threatER Enforce 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: Non-WiFi Enforcers

At least three NIC ports are required to be installed for the software to function properly for a non-WiFi Enforcer:

NIC port 1 - administration: the first port is for administration access, and should be attached to a protected-side network switch with DHCP access to the Internet. **This port must be connected prior to commencing an ISO installation, or the installation will not complete correctly.**

NIC port 2 - inside: this is the inside port for the layer 2 bridge (bump-in-a-wire). Once in production, it should be connected to your inside protected traffic. **Leave this port unconnected during the install.** You don't need to connect this port until you are ready to put the device inline in your production network post-installation. **The port must be supported by our installation of DPDK in order for it to be included as part of the bridging pair.** For our stock hardware offerings, this is always the case, but if you are bringing your own hardware, be sure to make sure your NICs are supported by DPDK before attempting to use them. You'll need to do some investigation to discover if your NIC hardware is supported. See our DPDK section below for more information.

NIC port 3 - outside: this is the outside port for the layer 2 bridge (bump-in-a-wire). Once in production, it should be connected to your outside network. **Leave this port unconnected during the install.** You don't need to connect this port until you are ready to put the device inline in your production network post-installation. **The port must be supported by our installation of DPDK in order for it to be included as part of the bridging pair.** For our stock hardware offerings, this is always the case, but if you are bringing your own hardware, be sure to make sure your NICs are supported by DPDK before attempting to use them. You'll need to do some investigation to discover if your NIC hardware is supported. See our DPDK section below for more information.

DPDK Support: Non-WiFi Enforcer NIC Requirement

threatER's Enforce software running in non-WiFi deployments support any Network card that utilizes one of the 6 Intel drivers listed below. Customers should therefore ensure that any NIC they intend to use alongside our software is leveraging a controller/driver set listed below.

- ixgbe: Any derivative of the following controllers: 82598, 82599, X520, X540, X550.
- igb: Any derivative of the following controllers: 82573, 82576, 82580, I210, I211, I350, I354, DH89xx.
- i40e: Any derivative of the following controllers: X710, XL710, X722, XXV710
- igc: Any derivative of the following controllers: I225, I226
- e1000e: Any derivative of the following controllers: 82571, 82572, 82573, 82574, 82583, ICH8, ICH9, ICH10, PCH, PCH2, I217, I218, I219
- e1000: Any derivative of the following controllers: 82540, 82545, 82546

To check compatibility of a network interface card (NIC), we recommend looking up the onboard controller type from your NIC's datasheet (or by contacting the vendor if they don't supply the information on their datasheet) in order to ensure that it is one of the above. For example, we have utilized a variety of NIC cards from Silicom in past systems which typically uses the Intel 82599 controller, which results in DPDK leveraging the supported ixgbe driver alongside it.

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.

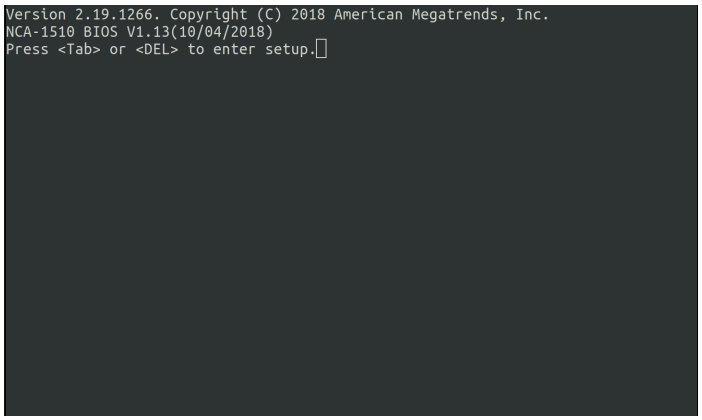
We strongly recommend that you select UEFI mode from your BIOS boot screen configuration. It is possible on some systems to attempt to install in a BIOS-only non-UEFI environment, but if it fails for any reason, your next step should be to reattempt the install after configuring your BIOS to use UEFI 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)

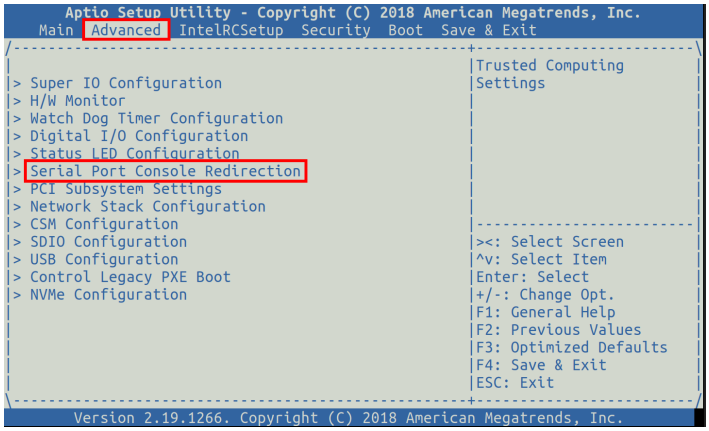
If you are performing the initial installation on a turnkey Lanner, you will need to follow the instructions below to configure the required BIOS settings. If you are reinstalling the software on an appliance that has already hosted the Enforce software, you may skip to the next section.

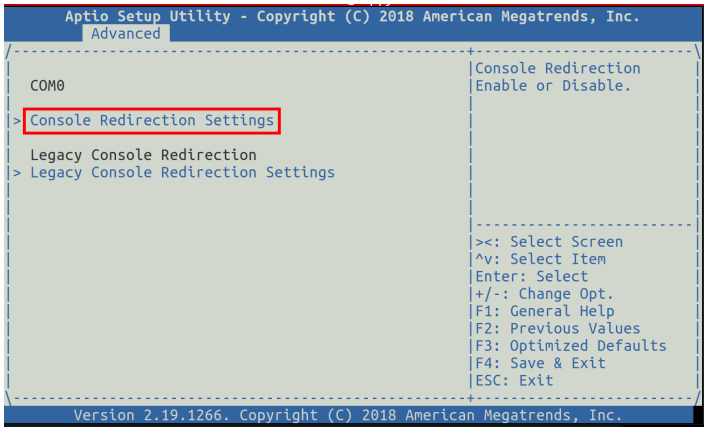
Some of the default BIOS settings in Lanner deployments need to be updated before the initial install. Specifically, the default serial console speed and the boot mode need to be updated.

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.

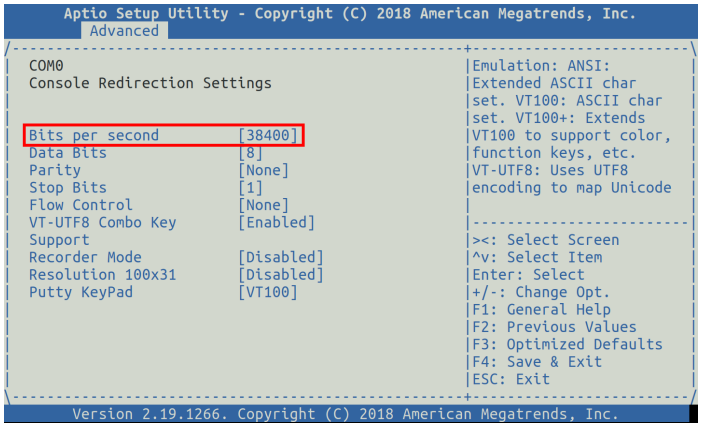


Under the "`Advanced`" tab, select "`Serial Port Console Redirection`", then select "`Console Redirection Settings`".

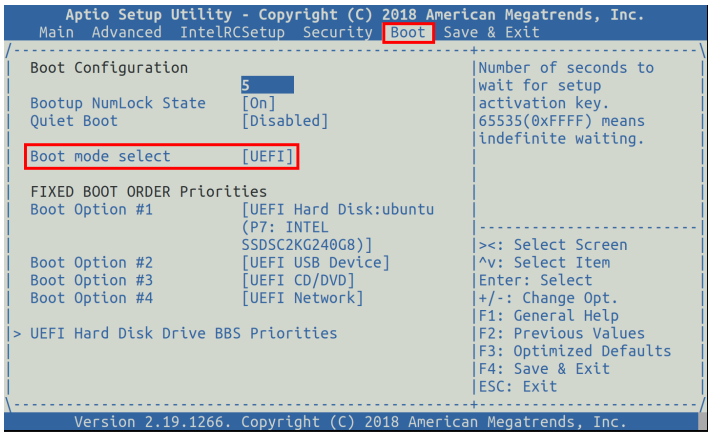


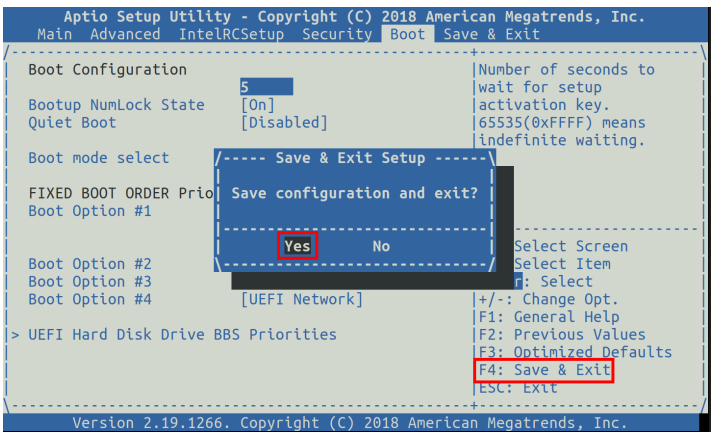


Change "Bits per second" to "38400".



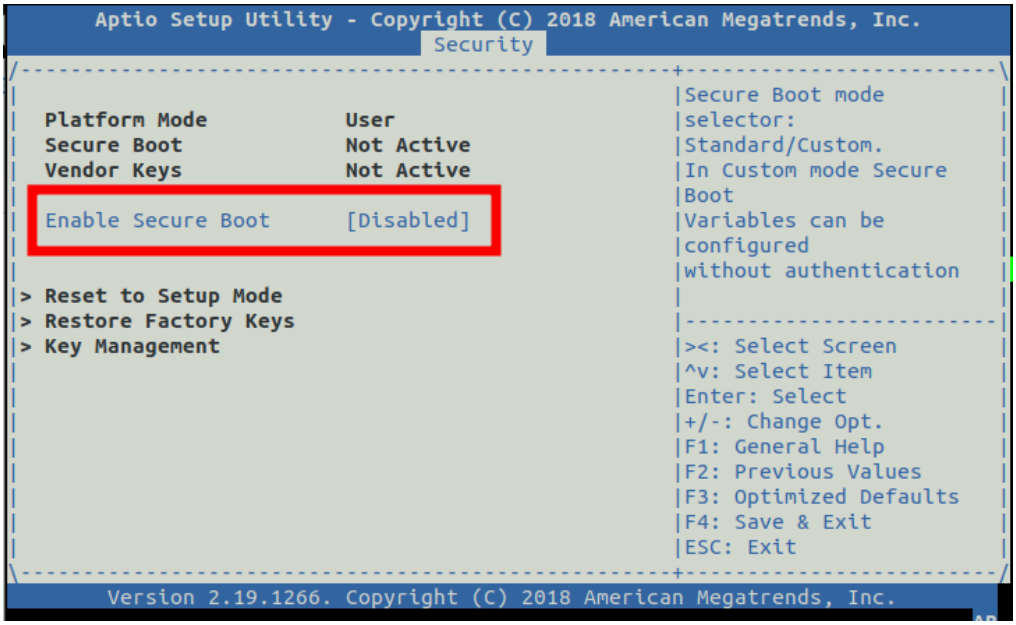
Press **<ESC>** two times to get back to the main menu. Select the "Boot" tab, and change "Boot mode select" to "UEFI". Then press **F4** to "Save and Exit" and select "Yes".





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.

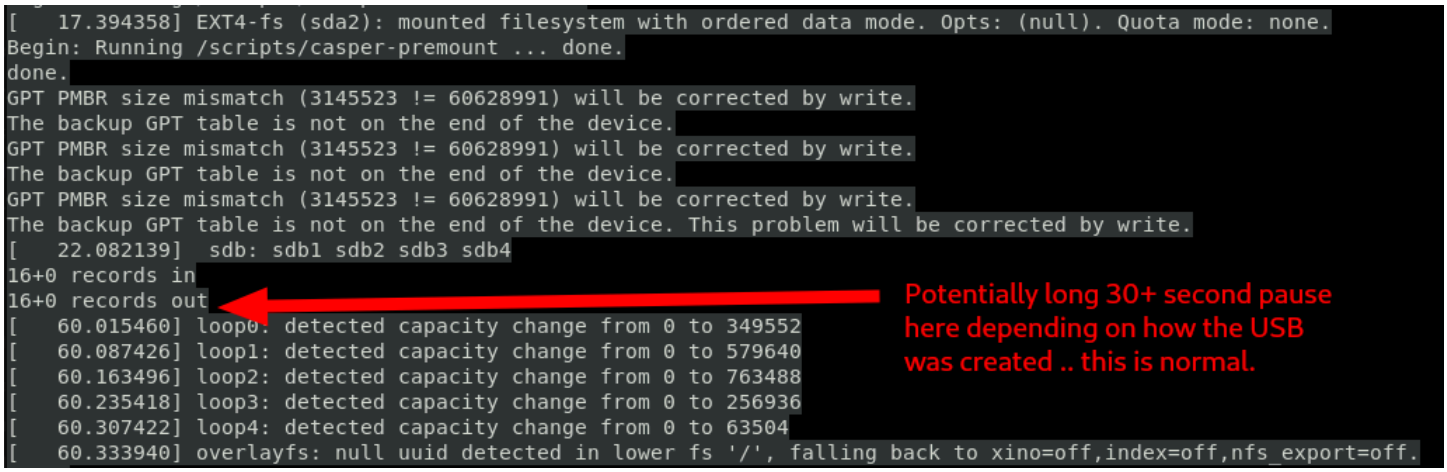
To follow the WiFi Enforcer installation flow, please use the threatER Enforce for WiFi - Software ISO Installation Guide.

Selection: Standard (Non-WiFi) Installation Flow (First GRUB Row)

When targeting our traditional deployment (such as on a Lanner NCA-1510D or Lanner NCA-5220 or similar), the standard installer will analyze your system and install the proper Ubuntu LTS image and then layer on Threater's software. Note that this is a very different flow than our WiFi Enforcer flow, since the underlying operating systems are quite different. In the case of the WiFi Enforcer, OpenWrt is the operating system of record, whereas in the traditional deployment, Ubuntu LTS is the operating system of record.

On some systems, once the standard installation starts, the screen may go dark for up to 30 seconds. This is completely normal. Be patient.

Eventually, some log messages will scroll on the screen - **be patient**, as the installer is basically doing a significant amount of background analysis of your system. You may even notice several long pauses to the tune of 30 seconds each or more. This is entirely normal. One example (amongst many possible scenarios of similar bootup delays) on the standard (non-WiFi) installer is:



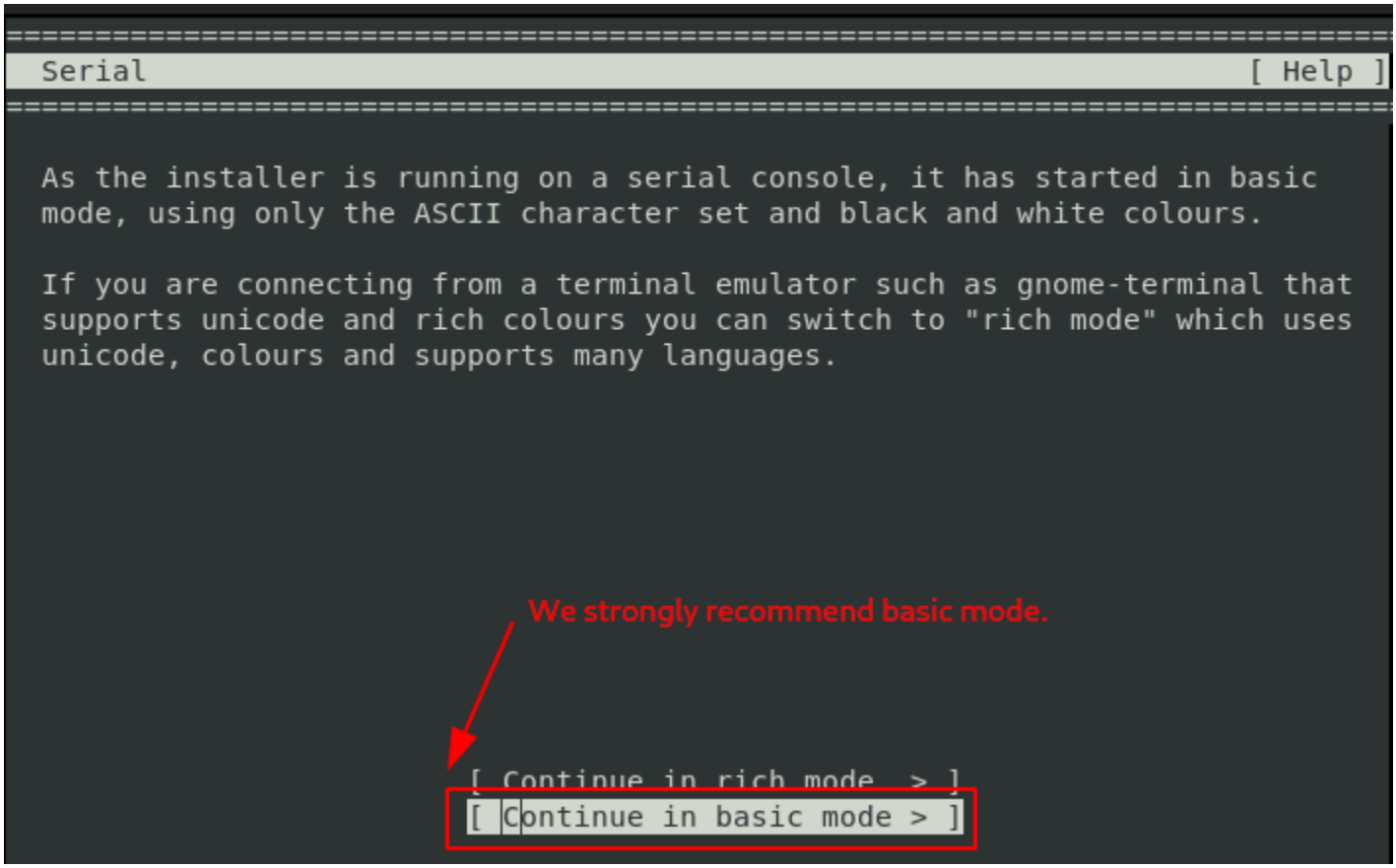
You may also see a variety of messages that may look like error messages - these are entirely normal as well. They are artifacts of the hoops the underlying Linux infrastructure has to go through for a variety of arbitrary hardware compatibility reasons.

Be patient, and the Linux detection and initialization process will eventually complete, and you'll then see the various menus as described in the remainder of this document.

Serial Mode Selection

If you used serial mode (and only if you used serial mode), you'll eventually be presented with a menu asking you whether you wish to proceed in "`rich mode`" or "`basic mode`". You will not see this menu in the keyboard + video mode.

You are at liberty to choose either serial setting depending on your serial terminal type, although we strongly recommend "`basic mode`" for highest compatibility for arbitrary environments. The remaining serial port screen captures in this document leverage "`basic mode`":



A Note About Subsequent Screen Captures in This Document

The remaining screen-capture examples in this document generally use the serial port format.

The instructions from this point forward are generally the same regardless of whether you are using a serial port or a keyboard+VGA installation paradigm, so you should be able to follow along nicely regardless of which installation mechanism you're employing.

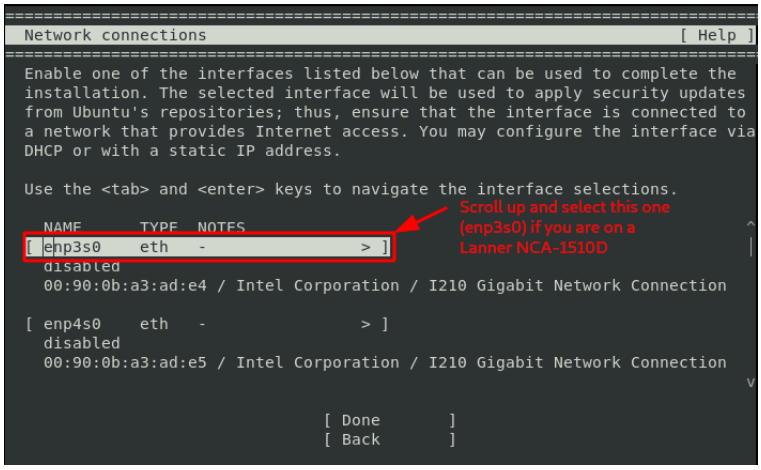
Interaction: Network Selection

After a portion of the automated installation finishes, you'll see a menu to select your active network interface, which is required for the installer to properly continue. All available system ports will be shown, and all are set to be initially disabled. **You must select the SINGLE port that you've connected your administration network cable to for DHCP and Internet access.** If you aren't sure which one it is, you should check your server manual(s).

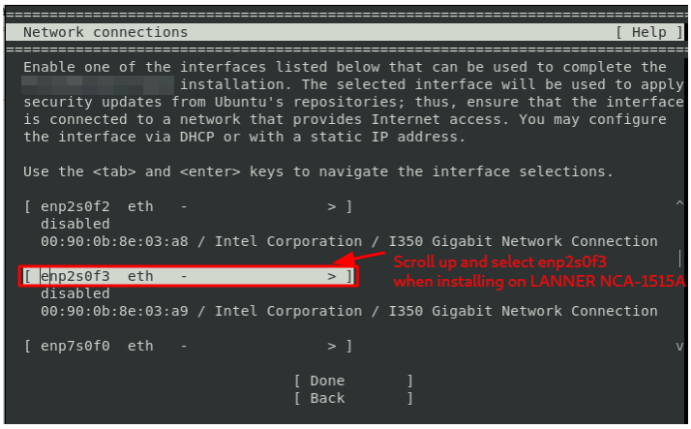
Purely for guidance, if you are installing our software on one of the same systems we currently use for our own turnkey deployments, then the information below may assist you with reasonable initial cabling and the proper

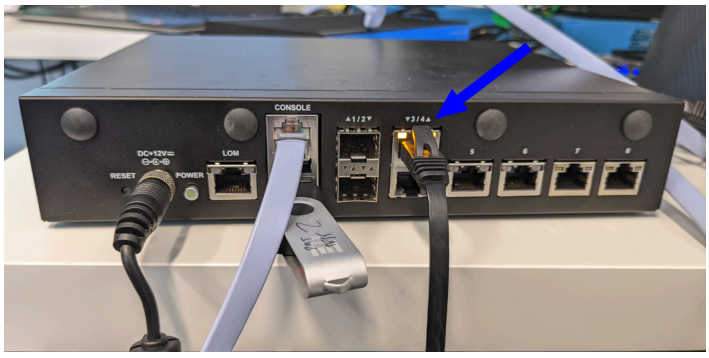
choice at ISO installer time. We also include information for some other legacy turnkey hardware that we have shipped in the past but are generally not currently shipping:

- *Lanner NCA-1510A or NCA-1510D*: this hardware has many ports, and they all do not appear on the screen at the same time. As such, **scroll to the very top of the list** using the up arrow key and find/choose `enp3s0` which corresponds to the leftmost copper port identified below with a blue arrow. Once you have selected `enp3s0`, hit enter:

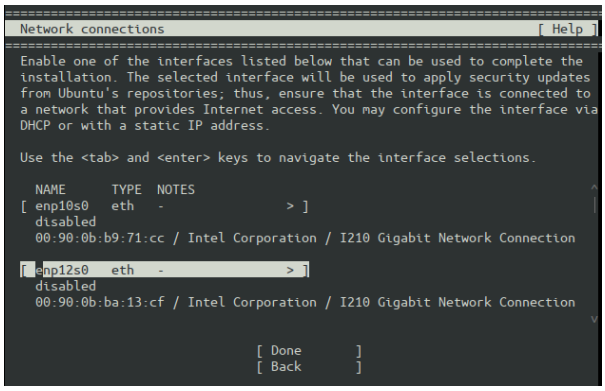


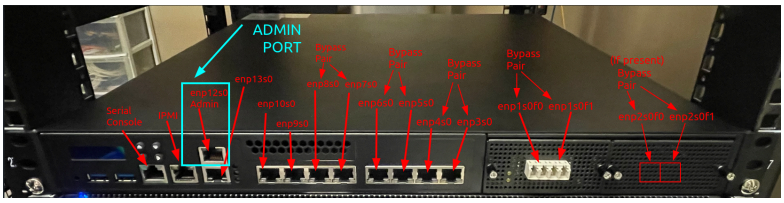
- *Lanner NCA-1515A*: this hardware has many ports, and they all do not appear on the screen at the same time. As such, scroll up in the list using the up arrow key and choose `enp2s0f3` which corresponds to the uppermost copper port in the port stack identified below with a blue arrow, then hit enter:





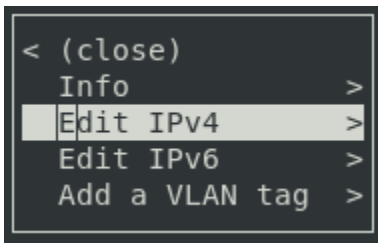
- *Lanner NCA-5220*: locate the proper admin port (enp12s0) you should connect to, and select it from the menu, which correlates to the port shown in the NCA-5220 image below:



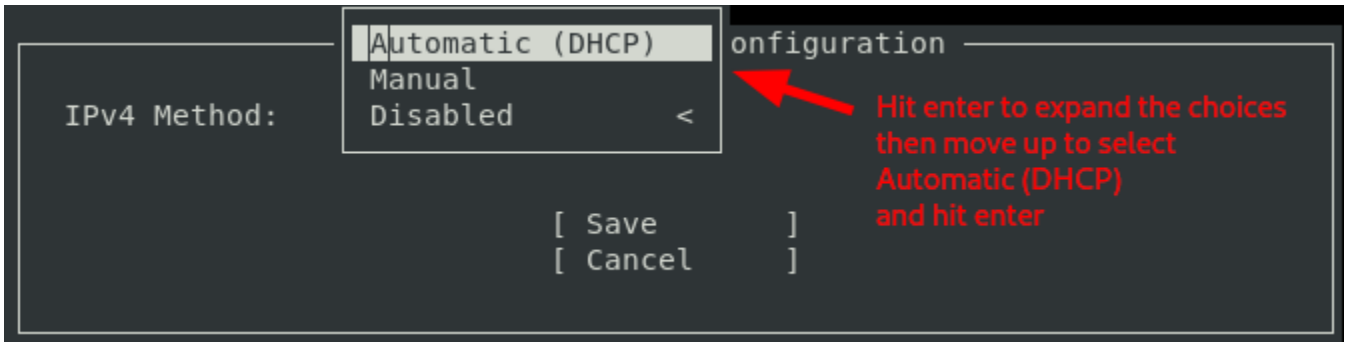


Interaction: Network Selection; Interface DHCP Config

After hitting enter on the proper interface on your particular installation system, you'll be presented with a sub-menu. From that sub-menu, use the arrow keys to navigate to "`Edit IPv4`" and hit enter:

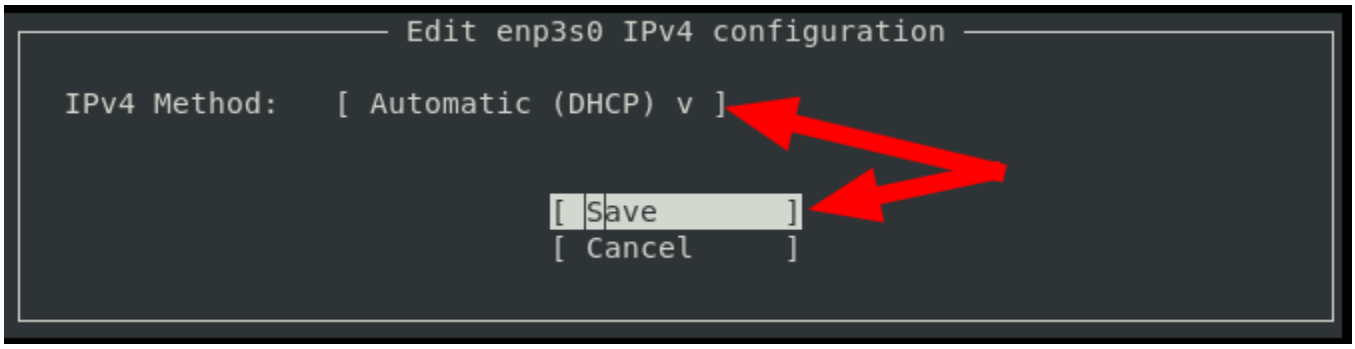


You'll see an overlay paint with "`Disabled`" shown in the selector for IPv4 Method. Hit enter on the word "`Disabled`" and then navigate to "`Automatic (DHCP)`" and hit enter:

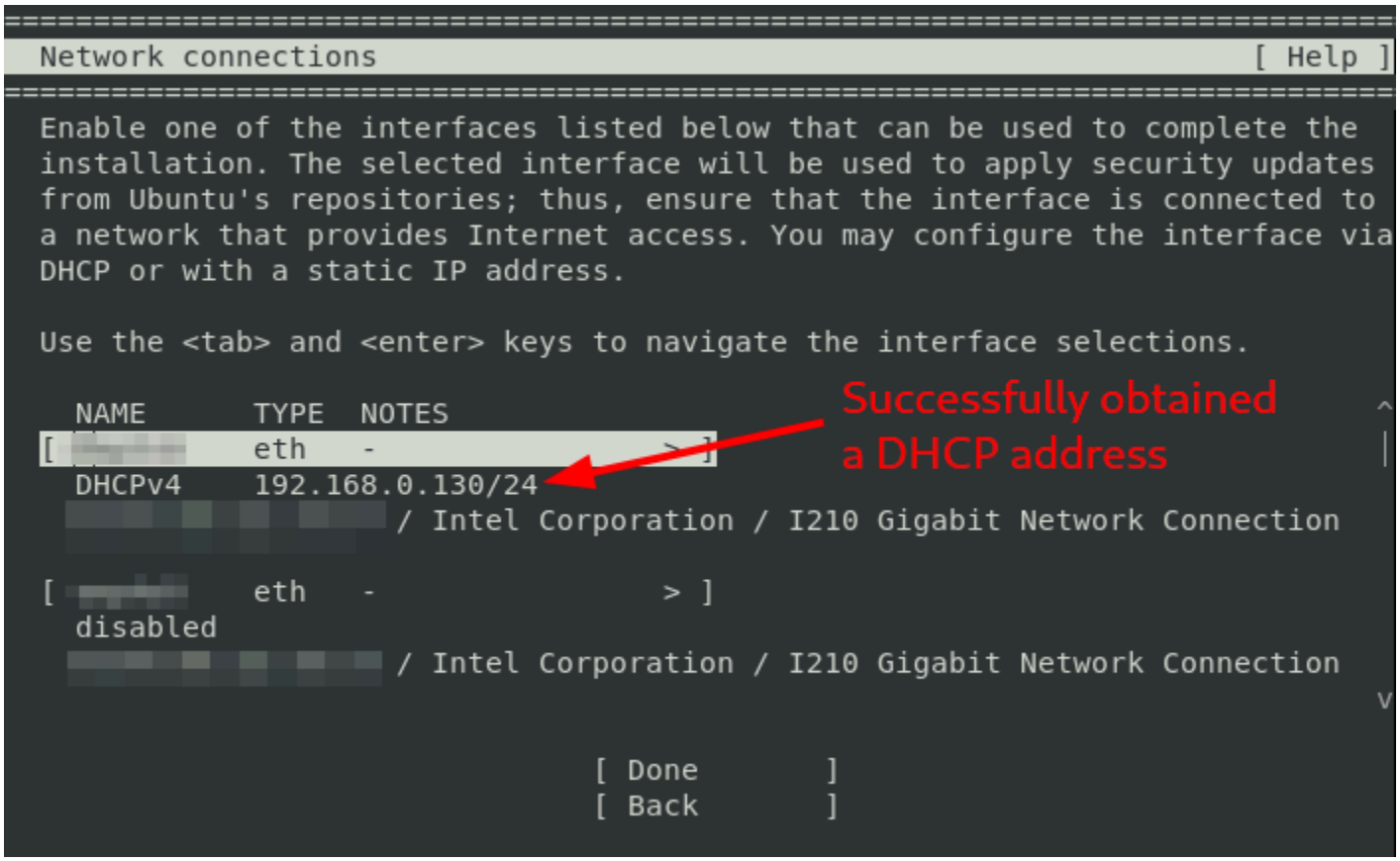


Warning: although it is technically possible to configure a manual, static IP address from the "`Manual`" option in that menu for the installer to use if you are certain it will have outbound Internet access during the install, we do not recommend this. Instead, it is strongly recommended to use DHCP. Note that it is critical for the installer to be able to reach the Internet during the installation process.

You'll now see that the IPv4 Method selected is indeed "`Automatic (DHCP)`". Navigate to "`Save`" and hit enter:



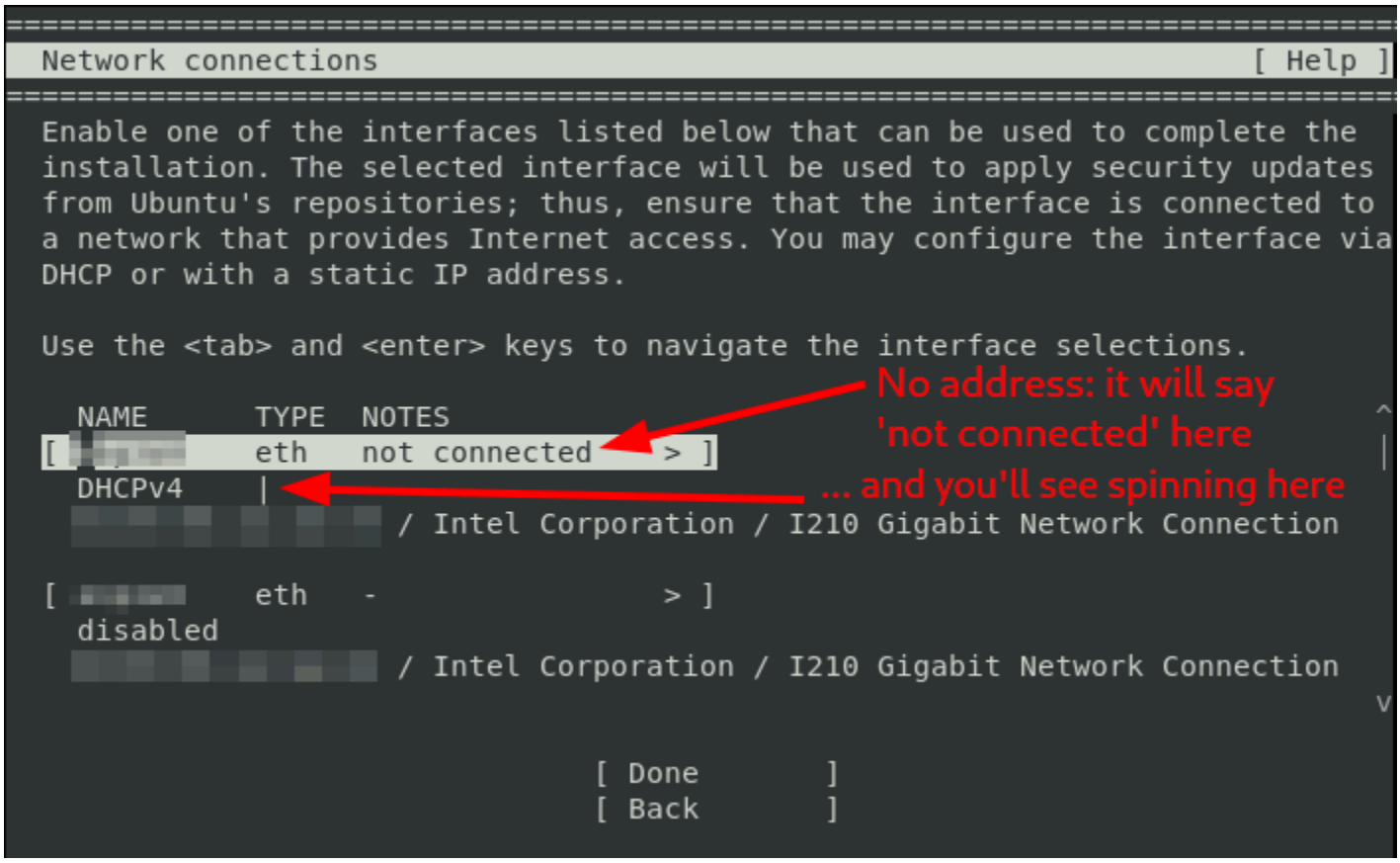
Upon selecting "`Save`," the screen will go back to your connections and if the proper port was indeed selected and the network it is connected to has a viable DHCP server running, you should see a valid DHCP address after patiently waiting for a few seconds. You will likely see different values, but here is an example output with the relevant section of the screen output highlighted:



Before continuing, double check that the interface name was correct for your hardware/environment, and double check that it pulled a proper DHCP address, and make any adjustments as needed.

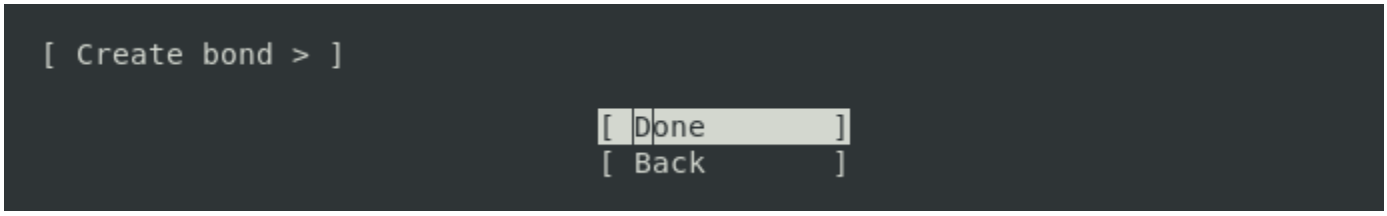
If a valid DHCP address does not appear within about 30 seconds, or if you see a spinning character designator next to the DHCPv4 indicator, it likely means that a DHCP server could not be found on that network. This generally means that you are not properly connected to your network. Here's an example where

a user mistakenly forgot to plug in the admin port `enp3s0` on their Lanner NCA-1510A or NCA-1510D to a proper network with a DHCP server and so they were unable to pull a DHCP address on that port:

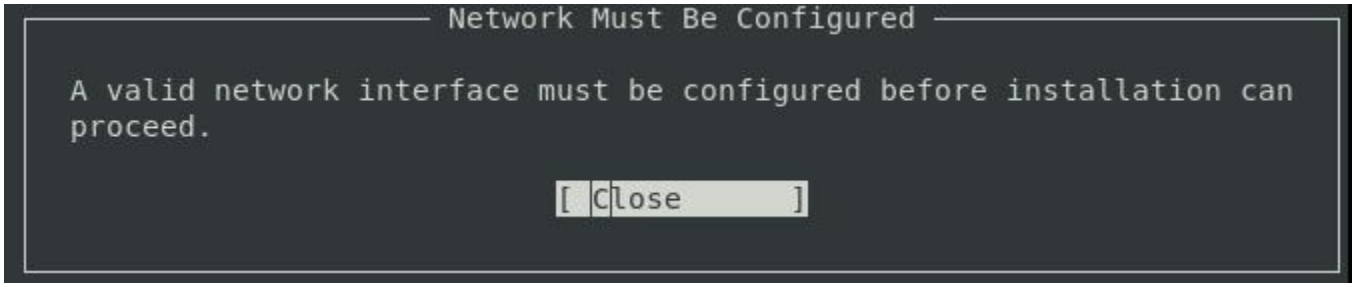


A savvy user with knowledge of the Linux command line can perform any necessary network connectivity troubleshooting by navigating to a shell via the "`Help`" selection at the top right of the install screens, hit enter, then navigate to "`Enter shell`" which will start a shell. From there you can issue a reasonable subset of Linux commands to check connectivity to Google, Ubuntu repos, etc. Exiting the shell with "`exit`" returns the user back to the install UI.

Once you are certain of your connectivity and the correct port was chosen and a proper DHCP address was made available, you should use the down arrow key to navigate to "`Done`" and hit enter:



Note that the installer will not let you continue until you have chosen and successfully configured a viable network interface. In the event a valid network interface is not properly selected, you'll see something similar to the following screen, and you should select '`Close`' and once back on the network connection selection screen, choose a suitable connection:



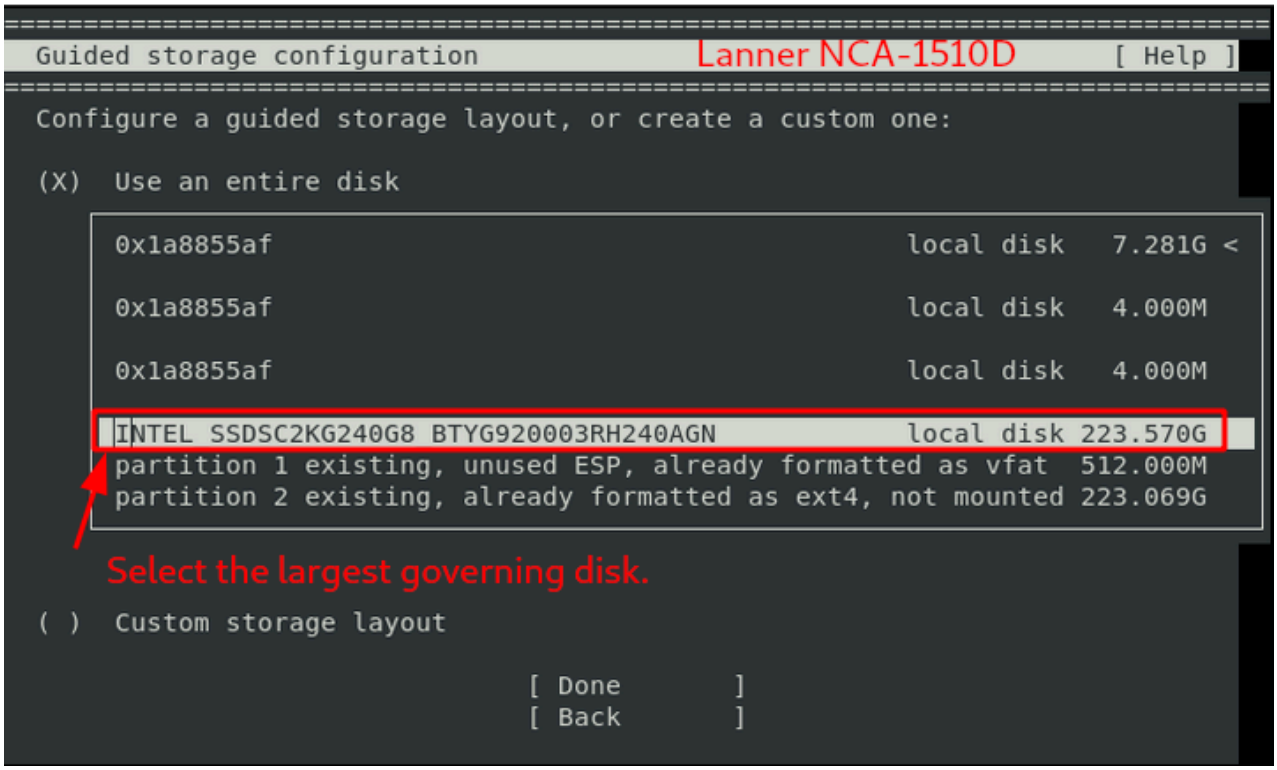
Do not attempt to continue without verifying that your connected administration port was able to obtain a viable DHCP address capable of reaching the Internet. It is critical that the installer be able to connect to the Internet for the remainder of the installation to proceed successfully. It will fail and the system will not function properly if you do not. You have been warned.

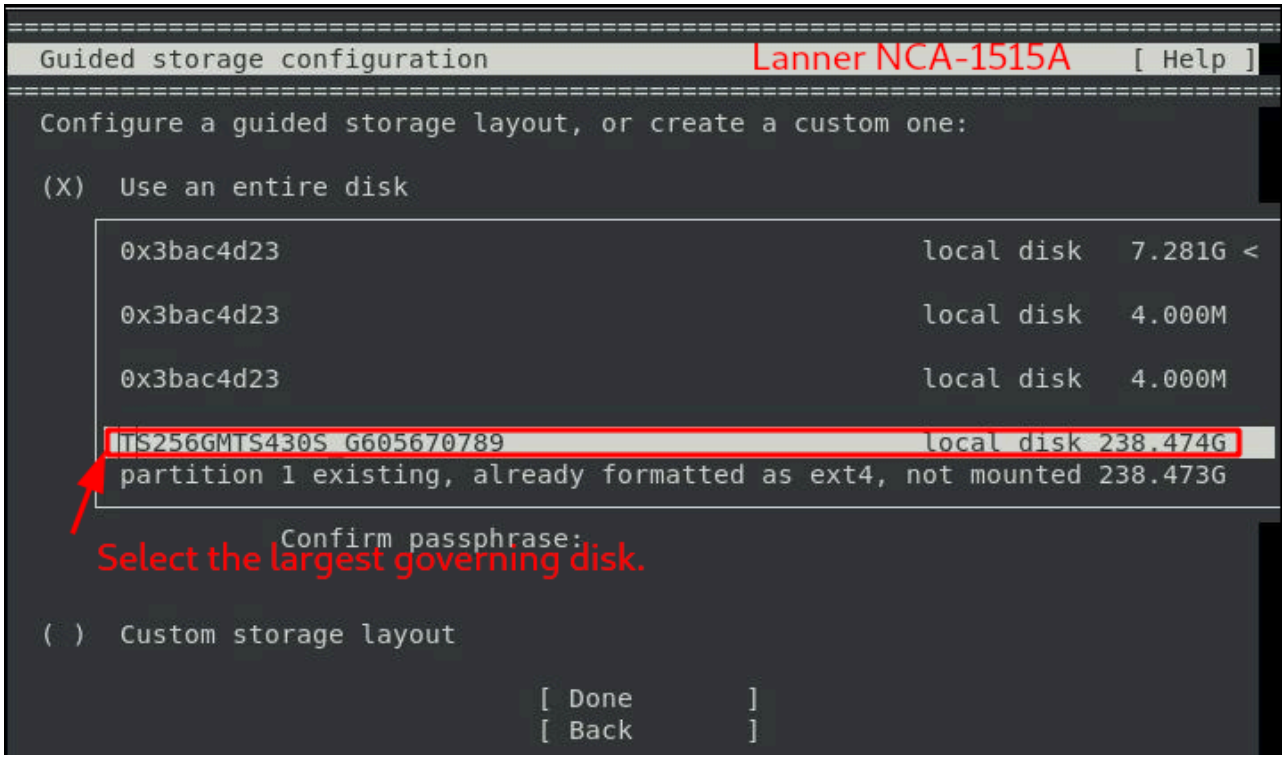
Interaction: Storage Selection

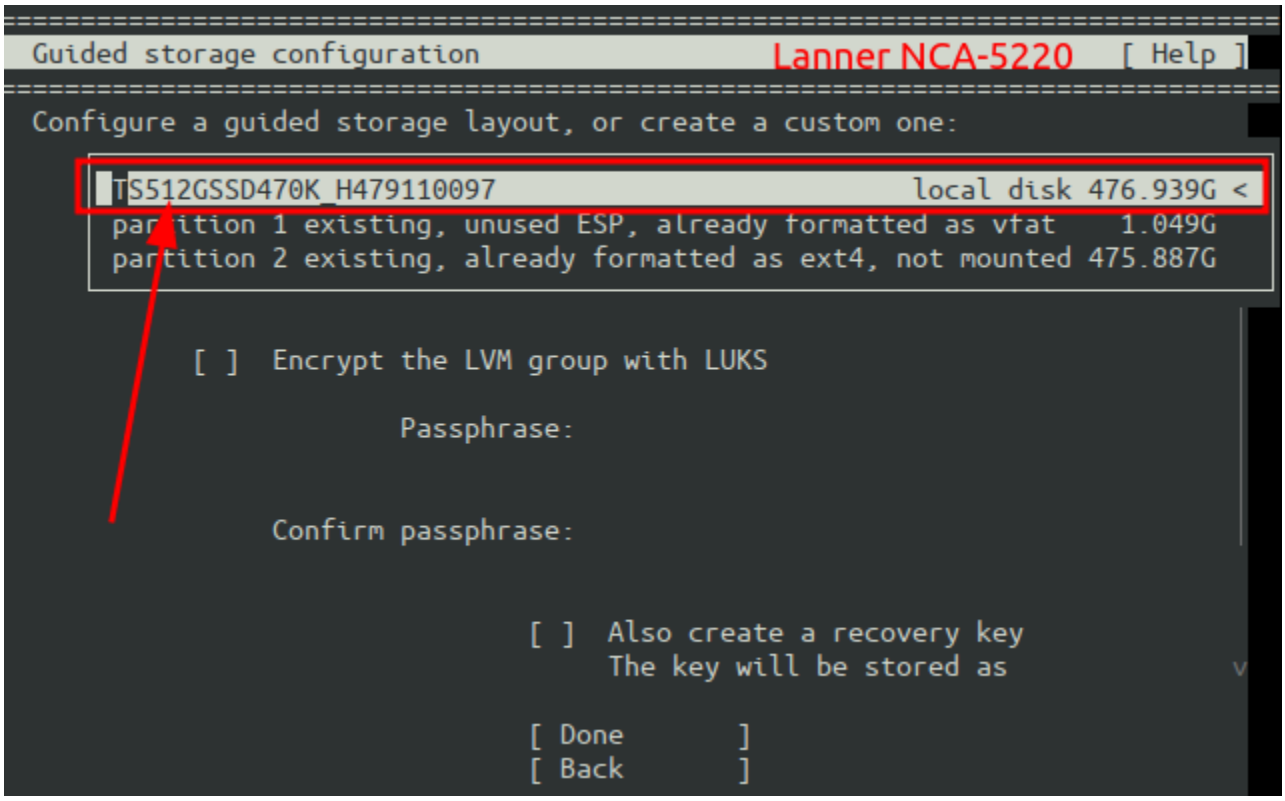
Once the networking configuration is complete, more automated steps will occur, and then you'll be presented with interactive screens for storage selection.

You'll need to choose the drive that threatER Enforce will be installed on. As such, make sure that "`Use an entire disk`" is selected, as designated by an "`(X)`" marker next to it. No other options should be marked as selected on the screen, so be sure to deselect them if they are. The space bar can be used to toggle the "`(X)`" markers as needed after navigating to them using the arrow keys.

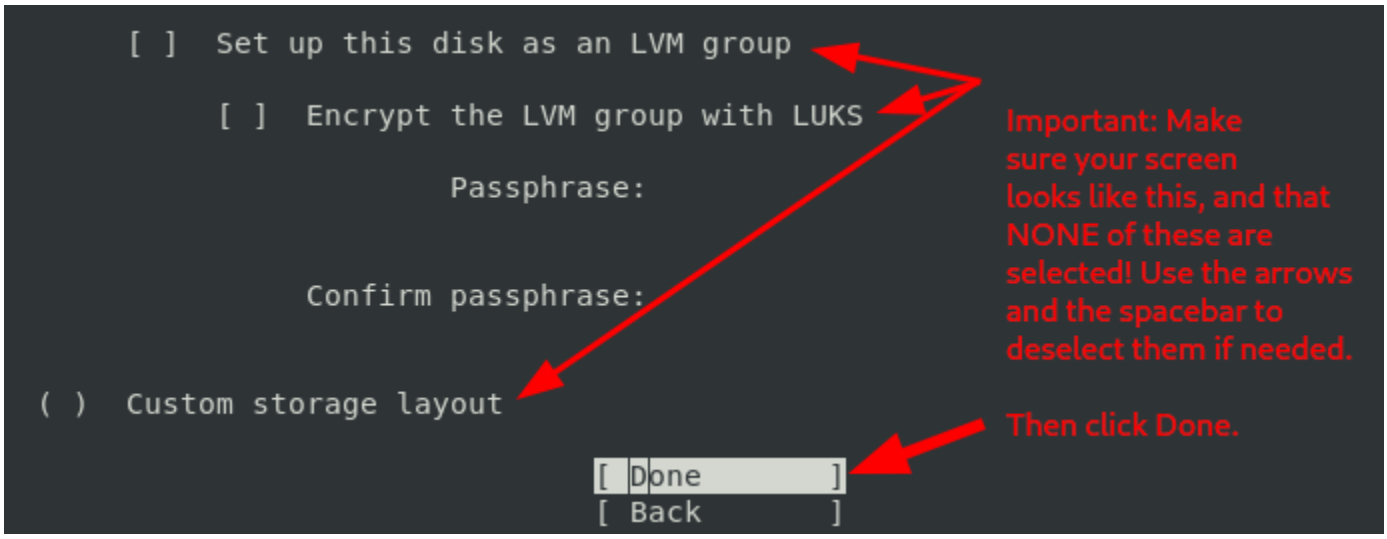
Hit enter on the drop-down next to "`Use an entire disk`" in order to choose the disk to install on. Generally, if you are unsure what disk to use, use the largest governing disk. A few typical example screens as to how this appears for various turnkey Lanner systems appear below for reference:


Guided storage configuration
Lanner NCA-1510D
[Help]
Configure a guided storage layout, or create a custom one:
(X) Use an entire disk
0x1a8855af local disk 7.281G <
0x1a8855af local disk 4.000M
0x1a8855af local disk 4.000M
INTEL SSDSC2KG240G8 BTYG920003RH240AGN local disk 223.570G
partition 1 existing, unused ESP, already formatted as vfat 512.000M
partition 2 existing, already formatted as ext4, not mounted 223.069G
Select the largest governing disk.
( ) Custom storage layout
[Done]
[Back]

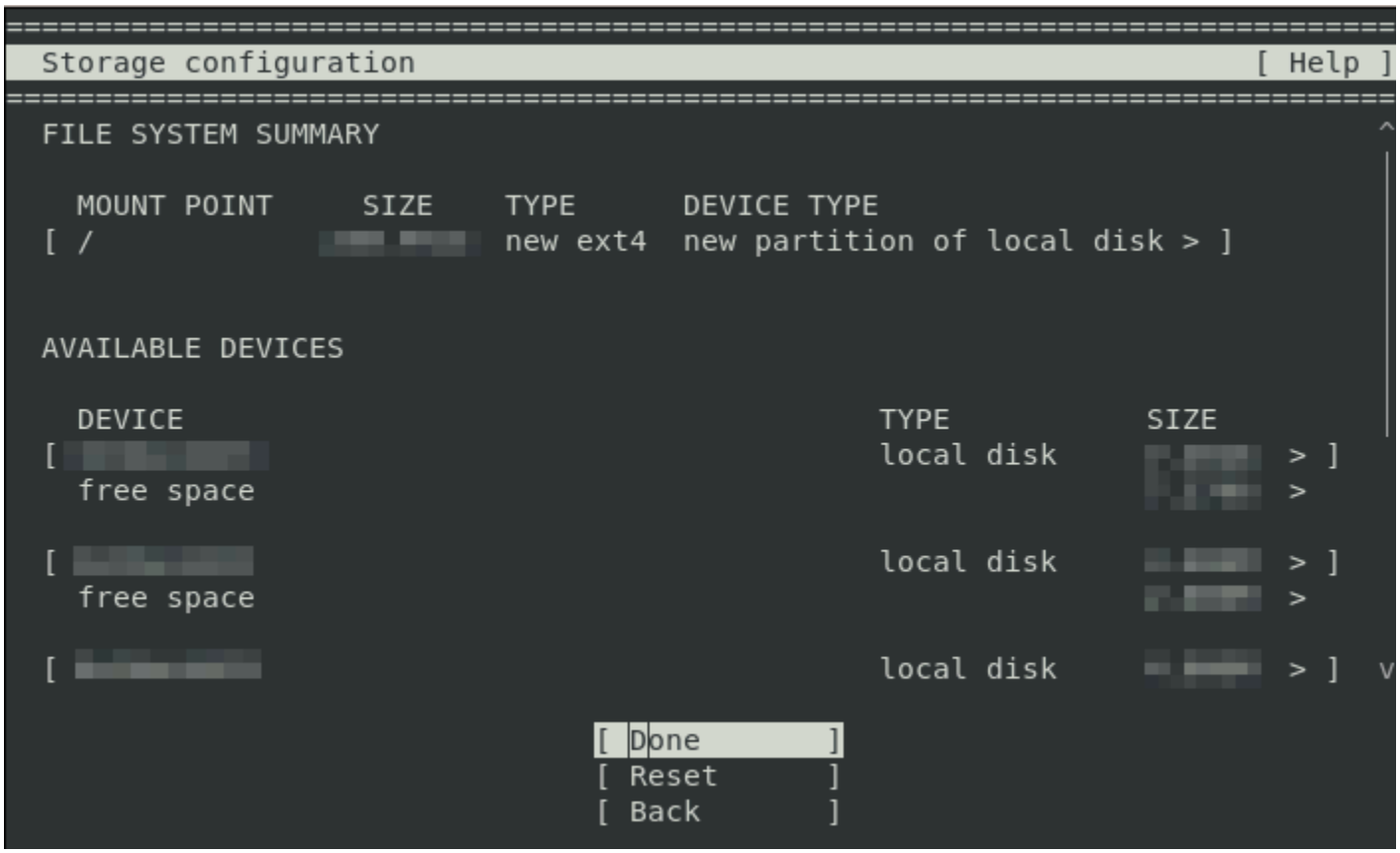

Guided storage configuration
Lanner NCA-1515A
[Help]
Configure a guided storage layout, or create a custom one:
(X) Use an entire disk
0x3bac4d23 local disk 7.281G <
0x3bac4d23 local disk 4.000M
0x3bac4d23 local disk 4.000M
TS256GMTS430S G605670789 local disk 238.474G
partition 1 existing, already formatted as ext4, not mounted 238.473G
Confirm passphrase:
Select the largest governing disk.
( ) Custom storage layout
[Done]
[Back]



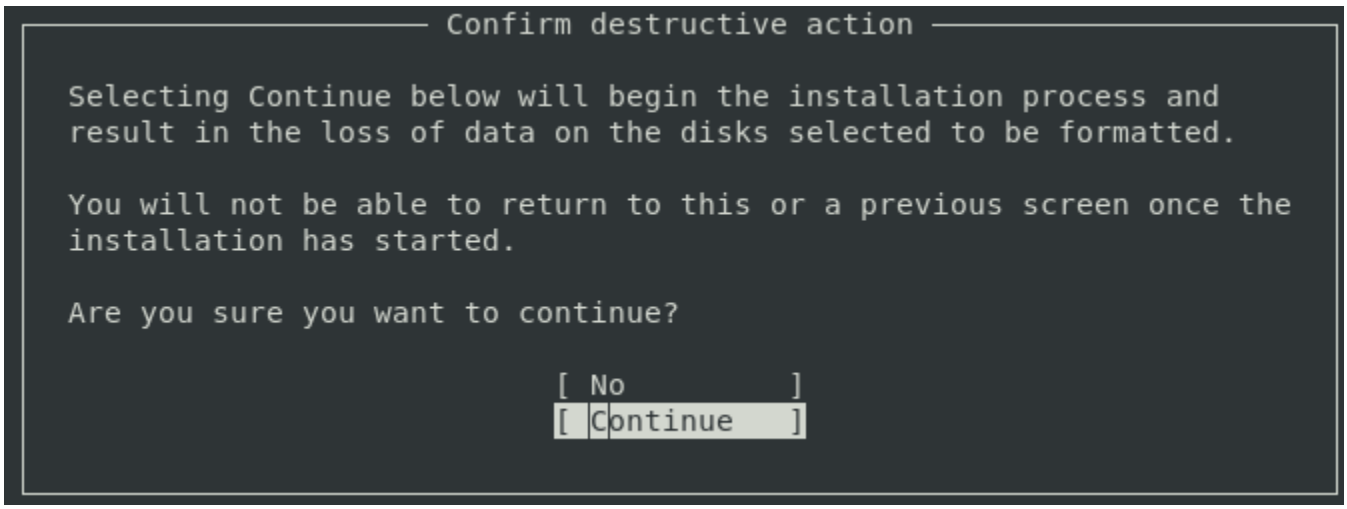
Before continuing, double-check the drive that you chose to be sure it was the correct drive. **Seriously, fight the urge to continue fast and double-check it and make sure you picked the correct drive.** Any data on the selected disk will be completely overwritten by the installer with no possibility of recovery of any overwritten data. Once you are certain the drive chosen is the correct drive and have ensured that NO other options are selected on the screen except for that single entire disk choice, use the down arrow key to navigate do "`Done`" and hit enter:



You'll see another confirmation screen for your storage selection. Your screen will likely differ somewhat from what is shown below, but regardless, **double-check it one more time**, and when you are sure it is correct for your environment, use the down arrow key to navigate to "`Done`" and hit enter:



You will then see one more confirmation screen for the drive selected, where it will warn you that the drive you have selected is about to be installed, meaning any existing data on the drive will be destroyed. Select "`Continue`" when you are ready to continue:



The installation will continue, and various logging information will appear on the screen. Be patient as the installation continues.

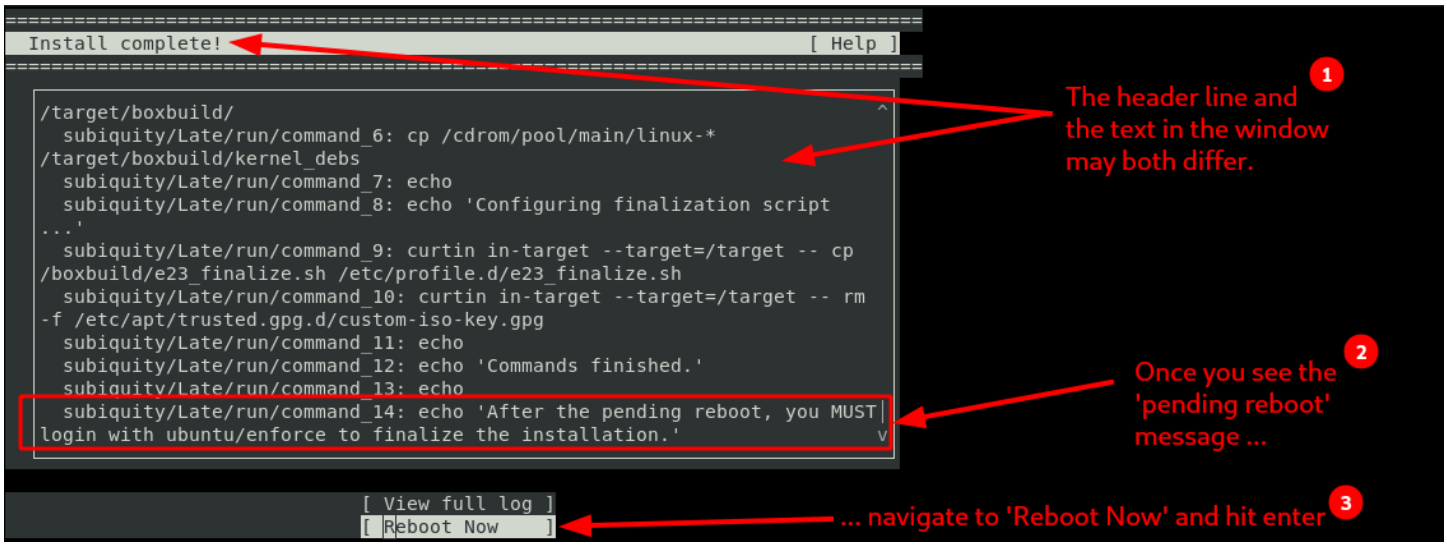
Possible Interaction: Boot Loader Installation

The installer will automatically attempt to determine where the boot loader should reside, and if it successfully determines a proper location, it will install it with no interaction step required.

However, if the installer is unable to determine a proper location, it may present a menu for you to choose from. In the rare case that you are presented with a menu of options for your target hardware, you should choose the **same** disk to which you installed the software.

Interaction: System Reboot and Initial Login for Configuration Finalization

When the base installer finishes, it will display a screen that resembles the following screen. Once you see it, navigate to "`Reboot Now`" and hit enter, and the system will reboot:



Once you've selected "`Reboot Now`" and pressed enter, one of two things will typically happen:

Scenario 1: on some hardware you may see the screen go completely dark for an extended period of time. If it stays dark for more than 30 seconds, then you should manually power down the unit and then remove the USB.

Scenario 2: If the reboot is able to automatically proceed, then you'll see a ton of messages scroll on the screen, culminating with a pause asking you to remove the USB media before continuing:

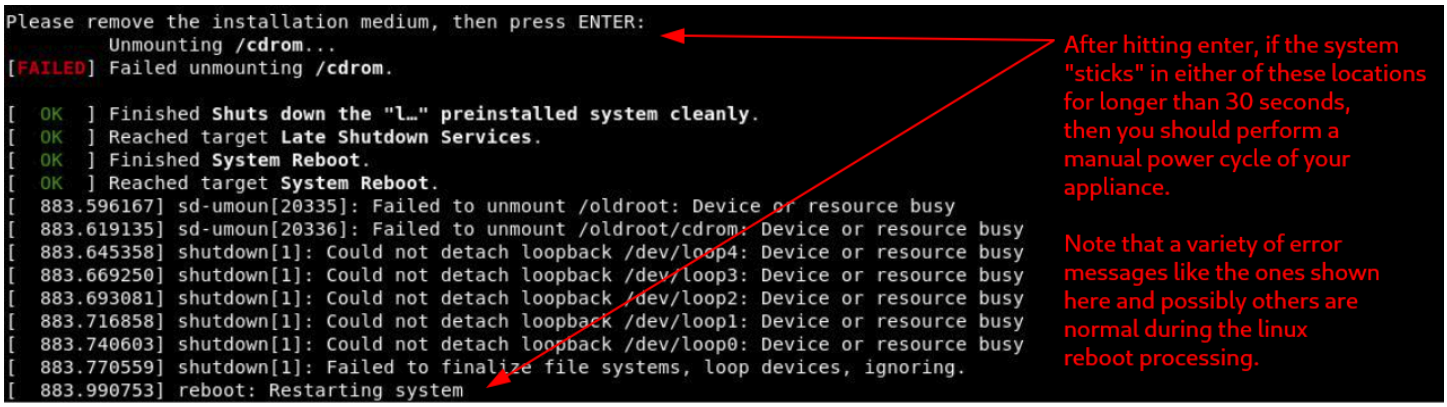
```
Please remove the installation medium, then press ENTER:
```

Remove the USB drive, and hit `Enter`.

Be patient, as it can take several seconds for internal cleanup before the system engages the reboot process. You may see a few error messages. Those are entirely normal. If, however, it takes more than 30 seconds and the screen sticks as denoted in the following screen capture, then you should hold down your system power button on your hardware until your hardware powers off. The time you must hold down the power button varies across various hardware types, but it is generally anywhere from 5 to 15 seconds.

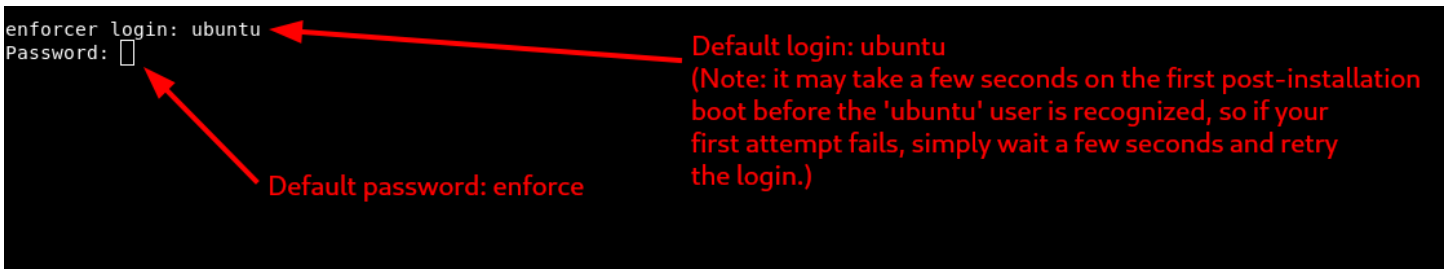
Finalizing the non-WiFi Configuration

After your hardware powers completely off, let go of the power button, wait 5 seconds, and then, ensuring the USB has been removed, press the power button to power the system back on:

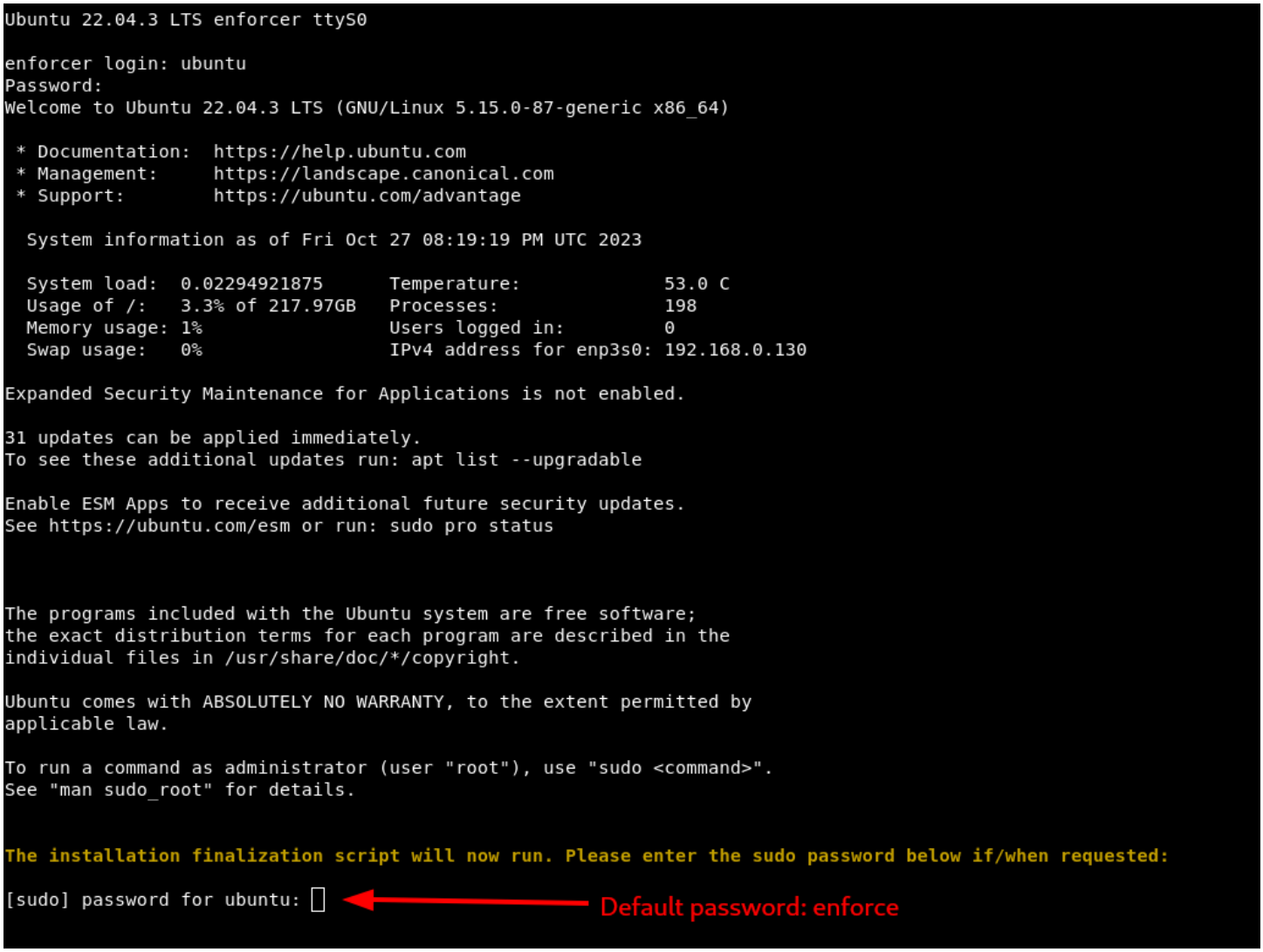


If you forgot to remove the USB, once the system reboots, you may find yourself back to the standard BIOS or UEFI installation menus. If that happens to you, just hold down the power button until the system powers down, then remove the USB, and then press the power button to turn the system back on manually.

Once the system properly reboots after the installation, you'll see a standard Linux login prompt appear that will generally resemble the following screen either via serial port access or video+keyboard access. Regardless of your input paradigm, enter **`ubuntu`** for the default login and **`enforce`** for the default password. It may take a few seconds on the first post-installation boot before the "**`ubuntu`**" user is recognized, so if your first attempt fails, simply wait a few seconds and try it again:



You will begin the initial login process, and a script will automatically run and ask you for the default system administration password. Re-enter the default password **`enforce`**:



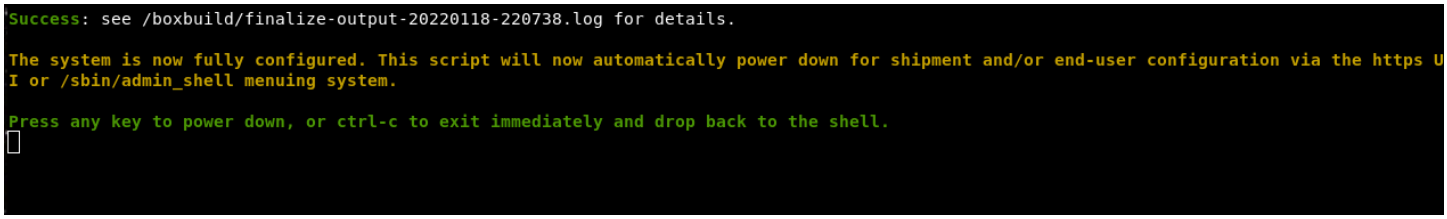
The script will automatically run through several automated steps, showing its status along the way with a variety of output. **Be patient**, as it can take a few minutes for the script to run to completion depending on your Internet access speed.

If the script runs into any error conditions, it will gracefully error and attempt to explain what difficulties it ran into. The software will not be installed, and you can investigate the issue, make any adjustments (often issues arise for example with network cabling mistakes), and then re-login to re-attempt the script run. The script will always attempt to run on each login until it succeeds, so you can repeat this as many times as might be needed as you perform triage.

Nine times out of ten, any errors are related to network configuration, so that's always the first thing to check.

Regardless of success or failure, each installation script run is logged into the directory with a file pattern of `/boxbuild/finalize*log`, so you can always peruse those output log files as needed. These logs can also be immensely useful to our Customer Success team if our assistance is needed during troubleshooting.

When the script successfully completes, you will see the following message:



At that point you can hit `Enter`, and the system will power down.

It will have the same factory default settings as one of our turnkey systems would have.

It is now ready to be shipped, onboarded, and subsequently installed as a bump-in-the-wire into a desired production network, such as next to your ISP modem.

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.

Non-WiFi Deployment Strategy

Note that our bump-in-a-wire architecture makes it trivial to deploy practically anywhere in a network. Most customers deploy us right next to their ISP modem, often between their ISP modem and their next generation firewall.

It is our strong recommendation that customers stick with the same topology that they currently have in place with regard to their existing next-generation firewall deployments. That is:

- If you have an on-premise next-generation firewall, it will be easiest to install our threatER Enforce software onto on-premise hardware meeting our minimum system specifications as described elsewhere in this document.
- If you have an on-premise HA pair of firewalls, then you'll want to install our threatER Enforce software into each of your HA legs, leveraging on-premise hardware meeting our minimum system specifications as described elsewhere in this document.
- If you are currently using virtualized next-generation firewalls (such as an existing third-party vendor's firewall VM running inside of VMware), then it will be easiest to install threatER Enforce into that same networked virtual environment alongside it.
- Note: we also support full cloud deployments with the same general guidelines: if you are securing things running in AWS, Azure, or GCP, then you should deploy us alongside those controls in AWS, Azure, or GCP. We have separate cloud deployment guides that our Customer Success team can provide you as needed.

Mixing and matching physical and virtualized security infrastructure is **not** recommended, as it will introduce potentially significant packet latency (and therefore impact end-user day-to-day performance) given excessive virtualized network routing between your physical and virtual infrastructure.