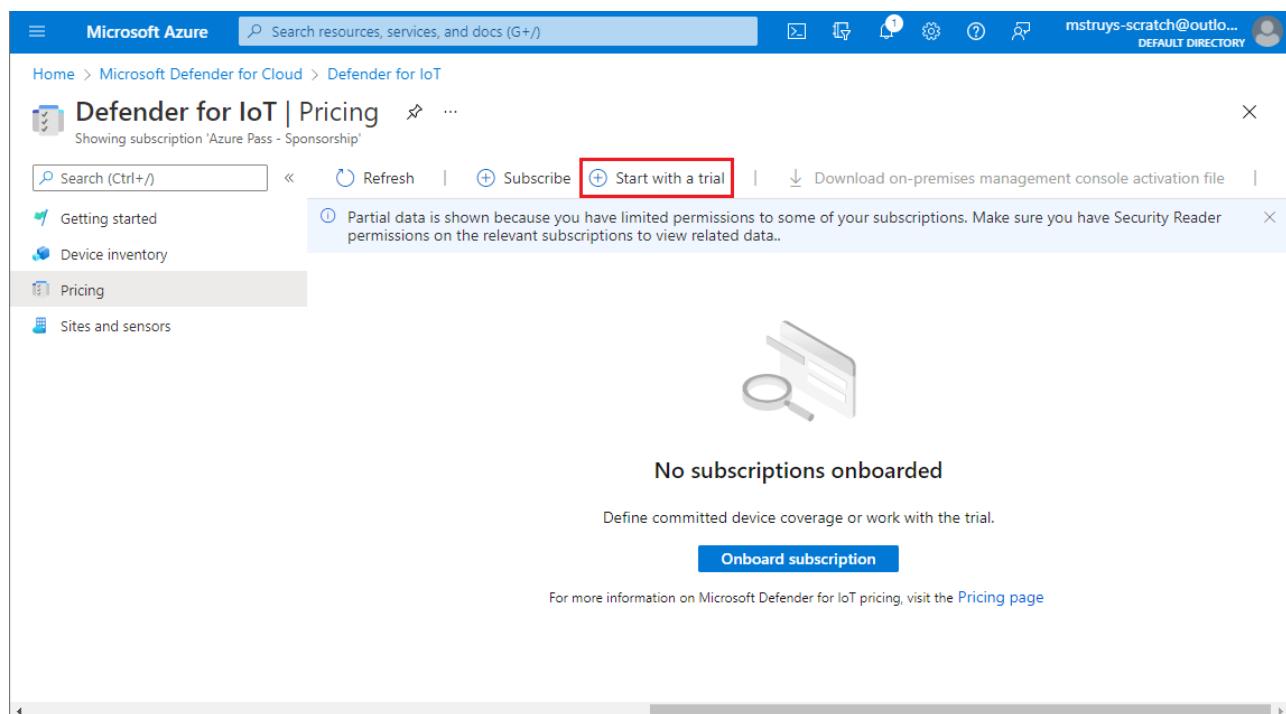
The screenshot shows the Microsoft Azure portal interface. The search bar at the top contains the text "Microsoft Defender for IoT". The search results list "Microsoft Defender for IoT" as the top item, which is highlighted with a red box. Other items in the list include "IoT Hub", "Microsoft Sentinel", "Form recognizers", and "Power Platform". To the left, there's a sidebar with "Azure services" and "Recent resources" sections. The "Recent resources" section lists several resource names. At the bottom, there's a URL bar with the address "https://ms.portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/".

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



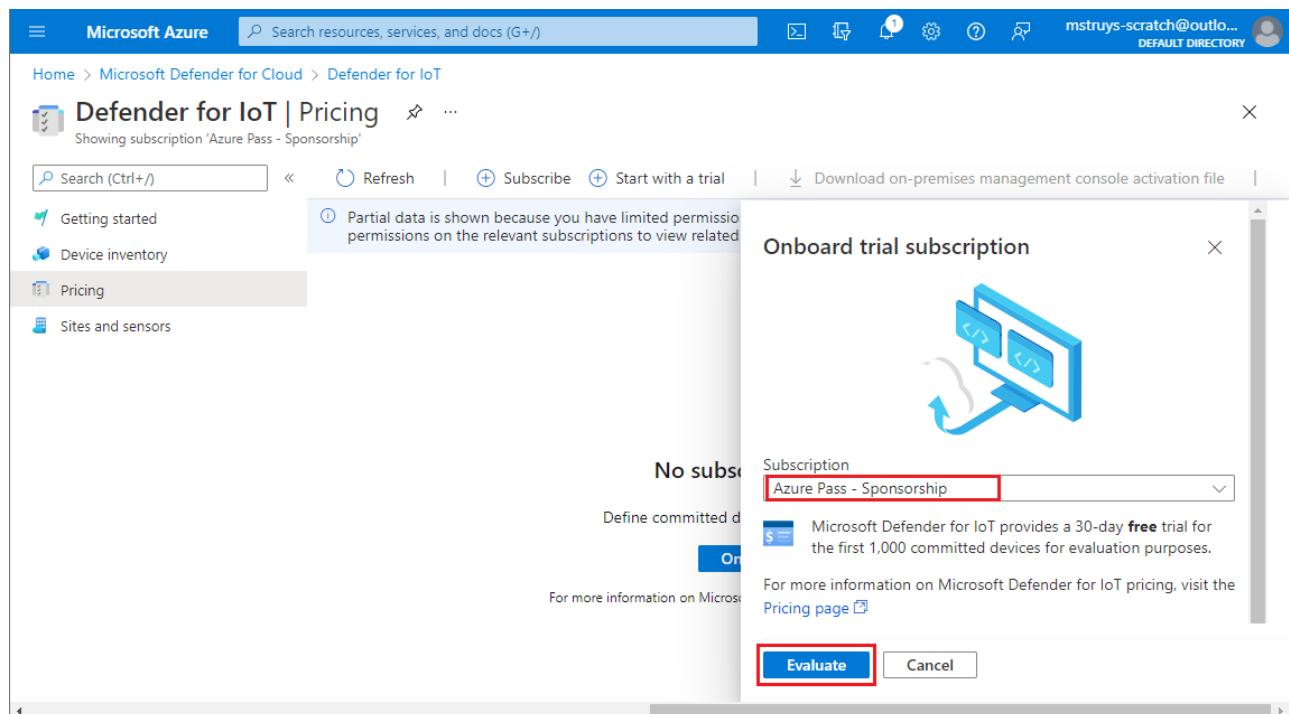
The screenshot shows the Microsoft Azure portal with the URL [https://portal.azure.com/#blade/Microsoft_Azure_IoTHub/DefenderForIoTBlade/GetStarted](#). The page title is "Defender for IoT | Getting started". The left sidebar has links for "Getting started", "Device inventory", "Pricing" (which is highlighted with a red box), and "Sites and sensors". The main content area features a large heading "Welcome to Microsoft Defender for IoT" and a brief description: "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." Below the description is a "Read more about the solution" link and an illustration of a smartphone displaying a network of nodes.

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



The screenshot shows the Microsoft Azure portal with the URL [https://portal.azure.com/#blade/Microsoft_Azure_IoTHub/DefenderForIoTBlade/Pricing](#). The page title is "Defender for IoT | Pricing". The left sidebar has links for "Getting started", "Device inventory", "Pricing" (which is highlighted with a red box), and "Sites and sensors". The main content area shows a message: "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..". It features a magnifying glass icon and the text "No subscriptions onboarded". A blue button labeled "Onboard subscription" is present. Below it, a note says: "Define committed device coverage or work with the trial." and "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**.



The screenshot shows the Microsoft Azure portal with the URL [https://portal.azure.com/#blade/Microsoft_Azure_IoTHub/DefenderForIoTBlade/Overview](#). The user is on the 'Pricing' page for Microsoft Defender for IoT. A modal window titled 'Onboard trial subscription' is displayed, asking the user to choose a subscription for a trial. The 'Subscription' dropdown is set to 'Azure Pass - Sponsorship'. The text inside the modal states: 'Microsoft Defender for IoT provides a 30-day **free** trial for the first 1,000 committed devices for evaluation purposes.' There are 'Evaluate' and 'Cancel' buttons at the bottom.

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.

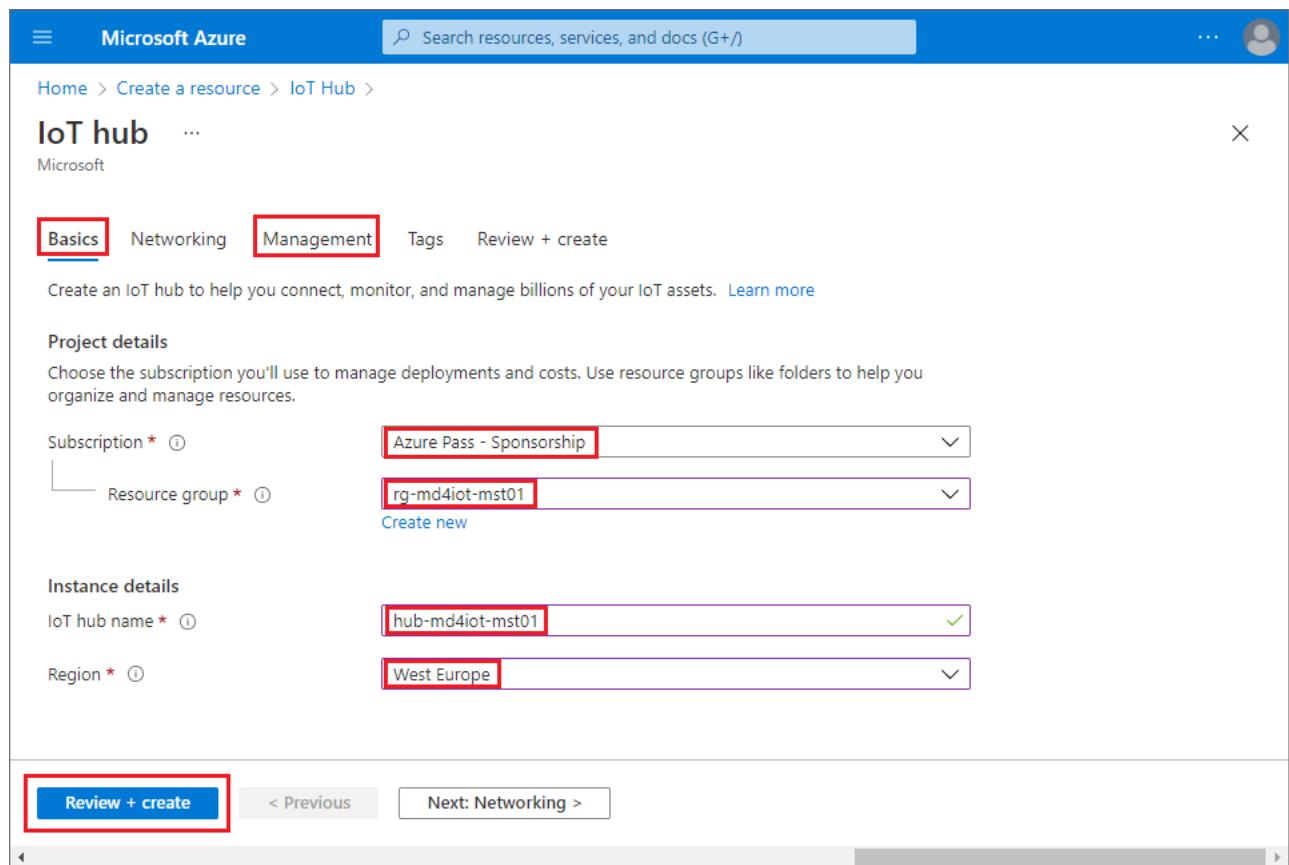
Task 2: Create an IoT Hub:

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).



The screenshot shows the Microsoft Azure portal interface for creating an IoT Hub. The top navigation bar includes 'Microsoft Azure', a search bar, and user profile icons. The main title is 'IoT hub' under 'Microsoft'. Below the title, there are tabs: 'Basics' (highlighted with a red box), 'Networking', 'Management', 'Tags', and 'Review + create'. A descriptive text states: 'Create an IoT hub to help you connect, monitor, and manage billions of your IoT assets.' A 'Learn more' link is provided. The 'Project details' section asks to choose a subscription and resource group. The selected subscription is 'Azure Pass - Sponsorship' and the resource group is 'rg-md4iot-mst01'. The 'Instance details' section specifies the IoT hub name as 'hub-md4iot-mst01' and the region as 'West Europe'. At the bottom, there are navigation buttons: 'Review + create' (highlighted with a red box), '< Previous', 'Next: Networking >', and a horizontal scroll bar.

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' interface in the Microsoft Azure portal. The 'Members' tab is active. The 'Selected role' dropdown is set to 'Contributor'. The 'Assign access to' section has 'User, group, or service principal' selected. The 'Members' section contains a '+ Select members' button. The 'Description' field is labeled 'Optional'. At the bottom, there are 'Review + assign', 'Previous', and 'Next' buttons.

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**.

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

The screenshot shows the Microsoft Azure 'Set up OT/ICS Security' wizard. The current step is 'Step 3: Register this sensor with Microsoft Defender for IoT'. The form includes fields for 'Sensor name' (set to 'myofflinesensor') and 'Subscription' (set to 'Azure Pass - Sponsorship (1000)'). A toggle switch labeled 'Cloud connected' is shown as off. A red box highlights the 'Register' button at the bottom left of the form.

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

The screenshot shows the Microsoft Azure 'Set up OT/ICS Security' wizard. A download dialog is open, prompting the user to choose what to do with the file 'myofflinesensor_a...'. The 'Save as' option is highlighted with a red box. Below the dialog, a success message states 'You have successfully registered and can activate your sensor'. A red box highlights the 'Finish' button at the bottom left.

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

The screenshot shows the Microsoft Azure Defender for IoT | Sites and sensors interface. At the top, there are navigation links: Home > Defender for IoT. Below that, a search bar and a refresh button are visible. On the right, there are three buttons: + Onboard OT sensor, + Onboard EloT sensor, and Push Threat Intelligence update (Preview). The main area displays a summary of sensor counts: All sensors (1), EloT (0), OT cloud connected (0), and OT (1). A search bar and an 'Add filter' button are located below the summary. The 'Sites and sensors' tab is selected. A table below shows one sensor entry:

	Sensor name	Sensor type	Zone	Subscription	Sensor version	Sensor status
<input type="checkbox"/>	Locally managed					
<input type="checkbox"/>	myofflinesensor	OT		Azure Pass...		

The row for 'myofflinesensor' is highlighted with a red box.

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

Tags: Key : Value [Add tag](#)

Zone * default

Create Zone

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.

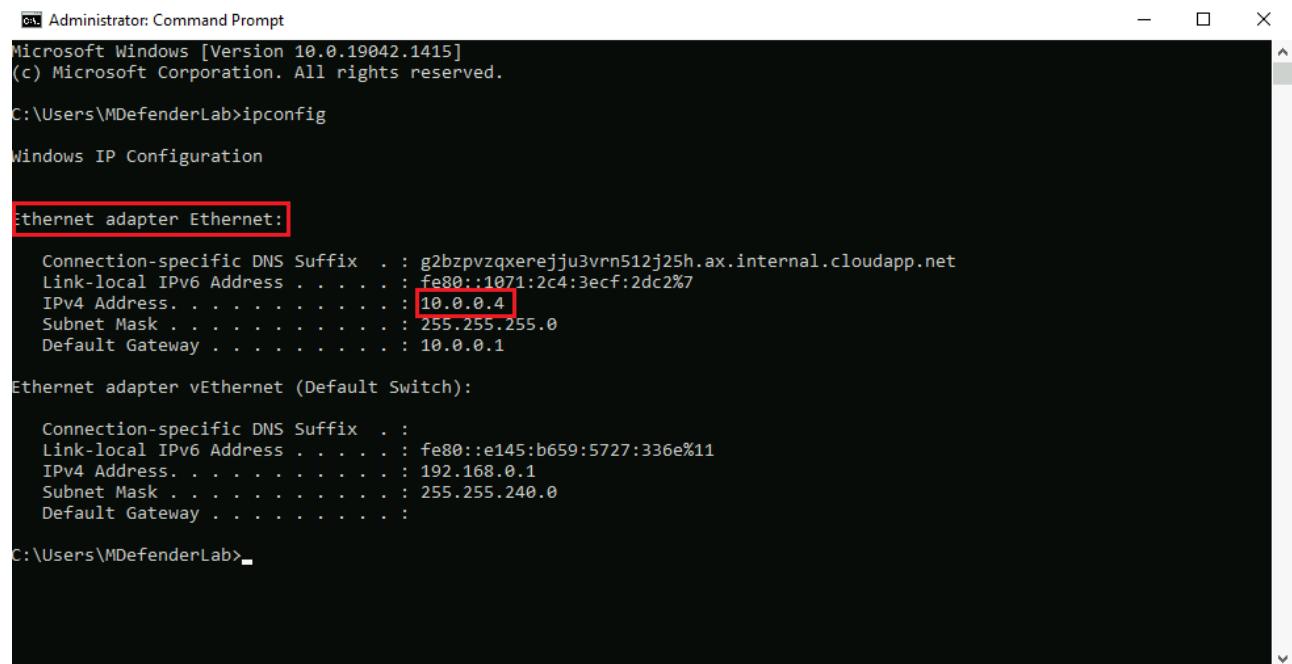
11. At this point you have 2 files downloaded locally (the activation files for your sensors). Since you are using RDP to connect to the Virtual Machine that will host your Microsoft Defender for IoT Sensor, you can simply copy the activation files and paste them in your VM using copy (ctrl-c) and paste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

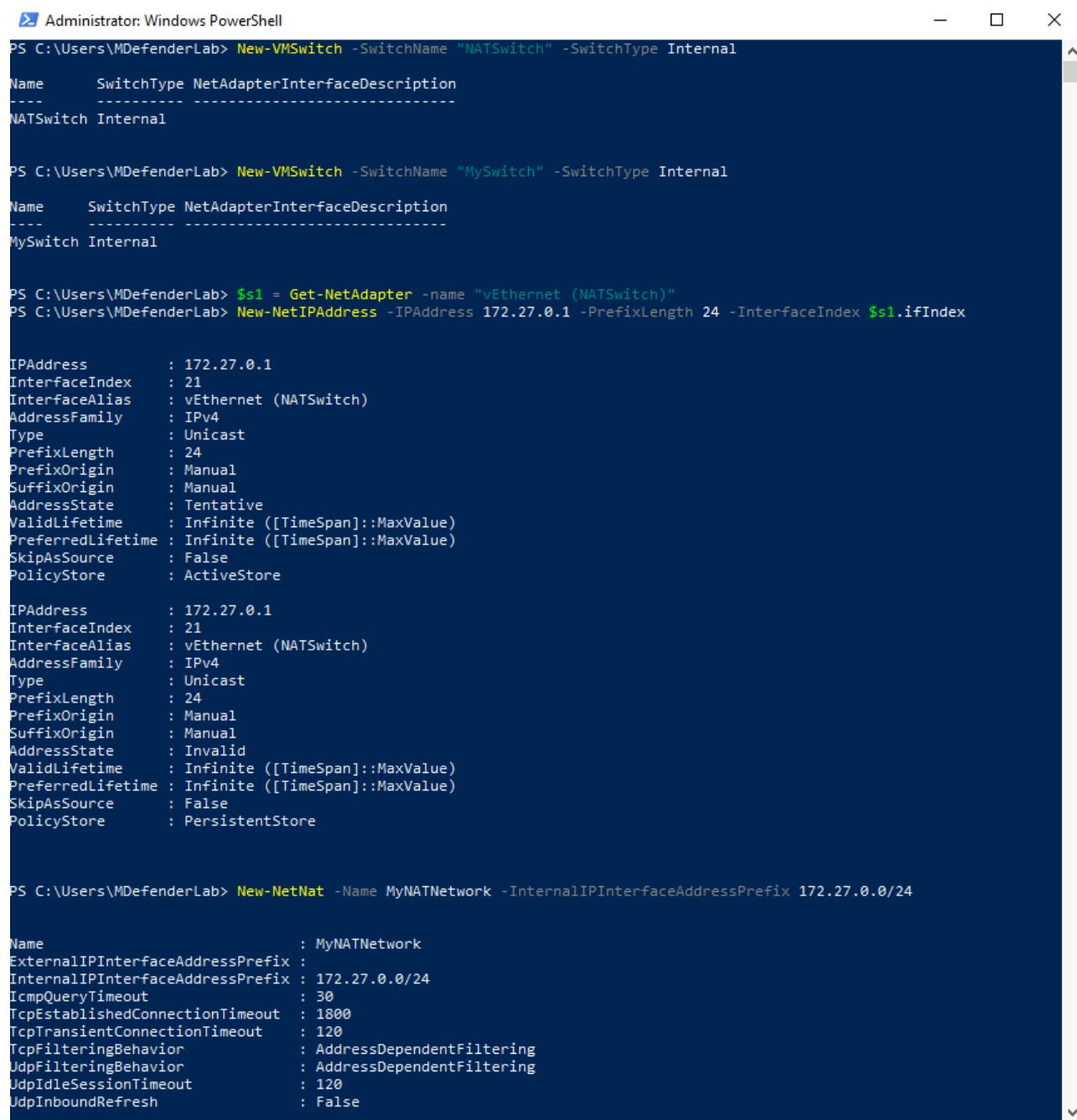
```
$s1 = Get-NetAdapter -name "vEthernet (NATSwitch)"
```

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". The command history is as follows:

```
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

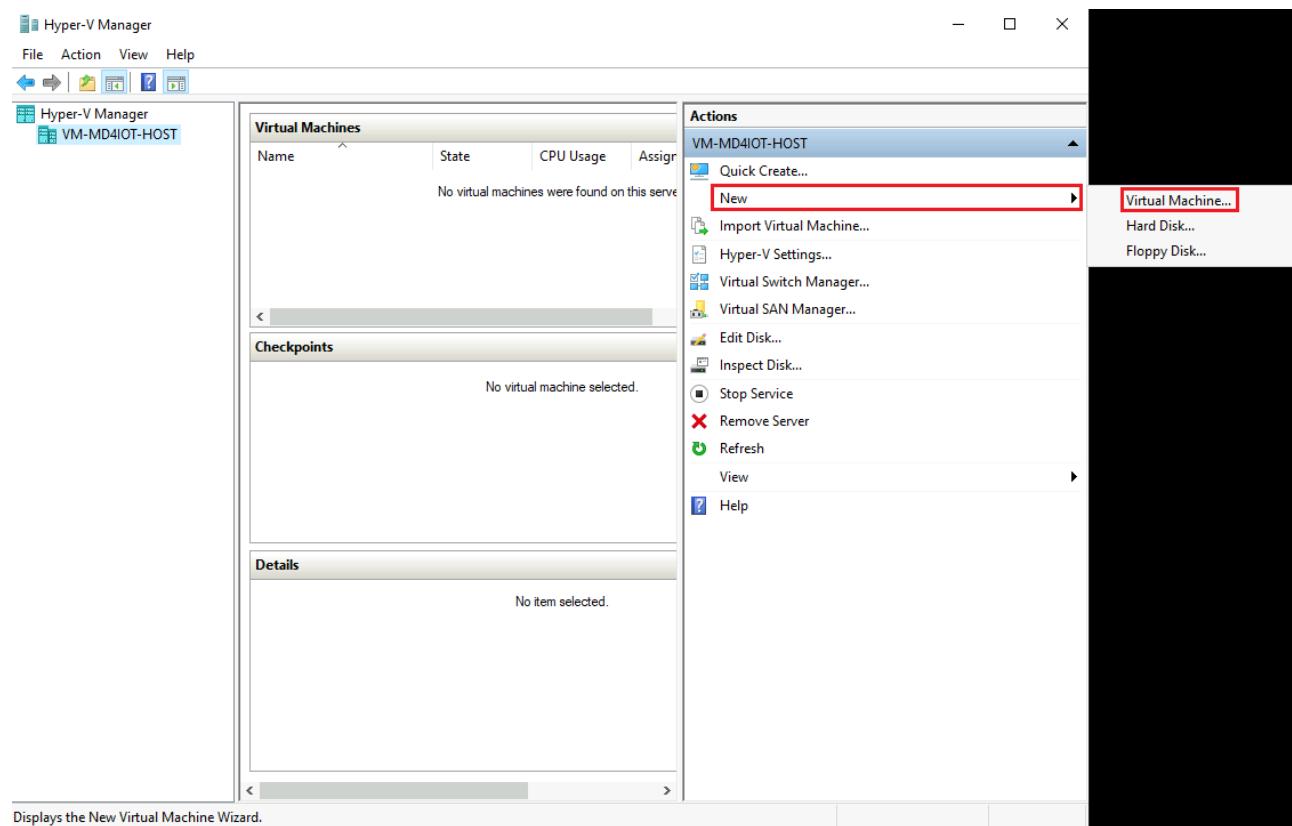
IPAddress      : 172.27.0.1
InterfaceIndex  : 21
InterfaceAlias  : vEthernet (NATswitch)
AddressFamily   : IPv4
Type           : Unicast
PrefixLength    : 24
PrefixOrigin    : Manual
SuffixOrigin    : Manual
AddressState    : Tentative
ValidLifetime   : Infinite ([TimeSpan]::.MaxValue)
PreferredLifetime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

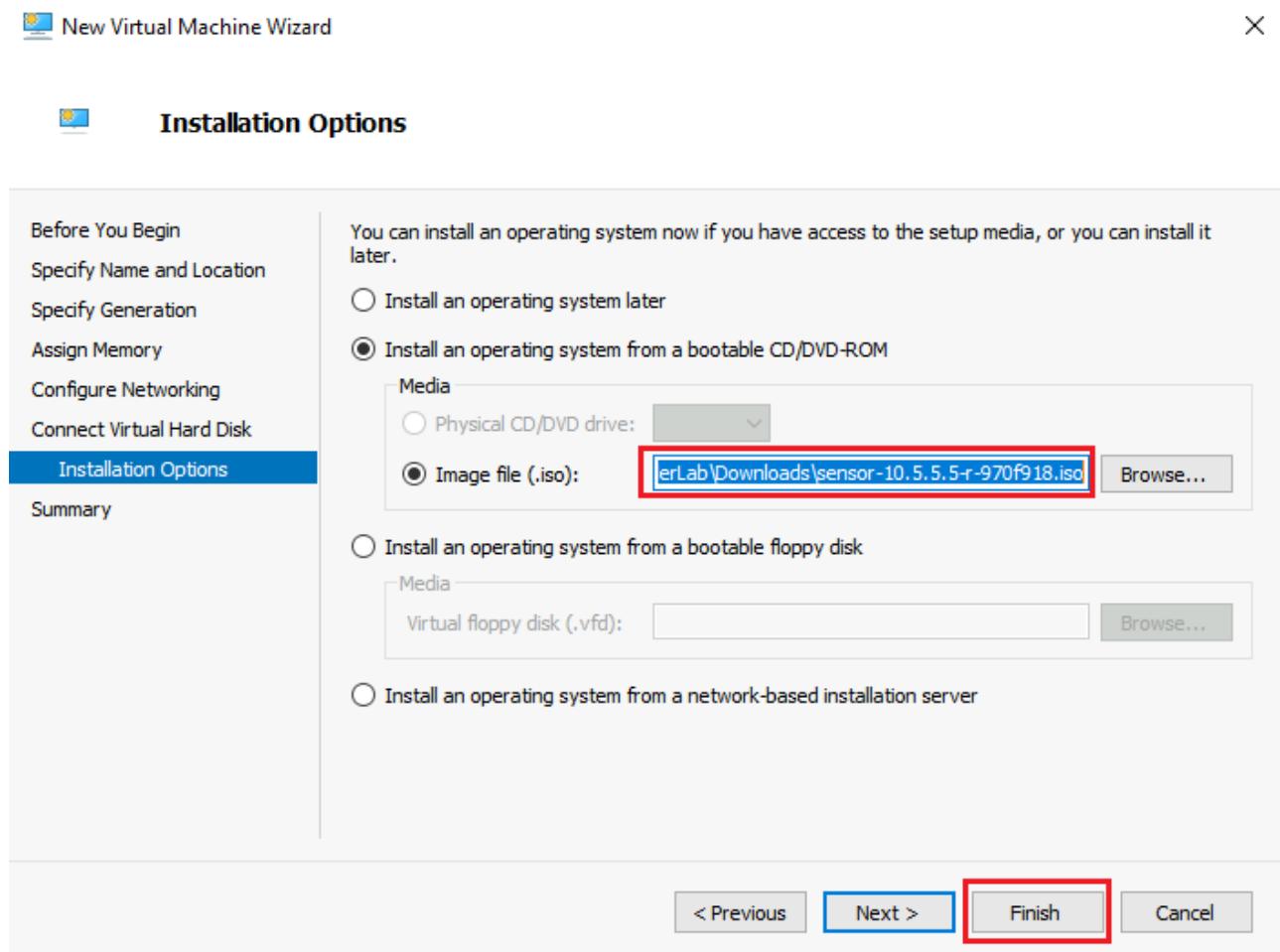
PS C:\Users\MDefenderLab> New-NetNat -Name MyNATNetwork -InternalIPInterfaceAddressPrefix 172.27.0.0/24

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 **md4iotssensoroffline** 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**



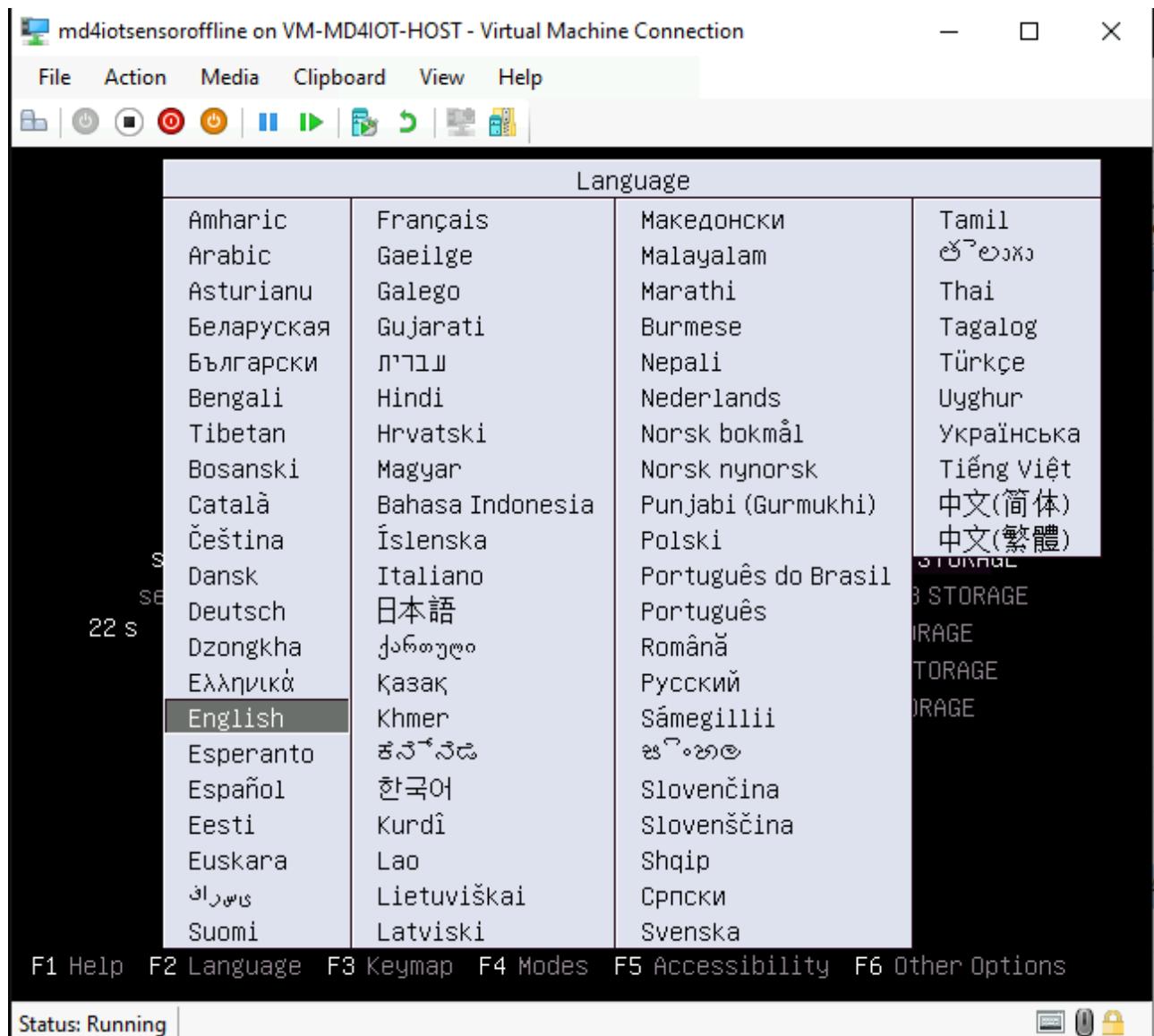
9. Right click on the Virtual machine that you just created, select **Settings** in the **Add Hardware** section and select **Network Adapter**, followed by clicking on **Add**. Now select the virtual switch created previously with the name **My Switch**, and click **Apply**. Increase the Processor number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

Task 2: Configure a Microsoft Defender for IoT offline sensor

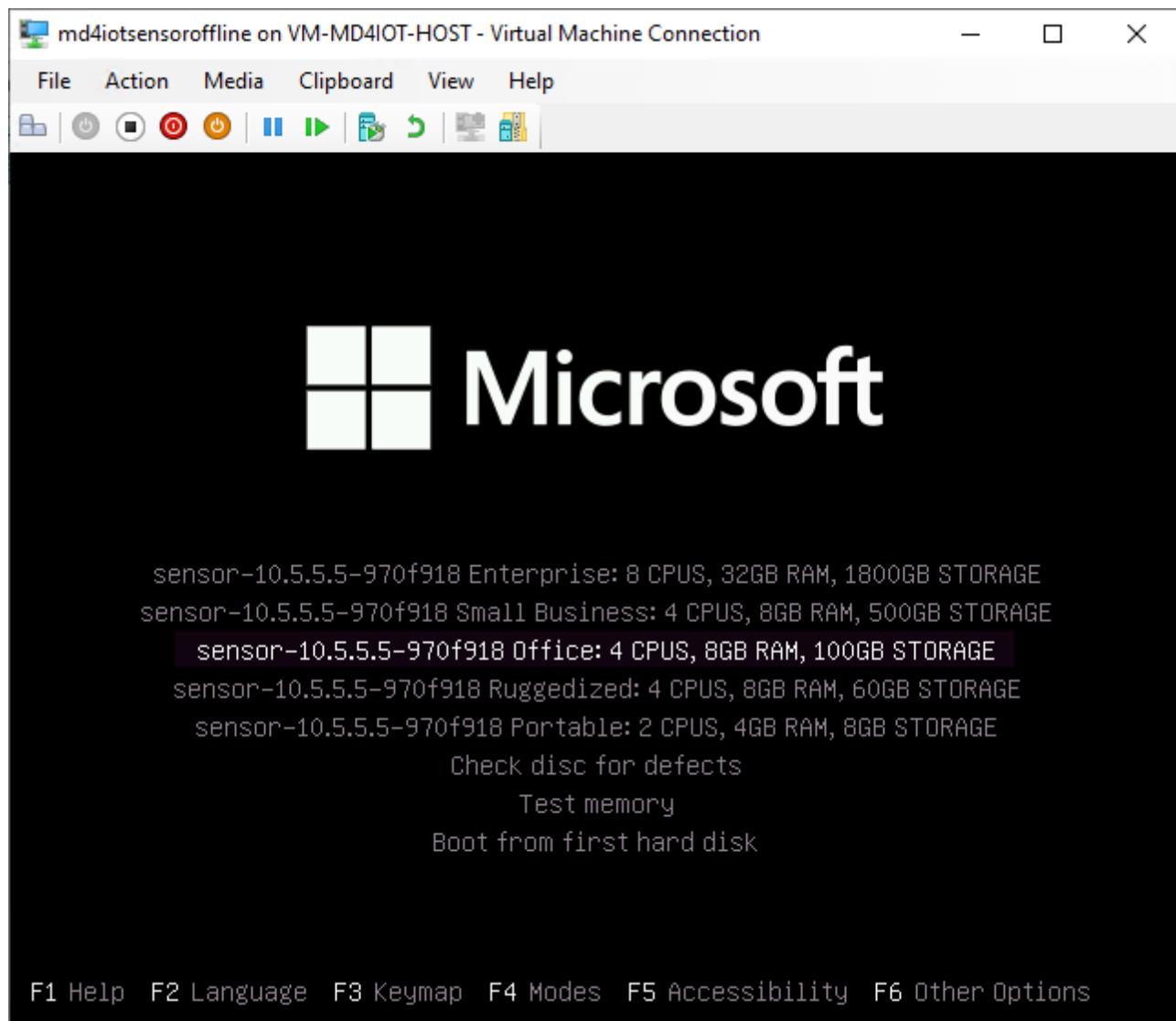
During this task we will configure Azure Defender based on the IPs highlighted before, this first configuration will be based on an offline sensor.

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
[Icons]
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@,gxr!0erf

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: qec2B0lbrpmcial^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

```

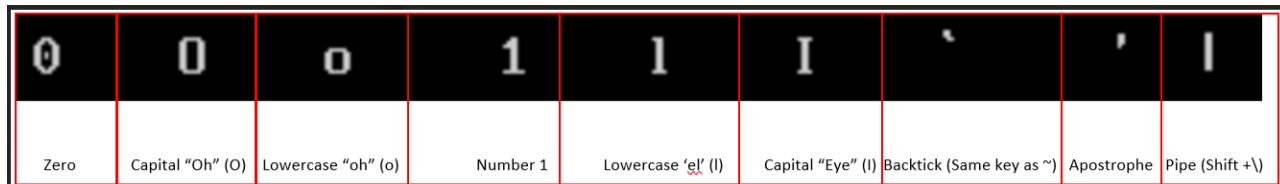
7. Once the installation finished you will ask to login, enter the credentials from previous step. In this screen you can also validate the IP, you will use that IP in your browser.

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.

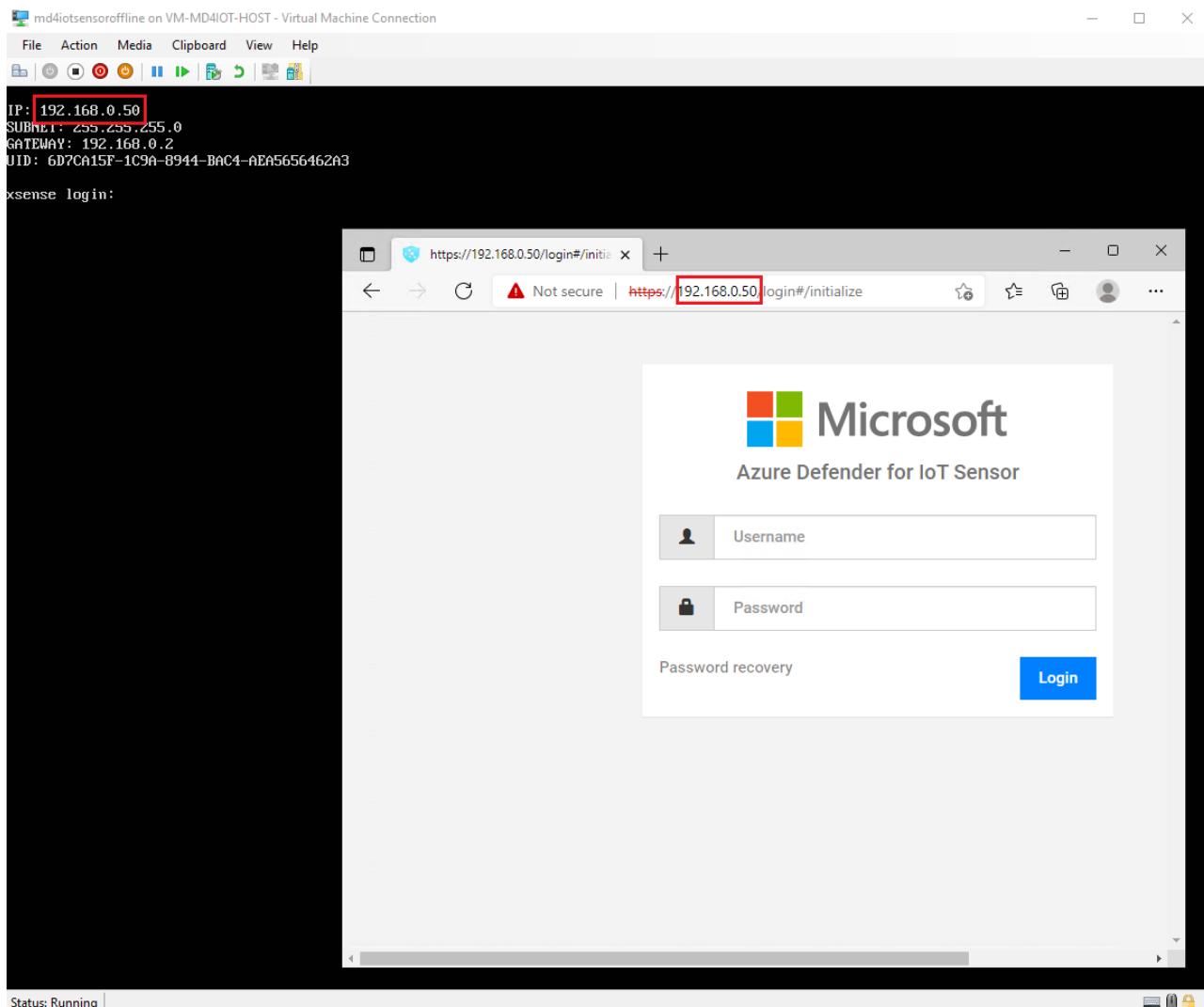
Troubleshooting Note: Once the installation is complete, you will be able to access Azure Defender Console. Check if you can open a cmd window, ping the IP Address you entered in the step 'Configure management network interface'. If the request times out, you will need to reconfigure this step again,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

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

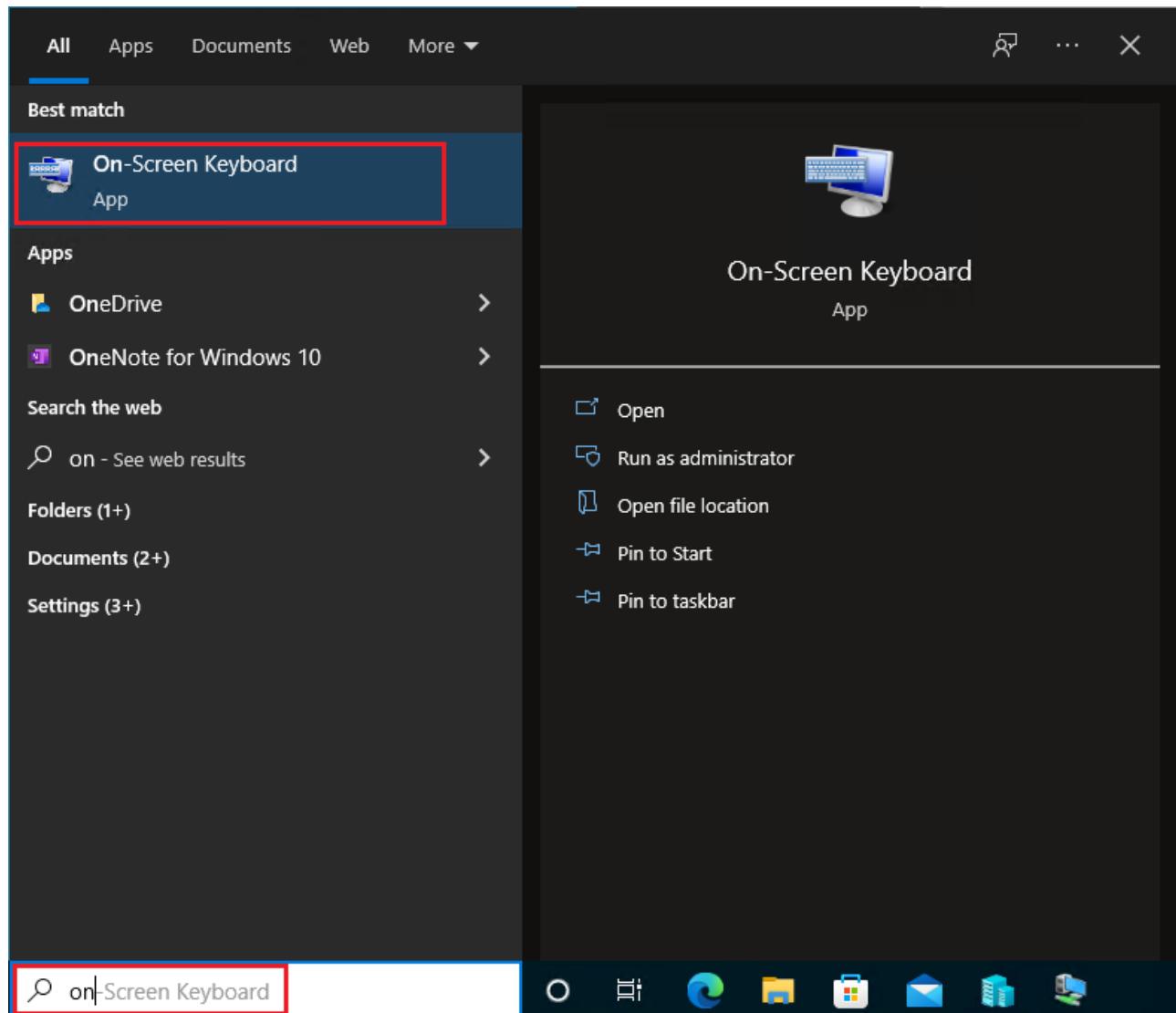
In the next steps you will be prompt to enter the password capture above, some characteres look alike but they are not, this image will help you to identify some of them.



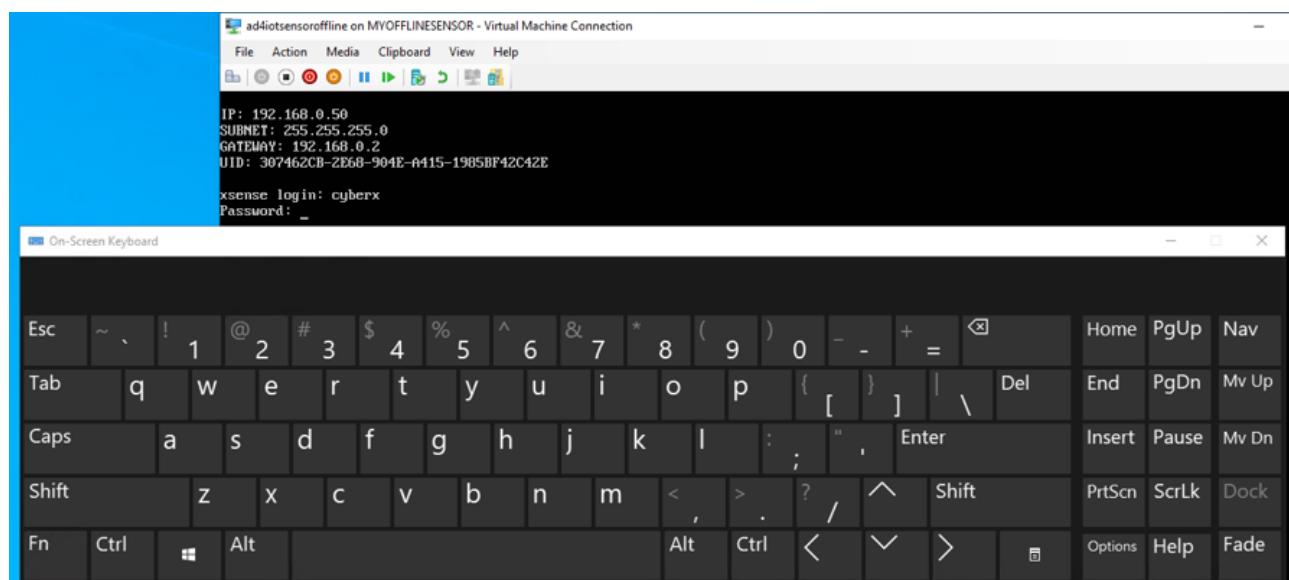
8. Login with the credentials provided in step 4.



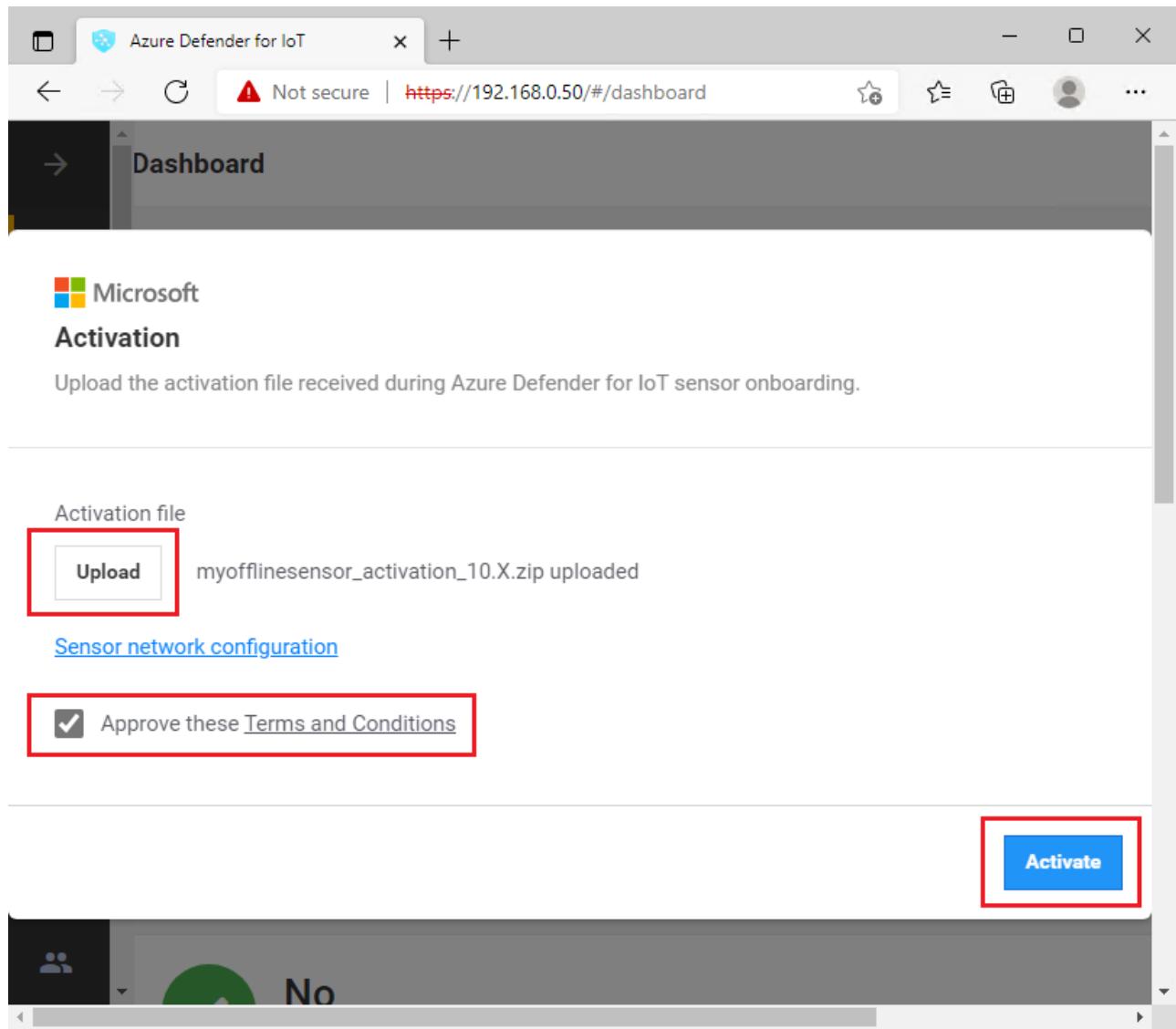
NOTE: the "md4iotsensoroffline" VM's keyboard layout is US by default, and it may not match the layout of your physical keyboard. To avoid issues when entering the password, you may use the windows 10 on-screen keyboard. To run it, type "osk" in the search box and click on "On-Screen Keyboard"...



...and use it to enter the credentials:

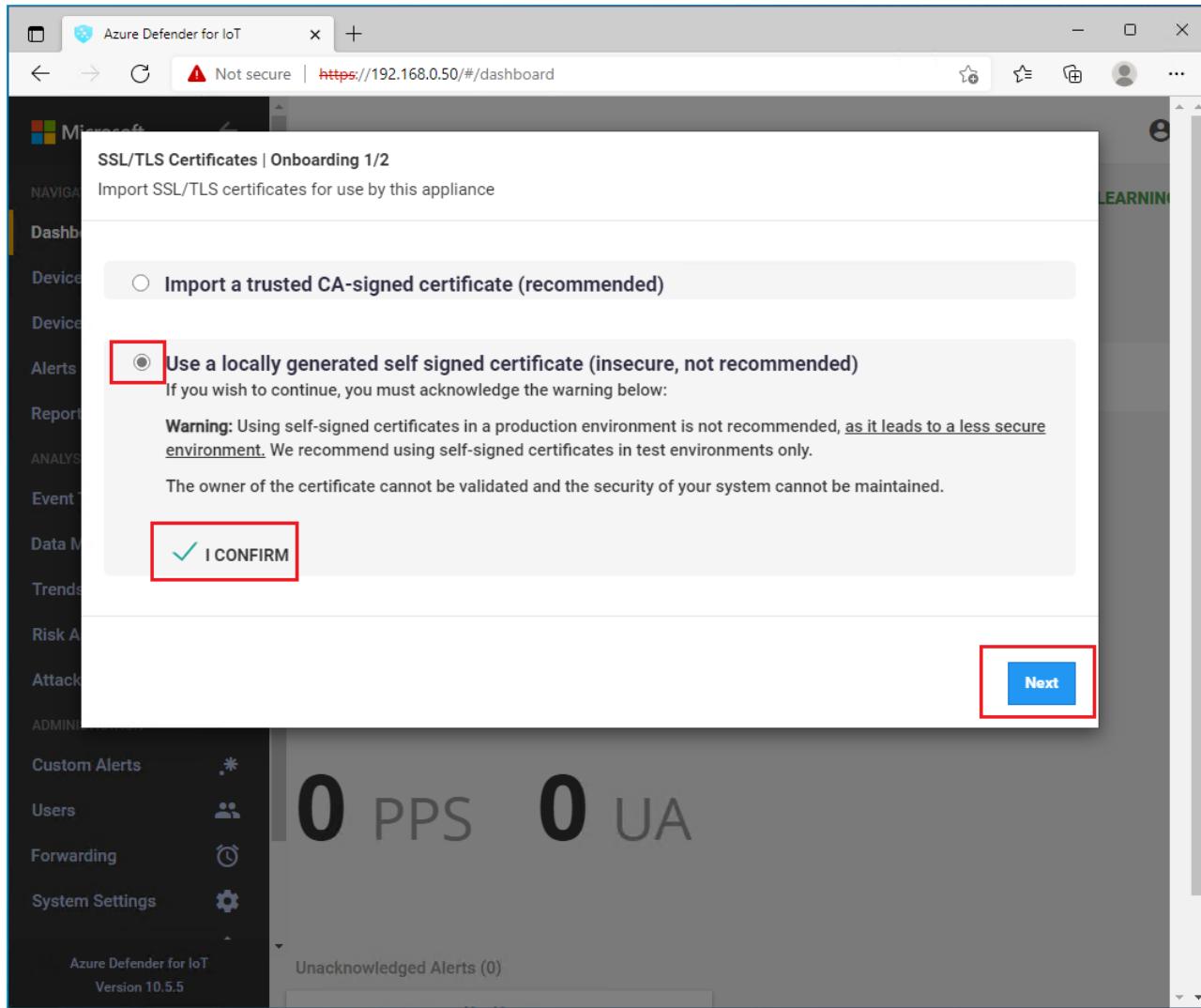


9. Next, you will be asked to activate the product, click **Upload**, then **Browse Files**, in your downloads folder select the file you downloaded from the Storage Explorer, in this example **myofflinesensor.zip**.



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.

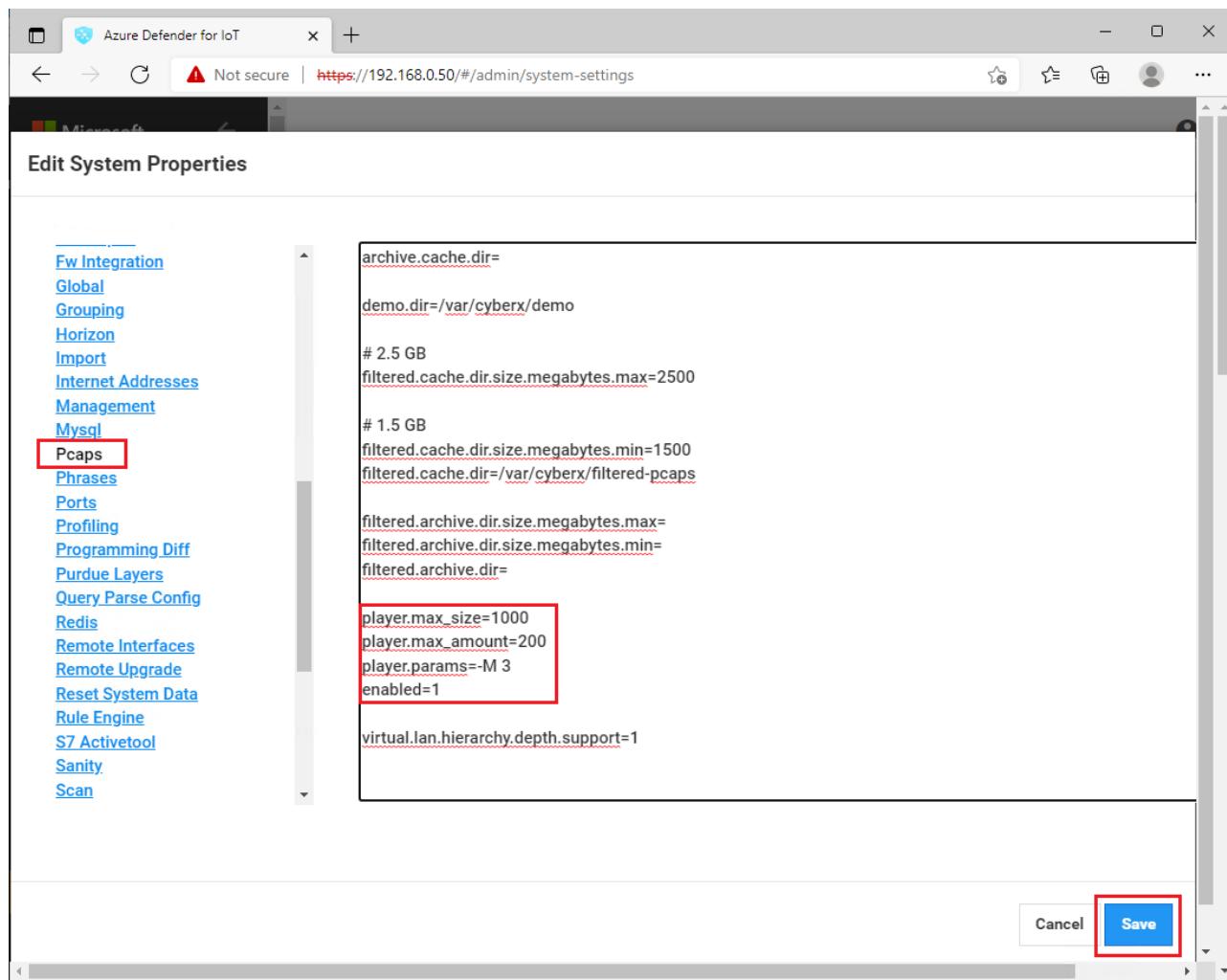
The screenshot shows the Azure Defender for IoT dashboard. On the left, a navigation sidebar lists various sections like Dashboard, Devices Map, Device Inventory, Alerts, Reports, Event Timeline, Data Mining, Trends & Statistics, Risk Assessment, Attack Vectors, Custom Alerts, Users, Forwarding, and System Settings. The 'System Settings' option is highlighted with a red box. The main dashboard area displays a welcome message: '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.' Below this, there are four green circular icons with checkmarks, each labeled 'No' followed by a severity level: 'Critical', 'Major', 'Minor', and 'Warnings'. To the right, a large digital clock shows '0 PPS' and '0 UA'. At the bottom, it says '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):

The screenshot shows the Azure Defender for IoT web interface. On the left, there's a navigation sidebar with various options like Dashboard, Devices Map, Device Inventory, Alerts, Reports, Event Timeline, Data Mining, Trends & Statistics, Risk Assessment, Attack Vectors, Custom Alerts, Users, Forwarding, and System Settings. The System Settings option is highlighted with a red box. The main content area has sections for Active Directory, Mail Server, ClearPass, SNMP MIB Monitoring, and ServiceNow. A prominent feature is the 'PCAP Player' section, which includes a play button icon, the text 'upload and replay PCAP files', and three buttons: 'Upload', 'Play All', and 'Clear All'. This entire 'PCAP Player' section is also highlighted with a red box. Below it is the 'Engines' section with a gear icon and the text 'controlling engines'. Under 'Engines', there are two entries: 'Protocol Violation' (Enabled) and 'Policy Violation' (Enabled). The URL in the browser bar is https://192.168.0.50/#/admin/system-settings.

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 web interface. On the left, there's a navigation sidebar with various options like Dashboard, Devices Map, Device Inventory, Alerts, Reports, Event Timeline, Data Mining, Trends & Statistics, Risk Assessment, Attack Vectors, Custom Alerts, Users, Forwarding, and System Settings. The System Settings option is highlighted with a red box. The main content area has several tiles: Active Directory, Mail Server, ClearPass, SNMP MIB Monitoring, and ServiceNow. Below these is a section titled 'PCAP Player' with the sub-instruction 'upload and replay PCAP files'. It features three buttons: 'Upload', 'Play All' (which is highlighted with a red box), and 'Clear All'. A list of PCAP files is shown: 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.

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

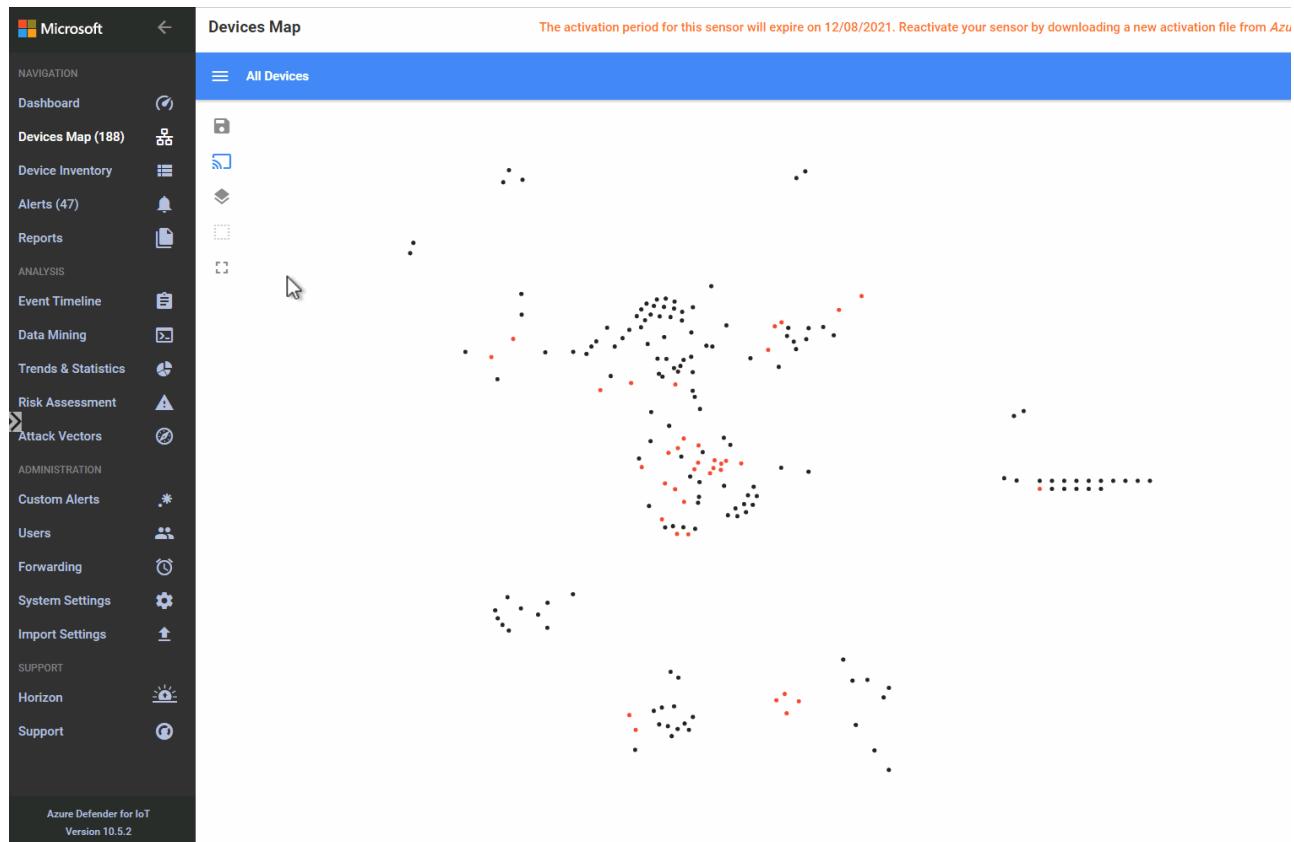
After Defender for Cloud learnt about your environment it will be able to share insights pretty fast.

Task 1: Devices Map

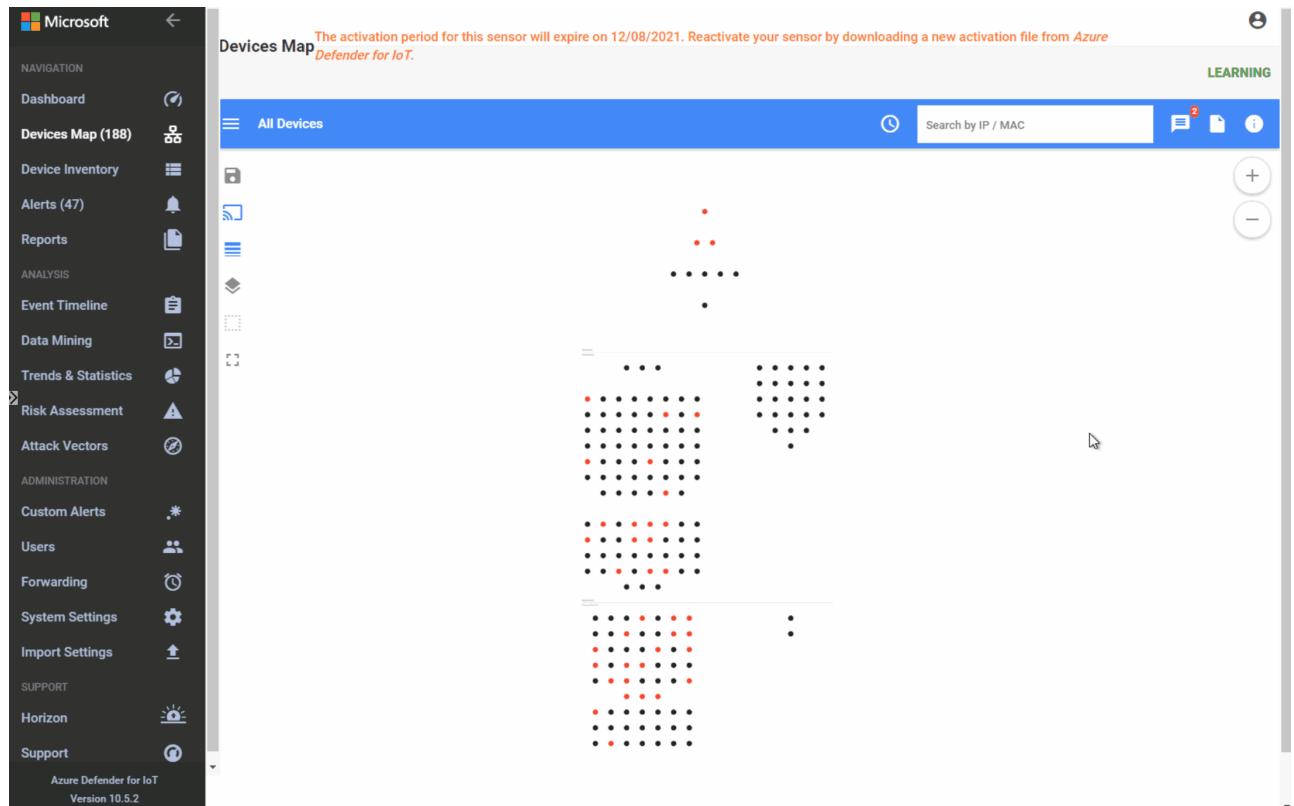
Your first interaction with Devices map you will see a similar map like the one below (details of what you actually see may vary):



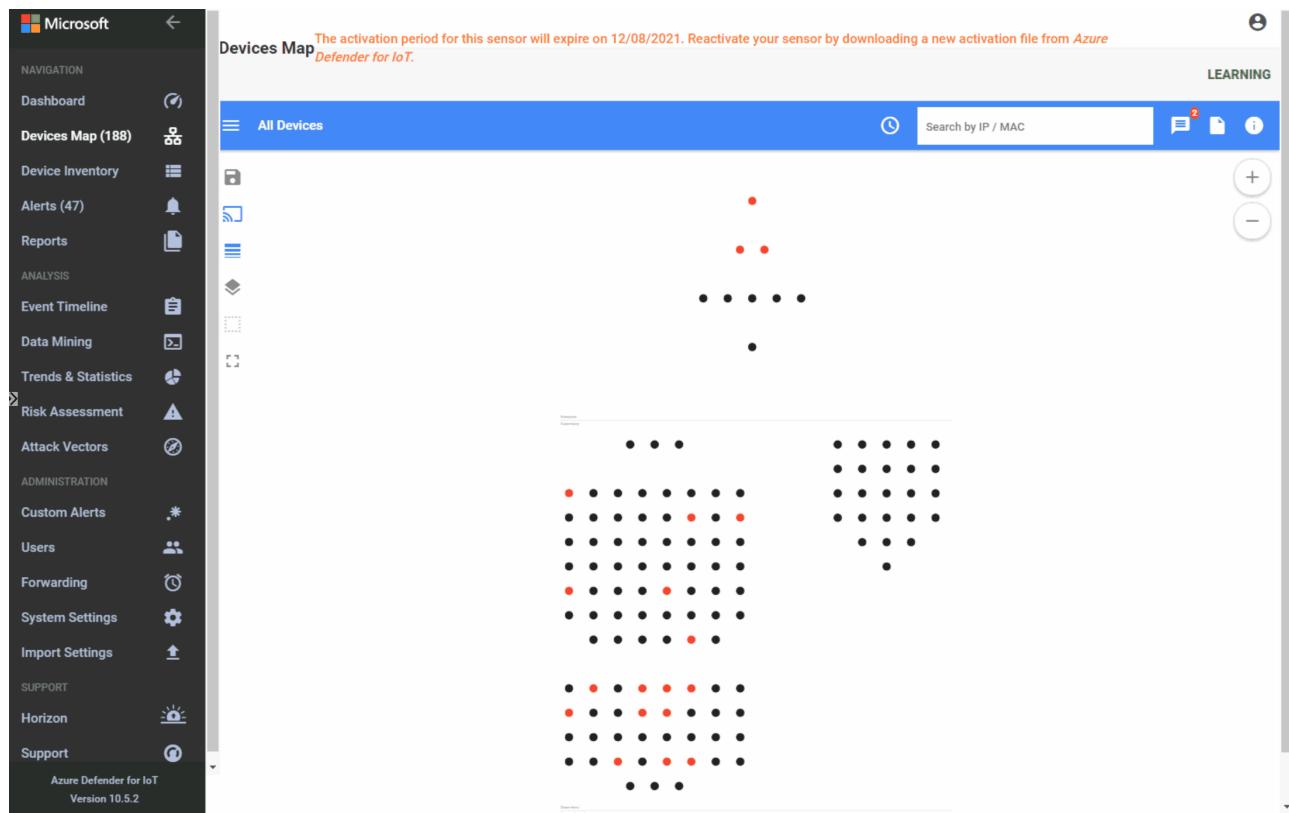
1. Use the four icon bar on the left to select **Layout by Purdue**. In this model you will see the different layers between Corporate IT and site operations.



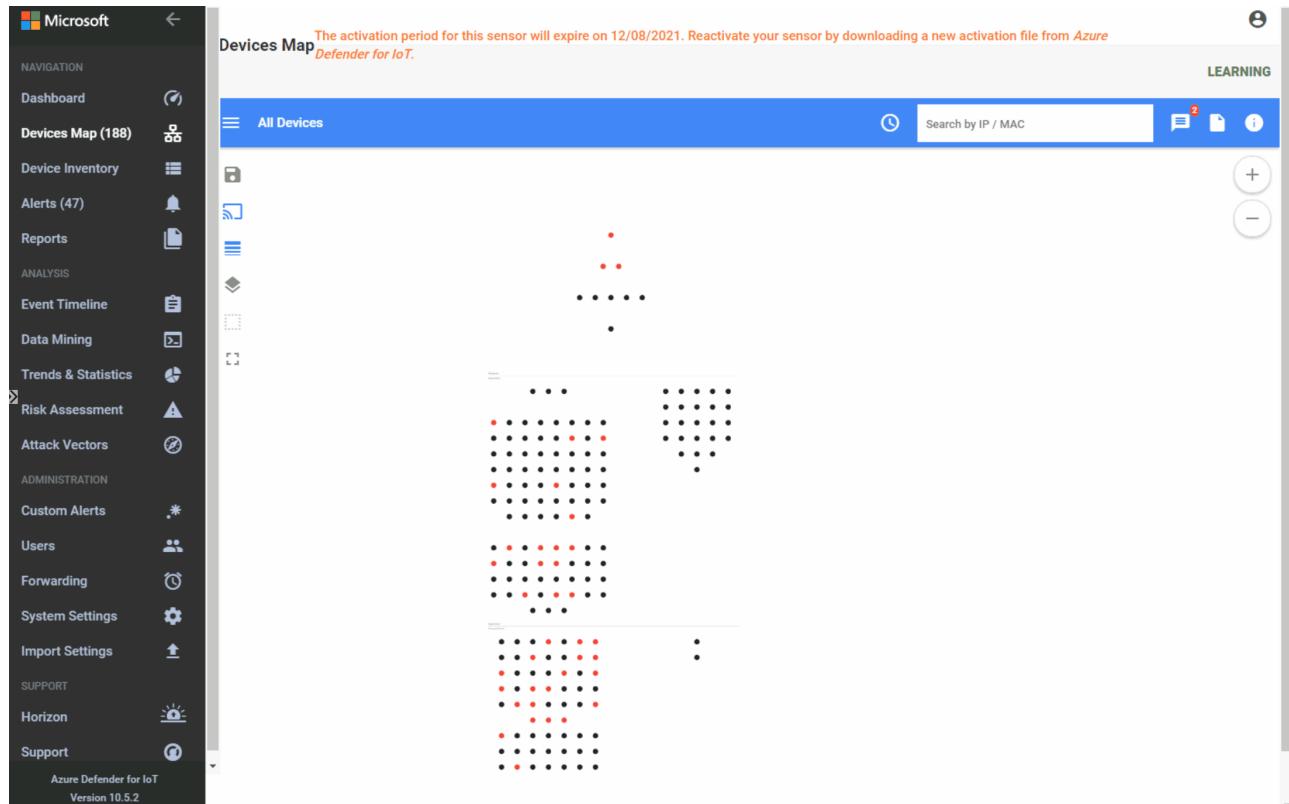
2. Check your notifications available and you can take action at this point.



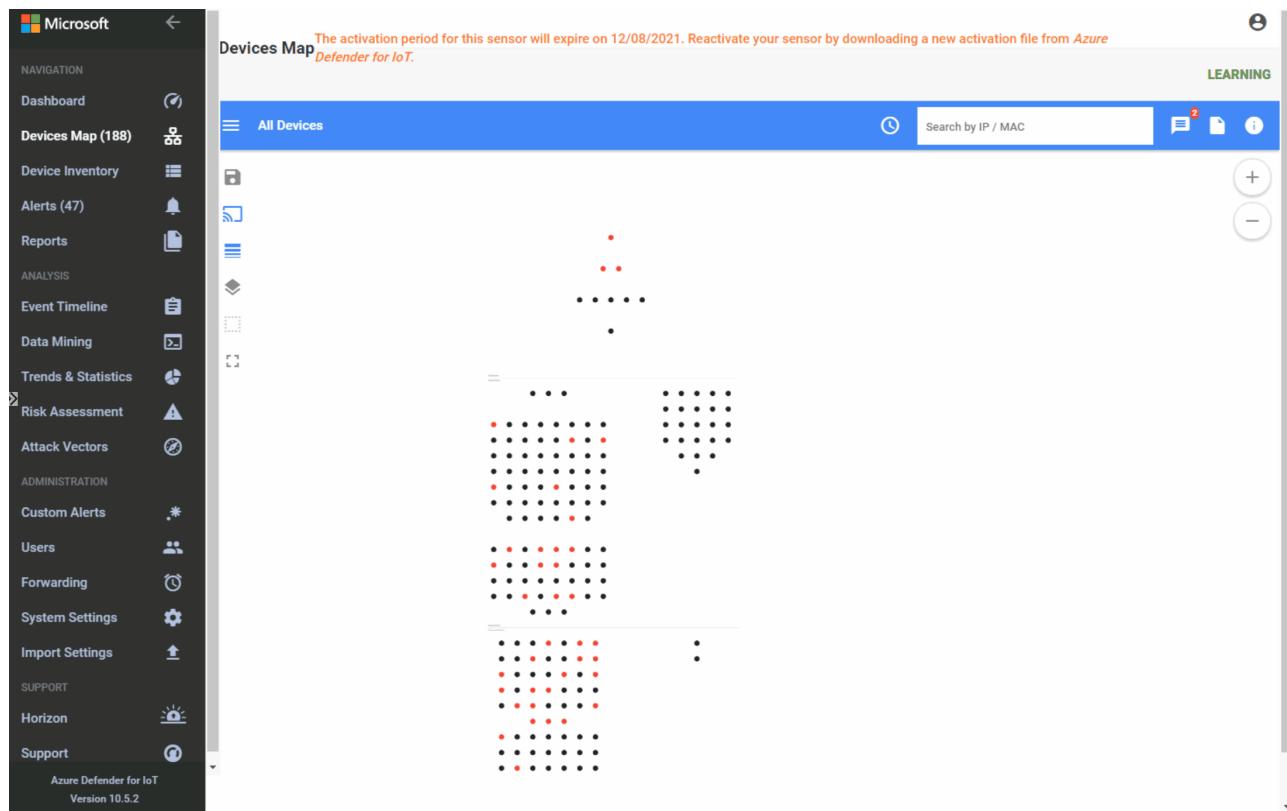
3. For each device right click to analyze properties, show events, reports and simulate attack vectors.



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 under the 'Alerts' section. It displays three main sections:

- Important Alerts (3):** Contains three operational alerts:
 - EtherNet/IP CIP Service Request Failed** | 16 hours ago: EtherNet/IP server 192.168.10.120 returned an error result Connection failure to client 192.168.10.1...
 - POLICY VIOLATION Firmware Change Detected** | 16 hours ago: Firmware was changed on a network asset. This may be a planned activity, for example an authorized...
 - OPERATIONAL Controller Stop** | 16 hours ago: Device 192.168.10.105 sent a stop command to controller 192.168.10.120 using protocol EtherNet/I...
- Pinned Alerts (0):** No Alerts
- Recent Alerts (3):** Contains three recent alerts:
 - POLICY VIOLATION Firmware Change Detected** Nov 9 15:53: Firmware was changed on a network asset. This may be a planned activity, for example an authorized...
 - OPERATIONAL EtherNet/IP CIP Service Request Failed** Nov 9 15:52: EtherNet/IP server 192.168.10.120 returned an error result Connection failure to client 192.168.10.1...
 - OPERATIONAL Controller Stop** Nov 9 15:52: Device 192.168.10.105 sent a stop command to controller 192.168.10.120 using protocol EtherNet/I...

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 under the 'Device Inventory' section. It displays a table of assets:

IP Address	Name	Last Seen	Type	Protocols	MAC Address	Vendor	Firmware Versi
192.168.1.8	PLANT	Nov 9, 2021 3:56:50 PM	Workstation	Netbios Datagram Service, SMB	00:1b:21:35:96:c2	INTEL CORPORATE	
192.168.1.14	PROD-2	Nov 9, 2021 3:56:50 PM	Workstation	Netbios Datagram Service, Netbios Name Service, SMB	00:02:a5:af:ee:fd	HEWLETT PACKARD	
224.0.0.252	224.0.0.252	Nov 9, 2021 3:56:50 PM	Multicast/Broadcast				
00:1b:1b:02:e6:78		Nov 9, 2021 3:56:50 PM	Unknown	Profinet DCP, Profinet Real-Time	00:1b:1b:02:e6:78	SIEMENS AG	
172.16.86.42	172.16.86.42	Nov 9, 2021 3:56:50 PM	PLC	BACNet, BACNet (NPDU)			3.6.38
172.16.36.205	172.16.36.205	Nov 9, 2021 3:56:50 PM	HMI	BACNet, BACNet (NPDU)			
192.168.1.121	192.168.1.121	Nov 9, 2021 3:56:50 PM	Unknown		00:a0:d1:2e:13:74	INVENTEC CORPORATION	
00:1b:1b:02:e6:0f		Nov 9, 2021 3:56:50 PM	Unknown	Profinet DCP, Profinet Real-Time	00:1b:1b:02:e6:0f	SIEMENS AG	
172.16.36.1	172.16.36.1	Nov 9, 2021 3:56:50 PM	PLC	BACNet, BACNet (NPDU)	00:21:70:b1:d1:08	DELL INC.	3.30
00:1b:1b:35:84:10		Nov 9, 2021 3:56:50 PM	Unknown	Profinet DCP, Profinet Real-Time	00:1b:1b:35:84:10	SIEMENS AG	
192.168.1.117	LAW	Nov 9, 2021 3:56:50 PM	Workstation	Netbios Datagram Service, Netbios Name Service, RPC Endpoint Mapper, SMB	00:1c:23:f3:38:73	DELL INC.	
192.168.1.128	LAPTOP-2	Nov 9, 2021 3:56:50 PM	Workstation	Netbios Datagram Service, Netbios Name Service, SMB	00:0d:9d:45:63:14	HEWLETT PACKARD	
172.16.1.120	172.16.1.120	Nov 9, 2021 3:56:50 PM	Unknown		00:04:75:e2:44:8f	3COM	
192.168.25.177	192.168.25.177	Nov 9, 2021 3:56:50 PM	HMI	Siemens S7 Plus			
192.168.1.23	192.168.1.23	Nov 9, 2021 3:56:50 PM	Unknown		00:02:a5:96:65:9a	HEWLETT PACKARD	
192.168.1.32	SHIPPING	Nov 9, 2021 3:56:50 PM	Workstation	Netbios Datagram Service, Netbios Name Service, SMB	00:02:a5:c8:4c:45	HEWLETT PACKARD	
192.168.0.90	192.168.0.90	Nov 9, 2021 3:56:50 PM	Unknown		00:07:e9:7e:08:0e	INTEL CORPORATION	
192.168.1.111	PROD-15	Nov 9, 2021 3:56:50 PM	Workstation	Netbios Datagram Service, Netbios Name Service, SMB	00:02:a5:e3:de:de	HEWLETT PACKARD	
192.168.1.102	192.168.1.102	Nov 9, 2021 3:56:50 PM	Unknown	Netbios Name Service			
192.168.1.115	PROD-3	Nov 9, 2021 3:56:50 PM	Workstation	Netbios Datagram Service, Netbios Name Service, SMB	00:02:a5:94:08:4b	HEWLETT PACKARD	
172.16.36.2	172.16.36.2	Nov 9, 2021 3:56:50 PM	HMI	BACNet, BACNet (NPDU)			
192.168.0.52	192.168.0.52	Nov 9, 2021 3:56:50 PM	Unknown		00:08:a1:61:70:fc	CNET TECHNOLOGY INC.	

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' interface in the Azure Defender for IoT portal. The left sidebar has a 'Data Mining' section highlighted with a red box. The main form has a 'Name' field set to 'PLC Firmware Versions' and a 'Description' field containing the text 'This report shows the firmware versions for different PLCs'. Under 'Order By', the 'Category' tab is selected. In the 'Filters' section, there's a dropdown for 'Device' with 'Firmware Version (GENERIC)' selected, which is also highlighted with a red box. Other filter options include 'Additional Data (GENERIC)', 'Model (GENERIC)', 'Module Address (GENERIC)', 'Rack (GENERIC)', 'Serial (GENERIC)', and 'Slot (GENERIC)'. There are also fields for 'IP Address', 'Port', and 'MAC Address' with their respective examples. At the bottom right are 'Close' and 'Save' buttons.

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.

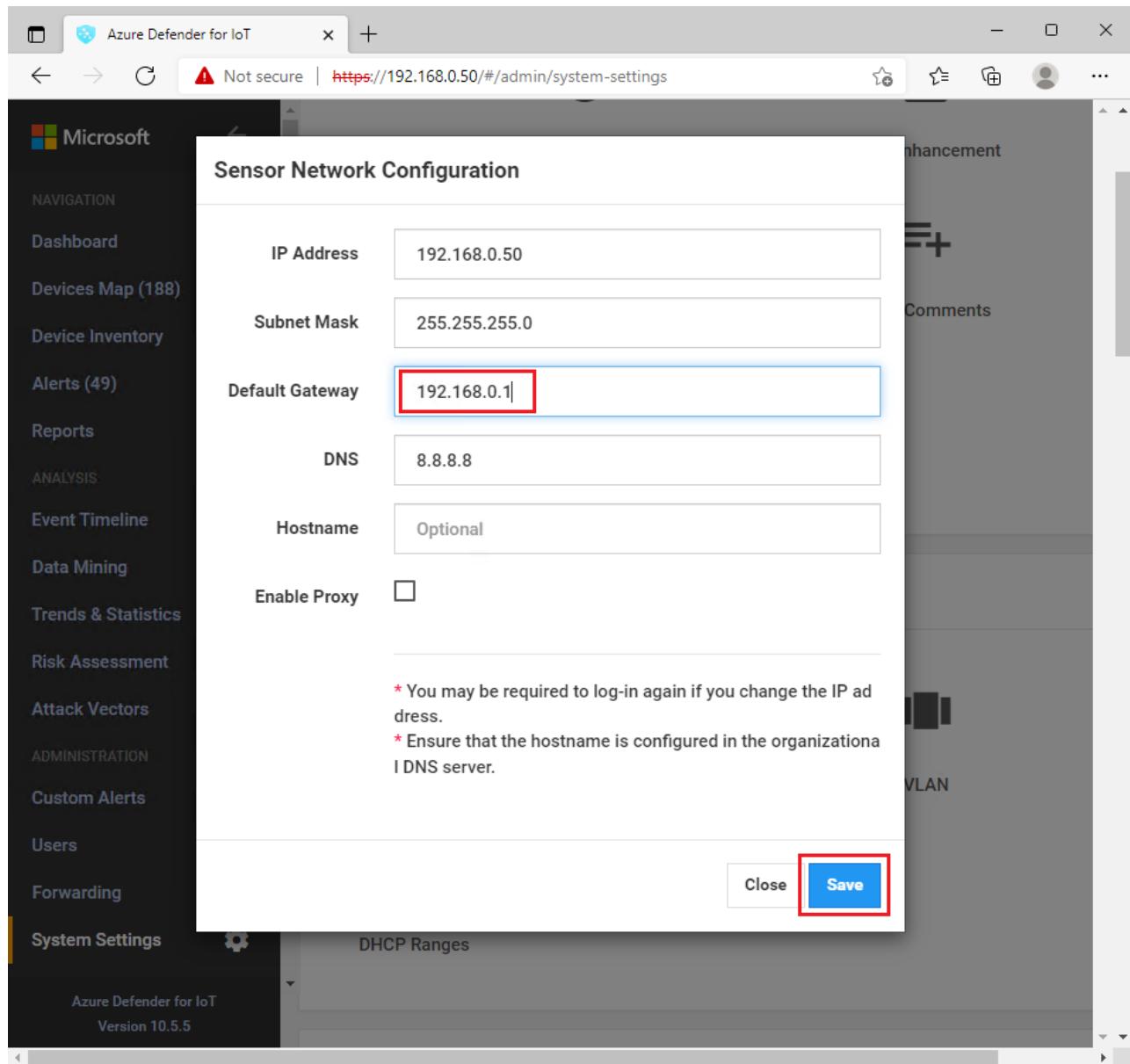
Task 1: Reconfiguring sensor

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

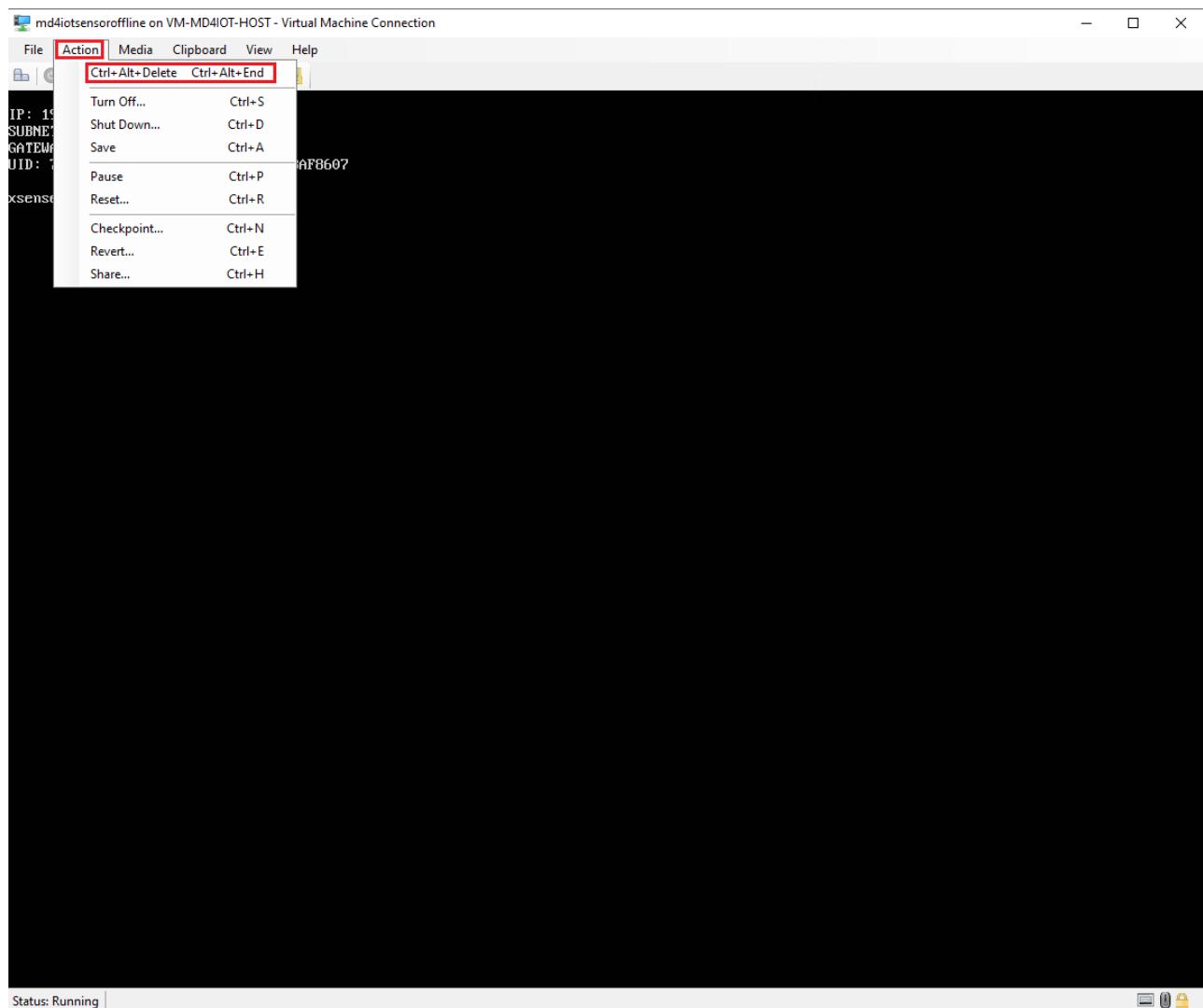
1. In your sensor's Azure Defender for IoT Portal (in the Virtual Machine), select **System Settings** and **Network**.

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' currently selected. The main content area has tabs for System Statistics, Time & Regional, Access Tokens, and Data Enhancement. Below these are several icons: Connection to Management Console, Reactivation, Export, Alert Comments, System Properties, and SSL/TLS Certificates. A large section titled 'Networking' contains icons for Network (which is highlighted with a red box), Subnets, Port Aliases, VLAN, and DHCP Ranges.

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. On the left, there's a navigation sidebar with various options like Dashboard, Devices Map, Device Inventory, Alerts, Reports, Event Timeline, Data Mining, Trends & Statistics, Risk Assessment, Attack Vectors, Custom Alerts, Users, Forwarding, Auto Discovery, and System Settings. The 'System Settings' option is selected and highlighted with a red box. At the bottom of the sidebar, it says '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 has several icons and links: System Statistics, Time & Regional, Access Tokens, Data Enhancement, Connection to Management Console, Export, Alert Comments, System Properties, and SSL/TLS Certificates. The 'Networking' section has icons for Network, Subnets, Port Aliases, VLAN, and DHCP Ranges. The 'Active Discovery' section is currently empty. At the bottom of the main content area, it says '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:

hub-md4iot-mst01 IoT Hub

IoT Hub Usage

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

Number of messages used

Number of messages used (Max) hub-md4iot-mst01 2

Device to cloud messages

Telemetry messages sent (Count) hub-md4iot-mst01

Connected Devices

Connected devices (Max) hub-md4iot-mst01

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.

The screenshot shows the Microsoft Azure portal interface for an IoT Hub named 'hub-md4iot-mst01'. The left sidebar has a 'Defender for IoT' section with 'Security Alerts' selected, indicated by a red box. The main content area displays a table of security alerts:

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 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**

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.

The screenshot shows the Microsoft Sentinel Data connectors page. On the left, there's a navigation sidebar with options like Create, Manage view, Filter for any field..., Name (sorted), and a workspace dropdown showing 'MyLogWorkspace-mst02'. Below these are sections for Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence), Content management (Content hub (Preview), Repositories (Preview), Community), Configuration (Data connectors, Analytics, Watchlist, Automation), and a bottom navigation bar with Page 1 of 1.

The main area is titled 'Microsoft Sentinel | Data connectors' and shows '120 Connectors' with '1 Connected'. A search bar at the top right contains the text 'defender'. The results list includes:

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

2. Click the **Open Connector Page**

Microsoft Defender for IoT (Preview)

Not connected Status Microsoft Provider 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 0

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.

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	Connect 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	Connect Disconnect 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.

The screenshot shows the Microsoft Azure Microsoft Sentinel - Microsoft Defender for IoT (Preview) interface. At the top, there's a navigation bar with 'Home > Microsoft Sentinel > Microsoft Sentinel > Microsoft Defender for IoT (Preview)'. Below the navigation, there's a 'Instructions' section with a 'Next steps' button highlighted by a red box. Under 'Recommended workbooks', there's a link to 'Azure Defender for IoT Alerts' from Microsoft. In the 'Query samples' section, there are two examples: 'All logs' and 'Summarize by severity', each with a 'Run' button. Below that, under 'Relevant analytics templates (1)', there's a table with one item: 'High Create incidents based on Azure Defender f...' with 'Microsoft Secur...' and 'Microsoft Defender ...' data sources, and a 'Tactics' column. A 'CREATE RULE' button is at the top right of the table, and a 'Create rule' button is highlighted with a red box at the bottom right of the table row.

- 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.

The screenshot shows the 'Analytics rule wizard - Create new rule from template' page. The title is 'Analytics rule wizard - Create new rule from template' with a back arrow. Below it, a sub-header says 'Create incidents based on Azure Defender for IOT alerts'. There are three tabs: 'General', 'Automated response', and 'Review and create', with 'Review and create' being the active tab. A green success message 'Validation passed.' is displayed. The 'Analytics rule details' section shows a 'Name' of 'MyNewRule', a 'Description' of 'Create incidents based on all alerts generated in Azure Defender for IOT', and a 'Status' of 'Enabled'. The 'Analytics rule logic' section includes settings for 'Microsoft security service' (Microsoft Defender for IoT), 'Filter by severity' (Any), 'Include by alert name(s)' (Any), and 'Exclude by alert name(s)' (Any). The 'Automated response' section shows 'Incident trigger (preview)' as 'Not configured'. At the bottom, there are 'Previous' and 'Create' buttons, with 'Create' highlighted by a red box.

- 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, there's a navigation sidebar with various options like Home, Microsoft Sentinel, Threat management, Content management, Configuration, and Analytics (which is selected). The main area displays a list of 'Active rules' with a red box around the 'Rule templates' tab. A search bar and filters for Severity (All), Rule Type (All), Tactics (All), and Data sources (All) are visible. The list includes several entries such as 'TEARDROP memory-only dropper', 'Exchange SSRF Autodiscover ProxyShell - Detection', and 'Alsid Password Guessing'. On the right, a detailed view of a specific rule template for 'TEARDROP memory-only dropper' is shown, with a red box around the 'Create rule' button at the bottom.

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 a red box around the 'Alerts (48)' option. The main area shows a list of 'Important Alerts (48)' under the 'POLICY VIOLATION' category. Each alert entry includes a checkbox. One checkbox is checked and highlighted with a red box, while others are unchecked. A large red box highlights the 'Acknowledge All' button at the top right of the alert list.

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, there is a sidebar with various navigation options: 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' option is highlighted with a red box. At the top right, there are links for Active Directory, Mail Server, and ClearPass. The main content area is titled 'PCAP Player' with the sub-instruction 'upload and replay PCAP files'. It features a large play button icon. Below the title are three buttons: 'Upload', 'Play All' (which is also highlighted with a red box), and 'Clear All'. A list of PCAP files is displayed below these buttons:

- 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

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 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 Settings

Open incidents by severity

Severity	Count
High (4)	4
Medium (10)	10
Low (2)	2
Informational (0)	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	Unassigned
High	15	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Low	14	Outstation Restarted	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Medium	13	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Medium	12	Firmware Change Detected	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Low	11	Controller Stop	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
High	10	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Medium	9	EtherNet/IP CIP Service Requ...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Medium	8	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
High	7	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Medium	6	Unknown Object Sent to Out...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Medium	5	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unassigned
Medium	4	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unassigned
Medium	3	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unassigned
Medium	2	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unassigned

< 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 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 Settings

Open incidents by severity

Severity	Count
High (4)	4
Medium (10)	10
Low (2)	2
Informational (0)	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	Unassigned
High	15	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Low	14	Outstation Restarted	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Medium	13	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Medium	12	Firmware Change Detected	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Low	11	Controller Stop	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
High	10	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Medium	9	EtherNet/IP CIP Service Requ...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Medium	8	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
High	7	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Medium	6	Unknown Object Sent to Out...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unassigned
Medium	5	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unassigned
Medium	4	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unassigned
Medium	3	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unassigned
Medium	2	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unassigned

Unauthorized Internet Connectivity Detected Incident ID: 16 Investigate in Microsoft Defender for IoT

Owner: Unassigned Status: New Severity: High

Description: A source device defined as part of your network is communicating with Internet addresses. The source is not authorized to communicate with Internet addresses.

Evidence: N/A Events: 1 Alerts: 0 Bookmarks: 0

Last update time: 01/25/22, 04:42 PM Creation time: 01/25/22, 04:42 PM

Entities (4): 141.81.0.130, 10.200.1.134, HUB-MD4OT-MST..., 10.200.1.124

Tactics (1): Initial Access

View full details >

Tags: View full details Actions

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.

The screenshot shows the Microsoft Azure Microsoft Sentinel Incident view. A specific incident titled "Unauthorized Internet Connectivity Detected" is selected. The "Investigate" button at the bottom left of the main content area is highlighted with a red box. The incident details include a timeline entry for "Jan 25 4:41 PM" with the message "Unauthorized Internet Connectivity Detected [High] | Detected by Microsoft Defender for IoT | Tactics: Initial Access". The right pane displays detailed information about the incident, such as its status (High severity, New), entities involved (141.81.0.130, 10.200.1.124, HUB-MD4IOT-MST01, 10.200.1.124), and tactics used (Initial Access). The "Investigate" button is also highlighted in the bottom navigation bar.

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

The screenshot shows the Microsoft Azure Microsoft Sentinel Investigation view. It displays a network graph where a central shield icon represents the "Unauthorized Internet Connectivity Detected" incident. Four nodes are connected to it: "141.81.0.130", "10.200.1.124", "10.200.1.124", and "HUB-MD4IOT-MST01". The "Investigate" button at the top left of the main content area is highlighted with a red box. The right pane shows the detailed description of the incident: "A source device defined as part of your network is communicating with Internet addresses. The source is not authorized to communicate with Internet addresses." The "Investigate" button is also highlighted in the bottom navigation bar.

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"
```

The screenshot shows the Microsoft Sentinel Log Analytics workspace. On the left, the navigation pane is visible with sections like General, Overview, Logs (which is selected and highlighted with a red box), News & guides, Threat management, Content management, and Configuration. The main area displays a query editor with the following content:

```

New Query 1*
MyLogWorkspace-mst02
Run Time range : Last 24 hours
1 SecurityAlert
2 | where ProviderName contains "IoTSecurity"
    
```

The results table shows 51 records from the last 24 hours. The columns include TimeGenerated [UTC], DisplayName, AlertName, AlertSeverity, and Description. Some entries are collapsed. The results table has a header row and approximately 10 data rows.

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

The screenshot shows the Microsoft Sentinel Log Analytics workspace. The navigation pane is partially visible on the left. The main area displays a query editor with the following content:

```

Run Time range : Last 7 days
1 SecurityAlert
2 | where CompromisedEntity == "hub-md4iot-mst01"
    
```

The results table shows 5 items from the last 7 days. The columns include TimeGenerated [UTC], DisplayName, AlertName, AlertSeverity, and Description. The results table has a header row and approximately 5 data rows.

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            172.22.16.1:57242    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
tintcp6    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.
sin=
```