Set up your virtual environment

1. Download and deploy a free Windows VM directly from Microsoft.
    a. Get the “VMWare” version of the workstation.
    b. Take notice of the “Expiration date” of your VM, it will stop working after this date, but you can always download a new one.
    c. Once downloaded, unzip the VM and double-click the WinDev####Eval.ovf file to import the VM into VMware, but do not start it up yet.
    d. If you have 16 GB of RAM or less, modify it to 4GB. If the VM run slow, it may be due to insufficient RAM.
    e. I have highlighted every command that would be needed to be used with cmd/ powershell for ease of use.

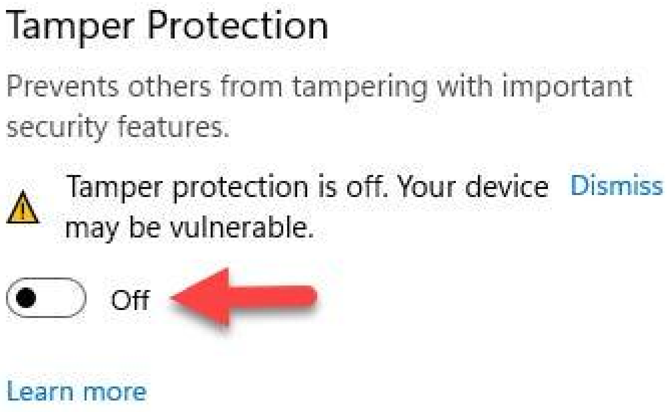
Setup your Windows VM

1. Power on the VM for the first time
    a. It will automatically log you in as “user”.
    b. Wait for the desktop to appear.

Disable Defender on Windows VM

We will be Permanently disabling Microsoft Defender so it doesn’t interfere with what we are planning. In Windows 11, MS Defender will turn itself on, so you will need to follow this guide to the exact letter. These steps are closely derived from this guide and this one as well, but with fewer screenshots. If you need more guidance, see the original guides.

1. Disable Tamper Protection
    a. Click the “Start” menu icon
    b. Click “Settings”
    c. Click “Privacy & security” on the left
    d. Click “Windows Security”
    e. Click “Virus & threat protection”
    f. Under “Virus & threat protection settings” click “Manage settings”
    g. Toggle OFF the “Tamper Protection” switch. When prompted, click “Yes”
    h.



Tamper Protection

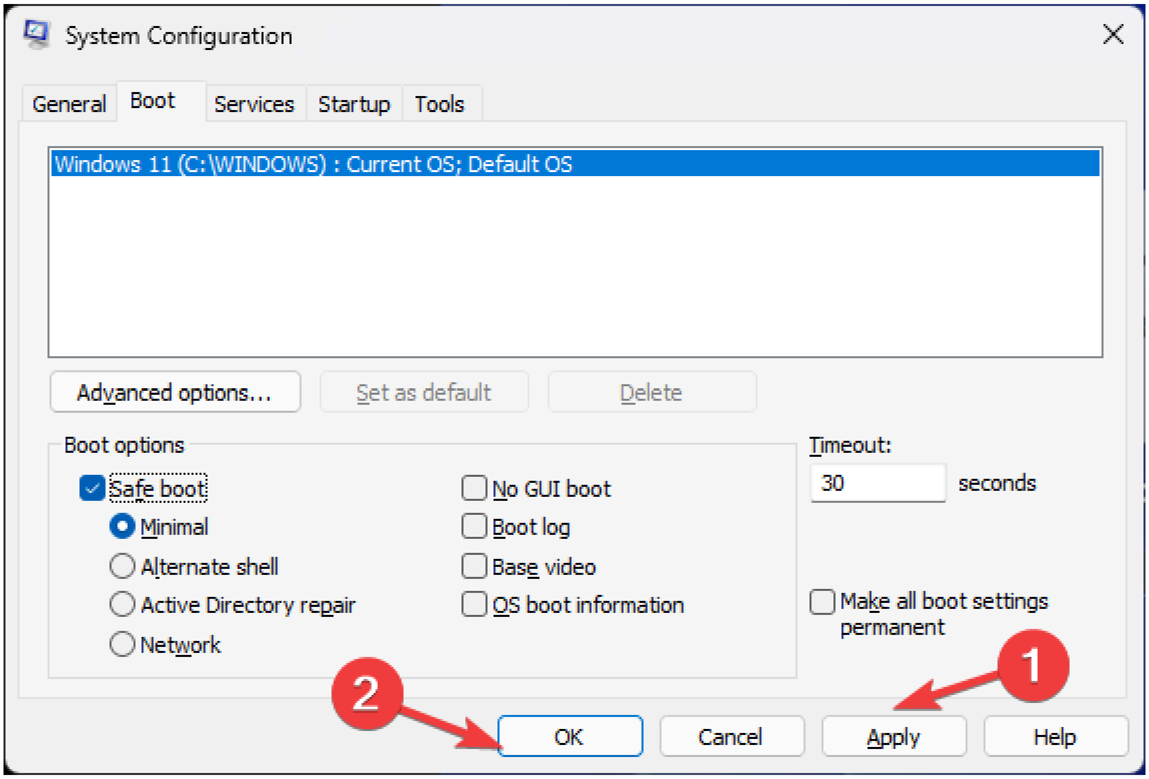
Prevents others from tampering with important security features.

Tamper protection is off. Your device may be vulnerable.

    i. While you’re in there, **toggle every other option OFF** as well, even though we’re about to take care of it a couple different ways.
    j. Close the windows we just opened.

2. Permanently Disable Defender via Group Policy Editor
   a. Click the “Start” menu icon
   b. Type “cmd” into the search bar within the Start Menu
   c. Right+Click “Command Prompt” and click “Run as administrator”
      i. Run the following command
      “gpedit.msc”
   d. Inside the Local Group Policy Editor
      i. Click Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus
      ii. Double-click “Turn off Microsoft Defender Antivirus”
      iii. Select “Enabled”
      If you enable this policy setting, Microsoft Defender Antivirus does not run, and will not scan computers for malware or other potentially unwanted software.
      iv. Click Apply
      v. Click OK
3. Permanently Disable Defender via Registry
   a. From the same administrative command prompt we previously opened, copy/paste this command and press Enter
   “REG ADD "hklm\software\policies\microsoft\windows defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f”

4. Prepare to boot into Safe Mode to disable all Defender services
    a. Click the “Start” menu icon
    b. type “msconfig” into the search bar within the Start Menu
    c. Go to “Boot” tab and select “Boot Options”
        i. Check the box for “Safe boot” and “Minimal



System Configuration

Windows 11 (C:\WINDOWS) : Current OS; Default OS

Boot options

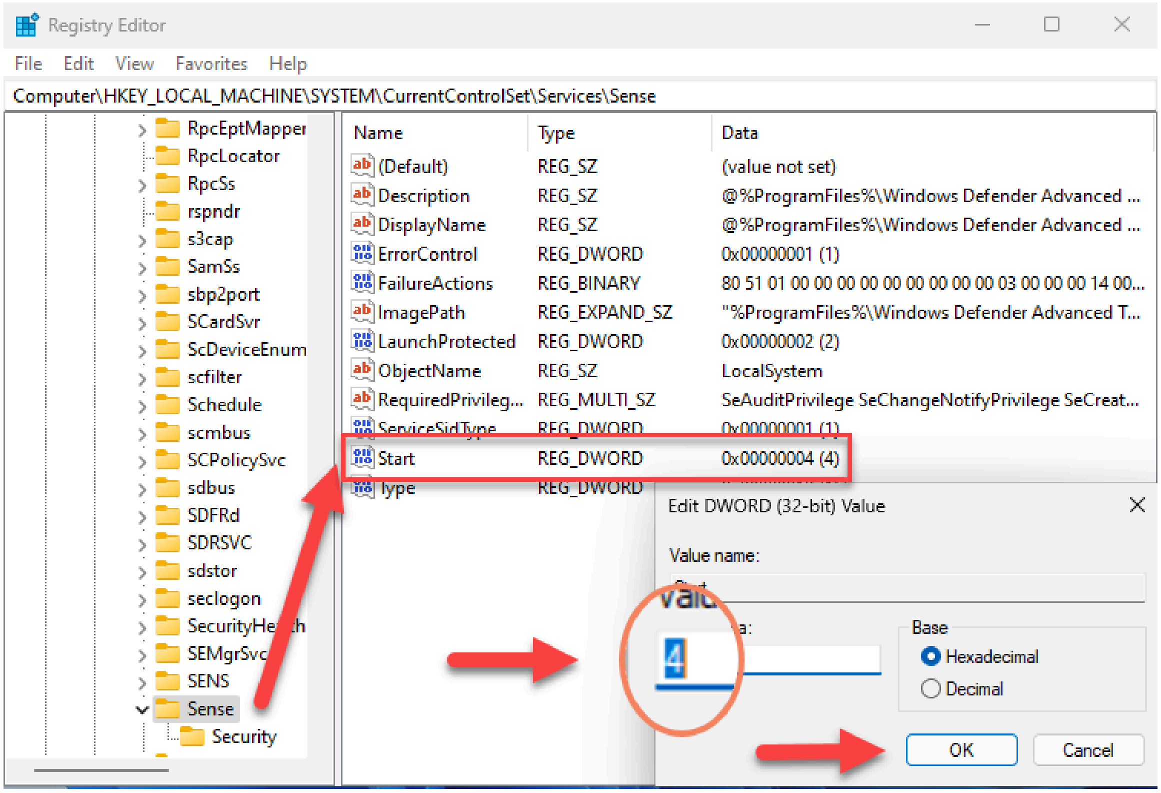
☑ Safe boot
● Minimal
○ Alternate shell
○ Active Directory repair
○ Network

□ No GUI boot
□ Boot log
□ Base video
□ OS boot information

Timeout: 30 seconds

□ Make all boot settings permanent

        ii. Click Apply and OK
    d. System will restart into Safe Mode
5. Now, in Safe Mode, we’ll disable some services via the Registry
    a. Click the “Start” menu icon
    b. Type “regedit” into the search bar and hit Enter
    c. For each of the following registry locations, you’ll need to browse to the key, find the “Start” value, and change it to 4
        i. This causes windows defender to essentially start these services when it boots.

d. 

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sense

Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	@%ProgramFiles%\Windows Defender Advanced ...
DisplayName	REG_SZ	@%ProgramFiles%\Windows Defender Advanced ...
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	80 51 01 00 00 00 00 00 00 00 00 00 03 00 00 00 14 00...
ImagePath	REG_EXPAND_SZ	"%ProgramFiles%\Windows Defender Advanced T...
LaunchProtected	REG_DWORD	0x00000002 (2)
ObjectName	REG_SZ	LocalSystem
RequiredPrivileg...	REG_MULTI_SZ	SeAuditPrivilege SeChangeNotifyPrivilege SeCreat...
ServiceSidType	REG_DWORD	0x00000001 (1)
Start	REG_DWORD	0x00000004 (4)
Type	REG_DWORD	

Value name:

Value data: 4

Base

● Hexadecimal

○ Decimal

i. Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sense

ii. Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdBoot

iii. Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinDefend

iv. Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdNisDrv

v. Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdNisSvc

vi. Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdFilter

6. Leave Safe Mode the same way we got into it
    a. Click the “Start” menu icon
    b. type “msconfig” into the search bar within the Start Menu

    c. Go to “Boot” tab and select “Boot Options”
        i. Uncheck the box for “Safe boot”
        ii. Click Apply and OK
    d. System will restart into a normal desktop environment, now (hopefully) Defender-free.

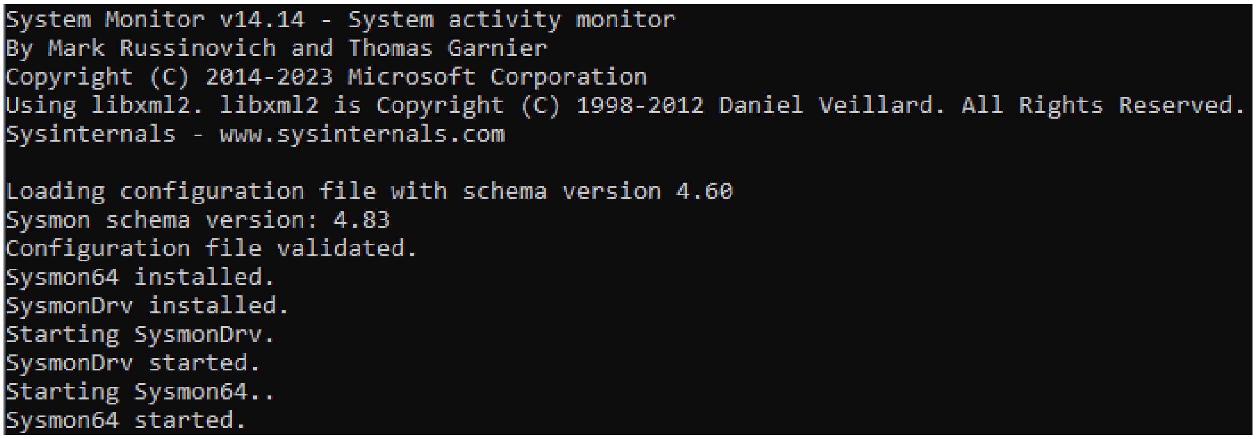
Prevent the VM from going into standby

1. From an administrative command prompt, let’s prevent the VM from going into sleep/standby mode during our lab
    a. powercfg /change standby-timeout-ac 0
    b. powercfg /change standby-timeout-dc 0
    c. powercfg /change monitor-timeout-ac 0
    d. powercfg /change monitor-timeout-dc 0
    e. powercfg /change hibernate-timeout-ac 0
    f. powercfg /change hibernate-timeout-dc 0

Install Sysmon in Windows VM

This is mostly optional as we don't directly use Sysmon in this guide, but recommended to familiar having it.

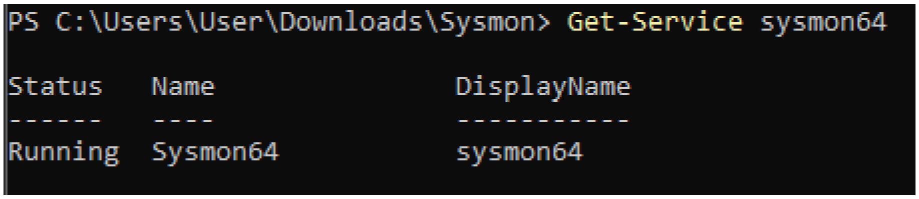
1. Launch an **Administrative** PowerShell console for the following commands
    a. Click the "Start" menu icon
    b. Type "powershell" into the search bar within the Start Menu
    c. Right+Click "Windows PowerShell" and click "Run as administrator"
2. Download Sysmon with the following command. Read more about Sysmon here.
    ```
    Invoke-WebRequest -Uri https://download.sysinternals.com/files/Sysmon.zip -OutFile C:\Windows\Temp\Sysmon.zip
    ```
3. Unzip Sysmon.zip with the following command
    ```
    Expand-Archive -LiteralPath C:\Windows\Temp\Sysmon.zip -DestinationPath C:\Windows\Temp\Sysmon
    ```
4. Download SwiftOnSecurity's Sysmon config with the following command.
    ```
    Invoke-WebRequest -Uri https://raw.githubusercontent.com/SwiftOnSecurity/sysmon-config/master/sysmonconfig-export.xml -OutFile C:\Windows\Temp\Sysmon\sysmonconfig.xml
    ```
5. Install Sysmon with Swift's config with the following commands.
    ```
    C:\Windows\Temp\Sysmon\Sysmon64.exe -accepteula -i
    ========
    C:\Windows\Temp\Sysmon\sysmonconfig.xml
    ```

6. 

```
System Monitor v14.14 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2023 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.60
Sysmon schema version: 4.83
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
```

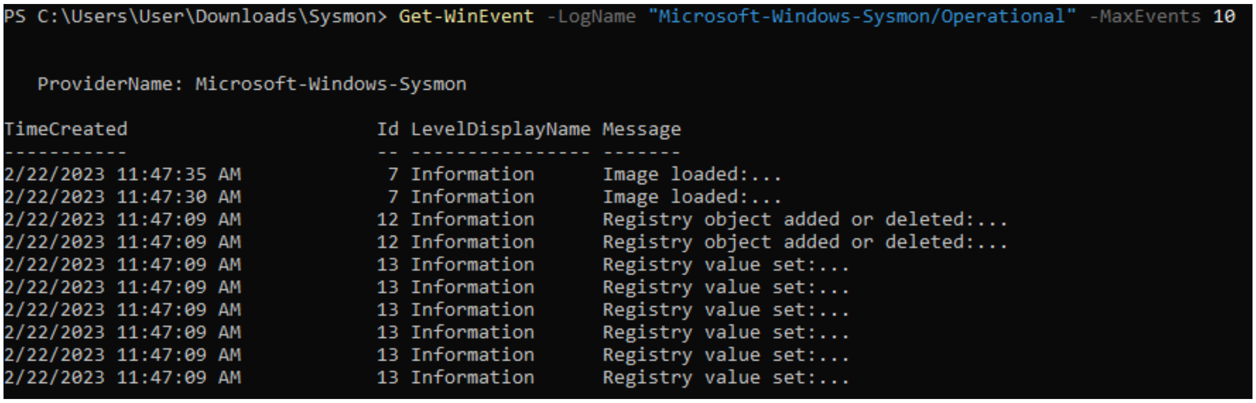
7. Validate Sysmon64 service is installed and running
   Type in “Get-Service sysmon64”

8. 

```
PS C:\Users\User\Downloads\Sysmon> Get-Service sysmon64

Status   Name               DisplayName
------   ----               -----------
Running  Sysmon64           sysmon64
```

9. Check for the presence of Sysmon Event Logs
   Type in ‘Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" -MaxEvents 10’

10. 

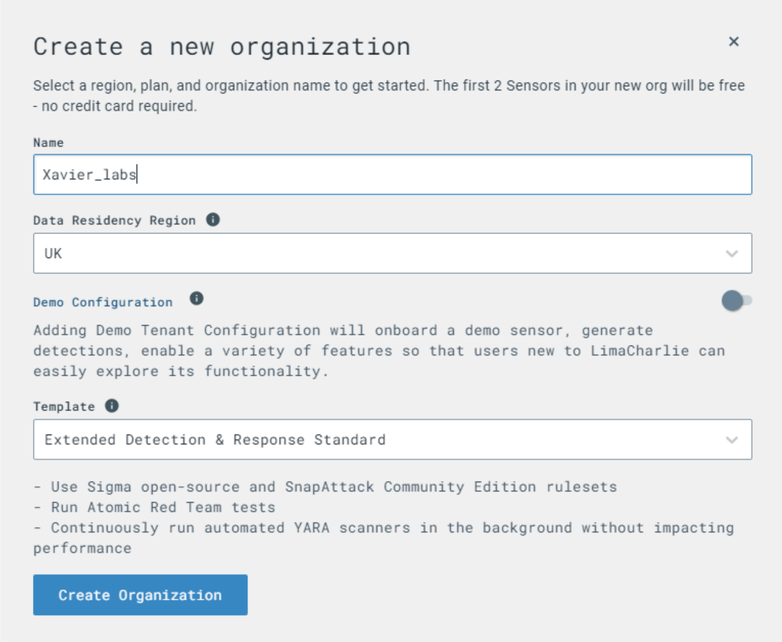
```
PS C:\Users\User\Downloads\Sysmon> Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" -MaxEvents 10


   ProviderName: Microsoft-Windows-Sysmon

TimeCreated                      Id LevelDisplayName Message
-----------                      -- ---------------- -------
2/22/2023 11:47:35 AM             7 Information      Image loaded:...
2/22/2023 11:47:30 AM             7 Information      Image loaded:...
2/22/2023 11:47:09 AM            12 Information      Registry object added or deleted:...
2/22/2023 11:47:09 AM            12 Information      Registry object added or deleted:...
2/22/2023 11:47:09 AM            13 Information      Registry value set:...
2/22/2023 11:47:09 AM            13 Information      Registry value set:...
2/22/2023 11:47:09 AM            13 Information      Registry value set:...
2/22/2023 11:47:09 AM            13 Information      Registry value set:...
2/22/2023 11:47:09 AM            13 Information      Registry value set:...
2/22/2023 11:47:09 AM            13 Information      Registry value set:...
```

Install LimaCharlie EDR on Windows VM

LimaCharlie is a very powerful “SecOps Cloud Platform”. It not only comes with a cross-platform EDR agent, but also handles all of the log shipping/ingestion and has a threat detection engine. They have a free tier which made it an instrumental part of this guide.

1. Create a free LimaCharlie account.
    a. LimaCharlie will ask you a few questions about your role. Answer however you wish, it just helps their developers build a better product
2. Once logged into LimaCharlie, create an organization
    a. Name: whatever you want, but it must be unique
    b. Data Residency: whatever is closest
    c. Demo Configuration Enabled: disabled
    d. Template: Extended Detection & Response Standard
    e. 

Create a new organization

Select a region, plan, and organization name to get started. The first 2 Sensors in your new org will be free - no credit card required.

Name: Xavier_labs

Data Residency Region: UK

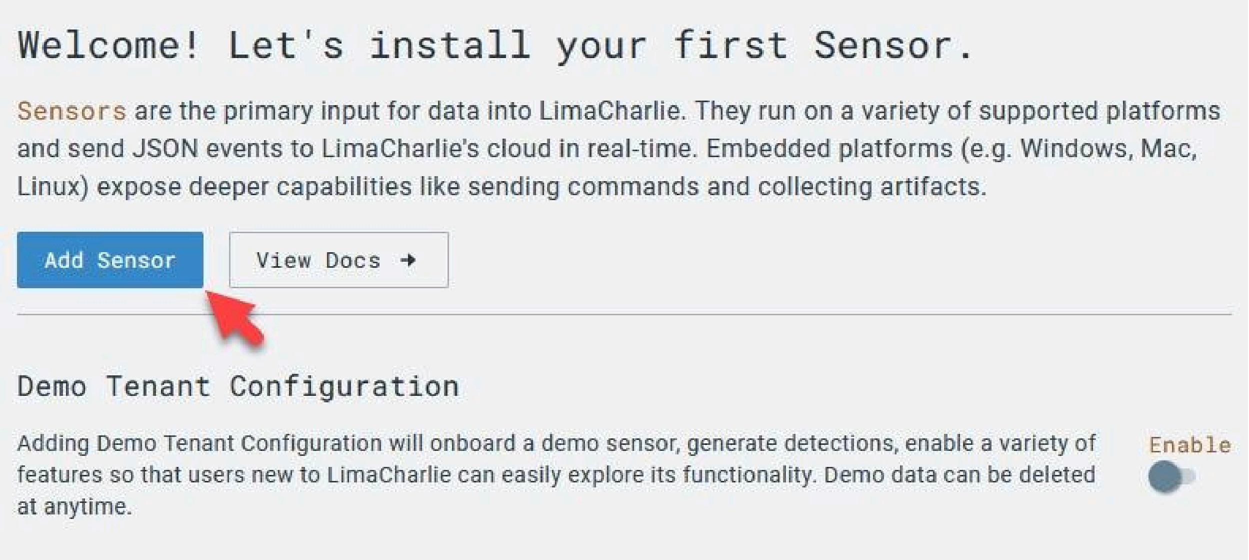
Demo Configuration

Adding Demo Tenant Configuration will onboard a demo sensor, generate detections, enable a variety of features so that users new to LimaCharlie can easily explore its functionality.

Template: Extended Detection & Response Standard

- Use Sigma open-source and SnapAttack Community Edition rulesets
- Run Atomic Red Team tests
- Continuously run automated YARA scanners in the background without impacting performance

3. Once the org is created, click “Add Sensor”



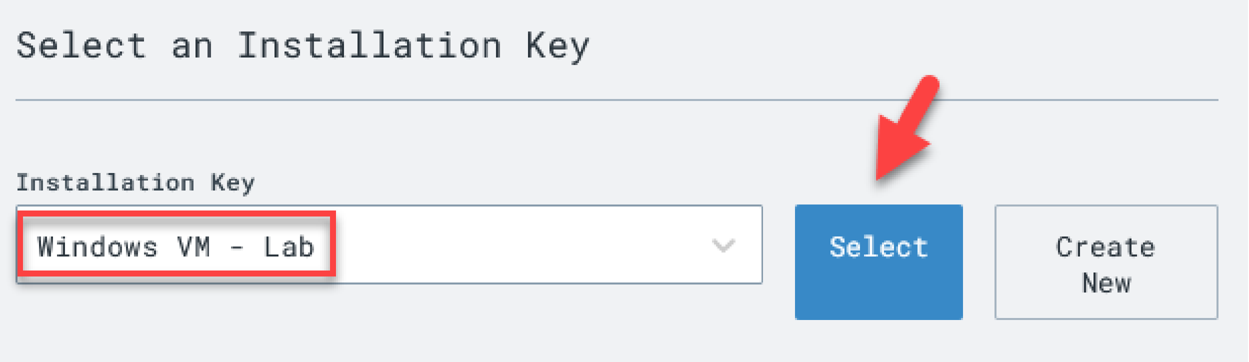
Welcome! Let's install your first Sensor.

Sensors are the primary input for data into LimaCharlie. They run on a variety of supported platforms and send JSON events to LimaCharlie's cloud in real-time. Embedded platforms (e.g. Windows, Mac, Linux) expose deeper capabilities like sending commands and collecting artifacts.

Demo Tenant Configuration

Adding Demo Tenant Configuration will onboard a demo sensor, generate detections, enable a variety of features so that users new to LimaCharlie can easily explore its functionality. Demo data can be deleted at anytime.

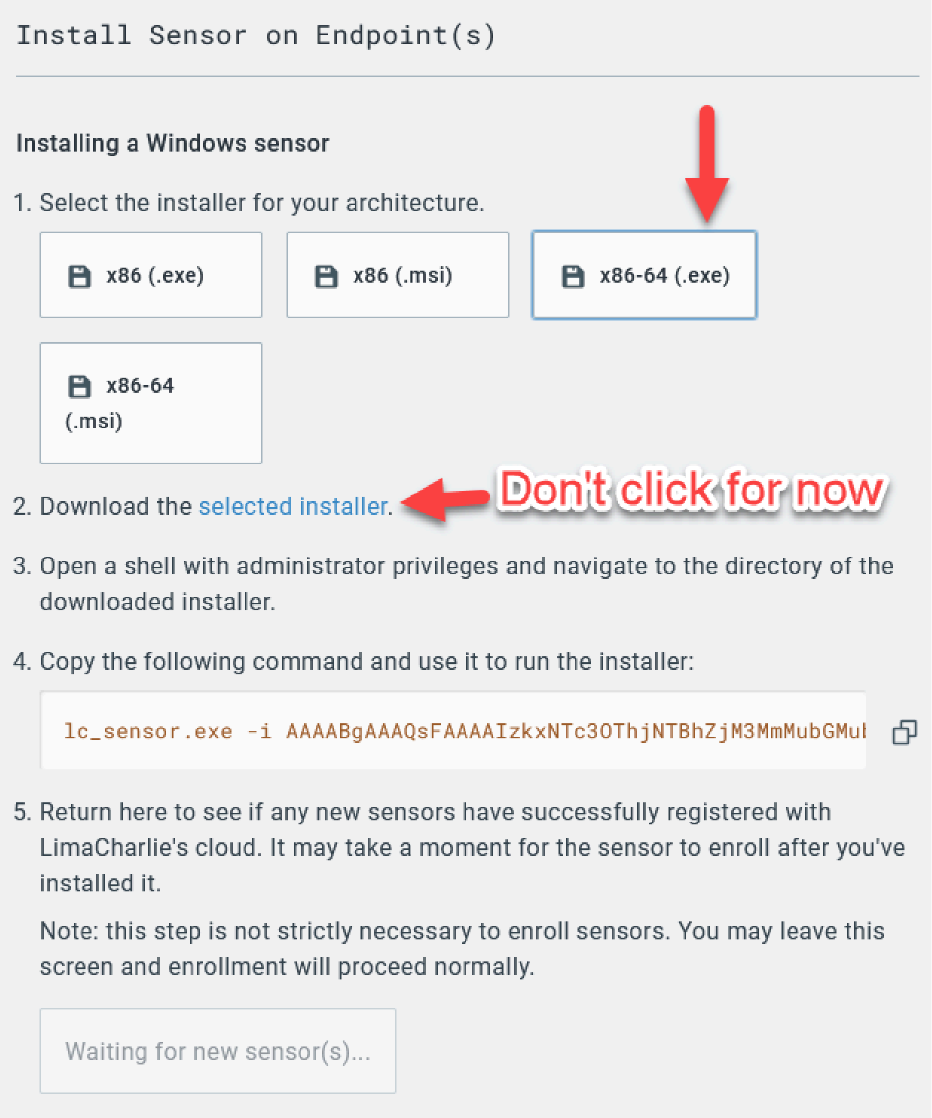
i. Select Windows
ii. Provide a description such as: Windows VM - Lab
iii. Click Create
iv. Select the Installation Key we just created



Select an Installation Key

Installation Key: Windows VM - Lab

v. Specify the x86-64 (.exe) sensor, but then skip ahead to my instructions versus the ones provided.



Installing a Windows sensor

1. Select the installer for your architecture.
2. Download the selected installer.

Don't click for now

3. Open a shell with administrator privileges and navigate to the directory of the downloaded installer.
4. Copy the following command and use it to run the installer:

```
lc_sensor.exe -i AAAABgAAAQsFAAAAIzkxNTc3OThjNTBhZjM3MmMubGMu
```

5. Return here to see if any new sensors have successfully registered with LimaCharlie's cloud. It may take a moment for the sensor to enroll after you've installed it.

   Note: this step is not strictly necessary to enroll sensors. You may leave this screen and enrollment will proceed normally.

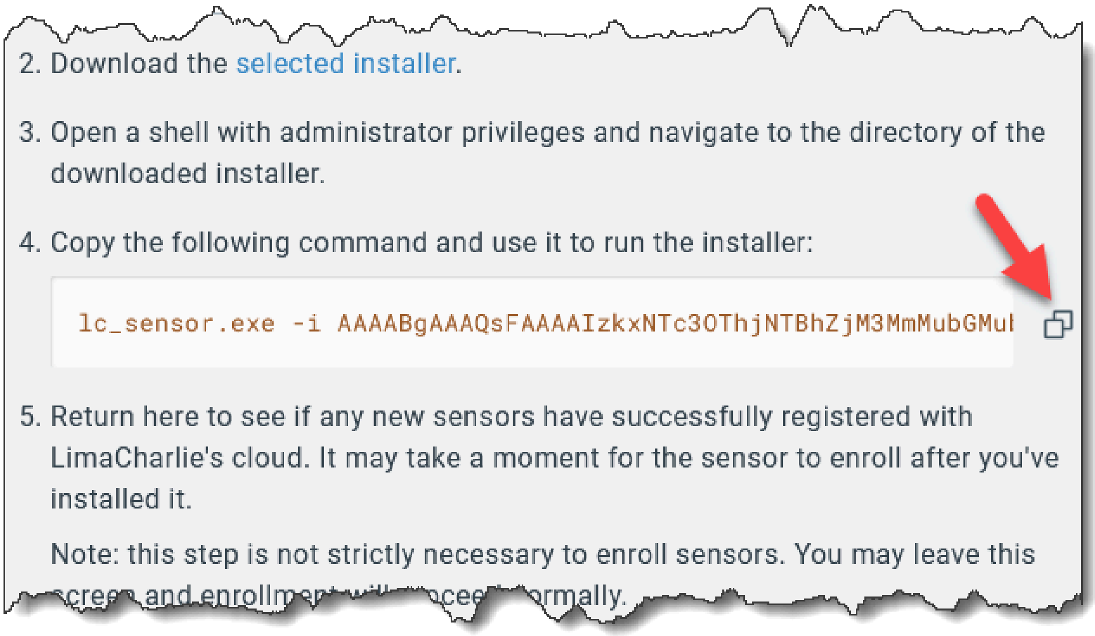
vi. IN THE **WINDOWS VM**, open an Administrative PowerShell prompt and paste the following commands:

```
cd C:\Users\User\Downloads
Invoke-WebRequest -Uri https://downloads.limacharlie.io/sensor/windows/64 -Outfile C:\Users\User\Downloads\lc_sensor.exe
```

vii. Shift into a standard command prompt by running this command

```
cmd.exe
```

viii. Next, we will copy the install command provided by LimaCharlie which contains the installation key. Paste this command into your open terminal.



2. Download the selected installer.

3. Open a shell with administrator privileges and navigate to the directory of the downloaded installer.

4. Copy the following command and use it to run the installer:

```
lc_sensor.exe -i AAAABgAAAQsFAAAAIzkxNTc3OThjNTBhZjM3MmMubGMu
```

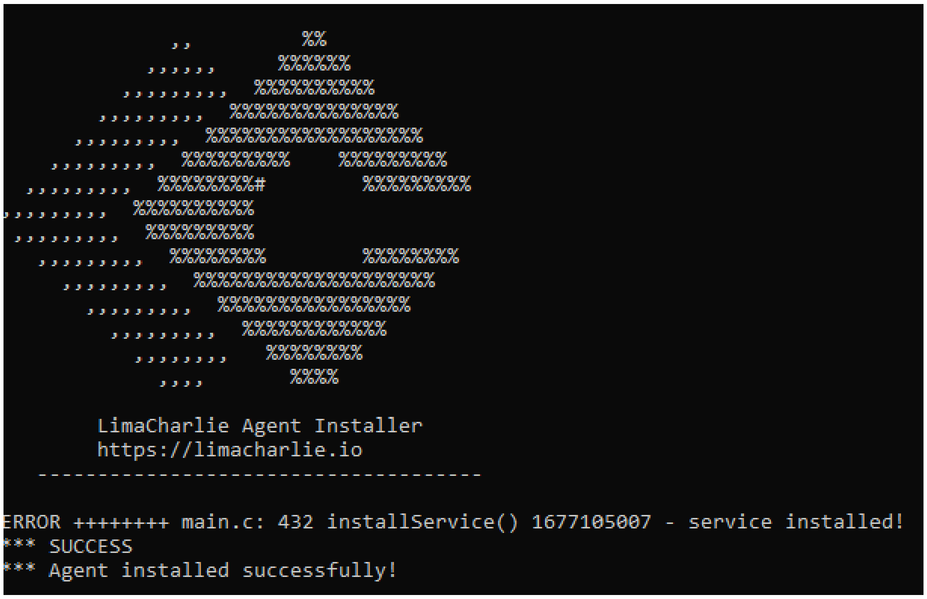
5. Return here to see if any new sensors have successfully registered with LimaCharlie's cloud. It may take a moment for the sensor to enroll after you've installed it.

Note: this step is not strictly necessary to enroll sensors. You may leave this screen and enrollment will proceed normally.

ix. Paste this command into the admin command prompt in your Windows VM.

1. Take note, if lc_sensor.exe is not in the command, you will have to add it in yourself.

x. This is the expected output, ignore the “ERROR” that says “service installed!



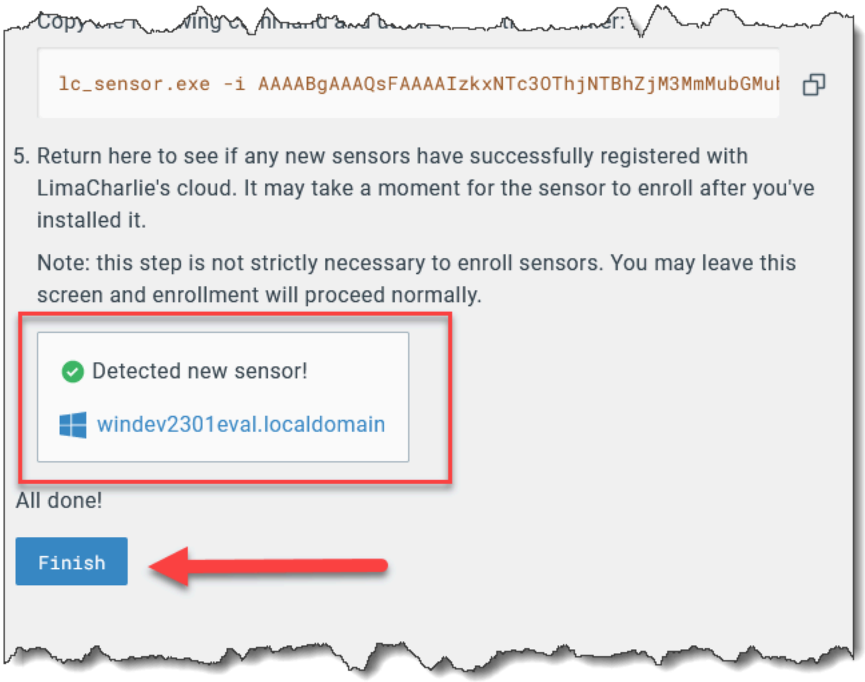
```
              ,,         %%
            ,,,,,,     %%%%%%
          ,,,,,,,,,  %%%%%%%%%%
        ,,,,,,,,,  %%%%%%%%%%%%%%
      ,,,,,,,,,  %%%%%%%%%%%%%%%%%%
    ,,,,,,,,,  %%%%%%%%%    %%%%%%%%%
  ,,,,,,,,,  %%%%%%%%#        %%%%%%%%%
,,,,,,,,,  %%%%%%%%%%
 ,,,,,,,,,  %%%%%%%%%
   ,,,,,,,,,  %%%%%%%%        %%%%%%%%
     ,,,,,,,,,  %%%%%%%%%%%%%%%%%%%%
       ,,,,,,,,,  %%%%%%%%%%%%%%%%
         ,,,,,,,,,  %%%%%%%%%%%%
           ,,,,,,,,   %%%%%%%%
             ,,,,       %%%%


        LimaCharlie Agent Installer
        https://limacharlie.io
   -------------------------------------

ERROR ++++++++ main.c: 432 installService() 1677105007 - service installed!
*** SUCCESS
*** Agent installed successfully!
```

1. If you experience an error trying to install the EXE, try the x86-64 MSI option on the LimaCharlie installer dialog.

xi. If everything worked correctly, in the LimaCharlie web UI you should also see the sensor reporting in.



```
lc_sensor.exe -i AAAABgAAAQsFAAAAIzkxNTc3OThjNTBhZjM3MmMubGMul
```

5. Return here to see if any new sensors have successfully registered with LimaCharlie's cloud. It may take a moment for the sensor to enroll after you've installed it.

Note: this step is not strictly necessary to enroll sensors. You may leave this screen and enrollment will proceed normally.

✓ Detected new sensor!

windev2301eval.localdomain

All done!

b. Now let’s configure LimaCharlie to also ship the Sysmon event logs alongside its own EDR telemetry
    i. In the left-side menu, click “Artifact Collection”
    ii. Next to “Artifact Collection Rules” click “Add Rule”
        1. Name: windows-sysmon-logs
        2. Platforms: Windows
        3. Path Pattern: wel://Microsoft-Windows-Sysmon/Operational:*
        4. Retention Period: 10
        5. Click “Save Rule”
    iii. LimaCharlie will now start shipping Sysmon logs which provide a wealth of EDR-like telemetry, some of which is redundant to LC’s own telemetry, but Sysmon is still a very powerful visibility tool that runs well alongside any EDR agent.
        1. The other reason we are ingesting Sysmon logs is that the built-in Sigma rules we previously enabled largely depend on Sysmon logs as that is what most of them were written for.

c. You can snapshot this Windows version in case your windows get hosed later on, but this is optional.