threatER Enforce for WiFi Software ISO Installation Guide (Build 270+)

Updated, 8 September 2025

Table of Contents

Overview

threatER Enforce is our software stack that runs on a physical server or virtual machine. A physical server or virtual machine with the threatER Enforce software installed is referred to as an Enforcer. The threatER portal is our central cloud-management platform that is responsible for full cloud-based management of our solution.

This guide is suitable for use for threatER Enforce software releases with a Build number of 270 or higher.

This document describes the typical installation process when using a USB 3.0 thumb drive containing the threatER Enforce ISO image to install the threatER Enforce software on a physical server meeting minimum hardware requirements (as described later) or virtual machine (such as VMware or KVM).

If your intent is to deploy into AWS, Azure, or Google Cloud, you're reading the wrong document. Please contact our Customer Success team for applicable documentation for those environments.

Turnkey Shipments

Although this guide can be used to install our software on any hardware meeting our minimum specifications as described later, it may be useful to know which turnkey hardware that we ourselves ship after installing our software. Preinstalled systems are drop-shipped from our box build partner, and as of April 2025, we are currently sourcing the following types of fully built/installed systems:

- 1G Set-top Enforcer: Lanner NCA-1510D and Lanner NCA-1515A
    - Deployed as a bump on the wire, typically next to the ISP modem, often in a datacenter or IT closet
    - Passively cooled
    - One-pair NIC bypass support, copper only (no fiber)
    - Intel(R) Atom(TM) CPU C3758 @ 2.2GHz (8 core/8 thread for up to bidirectional 1Gbps performance)

- 10G Rack-mount Enforcer: Lanner NCA-5220
    - Deployed as a bump on the wire, typically next to the ISP modem, often in a datacenter or IT closet
    - Actively cooled by internal fans
    - NIC Bypass support
    - Fiber support available (MMF or SMF, specified at time of ordering, with bypass)
    - Intel(R) Xeon(R) E-2246G CPU @ 3.60GHz (6 core/12 threat for up to bidirectional 10Gbps performance)

- WiFi Enforcer: Lanner NCA-1040SEB
    - Deployed centrally in an office environment for best WiFi coverage
    - Intel(R) Celeron(R) J6412 @ 2.00GHz (4 core/4 thread for high-performing wired and WiFi performance)

Prerequisites / Installation System Requirements

If you wish to procure and install your own hardware instead of using our turnkey shipments, the rest of this guide will be useful for you. We'll start by describing the system requirements.

The physical or virtual machine you are installing must meet the following minimum set of system requirements:

CPU

In general, the target system must utilize a 64-bit Intel processor with at least 2 physical cores running at 2.2GHz or more in order to support bidirectional 1Gbps operation. More cores can of course be used, and the more that are used the faster system bootup will be, and software updates will also be faster as well.

When installing for WiFi, for the most performant system, 4 cores are strongly recommended @ 2GHz.

For bidirectional 10Gbps operation, at least 12 logical cores (generally implemented as 6 physical cores with hyperthreading, yielding 12 logical cores) running at least 2.9GHz are required.

RAM

For <= 1Gbps sustained bidirectional operation, your system must have at least 4GB of RAM installed. More RAM can be used. The more RAM that is made available, the larger the internal logs buffers will be, and the better overall system performance will be.

For up to 10Gbps of sustained bidirectional operation, your system must have at least 16GB of RAM installed, with 64GB **strongly recommended**. The more RAM that is made available, the larger the internal logs buffers will be, and the better overall system performance will be.

Important Note: The non-WiFi threatER Enforce software installations reserve a quantity of 2M system hugepages at startup. System hugepages should not be reserved via the linux command line nor should any other system process resident on the server utilize system hugepages.

Storage

For server deployments of all types (1G, 10G, WiFi, cloud, virtual, etc), a Solid-State Drive (SSD) is **required** for the installation target. It must be at least 32GB in size. Installations leveraging other storage types are not supported and may cause the system to drop packets or otherwise perform poorly.

NIC: WiFi Enforcers

threatER's WiFi Enforcers require at least one hardwired port for WAN connectivity. Other hardwired ports can be used as part of the protected bridge, for local hardwired LAN networks (such as printers, VoIP phones, other switches and routers, and so on).

Additionally, for proper WiFi operation, our WiFi Enforcer software requires that you utilize the **MEDIATEK Corp. MT7915E 802.11ax PCI Express Wireless Network Adapter**. No other media adapter is currently supported for WiFi operation.

Note that our turnkey hardware for our WiFi Enforcer is a variant of the Lanner NCA-1040SEB, which includes four hardwired ports (three LAN ports and one WAN port, as configured in OpenWrt), plus the aforementioned WiFi chipset.

Note that unlike our standard non-WiFi layer 2 Enforcers, DPDK is **not** used in our WiFi product, so there are no DPDK compatibility issues to be concerned with.

Requirement: Internet (All Enforcers)

You MUST have DHCP-enabled internet access for a non-WiFi Enforcer installation to succeed. In the case of the non-WiFi Enforcer, this is because of Ubuntu LTS installation requirements and the importance of being able to fetch the latest packages and security updates at install time. Prior to powering on the system to be installed, be sure to connect an Ethernet cable to the admin port on your installation target and make sure it is connected to a network with a DHCP server (so that it can pull the IP it will use at installation time for Internet-driven package pulls and security updates related to the underlying Ubuntu LTS operating system).

In the case of the WiFi Enforcer, you don't explicitly need an Internet connection to perform a WiFi install. A common approach would be to perform the ISO install, then point a browser to 192.168.1.1 via one of the LAN ports from a laptop for final provisioning by an end customer (which would typically be post-installation/post-shipment).

Serial Port or Video+Keyboard Access (All Enforcers)

For necessary interactions during the installation, you will need to have either 38400 baud serial port access or video+keyboard access to your target installation system.

Video+keyboard access is straightforward. If your target system includes a supported video connection, you can simply plug in a compatible monitor to your target system's video port, and plug in a USB keyboard, and off you go. **Note that DisplayPort video connections, if available, are NOT supported, so do not attempt to use them; if DisplayPort is the only available video connection, you should use the serial port access scheme as described below**.

If using serial port access, we recommend connecting to the serial port with a linux laptop, and leverage the popular `screen` utility. Use '`sudo apt update && sudo apt install screen`' if it is not already

installed on your host linux laptop. You can then connect a suitable USB serial port adapter between a USB port on your host laptop and the target system's serial port for access. **Be sure to investigate your target system's hardware user manual for information about its physical serial port connection requirements before purchasing a suitably matched USB serial port adapter from a third-party supplier (such as Amazon, Walmart, Target, Best Buy, and so forth), if that's the route you're taking.** Most of our own turnkey hardware shipments include a serial console adapter cable that is likely to work with most systems out-of-the-box, but be aware that you may require an alternative cabling type.

For reference, our own go-to command line invocation to use `screen` from a linux-enabled laptop is:

```
$ sudo screen -L -Logfile /tmp/screen.log -c ~/.screen-config /dev/ttyUSB0 38400
```

where `~/.screen-config` is a file with the following contents:

```
efscrollback 1024
ignorecase yes
bindkey -d -k kb stuff "\010"
```

You can use any popular Linux text editor of your choice (`vim`, `nano`, etc) to create that configuration file in your home directory.

Note that you are not forced to use a Linux laptop and/or screen to access the serial port. You can use other tools, as long as you know how to configure and use them. For example, we often see Windows users relying on the popular tool `putty`.

However, note that if you are using serial port access, you must configure the serial port baud rate in your BIOS settings for 38400 baud. The installer requires that all serial port access be at the rate of 38400 baud.

A Note on Turnkey Bypass Capability in Non-WiFi Enforcers

All of our turnkey non-WiFi systems currently support hardware-based network bypass. This ensures that in the event of a hardware fault (to include full power loss), traffic will still pass through. This means that Internet-based traffic will still flow, albeit unprotected until the hardware or power fault is rectified. For customers building out their own hardware, note that we can auto-detect and support bypass capability only for certain (but not necessarily all) Lanner, Supermicro, and (limited) Silicom hardware.

However, we like to point out that bypass can provide a false sense of security. Although it is true that traffic will still flow in the event of a failure, in the failure mode, traffic is completely unprotected. That's bad.

As such, for the **most** robust environments, we recommend a true HA arrangement so that a single point of failure (ie, a single server) is not introduced. Put another way, for customers providing their own hardware, if they have purchased a standard license and an additional HA license, a better design would be to turn up **two** physically identical systems, one in each existing HA path, neither utilizing bypass, and use standard industry HA failover techniques when a failure is detected by the customer's existing HA management scheme. We

have a separate document available from our Customer Success team describing the intricacies of HA environments as related to a proper security stack for customers who wish to consider best-practices options.

Note that the WiFi Enforcer, by virtue of the fact that it is not a bump in the wire in a critical IT path but is instead a straightforward WiFi router meant to connect WiFi endpoints, does not support bypass capability. We recommend a hot standby for WiFi deployments that can be rapidly enabled as needed in the event of a failure.

Installation Interactions and Connectivity

If you utilize a serial port (or if that is all your server has available) for configuration, be sure to go into your BIOS settings and make sure it is set for 38400 baud. No other installation baud rate is supported when using the installer in serial port mode. You must use 38400 baud.

In addition, ensure that the BIOS "Secure Boot" feature is disabled. The Enforce software utilizes several out-of-tree device drivers that require that Secure Boot be disabled. See the "Initial Lanner BIOS Configuration" section below.

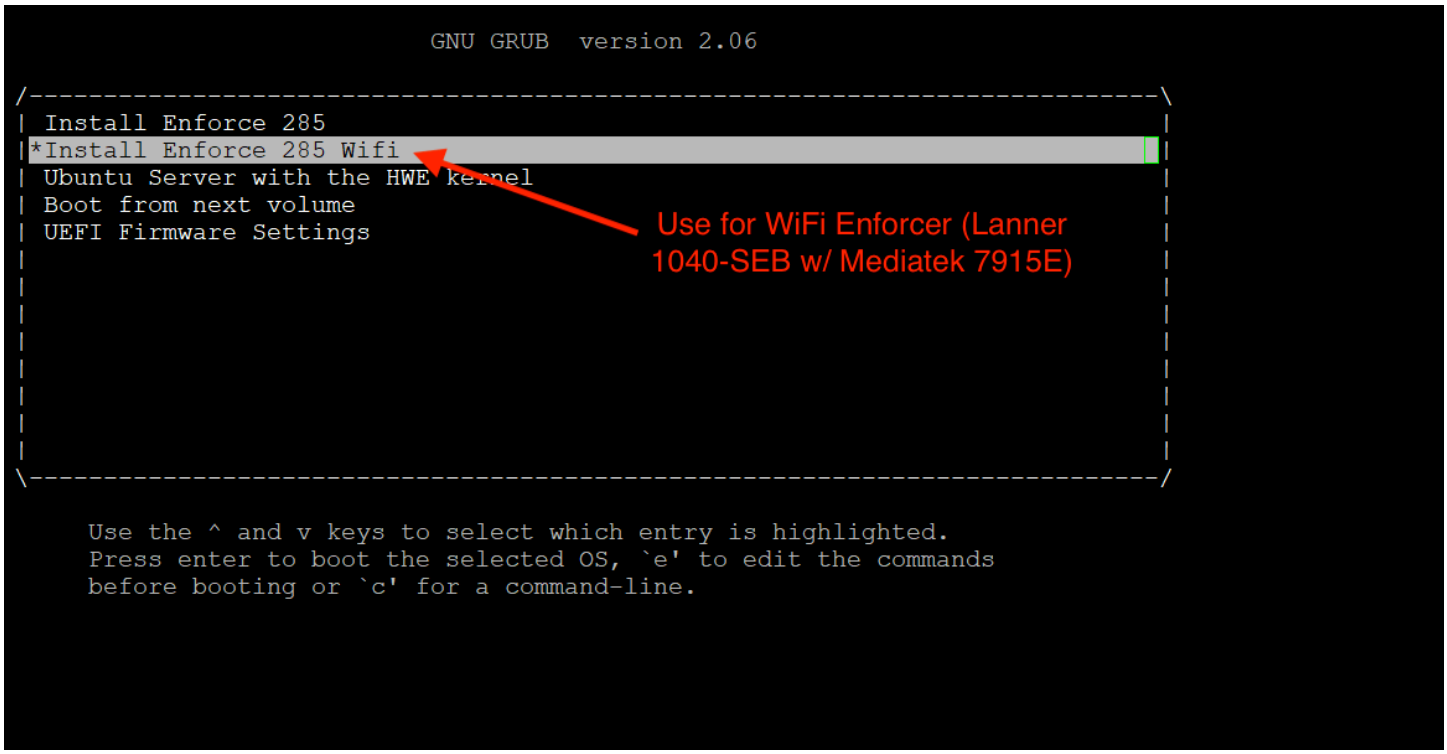
Note that for details on your specific BIOS screens and entry into those screen(s) on system power-up, you should refer to your manual(s) for the server you are installing on.

Many systems allow you to enter into the BIOS on power-up by repeatedly pressing the `Delete` key on your keyboard, but other systems require specific function key(s), for example, `F2` is commonly seen on some systems. Pay attention to your serial port or video output depending on your connection paradigm during power-up as most systems will display the BIOS screen connection detail very early in the boot process. Most systems give you only a few seconds to initiate BIOS screen activity.

USB Installation Procedure (All Enforcers)

The same threatER Enforce ISO Installer is used for both our layer 2 bump in the wire architectures as well as our WiFi Enforcer architecture. An initial menu allows you to choose which you are installing, either our standard installer, or if you are targeting supported WiFi hardware, the WiFi installer.

The initial menu you see when the USB installer runs will allow you to choose between the two. There is purposely no timeout on this menu. You must choose one to match the target system that you are deploying on:



The installation is fully automated to the extent reasonable, but there are several important procedural steps that you must follow. Additionally, there are a few menu selections and interactions that will occur that you will need to provide answers for throughout the process. These are all documented in the sections that follow.

For directions on creating a USB installer, please see the documentation in our Knowledge Base. You can also download the ISO file for our latest software release from our public Dropbox folder.

Configure BIOS for USB Booting (All Enforcers)

Your server must have an available bootable USB port. Although it is possible to boot from USB 2.0 ports, for the fastest possible installation times, we generally **recommend using a USB 3.0 port (and therefore a USB 3.0 compliant thumb drive housing our ISO image)** if available.

There are color coding conventions for USB connectors. USB connectors having a blue tongue support USB 3.0 transfer feeds, and teal blue support USB 3.1 transfer speeds, so for fastest operation, you should use a blue or teal blue port. Ports with a white or black tongue run at much slower USB speeds.

Many servers have such ports both in the front and the rear of the unit, however, some support booting only from rear ports. Consult the manuals for your target system so that you know whether or not any special scenarios apply to you. In general, we recommend that you boot from rear ports, as those are most likely to work out-of-the-box for booting on most systems.

Before powering on the system, ensure that you have done the following. All of these are required. **The installation will not succeed if you do not ensure that you have:**

1. With the server initially powered off,
2. Insert the USB containing threatER Enforce ISO image into a bootable USB port,
3. Connect an ethernet cable from the desired administration port (or the WAN port for a WiFi Enforcer) on the system being installed to a network switch in your environment that is capable of serving a DHCP IP for Internet access,
4. Connect to the target device's serial port at 38400 baud **or** use a supported video+keyboard (note: DisplayPort is **NOT** supported) connection arrangement, and,
5. Last but not least power on the system by pressing its power button, paying attention to either the serial port output or the video output as applicable, so that you can enter your system's BIOS settings screens to select the threatER Enforce ISO Installation USB to boot from.

Note that for details on your specific BIOS screens and entry into those screen(s) on system power-up, you should refer to your manual(s) for the server you are installing on.

*Legacy BIOS vs. UEFI/EFI Support (**UEFI Strongly Recommended/Preferred, and in Some Cases, Required**) (All Enforcers)*

The threatER WiFi Enforcer installation requires UEFI support. Legacy BIOS modes are not supported and cannot be used.

The standard/non-WiFi threatER Enforce ISO Installer attempts to support both legacy BIOS and UEFI/EFI modes of operation, however, BIOS modes are being deprecated by modern software (including Linux operating systems) in favor of UEFI, and as such, it is possible that BIOS boot modes will not function on some systems with the USB thumb drive installer. The mode of operation of your system at boot-up time is generally able to be set in the BIOS screens which you can navigate to on power-on. For details, consult the hardware user manual for your particular target hardware.

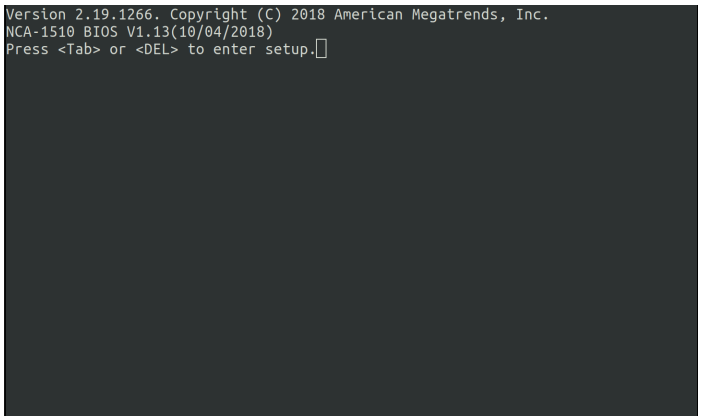
We strongly recommend that you select UEFI mode from your BIOS boot screen configuration. It is possible on some systems to attempt to install in a BIOS-only non-UEFI environment, but if it fails for any reason, your next step should be to reattempt the install after configuring your BIOS to use UEFI mode. If the hardware you are attempting to install on fails using BIOS mode and it does not support UEFI mode, you will need to procure different hardware to install on using UEFI mode.

Initial Lanner BIOS Configuration (All Enforcers)

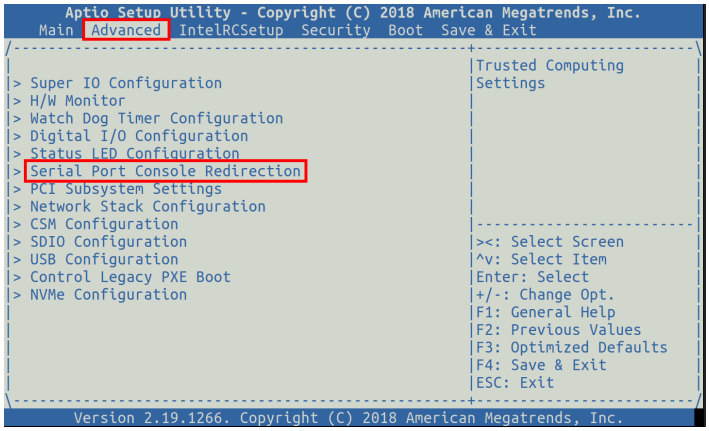
If you are performing the initial installation on a turnkey Lanner, you will need to follow the instructions below to configure the required BIOS settings. If you are reinstalling the software on an appliance that has already hosted the Enforce software, you may skip to the next section.

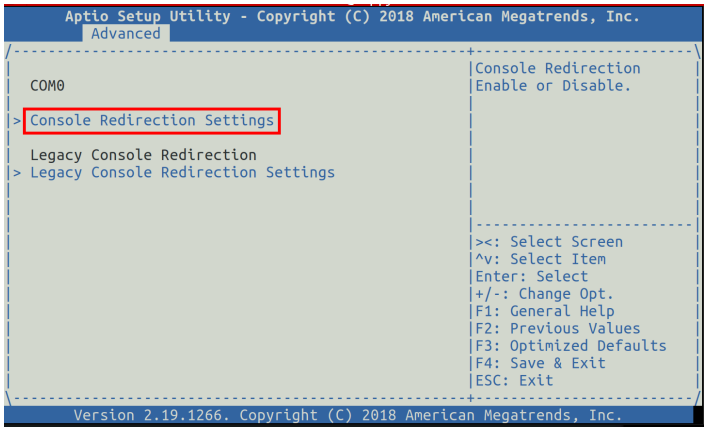
Some of the default BIOS settings in Lanner deployments need to be updated before the initial install. Specifically, the default serial console speed and the boot mode need to be updated.

Connect the USB/Serial console cable, start the serial console program with the speed set to **115200**, and power on the Lanner. Press **<TAB>** or **<DEL>** to enter the BIOS when prompted.

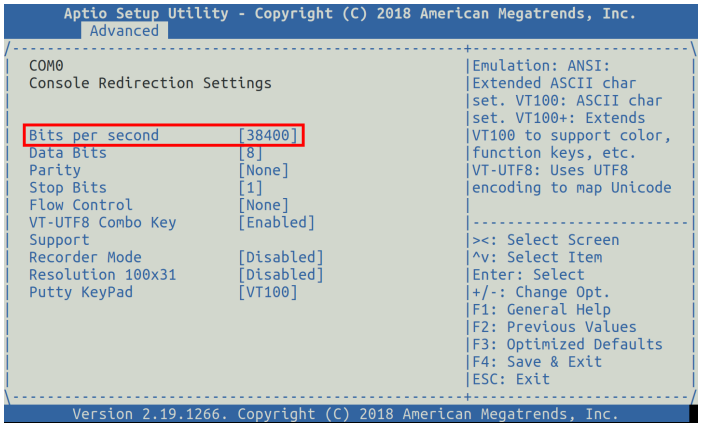


Under the "`Advanced`" tab, select "`Serial Port Console Redirection`", then select "`Console Redirection Settings`".

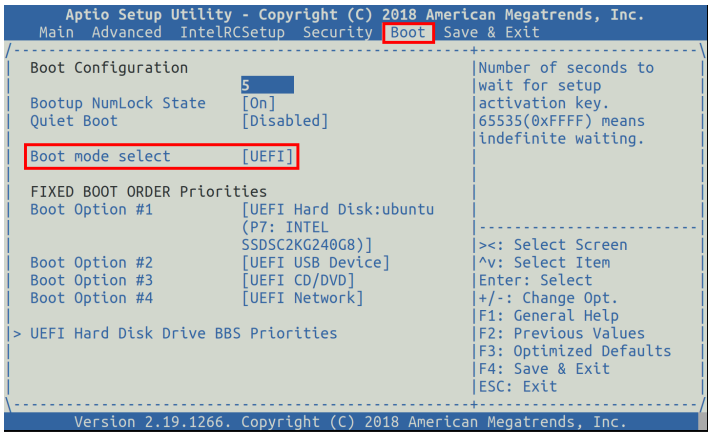


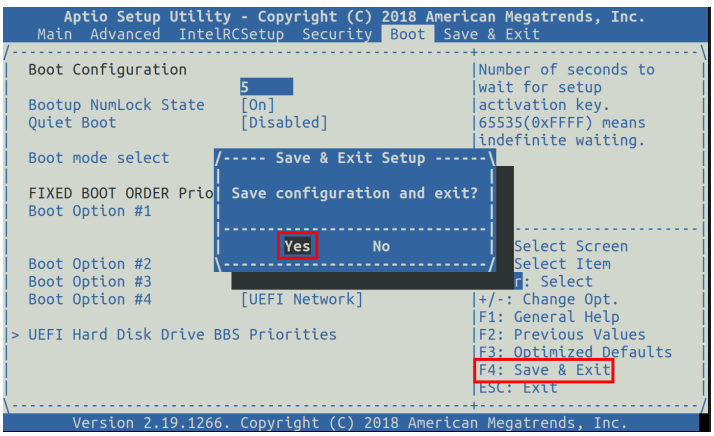


Change "Bits per second" to "38400".



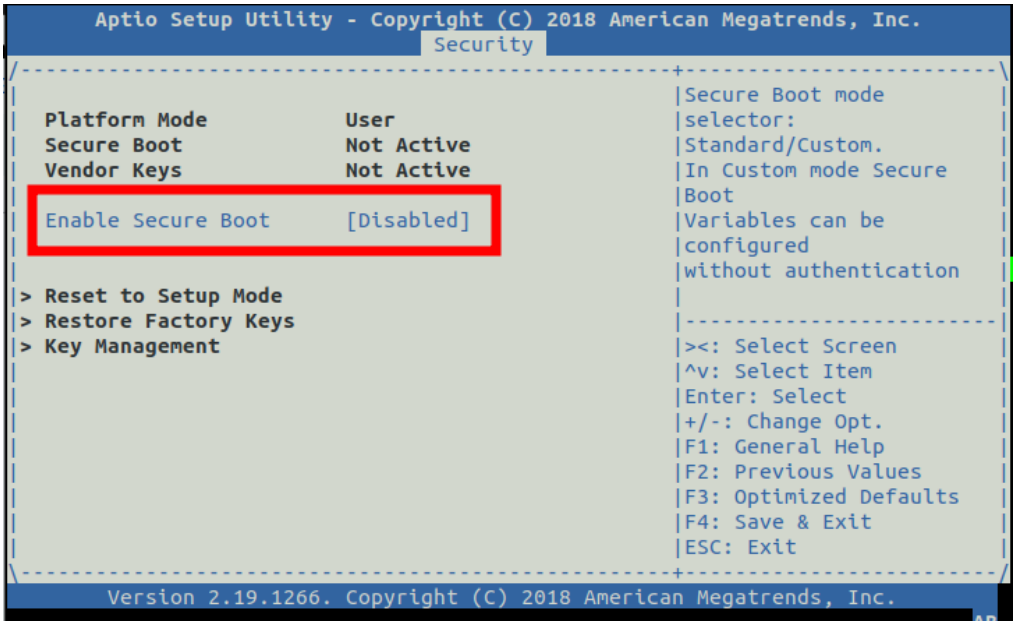
Press **<ESC>** two times to get back to the main menu. Select the "Boot" tab, and change "Boot mode select" to "UEFI". Then press **F4** to "Save and Exit" and select "Yes".





After saving the BIOS settings, exit the serial console program you are using and restart it with the speed set to **38400**. Now that all the serial console settings are 38400 and UEFI mode is configured, you can continue with the install with confidence.

Lastly navigate back to the main menu and select “Security” and ensure that “Secure Boot” is disabled. Both the non-WiFi Enforcer and the WiFi Enforcer require that Secure Boot be disabled prior to beginning installation.



Initial Menu and Type Selection (All Enforcers)

For a 38400 serial port install, after you have properly configured your BIOS for a serial port baud rate of 38400 baud, for USB booting, and powered the system on, you will see a simple menu resembling the following:

You must choose the proper installer for your target system. There is no timeout period on this screen, so you are forced to choose the one that you want.

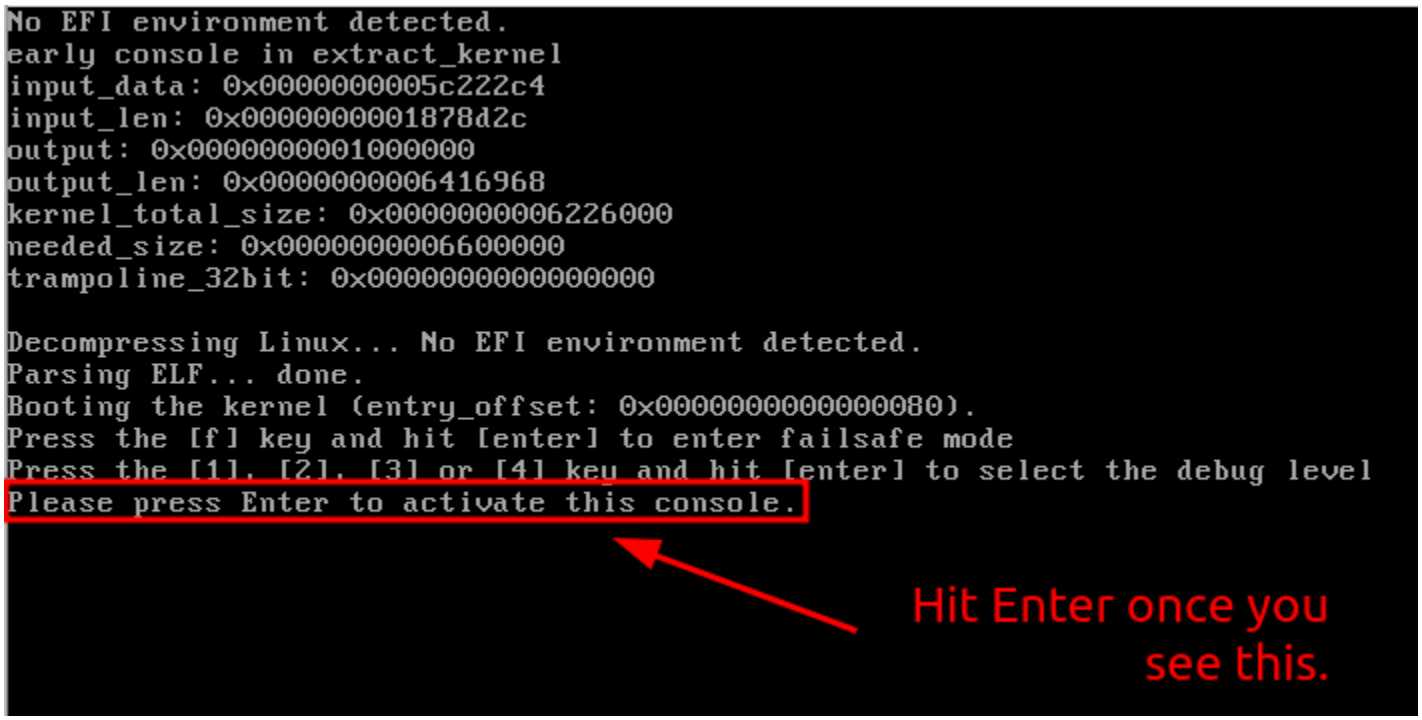
For the standard (non-WiFi) Enforcer installation flow, please use the [threatER Enforce - Software ISO Installation Guide].

Selection: WiFi Enforcer Installation Flow (Second GRUB Row)

The WiFi installer will analyze your system and install the proper OpenWrt image and then layer on Threater's software.

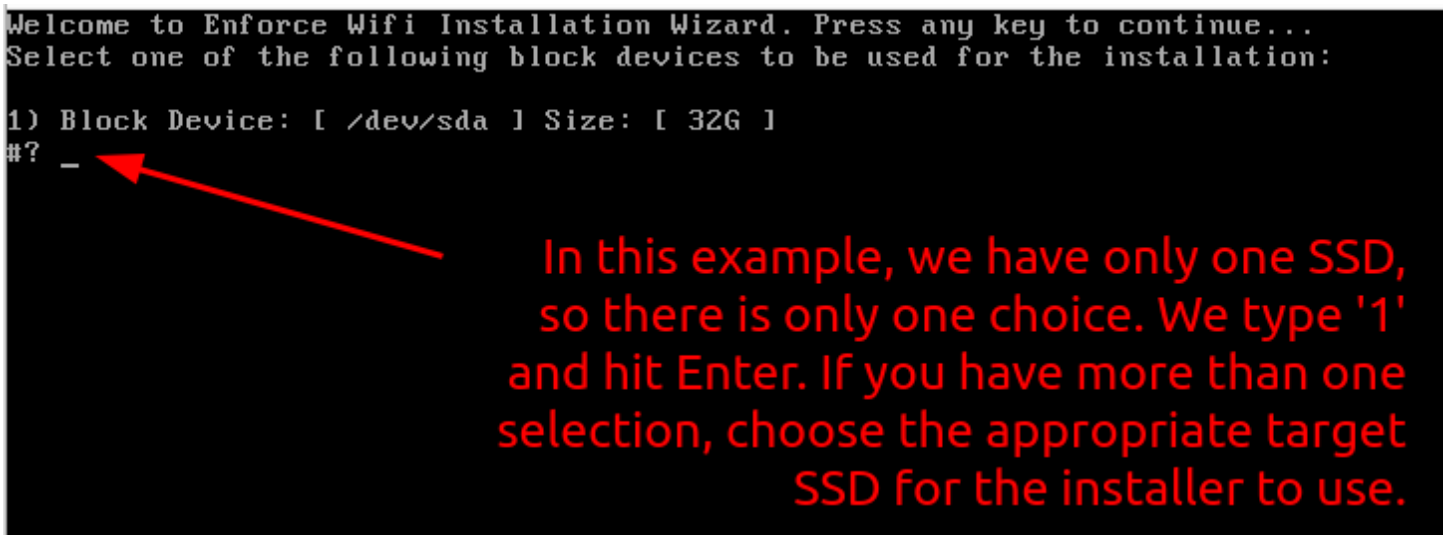
If you are selecting the WiFi installer, you are likely targeting the Lanner 1040-SEB, since as of the time this section of the document was updated, that was the only supported turnkey system for our WiFi Enforcer installation.

As soon as you select the 'Install Enforce XXX Wifi' option, you'll see the following screen, be patient, and you'll eventually see the highlighted line:

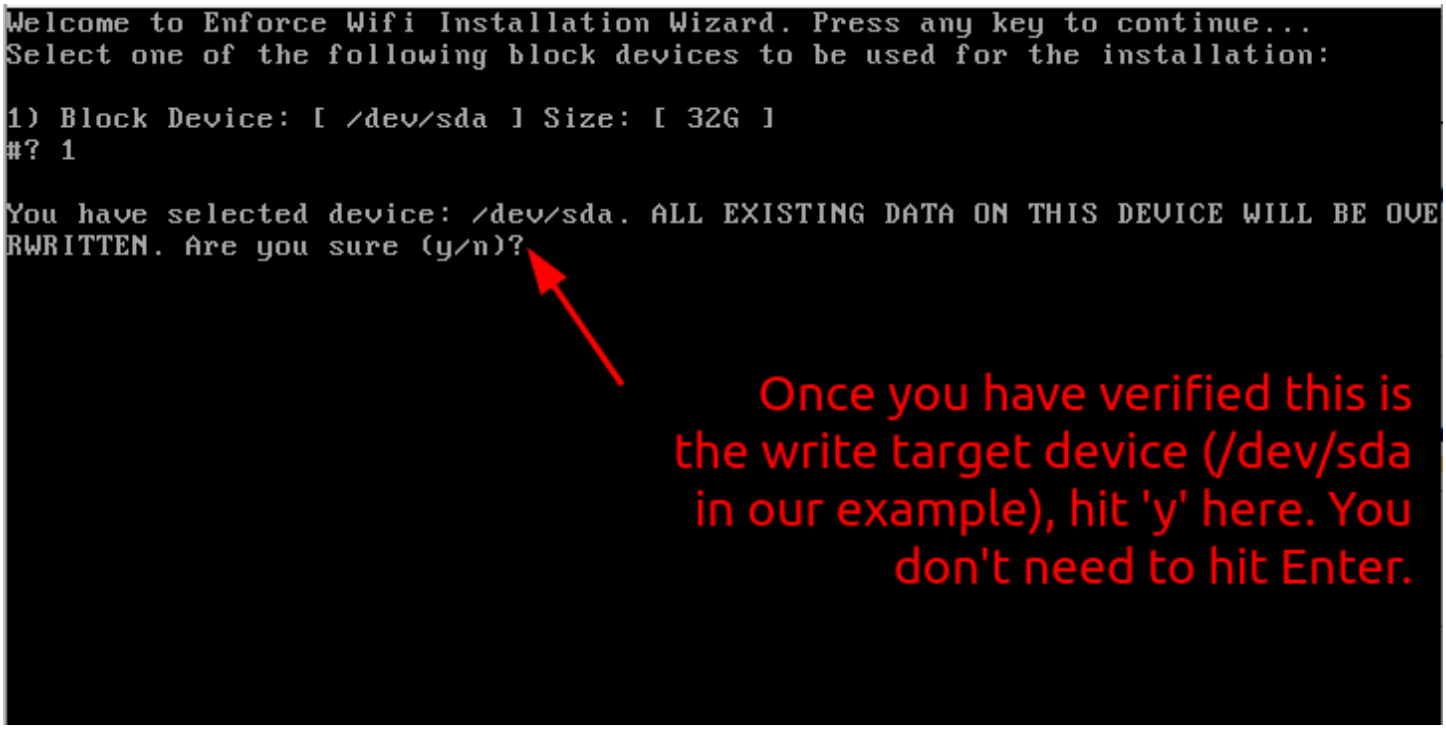


Once you see that line, hit the `Enter` key, and the Enforce WiFi installation wizard will commence. You will then see the following welcome line:

Hit `Enter` again to continue. You will then see a list of block devices that the software can be installed on. You should select the desired SSD target for the installer to use:

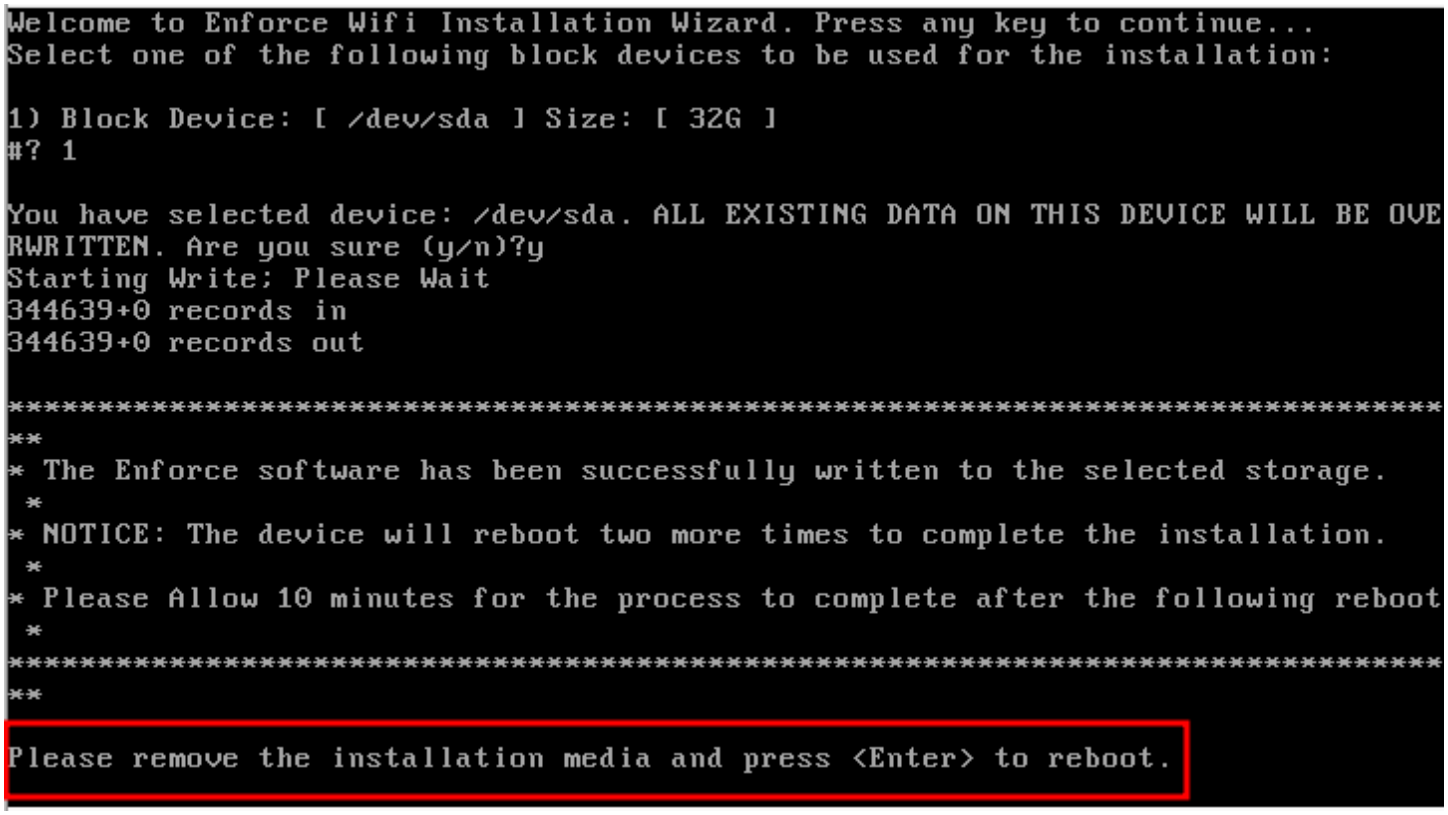


You will be presented with a short question so that you can positively acknowledge that you have chosen the correct SSD, since the installer will completely overwrite it. That is, this is a 100% destructive operation, so be sure that you have chosen correctly:



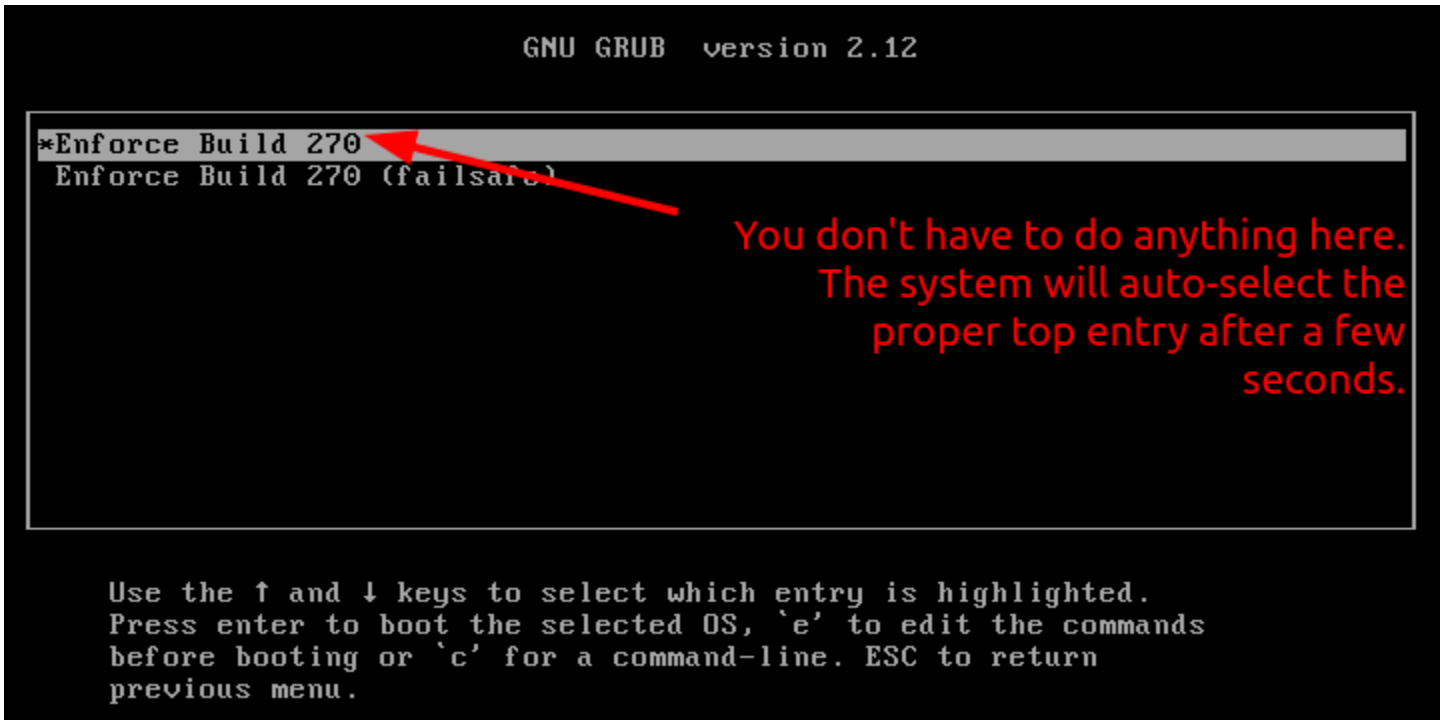
Once you have verified that the select is the correct target, hit the '`y`' key. You do not need to hit `Enter`.

After all initial installation write operations complete to the target device, you will see the following screen, highlighting that it is time to remove the USB installation media and press Enter to reboot:



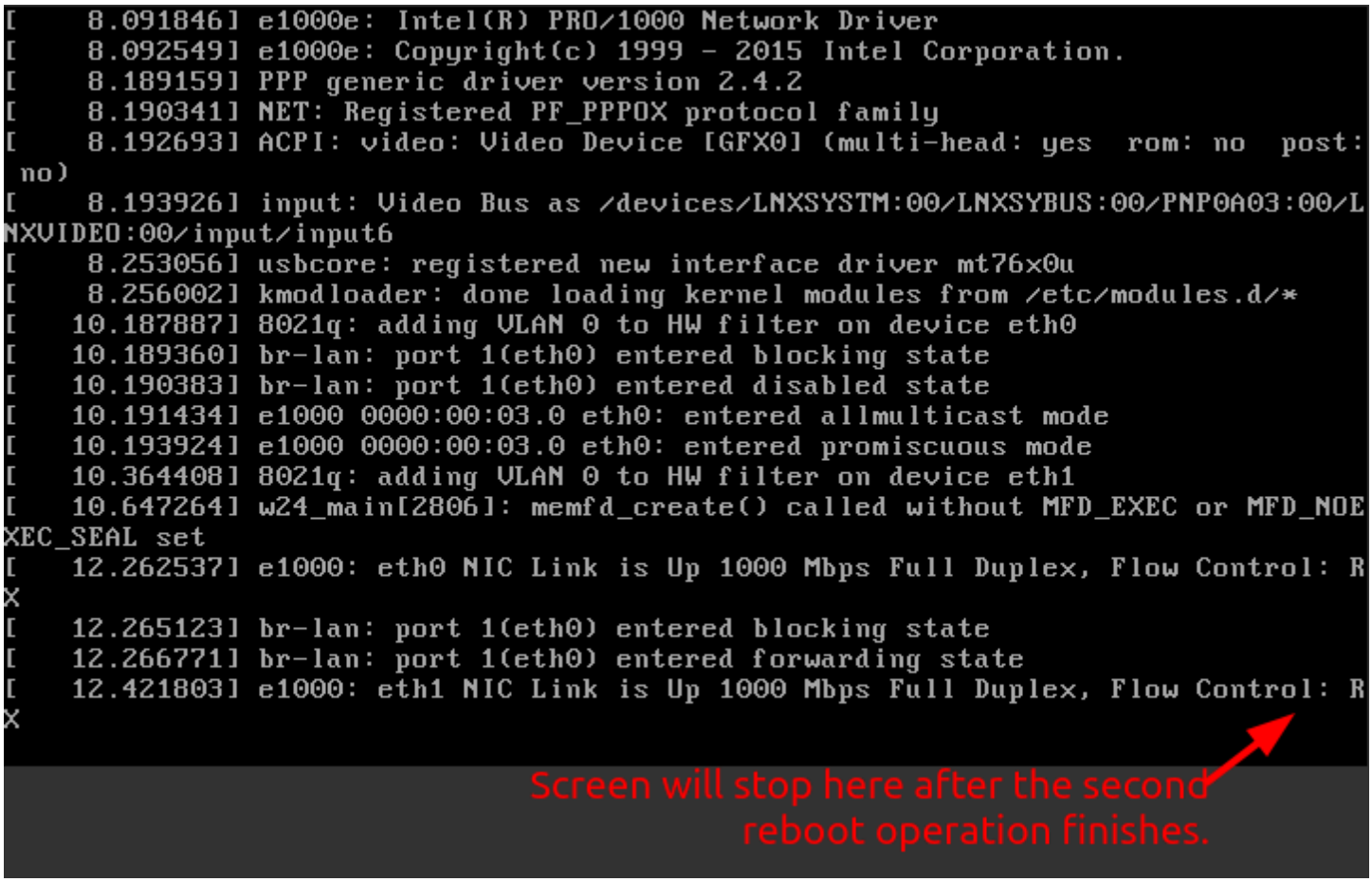
Remove the USB installer now, and then hit `Enter` to reboot. **Per the notice shown above, after you remove the media and reboot, the system will continue the installation and will subsequently reboot two more times during the ensuing process.**

You may see a screen come up briefly that lists both the installation build number as well as a failsafe build number - this screen will timeout quickly (after a few seconds) so you don't have to hit any key (unless you're impatient and don't want to wait the 3 seconds, then go ahead and select the top one):

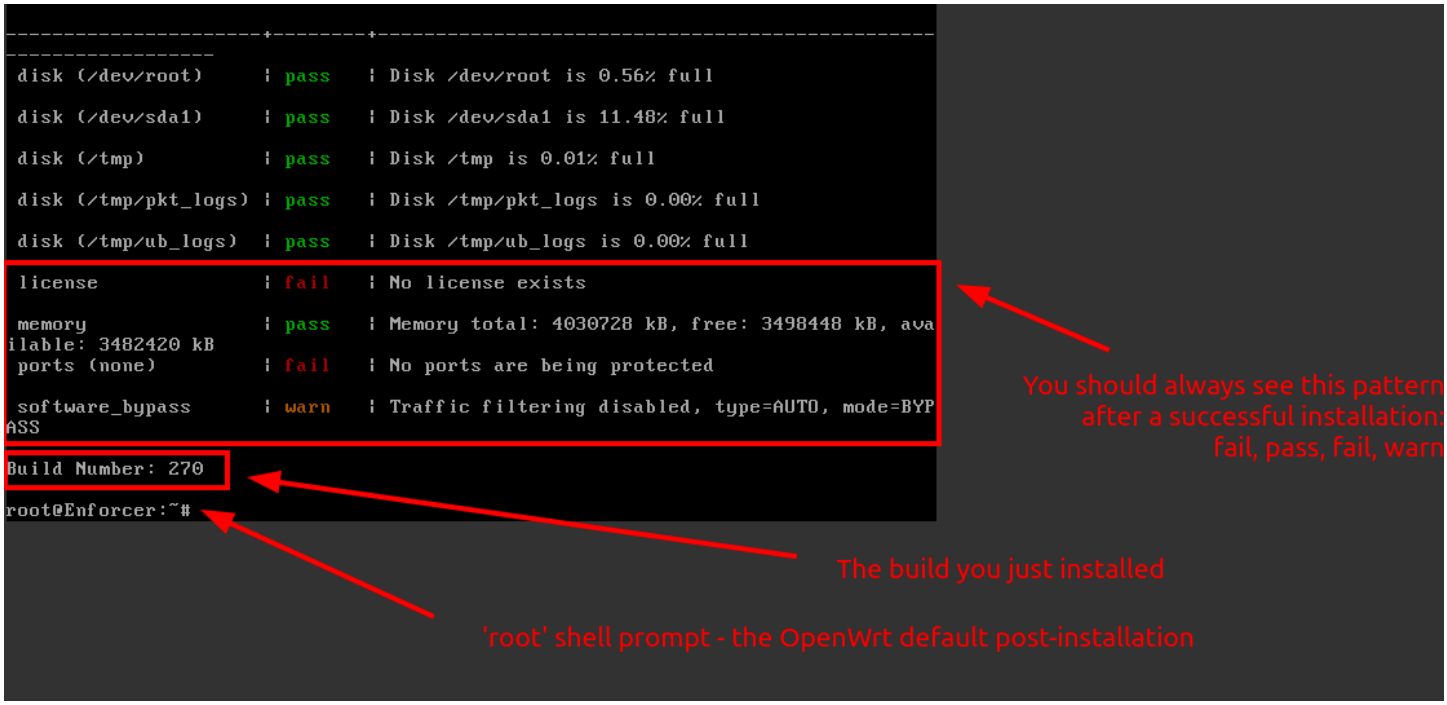


The system will now undergo several automated steps to include the **two additional reboots** as it automatically extends and resizes partitions. You'll see some messages that it is working and notices in ALL CAPS that it will be resizing, repartitioning and rebooting. Be patient as it does so. Each time you'll see the screen shown above reappear and the system will auto-select and continue. You do not need to do anything - you just need to wait. The process will complete within a few minutes.

After the second reboot finishes, you'll see information similar to what is shown below, and it will appear that the screen has stopped (a good rule of thumb is to make sure you see this for 10 seconds or so with no other activity, if you haven't been paying attention to the reboot messages):



You can now hit Enter and you will be logged into the serial console as the root user:



At this point, the installation is finished. You will see the fail / pass / fail / warn status and the build number that you successfully installed. Those statuses will stay that way until the final configuration and activation is done by the end user at a later time. You should now safely powerdown the system by typing the `poweroff` command and hitting `Enter`:

The system will then shut down.

It can now be packaged up for shipment. Or, if you are the end customer, you can proceed with our standard Onboarding flow, as documented in our Knowledge Base and run by our Customer Success team.

You can skip the next several sections that detail the non-WiFi Enforcer installation, as that does not apply to you, as you've just installed the WiFi Enforcer. You can pick back up at the section **Factory Settings Detail**.

Factory Settings Detail

For reference, after power down occurs as described above post-installation for both the WiFi and non-WiFi installation modes, the next time the system powers up it will have the following factory default settings.

Specifically, these are:

- For non-WiFi installs (leveraging Ubuntu LTS):
  - The default administration port networking will have been set to an initial static IP of `192.168.1.1/24`,
  - The pre-configured default primary name server is `8.8.8.8` (Google DNS) and the secondary is `1.1.1.1` (Cloudflare DNS).
  - The default user login and password for SSH access (where applicable) remain `ubuntu` and `enforce`, respectively. (It is recommended that the end user change this behavior to suit their security needs during onboarding.)
- For WiFi installs (leveraging OpenWrt):
  - For turnkey Lanner 1040-SEB hardware:
    - The WAN port will generally be the 'highest' numbered port: Port 4 (which maps internally to eth3 [since the internal port naming convention is eth0, eth1, eth2, eth3]). It will pull DHCP for its WAN-side IP address. The default DNS will be as advertised by the DHCP peer.
    - The remaining ports (Port 1, Port 2, and Port 3, aka, eth0, eth1, and eth2) and the WiFi are bridged for LAN access.
    - Two default SSIDs are created: Enforce_5G and Enforce_2G
    - The default security profile is WPA2-PSK for both, with an eight-character initial key/password of: **`enforce!`**
  - The default user login and password for SSH and HTTPS access (where applicable) are `root` and `enforce`, respectively. (It is recommended that the end user change this behavior to suit their security needs during onboarding.)
  - The serial port console when initially connected has no login. This guarantees immediate `root` access after installation. (It is recommended that the end user change this behavior to suit their security needs during onboarding.)
- It is **strongly** advised that the **end customer** modify the default user credentials as the very first step in the onboarding process, and certainly before insertion into their production network. **Failing to do this introduces your organization to a serious security risk, especially from an insider threat poking around using factory default access credentials.** Make sure to use a strong password that you will not forget and/or store it in a safe place. There is no way for our Customer Success team to recover passwords that you forget. That means that if you lose your password, you will need to reinstall the software from the USB ISO image.

Post-Installation Onboarding

After a successful installation and shipment, the next step is typically to have an Onboarding session with one of our Customer Success team members, to ensure that you are able to activate the software and correctly connect to our cloud-based management portal. This ensures that any policy, threat, and general list detail are being delivered properly in real-time to your newly installed threatER Enforce software.

In the case of WiFi, it also helps you with any specific WiFi configuration you might desire. Although we at Threater can certainly assist with some WiFi considerations, note that all WiFi-specific configuration details are stock OpenWrt (we purposely don't mess with the stock WiFi support in OpenWrt), which affords a very large and helpful online support system.

We strongly recommend that if this is your first threatER Enforce software deployment, that you contact our Customer Success team and go through an Onboarding session with them so that you can be assured that your configuration is complete and correct and you are well-protected before installing the unit into your production network.

Serial port connectivity via a laptop for onboarding is the generally recommended approach for seamless and straightforward initial configuration, although in some cases, it is possible to use a laptop with an ethernet cable connected where the laptop's IP address is manually set to a static value of something on the same subnet as the software's default IP of 192.168.1.1/24. Assigning a manual, temporary IP such as 192.168.1.2 with a 24-bit subnet mask of 255.255.255.0 to your laptop would suffice, for example. Or, in the case of WiFi, simply connecting to the default WiFi SSID which subsequently allows you to target 192.168.1.1 via a browser or an SSH session can also suffice.

In general, the Onboarding team will walk you through the policy and list configuration in our cloud-based portal, and also walk you through threatER Enforce configuration (such as configuring default networking, first-time device activation by entering your threatER portal credentials, license assignment, changing default password access, adjusting your hostname, setting up syslog exports, mapping resource and service groups, and so on).

When you work with our Onboarding team, they will typically need an employee on your side with direct local access to the device for proper initial IP assignment and access. After the networking configuration is completed to match your environment, you should be able to remotely access the secure web-based UI via https from a web browser, assuming you have a properly architected IT environment with admin-side access capabilities (such as perhaps via a pre-existing VPN from which you access administration ports on your other IT infrastructure).

Once reachable, the default credentials for login to the threatER Enforce software's non-WiFi https web-based UI are a username of `admin` with password `admin`. The default ssh login is `ubuntu` with password `enforce`.

For WiFi installations, the default https and ssh credentials are the same: the username is `root` and the password is `enforce`.

We strongly recommend that the end customer change all default credentials during initial onboarding.

Post-Onboarding Deployment Strategies

Once you have completed your threatER Enforce software installation and your onboarding session, it's time to deploy our solution into your network.

WiFi Deployment Strategy

Deploying our WiFi Enforcer is trivial.

The ideal deployment will be centralized with respect to your workforce and endpoints who will be connecting to the WiFi, for best possible WiFi coverage.

For most small offices, that kind of coverage will likely suffice. For cases where you require more WiFi coverage, you can use any kind of other WiFi access in range to extend the network. This can be via existing networks you already have in place or even cheap additional third-party WiFi routers that you might procure from elsewhere, such as Amazon. As long as those additional routers can see and connect to the SSID(s) broadcast by our WiFi Enforcer, they can be used. Alternatively, and for better far-reach performance, consider the use of hardwired infrastructure to connect your various WiFi points in more performant fashion.

In a proper architecture, you will only ever need "one" threatER WiFi Enforcer per location (although you may wish to procure a hot spare to keep on standby, of course, in the event of a hardware failure).

Outside of plugging in power, you'll generally run a physical Ethernet cable from the WiFi Enforcer's WAN port to your ISP modem and/or wall jack where 'Internet' is made available.

If you have hardwired infrastructure in need of protection, such as an office printer, Internet-enabled TV(s), or VoIP phones or other similar things, you can use the hardwired LAN ports, or of course you can use an existing switch and then run a single Ethernet cable from that switch to our WiFi Enforcer. Any and all connections to any of the LAN ports or the WiFi are always protected by your lists and policies as configured in our SaaS-based management portal.