Seqrite Unified Threat Management 2.3 GA

Release Notes- GA

Dated 13 August 2019

Copyright Information

Trademarks

License Terms

Contents

Revision History

The information in this document is provided for the sole use of Quick Heal Research and Development, Incidence Response and Support Team. It is strictly forbidden to publish or distribute any part of this document to any other party.

Version	Date	Comment
UTM2.3	13th August 2019	Version 2.3 GA Release

Abstract

Seqrite Unified Threat Management Release Notes for version 2.3 contains the following information about the released build:

- Build Information
- New Features and Enhancements
- Bug Fixes
- Known Issues and Work arounds
- Appendix

Build Information

Build 2.3 version released on 13th August 2019

Seqrite UTM GA Build 2.3 details:

Product Name	Release Date	MD5 Checksum	Build Version
Seqrite Unified Threat Management	13 August 2019	7cf8fc85decd1d1827d6694ec2c0dcd3	Build 2.3.0.41

New Features and Enhancements

1. **Dashboard Changes**

   As part of this revamp activity; Information is split in two tabs "Status" and "Security" for more clarity and added information at a glance.

2. **Country based blocking**

   You may need to block network traffic to and from certain countries that are known to be sources of cyber-attacks. Some geographical regions may harbour individuals who carry out repeated brute force login attacks on your network and may need to be blocked. You also might want to prevent users in your computer network from accessing these networks. Seqrite UTM allows you to block all incoming traffic from and towards these countries via this feature.

3. **Auto configuration**

   This feature automatically detects the LAN, WAN interfaces on the UTM and provides a list of IP addresses which could be assigned to those interfaces. This removes the manual process of configuring the interfaces

4. **Safe search**

   Enable this option to apply Safe search for Google, Bing and Youtube search results. Enabling Safe search filters out explicit content from search results.

5. **USB Tethering**

   Support for USB tethering via USB port

6. **Traffic Shaping**

   You can create a traffic shaping policy that restricts the bandwidth for users and groups based on protocols. Here you can restrict the upload and download speeds for users based on HTTP and HTTPS protocols. You can also configure the maximum upload and download limits for VPN connections.

7. **IPSec / MPLS failover Support**

8. **Corporate email (Gmail) whitelist**

   You may require blocking google mail server (gmail.com) for personal email as well as other corporate email and allow your own corporate domain Gmail. You can do this by adding your corporate sub domain in the whitelist

9. **Policy enforcement on SSL VPN users**

   You can now apply the group policy settings to the SSL VPN remote users. The policies will be applied in the same way as it is applied to the LAN users.

10. **TCP-Dump on CLI**

    To help the administrator, troubleshoot network issues, we have provided the option to capture packets on the UTM interfaces.

11. **Enhancement in DoS, DDoS protection**

    Source and destination-based flood rate can now be configured, and data of attacker and victim is not displayed on the dashboard

Bug Fixes – part of UTM 2.3

Summary
Fix for display of garbage characters in CSV report format.
Antispam page shows "Read only" error to super admin
Copyright issues fixes.
Unable to configure IPSec site to site VPN with pre-shared key in plain text.

Known Issues

The following table lists some of the important known issues to consider in version 2.3.

Serial #	Summary of known issue
1	**High Availability**: Old Master UTM device remains master after some time. This is an intermittent issue. **Workaround**: None
2	**High Availability**: Failover in bridge mode might take 1 minute or more time **Workaround**: None
3	CLI admin password resets to factory default after firmware upgrade
4	Time Quota policy applied on a group didn't block https sites when MITM is OFF
5	Network Interface page may take up to 10 seconds to load

Important Points to Note:

Some crucial points to note for various features added in UTM 2.3

- **USB Tethering**
    - This interface can be used as fail over and in policy-based routing. It cannot be used in firewall rules
- **Country Based Blocking**
    - Countries which have a lot of networks (US, UK, France etc) take more than 4 minutes to get enabled. User will be block and UI will be in busy wait state.
    - Domains and subnets are not supported in exclusions
    - If United States is blocked, then few websites might misbehave even though they are hosted on one single IP. This is because these websites contain some widget/tool (for e.g. google AdSense) which is hosted on an IP located in US.
    - Country Based Blocking will be bypassed if the host's browser mode is working in proxy mode.
    - Country Based Blocking will not work for SSL VPN users.
    - No user login page will be shown if the user is accessing an IP/domain of a blocked country. As the blocking is done before redirecting anything to the proxy.
- **TCP-Dump on CLI**
    - Packet capture taken from CLI cannot be downloaded onto local machine
- **Policy enforcement on SSL VPN users**
    - Different users can login with the same SSL VPN download package.

Appendix

Installation of UTM version 2.3

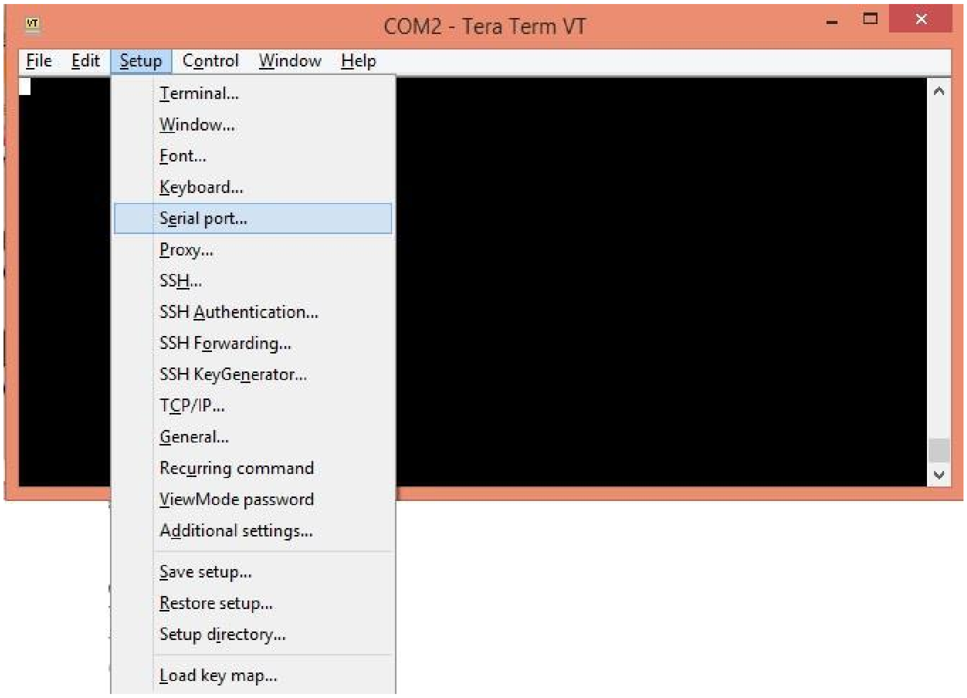
- ### Using ISO

1. To install UTM 2.3, you need bootable USB drive. A 2.3 bootable USB drive could be created writing the 2.3 ISO to the USB drive using tools such as Rufus.

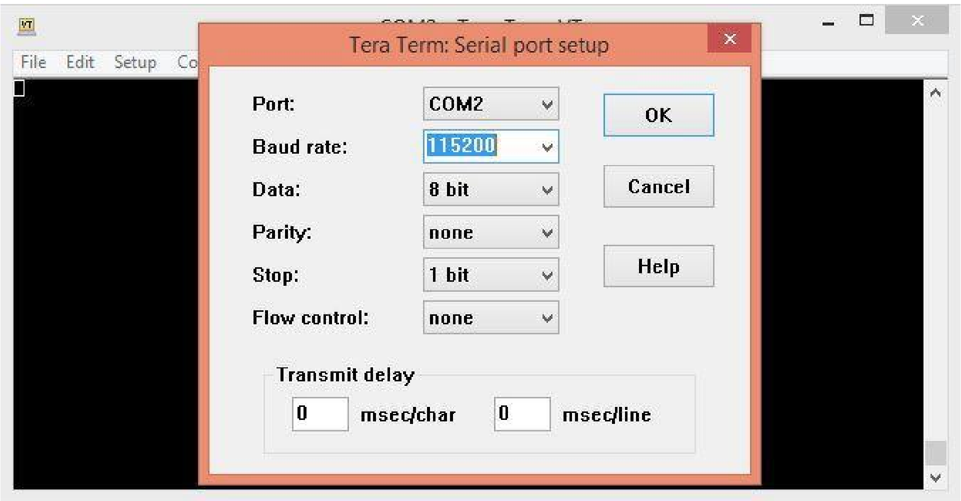
2. Once you have the 2.3 bootable USB drive ready, plug it in USB port of UTM, attach console cable.

3. Use Tera Term or Putty on MS Windows and Minicom for Linux to connect to the UTM device.

4. Open Tera term and select Serial port (ex: COM2: Communication port)



5. Configure baud rate by selecting Setup -> serial port



Tera Term: Serial port setup

Port: COM2

Baud rate: 115200

Data: 8 bit

Parity: none

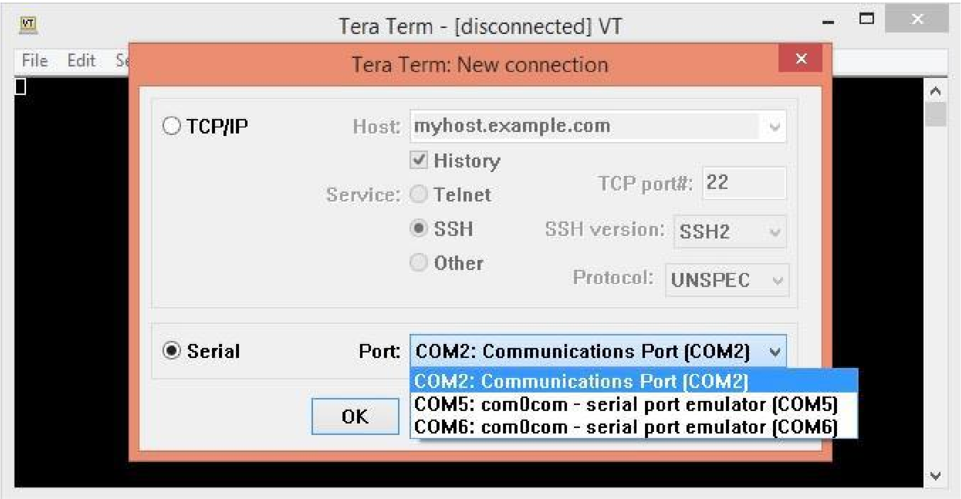
Stop: 1 bit

Flow control: none

Transmit delay

0 msec/char 0 msec/line

6. Select baud rate here as 115200.



Tera Term - [disconnected] VT

Tera Term: New connection

○ TCP/IP Host: myhost.example.com

☑ History

Service: ○ Telnet TCP port#: 22

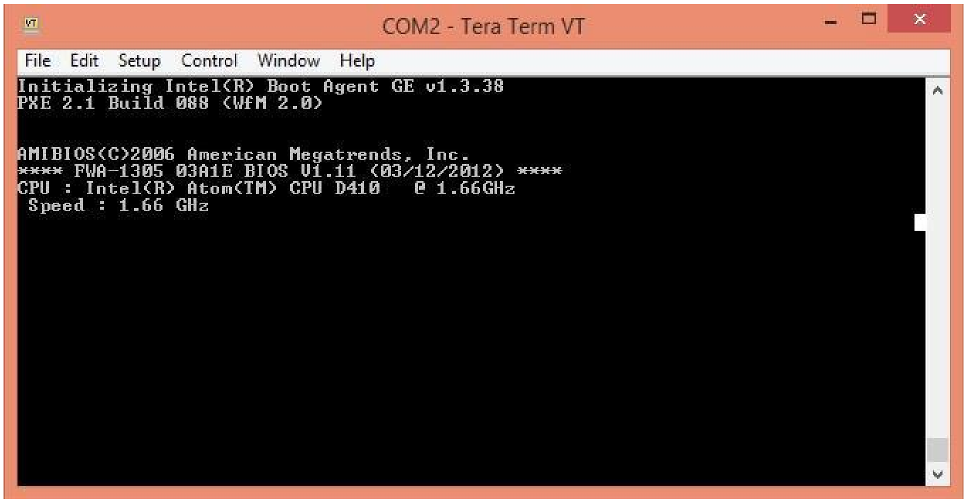
● SSH SSH version: SSH2

○ Other Protocol: UNSPEC

● Serial Port: COM2: Communications Port (COM2)

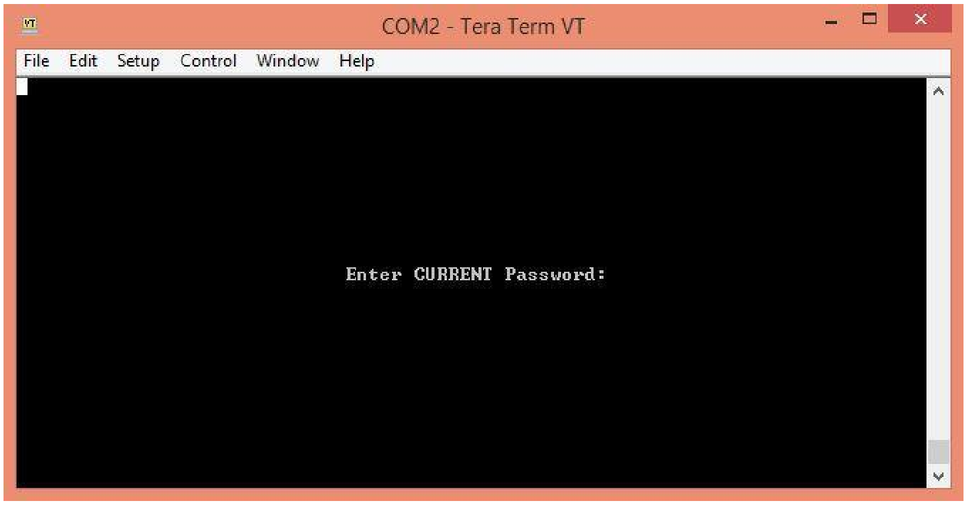
COM2: Communications Port (COM2)
COM5: com0com - serial port emulator (COM5)
COM6: com0com - serial port emulator (COM6)

7. Now Power On the UTM. You would see the screen as below:



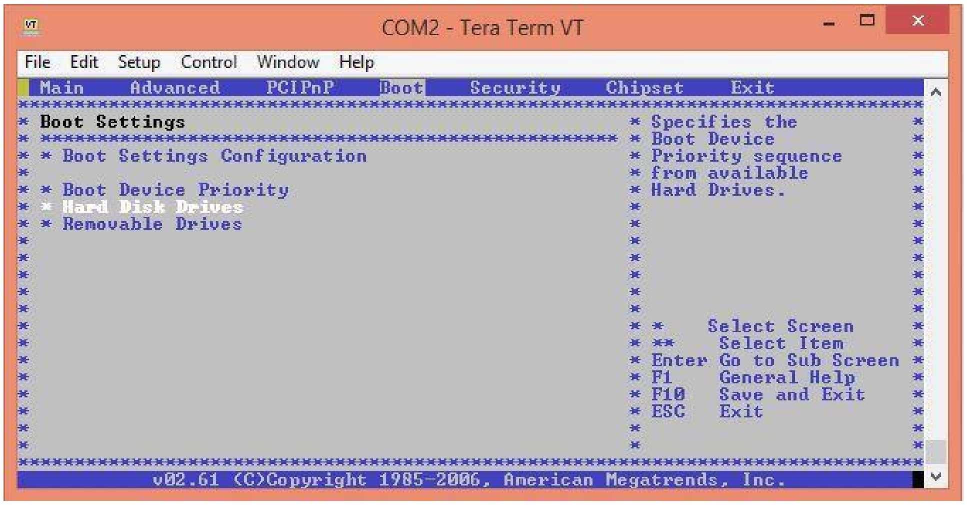
```
Initializing Intel(R) Boot Agent GE v1.3.38
PXE 2.1 Build 088 (WfM 2.0)


AMIBIOS(C)2006 American Megatrends, Inc.
***** FWA-1305 03A1E BIOS V1.11 (03/12/2012) *****
CPU : Intel(R) Atom(TM) CPU D410   @ 1.66GHz
 Speed : 1.66 GHz
```

8. To select USB drive as first boot priority, hit button 'Delete' to enter into BIOS. Enter the BIOS password shared separately.



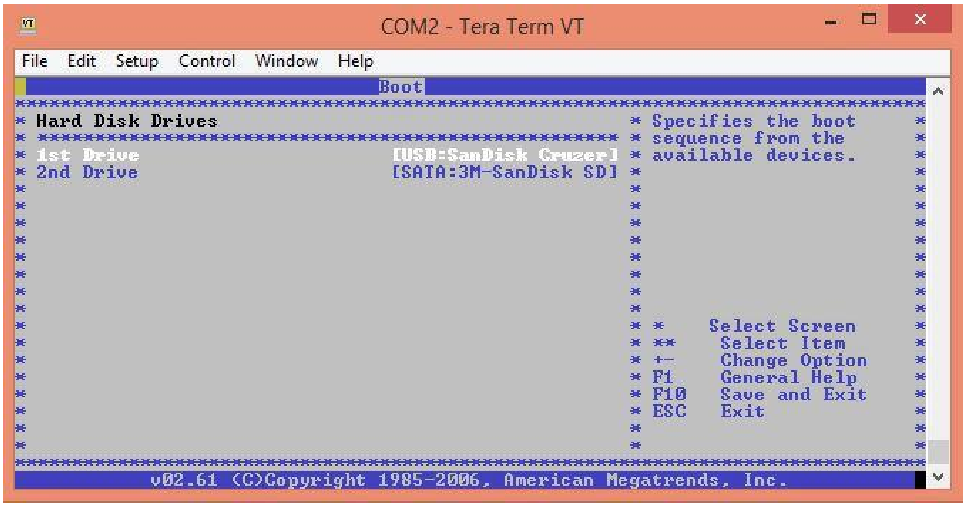
```
Enter CURRENT Password:
```

9. In BIOS, Go to Boot -> Hard Disk Drive



```
  Main     Advanced     PCIPnP     Boot     Security     Chipset     Exit
 Boot Settings                                      * Specifies the
                                                    * Boot Device
 * Boot Settings Configuration                      * Priority sequence
                                                    * from available
 * Boot Device Priority                             * Hard Drives.
 * Hard Disk Drives
 * Removable Drives

                                                    * *    Select Screen
                                                    * **    Select Item
                                                    * Enter Go to Sub Screen
                                                    * F1    General Help
                                                    * F10   Save and Exit
                                                    * ESC   Exit

           v02.61 (C)Copyright 1985-2006, American Megatrends, Inc.
```

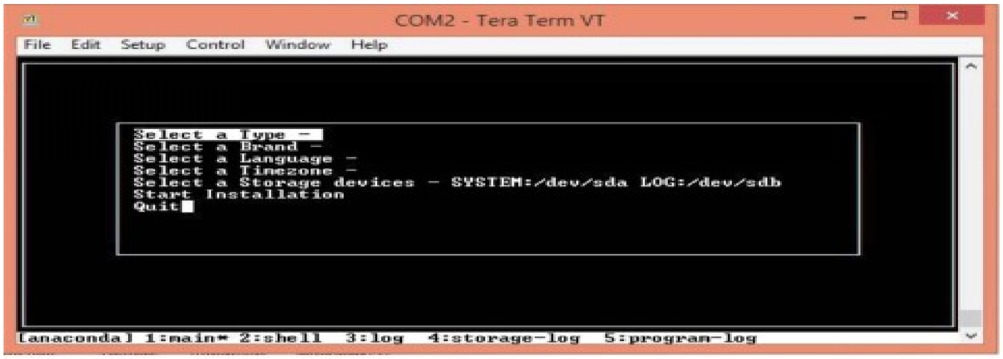
10. Choose the USB drive as the bootable drive



```
                                     Boot
 Hard Disk Drives                                   * Specifies the boot
                                                    * sequence from the
 1st Drive                    [USB:SanDisk Cruzer]  * available devices.
 2nd Drive                    [SATA:3M-SanDisk SD]  *

                                                    * *    Select Screen
                                                    * **    Select Item
                                                    * +-    Change Option
                                                    * F1    General Help
                                                    * F10   Save and Exit
                                                    * ESC   Exit

           v02.61 (C)Copyright 1985-2006, American Megatrends, Inc.
```

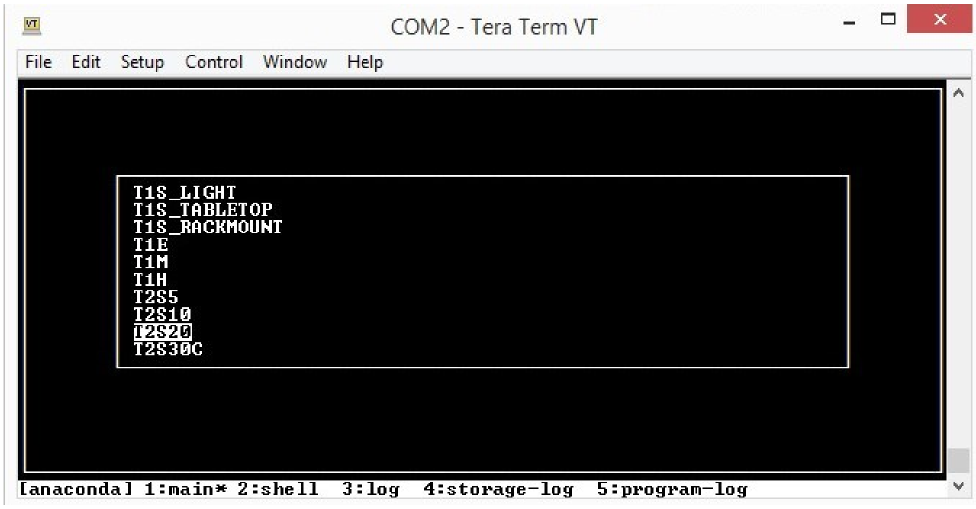
11. Save the changes and Exit.

12. Now reboot the device and you should see installation menu. Options seen are: Hardware Type, Brand, Language, Time zone and Storage device.



```
Select a Type -
Select a Brand -
Select a Language -
Select a Timezone -
Select a Storage devices - SYSTEM:/dev/sda LOG:/dev/sdb
Start Installation
Quit

[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log
```

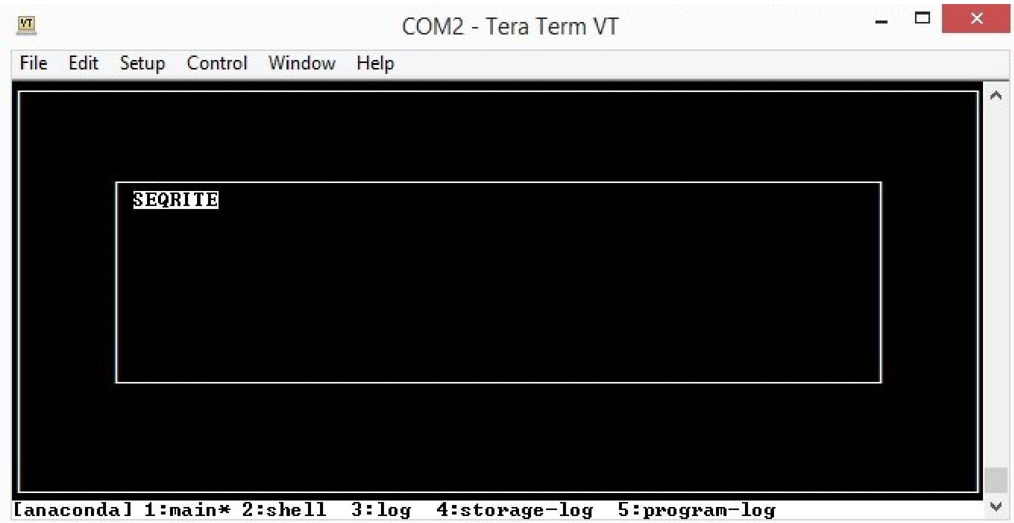
13. Select the hardware type. For example, for T2S-20 device choose, T2S20 option.



```
T1S_LIGHT
T1S_TABLETOP
T1S_RACKMOUNT
T1E
T1M
T1H
T2S5
T2S10
T2S20
T2S30C
```

```
[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log
```

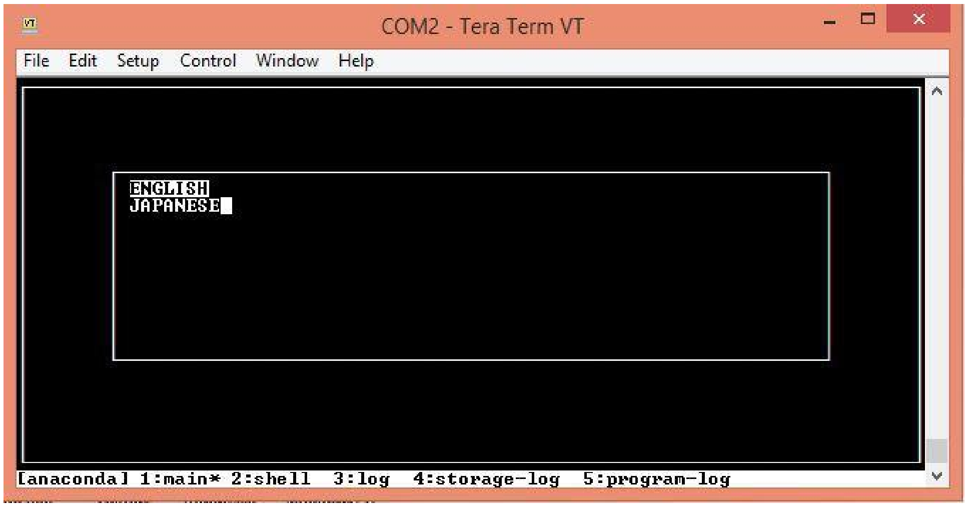
14. Now goto ‘Select a Brand’ and choose Seqrite to install Seqrite UTM



```
SEQRITE
```

```
[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log
```

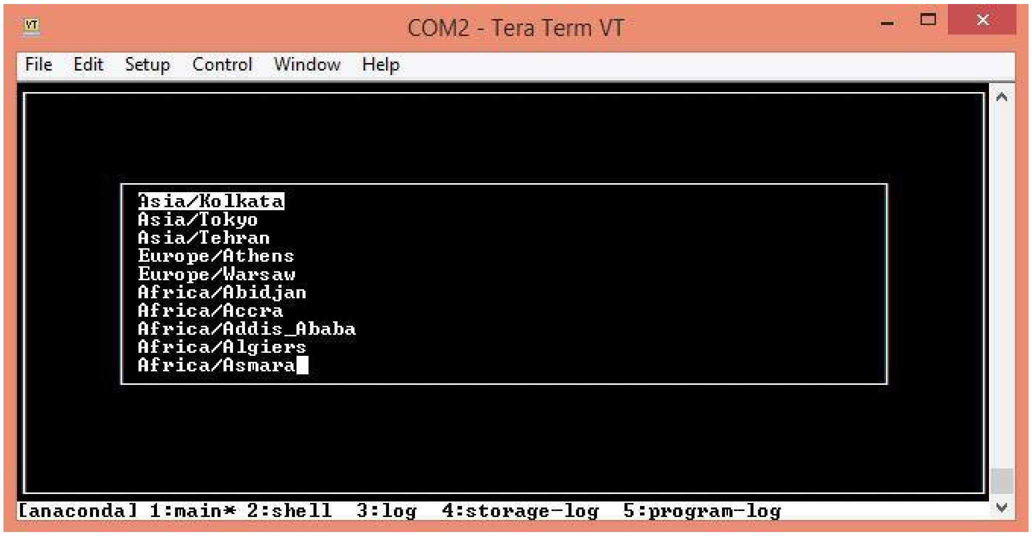
15. Now choose ‘Select a Language’ and select *English*.



```
ENGLISH
JAPANESE
```

```
[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log
```

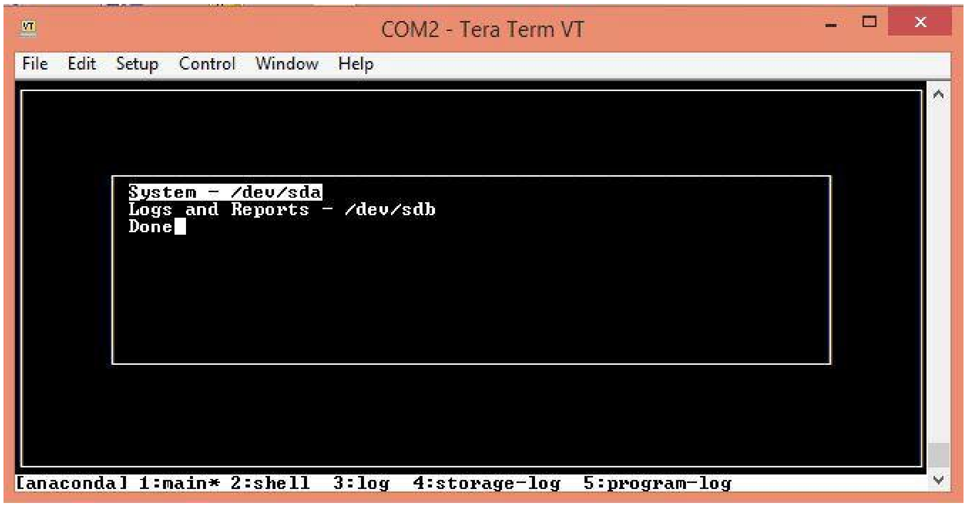
16. Go to *Select a Time zone* and select *Asia/Kolkata* for Indian time zone.



```
Asia/Kolkata
Asia/Tokyo
Asia/Tehran
Europe/Athens
Europe/Warsaw
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara
```

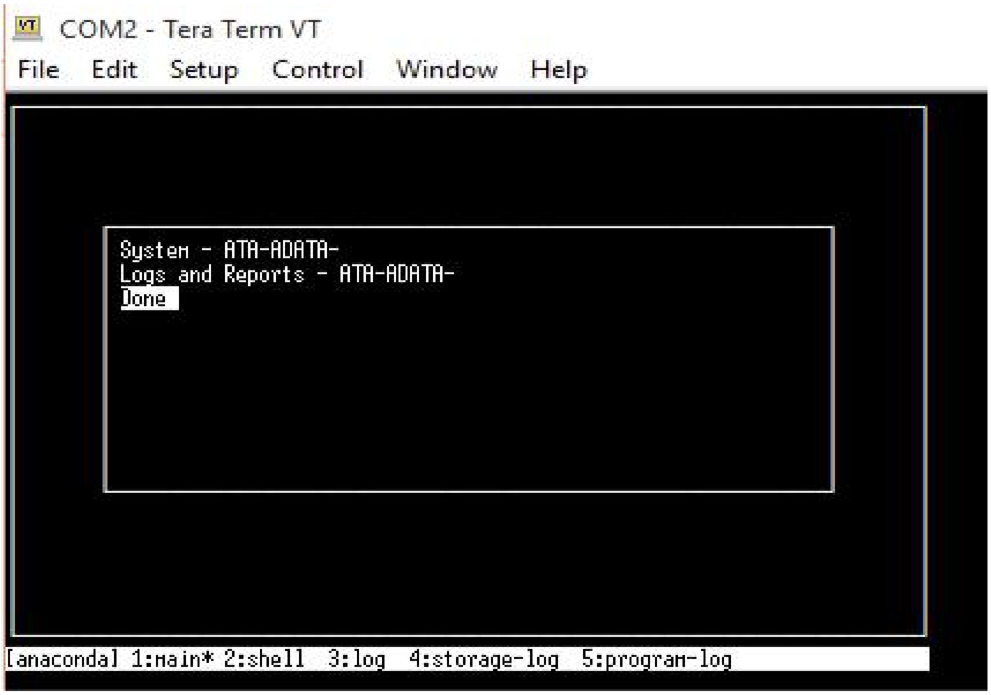
```
[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log
```

17. *Choose 'Select a storage device' and select option who has prefix ATA for System*



```
System - /dev/sda
Logs and Reports - /dev/sdb
Done

[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log
```

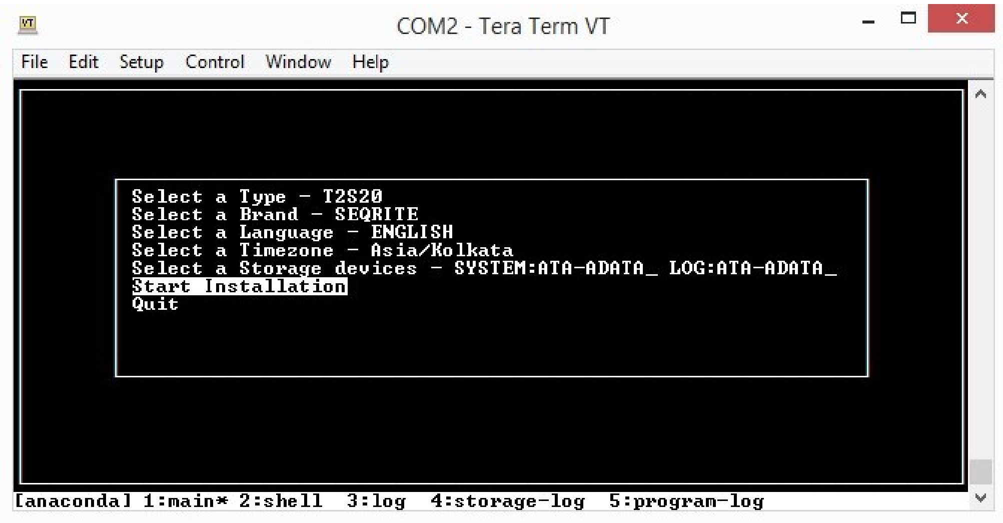
18. Select the same ATA device for *Logs and Reports* too. The screen would like the following for devices with Adata.



```
System - ATA-ADATA-
Logs and Reports - ATA-ADATA-
Done

[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log
```

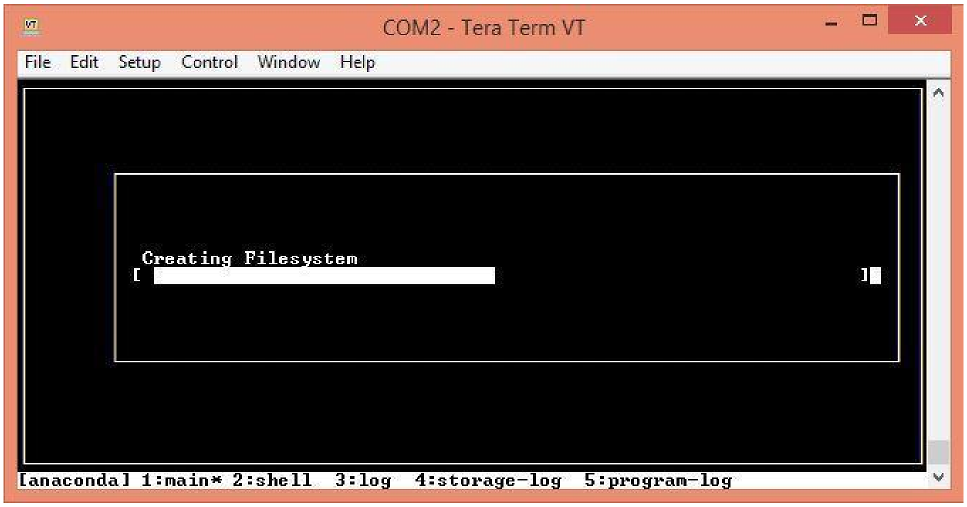
19. Note that devices with Cactus CF would have '*ATA-CACTUS*' while those with Sandisk (Old devices) would have 'ATA-Sandis' (not supported anymore) as the option. For T2M-250 with Intel SSDs, it would be ATA-Intel.

20. Click on Done to exit from storage device menu.



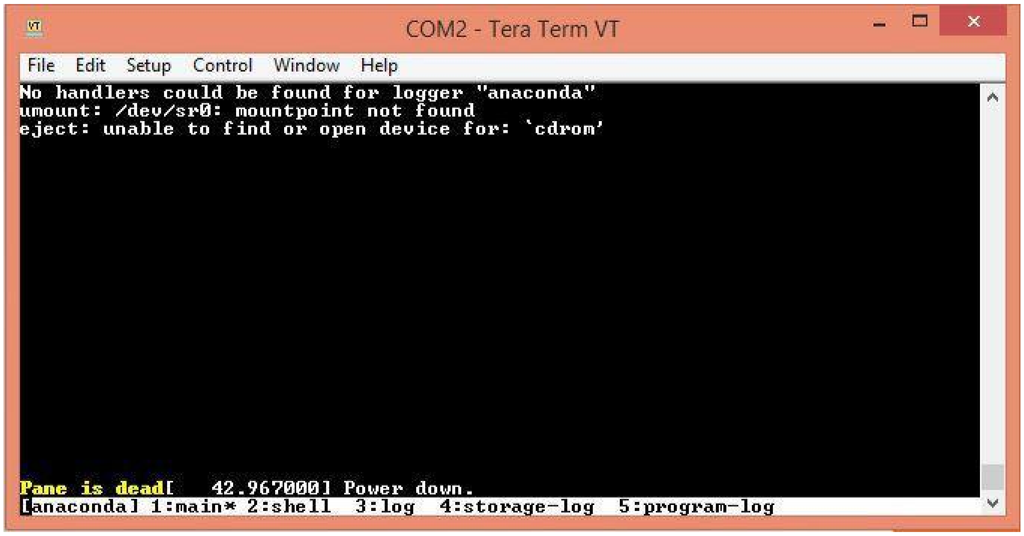
```
Select a Type - T2S20
Select a Brand - SEQRITE
Select a Language - ENGLISH
Select a Timezone - Asia/Kolkata
Select a Storage devices - SYSTEM:ATA-ADATA_ LOG:ATA-ADATA_
Start Installation
Quit

[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log
```

21. Verify all the values selected. Now select Start Installation.



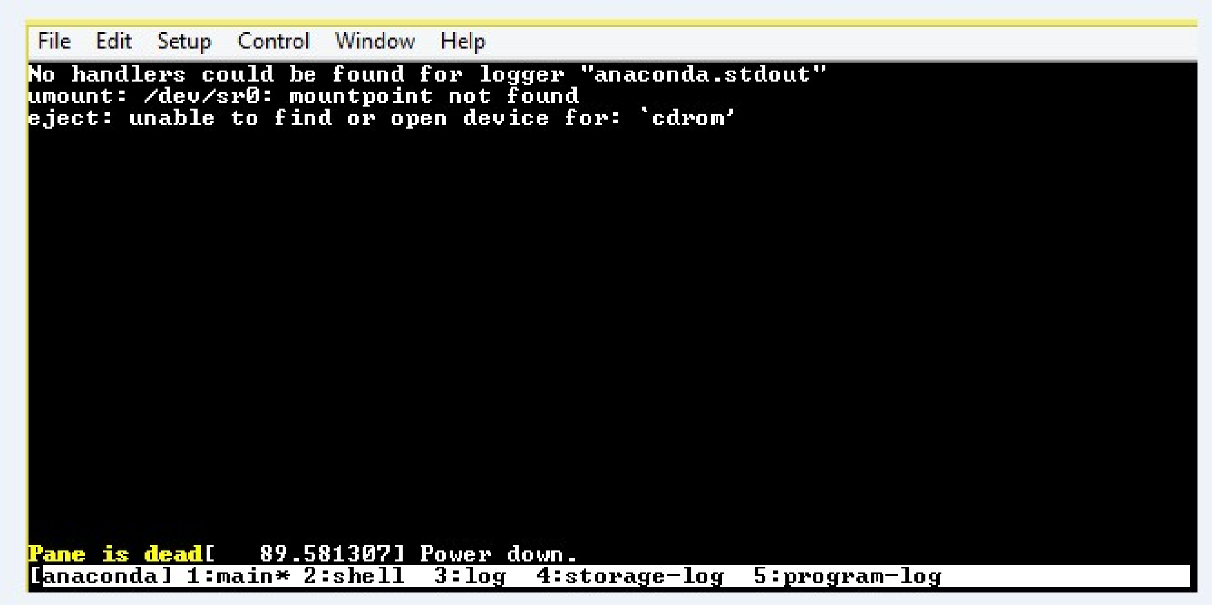
```
Creating Filesystem
[                                                  ]

[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log
```

22. After installation is done, UTM will reboot and once again will go to UTM installation menu (As boot device priority remain same for USB). Once you see the menu, select on Quit. You would error for eject command saying ‘unable find or open device for : cdrom’. Ignore this message.



```
No handlers could be found for logger "anaconda"
umount: /dev/sr0: mountpoint not found
eject: unable to find or open device for: `cdrom'





Pane is dead[   42.967000] Power down.
[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log
```

23. After selecting Quit, message will be visible as 'Pane is dead'. Now turn off the UTM, remove USB and restart the UTM. You will see screen as follows:



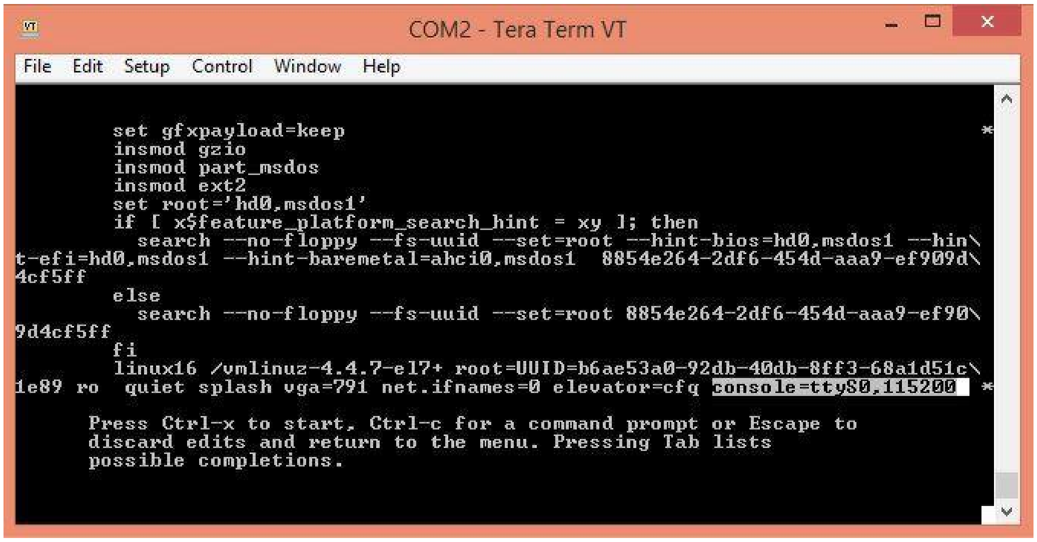
```
No handlers could be found for logger "anaconda.stdout"
umount: /dev/sr0: mountpoint not found
eject: unable to find or open device for: `cdrom'





Pane is dead[   89.581307] Power down.
[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log
```

24. Wait till UTM reboot two times and then login prompt will appear.

25. If you are installing on T1 series of device, after Step 22, in order to see the login prompt, you need to press 'e' to enter into grub menu and make changes in grub. This need to be done for each reboot.

26. To modify grub, do the following.

Scroll down to line which starts with 'linux16', press button 'end' to reach end of the line and type *'console=ttyS0,115200'* as shown above and press Cntrl+x. After this step, you would see further installation process and after two reboot you can see login screen.



```
        set gfxpayload=keep                                                *
        insmod gzio
        insmod part_msdos
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hin\
t-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1  8854e264-2df6-454d-aaa9-ef909d\
4cf5ff
        else
          search --no-floppy --fs-uuid --set=root 8854e264-2df6-454d-aaa9-ef90\
9d4cf5ff
        fi
        linux16 /vmlinuz-4.4.7-el7+ root=UUID=b6ae53a0-92db-40db-8ff3-68a1d51c\
1e89 ro  quiet splash vga=791 net.ifnames=0 elevator=cfq console=ttyS0,115200  *

      Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
      discard edits and return to the menu. Pressing Tab lists
      possible completions.
```

27. Once login screen is visible, login as *admin* to change IP address from the default if required.

28. To register device, connect ethernet cable to eth0 and access UTM with IP http://192.168.1.1:88. This is default IP address assigned to UTM post installation. Make sure you do not have any other device with same IP as this.

Supported Devices

Following hardware devices are supported in 2.3

- T1S
- T1M
- T1E *
- T2S-5
- T2S-10
- T2S20
- T2S-30C
- T2S-30
- T2S-60
- T2M-100
- T2M-250
- T2E-500
- NGS-130
- T1E 10 port device although supported, requires an extra step of manually rebooting the device once after the installation is over.

- ### Via Firmware upgrade functionality

Important: Firmware upgrade is a critical operation that affects the software of the UTM device. Please backup your configuration, critical logs and reports before proceeding with firmware upgrade.

To apply 2.3, Admin must manually download and Install the upgrade via System->Firmware Upgrade option.
Following are steps to install 2.3 firmware online for 2.3 GA:

1. Login to the UI and navigate to the path System -> Firmware Upgrade
2. Under Firmware List, under Actions column, Choose the option 'Download & Install' to install the firmware immediately.
3. <u>NOTE:</u> If you do not have internet connection on the UTM, then you can also perform an offline firmware upgrade. An offline upgrade file can be made available to you by our support team.

NOTE:
If the UTM devices are on 2.2 version lower than 2.2.7.1, then Admin must apply update to bring it to 2.2.7.1 version first; so that upgrade to UTM 2.3 could be done.

Help and support information

For more details on how to use the features and other relevant information, refer to the Help section of Seqrite UTM. For additional technical support, consult the Seqrite UTM technical support center.

Seqrite Support Contact information:

Phone Support: India Toll Free - 1800 212 7377
E-mail Support: utmsupport@seqrite.com
For International support contacts, Web or Chat Support options please visit:
https://www.seqrite.com/seqrite-support-center/