

[mpram / Azure-Defender-for-IoT](#) Public

[Code](#)[Issues](#)[Pull requests](#)[Actions](#)[Projects](#)[Wiki](#)[Security](#)[main](#) 

[Azure-Defender-for-IoT / HOL Steps](#) / Azure Defender for IoT HOL.md

**mpram** Azure Defender for IoT/OT HOL History

3 contributors



690 lines (351 sloc) | 31.5 KB

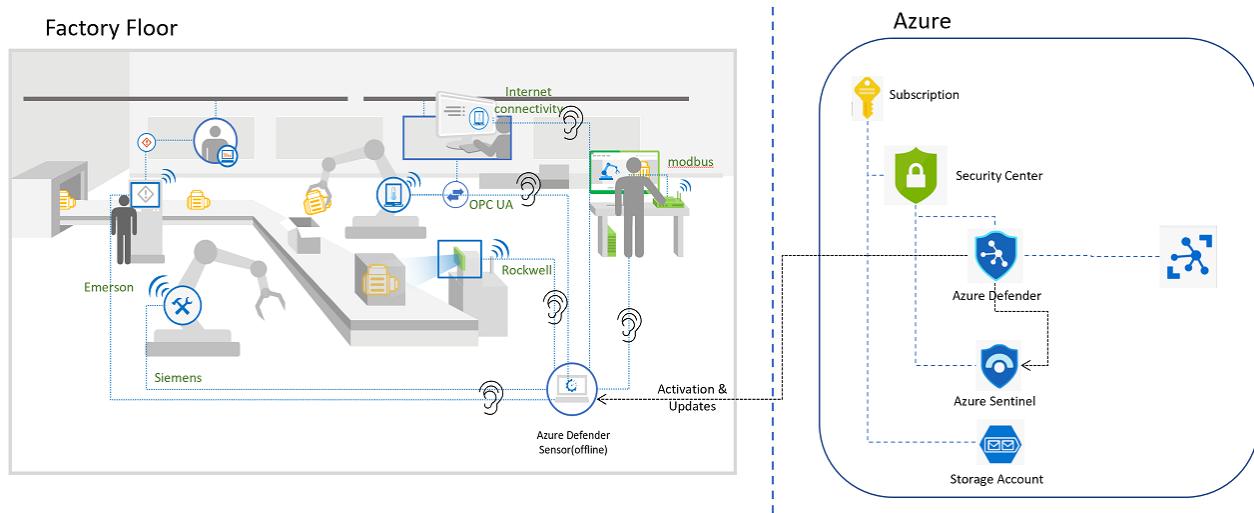


Internet of Things - Azure Defender for IoT HOL

Before starting this Lab make sure you completed the steps specified in [Azure Defender for IoT BHOL.md](#) File in this repository.

Architecture Diagram

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



Content:

- Exercise #1: Enabling Defender
 - Task 1: Enabling Azure Defender for IoT
 - 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
 - Task 3: Configure Azure Defender
- 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: Troubleshooting

Exercise #1: Enabling Defender

Task 1: Enabling Azure Defender for IoT

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

Enable Azure Defender on 1 subscriptions			
Name	Total resources	Azure Defender Plan	
<input checked="" type="checkbox"/> Azure Pass - Spo...	2	Off (30 trial days left)	
<input type="checkbox"/> mylogworkspace	0	Off	

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

The screenshot shows the Azure Security Center interface. The left sidebar has sections for General, Cloud Security, and Management. Under Cloud Security, 'Azure Defender' is highlighted with a red box. The main area shows a timeline from 25 Sun to 15 Sun with counts for Secure Score (0), Regulatory compliance (0), and Azure Defender (4). Under Management, there are sections for Pricing & settings, Security policy, Security solutions, Workflow automation, Coverage, and Cloud connectors. The 'Advanced protection' section lists VM vulnerability assessment (7 Unprotected), Just-in-time VM access (4 Unprotected), Adaptive application control (None Unprotected), Container image scanning (None Unprotected), Adaptive network hardening (1 Unprotected), SQL vulnerability assessment (None Unprotected), File integrity monitoring, and Network map. The 'IoT security' box is also highlighted with a red box.

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

The screenshot shows the 'Advanced protection' section of the Azure Security Center. It includes a timeline from 25 Sun to 15 Sun with counts for Secure Score (0), Regulatory compliance (0), and Azure Defender (4). Under Management, there are sections for Pricing & settings, Security policy, Security solutions, Workflow automation, Coverage, and Cloud connectors. The 'Advanced protection' section lists VM vulnerability assessment (7 Unprotected), Just-in-time VM access (4 Unprotected), Adaptive application control (None Unprotected), Container image scanning (None Unprotected), Adaptive network hardening (1 Unprotected), SQL vulnerability assessment (None Unprotected), File integrity monitoring, and Network map. The 'IoT security' box is highlighted with a red box.

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

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

Home > Security Center > Defender for IoT >

Pricing

[Subscribe](#) [Start with a trial](#) | [Download on-premises management console activation file](#) | [Refresh](#)

Azure Defender for IoT on-premises agentless monitoring now generally available
For more information on Defender for IoT pricing, visit the [Pricing page](#).

Pricing

Manage subscriptions and committed devices in your Azure Defender for IoT account.

Subscription	Number of committed devices
<input checked="" type="checkbox"/>  <input type="text" value=""/>	1000

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

Task 2: Create an IoT Hub:

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

1. Go to the resource group you created for this training, in the Overview panel, you will see at the top **+ Create**, click there and type **IoT Hub** in the search box, then click **Create**.
2. In the next screen you will ask to fill the **Basics** tab:
 - **Subscription:** Select the Subscription you are working on.
 - **Resource Group:** Should be the resource group created in previous step.
 - **IoT Hub Name:** adt4iothub+SUFFIX
 - **Region:** East US.

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 * ⓘ

▼

Resource group * ⓘ

▼

[Create new](#)

Instance details

IoT hub name * ⓘ

✓

Region * ⓘ

▼

[Review + create](#)

[< Previous](#)

[Next: Networking >](#)

[Automation options](#)

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

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

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

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

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

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

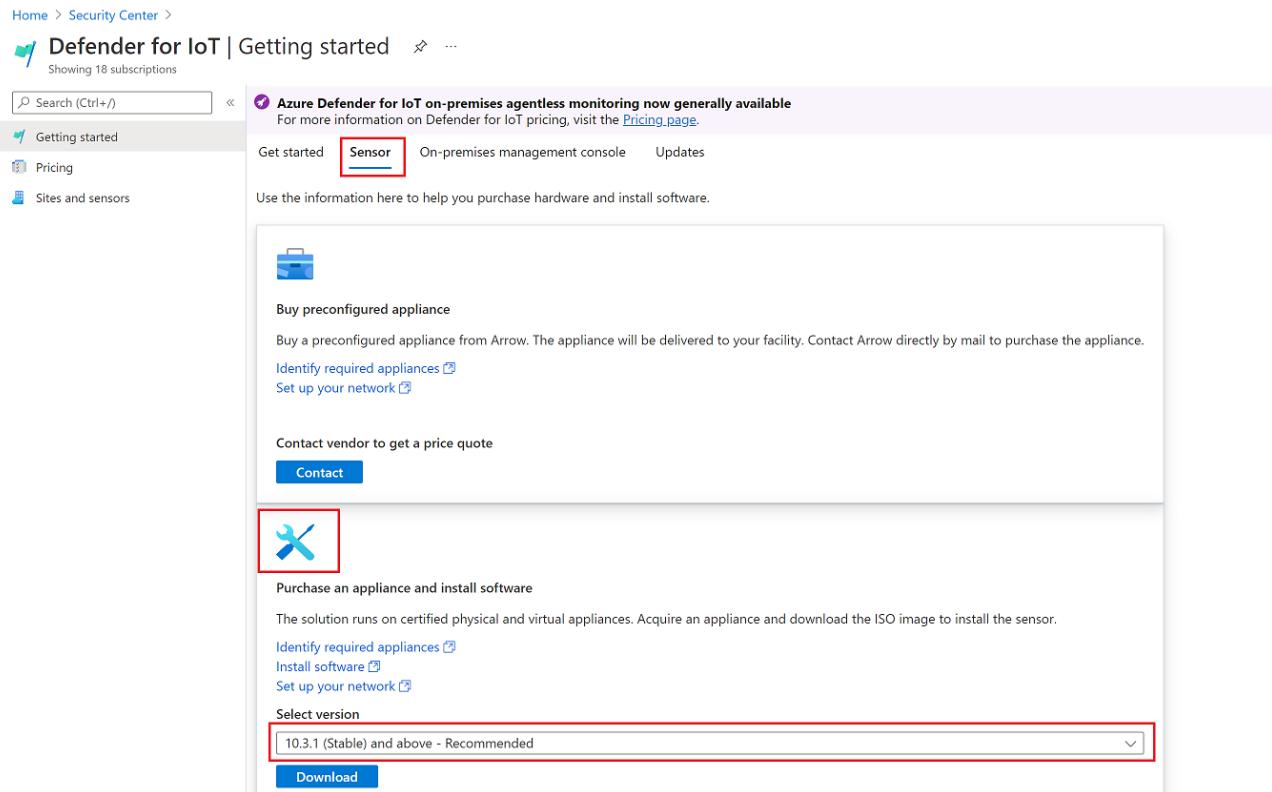
The screenshot shows the Azure Pass - Sponsorship | Access control (IAM) blade. The 'Access control (IAM)' menu item is highlighted with a red box. The 'Add' button is also highlighted with a red box. The 'Contributor' role and 'User, group, or service principal' assignment are selected in the 'Add role assignment' dialog box. The 'Save' button is highlighted with a red box.

Task 3 - Onboarding sensors

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

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

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



The screenshot shows the 'Getting started' section of the Azure Defender for IoT portal. The 'Sensor' tab is selected, indicated by a red box. A dropdown menu for 'Select version' is open, showing the option '10.3.1 (Stable) and above - Recommended', which is also highlighted with a red box. Below the dropdown is a 'Download' button.

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

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

Defender for IoT | Sites and sensors

Showing 18 subscriptions

Onboard sensor

Push Threat Intelligence update (Preview)

Azure Defender for IoT on-premises agentless monitoring now generally available. For more information on Defender for IoT pricing, visit the [Pricing page](#).

Sensors 0

Cloud connected 0

Locally managed 0

There are no sensors to display

Sensor name ↓

Sensor type

Zone

Subscription

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

Home > Defender for IoT >

Onboard sensor

Showing subscription 'Joe Azure Subscription'

Register sensor

Download activation file

Register this sensor with Azure Defender for IoT

Sensor name *

myofflinesensor

Subscription *

Onboard subscription

Deploy for:

An enterprise network (Cloud connected)

An operational network (Cloud connected)

An operational network (On premises)

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

Home > Security Center > Defender for IoT >

Onboard sensor

Showing 18 subscriptions

1 Register sensor 2 Download activation file

Your sensor is registered with Azure Defender for IoT. To complete sensor onboarding, download the activation file and install it on your sensor.

[Learn about sensor activation](#)

[Download activation file](#)

[Finish](#)

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

Home > Security Center > Defender for IoT

Defender for IoT | Sites and sensors

Showing 18 subscriptions

Search (Ctrl+ /) < + Onboard sensor | ⚡ Push Threat Intelligence update (Preview) | Export |

Getting started | Pricing | Sites and sensors

⚡ Azure Defender for IoT on-premises agentless monitoring now generally available
For more information on Defender for IoT pricing, visit the [Pricing page](#).

Search Add filter

1 Sensors 0 Cloud connected 1 Locally managed

Showing one sensor

Sensor name	Sensor type	Zone	Subscription
myofflinesensor	Locally managed		Microsoft In...

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

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

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

Site Section

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

Home > Defender for IoT >

Onboard sensor x ...

Showing subscription 'Joe Azure Subscription'

Sensor name *

Subscription *

[Onboard subscription](#)

Deploy for: *

An enterprise network (Cloud connected)

An operational network (Cloud connected)

An operational network (On premises)

Automatic Threat Intelligence Updates (Preview)  (Preview)

Microsoft continually updates threat intelligence to cover the latest threats and to constantly tweak detection logic, enhancing the ability to accurately identify threats.

Site * i

Hub * (Preview)

[Create IoT Hub for your site](#) 

It takes approximately 10 minutes for a new IoT Hub to be active and ready to use

Name *

Tags (Preview)

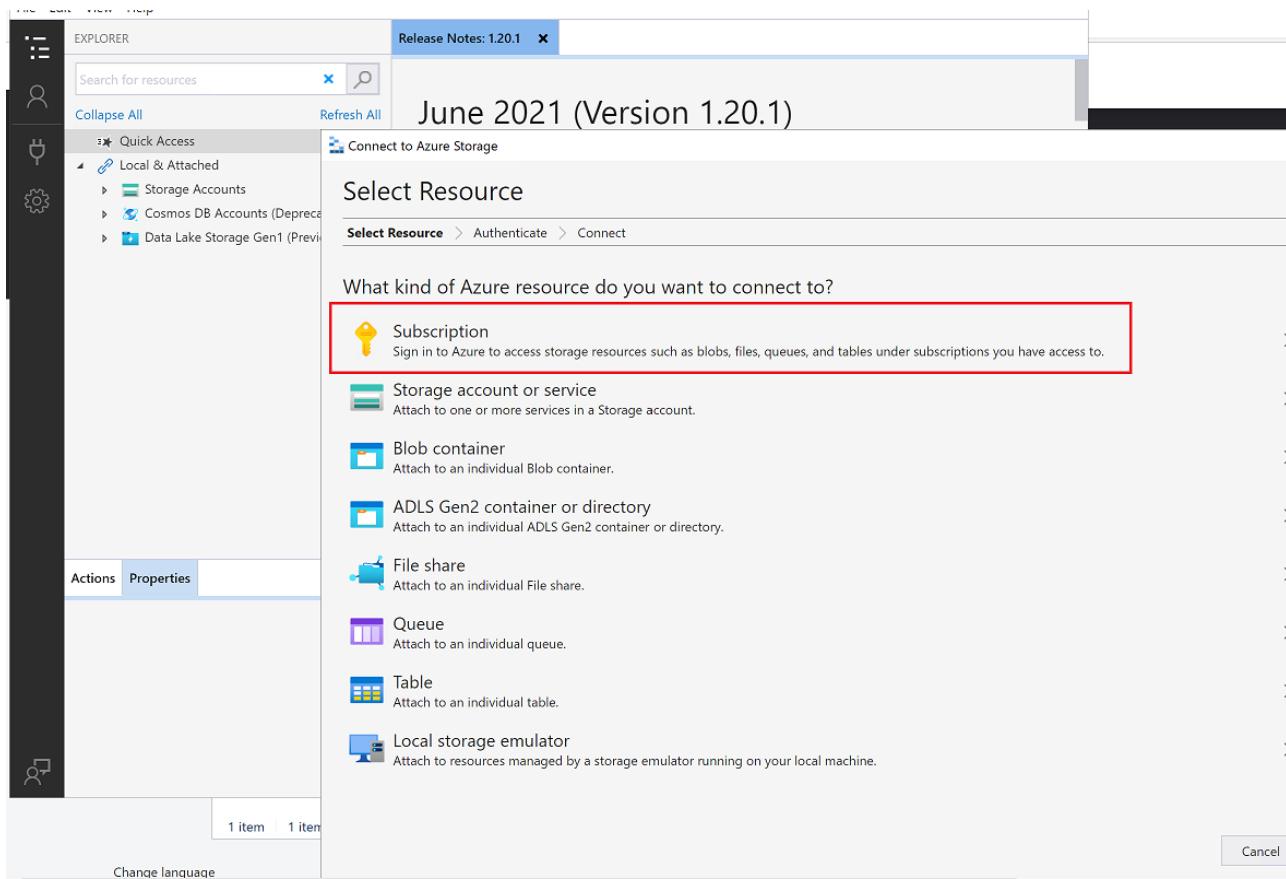
[+Delete tag](#)

8. Click **Register**.

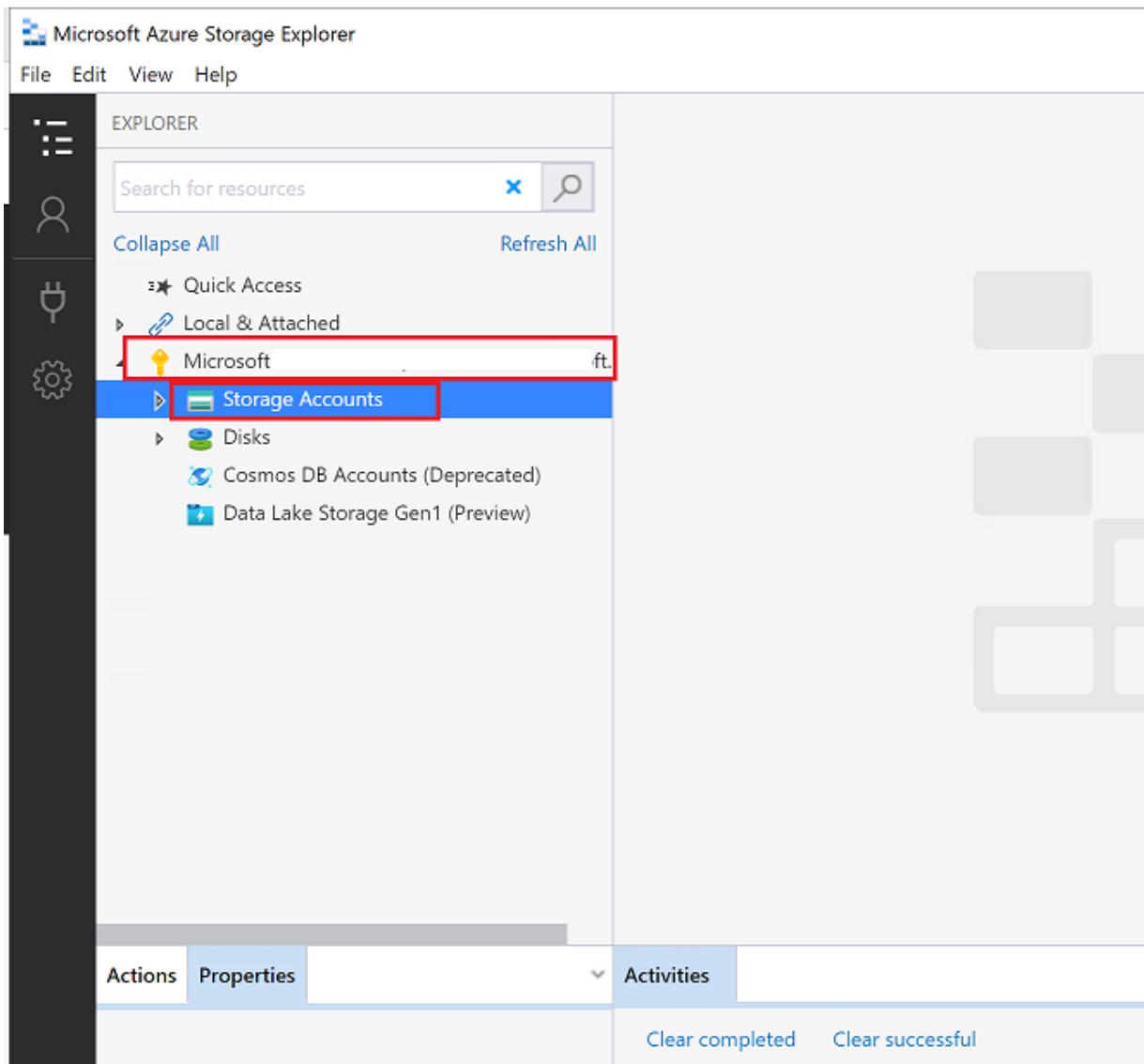
9. In the next step **Download activation file** and click **Finish**.

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

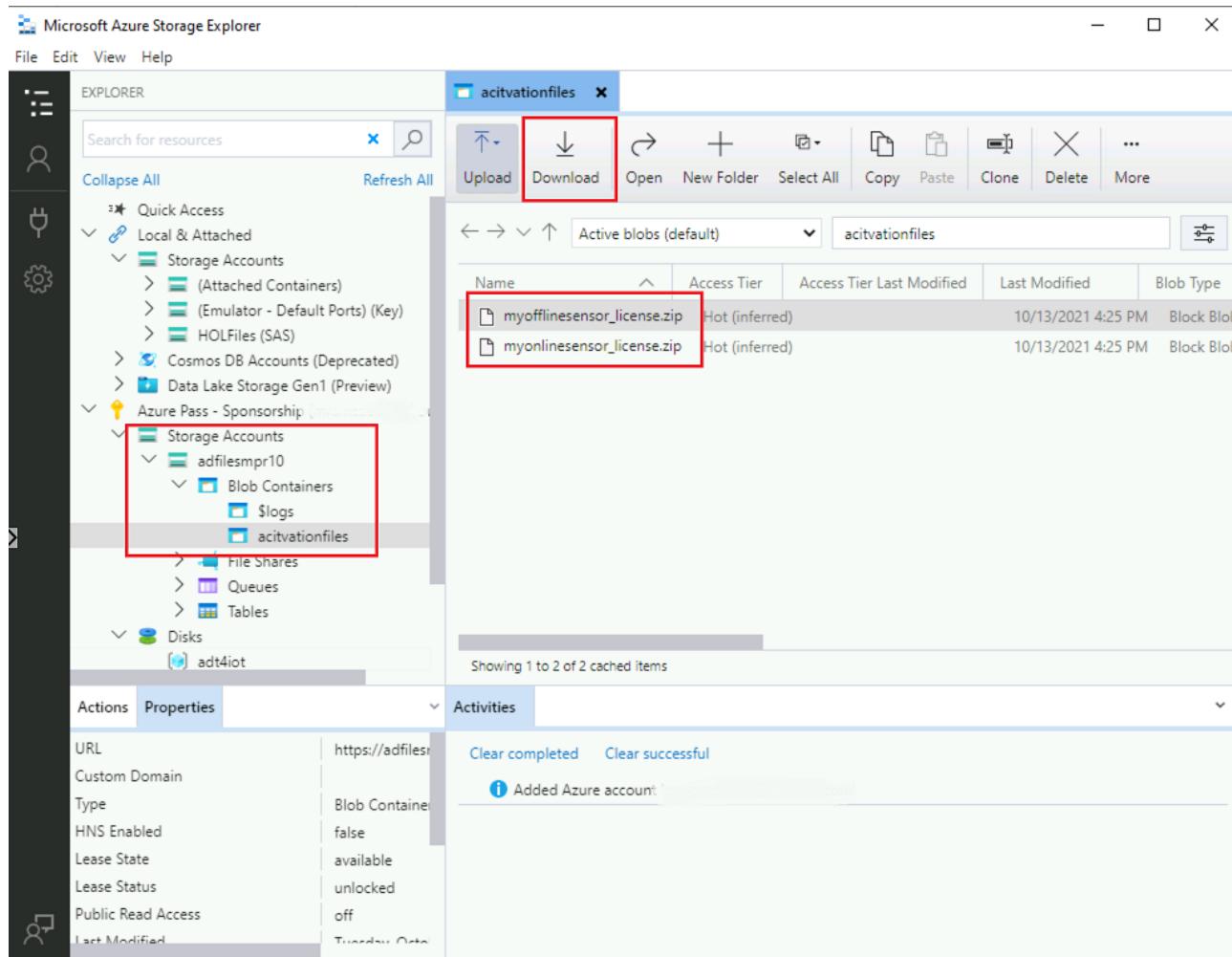
11. At this point you have 3 files downloaded locally (two zips licenses sensors and the iso file) we will upload them to the Storage account created in the section **Azure Defender for IoT BHOL**, this way we will be able to make them available to download in the Virtual Machine. Another option could be to download the files directly in the Virtual Machine, if you are login in the Azure Portal inside the VM. However, sometimes you will have policies on place not allowing this, so the storage account route will make this feasible.
12. To Upload the Files, go to the Storage Account you created before in the Azure Portal. On the left panel select **Containers**, on the right side, click on **activationfiles**, next on the top menu click **Upload** browse to the location where you download the files, select all of them and click **Upload**.
13. Go back to the windows Virtual Machine, open **Storage Explorer**. You will be ask to login to your Azure account where you just upload the files. Then select **Subscription**.



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



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



Exercise #2: Setting up your offline sensor

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

Task 1: Set up your Virtual Machine

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

```
c:\ Administrator: Command Prompt

Windows IP Configuration

Ethernet adapter Ethernet 5:

Connection-specific DNS Suffix  . : 5nlb1axu3fnuvn55yxvuctaega.bx.internal.cloudapp.net
Link-local IPv6 Address . . . . . : fe80::5d9c:abf:7e94:978%35
IPv4 Address. . . . . : 10.0.0.5
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.0.1

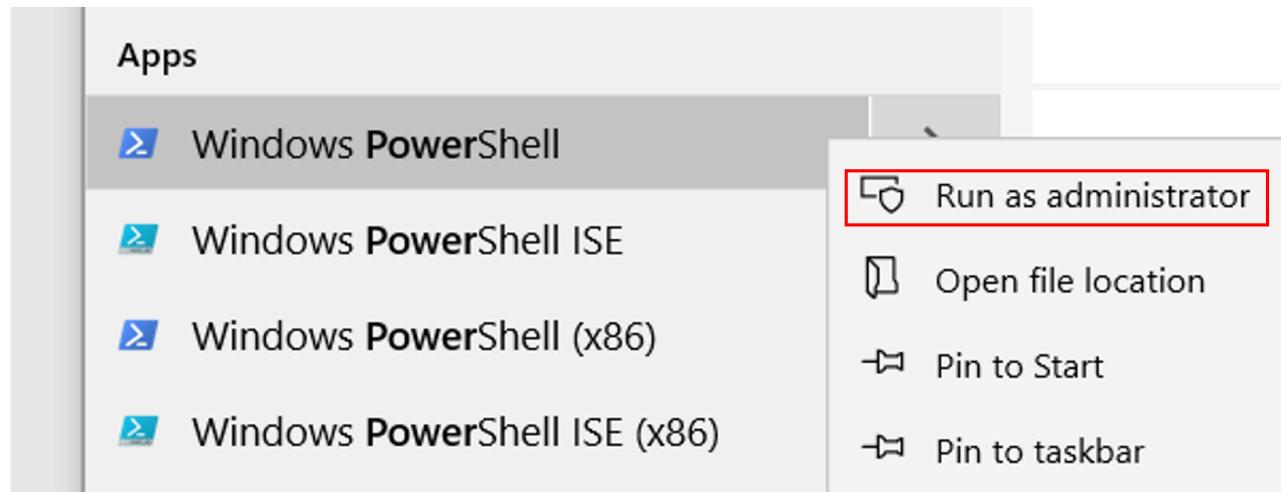
Ethernet adapter vEthernet (Default Switch):

Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::2484:e5e2:a574:98c8%52
IPv4 Address. . . . . : 172.25.48.1
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
```

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

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

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



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

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

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

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

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

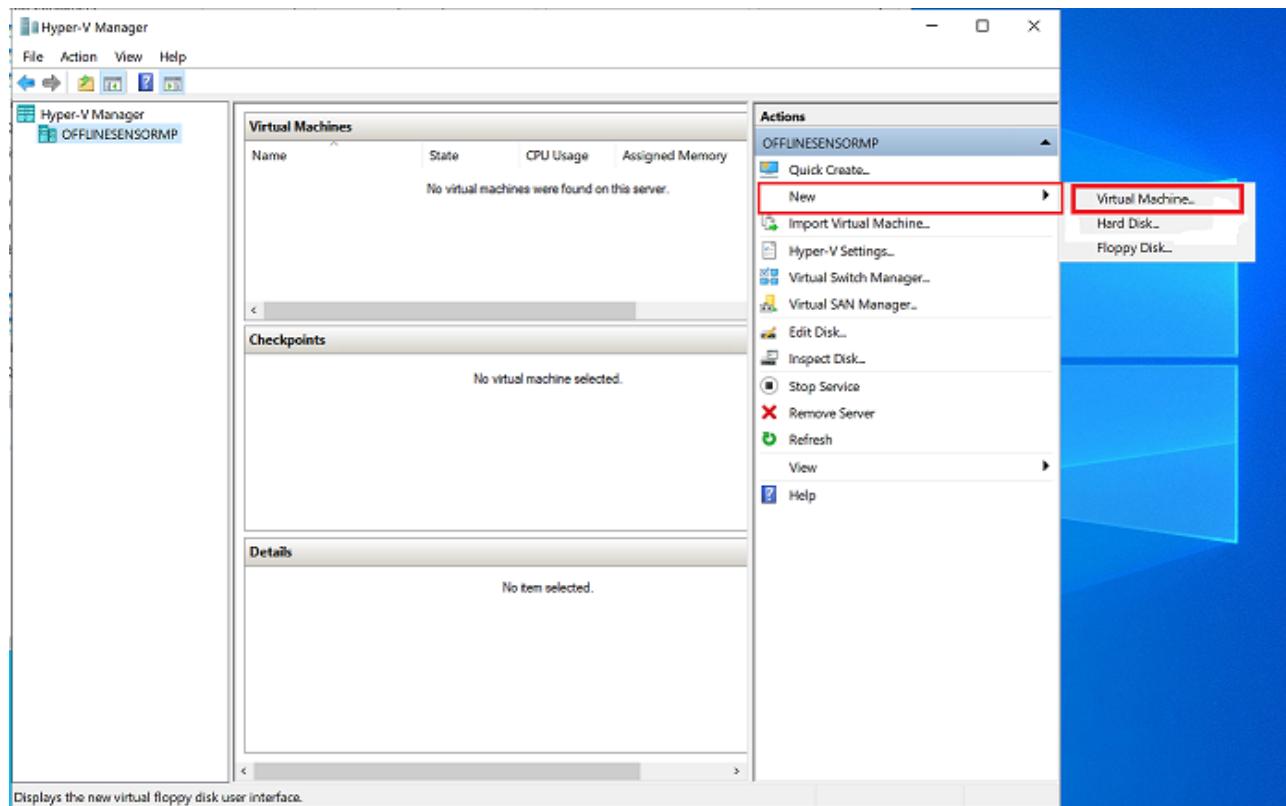
6. Assign an IP address to the NATSwitch (either 192.168.0.1 or 172.27.0.1) depending on your network address based on step 1.

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

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

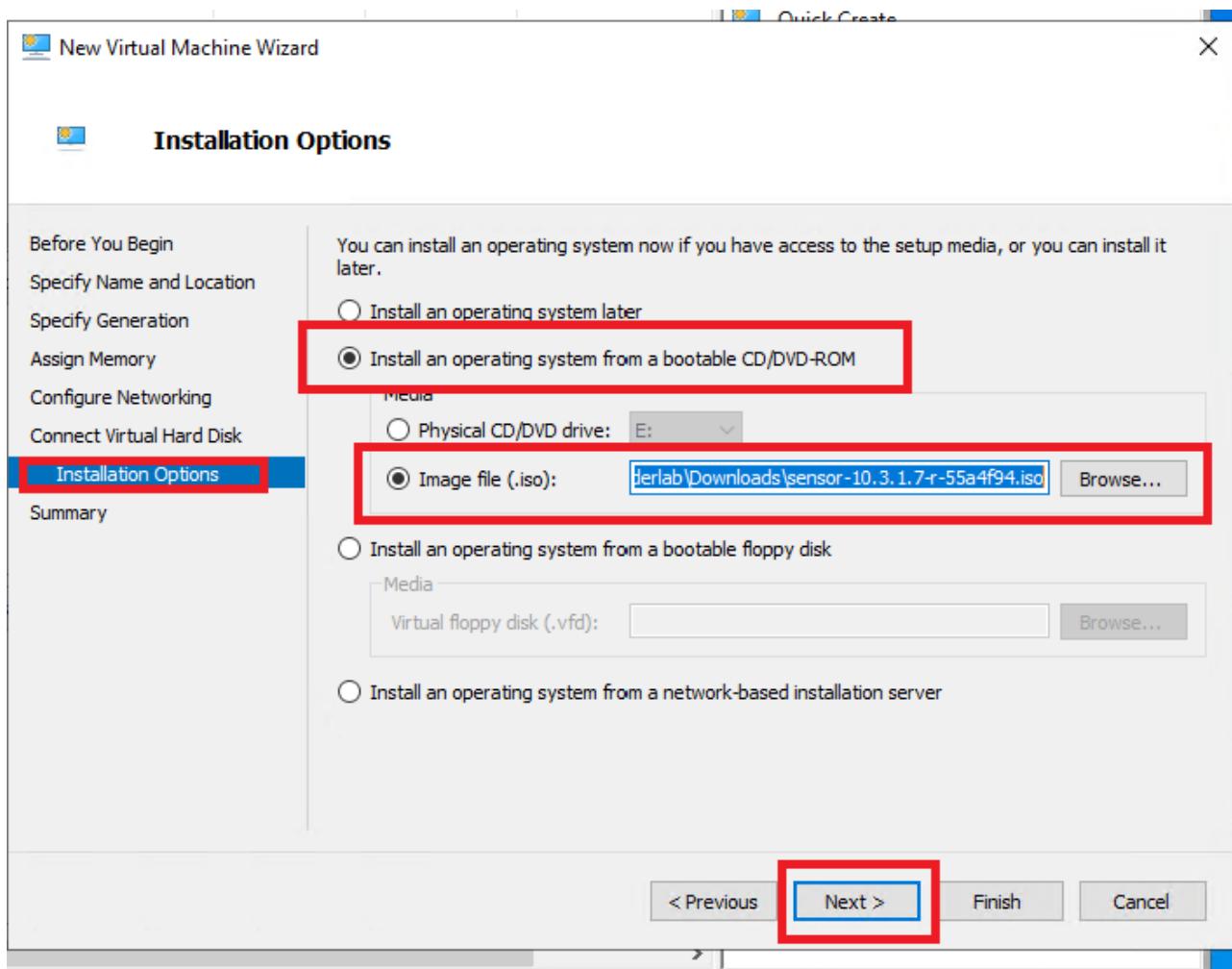
```
New-NetNat -Name MyNATnetwork -InternalIPInterfaceAddressPrefix 192.168.0.0/24
```

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



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

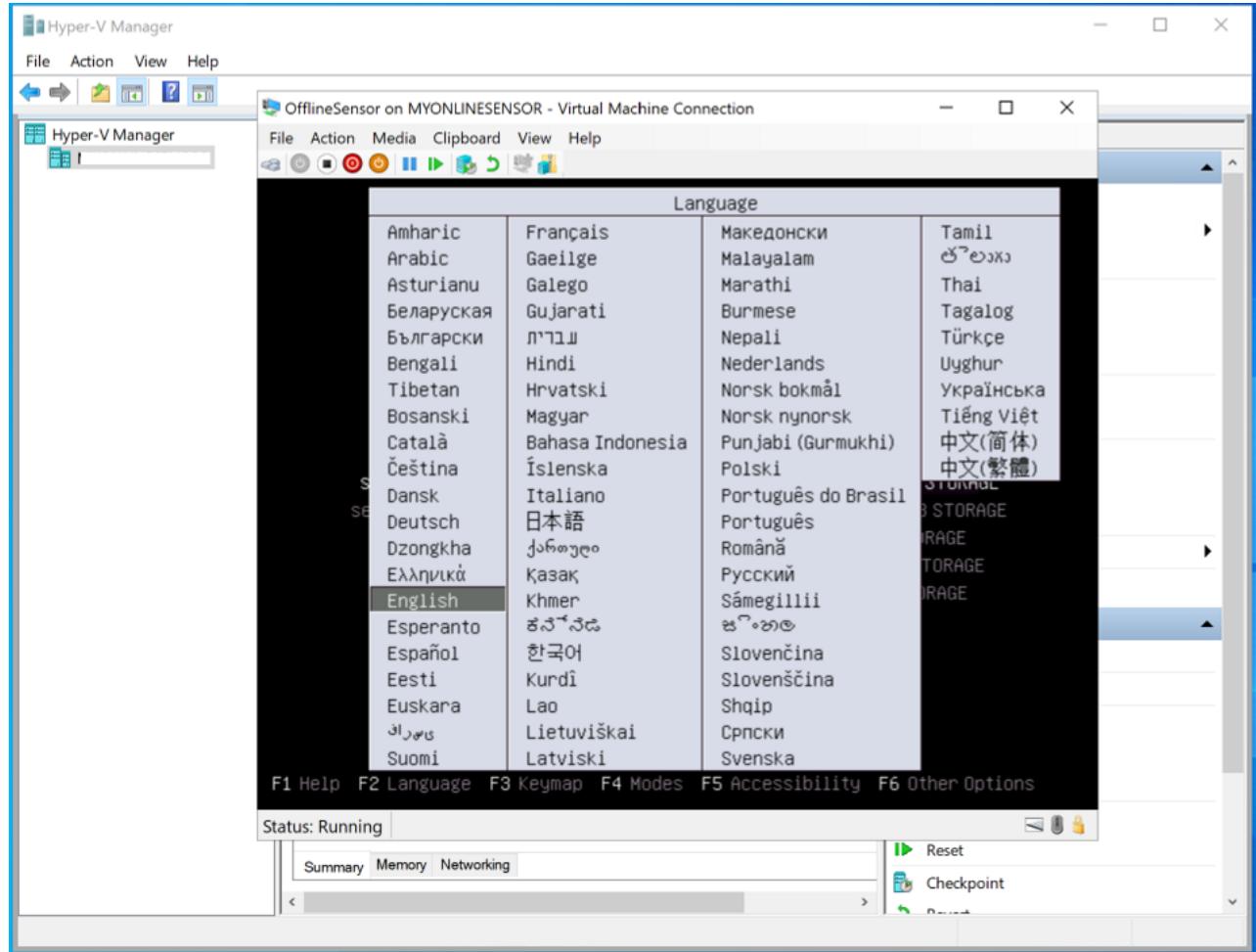
- Specify Generation, select Generation 1, click Next again.
- Change the memory to 8196MB, Next.
- Configure Network tab, select in Connection, NATSwitch, Next.
- Connect Virtual Hard Disk tab, Create a virtual hard disk click Next.
- Installation Options, select Install an operating system from a bootable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



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

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

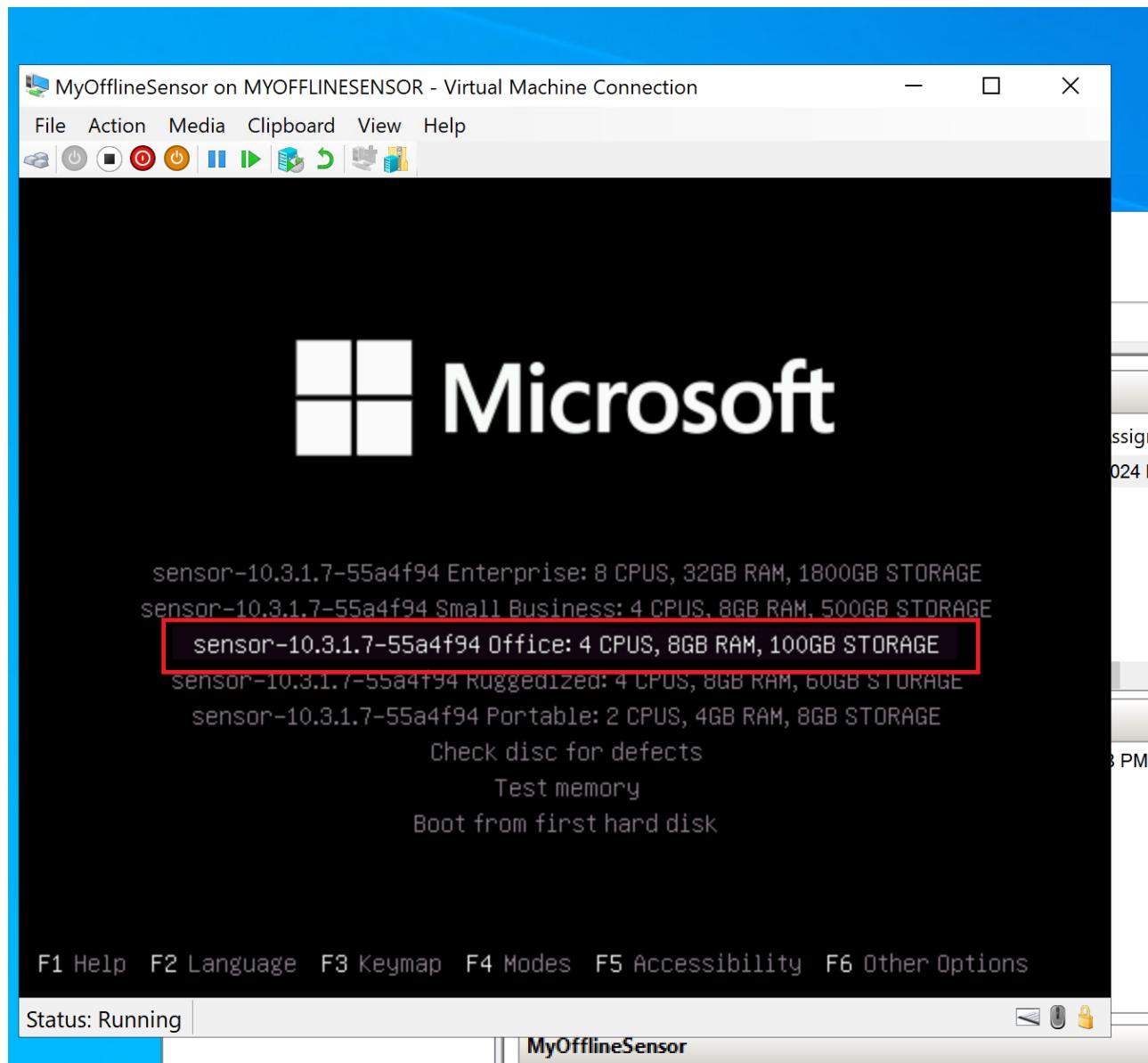
Note!: If you don't see that screen below, your installation timed out or you pressed enter selecting a different configuration by mistake, delete the virtual machine and start this task over.



Task 2: Configure Azure Defender

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

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



3. You will be asked to fulfill some parameters, it is **VERY IMPORTANT** you pay attention to the previous task because you will use the network information you captured before, this is unique to each Virtual Machine. So the following is an **EXAMPLE**.
- **configure hardware profile:** **office**, then press enter.
 - **Configure network interface**, type **eth0**
 - **Configure management network interface:** in this example we're using **192.168.0.50**, you will use one of the **Ipv4 Addresses** depending on your network scope from the previous task, either **192.168.0.50** or **172.27.0.50**. Click Enter to continue. **Take a note of this IP you will need it later on.**
 - **Subnets mask:** **255.255.255.0** this will be the **SAME** for everyone.
 - **Configure DNS:** **8.8.8.8**

- **Configure default gateway IP Address:** We are 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**.

Now the installation will run for 10-15 minutes.

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

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

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

```
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

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

```
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-----
his is your generated login information
pliance ID: 834A0C38-4DB4-B041-8177-B0336D0319A7
sername: cyberx
assword: =c5=r,Rh0u17::_u

MPORTANT - this is the only time this information will be displayed
lease safely backup this information and press enter to continue

ress Enter to continue...
inished showing prompt
tarting to show prompt title: Credentials message:

-----Credentials-----
his is your generated login information
pliance ID: 834A0C38-4DB4-B041-8177-B0336D0319A7
sername: support
assword: 07sxouG8T3f1?K""

MPORTANT - this is the only time this information will be displayed
lease safely backup this information and press enter to continue

ress Enter to continue...
Status: Running |
```

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

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

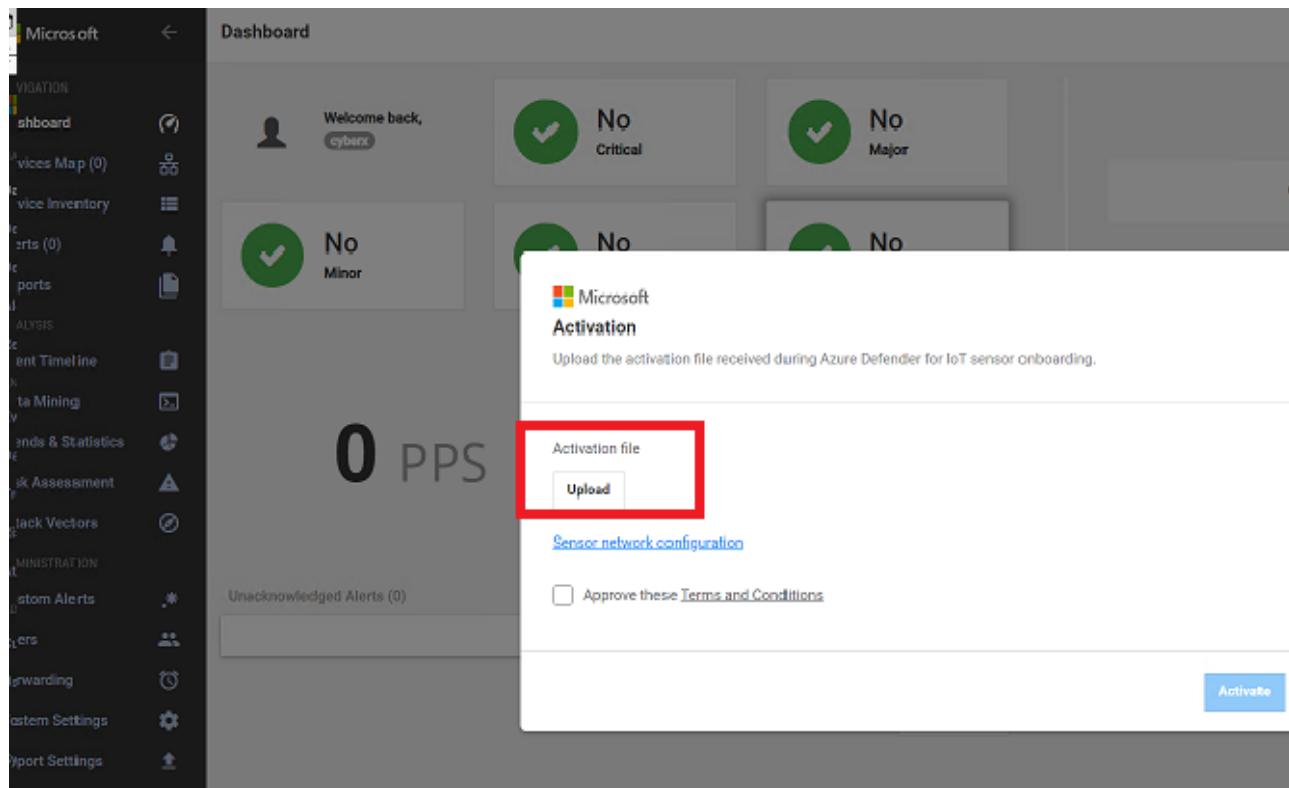
In the next steps you will be prompted to enter the password capture above, some characters look alike but they are not, this image will help you to identify some of them.

0	0	o	1	l	I	'	'	l
Zero	Capital "Oh" (O)	Lowercase "oh" (o)	Number 1	Lowercase 'el' (l)	Capital "Eye" (I)	Backtick (Same key as ~)	Apostrophe	Pipe (Shift + \)

6. Login with the credentials provided in step 4.

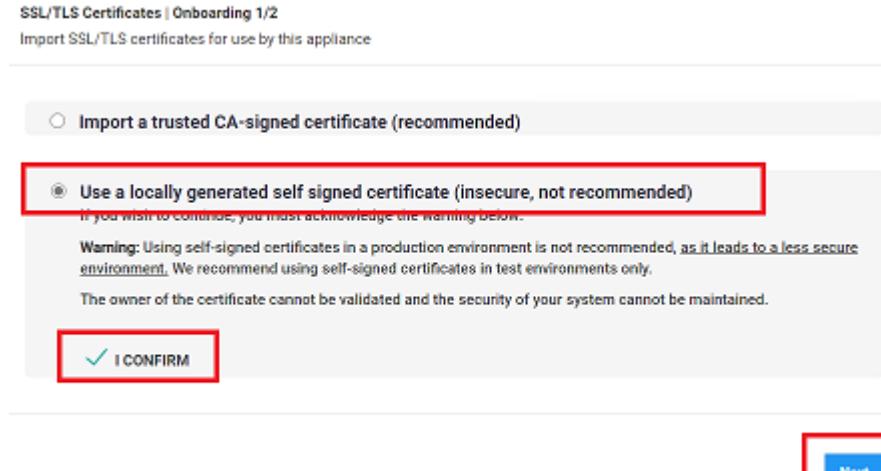
The image shows a terminal window on the left and a browser window on the right. The terminal window displays system information including IP: 192.168.0.50, SUBNET: 255.255.255.0, GATEWAY: 192.168.0.1, and a long UID. The browser window shows a 'Not secure' warning for the URL https://192.168.0.50/login#/dashboard. The dashboard page is titled 'Microsoft Azure Defender for IoT Sensor' and contains fields for 'Username' and 'Password', along with 'Password recovery' and 'Login' buttons.

7. 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**.



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

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



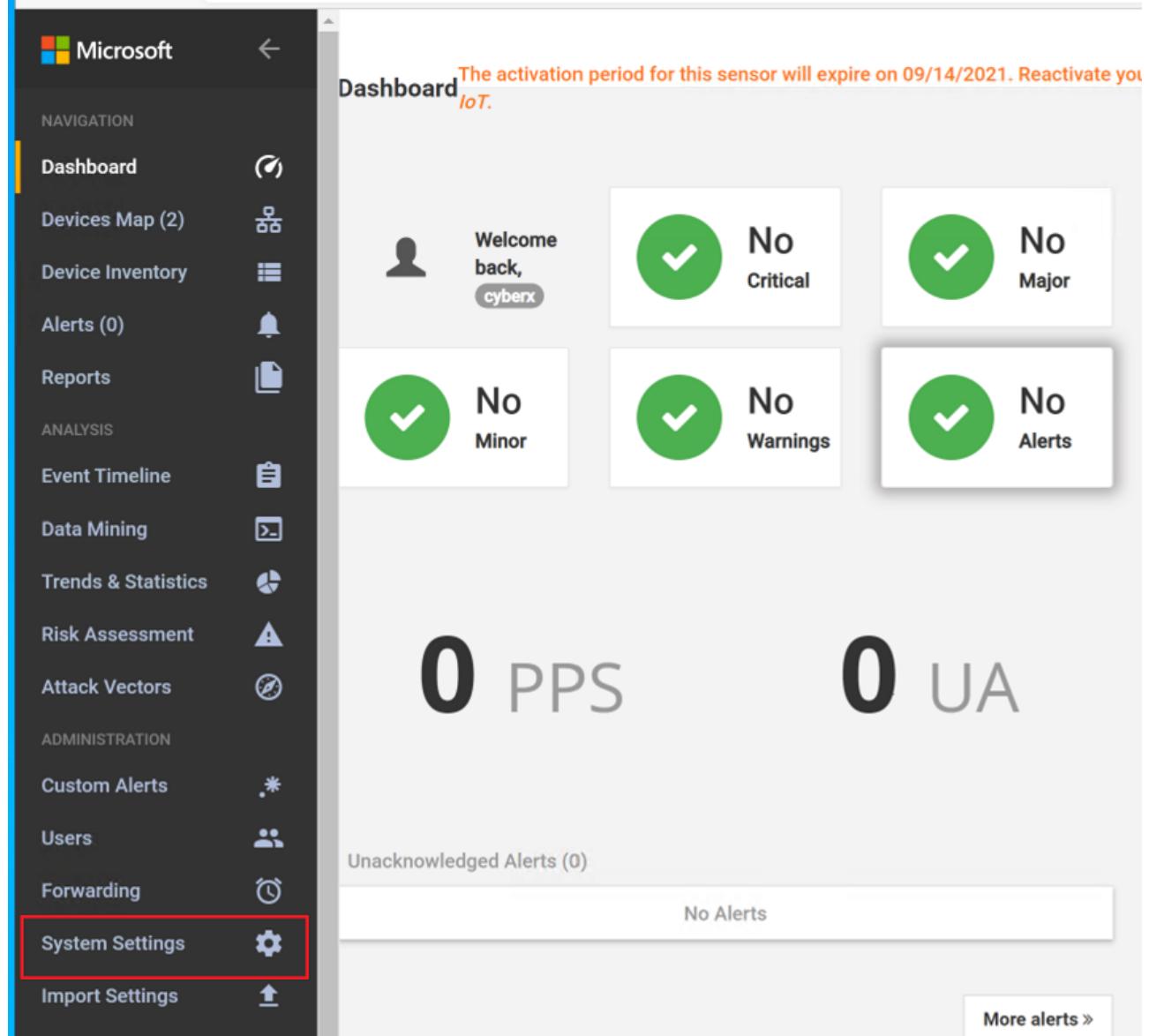
10. For this lab in the next step we will **Disable** the system wide validation. Finish.

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

Exercise 3: Enabling system settings

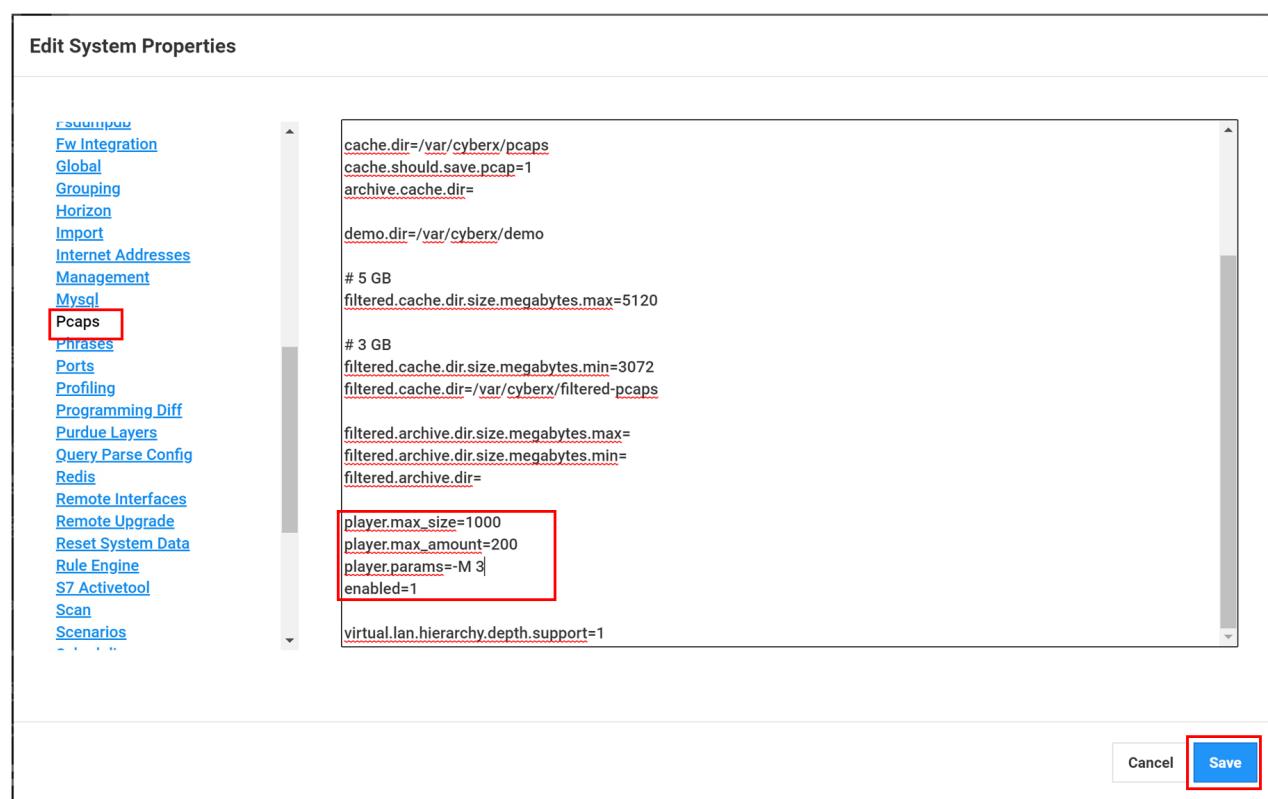
Task 1: System Properties

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



The screenshot shows the Azure Defender for IoT portal. On the left, a dark sidebar menu is open, showing various navigation options like Dashboard, Devices Map, Device Inventory, and System Settings. The 'System Settings' option is highlighted with a red box. The main dashboard area shows a 'Welcome back, cyberx' message and a status summary: 'No Critical', 'No Major', 'No Minor', 'No Warnings', and 'No Alerts'. Below this, large numbers '0 PPS' and '0 UA' are displayed. At the bottom, there is a section for 'Unacknowledged Alerts (0)' with a 'No Alerts' message and a 'More alerts >' button.

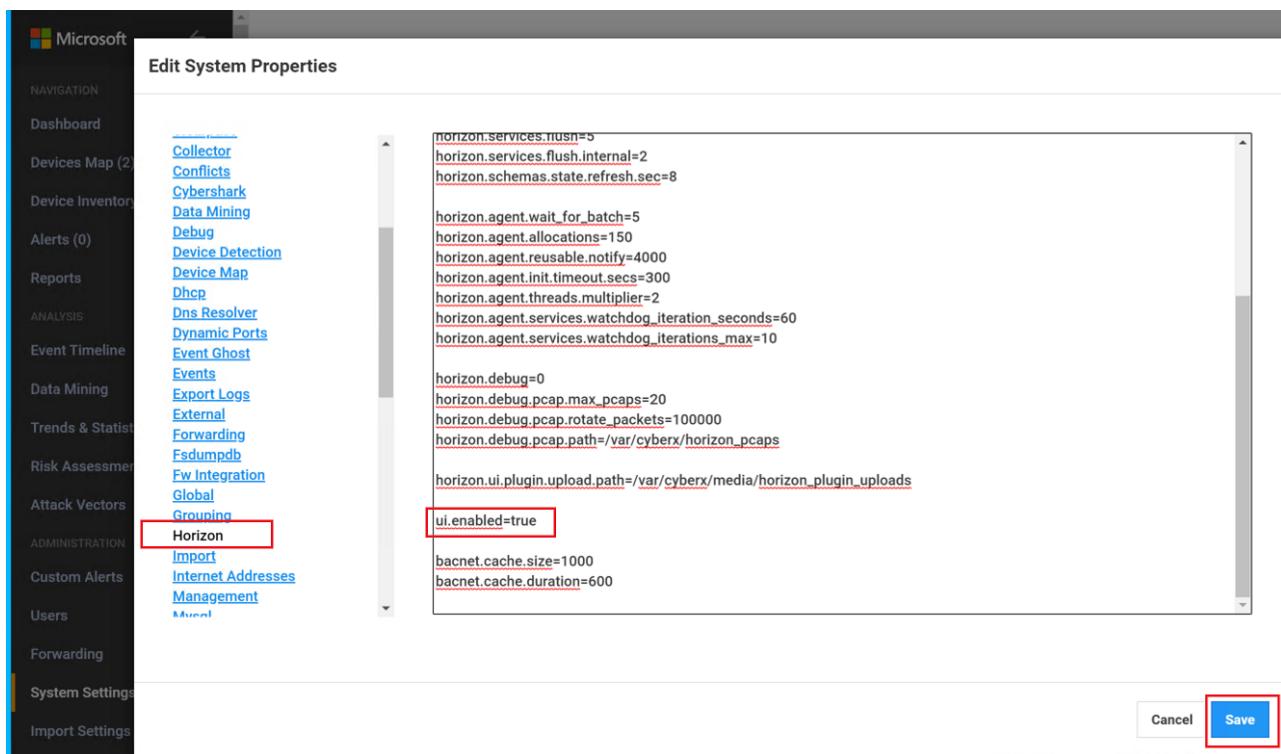
2. Next, look for the icon **System Properties** on the right side. Click in the icon, you will see a pop up warning, select **Ok**.
3. In the new window on the left side, scroll down until you see **Pcaps**, click there. Now on the right side scroll all the way down and we will modify three parameters as shown below:
 - o **player_max_amount=200**
 - o **enabled=1**
 - o **player.params=-M 3**



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

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

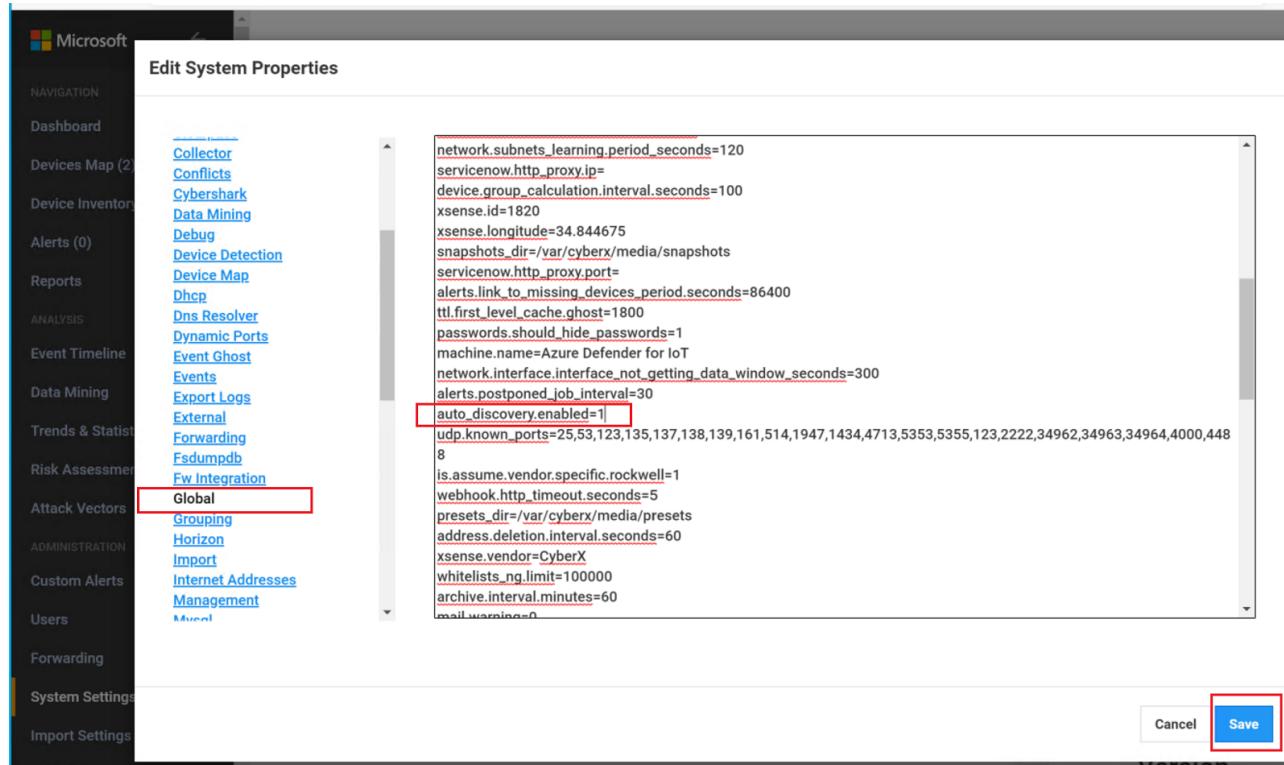
- o ui.enabled=true



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

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

- o `auto_discovery.enabled=1`



Microsoft

NAVIGATION

- Dashboard
- Devices Map (2)
- Device Inventory
- Alerts (0)
- Reports
- ANALYSIS
- Event Timeline
- Data Mining
- Trends & Statistics
- Risk Assessment
- Attack Vectors
- ADMINISTRATION
- Custom Alerts
- Users
- Forwarding
- System Settings
- Import Settings

Edit System Properties

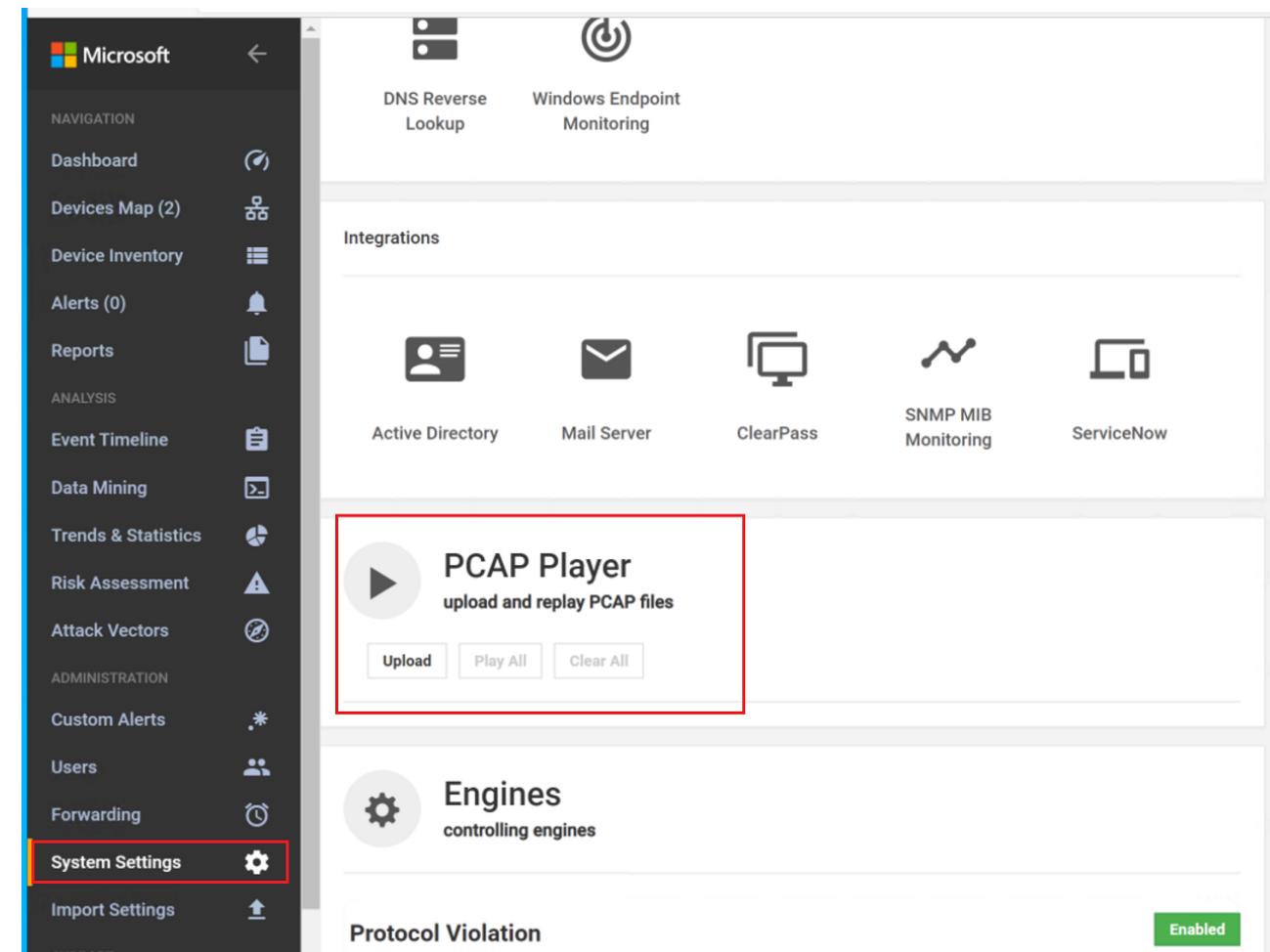
Collector
Conflicts
Cybershark
Data Mining
Debug
Device Detection
Device Map
Dhcp
Dns Resolver
Dynamic Ports
Event Ghost
Events
Export Logs
External
Forwarding
Fdumpdb
Fw Integration
Global auto_discovery.enabled=1
Grouping
Horizon
Import
Internet Addresses
Management
Misc

```
network.subnets_learning.period_seconds=120
servicenow.http_proxy.ip=
device.group_calculation.interval.seconds=100
xsense.id=1820
xsense.longitude=34.844675
snapshots_dir=/var/cyberx/media/snapshots
servicenow.http_proxy.port=
alerts.link_to_missing_devices_period.seconds=86400
ttl.first_level_cache.ghost=1800
passwords.should_hide_passwords=1
machine.name=Azure Defender for IoT
network.interface.interface_not_getting_data_window_seconds=300
alerts.postponed_job_interval=30
auto_discovery.enabled=1
udp.known_ports=25,53,123,135,137,138,139,161,514,1947,1434,4713,5353,5355,123,2222,34962,34963,34964,4000,448
8
is.assume.vendor.specific.rockwell=1
webhook.http_timeout.seconds=5
presets_dir=/var/cyberx/media/presets
address.deletion.interval.seconds=60
xsense.vendor=CyberX
whitelists_ng.limit=100000
archive.interval.minutes=60
mail.warnings=0
```

Cancel Save

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

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



The screenshot shows the Azure Defender for IoT interface. On the left, a dark sidebar lists various navigation options: Dashboard, Devices Map (2), Device Inventory, Alerts (0), Reports, Event Timeline, Data Mining, Trends & Statistics, Risk Assessment, Attack Vectors, Custom Alerts, Users, Forwarding, System Settings (which is selected and highlighted with a red box), and Import Settings. The main content area includes sections for DNS Reverse Lookup, Windows Endpoint Monitoring, Integrations (Active Directory, Mail Server, ClearPass, SNMP MIB Monitoring, ServiceNow), and a PCAP Player section. The PCAP Player section is highlighted with a red box and contains a play button icon, the text 'PCAP Player upload and replay PCAP files', and three buttons: 'Upload', 'Play All', and 'Clear All'. Below this is an 'Engines' section with a gear icon and the text 'controlling engines'. At the bottom, there is a 'Protocol Violation' section with a green 'Enabled' button.

Task 2: Pcap Files

1. In previous steps you already downloaded a **holpcaps.zip** file from the Storage account. It should be in the Virtual Machine **Downloads** folder, unzip that file.
2. Go back to Azure Defender, Click on **System Settings**, then **PCAP Player** now select **Upload, Browse Files**, browse to the folder where you download the files in the previous step, select all the files and click **Open**. This operation will take a few minutes to upload all the files.
3. At this point you should see all the files uploaded.

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

Exercise 4: Analyzing the Data

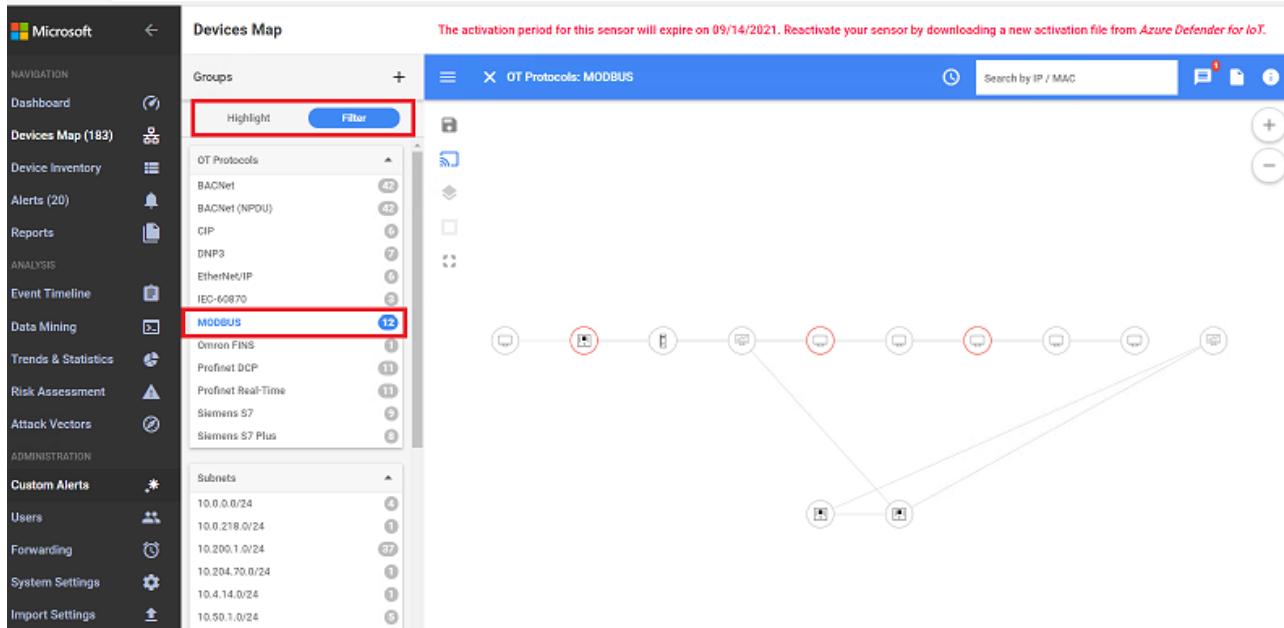
After Azude Defender learnt about your environment it will be able to share insights pretty fast.

Task 1: Devices Map

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

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

2. Check your notifications available and you can take action at this point.
3. For each device right click to analyze properties, show events, reports and simulate attack vectors.
4. In the 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

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

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

2. If we remove the device filter from the top of the screen, then click **Confirm** you will see 20 Alerts in process.
3. Apply **Custom Groups** to filter different scenarios, such as **Unclassified subnets** then **Confirm**

Task 3: Device Inventory

1. In this view, filter all your devices by **Is Authorized**, True or False are possible values.
2. Organize your devices based on filters.
3. Export the list to a csv files.

Task 4: Event Timeline

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

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

Task 5: Data Mining

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

1. Go To **+**, **New report**, in the categories section select **Modules and Firmware update versions**
2. Assign a name to your report. Then go to Filters, **add** and select **Firmware version(generic)**

The screenshot shows the 'Data Mining' section of the Azure Defender for IoT interface. On the left, the 'Data Mining' menu item is highlighted with a red box. The main area is titled 'Create new Report' with a message about an expiring sensor. It has sections for 'Categories (All)', 'Name', 'Description', 'Save to Reports Page', 'Order By' (Category selected), and 'Filters'. The 'Filters' section is expanded, showing a list of categories and specific filters for 'Device', 'IP Address', 'Port', and 'MAC Address'. A new filter 'Firmware Version (GENERIC)' is added and highlighted with a red box. The 'Save' button is also highlighted with a red box.

3. In the new field added **Firmware Version(GENERIC)** add **0.4.1**, then **Save**.
4. You can remove the filter to list all the firmware updates version in your list also.
5. Export you report(pdf, csv) for further actions.

Task 6: Risk Assessment

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

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

Exercise 5: Online Sensor

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

Task 1: Reconfiguring sensor

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

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

3. You will ask to login, then you can start to reconfigure the network settings, you will only change **one** value, **configure default gateway IP address** you will assign the IP Address of the NATSwitch value configured in previous steps, either 192.168.0.1 or 172.27.0.1, you will keep all the other values as before.

```
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
    <- Only change this

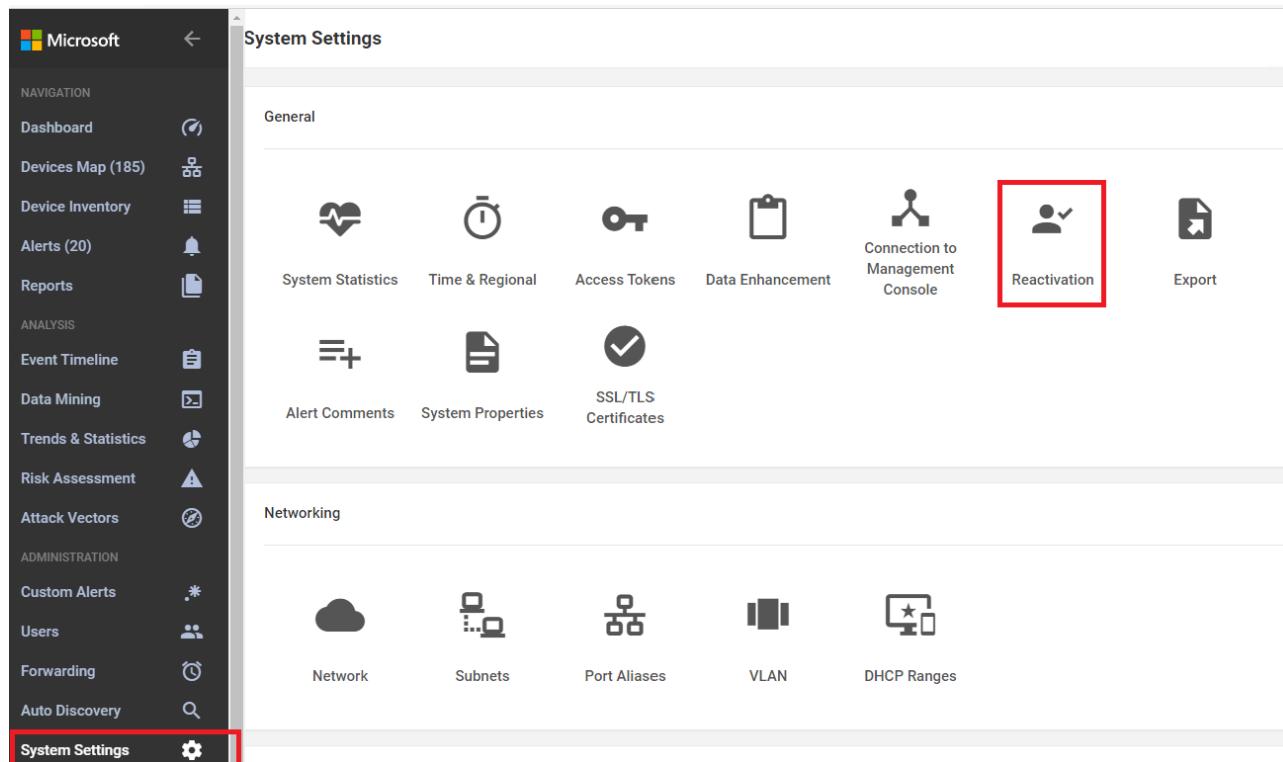
configure input interface(s)
- docker0
- eth1
- veth2138163
Please type your selected item(s) (separate with ","): eth1

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

4. Type **Y** at the end of the process to apply the change, it will run a reconfiguration and reboot.
5. After logging back in, test that you have external connectivity: **ping 8.8.8.8** in the Ubuntu sensor, you should now receive a different message containing "...icmp...". Note: hit Cntrl-C to stop the pinging.

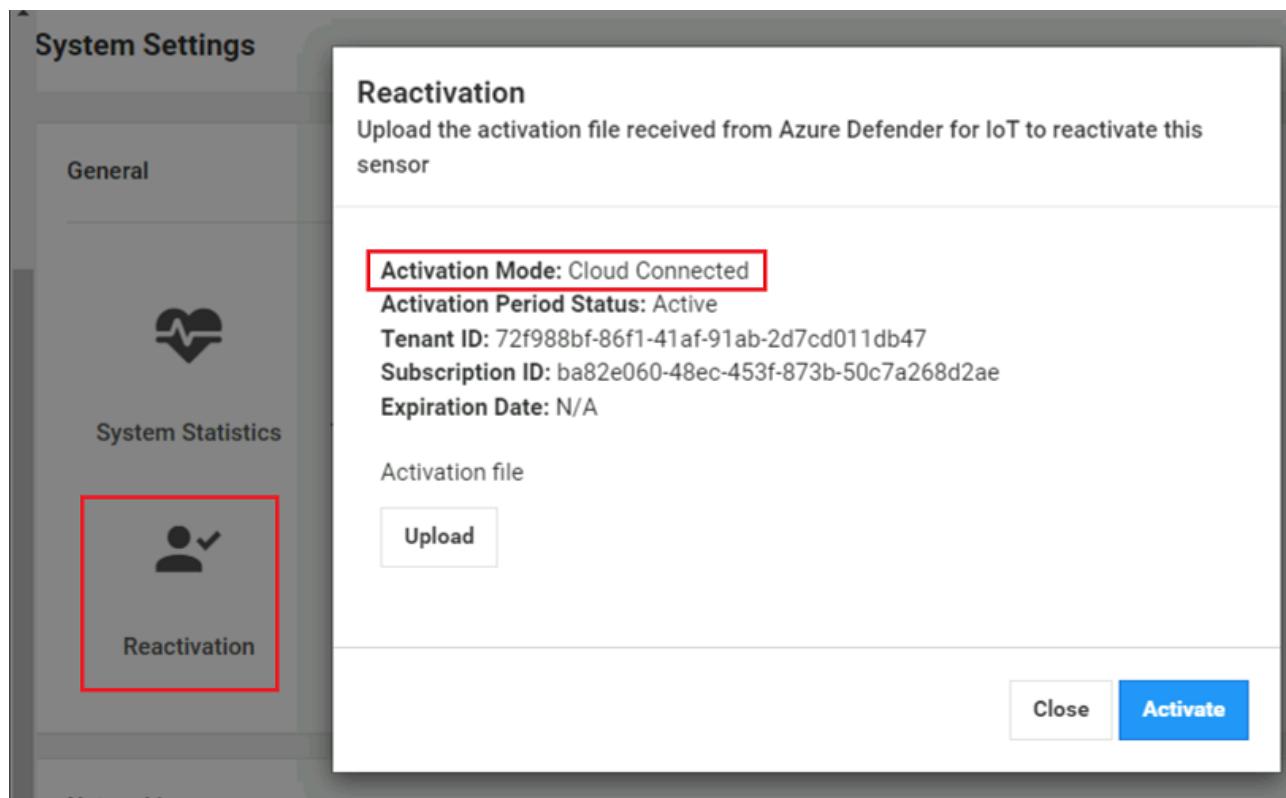
6. Now that your sensor has connectivity, go to the Azure Defender Portal, select **System Settings** and then, **Reactivation**.

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

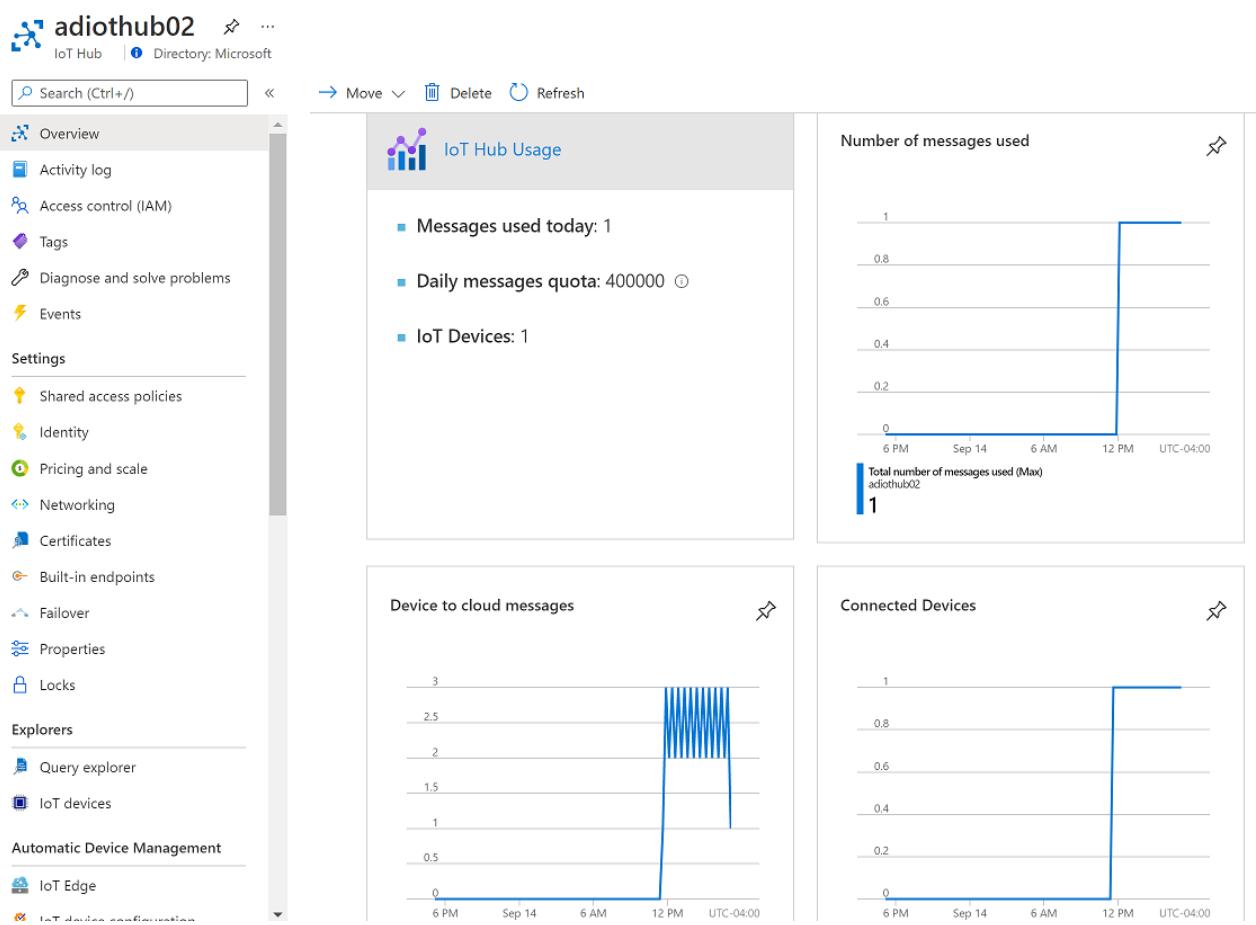


8. Last, you should receive a message showing your sensor modified to **Connected**.

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



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



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

Description	Count	Detected By	Environment	Date
Address Scan Detected	1	Microsoft	Devices	09/30/21
Unauthorized Internet Connectivity Dete...	12	Microsoft	Devices	09/30/21
Suspicion of Malicious Activity (BlackEne...	2	Microsoft	Devices	09/30/21
Suspicion of NotPetya Malware - Illegal S...	3	Microsoft	Devices	09/30/21
Port Scan Detected	2	Microsoft	Devices	09/30/21
Invalid SMB Message (DoublePulsar Backdo...	3	Microsoft	Devices	09/30/21
Unauthorized Internet Connectivity Dete...	10	Microsoft	Devices	09/14/21
Port Scan Detected	2	Microsoft	Devices	09/14/21
Modbus Exception	5	Microsoft	Devices	09/30/21
RPC Operation Failed	5	Microsoft	Devices	09/30/21
Firmware Change Detected	1	Microsoft	Devices	09/30/21
Malicious Domain Name Request	1	Microsoft	Devices	09/30/21
EtherNet/IP CIP Service Request Failed	2	Microsoft	Devices	09/30/21
Honeywell Firmware Version Changed	1	Microsoft	Devices	09/30/21
Device Failed to Receive a Dynamic IP Ad...	2	Microsoft	Devices	09/30/21
Modbus Exception	3	Microsoft	Devices	09/14/21
Function Code Not Supported by Outsta...	1	Microsoft	Devices	09/14/21
Firmware Change Detected	1	Microsoft	Devices	09/14/21
Incorrect Parameter Sent to Outstation	1	Microsoft	Devices	09/14/21

Exercise 6: Integrate with Sentinel

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

Task 1: Enabling IoT to Integrate with Sentinel

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

Home > adt4iot > adt4iothubmpr

adt4iothubmpr | Settings

- IoT Hub
- Search (Ctrl+/)
- IoT device configuration
- Device updates
- Messaging**
 - File upload
 - Message routing
- Security**
 - Overview
 - Security Alerts
 - Recommendations
 - Settings**
- Monitoring**
 - Alerts

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 Azure Defender for IoT**

[Home](#) > [adt4iot](#) > [adt4iothubmpr](#) >

Settings | Data Collection

adt4iothubmpr

Defender for IoT

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

Enable Azure Defender for IoT

Workspace configuration

You can use Log Analytics to investigate raw events, alerts and recommendations generated by 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

Create New Workspace

Task 2: Connecting Data Connectors

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

Home > Azure Sentinel > Add Azure Sentinel to a workspace > Azure Sentinel

Azure Sentinel | Data connectors

Selected workspace: 'mylogworkspace'

Search (Ctrl+/
Guides & Feedback Refresh

General

- Overview
- Logs
- News & guides

Content management

- Solutions (Preview)
- Community

Threat management

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

Configuration

- Data connectors**
- Analytics

116 Connectors 0 Connected

defender Providers : All Data Type

Status	Connector name	Provider
Green	Azure Defender	Microsoft
Yellow	Azure Defender for IoT (Preview)	Microsoft
Green	Microsoft 365 Defender (Preview)	Microsoft
Green	Microsoft Defender for Endpoint	Microsoft
Green	Microsoft Defender for Identity	Microsoft
Green	Microsoft Defender for Office 365 (Preview)	Microsoft

2. Click the Open Connector Page

Azure Defender for IoT (Preview)

Not connected

Microsoft Provider

Last Log Received

Description

Gain insights into your IoT security by connecting Azure Defender for IoT alerts to Azure 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

100

80

60

40

20

Go to log analytics

Open connector page

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

Home > Azure Sentinel > Azure Sentinel > Azure Defender for IoT (Preview) ...

Azure Defender for IoT (Preview)

Not connected Microsoft Provider Last Log Received

Description

Gain insights into your IoT security by connecting Azure Defender for IoT alerts to Azure 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

100
80
60
40
20
0

September 25 September 27 September 29

Total data received 10

Instructions Next steps

Prerequisites

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

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

Configuration

Connect Azure Defender for IoT to Azure Sentinel

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

Azure Defender for IoT pricing model >

Select the relevant Subscriptions to connect

Connect All Disconnect All

Search

Subscription ↑↓

AIA Account

Connect (highlighted with a red arrow) Disconnect Status Disconnected

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

Status

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.

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



Analytics rule wizard - Create new rule from template

Create incidents based on Azure Defender for IOT alerts

[General](#)[Automated response](#)[Review and create](#)

Create an analytics rule that creates incidents based on alerts generated in another Microsoft security service.

Analytics rule details

Name *

 Create incidents based on Azure Defender for IOT alerts

Description

 Create incidents based on all alerts generated in Azure Defender for IOT

Status

[Enabled](#) [Disabled](#)

Analytics rule logic

Microsoft security service *

 Azure Defender for IoT

Filter by severity

 Any Custom

Include specific alerts

Only create incidents from alerts that contain the following text in the alert name

[Next : Automated response >](#)

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

40 Active rules

Rules by severity

High (3) Medium (0) Low (0) Informational (37)

Active rules Rule templates

Severity ↑ Name ↑ Rule type ↑ Data sources Tactics

Severity	Name	Rule type	Data sources	Tactics
High	TEARDROP memory-only drop...	Scheduled	Microsoft 365 Defe...	Execution Persistence
High	Exchange SSRF Autodiscover Pr...	Scheduled	Azure Monitor (IIS)	Initial Access
High	Alsid Password Guessing	Scheduled	Alsid for Active Dire...	Credential Access
High	User login from different count...	Scheduled		Initial Access
High	SUNBURST and SUPERNOVA b...	Scheduled		
High	Solorigate Named Pipe	Scheduled	Security Events +1	Lateral Moveme...
High	Modified domain federation tr...	Scheduled	Azure Active Direct...	Credential Access
High	Create incidents based on Azur...	Microsoft Secur...	Azure Active Direct...	
High	Vectra AI Detect - Account in t...	Scheduled	AI Vectra Detect (Pr...	Execution Persistence
High	First access credential added to...	Scheduled	Azure Active Direct...	Credential Access
High	Security Service Registry ACL M...	Scheduled	Security Events +1	Defense Evasion
High	Solorigate Network Beacon	Scheduled	DNS (Preview) +5	Command and ...

Severity : All Rule Type : All Tactics : All More (1)

Search

Rule query

```
DeviceEvents
| where ActionType has "ExploitGuardNonMicrosoftSignedBlocked"
| where InitiatingProcessFileName contains "svchost.exe" and FileName contains "NetSetupSvc.d1l"
```

Rule frequency

Run query every 1 day

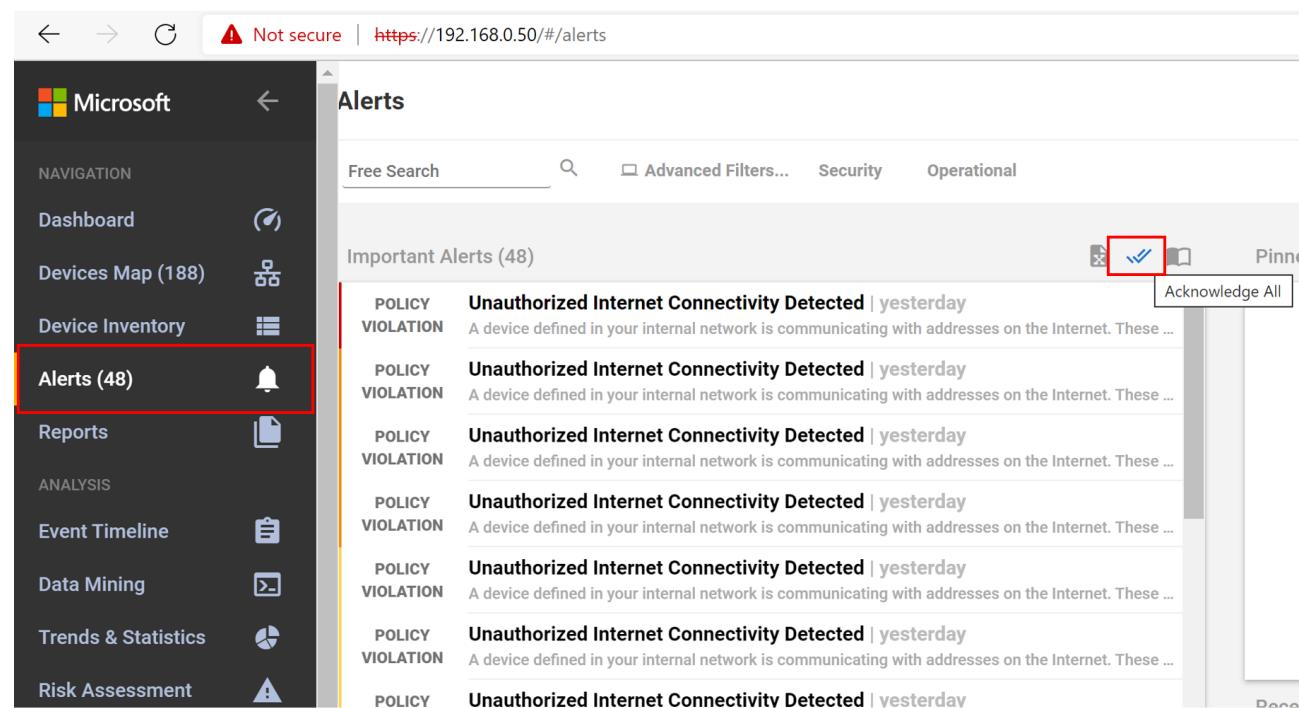
Note:

- You haven't used this template yet; You can use it to create analytics rules.
- One or more data sources used by this rule is missing. This might limit the functionality of the rule.

Create rule

Task 3: Acknowledge Alerts and Re-run PCAPs

1. Go back to your browser interface and acknowledge all of the alerts. The reason we are doing this is so we can re-run the alerts to show how they are sent and analyzed by Sentinel.
 - i. Navigate to the Alerts Page
 - ii. Click the double check box
 - iii. Click **Ok** to acknowledge the alerts



Alerts

Free Search Advanced Filters... Security Operational

Important Alerts (48)

POLICY VIOLATION	Unauthorized Internet Connectivity Detected yesterday A device defined in your internal network is communicating with addresses on the Internet. These ...
POLICY VIOLATION	Unauthorized Internet Connectivity Detected yesterday A device defined in your internal network is communicating with addresses on the Internet. These ...
POLICY VIOLATION	Unauthorized Internet Connectivity Detected yesterday A device defined in your internal network is communicating with addresses on the Internet. These ...
POLICY VIOLATION	Unauthorized Internet Connectivity Detected yesterday A device defined in your internal network is communicating with addresses on the Internet. These ...
POLICY VIOLATION	Unauthorized Internet Connectivity Detected yesterday A device defined in your internal network is communicating with addresses on the Internet. These ...
POLICY VIOLATION	Unauthorized Internet Connectivity Detected yesterday A device defined in your internal network is communicating with addresses on the Internet. These ...
POLICY VIOLATION	Unauthorized Internet Connectivity Detected yesterday A device defined in your internal network is communicating with addresses on the Internet. These ...
POLICY VIOLATION	Unauthorized Internet Connectivity Detected yesterday A device defined in your internal network is communicating with addresses on the Internet. These ...

Acknowledge All

4. Now go to the System Setting tab.

5. Click the Play All on the PCAP Files to replay simulating the alerts.

Task 4: Sentinel interaction with IoT Incidents

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

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

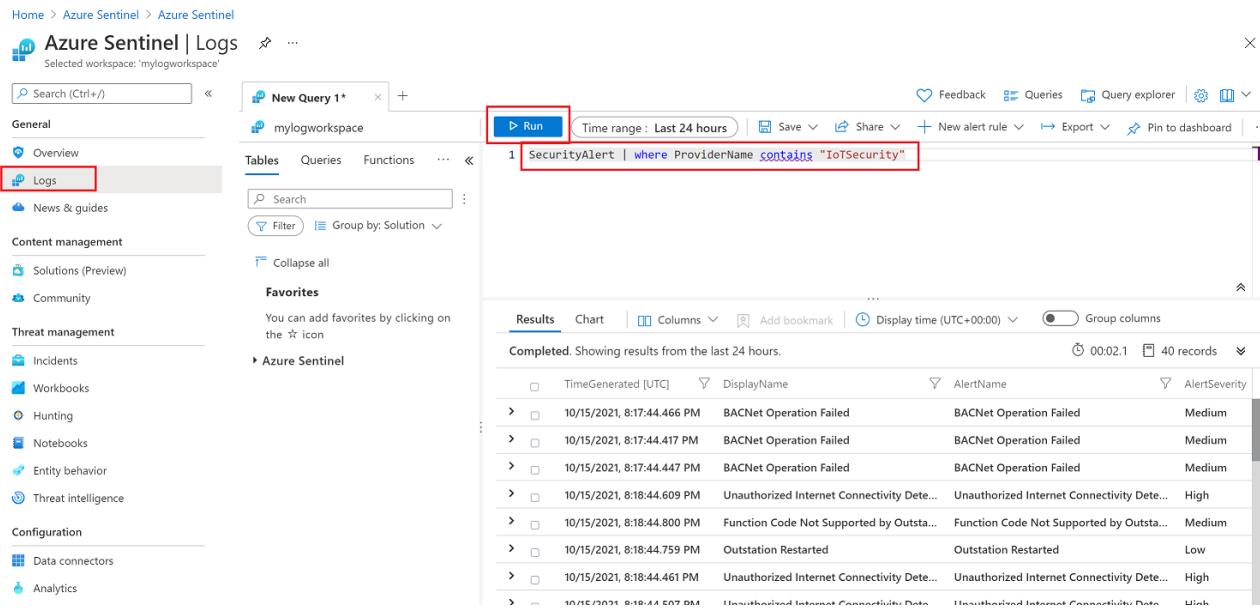
3. It will take you to this screen to get all the information relative to the incident. This allows analyst to get more details on the entity including what other alerts made up the incident, playbooks to enrich the context of the alert, and comments section to leave details on what the analyst discovered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

Task 5: Kusto Query Language to Find Alert Details

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

Here are two basic examples:

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



The screenshot shows the Azure Sentinel Logs interface. The left sidebar is collapsed, and the main area shows a query results table. The query is:

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

The results table has the following columns and data:

TimeGenerated [UTC]	DisplayName	AlertName	AlertSeverity
10/15/2021, 8:17:44.466 PM	BACNet Operation Failed	BACNet Operation Failed	Medium
10/15/2021, 8:17:44.417 PM	BACNet Operation Failed	BACNet Operation Failed	Medium
10/15/2021, 8:17:44.447 PM	BACNet Operation Failed	BACNet Operation Failed	Medium
10/15/2021, 8:18:44.609 PM	Unauthorized Internet Connectivity Dete...	Unauthorized Internet Connectivity Dete...	High
10/15/2021, 8:18:44.800 PM	Function Code Not Supported by Outsta...	Function Code Not Supported by Outsta...	Medium
10/15/2021, 8:18:44.759 PM	Outstation Restarted	Outstation Restarted	Low
10/15/2021, 8:18:44.461 PM	Unauthorized Internet Connectivity Dete...	Unauthorized Internet Connectivity Dete...	High
10/15/2021, 8:18:44.444 PM	Unauthorized Internet Connectivity Dete...	Unauthorized Internet Connectivity Dete...	High

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

Completed. Showing results from the last 7 days. 00:00

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 devi
10/1/2021, 4:00:04.087 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server retur
10/1/2021, 4:00:07.358 PM	Controller Stop	Controller Stop	Low	The source de
10/1/2021, 4:00:07.445 PM	Port Scan Detected	Port Scan Detected	High	A source devi

Exercise 7: Clean Up

Task 1: Delete resources

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

Search for the Resource Group created for this training.

Select Delete resource group on the top right side.

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

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

Appendix: Troubleshooting

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

`cyberx-xsense-sanity`

```
Last login: Wed Sep 29 10:11:10 2021
cyberx@xsense: ~ cyberx-xsense-sanity
[+] C-Cobra Engine | Running for 0:15:59
[+] 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      0 127.0.0.1:39428      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      172.22.16.1:57841      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: ~
```

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      0 172.22.16.2:22      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 adgiothol.azure-devices.net
PING ihsu-eastus-4.eastus.cloudapp.azure.com (20.49.110.134) 56(84) bytes of data.
 64 bytes from ihsu-eastus-4.eastus.cloudapp.azure.com (20.49.110.134):
```