# Defender For Endpoint (MDE) Onboarding Index

 Defender for Endpoint Plan 1:

 Defender for Endpoint Plan 2:

 Requirements

 Licensing Requirements

 Difference between Microsoft \*\*Defender for Business servers\*\* and \*\*Microsoft Defender for Servers Plan 1 and Plan 2\*\*

 Network and Data Storage and Configuration Requirements  Microsoft Defender Antivirus Configuration Requirement

 MDE on non-Microsoft Products  Mac OS

 Not Currently Supported on macOS Endpoints:  Linux

 Not Currently Supported on Linux Endpoints:

 Android  IOS

 Onboarding Servers to Microsoft Defender for Endpoint.

 Onboarding Using Local Script

 Onboarding 2019 and 2022 Servers.

 Registry Which Shows the Onboarding Status

 Registry of a Machine Which is On-boarded

 Registry of a Machine Which is not yet On-boarded  Onboarding 2012 and 2016 Servers

 Windows 2016 Server Onboarding

 Onboarding Linux (Ubuntu) Servers  Onboarding Linux (CentOS) Servers

# Defender for Endpoint Plan 1:

Microsoft Defender for Endpoint P1 delivers core endpoint protection capabilities such as  Next-generation protection

 Manual response actions

 Attack surface reduction capabilities  Attack surface reduction rules

 Ransomware mitigation

 Device control  Web protection

 Network protection Network firewall

 Application control

 Centralized configuration and management  Role-based access control

 APIs

 Protection for a variety of platforms

Microsoft Defender for Endpoint P1 is available as a standalone user subscription license and as part of Microsoft 365 E3/A3/G3.

# Defender for Endpoint Plan 2:

Microsoft Defender for Endpoint P2 delivers comprehensive endpoint protection capabilities including *all the capabilities of Microsoft Defender for Endpoint P1* with additional capabilities such as

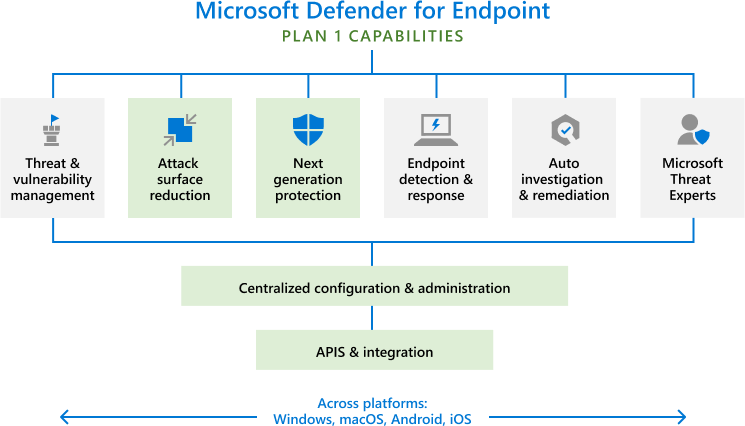
 Core Defender Vulnerability Management  Attack surface Reduction

 Next-generation Protection

 Endpoint detection And response

 Automated investigation And remediation  Microsoft Threat Experts

The green boxes in the following image depict what's included in Defender for Endpoint Plan 1:



# Requirements

## Licensing Requirements

[source](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum-requirements?view=o365-worldwide&%3A~%3Atext=Business%20requirements.-%2CLicensing%20requirements%2C-Defender%20for%20Endpoint)

**!** To onboard servers to the standalone versions of Defender for Endpoint, server licenses are

required.

 Microsoft Defender for Servers Plan 1 or Plan 2 (as part of the [Defender for Cloud](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction)) offering.

 Microsoft Defender for Endpoint for Servers.  Defender for business.

 To onboard an instance of servers you need an additional license called *Microsoft*

*Defender for Business servers*

 Microsoft Defender for Business servers is available as an add-on to Microsoft 365 Business Premium and the standalone version of Defender for Business.

### Difference between Microsoft Defender for Business servers and Microsoft Defender for Servers Plan 1 and Plan 2

[source](https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-faq?view=o365-worldwide&what-happens-if-i-have-a-mix-of-microsoft-endpoint-security-subscriptions%3A~%3Atext=What%20is%20the%20difference%20between%20Microsoft%20Defender%20for%20Business%20servers%20and%20Microsoft%20Defender%20for%20Servers%20Plan%201%20and%20Plan%202%3F)

|  |  |
| --- | --- |
| **Microsoft Defender for Business servers** | **Microsoft Defender for Servers Plan 1 / Plan 2** |
| [Microsoft Defender for Business servers](https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/get-defender-business?view=o365-worldwide&how-to-get-microsoft-defender-for-business-servers) is an add-on to Defender for Business and Microsoft 365 Business Premium only. | [Microsoft Defender for Servers Plan 1/Plan 2 is an enterprise-focused offering that can](https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers) be purchased with any other Microsoft cloud plan. |
| Provides a single endpoint security experience for both clients and servers within the Microsoft Defender portal ([https://security.microsoft.com](https://security.microsoft.com/)). | Part of [Microsoft Defender for Cloud](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction) |
| Designed for businesses with up to 300 employees. | Includes advanced threat hunting with six months of data retention and the Microsoft Threat Experts service. |
| Enables customers who don't necessarily have a security background to set up, configure, and protect company devices, including servers. | The admin experience for Defender for Cloud resides within the Azure portal ([https://portal.azure.com](https://portal.azure.com/)). |

## Network and Data Storage and Configuration Requirements

When you run the onboarding wizard for the first time, you must choose where your Microsoft Defender for Endpoint-related information is stored: in the European Union, the United Kingdom, or the United States datacenter.

**!** You cannot change your data storage location after the first-time setup.

## Microsoft Defender Antivirus Configuration Requirement

Defender for Endpoint agent depends on *Microsoft Defender Antivirus (MDA)* to scan files and provide information about them.

When *Microsoft Defender Antivirus* isn't the primary antimalware solution in your organization but Defender for Endpoint (MDE) is still used, *MDAV enters passive mode*. This mode implies a specific set of limitations compared to its active state:

Active mode benefits:  Scan files.

 Report threats.

 Provide EDR capabilities Passive mode *Limitations*:

 Real-time protection.

 Scheduled scans.  EDR functionality.

 Attack surface reduction.

 Network protection.

passive mode turns MDAV into a reporting and monitoring tool. It helps identify potential threats but leaves the actual mitigation and response to your chosen primary solution.

# MDE on non-Microsoft Products

 You'll need to confirm the Linux distributions and versions of Android, iOS, and macOS are compatible with Defender for Endpoint.

## Mac OS

 Microsoft Defender for Endpoint on macOS offers  antivirus,

 endpoint detection and response (EDR),  vulnerability management capabilities.

For the three latest released versions of macOS.

 Customers can deploy and manage the solution through Microsoft Intune and Jamf.

### Not Currently Supported on macOS Endpoints:

 Security Management for Microsoft Defender for Endpoint

## Linux

 Microsoft Defender for Endpoint on Linux offers  antivirus (AV),

 endpoint detection and response (EDR),

 vulnerability management capabilities for Linux servers.

 Includes a full command line experience to configure and manage the agent, initiate scans, and manage threats.

 We support recent versions of the six most common Linux Server distributions: RHEL 7.2+, CentOS Linux 7.2+, Ubuntu 16 LTS, or higher LTS, SLES 12+, Debian 9+, and Oracle Linux 7.2.

### Not Currently Supported on Linux Endpoints:

 Data loss prevention

 Security Management for Microsoft Defender for Endpoint

## Android

Running 6.0 and higher Web protection

 Anti-phishing

 Blocking of unsafe connections

 Scan for

 Malware

 Unwanted applications

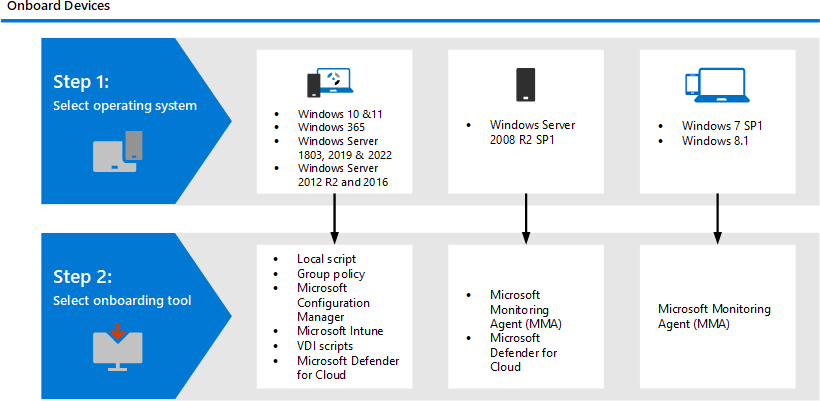
 Additional breach prevention capabilities through integration with Microsoft Intune and Conditional Access.

## IOS

Running ISO 11.0 and higher.

Devises that are registered within customer's tenant are supported. Same Features which are provided to Android.

# Onboarding Servers to Microsoft Defender for Endpoint.



## Onboarding Using Local Script

You first manually onboard individual devices to MDE.

You might want to do this first when *testing* the service before you commit to onboarding all the devices in your network.

This script has been optimized for use on up to ten devices.

Local scripting is a special onboarding method for evaluating (testing) Microsoft Defender for Endpoint.

The data reporting frequency is *higher* than with other onboarding methods when onboarding using a local script.

Not normally used in production deployments.

Microsoft recommends limiting the number of deployments using local scripts to *ten*.

If you want to onboard more than 10 devices, it is recommended to use other deployment options like *Group Policy* or *Microsoft Endpoint Configuration Manager*.

The onboarding process is straight forward for 2019 and 2022 servers as the *MDE.Windows* extension is already integrated with operating system. We just have to provision it using the onboarding script

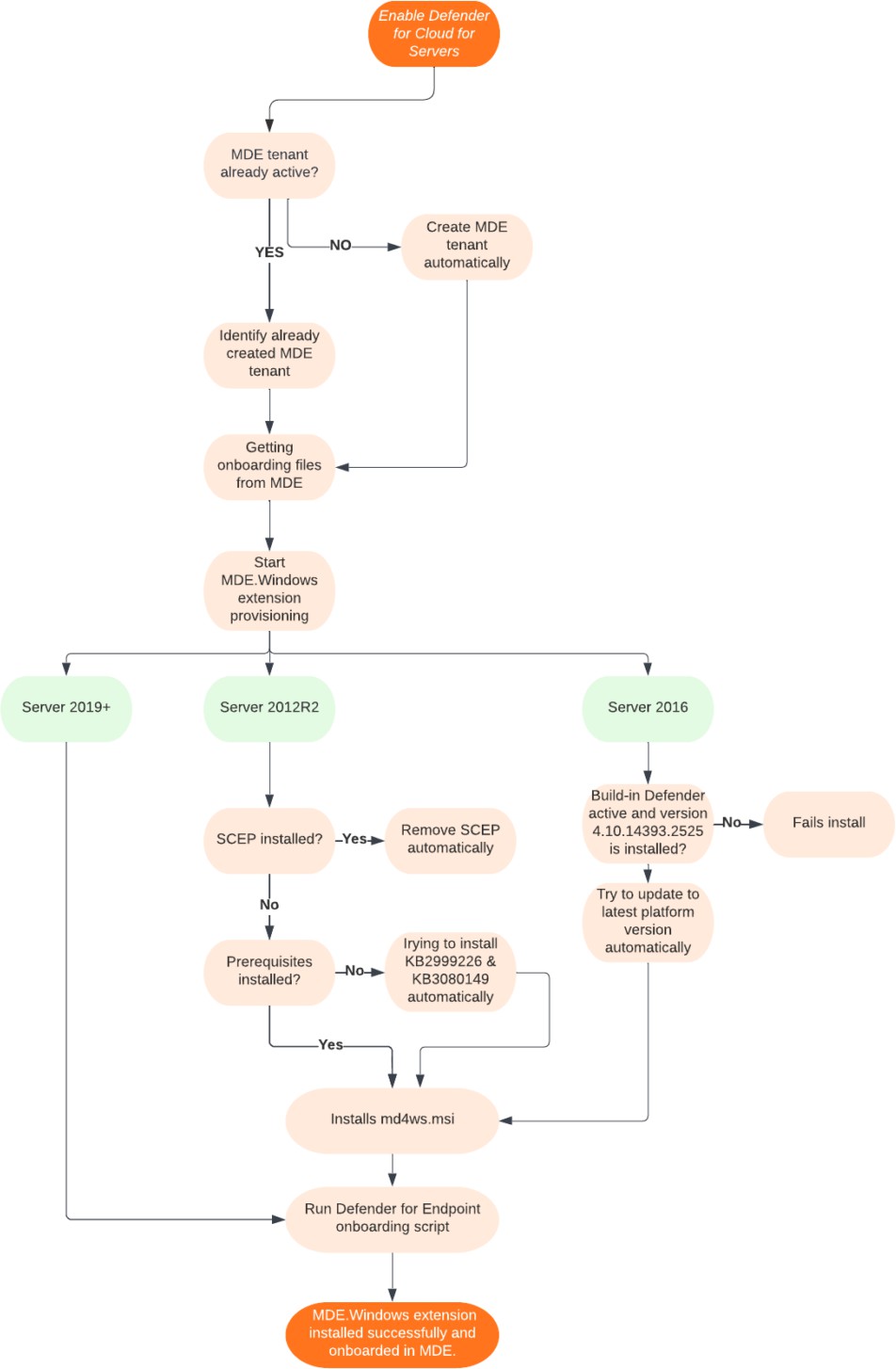
But in previous versions 2019 and 2012 servers needs some extra steps to onboard. There are some pre-requisites for the on-boarding process.

 The servers needs to be updated (security updates).

 Two packages *md4ws.msc* package and *on-boarding script* needs to be downloaded from the defender portal.

 Md4ws script should be executed and then on-boarding script.

This will now on-board the server to MDE.

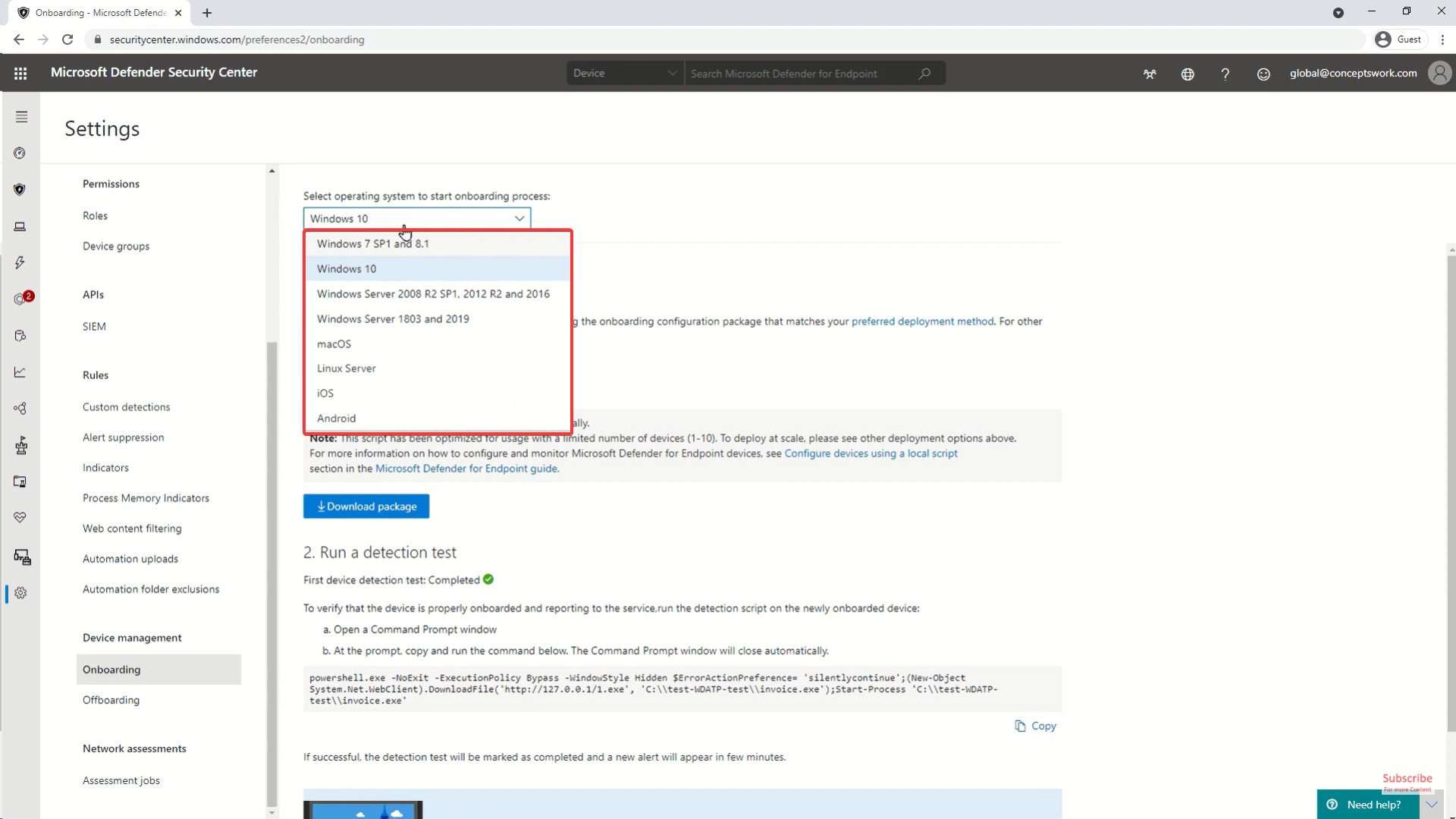


### Onboarding 2019 and 2022 Servers.

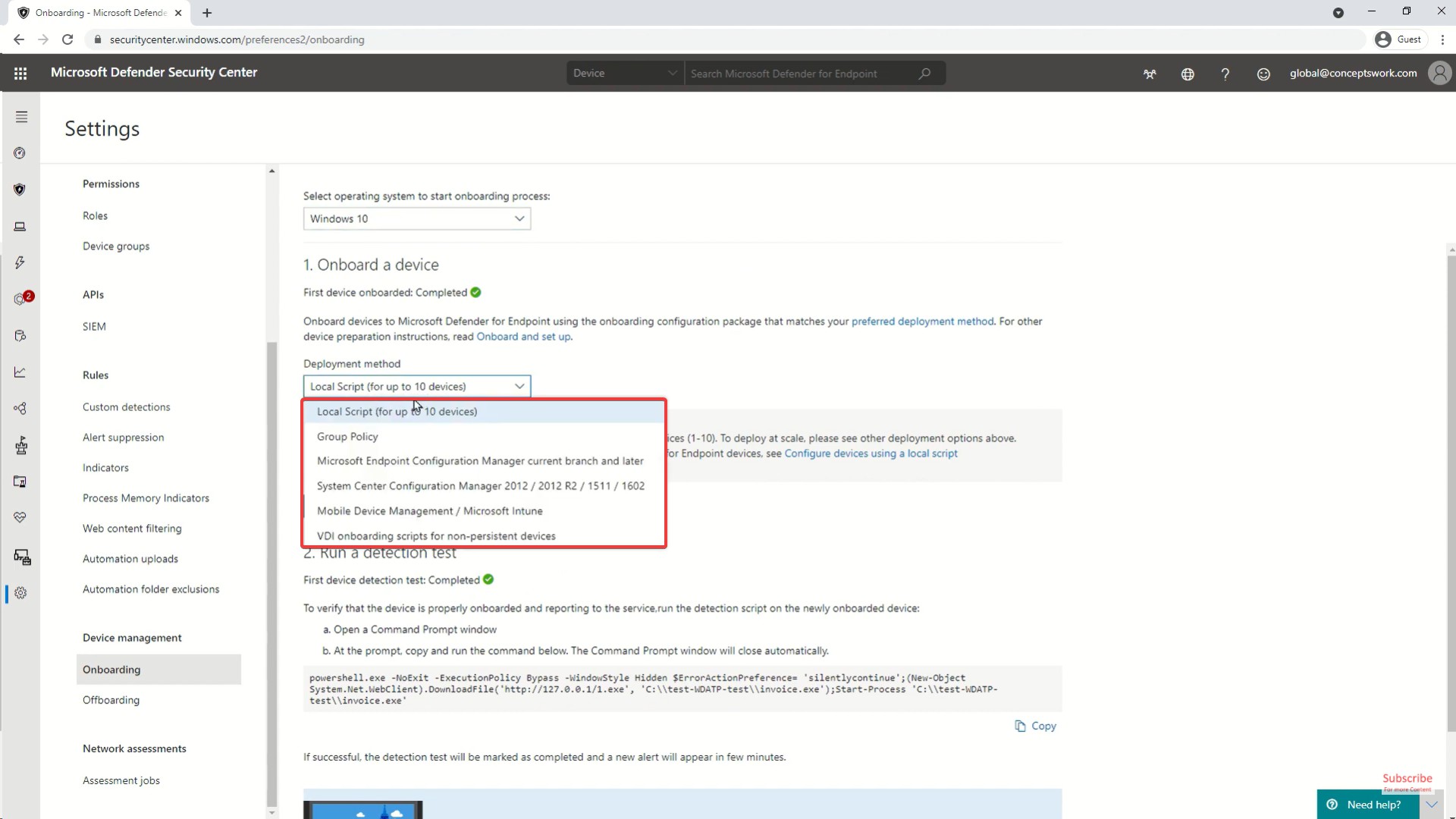
You can get the *Local Script package* from the *Microsoft Defender portal*. Click on

Settings > Onboarding

Select an operating system : The process of onboarding will change depending on the operating system you choose.



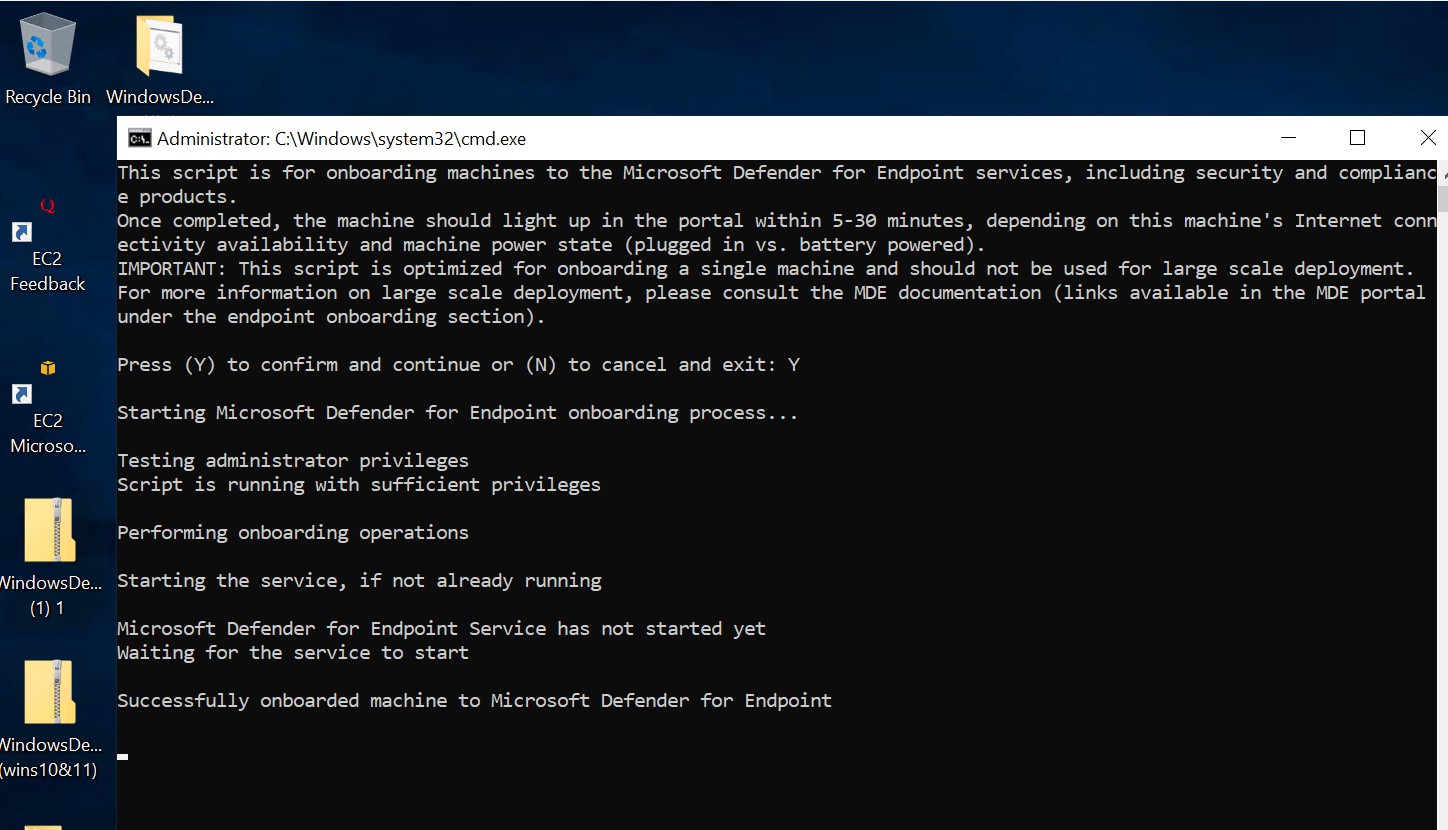
Deployment model : Select *Local Script*



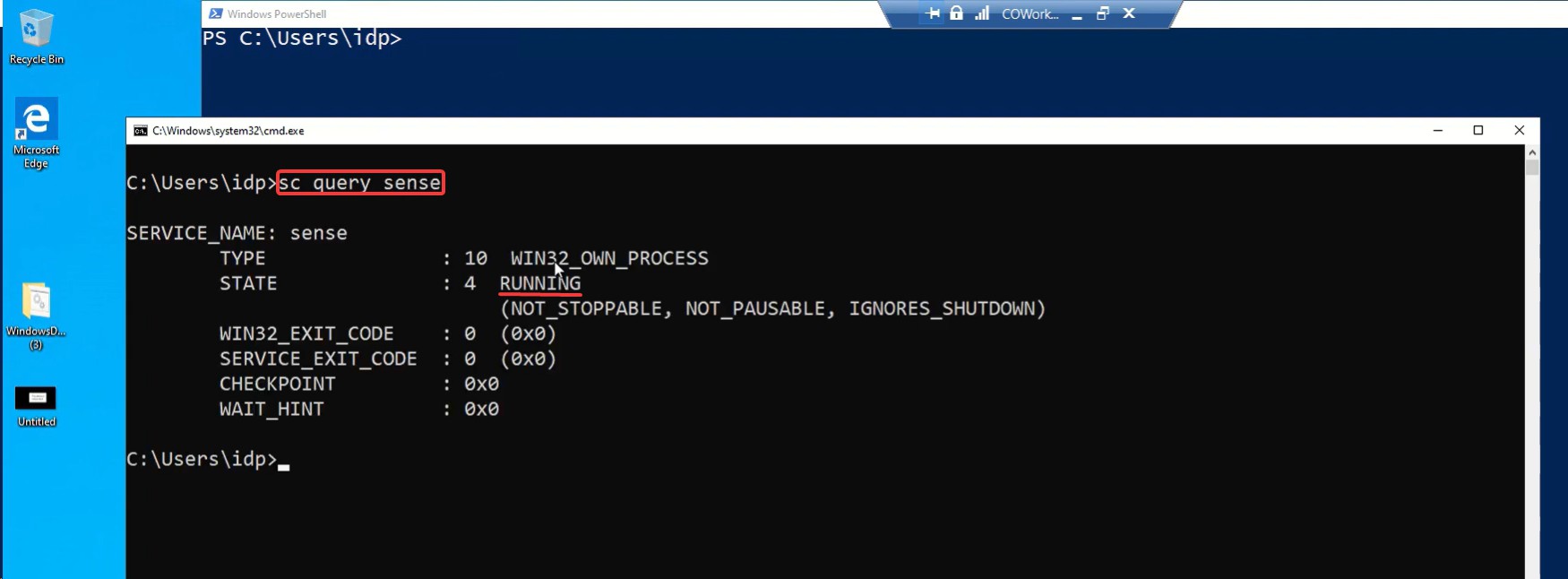
Now you can download the Package.

Run the Script by extracting the package in the server you want to onboard. You can only run the script as an administrator.

The onboarding process will begin.



You can run the cmd command to check the status of on-boarding.

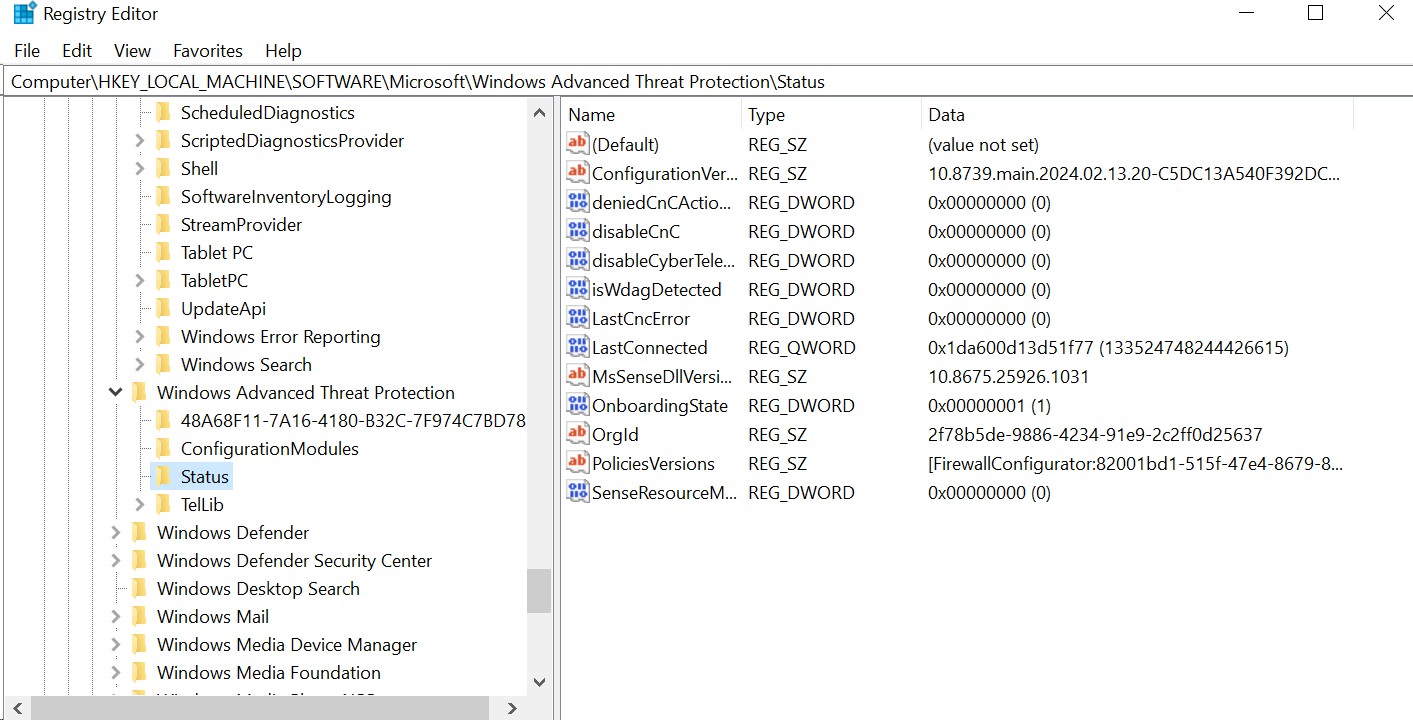


sc query sense

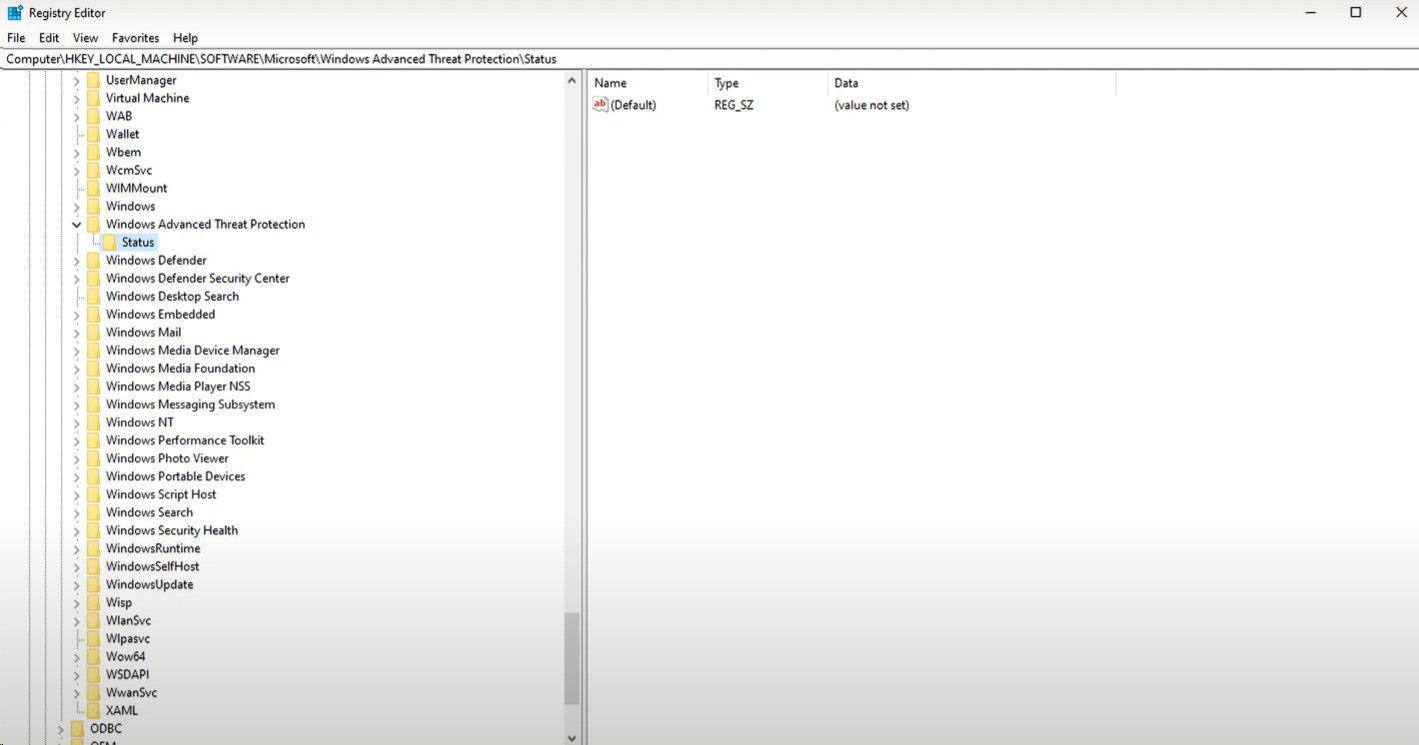
#### Registry Which Shows the Onboarding Status

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\Advanced Threat Protection\Status

**Registry of a Machine Which is On-boarded**

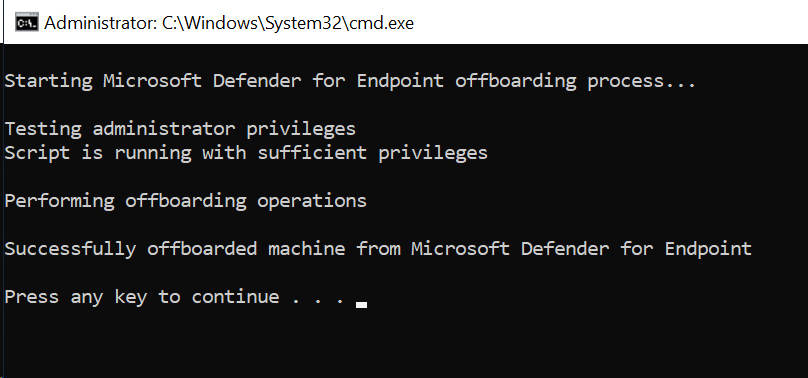


**Registry of a Machine Which is not yet On-boarded**



 Running the On-boarding Script will change the registry.

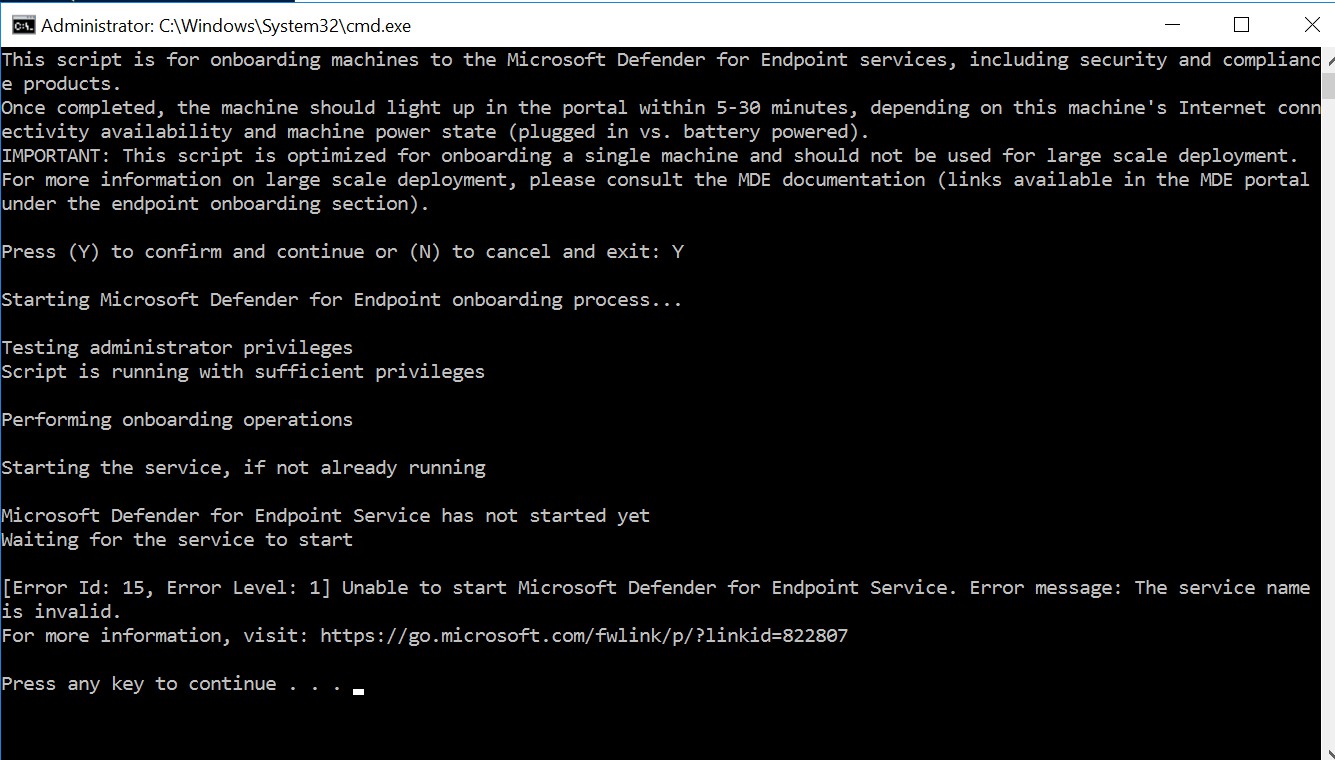
 It will take some time to show the on-boarded in defender endpoint portal.  You can also offboarding using Local Script.



 This will change the registry properties: OnboardingState to 0.

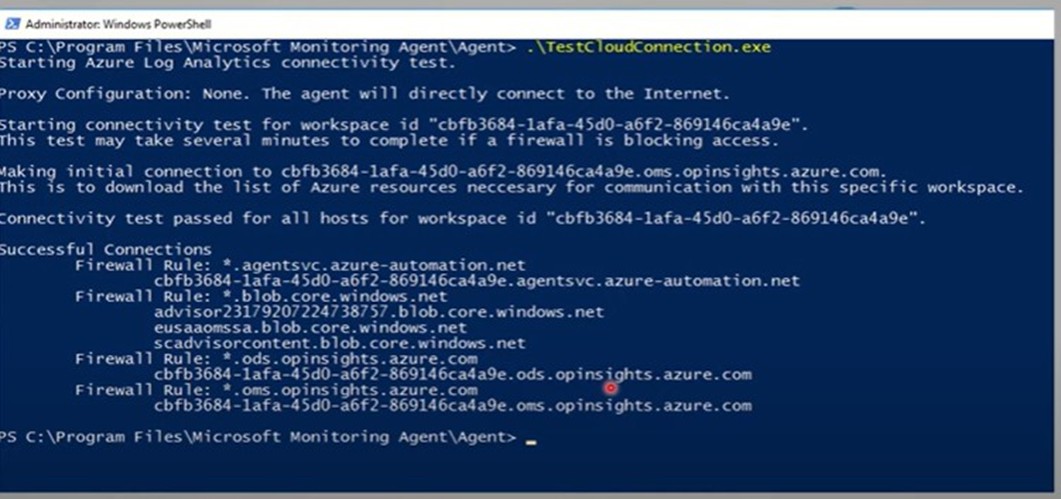
### Onboarding 2012 and 2016 Servers

 If you try to on-board directly, it will give you an error.



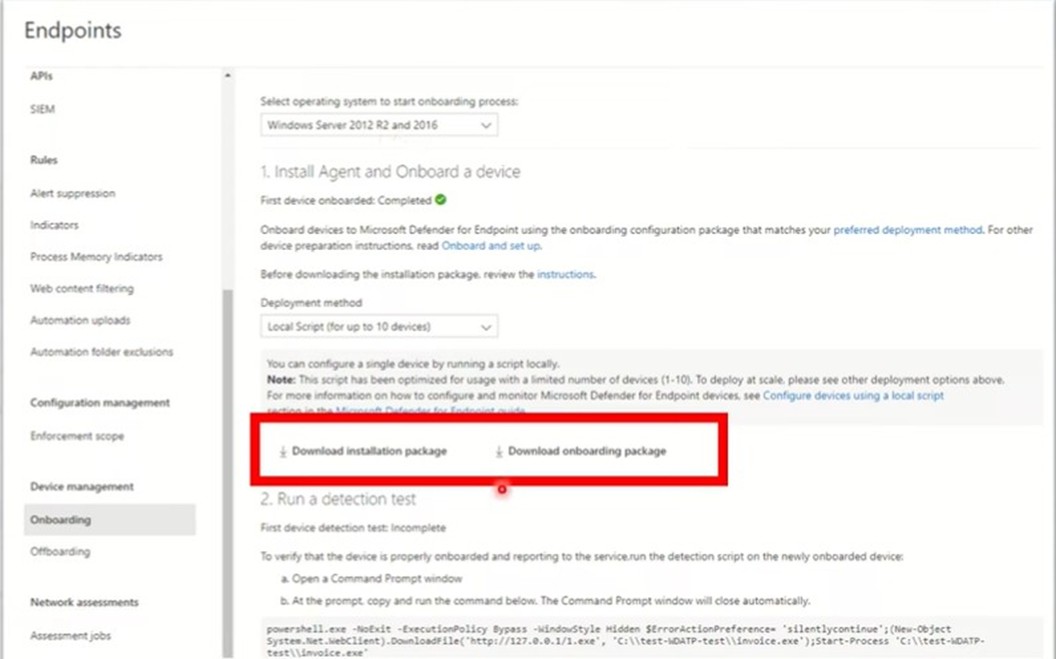
#### Windows 2016 Server Onboarding

In Older method the MMA agent is inbuilt in 2016, just have to turn on "Windows defender features" and then check in settings if Windows Defender appears in the blade or if in Recovery tabs there is Microsoft defender. So, you have to install an MMA agent manually along with



In the workflow we can see or select to install windows defender features and check by accessing windows defender

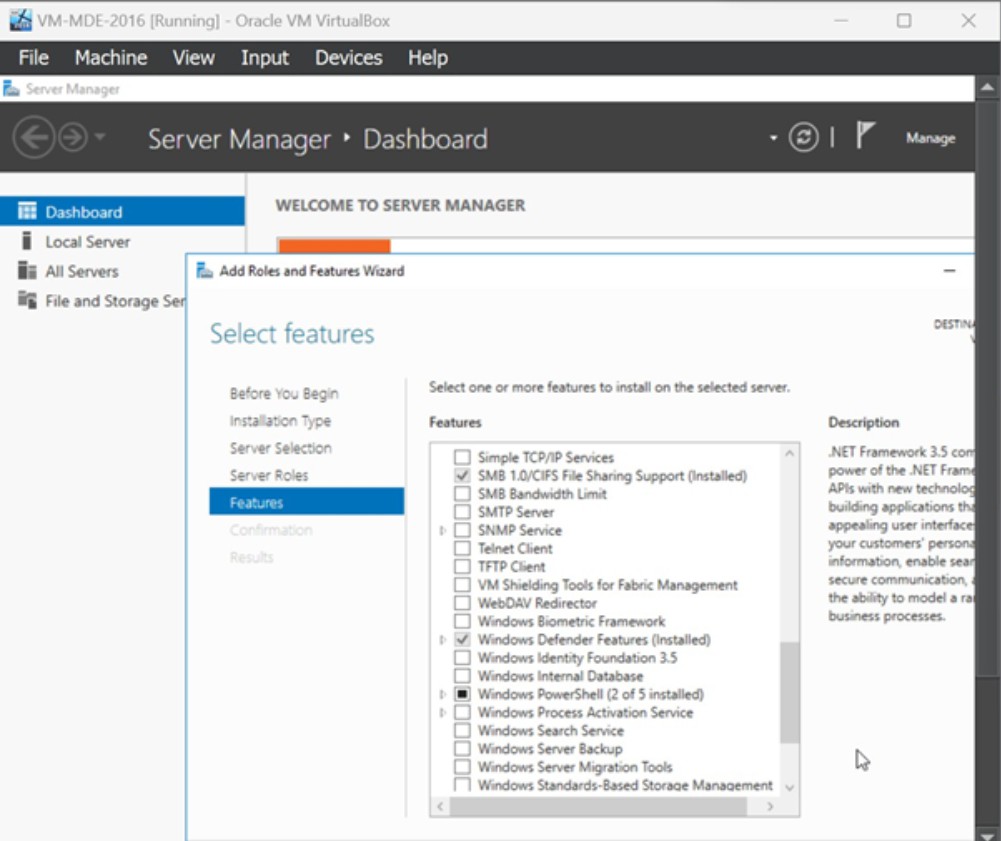
But, the new solution which is the modern unified solution for 2012 and 2016 is as simple as a toggle button.



Here as you can see the process has been streamlined a lot and it just shows up as an option to just choose and complete the same process twice as quickly.



So since we already know that the AV solution is there on the 2016 one in-built what it does is the solution aids in installing the EDR solution as well and then we can just go ahead and complete the onboarding steps.



The installation package is Windows Defender Antivirus agent

**Prerequisites for Windows Server 2016**

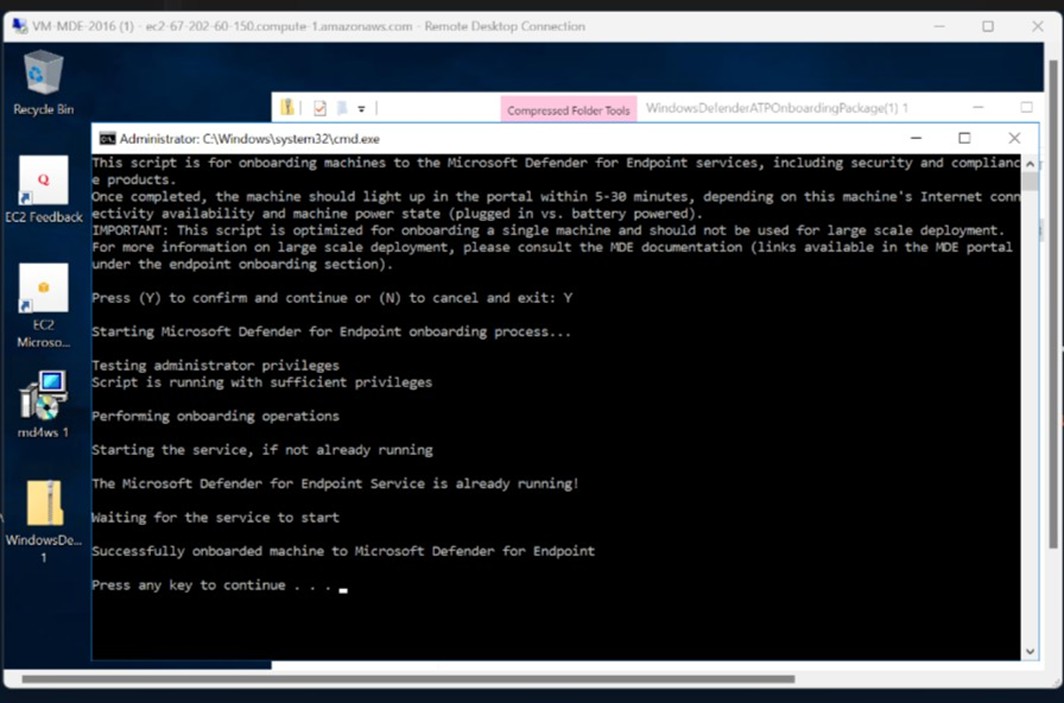
It's recommended to install the latest available SSU and LCU on the server.

The Servicing Stack Update (SSU) from September 14, 2021 or later must be installed. The Latest Cumulative Update (LCU) from September 20, 2018 or later must be installed.

Enable the Microsoft Defender Antivirus feature and ensure it's up to date. For more [information on enabling Defender Antivirus on Windows Server, see Re-enable Defender](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-update-mdav-to-latest-ws?view=o365-worldwide&re-enable-microsoft-defender-antivirus-on-windows-server-if-it-was-disabled) [Antivirus on Windows Server if it was disabled and Re-enable Defender Antivirus on Windows Server if it was uninstalled.](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-update-mdav-to-latest-ws?view=o365-worldwide&re-enable-microsoft-defender-antivirus-on-windows-server-if-it-was-uninstalled)

Download and install the latest platform version using Windows Update. Alternatively, download the update package manually from the [Microsoft Update Catalog](https://www.catalog.update.microsoft.com/Search.aspx?q=KB4052623) or from [MMPC](https://go.microsoft.com/fwlink/?linkid=870379&arch=x64)

You have to go to the Windows Defender Settings as well and update it manually if required. After the updates are done and the KB packages are up to date, then you have to reboot it and then start your onboarding process aka The MSI installation package and then onboarding script.



### Onboarding Linux (Ubuntu) Servers

The process is different from Ubuntu and CentOS distributions.

Install if isn't installed yet.

curl

sudo apt-get install curl

Install if it isn't installed yet:

libplist-utils

prod

sudo apt-get install libplist-utils

If you're running

Ubuntu 22.04

and wish to deploy MDE from the

curl -o microsoft.list https://packages.microsoft.com/config/[distro]/[version]/[channel].list

channel.

curl -o microsoft.list https://packages.microsoft.com/config/ubuntu/18.04/prod.list

Install repository configuration, if you chose channel:

prod

sudo mv ./microsoft.list /etc/apt/sources.list.d/microsoft-[channel].list

sudo mv ./microsoft.list /etc/apt/sources.list.d/microsoft-prod.list

Install package if not already installed:

gpg

sudo apt-get install gpg

If is not available, then install gnupg .

gpg

sudo apt-get install gnupg

Install Microsoft GPG public key Debian 11 and earlier

Debian 12 and later

curl -sSL https://packages.microsoft.com/keys/microsoft.asc | gpg --dearmor | sudo tee

/etc/apt/trusted.gpg.d/microsoft.gpg > /dev/null

Install the

curl -sSL https://packages.microsoft.com/keys/microsoft.asc | gpg --dearmor | sudo tee

/usr/share/keyrings/microsoft-prod.gpg > /dev/null

HTTPS driver

sudo apt-get install apt-transport-https

Update the repository metadata:

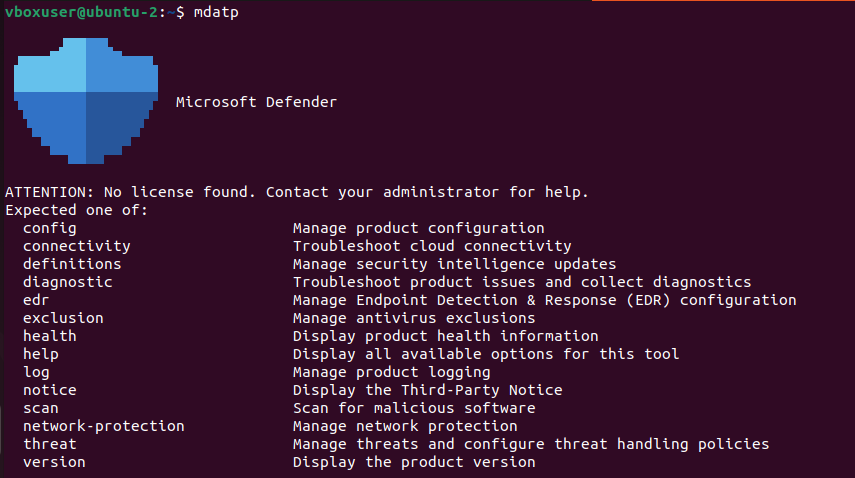
sudo apt-get update

Install

mdatp

sudo apt-get install mdatp

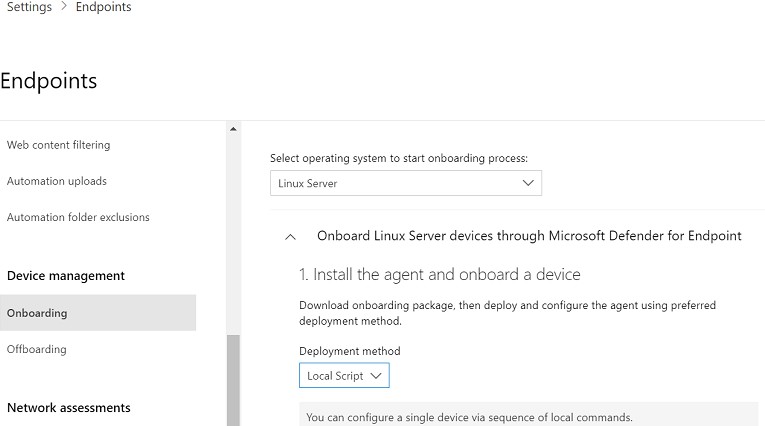
Now verify if it has downloaded



mdatp

Download the for linux in defender portal

onboarding package



Run CMD as administrator. Change the prompt path to the

folder.

downloads

cd Downloads

Unzip the onboard package

unzip WindowsDefenderATPOnboardingPackage.zip

Output

Install python if you don't have it.

Archive: WindowsDefenderATPOnboardingPackage.zip inflating: MicrosoftDefenderATPOnboardingLinuxServer.py

If you're running RHEL 8.x or Ubuntu 20.04 or higher, you'll need to use python3 . For the rest of distros and versions, you'll need to use python .

orgId

sudo apt-get python3

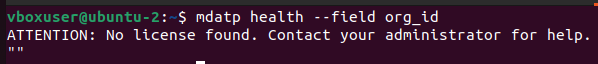
Initially the client device is not associated with an blank.

organization

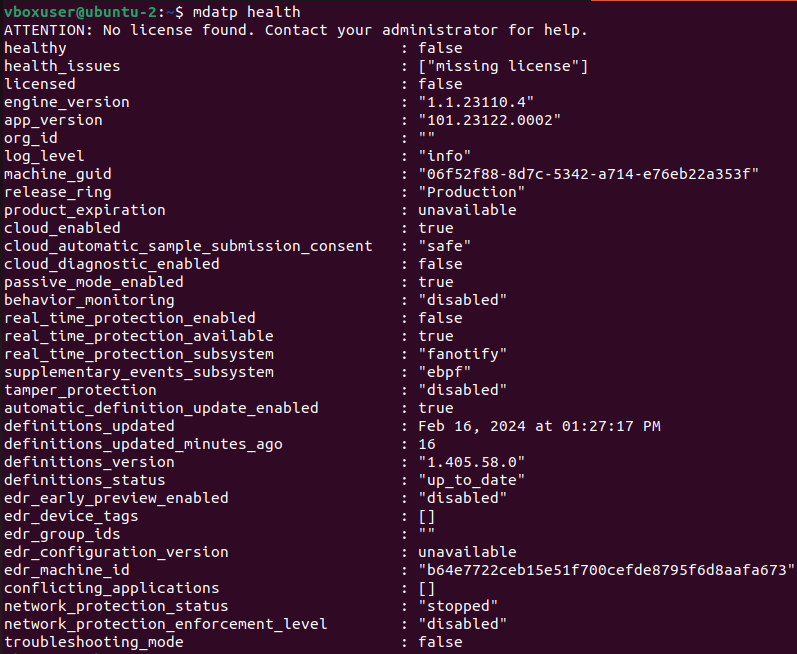
and the

attribute is

mdatp health --field org\_id



Initial Health before on-boarding



mdatp health

Compile the python file (onboarding script)

sudo python3 MicrosoftDefenderATPOnboardingLinuxServer.py

Or

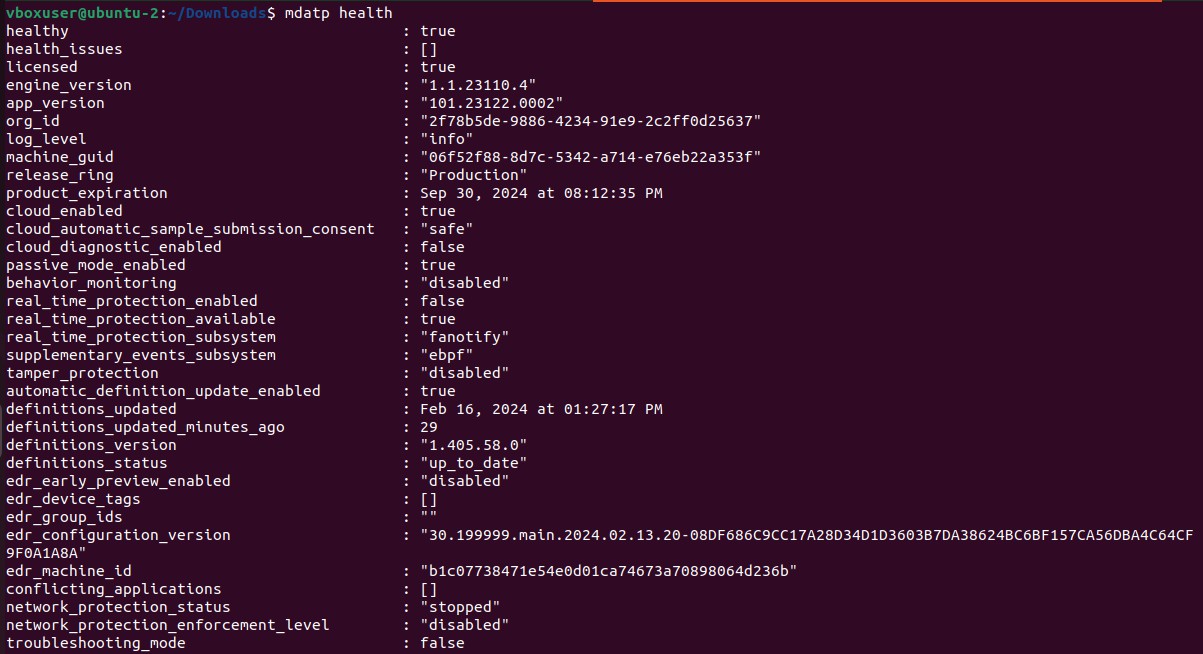


sudo python MicrosoftDefenderATPOnboardingLinuxServer.py

This will onboard the Linux server to MDE

To verify, use

mdatp



mdatp health --field org\_id

mdatp health

Usually takes 24 hours to onboard.

### Onboarding Linux (CentOS) Servers

The process of onboarding Centos servers is same as ubuntu servers.

Difference is that you use instead of sudo . The entire process will be same.

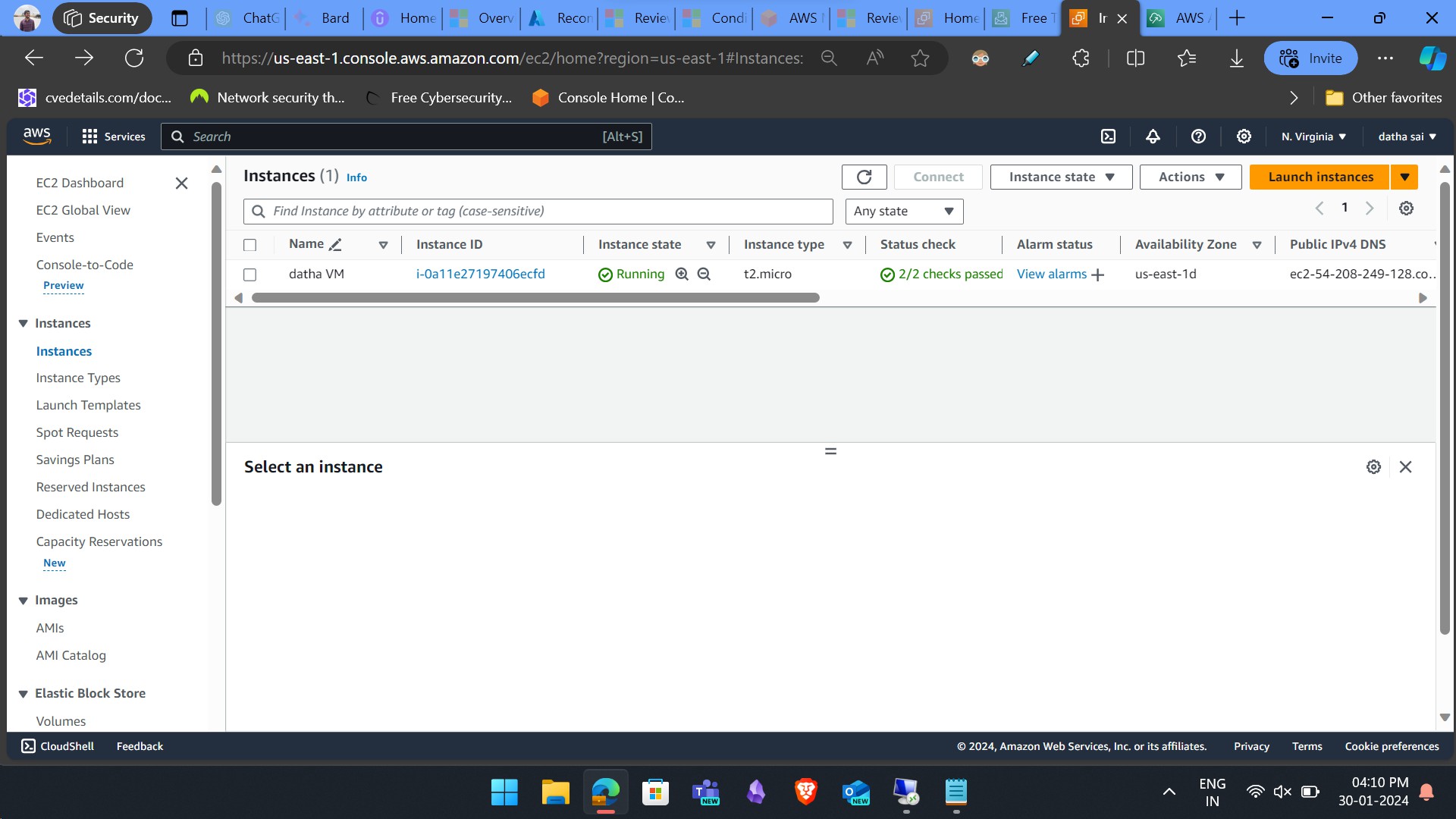
yum

# Onboarding via Arc

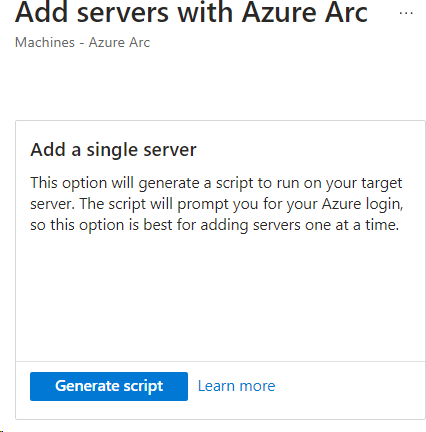
## EC2 Instance in *AWS*

Server from different cloud providers can be directly onboarded to Azure environment using a server called ARC.

Here we are spinning up a server in AWS environment and on-boarded using ARC.

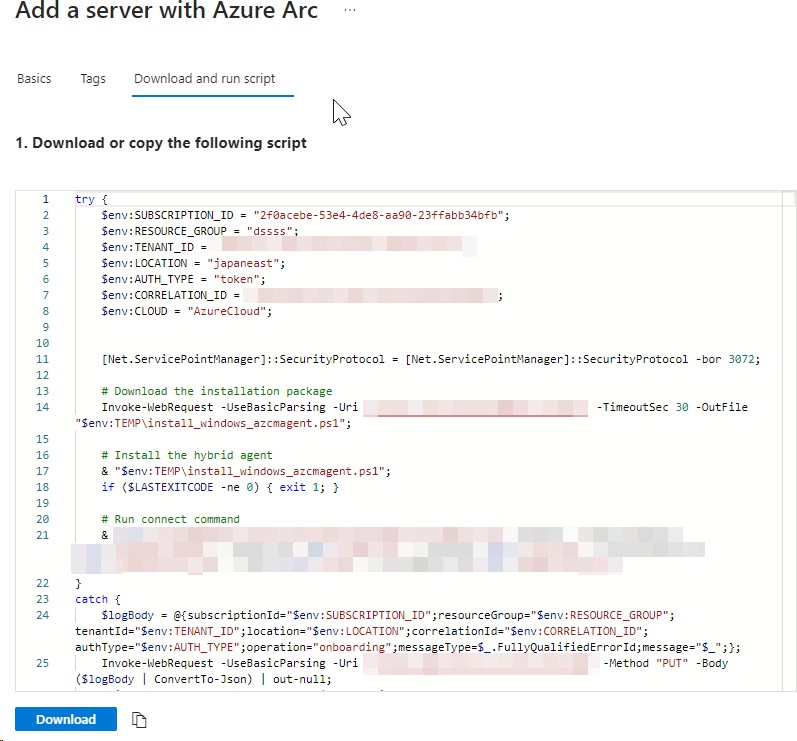


## Onboarding to Azure Using *ARC*



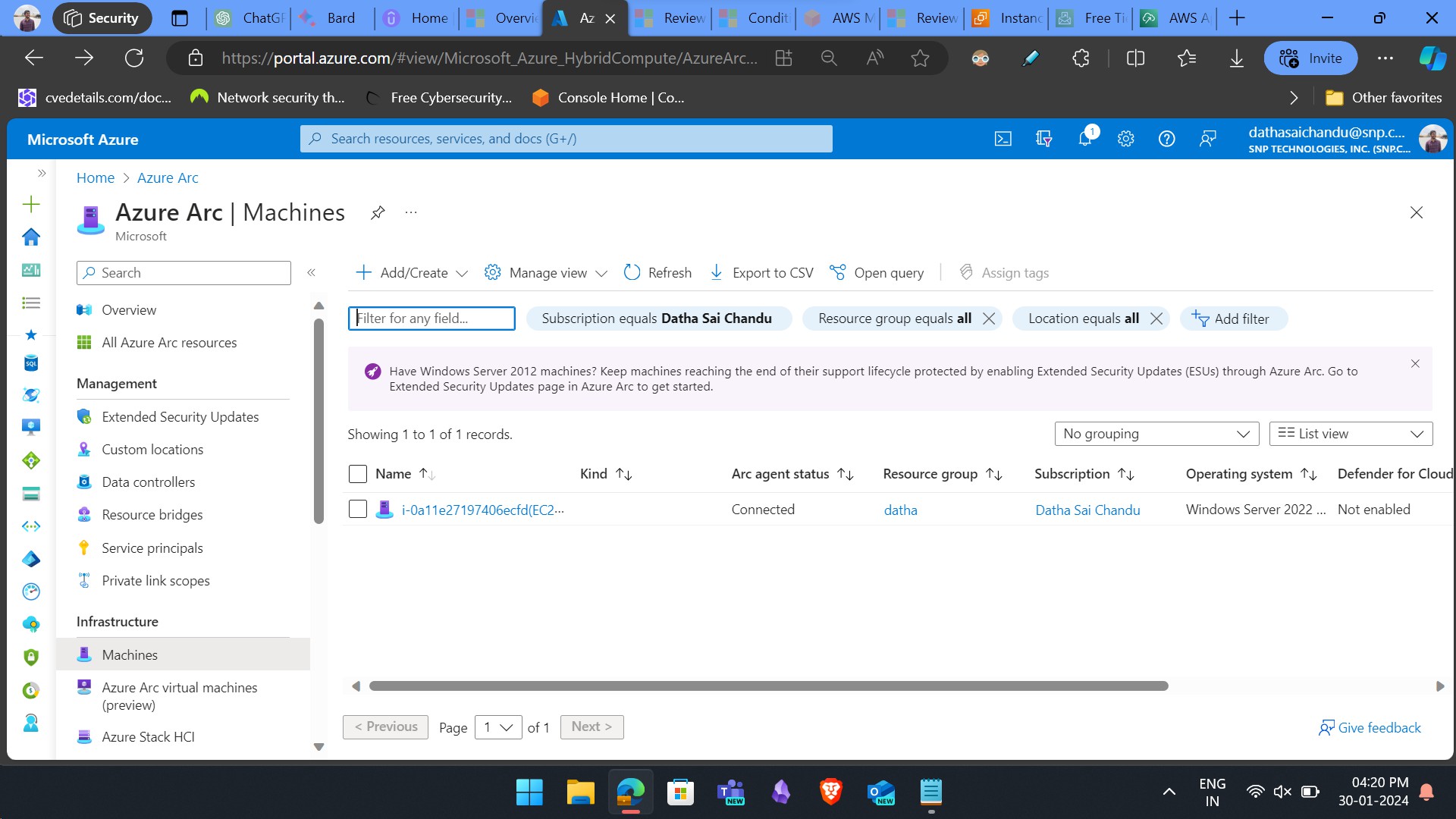
 A script is generated which we use to execute it in powershell with administrator permissions on the server you want to onboard.

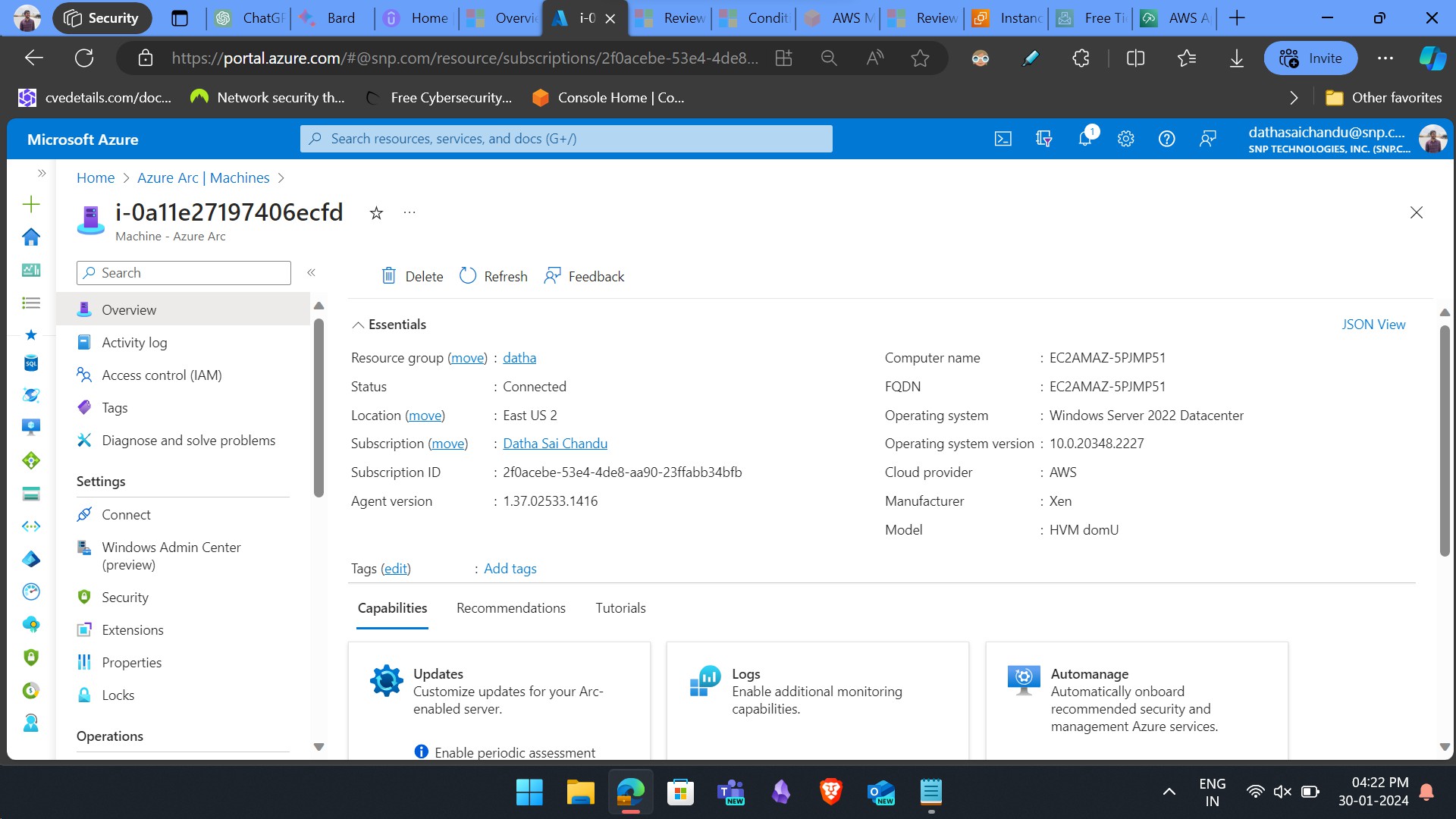
 Click on Generate script and select a region and operating system (Windows or Linux).



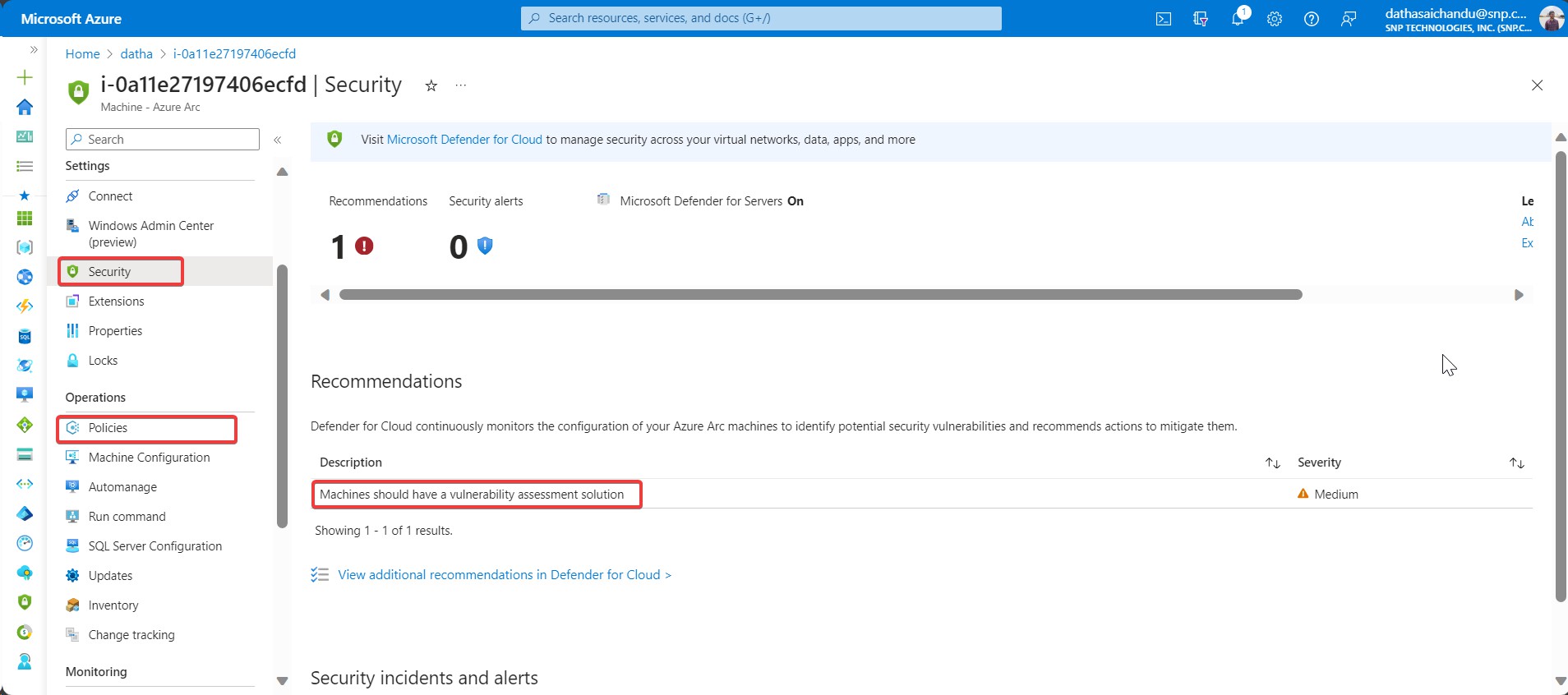
After running the script, the authentication process will happen in that server browser. After you enter the credentials, the on-boarding process will start.

You can see the EC2 server as ARC enabled server in Azure.



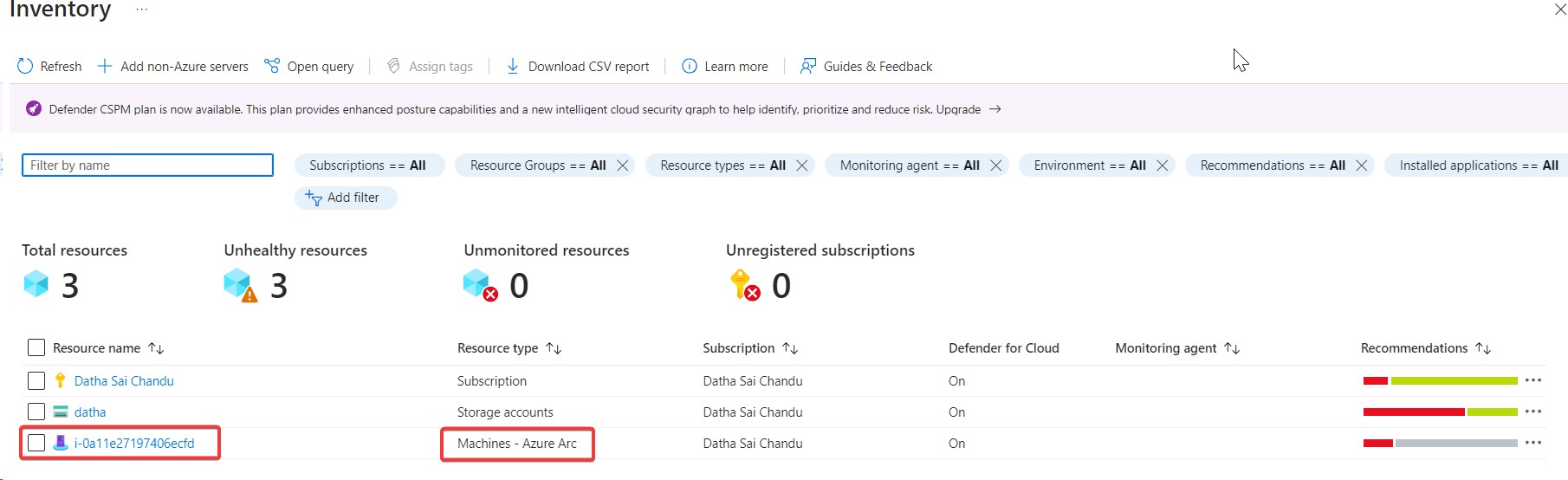


## We Can Manage and Monitor the EC2 in Azure



 The policies and defender can work on that EC2 instance.

## EC2 in Defender Inventory



You will also find that server in the inventory of Defender for cloud.

# Limitations

## Local Script Limitations

This script has been optimized for use on up to ten devices.

The script collects data from the device and transmits it to MDE. The frequency rate is higher than with other onboarding methods when onboarding using a local script. The impacts can be:

 Increased network traffic  Higher resource usage

Not ideal for production. Only for the Evaluation purposes.

## Onboarding Server to Microsoft Defender for Endpoint Through GROUP POLICY

Brief mechanism of onboarding using GROUP POLICY, so If organization wants to onboard all their devices to defender for endpoint to protect devices and endpoints from various cyber threats. But they have large number of servers or devices and they need a convenient way and easy way to onboard all their devices to defender for endpoint they can use a method provided by defender for endpoint i.e GROUP POLICY.

Let’s see how it works – So basically what happens is we just need the installation package and a onboarding script which will be required to be installed and run on the devices for onboarding.

This package can be available form the defender portal <https://security.microsoft.com/> .

Go to Setting blade > Endpoints > Onboarding

Now the onboarding page will be opened, now here Select the type of OS to start the onboarding process. Select the OS type and then chose the deployment method, so here it would be Group Policy. After that on the same page we can see the package to be downloaded (it will be zip file). Now this package consists of a will be used for onboarding. Now just go to Group Policy Management Console and then to control panel and schedule a new task and for that task give action and now provide the file location that was brought for the onboarding, then save the task. Now that group policy will be distributed to all the devices connected to that domain controller and it will take some time to get reflected on Defender for endpoint portal.  
And then all the devices will be visible on the defender for Endpoint portal.

Prerequisites –

To use Group Policy (GP) updates to deploy the package, you must be on Windows Server 2008 R2 or later.

For Windows Server 2019, you may need to replace NT AUTHORITY\Well-Known-System-Account with NT AUTHORITY\SYSTEM of the XML file that the Group Policy preference creates.

Here is step by step guide –

Step 1:  
Go to Microsoft Defender Portal <https://security.microsoft.com/>   
Go to Setting blade > Endpoints > Onboarding   
Now the onboarding page will be opened, now here Select the type of OS to start the onboarding process.

TAKE A NOTE!

Here chose the correct OS type for example if the server you like to onboard is windows 2019 server then select the same server name, because the package and onboarding script generated will work for that particular server. Now that can be a limitation that you have to take care of while selecting the OS type.

Step 2:  
Now Down in the same page there will be drop down box for **DEPLYMENT METHOD** chose **GROUP POLICY** the for onboarding.

Step 3:  
After selecting the deployment method it will show a download package which will be .zip file

Download the .zip file to a location that can be accessed by the device. That file will consist of folder called *OptionalParamsPolicy* and the file *DeviceComplianceLocalOnboardingScript.cmd*   
Once You have downloaded the package now copy it to domain controller or the server where you will apply the group policy.

Step 4:  
Now on that domain controller, go to the **Group Policy Management Console(GPMC)** and then right click the **Group Policy Object(GPO)** and then click on **EDIT.**

**Step 5:**In the Group Policy Management editor, go to **Computer Configuration** , then **Preferences** and then  **Control Panel** settings.

Step 6:Right click on  **Scheduled Task** , point to  **NEW** and then Click  **Immediate Task**

Step 7:  
In the **Task** window that opens, go to the **General** tab. Under **Security options** click **Change User or Group** and type SYSTEM and then click **Check Names** then **OK**. NT AUTHORITY\SYSTEM appears as the user account the task will run as.

Step 8:  
Select **Run whether user is logged on or not** and check the **Run with highest privileges** check box.

Step 9:  
Go to the **Actions** tab and click **New...** Ensure that **Start a program** is selected in the **Action** field. Enter the file name and location of the shared *WindowsDefenderATPOnboardingScript.cmd* file.

Step 10:  
Click **OK** and close any open GPMC windows.

TAKE A NOTE!

It can take several days for devices to start showing on the Devices list. This includes the time it takes for the policies to be distributed to the device, the time it takes before the user logs on, and the time it takes for the endpoint to start reporting.

**GPO limitations:**

* **Complexity and size:** Large and complex GPOs can cause performance issues and replication delays, impacting onboarding speed and success.
* **Network bandwidth:** The larger the number of servers can increase the network traffic during onboarding, potentially putting strain on your network infrastructure.
* **Resource consumption:** Onboarding requires processing power and memory on both the domain controller and target servers which will impact on performance.
* **Management complexity:** Manually managing scripts for a large number of servers can become tediosus task.

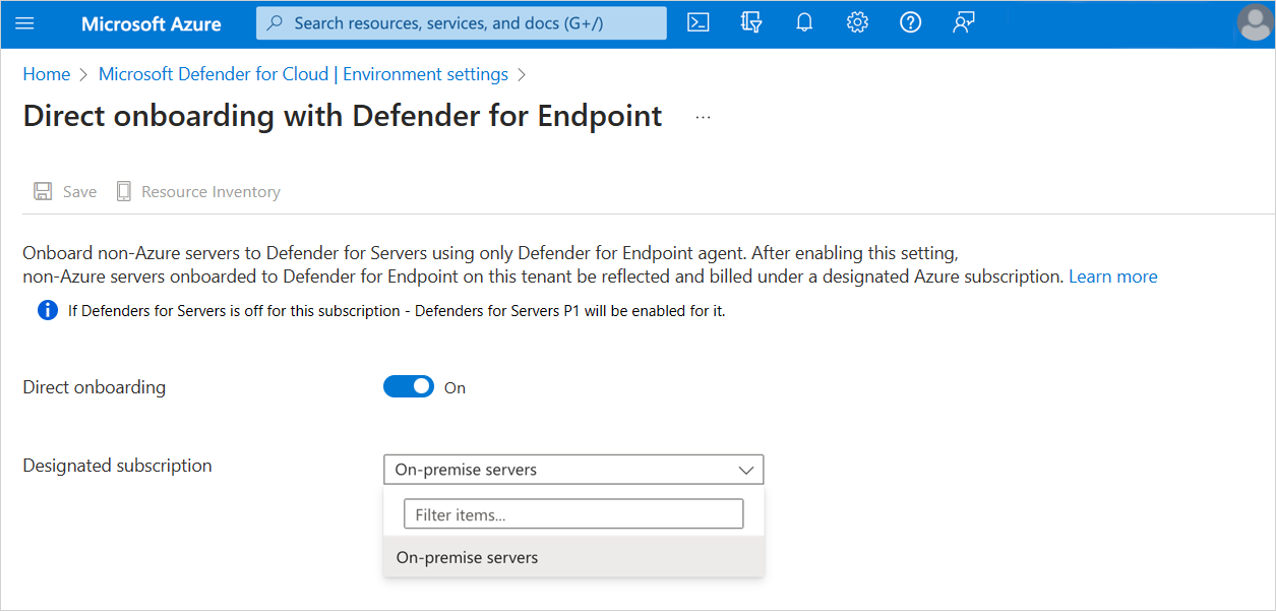
## Onboarding any non azure servers running on defender for endpoint to defender for cloud

This capability of onboarding of non azure server to defender for cloud which are currently running on defender for endpoint is known as **DIRECT ONBOARDING**.   
How does Direct Onboarding work?

Direct onboarding is a seamless integration between Dfender for endpoint and defender for cloud, that does not require extra software deployment on your server which we did while onboarding through local script.  
Once enabled, it also shows your non-Azure server devices onboarded to Defender for Endpoint in Defender for Cloud, under a designated Azure Subscription you configure.  Azure Subscription is used for licensing, billing, alerts, and security insights but doesn't provide server management capabilities such as Azure Policy, Extensions, or Guest configuration.

Can be recommended to à This onboarding path is ideal for customers with mixed and hybrid server estate who wish to consolidate server protection under Defender for Servers.

This direct onboarding is opt-in setting at the tenant level which means you should have Microsoft Entra Global Admin Role or Microsoft Entra Security Admin role to enable the direct onboarding.



**Enabling in the Defender for Cloud portal**

1. Go to **Defender for Cloud** > **Environment Settings** > **Direct onboarding**.
2. Switch the **Direct onboarding** toggle to **On**.
3. Select the subscription you would like to use for servers onboarded directly with Defender for Endpoint.
4. Select **Save**.

Shortly after you enable this setting, your server devices will show under the designated subscription. Alerts, software inventory, and vulnerability data are integrated with Defender for Cloud, in a similar way to how it works with Azure VMs.

Current Limitations

1. **Plan Support**

If you are onboarding the azure servers to the subscription which has defender for server plan 1 enabled then all the features of defender for server plan1 will be available to that server  but if the subscription has plan 2 enabled then the server will be able to get all the features of the plan1 as well as defender for vulnerability management with addon features.   
The limitations comes for the NON-AZURE servers such that those servers which don’t have any presence in azure environment will not able to access all the features of defender for server plan 2. But they will get the features of plan.   
Whether you enable the plan2 in your defender for cloud then too the servers will not get all the features of plan2, because some features require deployment of agents in the server  to access them.   
For that reason you can 1 thing is deploy those server through ARC but then deploying through will create a instance of that server which can get the services of the arc but it wont help in all the plan 2 features.   
So that’s the limitations.

1. **Multi-cloud Support**

So multi cloud is productive feature for defender for cloud as you can see different cloud environment servers and like AWS and GCP etc , but it becomes a limitation for defender for endpoint because if you do direct onboarding to defender for cloud then all the servers which were on endpoint portal will show in one single pane not in a segregated way like these servers are of AWS and these are of GCP.     
Here the user can do one thing is that while deploying that servers, name it respectively according to their cloud platform.

1. **Simultaneous Onboarding**

So here it simply says dont deploy server through multiple methods as it will lead to extra charge i.e. check once that if u have already onboarded servers before with other method if yes then rather delete it and then gain deploy otherwise the defender for cloud will consider it as 2 different servers and charge for both of them. Also it tries its best to keep them as one single server but sometimes it does not recognise because of the servers being deployed with older versions and charges for both as it considers both fo them as different.

However the servers having old versions of defender for endpoint will have some limitations like reduced protections(Older versions may lack the latest threat intelligence updates, vulnerability patches, or behavioural analysis capabilities), compatibility issues(Older versions may not be fully compatible with the latest operating systems, applications, or security standards, leading to compatibility issues and potential security gaps).

Please check the version of the agent for the given provided list of OS

|  |  |
| --- | --- |
| **Operating System** | **Minimum agent version** |
| Windows 2019 | 10.8555 |
| Windows 2012 R2, 2016 (modern, unified agent) | 10.8560 |
| Linux | 30.101.23052.009 |