Creating and Maintaining your Detonation Environment

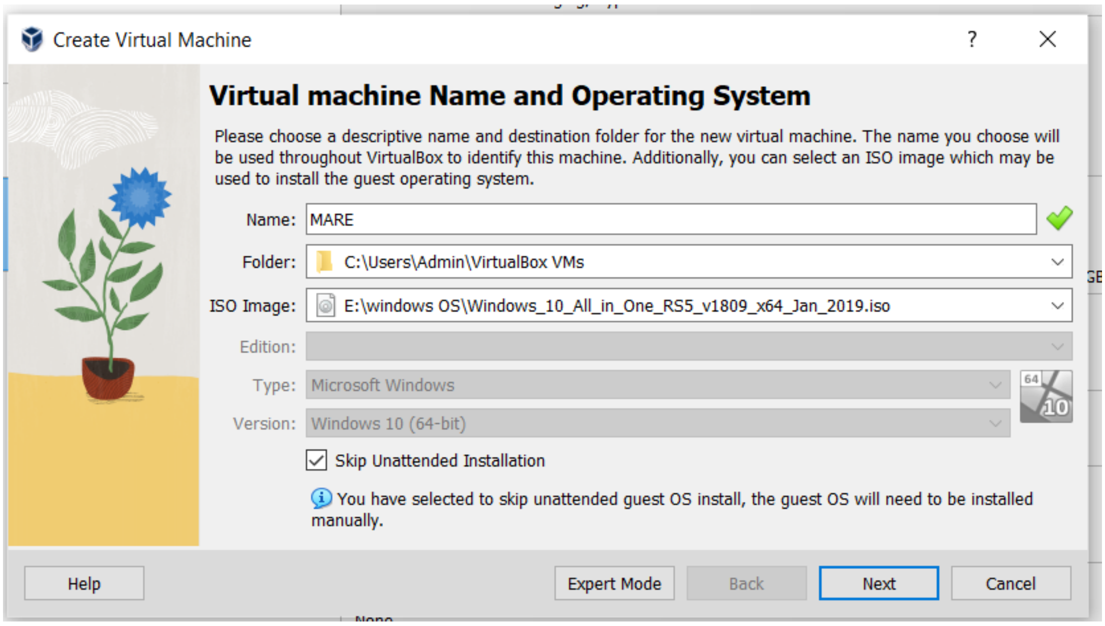
Technical requirements

The following are the requirements for this lab:

- A PC/Mac with at least 8 GB of memory and a quad-core processor
- An internet connection
- FLARE VM GitHub package: https://github.com/fireeye/flare-vm
- The latest VirtualBox installer: https://virtualbox.org/wiki/downloads
- A Windows 10 ISO and product key

Text book : Malware Analysis Techniques Tricks for the triage of adversarial software Dylan Barker, 2021

Setting up VirtualBox with Windows 10



Create Virtual Machine

Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: MARE

Folder: C:\Users\Admin\VirtualBox VMs

ISO Image: E:\windows OS\Windows_10_All_in_One_RS5_v1809_x64_Jan_2019.iso

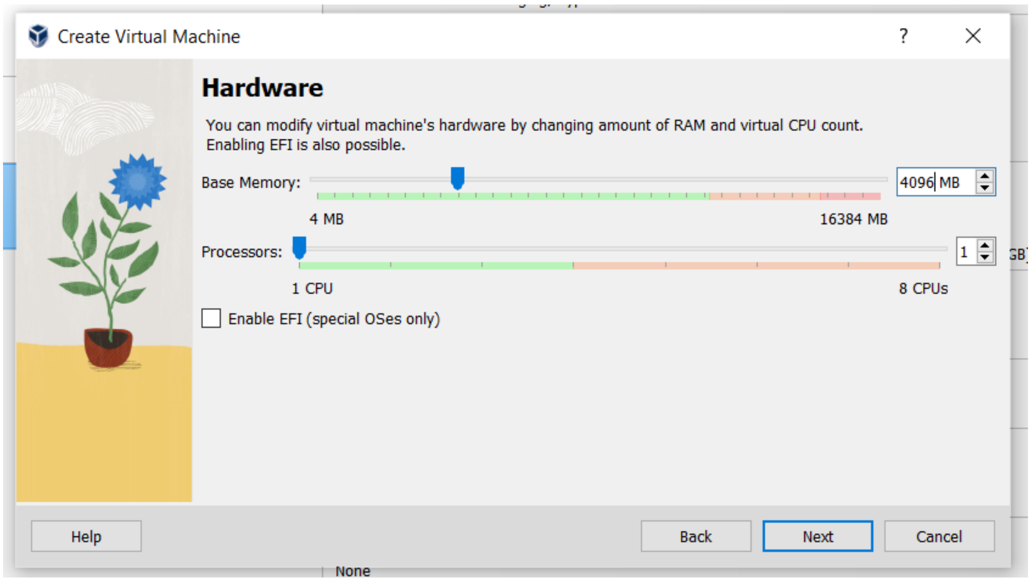
Edition:

Type: Microsoft Windows

Version: Windows 10 (64-bit)

☑ Skip Unattended Installation

You have selected to skip unattended guest OS install, the guest OS will need to be installed manually.



Create Virtual Machine

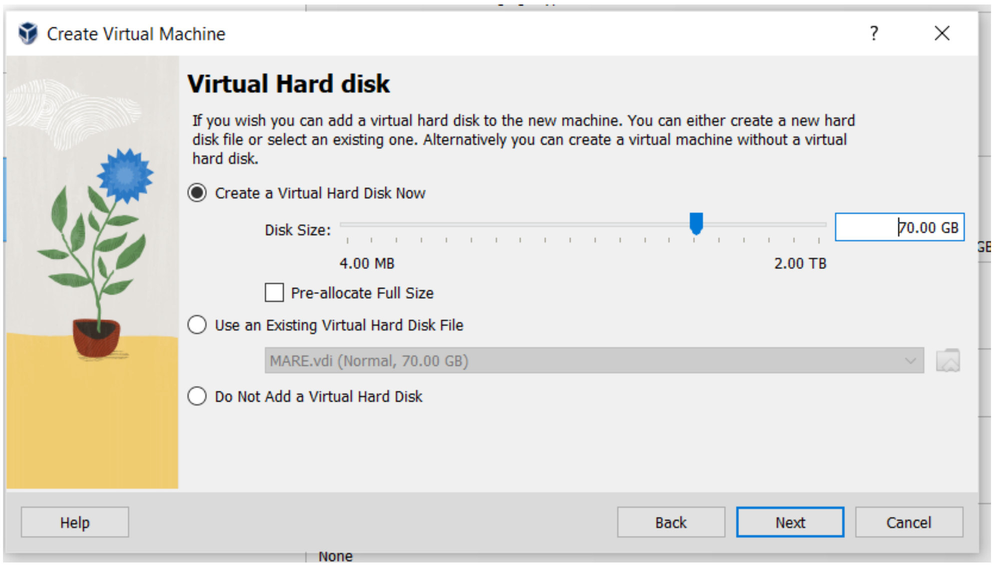
Hardware

You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 4096 MB

Processors: 1

☐ Enable EFI (special OSes only)



Create Virtual Machine

Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

● Create a Virtual Hard Disk Now

Disk Size: 70.00 GB

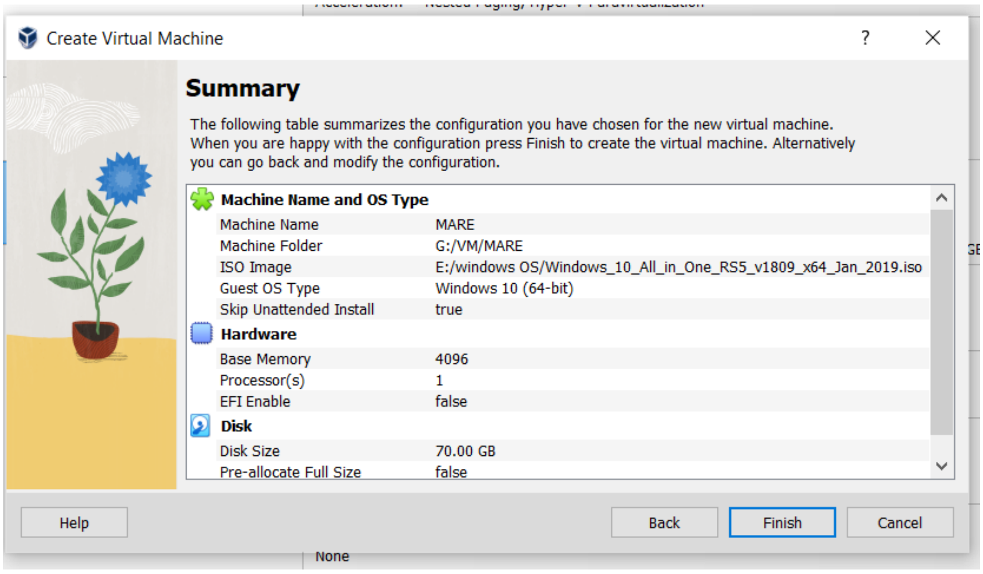
4.00 MB 2.00 TB

□ Pre-allocate Full Size

○ Use an Existing Virtual Hard Disk File

MARE.vdi (Normal, 70.00 GB)

○ Do Not Add a Virtual Hard Disk



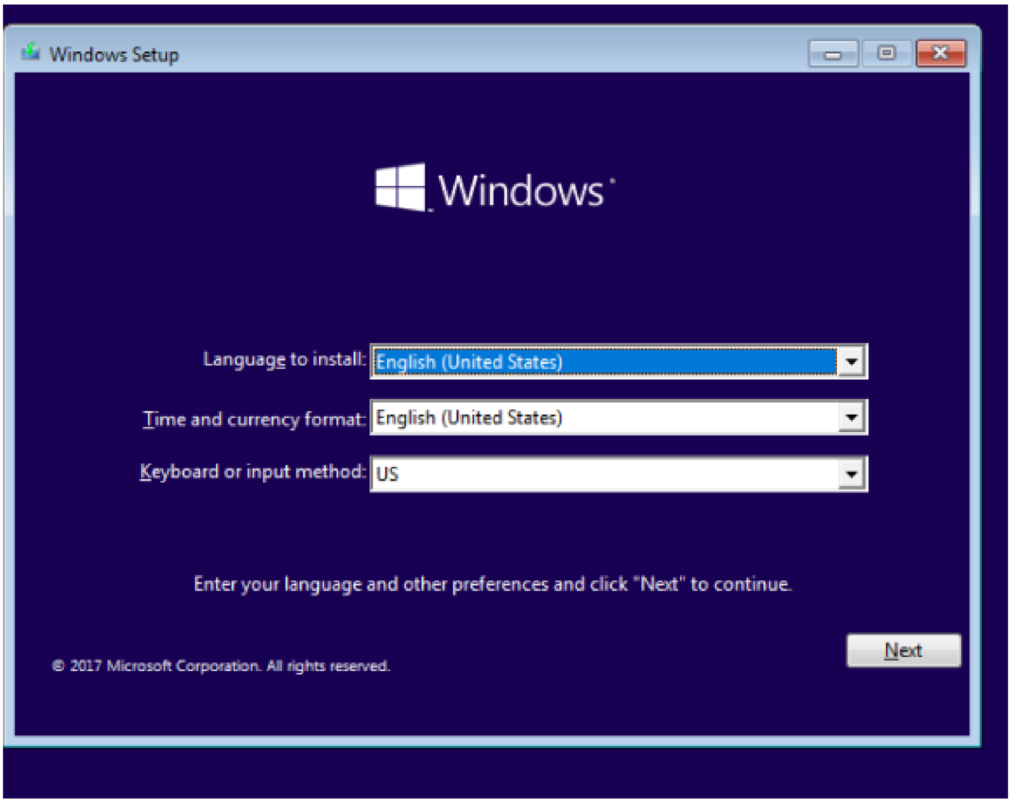
Create Virtual Machine

Summary

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

Machine Name and OS Type	
Machine Name	MARE
Machine Folder	G:/VM/MARE
ISO Image	E:/windows OS/Windows_10_All_in_One_RS5_v1809_x64_Jan_2019.iso
Guest OS Type	Windows 10 (64-bit)
Skip Unattended Install	true
Hardware	
Base Memory	4096
Processor(s)	1
EFI Enable	false
Disk	
Disk Size	70.00 GB
Pre-allocate Full Size	false

Windows 10 installation



Windows Setup

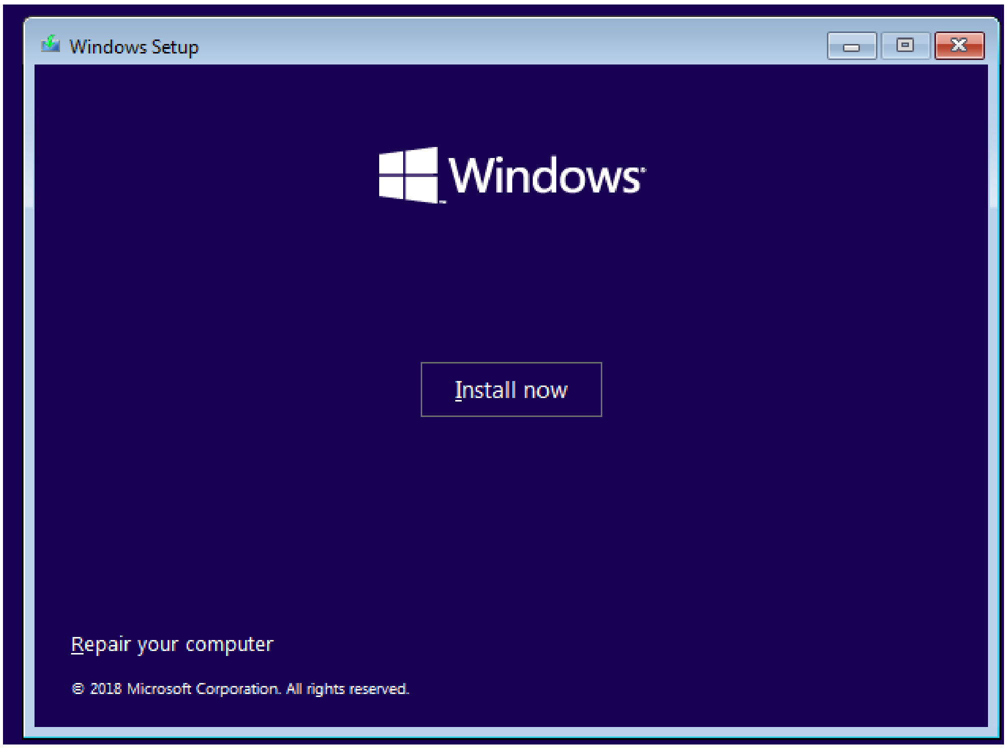
Language to install: English (United States)

Time and currency format: English (United States)

Keyboard or input method: US

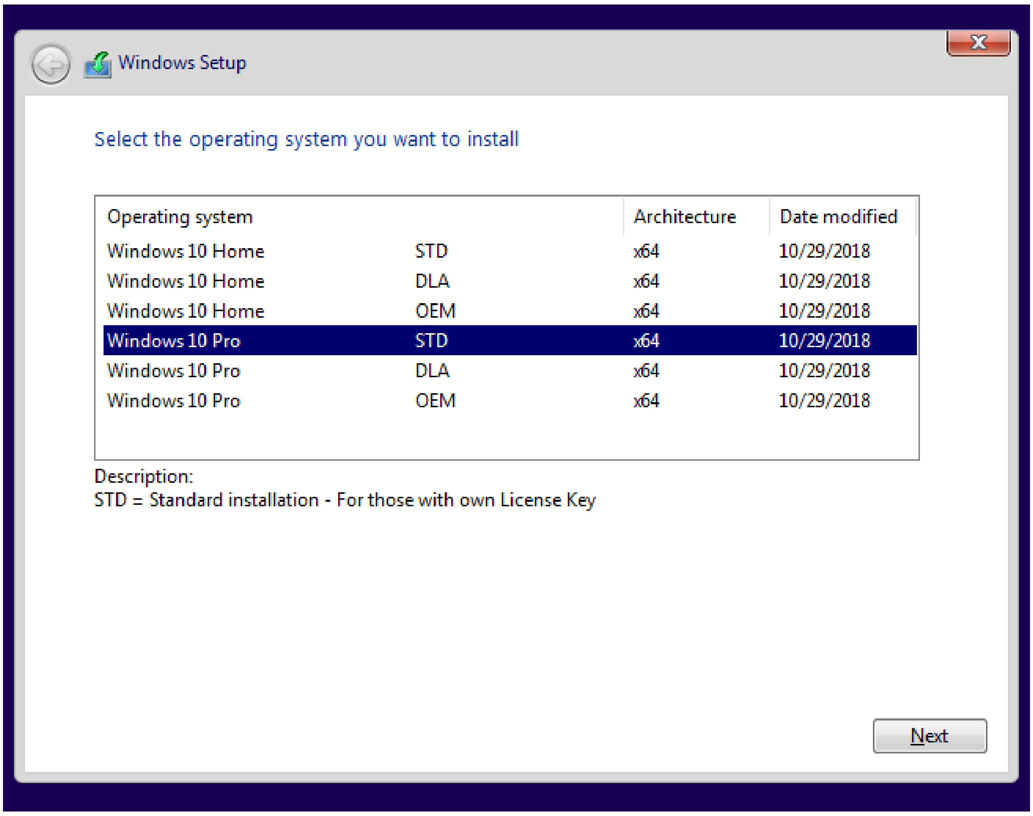
Enter your language and other preferences and click "Next" to continue.

© 2017 Microsoft Corporation. All rights reserved.



Windows Setup

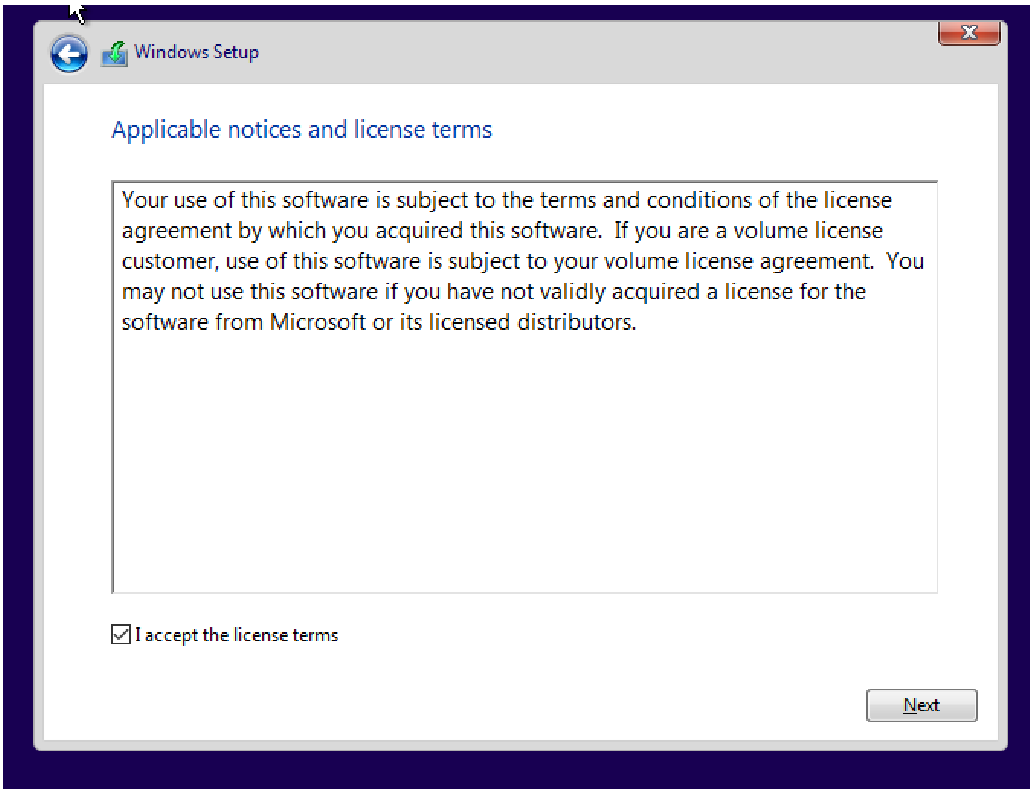
© 2018 Microsoft Corporation. All rights reserved.



Select the operating system you want to install

Operating system		Architecture	Date modified
Windows 10 Home	STD	x64	10/29/2018
Windows 10 Home	DLA	x64	10/29/2018
Windows 10 Home	OEM	x64	10/29/2018
Windows 10 Pro	STD	x64	10/29/2018
Windows 10 Pro	DLA	x64	10/29/2018
Windows 10 Pro	OEM	x64	10/29/2018

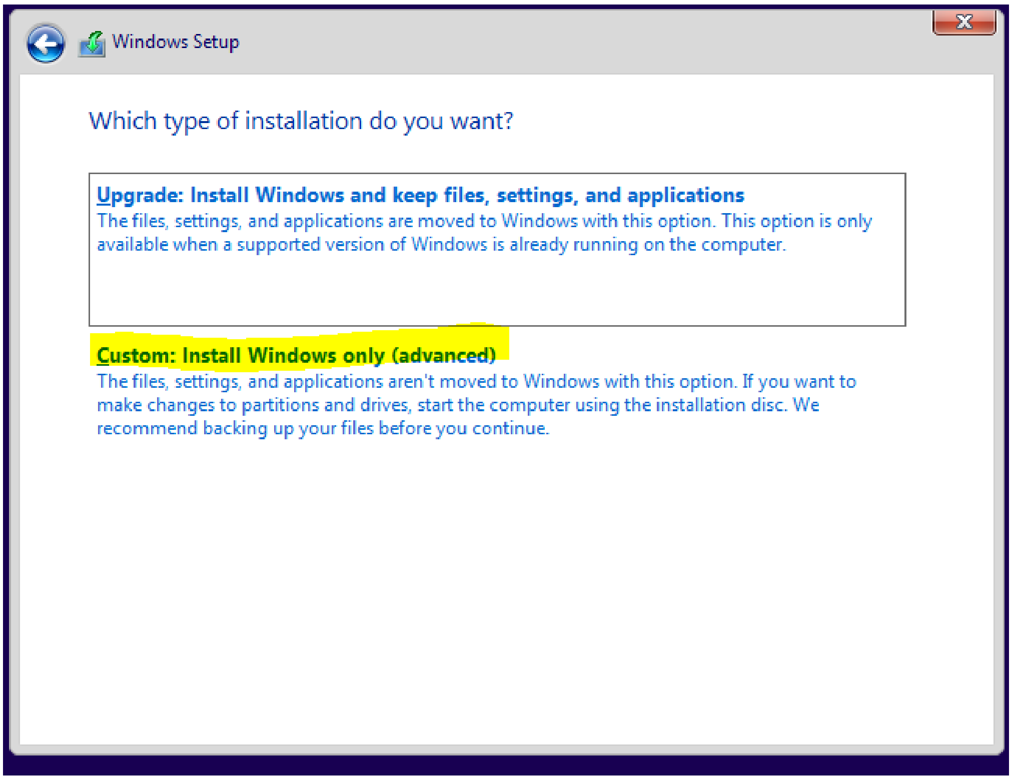
Description:
STD = Standard installation - For those with own License Key



Applicable notices and license terms

Your use of this software is subject to the terms and conditions of the license agreement by which you acquired this software. If you are a volume license customer, use of this software is subject to your volume license agreement. You may not use this software if you have not validly acquired a license for the software from Microsoft or its licensed distributors.

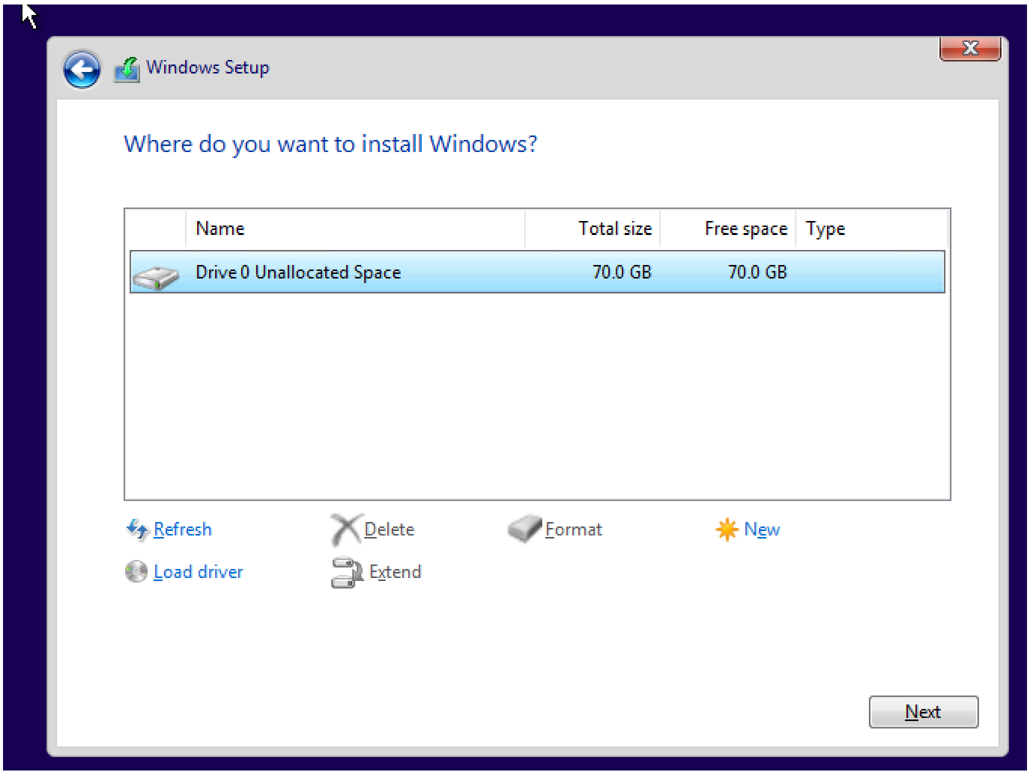
☑ I accept the license terms



Which type of installation do you want?

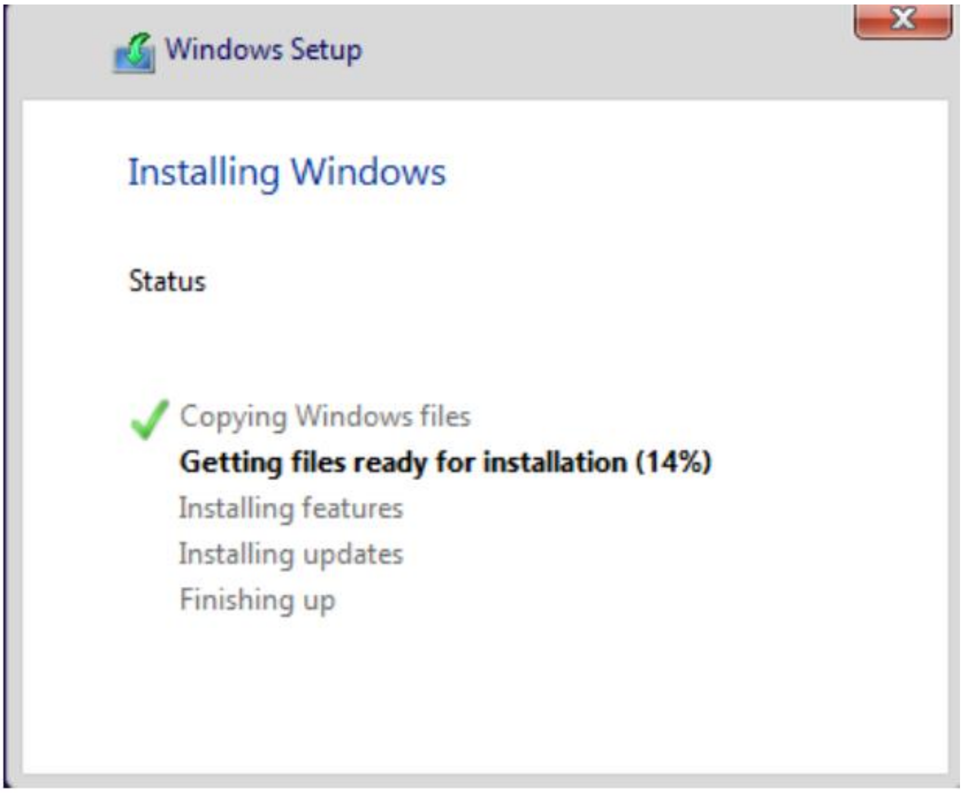
Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.



Where do you want to install Windows?

Name	Total size	Free space	Type
Drive 0 Unallocated Space	70.0 GB	70.0 GB	



Windows Setup

Installing Windows

Status

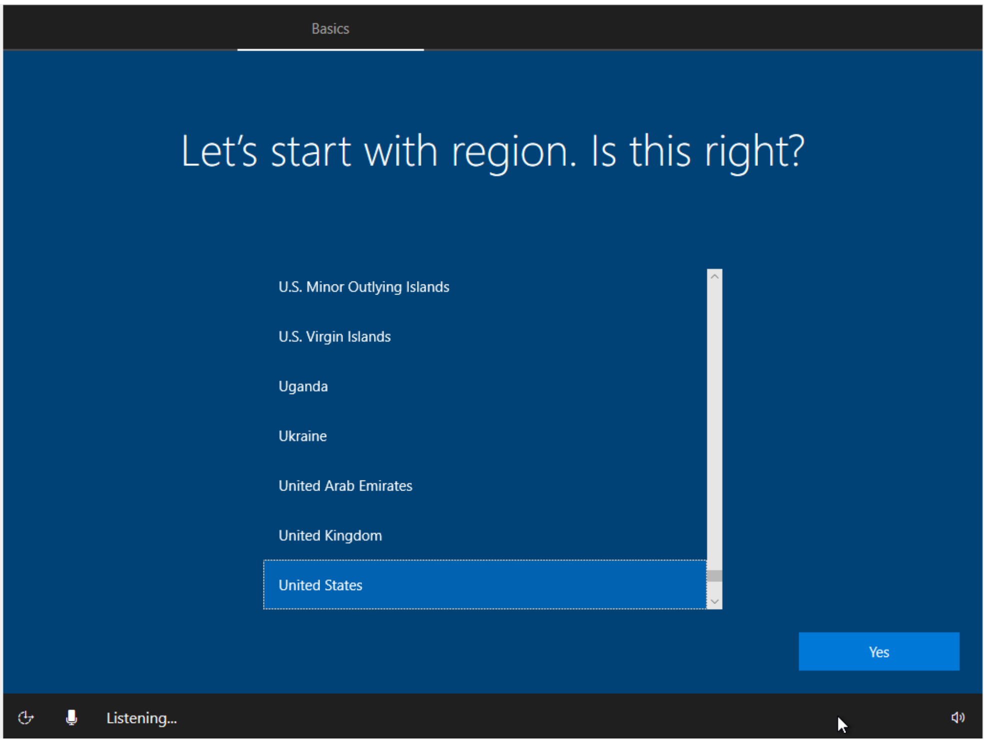
✓ Copying Windows files

Getting files ready for installation (14%)

Installing features

Installing updates

Finishing up



Basics

Let's start with region. Is this right?

U.S. Minor Outlying Islands

U.S. Virgin Islands

Uganda

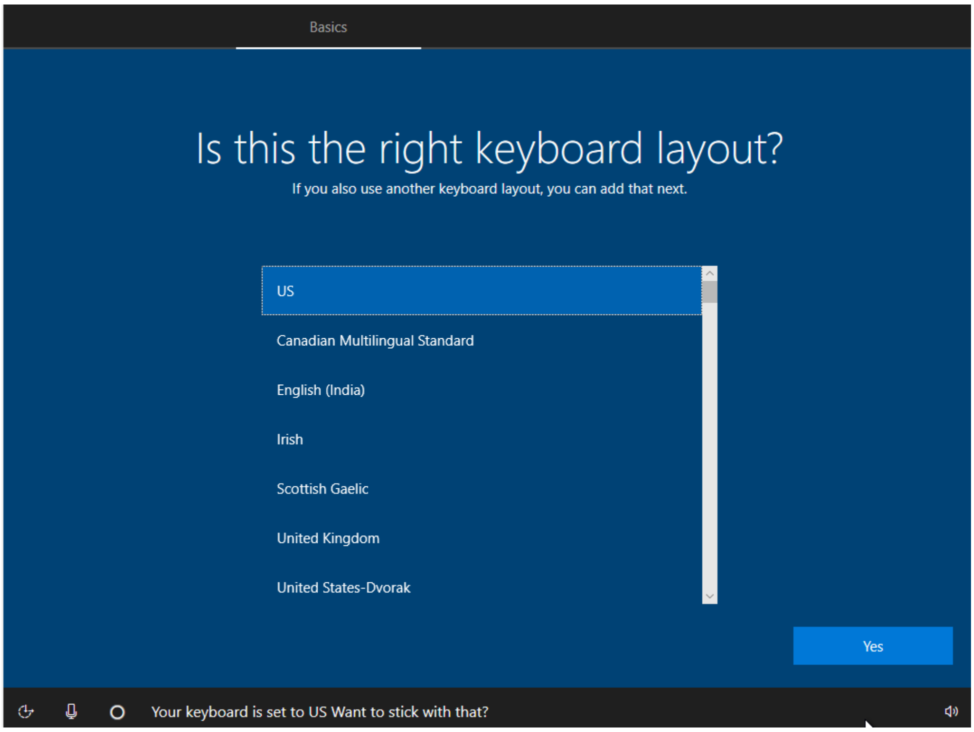
Ukraine

United Arab Emirates

United Kingdom

United States

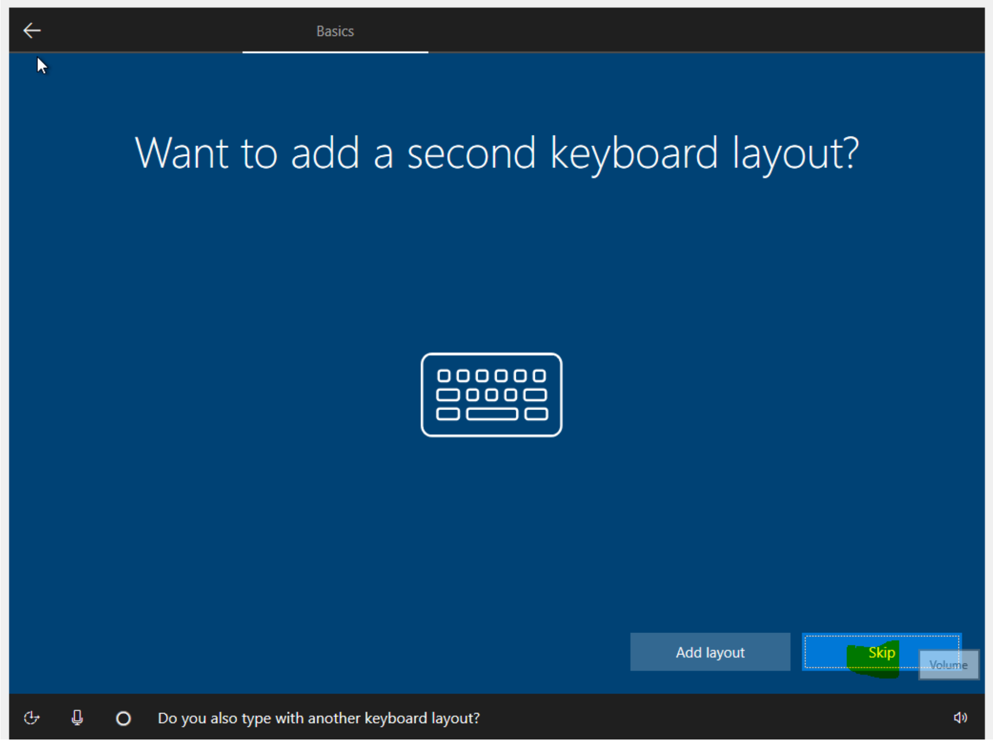
Listening...



Is this the right keyboard layout?

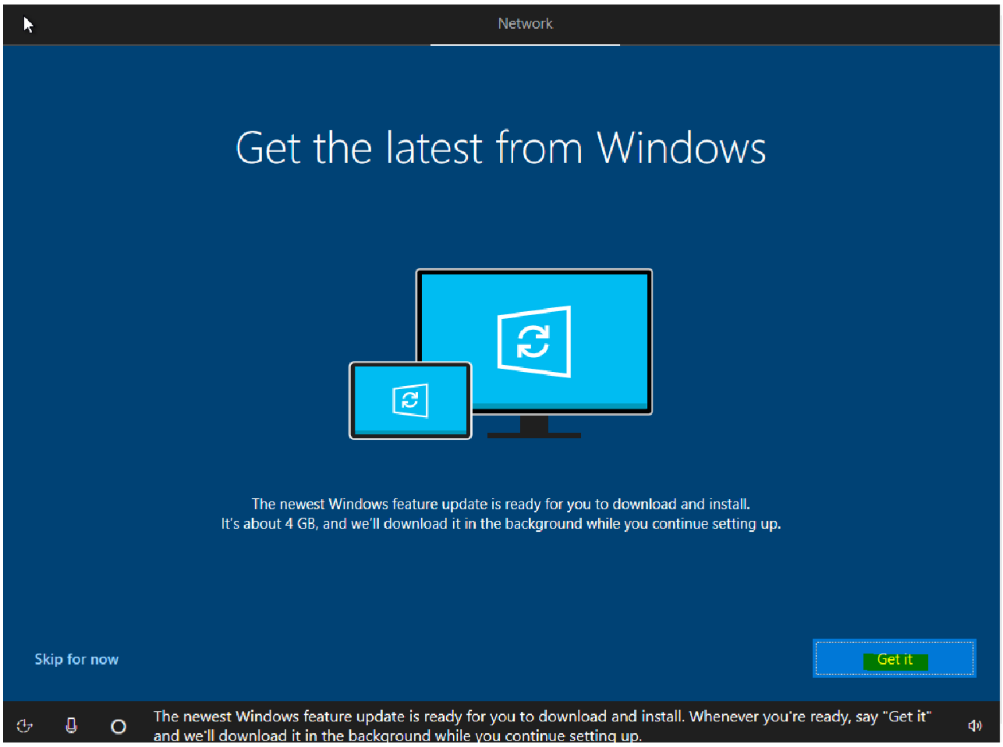
If you also use another keyboard layout, you can add that next.

Your keyboard is set to US Want to stick with that?



Want to add a second keyboard layout?

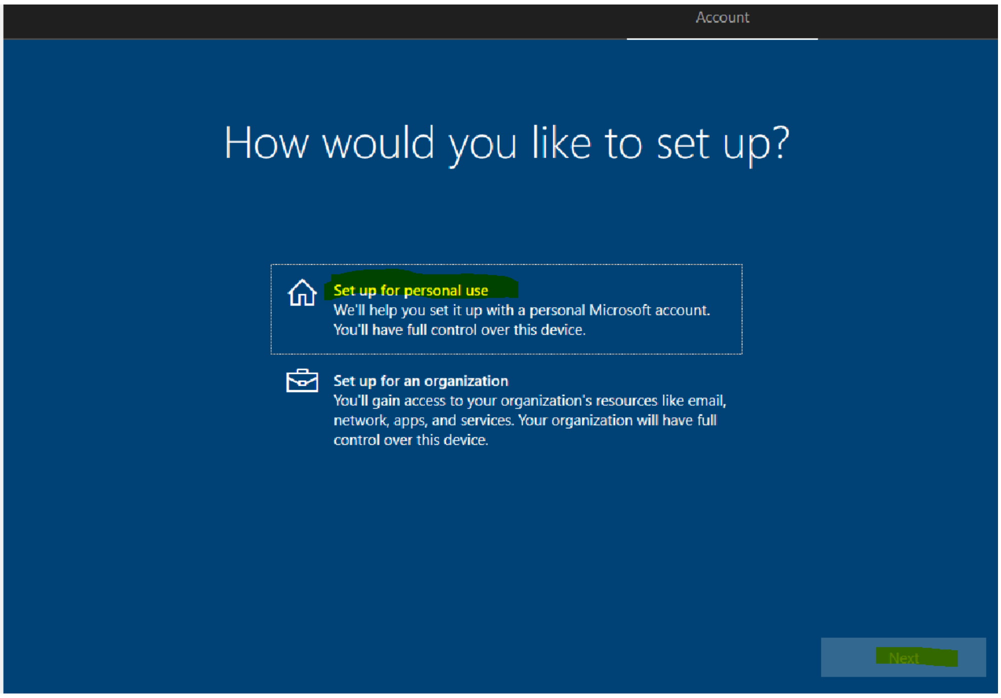
Do you also type with another keyboard layout?



Get the latest from Windows

The newest Windows feature update is ready for you to download and install.
It's about 4 GB, and we'll download it in the background while you continue setting up.

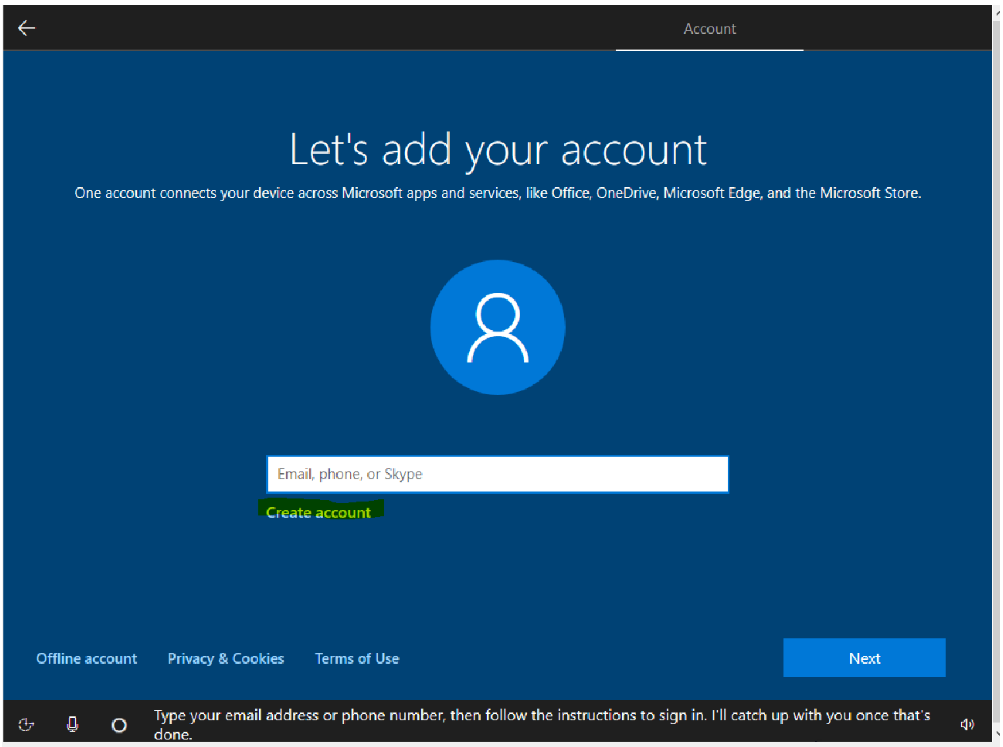
The newest Windows feature update is ready for you to download and install. Whenever you're ready, say "Get it" and we'll download it in the background while you continue setting up.



How would you like to set up?

Set up for personal use
We'll help you set it up with a personal Microsoft account. You'll have full control over this device.

Set up for an organization
You'll gain access to your organization's resources like email, network, apps, and services. Your organization will have full control over this device.

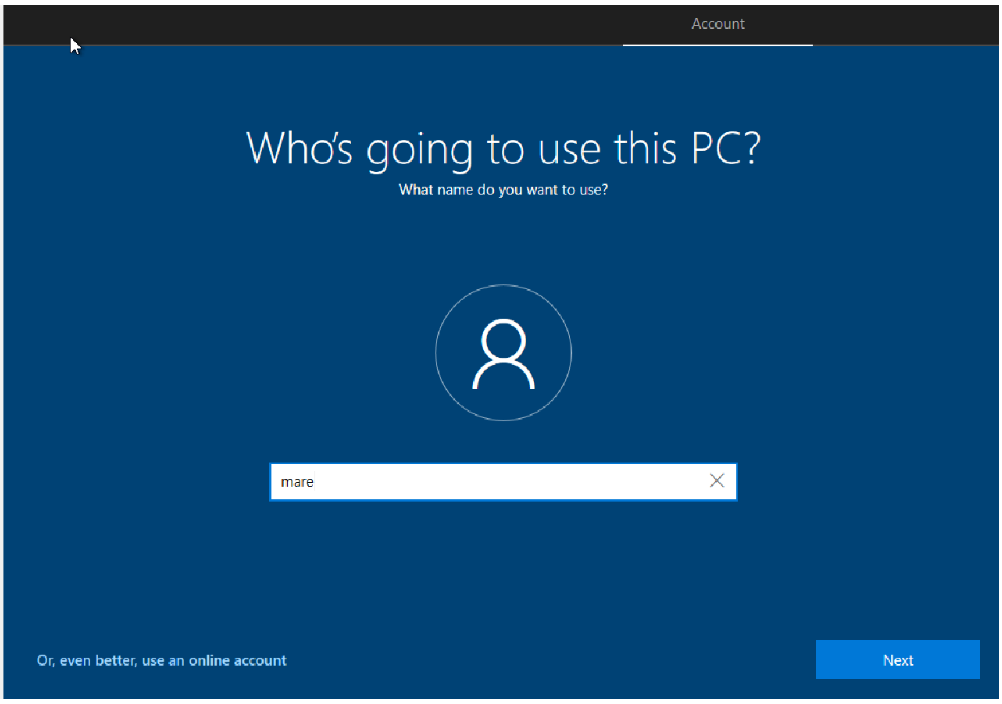


Let's add your account

One account connects your device across Microsoft apps and services, like Office, OneDrive, Microsoft Edge, and the Microsoft Store.

Type your email address or phone number, then follow the instructions to sign in. I'll catch up with you once that's done.

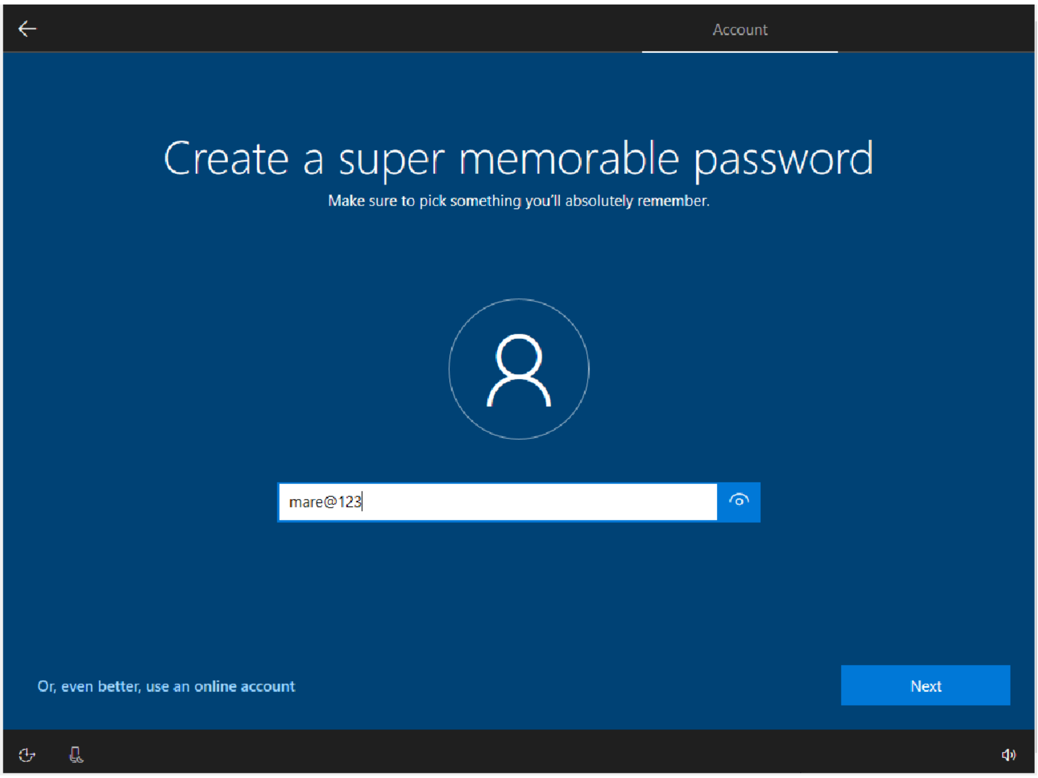
User name and password as per your choice



Who's going to use this PC?

What name do you want to use?

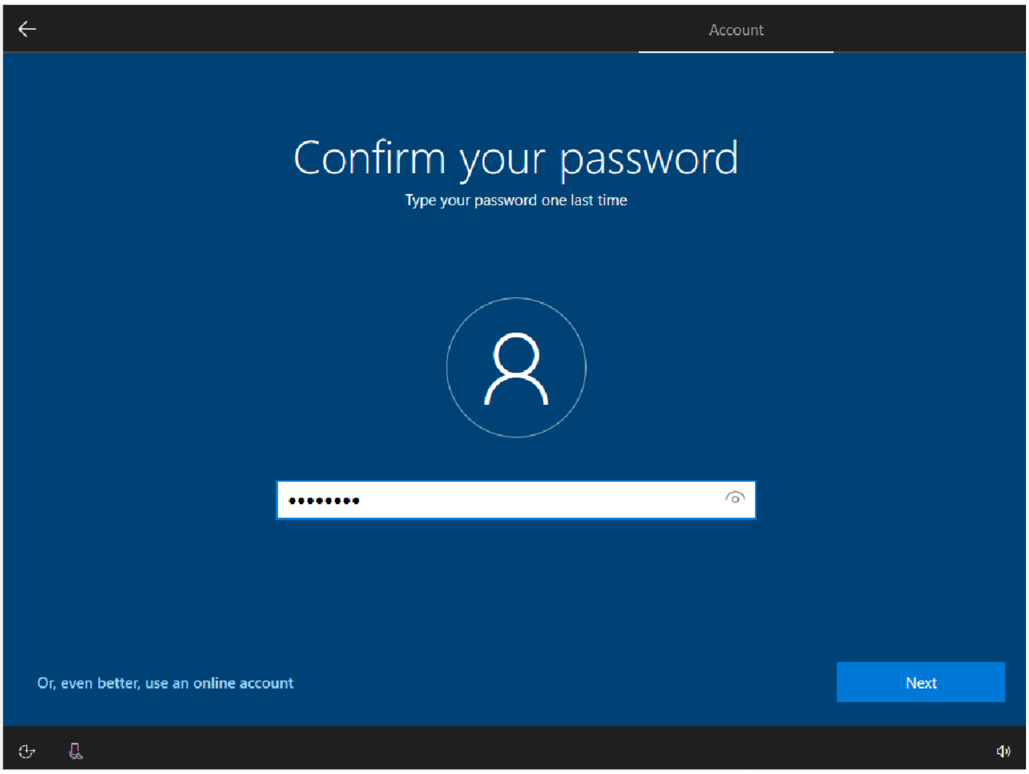
mare



Create a super memorable password

Make sure to pick something you'll absolutely remember.

mare@123

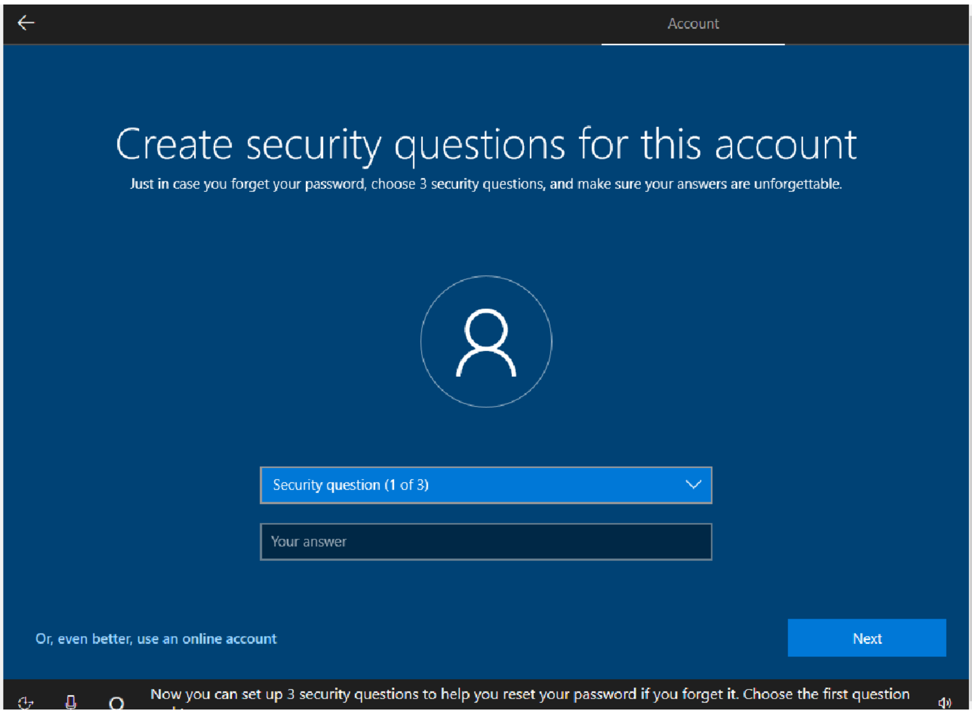


Confirm your password

Type your password one last time

••••••••

Question and answer as per your choice

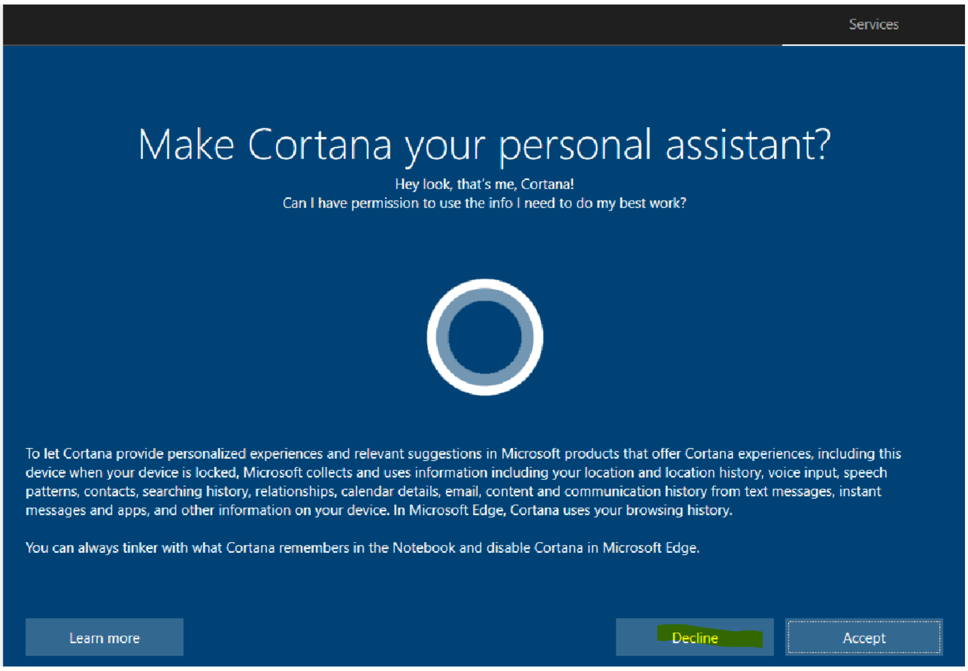


Account
Security question (1 of 3)
Your answer
Or, even better, use an online account
Next

Create security questions for this account

Just in case you forget your password, choose 3 security questions, and make sure your answers are unforgettable.

Now you can set up 3 security questions to help you reset your password if you forget it. Choose the first question

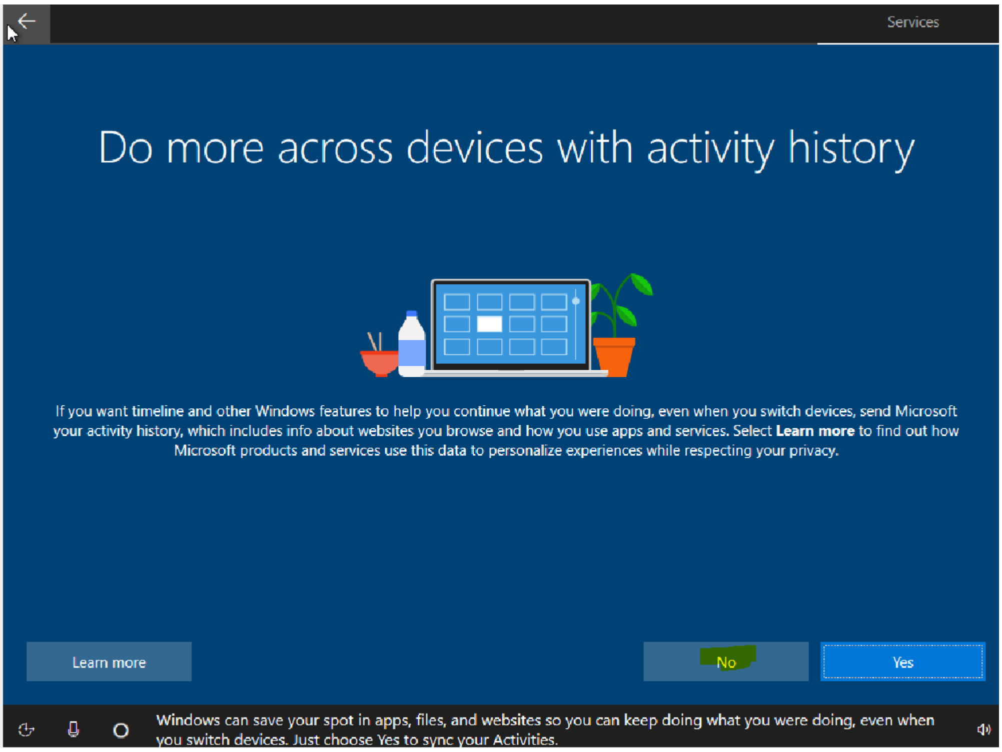


Make Cortana your personal assistant?

Hey look, that's me, Cortana!
Can I have permission to use the info I need to do my best work?

To let Cortana provide personalized experiences and relevant suggestions in Microsoft products that offer Cortana experiences, including this device when your device is locked, Microsoft collects and uses information including your location and location history, voice input, speech patterns, contacts, searching history, relationships, calendar details, email, content and communication history from text messages, instant messages and apps, and other information on your device. In Microsoft Edge, Cortana uses your browsing history.

You can always tinker with what Cortana remembers in the Notebook and disable Cortana in Microsoft Edge.

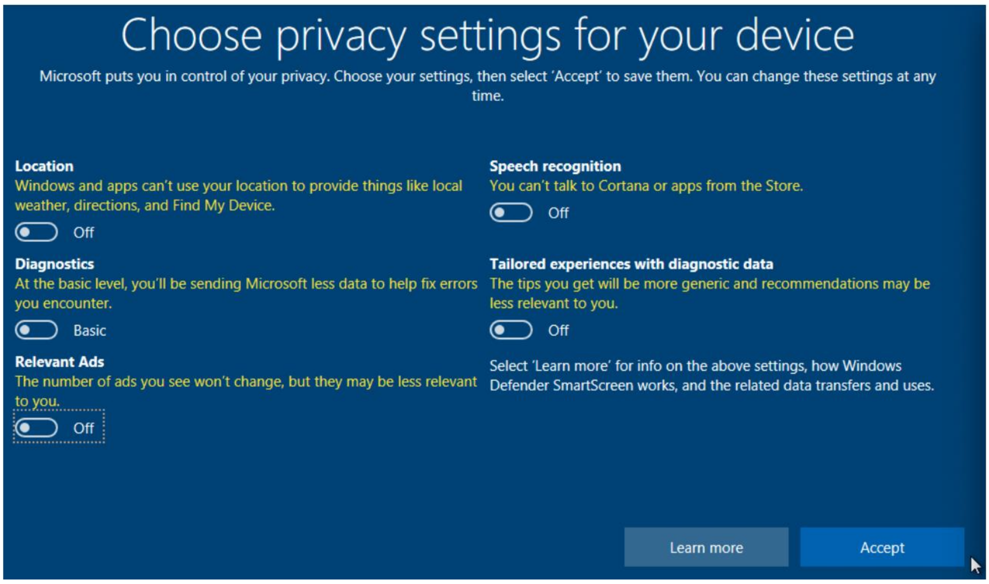


Do more across devices with activity history

If you want timeline and other Windows features to help you continue what you were doing, even when you switch devices, send Microsoft your activity history, which includes info about websites you browse and how you use apps and services. Select **Learn more** to find out how Microsoft products and services use this data to personalize experiences while respecting your privacy.

[✓ No]

Windows can save your spot in apps, files, and websites so you can keep doing what you were doing, even when you switch devices. Just choose Yes to sync your Activities.



Choose privacy settings for your device

Microsoft puts you in control of your privacy. Choose your settings, then select 'Accept' to save them. You can change these settings at any time.

Location
Windows and apps can't use your location to provide things like local weather, directions, and Find My Device.
Off

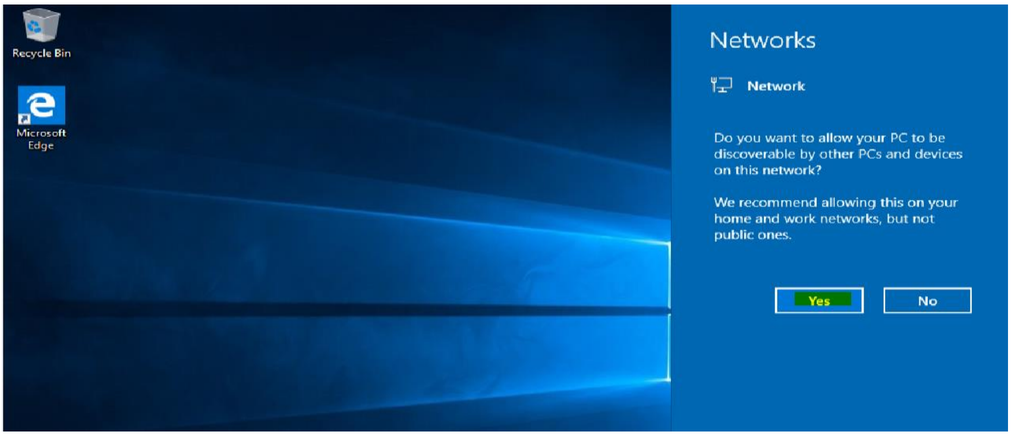
Diagnostics
At the basic level, you'll be sending Microsoft less data to help fix errors you encounter.
Basic

Relevant Ads
The number of ads you see won't change, but they may be less relevant to you.
Off

Speech recognition
You can't talk to Cortana or apps from the Store.
Off

Tailored experiences with diagnostic data
The tips you get will be more generic and recommendations may be less relevant to you.
Off

Select 'Learn more' for info on the above settings, how Windows Defender SmartScreen works, and the related data transfers and uses.



Networks

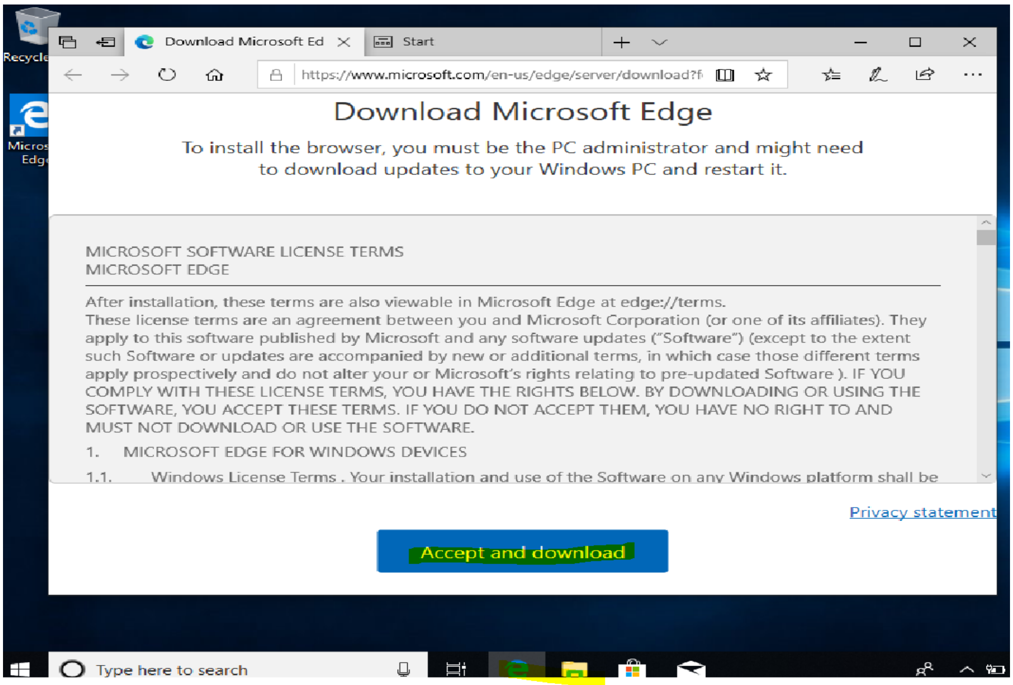
Network

Do you want to allow your PC to be discoverable by other PCs and devices on this network?

We recommend allowing this on your home and work networks, but not public ones.

[✓ Yes] No

Launch the browser install Microsoft edge



Download Microsoft Edge

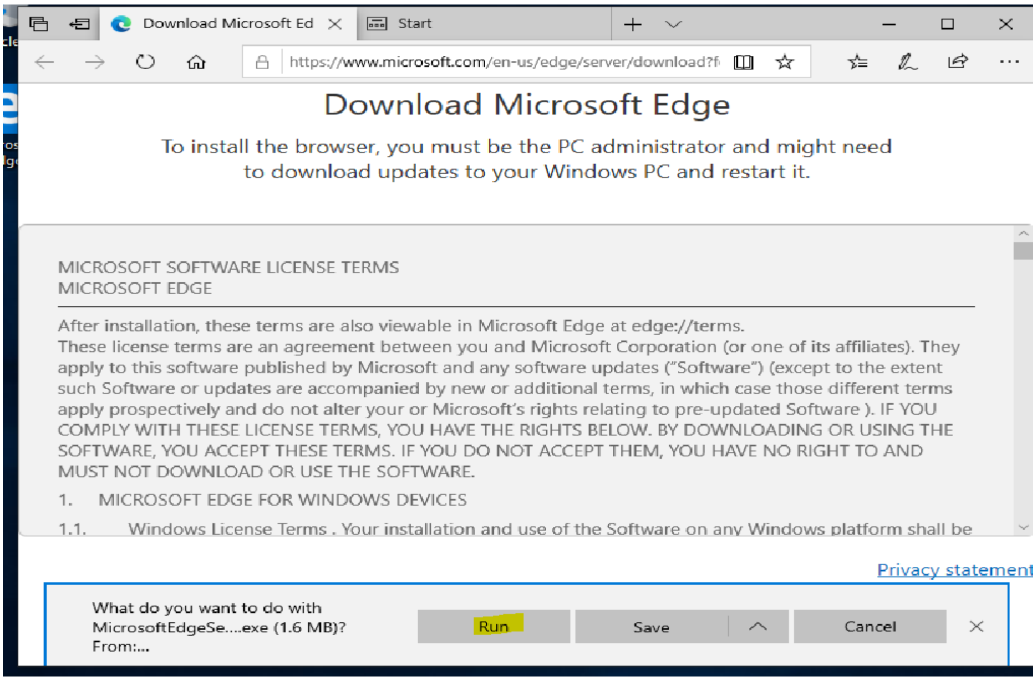
To install the browser, you must be the PC administrator and might need to download updates to your Windows PC and restart it.

MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT EDGE

After installation, these terms are also viewable in Microsoft Edge at edge://terms.
These license terms are an agreement between you and Microsoft Corporation (or one of its affiliates). They apply to this software published by Microsoft and any software updates ("Software") (except to the extent such Software or updates are accompanied by new or additional terms, in which case those different terms apply prospectively and do not alter your or Microsoft's rights relating to pre-updated Software). IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE RIGHTS BELOW. BY DOWNLOADING OR USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, YOU HAVE NO RIGHT TO AND MUST NOT DOWNLOAD OR USE THE SOFTWARE.

1. MICROSOFT EDGE FOR WINDOWS DEVICES

1.1. Windows License Terms . Your installation and use of the Software on any Windows platform shall be



Download Microsoft Edge

To install the browser, you must be the PC administrator and might need to download updates to your Windows PC and restart it.

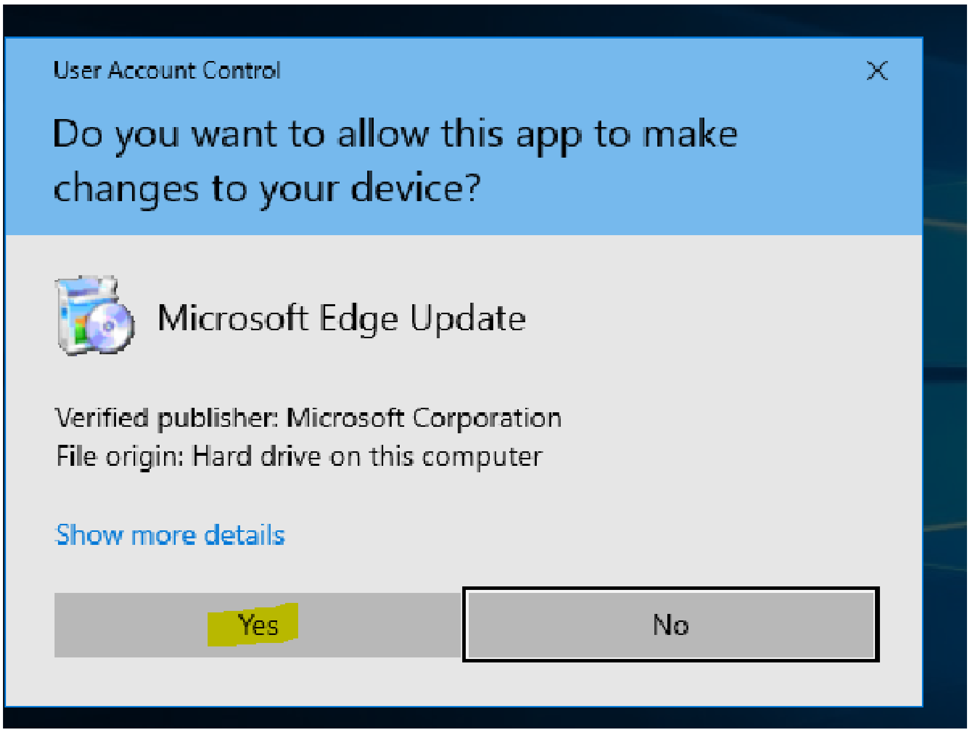
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT EDGE

After installation, these terms are also viewable in Microsoft Edge at edge://terms.
These license terms are an agreement between you and Microsoft Corporation (or one of its affiliates). They apply to this software published by Microsoft and any software updates ("Software") (except to the extent such Software or updates are accompanied by new or additional terms, in which case those different terms apply prospectively and do not alter your or Microsoft's rights relating to pre-updated Software). IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE RIGHTS BELOW. BY DOWNLOADING OR USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, YOU HAVE NO RIGHT TO AND MUST NOT DOWNLOAD OR USE THE SOFTWARE.

1. MICROSOFT EDGE FOR WINDOWS DEVICES

1.1. Windows License Terms . Your installation and use of the Software on any Windows platform shall be

What do you want to do with MicrosoftEdgeSe....exe (1.6 MB)?
From:...

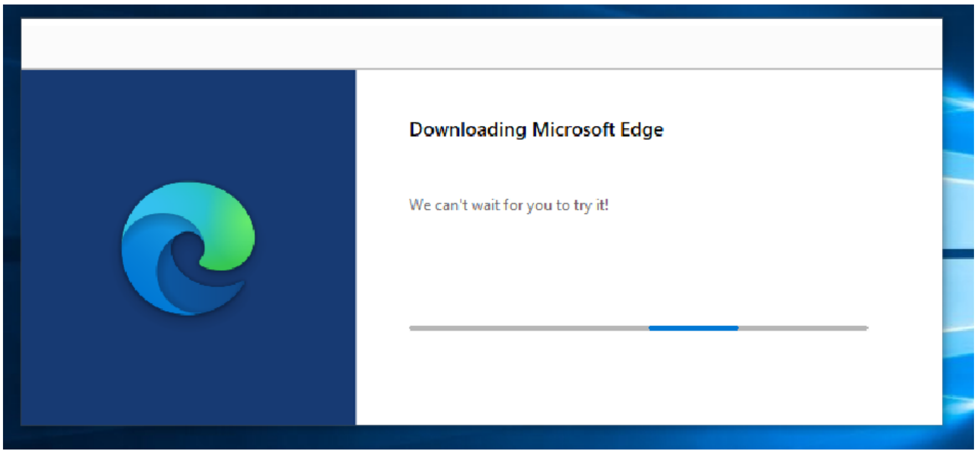


User Account Control

Do you want to allow this app to make changes to your device?

Microsoft Edge Update

Verified publisher: Microsoft Corporation
File origin: Hard drive on this computer

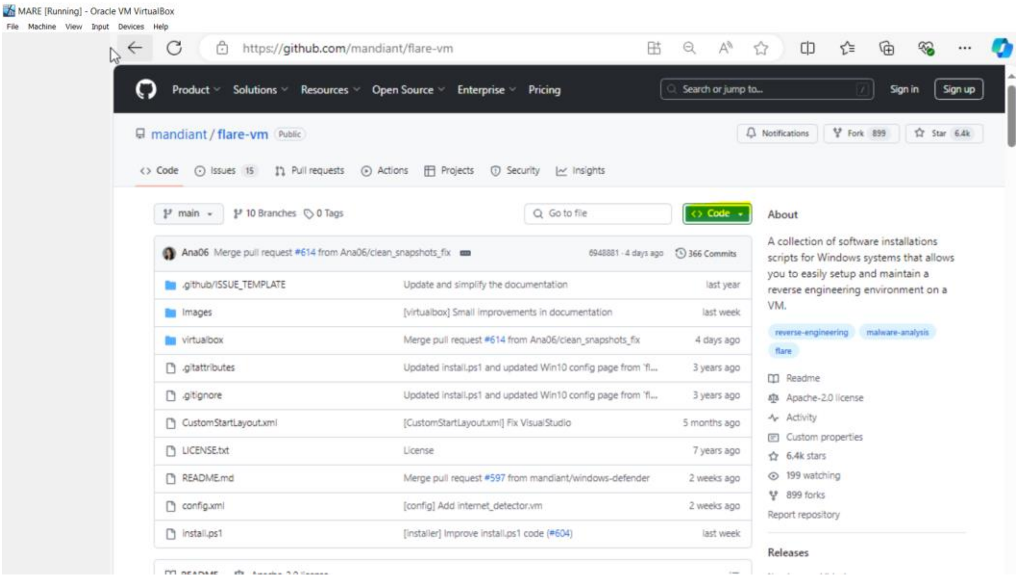


Downloading Microsoft Edge

We can't wait for you to try it!

Download the FLARE VM package

FLARE VM, a PowerShell script that can automatically download and install nearly every tool a malware analyst would need. The script is publicly available on GitHub at the following address: https://github.com/fireeye/flare-vm



MARE [Running] - Oracle VM VirtualBox

https://github.com/mandiant/flare-vm

mandiant / flare-vm Public

main · 10 Branches · 0 Tags · Code

Ana06 Merge pull request #614 from Ana06/clean_snapshots_fix · 6948881 · 4 days ago · 366 Commits

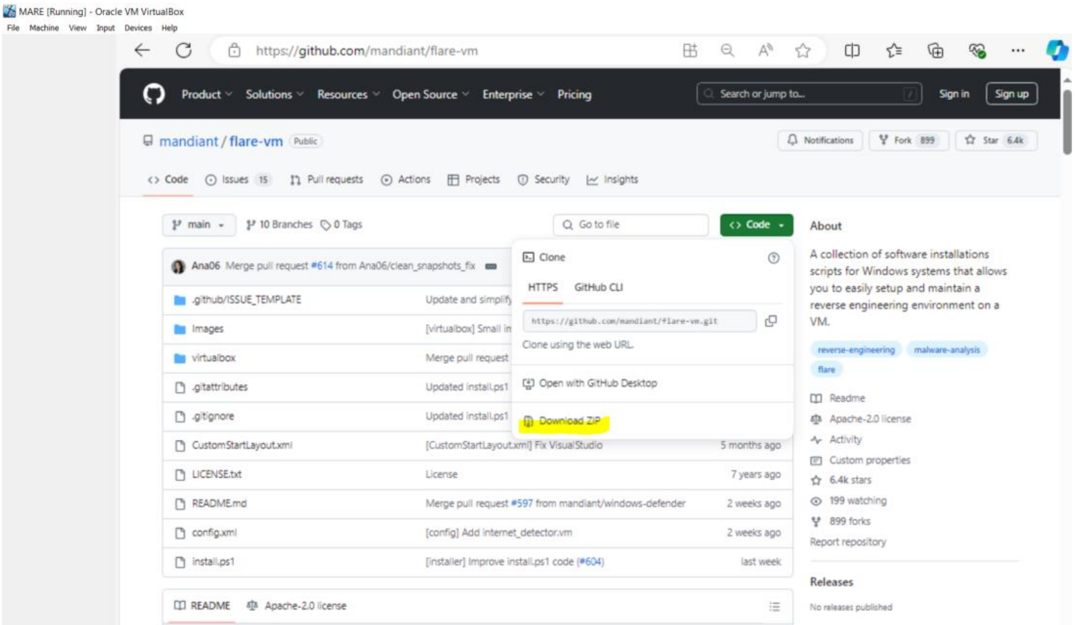
.github/ISSUE_TEMPLATE	Update and simplify the documentation	last year
Images	[virtualbox] Small improvements in documentation	last week
virtualbox	Merge pull request #614 from Ana06/clean_snapshots_fix	4 days ago
.gitattributes	Updated install.ps1 and updated Win10 config page from 'fl...	3 years ago
.gitignore	Updated install.ps1 and updated Win10 config page from 'fl...	3 years ago
CustomStartLayout.xml	[CustomStartLayout.xml] Fix VisualStudio	5 months ago
LICENSE.txt	License	7 years ago
README.md	Merge pull request #597 from mandiant/windows-defender	2 weeks ago
config.xml	[config] Add internet_detector.vm	2 weeks ago
install.ps1	[installer] Improve install.ps1 code (#604)	last week

About

A collection of software installations scripts for Windows systems that allows you to easily setup and maintain a reverse engineering environment on a VM.

reverse-engineering · malware-analysis · flare

Readme · Apache-2.0 license · Activity · Custom properties · 6.4k stars · 199 watching · 899 forks



MARE [Running] - Oracle VM VirtualBox

https://github.com/mandiant/flare-vm

mandiant / flare-vm Public

main · 10 Branches · 0 Tags · Code

Clone

HTTPS · GitHub CLI

https://github.com/mandiant/flare-vm.git

Clone using the web URL.

Open with GitHub Desktop

Download ZIP

Ana06 Merge pull request #614 from Ana06/clean_snapshots_fix

.github/ISSUE_TEMPLATE	Update and simplify	
Images	[virtualbox] Small im	
virtualbox	Merge pull request	
.gitattributes	Updated install.ps1	
.gitignore	Updated install.ps1	
CustomStartLayout.xml	[CustomStartLayout.xml] Fix VisualStudio	5 months ago
LICENSE.txt	License	7 years ago
README.md	Merge pull request #597 from mandiant/windows-defender	2 weeks ago
config.xml	[config] Add internet_detector.vm	2 weeks ago
install.ps1	[installer] Improve install.ps1 code (#604)	last week

About

A collection of software installations scripts for Windows systems that allows you to easily setup and maintain a reverse engineering environment on a VM.

reverse-engineering · malware-analysis · flare

Readme · Apache-2.0 license · Activity · Custom properties · 6.4k stars · 199 watching · 899 forks

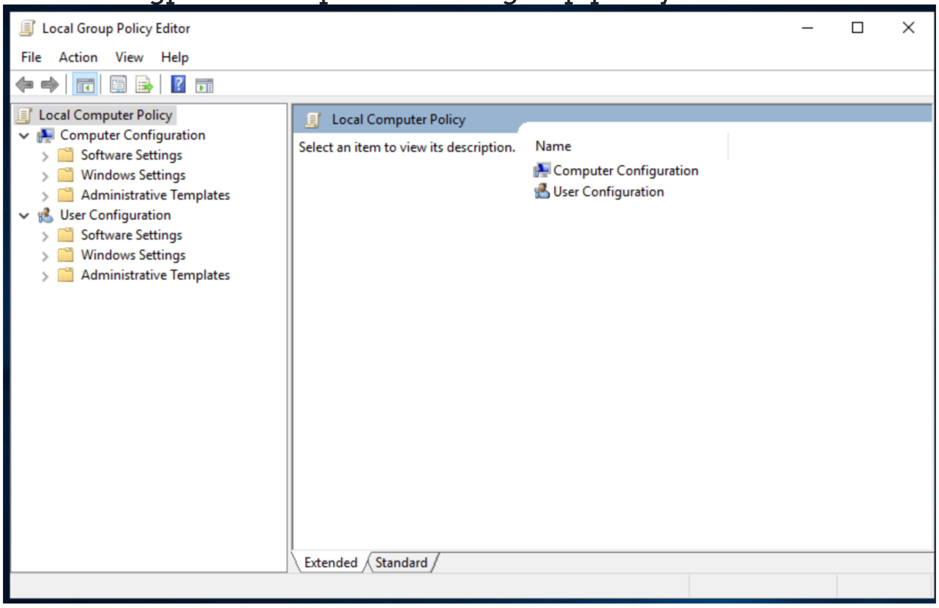
Releases

No releases published

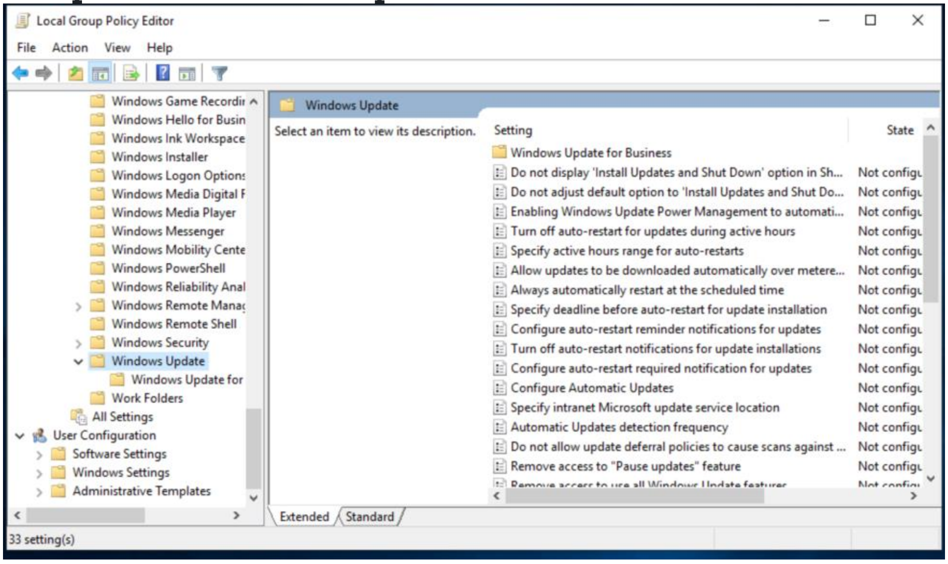
Prerequisite settings

- **Disable Windows Updates (at least until installation is finished)**

➢ Search for gpedit and open the local group policy editor

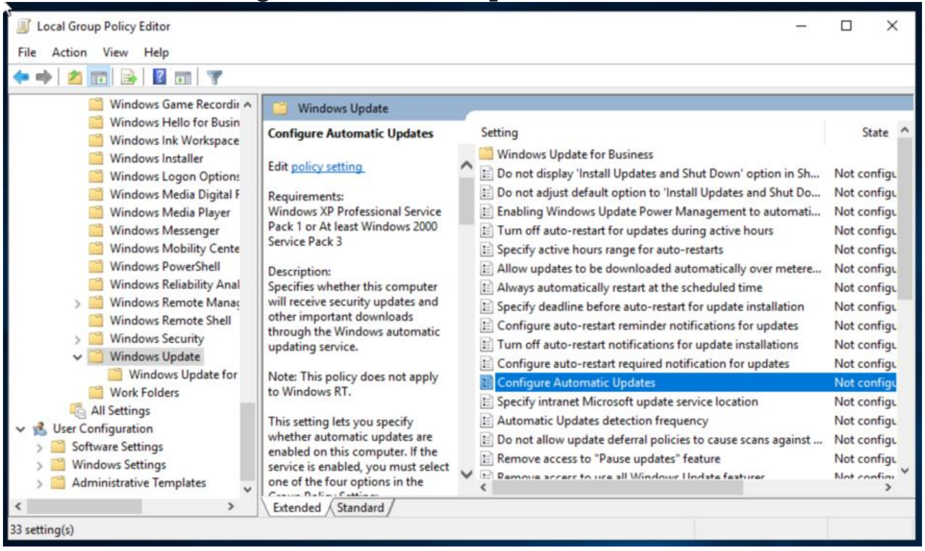


➢ Navigate to **computer configuration->Administrative Templates->Windows Components->Windows Update**



Setting	State
Windows Update for Business	
Do not display 'Install Updates and Shut Down' option in Sh...	Not configu
Do not adjust default option to 'Install Updates and Shut Do...	Not configu
Enabling Windows Update Power Management to automati...	Not configu
Turn off auto-restart for updates during active hours	Not configu
Specify active hours range for auto-restarts	Not configu
Allow updates to be downloaded automatically over metere...	Not configu
Always automatically restart at the scheduled time	Not configu
Specify deadline before auto-restart for update installation	Not configu
Configure auto-restart reminder notifications for updates	Not configu
Turn off auto-restart notifications for update installations	Not configu
Configure auto-restart required notification for updates	Not configu
Configure Automatic Updates	Not configu
Specify intranet Microsoft update service location	Not configu
Automatic Updates detection frequency	Not configu
Do not allow update deferral policies to cause scans against ...	Not configu
Remove access to "Pause updates" feature	Not configu
Remove access to use all Windows Update features	Not configu

- Double click Configure Automatic Updates and disable it.



Configure Automatic Updates

Edit policy setting

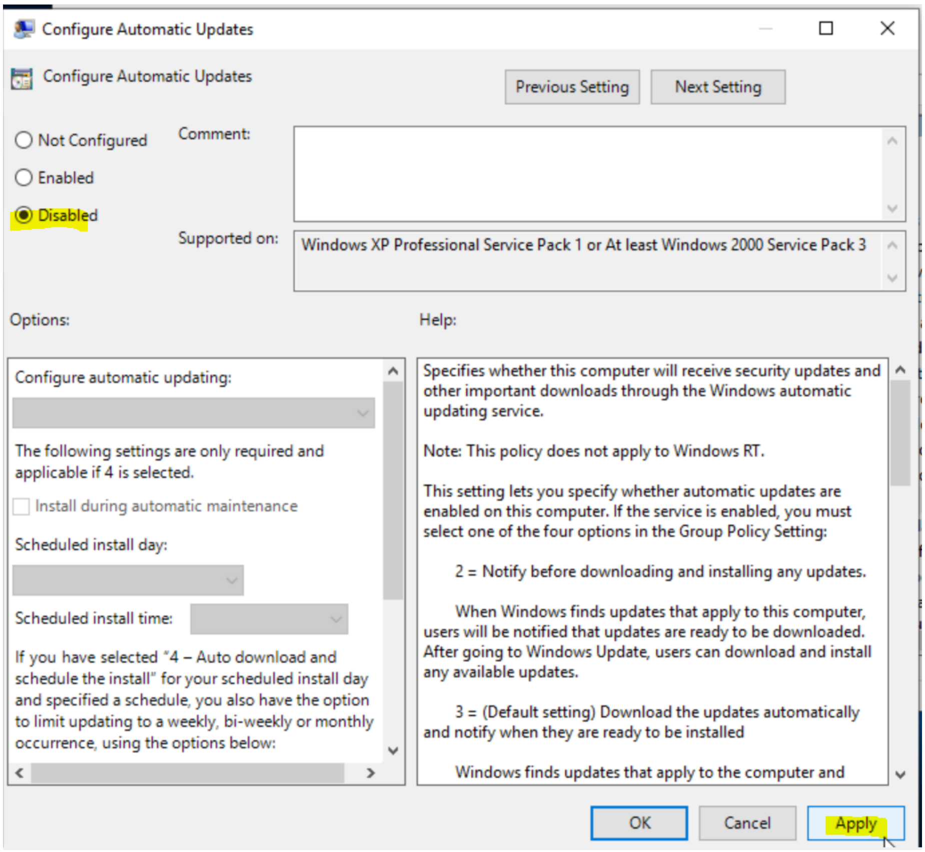
Requirements:
Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3

Description:
Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

Setting	State
Windows Update for Business	
Do not display 'Install Updates and Shut Down' option in Sh...	Not configu
Do not adjust default option to 'Install Updates and Shut Do...	Not configu
Enabling Windows Update Power Management to automati...	Not configu
Turn off auto-restart for updates during active hours	Not configu
Specify active hours range for auto-restarts	Not configu
Allow updates to be downloaded automatically over metere...	Not configu
Always automatically restart at the scheduled time	Not configu
Specify deadline before auto-restart for update installation	Not configu
Configure auto-restart reminder notifications for updates	Not configu
Turn off auto-restart notifications for update installations	Not configu
Configure auto-restart required notification for updates	Not configu
Configure Automatic Updates	Not configu
Specify intranet Microsoft update service location	Not configu
Automatic Updates detection frequency	Not configu
Do not allow update deferral policies to cause scans against ...	Not configu
Remove access to "Pause updates" feature	Not configu
Remove access to use all Windows Update features	Not configu



○ Not Configured

○ Enabled

● Disabled

Comment:

Supported on: Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3

Options:

Configure automatic updating:

The following settings are only required and applicable if 4 is selected.

□ Install during automatic maintenance

Scheduled install day:

Scheduled install time:

If you have selected "4 – Auto download and schedule the install" for your scheduled install day and specified a schedule, you also have the option to limit updating to a weekly, bi-weekly or monthly occurrence, using the options below:

Help:

Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading and installing any updates.

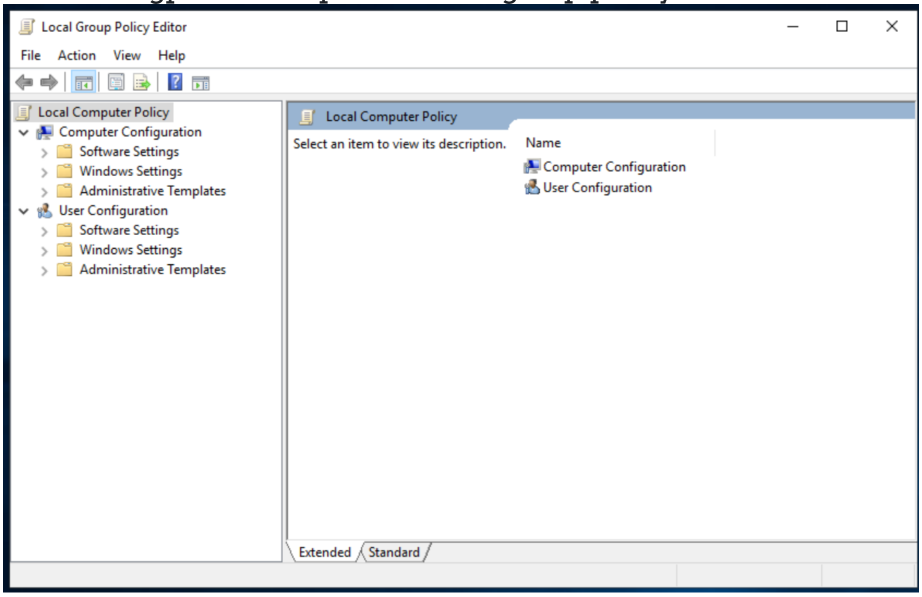
When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.

3 = (Default setting) Download the updates automatically and notify when they are ready to be installed

Windows finds updates that apply to the computer and

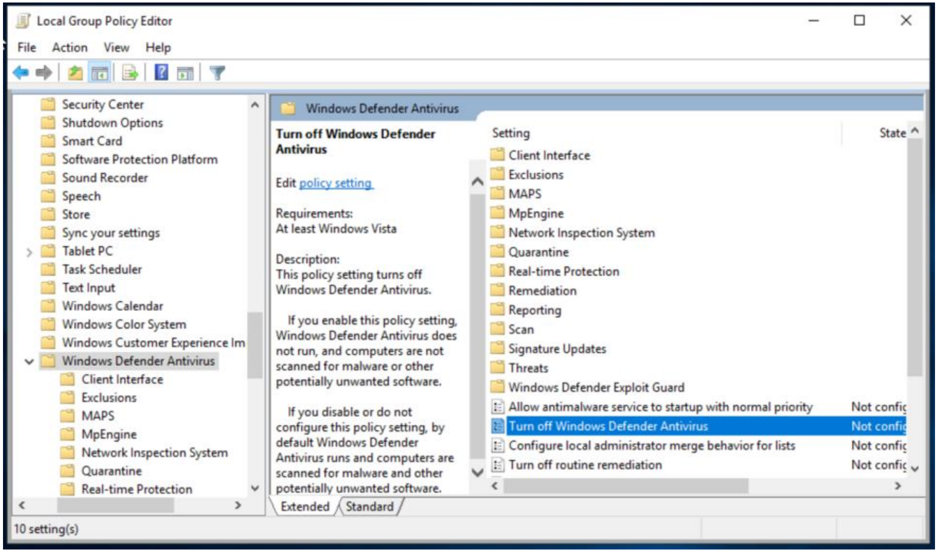
- **Disable Tamper Protection and any Anti-Malware solution (e.g., Windows Defender), preferably via Group Policy.**

- Search for gpedit and open the local group policy editor



Select an item to view its description.

- Navigate to **computer configuration->Administrative Templates->Windows Components->Windows Defender Antivirus**



Turn off Windows Defender Antivirus

Edit policy setting

Requirements:
At least Windows Vista

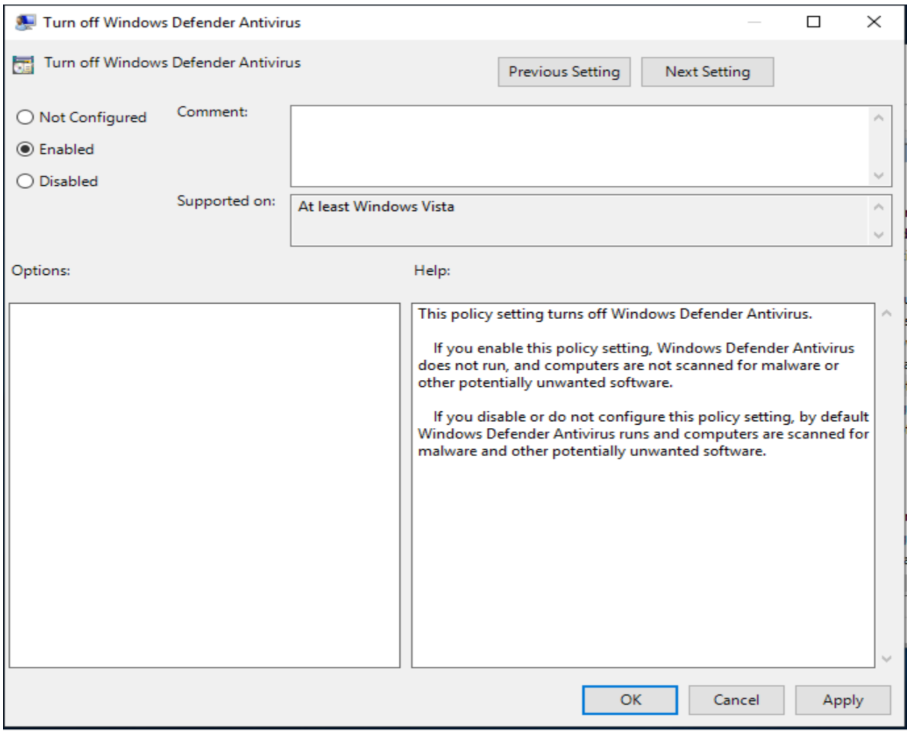
Description:
This policy setting turns off Windows Defender Antivirus.

If you enable this policy setting, Windows Defender Antivirus does not run, and computers are not scanned for malware or other potentially unwanted software.

If you disable or do not configure this policy setting, by default Windows Defender Antivirus runs and computers are scanned for malware and other potentially unwanted software.

Setting	State
Client Interface	
Exclusions	
MAPS	
MpEngine	
Network Inspection System	
Quarantine	
Real-time Protection	
Remediation	
Reporting	
Scan	
Signature Updates	
Threats	
Windows Defender Exploit Guard	
Allow antimalware service to startup with normal priority	Not config
Turn off Windows Defender Antivirus	Not config
Configure local administrator merge behavior for lists	Not config
Turn off routine remediation	Not config

- ➢ Double click on Turn off Windows Defender Antivirus and disable it



Turn off Windows Defender Antivirus

Turn off Windows Defender Antivirus

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

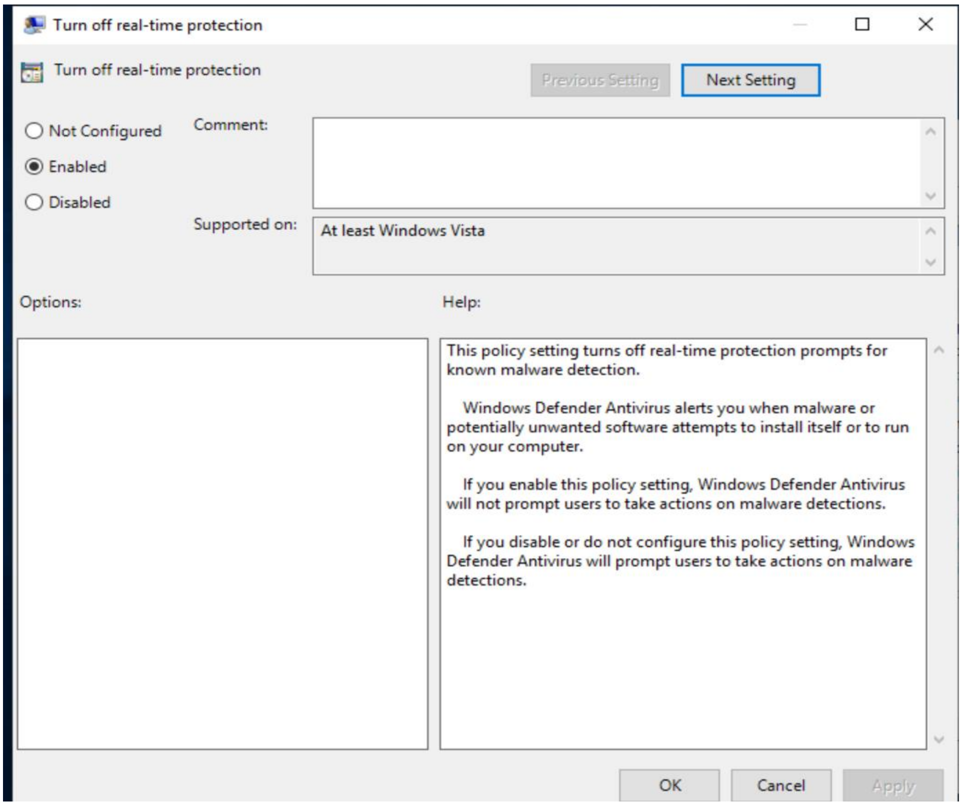
Help:

This policy setting turns off Windows Defender Antivirus.

If you enable this policy setting, Windows Defender Antivirus does not run, and computers are not scanned for malware or other potentially unwanted software.

If you disable or do not configure this policy setting, by default Windows Defender Antivirus runs and computers are scanned for malware and other potentially unwanted software.

- ➢ Navigate to **computer configuration->Administrative Templates->Windows Components->Windows Defender Antivirus->Real-time Protection**
- ➢ Double click on Turn off real-time protection



Turn off real-time protection

Turn off real-time protection

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Help:

This policy setting turns off real-time protection prompts for known malware detection.

Windows Defender Antivirus alerts you when malware or potentially unwanted software attempts to install itself or to run on your computer.

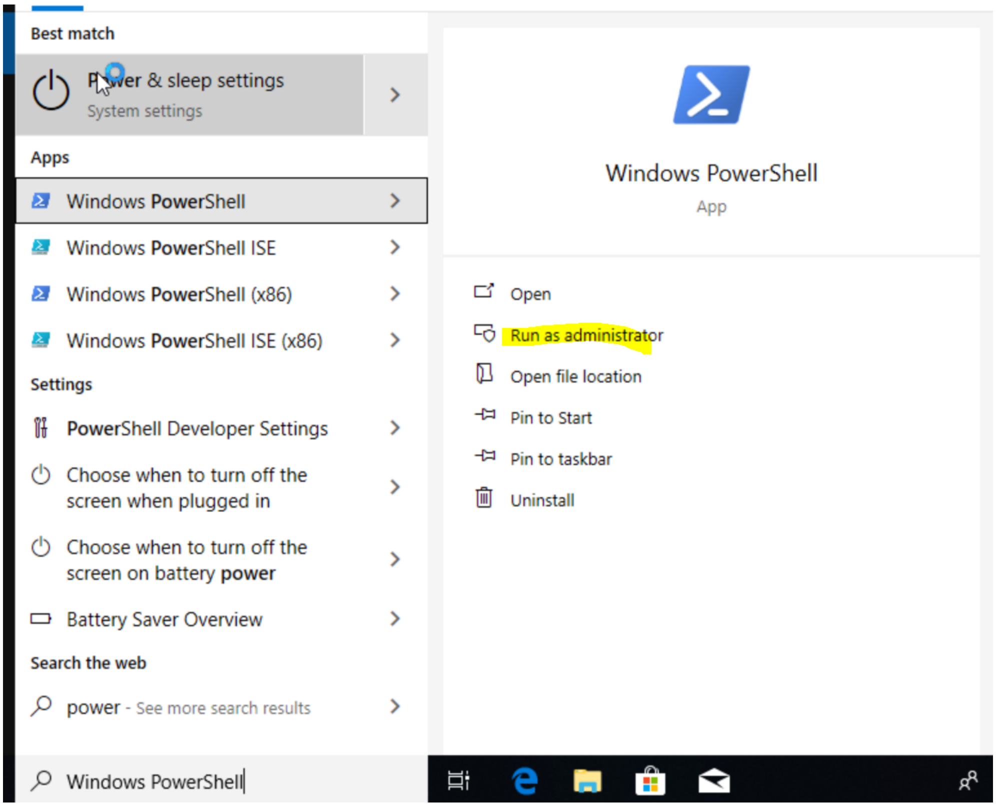
If you enable this policy setting, Windows Defender Antivirus will not prompt users to take actions on malware detections.

If you disable or do not configure this policy setting, Windows Defender Antivirus will prompt users to take actions on malware detections.

- ➢ Install >NET 4.8 framework as well
- ➢ Restart the system

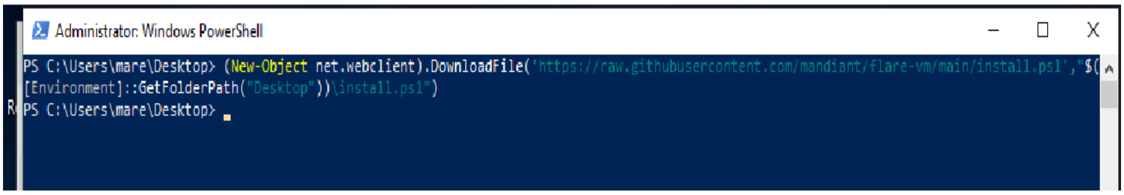
FLARE-VM installation

- Open a PowerShell prompt as administrator

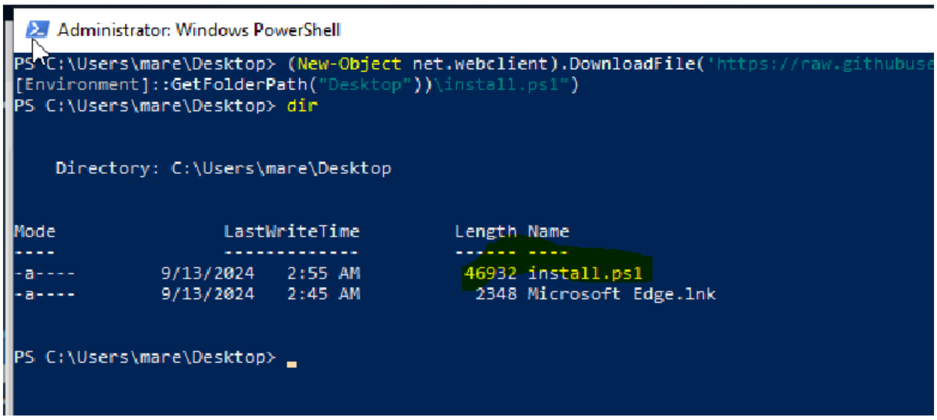


- Download the installation script installer.ps1 to your Desktop:
    - (New-Object net.webclient).DownloadFile('https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1',"$([Environment]::GetFolderPath("Desktop"))\install.ps1")

Copy and paste the above in the prompt

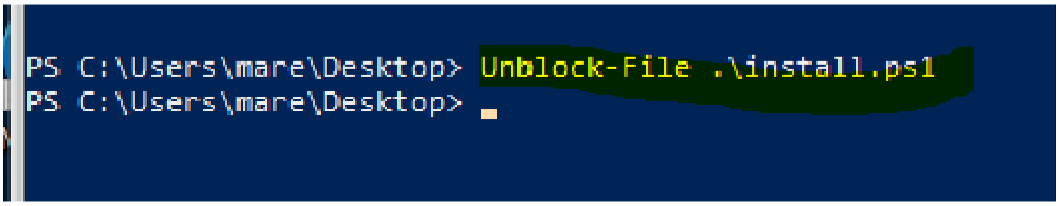


```
PS C:\Users\mare\Desktop> (New-Object net.webclient).DownloadFile('https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1',"$(
[Environment]::GetFolderPath("Desktop"))\install.ps1")
PS C:\Users\mare\Desktop> _
```



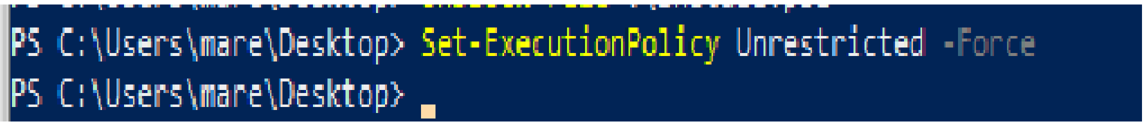
```
PS C:\Users\mare\Desktop> (New-Object net.webclient).DownloadFile('https://raw.githubuse
[Environment]::GetFolderPath("Desktop"))\install.ps1")
PS C:\Users\mare\Desktop> dir


    Directory: C:\Users\mare\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        9/13/2024   2:55 AM          46932 install.ps1
-a----        9/13/2024   2:45 AM           2348 Microsoft Edge.lnk


PS C:\Users\mare\Desktop>
```

- Unblock the installation script:
  - Unblock-File .\install.ps1



```
PS C:\Users\mare\Desktop> Unblock-File .\install.ps1
PS C:\Users\mare\Desktop>
```

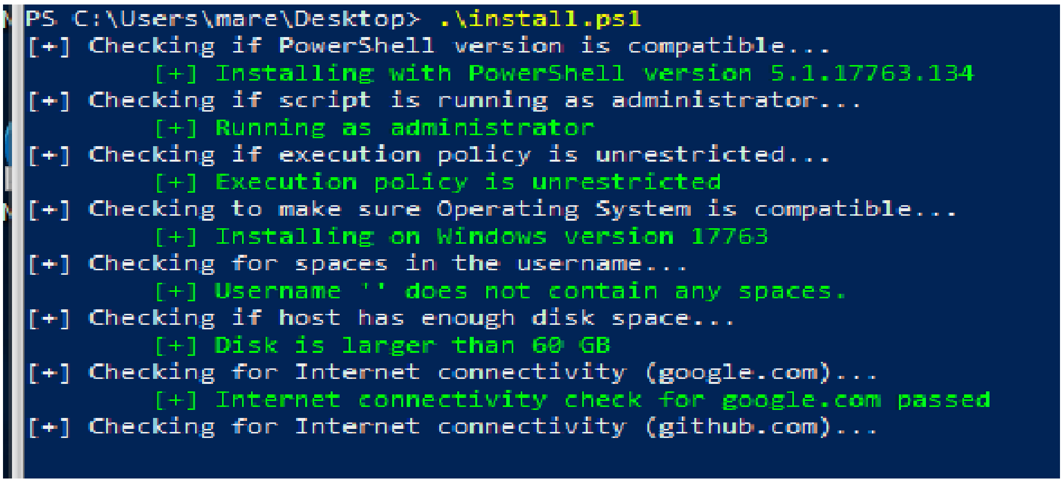
- Enable script execution:
  - Set-ExecutionPolicy Unrestricted -Force



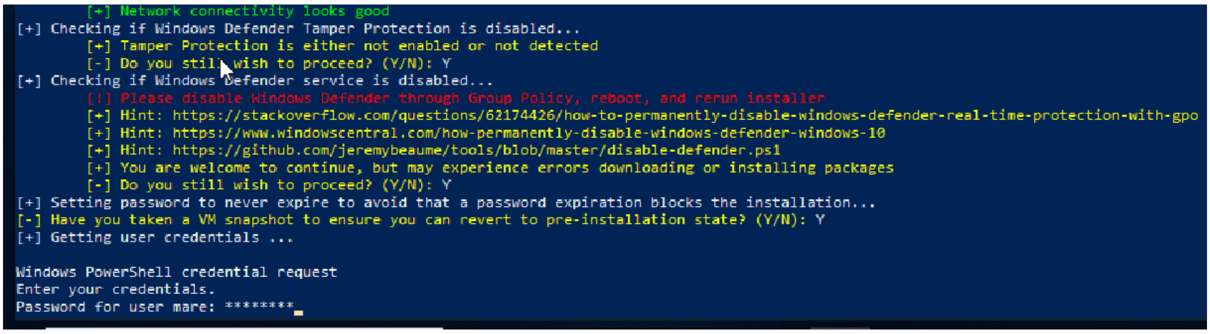
```
PS C:\Users\mare\Desktop> Set-ExecutionPolicy Unrestricted -Force
PS C:\Users\mare\Desktop>
```

    - If you receive an error saying the execution policy is overridden by a policy defined at a more specific scope, you may need to pass a scope in via Set-ExecutionPolicy Unrestricted -Scope CurrentUser -Force. To view execution policies for all scopes, execute Get-ExecutionPolicy -List

- Finally, execute the installer script as follow:
  - .\install.ps1

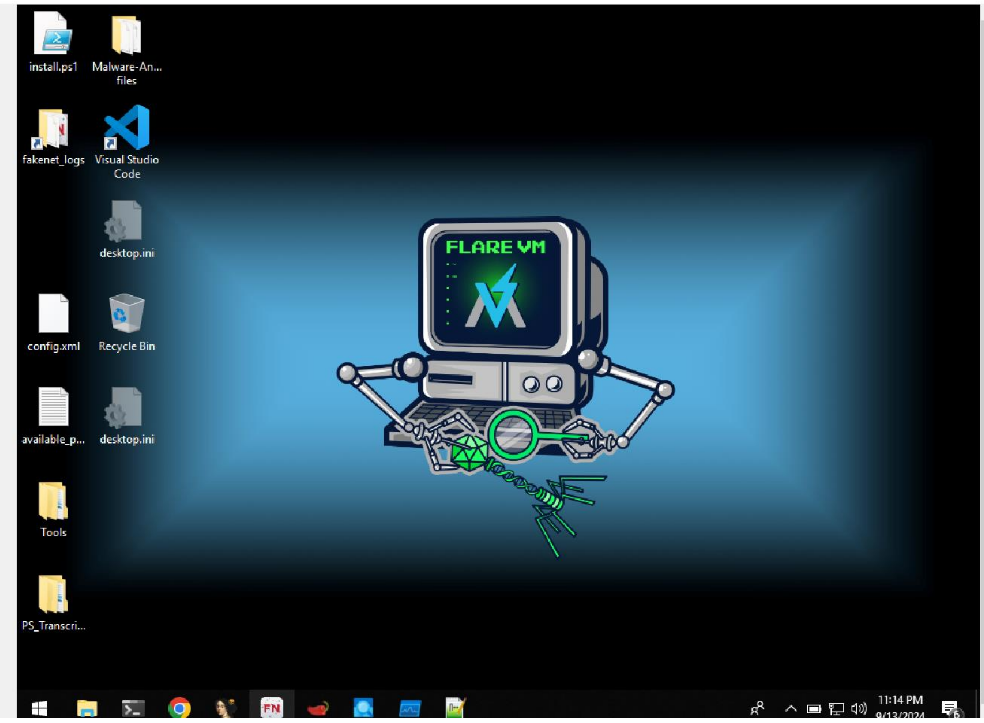


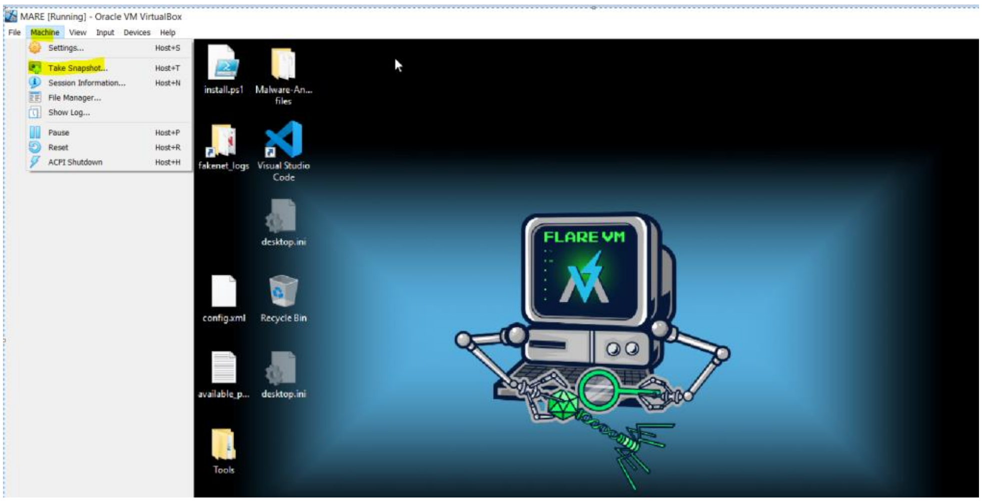
```
PS C:\Users\mare\Desktop> .\install.ps1
[+] Checking if PowerShell version is compatible...
        [+] Installing with PowerShell version 5.1.17763.134
[+] Checking if script is running as administrator...
        [+] Running as administrator
[+] Checking if execution policy is unrestricted...
        [+] Execution policy is unrestricted
[+] Checking to make sure Operating System is compatible...
        [+] Installing on Windows version 17763
[+] Checking for spaces in the username...
        [+] Username '' does not contain any spaces.
[+] Checking if host has enough disk space...
        [+] Disk is larger than 60 GB
[+] Checking for Internet connectivity (google.com)...
        [+] Internet connectivity check for google.com passed
[+] Checking for Internet connectivity (github.com)...
```



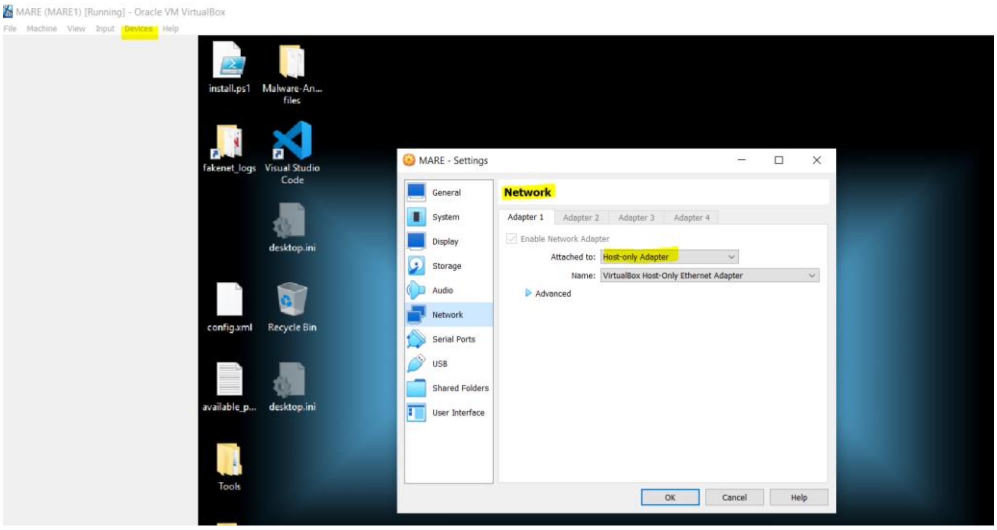
```
        [+] Network connectivity looks good
[+] Checking if Windows Defender Tamper Protection is disabled...
        [+] Tamper Protection is either not enabled or not detected
        [-] Do you still wish to proceed? (Y/N): Y
[+] Checking if Windows Defender service is disabled...
        [!] Please disable Windows Defender through Group Policy, reboot, and rerun installer
        [+] Hint: https://stackoverflow.com/questions/62174426/how-to-permanently-disable-windows-defender-real-time-protection-with-gpo
        [+] Hint: https://www.windowscentral.com/how-permanently-disable-windows-defender-windows-10
        [+] Hint: https://github.com/jeremybeaume/tools/blob/master/disable-defender.ps1
        [+] You are welcome to continue, but may experience errors downloading or installing packages
        [-] Do you still wish to proceed? (Y/N): Y
[+] Setting password to never expire to avoid that a password expiration blocks the installation...
[-] Have you taken a VM snapshot to ensure you can revert to pre-installation state? (Y/N): Y
[+] Getting user credentials ...

Windows PowerShell credential request
Enter your credentials.
Password for user mare: ********_
```

Take a snapshot with all the tools installed before performing any malware analysis and reverse engineering





Isolating your environment

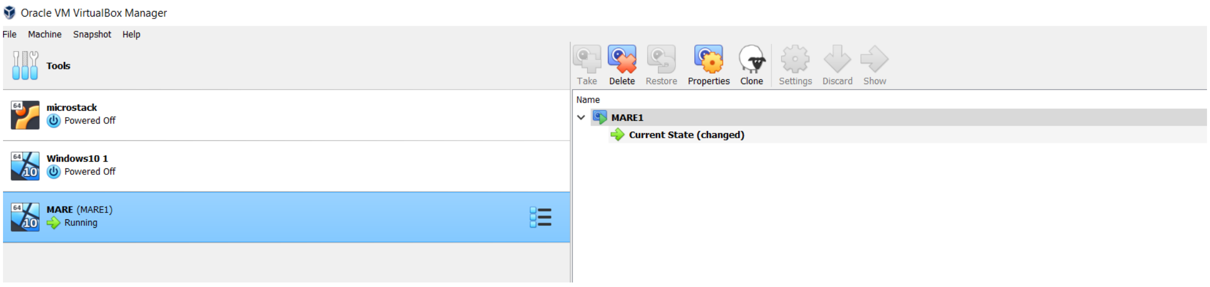


Network

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter



microstack Powered Off

Windows10 1 Powered Off

MARE (MARE1) Running

MARE1

Current State (changed)